

ВЫСШЕЕ

ОБРАЗОВАНИЕ

А. П. Горюшкин

АБСТРАКТНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

Учебник

УМО ВО
РЕКОМЕНДУЕТ

 **Юрайт**
PUBLISHED BY

А. П. Горюшкин

АБСТРАКТНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

УЧЕБНИК ДЛЯ ВУЗОВ

*Рекомендовано Учебно-методическим отделом высшего образования в качестве
учебника для студентов высших учебных заведений, обучающихся
по математическим, ИТ-направлениям*



Курс с практическими заданиями и дополнительными материалами
доступен на образовательной платформе «Юрайт»,
а также в мобильном приложении «Юрайт.Библиотека»

Москва • Юрайт • 2024

УДК 512(075.8)
ББК 22.14я73
Г71

Автор:

Горюшкин Александр Петрович — кандидат физико-математических наук, доцент, профессор кафедры математики и физики физико-математического факультета Камчатского государственного университета имени Витуса Беринга (г. Петропавловск-Камчатский).

Рецензенты:

Фещенко Л. К. — кандидат физико-математических наук, доцент кафедры математики и физики физико-математического факультета Камчатского государственного университета имени Витуса Беринга (г. Петропавловск-Камчатский);

Паровик Р. И. — доктор физико-математических наук, профессор кафедры математики и физики, декан физико-математического факультета Камчатского государственного университета имени Витуса Беринга (г. Петропавловск-Камчатский).

Горюшкин, А. П.

Г71 Абстрактная и компьютерная алгебра : учебник для вузов / А. П. Горюшкин. — Москва : Издательство Юрайт, 2024. — 691 с. — (Высшее образование). — Текст : непосредственный.

ISBN 978-5-534-14085-9

В основу издания положен курс лекций по дисциплине «Элементы абстрактной и компьютерной алгебры», читавшийся автором в течение ряда лет для студентов различных специальностей Камчатского государственного университета имени Витуса Беринга. Издание представляет собой систематическое изложение основ классической алгебры с краткими, но полными доказательствами и с обсуждением особенностей методики компьютерного изучения алгебраических объектов. В качестве компьютерных математических программ выбран наиболее приспособленный для обработки символьных данных пакет компьютерных математических программ Maple. Представлены все основные задачи, связанные с машинным исследованием групп подстановок, абстрактных групп, кольца целых чисел, и его гомоморфных образов, а также колец многочленов от одного и нескольких переменных.

Соответствует актуальным требованиям федерального государственного образовательного стандарта высшего образования.

Для студентов вузов, обучающихся по направлению подготовки «Педагогическое образование», профилю «Информатика». Может быть полезным для студентов других направлений подготовки, имеющих в государственном образовательном стандарте дисциплины «Информатика», «Математика», «Элементы абстрактной и компьютерной алгебры», а также для отдельных специальностей СПО, учителей математики и информатики и учащихся старших классов гимназий и лицеев.

УДК 512(075.8)

ББК 22.14я73

Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

ISBN 978-5-534-14085-9

© Горюшкин А. П., 2021

© ООО «Издательство Юрайт», 2024

Оглавление

Предисловие	5
Введение.....	7
Тема 1. Группы, кольца, поля, булевы алгебры	13
1.1. Полугруппы.....	13
1.2. Моноиды.....	20
1.3. Группы	23
1.4. Кольца.....	37
1.5. Поля	51
1.6. Поле комплексных чисел.....	57
1.7. Булевы алгебры	73
Контрольные задания	82
Тема 2. Алгебры и алгебраические системы	83
2.1. Отношения	83
2.2. Функция.....	91
2.3. Порядок	99
2.4. Эквивалентность.....	108
2.5. Мощность	122
2.6. Алгебры	143
Контрольные задания	152
Тема 3. Целые числа и кольца классов вычетов.....	153
3.1. Отношение делимости	153
3.2. Идеалы в кольце целых чисел	159
3.3. Строение мультипликативной полугруппы натуральных чисел...	172
3.4. Диофантовы уравнения первой степени.....	181
3.5. Гомоморфный образ кольца целых чисел.....	186
3.6. Вычисления в гомоморфных образах.....	195
Контрольные задания	218
Тема 4. Подгруппы и фактор-группы	219
4.1. Простейшие свойства подгрупп.....	219
4.2. Циклические подгруппы	233
4.3. Смежные классы и сравнимость по модулю подгруппы	241
4.4. Гомоморфизмы и нормальные делители.....	249
4.5. Абелевы, разрешимые и нильпотентные группы.....	260
4.6. Преобразования множеств и группы преобразований.....	269
Контрольные задания	279

Тема 5. Подкольца и фактор-кольца.....	281
5.1. Подалгебра кольца	281
5.2. Прямое произведение колец.....	291
5.3. Гомоморфизмы колец.....	297
5.4. Свойства делимости в целостном кольце.....	307
5.5. Свойства колец.....	315
Контрольные задания	336
Тема 6. Многочлены	338
6.1. Многочлены над целостными кольцами	338
6.2. Теория делимости в кольце многочленов.....	350
6.3. Сохранение гауссовости при переходе к кольцу многочленов.....	358
6.4. Многочлены над числовыми полями	366
6.5. Многочлены от нескольких переменных	415
6.6. Дискриминант и результатant	428
Контрольные задания	446
Тема 7. Строение полей	448
7.1. Простые расширения полей	448
7.2. Конечные расширения полей.....	457
7.3. Алгебраические расширения	463
7.4. Разрешимость алгебраических уравнений в радикалах.....	468
7.5. Конечные поля.....	483
7.6. Первоначальное представление о теории кодирования.....	492
Контрольные задания	507
Тема 8. Компьютерное исследование групп.....	509
8.1. Исследование групп подстановок.....	509
8.2. Подгруппы конечной группы.....	520
8.3. Подгруппы с особыми свойствами	530
8.4. Фактор-группы	554
8.5. Исследование абстрактной группы	556
8.6. Копредставления и группы подстановок.....	579
Контрольные задания	607
Тема 9. Компьютерное исследование колец.....	608
9.1. Машинные вычисления в кольце целых чисел.....	608
9.2. Машинные вычисления в кольце классов вычетов.....	622
9.3. Машинные вычисления в кольце многочленов	626
9.4. Дифференцирование и интегрирование.....	633
9.5. Корни многочленов и связанные с ними задачи	648
Контрольные задания	669
Глоссарий алгебры	670
Библиографический список	679
Приложение	680

Предисловие

Методы абстрактной алгебры в настоящее время находят широчайшее применение в самых разных разделах фундаментальной и прикладной математики. Важными сферами приложений абстрактной алгебры стали создание и использование электронно-вычислительных машин (ЭВМ), разработка средств хранения, передачи и переработки информации. Абстрактная алгебра — дисциплина, являющаяся фундаментальной математической основой развития операционного мышления, позволяющего наименьшими средствами достигать наилучших результатов в любой области исследования, связанной с применением компьютера.

Изучение абстрактной и компьютерной алгебры является обязательным элементом подготовки специалистов ВПО и СПО по прикладной математике и информатике, инженеров и техников, занимающихся разработкой ЭВМ. Вне сомнения, в ближайшем будущем и в средней школе будут использоваться различные символьные пакеты компьютерной алгебры, а отдельные элементы абстрактной алгебры войдут в программы профильной школы. Ознакомление с основами абстрактной и компьютерной алгебры является важной составляющей в подготовке как будущего учителя информатики, так и инженера, техника, связанных с проектированием ЭВМ.

Изучение дисциплины «Абстрактная и компьютерная алгебра» направлено на формирование профессиональной компетенции: готовность реализовывать образовательные программы по учебному предмету в соответствии с требованиями образовательных стандартов.

Студент, изучивший дисциплину, должен:

знать

- основные понятия фундаментальной и компьютерной алгебры;
- определения и свойства математических объектов в этой области;
- формулировки основных утверждений, методы их доказательства;
- возможные сферы приложений алгебраических абстракций, необходимых для успешного изучения математических и теоретико-информационных дисциплин, решения задач, возникающих в информатике и других профессиональных сферах;

уметь

- применять методы алгебры для решения математических задач, построения и анализа моделей в прикладных задачах математики и информатики;
- решать задачи вычислительного и теоретического характера в области фундаментальной и компьютерной алгебры;
- доказывать основные результаты;
- производить необходимые вычисления в одной из систем компьютерной математики;

владеть

- математическим аппаратом фундаментальной и компьютерной алгебры;
- методами решения типовых задач и доказательства утверждений в этой области;
- методикой построения, анализа и применения математических моделей для прикладных задач математики и информатики;
- навыками применения современного математического инструментария для решения задач математики и информатики;
- методами вычислений в наиболее употребительных системах компьютерной математики.

Введение

1. Что изучает алгебра?

Объектом изучения математики являются множества с операциями и отношениями. Множество с операциями и отношениями называют *алгебраической системой*.

Если на множестве заданы одни операции, то систему принято называть *алгеброй*. Множество с отношениями называется *моделью*.

Понятие алгебраической системы носит общий, можно сказать, философский характер. Любая другая наука (в частности, математика,) изучает, по существу, только алгебраические системы. Более того, весь окружающий мир и мы сами представляем собой собрание каких-то элементов (клеток, атомов, элементарных частиц), находящихся в каких-то отношениях (иногда функциональных).

Нет в мире ничего, кроме алгебраических систем.

Особенность алгебры в том, что эта наука имеет своим объектом изучения не единственную алгебру или единственную систему. Отличие алгебры-науки от других наук (в том числе математических) заключается в том, что алгебра изучает целые классы алгебр и алгебраических систем.

Ответ на вопрос «Что изучает алгебра?» выглядит как игра слов: «Алгебра изучает алгебры». В этом предложении первое слово «алгебра» означает алгебру-науку, а второе — алгебры — множества с операциями.

Обычно множество A и алгебру, определенную на A , обозначают одним и тем же символом. Если f_1, f_2, \dots, f_n — набор операций (различных местностей) на множестве A , то алгебру A обычно записывают в виде

$$A = \langle A; f_1, f_2, \dots, f_n \rangle.$$

Кроме операций, на A могут быть определены и отношения (тоже различных местностей) R_1, R_2, \dots, R_m . Тогда

$$A = \langle A; f_1, f_2, \dots, f_n, R_1, R_2, \dots, R_m \rangle$$

является алгебраической системой¹.

¹ От греч. *συστήμα* — «состоящее из частей».

Например, множество натуральных чисел с операциями сложения и умножения образует алгебру

$$N = \langle N; +, \cdot \rangle$$

натуральных чисел. Эта алгебра с отношениями порядка и делимости превращается в (алгебраическую) систему натуральных чисел

$$N = \langle N; +, \cdot; \leq, | \rangle.$$

Именно эту систему обычно называют *арифметикой*.

Символы операций и отношений алгебраической системы называют *сигнатурой*, а их местности — *типом*. Например, сигнатура алгебраической системы $\langle N; +, \cdot; \leq, | \rangle$ — это $\{ +, \cdot; \leq, | \}$, а ее типом является $(2, 2; 2, 2)$.

Операции — это частные случаи отношений. Поэтому и алгебры, и алгебраические системы являются частными случаями моделей.

2. Что означает слово «абстрактная»?

Некоторые, различные с виду математические системы по существу одинаковы.

Что значит «по существу»?

Из-за разных обстоятельств и элементы, и операции, и отношения математической системы могут иметь различные названия и обозначения.

Пусть $A_1 = \langle A_1; \circ \rangle$ и $A_2 = \langle A_2; \bullet \rangle$ — две алгебры с одной двухместной операцией каждая, а φ — взаимно однозначное отображение множества A_1 на A_2 . Отображение φ *сохраняет операцию*, если для каждых элементов x, y из множества A_1

$$\varphi(x \circ y) = \varphi(x) \bullet \varphi(y).$$

Аналогично определяется сохранение операций меньших и больших местностей. Например, если g — одноместная операция в алгебрах A_1 и A_2 , то сохранение операции и отображении φ означает, что для каждых x из A_1

$$\varphi(g(x)) = g(\varphi(x)).$$

Если g — это n -одноместная операция в алгебрах A_1 и A_2 , то отображение φ сохраняет g — это значит, что для каждых x_1, x_2, \dots, x_n , из A_1

$$\varphi(g(x_1, x_2, \dots, x_n)) = g(\varphi(x_1), \varphi(x_2), \dots, \varphi(x_n)).$$

Отображение, сохраняющее все операции алгебры, называют *гомоморфизмом*.

Пусть $M_1 = \langle M_1; R \rangle$ и $M_2 = \langle M_2; R \rangle$ — две модели с одним двухместным отношением R , а φ — отображение множества M_1 на M_2 . Отображение φ является *гомоморфизмом* моделей, если φ сохраняет отношение (для любых элементов x, y из M_1): из истинности предложения $x R y$ следует истинность $\varphi(x) R \varphi(y)$:

$$x R y \Rightarrow \varphi(x) R \varphi(y).$$

В случае *изоморфизма* моделей для сохранения отношения требуется более жесткое правило (для любых элементов x, y из M_1):

$$x R y \Leftrightarrow \varphi(x) R \varphi(y).$$

Аналогично определяется сохранение отношений других местностей.

Гомоморфизм — частный случай отображения, поэтому он может быть взаимно однозначным **в** (внутри множества) или взаимно однозначным **на** (на все множество). Множества A_1 и A_2 могут совпадать, и тогда получатся гомоморфизмы *в себя*. Соответствующие названия приведены в следующей таблице.

Вид морфизма	Свойства отображения
Гомоморфизм	Отображение, сохраняющее операции
Мономорфизм	Взаимно однозначный гомоморфизм в
Эпиморфизм	Гомоморфизм на
Изоморфизм	Мономорфизм и эпиморфизм одновременно
Эндоморфизм	Гомоморфизм в себя
Автоморфизм	Изоморфизм на себя

При сохранении операций имеют в виду главные операции алгебры, занесенные в сигнатуру. Некоторые операции алгебры могут определяться в аксиомах (как, например, нульместная операция «нейтральный элемент» или одноместная — «взятие обратного элемента»).

Неглавные операции алгебры тоже сохраняются при гомоморфизме *на*, т. е. эпиморфизм переводит нейтральный элемент в нейтральный, поглощающий — в поглощающий, обратный — в обратный, противоположный — в противоположный.

Свойство алгебр или алгебраических систем называют *абстрактным*, если оно сохраняется при изоморфизме. Точнее говоря, свойство абстрактно, если из того, что им обладает некоторая алгебраическая система, следует, что этим свойством обладают и все системы, с ней *изоморфные*.

Изоморфные алгебры обладают одинаковыми свойствами — любое утверждение, доказанное для одной алгебры, автоматически выполняется для любой алгебры, ей изоморфной.

Науку алгебру называют *общей* (или *абстрактной*) потому, что она изучает лишь абстрактные свойства.

3. Подалгебры

Пусть A — алгебра, f — одна из ее операций, а H — непустое подмножество множества A . Подмножество H *замкнуто* относительно f , если для любых элементов a_1, a_2, \dots, a_n из H элемент $f(a_1, a_2, \dots, a_n)$ снова принадлежит H .

Например, если \circ — двухместная операция в алгебре, то замкнутость H относительно этой операции означает, что

$$a \in H, b \in H \Rightarrow a \circ b \in H.$$

Если H является алгеброй того же типа и удовлетворяет тем же аксиомам, что и алгебра A , то H называют *подалгеброй* алгебры A .

Для того чтобы подчеркнуть, что H — не просто подмножество множества A ($H \subset A$), но и подалгебра, используют символику $H < A$, где знак $<$, похожий на строгое числовое неравенство, используется так же, как и знак \subset , т. е. не обязательно в строгом смысле (H может и совпадать с A).

Множество подалгебр упорядочено отношением включения. Наибольшим элементом в таком порядке является множество — носитель самой алгебры. Наименьшего элемента, т. е. подалгебры, содержащейся в каждой подалгебре, может и не существовать.

Отношение «быть подалгеброй» является отношением частичного порядка.

В любой алгебре пересечение любой совокупности подалгебр или пусто, или является подалгеброй.

Объединение возрастающей цепочки подалгебр

$$A_1 < A_2 < \dots < A_n < \dots$$

алгебры A является подалгеброй.

Дело в том, что в операции алгебры участвует конечное число элементов, поэтому все они находятся в некотором звене этой цепи, а значит, и результат операции, примененной к этим элементам, лежит там же.

Пусть M — непустое подмножество алгебры A . Рассмотрим пересечение всех подалгебр алгебры A , содержащих множество M . Пересечение всех подалгебр алгебры A , содержащих множество M , является наименьшей подалгеброй, содержащей M .

Наименьшая подалгебра, содержащая множество M , называется *подалгеброй, порожденной множеством M* . Эту подалгебру обозначают в разных ситуациях символом $gr(M)$, или $алг(M)$, или просто (M) — буквы «алг» в конкретных случаях заменяются сокращенными названиями изучаемых алгебр.

Случайно этой подалгеброй может оказаться вся алгебра A .

Если у алгебры найдется конечное порождающее множество, то алгебру называют *конечно порожденной*.

В алгебре могут выполняться какие-то соотношения между порождающими элементами (такие соотношения называют определяющими), или даже тождества. Например, в алгебре $N = \langle N; +, \cdot \rangle$ обе операции *ассоциативны* (в русской школе обычно говорят: «обладают сочетательным свойством») и коммутативны (в русской школе коммутативность принято называть переместительным свойством).

Если алгебра A конечно порождена, то каждая возрастающая цепочка подалгебр

$$A_1 < A_2 < \dots < A_n < \dots$$

алгебры A обрывается на конечном шаге.

Для некоторого класса алгебр возникает естественная проблема: как узнать для произвольного набора элементов a, a_2, \dots, a_m и произвольного элемента b , принадлежит элемент b подалгебре $gp(M)$ или нет.

В случае, когда существует алгоритм для решения такой задачи, говорят, что *проблема вхождения* в классе этих алгебр *алгоритмически разрешима*.

4. Классификация алгебр

Алгебры классифицируются по числу и свойствам операций.

Важнейшими алгебрами с одной операцией являются *группы* (и их обобщения — *полугруппы* и *моноиды*), а важнейшие алгебры с двумя операциями — это *кольца* (и частные случаи колец — *поля* и *тела*).

Определение и свойства важнейших алгебраических алгебр будут обсуждаться в первой же теме.

Пока зададим следующий вопрос...

5. Что значит «Изучить алгебраическую систему»?

Любой реальный или идеальный объект фактически является алгебраической системой (или алгеброй). Поэтому сущность алгебры (как науки) состоит не в выборе объекта изучения, а в методе исследования алгебраической системы.

Изучение алгебры A алгебраическим методом состоит в исследовании *внутреннего устройства* алгебры A и ее *внешних связей*.

Изучение внутреннего устройства алгебры — это исследование свойств решетки (или полурешетки) $L(A)$ подалгебр алгебры A .

Решетка $L(A)$ подалгебр алгебры A лишена жизни. Ее можно оживить, рассмотрев автоморфизмы алгебры. Тогда множество $L(A)$ будет отображаться в себя (может быть, на себя). Более точно, некоторые элементы решетки подалгебр будут перемещаться при автоморфизмах, некоторые переходят сами в себя, а другие вообще остаются неподвижными. Это значит, что с исследованием алге-

бры A связано изучение ее группы автоморфизмов $Aut(A)$. Полугруппа эндоморфизмов $End(A)$ алгебры A тоже может много сказать о ее внутренних свойствах.

Таким образом, понятия решетки, группы, полугруппы действительно являются важнейшими — эти алгебры *сопутствуют* изучению любой другой алгебры (или алгебраической системы).

Кроме внутреннего устройства алгебры A представляют интерес и ее *внешние связи*, т. е. все гомоморфизмы на однотипные алгебры.

Практически эта задача снова сводится к внутреннему устройству алгебры A , так как гомоморфное отображение A полностью определяется отношением *конгруэнции* на A , и описание гомоморфизмов (с точностью до изоморфизма) сводится к описанию конгруэнций исследуемой алгебры.

Итак, изучить алгебру (алгебраическую систему) A — это означает, в первую очередь, найти и исследовать сопутствующие структуры для A :

- 1) решетку $L(A)$ подалгебр алгебры A ;
- 2) группу $Aut(A)$ автоморфизмов алгебры A ;
- 3) полугруппу $End(A)$ эндоморфизмов алгебры A ;
- 4) конгруэнции алгебры A .

Ответить на такие и другие естественные вопросы (например, о числе элементов в алгебре, о выполнении в этой алгебре каких-либо тождеств и т. п.) часто бывает очень непросто.

Начиная с 1970-х гг. для решения алгебраических проблем пришли на помощь компьютеры и *компьютерная алгебра*.

6. Что такое «Компьютерная алгебра»?

В середине XX в. на стыке математики и информатики возникло и бурно развивается новое направление — *компьютерная, или символьная, математика*. Компьютерные пакеты символьных математических вычислений позволяют проводить формульные вычисления в различных областях математики и ее приложениях.

Компьютер освобождает исследователя от сложных и громоздких формульных вычислений и требует от него более глубоких предметных знаний и навыков владения символьными пакетами.

В основе представления значительной части символьных данных в компьютере лежат реализации алгоритмов абстрактной алгебры на языках программирования.

Среди разнообразных систем компьютерной алгебры особое место по доступности и возможностям применения занимает пакет символьных математических вычислений *Maple*, разработанный в университете Ватерлоо в Канаде.

Тема 1

ГРУППЫ, КОЛЬЦА, ПОЛЯ, БУЛЕВЫ АЛГЕБРЫ

Основные понятия: полугруппа, моноид, группа, комбинаторное представление группы, кольцо, поле, поле комплексных чисел, числовое поле, изоморфизм, мономорфизм, поле частных.

Основные факты: каждая конечная группа изоморфна группе подстановок, каждая группа изоморфно вложима в некоторое кольцо, все циклические группы одинакового порядка изоморфны, каждое целостное кольцо изоморфно вложимо в некоторое поле.

Обсудим определения и простейшие свойства таких алгебраических объектов, которые наиболее часто встречаются и плодотворно используются в математике и других областях науки и техники.

Среди алгебр с одной операцией важнейшими являются группы, среди алгебр с двумя операциями — кольца и частные случаи колец — поля.

Еще один важный математический объект, особенно полезный при изучении алгебры множеств и алгебры высказываний, — булева алгебра.

Группа — это фундаментальное понятие современной математики. Теория функций, топология, кристаллография, квантовая механика и другие области естествознания в настоящее время немыслимы без применения этого математического объекта.

Группа является частным случаем моноида, а тот, в свою очередь, — частным случаем полугруппы.

1.1. Полугруппы

Множество с одной ассоциативной операцией называется полугруппой. Иначе говоря, множество M с операцией \circ является полугруппой, если для любых элементов a, b, c из M

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

В обозначении обычно используется лишь символ множества-носителя полугруппы, т. е. говорят просто «полугруппа M », имея в виду $M = \langle M; \circ \rangle$.

Операция в полугруппе может называться сложением и обозначаться символом $+$. В этом случае говорят, что полугруппа записана *аддитивно*. Если операция в полугруппе является умножением, то полугруппа записана *мультипликативно*.

Приведем фрагмент аддитивно-мультипликативного словаря, используя терминологию школьного курса математики.

Аддитивный язык	Мультипликативный язык
Сложение	Умножение
$+$	\cdot
Сумма	Произведение
Слагаемые	Сомножители
Вычитание	Деление
Делимое	Уменьшаемое
Делитель	Вычитаемое
Разность	Частное
Ноль	Единица
0	1
Противоположный	Обратный
$-a$	a^{-1}
Кратное	Степень
na	a^n
Деление на n	Извлечение корня n -й степени
$\frac{a}{n}$	$\sqrt[n]{a}$

Произвольную полугруппу принято считать записанной *мультипликативно*, поэтому все основные свойства полугрупп (в частности, *моноидов* и *групп*) формулируются и доказываются, как правило, на мультипликативном языке.

Полугруппа Π называется полугруппой с делением, если каждое из уравнений $ax = b$ и $ya = b$ имеет единственное решение в Π для любых элементов a, b из Π .

Полугруппа $\langle \Pi; \cdot \rangle$ называется полугруппой с нулем, если в ней содержится аннулирующий (поглощающий) элемент, т. е. такой элемент 0, что для каждого x из Π выполняются тождества

$$x \cdot 0 = 0 \cdot x = 0.$$

Закон ассоциативности в мультипликативно записанной полугруппе означает, что значение произведения *трех* элементов полугруппы не зависит от расстановки скобок.

Число «три» можно заменить любым натуральным n и получить, таким образом, обобщенный закон ассоциативности: значение произведения $a_1 \cdot a_2 \cdot \dots \cdot a_n$ элементов полугруппы не зависит от расстановки скобок.

Индукцией по n — числу множителей — покажем, что любую расстановку скобок в произведении можно заменить левой расстановкой:

$$(\dots((a_1 \cdot a_2) \cdot a_3) \dots) \cdot a_{n-1} \cdot a_n.$$

База индукции ($n = 3$) — это сам закон ассоциативности.

Шаг индукции. Если $n > 3$ и

$$a_1 \cdot a_2 \cdot \dots \cdot a_n = A \cdot B,$$

то по индуктивному предположению расстановку скобок в A и B можно заменить левой расстановкой. Если $B = a_n$, то все доказано. Если

$$B = (\dots((a_k \cdot a_{k+1}) \cdot a_{k+2}) \dots) \cdot a_{n-1} \cdot a_n = C \cdot a_n,$$

то

$$AB = A(C \cdot a_n) = (A \cdot C)a_n.$$

По индуктивному предположению расстановку скобок в произведении AC можно заменить левой расстановкой. Шаг индукции и обобщенный закон ассоциативности доказаны.

Благодаря обобщенному закону ассоциативности можно говорить о *степени элемента*: значение произведения n одинаковых сомножителей не зависит от расстановки скобок.

Соответственно, в аддитивной записи можно говорить без всяких оговорок о расстановке скобок в сумме равных слагаемых (кратном элементе).

Кроме того, становится возможным использование символа $\prod_{i=1}^n a_i$, под которым понимается произведение $a_1 \cdot a_2 \cdot \dots \cdot a_n$, а в аддитивной записи соответственно¹

$$\sum_{i=1}^n \overset{\text{опр}}{a_i} = a_1 + a_2 + \dots + a_n.$$

Подалгебра полугруппы называется *подполугруппой*.

¹ Символ « $\overset{\text{опр}}{=}$ » означает «равно по определению».

Непустое подмножество H будет подполугруппой полугруппы $\langle P; \circ \rangle$ тогда и только тогда, когда оно замкнуто относительно операции, т. е.

$$x \in H, y \in H \Rightarrow x \circ y \in H.$$

Преобразованием множества называют любое отображение этого множества в себя. Последовательное выполнение (называемое еще композицией, или суперпозицией) отображений является ассоциативной операцией, и, таким образом, любое множество преобразований произвольного множества M , замкнутое относительно композиции, будет полугруппой относительно этой операции.

В частности, полугруппу образует множество всех преобразований множества M . Такая полугруппа называется симметрической полугруппой на множестве M .

Если множество M состоит из n элементов, то симметрическая полугруппа множества M содержит n^n элементов.

Если A — произвольная алгебра (или алгебраическая система), то гомоморфное отображение алгебры A в себя называют эндоморфизмом.

Эндоморфизм — это частный случай преобразования множества; следовательно:

1) множество $End(A)$ всех эндоморфизмов алгебры A в себя с операцией «композиция» образует полугруппу;

2) полугруппа $End(A)$ эндоморфизмов алгебры A является подполугруппой симметрической полугруппы множества A .

Это значит, что понятие полугруппы является ключевым при исследовании любой алгебры (или алгебраической системы).

При исследовании алгебры необходимо изучить полугруппу ее эндоморфизмов.

Две полугруппы $\langle A; \circ \rangle$ и $\langle B; \bullet \rangle$ называются изоморфными¹, если существует взаимно однозначное соответствие φ между элементами множеств A и B , сохраняющее операцию (для любых x, y из A):

$$\varphi(x \circ y) = \varphi(x) \bullet \varphi(y).$$

Взаимно однозначное отображение, сохраняющее операцию, называется изоморфизмом.

В качестве простейшего примера пары неизоморфных полугрупп можно указать числовые множества $M_1 = \{0, 1\}$ и $M_2 = \{-1, 1\}$ с обычным умножением. Если две полугруппы изоморфны, то на них одновременно выполняются или не выполняются любые тождества. Однако на множестве M_1 для любого элемента x верно равенство $x^2 = x$ (тождество идемпотентности); или говорят еще: «Все элементы

¹ От греч. *ισος* — «равный», *μορφη* — «вид, форма».

из M_1 идемпотенты». Однако в множестве M_2 элемент -1 идемпотентом не является.

Может случиться, что подполугруппа Π содержит изоморфный образ Π_2 полугруппы Π_1 . В таком случае говорят, что Π_1 изоморфно вложима в полугруппу Π . Взаимно однозначное отображение ν (внутрь) называют *мономорфизмом*¹. Таким образом, изоморфизм — это частный случай мономорфизма.

Отображение, сохраняющее операцию, но не обязательно взаимно однозначное, называется *гомоморфизмом*². Гомоморфный (в частности изоморфный) образ полугруппы является полугруппой.

Элементы x, y называют *перестановочными* (или *коммутирующими*), если

$$x \cdot y = y \cdot x.$$

Например, в любой полугруппе степени одного и того же элемента x перестановочны (для любых целых чисел i, j):

$$x^i \cdot x^j = x^{i+j} = x^j \cdot x^i.$$

Полугруппа, в которой любые два элемента перестановочны, называется *коммутативной*. Если полугруппа состоит из натуральных степеней одного и того же элемента (ее называют тогда *моногенной*, или *циклической*), то она коммутативна. Все числовые (и аддитивные, и мультипликативные) полугруппы тоже коммутативны.

Закон коммутативности в полугруппе означает, что значение произведения двух элементов полугруппы не зависит от перестановок сомножителей.

Вместо двух можно взять любое число сомножителей и с помощью индукции по числу множителей получить *обобщенный закон коммутативности*: значение произведения $a_1 \cdot a_2 \cdot \dots \cdot a_n$ элементов коммутативной полугруппы не зависит от перестановок сомножителей.

Благодаря обобщенным законам ассоциативности и коммутативности становится возможным использование символов $\sum_{i \in I} a_i$ и $\prod_{i \in I} a_i$, где I — некоторое (может быть неупорядоченное) множество индексов.

Подполугруппа, порожденная множеством M , является пересечением всех подполугрупп полугруппы Π , содержащих M , а ее элементы — всевозможные произведения элементов из M . Любая полугруппа обладает порождающим множеством; например, в качестве такового можно просто взять все ее элементы.

¹ От греч. *μονος* — «один», *морфη* — «вид, форма».

² От греч. *ομος* — «подобный», *морфη* — «вид, форма».

Равенства $u = w$, где u, w — некоторые произведения порождающих элементов полугруппы, называют *соотношениями* полугруппы. Например, соотношения вида $ab = c$, где a, b пробегает всю полугруппу, полностью задают полугруппу. Однако в действительности для задания полугруппы вовсе нет необходимости переписывать все произведения; все соотношения в полугруппе являются следствиями некоторого множества *определяющих соотношений*.

Запись

$$a_1, a_2, \dots, a_n; U_1 = W_1, U_2 = W_2, \dots, U_m = W_m >$$

означает, что полугруппа Π порождается элементами a_1, a_2, \dots, a_n и имеет определяющие соотношения

$$U_1 = W_1, U_2 = W_2, \dots, U_m = W_m$$

(n, m не обязательно конечны или даже счетны).

Можно считать, что элементами полугруппы Π являются всевозможные слова в алфавите a_1, a_2, \dots, a_n . Если X — произвольный элемент из Π и внутри X содержится подслово, являющееся левой или правой частью определяющего соотношения, то это подслово можно заменить второй частью соотношения. Например, элемент $X_1 W_1 X_2$ получен из элемента $X_1 U_1 X_2$ с помощью определяющего соотношения $U_1 = W_1$ (здесь X_1 или X_2 могут быть и пустыми).

Два элемента X и Y в полугруппе Π равны тогда и только тогда, когда их можно связать конечной цепочкой преобразований такого вида.

Если существует алгоритм для узнавания, равны или нет два произвольных элемента полугруппы Π , то говорят, что в полугруппе Π разрешима *проблема* (равенства) *слов*.

Множество определяющих соотношений может быть пустым. В таком случае полугруппа называется *свободной*. Например, аддитивная полугруппа натуральных чисел — свободная моногенная полугруппа. Каждая полугруппа является гомоморфным образом некоторой свободной полугруппы.

Если $\Pi = \langle a_1, a_2, \dots, a_n \rangle$ — конечно порожденная свободная полугруппа, то два ее элемента U и W равны тогда и только тогда, когда в них совпадают все буквы. Другими словами, в свободной полугруппе алгоритмически разрешима *проблема слов*.

Проблема слов имеет алгоритмическое решение далеко не всегда. Например, для полугруппы

$$\begin{aligned} \Pi_1 = \langle a_1, a_2, a_3, a_4, a_5; a_1 a_3 = a_3 a_1, a_1 a_4 = a_4 a_1, a_2 a_3 = a_3 a_2; \\ a_2 a_4 = a_4 a_2, a_5 a_3 a_1 = a_3 a_5, a_5 a_4 a_2 = a_4 a_5, a_3 a_3 = a_3 a_3 a_1 a_5 \rangle \end{aligned}$$

проблема слов алгоритмически неразрешима. Это значит, что *никогда* никакая вычислительная техника ни по какой программе

не сможет распознавать, равны или нет два произвольно выбранных элемента из полугруппы Π_1 .

Пусть A и B — две мультипликативно записанные полугруппы. Рассмотрим декартово множество $A \times B$ и определим на нем операцию покомпонентно, т. е.

$$(a, b) \cdot (c, d) \stackrel{\text{опр}}{=} (a \cdot c, b \cdot d).$$

Новое умножение также будет ассоциативным, т. е. в результате получится полугруппа $A \times B$, называемая *прямым произведением полугрупп A и B* .

Например, мультипликативная полугруппа ненулевых целых чисел изоморфна прямому произведению полугрупп $A = \langle \{1, -1\}; \cdot \rangle$ и $B = \langle \mathbb{N}; \cdot \rangle$.

Если полугруппа A состоит из $|A|$ элементов, а полугруппа B — из $|B|$ элементов, то $A \times B$ содержит $|A| \cdot |B|$ элементов. В частности, прямое произведение конечных полугрупп снова является конечной полугруппой.

Прямое произведение коммутативных полугрупп снова коммутативно. Это значит, что свойство коммутативности сохраняется при прямом произведении. Вообще любое свойство, выражаемое тождеством (например, идемпотентности $x^2 = x$, нильпотентности $x^n = 0$ и т. п.) сохраняется при прямом произведении полугрупп.

Число полугрупп-сомножителей может быть и больше двух. Прямое произведение полугрупп A_1, A_2, \dots, A_n имеет своим множеством декартово произведение

$$A_1 \times A_2 \times \dots \times A_n.$$

Элементами декартова произведения являются n -ки элементов, т. е. всевозможные наборы (a_1, a_2, \dots, a_n) . Умножение этих наборов определяется так же, как и для пар, т. е. покомпонентно.

Если две полугруппы Π_1 и Π_2 представлены с помощью порождающих множеств и определяющих соотношений,

$$\Pi_1 = \langle a_1, a_2, \dots, a_n; U_1 = W_1, U_2 = W_2, \dots, U_m = W_m \rangle;$$

$$\Pi_2 = \langle b_1, b_2, \dots, b_k; S_1 = T_1, U_2 = W_2, \dots, U_l = W_l \rangle,$$

то прямое произведение этих полугрупп имеет представление:

$$\Pi_1 \times \Pi_2 = \langle a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_k;$$

$$U_1 = W_1, U_2 = W_2, \dots, U_m = W_m;$$

$$S_1 = T_1, U_2 = W_2, \dots, U_l = W_l,$$

$$a_i b_j = b_j a_i \ (i = 1, 2, \dots, n; \ j = 1, 2, \dots, k) \rangle.$$

1.2. Моноиды

Элемент e называется *нейтральным* в алгебре $\langle A; \cdot \rangle$, если для каждого элемента x из A

$$xe = ex = x.$$

Полугруппа с нейтральным элементом называется *моноидом*.

На мультипликативном языке нейтральный элемент обычно называют *единицей* и обозначают символом 1 (похожим на числовую единицу). На аддитивном языке нейтральный элемент называется *нулем* и обозначается символом 0.

Симметрическая полугруппа образует моноид. Единицей в этом моноиде является отображение $x \mapsto x$ переводящее каждый элемент x из исходного множества в себя.

Моноид можно задать как полугруппу с помощью порождающих множеств и определяющих соотношений, просто отдав роль нейтрального элемента одному из порождающих. Например, полугруппа, заданная представлением

$$\begin{aligned} \langle a_1, a_2, \dots, a_n; U_1 = W_1, U_2 = W_2, \dots, U_m = W_m, \\ a_1 a_i = a_i, a_i a_1 = a_i \ (i = 1, 2, \dots, n) \rangle \end{aligned}$$

является моноидом, а элемент a_1 в нем нейтральный.

Прямое произведение $A \times B$ моноидов A и B снова будет моноидом. Единицей в $A \times B$ является пара (e_1, e_2) , состоящая из единиц моноидов A и B соответственно.

Множество $\{(a, e_2) \mid a \in A\}$ образует подмоноид, изоморфный моноиду A , а подмоноид $\{(e, b) \mid b \in B\}$ изоморфен моноиду B .

Число прямых сомножителей-моноидов может быть любым, в том числе и бесконечным. Например, если $M_1, M_2, \dots, M_n, \dots$ — счетное число моноидов, то элементами прямого произведения $M_1 \times M_2 \times \dots \times M_n \times \dots$ являются всевозможные последовательности

$$(x_1, x_2, \dots, x_n, \dots)$$

элементов x_i из M_i , причем *почти все* (т. е. все, кроме конечного числа) элементы этих последовательностей являются нейтральными.

Именно так устроен мультипликативный моноид натуральных чисел. Прямыми сомножителями моноида $\langle \mathbb{N}; \cdot \rangle$ являются подмоноиды

$$\{2^k \mid k \in \mathbb{Z}_0\}, \{3^k \mid k \in \mathbb{Z}_0\}, \{5^k \mid k \in \mathbb{Z}_0\}, \dots, \{p_i^k \mid k \in \mathbb{Z}_0\}, \dots,$$

состоящие из всех неотрицательных степеней i -го простого числа.

В определении моноида говорится о *наличии* нейтрального элемента, но не утверждается, что такой элемент единственный. Однако *каждый моноид содержит единственный нейтральный элемент*.

Действительно, если e_1 и e_2 — два нейтральных элемента, то $e_1 e_2 = e_2$, так как e_2 нейтральный, и $e_1 e_2 = e_1$, так как e_1 нейтральный. Следовательно, $e_1 = e_2$.

Если φ — гомоморфизм моноида M на алгебру G и e — нейтральный элемент в M , то для каждого элемента x из M

$$\varphi(ex) = \varphi(e)\varphi(x) = \varphi(x) \text{ и } \varphi(xe) = \varphi(x)\varphi(e) = \varphi(x).$$

Это значит, что $\varphi(e)$ — нейтральный элемент в G .

Вместе с сохранением ассоциативности это означает, что гомоморфный (и, в частности, изоморфный) образ моноида сам является моноидом.

Моноид, содержащий более одного элемента, имеет по крайней мере один (тривиальный) гомоморфизм, не являющийся изоморфизмом. Это отображение, переводящее все элементы моноида в нейтральный элемент.

Моноид, не имеющий нетривиальных гомоморфизмов, называется *простым*.

Пусть M — моноид, H — непустое подмножество множества M . Если H замкнуто относительно операции, то H образует подполугруппу моноида M . Однако для того, чтобы быть подмоноидом, этого недостаточно. Например, множество четных чисел — это подполугруппа, но не подмоноид моноида $\langle \mathbb{N}; \cdot \rangle$: среди четных чисел нет нейтрального по умножению.

Обычно считают, что подполугруппа образует подмоноид, если она содержит нейтральный элемент всего моноида (т. е. нейтральный элемент представляет нульместную операцию моноида).

При таком договоре подмножество $\{0\}$ хотя и является моноидом, но не образует подмоноида моноида $\langle \{1, -1, 0\}; \cdot \rangle$.

Если полугруппа не содержит нейтрального элемента, т. е. не является моноидом, то ее легко превратить в моноид, просто дополнив ее множество-носитель нейтральным элементом.

Пусть Π — произвольная полугруппа без нейтрального элемента. Добавим к множеству Π новый элемент e и пополним таблицу умножения полугруппы дополнительными произведениями (для каждого элемента x из Π):

$$ex = xe = x, \quad ee = e.$$

Свойство ассоциативности умножения на расширенном множестве сохраняется, а новый элемент e является нейтральным.

Таким образом, каждая полугруппа изоморфно вложима в моноид.

Например, множество, состоящее из всех четных чисел и единицы, образует мультипликативный моноид, содержащий моноид четных чисел.

Пусть M — моноид с нейтральным элементом e . Каждому элементу g поставим в соответствие отображение φ_g множества M в себя, переводящее любой элемент x из M в xg :

$$\varphi_g : x \mapsto xg.$$

Благодаря ассоциативности отображение $\psi: g \mapsto \varphi_g$ сохраняет операцию:

$$\psi(uv) = \psi(u)\psi(v).$$

Для различных элементов u, v отображения φ_u и φ_v различны, так как

$$\varphi_u : e \mapsto u, \quad \varphi_v : e \mapsto v.$$

Таким образом, отображение ψ является мономорфизмом, или, другими словами, *каждый моноид изоморфно вложим в симметрическую полугруппу*.

Отсюда следует, что любая полугруппа Π изоморфна некоторой полугруппе преобразований множества M , где M — это множество Π , возможно, пополненное одним элементом.

Элемент a из моноида $M = \langle M; \cdot \rangle$ с нейтральным элементом e называется *обратимым*, если система уравнений

$$\begin{cases} a \cdot x = e, \\ x \cdot a = e \end{cases}$$

имеет решение в M .

На мультипликативном языке решение такой системы обозначают символом a^{-1} и называют элементом, *обратным для a* . На аддитивном языке роль обратного исполняет *противоположный элемент*.

Если x, y — два элемента, обратных для элемента a , то из $ax = e$ следует $uax = ue$, откуда $x = y$. Это значит, что *каждый элемент в моноиде имеет не более одного обратного*.

Предположим, что элемент a обратим в моноиде G , а φ — гомоморфное отображение моноида G на моноид G_1 . Равенства, имеющие вид $a^{-1} \cdot a = e$ и $a \cdot a^{-1} = e$ в моноиде G , в гомоморфном образе моноида превращаются в равенства

$$\varphi(a^{-1}) \cdot \varphi(a) = \varphi(e) \text{ и } \varphi(a) \cdot \varphi(a^{-1}) = \varphi(e).$$

Это значит, что гомоморфный образ обратимого элемента сам является обратимым:

$$\varphi(a^{-1}) = [\varphi(a)]^{-1}.$$

Допуская вольность речи, можно сказать, что обратный элемент при гомоморфизме переходит в обратный.

Нейтральный элемент является обратимым, поэтому множество обратимых элементов моноида не пусто, более того, оно содержит единичный элемент. Если x, y обратимы, то xy тоже обратим и

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Отсюда следует, что множество обратимых элементов моноида является подмоноидом.

Случайно может оказаться, что множество обратимых элементов моноида совпадает с самим моноидом. В таком случае моноид называют *группой*.

1.3. Группы

Группой называют моноид, в котором каждый элемент обратим. Напишем это важное определение подробно.

Алгебра $G = \langle G; \cdot \rangle$ — *группа*, если:

- 1) операция \cdot ассоциативна;
- 2) в G существует такой элемент e , что для каждого a из G

$$a \cdot e = e \cdot a = a;$$

- 3) для каждого элемента a из G существует такой элемент x в G , что

$$a \cdot x = x \cdot a = e.$$

Полугруппы $\langle \mathbb{Z}; + \rangle$, $\langle \mathbb{Q}; + \rangle$, $\langle \mathbb{R}; + \rangle$, $\langle \mathbb{C}; + \rangle$ — это аддитивные группы целых, рациональных, действительных и комплексных чисел; а $\mathbb{Q}^* = \langle \mathbb{Q} \setminus \{0\}; \cdot \rangle$, $\mathbb{Q}_+^* = \langle \mathbb{Q}_+ \setminus \{0\}; \cdot \rangle$, $\mathbb{R}^* = \langle \mathbb{R} \setminus \{0\}; \cdot \rangle$, $\mathbb{R}_+^* = \langle \mathbb{R}_+ \setminus \{0\}; \cdot \rangle$, $\mathbb{C}^* = \langle \mathbb{C} \setminus \{0\}; \cdot \rangle$ — мультипликативные числовые группы.

Подалгебра группы называется *подгруппой*.

Если H — подгруппа группы G , то символически это обычно записывают так: $H < G$, где знак $<$ означает не обязательно строгое включение.

Для того чтобы непустое H из группы $\langle G; \cdot \rangle$ было подгруппой, необходимо и достаточно, чтобы H было замкнуто относительно умножения и взятия обратного, т. е.

$$x \in H, y \in H \Rightarrow x \cdot y \in H, x^{-1} \in H.$$

Моноид — это частный случай полугруппы, а группа — частный случай моноида. Поэтому в группе выполняется обобщенный закон ассоциативности, в группе содержится единственный нейтральный элемент, и для каждого элемента есть в точности один обратный.



Алгебры с одной операцией

Иногда бывают полезными и классы алгебр с одной операцией, более широкие, чем класс полугрупп. Множество с одной двухместной операцией (на которую, вообще говоря, не наложено никаких условий) называется *группоидом*, а множество с одной *частичной* (т. е. не всюду определенной операцией) называют *затравкой*. Например, множество натуральных чисел с вычитанием — это всего лишь *затравка*, натуральные числа со сложением — *полугруппа*, целые неотрицательные числа со сложением — это *моноид*, а все целые числа со сложением — *группа*.

Вернемся к обсуждению свойств групп.

Группа является полугруппой с делением.

Действительно, в группе $xa = b$ и $ay = b$ имеют единственное решение для любых элементов a, b . Например, умножив равенство $xa = b$ на элемент a^{-1} , получим $x = ba^{-1}$. Из $x_1a = x_2a$ следует $x_1 = x_2$; поэтому решение такого уравнения единственно.

В то же время из однозначной разрешимости таких уравнений и ассоциативности операции следует существование единицы и обратного элемента.

Другими словами, *полугруппа с делением является группой*.

Докажем это утверждение. Пусть Π — полугруппа с делением. Тогда для любого элемента a найдется единственная правая единица $1_{a, \text{пр}}$, т. е.

$$a \cdot 1_{a, \text{пр}} = a.$$

Если b — другой элемент из Π , то найдется такой элемент x , что $xa = b$. Тогда

$$b \cdot 1_{a, \text{пр}} = (xa) \cdot 1_{a, \text{пр}} = x(a \cdot 1_{a, \text{пр}}) = xa = b.$$

Таким образом, правая единица $1_{\text{пр}}$ для одного элемента из Π является правой единицей и для всех остальных. Точно так же найдется общая для всех левая единица $1_{\text{лв}}$. Теперь из равенств

$$1_{\text{лв}} \cdot 1_{\text{пр}} = 1_{\text{пр}} \text{ и } 1_{\text{лв}} \cdot 1_{\text{пр}} = 1_{\text{лв}}$$

следует

$$1_{\text{пр}} = 1_{\text{лв}}.$$

Итак, в полугруппе с делением содержится единичный элемент.

Теперь остается показать, что левый обратный для каждого элемента является одновременно и правым обратным. Пусть $xa = 1$ и $ay = 1$. Тогда из равенств

$$xay = (xa)y = 1 \cdot y;$$

$$xay = x(ay) = x \cdot 1 = x$$

следует $x = y$.

Из равенства $xx = x$ следует $x = 1$, поэтому в группе содержится единственный идемпотент — единица. Это значит, что единица содержится в любой подгруппе группы и, следовательно, пересечение любого числа подгрупп не пусто и само является подгруппой.

Гомоморфное отображение группы сохраняет ассоциативность, переводит нейтральный элемент в нейтральный, а обратный — в обратный. Иначе говоря, *гомоморфный (и, в частности, изоморфный) образ группы сам является группой.*

Таким образом, свойство «быть группой» абстрактное.

Группа, не имеющая нетривиальных гомоморфизмов, называется *простой*.

Точнее, группа проста, если ее гомоморфное, но не взаимно однозначное отображение переводит все элементы этой группы в нейтральный элемент.

Группы $\langle \mathbf{R}_+; + \rangle$ и $\langle \mathbf{R}; \cdot \rangle$ изоморфны, это означает, что операции умножения и сложения на этих множествах по существу не отличаются.

Полугруппы $\langle \mathbf{Q}_+; + \rangle$ и $\langle \mathbf{Q}; \cdot \rangle$ тоже являются группами, но операции сложения и умножения в них различаются существенно.

Другими словами, аддитивная группа рациональных чисел и мультипликативная группа положительных рациональных чисел не изоморфны.

Для доказательства неизоморфности достаточно указать хотя бы одно свойство, которым обладает одна группа, но не обладает другая. Например, в группе $\langle \mathbf{Q}_+; + \rangle$ уравнение $2x = a$ имеет решение для любого a из \mathbf{Q}_+ , а соответствующее ему уравнение на мультипликативном языке $x^2 = b$ имеет решение не для всех b из \mathbf{Q} .

Для любого натурального n существует группа из n элементов. Таковой будет, например, группа корней n -й степени из единицы или изоморфная ей группа вращений правильного n -угольника.

Группа вращений n -угольника — это частный случай группы симметрий.

Если ϑ — геометрическая фигура на плоскости (или в пространстве), то множество всех таких движений плоскости (пространства), переводящих ϑ на себя, с операцией «композиция» образует группу. Эту группу называют *группой самосовмещений*, или *группой симметрий* фигуры ϑ .

Как и любая полугруппа, группа может быть задана с помощью порождающих элементов и определяющих соотношений между порождающими элементами.

В группе каждый элемент имеет обратный, поэтому вместо равенства $U = W$ можно писать $UW^{-1} = 1$. Это значит, что все определяющие соотношения группы можно представить в виде произведений порождающих и их обратных, равных единичному элементу.

Единичный элемент и символ равенства в записи представления группы обычно опускаются. Иначе говоря, если группа G порождается элементами a_1, a_2, \dots, a_n и имеет определяющие соотношения R_1, R_2, \dots, R_m , то пишут

$$G = \langle a_1, a_2, \dots, a_n; R_1, R_2, \dots, R_m \rangle.$$

Тривиальные соотношения, выполняющиеся в любой группе $xx^{-1} = x^{-1}x = 1$, среди определяющих соотношений не пишут.

Если числа n, m конечны, то группа называется *конечно-определенной*. Конечно-определенную группу, в которой $n = m$, называют *сбалансированной*.

Существуют группы, для которых проблема слов алгоритмически неразрешима, т. е. не существует алгоритма для узнавания, равен ли произвольный элемент такой группы единице или нет.

Группа называется *свободной*, если ее можно представить с пустым множеством нетривиальных соотношений (порождающие элементы в таком случае называются *свободными*).

Свободную группу F_r на r свободных порождающих называют группой *ранга* r :

$$F_r = \langle a_1, a_2, \dots, a_r \rangle.$$

В свободной группе проблема слов алгоритмически разрешима. Если после естественных сокращений в слове, представляющем элемент свободной группы, слово не исчезнет полностью (т. е. в нем останутся неединичные элементы), то это слово представляет неединичный элемент.

Число элементов группы называют *порядком группы*. Если G — множество группы, то порядок обозначают символом $|G|$.

Задача вычисления порядка в классе всех конечно-определенных групп алгоритмически неразрешима. Это значит, что не существует алгоритма, который по произвольному конечному заданию группы сообщал бы, сколько элементов содержится в этой группе.

Впрочем, неразрешима проблема узнавания какого-то конкретного порядка, т. е. нет алгоритма для решения любой из следующих задач: является ли группа конечной или бесконечной, содержит ли она более одного элемента, содержит ли она более (или в точности) n элементов при фиксированном n и т. п.

Прямое произведение групп A и B является группой и содержит изоморфные копии групп-сомножителей.

Если две группы G_1 и G_2 представлены с помощью порождающих множеств и определяющих соотношений

$$G = \langle a_1, a_2, \dots, a_n; R_1, R_2, \dots, R_m \rangle;$$

$$G_2 = \langle b_1, b_2, \dots, b_k; S_1, S_2, \dots, S_l \rangle,$$

то прямое произведение этих групп имеет представление

$$G_1 \times G_2 = \langle a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_k; R_1, R_2, \dots, R_m, S_1, S_2, \dots, S_l, a_i b_j = b_j a_i (i = 1, 2, \dots, n; j = 1, 2, \dots, k) \rangle.$$

Элемент $x y x^{-1} y^{-1}$ называют *коммутатором* элементов x, y . Два элемента перестановочны тогда и только тогда, когда их коммутатор равен единице.

Таким образом, соотношения $a_i b_j = b_j a_i$ в представлении прямого произведения можно заменить коммутаторами этих элементов.

Группу, обладающую одним порождающим, называют *циклической*. Точнее говоря, группа G циклическая с порождающим элементом a , если $G = \{a^k \mid k \in \mathbb{Z}\}$. Пишут: $G = \text{гр}(a)$.

Группа вращений правильного n -угольника и группа корней n -й степени из единицы являются циклическими n -го порядка.

Каждый элемент a произвольной группы G содержится в циклической подгруппе $\text{гр}(a)$. Порядок $\text{гр}(a)$ называют порядком элемента a . Другими словами, n — конечный порядок элемента a , если $a^n = 1$ и n — наименьшее натуральное число с таким свойством. Элементами конечного порядка по умолчанию имеют в виду неединичные элементы группы. Если в группе G есть элементы конечного порядка, то говорят, что группа G с *кручением* (а если нет, то G называют группой без кручения).

Циклическая группа из n элементов имеет представление $\langle a; a^n \rangle$. Бесконечная циклическая группа — это свободная группа ранга один. Например, $\langle \mathbb{Z}; + \rangle$ — бесконечная циклическая группа, записанная аддитивно (заметим, что как полугруппа \mathbb{Z} порождается не менее чем двумя элементами, т. е. не является моногенной).

Если в циклической группе $\text{гр}(a)$ для некоторых различных i, j выполняется равенство $a^i = a^j$, то $a^{i-j} = 1$, и поэтому $\text{гр}(a)$ содержит не более $i - j$ элементов. Следовательно, в бесконечной циклической группе все элементы $a^k (k \in \mathbb{Z})$ различны. Отображение множе-

ства $\text{гр}(a)$ на множество \mathbb{Z} , переводящее каждый элемент a^k в число k , взаимно однозначно и сохраняет операцию. Это значит, что все бесконечные циклические группы изоморфны.

То же самое верно и для конечных циклических групп. Действительно, если $A = \langle a; a^n \rangle$ и $B = \langle b; b^n \rangle$, то отображение $\varphi: A \rightarrow B$, заданное правилом

$$\varphi(a^i) = b^i,$$

взаимно однозначно и сохраняет операцию.

Циклические группы одинаковых порядков изоморфны.

Порождающие элементы гомоморфного прообраза переходят при гомоморфизме в порождающие элементы образа. Поэтому гомоморфный образ циклической группы снова является циклической группой.

Пусть H — ненулевая подгруппа группы $\langle \mathbb{Z}; + \rangle$ и d — наименьшее положительное число, принадлежащее H . Если $x \in H$ и r — остаток от деления x на d , то r — тоже элемент из H . Это значит, что подгруппа H состоит из кратных d , и, таким образом, любая подгруппа бесконечной циклической группы сама циклическая.

Это утверждение верно для циклической группы любого порядка. Если H — неединичная подгруппа группы $A = \langle a; a^n \rangle$ и d — такое наименьшее положительное число, что $a^d \in H$, то $H = \text{гр}(a^d)$.

Каждая подгруппа циклической группы является циклической.

Прямое произведение

$$A \times B = \langle a, b; a^n, b^m, aba^{-1}b^{-1} \rangle$$

двух циклических групп $A = \langle a; a^n \rangle$ и $B = \langle b; b^m \rangle$ имеет порядок mn . Элемент ab — элемент наивысшего порядка в группе $A \times B$, и этот порядок равен НОК $[n, m]$.

Это значит, что *прямое произведение двух конечных циклических групп является циклической группой тогда и только тогда, когда порядки этих групп взаимно просты.*

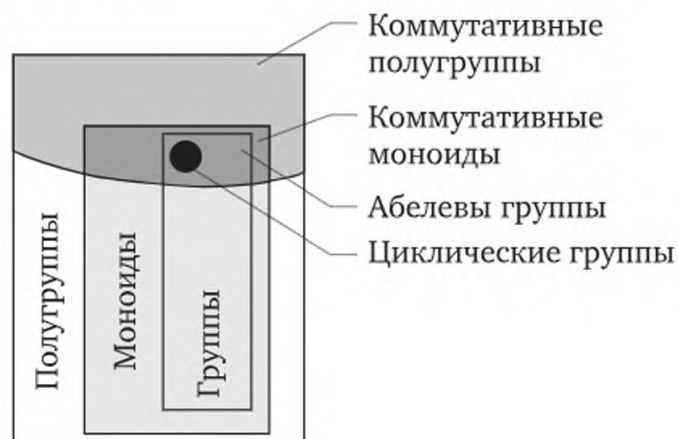
Если A, B — циклические группы и одна из них бесконечна, то прямое произведение $A \times B$ не порождается одним элементом, т. е. не образует циклическую группу.

Пока прервем обсуждение свойств циклических групп. Они несложны, но целесообразно сначала обсудить простейшие свойства подгрупп и свойства делимости целых чисел.

Коммутативная группа называется *абелевой*¹. В абелевой группе любые два элемента перестановочны: $xu = ux$ для любых элементов x, u .

¹ В честь норвежского математика Нильса Хенрика Абеля (Abel, 1802—1829), который первым обнаружил связь между коммутативными группами и проблемой разрешимости в радикалах алгебраических уравнений.

Для перестановочности всех элементов группы достаточно перестановочности ее порождающих. Поэтому если среди соотношений группы присутствуют все коммутаторы ее порождающих, то эта группа абелева. Все числовые (и аддитивные, и мультипликативные) группы абелевы.



Умножение элементов циклической группы сводится к сложению целых чисел (и последующему делению на натуральное число, если группа конечна). Поэтому все циклические группы абелевы.

Поскольку любой элемент группы порождает циклическую подгруппу, любая неединичная группа содержит неединичные абелевы подгруппы и, более того, является теоретико-множественным объединением абелевых групп.

Группы порядка меньше пяти абелевы; а S_3 (и изоморфная ей группа симметрий правильного треугольника) является наименьшей неабелевой группой.

Неабелевой группой будет группа симметрий любого n -угольника.

Прямое произведение абелевых групп само является абелевой группой. В частности, прямое произведение циклических групп образует абелеву группу.

Для конечных (и даже для конечно-порожденных) групп верно и обратное утверждение: *каждая конечно-порожденная абелева группа является прямым произведением циклических групп.*

Бесконечно-порожденная абелева группа может и не разлагаться в прямое произведение циклических подгрупп. Например, любые две ненулевые подгруппы аддитивной группы рациональных чисел имеют ненулевое пересечение, поэтому группа $\langle \mathbb{Q}; + \rangle$ вообще неразложима в нетривиальное прямое произведение.

Обычно для абелевых групп используют аддитивную запись. Для абелевой группы нет необходимости говорить о левом и правом вычитании, и так же, как и в школьном курсе математики, *разностью* $a - b$ называют решение уравнения $x + b = a$, т. е.

$$a - b = a + (-b).$$

В полугруппе выполняется закон *правого сокращения*, если для любых ее элементов a, b, c из $ba = ca$ следует $b = c$. Аналогично определяется левое сокращение.

Выполнение левого и правого сокращения называют просто *законом сокращения*.

Если полугруппа Π конечна и в ней выполняется закон сокращения, то для любого элемента x из Π все три множества $\Pi, x\Pi$ и Πx совпадают. Отсюда следует, что Π — полугруппа с делением и, следовательно, группа. Другими словами, *конечная полугруппа с законом сокращения является группой*.

Пример моноида $\langle \mathbb{N}; + \rangle$ показывает, что для бесконечных моноидов недостаточно условия сокращения, чтобы быть группой.

В группе условие сокращения выполняется. Поэтому если в полугруппе Π не выполняется условие сокращения, то она не может содержаться ни в какой группе (или, точнее, не существует изоморфного вложения полугруппы Π ни в какую группу).

Однако выполнения условия сокращения для полугруппы недостаточно для ее вложимости в некоторую группу¹. Например, полугруппа

$$\Pi = \langle a, b; a^2b^2 = b^2a^2, a^2bab^2 = b^2aba^2 \rangle$$

обладает условием сокращения, но не изоморфна никакой подполугруппе никакой группы.

В группе только единица является идемпотентом. В симметрической полугруппе множества M , состоящего из более чем одного элемента, содержится более одного идемпотента, поэтому данная полугруппа никогда не является группой. Однако множество всех взаимно однозначных отображений любого множества M на себя с операцией «композиция» уже образует группу.

Группу, состоящую из всех взаимно однозначных отображений множества M на себя, называют *симметрической*.

Биекция множества M на себя называется *подстановкой*. Подстановку f на множестве $M = \{a_1, a_2, \dots, a_n\}$ записывают в виде таблицы из двух строк и n столбцов:

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & \dots & f(a_n) \end{pmatrix}.$$

При фиксированном порядке элементов M каждая подстановка однозначно задается второй строкой — перестановкой элементов M .

¹ Впервые пример такого рода полугруппы был получен в 1939 г. русским математиком Анатолием Ивановичем Мальцевым (1909—1967), с 1958 г. действительным членом Академии наук СССР.

Символом S_M , или $S_{|M|}$, принято обозначать множество всех подстановок множества M . Если $|M| = n$, то, соответственно, символ имеет вид S_n . Подстановки n -элементного множества называют *подстановками степени n* .

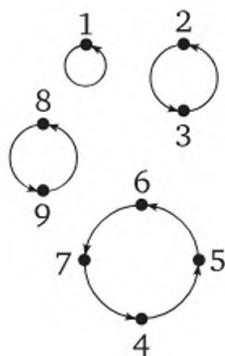
Пусть $M = \{1, 2, \dots, n\}$. Тогда подстановка f множества M имеет вид

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

Число всех перестановок множества из n символов (оно же число подстановок этого множества) равно $n!$. Свойства группы подстановок не зависят от свойств элементов исходного множества. Поэтому, когда нет оговорок, по умолчанию имеют в виду, что множество $M = \{1, 2, \dots, n\}$.

Пусть a — произвольный элемент из M , а $f \in S_n$. При действии на элемент a подстановкой f , затем f^2, f^3 и т. д. получим в результате подмножество, элементы которого циклически переставляются подстановкой f . Подстановка f распадается в произведение *циклов*, не имеющих общих элементов. Некоторые циклы состоят всего из одного элемента, и этот элемент при действии подстановки остается неподвижным.

Каждый цикл подстановки передвигает по кругу (циклически) элементы одного подмножества, оставляя все прочие элементы из M на месте.



Граф подстановки

На графе подстановки цикл действительно можно расположить на окружности¹, а действие подстановки будет состоять во вращении этой окружности.

Подстановка

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 2 & 5 & 6 & 7 & 4 & 9 & 8 \end{pmatrix},$$

¹ Цикл — от греч. $\chi\upsilon\chi\lambda\omicron\varsigma$ — «окружность, круг».

граф которой изображен на рисунке, имеет четыре цикла, причем элемент 1 неподвижен (одноэлементный цикл).

Подстановка на рисунке является произведением подстановок на отдельных подмножествах $\{1\}$, $\{2, 3\}$, $\{4, 5, 6, 7\}$, $\{8, 9\}$, на каждом из подмножеств подставка является циклом (для краткости записи одноэлементный цикл, оставляющий все элементы на месте, пропущен):

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 2 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} \times \\ \times \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 5 & 6 & 7 & 4 & 8 & 9 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 9 & 8 \end{pmatrix}.$$

Эту запись можно сделать еще короче. Цикл, перемещающий элемент a_1 в элемент a_2 , a_2 в a_3 , ..., a_{n-1} в a_n и a_n в a_1 , обозначают символом $(a_1 a_2 a_3 \dots a_n)$.

Это значит, что подстановка является произведением циклов

$$\alpha = (1) \cdot (2\ 3) \cdot (4\ 5\ 6\ 7) \cdot (8\ 9),$$

или еще короче (не выписывая неподвижных элементов):

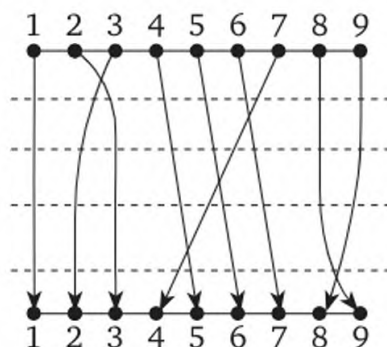
$$\alpha = (2\ 3)(4\ 5\ 6\ 7)(8\ 9).$$

В пакете прикладных математических программ *Maple* циклы подстановки записываются чуть иначе. Например, наша подстановка α для машинной обработки должна иметь вид

$$[[2, 3], [4, 5, 6, 7], [8, 9]].$$

Цикл из двух элементов называют *транспозицией*. Например, в подстановке на рисунке циклы $(2\ 3)$ и $(8\ 9)$ — транспозиции.

В представлении α лишь две транспозиции. На самом деле подстановка α является произведением одних только транспозиций. Это разложение можно увидеть на графе подстановки с двумя экземплярами множества M .



Транспозиции на графе подстановки

Проведем горизонтальные линии по графу подстановки таким образом, чтобы между каждой парой линий оказалось в точности одно пересечение стрелок. Каждое такое пересечение и изображает транспозицию (причем соседних символов). С помощью линий, построенных на рисунке, получается разложение α :

$$\alpha = (23)(67)(56)(45)(89).$$

Это свойство не является каким-то особым, которым обладают лишь специально подобранные подстановки. Каждая подстановка является произведением транспозиций.

Для доказательства можно воспользоваться теми же соображениями или предварительно разложить подстановку в произведение циклов, а каждый цикл — в произведение транспозиций, используя тождество (для любых a_1, a_2, \dots, a_m)

$$(a_1 a_2 \dots a_m) = (a_1 a_2)(a_1 a_2) \dots (a_1 a_m).$$

Если воспользоваться этой идеей, то получится второе представление подстановки $\alpha = (1) \cdot (2\ 3) (4\ 5\ 6\ 7) (8\ 9)$ в виде произведения транспозиций:

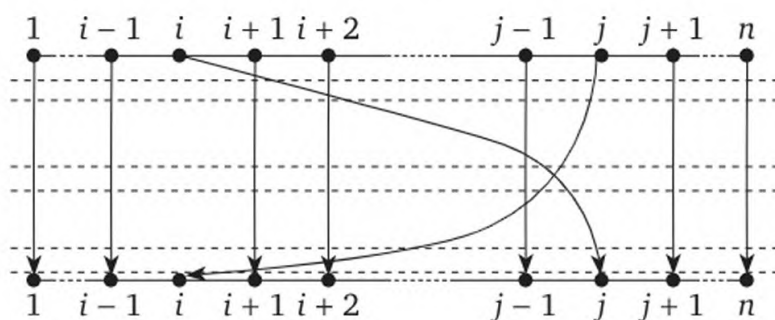
$$\alpha = (1) \cdot (2\ 3) (4\ 5\ 6\ 7) (8\ 9) = (2\ 3)(4\ 5)(4\ 6)(4\ 7)(8\ 9).$$

Впрочем, непосредственно из схемы видно, что транспозиции нельзя выбрать произвольным образом.

Каждая подстановка на множестве $\{1, 2, \dots, n\}$ является произведением транспозиций, перемещающих соседние символы. Это значит, что симметрическая группа S_n порождается транспозициями вида $(ii+1)$, где $i = 1, 2, \dots, n-1$.

Число транспозиций в представлении подстановки с помощью рассеченного графа равно числу точек пересечения стрелок в графе. Однако стрелки можно изогнуть и по-другому, тогда число точек пересечения изменится. Это означает, что такой способ получения разложения подстановки в произведение транспозиций не однозначен (а ведь есть и другие приемы).

Непосредственно из схемы видно, что произвольная транспозиция (ij) является произведением нечетного числа транспозиций, переставляющих соседние символы.



Транспозиция (ij)

Впрочем, и непосредственная проверка схемы несложна:

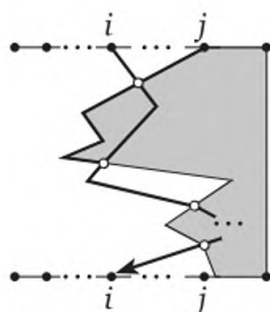
$$(i\ j) = (i\ i+1) \cdot (i+1\ i+2) \cdot \dots \cdot (j-1\ j) \cdot \dots \cdot (i+1\ i+2) \cdot (i\ i+1).$$

Единичное отображение множества изображается единичной подстановкой

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Естественное представление единичной подстановки имеет нуль транспозиций (0 — число четное).

Возьмем произвольное представление единичной подстановки в произведение транспозиций. Каждую транспозицию можно заменить произведением транспозиций, передвигающих лишь соседние символы. Четность числа множителей от такой замены не изменится. Соответствующий граф единичной подстановки будет иметь пересечений стрелок в точности столько, сколько транспозиций участвует в ее представлении. Все стрелки на графе можно считать ломаными линиями.



Число пересечений четно

Поскольку каждый многоугольник делит плоскость на две области, каждые две стрелки графа имеют четное число пересечений. Отсюда следует, что любое разложение единичной подстановки в произведение транспозиций имеет четное число множителей.

Учитель сказал, что в молодости он каждое утро трижды переплывал реку Янцзы. Ученик вежливо заметил: «Извините, Учитель, но чтобы вернуться домой, Вам пришлось бы переплыть реку и в четвертый раз»

(анекдот из жизни Конфуция).

Из этого свойства единичной подстановки следует свойство всех подстановок.

Если подстановку можно представить в виде произведения четного числа транспозиций, то и любое другое представление этой подстановки будет иметь четное число транспозиций.

Каждое целое число является либо четным, либо нечетным, поэтому в предыдущем предложении вместо слова «четный» можно написать «нечетный».

Подстановку называют *четной*, если ее можно представить в виде четного числа транспозиций, и *нечетной* — в противном случае.

Введем функцию, определенную на множестве S_n со значениями в множестве $\{1, -1\}$. Функция будет называться *знак подстановки*, обозначаться символом sgn и определяться следующим правилом (для каждой σ из S_n):

$$\text{sgn } \sigma = \begin{cases} 1, & \text{если } \sigma \text{ — четная,} \\ -1, & \text{если } \sigma \text{ — нечетная.} \end{cases}$$

Для транспозиции обратной подстановкой является она сама. Поэтому для получения обратной подстановки для произведения транспозиций достаточно эти же транспозиции записать в обратном порядке, например,

$$[(2\ 3)(4\ 5)(4\ 6)(4\ 7)(8\ 9)]^{-1} = (8\ 9)(4\ 7)(4\ 6)(4\ 5)(2\ 3).$$

Таким образом, для любой подстановки α из S_n

$$\text{sgn } \alpha^{-1} = \text{sgn } \alpha.$$

Сумма четных чисел — снова число четное. Поэтому множество A_n всех четных подстановок образует подгруппу группы S_n . Эта подгруппа называется *знакопеременной*¹ (или *альтернативной*) группой.

Сумма четного и нечетного числа — число нечетное. Поэтому для любой подстановки α из S_n и любой нечетной подстановки β выполняется равенство

$$\text{sgn } \alpha\beta = -\text{sgn } \alpha.$$

Умножим все элементы из A_n на фиксированную нечетную подстановку β . Элементы из $A_n\beta$ — это все нечетные подстановки. Следовательно, знакопеременная группа A_n содержит в точности половину всех подстановок из S_n .

Транспозиция — это нечетная подстановка, и умножение на нее меняет знак подстановки. Умножение на транспозицию означает перестановку мест в нижней или верхней строке подстановки (в зависимости от того, с какой стороны происходит умножение). Таким

¹ Название «знакопеременная» парадоксально, оно связано с тем, что каждая четная подстановка переменных x_i не изменяет знак многочлена $\prod_{1 \leq i < j \leq n} (x_i - x_j)$.

образом, перемена местами двух элементов нижней (или верхней) строки меняет четность подстановки. Свойства суммы четных и нечетных чисел означают, что для любых подстановок α и β :

$$\operatorname{sgn} \alpha \beta = \operatorname{sgn} \alpha \cdot \operatorname{sgn} \beta.$$

Это значит, что отображение $\sigma \mapsto \operatorname{sgn} \sigma$, ставящее каждой подстановке σ в соответствие ее знак $\operatorname{sgn} \sigma$, является гомоморфизмом симметрической группы S_n в мультипликативную группу $\langle \{1, -1\}; \cdot \rangle$.

Симметрическая группа S_n порождается транспозициями, причем транспозиции можно выбрать так, что они перемещают лишь соседние элементы. Все $(n - 1)$ таких транспозиций можно получить из одной транспозиции $\alpha = (1\ 2)$ и цикла $\beta = (1\ 2\ 3 \dots n)$.

Для каждого $k = 0, 1, \dots, (n - 2)$ k -я степень подстановки β переводит единицу в $k + 1$, а 2 переведет в $k + 2$:

$$\beta^k(1) = k + 1;$$

$$\beta^k(2) = k + 2.$$

Следовательно, k -я степень β переведет элемент $k + 1$ в 1, а элемент $k + 2$ перейдет в 2:

$$\beta^{-k}(k + 1) = 1;$$

$$\beta^{-k}(k + 2) = 2.$$

Отсюда получается, что

$$\beta^{-k} \alpha \beta^k(k + 1) = k + 2;$$

$$\beta^{-k} \alpha \beta^k(k + 2) = k + 1.$$

Все прочие элементы подстановка $\beta^{-k} \alpha \beta^k$ оставляет на месте. Это значит, что

$$\beta^{-k} \cdot \alpha \cdot \beta^k = (k + 1\ k + 2).$$

Итак, с помощью подстановок α, β можно получить все транспозиции, переставляющие соседние элементы. Группа S_2 циклическая, т. е. порождается одним элементом.

Для всех натуральных чисел $n > 2$ группа S_n уже не циклическая (она даже не абелева), но порождается всего лишь двумя элементами.

Если множество M конечно и состоит из n элементов, то вместо S_M обычно пишут S_n . Группа S_n имеет порядок $n!$ и при $n \geq 3$ неабелева.

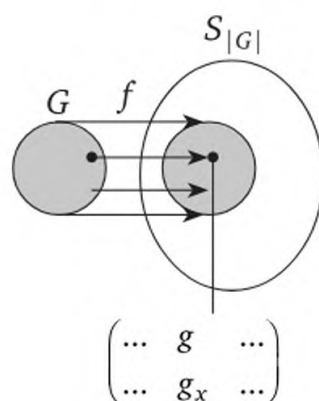
Подгруппу симметрической группы называют *группой подстановок*.

Симметрическая группа S_3 неабелева, и число шесть — это наименьший порядок неабелевой группы.

Пусть G — произвольная группа. При изоморфном вложении f моноида G в симметрическую полугруппу образ группы G окажется в симметрической группе $S_{|G|}$.

Таким образом, каждая группа изоморфна некоторой группе подстановок.

В частности, каждая конечная группа порядка n изоморфно вложима в группу S_n . Этот факт по имени автора называют *теоремой Кэли*¹.



К теореме Кэли

Поскольку каждая группа S_n порождается двумя элементами, теорема Кэли означает, в частности, что каждая конечная группа изоморфно вложима в 2-порожденную группу.

Если A — произвольная алгебра (или алгебраическая система), то изоморфное отображение алгебры A в себя называют *автоморфизмом*.

Поскольку автоморфизм — это частный случай подстановки, имеем:

- 1) множество $\text{Aut}(A)$ всех автоморфизмов алгебры A с операцией «композиция» образует группу;
- 2) группа $\text{Aut}(A)$ автоморфизмов алгебры A является подгруппой симметрической группы множества A .

Таким образом, понятие группы также является важным при исследовании любой алгебры (или алгебраической системы). Исследовать алгебру — это означает, в частности, *изучить группу автоморфизмов этой алгебры*.

1.4. Кольца

Самая распространенная связь между двумя двухместными операциями — это закон *дистрибутивности*.

¹ Артур Кэли (Cayley, 1821—1895) — английский математик, с 1863 г. — профессор Кембриджского университета. Теорема о представимости любой группы подстановками доказана А. Кэли в 1854 г.

Пусть $A = \langle A; \oplus, \otimes \rangle$ — алгебра с двумя двухместными операциями; первую условно назовем сложением, а вторую — умножением. Умножение *дистрибутивно* относительно сложения, если для любых a, b, c из A

$$\begin{aligned}a \otimes (b \oplus c) &= (a \otimes b) \oplus (a \otimes c); \\(b \oplus c) \otimes a &= (b \otimes a) \oplus (c \otimes a).\end{aligned}$$

Первое тождество называют иногда левым дистрибутивным законом, второе — правым. Если умножение коммутативно, то говорят просто: *дистрибутивный закон*.

Например, дистрибутивный закон выполняется для сложения и умножения чисел, точнее, умножение дистрибутивно относительно сложения. Дистрибутивно объединение относительно пересечения множеств и наоборот — пересечение относительно объединения. Два дистрибутивных закона связывают конъюнкцию и дизъюнкцию высказываний.

Алгебра $A = \langle A; \oplus, \otimes \rangle$ с двумя операциями называется *полукольцом*, если одна из операций (\oplus) ассоциативна и коммутативна и имеет нейтральный элемент, а вторая (\otimes) дистрибутивна относительно первой.

Другими словами, $A = \langle A; \oplus, \otimes \rangle$ — полукольцо, если:

- 1) $A = \langle A; \oplus, \otimes \rangle$ — коммутативный моноид;
- 2) для любых x, y, z из K

$$\begin{aligned}x \otimes (y \oplus z) &= (x \otimes y) \oplus (x \otimes z); \\(y \oplus z) \otimes x &= (y \otimes x) \oplus (z \otimes x).\end{aligned}$$

Обычно первую из операций полукольца называют *сложением*, а вторую — *умножением*. В записи полукольца как алгебры из символов операций первым пишут символ, изображающий сложение, вторым — умножение.

Гомоморфный (и, в частности, изоморфный) образ полукольца является полукольцом. Свойство «быть полукольцом» абстрактное.

Прямое произведение полуколец образует полукольцо.

Отсутствие нейтрального элемента в полукольце легко поправить — нулевой элемент можно присоединить к множеству A , положив (для каждого элемента x из A):

$$\begin{aligned}x \oplus 0 &= 0 \oplus x = x; \\0 \otimes x &= x \otimes 0 = 0; \\0 \oplus 0 &= 0 \oplus 0 = 0; \\0 \otimes 0 &= 0 \otimes 0 = 0.\end{aligned}$$

Аддитивная полугруппа тогда превратится в моноид, а свойство дистрибутивности будет распространено на более широкое множество. Это значит, что каждое полукольцо без нуля изоморфно вло-

жимо в полукольцо с нулем. Поэтому, хотя в системе $\langle \mathbb{N}; +, \cdot \rangle$ и нет нейтрального элемента по сложению, возможность такого мономорфизма позволяет говорить о *полукольце натуральных чисел*.

Алгебра $K = \langle K; +, \cdot \rangle$ с двумя операциями называется *кольцом*, если:

- 1) $\langle K; +, \cdot \rangle$ — абелева группа;
- 2) операции связаны дистрибутивным законом (для любых x, y, z из K):

$$x \cdot (y + z) = x \cdot y + x \cdot z;$$

$$(y + z) \cdot x = y \cdot x + z \cdot x.$$

Кольцо является частным случаем полукольца.

В каждой абелевой группе можно определить умножение так, чтобы она превратилась в кольцо, например, положив по определению $x \cdot y = 0$ для любых элементов x, y из этой группы. Такое кольцо называют *кольцом с нулевым умножением*.

Кольцо $K_1 = \langle K_1; +, \cdot \rangle$ *изоморфно* кольцу $K_2 = \langle K_2; +, \cdot \rangle$ если существует отображение φ множества K_1 на множество K_2 , сохраняющее операции кольца (для любых x, y из K_1):

$$\varphi(x + y) = \varphi(x) + \varphi(y);$$

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y).$$

Как обычно, если не требовать взаимной однозначности отображения φ , сохраняющего операции, то φ будет всего лишь *гомоморфизмом колец*.

Кольцевой гомоморфизм является, в частности, групповым, и кольцо, не имеющее нетривиальных гомоморфизмов, называется *простым*. Другими словами, кольцо K просто, если любой его гомоморфизм либо является изоморфизмом, либо отображает все элементы из K в нуль.

При гомоморфизме сохраняется любое тождество, связывающее операции, в частности сохраняется закон дистрибутивности. Кроме того, если φ — гомоморфизм кольца K на алгебру K_1 и 0 — нуль в K , то $\varphi(0)$ — нуль в K_1 и $\varphi(-x) = -\varphi(x)$. Поэтому гомоморфный (и, в частности, изоморфный) образ кольца является кольцом. Свойство «быть кольцом» абстрактное, оно сохраняется при изоморфизме: алгебра, изоморфная кольцу, сама является кольцом.

Свойства *умножения* (ассоциативность, коммутативность, наличие единицы и т. п.) переносятся на название самого кольца. Например, кольцо $\langle K; +, \cdot \rangle$ *ассоциативно*, если умножение в нем ассоциативно, и *коммутативно*, если все элементы перестановочны при умножении.

Кольцо, содержащее нейтральный элемент по умножению, называют *кольцом с единицей*. Обычно считают, что единица отлична

от нуля кольца (если единица совпадает с нулем, то кольцо не содержит ненулевых элементов, — такое кольцо называют *нулевым*).

Прямое произведение колец снова является кольцом, более того, свойства колец, заданные с помощью тождеств, сохраняются при прямом умножении.

Как и для групп, число элементов кольца называют *порядком*.

Нейтральный по сложению элемент кольца, как обычно для аддитивной записи, называется *нулем* и обозначается символом 0.

Если x — произвольный элемент кольца, то

$$x \cdot 0 = x(0 + 0) = x \cdot 0 + x \cdot 0.$$

Прибавив к левой и правой частям этого равенства элемент $-x \cdot 0$, получим: $x \cdot 0 = 0$. Аналогично $0 \cdot x = 0$.

Таким образом, *нуль кольца является поглощающим элементом по умножению*.

Другими словами, для любых элементов x, y кольца выполняется утверждение:

$$\text{если } x = 0 \text{ или } y = 0, \text{ то } xy = 0.$$

Обратное утверждение:

$$\text{если } xy = 0, \text{ то } x = 0 \text{ или } y = 0,$$

верно не для каждого кольца.

Например, в кольце квадратных матриц $M_2(\mathbf{R})$ произведение двух ненулевых матриц может оказаться нулевой матрицей.

Множество $F(K)$ всевозможных функций, определенных в кольце K , и со значениями в K образует кольцо с естественными операциями сложения и умножения функций. Если K содержит по крайней мере три элемента, то в кольце $F(K)$ есть ненулевые функции, произведение которых является нулевой функцией.

Если $\langle K; +, \cdot \rangle$ — кольцо, то $\langle K; + \rangle$ является абелевой группой и, следовательно, можно говорить о *вычитании* как об операции в K , а именно положив по определению

$$\overset{\text{опр}}{x - y} = x + (-y).$$

Пусть x, y, z — произвольные элементы кольца. Тогда

$$xy = x[y + (-z) + z] = x[y + (-z)] + xz = x(y - z) + xz,$$

откуда

$$x(y - z) = xy - xz.$$

Это означает, что умножение в кольце дистрибутивно относительно вычитания.

В дистрибутивном законе упоминаются лишь два слагаемых, но число слагаемых может быть *любым*. Индукцией по m -числу слагаемых получается, что для любых элементов x_i, y из кольца:

$$\begin{aligned}(x_1 + x_2 + \dots + x_m) \cdot y &= x_1 \cdot y + x_2 \cdot y + \dots + x_m \cdot y; \\ y \cdot (x_1 + x_2 + \dots + x_m) &= y \cdot x_1 + y \cdot x_2 + \dots + y \cdot x_m.\end{aligned}$$

Из этих двух тождеств получается *обобщенный дистрибутивный закон* (для любых элементов x_i, y_j из кольца):

$$(x_1 + x_2 + \dots + x_m) \cdot (y_1 + y_2 + \dots + y_n) = \sum_{i=1}^m \sum_{j=1}^n x_i \cdot y_j.$$

В частности, все элементы x_i и y_j могут быть равны. Обозначим символом mx сумму m слагаемых, равных x ; а символом ny — сумму из n слагаемых, равных y :

$$\begin{aligned}mx &= \underbrace{x + x + \dots + x}_m; \\ ny &= \underbrace{y + y + \dots + y}_n.\end{aligned}$$

Тогда имеем: $mx \cdot ny = mn(xy)$.

Для колец, состоящих из чисел, выполняется *правило знаков* при умножении. Это свойство общее для всех колец, т. е. для каждого элементов a, b из любого кольца:

$$\begin{aligned}a \cdot (-b) &= (-a) \cdot b = -a \cdot b; \\ (-a) \cdot (-b) &= a \cdot b.\end{aligned}$$

Действительно,

$$\begin{aligned}a \cdot (-b) &= a \cdot (0 - b) = a \cdot 0 - a \cdot b = -a \cdot b; \\ (-a) \cdot (-b) &= -[a \cdot (-b)] = -[-a \cdot b] = a \cdot b.\end{aligned}$$

Для любого натурального числа m существует абелева (и даже циклическая) группа G , состоящая из m элементов. Записав эту группу аддитивно: $G = \langle G; + \rangle$, несложно превратить ее в кольцо, положив по определению (для всех x, y из G) $xy = 0$. Такое умножение называют *нулевым*, и оно малоинтересно. Однако то, что верно для групп, выполняется и для настоящих колец: для любого натурального m существует кольцо с ненулевым умножением, состоящее из m элементов.

Этим кольцом является гомоморфный образ кольца целых чисел, построенный следующим образом. Разобьем множество целых чисел на подмножества, включив в каждое такое подмножество все числа, имеющие одинаковые остатки при делении на m .

При делении целого числа на m может получиться в точности один из остатков: $0, 1, \dots, m - 1$. Это значит, что таких подмножеств

будет m и все они имеют попарно пустые пересечения, а в объединении дают все множество \mathbb{Z} .

Такие подмножества принято называть *классами вычетов по модулю m* ; множества классов обозначают символом \mathbb{Z}_m .

Если A, B — два класса вычетов, то определим сложение и умножение по правилам:

$$A + B = \{a + b \mid a \in A, b \in B\};$$

$$A \cdot B = \{a \cdot b \mid a \in A, b \in B\}.$$

Как сумма, так и произведение классов снова состоят из целых чисел, имеющих одинаковые остатки при делении на m , т. е. образуют классы вычетов. Следовательно, множество \mathbb{Z}_m с операциями «сложение» и «умножение» образует алгебру.

Отображение множества \mathbb{Z} на множество \mathbb{Z}_m , ставящее в соответствие каждому целому числу тот класс, в котором это число находится, сохраняет операции, т. е. является гомоморфизмом. Гомоморфный образ кольца снова является кольцом, поэтому $\langle \mathbb{Z}_m; +, \cdot \rangle$ образует кольцо.

В ассоциативном кольце $\langle K; +, \cdot \rangle$ множество K с операцией умножения $\langle K; \cdot \rangle$ образует мультипликативную полугруппу.

В то же время любая полугруппа изоморфно вкладывается в мультипликативную полугруппу некоторого ассоциативного кольца.

Действительно, если G — произвольная мультипликативно записанная полугруппа, а K — произвольное кольцо с единицей (например, кольцо целых чисел), то множество

$$KG = \{a_1 g_1 + a_2 g_2 + \dots + a_n g_n \mid n \in \mathbb{N}, a_1, a_2, \dots, a_n \in K, g_1, g_2, \dots, g_n \in G\}$$

с естественно определенными операциями сложения и умножения является кольцом.

Естественное сложение — это приписывание второго слагаемого к первому с последующим приведением подобных членов. Естественное умножение состоит в раскрытии скобок в соответствии с обобщенным законом дистрибутивности, умножении элементов из G и приведении подобных членов.

В полугрупповом кольце KG множество элементов вида $1 \cdot g$ образует полугруппу, изоморфную полугруппе G .

Если полугруппа G является группой, то KG является *групповым кольцом*. Под словами «групповое кольцо» обычно имеют в виду целочисленное групповое кольцо $\mathbb{Z}G$.

Отметим, что если элемент g из G имеет конечный порядок n , то $1 + g^2 + \dots + g^{n-1}$ и $g - 1$ не равны нулю, но их произведение

$$(1 + g^2 + \dots + g^{n-1})(g - 1) = g^n - 1 = 0.$$

Это значит, что если группа G с кручением, то в групповом кольце ZG есть делители нуля.

Верно ли обратное утверждение, т. е. может ли групповое кольцо группы без кручения содержать делители нуля, пока (2021 г.) неизвестно.

Как в любом моноиде, некоторые элементы ассоциативного кольца с единицей могут быть обратимыми, и множество таких элементов в ассоциативном кольце с единицей образуют мультипликативную группу.

Таким образом, с ассоциативным кольцом с единицей связаны две группы — аддитивная группа кольца $\langle K; + \rangle$, состоящая из всех элементов кольца, и мультипликативная группа кольца $\langle K^*; \cdot \rangle$, состоящая из всех обратимых элементов этого кольца.

Например, для кольца целых чисел $Z^* = \{-1, 1\}$, для кольца рациональных (или действительных) чисел мультипликативные группы состоят из всех ненулевых элементов.

Два элемента a, b из кольца называются делителями нуля, если $a \neq 0$ и $b \neq 0$, но $a \cdot b = 0$. Например, множество функций, определенных на множестве R или на некотором интервале R и со значениями в R , образует ассоциативно-коммутативное кольцо с единицей и с делителями нуля.

Ненулевое ассоциативно-коммутативное кольцо без делителей нуля называют целостным кольцом (или областью целостности).

Множества Z, Q, R или C с обычными операциями сложения и умножения образуют числовые кольца. Все эти кольца целостные.

Прямое произведение не сохраняет целостность кольца. Действительно, если $A = \langle A; +, \cdot \rangle$ и $B = \langle A_2; +, \cdot \rangle$ — два ненулевых кольца, а $A \times B$ — их прямое произведение, то для любых $a \in A, b \in B$ произведение $(a, 0)$ и $(0, b)$ равно нулю.

Поглощающее свойство нуля кольца не позволяет говорить о мультипликативном сокращении на всем множестве кольца. Но ноль может оказаться единственным исключением.

В кольце K выполняется закон (левого) сокращения, если для любых a, b, c из K

$$ab = ac \text{ и } a \neq 0 \Rightarrow b = c.$$

Для того чтобы в кольце выполнялся закон сокращения, необходимо и достаточно отсутствие делителей нуля.

Действительно, если в кольце элементы a, b отличны от нуля, но $a \cdot b = 0$, то $a \cdot b = a \cdot 0$ и закон сокращения не выполняется. В то же время, если $ab = ac$ и $a \neq 0$, то $ab - ac = 0$ и, следовательно, $a(b - c) = 0$. Если в кольце нет делителей нуля, то отсюда следует $b - c = 0$.

Кроме числовых колец, в геометрических и физических приложениях важную роль играет кольцо, состоящее из трехмерных век-

торов с операциями сложения и векторного умножения. Это кольцо не является ни ассоциативным, ни коммутативным, да и нейтрального элемента по умножению там нет. Свойства этого кольца иные.

Кольцо называют *лиевым* (или кольцом *Ли*¹), если в нем выполняются тождества

$$a^2 = 0;$$

$$a(bc) + b(ca) + c(ab) = 0.$$

Множество трехмерных векторов с операциями «сложение» и «векторное умножение» образуют лиево кольцо.

Из тождества $a^2 = 0$ следует свойство антикоммутативности

$$ab = -ba.$$

Действительно,

$$(a + b)^2 = a^2 + ab + ba + b^2 = 0,$$

откуда

$$ab + ba = 0.$$

Ассоциативные кольца — это сильное обобщение *числовых колец*. Лиевы кольца, образно говоря, обобщают *геометрию* (евклидова геометрия — это исследование свойств лишь одного, конкретного лиева кольца трехмерных векторов). Между этими типами колец (образно говоря, представляющих числа и фигуры), есть тесная связь.

Пусть $\langle K; +, \cdot \rangle$ — ассоциативное кольцо. Введем на множестве K новую операцию умножения \circ по правилу: $x \circ y = x \cdot y - y \cdot x$. Новое кольцо $\langle K; +, \circ \rangle$ является лиевым (которое называют *обертывающим* кольцо $\langle K; +, \cdot \rangle$).

Верно и обратное утверждение: каждое лиево кольцо является обертывающим для некоторого ассоциативного кольца.

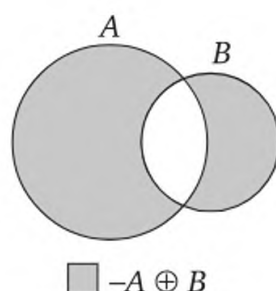
Кольцо называется *идемпотентным*, если в нем выполняется тождество $x^2 = x$.

Ассоциативное, идемпотентное кольцо с единицей называют *булевым* кольцом (или кольцом *Буля*²).

Булевым кольцом является, например, множество всех классов равносильных формул высказываний с операциями «отрицание эквиваленции» и «конъюнкция».

¹ В честь норвежского математика *Мариуса Софуса Ли* (Lie, 1842—1899).

² *Джордж Буль* (Boole, 1815—1864) — английский математик и логик.



Симметрическая разность

Симметрическая разность подмножеств \oplus ассоциативна, коммутативна и обладает нейтральным элементом — его роль играет пустое множество. Кроме того, для каждого, подмножества A

$$A \oplus A = \emptyset.$$

Пересечение дистрибутивно относительно симметрической разности

$$A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C).$$

Это значит, что множество $P(M)$ всех подмножеств множества M с операциями «симметрическая разность» и «пересечение» образует кольцо. Кольцо $\langle P(M); \oplus, \cap \rangle$ называют *кольцом множеств*. Пересечение ассоциативно, идемпотентно и обладает нейтральным элементом (его роль играет все множество M), следовательно, кольцо множеств булево.

Если M конечно, то и $P(M)$ конечно. Таким образом, для любого n существует булево кольцо, состоящее из 2^n элементов.

Впрочем, истинность последнего утверждения можно увидеть и из других соображений. Прямое произведение булевых колец снова является булевым кольцом. Пусть B — кольцо подмножеств одноэлементного множества. В кольце B два элемента, а число элементов в прямой степени B^n равно 2^n .

Непустое подмножество H кольца K , само являющееся кольцом относительно тех же операций, что и K , называется *подкольцом*.

Для того чтобы H было подкольцом, необходимо и достаточно, чтобы H было подгруппой аддитивной группы кольца и было замкнуто относительно умножения.

Другими словами, непустое подмножество H из кольца K является кольцом, если H замкнуто относительно операций сложения, вычитания и умножения, т. е.

$$x \in H, y \in H \Rightarrow x + y \in H, x - y \in H, x \cdot y \in H.$$

Например, сумма, разность и произведение четных чисел снова являются четными числами, поэтому множество четных чисел обра-

зует кольцо. Множество нечетных чисел не замкнуто относительно сложения (сумма двух нечетных чисел не является нечетным числом), и множество нечетных чисел кольцо не образует. На самом деле нет необходимости проверять все три арифметические операции; для того чтобы быть подкольцом, достаточно замкнутости относительно вычитания и умножения:

$$x \in H, y \in H \Rightarrow x - y \in H, x \cdot y \in H.$$

Наибольшее числовое кольцо — это кольцо комплексных чисел \mathbb{C} . Под словами «числовое кольцо» понимают (как правило, ненулевое) подкольцо кольца \mathbb{C} .

Таким образом, числовое кольцо — это множество комплексных чисел, замкнутое относительно вычитания и умножения.

Если M — произвольное непустое подмножество кольца K , то наименьшее подкольцо, содержащее M , называется подкольцом, порожденным M . Например, кольцо целых чисел порождается одним элементом — единицей, а кольцо рациональных чисел порождается дробями вида $\frac{1}{p}$, где p — всевозможные простые числа.

Сумма и разность конечных десятичных дробей снова является конечной десятичной дробью. Поэтому множество конечных десятичных дробей образует кольцо.

Конечная десятичная дробь — это дробь вида $\frac{1}{2^n 5^m}$, где $n, m \in \mathbb{Z}_0$. Это означает, что подкольцо конечных десятичных дробей порождается элементами $\frac{1}{2}$ и $\frac{1}{5}$.

Пусть M — некоторое множество простых чисел. Множество рациональных чисел, представимых несократимой дробью $\frac{a}{b}$, где в разложение числа b входят простые множители только из множества M , является подкольцом кольца \mathbb{Q} . Это подкольцо порождается всеми дробями $\frac{1}{p_i}$, где p_i принадлежит M .

Напомним, что \mathbb{Q} счетно, а в счетном множестве содержится континуум подмножеств, поэтому в поле рациональных чисел содержится не более чем континуум подколец. В то же время множество простых чисел счетно, и в этом множестве можно выбрать континуум различных подмножеств M .

Поскольку различные подмножества M порождают различные подкольца, в кольце рациональных чисел \mathbb{Q} содержится в точности континуум подколец.

Рассмотрим связь между полукольцами и кольцами.

Сначала рассмотрим ситуацию на конкретном примере: покажем, что полукольцо целых неотрицательных чисел \mathbf{Z}_0 изоморфно вложено в кольцо \mathbf{Z} целых чисел.

Пусть A — декартов квадрат $\mathbf{Z} \times \mathbf{Z}$. Введем на A отношение \sim по правилу

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

Это отношение рефлексивно, симметрично и транзитивно, т. е. является эквивалентностью. Символом $[(a, b)]$ обозначим смежный класс, содержащий пару (a, b) , а фактор-множество — символом A/\sim .

Пусть $B = A/\sim$. Определим операции в A по определению:

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d); \\ (a, b) \cdot (c, d) &= (ac + bd, bc + ad).\end{aligned}$$

Отношение эквивалентности на A согласовано с операциями. Если $(a, b) \sim (a_1, b_1)$ и $(c, d) \sim (c_1, d_1)$, то

$$(a, b) + (c, d) \sim (a_1, b_1) + (c_1, d_1)$$

и

$$(a, b) \cdot (c, d) \sim (a_1, b_1) \cdot (c_1, d_1).$$

Благодаря этой согласованности можно говорить об операциях на смежных классах, полагая:

$$\begin{aligned}[x] + [y] &= [x + y]; \\ [x] \cdot [y] &= [x \cdot y].\end{aligned}$$

Система $\langle B; +, \cdot \rangle$ и есть искомая алгебра, т. е. $\langle B; +, \cdot \rangle$ является кольцом и B содержит как подсистему систему целых неотрицательных чисел \mathbf{Z}_0 . Кроме того, каждый элемент из B является разностью элементов из \mathbf{Z}_0 , поэтому B — наименьшее кольцо, содержащее подкольцо \mathbf{Z}_0 .

Более того, это построенное кольцо B — ассоциативно-коммутативное с единицей. Из неравенств $a > b$ и $c > d$ следует, что $ac + bd > bc + ad$, а это значит, что в построенном кольце нет делителей нуля и, следовательно, построенное кольцо B целостное.

Итак, полукольцо натуральных чисел изоморфно вложено в целостное кольцо.

При доказательстве того, что алгебра B является кольцом, никаких особых свойств целых неотрицательных чисел не используется (более того, вкладывать можно было и систему натуральных чисел),

важно лишь, что аддитивная полугруппа $\langle \mathbb{Z}_0; + \rangle$ удовлетворяет закону сокращения (для каждого a, b, c из \mathbb{Z}_0):

$$a + b = a + c \Rightarrow b = c.$$

Иногда под словом «полукольцо» понимают только полукольца, в которых аддитивная полугруппа удовлетворяет закону сокращения (а нейтральный элемент не обязателен).

При этом договоре можно говорить о полукольце натуральных чисел, а предыдущее доказательство почти буквально переносится на все такие полукольца: *каждое полукольцо изоморфно вложимо в кольцо*.

При вложении полукольца в кольцо происходит одновременно и вложение его аддитивной полугруппы в группу. Важно лишь то, что эта полугруппа коммутативна и с сокращением. Вычленив из доказательства о вложении полуколец в кольца ту часть, которая касается только аддитивной полугруппы, получаем, что *каждая коммутативная полугруппа с сокращением изоморфно вложима в группу*.

Пусть K — кольцо с единицей e . Множество всех элементов K с операцией «сложение» образует группу, и в этой группе каждый элемент (в том числе и единичный) имеет порядок.

Порядок единичного элемента e в аддитивной группе кольца называют *характеристикой* кольца K и обозначают символом $\text{char } K$.

Иначе говоря, характеристика кольца равна такому наименьшему натуральному числу n , что $ne = 0$; а если такого числа n не существует (т. е. единица имеет бесконечный порядок), то характеристика кольца считается равной нулю. Например, характеристики всех ненулевых числовых колец нулевые, а характеристика кольца класса вычетов \mathbb{Z}_m равна m . Кольцо характеристики 1 состоит из одного нуля.

Если k — положительная характеристика кольца K и a — произвольный элемент из K , то $ka = 0$. Действительно,

$$k \cdot a = \underbrace{a + a + \dots + a}_k = a(\underbrace{e + e + \dots + e}_k) = a \cdot 0 = 0.$$

Это значит, что в кольце положительной характеристики k аддитивные порядки всех элементов являются делителями числа k . В частности, если характеристика кольца является простым числом p , то все ненулевые элементы этого кольца имеют аддитивный порядок, равный p .

Предположим, что характеристика кольца положительна и не проста, т. е. равна ab , где $1 < a$ и $1 < b$. Тогда

$$ab \cdot e = (a \cdot e)(b \cdot e) = 0,$$

причем $a \cdot e \neq 0$ и $b \cdot e \neq 0$. Следовательно, кольцо с положительной составной характеристикой содержит делители нуля.

Целостное кольцо не содержит делителей нуля, поэтому положительная характеристика целостного кольца должна быть простым числом.

Ассоциативность, коммутативность, наличие единицы и простая характеристика не гарантируют целостности кольца.

Групповое кольцо KG имеет такую же характеристику, что и кольцо K , но если в G есть элементы конечного порядка, то KG содержит делители нуля.

Прямое произведение двух ассоциативно-коммутативных колец с единицами и одной и той же характеристики p является снова ассоциативно-коммутативным, с единицей и с той же характеристикой p . Однако это прямое произведение содержит делители нуля, и потому нецелостное.

Например, кольцо подмножеств $\langle P(M); \oplus, \cap \rangle$ множества M , состоящего более чем из одного элемента, образует ассоциативно-коммутативное кольцо с единицей (роль ее играет само множество M), имеет характеристику 2. Кольцо $P(M)$ не является целостным кольцом — оно разложимо в прямое произведение подколец, поэтому в нем есть делители нуля.

Заметим, что в кольце множеств каждый элемент является идемпотентным: $X \cap X = X$ для каждого подмножества X .

Оказывается, что не только $\langle P(M); \oplus, \cap \rangle$, но и любое кольцо, в котором каждый элемент — идемпотент, имеет характеристику 2.

Действительно, поскольку $e + e$ — идемпотент,

$$(e + e)^2 = e + e.$$

При этом из закона дистрибутивности следует:

$$(e + e)^2 = (e + e)(e + e) = e^2 + e^2 + e^2 + e^2 = e + e + e + e.$$

Отсюда: $e + e = 0$. Отметим дополнительно, что кольцо, состоящее только из идемпотентов, коммутативно. Докажем это утверждение. Пусть x, y — два элемента из такого кольца; используя дистрибутивный закон и свойства идемпотентности, получаем:

$$(x + y)^2 = (x + y)(x + y) = x^2 + xy + yx + y^2 = x + xy + yx + y = x + y.$$

Из последнего равенства следует, что $xy + yx = 0$, а поскольку характеристика такого кольца равна двум, $xy = yx$.

Отметим, что в ненулевом кольце, в котором каждый элемент — идемпотент, коммутативность равносильна антикоммутативности, но тождество $x^2 = 0$ не выполняется. Это значит, что тождество $x^2 = 0$ сильнее тождества антикоммутативности.

Пусть K — ассоциативно-коммутативное кольцо с единицей и с простой характеристикой p . Покажем, что для любых a, b из K выполняются равенство

$$(a+b)^p = a^p + b^p.$$

Раскроем степень бинома по формуле Ньютона:

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \dots + \binom{p}{k}a^{p-k}b^k + \dots + b^p.$$

Каждый промежуточный коэффициент $\binom{p}{k}$ бинома (при $1 < k < p$) имеет вид

$$\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{1 \cdot 2 \cdot \dots \cdot k}.$$

Ни одно из чисел из $1 \cdot 2 \cdot \dots \cdot k$ не делит p , поэтому число $\binom{p}{k}$ делится на p . Поскольку $\text{char } K = p$, все промежуточные слагаемые исчезнут и разложение бинома примет вид

$$(a+b)^p = a^p + b^p.$$

Теперь индукцией по n проверяем, что в кольце K выполняется тождество (для любого n)

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

База (при $n = 1$) уже доказана, а доказательство шага индукции имеет вид

$$(a+b)^{p^n} = ((a+b)^{p^{n-1}})^p = (a^{p^{n-1}} + b^{p^{n-1}})^p = a^{p^n} + b^{p^n}.$$

Применим полученное тождество к элементам $(a-b)$ и b :

$$a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n}.$$

Отсюда:

$$(a-b)^{p^n} = a^{p^n} - b^{p^n}.$$

Кроме того, непосредственно из свойств ассоциативности и коммутативности умножения следует, что $(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n}$.

Эти наблюдения означают, что для любого натурального n в ассоциативно-коммутативном кольце с единицей и с простой характеристикой p множество всех решений уравнения $x^{p^n} = x$ образуют подкольцо. Кроме того, это значит, что для любого натурального n отображение, переводящее каждый элемент x в x^{p^n} , является гомоморфным (т. е. эндоморфизмом кольца).

Конечно, эти отображения не обязательно различны (а если в кольце выполняется тождество идемпотентности, то все эти гомоморфизмы единичные).

Вернемся вновь к произвольным ненулевым ассоциативным и ассоциативно-коммутативным кольцам с единицей. Поскольку нулевой элемент обладает поглощающим свойством, он не имеет обратного в таком кольце.

Однако может случиться, что все элементы кольца, кроме нуля, обратимы. Этот случай заслуживает особого внимания.

1.5. Поля

Полем называют ненулевое ассоциативно-коммутативное кольцо с единицей, в котором все ненулевые элементы обратимы.

Таким образом, кольцо $\langle K; +, \cdot \rangle$ — поле, если $\langle K \setminus \{0\}; \cdot \rangle$ — абелева группа, т. е., в частности, $K^* = K \setminus \{0\}$. В случае, когда $K^* = K \setminus \{0\}$, но умножение не обязательно коммутативно, K называют телом.

Поле — это коммутативное тело.

Множество $K \setminus \{0\} \neq \emptyset$, поэтому поле и тело состоят не менее чем из двух элементов. Если x, y — элементы поля и $xy = 0$, а $x \neq 0$, то $y = 0$. Это значит, что делитель нуля не имеет обратного: поле — это целостное кольцо. В частности, это означает, что поле неразложимо в прямое произведение подполей. В кольце положительной составной характеристики содержатся делители нуля, поэтому положительная характеристика поля должна быть простым числом.

Простая характеристика ассоциативно-коммутативного кольца с единицей не гарантирует даже целостности и тем более свойства «быть полем».

Поскольку умножение в поле коммутативно, можно говорить о делении на ненулевой элемент, понимая под отношением $\frac{a}{b}$ элемент $a \cdot b^{-1}$. Сложение и деление в поле связаны дистрибутивным законом (для каждого $a \neq 0, b, c$):

$$\frac{b+c}{a} = \frac{b}{a} + \frac{c}{a}.$$

Вычитание и деление в поле связаны дистрибутивным законом (для каждого $a \neq 0, b, c$):

$$\frac{b-c}{a} = \frac{b}{a} - \frac{c}{a}.$$

Правило знаков для поля не только при умножении, но и при делении, т. е. для любых элементов $a, b \neq 0$ из поля:

$$\frac{-a}{b} = \frac{a}{-b} = -\frac{a}{b} \text{ и } \frac{-a}{-b} = \frac{a}{b}.$$

Из школьного курса математики известны правила сравнения дробей (*основное свойство дроби*) и нахождения суммы, разности, произведения и частного двух дробей. Все эти правила основаны лишь на определении поля.

Для любых элементов a, b, c, d из поля ($b \neq 0, d \neq 0$) выполняются следующие утверждения:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c;$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd};$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d};$$

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd};$$

$$\frac{a}{b} : \frac{c}{d} = \frac{a \cdot d}{b \cdot c}, \quad c \neq 0.$$

Свойство «быть полем» абстрактное: алгебра, изоморфная полю, сама является полем. Пусть K — конечное ассоциативно-коммутативное кольцо без делителей нуля. Отсутствие делителей нуля равносильно выполнению закона сокращения. Если a — произвольный ненулевой элемент из K , то множество $Ka = \{xa \mid x \in K\}$ совпадает с K . Следовательно, мультипликативная полугруппа $\langle K^*; \cdot \rangle$, состоящая из ненулевых элементов K , — это полугруппа с делением. Каждая полугруппа с делением образует группу. Поэтому *каждое конечное целостное кольцо является полем*.

Рассмотрим примеры конечных целостных колец, т. е. конечных полей, причем начнем с наименьшего возможного числа элементов поля.

Наименьшее кольцо (группа, моноид, полугруппа) состоит из одного элемента. В поле должны находиться по крайней мере два элемента — нуль и единица. Построим сначала поле P из двух элементов. Множество этого поля — $\{0, 1\}$.

Таблица сложения должна быть таблицей группы, т. е. нуль — это нейтральный элемент, и каждый элемент должен иметь противоположный. Такая таблица возможна только одна:

+	0	1
0	0	1
1	1	0

Построение таблицы умножения основано на том факте, что нуль является поглощающим элементом кольца, а единица — нейтральным:

·	0	1
0	0	0
1	0	1

Построение алгебры $\langle P; +, \cdot \rangle$ закончено. Осталось проверить, что определенные сложение и умножения обладают нужными свойствами.

Проверка эта несложна, однако ее можно и не делать, а просто указать объект, изоморфный построенному и обладающий нужными свойствами. Множество \mathbb{Z} целых чисел разделим на два класса: класс A — четные числа и класс B — нечетные. Определим операции на классах по правилам:

$$A + B = \overset{\text{опр}}{\{a + b \mid a \in A, b \in B\}};$$

$$A \cdot B = \overset{\text{опр}}{\{a \cdot b \mid a \in A, b \in B\}}.$$

Таблицы действий будут иметь вид

+	A	B
A	A	B
B	B	A

·	A	B
A	A	A
B	A	B

Соответствие по правилу $A \mapsto 0, B \mapsto 1$ является изоморфизмом. Однако умножение и сложение классов основаны на умножении и сложении чисел, поэтому эти операции ассоциативны и связаны дистрибутивным законом.

Так, поле, состоящее из двух элементов, существует, и с точностью до изоморфизма это поле единственно. Обозначают это поле символом \mathbb{Z}_2 и называют *полем классов вычетов по модулю 2*.

В поле \mathbb{Z}_2 оба элемента идемпотенты, т. е. поле из двух элементов является булевым кольцом. Это то же самое булево кольцо подмножеств одноэлементного множества, которое появилось ранее. Заме-

тим, что это единственный пример алгебры, являющейся одновременно полем и булевым кольцом. Действительно, в булевом кольце все элементы — идемпотенты, в любом поле таких элементов в точности два: нуль и единица. Поле \mathbb{Z}_2 единственное, где других элементов, кроме 0 и 1, нет вовсе.

Построенный пример кольца классов вычетов по модулю 2 — всего лишь частный случай из бесконечной серии таких колец. Вместо двойки можно взять любое натуральное $m > 1$ и построить на множестве классов, равноостаточных при делении на m , кольцо классов вычетов \mathbb{Z}_m по модулю m . Однако при составном числе m кольцо \mathbb{Z}_m содержит делители нуля и (несмотря на то, что оно ассоциативно, коммутативно и с единицей) полем не является.

Если p — простое число, то произведение двух целых чисел, не делящихся на p , снова не делится на p . Это значит, что кольцо \mathbb{Z}_p не имеет делителей нуля и, следовательно, целостное. Напомним, что конечное целостное кольцо является полем, и, таким образом, для любого простого числа p найдется поле характеристики p (и более того, состоящее из p элементов).

Свойство «быть полем» абстрактное: алгебра, изоморфная полю, сама является полем. По аналогии с группами и кольцами сейчас следовало бы сказать о гомоморфных образах поля. В действительности, однако, ситуация с гомоморфизмами полей обстоит значительно проще.

Отображение кольца на нулевое кольцо называют нулевым гомоморфизмом. Для полей о таком гомоморфизме говорить нельзя (в поле должно быть не менее чем два элемента). Оказывается, что поле не имеет гомоморфизмов, отличных от изоморфизмов.

Пусть кольцо $P = \langle P; +, \cdot \rangle$ является полем, и φ — гомоморфизм этого кольца на кольцо P_1 . Если φ — не изоморфизм, то в поле P найдутся два различных элемента a и b , переходящих в один и тот же элемент из P_1 : $\varphi(a) = \varphi(b)$. Тогда $\varphi(a - b) = 0$. Но любой элемент x из P можно представить в виде

$$x = [x \cdot (a - b)^{-1}] \cdot (a - b),$$

поэтому

$$\varphi(x) = \varphi(x \cdot (a - b)^{-1}) \varphi(a - b) = 0.$$

Следовательно, любой гомоморфизм, не являющийся изоморфизмом, отображит любой элемент поля в нуль. Другими словами, *поле является простым кольцом*.

Отсюда следует, в частности, что если отображение φ поля P в некоторую алгебру сохраняет операции и при этом не переводит все элементы из P в один и тот же элемент, то φ взаимно однозначно.

Покажем, что любое целостное кольцо изоморфно вложимо в поле.

Пусть K — целостное кольцо. На множестве $M = K \times (K \setminus \{0\})$ определим операции сложения и умножения:

$$(a, b) + (c, d) \overset{\text{опр}}{\Leftrightarrow} (ad + bc, bd);$$

$$(a, b) \cdot (c, d) \overset{\text{опр}}{=} (ac, bd).$$

Кроме того, введем на множестве M отношение \sim по правилу

$$(a, b) \sim (c, d) \overset{\text{опр}}{=} ad = bc.$$

Это отношение рефлексивно, симметрично и транзитивно, т. е. является эквивалентностью, и эта эквивалентность согласована с операциями. Следовательно, операции можно определить над смежными классами $[x]$, $[y]$, полагая по определению:

$$[x] + [y] \overset{\text{опр}}{=} [x + y];$$

$$[x] \cdot [y] \overset{\text{опр}}{=} [x \cdot y].$$

Получившаяся в результате алгебра $\langle M / \sim; +, \cdot \rangle$ образует поле, и это поле содержит изоморфную копию кольца K . Таким образом, *каждое целостное кольцо изоморфно вложимо в некоторое поле.*

Наименьшее поле \bar{K} , содержащее целостное кольцо K , называется *полем частных* кольца K . Именно поле частных и построено в только что приведенном рассуждении.

Представление элементов поля частных в виде отношений элементов исходного кольца означает, что *поле частных \bar{K} целостного кольца K единственно с точностью до изоморфизма.*

Непустое подмножество H поля P называется *подполем* поля P , если H образует поле относительно тех же операций, что и P .

Подполе, в частности, является подкольцом, поэтому подполе H должно быть замкнуто относительно умножения и вычитания. Этих условий для того, чтобы быть подполем, недостаточно.

Если P — поле, а H — его подмножество, состоящее не из одного нуля, то H образует подполе тогда и только тогда, когда оно замкнуто относительно вычитания и деления на ненулевой элемент.

Пересечение любого числа подполей поля снова является подполем. В частности, пересечение P_0 всех подполей поля P тоже образует подполе, и P_0 уже не содержит собственных подполей. Подполе P_0 принято называть простым. Таким образом, каждое поле является расширением своего простого подполя.

Простое подполе порождается единичным элементом.

Наибольшее числовое поле — это поле комплексных чисел \mathbb{C} , а под *числовым полем* понимают любое подполе поля \mathbb{C} .

Наименьшее числовое поле — это поле рациональных чисел \mathbb{Q} .

Если T — произвольное тело нулевой характеристики, то подкольцо K , порожденное единицей, будет изоморфно кольцу целых чисел. Поле частных кольца K будет содержаться в теле T . Следовательно, каждое тело нулевой характеристики содержит в точности одно подполе, изоморфное полю рациональных чисел, и в точности одно подкольцо, изоморфное кольцу целых чисел.

Рассмотрим кольцо ненулевой простой характеристики. Напомним, что в ассоциативно-коммутативном кольце простой характеристики p множество H решений уравнения $x^{p^n} = x$ образует подкольцо.

Позже мы увидим, что множество корней многочлена степени m имеет не более чем m элементов (и, в частности, это множество конечно). Конечное целостное кольцо является полем, а его подкольцо — подполем. Следовательно, в конечном поле характеристики p множество решений уравнения $x^{p^n} = x$ всегда образует подполе.

Основные школьные системы целых, рациональных и действительных чисел не только являются кольцами (целые числа) и полями (рациональные и действительные числа), но и упорядочены отношением \leq .

Кольцо K упорядочиваемо, если в K можно выделить такое непустое подмножество K_+ , что:

а) K_+ замкнуто относительно сложения и умножения ($x, y \in K_+ \Rightarrow x + y, x \cdot y \in K_+$);

б) для каждого x из K выполняется одно из трех утверждений: $x = 0$, либо $x \in K_+$, либо $-x \in K_+$, т. е. множество K распадается на смежные классы: $K_+, -K_+, \{0\}$ ¹.

Множество K_+ называют множеством *положительных элементов* (или *конусом положительности*) кольца K .

Упомянутые числовые множества удовлетворяют этому определению, т. е. в них можно указать конус положительности.

С помощью унарного отношения «быть положительным» определяется бинарное отношение «больше».

Пусть кольцо K упорядочено с помощью подмножества положительных элементов K_+ . Так же, как в школьном курсе математики, определим бинарное отношение на множестве K по правилу

$$\overset{\text{опр}}{x < y} \Leftrightarrow y - x \in K_+.$$

Введенное таким образом отношение «меньше» обладает всеми привычными свойствами отношения порядка для числовых множеств и является отношением линейного порядка.

¹ Это свойство называют условием *трихотомии* (от греч. τριχότμειν — «разделяю на три»).

Сложение в упорядоченном кольце K монотонно относительно отношения $<$:

$$x < x_1, y < y_1 \Rightarrow x + y < x_1 + y_1.$$

Умножение на положительные элементы в упорядоченном кольце K монотонно относительно отношения $<$:

$$x < x_1, 0 < y < y_1 \Rightarrow xy < x_1 y_1.$$



Алгебры с двумя операциями

Удобно начинать изучать свойства отношений и операций на конечных объектах небольшой мощности. Неплохо бы и линейное упорядочение колец (и, в частности, полей) сначала рассмотреть на конечных объектах.

Эта идея, к сожалению, невыполнима, так как конечное кольцо не упорядочиваемо. Любое конечное подмножество кольца, замкнутое относительно сложения, является замкнутым и относительно взятия противоположного элемента; поэтому замкнутость K_+ относительно сложения и правило трихотомии для конечного множества K_+ невыполнимы. Это значит, что конус положительности линейно упорядоченного кольца и поля всегда бесконечен.

В заключение данного пункта темы еще раз вспомним связь между множествами основных алгебр с двумя операциями.

Поля — это частные случаи тел, а те, в свою очередь, частные случаи колец, кольца — частные виды полуколец. Важнейшим из числовых полей является поле комплексных чисел.

1.6. Поле комплексных чисел

В кольце целых чисел разрешимы не все уравнения первой степени, т. е. уравнения вида $ax + b = 0$, где $a \neq 0$. Однако в поле рациональных чисел все такие уравнения уже разрешимы.

Можно сказать, что поле рациональных чисел получилось присоединением к кольцу целых чисел всех корней многочленов первой степени.

Расширение поля \mathbf{Q} до поля \mathbf{R} действительных чисел произошло в связи с задачами, связанными с измерением. Тем самым к рациональным числам присоединены корни многих алгебраических уравнений, но и над полем действительных чисел есть уравнения, не имеющие решений в поле \mathbf{R} .

Простейшим примером такого уравнения будет $x^2 + 1 = 0$.

Наименьшее поле, которое содержит подполе действительных чисел и решение уравнения $x^2 + 1 = 0$, называют *полем комплексных чисел*. Одно из решений уравнения $x^2 + 1 = 0$ обозначают буквой i и называют *мнимой единицей* (второе решение — это $-i$). Поле комплексных чисел обозначают символом \mathbf{C} .

Доказательства существования поля \mathbf{C} можно провести конструктивно, т. е. с помощью теоретико-множественных операций построить поле \mathbf{C} , используя поле \mathbf{R} как исходный материал.

Подобно тому, как в элементарной геометрии решаются задачи на построение с помощью циркуля и линейки, при построении поля \mathbf{C} также можно сначала провести *анализ*, т. е. предположить, что поле \mathbf{C} существует, и посмотреть, что из этого следует.

Анализ. Пусть поле комплексных чисел существует. Тогда среди элементов этого поля должны содержаться и все числа вида $a + bi$, где a, b — действительные числа и $i^2 + 1 = 0$. Такое представление числа будет единственным (в противном случае i окажется действительным числом, а это не так). Единственность, в частности, означает, что если $a + bi = 0$, то $a = b = 0$.

Теперь из аксиом поля следует, что если $z_1 = a + bi$, $z_2 = c + di$ — два комплексных числа, то

$$\begin{aligned} z_1 + z_2 &= (a + bi) + (c + di) = (a + c) + (b + d)i; \\ z_1 \cdot z_2 &= (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i. \end{aligned}$$

Таким образом, множество M чисел вида $a + bi$, где $a, b \in \mathbf{R}$ и $i^2 = -1$, замкнуто относительно сложения и умножения.

Замкнуто оно и относительно вычитания:

$$(a + bi) - (c + di) = (a - c) + (b - d)i$$

и относительно деления на ненулевой элемент:

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i.$$

Таким образом, множество M само является полем, и это поле содержит \mathbf{R} и i .

Однако \mathbf{C} — минимальное с такими свойствами, поэтому множество M совпадает с множеством \mathbf{C} .

Итак, если поле комплексных чисел существует, то каждое комплексное число имеет вид $a + bi$, где a, b — действительные числа и $i^2 + 1 = 0$.

Анализ закончен.

Теперь можно построить поле \mathbb{C} , взяв в качестве его множества декартов квадрат $\mathbb{R} \times \mathbb{R}$ и определив арифметические операции так, как подсказывает анализ задачи.

Разумеется, после построения (описания множества-носителя и операций на нем) следует провести доказательство того, что построено именно то, что и хотели.

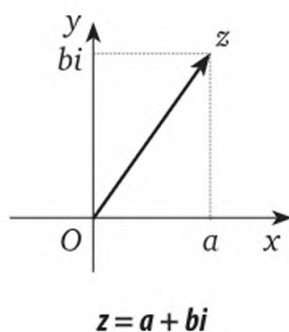
Проверка аксиоматики и требуемых свойств построенного поля вполне рутинная.

Таким образом, верно следующее утверждение: если существует поле действительных чисел, то существует и поле комплексных чисел.

Как и в элементарной геометрии, не лишен смысла вопрос о числе решений этой задачи, т. е. вопрос: сколько существует различных полей комплексных чисел? Разумеется, как обычно в алгебре, изоморфные поля не считаются различными. Главный результат проведенного анализа о виде комплексного числа позволяет легко ответить и на этот вопрос.

Если все поля действительных чисел изоморфны, то изоморфны и поля комплексных чисел. Другими словами, существует единственное поле комплексных чисел. На логическом языке это значит, что если аксиоматика действительных чисел категорична, то категорична и аксиоматика поля комплексных чисел.

Представление комплексного числа z в виде $z = a + bi$, где a, b — действительные числа и $i^2 + 1 = 0$, называют *алгебраической формой*.



Если предположить, что одно и то же комплексное число имеет две различные алгебраические формы, то, как следствие, получится, что число i действительное.

Каждое комплексное число имеет единственную алгебраическую форму.

Первое слагаемое алгебраической формы принято называть *действительной частью*, а действительный множитель второго слага-

емого называют *мнимой частью* числа. Для них приняты обозначения:

$$a = \operatorname{Re} z;$$

$$b = \operatorname{Im} z,$$

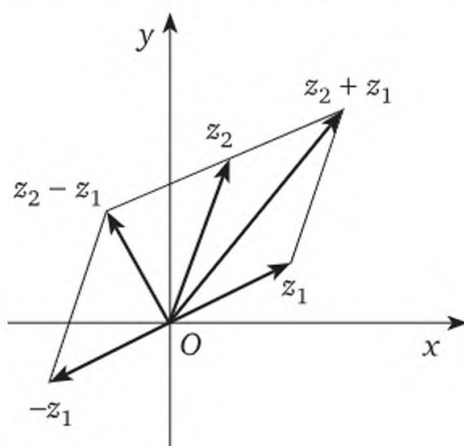
т. е. $Z = \operatorname{Re} z + \operatorname{Im} z \cdot i$.

Множество действительных чисел наглядно изображается в виде числовой прямой.

Множество комплексных чисел находится во взаимно однозначном соответствии с декартовым квадратом $\mathbf{R} \times \mathbf{R}$ множества \mathbf{R} , который наглядно изображается координированной плоскостью.

Каждое комплексное число можно представить точкой на плоскости с декартовыми прямоугольными координатами. На оси абсцисс комплексной плоскости находятся действительные части комплексных чисел, поэтому ее называют иногда *действительной осью*, а ось ординат — соответственно, *мнимой осью*.

Каждая точка плоскости изображает одно комплексное число, и наоборот — комплексное число изображается одной точкой. Можно соединить начало координат с этой точкой, и, таким образом, каждое комплексное число будет изображено радиус-вектором.



Сложение и вычитание комплексных чисел

Двумерные векторы над полем действительных чисел так же, как и комплексные числа, представляются парами действительных чисел, и сложение векторов происходит также покомпонентно (первая координата складывается с первой, а вторая — со второй).

Сложение комплексных чисел происходит тоже покомпонентно (если компонентами назвать действительную и мнимую части). Это значит, что при сложении комплексных чисел векторы, их изображающие, складываются по правилу параллелограмма.

Как в векторах с операциями сложения, так и в комплексных числах с той же операцией есть нечто общее: обе эти системы являются прямыми суммами двух групп $\langle \mathbf{R}; + \rangle$.

Итак, аддитивная группа комплексных чисел является прямой суммой аддитивных групп действительных чисел:

$$\mathbf{C} = \mathbf{R} \oplus \mathbf{R}.$$

У поля действительных чисел нет ни одного нетривиального автоморфизма.

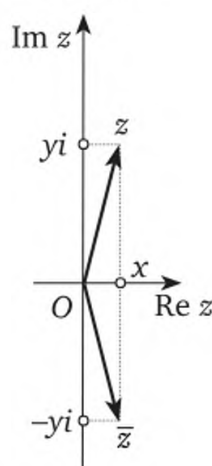
Геометрическая иллюстрация поля \mathbf{C} подсказывает, что по крайней мере один неединичный автоморфизм в группе автоморфизмов $\text{Aut}(\mathbf{C})$ поля \mathbf{C} есть¹.

Геометрические соображения следующие: осевая симметрия в действительной оси является взаимно однозначным отображением комплексной плоскости на себя и явно сохраняет операцию сложения. Остается проверить только сохранение умножения.

Введем более точное определение.

Пусть $z = x + yi$ — произвольное комплексное число. Число $x - yi$ называют сопряженным с числом z и обозначают символом \bar{z} .

Из определения видно, что отображение $z \mapsto \bar{z}$ является взаимно однозначным, и $\bar{\bar{z}} = z$ тогда и только тогда, когда z — действительное число. Кроме того, непосредственным вычислением проверяется, что $z_1 + z_2 = \bar{z}_1 + \bar{z}_2$, $z_1 \cdot z_2 = \bar{z}_1 \cdot \bar{z}_2$.



Комплексно сопряженные числа

Все это вместе означает, что отображение, переводящее число в комплексно сопряженное, является автоморфизмом поля комплексных чисел. Этот автоморфизм оставляет поле действительных чисел неподвижным: если z — действительное число, то $\bar{z} = z$.

Если числа z и \bar{z} сопряженные, то $z + \bar{z}$ и $z \cdot \bar{z}$ принадлежат \mathbf{R} . Поэтому если $z \neq \bar{z}$, то эти числа являются корнями одного и того же многочлена второй степени с действительными коэффициентами.

¹ На самом деле $|\text{Aut}(\mathbf{C})| > \aleph$.

Впрочем, про многочлены с действительными коэффициентами любой положительной степени можно сказать больше.

Если число z является корнем многочлена $f(z)$ с действительными коэффициентами, то и \bar{z} — тоже корень этого многочлена.

Для доказательства достаточно подействовать автоморфизмом «переход к сопряженному» на равенство $f(z) = 0$, в результате чего появится нужное равенство $f(\bar{z}) = 0$.

Это означает, что на комплексной плоскости корни многочлена с действительными коэффициентами расположены симметрично относительно действительной оси.

В поле действительных чисел аддитивная группа оказалась изоморфной мультипликативной группе положительных действительных чисел.

Точного аналога этому факту в поле комплексных чисел нет по простой причине: поле комплексных чисел не упорядочиваемо (поэтому там нет понятий «положительный» и «отрицательный»). Действительно, если бы конус положительности \mathbb{C}_+ существовал, то любое из предположений $i \in \mathbb{C}_+$ или $-i \in \mathbb{C}_+$ приводило бы к противоречию.

Зададим на комплексной плоскости полярные координаты, положив началом координат точку O и выбрав в качестве полярной оси положительное направление действительной оси.

Полярный радиус — расстояние r от точки z до начала координат — называют *модулем* числа z . Обозначается модуль так же, как модуль действительного числа $|z|$.

Полярный угол φ точки z (угол, на который нужно повернуть полярную ось до совмещения ее с направлением на точку z) принято называть *аргументом* числа z .

Аргумент обозначается символом $\arg z$.

Аргумент определен с точностью до кратных 2π . Поэтому принято считать, что

$$-\pi \leq \arg z \leq \pi,$$

а символом $\text{Arg } z$ — обозначать $\arg z + 2\pi k$, где $k \in \mathbb{Z}$.

Аргумент для нуля не определен, но нулевое число, впрочем, и не нуждается в аргументах: нуль полностью задается своим модулем.

Если же ненулевое число z задано в алгебраической форме $z = a + bi$, то модуль $|z| = \sqrt{a^2 + b^2}$, а аргумент можно вычислить с помощью уравнений

$$\sin \arg z = \frac{b}{\sqrt{a^2 + b^2}}, \quad \cos \arg z = \frac{a}{\sqrt{a^2 + b^2}}.$$

Эти два равенства определяют $\arg z$ однозначно с точностью до сравнимости по модулю 2π . Точнее, если φ_1 и φ_2 — два решения системы уравнений

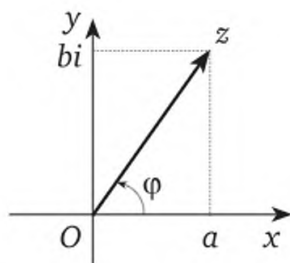
$$\begin{cases} \cos \varphi = c, \\ \sin \varphi = d, \end{cases}$$

то $\varphi_1 \equiv \varphi_2 \pmod{2\pi}$, т. е. $\varphi_1 = \varphi_2 + 2\pi k$, где k — целое число.

Таким образом осуществляется переход от декартовой системы координат к полярной системе на комплексной плоскости.

Пусть, наоборот, заданы полярные координаты комплексного (ненулевого) числа z :

$$|z| = r, \arg z = \varphi.$$



Тригонометрическая форма z

Тогда алгебраическую форму $a + bi$ числа z можно найти по формулам

$$a = r \cos \varphi, \quad b = r \sin \varphi.$$

Подставим в представление числа $z = a + bi$ вместо a, b эти значения и получим новое выражение для z :

$$z = r(\cos \varphi + i \sin \varphi).$$

Такое представление комплексного числа называют *тригонометрической формой*.

Тригонометрическая формула одновременно представляет число и в декартовых координатах (достаточно раскрыть скобки), и в полярных (в ней участвуют как модуль, так и аргумент числа).

Используя единственность алгебраической формы и равенство $\cos^2 \varphi + \sin^2 \varphi = 1$, получаем утверждение о единственности тригонометрической формы: если $r_1(\cos \varphi + i \sin \varphi)$ и $r_2(\cos \psi + i \sin \psi)$ — две тригонометрические формы одного и того же комплексного числа, то $r_1 = r_2$ и $\varphi \equiv \psi \pmod{2\pi}$.

Алгебраическую форму комплексного числа можно было взять произвольно — каждая пара действительных чисел a, b однозначно

задает комплексное число $a + bi$. То же самое (при естественных ограничениях) верно и для тригонометрической формы.

Для каждого действительного числа $r > 0$ и каждых действительных α, β , таких, что $\alpha^2 + \beta^2 = 1$, существует единственное комплексное число z , имеющее тригонометрическую форму

$$z = r(\cos \varphi + i \sin \varphi),$$

где $\cos \varphi = \alpha$, $\sin \varphi = \beta$.

Модуль комплексного числа $z = a + bi$, как и модуль действительного, — это расстояние от точки, изображающей число, до начала координат.

Если $b = 0$, то число z действительное и новое понятие модуля в точности совпадает со старым определением модуля.

Модуль произведения действительных чисел равен произведению модулей.

Это свойство распространяется на все комплексные числа: *модуль произведения комплексных чисел равен произведению модулей сомножителей.*

Последнее утверждение можно проверить непосредственным вычислением, а можно воспользоваться тождеством $|z| = \sqrt{z \cdot \bar{z}}$. Отметим, что, зная, как выглядит выражение для модуля, из равенства $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$, где α, β — произвольные комплексные числа, можно получить чисто арифметический факт: произведение сумм двух квадратов целых чисел само является суммой двух квадратов.

Продолжим перечисление свойств модуля комплексных чисел, взяв за основу свойства модуля действительных чисел. Как и для действительных чисел, для произвольных комплексных чисел α, β выполняются следующие неравенства:

- а) $|\alpha + \beta| \leq |\alpha| + |\beta|$;
- б) $|\alpha - \beta| \leq |\alpha| + |\beta|$;
- в) $|\alpha + \beta| \geq |\alpha| - |\beta|$;
- г) $|\alpha - \beta| \geq |\alpha| - |\beta|$.

Первое из них называют *неравенством треугольника*: длины векторов $\alpha, \beta, \alpha + \beta$ — это длины сторон этого треугольника.

Кроме свойства $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$, для любых действительных чисел α, β выполняется еще *правило знаков*:

$$(-\alpha)\beta = \alpha(-\beta) = -\alpha\beta \text{ и } (-\alpha)(-\beta) = \alpha\beta.$$

Знак действительного числа — это множитель, равный 1 или -1 . В случае комплексных чисел знак превращается в комплексное число, модуль которого равен единице. Правило знаков принимает другой вид: для любых комплексных чисел α, β

$$\operatorname{Arg}(\alpha \cdot \beta) = \operatorname{Arg} \alpha + \operatorname{Arg} \beta.$$

Действительно, если

$$\alpha = r_1(\cos \varphi_1 + i \sin \varphi_1), \quad \beta = r_2(\cos \varphi_2 + i \sin \varphi_2),$$

то

$$\alpha \cdot \beta = r_1 r_2 [\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)].$$

Итак, при умножении комплексных чисел их модули перемножаются, а аргументы складываются.

Для действительных чисел аргумент принимает лишь два значения: 0 и π . В первом случае знак равен единице, а во втором — минус единице. Правило знаков — это следствие свойства аргумента произведения.

Если число α представлено радиус-вектором α , то умножение α на число β означает, что вектор α поворачивается на угол $\arg \beta$, а модуль вектора α растягивается (или сжимается) в $|\beta|$ раз.

Если $|\beta| = 1$, то умножение на число β сводится лишь к повороту вектора α на некоторый угол.

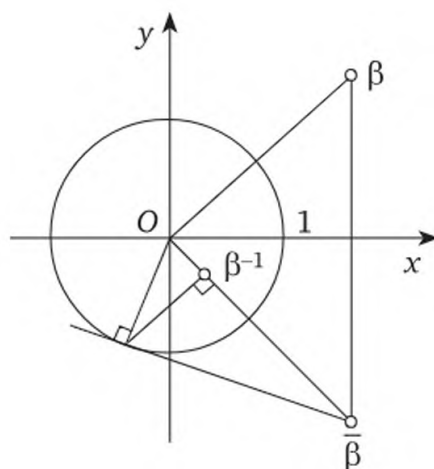
Деление (на ненулевое число) является операцией, обратной умножению, поэтому для любых комплексных чисел α, β ($\beta \neq 0$)

$$\left| \frac{\alpha}{\beta} \right| = \frac{|\alpha|}{|\beta|} \text{ и } \arg \left(\frac{\alpha}{\beta} \right) = \arg \alpha - \arg \beta.$$

Если число $\beta \neq 0$, то

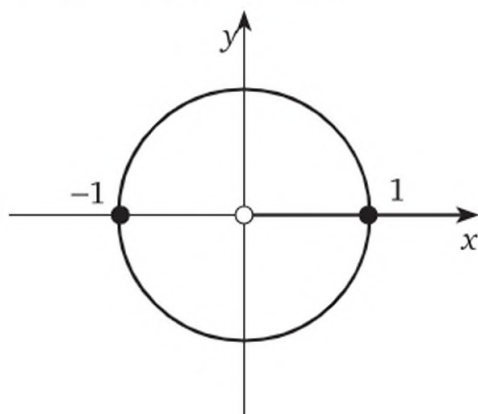
$$|\beta^{-1}| = |\beta|^{-1}, \quad \arg \beta^{-1} = -\arg \beta.$$

Последнее замечание означает, что геометрически комплексное число β^{-1} получается из числа β композицией осевой симметрии в оси абсцисс и инверсии в окружности единичного радиуса с центром в начале координат. На рисунке изображено соответствующее построение.



Построение β^{-1}

Правило знаков для действительных чисел означает, что мультипликативная группа ненулевых действительных чисел является прямым произведением мультипликативной группы положительных действительных чисел и группы, состоящей из действительных чисел, модуль которых равен единице.



Группа $\langle \mathbb{C} \setminus \{0\}; \cdot \rangle$

Мультипликативная группа ненулевых комплексных чисел является прямым произведением мультипликативной группы положительных действительных чисел и группы, состоящей из комплексных чисел, модуль которых равен единице.

На рисунке черным цветом выделены прямые множители мультипликативной группы ненулевых комплексных чисел.

Разложим функции e^x , $\cos x$ и $\sin x$ в ряды Тейлора:

$$e^x = 1 + \frac{x}{1!} + \dots + \frac{x^n}{n!} + \dots;$$

$$\sin x = x - \frac{x^3}{3!} + \dots + (-1)^n \frac{x^{2n+1}}{(2n+1)!} + \dots;$$

$$\cos x = 1 - \frac{x^2}{2!} + \dots + (-1)^n \frac{x^{2n}}{(2n)!} + \dots$$

Если теперь ряд для $\sin x$ умножить на i :

$$i \sin x = ix - i \frac{x^3}{3!} + \dots + i(-1)^n \frac{x^{2n+1}}{(2n+1)!} + \dots,$$

а затем сложить с рядом для $\cos x$, то получим ряд для e^{ix} :

$$e^{ix} = 1 + \frac{ix}{1!} - \frac{x^2}{2!} + \dots + i^n \frac{x^n}{n!} + \dots$$

Таким образом,

$$e^{ix} = \cos x + i \sin x.$$

Последнее тождество называют *формулой Эйлера*¹.
Из формулы Эйлера следует, что

$$re^{i\varphi} = r(\cos \varphi + i \sin \varphi).$$

Если $r > 0$, то выражение справа — это тригонометрическая форма комплексного числа. Выражение слева называют *экспоненциальной* (показательной) формой комплексного числа.

Этой же форме можно придать другой вид. Для любого действительного числа a число e^a положительно, поэтому любое ненулевое комплексное число можно представить в виде

$$e^{a+bi} = e^a(\cos b + i \sin b).$$

Умножение и деление в экспоненциальной форме подтверждают свойства модуля и аргумента, полученные ранее с помощью тригонометрической формы:

$$\begin{aligned} n_1 e^{i\alpha} \cdot r_2 e^{i\beta} &= n_1 r_2 e^{i(\alpha+\beta)}; \\ \frac{r_1 e^{i\alpha}}{r_2 e^{i\beta}} &= \frac{r_1}{r_2} e^{i(\alpha-\beta)}. \end{aligned}$$

Отметим, что для $x = \pi$ формула Эйлера принимает вид

$$e^{i\pi} = -1.$$

Перенесем -1 в левую часть равенства и в результате получим загадочную связь между всеми важнейшими константами математики ($e, \pi, i, 1, 0$):

$$e^{i\pi} + 1 = 0.$$

Используя индукцию по n , для равных множителей получаем следующее равенство (для каждого натурального числа n):

$$[r(\cos \varphi + i \sin \varphi)]^n = r^n(\cos n\varphi + i \sin n\varphi).$$

В честь автора эту формулу называют *формулой Муавра*².

Возвести комплексное число в натуральную степень n можно и с помощью бинома Ньютона.

Используя для возведения в степень числа $z = \cos \varphi + i \sin \varphi$ формулу Муавра и единственность алгебраической формы комплексного числа, можно получить школьные формулы, выражающие $\cos 2\varphi$, $\sin 2\varphi$, $\cos 3\varphi$, $\sin 3\varphi$ через $\cos \varphi$ и $\sin \varphi$.

¹ Леонард Эйлер (Euler, 1707—1783) — российский математик швейцарского происхождения.

² Абрахам де Муавр (Moivre, 1667—1754) — английский математик французского происхождения.

Впрочем, с помощью бинома Ньютона можно получить сразу общее выражение (для любого натурального n):

$$\cos nx = \cos^n x - \binom{2}{n} \cos^{n-2} x \sin^2 x + \binom{4}{n} \cos^{n-4} x \sin^4 x - \dots;$$

$$\sin nx = n \cos^{n-1} x \sin x - \binom{3}{n} \cos^{n-3} x \sin^3 x + \binom{5}{n} \cos^{n-5} x \sin^5 x - \dots$$

Своему происхождению поле комплексных чисел обязано невозможности извлечения корня квадратного из отрицательного числа в поле действительных чисел. Само поле \mathbb{C} по такой причине расширять не придется — в поле комплексных чисел извлекается корень любой степени из любого числа.

Используя формулу Муавра и единственность тригонометрической формы комплексного числа (более точно — единственность аргумента по модулю 2π), получаем формулу для нахождения корня n -й степени из любого комплексного числа α (эту формулу также получил А. де Муавр и ее также называют *формулой Муавра*¹).

Если комплексное число $\alpha = r(\cos \varphi + i \sin \varphi)$ отлично от нуля, то уравнение $z^n = \alpha$ имеет в точности n различных решений z_0, z_1, \dots, z_{n-1} , которые можно найти по формуле

$$z_k = \sqrt[n]{r} \left(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right),$$

где $k = 0, 1, \dots, n-1$.

Заметим, что все эти z_k имеют один и тот же модуль, поэтому находятся на окружности с радиусом $\sqrt[n]{r}$ и с центром в начале координат. Более того, каждый новый корень можно получить из предыдущего умножением на число

$$\left(\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \right),$$

т. е. поворотом на угол $\frac{2\pi}{n}$.

Таким образом, если комплексное число α отлично от нуля, то все корни n -й степени из α расположены в вершинах правильного n -угольника, вписанного в окружность с радиусом $\sqrt[n]{|\alpha|}$ и с центром в начале координат.

При решении уравнения $z^2 = \alpha$, где α — положительное действительное число, получается два значения. Одно из них $\sqrt{\alpha}$ — ариф-

¹ Эти формулы были получены А. де Муавром в 1707 г., современная запись предложена Л. Эйлером в 1748 г.

метический корень из числа α , второе получается умножением $\sqrt{\alpha}$ на -1 . Если бы взяли сначала корень $-\sqrt{\alpha}$, то снова умножением на 1 и -1 получаем все корни этого уравнения. Числа 1 и -1 — это решения уравнения $z^2 = 1$, т. е. корни второй степени из единицы.

В поле комплексных чисел эта идея (получить все корни из одного корня умножением его на корни из единицы) получает естественное обобщение.

Решение уравнения $z^n = 1$ называют *корнем n -й степени из единицы*. Обычно корни из единицы обозначают символ ϵ_k . Все свойства произвольных корней из ненулевого комплексного числа, разумеется, переносятся и на корни из единицы.

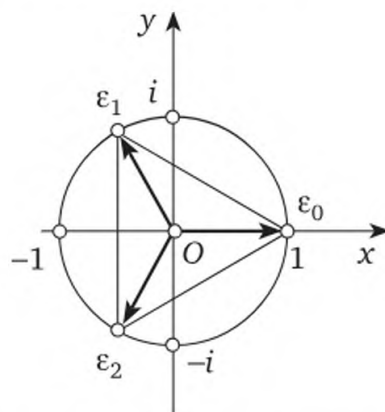
С учетом того, что все ϵ_k имеют модуль 1 , получаем, что корни n -й степени из единицы имеют вид

$$\epsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n},$$

где $k = 0, 1, 2, \dots, n-1$.

Для каждого натурального числа n существует n различных корней n -й степени из единицы.

Корни n -й степени из единицы расположены в вершинах правильного n -угольника, вписанного в окружность с единичным радиусом и с центром в начале координат.



Корни 3-й степени из единицы

Пусть M — множество всех корней n -й степени из единицы. Единица принадлежит M , кроме того, M замкнуто относительно умножения и взятия обратного. Множество корней n -й степени из единицы образует мультипликативную группу.

Обычно слово «мультипликативная» в этом случае лишь подразумевают и говорят просто о *группе корней n -й степени из единицы*.

В отличие от общей ситуации многоугольник корней n -й степени из единицы легко изобразить — одна из вершин этого n -угольника известна ($\epsilon_0 = 1$).

Непосредственно из формул для корней видно, что

$$\varepsilon_k = \varepsilon_1^k,$$

а это значит, что все корни n -й степени из единицы можно получить из корня

$$\varepsilon_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

с помощью возведения его в степень.

Группа корней n -й степени из единицы порождается одним элементом; т. е. эта группа циклическая.

Элемент, порождающий группу корней n -й степени из единицы, называют *первообразным корнем*.

Иначе говоря, комплексное число ε называют *первообразным корнем n -й степени из единицы*, если любой корень n -й степени из единицы получается из числа ε возведением в некоторую степень с целым показателем.

Кроме ε_1 , в группе корней n -й степени из единицы могут оказаться и другие корни, обладающие тем же свойством. Если два целых числа взаимно просты, то существуют целые u , v такие, что $au + bv = 1$. Используя это свойство, получаем следующее утверждение: число

$$\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$$

является первообразным корнем n -й степени из единицы тогда и только тогда, когда $\text{НОД}(n, k) = 1$.

Отметим дополнительно, что если

$$m = \frac{n}{\text{НОД}(n, k)},$$

то число

$$\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$$

является первообразным корнем m -й степени из единицы.

Если β — какое-нибудь решение уравнения $z^n = \alpha$ и $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}$ — корни n -й степени из единицы, то $\{\beta\varepsilon_0, \beta\varepsilon_1, \dots, \beta\varepsilon_{n-1}\}$ образует все множество решений этого уравнения. Если β — какое-нибудь решение уравнения $z^n = \alpha$, а ε — первообразный корень n -й степени из единицы, то $\{\beta, \beta\varepsilon, \beta\varepsilon^2, \dots, \beta\varepsilon^{n-1}\}$ является множеством решений этого уравнения.

Сделаем еще несколько дополнительных замечаний.

Используя школьную формулу для суммы членов геометрической прогрессии, получаем, что сумма всех корней n -й степени из единицы равна нулю.

Рассмотрим теперь корни из единицы различных степеней. Используя непосредственно тригонометрическую форму корня из единицы и свойство взаимно простых чисел, получаем, что если m и n взаимно просты, то произведение первообразных корней m -й и n -й степеней из единицы является первообразным корнем mn -й степени из единицы.

Обозначим символом G_k группу корней k -й степени из единицы. Последнее замечание о первообразных корнях означает, что если m и n взаимно просты, то группа G_{mn} корней mn -й степени из единицы является прямым произведением групп G_m и G_n .

Это достаточное условие разложимости группы корней из единицы в прямое произведение является и необходимым. Сформулируем его сначала на арифметическом языке, а затем в групповых терминах:

1) если m и n не взаимно просты, то произведение первообразных корней m -й и n -й степеней из единицы не является первообразным корнем mn -й степени из единицы;

2) если m и n не взаимно просты, то группа G_{mn} корней mn -й степени из единицы не является прямым произведением групп G_m и G_n .

Числовым полем называют любое подполе поля комплексных чисел.

Поле \mathbf{Q} рациональных чисел, поле \mathbf{R} действительных чисел, поле \mathbf{C} комплексных чисел — три примера числовых полей.

Непустое подмножество множества комплексных чисел образует числовое поле тогда и только тогда, когда оно состоит более чем из одного элемента и замкнуто относительно сложения, вычитания, умножения и деления не на нуль.

По определению, *наибольшее числовое поле* — это поле \mathbf{C} комплексных чисел.

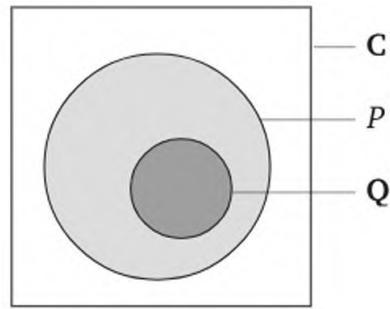
Каждое поле должно содержать единицу, а вместе с единицей и все кратные и единицы, и ее противоположной, а также все отношения этих кратных.

Иначе говоря, *наименьшее числовое поле* — это поле \mathbf{Q} рациональных чисел.

Таким образом, каждое числовое поле P является промежуточным между полем \mathbf{Q} рациональных чисел и полем \mathbf{C} комплексных чисел:

$$\mathbf{Q} \subset P \subset \mathbf{C}.$$

Заметим, что для решения уравнения $x^2 + 1 = 0$ вовсе не требуется большое (несчетное) поле комплексных чисел.



P — числовое поле

Присоединим мнимую единицу i к полю рациональных чисел, т. е. рассмотрим наименьшее числовое поле, содержащее число i . Те же соображения, что были проведены при построении поля комплексных чисел, показывают, что наименьшее числовое поле, содержащее элемент i , состоит из всех комплексных чисел вида $a + bi$, где a, b — рациональные числа.

Впрочем, еще до появления мнимой единицы можно было отметить числа, не принадлежащие полю Q . Классическим примером является неразрешимость в поле Q уравнения $x^2 - 2 = 0$. Если бы это был единственный недостаток поля рациональных чисел, то для его устранения вовсе не требовалось бы такое большое (несчетное) поле действительных чисел.

Точно такая же проверка, как для комплексных чисел, показывает, что наименьшее числовое поле, содержащее число $\sqrt{2}$, состоит из всех действительных чисел вида $a + b\sqrt{2}$, где a, b — рациональные числа.

Как и для любой алгебры, для полей можно говорить о подалгебре, порожденной некоторым множеством.

Пересечение любого числа числовых полей снова является числовым полем.

Поэтому если M — произвольное непустое множество комплексных чисел, то существует наименьшее поле, содержащее множество M .

Поскольку любое числовое поле содержит поле рациональных чисел, можно считать, что M присоединяется к полю Q . Пишут в таком случае о поле $Q(M)$.

В рассмотренных ранее примерах речь шла о присоединении i или $\sqrt{2}$ к полю Q , т. е. мы увидели, как устроены поля $Q(i)$ и $Q(\sqrt{2})$.

Заметим, что поля $Q(i)$ и $Q(\sqrt{2})$ счетны. Вспоминая свойства счетных множеств, видим, что и в других случаях, присоединяя к полю Q один элемент или конечное число элементов, мы получим лишь счетное поле. Более того, если множество M счетно, то и поле, порожденное множеством M , тоже счетно.

В несчетном множестве S найдется несчетное множество счетных подмножеств, порождающих различные поля. Поэтому суще-

ствуется не менее континуума различных числовых полей. Вполне может оказаться, что некоторые из этого множества числовых полей изоморфны (в действительности так оно и есть). Укажем для начала счетную серию попарно неизоморфных полей.

Чтобы легче увидеть неизоморфизм числовых полей, отметим сначала простое свойство изоморфизма: при изоморфизме числовых полей поле рациональных чисел остается неподвижным.

Последнее предложение означает, что если P_1 и P_2 — два числовых поля и f — изоморфное отображения поля P_1 на поле P_2 , то для каждого x из \mathbf{Q} $f(x) = x$.

Если бы поля $\mathbf{Q}(i)$ и $\mathbf{Q}(\sqrt{2})$ были изоморфны, то изоморфизм оставлял бы подполе рациональных чисел неподвижным. Уравнение $x^2 + 1 = 0$ имеет решение в поле $\mathbf{Q}(i)$, поэтому оно должно иметь решение и в поле $\mathbf{Q}(\sqrt{2})$. Пусть $a + b\sqrt{2}$ — решение этого уравнения, т. е.

$$(a + b\sqrt{2})^2 = -1.$$

Ни a , ни b не могут быть нулевыми (в противном случае квадрат действительного числа оказался бы отрицательным). Раскроем скобки и найдем выражение для числа $\sqrt{2}$:

$$\sqrt{2} = \frac{-1 - a^2 - 2b^2}{2ab}.$$

Число, стоящее справа в этом равенстве, рационально. Полученное противоречие показывает, что уравнение $x^2 + 1 = 0$ не имеет решения во втором поле. Эти поля обладают различными свойствами: они не изоморфны.

Число i — это $\sqrt{-1}$. Действуя таким же образом, как при доказательстве неизоморфизма полей $\mathbf{Q}(\sqrt{-1})$ и $\mathbf{Q}(\sqrt{2})$, обнаружим, что если p и q — различные простые числа, то поля $\mathbf{Q}(\sqrt{p})$ и $\mathbf{Q}(\sqrt{q})$ не изоморфны.

Множество простых чисел бесконечно (счетно), поэтому множество попарно неизоморфных числовых полей (даже подполей поля \mathbf{R}) не менее чем счетно.

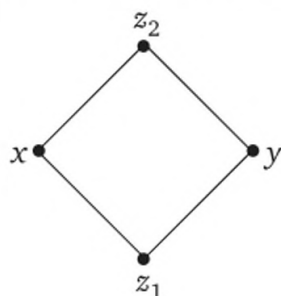
1.7. Булевы алгебры

Есть алгебра, которая связана с изучением любой алгебры или алгебраической системы. Такой алгеброй является *решетка*.

Если U — подмножество упорядоченного множества $\langle M; \leq \rangle$, то любой элемент x из M (не обязательно принадлежащий U) называют *верхней гранью* множества U , если $u \leq x$ для каждого элемента u из U .

Поменяв в определении верхней грани символ \leq на символ \geq , получим определение *нижней грани*.

На графе отношения порядка изображены верхняя грань (элемент z_2) и нижняя грань (элемент z_1) для двух элементов x, y .



Элемент m_0 из множества H называют *наименьшим* в H , если для любого h из H выполняется неравенство $m_0 \leq h$. Элемент m_1 из H называется *наибольшим* в H , если для любого h из H выполняется неравенство $h \leq m_1$. В множестве существует не более одного наибольшего и не более одного наименьшего элемента.

Наибольший элемент всего множества M называют *единицей*, а наименьший — *нулем*. Наименьший элемент (если он существует) в множестве верхних граней множества U называют *точной верхней гранью* U . Точную верхнюю грань подмножества U обычно обозначают символом $\sup U$. Аналогично наибольший элемент (в случае его существования) в множестве нижних граней множества U называют *точной нижней гранью* U . Точную нижнюю грань подмножества U обычно обозначают символом $\inf U$.

Например, в алгебре классов равносильных высказываний дизъюнкция $A \vee B$ является точной верхней гранью для высказываний A, B в порядке «логическое следствие», а конъюнкция $A \& B$ является точной нижней гранью для высказываний A, B .

В алгебре подмножеств в порядке «включение» объединение $A \cup B$ является точной верхней гранью для множеств A, B , а пересечение $A \cap B$ образует точную нижнюю грань.

Частично упорядоченное множество, в котором каждая пара элементов имеет точную верхнюю и точную нижнюю грани, называется *решеткой*. Можно считать, что «взятие точной грани» и «взятие точной нижней грани» — это две двухместные операции решетки. Может встретиться ситуация, когда точные верхние грани двух элементов существуют, а нижние — нет. Тогда говорят соответственно о верхней (и аналогично нижней) *полурешетке*. Если грани существуют не только для двух, но и для любого множества элементов, то решетку называют *полной*.

Непосредственно из определения граней следует, что операции решетки ассоциативны, коммутативны, идемпотентны и связаны законами поглощения.

Свойства операций «взятие точных граней» в решетке совершенно одинаковы. Различие проявляется только по отношению к нулю и единице (если они там есть).

Нуль решетки является поглощающим элементом для взятия точной нижней грани и нейтральным для взятия точной верхней грани.

Единица решетки является поглощающим элементом для взятия точной верхней грани и нейтральным для взятия точной нижней грани.

Решетку подалгебр алгебры A обозначают символом¹ $L(A)$ и называют структурой, *сопутствующей* алгебре A .

В общей ситуации множество подалгебр может и не оказаться решеткой (точнее, будет лишь частичной решеткой, т. е. операции объединения или пересечения будут выполнимы не всегда). Тогда под символом $L(A)$ понимается частичная решетка. Например, множество подполугрупп полугруппы может оказаться лишь верхней полурешеткой.

Для групп, колец, полей ситуация не усложняется, множества соответствующих подалгебр образуют полноценные решетки. Точнее говоря, множество подгрупп группы, множество подколец кольца, множество подполей поля являются решетками с единицей и нулем.

Исследование алгебры (алгебраической системы) состоит, в частности, в изучении решетки ее подалгебр (подсистем). Иногда с помощью решеток подалгебр можно установить неизоморфность объектов, так как если алгебры A_1 и A_2 изоморфны, то решетки $L(A_1)$ и $L(A_2)$ тоже изоморфны. Правда, изоморфизм решеток алгебр является необходимым, но недостаточным условием изоморфизма самих алгебр.

Алгебры с изоморфными решетками могут оказаться неизоморфными. Например, две группы простых и различных порядков неизоморфны, но имеют изоморфные решетки подгрупп, состоящие только из тривиальных подгрупп.

Пусть алгебра $L = \langle L; \inf, \sup \rangle$ является решеткой. Обозначим верхнюю грань символом \vee , нижнюю — символом \wedge :

$$\begin{aligned}\inf(x, y) &= x \wedge y; \\ \sup(x, y) &= x \vee y.\end{aligned}$$

Иногда операцию взятия верхней грани называют *объединением*, а взятия нижней грани — *пересечением* (и обозначают символами \cup , \cap , похожими на знаки теоретико-множественных операций). Таким образом, слова «пересечение» и «объединение» *двусмысленны*: это и теоретико-множественные операции, и операции в произвольной решетке.

¹ Буква L — первая буква английского слова *Lattice* — «решетка».

В любой решетке операции \wedge, \vee связаны законами поглощения:

$$(a \vee b) \wedge a = a, (a \wedge b) \vee a = a.$$

Решетка $L = \langle L; \wedge, \vee \rangle$ называется *дистрибутивной*, если операции \wedge и \vee связаны законами дистрибутивности:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z);$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

Если $L = \langle L; \wedge, \vee \rangle$ — дистрибутивная решетка, то алгебры $\langle L; \wedge, \vee \rangle$ и $\langle L; \vee, \wedge \rangle$ являются полукольцами.

Множество подмножеств некоторого множества с операциями «пересечение» и «объединение», множество классов равносильных высказываний с операциями «дизъюнкция» и «конъюнкция», множество целых неотрицательных чисел с операциями «наибольший общий делитель» и «наименьшее общее кратное», множество событий с операциями «и», «или» являются дистрибутивными решетками.

Таким образом, объектами изучения теории множеств, математической логики, теории чисел и теории вероятностей являются дистрибутивные решетки.

Для групп, колец и полей решетка подалгебр может оказаться случайной и дистрибутивной, но в общем случае это не так. Например, решетка подгрупп группы S_3 уже не дистрибутивна.

Дистрибутивная решетка является частным случаем решетки модулярной.

Решетка L называется *модулярной* (или *дедекиндовой*¹), если в ней выполняется тождество

$$x \wedge ((x \wedge y) \vee z) = (x \wedge y) \vee (x \wedge z).$$

Из тождества дистрибутивности следует тождество модулярности:

$$x \wedge ((x \wedge y) \vee z) = (x \wedge (x \wedge z)) \vee (x \wedge z) = (x \wedge y) \vee (x \wedge z),$$

поэтому каждая дистрибутивная решетка модулярна. Обратное утверждение неверно, например, решетка так называемых *нормальных* подгрупп (точное определение нормальной подгруппы будет приведено в п. 4.1) всегда модулярна, но не всегда дистрибутивна.

Решетка — частный случай алгебры, поэтому можно говорить о гомоморфизме и изоморфизме решеток.

¹ Рихард Юлиус Вильгельм Дедекинд (Dedekind, 1831—1916) — немецкий математик, профессор высшей технической школы в Брауншвейге (1862—1912).

Решетка $L_1 = \langle L_1; \wedge, \vee \rangle$ изоморфна решетке $L_2 = \langle L_2; \wedge, \vee \rangle$, если существует взаимно однозначное отображение φ множества L_1 на множество L_2 , сохраняющее операции решетки (для любых x, y из L_1):

$$\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y);$$

$$\varphi(x \vee y) = \varphi(x) \vee \varphi(y).$$

Как и для произвольных алгебр, свойство «быть решеткой» абстрактное: алгебра, изоморфная решетке, является решеткой.

Точнее алгебра, изоморфная дистрибутивной решетке, является дистрибутивной решеткой, а алгебра, изоморфная решетке с нулем и единицей, является решеткой с нулем и единицей.

Последнее утверждение можно выразить точнее. При гомоморфизме решеток нулевой элемент переходит в нулевой, а единичный — в единичный.

Решетка подгрупп группы $\langle \mathbb{Z}; + \rangle$ похожа на решетку $\langle \mathbb{Z}_0; \text{НОД}, \text{НОК} \rangle$, но не изоморфна ей (например, нулевая подгруппа — наименьшая в решетке $L(\mathbb{Z})$, но ноль — наибольший элемент во второй решетке). Граф одной из решеток получается из графа второй поворотом на 180° .

Такая же ситуация может встретиться и в других случаях, когда взаимно однозначное соответствие φ между элементами множеств-носителей решеток L_1 и L_2 не сохраняет операции, а меняет их местами:

$$\varphi(x \wedge y) = \varphi(x) \vee \varphi(y);$$

$$\varphi(x \vee y) = \varphi(x) \wedge \varphi(y).$$

В таком случае φ принято называть *антиизоморфизмом*. При антиизоморфизме ноль переходит в единицу, а единица — в ноль.

Например, решетка подгрупп циклической группы порядка n антиизоморфна решетке натуральных делителей числа n (с отношением делимости в качестве частичного порядка). Если циклическая группа бесконечна, то ее решетка подгрупп антиизоморфна решетке целых неотрицательных с тем же отношением делимости, т. е. с решеточными операциями «взятие наибольшего общего делителя» и «взятие наименьшего общего кратного».

Пусть $L = \langle L; \wedge, \vee \rangle$ — решетка с нулем и единицей. Обозначим ноль символом 0 , а единицу — символом 1 . Элемент x из L называют *дополнением* элемента a из L , если $a \wedge x = 0$ и $a \vee x = 1$.

Дополнение элемента a принято обозначать символом \bar{a} .

В дистрибутивной решетке с нулем и единицей каждый элемент имеет не более одного дополнения.

Действительно, если \bar{a} и a' — два дополнения для элемента a , то из $a \vee \bar{a} = 1$ следует $(a \vee \bar{a}) \wedge a' = a'$. Тогда по закону дистрибутивности $(a \wedge a') \vee (\bar{a} \wedge a') = a'$, откуда $\bar{a} \wedge a' = a'$. Из $a \vee a' = 1$ аналогичным образом следует $a' \wedge \bar{a} = \bar{a}$, откуда $\bar{a} = a'$.

Если каждый элемент решетки L имеет дополнение, то L называют решеткой с дополнениями. Дистрибутивная решетка с дополнениями называется булевой решеткой.

Например, решетка подмножеств некоторого множества с операциями «объединение» и «пересечение», решетка высказываний с операциями «конъюнкция» и «дизъюнкция» и решетка натуральных делителей натурального числа n , являющегося произведением различных простых чисел, являются булевыми решетками.

При этом решетки натуральных делителей натурального числа n , большего единицы и не равного произведению различных простых чисел, и всех целых неотрицательных чисел с операциями «наибольший общий делитель» и «наименьшее общее кратное» не являются булевыми.

В решетке множеств и в решетке высказываний операции связаны законами де Моргана. Эти законы в действительности выполняются в гораздо более общей ситуации.

В любой булевой решетке выполняются законы де Моргана:

$$\overline{a \vee b} = \bar{a} \wedge \bar{b} \text{ и } \overline{a \wedge b} = \bar{a} \vee \bar{b}.$$

Достаточно показать истинность лишь первого утверждения, которое равносильно двум следующим:

$$(a \vee b) \wedge (\bar{a} \wedge \bar{b}) = 0 \text{ и } (a \vee b) \vee (\bar{a} \wedge \bar{b}) = 1.$$

Вычисляем:

$$(a \vee b) \wedge (\bar{a} \wedge \bar{b}) = (a \wedge \bar{a} \wedge \bar{b}) \vee (b \wedge \bar{a} \wedge \bar{b}) = 0 \vee 0;$$

$$(a \vee b) \vee (\bar{a} \wedge \bar{b}) = (a \vee b \vee \bar{a}) \wedge (a \vee b \vee \bar{b}) = 1 \wedge 1 = 1.$$

Булева решетка полностью определяется отношением порядка. Однако ее можно представить и как алгебру с тремя операциями: «взятие точной верхней грани», «взятие точной нижней грани», «взятие дополнения», $B = \langle B; \wedge, \vee, \bar{} \rangle$. Операции \wedge, \vee обладают свойствами ассоциативности, коммутативности, идемпотентности и связаны дистрибутивными законами. Взятие дополнения дает тождества

$$\bar{\bar{a}} = a, (a \vee \bar{a}) \wedge b = b, (a \wedge \bar{a}) \vee b = b;$$

$$\overline{a \vee b} = \bar{a} \wedge \bar{b}, \overline{a \wedge b} = \bar{a} \vee \bar{b}.$$

Все перечисленные свойства операций полностью определяют булеву решетку.

Более того, такая система аксиом не является независимой, т. е. часть тождеств выражается через остальные. Обычно, впрочем,

систему аксиом булевой решетки делают еще более избыточной (но более удобной для использования).

Например, в список аксиом включают законы поглощения, а вместо доказательства того, что для любых элементов a, b

$$a \vee \bar{a} = b \vee \bar{b}, \quad a \wedge \bar{a} = b \wedge \bar{b},$$

сразу определяют нульместные операции — нуль и единица.

Поскольку булево кольцо состоит из идемпотентов, его характеристика равна двум и оно коммутативно.

В кольце множеств, кроме операций, есть частичный порядок — отношение включения. Это отношение выражается через операцию умножения (в кольце множеств роль умножения играет пересечение)

$$x \subset y \Leftrightarrow x = x \cap y$$

для любых множеств x, y .

Это свойство кольца множеств можно перенести без всяких изменений на произвольное булево кольцо. Другими словами, отношение \leq , введенное в булевом кольце $\langle B; +, \cdot \rangle$ по правилу

$$\overset{\text{опр}}{x \leq y} \Leftrightarrow x = x \cdot y,$$

является отношением частичного порядка.

Из идемпотентности умножения следует рефлексивность отношения \leq , а из ассоциативности — транзитивность. Если

$$x = x \cdot y, \quad y = x \cdot y,$$

то $x = y$, т. е. отношение \leq антисимметрично.

В булевой решетке подмножеств $P(M)$ с помощью операций решетки (объединение, пересечение и дополнение) была определена еще одна операция — симметрическая разность, и с этой операцией и пересечением множество $P(M)$ превратилось в булево кольцо. Точно такую же процедуру можно проделать с любой булевой решеткой.

Если $B = \langle B; \vee, \wedge \rangle$ — булева решетка, то множество B с операциями, заданными тождествами

$$\begin{aligned} x + y &= (\bar{x} \wedge y) \vee (x \wedge \bar{y}); \\ x \cdot y &= x \wedge y \end{aligned}$$

превращается в булево кольцо.

Для доказательства этого утверждения необходимо показать, что сложение ассоциативно, коммутативно, обладает нейтральным элементом и что каждый элемент имеет противоположный. Кроме того, нужно убедиться, что умножение дистрибутивно относительно сло-

жения (ассоциативность, идемпотентность, наличие нейтрального элемента для умножения сразу следуют из свойств операции \wedge).

Из симметричности определения сложения следует его коммутативность. Нуль решетки играет роль нуля по сложению:

$$x + 0 = (\bar{x} \wedge 0) \vee (x \wedge \bar{0}) = 0 \vee (x \wedge 1) = x \wedge 1 = x,$$

и каждый элемент является противоположным самому себе:

$$x + x = (\bar{x} \wedge x) \vee (x \wedge \bar{x}) = 0 \vee 0 = 0.$$

Проверим ассоциативность сложения:

$$\begin{aligned} x + (y + z) &= (\bar{x} \wedge ((\bar{y} \wedge z) \vee (y \wedge \bar{z}))) \vee (x \wedge ((\bar{y} \wedge z) \vee (y \wedge \bar{z}))) = \\ &= (\bar{x} \wedge ((\bar{y} \wedge z) \vee (y \wedge \bar{z}))) \vee (x \wedge ((y \vee \bar{z}) \wedge (\bar{y} \vee z))) = \\ &= (\bar{x} \wedge \bar{y} \wedge z) \vee (\bar{x} \wedge y \wedge \bar{z}) \vee (x \wedge y \wedge z) \vee (x \wedge \bar{y} \wedge \bar{z}) = \\ &= (\bar{x} \wedge \bar{y} \wedge z) \vee (x \wedge y \wedge z) \vee (\bar{x} \wedge y \wedge \bar{z}) \vee (x \wedge \bar{y} \wedge \bar{z}) = \\ &= (((x \wedge \bar{y}) \vee (\bar{x} \wedge y)) \wedge z) \vee (((\bar{x} \wedge y) \vee (x \wedge \bar{y})) \wedge \bar{z}) = \\ &= ((\bar{x} \wedge y) \vee (x \wedge \bar{y})) \wedge z \vee ((\bar{x} \wedge y) \vee (x \wedge \bar{y})) \wedge \bar{z} = (x + y) + z. \end{aligned}$$

Убедимся в выполнении дистрибутивного свойства:

$$\begin{aligned} xz + yz &= ((\bar{x} \wedge z) \vee (y \wedge z)) \vee ((x \wedge z) \wedge (\bar{y} \vee z)) = \\ &= ((\bar{x} \vee \bar{z}) \wedge (y \wedge z)) \vee ((x \wedge z) \wedge (\bar{y} \vee z)) = \\ &= (\bar{x} \wedge y \wedge z) \vee (x \wedge \bar{y} \wedge z) = ((\bar{x} \wedge y) \vee (x \wedge \bar{y})) \wedge z = (x + y)z. \end{aligned}$$

Таким образом, каждую булеву решетку можно превратить в булево кольцо.

Возможен и обратный переход: каждое булево кольцо можно превратить в булеву решетку.

Если $B = \langle B; +, \cdot \rangle$ — булево кольцо, то, положив (для всех x, y из B)

$$x \vee y = x + y + x \cdot y;$$

$$x \wedge y = x \cdot y;$$

$$\bar{x} = x + 1,$$

мы превратим кольцо B в решетку, и решетка эта булева.

Упорядочим сначала множество B , положив

$$\overset{\text{опр}}{x \leq y} \Leftrightarrow x = x \cdot y.$$

Это отношение рефлексивно, транзитивно и антисимметрично, т. е. является отношением порядка. В этом порядке нуль кольца является наименьшим элементом, а единица — наибольшим. Кроме того,

$$x(x + 1) = x + x = 0;$$

$$x + (x + 1) = x + x + 1 = 1,$$

следовательно, $x + 1$ действительно является дополнением элемента x .

Остается проверить, что введенные операции \vee , \wedge являются точными нижней и верхней гранями и связаны дистрибутивными законами.

Из равенств

$$x(x \cdot y) = x \cdot y;$$

$$y(x \cdot y) = x \cdot y$$

следует, что $x \cdot y$ — нижняя грань элементов x , y . Если z — такой элемент из B , что

$$z \cdot x = z \cdot x;$$

$$z \cdot y = z \cdot y,$$

то $z(x \cdot y) = x \cdot y$ и, следовательно, $x \cdot y$ — точная нижняя грань.

Тождества

$$x(x + y + x \cdot y) = x;$$

$$y(x + y + x \cdot y) = y$$

означают, что элемент $x + y + x \cdot y$ образует верхнюю грань элементов x , y .

Если z — такой элемент из B , что $z \cdot x = x$ и $z \cdot y = y$, то

$$z(x + y + x \cdot y) = x + y + x \cdot y$$

и, следовательно, элемент $x \cdot y$ является точной верхней гранью элементов x , y .

Остается убедиться в выполнении дистрибутивного свойства:

$$(x \wedge y) \vee (x \wedge z) = xy + xz + x y x z = xy + xz + x y z = x(y + xz + yz) = x \wedge (y \vee z);$$

$$(x \vee y) \wedge (x \vee z) = (x + y + xy)(x + z + xz) =$$

$$= x + xz + xxz + yx + yz + yxz + x y x + x y z + x y x z = x + yz + x y z = x \vee (y \wedge z).$$

Переход от кольца к решетке, а затем снова к кольцу по этим правилам даст исходное кольцо (соответственно путь «решетка — кольцо — решетка» завершается в исходной точке).

По имени автора, впервые заметившего эту связь между булевыми решетками и булевыми кольцами, этот факт называют *теоремой Стоуна*¹. Благодаря теореме Стоуна булево кольцо и булеву решетку, заданные на одном множестве, принято называть *булевой алгеброй*, а исследование булевой решетки можно заменить изучением булевых колец.

¹ Маршалл Харви Стоун (Stone, 1903—1989) — американский математик. Связь между булевыми решетками и булевыми кольцами установлена им в двух работах 1935 и 1936 г. (в работе 1936 г. М. Стоун ввел термин «булево кольцо»).

Контрольные задания

1. Докажите, что существует пять попарно неизоморфных полугрупп, состоящих из двух элементов.
2. Докажите, что полугруппа с делением является группой.
3. Докажите, что в моноиде существует единственный нейтральный элемент, а каждый элемент в моноиде имеет не более одного обратного.
5. Докажите, что множество обратимых элементов моноида образует подмоноид.
6. Докажите, что каждая группа изоморфно вложима в мультипликативную группу некоторого кольца.
7. Докажите, что мультипликативная группа ненулевых комплексных чисел неизоморфна аддитивной группе комплексных чисел.
8. Докажите, что конечный моноид с правым сокращением является группой.
9. Докажите, что в булевом кольце можно так определить пересечение, объединение и дополнение, что кольцо превратится в булеву решетку.
10. Докажите, что булево конечное кольцо изоморфно прямой степени двухэлементного поля.

Тема 2

АЛГЕБРЫ И АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

Основные понятия: бинарное отношение, композиция отношений, обратное отношение, эквивалентность, порядок, функция, разбиение на смежные классы, фактормножество, мощность, счетность, континуальность, алгебраическая операция, таблица Кэли, ассоциативность, коммутативность, изоморфизм, гомоморфизм, конгруэнция.

Основные факты: отношение эквивалентности задает разбиение множества на классы; разбиение на классы определяет разбиение множества на классы, отношение, мощности множеств не ограничены, любое упорядоченное множество изоморфно представляется подмножеством некоторого булеана с отношением включения.

После первоначального ознакомления с важнейшими алгебрами имеет смысл осмотреться и отметить несколько свойств алгебр вообще.

Алгебру вообще, т. е. множество с алгебраическими операциями, на которые первоначально не наложено никаких условий, принято называть *универсальной алгеброй*.

Остановимся сначала на точном определении и свойствах алгебраической операции. Заодно отметим полезные для будущего свойства двухместных отношений. Будет полезно сразу же обсудить связи между отношениями и операциями, в частности взаимосвязь конгруэнций и гомоморфизмов алгебраических систем.

Начнем с того, что алгебраическая операция — это частный случай отношения.

2.1. Отношения

Если A и B — два множества, то любое подмножество S декартова произведения $A \times B$ называют *соответствием* между элементами множеств A и B : $S \subset A \times B$.

Если элементы x, y (где $x \in A, y \in B$) находятся в соответствии S , $(x, y) \in S$, то принято писать: xSy , или $y = S(x)$ (читается: «элементы x и y связаны соответствием S », или «элемент y соответствует при соответствии S элементу x »), если S не имеет уже традиционного особого названия и особого обозначения.

В случае совпадения множеств A и B множество S является подмножеством декартова квадрата: $S \subset A \times A$.

В этом случае соответствие обычно называют *отношением* (точнее, *бинарным¹ отношением*). Для бинарного отношения чаще пользуются записью xSy (читается: «элемент x находится в отношении S с элементом y ») опять же в случае, если отношение S не имеет особого названия.

Бинарное отношение — частный случай соответствия между элементами двух множеств. При этом любое соответствие S между множествами A и B , $S \subset A \times B$ можно превратить в бинарное отношение

$$S \subset A \times B \subset (A \cup B) \times (A \cup B).$$

Число мест в отношении может быть и отлично от двух. Так, подмножество S декартова куба множества M

$$S \subset M^3 = M \times M \times M = \{(a_1, a_2, a_3) | a_1, a_2, a_3 \in M\}$$

образует *трехместное* отношение на M , и вообще подмножество n -й декартовой степени

$$S \subset M^n = \underbrace{M \times M \times \dots \times M}_n = \{(a_1, a_2, \dots, a_n) | a_1, a_2, \dots, a_n \in M\}$$

является n -местным отношением на множестве M . Наименьшее значение n равно единице. *Одноместное отношение* — это просто подмножество множества M .

Самое большое (называемое *полным*) соответствие — это все декартово произведение $A \times B$, самое маленькое (*пустое*) соответствие — пустое множество \emptyset .

Над соответствиями, как и над любыми множествами, можно выполнить операции объединения, пересечения и дополнения, — результат этих операций останется в декартовом произведении, т. е. снова является соответствием. Операции, произведенные над бинарными отношениями, снова дадут бинарные отношения.

Если соответствие W включает в себя соответствие T , $T \subset W$, то говорят, что W — *следствие* или *продолжение* соответствия T .

Кроме обычных для множеств операций над соответствиями можно выполнять еще две особые: операцию *обращения* и операцию *композиции*.

Если S — соответствие между множествами A и B , т. е. $S \subset A \times B$, то *обратным* для S соответствием называют соответствие S^{-1} между множествами B и A , $S^{-1} \subset B \times A$, заданное правилом

$$S^{-1} = \{(b, a) | (a, b) \in S\}$$

¹ От лат. *bis* — «два» и *ar* — «место».

или, другими словами,

$$bS^{-1}a \Leftrightarrow aSb.$$

Пусть S — соответствие между множествами A и B , а T — соответствие между множествами B и C :

$$S \subset A \times B, \quad T \subset B \times C.$$

Соответствие $S \circ T$ между множествами A и C :

$$S \circ T \subset A \times C$$

называют *композицией* (или *произведением*) соответствий, если

$$S \circ T = \{(a, c) \mid \text{существует } b \text{ из } B \text{ такой, что } aSb \text{ и } bTc\}.$$

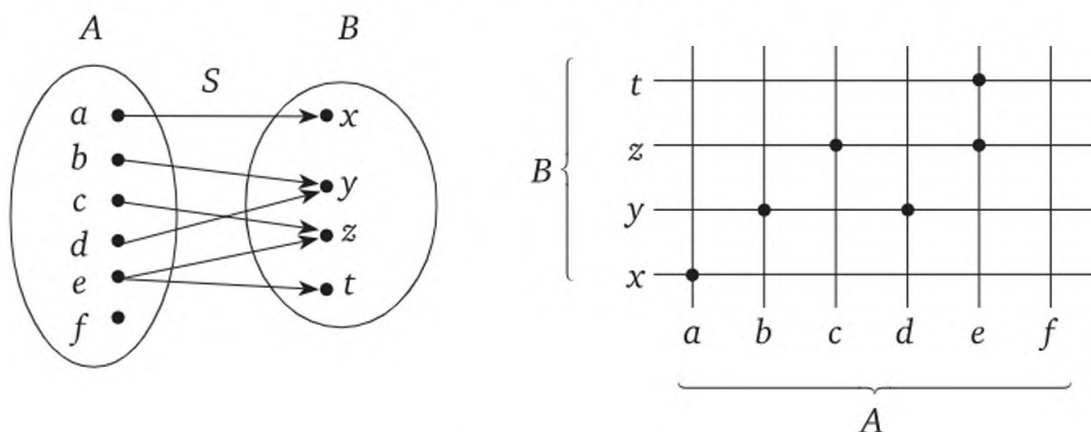
Композицию отношений можно записать иначе:

$$x(S \circ T)y \Leftrightarrow y = T(S(x)).$$

Понятия обратного соответствия и композиции соответствий лучше всего пояснить на наглядном графическом изображении. Графических изображений для соответствия два: *граф* и *график*.

Пусть S — соответствие между множествами A и B .

Изобразим элементы множества A и B точками на диаграмме Эйлера и соединим точки, находящиеся в соответствии S стрелками, а именно: если $y = S(x)$, то приведем стрелку из точки x в точку y .



Граф и график соответствия

Заметим, что стрелка — это не обязательно отрезок прямой: она может петлять и самопересекаться, важно лишь, что стрелка начинается в x и заканчивается в y .

Получившаяся в результате картинка называется *графом* соответствия S .

Рассмотрим пример соответствия на небольших множествах. Пусть даны два множества A и B и соответствие S между элементами этих множеств:

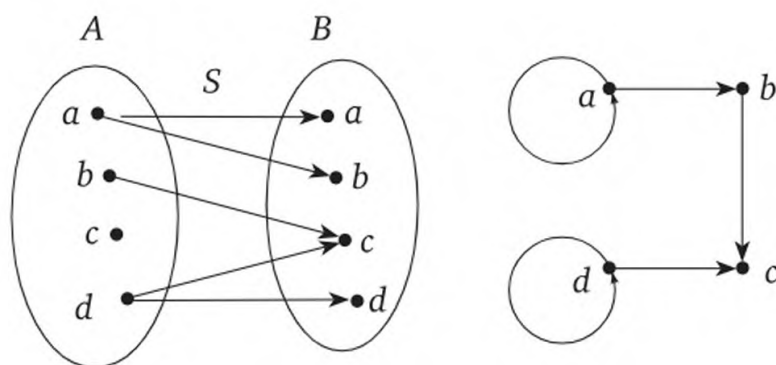
$$A = \{a, b, c, d, e\}, B = \{x, y, z, t\};$$

$$S = \{(a, x), (b, y), (z, t), (d, y), (e, z), (e, t)\}.$$

На рисунках изображены граф и график соответствия S .

Отношение — это другое название соответствия, поэтому, как и соответствие, его можно представить наглядно *графиком* или *графом*. При построении графа, как правило, нет необходимости брать два экземпляра исходного множества.

Например, пусть $S = \{(a, b), (a, a), (b, c), (d, c), (d, d)\}$ — бинарное отношение на множестве $\{a, b, c, d\}$. Это отношение можно представить двумя графами.



Графы бинарного отношения

Граф с двумя экземплярами множества M в школьном курсе математики иногда называют *диаграммой* отношения (соответствия).

Соответствие F между элементами множеств A и B называют *функциональным* (или *функцией*, или *отображением*), если для каждого элемента x из A и y_1, y_2 из B

$$xFy_1 \text{ и } xFy_2 \Rightarrow y_1 = y_2.$$

Отображение называют *взаимно однозначным* (или *разнозначной функцией*), если x_1, x_2 из A и y из B

$$x_1 Fy \text{ и } x_2 Fy \Rightarrow x_1 = x_2.$$

Таким образом, соответствие является взаимно однозначным отображением, если каждый элемент из A находится в соответствии с не более чем одним элементом из B , и наоборот — каждый элемент из B связан соответствием с не более чем одним элементом из A . Если к тому же для каждого элемента из A найдется элемент в B , связанный с ним этим соответствием, и для каждого элемента

из B найдется соответствующий элемент из A , то говорят, что между множествами A и B существует взаимно однозначное соответствие.

В таком случае с каждым элементом a из A связан в точности один элемент из B , и каждому b из B соответствует лишь один элемент из A . Иначе говоря, для каждого a из A предикат с одним переменным aFx становится истинным в точности для одного элемента b из B , и xFb имеет в точности одно решение в A .

Говорят еще, что множество A взаимно однозначно отображается на множество B (часто используется термин «биекция»).

В более общей ситуации одно множество может взаимно однозначно отображаться внутрь другого. Тогда говорят о взаимно однозначном *вложении* (или *инъекции*) одного множества в другое.

Если граф изображает взаимно однозначное отображение одного множества A на (или в) множество B , то нет двух (или более) стрелок, выходящих из одной точки в A . Кроме того, острия двух (и более) стрелок не упрутся одновременно в одну точку из B .

Простейшим примером взаимно однозначного соответствия между множествами является соответствие I между элементами множества A , отображающее любой элемент из A сам в себя: xIx . Это отображение принято называть *единичным* отображением¹, или *диагональю*.

Пусть F — взаимно однозначное отображение множества A на множество B . Для всякого соответствия есть обратное отображение, есть оно и для F :

$$xF^{-1}y \Leftrightarrow yFx.$$

Теперь для элемента a предикат aFx превращается в $xF^{-1}a$ и наоборот. Однако и тот, и другой обладают одним и тем же свойством (полностью характеризующее свойство взаимно однозначности отображения на). Это значит, что соответствие, обратное для взаимно однозначного отображения, снова является взаимно однозначным отображением.

Композиция взаимно однозначных отображений снова является взаимно однозначным отображением.

Отношение T на множестве M называют *рефлексивным*², если xTx для всех элементов x из M .

Отношение T *транзитивно*³, если из xTy и yTz следует xTz .

Отношение T *симметрично*, если из xTy следует yTx .

Отношение T *антисимметрично*, если из xTy и yTx следует $x = y$.

Отношение T называют *связным*, если любые два элемента множества связаны этим отношением (для каких-либо x, y): xTy или yTx .

¹ I — первая буква латинского слова *identicus* — «тождественный, одинаковый».

² От лат. *reflex* — «отражение».

³ От лат. *transit* — «передача».

Отношение T называется *иррефлексивным*, если ни один из элементов множества не находится в отношении T сам с собой. Иррефлексивность T равносильна рефлексивности \bar{T} .

Отношение T называется *асимметричным*, если xTy и yTx не выполняются одновременно для любых x, y : из xTy следует, что y, x не находятся в отношении T .

Если отношение иррефлексивно, то свойство антисимметричности для него равносильно асимметричности: иррефлексивное отношение T антисимметрично, если для каждого x, y из множества M :

$$xTy \Rightarrow \text{неверно, что } yTx,$$

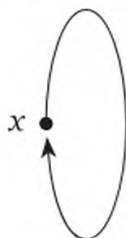
или, другими словами, $xTy \Rightarrow y\bar{T}x$.

Антисимметричность связного отношения можно записать в виде следующего свойства (для каждого x, y):

$$x \neq y \Rightarrow xTy \neq yTx.$$

Здесь символ неравенства использован два раза в различных смыслах: сначала как несовпадение элементов основного множества, а затем в смысле неравенства истинностных значений высказываний: если xTy — истинно, то yTx — ложно, и наоборот.

Для несвязного отношения это определение не подходит: оба высказывания могут оказаться ложными.



На графе рефлексивного отношения каждый элемент имеет стрелку, острый кончик которой упирается в начало (*петлеобразную стрелку*).

Отношение рефлексивно тогда и только тогда, когда его график содержит *диагональ* I :

$$I = \{(a, a) | a \in M\}.$$

График иррефлексивного отношения имеет с диагональю пустое пересечение.

Если на графе *транзитивного* отношения три точки x, y, z связаны стрелками, то непременно должна быть и *третья стрелка*, соединяющая элементы x и z .

Транзитивность отношения T означает, что если два элемента связаны композицией этого отношения, то они тоже находятся в этом же отношении, $T \circ T \subset T$.

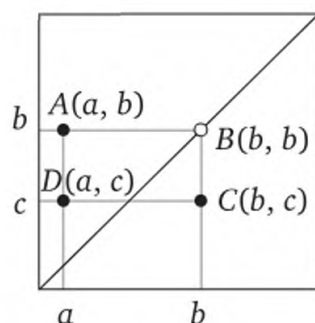


График транзитивного отношения

Рассмотрим особенности графика транзитивного отношения T . Пусть точка A соответствует паре (a, b) , а точка C — паре (b, c) . Если aTb и bTc , то точки A, B принадлежат графику и точка $D(a, c)$ тоже является точкой графика. Рассмотрим вспомогательную точку $B(b, b)$, которая находится на диагонали и является четвертой точкой прямоугольника $ABCD$. Точнее говоря, это третья точка: если a, b, c заданы, то есть и точки A, B, C , а четвертая вершина D попадет в график тогда и только тогда, когда отношение T транзитивно.

Симметричность отношения означает, что если на его графе есть стрелка, идущая в одном направлении, то есть и вторая стрелка, идущая в противоположном направлении.

Можно считать, что на графе симметричного отношения находятся особые, двухконцевые стрелы следующего вида.



Точки (a, b) и (b, a) графика отношения лежат *симметрично* относительно диагонали I , следовательно, график симметричного отношения симметричен относительно диагонали. Отношение T симметрично, если $T = T^{-1}$, т. е. график симметричного отношения не изменится, если его симметрично отразить в диагонали.

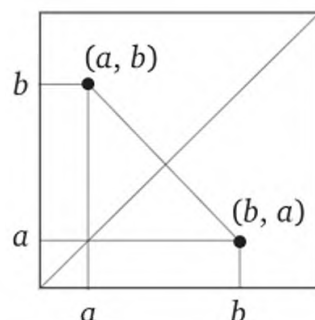


График симметричного отношения

Если отношение *антисимметрично* и на его графе из точки x идет стрелка в точку y , то обратного пути из y в x уже нет.

На графике антисимметричного отношения нет ни одной пары различных точек, симметричных относительно диагонали. Одно-

временное выполнение xTy и yTx означает, что элементы x, y связаны отношением $T \cap T^{-1}$. Асимметричность отношения сообщает, что это пересечение пусто, $T \cap T^{-1} = \emptyset$, а антисимметричность означает, что это пересечение содержится в диагонали, $T \cap T^{-1} \subset I$, т. е., в частности, может быть и пустым (если T иррефлексивно). Граф связного отношения не распадается на отдельные куски: из любой точки графа в любую точку можно пройти по направлению стрелки или против этого направления.

Связность отношения T означает, что объединение отношения и его обратного совпадает со всем декартовым квадратом: $T \cup T^{-1} = M \times M$.

Если график связного отношения симметрично отобразить в диагонали как оси симметрии, то объединение этих двух фигур — графика и его образа при симметрии — должно превратиться в весь декартов квадрат исходного множества (т. е. в черный квадрат).

Важнейшим среди соответствий является *функциональное соответствие*. Поскольку каждое бинарное отношение можно представить в виде соответствия, важнейшим видом бинарного отношения также явится *функциональное отношение*.

Функциональное соответствие — это отображение одного множества на другое или, что то же самое, функция, определенная в множестве A со значениями в множестве B . Если эти множества совпадают, $A = B = M$, то получим функциональное бинарное отношение (или, короче говоря, *функцию*¹), определенное на множестве M со значениями в множестве M .

Бинарное отношение F на множестве M является *функцией*, если для каждого элемента x из M из xFu и xFz следует $u = z$.

Рефлексивное, транзитивное и симметричное отношение называют *эквивалентностью*².

Отношение T — эквивалентность на множестве M , если T :

- 1) рефлексивно ($T \supset I$);
- 2) транзитивно ($T \circ T \subset T$);
- 3) симметрично ($T^{-1} \subset T$).

Эквивалентность часто обозначают символом \sim , т. е. \sim — эквивалентность на M , если для любых x, y, z из M :

- 1) $x \sim x$;
- 2) $x \sim y \Rightarrow y \sim x$;
- 3) $x \sim y, y \sim z \Rightarrow x \sim z$.

Конкретные эквивалентности (например, равенство, подобие фигур, параллельность прямых, равносильность предикатов, равномощность множеств и т. п.) имеют и свои личные обозначения. Эти обозначения обычно *симметричны* ($=, \cong, ||, \Leftrightarrow, \equiv$ и т. п.).

¹ От лат. *functio* — «деятельность».

² От лат. *aequus* — «равный» и *valentis* — «имеющий силу».

Рефлексивное, транзитивное и антисимметричное отношение называют *порядком*.

Отношение T — порядок на множестве M , если T :

- 1) рефлексивно ($T \supset I$);
- 2) транзитивно ($T \circ T \subset T$);
- 3) антисимметрично ($T \cap T^{-1} \subset I$).

Порядок часто обозначают символом $<$. Отношение $<$ — порядок на M , если для любых x, y, z из множества M :

- 1) $x < x$;
- 2) $x < y, y < z \Rightarrow x < z$;
- 3) $x < y, y < x \Rightarrow x = y$.

Символ, изображающий конкретное отношение порядка, обычно несимметричен, например, \geq — «не меньше»; \leq — «не больше»; \subset — «включается»; \Rightarrow — «логически влечет» и т. п.

Функция, эквивалентность и порядок — основные среди бинарных отношений, но вполне может случиться, что конкретное отношение не является ни функцией, ни эквивалентностью, ни порядком. Например, отношение следствия для предикатов (в частности, для уравнений или их систем) является лишь рефлексивным и транзитивным, но не симметричным, ни антисимметричным. Таковыми же свойствами обладает отношение делимости на множестве целых чисел.

Рефлексивное и транзитивное отношение называют *предпорядком*.

Иногда отношение обладает лишь свойствами рефлексивности и симметричности. Такое бинарное отношение называют *толерантностью*¹.

Предпорядок — это эквивалентность без симметричности (или порядок без антисимметричности), толерантность — эквивалентность без транзитивности. Впрочем, предпорядок и толерантность не являются главными персонажами среди бинарных отношений.

Основные виды бинарных отношений (образно говоря, *три кита математики*) следующие:

- 1) функция;
- 2) порядок;
- 3) эквивалентность.

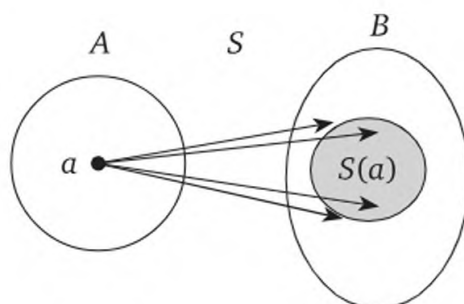
Рассмотрим каждое из этих отношений подробно.

2.2. Функция

Рассмотрим соответствие S между элементами множеств A и B : $S \subset A \times B$. Обозначим символом $S(a)$ множество всех элементов из B ,

¹ От лат. *tolerantia* — «терпение»; первоначально медицинский термин, означающий неотторжение инородных органов. Антонимом к *толерантности* является *иммунитет*.

находящихся в соответствии S с элементом a из A : $S(a) = \{b \in B \mid aSb\}$. Множество $S(a)$ называют *полным образом* элемента a ; любой элемент из $S(a)$ называется *образом* элемента a в B . Полный образ элемента может быть пустым множеством, но может состоять из нескольких элементов.



Полный образ

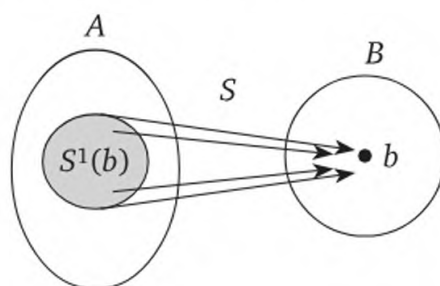
На графе отношения S образ элемента a — это все точки в множестве B , в которые упираются острия стрелок, выходящих из точки a .

Пусть b — элемент из множества B . Любой элемент из A , находящийся в соответствии S с элементом b , принято называть *прообразом* элемента b в A . Множество всех прообразов образует *полный прообраз* элемента b .

Полный прообраз обозначают символом $S^{-1}(b)$:

$$S^{-1}(b) = \{a \in A \mid aSb\}.$$

На диаграмме отношения S полный прообраз элемента b — это все точки выхода стрел с остриями в B .



Полный прообраз

Соответствие между элементами множеств A и B является *функциональным* (или *функцией*, или *отображением* из A в B), если для каждого элемента a из A полный образ $F(a)$ состоит не более чем из одного элемента. Это означает, что для каждых элементов x из A и y_1, y_2 из B

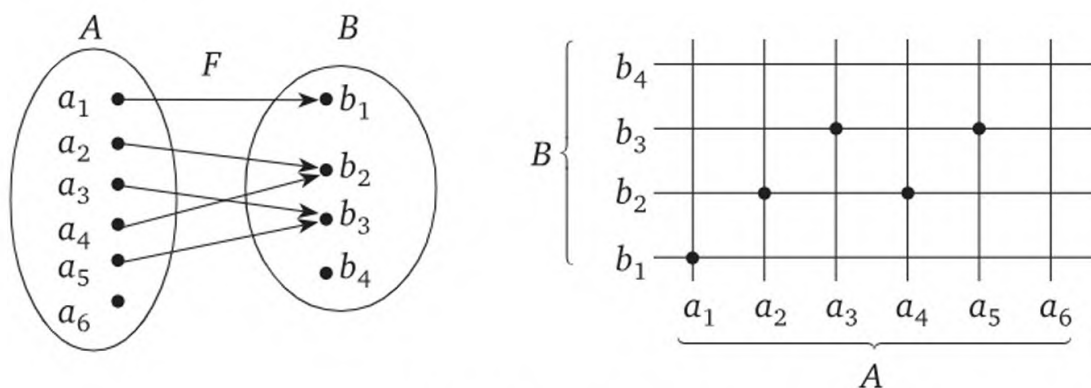
$$xFy_1 \text{ и } xFy_2 \Rightarrow y_1 = y_2.$$

Функциональность соответствия F между элементами множеств A и B означает, что каждый элемент из A имеет не более одного образа в B .

По существующей традиции для функционального соответствия F принято изменять порядок символов в записи xFu , окружать символ x круглыми скобками, а перед символом F ставить знак равенства. Иначе говоря, для функционального соответствия F вместо xFu пишут: $y = F(x)$.

Элемент x в такой ситуации принято называть *аргументом*, а элемент y — *функцией* x . Таким образом, слово «функция» двусмысленно: во-первых, это само *отображение* F , во-вторых, *результат* отображения $F(x)$.

Функциональность соответствия F подчеркивают особой записью, в которой участвуют и множества A и B . Запись $F : A \rightarrow B$ означает, что F — функция, определенная в множестве A со значениями в множестве B .



Граф и график функции

На графе функции из каждой точки a множества A выходит не более одной стрелки, а на вертикалях графика функции находится не более одной отмеченной точки.

Множество $E_F = \{F(a) \mid a \in A\}$ называют *областью значений* функции F . Область значений обозначают символом $F(A)$ или E_F .

На графе функции область значения состоит из всех тех точек, в которые упираются острия стрелок.

На рисунках область значений $E_F = F(A) = \{b_1, b_2, b_3\}$.

Множество всех элементов из A , имеющих образ при функциональном соответствии F , называют *областью определения* F . Область определения обозначают символом D_F .

$$D_F = \{a \in A \mid \text{существует } b \text{ из } B \text{ такой, что } F(a) = b\}.$$

На графе функции область определения состоит из всех точек, из которых выходят стрелки. На рисунках

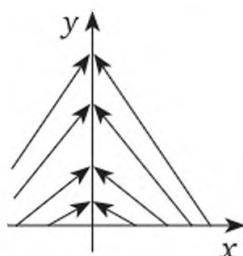
$$D_F = \{a_1, a_2, a_3, a_4, a_5\}.$$

Функция F отображает множество D_f на множество E_f .

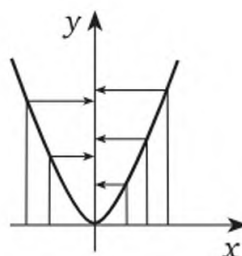
Множество действительных чисел можно изобразить в виде числовых прямых. На этом изображении можно поместить граф функции. Если провести все стрелки, то плоскость окажется полностью заштрихованной ими.

Граф функции можно представить наглядно с помощью графика этой функции.

Дело в том, что стрелки на графе функции — это не обязательно отрезки прямых. Стрелкой может быть любая линия, например ломаная. Это свойство дает возможность увидеть на графике числовой функции ее граф. Проведя стрелки графа в виде ломаных (состоящих из двух звеньев: одно параллельно оси абсцисс, а второе — оси ординат) и отмечая лишь точку излома стрелки, мы получим *график* функции. По этому графику можно восстановить любую стрелку *графа*. Можно считать, что мы видим граф (замаскированный) и график (явный) функции одновременно.



Граф функции



Граф (график) функции

Функция $f(x)$, определенная на конечном множестве M , может быть задана просто множеством

$$\text{Гр}_f = \{(x, f(x)) | x \in M\}.$$

Такое задание функции называют табличным, а множество Гр_f — *таблицей*. Впрочем, это же множество, причем для произвольной функции $f(x)$, также называют *графиком функции*. Отличие графика от таблицы — в их наглядном изображении. Таблица обычно изображается в виде схемы:

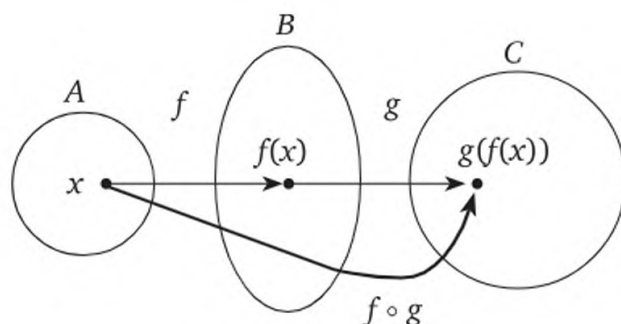
x	$f(x)$
x_1	$f(x_1)$
x_2	$f(x_2)$
...	...
x_n	$f(x_n)$

Над любыми соответствиями можно производить операции умножения, взятия обратного, объединения, пересечения и дополнения.

Заметим сначала, что композиция функциональных соответствий снова является функциональным соответствием.

Умножение функций как соответствий, чтобы отличить от числового умножения, обычно называют *суперпозицией* (или *сложной функцией*). Точнее говоря, если $f: A \rightarrow B$, а $g: B \rightarrow C$, то суперпозиция f и g состоит в последовательном выполнении сначала отображения f , а затем g . Суперпозиция $f \circ g: A \rightarrow C$ действует по правилу

$$f \circ g(x) = g(f(x)).$$



Композиция отображений

Обратное соответствие для функции не всегда будет функциональным. Если функция F принимает одно из значений хотя бы два раза, то обратное соответствие F^{-1} уже не функционально. Таким образом, однозначность — необходимое условие сохранения функциональности при обращении.

Это же условие является и достаточным. Если функция однозначная, то обратное соответствие для нее тоже будет функцией.

Иначе говоря, для того чтобы соответствие F^{-1} , обратное для функции F , снова было функцией, достаточно однозначности функции F . Таким образом, для того чтобы функция F имела обратную функцию F^{-1} , необходимо и достаточно однозначности F .

Функция — это частный случай соответствия, а соответствие — это множество особого вида. Поэтому можно говорить о теоретико-множественных операциях и отношениях, производимых над функциями.

Как обычно для соответствий, говорят, что функция f *продолжает* функцию g (или g является *ограничением* функции f), если $g \subset f$. В такой ситуации $D_g \subset D_f$, причем на множестве D_g значения этих функций совпадают.

Если множество значений функции F состоит более чем из двух элементов, то дополнение \bar{F} уже не является функцией.

Объединение $f \cup g$ функций f и g будет снова функцией тогда и только тогда, когда значения обеих функций в их общей части, т. е. на множестве $D_f \cap D_g$, совпадают.

В частности, если это пересечение пусто, $D_f \cap D_g = \emptyset$, то объединение этих функций всегда существует. Объединение можно, в свою очередь, вложить в еще более широкое множество. Это надмножество будет *общим продолжением* двух функций.

Свойство функциональности выполняется для всех элементов функционального соответствия. Поэтому этим свойством будут обладать и любые его подмножества. Иначе говоря, любое ограничение функции само является функцией.

Важным случаем функции является *алгебраическая операция*.

Алгебраической операцией на множестве M называют отображение f декартовой n -й декартовой степени M^n множества M в себя $f: M^n \rightarrow M$, если $D_f = M^n$.

В случае, когда $D_f \neq M^n$, говорят, что f — *частичная операция*.

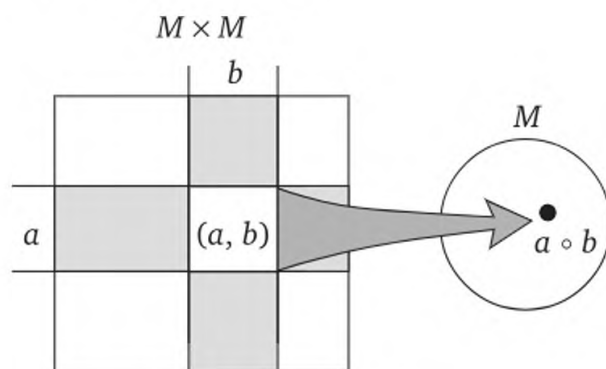
Число n называется *местностью*, или *арностью* операции. Наиболее распространены двухместные (*бинарные*) и одноместные (*унарные*) операции.

Символом $f(x_1, x_2, \dots, x_n)$ обозначают образ элемента (x_1, x_2, \dots, x_n) из M^n . Для конкретных элементов (a_1, a_2, \dots, a_n) из M элемент $f(a_1, a_2, \dots, a_n)$ принадлежит множеству M . При алгебраической операции каждый элемент из M^n должен иметь образ. Иначе говоря, отображение f является *всюду определенным*.

Одноместная операция f — это просто отображение множества M в себя.

Двухместная операция — это отображение декартова квадрата $M \times M$ в множество M . Двухместная операция отображает каждую пару элементов (a, b) в элемент $f(a, b)$.

Пусть на множестве M задана двухместная операция. Обозначим эту операцию символом \circ , т. е. каждому элементу (a, b) из декартова произведения $M \times M$ соответствует элемент $a \circ b$ из M . Представив элементы M в виде вертикальных и горизонтальных полос, получим наглядное представление декартова произведения $M \times M$ в виде квадрата, расчерченного на эти полосы. Элемент (a, b) изображается пересечением a -горизонтالي и b -вертикали. Операция f отображает квадратик (a, b) в $a \circ b$.



Двухместная операция

Это наглядное изображение можно сделать удобным для использования, если поместить элемент $a \circ b$ в квадратик (a, b) . Полученную таблицу действия операции f называют по имени автора *таблицей Кэли*.

M	\circ	\dots	b	\dots
	\vdots			
	a		$a \circ b$	
	\vdots			
M				

Таблица Кэли

Таблица умножения, изображаемая на обложках школьных тетрадей и ошибочно называемая «*таблица Пифагора*», представляет собой начальный фрагмент бесконечной таблицы Кэли для операции умножения на множестве натуральных чисел.

Можно говорить и о *нульместной* операции, т. е. об «отображении» пустого множества $\emptyset = M^0$ в M .

Слово «*отображение*» взято в кавычки, потому что это ненастоящее отображение — в множестве M^0 нет элементов, поэтому нет их и в $M^0 \times M$.

Нульместная операция — это просто *выделенное* в множестве M *подмножество*, в частности, это может быть всего лишь один элемент из M .

Пусть $\langle A; \circ \rangle$ — алгебра с двухместной операцией \circ .

Операция \circ называется *ассоциативной*, если для каждого элементов a, b, c из A

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

Говорят, что операция *коммутативна*, если для всех элементов a, b из A :

$$a \circ b = b \circ a.$$

Операция коммутативна, если ее таблица Кэли симметрична относительно диагонали. Элемент e из A называют *нейтральным* (или *единицей*), если для каждого элемента a из A

$$a \circ e = e \circ a = a.$$

Нейтральный элемент (если он есть) можно увидеть на таблице Кэли: в этом случае e -строка и e -столбец в точности совпадают со строкой и столбцом входа.

Элемент o из A называют *поглощающим* (или *аннулятором*, или *нулем*), если для каждого элемента a из A

$$a \circ o = o \circ a = o.$$

Если o — поглощающий элемент, то в таблице Кэли o -строка и o -столбец сплошь заполнены элементом o .

Пусть e — нейтральный элемент в A . Элемент a из A называют *обратимым*, если существует такой элемент x в A , что

$$a \circ x = x \circ a = e.$$

Элемент x в таком случае называют *обратным* для a .

Если элемент a обратим, то в таблице Кэли в a -строке и в a -столбце непременно найдутся нейтральные элементы e , причем расположены они симметрично относительно диагонали.

Поскольку в группе выполнимо деление, в групповой таблице Кэли каждый элемент встречается в каждой строчке и в каждом столбце в точности по одному разу.

Когда говорят об алгебре с двумя операциями, то имеют в виду, что между операциями есть какая-то связь.

Наиболее интересная, полезная и достаточно тесная связь между двумя двухместными операциями — это дистрибутивный закон. Пусть одна операция в алгебре называется сложением и обозначается символом $+$, а вторая — умножением и обозначается, как обычно, точкой (или ничем).

Тогда дистрибутивный закон означает, что для любых элементов для каждых элементов a, b, c из A

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c);$$

$$(b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

Чаще всего операция, играющая роль сложения, коммутативна, и двойная запись дистрибутивного закона не требуется.

Операции сложения и умножения (или операции, играющие эти роли) могут иметь самое различное происхождение и выполняться на разных множествах. Однако всегда договариваются о приоритетности умножения перед сложением: таким образом, отпадает необходимость в расстановке скобок. Дистрибутивный закон тогда принимает вид

$$a(b + c) = ab + ac;$$

$$(b + c)a = ba + ca.$$

2.3. Порядок

Если на множестве M определено отношение *порядка*, т. е. рефлексивное, транзитивное и антисимметричное отношение, то говорят, что множество M *упорядочено*.

Например, множества \mathbf{N} , \mathbf{Z} , \mathbf{Q} , \mathbf{R} с обычным отношением \leq упорядочены.

На графе отношения порядка принято не изображать петлеобразные стрелки, означающие рефлексивность. Не изображают и стрелок, являющихся следствием транзитивности. Более того, не принято ставить острия у стрелок: по умолчанию как бы невидимые острия стрел направлены сверху вниз (быть может, наискосок). Это значит, что если элементы x , y различны и $x < y$, то на графе точка y находится выше точки x и, кроме того, на графе есть постоянно снижающийся путь из y в x .

Если такого пути из x в y нет, как нет и обратного пути от y к x , то это значит, что элементы x , y *несравнимы*.

Теперь изобразим, согласно этим договоренностям, граф отношения порядка на множестве натуральных чисел.



Линейный порядок

Этот граф представляет собой часть прямой *линии*, уходящей вверх, с отмеченными на ней точками (натуральными числами). Такой вид граф имеет потому, что для любых натуральных чисел x , y непременно выполняется одно из двух утверждений: $x \leq y$ или $y \leq x$.

Иначе говоря, все элементы из \mathbf{N} оказались *связанными* этим отношением.

Бинарное отношение T обладает свойством *связности*, если все элементы связаны этим отношением, т. е. для всех элементов x , y из множества M либо xTy , либо yTx .

Связное отношение порядка называют *линейным порядком* (а множество с линейным порядком — *линейно упорядоченным*).

Множество натуральных чисел линейно упорядочено. Множества целых, рациональных и действительных чисел тоже линейно упорядочены отношением \leq .

Если в упорядоченном множестве не все элементы связаны между собой отношением порядка, то такой порядок называют *частичным* (а множество — *частично упорядоченным*).

Граф частично упорядоченного множества уже не вытягивается в одну линию.

Если из отношения порядка вычесть диагональ (т. е. отношение равенства), то порядок из нестрогого станет строгим. Это касается как частичного, так и линейного порядков.

Для порядка на числовом множестве строгий и нестрогий порядок изображаются различными символами: $<$ и \leq соответственно. Для отношения включения это необязательно: символ \subset изображает и нестрогий порядок тоже, хотя можно для этого использовать и символ \subseteq . В общей ситуации также символ $<$ может изображать как строгий, так и нестрогий порядок, но для нестрогого порядка иногда вводят символ \preceq .

Если T — отношение порядка, то обратное отношение T^{-1} также является порядком, причем строгость (нестрогость) порядка сохраняется.

Простейшим (нестрогим) порядком будет отношение равенства (оно же является и простейшей эквивалентностью). В этом отношении все различные элементы *несравнимы* между собой.

Примером отношения частичного порядка является *отношение делимости* на множестве натуральных чисел. Как обычно, определим отношение $|$ по правилу:

$$a \overset{\text{опр}}{|} b \Leftrightarrow \text{существует такое } c \text{ из } \mathbf{N}, \text{ что } a \cdot c = b.$$

Отношение делимости рефлексивно ($a = a \cdot 1$), транзитивно (если $b = a \cdot u$ и $c = b \cdot v$, то $c = a \cdot (u \cdot v)$) и антисимметрично (если $a = b \cdot u$ и $b = a \cdot v$, то $u \cdot v = 1$ и $a = b$).

Это означает, что отношение делимости является отношением *порядка* на множестве \mathbf{N} (а \mathbf{N} частично упорядочено этим отношением).

Отметим, что отношение делимости, рассматриваемое на всем множестве целых чисел, уже не является отношением порядка: оно не антисимметрично.

Если декартов квадрат множества M наглядно представить геометрическим квадратом, то график линейного порядка на M образует черный треугольник, гипотенуза которого совпадает с диагональю I . На рисунке изображен фрагмент графика отношения \leq на множестве натуральных чисел.

Для множества действительных чисел \mathbf{R} декартов квадрат представляется не геометрическим квадратом, а всей плоскостью с декартовыми координатами. Диагональ I на этом представлении — это биссектриса угла первой и третьей четвертей, а графиком линейно-

го порядка \leq на множестве \mathbf{R} является верхняя полуплоскость, определяемая диагональю I , вместе с этой диагональю.

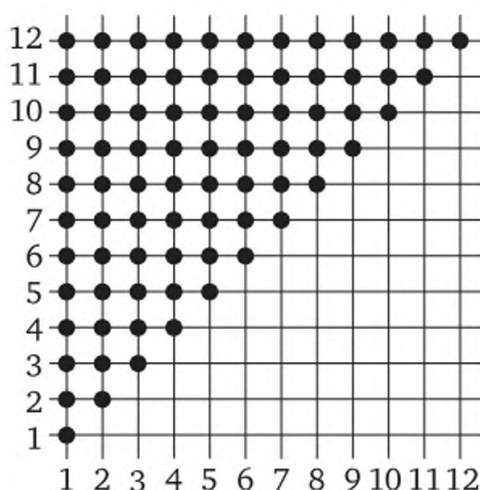


График линейного порядка

График частичного нестрогого порядка выглядит иначе. Диагональ в него попадает тоже, но черный треугольник график уже не образует.

Рассмотрим, например, отношение делимости на множестве \mathbf{N} . Поскольку из $a \mid b$ следует $a \leq b$, можно заранее предугадать, что график отношения \mid делимости на \mathbf{N} составит часть графика отношения \leq , т. е. новый график будет находиться внутри черного треугольника.

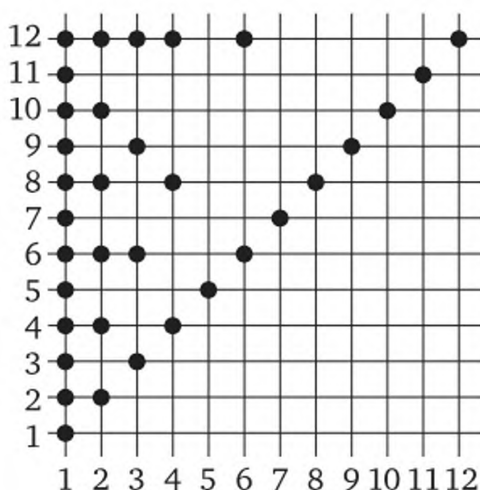
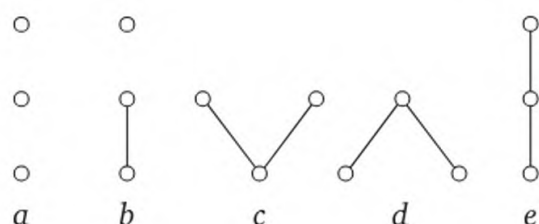


График отношения делимости

Множество из двух элементов $M = \{a, b\}$ можно упорядочить тремя способами:

- 1) оба элемента несравнимы;
- 2) $a < b$;
- 3) $b < a$.

Возьмем теперь множество из трех элементов и выясним, сколько отношений частичного порядка можно определить на этом множестве.



Отношения порядка на множестве из 3 элементов

Сначала посмотрим, сколько различных графов можно нарисовать, используя три точки. На схеме изображены эти графы без обозначения вершин. Граф *a* — это отношение, при котором все элементы несравнимы. На графе *b* два элемента сравнимы между собой, а третий — нет. На графе *c* два максимальных элемента и наименьший, а на графе *d* — два минимальных и наибольший. Граф *e* является изображением линейного порядка. Любой другой порядок на множестве из трех элементов будет совпадать с одним из пяти описанных типов.

На графе *a*, как бы ни были занумерованы вершины, порядок останется тем же самым. На графах *b* и *e* вершины можно расставить шестью различными способами, а на графах *c* и *d* — тремя. Суммируя все эти варианты, получаем, что на множестве из трех элементов можно задать отношение порядка 19 способами.

Если рассматривать лишь линейные порядки, то до расстановки обозначений вершин такой порядок *всего один*. Расставляя различными способами обозначения элементов, получаем, что на множестве будет в точности столько линейных порядков, сколько существует различных *перестановок* этого множества.

Еще раз подчеркнем, что для *каждого конечного множества существует лишь один тип линейного упорядочения*.

Для бесконечного множества это не так — одно и то же бесконечное множество можно линейно упорядочить существенно различными способами.

Рассмотрим, например, сначала *обычное* упорядочение множества натуральных чисел:

$$1 < 2 < 3 < 4 < 5 < 6 < \dots, \quad (*)$$

а затем *необычное*; объявим любое четное число больше любого нечетного (сохранив прежний порядок в подмножествах четных и нечетных чисел). В этом новом порядке натуральный ряд примет вид

$$1 < 3 < 5 < 7 < \dots < 2 < 4 < 6 < 8 < \dots. \quad (**)$$

Типы упорядочения (*) и (**) различны: при первом упорядочении каждое множество, состоящее из всех чисел, меньших данного числа, конечно, а во втором множество подмножество, состоящее из всех чисел, меньших любого четного числа, бесконечно.

Рассмотрим еще один пример упорядочения, широко распространенного и в науке, и в быту.

Пусть M — множество произвольных символов, которые назовем *буквами*, а M , соответственно, *алфавитом*. Среди символов поместим и символ пробела, например \square . Любую конечную цепочку букв назовем *словом*.

Упорядочение слов в словаре называют *словарным* (или *лексикографическим*¹) упорядочением.

$$M \left\{ \begin{array}{l} \square \\ a \\ b \\ c \\ \dots \\ d \end{array} \right.$$

Упорядочение по высоте

Текст в словаре идет сверху вниз, одно слово расположено *выше* или *ниже* другого, поэтому словарное упорядочение является упорядочением *по высоте*.

Словарное упорядочение является продолжением упорядочения алфавита. Пусть алфавит $M = \{\square, a, b, c, \dots, d\}$ упорядочен по высоте, причем символ пробела расположен *выше* всех остальных символов. Возьмем два слова в этом алфавите:

$$U = x_1 x_2 x_3 \dots x_n, \quad W = y_1 y_2 y_3 \dots y_m,$$

где $x_i, y_j \in M$. Если $n \neq m$, то, добавив необходимое число пробелов справа к слову меньшей длины, можно выровнять слова по длине. После этого можно сравнить эти слова по высоте.

Слово U в словаре будет расположено *выше* слова W , если

$$x_1 = y_1, \quad x_2 = y_2, \dots, x_{k-1} = y_{k-1},$$

но x_k выше y_k . Таким образом, словарное упорядочение определяется по первым различным символам.

Упорядочение слов по высоте («не выше» или «не ниже») является рефлексивным, транзитивным, антисимметричным и связным.

Короче говоря, словарное упорядочение является *линейным порядком*.

¹ От греч. слов $\lambda\epsilon\gamma\iota\chi\omicron\varsigma$ — «относящийся к слову» и $\gamma\rho\alpha\phi\omega$ — «пишу».

Пусть f — функция, определенная на множестве A со значениями в B , и оба множества упорядочены (может быть частично) отношением \prec . Говорят, что функция *монотонна*, если

$$x \prec x_1 \Rightarrow f(x) \prec f(x_1).$$

В частности, f может быть одноместной операцией на множестве M .

Если граф функции изображен на двух идентичных экземплярах исходного множества, то стрелки графа не опускаются вниз (в крайнем случае проходят горизонтально).

Если исходное множество упорядочено линейно и именно так расположено в декартовом квадрате для изображения графика монотонной функции, то каждая новая точка графика не ниже предыдущей.

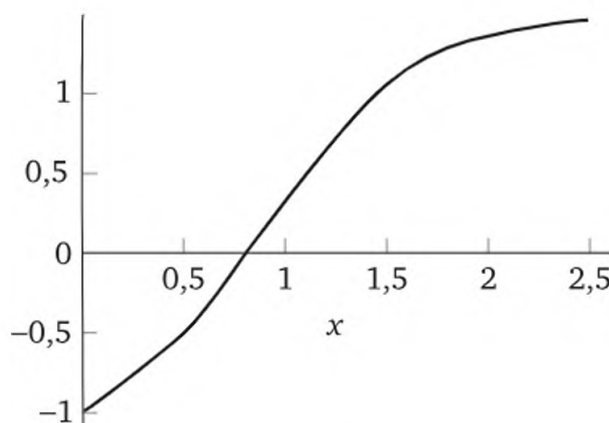


График монотонной функции

На рисунке изображен примерный вид графика монотонной (точнее, монотонно возрастающей) функции, определенной на \mathbf{R} и со значениями в \mathbf{R} .

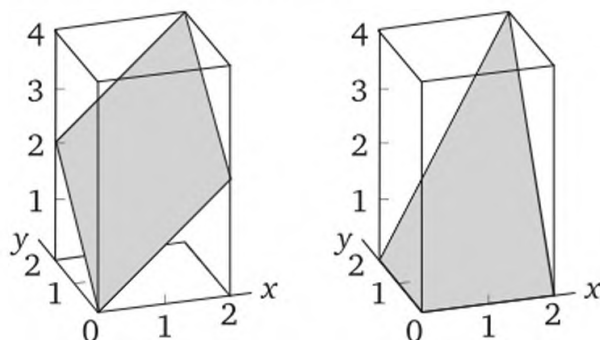
Если \circ — двухместная операция на M с отношением порядка \prec , то монотонность операции означает, что

$$x \prec x_1, y \prec y_1 \Rightarrow x \circ y \prec x_1 \circ y_1.$$

Точно так же, если исходное множество линейно упорядочено и именно так расположено в декартовом кубе, то, двигаясь по возрастанию любого из аргументов, мы не будем терять высоты.

Например, операция сложения на множестве действительных чисел монотонна, и график ее представляет наклонно расположенную плоскость, каждая точка которой увеличивает высоту при увеличении любого из слагаемых. Для наглядности на рисунке изображена часть графика для положительных действительных чисел. Монотонность в таком случае означает, что шарик, брошенный на график в любой точке, непременно скатится к началу координат.

Аналогичную (только более крутую) горку представляет собой график умножения на множестве положительных действительных чисел: умножение на \mathbf{R}_+ монотонно.



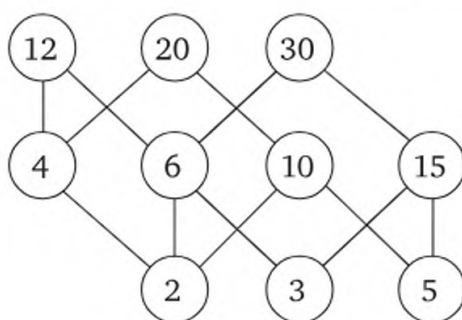
Графики сложения и умножения

Заметим, что отношение порядка — это не обязательно традиционный порядок на множестве чисел. Например, операция объединения множеств монотонна относительно включения, умножение на множестве натуральных чисел монотонно относительно делимости и т. п.

Элемент t из упорядоченного множества $\langle M; < \rangle$ называется *наибольшим*, если для любого элемента x выполняется $x < t$. Аналогичным образом определяется *наименьший* элемент в M : t называется *наименьшим*, если для любого элемента x выполняется $t < x$.

Элемент t называют *максимальным*, если в множестве M не существует такого элемента x , что $t < x$. Элемент t называют *минимальным*, если в множестве M не существует такого элемента x , что $x < t$.

Для частичного порядка понятия максимального и наибольшего (равно как и минимального и наименьшего) не совпадают.



Собственные делители числа 60

Например, в множестве *собственных* (т. е. отличных от единицы и самого числа) делителей числа 60, упорядоченном отношении делимости, нет наибольшего элемента, но есть три максимальных (12, 20, 30). Нет там и наименьшего элемента, но есть три минимальных элемента (2, 3, 5).

Если элемент является наибольшим, то он будет максимальным. Обратное утверждение, как показывает приведенный пример, неверно. Точно так же наименьший элемент минимальный, а обратное утверждение неверно. Однако если множество упорядочено линейно, то максимальный элемент будет и наибольшим (а минимальный — наименьшим). Иначе говоря, для линейного порядка понятия максимального и наибольшего (минимального и наименьшего) элементов совпадают.

Линейно упорядоченное множество (или подмножество частично упорядоченного множества) называют *цепью*.

Линейно упорядоченное множество называют *вполне упорядоченным*, если в нем каждое непустое подмножество имеет *наименьший* элемент.

Например, множество натуральных чисел вполне упорядочено отношением \leq , а множество целых чисел с тем же порядком не является вполне упорядоченным.

В 1904 г. Э. Цермело¹ доказал, что *любое множество можно вполне упорядочить*. Доказательство опирается на *аксиому выбора*, и более того, из теоремы Цермело *следует* аксиома выбора, т. е. аксиома выбора и теорема Цермело равносильны. Доказательство Цермело носит *косвенный* характер, и пока (2021 г.) никому не удалось привести хотя бы один пример вполне упорядочения множества \mathbf{R} действительных чисел.

Аксиома выбора имеет и другую равносильную формулировку 1935 г., вошедшую в историю как *лемма Цорна*²: *если каждая цепь частично упорядоченного множества имеет верхнюю грань, то каждый элемент множества не превышает некоторого максимального элемента из этого же множества*.

В частности, лемма Цорна означает, что при таком свойстве цепей в множестве непременно должен быть максимальный элемент. Чаще всего в доказательствах аксиома выбора используется в виде леммы Цорна.

В линейно упорядоченном множестве $\langle M; < \rangle$ выполняется условие *минимальности*, если каждое непустое подмножество этого множества имеет *наименьший* элемент. Линейно упорядоченное множество со свойством минимальности называют *вполне упорядоченным*.

Условие минимальности можно заменить другими, равносильными предложениями.

¹ Эрнст Цермело (Zermelo, 1871—1953) — немецкий математик, один из создателей аксиоматической теории множеств.

² Макс Август Цорн (Zorn, 1906—1993) — американский математик немецкого происхождения.

Условие индуктивности: если минимальный элемент множества M принадлежит подмножеству S из M и из того, что все элементы, предшествующие элементу a , принадлежат подмножеству S , следует, что и a принадлежит S , то $S = M$.

Условие обрыва убывающих цепей: каждая цепь

$$x_1 > x_2 > \dots > x_n > \dots$$

элементов множества M обрывается на конечном шаге.

Условия минимальности, индуктивности, обрыва убывающих цепей равносильны.

Покажем сначала, что *из условия индуктивности следует условие обрыва цепей*. Рассмотрим следующее свойство элемента x : цепочка

$$x > x_1 > x_2 > \dots > x_n > \dots,$$

начинающаяся с элемента x , обрывается на конечном шаге. Требования условия индуктивности выполнены, а это значит, что цепочка, начатая с *любого* элемента из множества M , обрывается.

Теперь установим методом от противного, что *из условия обрыва следует условие минимальности*. Пусть S — непустое множество множества M и для S не выполняется условие минимальности. Тогда для каждого элемента x из S всегда можно указать элемент, меньший его, и, следовательно, построить строго убывающую бесконечную цепочку элементов множества M . Полученное противоречие показывает, что такого подмножества S не существует.

Наконец, покажем, что *из условия минимальности следует условие индуктивности*.

Доказательство проведем также методом от противного, т. е. допустим, что для подмножества S посылка условия индуктивности выполнена, но множество S не совпадает с M . Тогда разность $M \setminus S$ не пуста и, следовательно, по условию минимальности содержит минимальный элемент a .

Элемент a не может быть минимальным во всем M : минимальный элемент всего множества уже попал в S по условию индуктивности. Это значит, что для любого элемента x если $x < a$, то x не принадлежит дополнению S .

Но это значит, что $x \in S$. Итак, для каждого $x < a$ следует, что $x \in S$, но тогда по условию индуктивности получаем, что $a \in S$. Получено противоречие, которое и доказывает наше утверждение.

Таким образом, установлена логическая цепочка утверждений:

Условие индуктивности	\Rightarrow	Условие обрыва убывающих цепей
Условие обрыва убывающих цепей	\Rightarrow	Условие минимальности
Условие минимальности	\Rightarrow	Условие индуктивности

Это означает, что из условия индуктивности следует условие минимальности, а из условия обрыва убывающих цепей — условие индуктивности: *все три условия равносильны*.

Говорят, что доказательство проведено методом математической индукции, если оно использует условие индуктивности (либо равносильное ему условие минимальности, либо условие обрыва убывающих цепей).

На этом пока приостановим рассмотрение свойств порядка.

Такие важные свойства, как архимедовость, дискретность, непрерывность и другие особенности порядка, будем обсуждать по мере актуальности, т. е. при изучении соответствующих математических систем.

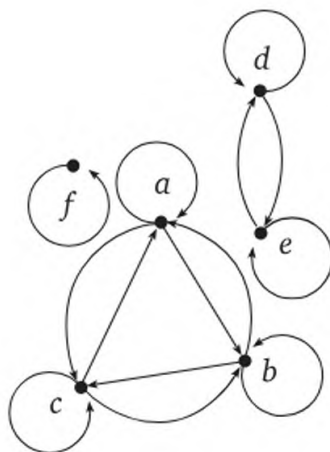
Переходим пока к третьему «математическому киту» — отношению эквивалентности.

2.4. Эквивалентность

Рассмотрим сначала на примере особенности графа и графика отношения эквивалентности. Зададим на множестве $M = \{a, b, c, d, e, f\}$ отношение эквивалентности T . Множество M конечно, поэтому T просто перечисляем:

$$T = \{(a, a), (a, b), (a, c), (b, a), (c, a), (b, c), (c, b), (b, b), (c, c), (d, d), (d, e), (e, d), (e, e), (f, f)\}.$$

Можно непосредственно убедиться, что T рефлексивно, транзитивно и симметрично, т. е. является отношением эквивалентности на множестве M .



Граф отношения эквивалентности

Впрочем, все перечисленные свойства еще лучше видны на графе отношения T . Бросается в глаза следующая особенность этого графа: он распадается на отдельные островки, причем ни один остров

никак не связан ни с каким другим, внутри же каждого островка проведены все, какие только можно, стрелки (ограничение отношения T на каждом острове является полным отношением).

Особые свойства графика отношения эквивалентности T также видны невооруженным глазом: этот график распадается на отдельные квадраты, диагонали которых лежат на диагонали декартова квадрата I . График представляет собой серию квадратов, нанизанных на диагональ.

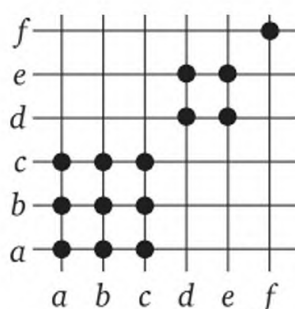


График отношения эквивалентности

В один квадрат на графике эквивалентности попадают элементы одного островка из графа этой эквивалентности.

Различные квадраты графика не имеют общих точек.

Рассмотрим теперь общую ситуацию, дав предварительно точное определение системе островков, возникших на графе эквивалентности (заодно будет раскрыта и тайна черных квадратов на графике эквивалентности).

Систему непустых подмножеств M_1, M_2, \dots, M_n (здесь n не обязательно конечное число) множества M называют разбиением M на смежные классы, если:

- 1) объединение множеств M_i совпадает со всем множеством M :

$$M_1 \cup M_2 \cup \dots \cup M_n = M;$$

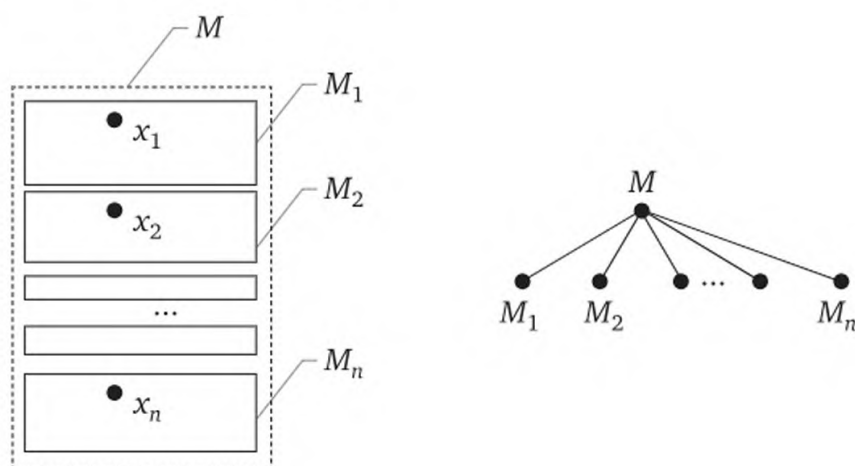
- 2) различные множества M_i, M_j не пересекаются:

$$M_i \neq M_j \Rightarrow M_i \cap M_j = \emptyset.$$

На рисунке изображено множество M , разбитое на смежные классы M_1, M_2, \dots, M_n , причем в каждом классе указан представитель своего класса. Множество x_1, x_2, \dots, x_n образует полную систему представителей. Слово «система» означает, что порядок элементов существенен.

Изображение может быть и другим, более лаконичным. Построим граф отношения включения для подмножеств, подразумевая по умолчанию, что пустое пересечение не изображается (в быту обычно используется гибрид этих схем, т. е. на графе отношения

включения вместо точек кругами — а чаще прямоугольниками — изображены смежные классы).



Разбиение множества на классы

Например, если под словом «школа» понимать множество учеников этой школы, то множество обычных школьных классов (1-й А, 1-й Б и т. д., 11-й А, 11-й Б и т. д.) образуют разбиение школы на смежные классы (и полную систему представителей образуют, например, делегаты общешкольной конференции с нормой представительства один класс — один ученик).

Отметим, что если речь идет об объединении попарно непересекающихся множеств, то вместо обычного символа объединения \cup обычно используется другой знак: \sqcup . В нашем случае это выглядит так:

$$M = M_1 \sqcup M_2 \sqcup \dots \sqcup M_n,$$

или в короткой записи:

$$M = \coprod_{i=1}^n M_i.$$

На множестве M , разбитом на смежные классы, введем бинарное отношение T по правилу

$$\overset{\text{опр}}{xTy} \Leftrightarrow x, y \text{ принадлежат одному классу.}$$

Отношение «быть одноклассником» рефлексивно, транзитивно и симметрично; иначе говоря, отношение T — эквивалентность. Это значит, что разбиение множества на классы определяет отношение эквивалентности на этом множестве.

Покажем, что выполняется и обратное утверждение: эквивалентность на множестве M определяет разбиение этого множества на классы.

Пусть \sim — эквивалентность на множестве M , а x — элемент из M . Рассмотрим множество $[x]$ всех элементов из M , эквивалентных элементу x :

$$[x] = \{y \in M \mid y \sim x\}.$$

Множество $[x]$ называют смежным классом по эквивалентности \sim с представителем x . Чтобы показать, что смежные классы по эквивалентности действительно являются смежными классами разбиения, заметим сначала, что если \sim — эквивалентность на множестве M , то для любых x, y из M

$$x \sim y \Leftrightarrow [x] = [y].$$

Поскольку отношение \sim рефлексивно, каждый элемент x принадлежит множеству $[x]$. Отсюда следует: во-первых, каждое такое множество не пусто; во-вторых, объединение всех подмножеств — это все множество M .

Теперь остается взять два различных подмножества $[x]$ и $[y]$ и показать, что их пересечение пусто.

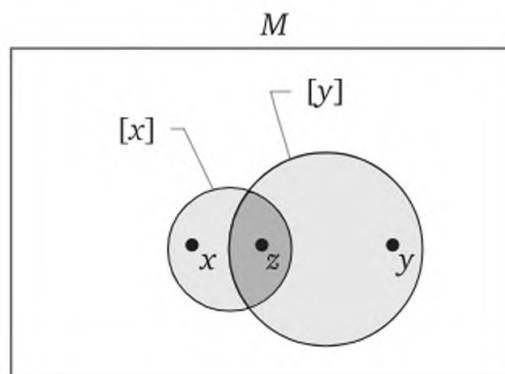
Заметим сначала, что если элемент y лежит в $[x]$, то для каждого z из M

$$z \sim x \Leftrightarrow z \sim y.$$

Это означает, что любой элемент из $[x]$ может быть выбран в качестве представителя этого множества или, другими словами, в множестве эквивалентных элементов все элементы равноправны:

$$z \sim x \Leftrightarrow [z] = [y].$$

Возьмем теперь два различных множества $[x]$ и $[y]$ и предположим, что их пересечение не пусто, т. е. существует такой элемент z , который принадлежит одновременно каждому из них.



Различные классы не пересекаются

Тогда имеем: $[x] = [z]$ и $[y] = [z]$, откуда $[x] = [y]$.

Таким образом, если классы имеют общий элемент, то они совпадают. Но это значит, что если классы не совпадают, то они не имеют общих элементов.

Итак, разбиение множества на классы определяет эквивалентность на этом множестве и наоборот — эквивалентность на множестве разбивает это множество на смежные классы.

Граф любого отношения эквивалентности распадается на отдельные островки. Внутри каждого островка проведены все возможные стрелки, а между отдельными островами этого архипелага нет никаких связей.

Система представителей для разбиения — это множество элементов, выбранных по одному из каждого смежного класса.

Отметим, что существование системы представителей в общем случае вовсе не очевидно. Хуже того, ссылаясь на существование такой системы, можно доказать факты, плохо согласующиеся с обыденным сознанием (например, что каждое тело конечного объема равносоставлено с двумя точно такими же телами).

Особая аксиома (свободного выбора) постулирует существование системы представителей. Некоторые следствия этой аксиомы очень сомнительны, поэтому современный исследователь, желая подчеркнуть чистоту своих доказательств, обычно отмечает, что аксиома выбора им не использовалась.

Впрочем, для простых случаев в применении аксиомы выбора и нет необходимости. Предположим, например, что дело происходит в множестве натуральных чисел. Положив в качестве представителя класса наименьшее число, лежащее в этом классе, мы получим полную систему представителей.

Множество всех смежных классов множества M по эквивалентности \sim называют фактор-множеством и обозначают символом M/\sim :

$$M/\sim = \{[x] \mid x \in M\}.$$

Если множество M специальным образом упорядочено — сначала все элементы первого смежного класса, затем второго и т. д., — то график отношения эквивалентности будет представлять систему черных непересекающихся квадратов, нанизанных на диагональ.

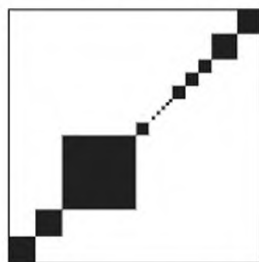


График эквивалентности

Наименьшая эквивалентность — это равенство, график которого состоит из диагонали, т. е. квадратов, выродившихся в точки. Наибольшая эквивалентность (полное отношение) имеет своим графиком большой черный квадрат, Казимир Малевич¹ мог назвать свою знаменитую картину «Полная эквивалентность».

Полная эквивалентность имеет всего лишь один класс разбиения. Следующая по простоте устройства эквивалентность имеет два смежных класса. Такая двухклассная эквивалентность полностью задается одним классом. Действительно, если A — не пустое и не совпадающее со всем множеством подмножество множества M , то A и \bar{A} определяют разбиение множества M и, соответственно, эквивалентность на M .

Можно привести примеры множеств, для которых настолько трудно установить, пусты они или нет, что до сих пор это никому не удалось сделать. Эти трудные множества дают примеры трудных эквивалентностей.

Пусть, например, A — множество совершенных чисел, B — множество нечетных чисел, а M — их объединение:

$$M = A \cup B.$$

Если пересечение A и B пусто, то мы получаем разбиение множества M на смежные классы и, следовательно, эквивалентность на M . Если пересечение не пусто, то это не эквивалентность.

Как обстоит дело в действительности, пока неизвестно.

Вернемся снова к связи эквивалентности и разбиения множества на смежные классы.

Отображение ε множества M на фактор-множество M/\sim , переводящее каждый элемент в смежный класс, в котором он лежит, т. е. $\varepsilon(x) = [x]$, называют естественным отображением множества M на свое фактор-множество.

Ситуация может быть и обратной. Если $f: M \rightarrow M_1$ — отображение множества M на множество M_1 , то отношение равнообразности, заданное правилом

$$x \sim y \overset{\text{опр}}{\Leftrightarrow} f(x) = f(y),$$

является эквивалентностью на M . Эту эквивалентность называют ядерной².

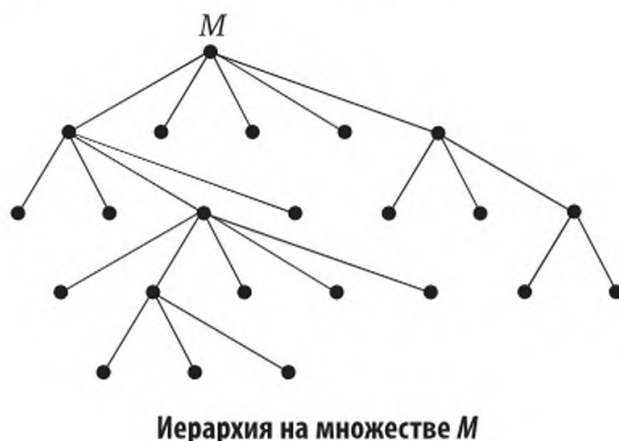
¹ Малевич Казимир Северинович (1878—1935) — русский художник. На выставке «0,10» в конце 1915 г. показал 39 полотен под общим названием «Супрематизм живописи», в том числе «Черный квадрат на белом фоне» — свое самое знаменитое произведение. Рыночная цена «Квадрата» в настоящее время — более 20 млн долл. США.

² Для гомоморфизмов особо важных алгебраических объектов (групп, колец, векторных пространств) ядерная эквивалентность задается некоторым подмножеством — ядром гомоморфизма.

Переход от множества M к фактор-множеству M/\sim называют факторизацией (или классификацией) множества M .

Обычно под классификацией понимают несколько эквивалентностей на одном множестве, причем каждая из эквивалентностей является продолжением другой: смежный класс по одной эквивалентности (более высокого уровня) распадается на смежные классы по другой эквивалентности (более низкого уровня). Все эквивалентности уровня выше первого являются частичными, т. е. симметричными и транзитивными, но не рефлексивными отношениями.

Граф отношения включения для смежных классов по таким эквивалентностям принято называть иерархией¹.



Подведем предварительные итоги.

Каждое отношение эквивалентности на множестве задает разбиение этого множества на смежные классы, и наоборот, каждое разбиение множества на смежные классы задает отношение эквивалентности на этом множестве.

Рефлексивное и транзитивное отношение называют предпорядком. Предпорядок может не быть ни эквивалентностью, ни порядком.

Например, отношение делимости на множестве целых чисел, отношение следствия для уравнений и систем уравнений, отношение следствия для предикатов — все это отношения предпорядка, не являющиеся ни порядком, ни эквивалентностью.

Пусть \prec — некоторый предпорядок на множестве M (говорят, что множество M предупорядочено). Отношение \sim на M , заданное правилом

$$\text{опр} \quad x \sim y \Leftrightarrow x \prec y \text{ и } y \prec x,$$

называют отношением ассоциированности.

¹ От греч. *hieros* — «священный» и *arche* — «власть». Обычно имеются в виду уровни рассматриваемых эквивалентностей.

Ассоциированность является эквивалентностью. Более того, если она связана с исходным отношением предпорядка следующим образом: $x \sim x_1$ и $y \sim y_1$, то высказывания $x < y$ и $x_1 < y_1$ равносильны:

$$x < y \Leftrightarrow x_1 < y_1.$$

Ассоциированность, как и каждая эквивалентность, разбивает множество на смежные классы, а отмеченная связь ассоциативности и $<$ позволяет корректно определить отношения между смежными классами, полагая

$$[x] < [y] \Leftrightarrow x < y.$$

На множестве смежных классов отношение предпорядка превращается в отношение порядка.

Предупорядоченное множество после факторизации по ассоциированности, заданной предпорядком, становится упорядоченным.

Например, отношение делимости, являющееся всего лишь предпорядком на множестве целых чисел, образует порядок на множестве классов ассоциированных элементов, в качестве представителей которых можно выбрать элементы из \mathbb{Z}_0 .

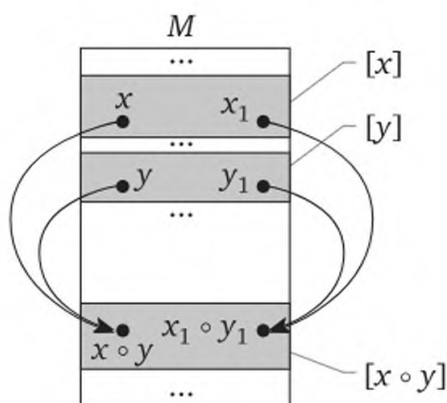
Пусть на множестве M заданы двухместная операция \circ и отношение эквивалентности \sim . Говорят, что эквивалентность согласована (или совместима) с операцией, если для всех элементов x, x_1, y, y_1 из M

$$x \sim x_1, y \sim y_1 \Rightarrow x \circ y \sim x_1 \circ y_1.$$

Если эквивалентность согласована с операцией, то операцию на M можно перенести на фактор-множество M/\sim , положив по определению:

$$[x] \circ [y] \stackrel{\text{опр}}{=} [x \circ y].$$

Это определение корректно, т. е. результат операции не зависит от выбора представителей в классах $[x], [y]$.



Согласованность эквивалентности и операции

Эквивалентность может быть согласованной и с одноместной операцией f :

$$x \sim x_1 \Rightarrow f(x) \sim f(x_1).$$

Аналогичным образом эквивалентность может согласовываться с операцией любой местности. Эквивалентность \sim согласована с n -местной операцией f , если для каждого элемента $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$

$$a_1 \sim b_1, a_2 \sim b_2, \dots, a_n \sim b_n \Rightarrow f(a_1, a_2, \dots, a_n) \sim f(b_1, b_2, \dots, b_n).$$

Эквивалентность может быть согласованной не только с операцией математической системы, но и с любым другим отношением на этой системе (в частности, с отношением порядка). Эквивалентность \sim согласована с n -местным отношением S , если для каждого $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ из $a_1 \sim b_1, a_2 \sim b_2, \dots, a_n \sim b_n$ следует равносильность:

$$S(a_1, a_2, \dots, a_n) \Leftrightarrow S(b_1, b_2, \dots, b_n).$$

Пусть, например, S — бинарное отношение. Тогда согласованность эквивалентности \sim и отношения S означает, что для всех a_1, a_2, b_1, b_2 из $a_1 \sim a_2, b_1 \sim b_2$ следует

$$a_1 S b_1 \Leftrightarrow a_2 S b_2.$$

Эквивалентность, согласованная со всеми операциями и отношениями алгебраической системы, называется конгруэнцией.

Отметим, что естественным обобщением эквивалентности является и толерантность — рефлексивное и симметричное бинарное отношение. Хотя толерантность и не разбивает множества на смежные классы, все равно можно говорить о согласованности толерантности и операции. В этом случае толерантность называют совместимой.

Совместимая толерантность — это обобщение конгруэнции.

Рассмотрим сначала несколько примеров эквивалентности из школьного курса математики. Первый пример — арифметический.

Пусть множество

$$M = \left\{ \frac{a}{b} \mid a \in \mathbf{Z}, b \in \mathbf{N} \right\}$$

состоит из всевозможных дробей, числитель которых — целое, а знаменатель — натуральное число.

Введем на множестве M отношение \sim по правилу

$$\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c.$$

Это отношение действительно эквивалентность, т. е. рефлексивно, транзитивно и симметрично. Как и всякая эквивалентность, отношение \sim разбивает множество дробей на смежные классы эквивалентных дробей. Смежный класс (подмножество всех эквивалентных дробей) называют рациональным числом, а множество всех смежных классов (т. е. фактор-множество M/\sim) обозначают буквой \mathbf{Q} и называют множеством рациональных чисел.

По школьной традиции множество и фактор-множество даже не различают (эквивалентность дробей — элементов из M — подразумевается по умолчанию) и пишут просто:

$$\mathbf{Q} = \left\{ \frac{a}{b} \mid a \in \mathbf{Z}, b \in \mathbf{N} \right\}.$$

Отношение равенства дробей не просто эквивалентность — это отношение согласовано с арифметическими операциями и отношением порядка, т. е. является конгруэнцией.

Приведем еще один пример арифметической эквивалентности, которая используется при обсуждении свойств рациональных и иррациональных чисел.

Отношение \sim на множестве \mathbf{R}_+ положительных действительных чисел, заданное правилом (для каждого x, y из \mathbf{R}_+)

$$x \sim y \Leftrightarrow \frac{\overset{\text{опр}}{x}}{y} \in \mathbf{Q}_+,$$

рефлексивно, симметрично и транзитивно, т. е. является эквивалентностью.

Это отношение принято называть соизмеримостью в множестве \mathbf{R}_+ , а эквивалентные в этом смысле элементы — соизмеримыми.

Теперь рассмотрим геометрический пример эквивалентности.

Пусть L — множество всех отрезков (на плоскости или в пространстве), а отношение \cong на множестве L определено правилом:

$$AB \overset{\text{опр}}{\cong} CD \Leftrightarrow \text{длины } AB \text{ и } CD \text{ равны.}$$

Это отношение является эквивалентностью и уже по своему определению согласовано операцией «длина отрезка»:

$$AB \cong CD \Leftrightarrow \text{длина } AB = \text{длина } CD.$$

Операция «длина отрезка» не совсем такая, как, скажем, операция «сложение дробей» из предыдущего примера. Операция сложения

ния отображает декартов квадрат $M \times M$ множества M в само множество M . Символически это выглядит так:

$$+: \left(\frac{a}{b}, \frac{c}{d} \right) \rightarrow \frac{ad+bc}{bd} \in M.$$

Результат операции находится внутри M , поэтому говорят, что сложение (как, впрочем, и вычитание, и умножение) является внутренней операцией.

Операция «длина» отображает множество L в другое множество — множество \mathbf{R}_0 неотрицательных действительных чисел. Множество \mathbf{R}_0 находится вне L , поэтому операцию такого рода (такими же являются в геометрии площадь и объем) называют внешней операцией. То, что «длина» — внешняя операция, не меняет существа дела: отношение \cong на множестве отрезков является конгруэнцией (которую принято называть конгруэнтностью).

Конгруэнтность на множестве отрезков можно перенести на множество всех фигур следующим образом. Две фигуры A и B назовем конгруэнтными, если существует взаимно однозначное отображение f фигуры A на фигуру B , сохраняющее длину отрезка. Это значит, что если $f(X)$ — образ точки X , $f(Y)$ — образ точки Y , то для каждой точки X, Y фигуры A выполняется равенство

$$\text{длина } XY = \text{длина } f(X)f(Y).$$

Конгруэнтность фигур согласована с длиной (если фигуры A, B имеют длину), с площадью (если фигуры A, B имеют площадь) и с объемом (если фигуры A, B имеют объем).

Кроме равенства длин, на множестве отрезков можно ввести отношение одинаковой направленности. Это тоже эквивалентность. Пересечение эквивалентностей само является эквивалентностью. Таким образом, свойство «иметь равные длины и равные направления» является эквивалентностью на множестве направленных отрезков. Смежный класс по этой эквивалентности называют вектором.

После арифметического и геометрического примеров эквивалентностей рассмотрим алгебраический образчик эквивалентности.

Рассмотрим множество всевозможных уравнений с одним неизвестным. Два уравнения равносильны, если их множества решений совпадают. Отношение равносильности является эквивалентностью. Множество всех уравнений разбивается на смежные классы равносильных уравнений.

Алгебраический пример можно естественным образом обобщить в логический.

Уравнение — это частный случай предиката, т. е. высказывания с переменной. Вместо уравнения можно взять произвольный предикат

кат (например, от одной переменной и определенный на некотором универсальном множестве U). Класс равносильных на U предикатов определяет одно и то же подмножество множества U , а множество всех предикатов распадается на смежные классы равносильных предикатов.

Вопрос о совпадении или несовпадении двух множеств — это вопрос о равносильности двух предикатов: принадлежат два предиката одному смежному классу по этой эквивалентности или нет? Можно было и не подниматься до алгебры предикатов, а ограничиться высказываниями.

Отношение логического следствия для высказываний является рефлексивным и транзитивным, т. е. предпорядком.

Две формулы F и G алгебры высказываний равносильны тогда и только тогда, когда $F \Rightarrow G$ и $G \Rightarrow F$. Другими словами, отношение равносильности является отношением ассоциированности для логического следования.

Как обычно для отношения предпорядка, отношение ассоциированности будет отношением порядка на множестве классов равносильных элементов. Это значит, что, хотя отношение логического следствия и не является отношением порядка на множестве всех формул алгебры высказываний, оно является порядком на множестве классов равносильных формул.

На множестве формул, упорядоченном отношением «логическое следствие», существуют наименьший и наибольший элементы.

Таблица истинности импликации означает, что из лжи следует все, что угодно, — это правда. Следовательно, тождественно ложная формула является наименьшим элементом на множестве формул. Аналогично, что истина следует из чего угодно, — это правда. Поэтому тождественно истинная формула является наибольшим элементом на множестве формул.

Логические операции были определены над высказываниями, но выполняются они над классами равносильных формул. То же самое касается и отношения логического следствия. Чтобы доказать корректность такого перехода, нужно установить согласованность отношения равносильности и логических операций и согласованность отношения равносильности и логического следствия.

Непосредственно с помощью таблиц истинности проверяется, что отношение равносильности согласовано с логическими операциями, т. е. если $A \Leftrightarrow A_1$ и $B \Leftrightarrow B_1$, то

$$A \& B \Leftrightarrow A_1 \& B_1;$$

$$A \vee B \Leftrightarrow A_1 \vee B_1;$$

$$A \rightarrow B \Leftrightarrow A_1 \rightarrow B_1;$$

$$A \leftrightarrow B \Leftrightarrow A_1 \leftrightarrow B_1;$$

$$\bar{A} \Leftrightarrow \bar{A}_1.$$

Так же проверяется, что отношение равносильности согласовано с отношением логического следствия, т. е. если $A \Leftrightarrow A_1$ и $B \Leftrightarrow B_1$, то:

$$A \Rightarrow B \text{ тогда и только тогда, когда } A_1 \Rightarrow B_1.$$

Последние наблюдения как раз и означают, что элементами алгебры высказываний в действительности являются не отдельные формулы, а классы равносильных формул.

Операции выполняются над классами, и логическое следствие — это отношение порядка на множестве классов. Отдельная формула — это лишь представитель класса. Каждый класс имеет бесконечное число представителей.

При изучении конкретных эквивалентностей и соответствующих им разбиений прежде всего возникает естественный вопрос: как узнать для произвольной пары элементов исходного множества, эквивалентны они или нет?

Эту задачу принято называть проблемой упрощения.

Пусть \sim — эквивалентность на M и M_i — соответствующие классы разбиения множества M . Число классов n не обязательно конечно; в каждом смежном классе M_1, M_2, \dots, M_n выберем по элементу x_i , представляющему этот класс. Множество x_1, x_2, \dots, x_n — полная система представителей.

Для множества с отношением эквивалентности какая-либо из систем представителей может оказаться привлекательнее остальных. Привлекательность чаще всего связана с простотой в том или ином смысле. Простейшая система и будет самой хорошей.

Пусть x_1, x_2, \dots, x_n — простейшая система представителей для эквивалентности \sim . Говорят, что для эквивалентности \sim и системы представителей x_1, x_2, \dots, x_n алгоритмически разрешима проблема упрощения, если существует алгоритм, позволяющий для любого элемента x из M указать простейший представитель x_i смежного класса $[x]$.

Разрешимость проблемы упрощения означает, что хотя бы теоретически можно представить некоторую вычислительную технику, которая решает эту задачу, а именно: получив произвольный элемент x , в конечное число шагов выдает элемент x_i , эквивалентный x . Если проблема упрощения алгоритмически разрешима, то для любой пары элементов x, y можно по единому алгоритму установить, эквивалентны x, y (лежат они в одном классе) или нет.

Отметим, что проблема упрощения разрешима далеко не всегда даже на множестве натуральных чисел.

Для эквивалентности, имеющей всего два смежных класса, проблема упрощения равносильна проблеме вхождения в некоторое подмножество.

Произвольное непустое собственное подмножество H множества M разбивает множество M на два класса: H и его дополнение — \bar{H} . Выберем в качестве представителей любую пару элементов a, b , один из которых принадлежит H (скажем, $a \in H$), а другой — нет ($b \notin H$). Тогда получаем формулировку проблемы упрощения в следующем виде. Найти алгоритм, позволяющий узнавать для любого элемента x из M , с каким из двух элементов — с a или с b — элемент x лежит в одном смежном классе. Иначе говоря, требуется алгоритм для узнавания, входит элемент x в подмножество H или нет.

Множество алгоритмов и множество подмножеств натуральных чисел состоят из различного числа элементов (множество подмножеств $P(\mathbb{N})$ существенно больше), поэтому существуют подмножества с заведомо неразрешимой проблемой вхождения.

Сокращая числитель и знаменатель дроби на наибольший общий делитель, мы получаем простой представитель (в виде несократимой дроби) для рационального числа, т. е. решаем проблему упрощения для множества дробей и отношения эквивалентности на этом множестве.

Представление рационального числа в виде десятичной дроби (пусть даже бесконечной, но периодической) — это тоже решение проблемы упрощения на том же множестве и с той же эквивалентностью, но с другой системой представителей.

Решение уравнения (или системы уравнений) состоит в поиске наиболее простого представителя класса равносильных уравнений, т. е. такого уравнения, которое уже и решать не надо — оно само выглядит как ответ.

Например, для системы уравнений с n неизвестными x_1, x_2, \dots, x_n , имеющей в точности одно решение, такими представителями будут системы уравнений:

$$\left\{ \begin{array}{ll} x_1 & = a_1, \\ & x_2 = a_2, \\ & \dots \\ & x_n = a_n. \end{array} \right.$$

Уже приведенных примеров достаточно, чтобы понять особую роль отношения эквивалентности в математике, однако рассмотрим еще один, может быть, самый важный пример отношения эквивалентности и связанного с ним отношения порядка, а именно: обсудим вопросы, связанные с понятием числа элементов множества.

Особенность ситуации состоит в том, что понятие множества является первичным: через это понятие определяются и все другие.

Понятия числа среди первичных нет, и задача состоит в том, чтобы определить понятие «число элементов множества», не используя понятие «число».

2.5. Мощность

Эта задача разрешима, и в основе ее решения лежит понятие равномощности.

Два множества A и B называют равномощными, если существует взаимно однозначное отображение f одного множества на другое, т. е. $f: A \rightarrow B$, причем прообраз B совпадает с множеством A , а образ A совпадает с множеством B , и различные элементы из A переходят в различные элементы из B .

Отношение «быть равномощным» бинарное (в нем два места). Можно было бы сказать, что равномощность — это бинарное отношение на множестве всех множеств, не будь у нас сведений о том, что понятие множества всех множеств противоречиво (заметим, что после появления понятия мощности противоречивость эта усиливается еще больше).

Чтобы не впасть в противоречие, ограничим себя каким-то классом множеств (подмножествами заданного множества M , множествами, построенными из имеющихся с помощью теоретико-множественных операций, и т. п.), и если этот класс хорошо определен, уже спокойно сможем говорить о бинарном отношении равномощности на классе множеств K .

Итак, на классе множеств K определено отношение равномощности. Отношение равномощности рефлексивно: отображение, переводящее каждый элемент x множества A в себя, является взаимно однозначным отображением множества A на себя.

Отношение равномощности симметрично: если $f: A \rightarrow B$ — взаимно однозначное отображение A на B , то отображение f^{-1} , определенное по правилу

$$f^{-1}(b) = a \overset{\text{опр}}{\Leftrightarrow} f(a) = b,$$

является взаимно однозначным отображением множества B на A .

Отношение равномощности транзитивно: если $f: A \rightarrow B$ и $g: B \rightarrow C$ — взаимно однозначные отображения на, то композиция $f \circ g$, переводящая каждый элемент a из A в $g(f(a))$, тоже является взаимно однозначным отображением множества A на множество C .

Итак, отношение равномощности рефлексивно, симметрично и транзитивно, короче говоря, эквивалентность.

Как всякая эквивалентность, она разбивает множество K на смежные классы. В один класс попадут все множества, состоящие из оди-

накового числа элементов (заметим, что определение понятия числа пока не требуется), а множества, состоящие из различного числа элементов, находятся в разных классах.

Число элементов множества M сейчас характеризуется тем, в каком смежном классе находится множество M . Сам смежный класс, содержащий множество M , и можно было бы объявить числом элементов в множестве M . Но смежный класс равномоощных множеств принято называть иначе.

Смежный класс по равномоощности называют мощностью множества.

Мощность множества M обозначают символом $n(M)$ или $|M|$. Если мощность M равна m , то это значит, что $M \in m$, но так не говорят и так не пишут. Принято говорить «мощность множества равна m » вместо «множество принадлежит мощности m » и соответственно писать $|M| = m$.

Мощность конечного множества принято называть числом элементом, а начальный отрезок натурального ряда брать представителем мощности конечного множества.

Множество (а точнее класс) мощностей — это еще не математический объект. Таковым он будет тогда, когда на нем будут определены отношения и операции (т. е. когда появится алгебраическая система).

На классе конечных мощностей определяются равенство и отношение порядка. Эти определения буквально переносятся на произвольные мощности.

Мощности сравнивают по правилу: $a \leq b$ тогда и только тогда, когда существуют такие множества A и B , что $|A| = a$, $|B| = b$, и взаимно однозначное отображение, которое переводит множество A на подмножество из B (инъекция A в B).

Отношение порядка для мощностей действительно является порядком.

Используя единичное отображение, видим, что отношение порядка \leq для мощностей рефлексивно. Поскольку произведение инъекций снова является инъекцией, отношение порядка \leq для мощностей транзитивно.

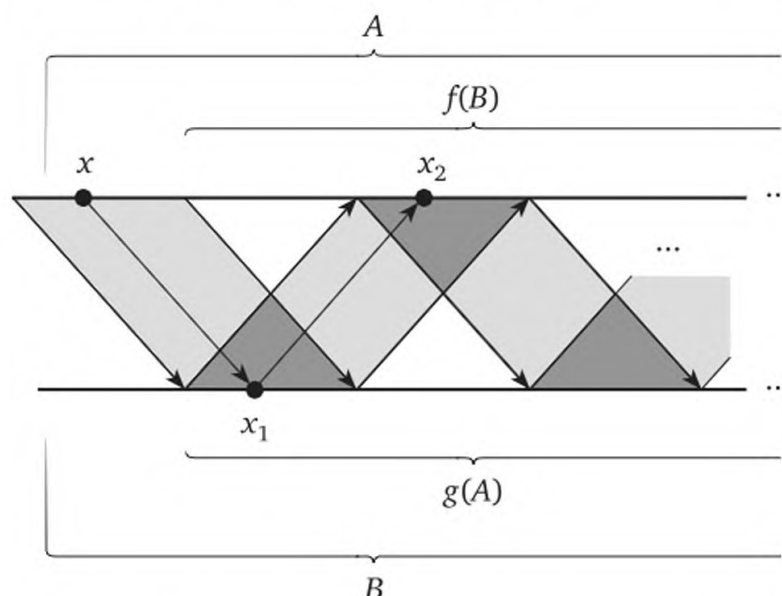
С доказательством антисимметричности дело обстоит чуть сложнее. Пусть g — инъекция множества A в множество B , а f — инъекция B в A . Если $f(B) = A$ или $f(A) = B$, то соответствующая инъекция является биекцией, множества A и B равномоощны.

Считая, что обе разности не пусты, можно устроить биекцию множества A на множество $f(B)$.

Если g — инъекция множества A в множество B , а f — инъекция B в A , то множества A и $f(B)$ равномоощны.

Разность $A \setminus f(B)$ можно «загнать внутрь» множества $f(B)$.

На рисунке символически изображены в виде лучей множества A и B . Стрелки, изображающие отображение g , идут сверху вниз (наискосок вправо), а f -стрелки — снизу вверх (наискосок вправо).



Разность $A \setminus f(B)$ можно «загнать внутрь» множества $f(B)$

На схеме видно, как использовать оба эти отображения для взаимно однозначного перемещения элементов из A в $f(B)$. Перемещаются, как бы отражаясь от B , лишь элементы внутри серых полос, а прочие элементы остаются неподвижными. Для примера на схеме выделен путь одного элемента: элемент x переходит сначала в x_1 , а затем в x_2 . Элемент x_2 аналогичным скачком переходит в некоторый элемент x_3 из $f(B)$ и т. д.

Теперь, используя транзитивность и симметричность отношения равномощности, получаем утверждение об антисимметричности.

Отношение порядка \leq для мощностей антисимметрично.

Доказательство утверждения об антисимметричности порядка для мощностей принадлежит сразу трем авторам: Кантору¹, Бернштейну² и Шредеру³, и носит название теоремы Кантора — Бернштейна (или Шредера — Бернштейна)⁴.

¹ *Георг Кантор (Cantor, 1845—1918)* — немецкий математик, создатель теории множеств, в работах 1879—1884 г. систематически изложил учение о бесконечности.

² *Феликс Бернштейн (Bernstein, 1878—1956)* — немецкий математик, ученик Г. Кантора, профессор университета в Геттингене (в 1933 г. эмигрировал в США).

³ *Эрнст Шредер (Schröder, 1841—1902)* — немецкий математик и логик, с 1876 г. — профессор Высшей технической школы в Карлсруэ. Автор первого систематического изложения математической логики. В 1890 г. ввел знаки \subset и \supset для отношения включения множеств.

⁴ Первое безупречное доказательство этой теоремы принадлежит Бернштейну. Оно опубликовано в книге Е. Бореля «Лекции по теории функций» в 1898 г.

Рефлексивность, транзитивность и антисимметричность отношения \leq для мощностей означает, что отношение \leq является отношением порядка.

На самом деле отношение порядка для мощностей обладает свойством связности.

Вспомним, как определяется отношение порядка для конечных мощностей (натуральных чисел) и какие доводы приводятся в доказательстве связности в школьном курсе математики.

Уже в начальном курсе математики присутствует два вида натуральных чисел. Один вид чисел предназначен для ответа на вопрос «сколько?». Эти числа количественные. Мощность — это количественное число в общем виде (число элементов в любом, конечном и бесконечном, множествах).

Кроме количественных натуральных чисел, применяются порядковые натуральные числа. Порядковое число отвечает на вопрос «который?». Например, пять — это количественное натуральное число, а пятое (пятый, пятая) — порядковое натуральное число.

Обратим внимание на то, что в школьном курсе математики сравниваются не количественные, а соответствующие им порядковые числа. Например, число 5 меньше числа 6, потому что пятое число в процессе счета (т. е. порядка) возникает раньше шестого числа. При таком подходе проблемы с доказательством связности отношения порядка нет. Одно из натуральных чисел (если они не равны) возникнет при счете раньше, а другое позже.

Чтобы эту идею реализовать в общем виде, нам нужно обобщение порядкового натурального числа и установление связей между этими общими порядковыми числами с обобщением количественных чисел (мощностями).

Заметим, впрочем, что точного определения натурального числа (ни порядкового, ни количественного) у нас пока нет. Мы пользуемся пока интуитивно-догматическими соображениями из школьного курса математики. Это означает, что, определив сейчас порядковые числа в общем виде, мы, в частности, получим и точное определение порядкового натурального числа.

Для определения мощности был взят класс множеств и отношение равномощности на этом классе. Отношение оказалось эквивалентностью и разбило класс на смежные подклассы. Эти подклассы и есть мощности.

Аналогичным образом поступим и при определении порядкового числа, т. е. возьмем класс множеств, введем некоторое отношение между множествами, которое является эквивалентностью, а смежный класс по этой эквивалентности назовем порядковым числом. Определение должно согласовываться со старым (пусть и неточным) представлением о натуральном порядковом числе. После этого надо будет ввести отношение порядка для порядковых чисел,

причем так, чтобы новый порядок являлся продолжением старого порядка на множестве натуральных порядковых чисел.

Приступаем к реализации этого плана.

В отличие от ситуации с мощностями, теперь возьмем множества не произвольные, а вполне упорядоченные (т. е. линейно упорядоченные и удовлетворяющие условию минимальности).

Два вполне упорядоченных множества $\langle M_1; \prec \rangle$ и $\langle M_2; \prec \rangle$ называют однотипными, если существует биекция $f: M_1 \rightarrow M_2$ одного множества на другое, сохраняющее отношение порядка (для любых x, y из M_1):

$$x \prec y \Leftrightarrow f(x) \prec f(y).$$

Однотипные множества изоморфны, как алгебраические системы, а отображение f — это изоморфизм.

Отношение однотипности для вполне упорядоченных множеств является аналогом равномощности для произвольных множеств. Точнее говоря, отношение однотипности является эквивалентностью.

Равнотипность (как и любая эквивалентность) разобьет класс множеств на смежные классы. Смежный класс по отношению однотипности называют порядковым числом.

Порядковые числа задаются своими представителями. Если даны два порядковых числа a и b , то равенство $a = b$ означает, что существует множество A , вполне упорядоченное по типу a , и существует множество B , вполне упорядоченное по типу b , и системы $\langle A; \prec \rangle$ и $\langle B; \prec \rangle$ изоморфны. Если же выполняется неравенство $a \neq b$, то системы $\langle A; \prec \rangle$ и $\langle B; \prec \rangle$ не изоморфны (в них или A и B не равномощны, или не существует биекции, сохраняющей отношение порядка).

Конечное множество можно линейно (а значит и вполне) упорядочить только по одному типу. Этот тип полностью определяется мощностью этого множества, и, следовательно, натуральное порядковое число однозначно определяется соответствующим количественным числом.

Однотипные множества равномощны. Это означает, что равномощность — это продолжение однотипности, следовательно, отношение однотипности разбивает на подклассы смежный класс по равномощности.

Иначе говоря, класс равномощных множеств может состоять из нескольких классов разнотипных множеств, т. е. количественное число — это совокупность нескольких порядковых чисел.

Различные неизоморфные упорядочения (даже при одной и той же мощности) представляют различные порядковые числа.

Для конечных множеств каждый класс по мощности состоит в точности из одного класса по типу, а вот бесконечное множество

действительно можно вполне упорядочить существенно различными способами.

Естественный порядок

$$1 < 2 < 3 < \dots < n < n+1 < \dots$$

множества натуральных чисел принято называть типом ω (омега). Таким образом, все упорядоченные множества, изоморфные ряду натуральных чисел, имеют тип ω .

Бесконечное множество можно упорядочить по типу, отличному от типа ω . Рассмотрим, например, множество рациональных чисел

$$M = \left\{ \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots, \frac{n}{n+1}, \dots, 1 \mid n \in \mathbf{N} \right\}$$

с обычным упорядочением, т. е.

$$\frac{1}{2} < \frac{2}{3} < \frac{3}{4} < \dots < 1.$$

Это множество также вполне упорядочено, но тип его другой — его обозначают символом $\omega + 1$.

В этом упорядочении перед единицей стоит бесконечно много элементов, в упорядочении типа ω элементов, обладающих таким свойством, нет.

Вполне упорядоченное множество

$$\frac{1}{2} < \frac{2}{3} < \frac{3}{4} < \dots < 1 + \frac{1}{2} < 1 + \frac{2}{3} < \dots < 1 + \frac{n}{n+1} < \dots$$

представляет еще один тип $(\omega + \omega)$, отличный от первых двух¹.

Другими словами, количественное число одно, а различных типов, ему соответствующих, по крайней мере три.

В действительности таких типов гораздо больше. Продолжая строить примеры такого же рода, можно заметить, что на счетном множестве существует бесконечное число различных порядковых типов.

Инъекцию f , сохраняющую отношение порядка, можно устроить и в само множество вполне упорядоченного множества на себя.

Такое отображение f обладает особым свойством. Если изобразить эту инъекцию на графе отношения порядка, то обнаружится, что ни одна из f -стрелок на графе порядка не идет вниз, изомор-

¹ Если A и B — два непересекающихся вполне упорядоченных множества, то общее продолжение порядков на множестве $A \cup B$, при котором для каждого $a \in A$, $b \in B$ выполняется $a < b$, является представителем суммы порядковых чисел, представленных A и B .

физм f может перемещать элементы из M только вверх (или оставлять их на месте). Точнее говоря, если f — изоморфизм вполне упорядоченного множества $< M; < >$ на свое подмножество, то для каждого элемента x из M

$$f(x) < x \text{ или } f(x) = x.$$

Для доказательства этого утверждения достаточно взять такое наименьшее x (оно существует благодаря условию минимальности), что $x < f(x)$. Но f сохраняет отношение порядка, поэтому тогда $f(f(x)) < f(x)$ вопреки выбору x .

Пусть x — произвольный элемент вполне упорядоченного множества M . Множество элементов из M , меньших элемента x , называют (начальным) отрезком множества M .

Само множество M является своим (несобственным) начальным отрезком. Все остальные отрезки (в том числе и пустое подмножество) собственные.

Теперь заметим, что свойство вполне упорядоченности аналогично свойству конечности. Конечное множество не равномощно своему собственному подмножеству, а вполне упорядоченное множество неизоморфно своему собственному начальному отрезку.

Действительно, из того, что инъекция, сохраняющая отношения, не перемещает элементы вниз на графе, следует, что не существует изоморфизма между вполне упорядоченным множеством и его собственным начальным отрезком.

Определим теперь отношение порядка на множестве порядковых чисел. Определение будет простым обобщением отношения порядка для порядковых натуральных чисел, которое вводится в начальной школе.

Если a, b — два порядковых числа с представителями A и B соответственно, то положим $a \leq b$, если A изоморфно начальному отрезку множества B .

Непосредственно из определения следует, что отношение порядка \leq на множестве порядковых чисел рефлексивно, транзитивно.

Из невозможности изоморфизма вполне упорядоченного множества и его собственного начального отрезка теперь следует, что отношение порядка \leq на множестве порядковых чисел антисимметрично.

Обозначим символом $M(a)$ множество порядковых чисел, строго меньших порядкового числа a . Множество порядковых чисел, строго меньших порядкового числа a , является вполне упорядоченным и имеет порядковый тип a .

Возьмем теперь два произвольных порядковых числа a, b и соответствующие им множества $M(a)$ и $M(b)$. Пересечение $M(a) \cap M(b)$ —

тоже вполне упорядоченное множество, следовательно, ему соответствует порядковое число c .

Из того, что $c \leq a$ и $c \leq b$, следует, что любые два порядковых числа сравнимы.

По теореме Цермело любое множество можно вполне упорядочить. Порядковые числа сравнимы между собой. Следовательно, и любые две мощности сравнимы.

Первоначально поставленная цель (доказательство линейности отношения порядка для любого множества мощностей) достигнута.

На самом деле, мощности не просто линейно упорядочены, но и вполне упорядочены.

Сначала убедимся, что этим свойством обладают порядковые числа.

Пусть M — произвольное множество порядковых чисел и $x \in M$. Если x не является наименьшим в M , то множество $M(a) \cap M$ вполне упорядочено и, следовательно, имеет наименьший элемент. Этот элемент является наименьшим в M . Другими словами, любое множество порядковых чисел вполне упорядочено.

Но теперь из связи между порядковыми и количественными числами следует, что любое множество мощностей вполне упорядочено.

В утверждениях о линейности и связности порядка для порядковых чисел и мощностей присутствуют слова «любое множество» (порядковых чисел или мощностей). Почему бы вместо «любое множество» не сказать просто «множество», имея в виду все множество мощностей (или порядковых чисел) сразу? Дело в том, что ни того, ни другого множества не существует.

Образно говоря, мощностей (и порядковых чисел) слишком много для того, чтобы образовывать множество. Поэтому и использовалось слово «класс» (класс мощностей, класс порядковых чисел), взять подмножество из класса (т. е. часть, не слишком большую и не приводящую к противоречию) нам никто не запрещает. Вот эта часть и входила в предыдущие утверждения под именем любого множества.

В заключение сделаем одно самокритичное замечание.

Хотя ранее уже широко применялись термины «конечное» и «бесконечное», определения конечного множества пока не было. Понятие конечного было основано на понятии натурального ряда, но интуитивно-наивное школьное определение натурального ряда как множества вида

$$\{1, 2, 3, \dots, n, \dots\}$$

не выдерживает серьезной критики.

К счастью, для определения понятия конечного множества натуральные числа и не требуются.

Подмножество H множества M , отличное от M , называют собственным подмножеством. Иначе говоря, H — собственное подмножество в M , если $M \setminus H \neq \emptyset$.

Множество M конечно, если оно не равномощно никакому своему собственному подмножеству.

Соответственно множество, равномощное некоторому своему собственному подмножеству, бесконечно.

Отношение порядка \leq для всех мощностей остается таким же и для конечных мощностей. Однако в конечном случае доказательство антисимметричности проще. Можно установить, не ссылаясь на теорему Кантора — Шредера — Бернштейна, что отношение порядка \leq для конечных мощностей антисимметрично.

Свойство конечности (и бесконечности) сохраняется при равномощности. Иначе говоря, множество, равномощное конечному множеству, само конечно.

Интуитивно очевидные свойства конечности легко проверяются и в случае точного определения. Например, подмножество конечного множества само конечно, а множество, содержащее бесконечное подмножество, само бесконечно.

Любое множество, равномощное с множеством натуральных чисел, называют счетным — его элементы можно пересчитать (не обязательно с помощью алгоритма).

Счетную мощность принято обозначать символом \aleph_0 (читается «алеф-нуль», где \aleph — первая буква древнефиникийского алфавита, прародительница греческой буквы α — альфа). Итак, $|\mathbb{N}| = \aleph_0$.

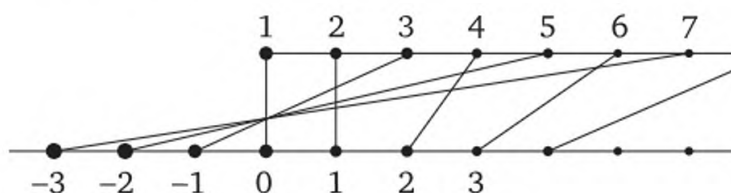
Например, множество целых неотрицательных чисел \mathbb{Z}_0 счетно. Действительно, отображение $f: \mathbb{Z}_0 \rightarrow \mathbb{N}$, заданное правилом $f(x) = x + 1$, является взаимно однозначным отображением одного множества на другое: $|\mathbb{Z}_0| = \aleph_0$.

Множества \mathbb{Z}_0 и \mathbb{N} отличаются всего лишь одним элементом. Поэтому их равномощность неудивительна.

Целых чисел вроде бы гораздо больше, чем натуральных — кроме \mathbb{N} , множество \mathbb{Z} содержит еще одно бесконечное множество:

$$-\mathbb{N} = \{-x \mid x \in \mathbb{N}\}.$$

И все-таки множества \mathbb{Z} и \mathbb{N} равномощны: между их элементами существует взаимно однозначное соответствие.



Множество \mathbb{Z} счетно

Это соответствие задается выписыванием (перечисляющим алгоритмом) множества

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\};$$

множество \mathbb{Z} счетно; $|\mathbb{Z}| = \aleph_0$.

Множество рациональных чисел \mathbb{Q} представляется значительно большим, чем множество целых чисел. Достаточно отметить, что между каждой парой сколь угодно близких друг другу рациональных чисел находится бесконечное подмножество рациональных чисел. Мощность множества \mathbb{Q} должна быть, на первый взгляд, больше мощности множества \mathbb{N} .

Однако оказывается, что рациональных чисел в точности столько же, сколько и целых. Иначе говоря, *множество \mathbb{Q} счетно*.

Действительно, каждое рациональное число можно представить и единственным образом в виде бесконечной десятичной периодической дроби (кроме случая девятки в периоде). Это значит, что каждое рациональное число представляется конечной цепочкой символов.

Множество всевозможных таких цепочек-слов счетно: сначала мы можем перечислить все слова из одного символа, затем — из двух, далее трехсимвольные и т. д. Для любого конечного числа n существует лишь конечное число множества n -буквенных слов (и, соответственно, рациональных чисел). Эти конечные подмножества можно упорядочить любым способом (например, по возрастанию), а в результате будет получен пересчет \mathbb{Q} . Множество \mathbb{Q} имеет такую же мощность, что и \mathbb{N} : $|\mathbb{Q}| = \aleph_0$.

Идея, примененная для пересчета \mathbb{Q} , переносится на общий случай.

Множество всевозможных конечных цепочек символов — слов в некотором алфавите — счетно, если алфавит конечен. Возьмем, например, множество всех предложений, использующих латинский и греческий алфавиты, кириллицу, знаки препинания (в том числе знак пробела), математические, логические символы и т. п. Тогда предложение, выражающее любое свойство элементов, будет представлять всего одно слово в этом расширенном алфавите.

Это значит, что множество всех свойств (предикатов) счетно. Следовательно, *лишь счетное число множеств можно задать с помощью свойств элементов этих множеств*.

Счетным будет и множество всевозможных алгоритмов. Каждый алгоритм (некоторая инструкция, состоящая из предложений) с использованием знака пробела будет представляться одним словом. Множество слов в счетном алфавите само счетно, следовательно, существует лишь счетное число множеств, которые можно задать перечисляющими алгоритмами.

Попробуем получить множество большей мощности с помощью теоретико-множественных операций. Фактически мы уже подсчитывали элементы в объединении двух счетных множеств при установлении счетности множества целых чисел.

Множество \mathbb{Z} является объединением двух непересекающихся счетных множеств, $\mathbb{Z} = \mathbb{Z}_0 \cup (-\mathbb{N})$, а пересчет множества \mathbb{Z} состоял в одновременном пересчете этих двух подмножеств.

Точно так же можно поступить и для произвольных непересекающихся множеств.

Если $A = \{a_1, a_2, a_3, \dots, a_n, \dots\}$ и $B = \{b_1, b_2, b_3, \dots, b_n, \dots\}$ — два счетных множества, то их объединение $A \cup B$ тоже счетно. Действительно,

$$A \cup B = \{a_1, b_1, a_2, b_2, a_3, b_3, \dots, a_n, b_n, \dots\}.$$

Суммой мощностей называют мощность непересекающихся множеств-представителей мощностей слагаемых

$$|A| + |B| = |A \cup B|,$$

где $A \cap B = \emptyset$.

Счетность объединения счетных множеств означает, что

$$\aleph_0 + \aleph_0 = \aleph_0.$$

Суммирование счетных мощностей не привело к еще большим мощностям.

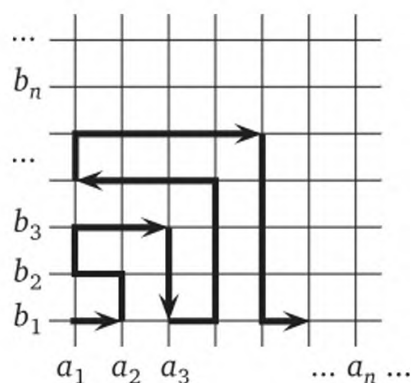
Заметим, что среди чисел таким же свойством (идемпотентности) обладает только число нуль: $0 + 0 = 0$. Сходство счетной мощности с числом нуль состоит не только в этом. Счетная мощность является наименьшей бесконечной мощностью.

Действительно, если M — произвольное бесконечное и несчетное множество, то из него можно последовательно выбрать счетное число элементов $x_1, x_2, \dots, x_n, \dots$ (если выборка оборвется на конечном шаге, то M конечно, а если M иссякнет после выборки, то M счетно). Если m — произвольная бесконечная мощность, то $\aleph_0 \leq m$.

После выборки множество $x_1, x_2, \dots, x_n, \dots$ можно разделить на два счетных непересекающихся подмножества (например, элементы на четных и нечетных местах) и одну часть вернуть на место взятого. В результате множество M будет иметь исходную мощность: $\aleph_0 + m = m$.

Правда, мы пока что никаких бесконечных множеств мощности m , больше счетной, не обнаружили. Посмотрим, может быть, декартово умножение позволит увеличить мощность и получить несчетное множество.

Декартово произведение $A \times B$ счетных множеств тоже счетно.



Перечисление элементов $A \times B$

На рисунке показан алгоритм перечисления элементов декартова произведения в виде пути последовательного обхода множества $A \times B$:

$$A \times B = \{(a_1, b_1), (a_2, b_1), (a_2, b_2), (a_1, b_2), (a_1, b_3), (a_2, b_3), (a_3, b_3), (a_3, b_2), (a_3, b_1), (a_4, b_1), \dots, a_n, \dots\}.$$

Произведением мощностей называют мощность декартова произведения множеств-представителей мощностей множителей:

$$|A| \cdot |B| = |A \times B|.$$

Счетность декартова произведения счетных множеств означает, что $\aleph_0 \cdot \aleph_0 = \aleph_0$. Умножение двух счетных мощностей не привело к большим мощностям.

Число нуль идемпотентно и относительно умножения: $0 \cdot 0 = 0$. Однако на этом аналогия с арифметическими операциями над числами заканчивается. Счетная мощность не является, подобно нулю, поглощающим элементом при умножении, его роль такая же, как у единицы, — нейтральная: если m — произвольная бесконечная мощность, то $\aleph_0 \cdot m = m$.

Декартово произведение счетных множеств является объединением счетного числа счетных множеств. Поэтому счетное объединение счетного числа счетных множеств само является счетным множеством.

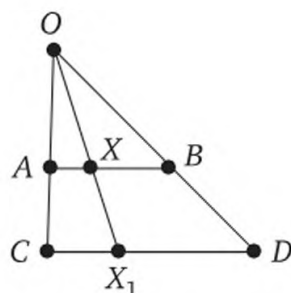
Итак, множества \mathbb{Z}_0 , \mathbb{Z} , \mathbb{Q} , а также множество всех предикатов и множество всех алгоритмов счетны. Не удалось получить из \aleph_0 большей мощности, используя суммирование даже бесконечного числа счетных множеств, ничего нового не дало и декартово умножение.

Так, может быть, действительно следует говорить просто «бесконечно большое», потому что все бесконечные мощности равны между собой?

Рассмотрим еще одну серию примеров.

Геометрическая фигура — это множество точек. Пусть AB и CD — два отрезка различной длины.

Число точек в отрезках одинаково — любые два отрезка равно-мощны.



Множества AB и CD равномощны

На схеме указано взаимное однозначное соответствие между этими множествами, переводящее каждую точку X одного отрезка в точку X_1 другого. Отсюда сразу следует, что равномощны все фигуры, являющиеся объединением конечного числа отрезков, например, любой m -угольник равномощен любому n -угольнику для любых m, n .

Аналогично устанавливается, что равномощны все окружности, эллипсы, овалы и вообще все линии ограниченной длины. Но длина может быть и неограниченной.

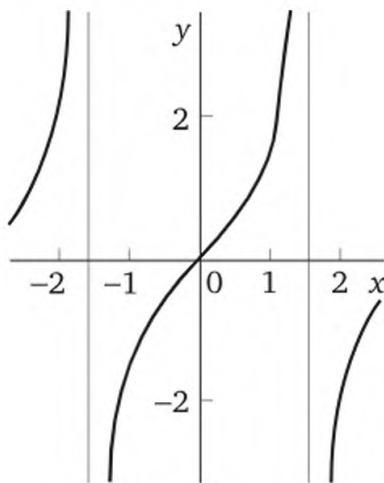


График $y = \operatorname{tg}(x)$

Функция $y = \operatorname{tg}(x)$ устанавливает взаимно однозначное соответствие между точками интервала $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ и точками прямой. Это значит, что точек во всей прямой ровно столько же, сколько их в любом числовом интервале.

Отрезки, ломаные, дуги окружностей — это все фигуры размерности один. Все фигуры размерности один равномощны.

Возьмем теперь фигуру размерности два, например квадрат.

Пусть $OABC$ — квадрат, являющийся декартовым произведением двух отрезков единичной длины:

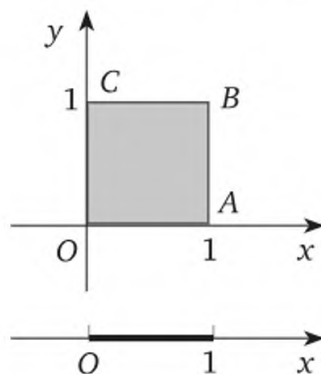
$$OABC = \{(x, y) \mid 0 \leq x \leq 1, 0 \leq y \leq 1\}.$$

Воспользуемся десятичной записью действительных чисел. Тогда:

$$x = 0, a_1 a_2 a_3 \dots, \quad y = 0, b_1 b_2 b_3 \dots,$$

где a_i, b_i — цифры (девятку в периоде не разрешается).

Если значение y не изменяется, то получается отрезок, параллельный оси абсцисс, в частности, $OA = \{(x, 0) \mid 0 \leq x \leq 1\}$.



Квадрат и отрезок равномощны

Пусть мощность множества точек отрезка OA равна m , а мощность множества точек квадрата $OABC$ равна n . Поскольку отрезок является подмножеством квадрата, $m \leq n$.

Покажем, что неравенство $m \leq n$ тоже верно. Поставим в соответствие каждой точке квадрата

$$(0, a_1 a_2 a_3 \dots; 0, b_1 b_2 b_3 \dots)$$

точку отрезка

$$(0, a_1 b_1 0 a_2 b_2 0 a_3 b_3 0 \dots; 0).$$

Если точки квадрата различны, то и соответствующие точки отрезка тоже будут различными. Более того, если разрешить записывать числа с девяткой в периоде, то одной точке квадрата окажутся поставленными в соответствие различные точки отрезка.

Например, точку $(0,1; 0,2)$ можно записать тогда и в виде $(0,09999\dots; 0,19999)$. Первому изображению соответствует точка отрезка $(0,12000000\dots; 0)$, а второму — другая $(0,010990990990\dots; 0)$.

Следовательно, возникает однозначное отображение множества точек квадрата внутрь отрезка. Но это как раз и означает, что $m \geq n$. Множество точек отрезка и множество точек квадрата равномощны.

Заметим, что здесь пришлось воспользоваться теоремой Кантора — Бернштейна об антисимметричности отношения \leq для мощностей. Но и без этой теоремы, дающей равенство мощностей, одно лишь неравенство (точек в квадрате не больше, чем в отрезке) уже впечатляет.

Если A равномощно A_1 , а B равномощно B_1 , то $A \times B$ равномощно $A_1 \times B_1$. Новое отображение является просто объединением исходных отображений.

Прямая Ox равномощна с отрезком OA . Отрезок OC равномощен с прямой Oy . Прямое произведение отрезка OA на OC — это квадрат $OABC$. Прямое произведение двух прямых — это вся плоскость.

Множество точек квадрата и множество точек плоскости равномощны.

Прямая Oz равномощна с отрезком OA . С отрезком OC равномощна вся плоскость xOy . Прямое произведение отрезка OA на OC — это квадрат $OABC$. Прямое произведение прямой и плоскости — это все трехмерное пространство. Следовательно, все трехмерное пространство и квадрат равномощны.

Итак, отрезок (любой, сколь угодно малой, но ненулевой длины), прямая, плоскость, все трехмерное пространство — все эти множества состоят из одинакового числа точек. Из такого же числа точек состоит любая фигура размерности один, два или три.

Хотя после этого может показаться, что бесконечность только одна, бесконечность не единственна.

Несчетные (и более чем несчетные) множества существуют.

Для начала докажем, что множество всех точек в интервале $[0, 1]$ несчетно.

Замечателен сам метод, которым делается это доказательство. В честь автора¹ он называется диагональным методом Кантора.

Допустим противное, т. е. предположим, что множество это счетно или, другими словами, все числа из этого интервала можно пересчитать: $x_1, x_2, x_3, \dots, x_n, \dots$.

Запишем каждое из этих чисел в виде десятичной дроби:

$$x_1 = 0, a_{11} a_{12} a_{13} \dots;$$

$$x_2 = 0, a_{21} a_{22} a_{23} \dots;$$

$$\dots\dots\dots$$

$$x_n = 0, a_{n1} a_{n2} a_{n3} \dots;$$

$$\dots\dots\dots$$

Запись этих чисел изображает как бы бесконечный квадрат, у которого мы видим лишь верхний левый угол. Рассмотрим диагональ

¹ Несчетность множества действительных чисел Г. Кантор доказал в 1874 г.

этого квадрата, идущую из этого угла. Этой диагонали метод и обязан своим названием «диагональный».

Итак, будем смотреть на диагональ этой записи якобы всех действительных чисел из интервала $[0, 1]$ и одновременно строить действительное число из этого интервала, но не попавшее в перепись всех таких чисел.

Число $x = 0, a_1 a_2 a_3 \dots a_n \dots$, где a_i — цифры, принадлежит нашему интервалу. Выберем эти цифры так, чтобы число x отличалось от любого числа в этом списке. Для этого положим цифру $a_1 \neq a_{11}$, а чтобы не получилось двусмысленностей сейчас и в дальнейшем, будем считать, что $a_1 \neq 9$. Какие бы дальше цифры не ставили, число x заведомо будет отличаться от x_1 .

Теперь перейдем ко второй цифре. Положим цифру $a_2 \neq a_{22}$, и снова на всякий случай $a_2 \neq 9$. Теперь мы точно знаем, что число x заведомо будет отличаться и от x_2 . Продолжим и далее движение по диагонали сопровождать построением числа x .

Положим цифру $a_3 \neq a_{33}$, и $a_3 \neq 9$, и т. д.: $a_n \neq a_{nn}$ и $a_n \neq 9$. Поскольку наше число отличается по крайней мере в одной цифре от числа x_n , оно отлично от всех чисел из этого списка. Полученное противоречие показывает, что предположение о возможности пересчета всех действительных чисел из интервала $[0, 1]$ ошибочно. Это значит, что множество действительных чисел из интервала $[0, 1]$ несчетно.

Было замечено ранее, что объединение счетного числа счетных множеств само счетно. Слово «объединение» нельзя заменить словами «декартово произведение». Для декартова произведения это утверждение неверно.

Элементом декартова произведения счетного числа множеств A_i принято называть последовательность элементов $(a_1, a_2, \dots, a_n, \dots)$, где $a_i \in A_i$. Только что проведенное рассуждение о несчетности множества $[0, 1]$ показывает, в частности, что *декартово произведение счетного числа конечных (десятиэлементных) множеств является несчетным*.

Множество чисел из интервала $[0, 1]$ равномощно множеству \mathbf{R} всех действительных чисел. Мощность $|\mathbf{R}|$ множества всех действительных чисел называют мощностью континуума и $[0, 1]$ обозначают¹ символом c или \aleph (буква «алеф» без индекса).

Любая геометрическая фигура размерности, не меньшей единицы (в частности, отрезки, прямые, плоскости и все пространство), имеют размерность \aleph .

Итак, *бесконечные мощности различимы*.

Существуют по крайней мере две бесконечности — счетная и континуальная. На самом деле, различных бесконечностей значительно больше.

¹ Символ c — первая буква латинского слова *continuum* (непрерывный).

Для конечных мощностей нет наибольших: для любого конечного множества M существует конечное множество M_1 большей мощности, $|M| < |M_1|$.

Точно такая же ситуация и для бесконечных мощностей: в предыдущем абзаце слова «конечных», «конечного», «конечное» можно просто вычеркнуть.

Для конечных множеств было установлено, что объединение конечного множества M и множества, состоящего из одного элемента, само конечно (и имеет большую мощность, чем M). Если бы задача состояла только в доказательстве существования множества мощности большей $|M|$, то решить ее можно было проще (причем сразу для всех множеств — конечных и бесконечных). Теперь мы уже знаем, что для конечных множеств $P(M)$ равномощно декартовой $|M|$ -й степени двухэлементного множества, поэтому $|P(M)| = 2^{|M|}$. Для конечных множеств число $|P(M)|$ значительно больше, чем $|M|$.

Для бесконечных множеств M это свойство сохранится.

Мощность множества $|P(M)|$ всех подмножеств множества M строго больше $|M|$.

Докажем это утверждение.

Множество $|M|$ содержит подмножество, равномощное множеству M : каждому элементу a можно поставить во взаимно однозначное соответствие подмножество $\{a\}$, содержащее только один этот элемент. Следовательно,

$$|M| \leq |P(M)|.$$

Теперь нужно показать, что мощность множества $P(M)$ строго больше мощности M , т. е. взаимно однозначного соответствия между элементами этих множеств не существует.

Доказательство проведем методом от противного, т. е. предположим, что существует такое взаимно однозначное соответствие f , которое переводит каждый элемент x из M в некоторое подмножество $f(x)$ множества M . При этом некоторые элементы x могут не лежать в своем образе $f(x)$.

Например, прообраз пустого множества обладает таким свойством.

Рассмотрим множество X всех таких элементов из M , которые не лежат в своем образе при отображении f :

$$X = \{x \in M \mid x \notin f(x)\}.$$

По нашему предположению, каждое подмножество множества M имеет прообраз при отображении f . Имеет его и множество X . Пусть $f(y) = X$. Тогда возникают две возможности:

- 1) $y \in X$;
- 2) $y \notin X$.

В первом случае по определению множества X получается, что $y \in f(y)$, т. е. $y \in X$, противоречие.

Остается вторая возможность. Снова по определению множества X и элемента y получаем, что из $y \notin X$ следует $y \in X$. Снова получили противоречие.

Итак, при нашем допущении о равномощности множества и его множества подмножеств в любом случае возникает противоречие. Взаимно однозначное соответствие между множествами $P(M)$ и M невозможно:

$$|P(M)| > |M|.$$

Мощности множеств не ограничены.

Неограниченность мощностей впервые была доказана Г. Кантором в 1878 г., и этот факт называют теоремой Кантора. Доказательство теоремы Кантора, по существу, использовало парадокс, который впоследствии получил название парадокса Рассела¹. Сам Кантор его не заметил, а возможно, и не хотел замечать — открытие Рассела (да и другие парадоксы теории множеств) Кантор переживал очень тяжело.

Из неограниченности мощностей следует, что понятие множества всех множеств противоречиво.

Действительно, если X — множество всех множеств, то мощность X наибольшая, но по теореме Кантора $|P(X)| > |X|$.

Образно говоря, различных множеств слишком много; свойство «быть множеством» не задает множества. Не будут множествами, впрочем, и многие части множества всех множеств. Когда желают сказать что-то о некоторой совокупности множеств, обычно употребляют слова «класс множеств, обладающих некоторым свойством».

Противоречивым будет и понятие множества всех мощностей. Действительно, предположим, что X — множество, содержащее по представителю каждой мощности. Какова бы ни была мощность m , в X найдется элемент — множество M — мощности m .

Возьмем объединение Y всех множеств, входящих в X . Тогда, с одной стороны, по теореме Кантора $|P(Y)| > |Y|$, а с другой — множество мощности $|P(Y)|$ содержится в Y . Полученное противоречие означает, что *множества, состоящего из представителей всех мощностей, не существует.*

Это значит, что и различных мощностей слишком много, свойство «быть представителем мощности» не задает множества. Когда

¹ Бертран Артур Уильям Рассел (Russell, 1872—1970) — английский математик, логик, философ. Пытался свести математику к логике, в 1902 г. сформулировал один из парадоксов теории множеств (парадокс Рассела): множества $\{x | x \notin x\}$ не существует.

все-таки возникает желание сказать что-то обо всех мощностях сразу, обычно употребляют слова «класс мощностей».

В то же время понятие множества конечных мощностей непротиворечиво. Точнее, существует множество, являющееся объединением представителей всех конечных мощностей. Для конечного множества M множество $P(M)$ подмножеств множества M содержит значительно больше элементов, чем M . Для $m > 1$ между числами m и 2^m содержится промежуточное число (а для $m > 2$ и не одно).

Для бесконечных множеств ситуация иная: между мощностью самого множества M и мощностью множества его подмножеств $P(M)$ промежуточных нет¹.

Покажем, что мощность множества действительных чисел — это в точности вторая бесконечная мощность: мощность множества \mathbb{R} равна мощности $P(M)$ множества подмножеств множества натуральных чисел.

Каждому подмножеству H любого множества N можно поставить во взаимно однозначное соответствие характеристическую функцию:

$$F(x) = \begin{cases} 0, & \text{если } x \notin H, \\ 1, & \text{если } x \in H. \end{cases}$$

Если F задать табличным способом в виде таблицы с двумя строками, то вторая строка таблицы — это некоторая последовательность нулей и единиц. Сколько таких последовательностей, столько и подмножеств у счетного множества.

Вместо десятичной позиционной системы счисления воспользуемся двоичной системой. Тогда запись $0, a_1 a_2 a_3 \dots a_n \dots$ означает следующее:

$$0, a_1 a_2 a_3 \dots a_n \dots = \frac{a_1}{2} + \frac{a_2}{2^2} + \frac{a_3}{2^3} + \dots + \frac{a_n}{2^n} + \dots,$$

где a_i — цифры двоичной системы, т. е. числа, равные единице или нулю. Любое число из интервала $[0, 1]$ имеет представление в двоичной записи. Как и девятка для десятичной системы, число 1 является особым — единицу в периоде можно заменить нулем².

¹ Строго говоря, это не совсем так. При аксиоматическом построении теории множеств оказалось, что это свойство для бесконечных мощностей может выполняться или не выполняться подобно тому, как выполняется постулат о параллельных в геометрии Евклида и не выполняется в геометрии Лобачевского. Однако, как и в случае с геометрией, теория множеств с промежуточными мощностями между M и $P(M)$ для бесконечных множеств M является экзотической.

² Это свойство объясняется тем, что и девятка в десятичной, и единица в двоичной системе на единицу меньше основания системы (в первом случае — десятки, во втором — двойки).

Каждому действительному числу $0, a_1a_2a_3...a_n...$ из интервала $[0, 1]$, записанному в двоичной системе счисления, поставим в соответствие последовательность

$$a_1, a_2, a_3, ..., a_n, ...,$$

состоящую из нулей и единиц, и, тем самым, подмножество множества натуральных чисел. Множества, в которые должны были отображаться числа с единицей в периоде, не появятся никогда (отметим, что это все множества, имеющие конечные дополнения; и множество таких множеств всего лишь счетно).

Итак, множество действительных чисел взаимно однозначно отображается на подмножество множества $P(N)$, следовательно, $|R| \leq |P(N)|$. В то же время $|N| < |R|$.

В естественной аксиоматике теории множеств между $|N|$ и $|P(N)|$ нет промежуточных, и полученные неравенства означают, что в первом случае на самом деле имеет место точное равенство:

$$|R| = |P(N)|.$$

Мощность $|R|$ является мощностью, непосредственно следующей за \aleph_0 .

Чтобы подчеркнуть связь между мощностью множества действительных чисел и счетной мощностью, мощность континуума обозначают символом 2^{\aleph_0} :

$$\aleph = 2^{\aleph_0}.$$

Множество всех подмножеств множества натуральных чисел несчетно, а множество предикатов лишь счетно. Следовательно, существует несчетное число множеств, не задаваемых с помощью предиката, т. е. свойства элементов этого множества.

Множество алгоритмов всего лишь счетное, поэтому существует несчетное число счетных множеств (подмножеств множества N), которые нельзя задать перечисляющим алгоритмом. Поскольку алгоритм перечисляет лишь счетное (или конечное) множество, любое несчетное бесконечное множество нельзя задать перечисляющим алгоритмом.

Из счетности множества алгоритмов следует также, что существует несчетное число подмножеств множества N , заданных неэффективно, — алгоритма, решающего проблему вхождения в такие множества, не существует.

Рассмотрим более тонкую ситуацию. Пусть множество M целых неотрицательных чисел задано перечисляющим алгоритмом. Является ли такое задание всегда эффективным? Ответ на этот вопрос отрицательный: существуют множества, заданные перечисляющим

алгоритмом, которые нельзя задать эффективно, т. е. алгоритма, решающего проблему вхождения, для них не существует.

Доказательство существования такого множества проводится диагональным методом Кантора аналогично доказательству несчетности континуума.

Рассмотрим алгоритмы, реализующие эффективность, т. е. решающие проблему вхождения в подмножества натуральных чисел. Алгоритм представляет собой инструкцию, т. е. множество слов в некотором алфавите, а если включить символ пробела, то одно слово. Множество таких слов можно упорядочить (например, по длине, а среди слов одинаковой длины — так, как упорядочены слова в словарях). Соответственно упорядочатся и все эффективно задаваемые множества:

$$M_1, M_2, \dots, M_i, \dots$$

Каждое множество однозначно представляется своей характеристической функцией, т. е. M_i можно задать с помощью последовательностей нулей и единиц (единицей на n -м месте отмечается вхождение, а нулем — не вхождение натурального числа n в M_i). Изобразим эти соответствия:

$$\begin{aligned} M_1 &\mapsto (a_{11}, a_{12}, a_{13}, \dots, a_{1n}, \dots); \\ M_2 &\mapsto (a_{21}, a_{22}, a_{23}, \dots, a_{2n}, \dots); \\ M_3 &\mapsto (a_{31}, a_{32}, a_{33}, \dots, a_{3n}, \dots); \\ &\dots\dots\dots \\ M_i &\mapsto (a_{i1}, a_{i2}, a_{i3}, \dots, a_{in}, \dots); \\ &\dots\dots\dots \end{aligned}$$

Символ a_{ij} — это число 0 или 1. Например, пустому множеству будет соответствовать последовательность нулей, а всему множеству Z_0 — последовательность единиц.

Теперь укажем перечисляющий алгоритм для нового множества M . Если $a_{11} = 0$, то число 1 включим в M , а если $a_{11} = 1$, то не включим. Далее, по аналогии, если $a_{22} = 0$, то число 2 включим в M , а если $a_{22} = 1$, то нет. Точно так же с числами 3, 4, 5 и т. д. В общем случае

$$i \in M \Leftrightarrow a_{ii} = 0$$

или, что то же самое,

$$i \in M \Leftrightarrow i \notin M_i.$$

Последнее означает, что для каждого i выполняется неравенство $M \neq M_i$.

Алгоритм перечисления элементов множества M указан. Поскольку M не совпадает ни с одним из множеств M_i , множество M не задается эффективно.

Это означает, что (по крайней мере теоретически) существует вычислительное устройство, которое последовательно, одно за другим выдает числа, принадлежащие множеству M , но никогда (ни теоретически, ни практически) не будет создана машина и не будет написана программа, позволяющие узнавать, принадлежит произвольное натуральное число n множеству M или нет.

2.6. Алгебры

Алгеброй называют множество с операциями.

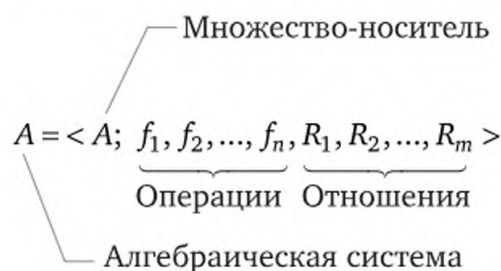
Часто множество A и алгебру, определенную на A , обозначают одним и тем же символом. Если f_1, f_2, \dots, f_n — набор операций (различных местностей) на множестве A , то алгебру A обычно записывают в виде

$$A = \langle A; f_1, f_2, \dots, f_n \rangle.$$

Кроме операций, на A могут быть определены и отношения (тоже различных местностей) R_1, R_2, \dots, R_m . Тогда

$$A = \langle A; f_1, f_2, \dots, f_n, R_1, R_2, \dots, R_m \rangle$$

является математической (или алгебраической) системой¹.



Основное понятие алгебры

Например, множество натуральных чисел с операциями сложения и умножения образует алгебру $\langle \mathbb{N}; +, \cdot \rangle$ натуральных чисел. Эта алгебра с отношениями порядка и делимости превращается в систему натуральных чисел $\langle \mathbb{N}; +, \cdot; \leq, | \rangle$. Именно эту систему часто называют арифметикой.

Объектами изучения алгебры (науки) являются алгебры (множества с операциями). Фраза «Алгебре — алгебры» построена аналогично лозунгам: «Миру — мир» или «Война — войне».

¹ От греч. *συστήμα* — «состоящее из частей».

Символы операций и отношений алгебраической системы называют сигнатурой, а их местности — типом системы. Например, сигнатура алгебраической системы $\langle N; +, \cdot; \leq, | \rangle$ — это $\{+, \cdot; \leq, |\}$, а ее типом является $(2, 2; 2, 2)$.

Операции — это частные случаи отношений. Поэтому и алгебры, и алгебраические системы являются частными случаями моделей.

Некоторые различные с виду математические системы по существу одинаковы. Что значит — «по существу»?

Из-за разных обстоятельств и элементы, и операции, и отношения математической системы могут иметь различные названия и обозначения. Например, систему натуральных чисел с операцией сложения $\langle N; + \rangle$ можно записать традиционно:

$$N_1 = \langle \{1, 2, 3, \dots\}; + \rangle,$$

а можно воспользоваться обозначениями древней Римской республики:

$$N_2 = \langle \{I, II, III, IV, V, VI, \dots\}; \textit{summa} \rangle.$$

И первая, и вторая математические системы являются системами натуральных чисел — это просто два описания на различных языках одного и того же объекта. Словарь для перевода с одного языка на другой — это взаимно однозначное соответствие f между элементами множеств N_1 и N_2 :

$$f(1) = I, f(2) = II, f(3) = III, f(4) = IV, f(5) = V, f(6) = VI, f(7) = VII, \dots$$

Это соответствие согласовано с операцией сложения следующим образом. Если элемент x переходит в $f(x)$, а элемент y — в $f(y)$, то сумма $x + y$ переходит в сумму соответствующих элементов во второй системе, т. е. $x + y$ переходит в элемент, обозначаемый символом $\langle f(x) \textit{summa} f(y) \rangle$. Иначе говоря, для всех элементов x, y из первой системы выполняется тождество:

$$f(x + y) = f(x) \textit{summa} f(y).$$

Все свойства натуральных чисел не зависят от языка и применяемых обозначений: любое утверждение, записанное на одном языке, автоматически становится верным и на любом другом языке.

Две модели N_1 и N_2 — это два изображения одного и того же объекта. Они имеют одну и ту же форму, в математике говорят: изоморфны.

Определим изоморфизм и более общее понятие гомоморфизма точно.

Пусть $A_1 = \langle A_1; \circ \rangle$ и $A_2 = \langle A_2; \circ \rangle$ — две алгебры с одной двухместной операцией \circ , а φ — отображение множества A_1 на A_2 .

Отображение φ сохраняет операцию, если для любых элементов x, y из множества A_1

$$\varphi(x \circ y) = \varphi(x) \circ \varphi(y).$$

Аналогично определяется сохранение операций меньших и больших местностей. Например, если g — одноместная операция в алгебрах A_1 и A_2 , то сохранение операции и отображение φ означает, что для любых x из A_1

$$\varphi(g(x)) = g(\varphi(x)).$$

Если g — это n -одноместная операция в алгебрах A_1 и A_2 , то отображение φ сохраняет g — это значит, что для любых x_1, x_2, \dots, x_n из A_1

$$\varphi(g(x_1, x_2, \dots, x_n)) = g(\varphi(x_1), \varphi(x_2), \dots, \varphi(x_n)).$$

Отображение, сохраняющее все операции алгебры, называют гомоморфизмом.

Пусть $M_1 = \langle M_1; R \rangle$ и $M_2 = \langle M_2; R \rangle$ — две модели с одним двухместным отношением R , а φ — отображение множества M_1 на M_2 . Отображение φ является гомоморфизмом моделей, если φ сохраняет отношение (для любых элементов x, y из M_1): из истинности предложения xRy следует истинность $\varphi(x)R\varphi(y)$,

$$xRy \Rightarrow \varphi(x)R\varphi(y).$$

В случае изоморфизма моделей для сохранения отношения требуется более жесткое правило (для любых элементов x, y из M_1):

$$xRy \Leftrightarrow \varphi(x)R\varphi(y).$$

Аналогично определяется сохранение отношений других местностей.

Гомоморфизм — частный случай отображения, поэтому он может быть инъективным, сюръективным или биективным. Множества A_1 и A_2 могут совпадать, и тогда получатся гомоморфизмы в себя. Соответствующие названия были приведены еще во введении в сводной таблице. Взаимно однозначное отображение одного множества в другое называется инъекцией, отображение на все множество — сюръекцией, а отображение, являющееся одновременно инъекцией и сюръекцией, принято называть биекцией. Таблица морфизмов принимает следующий вид.

Вид морфизма	Свойства отображения	Вид отображения
Гомоморфизм	Отображение, сохраняющее операции	Произвольное отображение одного множества в другое

Вид морфизма	Свойства отображения	Вид отображения
Мономорфизм	Взаимно однозначный гомоморфизм в	Инъекция
Эпиморфизм	Гомоморфизм на	Сюръекция
Изоморфизм	Мономорфизм и эпиморфизм одновременно	Биекция
Эндоморфизм	Гомоморфизм в себя	Отображение в себя
Аutomорфизм	Изоморфизм на себя	Биекция на себя (подстановка)

Свойство алгебр или алгебраических систем называют *абстрактным*, если оно сохраняется при изоморфизме. Точнее говоря, свойство абстрактно, если из того, что им обладает некоторая алгебраическая система, следует, что этим свойством обладают и все системы, с ней *изоморфные*.

Отметим несколько простейших свойств изоморфизмов и гомоморфизмов.

Отношение изоморфности является отношением эквивалентности на множестве алгебраических систем. Произведение гомоморфизмов алгебраических систем является гомоморфизмом, а произведение изоморфизмов алгебраических систем является изоморфизмом.

При сохранении операций имеют в виду главные операции алгебры, занесенные в сигнатуру. Некоторые операции алгебры могут определяться в аксиомах (как, например, нульместная операция «нейтральный элемент» или одноместная — «взятие обратного элемента»).

Неглавные операции алгебры тоже сохраняются при гомоморфизме *на*, т. е. эпиморфизм переводит нейтральный элемент в нейтральный, поглощающий — в поглощающий, обратный — в обратный, противоположный — в противоположный.

Рассмотрим несколько примеров изоморфных алгебр и алгебраических систем.

Начнем с моделей, т. е. множеств с отношениями.

Пусть M_1 — множество натуральных делителей числа 6 с отношением делимости, а M_2 — множество подмножеств двухэлементного множества $\{a, b\}$ с отношением включения. Модели $M_1 = \langle \{1, 2, 3, 6\}; | \rangle$ и $M_2 = \langle P\{a, b\}; \subset \rangle$ изоморфны. Этот изоморфизм можно проверить непосредственно по определению изоморфизма, но можно увидеть наглядно из графов этих отношений.

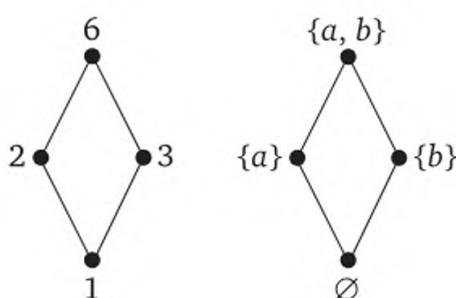
Две системы: $\langle \mathbf{R}; + \rangle$ — система всех действительных чисел с операцией сложения и $\langle \mathbf{R}_+; \cdot \rangle$ — система положительных действи-

тельных чисел с операцией умножения – тоже *изоморфны*. Отображение $f: \mathbf{R}_+ \rightarrow \mathbf{R}$, заданное правилом

$$f(x) = \log_a x, \text{ где } a > 0 \text{ и } a \neq 1,$$

взаимно однозначно и сохраняет операцию

$$\log_a (x \cdot y) = \log_a x + \log_a y.$$



Изоморфные модели

Этот изоморфизм означает, что сложение действительных чисел и умножение положительных чисел обладают совершенно одинаковыми свойствами.

Законы де Моргана для теоретико-множественных операций

$$\overline{A \cap B} = \overline{A} \cup \overline{B},$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B},$$

и связь между отношением включения и операцией дополнения

$$A \subset B \Leftrightarrow \overline{B} \subset \overline{A}$$

означают, что для произвольного множества M алгебраические системы

$$\langle P(M); \cap; \subset \rangle \text{ и } \langle P(M); \cup; \supset \rangle$$

изоморфны.

Рассмотрим пример изоморфизма из математической логики. Введем на множестве AB классов равносильных формул алгебры высказываний отношение логической посылки \Leftarrow по правилу: формула F — логическая посылка формулы G тогда и только тогда, когда G — логическое следствие формулы F .

Тогда из законов де Моргана

$$\overline{A \& B} = \overline{A} \vee \overline{B},$$

$$\overline{A \vee B} = \overline{A} \& \overline{B}$$

и закона контрапозиции

$$A \rightarrow B \Leftrightarrow \bar{B} \rightarrow \bar{A}$$

следует, что отображение, переводящее каждую формулу алгебры высказываний в ее отрицание, является изоморфизмом между алгебраическими системами высказываний:

$$AB = \langle AB; \&; \Rightarrow \rangle \text{ и } AB = \langle AB; \vee; \Leftarrow \rangle.$$

В связи с понятием изоморфизма отдельно обсудим свойства отношения порядка. Примером частично упорядоченного множества является множество $P(M)$ подмножеств множества M с отношением \subset включения.

Этот пример носит *фундаментальный* характер. Фундаментальность его заключается в том, что *любой порядок* является с точностью до обозначений порядком на некотором подмножестве множеств $P(M)$.

Пусть $\langle M; < \rangle$ — частично упорядоченное множество. Множество

$$[x] = \{y \in M \mid y < x\}$$

является элементом $P(M)$. Отображение, переводящее каждый элемент x из M в $[x]$, является взаимно однозначным отображением, переводящим множество M в множество $P(M)$, причем для каждого элемента x, y из M

$$x < y \Leftrightarrow [x] \subset [y].$$

Это означает, что отображение сохраняет отношение, и, таким образом, *любое упорядоченное множество изоморфно некоторому множеству подмножеств с отношением включения*.

Свойства, сохраняющиеся при изоморфизме, принято называть *абстрактными*. Точнее говоря, свойство P абстрактное, если из того, что свойством P обладает некоторая математическая система A_1 , этим свойством обладает и любая система A_2 , изоморфная системе A_1 .

Рассмотрим связь между изоморфизмами и гомоморфизмами.

В алгебре нет отношений, поэтому взаимно однозначный гомоморфизм алгебр является изоморфизмом.

Для алгебраических систем это не так. Например, отображение $\varphi: x \mapsto x$ системы $A = \langle \mathbb{N}; +; | \rangle$ в систему $B = \langle \mathbb{N}; +; \leq \rangle$ является гомоморфизмом. Это отображение сохраняет операцию сложения (и любую другую операцию любой местности, так как все элементы остаются неподвижными). Отношение \leq является продолжением отношения $|$, поэтому

$$x | y \Rightarrow x \leq y.$$

Это значит, что отображение φ удовлетворяет условию гомоморфизма для отношений (для любых натуральных x, y):

$$x \mid y \Rightarrow \varphi(x) \leq \varphi(y).$$

Однако несмотря на взаимную однозначность отображения φ , системы A и B не изоморфны (B упорядочена линейно, а в системе A порядок лишь частичный).

Таким образом, не каждый взаимно однозначный гомоморфизм алгебраической системы является изоморфизмом.

Для конечных систем и эндоморфизмов ситуация иная.

Каждый взаимно однозначный эндоморфизм конечной системы является автоморфизмом.

Действительно, если R — n -местное отношение на множестве M , а φ — взаимно однозначное гомоморфное отображение M на себя, то по определению

$$R(x_1, x_2, \dots, x_n) \Rightarrow R(\varphi(x_1), \varphi(x_2), \dots, \varphi(x_n)).$$

Обозначим символом φ^n степень (последовательное выполнение гомоморфизма φ). Поскольку произведение гомоморфизмов само является гомоморфизмом, для любого натурального $n > 1$ имеем:

$$R(\varphi(x_1), \varphi(x_2), \dots, \varphi(x_n)) \Rightarrow R(\varphi^n(x_1), \varphi^n(x_2), \dots, \varphi^n(x_n)).$$

Поскольку φ — подстановка конечного множества, некоторая ее k -я степень равна тождественной подстановке, т. е. $(\varphi^k(x_1), \varphi^k(x_2), \dots, \varphi^k(x_n))$ — это то же самое, что и $R(x_1, x_2, \dots, x_n)$:

$$R(\varphi(x_1), \varphi(x_2), \dots, \varphi(x_n)) \Rightarrow R(x_1, x_2, \dots, x_n).$$

Эквивалентность \sim называется согласованной с n -местной операцией f , если для каждой $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$

$$a_1 \sim b_1, a_2 \sim b_2, \dots, a_n \sim b_n \Rightarrow f(a_1, a_2, \dots, a_n) \sim f(b_1, b_2, \dots, b_n).$$

Эквивалентность \sim согласована с n -местным отношением S , если для каждой $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ из $a_1 \sim b_1, a_2 \sim b_2, \dots, a_n \sim b_n$ следует равносильность:

$$S(a_1, a_2, \dots, a_n) \Leftrightarrow S(b_1, b_2, \dots, b_n).$$

Эквивалентность, согласованная со всеми операциями и отношениями алгебраической системы, называется конгруэнцией.

Рассмотрим несколько важных примеров конгруэнций.

Отношение \sim на множестве дробей, заданное правилом

$$\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c,$$

согласовано с операциями сложения и умножения.

Отношение логической равносильности высказываний согласовано с логическими операциями и отношением «логическое следствие».

Изучение гомоморфизма, т. е. некоторой внешней связи изучаемой системы с однотипными системами, можно производить, оставаясь в самой изучаемой системе.

Гомоморфизм алгебраической системы задает отношение конгруэнции на множестве — носителе этой системы.

Конгруэнция на алгебраической системе определяет гомоморфизм этой системы.

Таким образом, с каждой алгебраической системой связано множество конгруэнций этой системы. Однако в математике интерес представляет обычно не множество само по себе, а множество с операциями.

Дополнение конгруэнции никогда не является конгруэнцией. Объединение конгруэнций может не оказаться конгруэнцией. Однако пересечение конгруэнций алгебраической системы A снова является конгруэнцией на A .

Пусть A — алгебра, f — одна из ее операций, а H — непустое подмножество множества A . Подмножество H замкнуто относительно f , если для любых элементов a_1, a_2, \dots, a_n из H элемент $f(a_1, a_2, \dots, a_n)$ снова принадлежит H .

Например, если \circ — двухместная операция в алгебре, то замкнутость H относительно этой операции означает, что

$$a \in H, b \in H \Rightarrow a \circ b \in H.$$

Если H является алгеброй того же типа и удовлетворяет тем же аксиомам, что и алгебра A , то H называют *подалгеброй* алгебры A . Часто для того чтобы подчеркнуть, что H — не просто подмножество множества A ($H \subset A$), но и подалгебра, используют символику $H < A$, где знак $<$, похожий на строгое числовое неравенство, используется так же, как и знак \subset , т. е. не обязательно в строгом смысле (H может и совпадать с A).

Множество подалгебр упорядочено отношением включения. Наибольшим элементом в таком порядке является множество — носитель самой алгебры. Наименьшего элемента, т. е. подалгебры, содержащейся в каждой подалгебре, может и не существовать.

Отношение «быть подалгеброй» является отношением частичного порядка.

В любой алгебре пересечение любой совокупности подалгебр или пусто, или является подалгеброй.

Объединение возрастающей цепочки подалгебр

$$A_1 < A_2 < \dots < A_n < \dots$$

алгебры A является подалгеброй.

Дело в том, что в операции алгебры участвует конечное число элементов, поэтому все они находятся в некотором звене этой цепи, а значит, и результат операции, примененной к этим элементам, лежит там же.

Пусть M — непустое подмножество алгебры A . Рассмотрим пересечение всех подалгебр алгебры A , содержащих множество M . Пересечение всех подалгебр алгебры A , содержащих множество M , является наименьшей подалгеброй, содержащей M .

Наименьшая подалгебра, содержащая M , называется *подалгеброй, порожденной множеством M* . Эту алгебру обозначают в разных ситуациях символом $gr(M)$, или $alg(M)$, или просто (M) — буквы «алг» в конкретных случаях заменяются сокращенными названиями изучаемых алгебр.

Случайно этой подалгеброй может оказаться вся алгебра A .

Если у алгебры найдется конечное порождающее множество, то алгебру называют *конечно порожденной*.

Если алгебра A конечно порождена, то каждая возрастающая цепочка подалгебр

$$A_1 < A_2 < \dots < A_n < \dots$$

алгебры A обрывается на конечном шаге.

Для некоторого класса алгебр возникает естественная проблема: как узнать для произвольного набора элементов a, a_2, \dots, a_m и произвольного элемента b , принадлежит элемент b подалгебре $gr(M)$ или нет.

В случае, когда существует алгоритм для решения такой задачи, говорят, что *проблема вхождения* в классе этих алгебр *алгоритмически разрешима*.

Чтобы получить порождающее множество объединения двух подалгебр, достаточно объединить порождающие множества подалгебр.

С пересечением ситуация сложнее. Во-первых, пересечение конечно порожденных подалгебр может оказаться не конечно порожденным. Во-вторых, даже если свойство конечной порожденности и сохраняется для пересечения, может оказаться, что не существует алгоритма для нахождения порождающих элементов пересечения для произвольных двух конечных наборов элементов из алгебр рассматриваемого класса.

Если же все пересечения конечно порожденных подалгебр сами конечно порождены и существует алгоритм для нахождения порождающих пересечений, то скажем, что в алгебре *алгоритмически разрешима проблема пересечения*.

Рассмотрим два примера подалгебр.

Пусть H — подалгебра алгебры целых чисел \mathbb{Z} с операциями сложения и вычитания и H состоит не из одного нуля. Взяв наименьший по модулю элемент d из H , с помощью теоремы о делении с остатком получаем, что *любая подалгебра алгебры $\langle \mathbb{Z}; +, - \rangle$ целых чисел с операциями сложения и вычитания состоит из целых чисел, кратных некоторому целому числу d* .

Предыдущее утверждение означает, что все подалгебры алгебры $\langle \mathbb{Z}; +, - \rangle$ являются *однопорожденными*.

Проблема вхождения для этой алгебры сводится к алгоритму деления, а проблема пересечения — это задача нахождения наименьшего общего кратного двух чисел.

Для целых неотрицательных чисел с той же операцией ситуация сложнее. Оказывается, все элементы, кроме конечного числа, из подалгебры алгебры $\langle \mathbb{Z}_0; + \rangle$ кратны некоторому целому числу d .

Доказательство этого утверждения будет опираться на свойства множества решений неопределенного линейного уравнения. Эти свойства, среди прочего, будут обсуждаться в следующих темах.

Контрольные задания

1. Докажите, что условия минимальности, индуктивности и обрыва убывающих цепей равносильны.
2. Докажите, что эквивалентность на множестве разбивает это множество на смежные классы, и, наоборот, разбиение множества на классы определяет эквивалентность на этом множестве.
3. Докажите, что предпорядок на множестве после факторизации по ассоциированности, заданной предпорядком, становится порядком.
4. Докажите, что отношение равномощности в классе множеств является эквивалентностью.
5. Докажите, что отношение включения в классе множеств является порядком.
6. Докажите, что мощности множеств можно линейно упорядочить.
7. Докажите, что множества точек отрезка и множество точек трехмерного пространства равномощны.
8. Докажите, что существуют несчетные множества.
9. Докажите, что мощности множеств не ограничены.
10. Докажите, что множества мощностей не существует.

Тема 3

ЦЕЛЫЕ ЧИСЛА И КОЛЬЦА

КЛАССОВ ВЫЧЕТОВ

Основные понятия: предпорядок, ассоциированность, сравнимость по модулю, конгруэнция, мультипликативная группа кольца, полная и приведенная системы вычетов, функция Эйлера, мультипликативное свойство целочисленной функции, линейное сравнение, цепная дробь, подходящая цепная дробь, смешанная и периодическая десятичная дробь, длина периода, порядок числа по модулю, неопределенные уравнения.

Основные факты: отношение сравнимости является конгруэнцией; функция Эйлера мультипликативна; решение неопределенного уравнения в кольце целых чисел можно свести к решению уравнения в кольце классов вычетов; вычисление остатков от деления и проверка арифметических действий сводится к вычислениям в гомоморфных образах; вычисление длины периода систематической дроби сводится к отысканию порядка элемента в мультипликативной группе кольца классов вычетов.

Обсудим свойства конкретного объекта — кольца целых чисел. Методология исследования такова, что конкретные идеи и способы решения задач, связанных с делимостью целых чисел, легко можно перенести на целые классы других, уже абстрактных колец.

3.1. Отношение делимости

Отношение делимости можно определить в любом целостном кольце K (том числе и в кольце \mathbb{Z} целых чисел) следующим правилом: элемент x делит элемент y , если в K существует такой z , что $xz = y$. Отношение делимости обычно обозначают символом $|$:

$$x \overset{\text{опр}}{|} y \Leftrightarrow (\exists z \in K) [xz = y].$$

Отношение делимости на множестве целых чисел является отношением предпорядка.

Определим на множестве \mathbb{Z} отношение ассоциированности \sim по правилу

$$a \overset{\text{опр}}{\sim} b \Leftrightarrow a | b \text{ и } b | a.$$

Отношение ассоциированности рефлексивно, транзитивно и симметрично, т. е. является эквивалентностью.

Как всякая эквивалентность, ассоциированность разбивает множество \mathbf{Z} на смежные классы. Число нуль образует один класс (нуль делится только сам на себя), а остальные классы содержат два элемента: a , $-a$, т. е. фактор-множество \mathbf{Z}/\sim имеет вид

$$\mathbf{Z}/\sim = \{\{0\}, \{1, -1\}, \{2, -2\}, \dots, \{a, -a\}, \dots\}.$$

Ассоциированность согласована с отношением делимости, а множество \mathbf{Z}/\sim частично упорядочено отношением делимости.

Неотрицательные целые числа \mathbf{Z}_0 обычно выбираются в качестве множества представителей классов ассоциированных элементов.

Граф отношения делимости на множестве \mathbf{Z}_0 имеет *наивысшую* точку (это число нуль — наибольший в смысле делимости элемент). Внизу графа находится единица — *наименьший* элемент в этом порядке.

Напомним, что множество \mathbf{Z}_0 вполне упорядочено отношением \leq , т. е. свойства элементов \mathbf{Z}_0 мы можем доказывать с помощью метода математической индукции.

Множество целых чисел уже не является вполне упорядоченным, и для всего \mathbf{Z} метод индукции непосредственно не пройдет.

Для элементов x из множества \mathbf{Z} , как правило, придется применять и *метод полной индукции*, рассматривая отдельно случаи $x = 0$, $x > 0$, $x < 0$.

Именно таким методом математической индукции (для неотрицательных чисел — индукцией по числу a) можно установить, что для кольца целых чисел выполняется *теорема о делении с остатком*.

Если a, b — целые числа, причем b не равно нулю, то существуют единственные целые неотрицательные числа q, r такие, что

$$a = b \cdot q + r \text{ и } 0 \leq r < |b|.$$

Доказательство. Рассмотрим случай, когда a, b — целые неотрицательные числа.

Докажем сначала существование частного и остатка индукцией по a .

База индукции: $a = 0$. Тогда утверждение теоремы верно: $0 = 0 \cdot b + 0$.

Шаг индукции: если теорема о делении с остатком верна для чисел a и b , то она будет верна и для чисел $a + 1$ и b .

По индуктивному предположению

$$a = b \cdot q + r, \tag{*}$$

где $0 \leq r < b$. Прибавим к левой и правой частям равенства (*) по единице и получим:

$$a+1=b \cdot q+r+1.$$

По индуктивному предположению имеем $r < b$. Порядок на множестве целых неотрицательных чисел *дискретен*, поэтому

$$r < b \Rightarrow r+1 \leq b.$$

Таким образом, могут встретиться два случая.

Случай первый: $r+1=b$. Тогда

$$a+1=b \cdot q+r+1=b \cdot q+b=b \cdot (q+1)+0—$$

представление вида (*).

Случай второй: $r+1 < b$. Тогда

$$a+1=b \cdot q+(r+1)—$$

требуемое представление. Шаг индукции и существование частного и остатка доказаны.

Если $a > 0$, но $b < 0$, то $-b > 0$ и $a = (-b)q + r$, где $0 \leq r < -b$. Тогда

$$a=b(-q)+r.$$

Если $a < 0$, то $-a = bq + r$, где $0 \leq r < |b|$. Отсюда:

$$a=b(-q)-r=bq_1+(|b|-r).$$

Снова $0 \leq |b| - r < |b|$, и существование частного и остатка доказано для любого целого a .

Докажем теперь *единственность* частного и остатка.

Предположим, что $a = b \cdot q + r$ и одновременно $a = b \cdot q_1 + r_1$. Тогда

$$b \cdot q + r = b \cdot q_1 + r_1,$$

откуда $b|(r-r_1)$. Из неравенства $|r-r_1| < |b|$ следует $r-r_1=0$. Поскольку \mathbb{Z} целостное (т. е. там выполняется закон сокращения), из равенства остатков следует равенство частных.

Теорема о делении с остатком означает, что при делении любого целого числа на натуральное число m могут появиться в точности m остатков: $0, 1, \dots, m-1$.

Пусть a, b — целые неотрицательные числа, $b > 0$, q — частное, а r — остаток при делении a на b . Равенство $a = b \cdot q + r$, где $0 \leq r$, означает, что $b \cdot q \leq a$. Из неравенства $r < b$ следует:

$$b \cdot q + r < b \cdot q + b,$$

откуда

$$a < b \cdot q + b.$$

Таким образом,

$$q \cdot b \leq a < (q+1) \cdot b.$$

Разделим все части на положительное число b (знаки неравенства от этого не изменятся):

$$q \leq \frac{a}{b} < q+1.$$

Это неравенство означает, что неполное частное q — это в точности *целая часть* числа $\frac{a}{b}$.

Деление *нацело* означает *отсутствие дробной части* при делении, т. е. отсутствие числа $\frac{r}{b}$. Целую часть действительного числа x принято обозначать символом $[x]$.

Дробная часть обозначается символом $\{x\}$, т. е. $\{x\} = x - [x]$.

Остаток от деления a на b принято обозначать символом $\text{Rest}(a, b)$ ¹.

Пусть g — натуральное число больше единицы. Для любого целого положительного числа a по теореме о делении с остатком имеем: $a = g \cdot q_1 + a_0$, где $0 \leq a_0 < g$. Теперь разделим q_1 на g :

$$q_1 = g \cdot q_2 + a_1, \quad 0 \leq a_1 < g.$$

Затем разделим q_2 на g : $q_2 = g \cdot q_3 + a_2$, и так далее до тех пор, пока не получим частное, равное нулю. Это значит, что мы произведем n раз деление на g :

$$q_{n-1} = g \cdot q_n + a_{n-1},$$

где $q_{n-1} \neq 0$, а на следующем $n+1$ шаге все заканчивается: $q_n = g \cdot 0 + a_n$.

Соберем все вместе, т. е. в первое равенство подставим значение q_1 из второго, затем заменим q_2 из третьего равенства и т. д., наконец, вместо q_n подставим a_n . Процесс и *результат сборки* выглядят так:

$$\begin{aligned} a &= gq_1 + a_0 = g(gq_2 + a_1) + a_0 = g(g(gq_3 + a_2) + a_1) + a_0 = \dots \\ &= \underbrace{g(g(\dots(g(a_n + a_{n-1}) + a_{n-2}) + a_{n-3}) + \dots + a_2) + a_1}_{n} + a_0. \end{aligned}$$

¹ Rest (нем.) — «остаток».

Теперь раскроем скобки и получим представление числа a в виде суммы степеней g с коэффициентами, причем значения коэффициентов — это целые неотрицательные числа из множества $\{0, 1, 2, \dots, g-1\}$:

$$a = a_n \cdot g^n + a_{n-1} \cdot g^{n-1} + a_{n-2} \cdot g^{n-2} \dots + a_2 \cdot g^2 + a_1 \cdot g + a_0.$$

Такое представление числа называют *систематической записью* в g -ичной системе счисления. Если число g равно 10, то система, соответственно, называется *десятичной*, а если, например, двум, то *двоичной*. Скобки в записи сумм и произведений можно не писать благодаря ассоциативным законам для сложения и умножения.

Таким образом, для записи любого целого неотрицательного числа достаточно g символов, обозначающих числа $0, 1, \dots, g-1$. Такая система записи называется *позиционной системой счисления с основанием g* .

Заметим, что предыдущее рассуждение о возможности систематического представления каждого целого неотрицательного числа является *доказательством существования* этого представления. Доказательство проведено *методом математической индукции* в форме условия обрыва убывающих цепей. Действительно, цепочка $a > a_0 > a_1 > \dots$ строго убывает и поэтому состоит из конечного числа элементов, так что наша сборка действительно возможна.

Покажем, что если $a_0 \neq 0$, то представление числа a в систематическом виде *единственно*. Доказательство проведем снова по индукции, но используя равносильное условию индуктивности условие *минимальности*.

Итак, пусть существует целое неотрицательное число a , обладающее двумя представлениями:

$$\begin{aligned} a &= a_n \cdot g^n + a_{n-1} \cdot g^{n-1} + a_{n-2} \cdot g^{n-2} + \dots + a_2 \cdot g^2 + a_1 \cdot g + a_0 = \\ &= b_m \cdot g^m + b_{m-1} \cdot g^{m-1} + b_{m-2} \cdot g^{m-2} + \dots + b_2 \cdot g^2 + b_1 \cdot g + b_0. \end{aligned}$$

По условию минимальности должно существовать наименьшее число с таким свойством. Будем считать, что a — это как раз и есть наименьшее число.

В каждом из представлений вынесем и сгруппируем слагаемые, имеющие множитель g , и вынесем этот множитель за скобку. Получим:

$$\begin{aligned} a &= (a_n \cdot g^{n-1} + a_{n-1} \cdot g^{n-2} + \dots + a_2 \cdot g + a_1) \cdot g + a_0 = \\ &= (b_m \cdot g^{m-1} + b_{m-1} \cdot g^{m-2} + \dots + b_2 \cdot g + b_1) \cdot g + b_0. \end{aligned}$$

Из того, что $0 \leq a_0 < g$ и $0 \leq b_0 < g$, следует, что числа a_0 и b_0 являются остатками от деления a на g :

$$a_0 = \text{Rest}(a, g), \quad b_0 = \text{Rest}(a, g),$$

следовательно, $a_0 = b_0$. По теореме о делении с остатком совпадают не только остатки, но и частные:

$$\begin{aligned} q &= a_n \cdot g^{n-1} + a_{n-1} \cdot g^{n-2} + \dots + a_2 \cdot g + a_1 = \\ &= b_m \cdot g^{m-1} + b_{m-1} \cdot g^{m-2} + \dots + b_2 \cdot g + b_1. \end{aligned}$$

Число q строго меньше a , поэтому q не принадлежит множеству чисел, обладающих двумя систематическими представлениями. Это значит, что представление q единственно, т. е. $n = m$ и

$$a_n = b_m, a_{n-1} = b_{m-1}, \dots, a_2 = b_2, a_1 = b_1.$$

Однако вместе с равенством $a_0 = b_0$ получаем, что число a , вопреки предположению, тоже обладает единственным представлением. Единственность систематического представления доказана.

В систематической записи числа знаки сложения (+) и показатели степеней у числа g можно опустить, записав лишь цифры:

$$a_n, a_{n-1}, a_{n-2}, \dots, a_2, a_1, a_0$$

(плюсы и показатели степеней легко восстанавливаются по тому месту (*позиции*), которое занимает цифра). Тогда запись числа a примет вид

$$a = \overline{a_n a_{n-1} \dots a_2 a_1 a_0}_g.$$

Черта наверху стоит для того, чтобы не спутать эту запись с записью произведения чисел

$$a_n, a_{n-1}, a_{n-2}, \dots, a_2, a_1, a_0,$$

а индекс g напоминает, что все это происходит в g -ичной системе счисления.

Если есть договор о значении g , которое не изменяется в ходе решения задач, то индекс g не пишется, а если к тому же нет и опасности принять это выражение за произведение $a_n \cdot a_{n-1} \cdot \dots \cdot a_2 \cdot a_1 \cdot a_0$, то черта вверху не проводится.

Поскольку в записи числа при таком подходе участвуют операции сложения и умножения, систему принято называть *аддитивно-мультипликативной системой счисления*¹.

¹ На пороге открытия аддитивно-мультипликативной позиционной десятичной системы счисления стоял уже Архимед, его сочинение «Исчисление песка» как раз посвящено задаче выражения сколь угодно больших чисел в системе счисления, близкой к десятичной. Позиционная система счисления, появившаяся лишь в VI—VII вв. н. э. (а в Европе — еще позже), является одним из величайших изобретений человечества; значение ее переоценить невозможно. Если бы Архимед не только начал, но и закончил построение позиционной системы, т. е. если бы позиционная система счисления появилась на тысячелетие раньше, то сейчас, вне сомнения, нас бы окружал совсем иной мир.

Каждое целое число обладает единственной систематической записью в аддитивно-мультипликативной системе счисления.

3.2. Идеалы в кольце целых чисел

Факт того, что отношение делимости является замаскированным отношением порядка, можно было легко обнаружить из следующих общих соображений.

Любое упорядоченное множество изоморфно некоторому множеству подмножеств с отношением включения. Изоморфизм этот устанавливается с помощью отображения элемента x в множество элементов (x) , не меньших (или не больших) элемента x .

Эту идею можно реализовать и в нашем конкретном случае.

Пусть a — элемент кольца Z . Рассмотрим множество $(a) = \{ak \mid k \in Z\}$ кратных этого элемента.

Множество (a) обладает следующими свойствами:

- 1) если $x, y \in (a)$, то $x - y \in (a)$;
- 2) если $x \in (a)$ и $z \in K$, то $xz \in (a)$.

Непустое подмножество целостного кольца, обладающее свойствами 1), 2), называют идеалом кольца. Множество кратных элемента образует идеал (который принято называть *главным идеалом*), а если в кольце K каждый идеал является множеством кратных некоторого элемента, то K называют *кольцом главных идеалов*.

Вернемся пока в кольцо целых чисел. Идеал (a) — главный идеал, порожденный элементом a .

Из определения делимости получаем (для любых целых чисел a, b):

$$a \mid b \Leftrightarrow (a) \supset (b).$$

Таким образом, отношение делимости в Z/\sim точно (т. е. изоморфно) моделируется отношением включения на множестве главных идеалов кольца Z .

В действительности, в Z нет неглавных идеалов. Если идеал I кольца Z состоит не из одного нуля, то возьмем наименьший по модулю элемент d из I и, используя теорему о делении с остатком, увидим, что $I = (d)$.

Кольцо целых чисел является кольцом главных идеалов.

Натуральные числа участвуют в определении кратного элемента. Но натуральные числа являются и элементами из Z , поэтому каждое подкольцо кольца целых чисел является идеалом.

Отметим еще, что если A, B — два идеала кольца Z , то их пересечение $A \cap B$ и сумма $A + B = \{a + b \mid a \in A, b \in B\}$ обладают идеальными свойствами: замкнуты относительно разности и умножения на любой элемент из Z .

Пересечение и сумма идеалов являются идеалами.

В кольце \mathbb{Z} все идеалы главные, поэтому как пересечение, так и сумма идеалов являются множествами кратных некоторых элементов, т. е. для каждого целых чисел a, b существуют такие целые числа x, y , что

$$(a) + (b) = (x) \text{ и } (a) \cap (b) = (y).$$

Числа x, y носят особые названия, и эти названия известны школьникам средних классов.

Число d называют *наибольшим общим делителем* целых чисел a, b и обозначают символом НОД (a, b) или просто (a, b) , если:

- 1) d является общим делителем a, b , т. е. $d|a$ и $d|b$;
- 2) среди общих делителей чисел a и b число d наибольшее в смысле делимости, т. е. если $c|a$ и $c|b$, то $c|d$.

Наибольший общий делитель определен только через отношение делимости, поэтому данное определение более естественно, чем школьное, в котором смешаны два порядка — линейное упорядочение \leq и отношение делимости $|$. За естественность, однако, приходится платить: вообще говоря, из определения не видно, почему для любых целых чисел должен существовать наибольший общий делитель. Поскольку сумма двух идеалов в кольце целых чисел является главным идеалом, любые два целых числа обладают наибольшим общим делителем. Каждый элемент из идеала $(a) + (b)$ имеет вид $ax + by$, где x, y — целые числа. Такое же представление будет иметь и порождающий элемент этого идеала, т. е. наибольший общий делитель чисел a, b . Это значит, что если d — наибольший общий делитель чисел a, b , то существуют такие целые числа u, v , что

$$au + bv = d.$$

Такое представление наибольшего общего делителя называют *линейным разложением*.

Итак, *наибольший общий делитель любых двух целых чисел всегда существует и обладает линейным разложением*.

Впрочем, слово «двух» здесь несущественно: сумма любого *конечного* числа идеалов снова является главным идеалом, поэтому для любого множества целых чисел существует наибольший общий делитель, который обладает линейным разложением.

Отметим, что и слово «конечное» в предыдущей фразе можно убрать, договорившись, что в сумме элементов, выбранных из идеалов-слагаемых, все слагаемые, кроме конечного числа, равны нулю (в таком случае говорят: «почти все равны нулю»). Утверждение о существовании наибольшего общего делителя верно для *любого* множества целых чисел.

Перейдем ко второму понятию для целых чисел, связанному уже с пересечением идеалов.

Точно так же, как и при определении наибольшего общего делителя, т. е. не смешивая различные отношения порядка, введем понятие *наименьшего общего кратного*.

Сначала напомним, что *обратным отношением* для делимости является отношение *кратности*, обозначаемое символом \vdots (читается: «делится на»): a делит b тогда и только тогда, когда b делится на a , или то же самое в символах:

$$a \mid b \Leftrightarrow b \vdots a.$$

Для взаимно обратных отношений «не меньше» (\geq) и «не больше» (\leq) обычно не возникает никаких недоразумений, когда свободно (не оговаривая, какой именно порядок имеется в виду) употребляют слова «наибольший» и «наименьший». Точно так же обстоит дело и с отношениями \mid и \vdots .

Заменим в определении наибольшего общего делителя символ \mid на \vdots , в результате чего получим определение *наименьшего общего кратного*.

Число m называют *наименьшим общим кратным* чисел a , b и обозначают символом НОК $[a, b]$ или просто $[a, b]$, если:

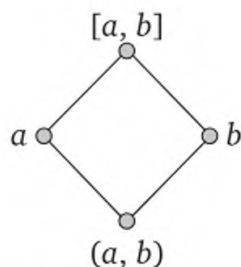
- 1) m является общим кратным a , b , т. е. $m \vdots a$ и $m \vdots b$;
- 2) среди общих делителей кратных a и b число m наименьшее в смысле делимости, т. е. если $c \vdots a$ и $c \vdots b$, то $c \vdots m$.

Снова заметим, что в школе наименьшее общее кратное определяется иначе. Новое определение снова опирается лишь на отношение делимости, и опять не видно, почему наименьшее общее кратное должно существовать для любых натуральных чисел.

Но после введения понятия идеала это уже не является проблемой. Поскольку пересечение двух идеалов в кольце целых чисел является главным идеалом, любые два целых числа обладают наименьшим общим кратным.

В пересечении может участвовать любое число идеалов, поэтому *любое множество целых чисел обладает наименьшим общим кратным*.

На графе отношения делимости на множестве \mathbb{Z}_0 наглядно представлены особые роли наибольшего общего делителя и наименьшего общего кратного любой пары элементов.



Точные грани в решетке делимости

Наименьшее общее кратное $[a, b]$ находится непосредственно над парой чисел a, b (ближе приблизиться одновременно к каждому числу пары нельзя — это и есть смысл слова «наименьший»); наибольший общий делитель (a, b) расположен непосредственно (ближе нельзя) под парой a, b .

Существование точных верхней и нижней граней означает, что система

$$\langle \mathbb{Z}; \text{НОД}, \text{НОК}; | \rangle$$

является решеткой.

Делимость определена с точностью до ассоциированности, поэтому в кольце целых чисел как НОД, так и НОК определены с точностью до знака: если $d = (a, b)$, $k = [a, b]$, то $\varepsilon d, \varepsilon k$, где $\varepsilon \in \{1, -1\}$, — тоже наибольший делитель и наименьшее общее кратное этих чисел.

Доказательство существования НОД и НОК, полученные в предыдущем пункте, являются косвенными, они не дают никаких указаний, как практически найти эти числа.

Существует, однако, и конструктивное доказательство этих фактов.

Покажем, что НОД (a, b) двух целых чисел a, b всегда существует, указав алгоритм для вычисления этого числа.

Можем считать, что эти числа не являются нулевыми одновременно. Правда, одно из них может быть и нулевым. Предположим, что так оно и есть: $a = 0$. Поскольку ноль делится на любое число, b тоже делит ноль и, следовательно, $(0, b) = b$.

Теперь покажем, что общий случай, когда оба числа отличны от нуля, сводится к этому, простейшему.

Процедура сведения к простейшему случаю основана на следующем наблюдении: если $a = bq + c$, где a, b, c, q — целые числа, то множества общих делителей чисел a, b и чисел b, c совпадают. В совпадающих множествах совпадают и их наибольшие элементы (в смысле любого упорядочения), т. е.

$$(a, b) = (b, c).$$

В качестве числа c в такой ситуации возьмем остаток от деления a на b . Как и раньше, обозначим символом $\text{Rest}(x, y)$ остаток от деления целого числа x на ненулевое число y . Тогда

$$(a, b) = (b, \text{Rest}(a, b)),$$

где $0 \leq \text{Rest}(a, b) < |b|$.

Взяв вместо исходной пары a и b новую, b и $\text{Rest}(a, b)$, можно снова выполнить деление, затем снова поменять пару и т. д. На каж-

дом таком шаге сохранится значение искомого наибольшего общего делителя:

$$\begin{aligned} r_1 &= \text{Rest}(a, b), \quad 0 \leq r_1 < |b|, \quad (a, b) = (b, r_1); \\ r_2 &= \text{Rest}(b, r_1), \quad 0 \leq r_2 < r_1, \quad (b, r_1) = (r_1, r_2); \\ r_3 &= \text{Rest}(r_1, r_2), \quad 0 \leq r_3 < r_2, \quad (r_1, r_2) = (r_2, r_3); \\ &\dots\dots\dots \\ r_{i+1} &= \text{Rest}(r_{i-1}, r_i), \quad 0 \leq r_{i+1} < r_i, \quad (r_{i-1}, r_i) = (r_i, r_{i+1}). \end{aligned}$$

Неравенства для остатков дают строго убывающую цепочку целых неотрицательных чисел:

$$|b| > r_1 > r_2 > r_3 > \dots > r_i > \dots,$$

а из аксиомы индукции следует, что *любая строго убывающая цепь целых неотрицательных чисел обрывается на конечном шаге*. Поэтому через конечное число шагов будет получен остаток, равный нулю.

Пусть $\text{Rest}(r_{k-1}, r_k) = 0$, тогда $(r_k, r_{k+1}) = (r_k, 0) = r_k$. Общий случай нахождения НОД свелся к случаю, когда одно из чисел равно нулю, *последний ненулевой остаток в этом процессе будет наибольшим делителем чисел a, b* .

В честь автора, впервые опубликовавшего этот алгоритм, описанную процедуру поиска НОД называют *алгоритмом Евклида*¹.

Существование (а заодно и вычисление) линейного разложения наибольшего общего делителя двух целых чисел также можно получить из алгоритма Евклида.

Каждое из равенств алгоритма Евклида можно записать в виде

$$r_i = au_i + bv_i,$$

где u_i, v_i — целые числа (которые можно найти с помощью неполных частных в алгоритме Евклида). Точно таким же представлением будет обладать и последний ненулевой остаток, т. е. НОД.

Итак, если $d = (a, b)$, то существуют такие целые числа u, v , что

$$au + bv = d,$$

причем числа u, v можно найти с помощью неполных частных алгоритма Евклида.

¹ Евклид, «Начала», книга VII. У Евклида описанный алгоритм относится к поиску *общей меры* отрезков a, b . Описанная процедура, которую можно производить с помощью циркуля и линейки, дает наибольший отрезок, укладывающийся целое число раз в отрезке a и в отрезке b .

Наименьшее общее кратное двух чисел мы можем найти теперь с помощью НОД:

$$[a, b] = \frac{ab}{(a, b)}.$$

Если наибольший общий делитель двух чисел равен единице, то они называются *взаимно простыми*. Из равенства $au + bv = 1$ следует $(a, b) = 1$, следовательно, два числа a, b взаимно просты тогда и только тогда, когда существуют такие целые числа u, v , что

$$au + bv = 1.$$

Наименьшее общее кратное взаимно простых чисел равно их произведению.

Наличие алгоритма для поиска наибольшего общего делителя позволяет сделать несколько следующих алгебраических замечаний.

Задача нахождения наименьшего общего кратного целых чисел алгоритмически разрешима.

Проблема вхождения для конечно порожденных подколец кольца целых чисел алгоритмически разрешима.

Проблема нахождения пересечения конечно порожденных подколец кольца целых чисел алгоритмически разрешима.

Целое число p , не принадлежащее множеству $\{0, 1, -1\}$, называют *простым*, если у него нет представлений в виде произведения целых чисел, кроме тривиальных:

$$p = a \cdot b \Rightarrow a \in \{1, -1\} \text{ или } b \in \{1, -1\}$$

Целое число, отличное от 1, -1 и нуля и не являющееся простым, называют *составным*.

Это определение означает, что множество целых чисел не делится на два класса — простые и составные. Кроме этих двух множеств, есть еще *третий* класс — $\{0, 1, -1\}$.

На графе отношения делимости на множестве целых неотрицательных чисел простые числа находятся непосредственно над единицей. Это значит, что во множестве $\mathbb{Z}_0 \setminus \{1\}$, упорядоченном отношением $|$, простые числа — это *минимальные элементы*.

Если натуральное число a — составное, $a = bc$, то из монотонности умножения следует, что $b < a$ и $c < a$.

Из транзитивности отношения делимости следует, что наименьший неединичный натуральный делитель любого числа является простым.

Испытывая на делимость все натуральные числа, меньшие данного натурального a , можно выяснить, просто число a или нет. Среди

таких испытаний будет много лишних, так как если $a = b \cdot c$ и $b > \sqrt{a}$, то $c < \sqrt{a}$. Следовательно, если число a составное, то у него есть неединичный натуральный делитель, не превосходящий \sqrt{a} . Таким образом, для выяснения простоты числа a достаточно попытаться разделить его на числа 2, 3, ... $[\sqrt{a}]$; если деление нацело ни разу не состоялось, то число a простое.

Наблюдение это опубликовано в 1202 г. Леонардо Пизанским¹ в трактате «Книга об абакке». Фибоначчи, правда, принадлежит лишь замечание об ускорении процесса вычислений при поиске простых чисел. Сама процедура поиска простых чисел в отрезке натурального ряда была известна к тому времени уже 1,5 тыс. лет.

Самый древний алгоритм поиска простых чисел в множестве $\{1, 2, 3, \dots, a\}$ называется *решетом Эратосфена*² и позволяет отсеивать составные числа из этого множества. Идея автора состоит в следующем. Зачеркнем сначала в отрезке $[1, a]$ единицу. Первое незачеркнутое число 2 простое. Оставим его незачеркнутым, но каждое второе зачеркнем (они непросты — делятся на 2). Число 3 — первое незачеркнутое — простое. Далее, оставив 3, зачеркнем каждое третье число. Первое незачеркнутое число снова просто. Продолжаем и далее таким же образом до тех пор, пока зачеркивать станет нечего. Оставшиеся незачеркнутыми числа будут простые. Благодаря наблюдению Фибоначчи этот процесс зачеркивания достаточно продолжить лишь до первого числа $\geq \sqrt{a}$.

Например, чтобы получить методом Эратосфена — Фибоначчи все простые числа, не превышающие число 30, достаточно из ряда 1, 2, 3, ..., 30 вычеркнуть все числа, кратные 2, 3, 5:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

Алгоритм Фибоначчи для проверки простоты числа a легко реализуется на вычислительной технике. В программу можно вставить увеличение значения a , и машина будет выдавать простые числа по порядку: 2, 3, 5, 7, 11, 13,

¹ Леонардо Пизанский, Фибоначчи (*Fibonacci*, 1180—1240) — итальянский математик. По его «Книге об абакке» многие поколения европейских математиков изучали индийскую позиционную систему счисления.

² Эратосфен Киренский (Ἐρατοσθένης, ок. 276—194 гг. до н. э.) — греческий ученый, друг Архимеда. Прославился тем, что первым измерил диаметр Земли. При практическом использовании своего метода поиска простых чисел Эратосфен применял технические средства своего времени — восковую дощечку и палочку для письма (стиль). Зачеркивание состояло в раздавливании соответствующего числа круглым концом стиля, поэтому в конце процесса восковая дощечка напоминала решето.

Проверку простоты чисел сравнительно небольшой разрядности машина производит мгновенно, поэтому сначала простые числа выдаются без задержек, одно за другим. Затем становятся заметны паузы между появлениями простых чисел, и чем дальше, тем паузы длиннее. Это означает, что интервалы, состоящие сплошь из составных чисел, увеличиваются. Это действительно так: существуют сколь угодно большие отрезки натурального ряда $[a, a + 1, \dots, a + m]$, состоящие только из составных чисел.

Простейшим примером такого отрезка будет интервал

$$[n! + 2, n! + 3, \dots, n! + n].$$

В то же время число $n! + 1$ не делится ни на одно число, меньшее или равное n , поэтому наименьший неединичный делитель числа $n! + 1$ является простым числом, большим n (случайно этот делитель может совпадать с самим числом $n! + 1$).

Это означает, что в интервале

$$[n + 1, n + 2, n + 3, \dots, n! + 1]$$

обязательно содержится хотя бы одно простое число. Поскольку число n здесь не ограничено, получаем результат, вошедший в историю¹ как *теорема Евклида о бесконечности множества простых чисел*.

Число $n! + 1$ слишком велико для поимки простого числа. Новое простое число можно разыскать, исходя из уже имеющихся простых чисел. Рассуждение Евклида из «Начал» следующее: если A , B , C — все простые числа, то наименьший простой делитель числа $A \cdot B \cdot C + 1$ является новым простым числом.

Евклидовская оценка

$$2 \cdot 3 \cdot 5 \cdot \dots \cdot p + 1$$

для поимки нового простого числа тоже слишком груба. На самом деле, как установил в 1852 г. русский математик П. Л. Чебышёв², начиная с числа a , большего трех, в множестве

$$\{a + 1, a + 2, a + 3, \dots, 2a - 2\}$$

всегда найдется хотя бы одно простое число. Как гипотеза это предложение вошло в историю под формулировкой «*Постулат Бертрана*»³.

¹ Считается, что доказательство теоремы о бесконечности множества простых чисел — это первое в истории цивилизации доказательство *методом от противного*.

² *Пафнутий Львович Чебышёв* (1821—1894) — русский математик и механик, основатель Петербургской математической школы.

³ *Жозеф Луи Франсуа Бертран* (*Bertrand*, 1822—1900) — французский математик, иностранный член-корреспондент (1859) и иностранный почетный член Петербургской АН, член Парижской академии наук (1856), профессор Коллеж де Франс (с 1862 г.).

Установлены также различного рода границы для n -го простого числа, и даже можно указать формулу для p_n .

Однако границы эти очень неточны (например, для каждого n выполняется неравенство $p_n \leq n^2+1$), и формулу n -го простого числа

$$p_n = \sum_{i=0}^{n^2+1} sg \left(n+1 - \sum_{j=2}^i \left([(j-1)!]^2 - j \cdot \text{INT} \left(\frac{[(j-1)!]^2}{j} \right) \right) \right),$$

где $\text{INT}(x)$ — целая часть числа x , применить практически весьма затруднительно.

По существу, эта формула всего лишь еще раз подчеркивает, что множество простых чисел рекурсивно (более того, его характеристическая функция примитивно рекурсивна). Несмотря на то, что есть алгоритм (и далеко не один) для узнавания того, просто число или нет, да и называются они словом «простые», вопросы о простых числах неожиданно оказались чрезвычайно сложными.

Многие вопросы о простых числах, поставленные столетия, а то и тысячелетия назад, не имеют ответа до сих пор. Вопросы, привлекательные своей простотой, часто оказываются невероятно сложными и не получающими решения в течение столетий, а то и тысячелетий.

Ни одна наука не имеет таких старых нерешенных проблем; мало того, что проблемы выдержали испытание временем, их формулировка предельно проста и понятна даже ученику начальной школы.

Рассмотрим несколько таких арифметических задач.

Число в школе Пифагора¹ называли *совершенным*, если оно совпадает с суммой своих собственных делителей. Например, числа 6, 28, 496, 8128 совершенные.

Тогда же, т. е. два с половиной тысячелетия назад, был поставлен вопрос: конечно или бесконечно множество совершенных чисел?

Во времена Евклида были известны всего лишь первые четыре совершенных числа. Безусловно, они знали бы их больше, если бы им удалось открыть позиционную систему счисления, но на теорию чисел это вряд ли бы существенно повлияло. Даже сейчас, во время машинных вычислений, когда становятся доступными для экспериментов числа с миллионами и миллиардами цифр, вопрос о совершенных числах по существу не продвинулся. Древние знали всего четыре числа, сейчас их известно всего лишь

¹ Пифагор Самосский (Πυθαγόρας, ок. 570 — ок. 500 лет до н. э.) — древнегреческий философ. По учению Пифагора основой благополучия являются красивые, т. е. совершенные числа. Например, государство с красивым числом членов высшего органа управления (Боярской думой, Государственным советом, парламентом и т. п.) будет вечно благоденствовать, а с некрасивым числом членов — быстро погибнет. Другими словами, *красота спасет мир*.

50, но главный вопрос — о числе совершенных чисел — остается без ответа.

Некоторое продвижение в решении задачи было сделано Эйлером в VIII в. Еще Евклид заметил, что число вида $2^{n-1} \cdot p$, где p — простое число вида $2^n - 1$, является совершенным. Эйлер доказал, что и обратное утверждение тоже верно: если четное число a совершенно, то $a = 2^{n-1} \cdot p$, где $p = 2^n - 1$ простое. Например,

$$6 = 2^1 \cdot 3;$$

$$28 = 2^2 \cdot 7;$$

$$496 = 2^4 \cdot 31;$$

$$8128 = 2^6 \cdot 127;$$

$$33\,550\,336 = 2^{12} \cdot 8191;$$

$$8\,589\,869\,056 = 2^{16} \cdot 131\,071;$$

$$137\,438\,691\,328 = 2^{18} \cdot 524\,287;$$

$$2\,305\,843\,008\,139\,952\,128 = 2^{30} \cdot 2\,147\,483\,647.$$

С помощью теоремы Эйлера получили описание все четные совершенные числа, но ответа на основной вопрос пока нет.

Число вида $M_n = 2^n - 1$ называют *числом Мерсенна*¹.

С помощью простого числа Мерсенна можно построить четное совершенное число, и наоборот, каждое четное совершенное число содержит простое число Мерсенна M_n в виде множителя, причем второй множитель — это 2^{n-1} . Например, простые числа

$$M_2 = 2^2 - 1 = 3;$$

$$M_3 = 2^3 - 1 = 7;$$

$$M_5 = 2^5 - 1 = 31;$$

$$M_7 = 2^7 - 1 = 127;$$

$$M_{13} = 2^{13} - 1 = 8191;$$

$$M_{17} = 2^{17} - 1 = 131\,071;$$

$$M_{19} = 2^{19} - 1 = 524\,287;$$

$$M_{31} = 2^{31} - 1 = 2\,147\,483\,647$$

входят в разложение совершенных чисел. Заметим, что числа M_{M_n} являются простыми лишь для $n = 2, 3, 5, 7$. Числа M_{8191} , $M_{131\,071}$, $M_{524\,287}$ уже непростые.

В течение последних десятилетий нахождение каждого нового числа Мерсенна было связано с появлением очередного поколения вычислительной техники и являлось демонстрацией возросших технических возможностей. Все числа Мерсенна, начиная с 13-го², были найдены только с помощью электронной вычислительной

¹ Марен Мерсенн (Mersenne, 1588—1648) — французский физик и теолог. Мерсенн первым измерил скорость звука в атмосфере и изобрел зеркальный телескоп. Вел обширную переписку с выдающимися учеными своего времени, которая способствовала распространению и обсуждению научных открытий, установлению связей между учеными.

² 13-е число Мерсенна равно $2^{521} - 1$. В его десятичной записи 157 цифр. В 12-м $M_{12} = 2^{127} - 1$, последнем «ручном» числе, — 39 цифр.

техники (иногда это было совсем не быстро — например, нахождение 30-го числа Мерсенна $2^{132\,049} - 1$ в 1983 г. продолжалось более 120 ч).

В 2021 г. известно 51 простое чисел Мерсенна. Самое большое из них —

$$2^{82\,589\,933} - 1,$$

найденное еще в декабре 2018 г. Десятичная запись числа имеет длину 24 862 048 цифр. Напечатанное убористым шрифтом на листах формата А4 это число займет более 31 тысяч страниц (это больше 20 экземпляров «Войны и мира» Л. Н. Толстого). Совершенное число, полученное из этого числа Мерсенна, будет еще в два раза больше.

Найденных четных совершенных чисел ровно столько, сколько простых чисел Мерсенна.

Нечетных совершенных чисел пока *не найдено ни одного*, и неизвестно, существуют ли они вообще. Хотя вполне возможно, что такие числа существуют и, может быть, их даже бесконечно много.

Одновременно с задачей о совершенных числах появилась и задача о дружественных числах.

Два числа называют *дружественными*, если сумма собственных делителей каждого их чисел равна другому числу. Так случилось, что пары дружественных (даже не очень больших) чисел находились с большим трудом. После первой пары (220 и 284), известной древним грекам, до нахождения следующих трех пар дружественных чисел прошло более двух тысяч лет. Современная вычислительная техника позволяет сравнительно легко находить все пары дружественных чисел в достаточно больших отрезках натурального ряда. Например, 220—284, 1184—1210, 2620—2924, 5020—5564, 6232—6368, 10 744—10 856, 12 285—14 595, 17 296—18 416, 63 020—76 084 — пары дружественных чисел, которые вычислительный пакет *Maple* находит непосредственным вычислением в течение долей секунды.

Совершенные числа являются как бы самодружественными. Разумеется, древние греки придавали дружественным числам особый смысл (тем более что их система обозначения чисел основывалась на алфавите и давала возможность для всевозможных спекуляций с числами, связанными с записью имен людей, названий городов, стран и т. п.). Рекомендовалось использовать дружественные числа при вручении взяток чиновникам, любовной магии и в других похожих житейских ситуациях.

Основная задача, впрочем, такая же, как и для совершенных чисел: конечно или бесконечно множество дружественных чисел? То, что техника значительно увеличила число дружественных чисел

(сейчас их известно около 1,5 тыс.), теории никак не помогло. Ответа на этот вопрос тоже пока нет.

Дружественные числа могут быть как четными, так и нечетными. Но все найденные пары дружественных чисел имеют одинаковую четность, и пока не найдено ни одной пары дружественных чисел разной четности (но нет и доказательства того, что в такой паре оба числа должны быть непременно одной четности).

Еще одной задачей такого же возраста (т. е. около 2500 лет) является *проблема близнецов*. Два простых числа p и $p + 2$ древние греки называли *близнецами*. Например, (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73) — пары близнецов.

Близнецов гораздо больше, чем дружественных (и уж тем более совершенных) чисел. Их число только на порядок меньше, чем вообще число простых чисел в данном интервале.

Интервал	Число близнецов в интервале	Число простых чисел в интервале
1—100	8	25
1—1000	35	168
1—10 000	205	1229
1—100 000	1224	9592
1—1 000 000	8169	78 498

Долгое время в учебнике математики для 6-го класса общеобразовательной средней школы на форзаце была помещена таблица простых чисел из интервала [2, 1000], причем близнецы были выделены белым цветом. Никаких ссылок на этот цвет в тексте учебника не было. Видимо, по замыслу авторов, любопытный ученик должен был сам поставить соответствующий вопрос. Вопрос этот такой же, как и для совершенных и дружественных чисел: конечно или бесконечно множество пар близнецов?

Трудность задач о совершенных, дружественных числах и о числах-близнецах проверена тысячелетиями. Есть и более молодые арифметические вопросы, оказавшиеся неожиданно трудными.

При построении правильного m -угольника с помощью циркуля и линейки появляются числа вида $F_n = 2^{2^n} + 1$. Такие числа в честь автора называют *числами Ферма*¹.

Пьер Ферма был совершенно уверен, что для любого n число F_n простое. Действительно,

$$F_0 = 3;$$

$$F_1 = 5;$$

¹ Пьер Ферма (Fermat, 1601—1665) — французский юрист и математик-любитель. Научные результаты П. Ферма опубликованы его сыном в сборнике «Разные сочинения» (1665).

$$F_2 = 17;$$

$$F_3 = 257;$$

$$F_4 = 65\,537$$

являются простыми. Однако начиная с числа F_5 все последующие F_n , известные в настоящее время, оказались составными числами.

Нахождение нового простого числа Ферма было явлением более значимым, чем появление еще одного числа Мерсенна или еще одной пары близнецов.

Существует ли шестое простое число Ферма, конечно или бесконечно множество простых чисел Ферма, пока неизвестно. Задача о простых числах Ферма молодая, ей чуть больше 300 лет. Широкую известность она приобрела, когда сын Ферма опубликовал в 1665 г. математические результаты своего покойного отца.

Тогда же было опубликовано и самое известное широкой публике утверждение (так называемая *Великая теорема Ферма*): для любого натурального $n > 2$ уравнение $x^n + y^n = z^n$ не имеет решений в целых положительных числах. Это утверждение удалось доказать лишь 330 лет спустя¹.

Еще моложе (и уже частично решена) *задача Гольдбаха*². Христиан Гольдбах в 1742 г. (в письме Леонарду Эйлеру) заметил, что каждое нечетное число больше шести можно представить в виде суммы трех простых. Эйлер заметил, что это утверждение верно, если каждое четное число больше двух можно представить в виде суммы двух простых.

Существование представления для четных чисел удалось установить в 1937 г. русскому математику И. М. Виноградову³. Он доказал, что для всех нечетных чисел, больших некоторого n , утверждение Гольдбаха верно. Это число n , правда, настолько велико, что пока проверить (даже с помощью современной техники) утверждение Гольдбаха для чисел, меньших n , невозможно.

Для четных чисел задача остается нерешенной. Современная техника позволяет найти такое представление для больших чисел (например, числа $10^{600} + 4091$ и $10^{600} - 4091$ являются простыми). Также можно заметить, что число таких представлений в виде суммы простых, увеличивается с возрастанием n .

¹ Доказательство великой теоремы Ферма получил английский математик Эндрю Уайлс (Wiles, род. 1963) в 1994 г. (опубликовано в 1995 г.).

² Христиан Гольдбах (Goldbach, 1690—1764) — российский математик немецкого происхождения, один из первых академиков (1725) Петербургской АН.

³ Иван Матвеевич Виноградов (1891—1983) — русский математик, академик АН СССР (1929), директор Математического института АН СССР им. В. А. Стеклова (1932—1983).

Например, число 10 можно представить тремя способами, 100 — двенадцатью, для 1000 число способов равно 56, для 10 000 — 254, для 100 000 — 1620, а для 1 000 000 — 10 804. Несмотря на заметное увеличение таких представлений с увеличением n , пока нет ни доказательства, что для любого четного n найдется хотя бы одно такое представление, ни опровергающего контрпримера.

Таким образом, слово «простые» для простых чисел обманчиво. Все перечисленные задачи связаны с простыми числами. Необычайная трудность этих вопросов объясняется тем обстоятельством, что простое число определяется на мультипликативном языке через умножение, а сами задачи имеют аддитивный характер — там непременно присутствует сумма.

3.3. Строение мультипликативной полугруппы натуральных чисел

На графе делимости множества натуральных чисел, больших единицы, простые числа расположены внизу. Они являются минимальными элементами и играют роль основания, фундамента графа.

Роль простых чисел действительно фундаментальна и выражается она так называемой **основной теоремой арифметики**: *каждое натуральное число, большее единицы, является простым или произведением простых, причем представление это единственно, с точностью до порядка множителей.*

«С точностью до порядка множителей» означает, что если какое-то число имеет два разложения

$$p_1 \cdot p_2 \cdot \dots \cdot p_n = q_1 \cdot q_2 \cdot \dots \cdot q_m$$

в виде произведения простых чисел p_i и q_j , то $n = m$ и при подходящем изменении нижних индексов множители p_i и q_j совпадают.

Основная теорема состоит из двух утверждений:

- 1) представление существует;
- 2) представление единственно.

Докажем сначала существование разложения числа a индукцией по a .

Воспользуемся аксиомой индукции в форме условия минимальности.

Предположим, что утверждение о существовании разложения не выполняется, т. е. существуют числа, которые нельзя представить в виде произведения простых множителей. По условию минимальности существует *наименьшее* такое число $a > 1$. Итак, число a не простое и не обладает разложением на простые множители. Наи-

меньший неединичный натуральный делитель p числа a является простым,

$$a = p \cdot b,$$

где p — простое число, следовательно, $p > 1$, поэтому $b < a$. Если бы число b обладало разложением в произведение простых,

$$b = p_1 \cdot p_2 \cdot \dots \cdot p_n,$$

то и a имело бы представление

$$a = p \cdot p_1 \cdot p_2 \cdot \dots \cdot p_n.$$

Значит, число b не имеет представления в виде произведения простых и b строго меньше a . Полученное противоречие с выбором числа a показывает, что числа, не обладающего разложением в произведение простых чисел, не существует.

Утверждение о существовании разложения доказано.

Докажем единственность разложения тоже по индукции и в той же форме — в виде условия минимальности.

Предположим, что существуют составные числа, обладающие различными представлениями. По условию минимальности найдется наименьшее число с таким свойством — пусть это число равно a . Итак,

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_n = q_1 \cdot q_2 \cdot \dots \cdot q_m,$$

где p_i, q_j — простые числа, причем наборы p_1, p_2, \dots, p_n и q_1, q_2, \dots, q_m различны. Различие проявляется и в том, что при любых перестановках первого набора никогда не получится второй набор.

Если в каждом из разложений встречается одно и то же простое число p , то, разделив на него обе части равенства, получим, что число $\frac{a}{p}$ обладает двумя различными разложениями и строго меньше числа a . Это противоречит выбору числа a как минимального, обладающего двумя разложениями.

Таким образом, минимальность числа a усилила различие разложений для a : ни одно простое число не встречается одновременно в первом и втором разложении числа a . Например, множитель q_1 отличен от любого p_i ($i = 1, 2, 3, \dots, n$).

Расположим простые числа в разложении в порядке возрастания:

$$p_1 \leq p_2 \leq \dots \leq p_n \text{ и } q_1 \leq q_2 \leq \dots \leq q_m.$$

Числа p_1, q_1 различны. Для определенности будем считать, что $q_1 < p_1$.

Число a составное, т. е. кроме множителя p_1 там должны быть и другие множители (может быть, равные p_1). Это значит, что $p_1 \cdot p_1 \leq a$. Но тогда $p_1 \cdot q_1 < a$.

Рассмотрим число $a - p_1 \cdot q_1$. Из неравенства $a - p_1 \cdot q_1 < a$ и выбора числа a следует, что $a - p_1 \cdot q_1$ обладает *единственным представлением* в виде произведения простых чисел.

Из единственности разложения $a - p_1 \cdot q_1$ на простые множители следует, в свою очередь, что каждый простой делитель этого числа должен входить в это единственное представление числа $a - p_1 \cdot q_1$.

Число a делится на простые p_1 и q_1 , поэтому данные числа должны входить в представление числа $a - p_1 \cdot q_1$:

$$a - p_1 \cdot q_1 = p_1 \cdot q_1 \cdot s_1 \cdot s_2 \cdot \dots \cdot s_k,$$

где s_t простые.

Разделим теперь число a на p_1 , в результате получим:

$$\frac{a}{p_1} = p_2 \cdot p_3 \cdot \dots \cdot p_n = q_1 \cdot s_1 \cdot s_2 \cdot \dots \cdot s_k.$$

Вспомним, что q_1 отлично от любого p_i ($i = 2, 3, \dots, n$). Следовательно, эти два разложения числа $\frac{a}{p_1}$ существенно *различны*.

Но число $\frac{a}{p_1}$ строго меньше числа a . Получено *противоречие* с выбором числа a .

Это противоречие означает, что предположение о существовании числа, обладающего двумя представлениями, *ложно* и, следовательно, каждое составное натуральное число имеет *единственное представление* в виде произведения простых.

Доказательство *единственности* представления закончилось.

Основная теорема арифметики доказана полностью.

Напомним, что *однопорожденная полугруппа* называется *моногенной*.

На алгебраическом языке основная теорема арифметики означает, что мультипликативная полугруппа $\langle \mathbb{N} \setminus \{1\}; \cdot \rangle$ натуральных чисел, больших единицы, является прямым произведением бесконечных моногенных полугрупп, порожденных простыми числами.

Моноид $\langle \mathbb{N}; \cdot \rangle$ отличается от полугруппы $\langle \mathbb{N} \setminus \{1\}; \cdot \rangle$ всего лишь одним прямым множителем — полугруппой $\langle \{1\}; \cdot \rangle$.

Множество M простых чисел счетно, поэтому множество $P(M)$ подмножеств множества M континуально. Это значит, что в моноиде $\langle \mathbb{N}; \cdot \rangle$ содержится континуум различных подмоноидов. Множество алгоритмов всего лишь счетно, поэтому среди этих подмоноидов находится несчетное число таких, для которых проблема вхождения алгоритмически неразрешима.

Впрочем, и в счетной серии содержатся подмоноиды с неразрешимой проблемой вхождения. Достаточно взять рекурсивно перечислимое, но не рекурсивное подмножество из M . Правда, обычно проблему вхождения формулируют для конечно порожденных подалгебр. Для конечно порожденных подмоноидов $\langle N; \cdot \rangle$ эта проблема разрешима.

Сделаем лишь одно замечание о доказательстве единственности. В нем нет, по существу, никаких ссылок, кроме как на вполне упорядоченность множества Z_0 .

Однако это его свойство является одновременно как достоинством, так и недостатком. Если мы захотим доказать аналогичное утверждение для произвольного целостного кольца K , то это K может оказаться вообще не упорядоченным и приведенные рассуждения для него не подойдут.

Приведем набросок другого пути к той же цели.

Из критерия взаимной простоты чисел следует, что *если число a делит произведение $b \cdot c$ и взаимно просто с числом b , то a делит c .*

Данный факт называют *теоремой Евклида о делимости*. Из этой теоремы следует, что если простое число p делит произведение простых $q_1 \cdot q_2$, то $p = \varepsilon q_1$ или $p = \varepsilon q_2$, где $\varepsilon \in \{1, -1\}$.

Теперь индукцией по числу множителей в произведении $q_1 \cdot q_2 \cdot \dots \cdot q_n$ можно доказать, что если простое число p делит произведение простых $q_1 \cdot q_2 \cdot \dots \cdot q_n$, то для некоторого i выполняется равенство $p = \varepsilon q_i$, где $\varepsilon \in \{1, -1\}$.

Отсюда индукцией по числу множителей в разложении целого числа получается утверждение о единственности представления составного натурального числа в виде произведения простых, а именно: *представление целого числа, по модулю большего единицы, в виде произведения простых чисел единственно с точностью до порядка и ассоциированности множителей.*

В разложении числа a на простые множители соберем одинаковые простые числа в степени и получим:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}.$$

Здесь все p_i — различные простые числа (обычно их выписывают в порядке возрастания: $p_1 < p_2 < \dots < p_n$), а α_i — натуральные числа. Такое представление числа a принято называть *каноническим*.

Основная теорема арифметики по существу утверждает, что *каждое натуральное число, большее единицы, обладает в точности одним каноническим представлением.*

Каждое положительное рациональное число a можно представить единственным образом в виде несократимой обыкновенной дроби. Числитель и знаменатель этой дроби обладают канониче-

ским представлением, следовательно, мультипликативная группа \mathbb{Q}_+ положительных рациональных чисел является прямым произведением бесконечных циклических групп:

$$\mathbb{Q}_+ = \text{гр}(2) \times \text{гр}(3) \times \text{гр}(5) \times \dots \times \text{гр}(p_i) \times \dots$$

Напомним, что аддитивная группа рациональных чисел неразложима в прямое произведение, поэтому мы снова увидели, что (в отличие от групп $\langle \mathbb{R}_+; \cdot \rangle$ и $\langle \mathbb{R}; + \rangle$) группы $\langle \mathbb{Q}_+; \cdot \rangle$ и $\langle \mathbb{Q}; + \rangle$ не изоморфны.

Заметим, что группа $\langle \mathbb{Q}; + \rangle$ тоже построена из циклических групп нетривиальным образом. Любая группа является теоретико-множественным объединением циклических подгрупп, но в группе $\langle \mathbb{Q}; + \rangle$ циклические подгруппы можно выбрать в виде возрастающей цепочки. Понятно, что эта цепочка будет строго возрастающей и бесконечной: сама группа $\langle \mathbb{Q}; + \rangle$ нециклическая.

Рассмотрим теперь основные числовые функции.

Числовой функцией обычно называют функцию, определенную для целых неотрицательных чисел со значениями в том же множестве.

Две числовые функции у нас уже появились. Это двухместные функции (a, b) и $[a, b]$.

Если число a обладает каноническим представлением

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n},$$

то любой делитель x числа a имеет вид

$$x = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n}.$$

Простые числа p_i в этом представлении те же самые, что и у числа a , показатели β_i удовлетворяют неравенствам $0 \leq \beta_i \leq \alpha_i$ для всех $i = 1, 2, \dots, n$.

Другими словами, для того чтобы число x делило число a , необходимо и достаточно, чтобы каждый простой множитель, входящий в разложение числа x , входил в разложение числа a в такой же или более высокой степени.

Каноническое разложение натурального числа a и полное описание делителей числа a позволяют найти НОД и НОК двух чисел a и b новым (таким же, как в школе) способом.

В каноническое разложение чисел a и b могут входить различные простые числа. Сделаем эти разложения равной длины, разрешив нулевые показатели степеней (если $\alpha = 0$ в множителе p^α , то p в разложение числа a не входит). Пусть число a имеет полуканоническую форму (с целыми неотрицательными α_i),

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n},$$

а число b , соответственно,

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n}.$$

Тогда

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot p_2^{\min\{\alpha_2, \beta_2\}} \cdot \dots \cdot p_n^{\min\{\alpha_n, \beta_n\}};$$

$$[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} \cdot p_2^{\max\{\alpha_2, \beta_2\}} \cdot \dots \cdot p_n^{\max\{\alpha_n, \beta_n\}}.$$

Заметим, что для любых x, y

$$\min\{x, y\} + \max\{x, y\} = x + y,$$

следовательно, для любых целых чисел a и b

$$(a, b) \cdot [a, b] = a \cdot b.$$

Вернемся к полуканоническим формам числа a и его делителя x . Используя эти формы, мы можем найти число $\tau(n)$ натуральных делителей и сумму $\sigma(n)$ натуральных делителей числа a . Число натуральных делителей $\tau(n)$ числа n с каноническим разложением $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m}$ равно

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1).$$

Сумма натуральных делителей $\sigma(n)$ числа n с каноническим разложением $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m}$ равна

$$\prod_{p_i} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Напомним, что математики школы *Пифагора* называли натуральное число *совершенным* (*красивым*), если оно совпадает с суммой своих собственных делителей, т. е. n совершенно, если $\sigma(n) = 2n$.

Например, числа 6, 28, 496, 8128, ... совершенные. Нетрудно догадаться, что скрывается под многоточием. Каноническое разложение каждого написанного числа имеет вид $2^{n-1} \cdot (2^n - 1)$, где $(2^n - 1)$ простое. Следующий результат получен еще *Евклидом*.

Если число $2^n - 1$ простое, то число $2^{n-1} \cdot (2^n - 1)$ совершенно.

Действительно, пусть $a = 2^{n-1} \cdot p$, где простое $p = 2^n - 1$, тогда:

$$\begin{aligned} \sigma(a) &= (1 + 2 + \dots + 2^{n-1}) \cdot (p + 1) = (2^n - 1) \cdot (2^n - 1 + 1) = \\ &= 2 \cdot 2^{n-1} (2^n - 1) = 2\sigma(a). \end{aligned}$$

Через два тысячелетия Эйлер показал, что для четных чисел верно и обратное утверждение: если четное число m совершенно, то оно имеет вид $m = 2^{n-1} \cdot (2^n - 1)$, где $2^n - 1$ — простое число.

Существуют ли нечетные совершенные числа и конечно или бесконечно множество совершенных чисел, неизвестно до сих пор.

Известно, что если n — нечетное совершенное число, то оно может иметь только вид

$$p^{4m+1}s^2,$$

где простое $p = 4k + 1$ и s не делится на p .

Не используя этот факт, можно заметить, что если n — нечетное совершенное число, то $\tau(n)$ при делении на 4 дает в остатке 2.

Действительно, все делители n нечетные, а число делителей четное (иначе не получится $\sigma(n) = 2n$).

Просуммировав равенства $ab = n$, где

$$a \in \left\{ x \mid x \text{ делит } n, x < \left[\frac{n}{2} \right] \right\},$$

получаем

$$\left[\frac{\tau(n)}{2} \right] (n+1) = 2n + 4t,$$

где $t \in \mathbb{Z}$. Число n имеет вид $2s + 1$, поэтому

$$[\tau(n)](s+1) = 2n + 4t,$$

откуда $\left[\frac{\tau(n)}{2} \right]$ нечетное, т. е. $\tau(n) = 4k + 2$.

Теорема Евклида о бесконечности множества простых чисел означает, что в прогрессии с первым членом 1 и разностью 1 бесконечно много простых.

Что можно сказать о произвольной прогрессии $ax + b$ первым членом b и разностью a ?

Если первый член и разность прогрессии не взаимно просты, то в такой прогрессии конечное число простых чисел (одно простое b или вообще ни одного).

Если $(a, b) = 1$, то ответ такой же, как у Евклида в частном случае: в прогрессии $ax + b$ бесконечно много простых.

Этот результат в честь автора называют *теоремой Дирихле*¹.

Доказательство теоремы Дирихле гораздо сложнее теоремы Евклида, однако в некоторых случаях удается почти прямое подражание рассуждению Евклида.

¹ *Петер Густав Лежен Дирихле (Dirichlet, 1805—1859)* — немецкий математик, профессор Берлинского (1831—1855) и Геттингенского (с 1855) университетов. Теорема о существовании бесконечного числа простых чисел в арифметической прогрессии доказана П. Дирихле в 1837 г.

Например, рассмотрим прогрессию $4x + 3$. Можно начать ее со второго члена (на бесконечность или конечность интересующего нас множества это не повлияет).

Допустим, что $7, 11, 19, \dots, p$ — это все простые из прогрессии $4x + 3$ ($x = 1, 2, \dots$). Тогда число

$$4(7 \cdot 11 \cdot 19 \cdot \dots \cdot p) + 3$$

лежит в той же прогрессии и не является произведением только простых чисел вида $4x + 1$. Желаемое противоречие получено: прогрессия $4x + 3$ содержит бесконечно много простых чисел.

Аналогичными рассуждениями устанавливается, что и прогрессия $6x + 5$ содержит бесконечно много простых чисел.

Рассмотрим прогрессию $4x + 1$. Произведение двух чисел вида $4x + 3$ имеет вид $4x + 1$; поэтому прием, использованный при обсуждении свойств прогрессии $4x + 3$, не пройдет. Однако в параграфе 3.6 мы увидим, что число вида $a^2 + 1$ никогда не делится на простое число вида $4x + 3$.

Используем этот факт прямо сейчас. Пусть $5, 13, \dots, p$ — все простые числа, попавшие в прогрессию $4x + 1$. Тогда число

$$(2 \cdot 5 \cdot 13 \cdot \dots \cdot p)^2 + 1$$

лежит в этой же прогрессии и не делится ни на два, ни на одно простое число вида $4x + 3$. Противоречие налицо.

Итак, *прогрессия $4x + 1$ содержит бесконечно много простых чисел.*

Аналогичные трудности возникают и с прогрессией $6x + 1$. Произведение чисел вида $6x + 5$ имеет вид $6x + 1$. Как и для предыдущей прогрессии, здесь нужна дополнительная информация. Такая информация (которая будет доказана позже) есть: число вида $a^2 + 3$ не делится на простое число вида $6x + 5$.

Теперь число

$$a = (2 \cdot 7 \cdot 13 \cdot \dots \cdot p)^2 + 3,$$

где $7, 13, \dots, p$ — все простые числа вида $6x + 1$, тоже принадлежит этой же прогрессии. Используя приведенное «воспоминание о будущем», получаем нужное противоречие.

Прогрессия $6x + 1$ содержит бесконечно много простых чисел.

Теорема Евклида не использовала основной теоремы арифметики. Однако ее применение открывает новые горизонты. Например, используя расходимость гармонического ряда и основную теорему арифметики, можно увидеть, что простые числа в натуральном ряду встречаются чаще, чем квадраты.

Ряд, составленный из чисел, обратных квадратам натуральных, сходится, в то время как ряд, составленный из чисел, обратных простым, расходится.

Докажем утверждение о расхождении ряда

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p_n} + \dots,$$

где p_n — n -е простое число, методом от противного. Предположим, что этот ряд сходится, т. е. имеет сумму. Если сумма ряда больше единицы, то, отбросив, если требуется, часть первых слагаемых, мы получим ряд

$$\frac{1}{p_k} + \frac{1}{p_{k+1}} + \dots + \frac{1}{p_n} + \dots,$$

сумма которого уже меньше единицы.

Бесконечная геометрическая прогрессия со знаменателем, меньшим единицы, сходится; следовательно, сходится и прогрессия

$$1 + \left(\frac{1}{p_k} + \frac{1}{p_{k+1}} + \dots \right) + \left(\frac{1}{p_k} + \frac{1}{p_{k+1}} + \dots \right)^2 + \dots \quad (*)$$

После раскрытия скобок среди слагаемых суммы (*) появятся слагаемые вида

$$\frac{1}{p_{i_1}^{\alpha_1} p_{i_2}^{\alpha_2} \dots p_{i_k}^{\alpha_k}},$$

где α_j — натуральные числа, а p_{i_j} — простые числа, и $i_j \geq k$. Более того, любая дробь такого вида непременно будет в сумме (*).

Пусть $t = 2 \cdot 3 \cdot \dots \cdot p_{k-1}$; тогда число $tm - 1$ при любом натуральном m не делится ни на одно простое число, меньшее p_k , поэтому делится только на оставшиеся простые числа. Следовательно, в сумме (*) встретятся слагаемые вида

$$\frac{1}{tm - 1},$$

где $m = 1, 2, 3, \dots$. Поскольку ряд (*) сходится, то сходится и ряд

$$\sum_{m=1}^{\infty} \frac{1}{tm - 1}$$

и тем более сходится ряд

$$\sum_{m=1}^{\infty} \frac{1}{tm} = t \cdot \sum_{m=1}^{\infty} \frac{1}{m}.$$

Однако отсюда следует сходимость гармонического ряда. Противоречие получено и этим установлено, что ряд, составленный из чисел, обратных к простым, расходится.

Отметим, что еще в 1919 г. Вирро Брун¹ доказал: ряд, составленный из чисел, обратных к простым близнецам, сходится. Это значит, что число пар близнецов *меньше*, чем простых неблизнецов. Даже может быть, что число близнецов конечно.

3.4. Диофантовы уравнения первой степени

Алгебраическое уравнение от любого числа неизвестных с целыми коэффициентами, решение которого разыскивается тоже в целых числах, называют *диофантовым уравнением*². Число неизвестных в диофантовом уравнении обычно не меньше двух, и в случае совместности множество решений бесконечно. Поэтому такие уравнения называют еще *неопределенными уравнениями*.

В докладе «Математические проблемы», сделанном 8 августа 1900 г. на 2-м Международном конгрессе математики в Париже, Д. Гильберт³ сформулировал 23 нерешенные математические проблемы, исследование которых, как он сказал, «может значительно стимулировать развитие науки».

Проблема Гильберта № 10 — это задача о разрешимости диофантова уравнения.

Декартову n -ю степень множества \mathbb{Z}_0 можно эффективно перечислить, поэтому если у нас есть алгоритм для узнавания, имеет ли данное диофантово уравнение решение или нет, то в конечном числе шагов, простым перебором, это решение можно найти.

Десятая проблема Гильберта оказалась алгоритмически неразрешимой⁴.

Отрицательное решение проблемы о диофантовых уравнениях делает тем более значимыми классы, для которых алгоритм распознавания совместных уравнений существует.

Например, один из этих классов — уравнения, входящие в формулировку Великой теоремы Ферма:

$$x^n + y^n = z^n, \text{ где } n > 2.$$

¹ Вирро Брун (Brun, 1885—1978) — норвежский математик, член Норвежской академии наук и литературы. Основные труды — по теории чисел.

² В честь Диофанта (Διοφάντος, ок. III в.) — греческого математика из Александрии. Сохранилось шесть книг (из 13) его трактата «Арифметика», где дается решение задач, в основном сводящихся к решению неопределенных уравнений.

³ Давид Гильберт (Hilbert, 1862—1943) — немецкий математик, профессор Геттингенского университета (1895—1930), иностранный почетный член АН СССР (с 1934 г.).

⁴ Решение 10-й проблемы Гильберта получено в 1970 г. российским математиком Юрием Владимировичем Матиясевичем (род. в 1947 г.).

Утверждение о несовместности такого уравнения на множестве целых неотрицательных чисел (записанное Пьером Ферма на полях «Арифметики» Диофанта) опубликовано Ферма-сыном в 1665 г. Это утверждение оказалось верным, но доказать его удалось лишь более чем через три столетия.

Обычно имеется в виду, что диофантово уравнение имеет не менее двух неизвестных, однако алгебраическое уравнение с целыми коэффициентами формально подпадает под определение. Простым испытанием делителей свободного члена такого уравнения можно выяснить, имеет оно целые решения или нет.

Другими словами, проблема совместности диофантова уравнения с одним неизвестным алгоритмически разрешима.

Поскольку кольцо целых чисел является кольцом главных идеалов, сумма любого числа идеалов порождается одним элементом. Это значит, что диофантово уравнение

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b$$

имеет решение в целых числах тогда и только тогда, когда НОД чисел a_1, a_2, \dots, a_n делит число b .

Таким образом, проблема совместности линейного уравнения с n неизвестными сводится к поиску наибольшего общего делителя, следовательно, эта проблема алгоритмически разрешима.

Однако даже решение простейшего уравнения $ax + by = c$ с двумя неизвестными для больших чисел a, b, c может оказаться весьма трудоемким. Значительно облегчить ситуацию могут *цепные дроби*.

Пусть рациональное число представлено несократимой дробью $\frac{a}{b}$, где a — целое, b — натуральное число. Несократимость дроби означает, что $(a, b) = 1$. Наибольший общий делитель равен последнему ненулевому остатку в алгоритме Евклида, примененного к числам a и b . Применим этот алгоритм и получим равенства:

$$\begin{aligned} a &= b \cdot q_1 + r_1; \\ b &= r_1 \cdot q_2 + r_2; \\ r_1 &= r_2 \cdot q_3 + r_3; \\ &\dots\dots\dots \\ r_{n-3} &= r_{n-2} \cdot q_{n-1} + 1; \\ r_{n-2} &= 1 \cdot q_n. \end{aligned}$$

Последний ненулевой остаток r_{n-1} (равный единице) появляется в предпоследнем равенстве; в последнем равенстве остаток равен нулю.

Теперь разделим первое равенство на b , второе — на r_1 , третье — на r_3 и т. д., предпоследнее — на r_{n-2} , последнее — на r_{n-1} , равное единице.

Получим:

$$\frac{a}{b} = q_1 + \frac{r_1}{b};$$

$$\frac{b}{r_1} = q_2 + \frac{r_2}{r_1};$$

$$\frac{r_1}{r_2} = q_3 + \frac{r_3}{r_2};$$

$$\frac{r_2}{r_3} = q_4 + \frac{r_2}{r_3};$$

.....

$$\frac{r_{n-1}}{r_{n-2}} = q_{n-1} + \frac{1}{r_{n-2}};$$

$$r_{n-2} = q_n.$$

Мы можем взять от второго равенства обратное и подставить значение $\frac{r_1}{b}$ в первое равенство:

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}}.$$

Затем возьмем обратное от второго равенства и подставим значение $\frac{r_2}{r_1}$ в полученное новое равенство для $\frac{a}{b}$:

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{r_3}{r_2}}}.$$

Продолжая и далее таким же образом, в результате получим представление числа $\frac{a}{b}$ в виде *многоэтажной* (говорят — *цепной*) дроби:

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots \frac{1}{q_{n-1} + \frac{1}{q_n}}}}.$$

Поскольку любое рациональное число можно представить обыкновенной несократимой дробью, получаем, что каждое рациональное число можно *развернуть* в конечную цепную дробь.

Наоборот, если дана цепная дробь такого вида, где целая часть и знаменатели — целые неотрицательные числа, то, выполнив вычисления, можно *свернуть* цепную дробь в обыкновенную. Эти наблюдения показывают, что *каждое рациональное положительное число может быть представлено конечной цепной дробью*.

«Свернув» дробь, т. е. выполнив действия, предписанные ее изображением, мы получим рациональное число. Таким образом, *множество рациональных чисел и множество конечных цепных дробей совпадают*.

Числители и знаменатели трех последовательных подходящих дробей, начиная с $i = 2$, связаны следующими равенствами:

$$P_i = q_i \cdot P_{i-1} + P_{i-2}, \quad Q_i = q_i \cdot Q_{i-1} + Q_{i-2}.$$

Числители и знаменатели двух последовательных подходящих дробей, начиная с $i = 1$, связаны равенством

$$\begin{vmatrix} P_{i-1} & P_i \\ Q_{i-1} & Q_i \end{vmatrix} = (-1)^i.$$

Последняя подходящая дробь — это сама дробь $\frac{a}{b}$, поэтому $P_n = a$, $Q_n = b$. Тогда

$$\begin{vmatrix} a & P_{n-1} \\ b & Q_{n-1} \end{vmatrix} = (-1)^n.$$

Отсюда:

$$aQ_{n-1}(-1)^n + bP_{n-1}(-1)^{n+1} = 1.$$

С помощью этого равенства можно гораздо эффективнее (с существенно меньшим числом арифметических действий) получить какое-нибудь конкретное решение уравнения $ax + by = 1$ (а следовательно, и решение уравнения $ax + by = c$).

Знание хотя бы одного конкретного решения позволяет описать все множество решений линейного диофантова уравнения. Рассмотрим сначала случай двух неизвестных.

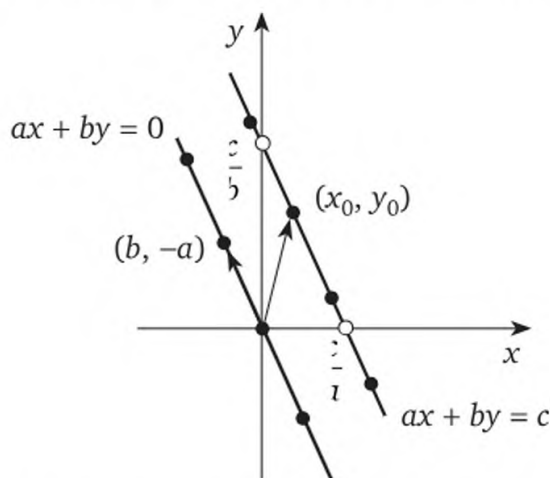
Пусть $ax + by = c$ — уравнение, в котором a, b, c — целые числа.

Очевидно, что если (a, b) не делит c , то уравнение не имеет решения, а если (a, b) делит c , то уравнение имеет решение.

Поэтому если $(a, b) = 1$, то уравнение имеет решение при любом c . К этому случаю сводится произвольное совместное уравнение такого вида. Действительно, разделив левую и правую части уравне-

ния на (a, b) , получим уравнение со взаимно простыми коэффициентами и равносильное исходному.

Если (x_0, y_0) — решение исходного уравнения, то $\{(x_0, y_0) + t(b, -a) \mid t \in \mathbb{Z}\}$ — это все множество решений данного уравнения.



Множество решений уравнения $ax + by = c$

Геометрический смысл уравнения следующий. Множество решений — это точки с целочисленными координатами, попавшие на прямую, описанную этим уравнением. Множество

$$\{t(b, -a) \mid t \in \mathbb{Z}\}$$

представляет собой все точки с целыми координатами, лежащие на графике зависимости $ax + by = 0$, а вектор (x_0, y_0) — вектор сдвига этой прямой. Наши точки расположены на прямой $ax + by = c$ на расстоянии $\sqrt{b^2 + (-a)^2}$ друг от друга.

Пусть теперь все параметры a, b, c в уравнении положительны. Уравнение прямой, заданной этим уравнением, можно задать в отрезках:

$$\frac{x}{\frac{c}{a}} + \frac{y}{\frac{c}{b}} = 1.$$

Если $c > ab$, то

$$\sqrt{b^2 + (-a)^2} < \sqrt{\left(\frac{c}{a}\right)^2 + \left(\frac{c}{b}\right)^2}.$$

Отсюда следует, что в положительном квадранте координированной плоскости на отрезке, соединяющем точки $\left(\frac{c}{a}, 0\right)$ и $\left(0, \frac{c}{b}\right)$, найдется хотя бы одна точка с целочисленными координатами.

Следовательно, если $c \geq ab$, то уравнение $ax + by = c$ имеет решения в целых неотрицательных числах.

Случай трех (и более) неизвестных в линейном диофантовом уравнении удобнее будет рассмотреть в п. 3.6.

При решении технических задач часто используется метод моделирования. Работу будущей плотины, корабля или самолета можно предварительно изучить с помощью уменьшенной копии объекта — модели. Иногда приходится изготавливать несколько моделей одного и того же объекта или его частей с целью изучения различных свойств. Для исследования каждого свойства строится тогда особая модель. Бывает, что трудные и не поддающиеся решению проблемы относительно исходного объекта оказываются более поддающимися для его модели.

Аналогичный метод — метод моделирования — можно применить и для изучения кольца целых чисел. Образно говоря, моделью алгебры, в частности кольца целых чисел, является ее гомоморфный образ, и вычисления в исходном кольце заменяются вычислениями в его гомоморфных образах.

Опишем сначала типичный гомоморфный образ кольца целых чисел.

3.5. Гомоморфный образ кольца целых чисел

Пусть m — некоторое целое число. Обозначим символом (m) множество кратных числа m . Множества (m) и $(-m)$ совпадают, поэтому обычно считают, что m неотрицательное, и называют его в той ситуации, которую сейчас будем обсуждать, *модулем*.

Введем теперь на множестве целых чисел бинарное отношение по правилу: два целых числа a, b находятся в этом отношении, если разность $(a - b)$ принадлежит множеству (m) .

В таком случае принято писать

$$a \equiv b \pmod{m}$$

и говорить: « a и b сравнимы по модулю m ».

Таким образом,

$$a \equiv b \pmod{m} \Leftrightarrow a - b \in (m).$$

Для чисел a, b включение $(a - b)$ в множество (m) означает, что m делит $(a - b)$ или, что то же самое, $a = b + km$, где k — целое число.

Из теоремы о делении с остатком следует, что каждое из этих двух условий будет выполняться тогда и только тогда, когда числа a, b имеют одинаковые остатки при делении на m .

Итак, предложения:

- 1) $a \equiv b \pmod{m}$;
- 2) $m \mid a-b$;
- 3) $a = b + km$, где $k \in \mathbb{Z}$;
- 4) $\text{Rest}(a, m) = \text{Rest}(b, m)$

равносильны.

Разность двух целых чисел равна нулю, а нуль делится на любое целое число. Это значит, что для любого числа a

$$a \equiv a \pmod{m}$$

или, другими словами, отношение сравнимости *рефлексивно*. Если число x делится на m , то и число $-x$ кратно m . Это значит, что для любых целых чисел a, b

$$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m},$$

т. е. отношение сравнимости *симметрично*. Если числа x, y оба делятся на m , то и их сумма $x + y$ тоже делится на m .

Следовательно,

$$a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}.$$

Отношение сравнимости *транзитивно*.

Итак, отношение сравнимости по модулю m является *эквивалентностью* на множестве целых чисел¹. Как любая эквивалентность, сравнимость по модулю разбивает множество на смежные классы. Поскольку отношение сравнимости является одновременно и отношением равноостаточности, различных смежных классов для $m > 0$ будет в точности столько, сколько существует различных остатков при делении на m . Таким образом, для положительного m возникает m различных классов.

Если $m = 0$, то отношение сравнимости превращается в обычное равенство (число ноль делится только на ноль). Это самая маленькая эквивалентность. Ее графиком является диагональ декартова квадрата. Другая крайность — $m = 1$; тогда сравнимость — эта полная эквивалентность и смежный класс — все множество целых чисел (а соответствующий график — «черный квадрат»).

Фактор-множество по отношению сравнимости по модулю m обозначают символом \mathbb{Z}_m . Таким образом, $|\mathbb{Z}_m| = m$.

¹ Еще проще будет доказательство свойств эквивалентности, если использовать равноостаточность как определение сравнимости. Однако приведенное рассуждение имеет сильное преимущество: оно почти буквально переносится на случай произвольного целостного кольца и его идеала (и даже на случай группы и подгруппы).

Отметим, что множество (m) кратных элемента m является подгруппой в группе $\langle \mathbb{Z}; + \rangle$. Смежные классы — элементы из \mathbb{Z}_m — имеют вид

$$[x] = (m) + x = \{mk + x \mid k \in \mathbb{Z}\}.$$

Эти смежные классы называют еще правыми смежными классами по подгруппе (m) , а их число — *индексом* подгруппы (m) в \mathbb{Z} .

Заметим, что понятия сравнимости (по модулю подгруппы), правого (и левого) смежного класса и индекса носят общеалгебраический характер и определяются для любой группы. Подробнее они будут обсуждаться в теме 4.

Пусть $[y]$ — смежный класс по сравнимости с представителем y . Если $x \in [y]$, то разность $x - m$ снова лежит в том же классе $[y]$; следовательно, *вычитание* модуля m из числа не выводит за пределы смежного класса, в котором это число находится. По этой причине смежный класс по отношению сравнимости по модулю m называют *классом вычетов по модулю m* .

Отношение сравнимости — не просто эквивалентность. С помощью условия 3) определения сравнимости легко проверяется, что эта эквивалентность согласована с операциями кольца \mathbb{Z} (для любых целых чисел a, b):

$$a \equiv a_1 \pmod{m}, b \equiv b_1 \pmod{m} \Rightarrow \begin{cases} a \cdot a_1 \equiv b \cdot b_1 \pmod{m}, \\ a + a_1 \equiv b + b_1 \pmod{m}. \end{cases}$$

Таким образом, отношение сравнимости по модулю образует *конгруэнцию* в кольце целых чисел.

Как и в произвольной алгебре, эта конгруэнция определяет гомоморфное отображение кольца целых чисел $\langle \mathbb{Z}; +, \cdot \rangle$ на факторалгебру $\langle \mathbb{Z}_m; +, \cdot \rangle$. Гомоморфный образ кольца образует кольцо, поэтому алгебра $\langle \mathbb{Z}_m; +, \cdot \rangle$ — кольцо, называемое *кольцом классов вычетов по модулю m* .

Набор из m чисел, выбранных из различных смежных классов по модулю m , называют *полной системой вычетов по модулю m* .

В качестве полной системы вычетов по модулю m можно взять, например, остатки от деления на число m :

$$0, 1, 2, \dots, m-1,$$

т. е. наименьшие неотрицательные вычеты в каждом смежном классе.

Можно выбрать абсолютно наименьший вычет в каждом классе. Тогда для нечетного m это будет система

$$0, \pm 1, \pm 2, \dots, \pm \left\lfloor \frac{m}{2} \right\rfloor,$$

где символ $[x]$ означает целую часть числа x .

Для четного m система представителей будет аналогичной, только число $\frac{m}{2}$ нужно взять в одном экземпляре (с плюсом или минусом по желанию).

Группа $\langle \mathbb{Z}_m; + \rangle$ является гомоморфным образом бесконечной циклической группы $\langle \mathbb{Z}; + \rangle$, поэтому она сама циклическая. Смежный класс $[1]$ будет ее порождающим. Мультипликативная группа \mathbb{Z}_m^* кольца $\langle \mathbb{Z}_m; +, \cdot \rangle$, состоящая из всех обратимых элементов этого кольца, может оказаться устроенной более сложно.

Мультипликативная группа \mathbb{Z}_m^* состоит из всех таких смежных классов $[a]$, что уравнение

$$[a] \cdot [x] = [1]$$

имеет решение в кольце \mathbb{Z}_m^* .

Нам сейчас нужны ответы на два вопроса о кольце \mathbb{Z}_m :

1) когда класс $[a]$ обратим?

2) сколько всего обратимых классов в \mathbb{Z}_m^* ?

Записав уравнение $[a][x] = [1]$ в виде сравнения

$$ax \equiv 1 \pmod{m}$$

и используя критерий взаимной простоты двух чисел, получаем ответ на первый вопрос: число a является представителем обратимого класса по модулю m тогда и только тогда, когда $(a, m) = 1$.

Иначе говоря,

$$[a] \in \mathbb{Z}_m^* \Leftrightarrow (a, m) = 1.$$

Систему представителей обратимых классов называют *приведенной системой вычетов по модулю m* .

Приведенную систему можно выбрать из любой полной системы вычетов.

Функцию $\varphi: \mathbb{N} \rightarrow \mathbb{N}$, заданную правилом $\varphi(n)$ = число натуральных чисел, меньших n и взаимно простых с n , называют *функцией Эйлера*.

Таким образом,

$$\varphi(m) = |\mathbb{Z}_m^*|.$$

Сделаем сейчас замечание общего характера о конечных группах. Пусть G — абелева, мультипликативно записанная группа конечного порядка n и

$$G = \{g_1, g_2, \dots, g_n\}.$$

Если a — произвольный элемент из G , то в множестве

$$aG = \{ag_1, ag_2, \dots, ag_n\}$$

все элементы различны, поэтому $G = aG$. Элементы в G перестановочны, так что

$$ag_1 \cdot ag_2 \cdot \dots \cdot ag_n = g_1 \cdot g_2 \cdot \dots \cdot g_n.$$

Снова из перестановочности элементов получается:

$$a^n \cdot g_1 \cdot g_2 \cdot \dots \cdot g_n = g_1 \cdot g_2 \cdot \dots \cdot g_n.$$

Сократим на $g_1 \cdot g_2 \cdot \dots \cdot g_n$ и получим $a^n = e$, где e — единичный элемент группы¹.

В рассматриваемой ситуации группа $\langle \mathbb{Z}_m^*; \cdot \rangle$ абелева, порядок ее равен $\varphi(m)$, а элемент $[a]$ принадлежит этой группе, если число a взаимно просто с модулем m .

Это значит, что если числа a , m взаимно просты, то

$$[a]^{\varphi(m)} = [1]$$

или, что то же самое на языке сравнений, для любого a , взаимно простого с модулем m ,

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Этот факт в честь автора называют *теоремой Эйлера*².

Чтобы практически пользоваться теоремой Эйлера, нужно уметь вычислять функцию Эйлера. В некоторых случаях это сделать нетрудно.

Например, если число p простое, то $\varphi(p) = p - 1$.

Отметим, что взаимная простота чисел a и p — это то же самое, что p не делит a . Таким образом, получается частный случай теоремы Эйлера: *если число a не делится на простое p , то $a^{p-1} \equiv 1 \pmod{p}$* .

По имени автора последнее предложение называют *теоремой Ферма*³.

У Ферма есть еще одно, более знаменитое утверждение, вошедшее в историю науки как *Великая (или большая) теорема Ферма*. Из-за этого обстоятельства теорему Ферма — частный случай теоремы Эйлера — называют *малой теоремой Ферма*.

¹ Чуть позже увидим, что на самом деле этим свойством обладают не только абелевы, но и любые конечные группы.

² Этот факт (в другой формулировке) открыт Эйлером в 1760 г.; понятие функции Эйлера появилось лишь в 1763 г.

³ *Пьер Ферма* (1601—1665) — французский математик-любитель (юрист по профессии). Теорема о делимости $a^{p-1} - 1$ на p сформулирована им (без доказательства) в 1640 г.

Рассмотрим пример, связанный с пробелом в доказательстве бесконечности множества простых чисел вида $4n + 3$. Там использовалось утверждение о том, что число вида $a^2 + 1$ никогда не делится на простое $p = 4n + 3$. Понятно, что $p > 2$ и что a не делится на p .

Предположим, что утверждение о неделимости $a^2 + 1$ на p неверно, т. е. для некоторого числа a выполняется сравнение $a^2 \equiv -1 \pmod{p}$.

Возведем обе части сравнения в степень $\frac{p-1}{2}$:

$$(a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

По малой теореме Ферма

$$a^{p-1} \equiv 1 \pmod{p},$$

а число $\frac{p-1}{2}$ нечетное, следовательно,

$$1 \equiv -1 \pmod{p},$$

что невозможно.

Используя закон контрапозиции, малую теорему Ферма можно сформулировать в виде достаточного условия простоты числа: если существует такое число a , что p не делит ни a , ни $a^{p-1} - 1$, то p — простое.

Используя этот факт, можно установить, что число p простое, не получив ни одного собственного делителя числа a .

Впрочем, эту задачу (узнать, простое число a или составное) можно решить и другим способом, также не находя ни одного настоящего делителя этого числа.

Если число p простое, то кольцо $\langle \mathbb{Z}_p; \cdot \rangle$ является полем и его мультипликативная группа состоит в точности из $p - 1$ элементов.

Многочлен с коэффициентами из поля имеет корней не больше, чем степень этого многочлена. Это означает, в частности, что уравнение второй степени $X^2 = [1]$ имеет в поле \mathbb{Z}_p не более двух решений.

Эти решения видны непосредственно: $X_1 = [1]$, $X_2 = [-1]$. Следовательно, в мультипликативной группе \mathbb{Z}_p^* только два элемента ($[1]$ и $[-1]$) совпадают со своими обратными; значит, все остальные элементы из \mathbb{Z}_p^* можно разбить на пары взаимно обратных элементов. Произведение всех элементов из \mathbb{Z}_p^* в результате будет равно $[-1]$ (или, что то же самое, $[p - 1]$):

$$[1] \cdot [2] \cdot [3] \cdot \dots \cdot [p - 1] = [-1].$$

На языке сравнений это выглядит так: если p — простое число, то

$$(p - 1)! \equiv -1 \pmod{p}.$$

В то же время, если p составное, $p = ab$, где $1 < a < p$, то равенство

$$1 \cdot 2 \cdot \dots \cdot a \cdot \dots \cdot (ab-1) = -1 + ab$$

невозможно. Собирая все вместе, получаем необходимое и достаточное условие свойства «быть простым числом»: *целое число p тогда и только тогда является простым, когда*

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Автор Э. Варинг¹ назвал это свойство в честь своего ученика Дж. Вильсона² критерием Вильсона.

Заметим, что этот факт допускает простое обобщение. Пусть G — конечная группа, в которой каждый неединичный элемент не совпадает со своим обратным. Это значит, что в группе G нет элементов второго порядка:

$$x^2 = 1 \Leftrightarrow x^{-1} = x.$$

Тогда все неединичные элементы этой группы можно соединить в пары взаимно обратных. Если группа G абелева, то произведение всех элементов такой группы равно единице. Кроме того, возможность соединения неединичных элементов в пары означает, что если в группе нет элементов второго порядка, то порядок этой группы — нечетное число. Используя закон контрапозиции, тот же факт запишем иначе: *если порядок группы — четное число, то она содержит элемент второго порядка.*

Чтобы пользоваться теоремой Эйлера в самом общем случае (а не только для простых модулей), нужна формула для вычисления функции Эйлера. Получим эту формулу постепенно, используя каноническое представление натурального числа.

Обобщим сначала то, что уже есть: если p — простое число, то $\varphi(p) = p - 1$. Вместо простого числа возьмем теперь степень простого p^α .

В множестве чисел

$$1, 2, \dots, p, p+1, \dots, 2p, \dots, kp, kp+1, \dots, p^\alpha - 1, p^\alpha$$

содержится в точности $p^{\alpha-1}$ чисел, не взаимно простых с числом p^α , т. е. если p — простое число, то $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Образно выражаясь, в поисках формулы для $\varphi(m)$ нами уже пройден «атомарный» уровень (когда модуль — простое число) и «моле-

¹ Эдуард Варинг (Waring, 1734—1798) — английский математик, профессор Кембриджского университета (с 1760 г.).

² Джон Вильсон (Wilson, 1741—1793) — английский математик. Вильсон открыл этот критерий, а Варинг доказал и опубликовал его в работе «Алгебраические размышления» (1779).

кулярный» (когда модуль является степенью простого числа). Осталось связать все «молекулы числа» вместе.

Основой связки, естественно, является каноническая форма натурального числа. Точнее, каждое натуральное число a можно представить в каноническом виде:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n},$$

где p_i — различные простые числа. Особо подчеркнем, что степени различных простых чисел взаимно просты.

Функция f , определенная на множестве натуральных чисел, называется *мультипликативной*, если для любых взаимно простых a, b выполняется равенство

$$f(a \cdot b) = f(a) \cdot f(b).$$

Доказав, что функция Эйлера мультипликативная, мы тем самым свяжем наши результаты об отдельных $\varphi(p^\alpha)$ в единое целое.

Итак, сейчас главная цель — показать, что функция Эйлера мультипликативная.

Для начала заметим, что если числа a, b взаимно просты, то кольцо классов вычетов \mathbb{Z}_{ab} является прямым произведением колец \mathbb{Z}_a и \mathbb{Z}_b .

Действительно, множество элементов $[x]$, где x кратно a , образует подкольцо B в кольце \mathbb{Z}_{ab} , изоморфное кольцу \mathbb{Z}_b . Аналогично множество элементов $[y]$, где y кратно b , образует подкольцо A в \mathbb{Z}_{ab} , изоморфное кольцу \mathbb{Z}_a . Пересечение подколец A и B содержит только нулевой элемент, произведение любых ненулевых элементов, взятых из разных подколец, равно нулю. Наконец, каждый элемент из \mathbb{Z}_{ab} можно представить в виде суммы $a + b$, где $a \in A$ и $b \in B$. Все это означает, что кольцо \mathbb{Z}_{ab} изоморфно прямому произведению $A \times B$.

Обратимые элементы прямого произведения колец получают-ся из обратимых элементов колец-сомножителей. Следовательно, если K_1 и K_2 — два ассоциативных кольца с единицами, а K_1^*, K_2^* — их мультипликативные группы, то

$$(K_1 \times K_2)^* = K_1^* \times K_2^*.$$

В частности, если K_1 и K_2 — два ассоциативных кольца с единицами, то

$$|(K_1 \times K_2)^*| = |K_1^*| \times |K_2^*|.$$

Для нашего кольца классов вычетов последнее замечание означает, что если $m = ab$ и числа a, b взаимно просты, то

$$|\mathbb{Z}_m^*| = |\mathbb{Z}_a^*| \times |\mathbb{Z}_b^*|.$$

С использованием обозначения функции Эйлера последнее равенство помогает получить желаемое: *функция Эйлера $\varphi(m)$ мультипликативна*.

По индукции мультипликативное свойство можно распространить на любое число сомножителей. Таким образом, получается формула для вычисления функции Эйлера:

$$\varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \dots (p_n^{\alpha_n} - p_n^{\alpha_n-1}).$$

Эту формулу можно представить в более короткой записи, не выписывая явно каноническую форму числа m , а лишь упомянув простые делители p этого числа:

$$\varphi(m) = m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right).$$

Эта формула уже достаточно удобна для вычислений.

Несмотря на наличие формулы, свойства функции Эйлера до сих пор остаются загадочными. Например, до сих пор неизвестно: верно ли, что каждое свое значение функция Эйлера принимает не менее двух раз¹. Иначе говоря, верно ли, что для каждого натурального n , если уравнение $\varphi(x) = n$ имеет решение, то таких решений больше одного?

Пока что обсуждались вопросы, связанные с изучением внутреннего устройства самого объекта — кольца класса вычетов. Рассмотрим какую-нибудь конкретную задачу.

Одна из самых первых задач, изучаемых в школьном курсе математики, — это задача о решении уравнений. Естественно, что такая задача начинается с обсуждения самых простых уравнений — линейных с одним неизвестным, т. е. уравнений вида $ax = b$.

Исследованию и решению такого уравнения в школьном курсе математики существенно благоприятствует то обстоятельство, что множество, на котором происходит действие, является полем. Это значит, что каждый ненулевой элемент a является обратимым. Поэтому если $a \neq 0$, то $a^{-1}b$ — единственное решение уравнения $ax = b$.

Эти рассуждения дословно переносятся на любое поле, в том числе и на поле \mathbb{Z}_p классов вычетов по простому модулю.

Однако в кольце \mathbb{Z}_m классов вычетов по составному модулю уже не каждый ненулевой элемент обратим, поэтому приходится ожидать ухудшения ситуации с решением даже этого простейшего уравнения. Эти пессимистические ожидания действительно оправдываются.

¹ Вопрос получил известность как *гипотеза Кармайкла*. Роберт Даниэль Кармайкл (1879—1967) — американский математик.

3.6. Вычисления в гомоморфных образах

Уравнение $[a][x] = [b]$, где $[a]$, $[b]$ принадлежат кольцу \mathbb{Z}_m , а $[x]$ — неизвестный класс вычетов, удобнее записать в виде сравнения с неизвестным x :

$$ax \equiv b \pmod{m}. \quad (*)$$

Если x_0 удовлетворяет этому сравнению, то и все элементы из смежного класса $[x_0]$ — тоже решения сравнения (*).

Иначе говоря, множество решений сравнения (*) — это подмножество множества целых чисел. Это множество решений распадается на несколько смежных классов по модулю m .

Числом различных решений сравнения (*), естественно, называют число различных классов вычетов по модулю m .

Если элемент $[a]$ обратим, т. е. $(a, m) = 1$, то сравнение (*) имеет единственное решение. Действительно, если число c такое, что $ac \equiv 1 \pmod{m}$, то

$$x \equiv cb \pmod{m}$$

есть единственное решение сравнения (*).

Предположим, что $[a]$ — необратимый элемент, т. е. $(a, m) = d > 1$.

Пусть x_0 — решение сравнения (*). Тогда

$$ax_0 \equiv b \pmod{m},$$

т. е. $ax = b + mk$ для некоторого целого k . Из делимости на d чисел a и m следует делимость на d числа b . Это значит, что необходимым условием разрешимости сравнения

$$ax \equiv b \pmod{m}$$

является делимость $(a, m) \mid b$.

Этого условия достаточно для существования решения. Действительно, пусть $d = (a, m)$, тогда $a = da_1$, $m = dm_1$ и $(a_1, m_1) = 1$. Если $b = db_1$, то сравнения

$$ax \equiv b \pmod{m} \text{ и } a_1x \equiv b_1 \pmod{m_1}$$

равносильны на множество целых чисел, их множества решений как подмножества из \mathbb{Z} совпадают. О втором сравнении уже известно, что оно всегда имеет единственное решение по модулю m_1 .

Итак, необходимым и достаточным условием разрешимости сравнения

$$ax \equiv b \pmod{m}$$

является делимость числа b на число (a, m) .

Задача о множестве решений сравнения была поставлена для кольца Z_m , но ответ, вообще говоря, появляется в другом кольце — Z_{m_1} . Поэтому для окончательного решения вопроса необходимо выяснить, какая связь существует между смежными классами по модулю m и по модулю m_1 .

Обозначим смежный класс по модулю m символом $[x]$, а смежный класс по модулю m_1 — символом \bar{y} . Тогда для каждого i, j из множества $0, 1, \dots, d-1$ и каждого целого k выполняются условия:

- 1) $[k + im_1] \subset \bar{k}$;
- 2) $[k + im_1] \neq [k + jm_1]$, если $i \neq j$;
- 3) $\prod_{i=1}^{d-1} (k + jm_i) = k$.

Эти три свойства означают, что любой класс вычетов по модулю m_1 распадается в точности на d классов по модулю m .

Теперь мы можем точно ответить на вопрос не только о разрешимости линейного сравнения с одним неизвестным, но и о числе решений, причем в исходном кольце классов вычетов.

Сравнение $ax \equiv b \pmod{m}$, где $(a, m) = d$, имеет d решений по модулю m , если d делит b , и не имеет решений, если d не делит b .

Как найти решение сравнения?

Кроме простого перебора вариантов, уместного лишь для небольших модулей, можно воспользоваться для первоначальной записи решения теоремой Эйлера. Действительно, числа a и m при поиске решения сравнения можно считать взаимно простыми. Но тогда по теореме Эйлера

$$a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m}$$

и отсюда получается решение сравнения $ax \equiv b \pmod{m}$:

$$x \equiv a^{\varphi(m)-1} \cdot b \pmod{m}.$$

Такая запись решения выглядит непривлекательно, да и возведение в степень быстро приводит к очень большим числам. Впрочем, эту степень можно найти, выполняя все вычисления в кольце классов вычетов, заменяя каждый промежуточный результат вычислений на остаток при делении его на m .

Вполне очевидно, что трудоемкость нахождения решения сравнения (не обязательно первой степени) связана с величиной модуля. Впрочем, если модуль является произведением взаимно простых чисел, то большую задачу можно разбить на несколько мелких. Сделать это можно с помощью так называемой *китайской теоремы об остатках*.

Заметим сначала, что НОК взаимно простых чисел равно их произведению. Иначе говоря, если $m = m_1 m_2$ и $(m_1, m_2) = 1$, то для каждого целого числа a

$$m \mid a \Leftrightarrow m_1 \mid a \text{ и } m_2 \mid a.$$

Это означает, в частности, что сравнение

$$ax \equiv b(\bmod m)$$

равносильно системе сравнений

$$\begin{cases} ax \equiv b(\bmod m_1); \\ ax \equiv b(\bmod m_2). \end{cases}$$

Пусть теперь число $m = m_1 m_2 \dots m_n$, причем множители m_i попарно взаимно просты. Тогда сравнение

$$ax \equiv b(\bmod m)$$

равносильно системе сравнений

$$\begin{cases} ax \equiv b(\bmod m_1); \\ ax \equiv b(\bmod m_2); \\ \dots\dots\dots \\ ax \equiv b(\bmod m_n). \end{cases}$$

Если $(a, m) = 1$, то каждое из сравнений системы имеет решение (единственное по модулю m_i) и система равносильна следующей:

$$\begin{cases} x \equiv c_1(\bmod m_1); \\ x \equiv c_2(\bmod m_2); \\ \dots\dots\dots \\ x \equiv c_n(\bmod m_n). \end{cases} \quad (*)$$

Теперь задача состоит в том, чтобы снова собрать исходный модуль m . Эту сборку начнем с первых множителей m_1 и m_2 , т. е. возьмем два первых сравнения системы (*):

$$\begin{cases} x \equiv c_1(\bmod m_1); \\ x \equiv c_2(\bmod m_2). \end{cases}$$

Первое сравнение можно записать в виде равенства

$$x = c_1 + m_1 k,$$

где k — некоторое целое число. Подставив этот x во второе сравнение, получим

$$c_1 + m_1 k \equiv c_2(\bmod m_2),$$

что равносильно

$$m_1 k \equiv c_2 - c_1(\bmod m_2).$$

Это сравнение с неизвестным k имеет единственное решение по модулю m_2 ,

$$k \equiv k_0 \pmod{m_2},$$

откуда $k = k_0 + m_2 t$, где t — целое число. Получаем окончательное по модулю $m_1 m_2$ выражение для x :

$$x \equiv c_1 + m_1 k_0 \pmod{m_1 m_2}.$$

Полученное сравнение имеет такое же множество решение в множестве целых чисел, что и система, состоящая из двух первых сравнений из (*). Это значит, что первые два сравнения системы (*) можно заменить одним, множество системы от этого не изменится.

Индукцией по числу сравнений в системе получается следующее утверждение, вошедшее в историю математики как *китайская теорема об остатках*: если числа m_1, m_2, \dots, m_n попарно взаимно просты, то для любых целых чисел c_1, c_2, \dots, c_n система сравнений

$$\begin{cases} x \equiv c_1 \pmod{m_1}; \\ x \equiv c_2 \pmod{m_2}; \\ \dots\dots\dots \\ x \equiv c_n \pmod{m_n} \end{cases}$$

имеет единственное решение по модулю $m_1 \cdot m_2 \cdot \dots \cdot m_n$.

Китайская теорема означает, что задача «найти число, которое при делении на числа m_i дает соответственно остатки c_i » всегда имеет решение, если m_i попарно взаимно просты.

Из школьного курса математики известно, что группы $\langle \mathbf{R}; + \rangle$ и $\langle \mathbf{R}_+; \cdot \rangle$ изоморфны. А именно: отображение $f: \mathbf{R}_+ \rightarrow \mathbf{R}$, заданное правилом

$$f(x) = \log_a x,$$

является изоморфизмом ($a \neq 1, a > 0$).

Сохранение операции отображением \log_a записывается так:

$$\log_a (x \cdot y) = \log_a x + \log_a y.$$

С помощью этого изоморфизма задачу о положительных действительных числах, сформулированную на языке умножения, можно перевести на язык сложения (но уже на множестве всех действительных чисел).

Например, уравнение $x^n = a$ в мультипликативной группе $\langle \mathbf{R}_+; \cdot \rangle$ превращается в аддитивной группе $\langle \mathbf{R}; + \rangle$ в уравнение вида $nx = b$.

Аналогично перевод уравнения $a^x = c$ с мультипликативного языка на аддитивный дает уравнение $xa = d$.

На аддитивном языке уравнения выглядят (и внешний вид здесь не обманчив) гораздо доступнее по сравнению с соответствующими мультипликативными задачами. По существу, этот изоморфизм выглядит как неожиданный подарок природы для человеческой цивилизации.

Точно такой же подарок природа приготовила и в мультипликативной группе \mathbf{Z}_p^* кольца классов вычетов по простому модулю p .

Эта группа состоит из $p - 1$ элементов. Наиболее просто устроенная группа из k элементов — это циклическая группа порядка k . Оказывается, что группа $\langle \mathbf{Z}_p^*; \cdot \rangle$ именно такая, предельно простая по устройству. *Мультипликативная группа кольца классов вычетов по простому модулю циклическая.*

Обнаружил (и нестрого доказал в 1761 г.) этот замечательный факт Эйлер, а первое безупречное доказательство принадлежит Лежандру¹ (1830).

В действительности выполняется более сильное утверждение: конечная группа, состоящая из элементов поля, является циклической.

Доказательство. Пусть G — конечная подгруппа из некоторого поля P и порядок G равен n . Предположим, что a — элемент максимального порядка k из G . По определению порядка $k \leq n$.

Циклическость G означает, что $k = n$. Покажем, что $n \leq k$, и этим будет установлено требуемое равенство.

Пусть g — произвольный элемент из G и m — порядок этого элемента. Покажем, что m непременно делит k . Предположим, что это не так. Тогда, используя канонические разложения чисел m и k , можно представить эти числа в виде

$$m = m_1 m_2, \quad k = k_1 k_2,$$

где $(m_1, k_1) = 1$, а $[m, k] = m_2 k_2$. Но тогда элемент $a^{k_2} b^{m_2}$ имеет порядок, равный $[m, k]$, больший, чем k . Полученное противоречие означает, что порядок любого элемента из G делит максимальный порядок k . Следовательно, каждый элемент из G является корнем многочлена $x^k - 1$.

Теперь снова воспользуемся фактом того, что многочлен с коэффициентами из поля имеет корней не больше, чем его степень². В частности, многочлен $x^k - 1$, где 1 — единица поля P , имеет не более чем k корней, а значит, $n \leq k$, что и доказывает теорему Лежандра.

¹ Адриен-Мари Лежандр (Legendre, 1752—1833) — французский математик. В 1787 г. принял участие в вычислении длины дуги меридиана между Барселоной и Дюнкерком, сделанном для определения длины метра.

² Доказанным впервые также Лежандром.

Все циклические группы одинакового порядка изоморфны.

Аддитивная группа $\langle \mathbb{Z}_{p-1}; + \rangle$ кольца классов вычетов по модулю $p - 1$ является циклической порядка $p - 1$, и $\langle \mathbb{Z}_p^*; \cdot \rangle$ тоже состоит из $p - 1$ элементов.

Следовательно, группы $\langle \mathbb{Z}_{p-1}; + \rangle$ и $\langle \mathbb{Z}_p^*; \cdot \rangle$ изоморфны.

Порождающий элемент циклической группы называют еще *первообразным* элементом (или первообразным корнем). Для группы \mathbb{Z}_p^* первообразным элементом принято называть и число-представитель порождающего класса.

Циклическость группы $\langle \mathbb{Z}_p^*; \cdot \rangle$ означает, что по простому модулю p существует первообразный элемент, т. е. элемент, мультипликативный порядок которого равен в точности $p - 1$.

Чтобы пожинать плоды изоморфизма между мультипликативной группой \mathbb{Z}_p^* и аддитивной группой \mathbb{Z}_{p-1} , нам следует ввести понятие, аналогичное школьным *логарифмам*.

Впрочем, ситуация сейчас существенно проще, чем с логарифмами, изучаемыми в школе. Там логарифмы были определены на бесконечном (континуальном), непрерывном множестве. Наше множество конечное, поэтому в нем нет непрерывности — оно дискретное и логарифмы в нем тоже дискретные.

Элементами изоморфных групп $\langle \mathbb{Z}_{p-1}; + \rangle$ и $\langle \mathbb{Z}_p^*; \cdot \rangle$ являются смежные классы вычетов по различным модулям. Чтобы их различать, смежный класс по модулю p с представителем x обозначим символом $[x]$, а смежный класс по модулю $p - 1$ с тем же самым представителем обозначим символом \bar{x} .

Если g — первообразный элемент в \mathbb{Z}_p^* , то

$$\mathbb{Z}_p^* = \{[g]^0, [g]^1, [g]^2, \dots, [g]^{p-2}\}.$$

В свою очередь,

$$\mathbb{Z}_{p-1} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-2}\}.$$

Отображение

$$f([g]^i) = \bar{i}$$

изоморфно отображает первую группу на вторую.

Пусть теперь элемент $[a]$ принадлежит группе \mathbb{Z}_p^* , т. е. p не делит a . Тогда для некоторого числа i выполняется равенство

$$[a] = [g]^i.$$

Число i в этом равенстве называют *индексом* числа a при основании g по модулю p и пишут:

$$i = \text{ind}_g a.$$

Таким образом, отображение $f: \mathbb{Z}_p^* \rightarrow \mathbb{Z}_{p-1}$ переписывается в виде

$$f([a]) = \text{ind}_g a,$$

т. е. отображение f построено точно так же, как и упомянутый ранее изоморфизм между мультипликативной группой положительных действительных чисел и аддитивной группой всех действительных чисел.

На языке сравнений изоморфизм f означает, что если p — простое число, а g — первообразный корень по модулю p , то для любых a, b , взаимно простых с p ,

$$a \equiv b(\text{mod } p) \Leftrightarrow \text{ind}_g a \equiv \text{ind}_g b(\text{mod } p-1).$$

Если p — простое число, g — первообразный корень по модулю p , то для любых целых чисел a, b , взаимно простых с числом p , выполняется сравнимость:

$$\text{ind}_g(a \cdot b) \equiv \text{ind}_g a + \text{ind}_g b(\text{mod } p-1).$$

Индукцией по n последнее свойство обобщается на натуральную степень: если p — простое число, а g — первообразный корень по модулю p , то для любого целого числа a , взаимно простого с p , и любого целого неотрицательного числа n :

$$\text{ind}_g a^n \equiv n \cdot \text{ind}_g a(\text{mod } p-1).$$

Теперь, как и для логарифмов, с помощью индексов поиск решения сравнений

$$x^n \equiv a(\text{mod } p), \quad a^x \equiv b(\text{mod } p)$$

сводится к решению некоторых *линейных* сравнений по модулю $p-1$.

Для такого перехода нужна таблица, аналогичная таблице логарифмов, — *таблица индексов* (для обратного перевода, соответственно, *таблица антииндексов*).

В отличие от настоящих логарифмов, для которых поиск основания — не проблема, для дискретных, «игрушечных» логарифмов (индексов) сначала нужно найти основание — первообразный элемент.

Впервые таблицы индексов для простых чисел, меньших 1000, были опубликованы в 1839 г. В честь своего создателя они называются *таблицами Якоби*¹.

¹ Якоб Карл Густав Якоби (Jacobi, 1804—1851) — немецкий математик, иностранный член-корреспондент (1830) и иностранный почетный член (1833) Петербургской Академии наук.

Для поиска первообразного элемента вручную (или с помощью вычислительной техники) можно учесть следующее обстоятельство. Первообразный элемент g имеет порядок $p - 1$ в группе $\langle \mathbb{Z}_p^*; \cdot \rangle$. Порядок любого элемента из этой группы является делителем числа $p - 1$. Для нечетного простого p число $p - 1$ четно. Если порядок элемента g больше, чем $(p - 1) / 2$, то он точно равен $p - 1$.

В общем случае для произвольного модуля m картина не меняется: если порядок элемента g больше максимального собственного делителя числа $\varphi(m)$, то порядок g по модулю m равен $\varphi(m)$ и g — первообразный по модулю m . К сожалению, первообразный элемент для составного модуля может и не существовать, например: группа \mathbb{Z}_8^* , состоящая из четырех элементов, не содержит элементов четвертого порядка.

В то же время, если $m = m_1 m_2 \dots m_n$, где m_i попарно взаимно просты, то группа \mathbb{Z}_m^* распадается в прямое произведение:

$$\mathbb{Z}_m^* = \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \dots \times \mathbb{Z}_{m_n}^*.$$

На основе этого наблюдения иногда можно ответить на вопрос, для каких модулей первообразный элемент существует, а для каких нет? Например, $|\mathbb{Z}_2^*| = 1$, поэтому если p — простое нечетное число, то первообразный элемент по модулю $2p$ существует.

При этом если числа m и n не взаимно просты, то прямое произведение циклических групп порядков m и n не является циклической группой. Поэтому если числа a , b взаимно просты и нечетны, то первообразного элемента по модулю ab не существует.

Поскольку подгруппа циклической группы снова циклическая, предыдущее замечание означает, что если в каноническое разложение числа m входят по крайней мере два различных простых нечетных числа, то группа \mathbb{Z}_m^* — не циклическая.

Отметим, что если p — нечетное простое число, то группа $\mathbb{Z}_{p^k}^*$ тоже циклическая, а если $k > 2$, то группа $\mathbb{Z}_{2^k}^*$ — нециклическая.

Снова ссылаясь на то, что $|\mathbb{Z}_2^*| = 1$, получаем, что группа $\mathbb{Z}_{2p^k}^*$ тоже циклическая.

Непосредственно проверкой можно убедиться, что группа \mathbb{Z}_4^* циклическая.

Таким образом, группа $\langle \mathbb{Z}_m^*; \cdot \rangle$ является циклической тогда и только тогда, когда $m \in \{2, 4, p^k, 2p^k\}$, где $k \geq 1$.

Отметим, наконец, что, несмотря на многолетние (и даже многовековые) исследования, свойства первообразных чисел по простому модулю остаются загадочными. Например, до сих пор неизвестно, является ли каждое простое число p первообразным элементом по бесконечному числу простых модулей.

Более того, нет ответа на этот вопрос даже для числа $p = 2$.

Вернемся снова к уравнениям в кольце классов вычетов.

В школьном курсе математики, кроме линейных, неплохо представлены и квадратные уравнения. А что можно сказать о квадратных уравнениях над полем \mathbb{Z}_p ?

Квадратное уравнение в поле \mathbb{Z}_p имеет вид

$$[a]X^2 + [b]X + [c] = [0],$$

где X — неизвестный класс вычетов.

Все сведения из школьного курса математики о корнях многочлена второй степени полностью применимы в этой ситуации: и формулы Виета остаются верными, и нахождение корней многочлена через дискриминант тоже остается в силе.

Это значит, что формула

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

для нахождения корней квадратного уравнения

$$ax^2 + bx + c = 0$$

верна для любого поля, в том числе и для конечного.

Необходимы лишь договоренности о формах записи. Во-первых, в кольце \mathbb{Z}_p не говорят о делении и об обратном элементе и не пишут a^{-1} . Вместо деления говорят о решении линейного сравнения, в частности вместо a^{-1} речь идет о решении сравнения

$$ax \equiv 1 \pmod{p}.$$

Во-вторых, вместо записи \sqrt{d} также придется говорить о решении сравнения

$$x^2 \equiv d \pmod{p}. \quad (*)$$

Понятно, что случай $d = 0$ тривиальный, поэтому по умолчанию при обсуждении решения сравнения вида (*) имеют в виду ненулевой элемент d .

Пусть d — ненулевой элемент поля \mathbb{Z}_p . Если сравнение (*) имеет решение в поле \mathbb{Z}_p , то d называют *квадратичным вычетом* по модулю p . Если не существует такого элемента c , что $d = c^2$, то элемент d называется *квадратичным невычетом*.

В поле \mathbb{Z}_2 всего один ненулевой элемент, он является квадратичным вычетом.

Если d — квадратичный вычет по модулю p , то символически записывают

$$\left(\frac{d}{p}\right) = 1,$$

а если d — невычет, то пишут

$$\left(\frac{d}{p}\right) = -1.$$

При фиксированном p символ $\left(\frac{d}{p}\right)$ изображает функцию, определенную на \mathbf{Z}_p^* , со значениями в множестве $\{1, -1\}$. По имени автора эту функцию называют *символом Лежандра*.

Иногда удобно при записи функции «символ Лежандра» использовать обычную функциональную символику, причем определяя ее на всем множестве \mathbf{Z}_p . Определение тогда имеет следующий вид.

Символом Лежандра называется функция χ , определенная в поле \mathbf{Z}_p со значениями в множестве $\{1, -1\}$ по правилу $\chi(0) = 0$ и

$$\chi(x) = \begin{cases} 1, & \text{если } x \text{ — квадратичный вычет,} \\ -1, & \text{если } x \text{ — квадратичный невычет.} \end{cases}$$

Впрочем, символ χ удобно использовать лишь в том случае, когда модуль зафиксирован; если же в утверждении появятся два модуля, то придется воспользоваться первой символикой.

Случай двухэлементного поля слишком прост, к тому же число 2 — «монстр» среди простых чисел: это единственное четное простое число. Эта четность часто мешает при формулировке общих утверждений о простых числах. Поэтому будем считать по умолчанию, что $p > 2$.

Пусть p — нечетное простое число. Если g — порождающий элемент мультипликативной группы ненулевых элементов поля \mathbf{Z}_p , то каждый ненулевой элемент этого поля имеет вид g^k . Сравнение

$$2x \equiv k \pmod{p}$$

имеет решение тогда и только тогда, когда число k четное. Это значит, что четные степени порождающего элемента являются квадратичными вычетами, а нечетные степени — квадратичными невычетами.

Таким образом, в поле \mathbf{Z}_p содержится $\frac{p-1}{2}$ квадратичных вычетов и ровно столько же квадратичных невычетов.

Единичный элемент — квадратичный вычет в любом поле, поэтому $\chi(1) = 1$.

Сумма четных чисел снова четная, а сумма четного и нечетного — нечетная (а произведение нуля с любым элементом поля — нулевой элемент). Следовательно, для любых a, b из \mathbf{Z}_p

$$\chi(ab) = \chi(a)\chi(b).$$

Таким образом, отображение χ сохраняет операцию умножения, т. е. является гомоморфизмом мультипликативной полугруппы $\langle \mathbb{Z}_p; \cdot \rangle$ на полугруппу $\langle \{0, 1, -1\}; \cdot \rangle$.

Очевидной индукцией число множителей можно увеличить до любого натурального n :

$$\chi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}) = \chi(p_1^{\alpha_1}) \chi(p_2^{\alpha_2}) \dots \chi(p_n^{\alpha_n}) = \chi(p_1)^{\alpha_1} \chi(p_2)^{\alpha_2} \dots \chi(p_n)^{\alpha_n}.$$

Поскольку квадрат целого числа является квадратичным вычетом, все показатели степеней α_i можно заменить остатками от деления α_i на два.

Отметим еще, что если $p > 2$, то квадратичных вычетов в точности столько же, сколько и квадратичных невычетов, поэтому

$$\sum_{a \in \mathbb{Z}_p} \chi(a) = 0.$$

Если $p > 2$, то $p - 1$ — четное число. Пусть d не делится на p . Тогда

$$d^{p-1} - 1 = \left(d^{\frac{p-1}{2}} - 1 \right) \left(d^{\frac{p-1}{2}} + 1 \right) \equiv 0 \pmod{p}.$$

Но в поле нет делителей нуля, следовательно, один или оба множителя должны быть нулевыми.

Если

$$d^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}, \quad d^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p},$$

то $-1 \equiv 1 \pmod{p}$ и $p = 2$. Таким образом, один и только один из этих множителей нулевой.

Заметим, что d является квадратичным вычетом тогда и только тогда, когда d — четная степень порождающего элемента g . Это значит, что

$$d \equiv g^k \pmod{p},$$

где k — четное.

Возведем левую и правую части этого сравнения в степень $\frac{p-1}{2}$ и получим:

$$d^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Таким образом,

$$d^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$$

тогда и только тогда, когда d — квадратичный вычет.

Соответственно, второй множитель будет нулевым,

$$d^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p},$$

тогда и только тогда, когда d — квадратичный невычет.

Итак,

$$d = \begin{cases} 1 \pmod{p}, & \text{если } x \text{ — квадратичный вычет,} \\ -1 \pmod{p}, & \text{если } x \text{ — квадратичный невычет.} \end{cases}$$

Это же можно записать короче (и эффектнее):

$$\chi(d) \equiv d^{\frac{p-1}{2}} \pmod{p},$$

или в другом обозначении:

$$\left(\frac{d}{p}\right) \equiv d^{\frac{p-1}{2}} \pmod{p}.$$

Это свойство функции χ называется *критерием Эйлера*¹. Критерий Эйлера дает новое доказательство того, что отображение χ сохраняет умножение.

Для $d = -1$ сравнение можно заменить равенством

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}.$$

Заметим: отсюда, следует, что -1 является квадратичным вычетом по модулю p (т. е. $a^2 + 1$ делится на p) тогда и только тогда, когда p имеет вид $4t + 1$. В частности, появляется утверждение, полученное сразу после доказательства малой теоремы Ферма: *при любом a число $a^2 + 1$ не делится на простое $p = 4t + 3$.*

Вычислить символ Лежандра можно вручную, критерий Эйлера и полная мультипликативность символа Лежандра значительно облегчают выкладки.

Однако ручные вычисления значительно ускоряются, если воспользоваться *законом квадратичной взаимности*: для различных нечетных простых p, q

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Нестрогие доказательства закона взаимности были получены Эйлером и Лежандром, первое безупречное доказательство было предложено Гауссом (1801).

¹ Открыто Леонардом Эйлером в 1755 г.

По квадратичному закону взаимности

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Применим закон квадратичной взаимности для вычисления $\left(\frac{-3}{p}\right)$, где p — простое число вида $6n + 5$. Сначала выделим множитель -1 :

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right).$$

По формуле Эйлера

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{6n+5-1}{2}} = (-1)^{3n+2} = -1.$$

Таким образом,

$$\begin{aligned} \left(\frac{-3}{p}\right) &= -\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} = -\left(\frac{6n+5}{3}\right) (-1)^{\frac{6n+5-1}{2} \cdot \frac{3-1}{2}} = \\ &= -\left(\frac{-1}{3}\right) (-1)^{3n+2} = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1. \end{aligned}$$

Итак, $\left(\frac{-3}{p}\right) = -1$, а это значит, что при любом целом a число $a^2 + 3$

не делится на простое вида $p = 6n + 5$. Отсюда, в частности, следует, что в прогрессии $6x + 5$ содержится бесконечно много простых чисел.

В заключение кратко рассмотрим примеры задач о целых числах, решение которых сводится к вычислениям в гомоморфных образах, т. е. в кольцах классов вычетов.

Арифметические приложения теории сравнений — это переформулировка задачи о целых числах на язык кольца классов вычетов и решение этой задачи в гомоморфном образе кольца \mathbb{Z} .

Например, вычислить остаток от деления на m в кольце целых чисел на языке кольца вычетов \mathbb{Z}_m — это задача о выяснении, какой именно элемент представляет данное целое число. Алгоритм нахождения остатка от деления на m , не находя частного, принято называть *признаком делимости*. Таким образом, признак делимости на m лучше получить в кольце классов вычетов по модулю m .

Аналогичным образом можно разыскивать решения неопределенного уравнения, искать остаток от деления на m конкретного, но очень большого числа; можно проверить арифметические действия, перейдя в гомоморфный образ, и, наконец, вычислить длину периода систематической дроби, не вычисляя цифр этого периода.

Отметим, что после описания множества решений линейного неопределенного уравнения появится возможность получить описание подполугрупп аддитивной полугруппы натуральных чисел.

Начнем, впрочем, с простой задачи, декларативное (т. е. бездоказательное) решение которой известно даже школьникам средних классов.

Нахождение остатка от деления на число m без вычисления частного может основываться на систематической записи числа.

Пусть

$$a = a_n g^n + a_{n-1} g^{n-1} + \dots + a_1 g + a_0 —$$

запись числа a в g -ичной системе счисления. Сравнимость по модулю m является конгруэнцией на \mathbb{Z} , поэтому вместо степеней g можно поставить любые числа, сравнимые с этими степенями — остаток от деления числа a на число m не изменится. Точнее говоря, для любого целого числа $g > 1$ если $g^i \equiv b_i \pmod{m}$, $i = 1, 2, \dots, n$, то

$$a_n g^n + a_{n-1} g^{n-1} + \dots + a_1 g + a_0 \equiv a_n b_n + a_{n-1} b_{n-1} + \dots + a_1 b_1 + a_0 \pmod{m}.$$

Число g здесь произвольное целое, большее единицы, как и произвольное m . По этой причине сформулированный признак делимости называют *обобщенным признаком делимости Паскаля*¹. Обобщенный признак Паскаля для небольших чисел m дает обычные школьные признаки делимости (а точнее равноостаточности, так как, применяя признак Паскаля, мы не только узнаем, делится ли число на m , но и какой остаток получится при этом делении).

Например, поскольку $10^i \equiv 0 \pmod{2}$, получаем, что при делении на 2 число дает такой же остаток, что и его последняя цифра при делении на 2.

Точно так же $10^i \equiv 0 \pmod{5}$, поэтому при делении на 5 число дает такой же остаток, что и его последняя цифра при делении на 5.

Поскольку $10^i \equiv 0 \pmod{4}$ для $i > 1$, получаем, что при делении на 4 число дает такой же остаток, что и число, изображенное его последними двумя цифрами.

Из сравнения $10^i \equiv 0 \pmod{8}$ для $i > 2$ соответственно получаем свойство восьмерки: при делении на 8 число дает такой же остаток, что и число, изображенное его последними тремя цифрами.

Поскольку $10^i \equiv 1 \pmod{3}$ и $10^i \equiv 1 \pmod{9}$, получаем известные из школы признаки делимости на 3 и на 9: число при делении на 3 (на 9) дает такой же остаток, что и сумма его цифр.

¹ Блез Паскаль (Pascal, 1623—1662) — французский математик, физик, религиозный философ и писатель. Обобщенный признак делимости найден Паскалем в 1654 г.

В обобщенном признаке делимости Паскаля иногда удобнее использовать не наименьшие неотрицательные, а абсолютно наименьшие (т. е. наименьшие по модулю) вычеты по модулю m .

Например, при $m = 11$ имеем

$$10^i \equiv (-1)^i \pmod{11},$$

поэтому при делении на 11 число дает такой же остаток, что и его знакопеременная сумма цифр.

Диофантово уравнение первой степени с двумя неизвестными уже появилось в предыдущей теме. Там указан способ нахождения какого-нибудь конкретного решения такого уравнения и запись общего решения.

Использование сравнений дает другой подход к такой задаче. Сравнения позволяют найти новые способы получения решения, а главное — существенно облегчают переход от двух неизвестным к трем, от трех к четырем и т. д.

Сначала все же рассмотрим диофантово линейное уравнение с двумя неизвестными

$$ax + by = c. \quad (*)$$

Можно считать, что $(a, b) = 1$.

Это уравнение можно записать в виде сравнения

$$ax \equiv c \pmod{b}$$

и, таким образом, свести решение уравнения (*) с двумя неизвестными к решению уравнения

$$[a][x] = [c]$$

уже с одним неизвестным $[x]$ в кольце \mathbf{Z}_b . Элемент $[a]$ — обратимый в \mathbf{Z}_b . Если c делится на a , то найти решение сравнения можно простым делением. Может случиться, что a не делит c , но $(a, c) = d > 1$. Тогда $[d]$ — тоже обратимый в \mathbf{Z}_b элемент и на d можно делить левую и правую части сравнения. После цепочки таких упрощений получим значение неизвестного класса $[x_0]$.

Для небольшого b сравнение с одной неизвестной можно решить простым перебором полной системы вычетов по модулю b или воспользоваться теоремой Эйлера.

Найдя значение x_0 , и подставив его в уравнение (*), можно найти y_0 . После этого можно воспользоваться общей формулой решений уравнения (*) и написать все множество решений.

Вообще говоря, эти задачи (решение неопределенного уравнения с двумя переменными и решение сравнения с одной переменной) очень взаимосвязаны. Иногда, наоборот, целесообразно при

решении уравнения (*) заменить свободный член c на единицу и решить сначала вспомогательное уравнение $ax + by = 1$ с помощью цепных дробей.

Увеличим теперь число неизвестных в неопределенном уравнении до трех. Пусть

$$ax + by + cz = d —$$

уравнение, в котором все коэффициенты — ненулевые целые числа.

Если (a, b, c) не делит d , то уравнение не имеет решения.

Если (a, b, c) делит d , то уравнение всегда имеет решение. Сократив, если требуется, левую и правую части уравнения на (a, b, c) , получим уравнение со взаимно простыми в совокупности коэффициентами. Можно считать, что уже $(a, b, c) = 1$.

Возникают следующие случаи:

- 1) по крайней мере два коэффициента из a, b, c взаимно просты;
- 2) все коэффициенты a, b, c попарно не взаимно просты.

Разберем каждый случай отдельно.

Первый случай. Пусть $(a, b) = 1$. Тогда уравнение

$$ax + by = d - cz$$

имеет решение при любом z .

Если $(x_0(z) + bt, y_0(z) - at)$ — конкретное решение этого сравнения, то

$$\{(x_0 + bt, y_0 - at, z) | t \in \mathbb{Z}\} —$$

множество решений исходного уравнения.

Второй случай. Пусть все пары a, b, c не взаимно просты и $k = (a, b)$.

Введем обозначения: $a_1 = \frac{a}{k}, b_1 = \frac{b}{k}$. Исходное уравнение принимает вид

$$ka_1x + kb_1y + cz = d,$$

что равносильно уравнению

$$ka_1x + kb_1y = d - cz,$$

Здесь $(a_1, b_1) = 1$. Это уравнение имеет решение тогда и только тогда, когда $d - cz$ делится на k , т. е. когда

$$d - cz \equiv 0 \pmod{k}. \quad (**)$$

По условию $(a, b, c) = 1$, поэтому $(c, k) = 1$. Следовательно, сравнение (**) будет иметь единственное решение по модулю k .

Если z_0 — число, удовлетворяющее сравнению (**), то $\{z_0 + kt \mid k \in \mathbb{Z}\}$ — все множество решений сравнения (**).

Теперь решение исходного уравнения сводится к решению заведомо совместного уравнения с двумя неизвестными x, y :

$$a_1x + b_1y = \frac{d - c(z_0 + kt)}{k}.$$

Решая его, получим $x = f(t), y = g(t)$, где f и g — многочлены первой степени от целого t . Множеством его решений является

$$\{(f(t), g(t), z_0 + kt) \mid t \in \mathbb{Z}\}.$$

Геометрический смысл решения следующий. Множество решений — это все точки с целыми координатами, попавшие на график плоскости

$$ax + by + cz = d.$$

Снова можно указать векторы с целочисленными координатами, порождающие эту плоскость как двумерное подпространство, и вектор сдвига, также имеющий целые координаты.

Векторы, порождающие плоскость,

$$ax + by + cz = 0,$$

зависят только от a, b, c . Поэтому, сдвинув параллельно эту плоскость, получим, что, начиная с некоторого числа d , для d и всех чисел, больших d , исходное уравнение имеет решение в *целых неотрицательных числах*.

Таким образом, если a, b, c положительные и $(a, b, c) = k > 1$, то уравнение

$$ax + by + cz = d$$

имеет решение для всех чисел d , кратных k и превышающих некоторое число m .

Аналогичным образом с помощью сравнений осуществляется переход от n неизвестных к $n + 1$ неизвестному. Обнаруженное свойство множества решений уравнения сохранится и при n неизвестных. Следовательно, уравнение

$$m_1x_1 + m_2x_2 + \dots + m_sx_s = c,$$

где $m_i \neq 0$ и $(m_1, m_2, \dots, m_s) = k$, имеет решение в целых неотрицательных числах для всех достаточно больших чисел c , кратных числу k .

Используем это свойство линейных неопределенных уравнений для описания подмоноидов моноида $\langle \mathbb{Z}_0; + \rangle$.

Напомним сначала об употреблении слов «почти все».

Говорят, что в счетном множестве *почти все* элементы обладают некоторым свойством, если множество элементов, не обладающих этим свойством, конечно.

Множество M из \mathbb{Z}_0 образует подмоноид в $\langle \mathbb{Z}_0; + \rangle$, если оно содержит нулевой элемент и замкнуто относительно сложения, т. е. $M < \mathbb{Z}_0$ тогда и только тогда, когда $0 \in M$ и

$$x, y \in M \Rightarrow x + y \in M.$$

Покажем, что подмоноид M почти весь состоит из кратных некоторого числа d .

Для доказательства рассмотрим три случая.

Случай 1. Множество M состоит из одного нуля. Тогда

$$M = \{0 \cdot k \mid k \in \mathbb{Z}_0\}.$$

Случай 2. Множество M состоит не из одного нуля, но в M содержится конечное подмножество, состоящее из взаимно простых чисел.

Пусть $m_i \in M$, $i = 1, 2, \dots, s$ и $(m_1, m_2, \dots, m_s) = 1$. Тогда для каждого достаточно большого целого числа c уравнение

$$m_1 x_1 + m_2 x_2 + \dots + m_s x_s = c$$

имеет решение в целых неотрицательных числах. Следовательно, M — это почти все множество \mathbb{Z}_0 .

Случай 3. Множество M состоит не из одного нуля, но любой конечный набор элементов из M не взаимно прост.

Покажем существование такого числа d , что M почти совпадает с множеством $\{d \cdot k \mid k \in \mathbb{Z}_0\}$. Выберем в множестве M наименьший положительный элемент m_1 и рассмотрим множество

$$M_1 = \{m_1 \cdot k \mid k \in \mathbb{Z}_0\}$$

всех кратных этого элемента.

Если $M_1 = M$, то все доказано.

Пусть $M \neq M_1$ и m_2 — наименьший положительный элемент из $M \setminus M_1$. Пусть

$$M_2 = \{m_2 \cdot k \mid k \in \mathbb{Z}_0\}.$$

Предположим, что $M = M_1 \cup M_2$. Тогда каждый элемент из M можно представить в виде $m_1 u + m_2 v$, где u, v — целые неотрицательные числа.

Если d — наибольший общий делитель чисел m_1, m_2 , то для всех достаточно больших c , делящихся на число d , уравнение

$$m_1 x_1 + m_2 x_2 = d$$

имеет решение в целых неотрицательных числах. Но это означает, что множество M почти совпадает с $\{d \cdot k \mid k \in \mathbb{Z}_0\}$.

Рассмотрим ситуацию, когда $M \neq M_1 \cup M_2$.

Пусть тогда $M_3 = M \setminus (M_1 \cup M_2)$, а m_3 — наименьшее положительное число из M_3 . Предположим, что $M \neq M_1 \cup M_2 \cup M_3$, и рассуждаем как раньше.

Продолжим и далее этот процесс, и пусть

$$M_k = M \setminus (M_1 \cup M_2 \cup \dots \cup M_{k-1}),$$

где $M_i = \{m_i \cdot k \mid k \in \mathbb{Z}_0\}$, а m_i — наименьшее положительное число из множества M_i .

Если d — наибольший общий делитель чисел m_i :

$$(m_1, m_2, \dots, m_k, \dots) = d,$$

то d имеет линейное разложение, в котором участвует конечное число чисел m_i . Точнее, для некоторого натурального s и целых u_i , $i = 1, 2, \dots, s$,

$$m_1 x_1 + m_2 x_2 + \dots + m_s x_s = d.$$

Тогда для всех достаточно больших c , кратных числу d , уравнение

$$m_1 x_1 + m_2 x_2 + \dots + m_s x_s = c$$

имеет решение в целых неотрицательных числах.

Это означает, что *каждый подмоноид моноида $\langle \mathbb{Z}_0; + \rangle$ почти совпадает с множеством кратных элемента d .*

Другими словами, все элементы из M , кроме конечного числа, делятся на d .

Это означает, что все подполугруппы в $\langle \mathbb{Z}_0; + \rangle$ тоже конечно порождены. Поэтому число различных подмоноидов в моноиде $\langle \mathbb{Z}_0; + \rangle$ всего лишь счетно, хотя множество $P(\mathbb{Z}_0)$ всех подмножеств множества \mathbb{Z}_0 несчетно.

Сам моноид $\langle \mathbb{Z}_0; + \rangle$ тоже конечно порожден (аддитивная полугруппа натуральных чисел даже однопорождена).

Зная порождающее множество подмоноида M , можно решить проблему вхождения в M , т. е. по единому алгоритму в конечное число шагов для любого натурального числа n выяснить, принадлежит n множеству M или нет.

Отметим, что мультипликативный моноид целых неотрицательных чисел бесконечно порожден (так как множество простых чисел бесконечно). Счетное множество содержит континуум подмножеств. Поэтому моноид $\langle \mathbb{Z}_0; \cdot \rangle$ содержит континуум различных подмоноидов.

Проблема вхождения в конечно порожденные подмоноиды моноида $\langle \mathbb{Z}_0; \cdot \rangle$ также разрешима. Однако можно алгоритмически

описать бесконечно порожденный подмоноид с неразрешимой проблемой вхождения. Для этого выберем рекурсивно перечислимое, но не рекурсивное множество простых чисел P . Тогда проблема вхождения в мультипликативный моноид, порожденный множеством P , алгоритмически неразрешима.

После этого общеалгебраического замечания вернемся вновь к применениям сравнений.

О другом применении кольца Z_m уже упоминалось при обсуждении теоремы Эйлера и малой теоремы Ферма. Речь идет о вычислении остатка от деления большой степени (или арифметического выражения, содержащего такие степени) на число m .

Используя вычисления в фактор-кольце Z_m , т. е. вычисления по модулю m , и теорему Эйлера, можно решить такую задачу нахождения остатка от деления на m , оставаясь в кольце Z_m .

Из того, что сравнимость является конгруэнцией, и из теоремы Эйлера следует, что если $(a, m) = 1$, то

$$a^b \equiv (\text{Rest}(a, m))^{\text{Rest}(b, \varphi(m))} \pmod{m}.$$

Таким образом, для вычисления остатка от деления на m сколь угодно большой степени числа, эту степень можно ограничить числом, не превышающим $\varphi(m) - 1$.

Случай не взаимно простых a и m с помощью деления левой и правой частей равенства (гарантированного теоремой о делении с остатком)

$$a^b = mq + r$$

на общий делитель (a, m) сводится к только что рассмотренному случаю, только искомым будет теперь число $\frac{r}{(a, m)}$.

Отметим еще одно из применений признаков делимости.

Любое равенство двух выражений

$$f(x_1, x_2, \dots, x_n) = g(x_1, x_2, \dots, x_n), \quad (***)$$

составленных из целых чисел x_i с помощью операций сложения, вычитания, умножения и возведения в степень, при гомоморфизме кольца Z в кольцо классов вычетов Z_m переходит в верное равенство

$$f([x_1], [x_2], \dots, [x_n]) = g([x_1], [x_2], \dots, [x_n])$$

в этом кольце.

Фактически в выражении может быть и деление, только все делители должны быть взаимно просты в кольце Z_m (тогда они попадут в мультипликативную группу этого кольца).

Таким образом, с помощью кольца классов вычетов Z_m мы можем проверить правильность выполнения арифметических действий.

Правда, ошибке при такой проверке, может быть, удастся скрыться: число, кратное модулю m , играет в Z_m роль нуля, а число $mk + 1$ — роль единицы.

Это значит, что равенство (***) может быть и неверным. Например, левая часть может отличаться от правой части слагаемым вида mk или множителем $mk + 1$. В кольце Z_m неверное равенство в Z превратится в верное равенство. Но если в Z_m равенство не выполняется, то (***) точно не выполняется.

Проще всего проделать проверку с помощью модуля 9 (или 11). Проверка равенства в Z_9 называется *правилом девятки*.

Предположим, что проверка с помощью правила девятки удалась. Это значит, что либо проверяемое равенство верно, либо его левая часть отличается на число, кратное девяти (или множителем $9k + 1$).

Вторая удачная проверка (например, с помощью кольца Z_{11}) этого же равенства делает истинность этого равенства еще более вероятной (хотя и не стопроцентной). В таком случае слагаемое, не портящее равенства, — это любое число, кратное 99, а множитель, также скрывающийся при переходе к гомоморфному образу, — это любое число вида $99k + 1$.

Последнее применение колец классов вычетов будет связано с обращением обыкновенной дроби в систематическую.

Пусть основание позиционной системы счисления равно g . Рассмотрим правильную несократимую дробь $\frac{a}{b}$, в которой знаменатель взаимно прост с основанием системы, т. е. $1 \leq a < b$, $(a, b) = 1$ и $(b, g) = 1$. Начнем обращать дробь $\frac{a}{b}$ в g -ичную, используя школьное правило деления «уголком»:

$$\begin{aligned} ga &= bq_1 + r_1; \\ gr_1 &= bq_2 + r_2; \\ gr_2 &= bq_3 + r_3; \\ &\dots\dots\dots \\ gr_{i-1} &= bq_i + r_i; \\ &\dots\dots\dots \end{aligned}$$

где $0 \leq r < b$. Из неравенств

$$a \geq bq_1 > 0 \text{ и } b > a$$

следует, что $g > q_1 \geq 0$ (и точно так же для остальных q_i).

Из этих равенств и получается представление для дроби $\frac{a}{b}$ —

$$\frac{a}{b} = \frac{q_1}{g} + \frac{q_2}{g^2} + \dots + \frac{q_i}{g^i} + \dots,$$

или в систематической записи

$$\frac{a}{b} = 0, q_1 q_2 \dots q_i \dots$$

Остатки r_i в равенствах, выражающих деления, отличны от нуля, они даже взаимно просты с числом b :

$$(b, r_1) = (ga, b) = 1;$$

$$(b, r_2) = (gr_1, b) = 1 \text{ и т. д.}$$

Следовательно, процесс деления никогда не оборвется и систематическая дробь, представляющая число $\frac{a}{b}$, бесконечна.

Различных остатков, взаимно простых с числом b , при делении на b может возникнуть не более чем $\varphi(b)$. Это значит, что наша дробь после обращения ее в систематическую является периодической и длина периода не превышает $\varphi(b)$.

Вычислим длину периода систематической дроби точно.

Запишем равенства, возникающие при делении, в виде сравнений:

$$ga \equiv r_1 \pmod{b};$$

$$gr_1 \equiv r_2 \pmod{b};$$

$$\dots\dots\dots$$

$$gr_{i-1} \equiv r_i \pmod{b};$$

$$\dots\dots\dots$$

и перемножим первые k сравнений. Получится сравнение

$$g^k r_1 r_2 \dots r_{k-1} \equiv r_1 r_2 \dots r_k \pmod{b}.$$

Сокращая на взаимно простые с модулем (а поэтому обратимые по модулю) числа r_i , получаем:

$$g^k a \equiv r_k \pmod{b}.$$

Теперь числа a и r_k сравнимы по модулю b тогда и только тогда, когда

$$g^k \equiv 1 \pmod{b}.$$

Поскольку $1 \leq a < b$ и $1 \leq r_i < b$, сравнимость $a \equiv r_k \pmod{b}$ равносильна равенству $a = r_k$.

Таким образом, для наименьшего числа k , для которого выполняется такое сравнение, k -й остаток *впервые* совпадает с числом a и начиная с этого момента *сформируется* период систематической дроби.

Иначе говоря, длина периода дроби $\frac{a}{b}$, где $1 \leq a < b$, $(a, b) = (g, b) = 1$, после обращения ее в g -ичную систематическую дробь равна порядку числа g по модулю b .

Ограничения, наложенные на числитель и знаменатель дроби, устранить легко. Если дробь неправильная, то можно выделить целую часть и дальнейшие вычисления проводить с правильной частью.

Если в каноническом разложении числа b содержатся степени простых чисел, входящих в разложение числа g , то получившаяся дробь будет иметь допериодическую часть.

Например, если $g = 10$ и

$$b = 2^k \cdot 5^m \cdot p_1 p_2 \dots p_n$$

где p_i — простые числа, отличные от 2 и 5, то обыкновенная несократимая дробь $\frac{a}{b}$ после обращения ее в десятичную будет иметь допериодическую часть, длина которой равна $\max\{k, m\}$.

Отметим, что порядок числа g по модулю b является делителем $\varphi(b)$. Это значит, что если $\varphi(b) = kp$, где p — простое число, и после k делений еще в качестве остатка не появилось число a , то для вычисления длины периода можно дальше и не делить: длина периода дроби равна в точности $\varphi(b)$.

Наконец, заметим, что если знаменатель дроби — простое число p , а в нашем распоряжении есть таблица индексов по модулю p , то вычисления длины периода можно провести с помощью этой таблицы.

Найдем, например, длину периода дроби $\frac{1}{97}$ после обращения ее в десятичную. Эта длина равна порядку числа 10 по модулю 97, т. е. наименьшему натуральному числу x такому, что

$$10^x \equiv 1 \pmod{97}.$$

Перейдем из группы $\langle \mathbb{Z}_{97}^*; \cdot \rangle$ в группу $\langle \mathbb{Z}_{96}; + \rangle$ и сведем тем самым наше показательное уравнение к уравнению линейному:

$$35x \equiv 0 \pmod{96}.$$

Число 35 обратимо по модулю 96: это значит, что на него можно разделить левую и правую части сравнения. Наименьшим положительным решением сравнения

$$x \equiv 0 \pmod{96}$$

является число 96. Следовательно, дробь $\frac{1}{97}$ после обращения ее в десятичную имеет 96 цифр в периоде.

Контрольные задания

1. Докажите, что отношение делимости в кольце целых чисел является предпорядком.

2. Докажите, что отношение ассоциированности для отношения делимости в кольце целых чисел образует эквивалентность. Найдите фактормножество по этой эквивалентности.

3. Докажите, что НОД чисел a и b линейно выражается через сами эти числа.

4. Докажите, что если числа a и b взаимно просты, то кольцо классов вычетов Z_{ab} является прямой суммой колец Z_a и Z_b .

5. Докажите, что для целых чисел a и b выполняется тождество

$$[a, b] = \frac{a \cdot b}{(a, b)}.$$

6. Докажите, что множество простых чисел вида $4n + 1$ бесконечно.

7. Сформулируйте и докажите теорему Эйлера.

8. Сформулируйте и докажите малую теорему Ферма.

9. Докажите, что проблема разрешимости системы линейных уравнений с целыми коэффициентами в множестве целых чисел алгоритмически разрешима.

10. Докажите, что в случае разрешимости системы сравнений первой степени с попарно простыми модулями решением будет класс вычетов по модулю, равному произведению модулей всех исходных сравнений.

Тема 4

ПОДГРУППЫ И ФАКТОР-ГРУППЫ

Основные понятия: подгруппа, смежный класс, индекс, гомоморфизм, изоморфизм, мономорфизм, группа подстановок, ядро гомоморфизма, нормальный делитель, фактор-группа, естественный гомоморфизм.

Основные факты: множество подгрупп образует решетку; порядок подгруппы делит порядок группы; гомоморфный образ группы изоморфен фактор-группе по ядру гомоморфизма.

Исследование любой алгебры в первую очередь состоит в изучении решетки подалгебр этой алгебры. Группы не являются здесь исключением. Более того, методы исследования подгрупп являются образцом для подражания при изучении других алгебр.

4.1. Простейшие свойства подгрупп

Непустое подмножество H является подгруппой группы G тогда и только тогда, когда:

- а) если $a \in H, b \in H$, то $a \cdot b \in H$;
- б) если $a \in H$, то $a^{-1} \in H$.

Если подмножество подгруппы конечно, то для того, чтобы оно было подгруппой, достаточно одного условия (но не достаточного в бесконечном случае). Если группа H — конечное подмножество группы G , то H является подгруппой тогда и только тогда, когда оно замкнуто относительно умножения, т. е. если $a, b \in H$, то $a \cdot b \in H$. Для любой группы два условия, необходимые и достаточные для того, чтобы быть подгруппой, можно заменить одним.

Непустое подмножество H является подгруппой тогда и только тогда, когда H замкнуто относительно деления (справа), т. е. если $a \in H, b \in H$, то $a \cdot b^{-1} \in H$.

Наличие общего элемента в каждой совокупности подгрупп означает, что пересечение любого числа подгрупп не пусто и с замкнутостью относительно произведения и взятия обратного (или деления) это означает, что пересечение любого числа подгрупп является подгруппой.

Предположим, что нам дана группа G и мы хотим описать ее подгруппы. Как задавать эти подгруппы для такого описания? Общая алгебраическая идея уже была продемонстрирована ранее: каждая подалгебра в алгебре может быть задана своим порождающим множеством.

В группах также для каждого подмножества M группы G существует наименьшая подгруппа группы G , содержащая M . Эту подгруппу называют подгруппой, порожденной множеством M , и обозначают символом $\text{гр}(M)$ или $\text{gr}(M)$.

По традиции элементы конечного множества M не окружают фигурными скобками, а вместо знака объединения ставят запятую.

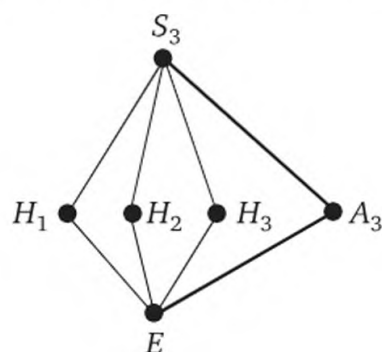
Например, если M состоит из одного элемента, $M = \{a\}$, то вместо $\text{гр}(\{a\})$ пишут $\text{гр}(a)$, а если $M = A \cup B$, то пишут $\text{гр}(M) = \text{гр}(A, B)$.

Если A и B — две подгруппы группы G , то наименьшей подгруппой, содержащей подгруппы A и B , будет $\text{гр}(A, B)$. Вместе с обычным теоретико-множественным пересечением это теоретико-групповое объединение превращает множество подгрупп группы G в решетку.

Рассмотрим, например, решетку $L(S_3)$ подгрупп симметрической группы S_3 . Пусть

$$H_1 = \text{гр}((1\ 2)), \quad H_2 = \text{гр}((1\ 3)), \quad H_3 = \text{гр}((2\ 3)), \quad A_3 = \text{гр}((1\ 2\ 3)).$$

Любая пара этих подгрупп имеет единичное пересечение и порождает всю группу S_3 . Других подгрупп, кроме этих шести, в группе S_3 нет. На рисунке изображена вся решетка $L(S_3)$.



Решетка $L(S_3)$

Можно проверить, что решетка эта не дистрибутивна.

Решетка подгрупп группы G обладает наибольшим и наименьшим элементами, но, вообще говоря, не дистрибутивна.

Конечно, если, например, решетка подгрупп группы G состоит всего из двух тривиальных подгрупп E и G , то дистрибутивность ей обеспечена.

Если a_1, a_2, \dots, a_n — порождающие элементы подгруппы H группы G , то каждый неединичный элемент из H можно представить в виде произведения элементов a_i и их обратных. Группа не обяза-

тельно абелева, поэтому эти произведения могут иметь любое число сомножителей.

Если внутри такого произведения рядом стоит порождающий элемент и его обратный, то их можно сократить (т. е. заменить нейтральным элементом, а нейтральный элемент выбросить, если остаются другие множители).

Исследуемая группа может оказаться построенной каким-то способом из более простых по устройству и свойствам подгрупп. Одной из наиболее простых конструкций такого рода является *прямое произведение* групп.

Рассмотрим, например, две группы: $A = \langle A; \cdot \rangle$ и $B = \langle A_2; \cdot \rangle$. Устроим новую алгебру $A \times B$ (*прямое произведение групп A и B*), взяв в качестве множества-носителя этой алгебры декартово произведение $A \times B$ и определив операцию покомпонентно. Точнее говоря,

$$A \times B = \{(a, b) \mid a \in A, b \in B\},$$

а операция $A \times B$ определена правилом (для каждого a_1, a_2 из A и b_1, b_2 из B):

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

Непосредственной проверкой аксиоматики группы проверяется, что прямое произведение групп является группой.

Если группы A и B конечны, то прямое произведение $A \times B$ тоже конечно и

$$|A \times B| = |A| \cdot |B|.$$

Если в каждой группе-сомножителе выполняются некоторые тождества, то эти тождества выполняются и в их прямом произведении.

Отметим, что если в группе G выполняется тождество, то этому тождеству будут удовлетворять и элементы всех подгрупп группы G .

Класс групп, описываемый тождествами, называется *многообразием групп*. Многообразие замкнуто не только относительно взятия прямых произведений, но и относительно взятия подалгебр и прямых произведений.

Общее замечание о многообразиях для групп можно конкретизировать для важных частных случаев. Например, можно говорить о многообразии абелевых групп.

Прямое произведение абелевых групп является абелевой группой.

Стоит обратить внимание на одно обстоятельство. Слово «произведение» даже для натуральных чисел *двусмысленно*. Можно говорить о произведении как результате операции, например: взяли два числа 2 и 3, перемножили и получили произведение, $2 \cdot 3 = 6$.

Множители взяли извне, поэтому такое произведение естественно назвать *внешним*. Именно внешним способом только что было определено прямое произведение групп. Но и для чисел возникает и обратная задача: дано число и требуется разложить его на множители: $6 = 2 \cdot 3$. Получение множителей *изнутри* можно назвать *внутренним* произведением. Хотя прямое произведение групп было определено внешним образом, на самом деле нас больше волновало внутреннее произведение.

Поскольку в алгебре изоморфные группы не считаются различными, определить внутреннее прямое произведение можно следующим образом.

Группа G разложима в прямое произведение своих подгрупп A и B , если G изоморфна $A_1 \times B_1$, где A изоморфна A_1 , а B изоморфна B_1 .

Каждая группа может быть тривиальным образом представлена в виде произведения самой себя и единичной группы. Под словами «прямое разложение» имеется в виду только нетривиальное разложение (так же как и для натуральных чисел, представление простого числа p в виде произведения $p = p \cdot 1$ не считается настоящим разложением).

Как обычно, опуская слова «с точностью до изоморфизма», получаем, что прямые сомножители являются подгруппами прямого произведения. Это значит, что если в группе G вообще нет нетривиальных подгрупп¹, то G неразложима в прямое произведение. Наличие подгрупп может и не спасти ситуацию.

Пусть $A \times B$ — прямое произведение двух групп A , B , определенное пока внешним образом. Пусть e — единичный элемент группы A и e_1 — единица в B . Тогда множество $A_1 = \{(a, e_1) | a \in A\}$ образует подгруппу в $A \times B$, изоморфную группе A . Множество $B_1 = \{(e_1, b) | b \in B\}$ является подгруппой в группе $A \times B$, изоморфной группе B . Поскольку лишь один элемент (e, e_1) попадает одновременно и в A_1 , и B_1 , пересечение $A_1 \cap B_1$ — это единичная подгруппа.

Это свойство, разумеется, переносится и на внутреннее произведение.

Таким образом, если группа G является прямым произведением подгрупп A и B , то обе эти подгруппы имеют единичное пересечение. Отсюда следует, что если в группе пересечение любых неединичных подгрупп неединичное, то эта группа неразложима в прямое произведение.

Например, в группе $\langle \mathbb{Z}; + \rangle$ любые две ненулевые подгруппы имеют ненулевое пересечение, поэтому аддитивная группа целых чисел неразложима в прямое произведение своих подгрупп.

¹ Неединичная конечная группа не имеет нетривиальных подгрупп тогда и только тогда, когда ее порядок — простое число.

По той же причине аддитивная группа рациональных чисел неразложима в прямое произведение своих подгрупп. Напомним, что на аддитивном языке вместо слов «прямое произведение» обычно говорят «прямая сумма» и вместо символа $A \times B$ пишут $A \oplus B$. Впрочем, предыдущие замечания можно сформулировать независимо от аддитивного или мультипликативного языка.

Группа $\langle \mathbb{Z}; + \rangle$ бесконечная циклическая. Все циклические группы одинакового порядка изоморфны, а это значит, что бесконечная циклическая группа неразложима в прямое произведение своих подгрупп.

Группа $\langle \mathbb{Q}; + \rangle$ — это объединение строго возрастающей цепочки циклических групп. Такая группа тоже неразложима в прямое произведение своих подгрупп.

Однако существования двух нетривиальных подгрупп с единичным пересечением может оказаться недостаточно для приморазложимости группы. В только что использованных обозначениях каждый элемент $(a, b) = (a, e_1)(e, b)$, т. е. если $G = A \times B$, то множество G состоит из всевозможных произведений элементов из A_1 на элементы из B_1 :

$$G = AB = \{ab \mid a \in A_1, b \in B_1\}.$$

Это значит, что если в группе G нет двух таких подгрупп A, B :

- 1) $A \cap B = E$;
- 2) $AB = G$,

то группа G неразложима в прямое произведение.

И все-таки этих двух свойств еще недостаточно для разложимости группы в прямое произведение.

Опять в тех же обозначениях, что и ранее, имеем, что для каждого элемента (a_1, e) из A_1 и каждого элемента (a, b) из G :

$$(a, b)(a_1, e)[(a, b)]^{-1} = (a, b)(a_1, e)(a^{-1}, b^{-1}) = (aa_1a^{-1}, beb^{-1}) = (a_2, e).$$

Короче говоря, если A_1 — прямой сомножитель группы G , то для каждого x из A и каждого y из G элемент xyx^{-1} принадлежит A_1 . Группу с таким свойством называют *нормальной* (или *нормальным делителем*).

Прямой сомножитель группы должен быть нормальным делителем группы.

В каждой неединичной группе есть по крайней мере два нормальных делителя — сама группа и единичная подгруппа. Эти делители принято называть *тривиальными*.

Группа называется *простой*, если у нее нет нетривиальных нормальных делителей. Простая группа заведомо неразложима в прямое произведение: нет нормальных делителей — нет и прямых множителей.

Подведем итоги. В пряморазложимой группе должны быть две нормальные подгруппы A, B , которые должны иметь единичное пересечение и в комплексе AB давать всю группу. После этого наблюдения уже неудивительно, что далеко не каждая группа окажется разложимой в прямое произведение.

Например, в симметрической группе S_3 только один нетривиальный нормальный делитель — группа A_3 , поэтому группа S_3 неразложима в прямое произведение своих подгрупп.

Как бы то ни было, обнаруженные свойства сомножителей внешнего прямого произведения групп дают возможность разложить данную группу в прямое произведение, если это разложение существует. В случае существования это разложение позволит свести изучение группы $A \times B$ задачам о группах-множителях.

Напомним, что если группы A и B имеют представление

$$\begin{aligned} A &= \langle a_1, a_2, \dots, a_n; R_1(a_i) = 1, R_2(a_i) = 1, \dots, R_k(a_i) = 1 \rangle; \\ B &= \langle b_1, b_2, \dots, b_m; Q_1(b_j) = 1, Q_2(b_j) = 1, \dots, Q_t(b_j) = 1 \rangle, \end{aligned}$$

то группу $A \times B$ можно задать в виде

$$\begin{aligned} A \times B = A &= \langle a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m; R_1(a_i), R_2(a_i), \dots, R_k(a_i); \\ Q_1(b_j), Q_2(b_j), \dots, Q_t(b_j), a_i b_j a_i^{-1} b_j^{-1}, i &= 1, 2, \dots, n; j = 1, 2, \dots, m \rangle. \end{aligned}$$

Например, группа, заданная представлением

$$G = \langle a, b; a^2, b^4, bab^{-1}a \rangle$$

является прямым произведением циклических групп $A = \langle a; a^2 \rangle$ и $B = \langle b; b^4 \rangle$ второго и четвертого порядков.

Для иллюстрации того, что прямое произведение может быть устроено не так просто, как циклическая группа, найдем решетку подгрупп этой группы. Поскольку G является прямым произведением своих подгрупп A и B , произвольный элемент этой группы имеет вид $a^i b^j$, где $i \in \{0, 1\}$, $j \in \{0, 1, 2, 3\}$, и такое представление элемента единственно. Отсюда, следует, что группа G состоит из $4 \cdot 2 = 8$ элементов.

Четвертая степень любого такого элемента равна единице, поэтому порядок любого элемента — это делитель числа 4. В частности, в группе G нет элемента порядка 8, поэтому группа G нециклическая.

Число 2 простое, поэтому все подгруппы порядка два — это циклические подгруппы, порожденные элементами второго порядка:

$$H_1 = A = \text{gr}(a), H_2 = \text{gr}(b^2), H_3 = \text{gr}(ab^2).$$

Пересечения любой пары этих подгрупп равно единичной подгруппе E .

Циклические подгруппы четвертого порядка порождаются элементами четвертого порядка:

$$H_4 = B = \text{гр}(b) = \{1, b, b^2, b^3\};$$

$$H_5 = \text{гр}(ab) = \{1, ab, b^2, ab^3\}.$$

Нециклическая подгруппа четвертого порядка в нашей группе одна — она порождается элементами второго порядка:

$$H_6 = \text{гр}(a, b^2) = \{1, a, b^2, ab^2\}.$$

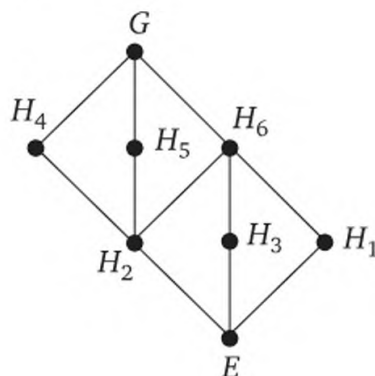
Для построения графа решетки подгрупп отметим, что

$$H_4 \cap H_5 = H_4 \cap H_6 = H_5 \cap H_6 = H_2;$$

$$H_1 \subset H_6, H_3 \subset H_6.$$

Итак, решетка подгрупп группы G содержит шесть нетривиальных подгрупп — $H_1, H_2, H_3, H_4, H_5, H_6$ и две тривиальные — саму группу G и единичную подгруппу E .

Взаимоположение этих подгрупп видно на графе этой решетки, представленном на рисунке.



Решетка подгрупп

По приведенным примерам построения решеток подгрупп видно, что проще иметь дело с группами подстановок.

Любая конечная группа, по теореме Кэли, изоморфна некоторой группе подстановок, и вычислительная техника позволяет этим изоморфизмом воспользоваться. Правда, иногда и вручную, по виду подстановок, порождающих группу, можно установить разложимость группы в прямое произведение. Для того чтобы группа подстановок, порожденная подстановками $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m$, распадалась в прямое произведение подгрупп $\text{гр}(a_1, a_2, \dots, a_n)$ и $\text{гр}(b_1, b_2, \dots, b_m)$, достаточно (но вовсе не необходимо), чтобы a_i и b_j перемещали различные символы.

Например, подгруппа группы S_6 , порожденная элементами $(1\ 2)$ и $(3\ 4\ 5\ 6)$, изоморфна только что рассмотренной группе $G = \langle a, b; a^2, b^4, bab^{-1}a \rangle$. Элементами этой группы являются подстановки:

$$e, (1\ 2), (3\ 4\ 5\ 6), (1\ 2)(3\ 4\ 5\ 6), (3\ 6\ 5\ 4), \\ (1\ 2)(3\ 5)(4\ 6), (3\ 5)(4\ 6), (1\ 2)(3\ 6\ 5\ 4).$$

Теперь рассмотрим два интересных и важных примера подгрупп группы G , в какой-то мере характеризующих *неабелевость* группы G . Единица перестановочна с любым элементом группы: $xe = ex$ для каждого x . Таким же свойством могут обладать и другие элементы полугруппы. Элементы, перестановочные со всеми элементами группы, называют *центральными*. Таким образом, z — *центральный* в группе G , если для каждого элемента x из G выполняется равенство $zx = xz$.

Множество всех центральных элементов группы G принято называть *центром* группы и обозначать символом $Z(G)$. Произведение центральных элементов снова принадлежит центру, и элемент, обратный для центрального элемента, тоже центральный. Таким образом, *центр группы является подгруппой*. Центр имеет любая группа, в крайнем случае он состоит только из единицы. Тогда принято говорить, что эта группа *без центра*.

Группа является абелевой тогда и только тогда, когда она совпадает со своим центром. Чем меньше центр, тем дальше эта группа по своим свойствам от абелевых групп.

Если a, b — два произвольных элемента группы G , то элемент вида $a^{-1}b^{-1}ab$ (или $aba^{-1}b^{-1}$) называют *коммутатором* элементов a, b . Подгруппу, порожденную коммутаторами, называют *коммутантом* группы G (или *производной* группы G).

Группа G является абелевой тогда и только тогда, когда ее коммутант равен единичной подгруппе.

Правда, если группа неабелева, то и центр, и коммутант могут не дать никакой существенной информации об этой группе. Группа может оказаться без центра (т. е. центр слишком мал), а коммутант ее, напротив, слишком велик — совпадающий со всей группой.

Например, таковыми будут все простые группы: там и центр, и коммутант совпадают с тривиальными подгруппами.

Два элемента a, b группы G называют *сопряженными*, если существует элемент c такой, что $b = c^{-1}ac$.

Элемент c в таком случае называют *сопрягающим элементом* (элемент b иногда называют *трансформой* элемента a). Заметим, что сопряжение можно писать и по-другому: sac^{-1} , так как c^{-1} — это элемент той же группы G .

Часто пользуются символикой: $c^{-1}ac = a^c$.

Заметим, что существуют группы (разумеется, бесконечные), для которых проблема сопряженности неразрешима, т. е. нет алгоритма, позволяющего для любой пары элементов ответить на вопрос, сопряжены они или нет.

Для некоторых бесконечных групп эта проблема имеет решение. Сопряжения уже встречались в линейной алгебре при изучении алгебры матриц и так называемых линейных групп. Подобные обратимые матрицы — это сопряженные элементы в полной линейной группе.

Если векторное пространство рассматривается над полем комплексных чисел (или любым алгебраически замкнутым полем), то каждая матрица является трансформой жордановой матрицы. Таким образом, проблема сопряженности в полной линейной группе над алгебраически замкнутым полем алгоритмически разрешима.

В конечной группе (например, в группе подстановок) с теоретической точки зрения проблемы сопряженности нет: в конечное число шагов всегда можно узнать, сопряжены два элемента или нет (хотя бы простым перебором всех вариантов). Другое дело, когда это требуется сделать не теоретически, а практически и не с помощью вычислительной техники, а вручную. Впрочем, иногда узнать, сопряжены или нет два элемента в группе, несложно и вручную.

Например, для выяснения, сопряжены или нет две подстановки из симметрической группы S_n в самой группе S_n для небольших n , вычислительная техника не требуется.

Если подстановка a представлена в виде произведения независимых циклов, то набор размеров этих циклов (n_1, n_2, \dots, n_k) назовем *устройством* подстановки a . Элементы набора разрешается менять местами (независимые циклы в подстановке перестановочны).

Непосредственным вычислением проверяется, что две сопряженные подстановки одинаково устроены.

Верно и обратное: если подстановки одинаково устроены, то они сопряжены в симметрической группе.

Например, подстановки

$$(123) (45) \text{ и } (14) (236)$$

устроены одинаково — 3, 2, и поэтому сопряжены в группе S_6 , а подстановка

$$(123) (456)$$

с ними не сопряжена, так как устроена иначе; ее устройство — 3, 3.

Пусть теперь G — произвольная группа, $\text{Aut}(G)$ — группа автоморфизмов, а $\text{End}(G)$ — полугруппа эндоморфизмов группы G .

Подгруппа H группы G называется *вполне характеристической*, если она *инвариантна* относительно любого эндоморфизма. Иначе

говоря, подгруппа H вполне характеристическая, если для каждого φ из $\text{End}(G)$

$$\varphi(H) < H.$$

Говорят еще: подгруппа H *выдерживает* любой эндоморфизм.

Если подгруппа выдерживает любой автоморфизм, то она называется *характеристической*.

Итак, H — характеристическая подгруппа группы G , если для любого α из $\text{Aut}(G)$

$$\alpha(H) < H.$$

Тривиальными примерами характеристических и даже вполне характеристических подгрупп являются сама группа G и ее единичная подгруппа E .

Заметим, что понятие инвариантного подпространства векторного пространства несколько иное, там оно связано с отдельно взятым линейным оператором. Дело в том, что если ввести понятие характеристического и вполне характеристического подпространства по аналогии с подгруппами, то особого смысла там эти понятия не получают: таковыми окажутся лишь само пространство и нулевое подпространство.

Теперь обратим внимание на связь сопряжений с автоморфизмами группы.

Пусть g — произвольный, но фиксированный элемент группы G . Отображение, переводящее каждый элемент x группы G в сопряженный $g^{-1}xg$, является биекцией, сохраняющей операцию, т. е. автоморфизмом группы G .

Такие автоморфизмы называют *внутренними автоморфизмами*.

Произведение двух внутренних автоморфизмов снова является внутренним автоморфизмом. Обратный к внутреннему автоморфизму — тоже внутренний автоморфизм. Это значит, что множество внутренних автоморфизмов образует группу. Группу всех внутренних автоморфизмов обозначают символом $\text{Inn}(G)$.

Группа $\text{Inn}(G)$ внутренних автоморфизмов группы G является подгруппой $\text{Aut}(G)$ — группы всех автоморфизмов G .

Если группа G абелева, то все внутренние автоморфизмы оставляют каждый элемент из G неподвижным. Если группа G неабелева, то существует по крайней мере одна пара неперестановочных элементов x, y . Их неперестановочность означает:

$$xyx^{-1} \neq y.$$

Иначе говоря, группа G абелева тогда и только тогда, когда $\text{Inn}(G) = E$.

Подгруппа N группы G называется *инвариантной подгруппой* (или *нормальной подгруппой*, или *нормальным делителем*), если

она выдерживает все внутренние автоморфизмы, в таком случае пишут: $N \triangleleft G$.

Подгруппа N — нормальный делитель, если для каждого элемента g из G выполняется включение: $g^{-1}Ng \subset N$.

Другими словами, непустое подмножество N группы G является нормальным делителем группы G , если для любых a, b из N и каждого g из G :

$$1) \quad a \in N, b \in N \Rightarrow a \cdot b^{-1} \in N;$$

$$2) \quad a \in N, g \in G \Rightarrow g^{-1}ag \in N.$$

Сопряжение можно представить и элементом g , и элементом g^{-1} , поэтому знак включения в определении нормального делителя можно заменить равенством. Подгруппа N — нормальный делитель группы G , если для каждого элемента g из G

$$g^{-1}Ng = N.$$

Заметим, что свойство нормальности подгруппы уже появилось ранее при обсуждении свойств прямых множителей группы.

Каждая вполне характеристическая подгруппа является характеристической, а каждая характеристическая — нормальной. Обратное утверждение неверно.

Например, если группа $G = A \times A$, то подгруппа A является нормальной в G , но не характеристической. Действительно, автоморфизм группы, переставляющий прямые сомножители, не оставляет подгруппу A на месте.

Свойства характеристичности, вполне характеристичности и нормальности сохраняются при пересечении. Это значит, что:

- пересечение любого числа вполне характеристических подгрупп является вполне характеристической подгруппой;
- пересечение любого числа характеристических подгрупп является характеристической подгруппой;
- пересечение любого числа нормальных делителей является нормальным делителем.
- Подгруппа, порожденная подгруппами, обладающими любым из перечисленных свойств, сама обладает таким же свойством.

Это значит, что в решетке подгрупп можно выделить подрешетку нормальных подгрупп, в этой подрешетке содержится подрешетка характеристических, а в ней — подрешетка вполне характеристических подгрупп. В последней решетке в любом случае содержится по крайней мере пара тривиальных подгрупп.

На рисунке, изображающем решетку подгрупп группы S_3 , черным цветом выделена подрешетка нормальных делителей. Заметим, что в группе S_3 единственная подгруппа порядка три, а у этой подгруппы нет нетривиальных подгрупп, поэтому A_3 не только нормальная, но и характеристическая и даже вполне характеристическая подгруппа.

Во втором примере группа абелева, следовательно, решетка подгрупп является одновременно и решеткой нормальных делителей. Однако ни одна из нормальных подгрупп, кроме тривиальных, не является даже характеристической.

Рассмотрим несколько примеров нормальных, характеристических и вполне характеристических подгрупп.

Сопряжение четной подстановки снова является четной подстановкой. Следовательно, знакопеременная группа A_n является нормальным делителем в симметрической группе S_n .

Из свойств определителя следует, что специальная линейная группа $SGL_n(P)$ является нормальным делителем в полной линейной группе $GL_n(P)$.

Сопряжение внутреннего автоморфизма произвольным автоморфизмом образует внутренний автоморфизм. Это значит, что

$$\text{Inn}(G) \triangleleft \text{Aut}(G).$$

Если группа G абелева, то любая ее подгруппа является нормальным делителем. Заметим, что обратное утверждение неверно. В неабелевой группе все подгруппы могут оказаться нормальными.

Например, в группе кватернионов

$$G = \langle i, j; i^4 = 1, j^4 = 1, i^{-1}j^3ij^{-1} = 1, i^2j^{-2} = 1 \rangle$$

все подгруппы являются нормальными делителями.

Обсудим еще один вопрос. Свойство быть подгруппой транзитивно: подгруппа подгруппы является подгруппой во всей группе:

$$A < B, B < G \Rightarrow A < G.$$

Можно ли здесь вставить слово «нормальной» (а на схеме заменить знак $<$ на \triangleleft)? Другими словами, верно ли, что нормальный делитель нормального делителя является нормальным делителем всей группы?

Ответ на этот вопрос отрицательный.

В группе S_4 подгруппа

$$K = \{e, (12)(34), (14)(23), (13)(24)\}$$

является нормальным делителем (кроме единичной, она содержит все подстановки устройства 2, 2 — произведения двух независимых транспозиций).

Группу K называют *четверной группой Клейна*¹ — она абелева, и любая ее подгруппа, например $H = \{e, (12)(34)\}$, — ее нормальный делитель. Группу Клейна обычно обозначают символом V_4 .

¹ Феликс Кристиан Клейн (Klein, 1849—1925) — немецкий математик. Основные его труды — по теории непрерывных групп, теории функций и неевклидовой

Однако H не является нормальным делителем во всей группе S_4 .

Таким образом, нормальный делитель нормального делителя не обязан быть нормальным делителем во всей группе.

Пусть теперь G — произвольная группа, и нас интересует, проста или нет эта группа? Группа не проста, если она содержит нетривиальную характеристическую или вполне характеристическую подгруппы.

При любом автоморфизме центральный элемент переходит в центральный, поэтому *центр* $Z(G)$ группы G является *характеристической подгруппой* в G .

Если G неабелева (т. е. не совпадает со своим центром), но с центром (т. е. $Z(G)$ не единичен), то G имеет нетривиальную характеристическую подгруппу.

Однако не в каждой группе центр является вполне характеристической подгруппой. Какую же вполне характеристическую подгруппу можно, по крайней мере, попытаться поискать в произвольной группе?

Коммутант является подгруппой, порожденной всевозможными значениями слов вида $xux^{-1}y^{-1}$. Вместо коммутатора можно было взять другое слово (или множество слов). Группу, полученную таким способом, называют *вербальной*.

При любом эндоморфизме элемент, имеющий вид значения некоторого слова, переходит в элемент такого же вида. Поэтому любая вербальная подгруппа вполне характеристическая. В частности, коммутант группы G является вполне характеристической подгруппой в G .

Например, коммутант симметрической группы S_n (где $n > 2$) порождается четными подстановками, поэтому совпадает с подгруппой A_n .

Таким образом, все группы S_n содержат по крайней мере одну вполне характеристическую подгруппу — A_n . Для любой подстановки из S_n можно подобрать непостоянную с ней подстановку. Это значит, что группа S_n без центра.

Пусть G — группа, а H — ее подгруппа. Может случиться, что H , не будучи нормальной во всей группе G , является нормальным делителем в некоторой промежуточной подгруппе группы G . Наибольшая такая промежуточная подгруппа $N_G(H)$ называется *нормализатором* H в G .

Такое определение неконструктивно — наибольший элемент может не существовать даже в конечном упорядоченном множестве. Однако нормализатор можно определить и по-другому.

геометрии. В его работе «Сравнительное обозрение новейших геометрических исследований» (1872), вошедшей в историю как «Эрлангенская программа», впервые изложена единая теоретико-групповая точка зрения на различные геометрии.

Если H — подгруппа группы G , то нормализатором $N_G(H)$ называют множество

$$\{x \in G \mid x^{-1}Hx = H\}.$$

Подгруппа H группы G будет нормальным делителем в G тогда и только тогда, когда $N_G(H) = G$.

Поскольку пересечение нормальных делителей — снова нормальный делитель, можно говорить о нормальном делителе группы, порожденном данным множеством M . Его называют *нормальным замыканием* M и обозначают символом $\langle M \rangle^G$.

Нормальное замыкание подмножества M в группе G равно подгруппе, порожденной всеми сопряжениями элементов из M элементами из G :

$$\langle M \rangle^G = \text{gp}(\{m^g \mid m \in M, g \in G\}).$$

Подгруппа H является нормальным делителем в G тогда и только тогда, когда H совпадает со своим нормальным замыканием.

Если A, B — подгруппы абелевой группы G , то наименьшей подгруппой, содержащей A и B , будет

$$AB = \{ab \mid a \in A, b \in B\}.$$

Дело, однако, здесь не в коммутативности умножения, а в том, что в абелевой подгруппе каждая подгруппа нормальна.

Если A, B — два нормальных делителя группы G , то наименьшей подгруппой, содержащей A и B , будет

$$AB = \{ab \mid a \in A, b \in B\}.$$

Эта наименьшая подгруппа является к тому же и нормальным делителем. Таким образом, нормальное замыкание двух нормальных делителей совпадает с комплексом AB .

Для произвольных подгрупп это не так. Если A, B — подгруппы группы G , то наименьшая подгруппа, содержащая A и B , содержит комплекс AB , но не обязательно совпадает с ним.

Заметим еще, что нормальное замыкание подмножества тоже не обязательно совпадает с подгруппой, порожденной этим подмножеством.

Например, в группе S_n нормальное замыкание любой подгруппы, порожденной транспозицией, совпадает со всей группой S_n .

Если $n \geq 5$, то нормальное замыкание любого неединичного элемента в группе A_n совпадает со всей группой A_n . Это означает, что группа A_n проста, т. е. не содержит нетривиальных нормальных делителей.

В абелевой группе все подгруппы нормальны, поэтому абелева группа будет проста тогда и только тогда, когда в ней вообще нет нетривиальных подгрупп (для неединичной группы это случится лишь в том случае, когда группа конечна и порядок ее — простое число).

Группы $GL_n(P)$ непросты, если $n > 1$ и поле P содержит более двух элементов¹.

Все группы S_n для $n > 2$ содержат нетривиальный нормальный делитель A_n , т. е. они тоже непросты.

4.2. Циклические подгруппы

В первой, ознакомительной теме появилось лишь определение циклической группы и обозначены самые простейшие свойства таких групп. Сейчас, после темы о свойствах сравнений в кольце целых чисел, эти свойства можно обсуждать более осмысленно.

Напомним: циклической подгруппой называется подгруппа, состоящая из степеней одного элемента. Таковой может оказаться и вся группа. Например, аддитивная группа целых чисел является бесконечной циклической группой.

Множество вращений правильного n -угольника с операцией «композиция» является циклической группой порядка n .

Множество корней n -й степени из единицы в поле комплексных чисел является мультипликативной циклической группой порядка n .

Если g — порождающий элемент группы G , то каждый элемент из G имеет вид g^i . Из коммутативности сложения целых чисел следует, что циклическая группа абелева, или (по закону контрапозиции) любая неабелева группа нециклическая.

Может ли группа быть абелевой и нециклической?

Да, может. Например, не существует такого рационального числа g , что любое рациональное является кратным этого g . Иначе говоря, аддитивная группа рациональных чисел нециклическая.

Нет и рационального числа g такого, что любое рациональное является степенью этого g . Это касается как всех ненулевых рациональных чисел, так и только положительных. Поэтому мультипликативная группа ненулевых рациональных чисел тоже нециклическая и мультипликативная группа положительных рациональных чисел нециклическая.

На последние два утверждения можно взглянуть с иной точкой зрения. Бесконечная циклическая группа неразложима в прямое произведение, поэтому любая бесконечная группа, разложимая

¹ Для $n > 2$ и двухэлементного поля P все группы $GL_n(P)$ просты.

в прямое произведение (или лишь содержащая две неединичные подгруппы с единичным пересечением), точно нециклическая.

Единичная группа и группа из двух элементов явно циклические, поэтому абелевы. Сколько элементов в наименьшей неабелевой группе? Сколько элементов в наименьшей нециклической группе?

С помощью простого перебора таблиц Кэли можно увидеть, что группа самосовмещений правильного треугольника (она же симметрическая группа S_3) — это наименьшая неабелева группа.

Группа самосовмещений ромба (она же прямое произведение двух циклических групп второго порядка, она же группа Клейна V_4) — это наименьшая нециклическая группа. Таким образом, наименьшая нециклическая группа состоит из четырех элементов.

В любой группе каждый элемент порождает циклическую подгруппу, поэтому каждая группа является теоретико-множественным объединением циклических групп.

Поскольку все циклические группы абелевы, любая неединичная группа содержит хотя бы одну неединичную абелеву подгруппу. Более того, каждая группа является теоретико-множественным объединением абелевых групп.

Если g — произвольный элемент группы G , то порядок циклической группы $\text{gr}(g)$ зависит от следующих обстоятельств. Может случиться одно из двух:

- 1) все степени элемента g различны;
- 2) некоторые степени элемента g совпадают.

В первом случае $\text{gr}(g)$ бесконечна. Во втором случае равенство $g^i = g^j$ означает, что $|G| \leq |i - j|$.

Более точно ситуация описывается с помощью понятия «*порядок элемента*».

Пусть G — мультипликативно записанная группа, e — единица группы, g — произвольный ее элемент. Наименьшее натуральное число n такое, что $g^n = e$, называют *порядком* элемента g . Если такого числа n не существует, то говорят что g — элемент *бесконечного порядка*.

Если все натуральные степени элемента g различны ($g^m \neq g^n$ при $m \neq n$), то g имеет бесконечный порядок.

Если для некоторых различных натуральных чисел m, n выполняется равенство $g^m = g^n$, то элемент g имеет конечный порядок.

Используя теорему о делении с остатком, получаем, что если элемент g имеет порядок m , то $g^k = e$ тогда и только тогда, когда число k делится на m .

Другими словами, если элемент g имеет порядок m , то

$$g^k = g^n \Leftrightarrow k \equiv n \pmod{m}.$$

Отметим еще два полезных свойства порядка.

Если a и b — перестановочные групповые элементы порядков m и n соответственно и числа m , n взаимно просты, то в группе найдется элемент, порядок которого равен mn .

Как обобщение ситуации: если a и b — перестановочные групповые элементы порядков m и n соответственно, то в группе найдется элемент, порядок которого равен НОК $[a, b]$.

Заметим, что, по существу, именно это свойство перестановочных элементов было использовано при доказательстве теоремы Лежандра о цикличности конечной мультипликативной группы, состоящей из элементов поля.

Отметим теперь, что слово «порядок» стало двусмысленным — это и число элементов в группе (или подгруппе), и число, связанное со степенями элемента группы. Эта двусмысленность легко устраняется, так как порядок циклической группы $\text{гр}(g)$ является порядком элемента g .

Обсудим еще раз подробно свойства бесконечной циклической группы. В бесконечной циклической группе $\text{гр}(g)$ все степени элемента g различны, точнее, если $\text{гр}(g)$ бесконечна, то из $m \neq n$ следует $g^m \neq g^n$.

Поэтому если группа $\text{гр}(g)$ бесконечна, то отображение $f: \mathbb{Z} \rightarrow \text{гр}(g)$ по правилу: $f(k) = g^k$ является биективным.

Поскольку $g^n g^m = g^{n+m}$, отображение f сохраняет операцию. Иначе говоря, каждая бесконечная циклическая группа изоморфна аддитивной группе целых чисел.

Итак, если речь идет о бесконечной циклической группе, то можно считать, что перед нами просто экземпляр группы $\langle \mathbb{Z}; + \rangle$.

Если же порядок конечный, то, используя теорему о делении с остатком для целых чисел, получаем: если n — такое наименьшее натуральное число, что $g^n = e$, то $\text{гр}(g)$ состоит из n элементов и $\text{гр}(g) = \{e, g, g^2, \dots, g^{n-1}\}$.

Теперь если две циклические группы $\text{гр}(a)$ и $\text{гр}(b)$ имеют одинаковый порядок, то отображение, переводящее элемент a^k первой группы в элемент b^k второй группы (для каждого целого k), является биективным и сохраняющим операции, т. е. изоморфизмом. Для бесконечных циклических групп это же изображение является изоморфизмом. Поэтому циклические группы одинакового порядка изоморфны.

При изучении конечной циклической группы мы можем пользоваться любым удобным эталоном (представителем циклической группы):

- 1) арифметическим (построенным из классов целых чисел);
- 2) геометрическим (группой самосовмещений);
- 3) группой корней из единицы.

Точнее говоря, каждая циклическая группа n изоморфна группе:

- $\langle \mathbb{Z}_n; + \rangle$ классов вычетов по модулю n ;
- вращений правильного n -угольника;
- корней n -й степени из единицы.

Любое из этих представлений можно устроить для любого натурального n . Поэтому для любого числа n существует циклическая группа порядка n .

Конечно, мы можем взять и универсальное представление циклической группы. Циклическая группа G , имеющая порядок n и порожденная элементом a , имеет представление

$$G = \langle a; a^n = 1 \rangle.$$

Если же G — бесконечная циклическая, то ее представление превращается в $G = \langle a \rangle$.

В этом представлении множество определяющих соотношений пусто. Можно, впрочем, написать на месте соотношений что-нибудь тривиальное. Например,

$$\langle a; 1=1 \rangle \text{ или } \langle a; a \cdot a^{-1} = 1 \rangle$$

являются представлениями бесконечных циклических групп.

Группа, свободная от отношений, называется *свободной группой*. Бесконечная циклическая группа — это однопорожденная свободная группа.

Чтобы найти порядок элемента g группы G , достаточно выяснить порядок подгруппы, порожденной этим элементом. Этот порядок появится в качестве показателя степени в представлении группы.

Найдем¹, например, порядки порождающих элементов в группе

$$G = \langle x, y; x^2 y x y^3 = 1, y^2 x y x^3 = 1 \rangle.$$

Подгруппа, порожденная элементом x , состоит из семи элементов; точно такая же подгруппа, порожденная элементом y . Это значит, что порядок каждого из порождающих элементов равен 7:

$$\text{гр}(x) = \langle x; x^7 = 1 \rangle; \text{гр}(y) = \langle y; y^7 = 1 \rangle.$$

Соотношения группы G можно записать иначе:

$$G = \langle x, y; x^7 = 1, y^7 = 1, x^2 y x y^3 = 1, y^2 x y x^3 = 1 \rangle.$$

Определить порядок подстановки можно без всякой вычислительной техники.

Если подстановка представляет собой цикл длины n , то при возведении в степень этого цикла первый раз получится единичная подстановка после n -го умножения. Таким образом, порядок цикла равен его длине. Если же подстановка a является произведением независимых циклов, то порядок a равен наименьшему кратному этих циклов.

¹ С помощью пакета математических вычислений *Maple*.

Например, порядок подстановки

$$(1\ 2\ 3)\ (4\ 5\ 6\ 7)\ (8\ 9\ 10\ 11\ 12)$$

равен 60. Отметим, что порядок подстановки может оказаться значительно больше ее степени.

Подгруппы циклических групп устроены так же просто, как и содержащие их группы.

Если H — ненулевая подгруппа аддитивной группы целых чисел, а d — наименьший положительный элемент из H , то, используя теорему о делении с остатком для целых чисел, видим, что любой элемент из H является кратным d , т. е. $H = \text{гр}(d)$. Иначе говоря, ненулевая подгруппа бесконечной циклической группы сама является бесконечной циклической.

Нулевая подгруппа, впрочем, тоже является циклической. Кроме того, теорему о делении с остатком можно использовать и в случае конечной циклической группы. Это значит, что уже без всяких оговорок верно предложение: каждая подгруппа циклической группы сама является циклической.

Свойство алгебры, которым обладает каждая ее подалгебра, называют *наследственным*. Например, конечность, абелевость — это примеры наследственных свойств для групп. Только что проведенное наблюдение о циклических группах означает, что и цикличность — тоже наследственное свойство.

Итак, цикличность наследуется при переходе к подгруппам.

При гомоморфизме (точнее, при эпиморфизме) образы порождающих элементов порождают гомоморфный образ алгебры. Для циклических групп получаем: *гомоморфный образ циклической группы является циклической группой*.

Кроме того, каждая циклическая группа является гомоморфным образом бесконечной циклической группы.

Любая ненулевая подгруппа аддитивной группы \mathbb{Z} бесконечна. Однако для каждого числа $m > 0$ индекс подгруппы $\text{гр}(m)$ в аддитивной группе целых чисел равен m , и другой подгруппы с таким индексом там нет (точное определение индекса подгруппы см. в параграфе 4.3). Это значит, что для любого натурального m в бесконечной циклической группе существует в точности одна подгруппа индекса m . Следовательно, решетка подгрупп группы $\langle \mathbb{Z}; + \rangle$ антиизоморфна решетке $\langle \mathbb{Z}_0; \text{НОД}, \text{НОК} \rangle$ при соответствии, переводящем $\text{гр}(a)$ в элемент a .

Например, нулевая подгруппа — наименьшая в решетке $L(\mathbb{Z})$, но нуль — наибольший элемент во второй решетке; единица — наименьший элемент во второй решетке, но $\text{гр}(1)$ — это вся группа \mathbb{Z} . Если $A = \text{гр}(a)$ и $B = \text{гр}(b)$ — две подгруппы из \mathbb{Z} , то пересечение $A \cap B$ порождается наименьшим общим кратным $[a, b]$, а $\text{гр}(a, b)$ поро-

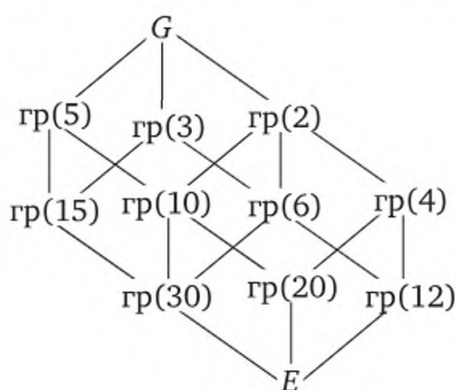
дается наибольшим общим делителем (a, b) . Это значит, что граф одной из решеток получается из графа второй поворотом на 180° .

Если $n = km$, то в группе $\text{гр}(a)$ порядка n найдется в точности один элемент порядка m , а именно a^k . Это значит, что если циклическая группа G состоит из n элементов, то для любого натурального делителя m числа n в группе G существует в точности одна подгруппа порядка m .

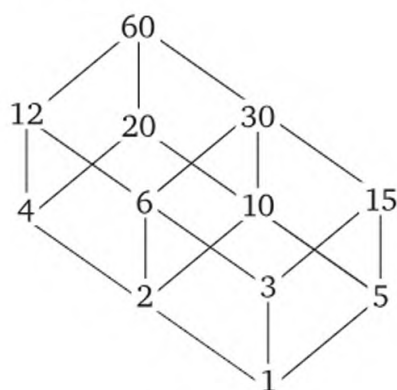
Таким образом, между подгруппами циклической группы порядка n и натуральными делителями числа n устанавливается взаимно однозначное соответствие.

Если подгруппе $\text{гр}(a)$ поставить в соответствие число a , то будет снова антиизоморфизм, такой же, как и в случае бесконечной циклической группы. Однако можно устроить и точное (т. е. сохраняющее отношение порядка без «переворачиваний») отображение. Для этого достаточно подгруппу $\text{гр}(a)$ отобразить в число $\frac{n}{a}$.

Решетка подгрупп циклической группы порядка n и решетка отношения делимости на множестве натуральных делителей числа n изоморфны. На рисунке изображены две решетки (подгрупп и натуральных делителей числа) для $n = 60$.



Решетка подгрупп



Решетка делителей

Кроме строения решетки подалгебр, алгебру характеризуют и ее полугруппа эндоморфизмов, и группа автоморфизмов.

При эндоморфизме порождающий элемент прообраза переходит в порождающий элемент образа. Поэтому каждому неотрицательному числу соответствует единственный эндоморфизм группы $\langle \mathbb{Z}; + \rangle$, причем отображение f_m , переводящее каждое целое число x в mx , сохраняет операции. Это значит, что полугруппа эндоморфизмов бесконечной циклической группы изоморфна мультипликативной полугруппе целых неотрицательных чисел.

В бесконечной циклической группе лишь два элемента (1 или -1) могут быть выбраны в качестве порождающих. При автоморфизме порождающий элемент переходит снова в порождающий

этой же группы, поэтому группа автоморфизмов бесконечной циклической группы является циклической второго порядка.

В курсе линейной алгебры было показано, что проблема вхождения в подпространства конечномерных векторного пространства имеет алгоритмическое решение (например, в виде теоремы Кронекера — Капелли).

Проблему вхождения можно поставить для любых алгебр, в том числе и для групп. Говорят, что в группе алгоритмически разрешима *проблема вхождения*, если существует алгоритм, позволяющий ответить, для любого набора ее элементов $\alpha_1, \alpha_2, \dots, \alpha_n, \beta$, принадлежит элемент β подгруппе $\text{гр}(\alpha_1, \alpha_2, \dots, \alpha_n)$ или нет. Проблема вхождения для групп решается не так просто, как для векторных пространств, а иногда и не решается вовсе.

Для конечных групп (в том числе и конечных циклических) можно считать эту проблему всегда разрешимой (хотя бы с помощью простого перебора вариантов).

Для бесконечной циклической группы тоже не возникает особой трудности в решении проблемы вхождения в конечно порожденную подгруппу. Конечно порожденная (впрочем, и бесконечно порожденная тоже) подгруппа бесконечной аддитивной циклической группы является циклической, порожденной некоторым элементом d . Если элемент β делится на этот d , то β принадлежит $\text{гр}(d)$, а если не делится, то не принадлежит. Таким образом, решение проблемы вхождения в бесконечной циклической группе сводится к вычислению наибольшего общего делителя конечного набора целых чисел, т. е., по существу, к алгоритму деления. В бесконечной циклической группе проблема вхождения алгоритмически разрешима.

Аналогичным образом в этой группе решается проблема пересечения: по любым двум конечным наборам целых чисел $\alpha_1, \alpha_2, \dots, \alpha_n$ и $\beta_1, \beta_2, \dots, \beta_m$ всегда можно найти порождающие элементы для подгруппы

$$\text{гр}(\alpha_1, \alpha_2, \dots, \alpha_n) \cap \text{гр}(\beta_1, \beta_2, \dots, \beta_m).$$

В бесконечной циклической группе алгоритмически разрешима проблема пересечения.

Итак, циклические группы поддаются изучению. И в классе всех циклических групп разрешима проблема изоморфизма, и в самих группах особых трудностей не возникает.

Может быть, похожая ситуация наблюдается с группами, обладающими двумя порождающими элементами?

Группа является *два-порожденной*, если в ней существуют два элемента такие, что любой элемент группы является произведением степеней этих двух элементов.

Не каждая группа является *два-порожденной*: конечно порожденная группа не более чем счетна, поэтому любая несчетная груп-

па (например, аддитивная группа действительных чисел) не порождается никаким конечным (и даже никаким счетным) множеством элементов.

Однопорожденные, т. е. *циклические*, группы оказались устроенными несложно.

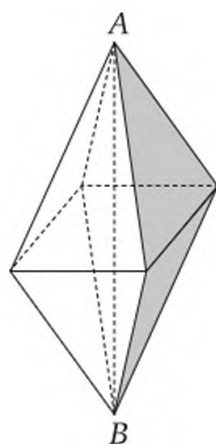
С два-порожденными группами ситуация намного сложнее.

Симметрическая группа порождается двумя элементами, а каждая конечная группа изоморфно вложима в симметрическую группу. Поэтому каждая конечная группа изоморфно вложима в два-порожденную группу.

В действительности имеет место гораздо более общий факт: *каждая счетная группа вложима в два-порожденную простую группу*.

Это означает, что внутреннее устройство два-порожденной группы может оказаться весьма сложным. Впрочем, если ограничить порядки порождающих элементов числом два, то такие группы устроены ненамного сложнее циклических.

Рассмотрим группы с двумя порождающими, каждый из которых имеет порядок два. Такие группы называют *группами диэдра*. Эта группа совпадает с самосовмещениями «двугранника» — двумя правильными пирамидами с общим основанием. На рисунке изображен диэдр, построенный с помощью четырехугольных пирамид.



Диэдр

Группа движений плоскости, переводящих правильный n -угольник на себя, порождается двумя элементами второго порядка — это пример диэдральной группы.

Если длину стороны правильного n -угольника зафиксировать (например, положить равным 1), а число n начать увеличивать, то угол между сторонами в пределе превратится в развернутый, а многоугольник — в прямую с отмеченными на ней целочисленными точками. Диэдр (двугранник) будет представлен двумя «гранями» — полуплоскостями, задаваемыми этой прямой.

Любая диэдральная группа является гомоморфным образом бесконечной диэдральной группы. Поэтому любая диэдральная группа имеет представление

$$G = \langle x, y, x^2, y^2, (xy)^n \rangle.$$

Например, группа диэдра, изображенного на рисунке, имеет представление

$$G = \langle x, y, x^2, y^2, (xy)^4 \rangle.$$

Если G — конечная группа движений и H — ее подгруппа, состоящая из движений, сохраняющих ориентацию, то H нормальна в G и индекс $|G : H|$ равен двум. Движением конечного порядка, сохраняющим ориентацию, может быть только вращение. Это значит, что если G — конечная группа движений плоскости, то G или циклическая, или содержит циклическую подгруппу H такую, что индекс H в G равен двум.

Это свойство позволяет описать все конечные группы движений. Это описание (разумеется, не строгое и не в алгебраических терминах) впервые получено Леонардо да Винчи¹, поэтому по традиции следующий факт называют *теоремой Леонардо да Винчи*: каждая конечная группа движений плоскости — это подгруппа группы самосовмещений правильного n -угольника.

Простейшие свойства и примеры групп уже рассматривались в предыдущих темах. В первой теме обсуждались свойства, следующие непосредственно из определения, в главах, посвященных числам (целым и комплексным), появились примеры циклических групп.

В одном важном, но частном случае появилось понятие отношения сравнимости по модулю подгруппы и индекса подгруппы. Сейчас эти и смежные понятия получают необходимую общность.

4.3. Смежные классы и сравнимость по модулю подгруппы

Каждая неединичная группа G содержит по крайней мере две подгруппы — единичную E и саму себя. Эти подгруппы принято называть *тривиальными*.

Любая нетривиальная подгруппа H группы G является промежуточной между тривиальными: $E < H < G$. Таким образом, единичная

¹ Леонардо да Винчи (Leonardo da Vinci, 1452—1519) — итальянский живописец, скульптор, архитектор, ученый и инженер, один из величайших деятелей эпохи Возрождения.

подгруппа E находится на наибольшей глубине в группе G . Сама G в качестве своей подгруппы представляет случай наиболее мелко-го вложения подгруппы в группу.



$$G > H > E$$

Как измерить промежуточные глубины?

Какая связь между порядком группы G и порядком ее подгруппы H ?

Для ответа на эти вопросы введем на группе G *отношение сравнимости* по модулю подгруппы H по правилу

$$x \equiv y(\text{mod } H) \stackrel{\text{опр}}{\Leftrightarrow} x \cdot y^{-1} \in H.$$

Фактически дословно повторяя доказательство для подгруппы (m) в группе целых чисел, получаем, что и в общем случае *отношение сравнимости по модулю подгруппы является отношением эквивалентности*.

В традиционном определении отношения эквивалентности участвуют три свойства: рефлексивность, транзитивность и симметричность. В определении подгруппы H также три свойства: H содержит единицу, H замкнуто относительно умножения и H замкнуто относительно взятия обратного.

Каждое из этих свойств подгруппы точно соответствует одному из свойств эквивалентности.

Самая маленькая эквивалентность — на множестве — это равенство, самая большая — полное отношение. Любая другая эквивалентность является промежуточной между этими двумя. Эти две эквивалентности на группе возникают благодаря тривиальным подгруппам — вся группа дает полное отношение, т. е. весь декартов квадрат $G \times G$, а единичная подгруппа E — равенство. Отношение равенства в группе является частным случаем отношения сравнимости по модулю подгруппы.

Как и любая эквивалентность, сравнимость по модулю подгруппы разобьет множество группы G на *смежные классы*.

Например, в аддитивной группе целых чисел множество (m) , состоящее из всех кратных числа m ($m > 0$), образует подгруппу. Отно-

шение сравнимости по модулю этой подгруппы, записанное на аддитивном языке, принимает вид

$$x \equiv y(\bmod(m)) \Leftrightarrow x - y \in (m).$$

Скобки вокруг m принято опускать, а принадлежность разности $x - y$ множеству (m) означает, что $x - y$ делится на m . С этими уточнениями определение сравнимости по модулю подгруппы становится следующим:

$$x \equiv y(\bmod m) \Leftrightarrow m \mid x - y.$$

Вернемся к нашему общему случаю, т. е. к группе G , записанной мультипликативно, ее подгруппе H и отношению сравнимости по модулю этой подгруппы.

Если x — элемент из G , то смежный класс с представителем x имеет вид

$$\begin{aligned} [x] &= \{y \in G \mid y \equiv x(\bmod H)\} = \{y \in G \mid y \cdot x^{-1} \in H\} = \\ &= \{y \in G \mid y \cdot x^{-1} = h, h \in H\} = \{y \in G \mid y = hx, h \in H\} = \{hx \mid h \in H\}. \end{aligned}$$

Итак, смежный класс $[x]$ совпадает с множеством $\{hx \mid h \in H\}$.

Последнее множество имеет особое название и обозначение.

Множество $Hg = \{hg \mid h \in H\}$, состоящее из всех произведений hg , где h пробегает все множество H , называют *правым смежным классом по подгруппе H с представителем g* .

Смежный класс отношения сравнимости по модулю подгруппы H — это в точности правый смежный класс по H , т. е.

$$Hx = Hy \Leftrightarrow x \equiv y(\bmod H).$$

Как и для любой эквивалентности, любой элемент из класса может быть выбран в качестве его представителя: для каждой подгруппы H и любых элементов x, y выполняется свойство

$$Hx = Hy \Leftrightarrow y \in Hx,$$

в частности $H = Hy \Leftrightarrow y \in H$.

Множество смежных классов на множестве M по эквивалентности \sim принято называть *фактор-множеством* и обозначать символом M/\sim . Мощность множества A обычно обозначают символом $|A|$, т. е. $|M/\sim|$ — это мощность фактор-множества M/\sim .

Таковы общие правила, но в рассматриваемой ситуации по традиции приняты другие обозначения. Множество смежных классов по отношению сравнимости по модулю подгруппы обозначают символом $G : H$, соответственно, символ $|G : H|$ обозначает число смежных классов по модулю H . Это число называют *индексом подгруппы H в группе G* .

Если Hg_1, Hg_2, \dots, Hg_n — все правые смежные классы в группе G по подгруппе H , то G является объединением этих непересекающихся множеств:

$$G = Hg_1 \cup Hg_2 \cup \dots \cup Hg_n = \coprod_{i=1}^n Hg_i.$$

И здесь есть своя, идущая еще с конца XVIII в. традиция в обозначениях. Вместо знака объединения используется знак сложения (+), т. е. пишут:

$$G = Hg_1 + Hg_2 + \dots + Hg_n.$$

Эту запись называют *правосторонним разложением* группы G по подгруппе H .

Аналогично можно определить и *левостороннее разложение* группы по подгруппе:

$$G = s_1H + s_2H + \dots + s_mH.$$

Левому разложению соответствует своя сравнимость по модулю подгруппы, также являющаяся эквивалентностью. Число элементов в левом классе Hx в точности равно числу элементов в xH . Поэтому нет необходимости говорить о левом или правом индексе — они равны: $m = n$.

Понятно, что если группа G абелева, то эти два разложения (левое и правое) полностью совпадают. Они совпадают и тогда, когда для каждого x из G выполняется равенство $Hx = xH$. Это произойдет тогда и только тогда, когда $x^{-1}Hx = H$, т. е. тогда, когда H — нормальный делитель в G .

Рассмотрим разложения по тривиальным подгруппам. По подгруппе G существует всего один смежный класс, так что разложение группы G по подгруппе G выглядит совершенно тривиально (точнее, тавтологично): $G = G$.

Если G конечна и g_1, g_2, \dots, g_n — все ее элементы, то каждый смежный класс по единичной подгруппе E состоит в точности из одного элемента и правостороннее разложение по единичной подгруппе E имеет вид

$$G = Eg_1 + Eg_2 + \dots + Eg_n = \{g_1\} + \{g_2\} + \dots + \{g_n\}.$$

Таким образом, тривиальные подгруппы — наибольшая и наименьшая в решетке подгрупп — имеют, соответственно, наибольшее и наименьшее значение своих индексов:

$$|G : G| = 1, \quad |G : E| = |G|.$$

Любая другая, промежуточная подгруппа имеет индекс i , который является промежуточным между единицей и порядком группы: $1 < i < |G|$.

Индекс подгруппы — вот что измеряет глубину погружения подгруппы в группу: чем больше индекс, тем глубже находится подгруппа. Если A, B — две подгруппы группы G и A содержится в B , то каждый смежный класс по B будет содержать несколько смежных классов по A .

Если A, B — подгруппы группы G и $A \leq B$, то

$$|G:B| \leq |G:A|.$$

Различные подгруппы группы G могут иметь одинаковые индексы, и наоборот — изоморфные подгруппы группы G могут иметь различные индексы. Как и порядки групп, различают конечные и бесконечные индексы.

Если H имеет бесконечный индекс в G , то и любая подгруппа H будет иметь бесконечный индекс в G . В частности, индекс пересечения $A \cap B$ в G бесконечен, если хотя бы один из индексов — $|G:A|$ или $|G:B|$ — бесконечен.

Другими словами, если индекс пересечения двух подгрупп конечен, то обе подгруппы имеют конечный индекс. Обратное утверждение тоже верно. Если $D = A \cap B$, то два элемента сравнимы по модулю D тогда и только тогда, когда они сравнимы по модулю A и по модулю B . Это значит, что смежный класс Dg получается как пересечение смежного класса Ag и смежного класса Bg . Поскольку число всевозможных непустых пересечений ограничено, в случае конечных индексов A в G и B индекс D тоже ограничен.

Если A, B — подгруппы в группе G , то $|G:A \cap B| \leq |G:A| \cdot |G:B|$.

В частности, это означает, что если A, B — подгруппы конечного индекса в группе G , то и пересечение $A \cap B$ имеет конечный индекс в G .

Таким образом, множество подгрупп конечного индекса в группе G образует подрешетку в решетке $L(G, E)$ всех подгрупп группы G .

Если порядок $|G|$ группы G конечен, то порядок $|H|$ и индекс $|G:H|$ ее подгруппы H также являются конечными. Связь между этими тремя числами установлена французским математиком Лагранжем¹ еще в XVIII в.

Все смежные классы отношения сравнимости по модулю подгруппы H равноможны. Действительно, каждый смежный класс Hg получается умножением всех элементов из H на g , и все эти произведения различны.

¹ Жозеф Луи Лагранж (Lagrange, 1736—1813) — французский математик и механик, иностранный член Петербургской академии наук (с 1776 г.). Цитируемая теорема о подгруппах конечных групп доказана им в 1773 г.

Один из смежных классов по подгруппе H — это сама подгруппа H . Это значит, что каждый смежный класс содержит столько же элементов, сколько и подгруппа H , т. е. $|H|$.

Число классов равно $|G : H|$, а общее число элементов в группе равно $|G|$. Следовательно, если H — подгруппа конечной группы G , то

$$|G| = |G:H| \cdot |H|.$$

Это свойство конечных групп называют по имени автора теоремы Лагранжа.

Иногда такой *точной* связи между порядком группы, порядком подгруппы и индексом подгруппы не требуется, а достаточно лишь следствия из теоремы Лагранжа: *порядок подгруппы делит порядок группы*.

Из-за этого свойства подгруппы конечных групп первоначально так и назывались: «делители группы». От той давней традиции в современном обиходе остались лишь слова «нормальный делитель».

Процедура поиска смежных классов по подгруппе H в конкретной группе G состоит в отделении сначала самой H , затем в нахождении смежного класса, представителем которого является любой элемент g из $G \setminus H$, после чего разыскивается любой элемент из $G \setminus (H \cup Hg)$ и т. д.

Рассмотрим два вычислительных примера.

Пусть S — симметрическая группа четвертой степени, т. е. $S = \text{гр}((12), (1234))$, а K — ее подгруппа, порожденная подстановками (12) (34) и (14) (23) , — четверная группа Клейна¹: $K = V_4$.

Найдем смежные классы по K в группе S (а точнее, укажем представителей этих классов). Вычисления (ручные или машинные) показывают, что этими представителями являются подстановки:

$$e, (2\ 4\ 3), (34), (2\ 3\ 4), (2\ 3), (2\ 4).$$

Это значит, что группу S можно разложить по модулю K следующим образом:

$$S = K + K(243) + K(34) + K(234) + K(23) + K(24).$$

Индекс K в S равен числу смежных классов, т. е. шести, $|S : K| = 6$.

Слова «можно разложить» означают, что есть и другие разложения, так как любой элемент из смежного класса является *полноправным представителем* своего класса.

Заметим, что по теореме Лагранжа порядок подгруппы K равен 4:

$$|K| = \frac{|S|}{|S : K|} = \frac{4!}{6} = 4.$$

¹ Феликс Христиан Клейн (Klein; 1849—1925) — немецкий математик и педагог.

Действительно,

$$K = \{e, (12)(34), (14)(23), (13)(24)\}.$$

Прделаем еще одно вычисление, на этот раз в группе, заданной комбинаторным представлением.

Пусть группа G задана представлением

$$G = \langle a, b, c; abca^{-1}b^{-1} = 1, bcabc^{-1} = 1, cabca^{-1} \rangle,$$

а H — ее подгруппа, порожденная элементом ab .

Найдем представителей смежных классов по подгруппе H в группе G . Вычисления показывают, что это элементы

$$1, a, c^2, c, ca, cacs, aca.$$

Следовательно, индекс H в G равен 7, а правостороннее разложение группы G имеет вид

$$G = H + Ha + Hc^2 + Hc + Hca + Hcas + Haca.$$

Отметим, что порядок группы G равен 63, поэтому подгруппа H состоит из девяти элементов.

Рассмотрим теперь примеры чуть более общего характера.

При фиксированном числе n четные подстановки составляют ровно половину всех подстановок. Это значит, что индекс знакопеременной подгруппы A_n в симметрической группе S_n равен двум.

Рассмотрим второй пример. Движения плоскости первого рода образуют подгруппу в группе всех движений. Произведение движения первого рода и движения второго рода дает движение второго рода. Поэтому группа движений распадается на два смежных класса по подгруппе движений, сохраняющих ориентацию. Иначе говоря, индекс подгруппы движений первого рода в группе всех движений плоскости равен двум.

Индекс, равный двум, имеет особое значение для свойства подгруппы.

Пусть G — группа, а H — подгруппа индекса 2. Вместо правостороннего разложения группы G на смежные классы Hg можно было разложить группу на левые классы gH . В произвольной группе эти классы, вообще говоря, не совпадают (хотя и равномощны). Однако если классов всего два и один из них — сама подгруппа H , то $Hg = gH$, где $g \notin H$.

В другой записи $g^{-1}Hg = H$. Если g принадлежит H , то это равенство (верное для любой подгруппы) тоже выполняется. Иначе говоря, в любой группе подгруппа индекса два является нормальным делителем.

Группа — частный случай полугруппы, и распространение теоремы Лагранжа на класс полугрупп было бы ее обобщением. Однако обобщение теоремы Лагранжа не выполняется. В мультипликативной полугруппе $\langle \{0; 1, -1\}; \cdot \rangle$ есть подполугруппы, состоящие из двух элементов, так что порядок подполугруппы не обязательно является делителем порядка полугруппы.

Теорема Лагранжа позволяет легко найти решетку подгрупп групп простого порядка. В ней всего два элемента, так как если порядок группы — простое число, то у такой группы нет подгрупп, кроме тривиальных.



Решетка подгрупп группы простого порядка

Это означает, в частности, что все группы, порядок которых — простое число, имеют изоморфные структуры подгрупп. Иначе говоря, структура подгрупп группы G не задает однозначно саму группу G .

Заметим еще, что найти индекс в конкретной конечно определенной группе может оказаться очень непросто. Алгоритма, решающего эту проблему для конкретной группы, может не существовать в природе.

Рассмотрим прямое произведение G двух свободных групп на двух порождающих:

$$G = \langle a, b \rangle \times \langle c, d \rangle = \langle a, b, c, d; ac = ca, ad = da, bc = cb, bd = db \rangle.$$

Оказалось, что для этой группы нет алгоритма, позволяющего вычислить индекс произвольной подгруппы, порожденной конечным числом элементов.

Правда, если индекс конечен (и сравнительно невелик), то он будет вычислен с помощью вычислительной техники. Например, подгруппа N , порожденная элементами $a^2, baba^{-1}, c^2, d, xdx^{-1}$, является нормальным делителем группы G , причем фактор-группа по этому нормальному делителю — это прямое произведение двух групп порядка два.

Однако алгоритма для узнавания, конечен или бесконечен этот индекс для произвольно выбранной подгруппы, не существует, поэтому если при машинном вычислении техника работает подозрительно долго, то это может означать, что индекс или бесконечный, или конечный (но слишком большой), но узнать заранее, какая именно сейчас ситуация, невозможно.

Вернемся к ситуации двух подгрупп группы G , причем одна из них содержится в другой. Непосредственно из определения ин-

декса видно, что индекс меньшей подгруппы не меньше индекса большей. После того как обнаружили равномощность смежных классов, можно сказать об этом точнее: *если A, B — подгруппы группы G и $A \leq B$, то*

$$|G : B| = |G : A| \cdot |B : A|.$$

Это утверждение обобщает теорему Лагранжа. Действительно, если A — единичная подгруппа, то

$$|G : A| = |G| \text{ и } |B : A| = |B|$$

и последнее выделенное утверждение превращается в теорему Лагранжа для подгруппы B .

4.4. Гомоморфизмы и нормальные делители

Под словом «гомоморфизм» будем сейчас понимать эпиморфизм, т. е. сюръективный гомоморфизм.

Как и в произвольной алгебре, основой гомоморфизма является отношение конгруэнции, т. е. эквивалентность, согласованная с операцией группы.

Эквивалентность \sim , заданная в группе $G = \langle G; \cdot \rangle$, согласована с операцией группы, если для каждого a_1, a_2, b_1, b_2 из G

$$a_1 \sim b_1, a_2 \sim b_2 \Rightarrow a_1 \cdot a_2 \sim b_1 \cdot b_2.$$

Напомним, что гомоморфный образ алгебры является как бы уменьшенной моделью изучаемого объекта. Изучение крупного (обычно бесконечного) алгебраического объекта может быть проведено с помощью его гомоморфного образа (или серии гомоморфных образов).

Изучение гомоморфизма группы G , т. е. некоторой внешней связи изучаемой группы с другими группами, можно производить, оставаясь в самой G .

Как и в любой алгебре, гомоморфизм группы задает отношение конгруэнции на множестве-носителе этой системы.

Действительно, ядерная эквивалентность, заданная гомоморфным отображением, согласована с операцией группы, т. е. является конгруэнцией.

Верно и обратное утверждение. Если на группе G задано отношение конгруэнции, то множество смежных классов по этой эквивалентности с операцией, определенной по представителям,

$$[x] \cdot [y] \stackrel{\text{опр}}{=} [x \cdot y]$$

образует гомоморфный образ группы G .

Таким образом, отношение конгруэнции на группе определяет гомоморфизм этой группы. Заметим, что пересечение любого числа конгруэнций группы G снова является конгруэнцией в G . Поэтому можно говорить о решетке конгруэнций на группе.

Итак, описание гомоморфизмов G сводится к описанию ее конгруэнций.

Пусть f — гомоморфное отображение группы $G = \langle G; \cdot \rangle$ на группу $G_1 = \langle G_1; \cdot \rangle$.

Как и при гомоморфизмах произвольных алгебр, особое внимание уделим полному прообразу нейтрального элемента. Нейтральный элемент в рассматриваемой ситуации — это единица e в группе G_1 .

Полный прообраз элемента e называют *ядром* (группового) гомоморфизма. Обычно ядро гомоморфизма f обозначают символом¹ $\text{Ker } f$:

$$\text{ядро } f = \text{Ker } f = \{x \in G \mid f(x) = e\}.$$

Напомним, что ядро линейного отображения оказалось подпространством, и наоборот, каждое подпространство является ядром некоторого линейного отображения.

Какая связь между гомоморфизмами группы и ее подгруппами? Используя критерий свойства «быть подгруппой», устанавливаем, что ядро гомоморфизма является подгруппой. Каждая ли подгруппа может быть ядром некоторого гомоморфизма?

Если отображение f является гомоморфизмом, то соответствующая ему ядерная эквивалентность должна быть конгруэнцией. Выясним, как выглядит ядерная эквивалентность для группового гомоморфизма. Пусть H — ядро гомоморфизма $f : G \rightarrow G_1$. Равенство $f(x) = f(y)$ равносильно $f(xy^{-1}) = e$, откуда

$$f(x) = f(y) \Leftrightarrow x \equiv y \pmod{H}.$$

Отсюда следует, что в группе G_1 содержится в точности столько же элементов, сколько и в фактор-множестве $G : H$:

$$|G_1| = |G : H|.$$

Поскольку f — гомоморфизм, сравнимость по модулю H согласована с операцией:

$$x \equiv x_1 \pmod{H}, y \equiv y_1 \pmod{H} \Rightarrow xy \equiv x_1 y_1 \pmod{H}.$$

Итак, если H — ядро гомоморфизма f , то сравнимость по модулю H является конгруэнцией.

¹ От нем. *Kern* — «ядро».

Верно и обратное утверждение: если сравнимость по модулю подгруппы H является конгруэнцией в группе G , то H — ядро гомоморфизма группы G .

Любая подгруппа, сравнимость по модулю которой не является конгруэнцией, не может быть ядром никакого гомоморфизма. Например, если $n > 2$, то любая подгруппа, порожденная одной транспозицией, задает эквивалентность в S_n , но эта эквивалентность — не конгруэнция.

Следовательно, *не каждая подгруппа группы G является ядром некоторого гомоморфизма группы G .*

Каким же свойством должна обладать подгруппа H , чтобы сравнимость по модулю оказалась конгруэнцией?

Из равенств

$$x_1 = h_1 x, \quad y_1 = h_2 y$$

должно следовать

$$x_1 y_1 = h_3 x y,$$

где h_1, h_2, h_3 — элементы из H . Нужно равенство получается тогда и только тогда, когда для каждого элемента h из H и каждого элемента x из G найдется такой элемент h' , что $hx = h'x$ или, в другой записи,

$$xhx^{-1} \in H.$$

Это значит, что ядро гомоморфизма группы G — не просто подгруппа. *Ядро гомоморфизма группы G является нормальной подгруппой в G .*

Впрочем, нормальную подгруппу чаще называют *нормальным делителем*.

Напомним, что элемент gxg^{-1} называется *сопряженным* для элемента x , а подгруппа H является нормальным делителем в группе G , если она вместе с каждым своим элементом x содержит и все его сопряженные в G элементы.

Обратим внимание на то, что отношение сопряженности рефлексивно, симметрично и транзитивно, т. е. является отношением эквивалентности на группе. Как каждая эквивалентность, отношение сопряженности разбивает группу на классы сопряженных элементов.

В отличие от смежных классов по подгруппе классы сопряженных элементов, вообще говоря, неравномощны. В любой группе есть класс сопряженных элементов, состоящий только из одного элемента. Если и все остальные классы сопряженных одноэлементные, то группа абелева. Верно и обратное: если классы сопряженных элементов группы G равномощны, то G абелева.

Это простое наблюдение легко обобщается следующим образом. *Класс сопряженных элементов состоит в точности из одного элемента тогда и только тогда, когда этот элемент центральный.*

Подгруппа является нормальным делителем тогда и только тогда, когда состоит из нескольких смежных классов по отношению эквивалентности.

Равенство $xh = h'x$, где h — элемент из нормального делителя H , а x — произвольный элемент из группы G , означает, что для каждого x множества Hx и xH совпадают. Верно и обратное утверждение: если правостороннее и левостороннее разложения группы G по подгруппе H совпадают, то H замкнуто относительно взятия сопряжений. Таким образом, снова видим уже знакомый факт: группа H является нормальным делителем группы G тогда и только тогда, когда левостороннее разложение группы G по H совпадает с правосторонним.

Отметим связь между гомоморфизмами и нормальными делителями группы.

Во-первых, непосредственно из определения гомоморфизма следует, что ядро замкнуто относительно взятия сопряжений, поэтому является нормальным делителем в гомоморфном прообразе.

Во-вторых, если на группе G задана конгруэнция, то множество N всех элементов, конгруэнтных единице группы G , является нормальным делителем группы G и эта конгруэнция совпадает со сравнимостью по модулю N .

Но если N — нормальный делитель группы G , то отношение сравнимости по модулю N является конгруэнцией. Это значит, что *каждый нормальный делитель группы является ядром некоторого гомоморфизма.*

Гомоморфный образ алгебры, построенный с помощью конгруэнции на этой алгебре, называют *фактор-алгеброй*. Для групп фактор-алгебра называется *фактор-группой*.

Обсудим построение фактор-групп и их свойства более подробно.

Итак, пусть N — нормальный делитель группы G . Отношение сравнимости по модулю N разбивает множество G на смежные классы. Фактор-множество $G : N$, состоящее из смежных классов по нормальному делителю N , принято обозначать символом G / N . Таким образом,

$$G / N = \{Hx \mid x \in G\}.$$

На этом множестве определим операцию по правилу

$$(Hx) \cdot (Hy) = H(x \cdot y).$$

Группа $\langle G / N; \cdot \rangle$ является фактор-группой группы G по нормальному делителю N .

Роль единицы в фактор-группе играет смежный класс N . Отображение $\varepsilon : G \rightarrow G / N$, переводящее каждый элемент x в свой смежный класс Nx , является гомоморфизмом. Этот гомоморфизм принято называть *естественным*. Ядром естественного гомоморфизма является нормальный делитель N .

Таким образом, *каждый нормальный делитель N группы G является ядром естественного гомоморфизма группы G на фактор-группу G / N .*

В качестве примера рассмотрим взаимоотношения симметрической группы S_n и знакопеременной группы A_n .

Группа A_n является нормальным делителем в группе S_n , а фактор-группа S_n / A_n циклическая и состоит из двух элементов. Отображение, переводящее каждую подстановку в ее знак, является гомоморфизмом группы S_n на группу $G_1 = \langle \{1, -1\}; \cdot \rangle$.

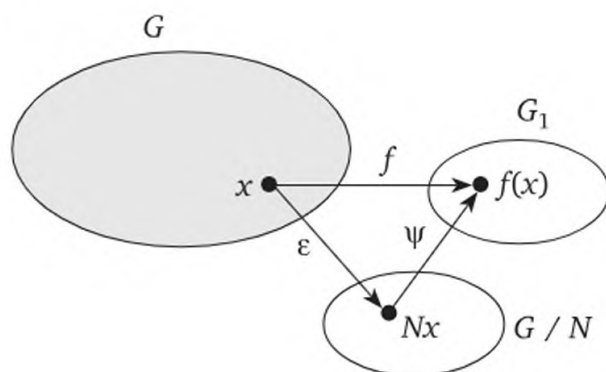
Заметим, что гомоморфизм $f : S_n \rightarrow G_1$ можно заменить естественным гомоморфизмом $\varepsilon : S_n \rightarrow S_n / A_n$ на фактор-группу S_n по нормальной подгруппе A_n . Такая замена возможна всегда — для любой группы и любого гомоморфизма этой группы. Утверждение о возможности такой замены носит название *теоремы о гомоморфизмах групп*.

Пусть f — гомоморфизм группы G на группу G_1 и $\text{Ker } f = N$. Вместе с данным отображением f и естественным гомоморфизмом ε определим соответствие $\psi : G / N \rightarrow G_1$ по правилу

$$\psi(Nx) = f(x).$$

Это соответствие является биективным и сохраняет операцию, т. е. группы G / N и G_1 изоморфны.

Итак, *гомоморфный образ группы изоморфен фактор-группе по ядру гомоморфизма.*



К теореме о гомоморфизмах групп

Это утверждение носит название *теоремы о гомоморфизмах групп*.

Для наглядности изобразим ситуацию на схеме.

Формулировку теоремы о гомоморфизмах можно уточнить. Из построения ψ видно, что любой гомоморфизм групп является произведением естественного гомоморфизма и некоторого изоморфизма. Другими словами, с точностью до изоморфизма все гомоморфизмы групп естественные.

Бывают ли неестественные гомоморфизмы?

Единичная группа имеет лишь один (естественный) гомоморфизм — на саму себя. Если группа G имеет порядок два, то у нее лишь два гомоморфизма: тождественный, оставляющий каждый элемент неподвижным, и отображение на единичную подгруппу. Оба гомоморфизма естественные.

Для всех остальных групп можно указать и неестественное отображение.

Если группа G_1 имеет порядок больше двух, то кроме естественного гомоморфизма группы G на G_1 найдется и неестественный гомоморфизм. Чтобы это увидеть, достаточно указать хотя бы один неединичный автоморфизм группы.

Теорема о гомоморфизмах групп позволяет свести описание всех гомоморфных образов к описанию нормальных делителей этой группы и фактор-групп.

Группа G , имеющая лишь тривиальные нормальные делители, называется *простой*. Если группа проста, то она не имеет гомоморфизмов, отличных от изоморфизма и отображения на единичную группу.

Например, простой является группа простого порядка, так как из теоремы Лагранжа следует, что она вообще не содержит подгрупп, кроме тривиальных.

Простыми будут и все знакопеременные группы A_n при $n \geq 5$.

Свойства гомоморфного прообраза сохраняются в гомоморфном образе. Для того чтобы установить несуществование гомоморфизма двух групп G_1 и G_2 , достаточно указать сохраняющееся при гомоморфизме свойство группы G_1 , которым не обладает G_2 .

Например, при гомоморфизме сохраняются свойства конечности, абелевости, конечной порожденности. Поэтому не может бесконечная группа быть гомоморфным образом конечной, не может неабелева группа быть гомоморфным образом абелевой, не может бесконечно порожденная группа быть гомоморфным образом конечно порожденной.

Более тонкое разделительное свойство потребуется найти для групп рациональных чисел — аддитивной $\langle \mathbb{Q}; + \rangle$ и мультипликативной $\langle \mathbb{Q}_+; \cdot \rangle$. Обе они абелевы, обе бесконечные и даже бесконечно порожденные и без кручения. И все-таки не существует гомоморфизма аддитивной группы рациональных чисел на мультипликативную группу положительных рациональных чисел. Другими словами, есть абстрактное свойство, которым обладает одна

из групп и не обладает вторая. Одно из таких свойств уже было отмечено ранее: одна из групп неразложима в прямое произведение своих подгрупп, а другая — разложима. Есть, конечно, и другие различия. Например, в группе $\langle \mathbb{Q}; + \rangle$ уравнение $2x = a$ имеет решение для любого элемента a , но соответствующее ему при изоморфизме (если бы такой изоморфизм существовал) уравнение $x^2 = b$ разрешимо в группе $\langle \mathbb{Q}^*; \cdot \rangle$ не для всех элементов b .

Вспомним о разложимости группы в прямое произведение. Именно тогда в нашем обсуждении и появилось первое упоминание о нормальных подгруппах. Если группа G разлагается в прямое произведение своих подгрупп, $G = A \times B$, то каждый сомножитель является нормальным делителем и, следовательно, можно говорить о фактор-группе G / A или G / B .

Непосредственно из определения прямого произведения следует, что элементы одного из прямых множителей являются представителями смежных классов по другому множителю. Более того, умножению этих классов точно соответствует умножение элементов-представителей. Другими словами, если группа является прямым произведением двух своих подгрупп, то фактор-группа по любому из ее прямых множителей изоморфна второму множителю.

Группа G может содержать две подгруппы A и B , которые имеют единичное пересечение; комплекс AB совпадает с группой G , но только одна подгруппа (например, A) нормальна в G . Тогда группу G называют *полупрямым произведением*, но фактор-группа G / A и в этом случае будет изоморфна группе B . Пишут:

$$G = A \rtimes B.$$

Отмеченное ранее свойство симметрических групп означает, что для $n > 2$ симметрическая группа S_n является полупрямым произведением знакопеременной группы A_n и циклической группы второго порядка $C = \langle c; c^2 \rangle$:

$$S_n = A_n \rtimes C.$$

Рассмотрим еще один пример фактор-группы. Четверная группа Клейна V_4 образует нормальный делитель в группе S_4 . Найдем фактор-группу S_4 / V_4 группы S_4 по подгруппе V_4 . Представителями смежных классов по подгруппе V_4 являются элементы

$$e, (2\ 3), (3\ 4), (2\ 4\ 3), (2\ 3\ 4), (2\ 4). \quad (*)$$

Но это в точности элементы группы S_3 , записанной на символах 2, 3, 4. Точнее говоря, множество $(*)$ образует подгруппу в S_4 , и эта подгруппа изоморфна S_3 . Но это значит, что группа S_4 совпадает с комплексом $S_3 V_4$.

Правда, S_4 не является прямым их произведением (S_3 — не нормальная подгруппа в S_4), но подгруппа, состоящая из элементов (*), не содержит ни одного неединичного элемента из K .

Это значит, что S_4 образует полупрямое произведение S_3 и V_4 :

$$S_4 = V_4 \rtimes S_3.$$

Итак, мы нашли фактор-группу S_4 / V_4 и попутно установили строение¹ группы S_4 .

Представление группы в виде порождающего множества с определяющими соотношениями является особенно удобным, когда требуется получить представление фактор-группы. Пусть группа G задана своим представлением:

$$G = \langle a_1, a_2, \dots, a_n; R_1(a_i) = 1, R_2(a_i) = 1, R_k(a_i) = 1 \rangle.$$

Предположим далее, что $h_1(a_i), h_2(a_i), \dots, h_s(a_i)$ — произвольное множество элементов из группы G , записанных в порождающих a_i , а N — нормальное замыкание этого множества в G .

Тогда фактор-группа G / N имеет представление

$$G / N = \langle a_1, a_2, \dots, a_n; R_1(a_i) = 1, R_2(a_i) = 1, R_k(a_i) = 1; \\ h_1(a_i) = 1, h_2(a_i) = 1, \dots, h_s(a_i) = 1 \rangle.$$

В частности, это значит, что каждая группа на n порождающих является гомоморфным образом группы F_n с таким же числом порождающих, но без соотношений. Таким образом, группа F_n имеет представление

$$F_n = \langle a_1, a_2, \dots, a_n \rangle.$$

Группа F_n называется *свободной группой* ранга n . Если в группе G выполняются некоторые тождества, то в качестве прообраза G можно взять свободную группу, факторизованную по нормальному делителю, порожденному значениями этих тождеств в группе F_n . Такая группа называется *приведенной свободной*. Например, таковой будет фактор-группа свободной группы по ее коммутанту. Эта группа называется *свободной абелевой группой*. Каждая абелева группа — это гомоморфный образ свободной абелевой группы.

Отметим еще, что группа G проста тогда и только тогда, когда добавление к соотношениям группы G любого неединичного элемента этой группы задает единичную группу.

Рассмотрим несколько конкретных примеров фактор-групп.

¹ Из того, что в группе S_4 нет элементов шестого порядка, тоже легко следует, что группа S_4 / V_4 изоморфна S_3 .

В бесконечной группе диэдра

$$G = \langle a, b; a^2 = 1, b^2 = 1 \rangle$$

возьмем нормальное замыкание N элемента $(ab)^3$. Тогда фактор-группа $G_1 = G/N$ имеет представление:

$$G_1 = \langle a, b; a^2 = 1, b^2 = 1, (ab)^3 = 1 \rangle.$$

Группа G_1 состоит из шести элементов, а таких групп всего две — циклическая и S_3 . Какая именно группа перед нами?

Сначала выясним, как устроен нормальный делитель N и как сильно он отличается от подгруппы H , порожденной элементом $(ab)^3$. Для этого найдем индекс H в G . Этот индекс совпадает с индексом нормального делителя N , $|G:H| = |G:N|$. Из того, что $H \subset N$, следует $H = N$. Это значит, что подгруппа, порожденная множеством, совпадает с нормальным замыканием этого множества.

Найдем порядки элементов a , ab , aba , $abab$, $ababa$ по модулю $H = \text{гр}((ab)^3)$. Напомним, что элемент сравним с единицей по модулю H , если этот элемент принадлежит H .

Вычисляем:

$$\begin{aligned} a^2 &\equiv 1(\text{mod } H); \\ (ab)^3 &\equiv 1(\text{mod } H); \\ (aba)^2 &= abaaba = ab \cdot 1 \cdot ba \equiv 1(\text{mod } H); \\ (abab)^3 &= (ababab)^2 \equiv 1(\text{mod } H); \\ (ababa)^2 &= ababaababa \equiv 1(\text{mod } H). \end{aligned}$$

Это означает, что в фактор-группе G/N нет элементов порядка 6, следовательно, эта группа не циклическая, поэтому она изоморфна S_3 .

Пусть N — нормальный делитель группы G . Образно говоря, фактор-группа G/N является моделью группы G . При изучении G возможно, что на некоторые вопросы относительно группы G удастся ответить быстрее с помощью ее модели — группы G/N .

Например, при изучении решетки подгрупп $L(G)$ группы G мы можем сначала изучить решетку промежуточных между N и G подгрупп.

Решетка $L(G, N)$ промежуточных между G и N подгрупп изоморфна решетке всех подгрупп фактор-группы G/N . Нормальный делитель при этом изоморфизме переходит в нормальный делитель, а индексы подгрупп сохраняются.

Затем можно изучить поведение подгрупп, не лежащих в нормальном делителе и не являющихся промежуточными. Заметим

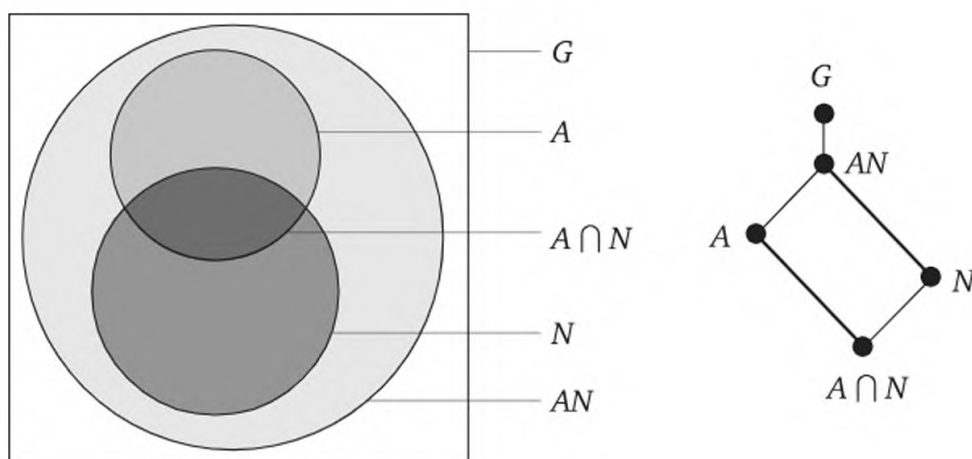
сначала, что если A — подгруппа, а N — нормальный делитель группы G , то множество

$$AN = \{an | a \in A, n \in N\}$$

является подгруппой группы G .

Если A — подгруппа, а N — нормальный делитель группы G , то $A \cap N$ является нормальным делителем в группе A . При естественном гомоморфизме ε группы A на фактор-группу $A / (A \cap N)$ образом группы A будет подгруппа $\varepsilon(A)$ группы $A / (A \cap N)$. Полным прообразом $\varepsilon^{-1}(\varepsilon(A))$ группы $\varepsilon(A)$ будет группа, большая, чем A . В полный прообраз попадут все элементы из ядра гомоморфизма — подгруппы $A \cap N$, а следовательно, и из подгруппы $\text{gr}(A, N)$. Группа N нормальна в группе G , поэтому

$$\text{gr}(A, N) = AN.$$



К теореме об изоморфизме

Никакой другой элемент группы G не переходит в $\varepsilon(A)$. Ограничением ядра отображения ε на подгруппе A является $A \cap N$. Это значит, что фактор-группа $(A / (A \cap N))$ изоморфна группе $\varepsilon(A)$, но группа AN / N тоже изоморфна $\varepsilon(A)$.

Итак, если A — подгруппа, а N — нормальный делитель группы G , то группы $(A / (A \cap N))$ и AN / N изоморфны.

Это предложение называют *теоремой об изоморфизме*.

На рисунке ситуация изображена двумя способами: в виде кругов Эйлера и в виде диаграммы Хассе — графа отношения включения. Видно, что вторая схема нагляднее. По существу, на второй схеме присутствуют и фактор-группы $(A / (A \cap N))$ и AN / N , которые изображены черными равными отрезками: равенство отрезков подчеркивает изоморфизм этих фактор-групп. Теперь, чтобы получить полное представление о решетке подгрупп группы G , остается лишь изучить решетку подгрупп группы N .

Группу можно изучать и иначе. Может оказаться, что она построена некоторым способом из более простых своих подгрупп. Одним из простейших способов построения алгебр является прямое произведение.

Довольно просто устроена циклическая группа. Несложно (и очень похоже на строение конечномерного векторного пространства) строение прямых произведений циклических групп.

Например, прямое произведение двух циклических групп порядка два имеет представление

$$\langle a, b; a^2 = 1, b^2 = 1, aba^{-1}b^{-1} = 1 \rangle,$$

где

$$\text{гр}(a) = \langle a; a^2 = 1 \rangle, \text{ гр}(b) = \langle b; b^2 = 1 \rangle.$$

Это четверная группа Клейна V_4 .

Мультипликативная группа ненулевых действительных чисел является прямым произведением мультипликативной группы положительных действительных чисел и группы $\langle \{1, -1\}; \cdot \rangle$.

Эта ситуация естественным образом обобщается на все множество комплексных чисел.

Мультипликативная группа ненулевых комплексных чисел является прямым произведением мультипликативной группы положительных действительных чисел и группы, состоящей из действительных чисел, модуль которых равен единице.

Две предыдущих группы несчетны, и поэтому устроены непросто. Множество рациональных чисел счетно. Мультипликативная группа, состоящая из 1 и -1 , входит в мультипликативную группу ненулевых рациональных чисел; поэтому, как и для действительных чисел, в группе $\langle \mathbb{Q}^*; \cdot \rangle$ можно выделить прямой множитель в виде циклической группы второго порядка.

Однако в группе \mathbb{Q}^* можно пойти значительно дальше. По основной теореме арифметики каждое натуральное число, большее единицы, можно представить единственным образом в виде произведения степеней простых чисел. Это значит, что мультипликативная полугруппа натуральных чисел является прямым произведением бесконечных однопорожденных (т. е. моногенных) полугрупп.

Единственность представления каждого рационального числа, большего единицы, в виде произведения целочисленных степеней простых чисел означает, что

$$\mathbb{Q}^* = \text{гр}(2) \times \text{гр}(3) \times \dots \times \text{гр}(p) \times \dots,$$

где p пробегает все множество простых чисел.

Таким образом, мультипликативная группа положительных рациональных чисел разложима в прямое произведение бесконечных циклических подгрупп.

Пересечение двух конгруэнций снова является конгруэнцией. Каждая конгруэнция на группе задается нормальным делителем, поэтому вопрос о том, что же представляет собой пересечение двух конгруэнций, — это вопрос о том, что можно сказать о фактор-группе по пересечению двух нормальных делителей.

Пусть A, B — нормальные делители группы G . Представим прямое произведение $(G/A) \times (G/B)$ внешним образом, т. е. как множество

$$\{(Ax, Bx) \mid x \in G\}$$

с покомпонентным умножением. Зададим отображение φ группы G в группу $(G/A) \times (G/B)$, полагая для каждого g из G

$$\varphi(g) = (Ag, Bg).$$

Отображение φ сохраняет операцию. Действительно,

$$\varphi(x \cdot y) = (Axy, Bxy) = (Ax, Bx) \cdot (Ay, By) = \varphi(x) \cdot \varphi(y)$$

и, следовательно, является гомоморфизмом. Роль единичного элемента в группе $(G/A) \times (G/B)$ играет пара (A, B) . Поэтому $\text{Ker } \varphi = A \cap B$.

Этим установлено, что если A, B — нормальные делители группы G , то фактор-группа $G/A \cap B$ изоморфно вкладывается в прямое произведение $(G/A) \times (G/B)$.

4.5. Абелевы, разрешимые и нильпотентные группы

Сначала упорядочим всю полученную ранее информацию о циклических группах.

Используя свойства первообразных корней из единицы (или свойства подстановок, или свойства порядка элемента из предыдущей темы) и изоморфизм циклических групп одинакового порядка, получаем, что прямое произведение двух конечных циклических групп взаимно простых порядков является циклической группой.

Прямое произведение двух конечных циклических групп, порядки которых не взаимно просты, не является циклической группой.

Если числа a и b взаимно просты, то прямое произведение двух циклических групп порядков a и b является циклической группой и состоит из ab элементов. Благодаря изоморфизму равномогущих циклических групп получаем, что *циклическая группа порядка ab ,*

где $\text{НОД}(a, b) = 1$, раскладывается в прямое произведение своих подгрупп порядков a и b .

Теперь покажем, что хотя в общем случае обращение теоремы Лагранжа и не выполняется, в некоторых частных случаях о существовании подгруппы заданного порядка в произвольной группе можно сказать что-то определенное.

Для начала сосредоточим свое внимание на абелевых группах.

Группа порядка p циклическая и, следовательно, содержит элемент порядка p . Индукцией по порядку n группы G покажем, что и любая другая абелева группа, порядок которой делится на p , содержит элемент порядка p .

Если абелева группа G имеет порядок $n = pt$ и содержит собственную подгруппу H , порядок которой делится на p , то по индукции H (а следовательно, и G) содержит нужный элемент. Если же порядок нетривиальной подгруппы не делится на p , то на p делится ее индекс. Пусть N — собственная подгруппа в G индекса pk , где $k < t$. Порядок N обозначим символом n_1 . Подгруппа N является нормальным делителем в G , фактор-группа G/N имеет порядок pk , поэтому G/N содержит элемент порядка p . Из теоремы об изоморфизме следует, что в группе G содержится подгруппа порядка pn_1 . Поскольку $pn_1 < pt$, можно снова воспользоваться индуктивной гипотезой.

Таким образом, если порядок конечной абелевой группы делится на простое число p , то в группе есть элемент порядка p .

Отсюда следует, что абелева группа проста тогда и только тогда, когда она конечна и порядок ее — простое число.

Покажем теперь, что конечно порожденная абелева группа является прямым произведением циклических групп.

Любая группа, имеющая n порождающих, является гомоморфным образом свободной группы на n свободных порождающих. Абелева группа — это гомоморфный образ свободной абелевой группы, т. е. группы, в которой определяющие соотношения — это лишь коммутаторы всех порождающих элементов.

Абелеву группу удобно записать на аддитивном языке. Тогда свободная абелева группа A на свободных порождающих a_1, a_2, \dots, a_n — это множество всевозможных линейных комбинаций вида

$$x_1 a_1 + x_2 a_2 + \dots + x_n a_n,$$

где x_i — целые числа. Образно говоря, такая группа образует как бы векторное пространство, только множество коэффициентов является не полем, а всего лишь кольцом (такое пространство называют *модулем*).

Как и для настоящих векторных пространств, элементы a_1, a_2, \dots, a_n называют *базисом* (или *базой*) свободной абелевой группы.

Аналогию с пространствами можно продолжить и далее. Все базисы векторного пространства можно получить из данного базиса с помощью элементарных преобразований первого и второго типа. В свободной абелевой группе такая же картина. Так, в кольце целых чисел обратимыми элементами являются лишь 1 и -1 , преобразованию первого типа соответствует замена одного из элементов базиса a_i на элемент $-a_i$. Преобразование второго типа повторяется буквально: если один из элементов базиса a_i заменить на $a_i + ka_j$, где $i \neq j$, то вновь полученная система снова будет базисом. С помощью комбинации элементарных преобразований можно получить перестановку двух элементов базиса.

Слово «базис» можно заменить словами «порождающая система». Это значит, что такими преобразованиями можно изменять не только базис всего пространства, но и порождающую систему любого подпространства, т. е. подгруппы свободной абелевой группы.

Пусть B — ненулевая подгруппа группы A , порожденная элементами b_1, b_2, \dots, b_m . Каждое b_j имеет единственное представление в виде линейной комбинации векторов базиса. Запишем все коэффициенты этих разложений в виде $(m \times n)$ -матрицы:

$$M = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix}.$$

Первоначально не предполагается, что подгруппа B обязательно конечно порождена, т. е. число строк в матрице M может быть бесконечным.

Элементарные преобразования столбцов матрицы M изменяют исходный базис другим базисом, а элементарные преобразования строк этой матрицы соответствуют изменению системы порождающих подгруппы B .

Рассмотрим все множество матриц, которые можно получить с помощью элементарных преобразований строк и столбцов из матрицы M . Среди таких матриц выберем матрицу с наименьшим по абсолютной величине ненулевым коэффициентом b_{ij} . Тогда все остальные элементы i -й строки и j -го столбца делятся на элемент b_{ij} (в противном случае с помощью элементарных преобразований можно получить элемент $< b_{ij}$).

С помощью элементарных преобразований можно сделать все элементы i -й строки и j -го столбца, кроме b_{ij} , нулевыми. Поменяем теперь i -ю строку на первую строку, а j -й столбец — на первый столбец. Теперь в левом верхнем углу полученной матрицы стоит ненулевой элемент, а все остальные элементы нулевые. Отделим

первую строку и первый столбец полученной матрицы и для оставшейся $(m - 1) \times (n - 1)$ -матрицы сделаем ту же самую процедуру.

Продолжим и далее таким же образом. В результате матрица примет диагональный вид

$$M_1 = \begin{pmatrix} d_1 & 0 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & d_2 & 0 & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & 0 & d_k & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{pmatrix}.$$

В этой матрице ненулевые элементы d_i расположены только по диагонали. В частности, если $m > n$, то внизу стоят заведомо нулевые строки. Этим строкам соответствуют нулевые элементы подгруппы B , и эти нулевые строки из матрицы можно удалить.

В получившемся новом базисе c_1, c_2, \dots, c_n подгруппа B имеет конечное число порождающих: $d_1 c_1, d_2 c_2, \dots, d_k c_k$. Перейдем теперь от аддитивного языка к мультипликативному. Представление фактор-группы A/B имеет вид

$$A/B = \langle c_1, c_2, \dots, c_n; c_1^{d_1}, c_2^{d_2}, \dots, c_k^{d_k}, [c_i, c_j], i, j \in \{1, 2, \dots, n\} \rangle.$$

Такое представление означает, что группа A/B является прямым произведением k циклических групп порядков d_1, d_2, \dots, d_k и свободной абелевой группы ранга $n - k$.

Напомним, что любая конечно порожденная абелева группа может быть представлена в виде такой фактор-группы.

Таким образом, каждая конечно порожденная абелева группа является прямым произведением циклических групп.

Если конечная циклическая группа G имеет составной порядок ab , где a, b взаимно просты, то G распадается в прямое произведение циклических групп $A \times B$.

Используя каноническое представление каждого числа d_1, d_2, \dots, d , каждую группу порядка d_i можно дополнительно разложить в прямое произведение циклических групп, порядки которых равны степеням простых чисел. Такие группы принято называть p -группами.

Итак, каждая конечно порожденная бесконечная абелева группа является прямым произведением циклических p -групп и бесконечных циклических групп, а каждая конечная абелева группа является прямым произведением циклических p -групп для всех простых чисел p , делящих порядок группы.

Для конечных абелевых групп разложимость в прямое произведение циклических p -подгрупп означает, в частности, что для них обращение теоремы Лагранжа выполняется: если число m делит порядок конечной абелевой группы G , то в G существует подгруппа порядка m .

Понятие разрешимости связано с самим происхождением групп. Своему появлению на свет группы обязаны задаче о разрешимости алгебраических уравнений в радикалах, т. е. задаче получения корней многочлена в виде выражений через его коэффициенты с помощью четырех арифметических действий и извлечения корней.

Эта задача разрешима для всех уравнений, степени которых не выше четырех, а неразрешимость ее в общем виде устанавливается с помощью групп подстановок корней. Пока, не вдаваясь в подробности, дадим лишь определение разрешимой группы, отметим простейшие свойства разрешимых групп и приведем в качестве важного примера серию неразрешимых групп.

Напомним, что подгруппа группы G , порожденная всеми коммутаторами, т. е. элементами вида $x y x^{-1} y^{-1}$, называется *коммутантом* группы G (или *производной группы* G). Обычно коммутант обозначается символом $[G, G]$.

Если группа G задана своим представлением, то фактор-группа $G/[G, G]$ группы G по ее коммутанту получается присоединением к определяющим соотношениям группы G всех коммутаторов ее порождающих элементов.

Группа G абелева тогда и только тогда, когда ее коммутант равен единичной подгруппе.

Более общая ситуация следующая.

Фактор-группа $G/[G, G]$ группы G по ее коммутанту абелева.

Это предложение легко усилить, можно говорить не о совпадении с коммутантом, а о включении коммутанта в нормальный делитель: *фактор-группа G/N группы G по нормальному делителю N является абелевой тогда и только тогда, когда N содержит коммутант $[G, G]$ группы G .*

Усиление можно проделать и в другую сторону. Пусть группа G содержит подгруппы A и B . Тогда нормальная подгруппа $[A, B]$, порожденная всевозможными элементами вида $a b a^{-1} b^{-1}$, где $a \in A$, $b \in B$, называют *взаимным коммутантом* подгрупп A , B .

Представление прямого произведения $A \times B$ получается из представлений групп A и B следующим образом.

Сначала просто объединяют представления множителей A и B ; группа с таким объединенным представлением называется *свободным произведением* A и B и обозначается символом $A * B$. Затем это свободное произведение факторизуется по взаимному коммутанту $[A, B]$ подгрупп A и B :

$$A \times B \cong \frac{A * B}{[A, B]}.$$

Группа G может оказаться неабелевой, а ее коммутант — абелевой подгруппой. Это значит, что коммутант коммутанта $[[G, G], [G, G]]$ для такой группы G равен единичной подгруппе.

Более общая, но похожая ситуация следующая. Рассмотрим ряд последовательных коммутантов в группе G :

$$G_1 = [G, G], G_2 = [G_1, G_1], \dots, G_m, G_{m+1} = [G_m, G_m], \dots$$

Каждая новая группа является нормальной подгруппой в предыдущей (более того, является нормальной и даже вполне характеристической подгруппой и во всей группе G):

$$G \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_m \triangleright \dots$$

Если для некоторого натурального числа m выполняется равенство $G_m = E$, то группу G называют m -ступенно разрешимой группой.

Ряд последовательных коммутантов называют еще рядом разрешимости. Формально в каждой группе можно построить ряд разрешимости, но лишь у разрешимых групп этот ряд достигает единицы.

На определение разрешимости можно взглянуть с иной точки зрения.

Все коммутанты являются вербальными подгруппами, т. е. подгруппами, порожденными значениями слов особого вида.

Для абелевой группы это слово $[x_1, x_2]$, для метабелевой — $[[x_1, x_2], [x_3, x_4]]$, для 3-ступенно разрешимой группы — $[[[x_1, x_2], [x_3, x_4]], [x_5, x_6], [x_7, x_8]]$ и т. д.

Однако коммутаторы можно организовать и не так витиевато, а проще.

Определим *простой коммутатор* $[x_1, x_2, \dots, x_{n-1}, x_n]$ длины n по индукции. Простой коммутатор длины 2 будет, как и раньше, $[x_1, x_2]$. Для $n > 2$ полагаем:

$$[x_1, x_2, \dots, x_{n-1}, x_n] \stackrel{\text{опр}}{=} [[x_1, x_2, \dots, x_{n-1}], x_n].$$

Если в группе G все простые коммутаторы длины n равны единице, то в группе выполняется тождество

$$[x_1, x_2, \dots, x_{n-1}, x_n] = 1.$$

Такая группа называется *нильпотентной*¹.

Наименьшее такое число n называют *классом nilпотентности*. Например, абелева группа — это nilпотентная класса один и одноступенно разрешимая группа.

¹ Иными словами, потенциально нулевой.

Пусть G — произвольная группа, а G_k — подгруппа, порожденная значениями простых коммутаторов длины k . Убывающая цепочка подгрупп

$$G = G_0 > G_1 > G_2 > \dots > G_k > \dots$$

называется нижним центральным рядом (*Lower Central Series, LCS*).

Группа G будет нильпотентной тогда и только тогда, когда ее нижний центральный ряд достигает единичной подгруппы.

Центральным рядом группы G называется невозрастающая по включению последовательность нормальных делителей группы G_i таких, что для каждого i фактор-группа G_{i-1} / G_i содержится в центре фактор-группы G / G_i .

LCS является центральным; более того, его члены содержатся в соответствующих членах любого центрального ряда той же группы. Именно этим объясняется слово «нижний» в определении LCS .

Центр любой группы является абелевой подгруппой, поэтому факторы в нижнем центральном ряде абелевы. Это означает, что нильпотентная группа разрешима.

Если группа проста и неабелева, то она неразрешима.

Все группы диэдра (в том числе и бесконечная) содержат циклическую группу, являющуюся нормальным делителем. Это значит, что каждая группа диэдра 2-ступенно разрешима.

Разрешимые группы второй степени называют еще метабелевыми группами. В метабелевой группе содержится абелев нормальный делитель, и фактор-группа по этому делителю абелева.

Например, группы диэдра D_n при $n > 2$ (в том числе и $n = \aleph_0$) неабелевы, но метабелевы.

Поскольку m -ступенная разрешимость группы задается тождеством, множество всех разрешимых групп, степени, не превышающей m , образует многообразие. Как в каждом многообразии, гомоморфный образ, подгруппа или прямое произведение разрешимых групп сами являются разрешимыми группами.

Неразрешимость для конечной группы G означает, что ее ряд последовательных коммутантов на каком-то шаге, не достигая единицы, стабилизируется, т. е. какая-то подгруппа из этого ряда совпадет со своим коммутантом.

Для бесконечной группы G , кроме того, могут возникнуть еще две ситуации:

- 1) ряд последовательных коммутантов в пересечение дает неединичную группу;
- 2) ряд коммутантов пересекается по единичной подгруппе.

В последнем случае группу G называют по типу упорядочения ряда коммутантов (а упорядочены они, как множество натуральных чисел) ω -разрешимой группой.

Само понятие группы возникло в связи с задачей нахождения формулы для выражения корней многочлена пятой и выше степени через его коэффициенты с помощью операций поля и извлечения корней. Правда, с этой задачей связаны лишь конечные группы.

С алгебраическим уравнением $f(x) = 0$ степени n связана некоторая группа подстановок на n символах. В честь автора, впервые установившего эту связь, такая группа называется *группой Галуа*¹ уравнения $f(x) = 0$.

Основная теорема теории Галуа следующая: *уравнение $f(x) = 0$ разрешимо в радикалах тогда и только тогда, когда его группа Галуа разрешима.*

Рассмотрим, например, уравнение $x^5 + x^2 + 1 = 0$ и выясним, можно ли выразить корни этого уравнения через коэффициенты с помощью арифметических операций и извлечения корней.

Группа Галуа этого уравнения состоит из 120 элементов и порождается подстановками (1 2) и (1 2 3 4 5), т. е. это вся симметрическая группа S_5 .

Теперь узнаем, разрешима ли группа S_5 , а для этого найдем ряд ее последовательных коммутантов:

$$[S_5, S_5] = A_5, [A_5, A_5] = A_5.$$

Это значит, что ряд стабилизировался на втором шаге: группа S_5 неразрешима, и корни уравнения $x^5 + x^2 + 1 = 0$ нельзя выразить в радикалах через коэффициенты этого уравнения.

Наличие одного такого конкретного уравнения означает, что общей формулы для нахождения корней алгебраического уравнения пятой степени не существует.

Проверку разрешимости S_5 можно было и не производить, так как уже ранее отмечено, что A_5 проста и, следовательно, неразрешима.

Узнаем теперь, не разрешима ли группа S_4 .

Ряд разрешимости группы S_4 имеет вид

$$S_4 > A_4 > K > E.$$

Последняя группа в этом ряду последовательных коммутантов единичная; группа S_4 разрешима. Поэтому, по теореме Галуа, любое уравнение четвертой (и ниже) степени разрешимо в радикалах. В частности, разрешимо уравнение с буквенными коэффициентами — существует формула, выражающая корни многочлена степени

¹ *Эварист Галуа* (Galois, 1811—1832) — французский математик, по существу построивший всю теорию конечных полей и полностью решивший задачу о разрешимости уравнений в радикалах, сведя вопросы теории полей к вопросам теории групп (возникшей именно благодаря *теории Галуа*). Активно занимался политической деятельностью, в результате которой был убит на дуэли.

не выше четвертой через коэффициенты этого многочлена с помощью арифметических операций и извлечения корней.

Рассмотрим еще один пример такого рода.

Выясним, разрешимо ли в радикалах уравнение шестой степени

$$x^6 + x^4 - x^3 + x^2 + x + 1 = 0.$$

Группа Галуа G этого уравнения является прямым произведением двух циклических порядков 3 и группы диэдра D_4 . Поскольку прямое произведение разрешимых групп разрешимо, эта группа также разрешима. Уравнение $x^6 + x^4 - x^3 + x^2 + x + 1 = 0$ разрешимо в радикалах.

Найдем, просто из любопытства, ряд разрешимости этой группы:

$$G_1 = [G, G] = \text{гр}((1\ 3)(2\ 4), (3\ 5)(4\ 6), (2\ 4)(3\ 5));$$

$$G_2 = [G_1, G_1] = \text{гр}((1\ 3\ 5), (2\ 4\ 6));$$

$$G_3 = [G_2, G_2] = E.$$

Ряд подгрупп достиг единичной подгруппы; группа разрешима. Следовательно, есть формула, выражающая корни этого уравнения через его коэффициенты. В этой формуле используются, кроме знаков арифметических действий, только извлечения корней. Заметим, что число извлечений корней мы можем определить по имеющемуся ряду разрешимости, но сейчас это не наша задача. Элементы теории Галуа будут более подробно обсуждаться в теме, посвященной расширениям полей.

Нахождение групп Галуа во всех приведенных примерах (кроме самого первого) было проделано с помощью вычислительной техники, точнее, с помощью пакета символьных математических вычислений *Maple*.

С помощью этого пакета можно исследовать группы, заданные представлением порождающими элементами и определяющими соотношениями, и группы, заданные как подгруппы симметрической группы.

Правда, вычислительных программ, касающихся групп подстановок, в пакете *Maple* значительно больше, чем для групп, заданных представлением.

Найти коммутант группы, ряд коммутантов, центр группы, проверить абелевость группы, найти максимальный нормальный делитель, содержащийся в данной подгруппе, проверить вхождение одной подгруппы в другую и т. п. в пакете *Maple* можно пока только для подгрупп симметрической группы.

Однако от общего представления конечной группы можно перейти к ее представлению подстановками.

Каждую конечную группу можно представить, по теореме Кэли, с помощью группы подстановок. Это представление можно полу-

чить и с помощью вычислительной техники, причем даже в общем виде.

Чтобы обсудить этот вид, нам нужны свойства объекта, который тесно связан с любой группой и который в явном и неявном виде многократно возникал раньше. Речь идет о *преобразованиях множества*.

4.6. Преобразования множеств и группы преобразований

Напомним, что *преобразованием* множества называют любое отображение этого множества в себя.

Множество всех преобразований образует полугруппу (даже моноид), а множество взаимно однозначных отображений на себя (биекций) — группу. По теореме Кэли, каждая группа изоморфно вложима в группу преобразований некоторого множества. Такое изоморфное представление называют *точным*.

Точность представления группы G преобразованиями множества M может и не потребоваться заранее, т. е. G может быть представлена преобразованиями M лишь гомоморфно. В таком случае говорят, что группа G *действует на множестве M* .

Множество отображений любого множества в себя образует моноид. Гомоморфное отображение группы G в этот моноид называют *действием группы на множестве M* .

Иначе говоря, группа G *действует на множестве M* , если для каждого элемента g из G и для каждого m из M однозначно определен элемент mg из M , причем

$$(mg_1)g_2 = (mg_1)g_2, \quad me = m$$

для каждого элемента g_1, g_2 из группы G и каждого m из множества M (здесь e — единица группы G).

Например, теорема Кэли означает, что любая группа действует на своем множестве. Группа движений плоскости действует на множестве точек плоскости.

Множество

$$mG = \{mg \mid g \in G\}$$

называют *G -орбитой* (или просто *орбитой*) элемента m . Отношение «лежать в одной орбите» является отношением эквивалентности, и множество M распадается на непересекающиеся орбиты.

Например, если G — группа вращений вокруг точки O , а множество M — точки плоскости, то орбита точки представляет собой окружность с центром в точке O .

Если a — произвольный элемент из M , то множество $St(a)$ всех элементов из G , оставляющих элемент a неподвижным, называют стабилизатором элемента a .

При действии группы G на множестве стабилизатор элемента является подгруппой группы G .

Мощность G -орбиты элемента a равна индексу стабилизатора элемента a в группе G .

Если H — подгруппа группы G , то G действует на множестве своих правых смежных классов, переводя смежный класс Hx в класс Hxg (такое действие называют *правым сдвигом*). Правые сдвиги при $H = E$ использовались уже ранее при доказательстве теоремы Кэли.

Если индекс H в G равен n , то действие группы G на множестве $\{Hg | g \in G\}$ правых смежных классов по H задает гомоморфное отображение φ группы G в группу S_n , действующее по правилу

$$\varphi(x) = \begin{pmatrix} H & \dots & Hg & \dots \\ Hx & \dots & Hgx & \dots \end{pmatrix}.$$

Элемент x из G принадлежит $N = \text{Ker } \varphi$ — ядру этого гомоморфизма тогда и только тогда, когда для любого g из G

$$Hgx = H.$$

Из равенства $Hx = H$ следует, что $x \in H$, поэтому ядро этого гомоморфизма является нормальным делителем группы G , содержащимся в H . Равенство $Hgx = H$ равносильно

$$g^{-1}Hgx = g^{-1}Hg,$$

а это означает, что элемент x принадлежит всем сопряжениям подгруппы H . Отсюда следует, что

$$\text{Ker } \varphi = \bigcap_{g \in G} g^{-1}Hg.$$

Значит, ядро N гомоморфизма φ образует наибольший (в смысле включения) нормальный делитель группы G , содержащийся в подгруппе H . Отсюда следует, в частности, что представление группы сдвигами правых смежных классов будет точным (т. е. изоморфным) лишь в том случае, если подгруппа H не содержит неединичных нормальных подгрупп группы G .

Индекс подгруппы N в G равен порядку гомоморфного образа группы, т. е. не превышает (а точнее, делит) число $n!$. Это значит, что подгруппа H конечного индекса n в группе G содержит нормальный делитель конечного индекса k в G . Этот индекс не превышает число $n!$ и, разумеется, не меньше числа n :

$$n \leq k \leq n!.$$

Кроме того, k делится на n и делит $n!$.

Ранее было отмечено, что подгруппа индекса 2 в группе G нормальна в G . В действительности это лишь частный случай общего факта. Число 2 вообще наименьшее простое натуральное число, поэтому оно будет наименьшим простым, делящим четный порядок группы.

Пусть p — наименьшее простое число, делящее порядок группы G , и в группе G нашлась подгруппа индекса p . Действуя сдвигами на множестве смежных классов по подгруппе H , получаем гомоморфное отображение G в группу S_p . Это значит, что в подгруппе H найдется нормальный делитель индекса k , и это число k делит $p!$ и делится на p . Это возможно лишь в одном случае: $k = p$.

Таким образом, если p — простое наименьшее простое число, делящее порядок группы G , то подгруппа индекса p в G нормальна в G .

Вместо правых сдвигов можно было рассмотреть действие на множестве левых смежных классов левыми сдвигами. В каждом случае (как правых, так и левых сдвигов) вместо всей группы G можно взять любую ее подгруппу.

Точнее, если H и S — две подгруппы группы G , то действие S на множестве $\{gH \mid g \in G\}$ левых смежных классов по H левыми сдвигами означает, что каждому элементу s из S соответствует отображение $gH \mapsto sgH$. В этом случае длина орбиты равна индексу стабилизатора элемента и, в частности, делит порядок подгруппы S .

Отображение, переводящее каждый элемент x из G в сопряженный элемент gxg^{-1} , тоже является действием группы на своем собственном множестве. Орбита элемента x в таком случае состоит из всех элементов, сопряженных с x , а стабилизатором x является множество перестановочных с ним элементов.

Поддействуем группой G на своем же множестве, переводя каждый элемент в сопряженный. Тогда орбитой элемента x будет в точности класс всех элементов, сопряженных с элементом x .

Можно обобщить ситуацию и рассмотреть действие сопряжением не на множестве G , а на его множестве подмножеств $P(G)$. Множество $P(G)$ также разбивается на классы сопряженных элементов — орбиты действия.

Если M — произвольное множество из группы G , то стабилизатор множества M при действии сопряженными на $P(G)$ является нормализатор множества M .

В частности, если M — подгруппа, то нормализатор M в G , как и раньше, — это наибольшая подгруппа группы G , в которой H — нормальный делитель. Как и для любого стабилизатора, нормализатор любого подмножества группы G является подгруппой в G , а индекс нормализатора подгруппы равен числу различных сопряжений этой подгруппы.

Нормализатор подгруппы содержит эту подгруппу, поэтому подгруппа конечного индекса в группе G имеет конечное число сопряжений в G . Если группа G конечна, то число различных подгрупп, сопряженных в G , является делителем порядка группы.

Вернемся к действию группы сопряжениями на самом множестве G .

Стабилизатор элемента x в G , т. е. множество

$$\{g \in G \mid g^{-1}xg = x\},$$

состоит из центральных по отношению к x элементов и называется *централизатором* элемента x в G . Централизатор обозначается символом $Z_G(x)$. Множество $Z_G(x)$ — это частный случай стабилизатора, поэтому централизатор любого элемента в группе G является подгруппой группы G , а индекс централизатора равен числу различных сопряжений элемента x .

Из теоремы Лагранжа теперь следует, что число элементов в каждом классе сопряженных элементов делит порядок группы. Правда, некоторые классы состоят только из одного элемента.

Централизатор элемента x является единичной подгруппой тогда и только тогда, когда этот элемент x центральный.

Один центральный элемент есть даже в группе без центра. Это единица группы. Пусть G — конечная группа. Подействуем группой G на множество G сопряжениями. Множество G распадется на непересекающиеся орбиты (классы сопряженных элементов), а число элементов в каждом классе делит число элементов в G :

$$|G| = \underbrace{1+1+\dots+1}_{|Z(G)|} + n_2 + n_3 + \dots + n_t,$$

где n_2, n_3, \dots, n_t — число элементов в классах сопряжений нецентральных элементов.

Получившееся равенство иногда называют *формулой классов*.

Если G — конечная группа, то число элементов в каждом классе сопряженных элементов делит порядок группы.

Для иллюстрации разобьем множество группы S_3 на классы сопряженных элементов:

$$S_3 = \{e\} \cup \{(12), (13), (23)\} \cup \{(123), (321)\}.$$

В первом классе один элемент, во втором — два, в третьем — три. Все эти числа делят число 6.

Как и для действия группы правыми или левыми сдвигами, в этом случае можно представлять действием сопряжениями не всю группу G , а лишь некоторую ее подгруппу H . Число элементов в орбитах тогда будут делителями порядка подгруппы H .

Рассмотрим теперь случай, когда G — конечная группа порядка p^m , где p — простое число. Поскольку по крайней мере одна из орбит одноэлементная, в этом случае должен найтись хотя бы еще один неединичный центральный элемент. Иначе говоря, если индекс $|G| = p^n$, где p — простое число, то центр $Z(G)$ группы G отличен от единицы.

Отметим, что если G — конечная группа порядка p^m , то все ее фактор-группы имеют порядки p^k , где $0 \leq k \leq m$. Используя это замечание о центре такой группы и индукцию по n , можно заметить, что если порядок группы G равен p^n , где p простое, то G содержит подгруппу порядка p^{n-1} .

Покажем теперь, что группы порядка p^m разрешимы.

Если порядок группы G равен p^n , где p простое, а H — подгруппа порядка p^{n-1} , то индекс $|G : H| = p$. Все группы порядка p абелевы, и, следовательно, H содержит коммутант группы G .

Если порядок группы G равен p^n , где p простое, то G не совпадает со своим коммутантом.

Но любая подгруппа группы порядка p^n сама имеет порядок такого вида. Поэтому индукцией по n теперь можно установить, что если группа имеет порядок p^n , где p — простое число, то она разрешима.

В частном случае — группах порядка p^2 — можно сказать даже больше. Покажем, что такая группа всегда абелева.

Пусть группа G имеет порядок p^2 , где p — простое число и G нециклическая, т. е. в ней нет элемента порядка p^2 . Предположим, что эта группа G неабелева, т. е. ее центр не совпадает с G . Центр группы G не единичен, следовательно, $Z(G)$ — это группа порядка p , т. е. циклическая группа, $Z(G) = \langle a \rangle$.

Кроме того, в группе G есть элемент b , не принадлежащий центру. Но тогда G совпадает с комплексом $Z(G) \cdot \langle b \rangle$ и $ab = ba$, значит, и элемент b также принадлежит центру.

Иначе говоря, группа порядка p^2 всегда абелева.

Если порядок конечной группы G четный и в ней все элементы имеют нечетный порядок, то простое объединение элементов в пары — элемент и его обратный — приводит к противоречию.

Если порядок конечной группы — четное число, то в ней содержится элемент второго порядка.

Это простое замечание можно обобщить на случай произвольного простого числа.

Пусть теперь G — конечная группа порядка mr , где p — простое число и $m > 1$. Предположим, что в G нет подгруппы порядка p , но тогда индекс любой собственной подгруппы делится на p . Подействуем группой G на своем множестве сопряжений. Множество G распадется на орбиты — смежные классы сопряженных.

Неодноэлементные орбиты будут представлять нетривиальные подгруппы, а потому будут кратны p . Поэтому число одноэлемент-

ных орбит (которые состоят из элементов центра) будет кратно p (в частности, отлично от единицы).

Но центр является абелевой группой, и в нем найдется элемент порядка p . Таким образом, группа G содержит собственную подгруппу, порядок которой делится на p , но эта подгруппа будет подгруппой и в группе G . Индукцией по m устанавливается, что в частном случае обращение теоремы Лагранжа выполняется.

Итак, если порядок конечной группы делится на простое число p , то в группе есть элемент порядка p .

Действительно, для любой степени p^m простого числа, делящей порядок конечной группы в этой группе, найдется подгруппа порядка p^m .

Следующие результаты вошли в историю как теоремы Силова¹.

Пусть p^m — наивысшая степень p^m простого числа, которая делит порядок конечной группы G . Подгруппа порядка p^m называется *силовской p -подгруппой*.

Для любого простого числа p — делителя порядка группы G — в этой группе найдется силовская p -подгруппа.

Пусть $|G| = kp^m$, где k не делится на простое число p . Рассуждаем далее индукцией по числу m . Случай $m = 1$ уже рассмотрен ранее.

Пусть $m > 1$. Если G абелева, то для любого делителя ее порядка найдется соответствующая подгруппа, и это утверждение следует из теории конечно порожденных абелевых групп. Следовательно, можно считать, что G неабелева, т. е. не совпадает со своим центром $Z(G)$. Если найдется элемент x из G , не принадлежащий центру, но с длиной орбиты, не делящейся на p , то индекс $Z_G(x)$ централизатора элемента x делится на p^m . По индуктивному предположению утверждение верно для подгруппы $Z_G(x)$, а следовательно, и для группы G .

Если длины орбит для любого x делятся на p , то из формулы классов

$$|G| = \underbrace{1+1+\dots+1}_{|Z(G)|} + n_2 + n_3 + \dots + n_t$$

следует, что порядок центра делится на p . Центр является абелевой группой, поэтому там найдется элемент a порядка p . Подгруппа $N = \langle a \rangle$ нормальна в группе G , а фактор-группа G/N имеет порядок kp^{m-1} . Для этой группы утверждение верно, т. е. в G найдется такая подгруппа H , что $\left| \frac{H}{N} \right| = p^{m-1}$. Но тогда порядок H равен p^m . Ут-

¹ Людвиг Силлов (Sylow, 1832—1918) — норвежский математик. С 1855 г. работал школьным учителем. В 1862—1863 г. Л. Силлов читал в университете лекции по теории Галуа и группам подстановок. Теоремы о подгруппах конечных групп были доказаны Силловым в 1872 г.

верждение доказано. По традиции доказанное предложение принято называть *первой теоремой Силова*.

В приведенном доказательстве первой теоремы Силова нигде не использовалось, что число k не делится на p . Другими словами, *если порядок конечной группы делится на степень p^m простого числа, то в группе есть элемент порядка p^m* .

Пусть теперь P — некоторая силовская p -подгруппа, а H — произвольная p -подгруппа группы G .

Покажем, что тогда H содержится в некотором сопряжении группы P . Пусть группа H действует правыми сдвигами на множестве левых классов $\{Pg | g \in G\}$ по подгруппе H в G . Множество $\{Pg | g \in G\}$ распадается на непересекающиеся орбиты, причем число элементов в каждой орбите делит порядок подгруппы H , равный степени числа p . Сумма всех длин орбит равна индексу подгруппы P в G , который не делится на p . Это значит, что найдется орбита, состоящая в точности из одного элемента, т. е. найдется такой смежный класс Hg , что для любого элемента h из H выполняется равенство

$$Pgh = Pg.$$

Это равенство можно записать иначе:

$$Pghg^{-1} = P.$$

Из равенства $Px = P$ следует, что $x \in P$. Итак, все элементы вида ghg^{-1} для каждого h из H принадлежат подгруппе P . Это значит, что $gHg^{-1} \subseteq P$. В частности, если сама H — силовская p -подгруппа, то $gHg^{-1} = P$.

Итак, все силовские p -подгруппы группы G сопряжены в G , а каждая p -подгруппа содержится в некоторой силовской p -подгруппе.

Это предложение принято называть *второй теоремой Силова*.

Третьей теоремой Силова называют утверждение о числе силовских p -подгрупп.

Пусть P_1, P_2, \dots, P_r — все силовские p -подгруппы группы G . Число r равно индексу нормализатора любой из P_i , поэтому делит порядок всей группы. Порядок нормализатора делится на p^m , поэтому индекс r не делится на p .

Поддействуем подгруппой P_1 сопряжениями на множестве $M = \{P_1, P_2, \dots, P_r\}$. Множество M распадется на непересекающиеся орбиты. Длина каждой орбиты делит порядок P_1 , поэтому длина равна степени числа p . Одна из орбит совпадает с группой P_1 , т. е. состоит из одного элемента. Это единственная одноэлементная орбита в множестве M . Действительно, если, например, $gP_2g^{-1} = P_2$ для любого элемента g из P_1 , то P_1P_2 является p -подгруппой и эта подгруппа содержит обе подгруппы P_1P_2 . Отсюда следует, что $P_1 = P_2$. Итак, одноэлементная орбита в точности одна, а длины всех остальных делятся на p .

Таким образом, число r силовских p -подгрупп группы G делит порядок группы G и $\text{Rest}(r, p) = 1$.

Отметим теперь, что центр любой p -группы отличен от единичной подгруппы, поэтому любая p -группа нильпотентна.

Поскольку нильпотентность задается тождеством, прямое произведение нильпотентных групп тоже нильпотентно¹. Следовательно, если конечная группа является прямым произведением своих силовских подгрупп, то она нильпотентна. Верно и обратное утверждение: каждая конечная нильпотентная подгруппа разложима в прямое произведение своих силовских p -подгрупп, где p — простые числа из разложения порядка группы на простые множители.

Таким образом, конечная группа нильпотентна тогда и только тогда, когда она является прямым произведением своих силовских подгрупп.

Рассмотрим теперь для иллюстрации правых сдвигов вычислительный пример, а именно найдем представление группы $G = \langle x, y; x^2ux^3, y^2xuy^3 \rangle$ подстановками.

В этой группе содержится 56 элементов. Если действовать формально, буквально следуя теореме Кэли, то нужно взять единичную подгруппу и множество сдвигов этой единичной подгруппы в G . В результате получится представление группы G группой подстановок на 56 символах. Представление порождающих элементов группы G в машинной записи имеет вид

$$\begin{aligned}x = & [[1, 2, 3, 14, 11, 12, 13], [4, 5, 28, 17, 32, 33, 34], \\& [6, 37, 38, 25, 19, 40, 41], [7, 36, 42, 56, 45, 46, 47], \\& [8, 44, 48, 50, 30, 31, 18], [9, 10, 15, 16, 29, 24, 39], \\& [20, 21, 22, 23, 53, 52, 54], [26, 27, 49, 51, 55, 43, 35]]; \\y = & [[1, 8, 9, 35, 5, 6, 7], [2, 19, 20, 46, 16, 17, 18], \\& [3, 4, 26, 30, 23, 24, 25], [10, 11, 22, 31, 32, 42, 43], \\& [12, 49, 38, 39, 44, 45, 21], [13, 36, 33, 54, 40, 50, 27], \\& [14, 15, 47, 37, 51, 52, 34], [28, 29, 53, 55, 56, 48, 41]].\end{aligned}$$

Как было отмечено ранее, порядки ее порождающих равны 7. Изображение порождающих в виде подстановок подтверждают те вычисления, однако работать с таким представлением непросто.

¹ По той же причине любая подгруппа и любой гомоморфный образ нильпотентной группы тоже нильпотенты.

Машину, конечно, не смутит большое число символов, однако можно найти и другие представления той же группы, для человека-вычислителя более приемлемые.

Возьмем в G подгруппу H , порожденную элементом x^2 , и найдем представление S группы G сдвигами правых смежных классов по H . Имеем новые изображения порождающих:

$$x_1 = [[2, 3, 7, 4, 8, 6, 5]]; y_2 = [[1, 2, 6, 8, 3, 4, 5]].$$

Группа, порожденная подстановками x_1, y_1 , имеет порядок 56, а это значит, что новое представление группой подстановок всего на восьми символах тоже оказалось точным (изоморфизмом).

Тайна такой точности проста — в подгруппе H нет нормального делителя группы G , кроме единичного. Получив представление группы в виде группы подстановок, можно исследовать ее и далее. Например, с помощью полученного представления группы G (любого — на 56 или на восьми элементах) можно установить, что эта группа метабелева, хотя и без центра. Разложив эту группу на смежные классы по подгруппе E , получим все элементы группы G в виде подстановок.

Порядок каждой подстановки виден с первого взгляда. Оказывается, что в этой группе все неединичные элементы имеют порядок 7 или 2, причем все семь элементов порядка два вместе с единицей образуют нормальную подгруппу N в этой группе.

Все элементы из N имеют порядок два, поэтому N — абелева группа, точнее N — прямое произведение трех циклических групп порядка два.

Подгруппа A , порожденная элементом

$$a = (1\ 2\ 6\ 8\ 3\ 4\ 5),$$

имеет порядок 7, пересекается с подгруппой N по единичной подгруппе, а комплекс AN совпадает с группой G . Это значит, что G является полупрямым произведением групп A и N . Это еще не вся информация о группе G . Поскольку полупрямое произведение неоднозначно задается своими множителями, нужно еще знать, как именно действует группа A сопряжениями на N . Но это уже нетрудно выяснить — достаточно рассмотреть сопряжения элемента

$$b = (1\ 2)(3\ 6)(4\ 7)(5\ 8)$$

с помощью степеней элемента a . Обнаружив среди этих сопряжений все порождающие подгруппы N , мы и получим новое представление группы G в порождающих a, b . Это представление уже полностью описывает ее строение.

Вернемся вновь к теоретическим наблюдениям.

Множество, на котором происходит действие, может быть само некоторой алгеброй (например, группой). Если все действия будут биекциями, а отображение группы точное, то речь пойдет о группе автоморфизмов (или ее подгруппе).

Множество автоморфизмов произвольной алгебры или алгебраической системы с операцией «композиция» образует группу. В частности, множество $\text{Aut}(G)$ автоморфизмов группы G тоже является группой.

Каждая ли группа может быть представлена как группа автоморфизмов некоторой группы?

Ответ на этот вопрос отрицательный: нет, не каждая.

Чтобы получить доказательство этого утверждения, нужна небольшая подготовка.

Напомним, что отображение, переводящее каждый элемент в его сопряженный, является автоморфизмом, который называется *внутренним автоморфизмом*. Внутренние автоморфизмы образуют подгруппу $\text{Inn}(G)$ группы $\text{Aut}(G)$.

Множество элементов группы, перестановочных со всеми ее элементами, — это центр группы. Центр $Z(G)$ группы G является нормальным делителем в группе G . Легко ответить на вопрос о факторгруппе по этому нормальному делителю в крайних случаях. Если центр группы — наибольший из возможных, т. е. группа G совпадает со своим центром, то G абелева и ее группа внутренних автоморфизмов единичная. В этом случае группа внутренних автоморфизмов изоморфна факторгруппе группы G по ее центру. Если центр минимальный, т. е. G без центра, то различные элементы из группы G задают различные внутренние автоморфизмы. В этом случае группа внутренних автоморфизмов изоморфна факторгруппе группы G по ее центру.

Если центр $Z = Z(G)$ группы G занимает промежуточное положение, то его индекс k отличен от единицы и порядка G :

$$G = Zg_1 + Zg_2 + \dots + Zg_k.$$

И в этом случае различные смежные классы по подгруппе Z задают различные внутренние автоморфизмы, а отображение $x \mapsto g_i$, переводящее каждый элемент в представитель своего класса, сохраняет операцию. Это значит, что всегда группа $\text{Inn}(G)$ внутренних автоморфизмов группы G изоморфна факторгруппе $G / Z(G)$ группы G по ее центру $Z(G)$.

Теперь обратим внимание на группы, у которых есть настоящие внешние (т. е. отличные от внутренних) автоморфизмы.

Если факторгруппа $G / Z(G)$ группы G по ее центру $Z(G)$ отлична от единицы, то группа G нециклическая.

В неабелевой группе всегда есть невнутренний автоморфизм, более того, группа внутренних автоморфизмов нециклическая.

Подгруппа циклической группы сама циклическая. Следовательно, группа автоморфизмов неабелевой группы нециклическая.

Возьмем теперь абелеву группу G порядка больше двух. Если в ней есть элемент a порядка больше двух, то отображение $x \mapsto x^{-1}$ является неединичным автоморфизмом группы G . Если же в группе G все элементы имеют порядок два, то G можно представить в виде

$$G = A \times B \times G_1,$$

где $A = \langle a; a^2 = 1 \rangle$ и $B = \langle b; b^2 = 1 \rangle$ — циклические группы второго порядка. Но тогда отображение, переводящее a в элемент b , а элемент b переводящий в элемент a и оставляющий остальные порождающие на месте, можно продолжить до автоморфизма всей группы G . Итак, если группа G абелева, порядка больше двух, то группа $\text{Aut}(G)$ содержит элемент второго порядка.

Из этих замечаний следует существование групп, не являющихся группами автоморфизмов никаких групп.

Например, циклическая группа не может быть группой автоморфизмов никакой неабелевой группы. Если в группе нет элементов второго порядка, то она не может быть группой автоморфизмов абелевой группы.

Следовательно, бесконечная циклическая группа не является группой автоморфизмов никакой группы.

Циклическая группа нечетного порядка не является группой автоморфизмов никакой группы.

Впрочем, такая конкретика, может быть, не имеет принципиального значения.

Более важен сам факт: существуют группы, не являющиеся группами автоморфизмов никакой группы

Контрольные задания

1. Докажите, что гомоморфный прообраз бесконечной группы является бесконечной группой.
2. Докажите, что число элементов группы G , сопряженных с данным элементом, делит порядок группы G .
3. Докажите, что отображение, переводящее каждый элемент x группы G в $g^{-1}xg$, является автоморфизмом группы G .
4. Докажите, что циклическая группа нечетного порядка не является группой автоморфизмов никакой группы.
5. Докажите, что если H — подгруппа группы G и x — элемент из G , то $x^{-1}Hx$ — тоже подгруппа в G .
6. Докажите, что любой гомоморфизм группы является произведением естественного гомоморфизма и некоторого изоморфизма.
7. Докажите, что аддитивная группа действительных чисел и мультипликативная группа положительных действительных чисел изоморфны.

8. Докажите, что аддитивная группа рациональных чисел и мультипликативная группа положительных рациональных чисел не изоморфны.

9. Докажите, что для любого четного $n \geq 6$ существует неабелева группа из $2n$ элементов.

10. Докажите, что не для каждого натурального n существует неабелева группа из n элементов.

Тема 5

ПОДКОЛЬЦА И ФАКТОР-КОЛЬЦА

Основные понятия: кольцо, целостное кольцо, идеал, главный идеал, сумма идеалов, евклидовость, простые и составные элементы целостного кольца, гомоморфизм, ядро гомоморфизма, фактор-кольцо, естественный гомоморфизм.

Основные факты: в кольце главных идеалов отношение делимости точно соответствует отношению включения между идеалами; евклидово кольцо является кольцом главных идеалов; кольцо главных идеалов — гауссово; гомоморфный образ кольца изоморфен фактор-кольцу по ядру гомоморфизма.

Понятие кольца — одно из важнейших понятий современной математики. С понятий группы и кольца начинается изучение курса алгебры. Простейшие свойства колец, их подколец и гомоморфных образов уже рассматривались в предыдущих темах.

Эта тема посвящается простым, но уже не таким поверхностным свойствам колец, их подалгебрам и гомоморфизмам. В заключение мы сделаем краткий обзор наиболее распространенных свойств колец.

5.1. Подалгебра кольца

Подалгебра кольца называется *подкольцом*.

Другими словами, если $\langle K; +, \cdot \rangle$ — кольцо, то его непустое подмножество H называется *подкольцом* (пишут $H < G$ или $H \leq G$), если алгебра $\langle H; +, \cdot \rangle$ является кольцом.

Само K и множество $O = \{0\}$, состоящее из нейтрального элемента по сложению, являются подкольцами любого кольца (*тривиальными подкольцами*). Изоморфные объекты в алгебре не различаются, поэтому символом O иногда обозначают нулевые подкольца, взятые из различных колец.

Для того чтобы говорить об алгебре H , необходима замкнутость H относительно операции

$$x, y \in H \Rightarrow x + y \in H;$$

$$x, y \in H \Rightarrow xy \in H.$$

Например, множество нечетных чисел по причине незамкнутости по сложению не образует подкольца в кольце целых чисел.

Замкнутости подмножества H относительно операций *недостаточно*, чтобы H было подкольцом. Например, подмножество натуральных чисел замкнуто относительно сложения и умножения, но $\langle \mathbb{N}; +, \cdot \rangle$ не является подкольцом кольца целых чисел.

Если H — подкольца кольца K , то символически это обычно записывают так: $H \leq K$ или $H < K$, где знак $<$ означает не обязательно строгое включение.

Например, для числовых колец:

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}.$$

Важным примером числового кольца является кольцо

$$\{a + bi \mid a, b \in \mathbb{Z}\},$$

называемое *кольцом целых гауссовых чисел*.

Как и любой алгебре, отношение «быть подкольцом» транзитивно: если A — подкольцо кольца B , а B — подкольцо кольца K , то A — подкольцо кольца K .

Поскольку подкольцо H кольца K является, в частности, подгруппой аддитивной группы K , множество H содержит нуль всего кольца.

Чтобы непустое подмножество кольца было подкольцом, необходимо, чтобы оно было замкнуто относительно обеих операций. Кроме того, оно должно быть группой по сложению. Этих условий уже достаточно для того, чтобы быть подкольцом.

Непустое подмножество H является подкольцом кольца K тогда и только тогда, когда:

- а) $a \in H, b \in H \Rightarrow a - b \in H$;
- б) $a \in H, b \in H \Rightarrow a \cdot b \in H$.

Если H — конечное подмножество кольца K , то H является подкольцом тогда и только тогда, когда оно замкнуто относительно сложения и умножения.

Наличие нулевого элемента в каждом подкольце означает, что пересечение любого числа подколец не пусто, и с замкнутостью относительно произведения и разности это означает, что *пересечение любого числа подколец является подкольцом*.

Аддитивная группа кольца непременно абелева, а коммутативность умножения в кольце необязательна. Как обычно, элемент кольца называют *центральным*, если он перестановочен со всеми элементами кольца.

Сумма, разность и произведение центральных элементов снова являются центральными, т. е. центр кольца является подкольцом.

Точно так же, как и для групп, кольцо коммутативно тогда и только тогда, когда оно совпадает со своим центром.

Заметим, впрочем, что роль центра для колец не так велика, как для групп. Например, центр группы является нормальным делителем (и даже характеристической подгруппой), а поэтому и ядром некоторого гомоморфизма группы. Центр кольца тоже выдерживает автоморфизмы этого кольца, однако вовсе не обязательно, что он будет ядром некоторого гомоморфизма этого кольца.

В реальных ситуациях сначала может появиться *надкольцо* K кольца H (чаще говорят «*расширение* H »), а затем уже H станет представлять интерес как *подкольцо* этого самого K .

Например, множество $F(K)$ всех функций, определенных на кольце K со значениями в K , образует кольцо.

На множестве $F(K) = \{f: K \rightarrow K\}$ операции задаются правилами

$$(f + g)(x) = f(x) + g(x);$$

$$(f \cdot g)(x) = f(x) \cdot g(x).$$

Исходное кольцо K входит в кольцо функций в качестве подкольца функций-констант. Функции можно рассматривать и не все, а, например, те, которые можно представить в виде многочлена (т. е. целые рациональные функции), или для кольца $K = \mathbf{R}$ непрерывные, или дифференцируемые, или интегрируемые и т. п.

В каждом таком случае важнейшим подкольцом будет кольцо функций-констант, т. е. элементов из K . Если K конечно, то кольцо функций, определенных на K со значениями в K , тоже конечно, а если K состоит не из одного нуля, то кольцо функций над K содержит делители нуля.

Существенную роль при изучении групп и подгрупп оказало понятие *порождающего множества*. Это понятие является общим для произвольных алгебр и алгебраических систем. Особое значение имеет оно и для колец.

Пусть M — произвольное непустое подмножество множества кольца K . Рассмотрим пересечение всех подколец кольца K , содержащих подмножество M . Поскольку пересечение любого числа подгрупп снова является подкольцом, а пересечение — наименьшее среди таких подколец, получаем, что для каждого подмножества M кольца K существует наименьшее подкольцо кольца K , содержащее M .

Это подкольцо называют подкольцом, *порожденным множеством* M .

Чаще ситуация будет не такая общая, как в группах. Подкольцо обычно порождается множеством, полученным присоединением к уже имеющемуся подкольцу новых элементов.

Например, если S — подкольцо кольца K и a — элемент из K , то кольцо, порожденное множеством $S \cup \{a\}$, обычно обозначают

символом $S[a]$ и называют *простым кольцевым расширением* подкольца S с помощью элемента a (или *кольцевым присоединением* элемента a к кольцу S).

Присоединение более одного элемента к кольцу S уже не называют простым (*простота* состоит в единственности присоединяемого элемента), однако вполне может таковым оказаться. Оформляют присоединение более двух элементов аналогичным образом. Например, $S[a, b]$ — это *кольцевое расширение* подкольца S с помощью элементов a, b .

Если A и B — два подкольца кольца K , то наименьшим подкольцом, содержащим A и B , будет кольцо, порожденное множеством $A \cup B$. Вместе с обычным теоретико-множественным пересечением это теоретико-кольцевое объединение превращает множество подколец кольца K в решетку. Как и для групп, решетка подколец обладает наименьшим и наибольшим элементами, но, вообще говоря, не дистрибутивна.

Кольцо $K_1 = \langle K_1; +, \cdot \rangle$ *изоморфно* кольцу $K_2 = \langle K_2; +, \cdot \rangle$, если существует биекция φ множества K_1 на множество K_2 , сохраняющая операции кольца (для любых x, y из L_1):

$$\varphi(x + y) = \varphi(x) + \varphi(y);$$

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y).$$

Отношение изоморфности является отношением эквивалентности на множестве колец. Произведение изоморфизмов колец является изоморфизмом.

Свойство «быть кольцом» абстрактное: *алгебра, изоморфная кольцу, является кольцом*.

Обратим внимание на то, что если f — изоморфизм кольца K на алгебру K_1 и 0 — нулевой элемент кольца K , а 0_1 — нуль в K_1 , то $f(0) = 0_1$ и $f(-x) = -f(x)$.

Другими словами, при изоморфизме (при гомоморфизме, впрочем, тоже) нуль переходит в нуль, а противоположный — в противоположный.

Отметим, что для любого натурального m существует кольцо с ненулевым умножением, состоящее из m элементов, например кольцо классов вычетов по модулю m .

Наименьшее кольцо состоит только из одного нуля (*нулевое кольцо*). Все нулевые кольца изоморфны. Поскольку существуют кольца любой конечной мощности с ненулевым умножением, пара неизоморфных колец (одно — с нулевым, а другое — с ненулевым умножением) для любого конечного порядка всегда найдется. Однако для малых мощностей¹ этими незатейливыми примерами дело и ограничивается.

¹ Точнее, для всех конечных колец, содержащих простое число элементов.

Кольца с ненулевым умножением, состоящие из двух (или трех) элементов, изоморфны.

Кольцо \mathbb{Z}_4 классов вычетов по модулю четыре и кольцо

$$K = \langle P(\{a, b\}); \oplus, \cap \rangle$$

подмножеств двухэлементного множества обладают различными свойствами. Например, в \mathbb{Z}_4 не все элементы идемпотенты, а в K — все. Группа $\langle \mathbb{Z}_4; + \rangle$ циклическая, а в аддитивной группе кольца K нет элементов четвертого порядка. Мультипликативные группы этих колец состоят из различного числа элементов. Одного из этих свойств достаточно для неизоморфизма.

Таким образом, существуют неизоморфные кольца с ненулевым умножением, состоящие из четырех элементов.

В приведенном примере кольца неизоморфны очень сильно — неизоморфны ни их аддитивная, ни мультипликативная группы.

Кольцо целых чисел и кольцо четных целых чисел имеют изоморфные аддитивные группы, но эти кольца неизоморфны (первое кольцо с единицей, а второе — нет).

Даже для числовых колец может случиться, что их аддитивные и мультипликативные группы изоморфны, а сами кольца — нет.

Заметим сначала, что числовое кольцо с единицей непременно содержит кольцо целых чисел. Более того, *при любом изоморфизме двух числовых колец с единицами кольцо целых чисел остается неподвижным.*

Пусть

$$K_1 = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\};$$

$$K_2 = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}.$$

Оба множества являются подкольцами кольца комплексных чисел. Представление каждого элемента из кольца K_1 в виде $a + b\sqrt{-2}$ единственно (точно так же, как единственно представление элементов из K_2 в виде $a + b\sqrt{-3}$).

Отображение

$$a + b\sqrt{-2} \mapsto a + b\sqrt{-3}$$

биективно и сохраняет операции. Таким образом, аддитивные группы колец K_1 и K_2 изоморфны.

Отображение, переводящее каждое комплексное число в его модуль, сохраняет умножение

$$|z \cdot z_2| = |z_1| \cdot |z_2|.$$

Но тогда

$$|z_1 \cdot z_2|^2 = |z_1|^2 \cdot |z_2|^2,$$

а это значит, что отображение $z \mapsto |z|^2$ тоже сохраняет операцию умножения.

Квадрат модуля числа $a + b\sqrt{-2}$ имеет вид $a^2 + 2b^2$ и является целым числом. Теперь если элементы α и β из кольца K_1 обратимы, то

$$|\alpha|^2 \cdot |\beta|^2 = |1|^2 = 1.$$

Решения уравнение $x^2 + 2y^2 = 1$ в целых числах исчерпываются парами: $(1, 0)$ и $(-1, 0)$. Поэтому мультипликативная группа кольца K_1 — это $K_1^* = \{1, -1\}$. Точно так же устанавливается, что и $K_2^* = \{1, -1\}$.

Мультипликативные группы этих колец изоморфны.

С помощью того же отображения числа в квадрат своего модуля в каждом из колец можно установить простоту элемента.

Например, число $\sqrt{-2}$ является простым элементом в кольце K_1 , а числа 2 , $(1 + \sqrt{-3})$ и $(1 - \sqrt{-3})$ простые в K_2 .

Предположим теперь, что кольца K_1 и K_2 изоморфны. При этом изоморфизме кольцо целых чисел, входящее как в K_1 , так и в K_2 , остается неподвижным. В частности, число 4 при этом изоморфизме перейдет само в себя, поэтому должно обладать одинаковыми свойствами в каждом из колец. Однако это не так. В кольце K_1 число 4 обладает единственным представлением в виде произведения простых элементов кольца K_1 :

$$4 = \sqrt{-2} \cdot \sqrt{-2} \cdot \sqrt{-2} \cdot \sqrt{-2},$$

а в кольце K_2 таких представлений два:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3}).$$

Таким образом, существуют неизоморфные кольца с изоморфными аддитивными и мультипликативными группами.

Заметим, что рассмотренное свойство означает, что мультипликативные полугруппы этих двух колец неизоморфны. Однако в природе есть и более тонкие примеры неизоморфных ассоциативных колец с изоморфными аддитивными группами и изоморфными мультипликативными полугруппами.

Важную роль в школьном (и не только) курсе математики играет множество десятичных дробей.

Сумма, разность и произведение конечных десятичных дробей снова являются конечной десятичной дробью; следовательно, *множество конечных десятичных дробей образует кольцо*.

Ситуацию с кольцом десятичных дробей можно обобщить, а именно вместо чисел 2 и 5 взять произвольные простые числа. Кольцо десятичных дробей — это просто подкольцо в \mathbb{Q} , порожденное элементами $\frac{1}{2}$ и $\frac{1}{5}$.

Пусть M — некоторое множество простых чисел. Множество рациональных чисел, представимых несократимой дробью $\frac{a}{b}$, где в разложение числа b входят простые множители только из множества M , является кольцом.

Числовое кольцо K_M из только что рассмотренного примера порождается всеми дробями $\frac{1}{p_i}$, где p_i принадлежит множеству M .

В счетном множестве содержится континуум подмножеств. Не каждое подмножество множества рациональных чисел является кольцом. Поэтому в поле рациональных чисел содержится не более чем континуум подколец. В то же время множество простых бесконечно (счетно), и в этом множестве можно выбрать континуум различных подмножеств M . Поскольку различные M дадут различные подкольца, содной стороны, получаем: *в кольце рациональных чисел содержится в точности континуум различных подколец.*

С другой стороны, множество алгоритмов всего лишь счетно. Так что в кольце рациональных чисел содержатся кольца, для которых проблема вхождения алгоритмически неразрешима.

Такое кольцо можно указать и более явно. Множество простых чисел бесконечно, точнее, счетно. Существуют множества натуральных чисел, которые можно задать перечисляющим алгоритмом, но для которых алгоритмически неразрешима проблема вхождения (рекурсивно перечислимые, но не рекурсивные множества).

Взяв такое множество M в качестве номеров простых чисел, построим подкольцо K_M . Проблема вхождения в это кольцо будет алгоритмически неразрешима.

Уже было отмечено, что для любого подмножества M кольца K существует наименьшее подкольцо, содержащее подмножество M . Пусть S — некоторое кольцо, а мы рассматриваем подкольца (в частности подполя, если они есть) этого кольца.

Если K_1 и K_2 — два кольца и одно из них содержит другое, то K_1 называется подкольцом кольца K_2 , а K_2 — расширением кольца K_1 . При обсуждении порождающих множеств было отмечено, что интерес представляют не просто порождающие множества подколец, а именно расширения подколец.

Если P — подполе кольца S , то естественно любое подкольцо (или даже поле), содержащее P , называть *расширением* поля P .

Расширение поля P является векторным пространством над P .

Пусть K — подкольцо кольца S и a — элемент из S . Простое расширение $K[a]$ еще не определяется однозначно — в различных кольцах простое расширение будет устроено, вообще говоря, по-разному.

Рассмотрим особо случай, когда K является полем.

Элемент α называют *трансцендентным* над K , если α не является корнем никакого многочлена с коэффициентами из K . В таком случае кольцо $K[\alpha]$ называют *простым трансцендентным расширением* кольца K .

Покажем, что простое трансцендентное расширение существует для любого кольца K (может быть, вначале и не являющегося подкольцом некоторого большого кольца).

Если трансцендентное простое расширение $K[\alpha]$ кольца K существует, то каждый ненулевой элемент из $K[\alpha]$ можно единственным образом представить в виде

$$a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + a_n\alpha^n,$$

где $n \in \mathbb{Z}_0$, $a_i \in K$, $a_n \neq 0$.

Если кольцо многочленов было бы уже определено, то можно было сказать, что элементы простого трансцендентного расширения являются значениями всех многочленов с коэффициентами из K . Правда, многочлен можно и не определять, а назвать соответствующее выражение значением целой алгебраической функции.

Если даны два элемента из $K[\alpha]$, то можно считать, что число n , участвующее в их представлениях, одно и то же (добавив, если нужно, несколько нулей).

Тогда естественным образом определяются сложение и умножение элементов из $K[\alpha]$.

Если трансцендентное простое расширение $K[\alpha]$ кольца K существует, то элементы из $K[\alpha]$ можно представить в виде

$$f(\alpha) = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + a_n\alpha^n;$$

$$g(\alpha) = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1} + b_n\alpha^n.$$

а сложение и умножение в $K[\alpha]$ выполняются по следующим правилам:

$$f(\alpha) + g(\alpha) \stackrel{\text{опр}}{=} (a_0 + b_0) + (a_1 + b_1)\alpha + \dots + (a_{n-1} + b_{n-1})\alpha^{n-1} + (a_n + b_n)\alpha^n;$$

$$f(\alpha) \cdot g(\alpha) \stackrel{\text{опр}}{=} a_0b_0 + (a_1b_0 + a_0b_1)\alpha + \dots + \left(\sum_{s+k=i} a_sb_k \right) \alpha^i + \dots + a_nb_n\alpha^n.$$

Два последних утверждения начинаются словом «если»: «Если простое трансцендентное расширение существует, то ...». Это значит, что эти утверждения являются лишь *анализом* задачи на построение простого трансцендентного расширения.

Теперь нужно произвести построение (а затем доказательство и исследование).

Заметим сначала, что моделью из конечного числа элементов здесь не обойтись, даже если исходное кольцо конечно, так как трансцендентное расширение кольца всегда бесконечно. Соответ-

ственно, любое конечное надкольцо кольца K не является трансцендентным расширением кольца K .

Кольцо функций над конечным кольцом само конечно, а многочлены — это лишь частный случай функции. Множество всех многочленов даже над конечным кольцом бесконечно. Поэтому в случае конечного кольца многочлен в алгебраическом смысле и многочлен в функциональном смысле — понятия различные. Понятно, что если многочлены равны в алгебраическом смысле, то они равны и как функции. Обратное же утверждение, по крайней мере для конечных колец, не выполняется.

Итак, первая проблема состоит в том, чтобы показать, что для любого кольца K существует $K[x]$ — простое трансцендентное расширение кольца K .

Для решения этой задачи есть два пути.

Если кольцо является полем, то трансцендентное расширение строится как линейная алгебра счетной размерности над этим полем. Элементы вида

$$e_k = (\underbrace{0, 0, \dots, 0}_{k \text{ нулей}}, 1, 0, 0, \dots)$$

образуют базис этой линейной алгебры, а равенства $e_i \cdot e_j = e_{i+j}$ задают таблицу умножения этой линейной алгебры.

Любое целостное кольцо изоморфно вложимо в поле (поле частных). Поэтому, предварительно вложив целостное кольцо в поле, можно взять линейную алгебру со счетным базисом и таблицей умножения (структурными константами), как требуется для кольца многочленов, а затем в этой алгебре взять подалгебру, состоящую из линейных комбинаций только с коэффициентами из кольца K .

По традиции целостное кольцо считается не состоящим из одного нуля. Итак, для каждого целостного кольца K и трансцендентного над K элемента x существует простое трансцендентное расширение $K[x]$.

Ограничение о целостности кольца, хотя и важное для дальнейших применений, можно обойти (и провести, по существу, то же самое построение для произвольного кольца K).

Говорят, что *почти все* элементы из множества M обладают свойством P , если лишь мощность подмножества элементов, не обладающих этим свойством, строго меньше подмножества элементов, этим свойством обладающих:

$$|\{x \mid x \in M, \bar{P}(x)\}| < |\{x \mid x \in M, P(x)\}|.$$

Для счетного множества M это значит, что почти все элементы из M обладают свойством P , если лишь конечное число элементов из M не обладает этим свойством.

Например, если в некоторой *последовательности* элементов

$$a_1, a_2, \dots, a_n, \dots$$

из некоторого кольца K все элементы, начиная с некоторого места, равны нулю кольца, то говорят, что *почти все элементы этой последовательности равны нулю*.

Рассмотрим множество M всех последовательностей элементов из кольца K , в которых почти все элементы равны нулю:

$$M = \{(a_1, a_2, \dots, a_n, 0, 0, \dots) \mid a_i \in K\}.$$

Таким образом, M — подмножество из счетной декартовой степени множества K . Заметим сначала, что множество M всех последовательностей элементов из кольца K , в которых почти все элементы равны нулю, счетно или равносильно множеству K . Как обычно в декартовом произведении, две последовательности из M равны, если все их члены совпадают.

Определим операции сложения и умножения элементов из M в соответствии с результатами анализа. Если $\alpha = (a_1, a_2, \dots, a_n, 0, 0, \dots)$, $\beta = (b_1, b_2, \dots, b_m, 0, 0, \dots)$ — две последовательности из M , то полагаем:

$$\begin{aligned} \alpha + \beta &= \overset{\text{опр}}{(a_0 + b_0, a_1 + b_1, \dots, a_i + b_i, \dots)}; \\ \alpha \cdot \beta &= \overset{\text{опр}}{\left(a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots, \sum_{s+k} a_s b_k, \dots \right)}. \end{aligned}$$

Назовем счетную последовательность элементов из K , в которой почти все элементы равны нулю, *почти нулевой* последовательностью.

Множество всех почти нулевых последовательностей элементов из кольца K с операциями сложения и умножения, определенными правилами

$$\begin{aligned} (a_1, \dots, a_n, \dots) + (b_1, \dots, b_m, \dots) &= (a_0 + b_0, a_1 + b_1, \dots, a_i + b_i, \dots); \\ (a_1, \dots, a_n, \dots) \cdot (b_1, \dots, b_m, \dots) &= \left(a_0 b_0, \dots, \sum_{s+k=i} a_s b_k, \dots \right) \end{aligned}$$

образует кольцо.

Элементы вида $(a, 0, 0, 0, \dots)$, где $a \in K$, образуют подкольцо K_1 , изоморфное кольцу K . Элемент $(0, 1, 0, 0, \dots)$ является трансцендентным над K .

Но это значит, что для каждого ненулевого кольца K и трансцендентного над K элемента x существует простое трансцендентное расширение $K[x]$.

Присоединение к кольцу алгебраических элементов даже равных степеней может дать неизоморфные кольца.

Для трансцендентных расширений ситуация иная.

Если a, b — два трансцендентных элемента над кольцом K , то, продолжая отображение $a \mapsto b$ на все кольцо $K[a]$, получим взаимно однозначное, сохраняющее операции отображение кольца $K[a]$ на кольцо $K[b]$.

Иначе говоря, *все простые трансцендентные расширения кольца K изоморфны*.

Чтобы подчеркнуть нетривиальность ситуации, заметим, что для нетрансцендентных расширений последнее утверждение неверно (даже если расширяемое кольцо является полем или конечным кольцом). Нетрансцендентные простые расширения кольца не обязательно изоморфны (даже если они имеют одинаковые размерности как модули). Существуют неизоморфные, но равномощные конечные кольца $K[a]$ и $K[b]$ — простые расширения кольца K .

Для трансцендентных простых расширений замечание об изоморфизме можно усилить, взяв два изоморфных кольца в качестве колец коэффициентов.

Если кольца K_1 и K_2 изоморфны, то их простые трансцендентные расширения $K_1[x]$ и $K_2[x]$ тоже изоморфны.

Верно ли обратное утверждение для произвольных колец, т. е. следует из изоморфизма колец многочленов $K_1[x]$ и $K_2[x]$ изоморфизм колец коэффициентов K_1 и K_2 , пока (2021 г.) неизвестно.

5.2. Прямое произведение колец

Прямое произведение $A \times B$ колец A, B было определено еще в первой теме. Прямое произведение колец снова является кольцом, но так же, как и для групп (и произвольных алгебр), возникает следующий нюанс.

Слова «прямое произведение колец» двусмысленны: можно говорить о произведении как результате операции (*внешнее произведение*) или о разложении данного кольца в прямое произведение (*внутреннее*).

Хотя прямое произведение колец было определено внешним образом, на самом деле для изучения конкретных колец более важно внутреннее произведение.

Поскольку в алгебре изоморфные кольца не считаются различными, определить внутреннее прямое произведение можно точно так же, как и для групп.

Кольцо K разложимо в прямое произведение своих подколец A и B , если K изоморфно $A_1 \times B_1$, где A изоморфно A_1 , а B изоморфно B_1 . Каждое кольцо может быть тривиальным образом представлено в виде произведения самого себя и нулевого кольца. Под словами «*прямое разложение*» имеются в виду только нетривиальные представления.

Нулем в прямом произведении колец будет пара $(0, 0_1)$, состоящая из нулей сомножителей, а если кольца A, B с единицами, то пара единиц станет единицей прямого произведения.

Множество $A_1 = \{(a, 0_1) \mid a \in A\}$ образует подкольцо в K , изоморфное кольцу A . Аналогично пары с первым нулевым компонентом образуют подкольцо B_1 , изоморфное кольцу B .

С алгебраической точки зрения (не различающей изоморфные объекты) можно считать, что кольца A и B содержатся в кольце K .

Таким образом, прямые сомножители являются подкольцами прямого произведения колец.

Информация о прямом произведении групп сразу же дополнительно дает, что если кольцо K является прямым произведением подколец A и B , то оба эти подкольца имеют нулевое пересечение и $K = A + B$.

Из того, что A и B — сомножители прямого произведения, следует, что произведение ab , где $a \in A$ и $b \in B$, должно равняться нулю.

Итак, кольцо K является прямым произведением своих подколец A и B тогда и только тогда, когда пересечение подколец A и B состоит из одного нуля, множество

$$A + B = \{a + b \mid a \in A, b \in B\}$$

совпадает со всем K и для каждого a из A и каждого b из B произведение ab равно нулю.

Если кольцо K разложимо в прямое произведение, то аддитивная группа $\langle K; + \rangle$ разложима в прямую сумму своих подгрупп. Прямые слагаемые аддитивной группы кольца — это в точности аддитивные группы колец сомножителей.

Так что если аддитивная группа кольца неразложима в прямую сумму подгрупп, то кольцо неразложимо в прямое произведение.

Правда, неразложимость этого кольца можно увидеть и из других, более простых соображений. Если $K = A \times B$, то все произведения $a \cdot b$, где $a \in A, b \in B$, равны нулю. Это значит, что ни одно кольцо без делителей нуля не разложимо в прямое произведение.

В частности, неразложимы в прямые произведение все числовые кольца. Неразложимо в прямое произведение и кольцо многочленов с коэффициентами из поля.

Пусть K — кольцо многочленов от одного переменного с действительными коэффициентами. Множество многочленов с нулевым свободным членом образует подкольцо A . Рассмотрим еще кольцо B , состоящее из нуля и многочленов нулевой степени. Кольца A и B имеют нулевое пересечение, сумма $A + B$ совпадает с K , и все-таки K не является их прямым произведением. Это значит, чтобы быть прямым сомножителем кольца, мало быть подкольцом — нужны какие-то дополнительные качества. Какие?

В группах прямые сомножители являются еще и нормальными делителями, но здесь это предположение не несет никакой информации: в абелевой группе любая подгруппа — нормальный делитель.

Пусть кольцо K разложимо в прямое произведение подколец. В тех же обозначениях, что и ранее, имеем, что для каждого элемента $(a_1, 0_1)$ из A_1 и каждого элемента (a, b) из K :

$$(a, b) \cdot (a_1, 0_1) = (a \cdot a_1, b \cdot 0_1) = (a \cdot a_1, 0_1);$$

$$(a_1, 0_1) \cdot (a, b) = (a_1 \cdot a, 0_1 \cdot b) = (a_1 \cdot a, 0_1).$$

Это значит, что если A является прямым сомножителем кольца K , то A замкнуто относительно умножений слева и справа на элементы из K . Подкольцо с таким свойством называют *двусторонним идеалом* кольца K . Если K коммутативно, то можно не говорить о двух сторонах идеала, а называть A просто *идеалом*.

Итак, если кольцо K является прямым произведением, то каждый сомножитель является двусторонним идеалом.

Заметим, что это свойство прямого сомножителя можно увидеть и «изнутри». Если $K = A \times B$ и a — произвольный элемент из A , $x = a_1 + b$ — элемент из K , то

$$A \cdot (a_1 + b) = aa_1 + ab = aa_1 + 0 = aa_1;$$

$$(a_1 + b) \cdot a = a_1a + ba = a_1a + 0 = a_1a.$$

Элементы a_1a и aa_1 принадлежат подкольцу A , т. е. A — двусторонний идеал в K .

Как обычно, появляется пара *тривиальных идеалов* — само кольцо и нулевое подкольцо. В дальнейшем под словом «идеал» имеется в виду, как правило, нетривиальный идеал.

После этого понятно, почему кольцо многочленов не является прямой суммой своих подколец, хотя подкольцо многочленов без свободных членов и является идеалом, но подкольцо, состоящее из нуля и многочленов нулевой степени, т. е. подкольцо коэффициентов, — не идеал.

Кольцо без нетривиальных идеалов называют *простым*.

Простое кольцо заведомо неразложимо в прямое произведение. Нет идеалов — нет и прямых множителей.

Если в кольце с единицей все элементы обратимы, то любой его ненулевой идеал совпадает со всем кольцом. В частности, тело (или даже поле) является простым кольцом.

В некотором смысле верно и обратное утверждение: простое целостное кольцо с единицей является полем.

Таким образом, получается критерий простоты целостного кольца: *целостное кольцо с единицей просто тогда и только тогда, когда оно является полем.*

Ни тело, ни поле неразложимы в прямое произведение — там нет делителей нуля. Однако в кольце $M_n(P)$ квадратных $(n \times n)$ -матриц с элементами из поля P есть делители нуля (если $n > 1$), но $M_n(P)$ не раскладывается в прямое произведение, потому что кольцо квадратных матриц с элементами из поля просто.

Действительно, если A — ненулевая матрица, то с помощью элементарных преобразований ее можно превратить в диагональную матрицу D , по диагонали которой стоят единицы и нули (число единиц равно рангу матрицы A). Умножением на подходящие матрицы все единицы, кроме одной, в матрице D можно превратить в нули, а затем переместить эту единицу (если нужно) в любую строчку и столбец.

Таким образом, подходящими умножениями слева и справа матрицу A можно превратить в матрицу E_{ij} . Но матрицы E_{ij} вместе со скалярными матрицами порождают кольцо матриц. Это значит, что если матрица A при гомоморфизме переходит в нуль, то в нуль переходят и все остальные матрицы.

Возвращаемся к произвольным кольцам.

В приморазложимом кольце должно быть два идеала: A и B . Эти идеалы должны иметь нулевое пересечение и в комплексе $A + B$ давать все кольцо. После этого неудивительно, что далеко не каждое кольцо окажется разложимым в прямое произведение.

Заметим, что перечисленные свойства, необходимые для того, чтобы подкольцо было прямым сомножителем, являются и достаточными.

Кольцо K является прямым произведением своих подколец A и B тогда и только тогда, когда A, B — двусторонние идеалы в K , пересечение $A \cap B$ состоит из одного нуля, а комплекс $A + B$ совпадает с K .

Напомним важный пример кольца, разложимого в прямое произведение, и заодно уточним некоторые детали. Пусть числа a и b взаимно просты и $K = \mathbb{Z}_{ab}$ — кольцо классов вычетов по модулю ab . Множества

$$A = \{[bk] \mid k \in \mathbb{Z}\};$$

$$B = \{[ak] \mid k \in \mathbb{Z}\}$$

образуют идеалы в K . Кольцо A изоморфно кольцу классов вычетов \mathbb{Z}_a , а B изоморфно кольцу \mathbb{Z}_b .

Пересечение A и B состоит из одного класса $[ab]$, являющегося нулем в K . Каждое целое число (в том числе и представители классов) можно представить в виде $au + bv$, следовательно, кольцо K совпадает с комплексом $A + B$.

Короче говоря, если числа a, b взаимно просты, то кольцо классов вычетов \mathbb{Z}_{ab} является прямым произведением колец \mathbb{Z}_a и \mathbb{Z}_b :

$$\mathbb{Z}_{ab} = \mathbb{Z}_a \times \mathbb{Z}_b.$$

Понятно, что число множителей может быть и больше двух. Каждое натуральное число m , большее единицы, можно представить в виде произведения степеней простых чисел:

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n},$$

эти степени попарно взаимно просты, поэтому кольцо классов вычетов \mathbf{Z}_m по модулю m распадается в прямое произведение колец:

$$\mathbf{Z}_m = \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbf{Z}_{p_n^{\alpha_n}}.$$

Обратимые элементы прямого произведения колец получаются из обратимых элементов колец-сомножителей.

Если A, B — ассоциативные кольца с единицей, то мультипликативная группа прямого произведения колец является прямым произведением мультипликативных групп множителей:

$$(A \times B)^* = A^* \times B^*.$$

Число элементов в прямом произведении $A \times B$ конечных алгебр A и B равно произведению $|A| \cdot |B|$. Поэтому, в частности, если A, B — ассоциативные кольца с единицей, то

$$|(A \times B)^*| = |A^*| \cdot |B^*|.$$

Напомним, что из последнего равенства следует мультипликативное свойство функции Эйлера $\varphi(m)$: если a, b взаимно просты, то

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Кольцо несложно устроено, если оно является прямым произведением несложных колец. Самым несложным ненулевым кольцом с ненулевым умножением можно считать кольцо \mathbf{Z}_2 , содержащее всего лишь два элемента. Заметим, что это кольцо является одновременно и булевым кольцом.

Прямое произведение булевых колец снова образует булево кольцо. В частности, прямая степень двухэлементного булева кольца является булевым кольцом.

Оказывается, что других конечных булевых колец нет: *каждое конечное булево кольцо изоморфно прямой степени кольца \mathbf{Z}_2 .*

Отсюда следует, что все конечные булевы кольца изоморфны, а число элементов в них равно 2^n .

Впрочем, утверждение о числе элементов конечного булева кольца можно увидеть, используя сведения из линейной алгебры. Любое булево кольцо $\langle B; +, \cdot \rangle$ является векторным пространством над полем $\mathbf{Z}_2 = \{0, 1\}$, если положить (для любого x из B):

$$1 \cdot x = x;$$

$$0 \cdot x = 0.$$

Любое конечномерное векторное пространство изоморфно арифметическому пространству. Отсюда следует, что каждое конечное булево кольцо состоит из 2^n элементов.

Кроме того, арифметическое векторное пространство является прямой суммой одномерных подпространств, поэтому аддитивная группа $\langle B; + \rangle$ является прямой степенью группы $\langle \mathbb{Z}_2; + \rangle$.

Остается показать, что не только аддитивная группа, но и все кольцо распадается в прямое произведение двухэлементных колец, т. е. с точностью до изоморфизма

$$B = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_n = \mathbb{Z}_2^n,$$

где n — натуральное число. Докажем это утверждение индукцией по размерности пространства B . При $n = 1$ B совпадает с полем \mathbb{Z}_2 .

Пусть для $n - 1$ утверждение о разложимости кольца в прямую сумму подколец выполняется, а кольцо B как векторное пространство имеет размерность n .

По теореме Стоуна булево кольцо является булевой решеткой, т. е. частично упорядочено.

Поскольку $B \setminus \{0\}$ — конечное множество, в нем есть минимальные элементы. Пусть α_1 — один из них, тогда для любого элемента x из B точная нижняя грань элементов α_1 и x равна 0 или α_1 .

В векторном пространстве любой ненулевой элемент можно дополнить до базиса пространства. Дополним до базиса $\alpha_1, \beta_2, \dots, \beta_n$ элемент α_1 . Перейдем к новому базису $\alpha_1, \alpha_2, \dots, \alpha_n$ следующим образом:

$$\alpha_i = \begin{cases} \beta_i, & \text{если } \alpha_1 \beta_i = 0; \\ \alpha_1 + \beta_i, & \text{если } \alpha_1 \beta_i = \alpha_1. \end{cases}$$

Система $\alpha_1, \alpha_2, \dots, \alpha_n$ получена из базиса элементарными преобразованиями, поэтому она действительно снова образует базис. Кроме того, если $\alpha_i = \alpha_1 + \beta_i$, то

$$\alpha_1 \alpha_i = \alpha_1 (\alpha_1 + \beta_i) = \alpha_1 + \alpha_1 \beta_i = \alpha_1 + \alpha_1 = 0.$$

Таким образом, кольцо B распадается в прямое произведение подколец $A = \{0, \alpha\}$ и подкольца B_1 , порожденного элементами $\alpha_2, \dots, \alpha_n$. Для подкольца B_1 по индуктивному предположению существует изоморфное представление в виде прямой степени \mathbb{Z}_2 :

$$B_1 = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{n-1} = \mathbb{Z}_2^{n-1}.$$

Но тогда $B = A \times B_1$ изоморфно прямой степени \mathbb{Z}_2^n .

Итак, все конечные булевы кольца одинакового порядка изоморфны, а благодаря теореме Стоуна все конечные булевы решетки тоже изоморфны.

В качестве образца булевой решетки можно взять решетку, исследованную самим автором (Джорджем Булем) — решетку подмножеств некоторого множества. Каждая конечная булева решетка изоморфна решетке всех подмножеств некоторого конечного множества.

В заключение отметим, что конечно порожденное подкольцо любого булева кольца конечно, поэтому любое тождество для булевой алгебры достаточно доказать для конечной алгебры, т. е. алгебры подмножеств конечного множества.

Гомоморфизмы колец, а также кольца многочленов от одной или нескольких переменных обсуждаются в следующих темах.

5.3. Гомоморфизмы колец

Понятия гомоморфизма и изоморфизма — важнейшие для всех алгебр. Любое кольцо является, в частности, аддитивно записанной абелевой группой, поэтому все свойства гомоморфизмов групп выполняются и для аддитивной группы кольца. Однако гомоморфизмы колец имеют свою специфику. Кольцо $K_1 = \langle K_1; +, \cdot \rangle$ — гомоморфный образ кольца $K = \langle K; +, \cdot \rangle$, если существует отображение φ множества K на множество K_1 , сохраняющее операции кольца (для любых x, y из K):

$$\begin{aligned}\varphi(x + y) &= \varphi(x) + \varphi(y); \\ \varphi(x \cdot y) &= \varphi(x) \cdot \varphi(y).\end{aligned}$$

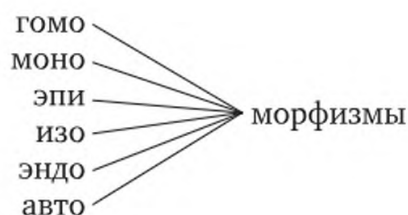
Отображение φ называют в таком случае *гомоморфизмом*.

Если φ — гомоморфизм кольца K на алгебру K_1 и 0 — нуль в K , то $\varphi(0)$ — нуль в K_1 и $\varphi(-x) = -\varphi(x)$. Кроме того, все тождества при гомоморфном отображении сохраняются; сохранится и дистрибутивность умножения относительно сложения. Поэтому *гомоморфный образ кольца является кольцом*.

В частности, если гомоморфизм является взаимно однозначным (т. е. изоморфизмом), то получаем, что изоморфный образ кольца является кольцом. Другими словами, свойство алгебры «быть кольцом» *абстрактное*.

Если отображение лишь сюръективное, но сохраняет операции, то его называют *эпиморфизмом*. Гомоморфизм в общем случае — это отображения *в* (внутри алгебры). Как и раньше (например, как для групп), под словом «гомоморфизм», как правило, будет пониматься эпиморфизм.

Приставки *эпи-, изо-, эндо-, авто-, гомо-* и *моно-* с корневым словом «морфизм» употребляются для колец точно так же, как и для групп (и для произвольных алгебр).



Гомоморфизмы колец обладают всеми свойствами гомоморфизмов всех алгебр; в частности, гомоморфизм задает конгруэнцию на кольце-прообразе, и наоборот — любая конгруэнция на множестве кольца определяет гомоморфизм этого кольца.

Для групп (кольцо является группой по сложению) конгруэнция, определяемая гомоморфизмом, полностью описывалась ядром этого (группового) гомоморфизма.

Если нет особых оговорок, то под словом «кольцо» сейчас будет подразумеваться ассоциативно-коммутативное кольцо без делителей нуля, т. е. *целостное кольцо* (к тому же, как правило, с единицей).

Кольцевой гомоморфизм является, в частности, гомоморфизмом аддитивных групп.

Пусть 0 — нулевой элемент кольца K_1 . Как и для группового гомоморфизма, полный прообраз нейтрального элемента при гомоморфизме $\varphi : K \rightarrow K_1$ называют *ядром гомоморфизма* φ :

$$\text{ядро } \varphi = \text{Ker } \varphi = \{x \in K \mid \varphi(x) = 0\}.$$

Ядро гомоморфизма $\varphi : K \rightarrow K_1$ колец K и K_1 является подкольцом в кольце K .

Действительно, если элементы x, y при гомоморфизме переходят в нулевой элемент, то их разность и произведение тоже переходят в нуль.

Обозначим $\text{Ker } \varphi = H$. Множество H образует подкольцо кольца K , и в частности $\langle H; + \rangle$ — это подгруппа группы $\langle K; + \rangle$. Кольцевой гомоморфизм является одновременно и групповым гомоморфизмом аддитивных групп колец. Гомоморфизм групп тесно связан со сравнимостью по модулю ядра: сравнимость по модулю H в K , заданная правилом

$$a \overset{\text{опр}}{\equiv} b \pmod{H} \Leftrightarrow a - b \in H,$$

согласована с операцией сложения.

Общие соображения о связи гомоморфизмов групп и конгруэнций на группах наводят на следующие предположения:

1) если H — ядро кольцевого гомоморфизма φ , то сравнимость по модулю H является *конгруэнцией*;

2) для того чтобы подкольцо H было ядром некоторого гомоморфизма, достаточно, чтобы сравнимость по модулю H была конгруэнцией.

Кроме того, ситуация с гомоморфизмами групп заставляет подозревать, что не каждое подкольцо кольца K является ядром некоторого гомоморфизма, как не каждая подгруппа способна быть ядром группового гомоморфизма.

Для того чтобы быть ядром группового гомоморфизма, подгруппа должна быть нормальной. Только для нормальной подгруппы сравнимость по модулю является конгруэнцией, и, соответственно, появляется фактор-группа и естественный гомоморфизм исходной группы на свою фактор-группу.

При описании кольцевого гомоморфизма или построении гомоморфизма для данного кольца возникает некий аналог нормальной подгруппы, но он не называется нормальным подкольцом. Его имя — *идеал*.

Пусть H — ядро гомоморфизма $\varphi : K \rightarrow K_1$. Мы уже знаем, что сравнимость по модулю подгруппы H согласована с операцией сложения:

$$a \equiv a_1 \pmod{H}, b \equiv b_1 \pmod{H} \Rightarrow a + b \equiv a_1 + b_1 \pmod{H}.$$

Предположим, что сравнимость по модулю H согласована и с операцией умножения, т. е.

$$a \equiv a_1 \pmod{H}, b \equiv b_1 \pmod{H} \Rightarrow ab \equiv a_1 b_1 \pmod{H}.$$

Тогда если $a_1 = a + h_1$, $b_1 = b + h_2$, то

$$a_1 b_1 = (a + h_1) \cdot (b + h_2) = ab + (ah_2 + h_1 b + h_1 h_2).$$

В случае согласованности с умножением элемент $ah_2 + h_1 b + h_1 h_2$ должен принадлежать подкольцу H .

Следовательно, для согласованности сравнимости по модулю H с умножением в кольце K достаточно, чтобы подкольцо H вместе с каждым своим элементом h содержало и произведение hx для всех элементов x из K :

$$ab \equiv a_1 b_1 \pmod{H}.$$

Это условие и необходимо; так, для a , сравнимого с нулем по модулю H , т. е. для $a = h$ элемента из H , имеем:

$$h \equiv 0 \pmod{H}, x \equiv x \pmod{H} \Rightarrow hx \equiv 0 \pmod{H}.$$

Последняя сравнимость означает, что hx принадлежит H .

Подведем итог: для того чтобы сравнимость по модулю подкольца H в кольце K была согласована не только со сложением, но и с умножением, необходимо и достаточно, чтобы подкольцо H было идеалом.

ножением, необходимо и достаточно замкнутости H относительно умножения на элементы кольца K .

Подкольцо, обладающее таким свойством, называют *идеалом* кольца K .

Другими словами, непустое подмножество I кольца K является идеалом, если:

- 1) $z, y \in I \Rightarrow x - y \in I$;
- 2) $x \in I$ и $z \in K \Rightarrow xz \in I$.

Наименьший идеал, содержащий подмножество M , состоящее из элементов кольца, принято изображать символом (M) . Фигурные скобки внутри круглых, как правило, опускают. Например, для случая двух порождающих вместо $(\{a, b\})$ пишут (a, b) .

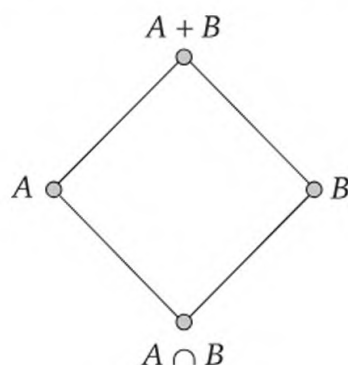
Пересечение любого числа идеалов содержит нулевой элемент, поэтому не пусто. Выполнение условий (1) и (2) для идеалов переносится на их пересечение, т. е. пересечение идеалов кольца снова образует идеал в этом кольце.

Если A, B — два идеала кольца K , то сумма идеалов

$$A + B = \{a + b \mid a \in A, b \in B\}$$

тоже является идеалом. Этот идеал — наименьший, содержащий идеалы A, B .

Таким образом, множество идеалов кольца образует решетку — подрешетку в решетке $L(K)$ всех подколец кольца K . На рисунке изображен типичный фрагмент этой решетки.



Решетка идеалов

Разумеется, этот ромбик в реальности может выродиться в отрезок, если один идеал содержится в другом.

Заметим: несмотря на то, что решетка $P(K)$ всех подмножеств множества K дистрибутивна (и даже булева), решетка идеалов всего лишь модулярна.

Докажем это утверждение, т. е. покажем, что для любых идеалов A, B, C кольца K :

$$A \cap [(A \cap B) + C] = (A \cap B) + (A \cap C).$$

Пусть x принадлежит $A \cap [A \cap B) + C]$, тогда

$$x \in A \text{ и } x = y + c,$$

где $y \in A \cap B$, $c \in C$. Отсюда следует, что $c = x - y$ принадлежит A , поэтому $c \in A \cap C$. Это значит, что $y + c$ принадлежит $(A \cap B) + (A \cap C)$ и, следовательно,

$$A \cap [(A \cap B) + C] \subset (A \cap B) + (A \cap C).$$

Докажем обратное включение. Пусть

$$x \in (A \cap B) + (A \cap C),$$

тогда $x \in (A \cap B) + C$. Кроме того, $x = y + z$, где $y \in A \cap B$ и $z \in A \cap C$, и, следовательно, элемент x принадлежит A :

$$A \cap [(A \cap B) + C] \supset (A \cap B) + (A \cap C).$$

Итак, *решетка идеалов целостного кольца модулярна.*

Связь между понятиями идеала и нормального делителя теснее, чем это кажется на первый взгляд. Решетка нормальных делителей группы тоже модулярна, причем доказательство модулярности решетки нормальных делителей в группе почти буквально повторяет приведенное доказательство модулярности решетки идеалов кольца.

Вернемся, впрочем, к обсуждению связи между идеалами кольца и его гомоморфизмами. Нуль является поглощающим элементом кольца, поэтому ядро гомоморфизма $\varphi : K \rightarrow K_1$ колец K и K_1 является идеалом в кольце K .

Не каждое подкольцо кольца обязано удовлетворять дополнительному идеальному свойству. Например, множество коэффициентов K образует кольцо, но не идеал в кольце всех многочленов $K[x]$ с коэффициентами из K . Следовательно, *не каждое подкольцо является ядром кольцевого гомоморфизма.*

Каждый ли идеал кольца является ядром некоторого гомоморфизма кольца? Другими словами, переносится ли теорема о гомоморфизмах групп на кольца?

Ответ на этот вопрос положительный: да, каждый идеал является ядром некоторого (точнее, естественного) гомоморфизма.

Докажем это утверждение.

Пусть I — идеал кольца K . Используя построение для групп, устроим гомоморфизм, ядром которого является I . Как и для групп, символом K/I обозначим фактор-множество по сравнимости по модулю I :

$$K/I = \{I, \dots, I + x, \dots, I + y, \dots\}.$$

Теперь для доказательства нашего утверждения достаточно показать, что отношение сравнимости по модулю I и операции кольца согласованы:

$$x \equiv x_1 \pmod{I}, y \equiv y_1 \pmod{I} \Rightarrow x + y \equiv x_1 + y_1 \pmod{I};$$

$$x \equiv x_1 \pmod{I}, y \equiv y_1 \pmod{I} \Rightarrow x \cdot y \equiv x_1 \cdot y_1 \pmod{I}.$$

Согласованность сравнимости со сложением выполняется потому, что кольцевой гомоморфизм является групповым гомоморфизмом для аддитивных групп колец. Согласованность сравнимости с умножением выполнена благодаря дополнительному идеальному свойству подкольца I , а именно замкнутости относительно умножения на произвольные элементы кольца.

Согласованность сравнимости по модулю I с операциями кольца позволяет определить операции на множестве K/I смежных классов по идеалу следующими правилами:

$$(I + x) + (I + y) = I + (x + y), (I + x) \cdot (I + y) = I + x \cdot y.$$

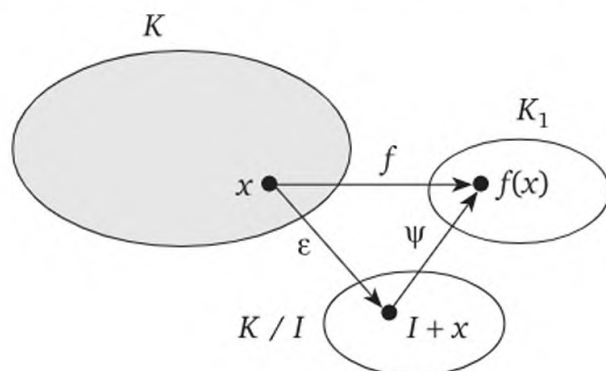
Кольцо $\langle K/I; +, \cdot \rangle$ называют *фактор-кольцом* кольца K по идеалу I .

Отображение $\varepsilon : K \rightarrow K/I$, переводящее каждый элемент x кольца K в смежный класс $I + x$, сохраняет операции, т. е. является *гомоморфизмом*.

Гомоморфизм ε , как и для произвольной алгебры, принято называть *естественным гомоморфизмом* кольца.

Роль нуля в кольце K/I играет идеал I , поэтому ядром естественного гомоморфизма является I . Этим установлено, в частности, что *каждый идеал кольца является ядром некоторого гомоморфизма*.

Как и для групп, естественными гомоморфизмами фактически исчерпываются все гомоморфизмы кольца. Иначе говоря, и для колец выполняется *теорема о гомоморфизмах*: *гомоморфный образ кольца изоморфен фактор-кольцу по ядру гомоморфизма*.



К теореме о гомоморфизмах колец

Изобразим ситуацию графически. Схема в точности такая же, как и для групп. Точнее, это и есть иллюстрация группового го-

гомоморфизма f аддитивных групп K и K_1 . Оказалось, что изоморфизм ψ вместе со сложением сохраняет и умножение в кольце. Из схемы, приведенной на рисунке, видно, что произвольный гомоморфизм f является композицией естественного гомоморфизма ε и некоторого изоморфизма ψ :

$$f = \varepsilon \circ \psi.$$

Это значит, что с точностью до изоморфизма все гомоморфизмы колец естественные.

Таким образом, как и для групп, описание всех гомоморфных образов кольца K (образно говоря, всех «внешних связей» кольца K) можно получить, не выходя из этого K . Вместо исследования гомоморфизмов кольца достаточно изучить его идеалы.

Например, если в кольце нет идеалов (кроме тривиальных — нулевого и самого кольца K), то нет и нетривиальных гомоморфизмов. Тривиальными гомоморфизмами являются изоморфизмы и нулевой гомоморфизм.

Кольцо без нетривиальных идеалов называют *простым кольцом*.

Например, поле не имеет нетривиальных идеалов, поэтому является простым кольцом. В поле содержится не менее двух элементов. Поэтому, говоря о гомоморфизме полей, нулевой гомоморфизм придется исключить. При таком договоре простота поля как кольца означает, что любой гомоморфизм поля является изоморфизмом.

Все предыдущие рассуждения касались коммутативных колец. Для некоммутативных колец ядро гомоморфизма I является двусторонним идеалом, т. е. для I выполняется условие

$$x \in I; z_1, z_2 \in K \Rightarrow z_1 x z_2 \in I.$$

Если некоммутативное кольцо не имеет нетривиальных двусторонних идеалов, то оно просто.

Ненулевой двусторонний идеал тела содержит все элементы этого тела, следовательно, тело — простое кольцо.

Можно говорить о простоте и нецелостного кольца. Например, для $n > 1$ полное матричное кольцо $M_n(P)$ над полем P не содержит двусторонних идеалов и поэтому просто: у матричного кольца тоже нет нетривиальных гомоморфизмов.

Вернемся вновь к целостным кольцам.

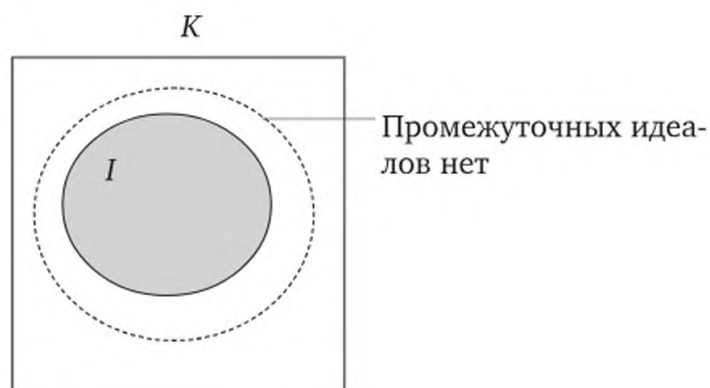
Все идеалы кольца \mathbf{Z} целых чисел были уже описаны ранее — это в точности множества кратных некоторого целого числа.

Идеал кольца, порожденный одним элементом a , называют *главным идеалом* и обозначают символом (a) . Все идеалы в кольце целых чисел главные.

Все гомоморфные образы кольца \mathbf{Z} — это с точностью до изоморфизма кольца классов вычетов $\mathbf{Z}_m = \mathbf{Z}/(m)$. Заметим, что $\mathbf{Z}/(2)$ —

это двухэлементное поле, да и вообще $\mathbf{Z}/(p)$ — поле тогда и только тогда, когда p — простое число.

Это неслучайно: между (p) и \mathbf{Z} нет промежуточных идеалов, поэтому фактор-кольцо $\mathbf{Z}/(p)$ является простым и, следовательно, образует поле.



I — максимальный идеал в кольце K

В общем случае это свойство сохранится. Если идеал I максимальный в целостном с единицей кольце K , то фактор-кольцо K/I является полем.

Докажем это утверждение.

Фактор-кольцо K/I ассоциативно-коммутативное и содержит единицу, ее роль играет смежный класс $I + 1$.

Если класс $I + x$ ненулевой, то $x \notin I$. Поэтому идеал (I, x) в кольце K , порожденный множеством $I \cup \{x\}$ и элементом x , совпадает со всем кольцом K . Идеал $I \cup \{x\}$ является суммой идеалов:

$$I \cup \{x\} = I + (x).$$

Вхождение единицы в эту сумму означает, что для некоторого элемента h из I и элемента u из K

$$1 = h + xu.$$

Иначе говоря,

$$xu \equiv 1 \pmod{I}.$$

Следовательно, класс $I + u$ — элемент фактор-кольца, обратный для элемента $I + x$. Это значит, что у каждого ненулевого элемента в фактор-кольце есть обратный. Кольцо K/I образует поле.

Верно и обратное утверждение: если K/I — поле, то идеал I максимальный в K . Действительно, если I — не максимальный, то найдется такой элемент x , что

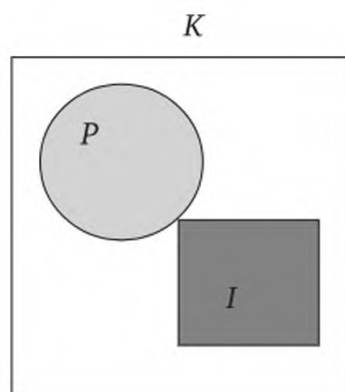
$$I + (x) \neq K.$$

Если бы единица попала в $I + (x)$, то там находились бы и все остальные элементы кольца. Поэтому для всех элементов u из K :

$$I + xu \neq I + 1.$$

Элемент $I + x$ необратим.

Таким образом, если K — целостное кольцо с единицей, то фактор-кольцо K/I является полем тогда и только тогда, когда идеал I максимальный в кольце K .



P — подполе кольца K

Перед следующим наблюдением напомним, что если в частично упорядоченном множестве каждое линейно упорядоченное подмножество имеет верхнюю грань, то по лемме Цорна в этом множестве есть максимальные элементы.

Пусть целостное кольцо K содержит в качестве подкольца некоторое поле P . Рассмотрим все идеалы кольца, имеющие с P нулевое пересечение. Объединение возрастающей цепочки таких идеалов снова является идеалом с тем же свойством. Поэтому по лемме Цорна найдется максимальный (с нулевым пересечением с P) идеал I . Однако этот идеал I будет просто максимальным в P , так как любой идеал, пересекающийся с P не по нулевому идеалу, содержит все элементы кольца K .

Если K — целостное кольцо, содержащее поле P , то в K существует такой идеал I , что фактор-кольцо K/I является полем и это поле содержит изоморфную копию P .

С помощью фактор-колец мы можем указать новое построение поля комплексных чисел, а заодно и кольца $\mathbb{Z}[i]$ целых гауссовых чисел:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}.$$

Покажем, что поле комплексных чисел изоморфно фактор-кольцу кольца многочленов $\mathbb{R}[x]$ с действительными коэффициентами по идеалу I , порожденному многочленом $x^2 + 1$.

Отметим, что элемент $x^2 + 1$ простой в кольце $\mathbf{R}[x]$, поэтому идеал I максимальный в $\mathbf{R}[x]$. Действительно, если H — промежуточный идеал, т. е.

$$I < H < K,$$

то H порождается многочленом, который делит многочлен $x^2 + 1$. Нетривиальных делителей в кольце $\mathbf{R}[x]$ у этого многочлена нет, следовательно, фактор-кольцо K/I образует поле.

Фактор-кольцо K/I можно представить в виде

$$K/I = \{I + (a + bx) \mid a, b \in \mathbf{R}\},$$

так как остаток от деления на $x^2 + 1$ — это многочлен степени не выше первой.

Вычислим сумму и произведение смежных классов:

$$\begin{aligned}(I + (a + bx)) + (I + (c + dx)) &= I + (a + c) + (b + d)x; \\ [I + (a + bx)] \cdot [I + (c + dx)] &= I + [ac + (bc + ad)x + bdx^2] = \\ &= I + [(ac - bd) + (ad + bc)x].\end{aligned}$$

Соответствие $I + (a + bx) \mapsto a + bi$, где $a, b \in \mathbf{R}$, является взаимно однозначным, сохраняющим операции. Таким образом, поле комплексных чисел изоморфно фактор-кольцу

$$\frac{\mathbf{R}[x]}{(x^2 + 1)}.$$

Аналогичным образом в кольце $\mathbf{Z}[x]$ многочленов с целыми коэффициентами построим идеал H , порожденный многочленом $x^2 + 1$.

Поскольку остаток от деления на $x^2 + 1$ — это многочлен степени не выше первой, фактор-кольцо K/H можно представить в виде

$$K/H = \{H + (a + bx) \mid a, b \in \mathbf{Z}\}.$$

Вычислим сумму и произведение смежных классов:

$$\begin{aligned}(H + (a + bx)) + (H + (c + dx)) &= H + (a + c) + (b + d)x; \\ (H + (a + bx)) \cdot (H + (c + dx)) &= H + ac + (bc + ad)x + bdx^2 = \\ &= H + (ac - bd) + (ad + bc)x.\end{aligned}$$

Отображение $H + (a + bx) \mapsto a + bi$, где $a, b \in \mathbf{Z}$, является взаимно однозначным, сохраняющим операции, и, таким образом, кольцо целых гауссовых чисел изоморфно фактор-кольцу

$$\frac{\mathbf{Z}[x]}{(x^2 + 1)}$$

кольца многочленов $\mathbf{Z}[x]$ с целыми коэффициентами по идеалу, порожденному многочленом $x^2 + 1$.

Обратим внимание на то, что многочлен $x^2 + 1$ не раскладывается на множители первой степени с целыми коэффициентами, т. е. он играет в кольце $\mathbf{Z}[x]$ роль *простого элемента*, но идеал, порожденный им, *не максимальный*.

Кольцо целых гауссовых чисел не является полем, в нем обратимы лишь элементы, имеющие единичный модуль:

$$(\mathbf{Z}[i])^* = \{1, -1, i, -i\}.$$

Действительно, если $a + bi$ и $c + di$ — делители единицы, то

$$(a + bi)(c + di) = 1.$$

Поэтому

$$|a + bi|^2 \cdot |c + di|^2 = |1|^2 = 1.$$

Отсюда $a^2 + b^2 = 1$, следовательно, $a = 0$ или $b = 0$ и, соответственно, $b = \pm 1$, $a = \pm 1$.

В кольце целых чисел множество обратимых элементов было еще меньше, всего лишь $\{1, -1\}$, но с идеалами ситуация иная: в кольце \mathbf{Z} множество максимальных идеалов и множество идеалов, порожденных простыми элементами, совпадают.

Идеалы представляют интерес не только в связи с разложимостью в прямое произведение и гомоморфизмами колец. Существует тесная связь между идеалами, порожденными одним элементом, и отношением делимости в кольце.

Обычно отношение делимости рассматривают лишь в целостных кольцах.

5.4. Свойства делимости в целостном кольце

Отношение делимости в целостном кольце K можно определить точно так же, как в кольце \mathbf{Z} целых чисел. Отношение делимости в K обозначают тем же символом $|$:

$$x \overset{\text{опр}}{|} y \Leftrightarrow (\exists z \in K) [xz = y].$$

Отношение делимости в целостном кольце рефлексивно и транзитивно, т. е. является отношением *предпорядка*. Определим, как обычно, отношение *ассоциированности* \sim (для всех элементов a, b из K):

$$a \overset{\text{опр}}{\sim} b \Leftrightarrow a | b \text{ и } b | a.$$

Отношение ассоциированности рефлексивно, транзитивно и симметрично, т. е. является эквивалентностью.

В ассоциативном кольце K с единицей множество K^* обратимых элементов (делителей единицы) образует мультипликативную группу.

Если два ненулевых элемента a, b ассоциированы, то для некоторых элементов c, d выполняются равенства

$$ac = b, bd = a.$$

Отсюда следует, что $bdc = b$. Поскольку в целостном кольце выполняется закон сокращения, из равенства $bdc = b$ следует: $dc = 1$. Это значит, что дополняющие множители, участвующие в ассоциировании элементов, являются делителями единицы.

На делитель единицы делится любой элемент кольца, и, следовательно, $a \sim b$ тогда и только тогда, когда $a = \varepsilon b$, где $\varepsilon \in K^*$:

$$a \sim b \Leftrightarrow (\exists \varepsilon \in K^*) [a = \varepsilon b].$$

Как всякая эквивалентность, ассоциированность разбивает множество K на смежные классы. Число нуль образует один класс (нуль делится только сам на себя), а остальные классы содержат столько элементов, сколько их в группе делителей единицы.

Ассоциированность согласована с отношением делимости: если $a \sim a_1$ и $b \sim b_2$, то

$$a | b \Leftrightarrow a_1 | b_2.$$

Другими словами, фактор-множество K / \sim частично упорядочено отношением делимости.

Граф отношения делимости на множестве K / \sim имеет наивысшую точку (это нулевой класс, состоящий из одного нуля, — наибольший в смысле делимости элемент). Внизу графа находится класс K^* — наименьший элемент в этом порядке.

Любое упорядоченное множество изоморфно некоторому множеству подмножеств с отношением включения. Изоморфизм этот устанавливается с помощью отображения элемента x в множество элементов (x), не меньших (или не больших) элемента x . Эту идею удобно применить для изучения отношения делимости в целостном кольце.

Множество $(a) = \{ak \mid k \in K\}$ кратных элемента a в кольце K образует идеал, который называют главным идеалом, порожденным элементом a .

Из определения делимости получаем (для любых элементов a, b из K):

$$a | b \Leftrightarrow (a) \supset (b);$$

$$a \sim b \Leftrightarrow (a) = (b).$$

Это значит, что отношение делимости в кольце K изоморфно представляется отношением включения на множестве главных идеалов кольца K .

Вспомним, что если A, B — два (не обязательно главных) идеала кольца K , то их пересечение $A \cap B$ и сумма $A + B$ снова являются идеалами того же кольца.

Множество всевозможных сумм

$$a_1b_1 + a_2b_2 + \dots + a_kb_k.$$

где $a_i \in A, b_i \in B$, образует идеал, который обозначают символом AB и называют *произведением* идеалов.

Сумма двух идеалов A и B случайно может совпасть со всем кольцом K . В таком случае эти идеалы называют *взаимно простыми*. Если кольцо K с единицей, то для совпадения $A + B$ со всем кольцом достаточно, чтобы в эту сумму попала единица кольца.

Отметим, что взаимно простые в обычном смысле элементы (т. е. элементы, наибольший общий делитель которых равен единице) могут порождать не взаимно простые идеалы. Например, идеалы (x) и (2) в кольце $\mathbb{Z}[x]$ не взаимно просты:

$$(x) + (2) \neq \mathbb{Z}[x],$$

хотя многочлены x и 2 взаимно просты.

Пусть K — кольцо с единицей и A, B, C — его идеалы. Если идеал A взаимно прост с идеалом B и с идеалом C , то A взаимно прост и с идеалом $B \cap C$. Действительно, для некоторых элементов a_1, a_2 из A, b из B и c из C

$$a_1 + b = 1, a_2 + c = 1.$$

Следовательно, и

$$u = (a_1 + b)(a_2 + c) = 1.$$

Элемент

$$u = (a_1a_2 + a_1c + ba_2) + bc$$

принадлежит идеалу $A + B \cap C$, поэтому $A + B \cap C = K$, а это и означает, что идеалы A и $B \cap C$ взаимно просты.

Китайская теорема об остатках на языке идеалов в кольце \mathbb{Z} означает, что если каждая пара различных идеалов I_1, I_2, \dots, I_n в сумме дает все кольцо \mathbb{Z} , то для любых элементов c_1, c_2, \dots, c_n из кольца \mathbb{Z} пересечение смежных классов $I_i + c_j$ не пусто:

$$(I_1 + c_1) \cap (I_2 + c_2) \cap \dots \cap (I_n + c_n) \neq \emptyset.$$

Докажем это утверждение для произвольного целостного кольца K с единицей. Проведем доказательство методом математической индукции, а именно индукцией по n .

База индукции. Пусть $n = 2$. Равенство $I_1 + I_2 = K$ означает, что любой элемент x из K можно представить в виде

$$x = m_1 + m_2,$$

где $m_1 \in I_1$ и $m_2 \in I_2$. Элемент $c_1 - c_2$ не является исключением:

$$c_1 - c_2 = m_1 + m_2,$$

а это значит, что элемент

$$-m_1 + c_1 = m_2 + c_2$$

принадлежит пересечению $(I_1 + c_1) \cap (I_2 + c_2)$. База индукции доказана. Доказанное утверждение означает, что система из двух сравнений со взаимно простыми идеалами I_1 и I_2

$$\begin{cases} x \equiv c_1 \pmod{I_1}, \\ x \equiv c_2 \pmod{I_2} \end{cases} \quad (*)$$

всегда имеет решение.

Заметим, что система (*) равносильна системе

$$\begin{cases} x \equiv c_1 \pmod{I_1 \cap I_2}, \\ x \equiv c_2 \pmod{I_2 \cap I_2} \end{cases}$$

и любые два решения системы (*) сравнимы по модулю $I_1 \cap I_2$.

Шаг индукции. По индуктивному предположению утверждение верно для $n - 1$ идеала, а доказать его сейчас требуется для I_1, I_2, \dots, I_n идеалов, где $n > 2$. Утверждение китайской теоремы означает, что система сравнений

$$\begin{cases} x \equiv c_1 \pmod{I_1}, \\ x \equiv c_2 \pmod{I_2}, \\ \dots\dots\dots \\ x \equiv c_n \pmod{I_n} \end{cases} \quad (**)$$

для наших идеалов всегда имеет решение.

Пусть x_0 — решение системы (*) из базы индукции. Это значит, что система сравнений (**) равносильна системе

$$\begin{cases} x \equiv x_0 \pmod{I_1 \cap I_2}, \\ x \equiv c_3 \pmod{I_3}, \\ \dots\dots\dots \\ x \equiv c_n \pmod{I_n}. \end{cases}$$

Идеал $I = I_1 \cap I_2$ взаимно прост с идеалами I_3, \dots, I_n , поэтому по индуктивному предположению система, состоящая из $n - 1$ сравнения, решение имеет.

Шаг индукции и китайская теорема об остатках доказаны.

Относительно строения кольца Z_m китайская теорема об остатках — это просто другая формулировка уже доказанного ранее факта: если $m = m_1 m_2 \dots m_n$, где m_i попарно взаимно просты, то кольцо Z_m разлагается в прямое произведение:

$$Z_m = Z_{m_1} \times Z_{m_2} \times \dots \times Z_{m_n}.$$

Ситуация с кольцом целых чисел допускает естественное обобщение.

Пусть K — целостное кольцо, а I и J — идеалы кольца K такие, что $I + J = K$. Тогда для любых элементов x, y из K пересечение смежных классов $I + x$ и $J + y$ не пусто, а фактор-кольцо $K / (I \cap J)$ изоморфно прямому произведению $(K / I) \times (K / J)$.

Главный идеал — это однопорожденный идеал. Вполне может случиться, что в кольце все идеалы хотя и не главные, но конечно порожденные.

Объединение возрастающей цепочки идеалов является идеалом, поэтому если все идеалы кольца K конечно порождены, то каждая возрастающая цепочка через конечное число звеньев захватит все порождающие элементы объединения этой цепочки. Следовательно, цепочка обрывается (а точнее, стабилизируется) на конечном шаге.

Отношение делимости в целостном кольце K частично упорядочивает фактор-множество $K_1 = K / \sim$ кольца K по ассоциированности \sim . Элемент K^* , состоящий из делителей единицы кольца K , будет наименьшим, а $\{0\}$ — наибольшим в этом отношении порядка.

Выбросим наименьший и наибольший элементы из множества K_1 . Вполне может случиться, что после выбрасывания там ничего и не останется, но тогда и говорить будет не о чем. Если же множество $K_1 \setminus (\{0\} \cup K^*)$ не пусто, то представителей минимальных классов (если они там есть) называют простыми элементами кольца K .

Другими словами, элемент p из целостного кольца K является простым, если p — не делитель единицы, не ноль и

$$p = ab \Rightarrow a \in K^* \text{ или } b \in K^*.$$

Ненулевой, необратимый и непростой элемент кольца называют составным.

Иначе говоря, a составной, если его можно представить в виде

$$a = bc, \text{ где } b \notin K^* \text{ и } c \notin K^*.$$

Все кольцо K распадается на четыре непересекающихся класса (некоторые из них, может быть, и пусты): нуль, делители единицы, простые элементы, составные элементы.



Строение кольца

На языке идеалов простота элемента p означает, что между идеалом (p) и кольцом K нет промежуточных *главных* идеалов: (p) — максимальный главный идеал, не совпадающий с кольцом K .

Соответственно, если a — составной элемент, то между идеалом (a) найдется промежуточный *главный* идеал (b) , не совпадающий ни с идеалом (a) , ни с кольцом K :

$$(a) \subset (b) \subset K.$$

В целостном кольце выполняется закон сокращения. Если a является произведением двух простых элементов, $a = p_1 p_2$ и (x) — промежуточный идеал между (a) и (p_2) , то

$$a = xk = p_2 mk = p_1 p_2$$

и по закону сокращения $mk = p_1$. Но тогда m или k — делитель единицы и, следовательно, (x) — ненастоящий промежуточный идеал в цепочке:

$$(a) \subset (x) \subset (p_2).$$

На самом деле, он совпадает с идеалом (a) или с идеалом (p_2) .

Итак, если $a = p_1 p_2$, то в цепочке идеалов

$$(a) \subset (p_2) \subset K$$

нельзя поместить промежуточный идеал.

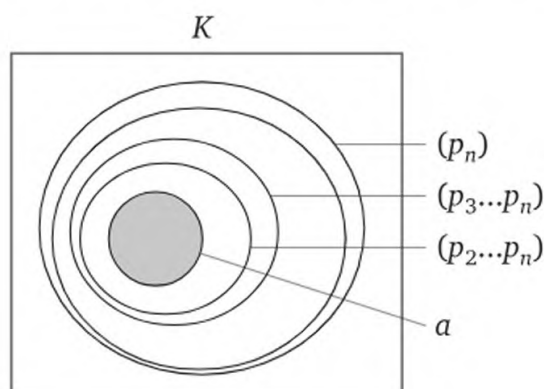
В общей ситуации если элемент a можно представить в виде произведения простых элементов

$$a = p_1 p_2 \dots p_n,$$

то цепочка

$$(a) \subset (p_2 \cdot \dots \cdot p_n) \subset (p_3 \cdot \dots \cdot p_n) \subset \dots \subset (p_n) \subset K$$

вложенных друг в друга идеалов *плотная*: в этой цепочке все идеалы, кроме K , — максимальные главные идеалы в следующем идеале.



Возрастающая цепочка идеалов

Основная теорема арифметики, утверждающая, что каждое целое число, отличное от 0, 1 и -1 , является простым или произведением простых, причем это произведение единственно с точностью до порядка и ассоциированности множителей, означает, что в кольце целых чисел от любого ненулевого собственного идеала можно протянуть плотную (и в некотором смысле единственную) цепочку главных идеалов.

Заметим, что в произвольном целостном (и даже числовом) кольце аналог основной теоремы арифметики выполняется не всегда.

Например, в кольце $\langle \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}; +, \cdot \rangle$ число 4 обладает двумя различными представлениями в виде произведения простых неассоциированных множителей:

$$4 = 2 \cdot 2 = (1 - \sqrt{-3}) \cdot (1 + \sqrt{-3}).$$

В кольце $\langle \{a + b\sqrt{-7} \mid a, b \in \mathbb{Z}\}; +, \cdot \rangle$ число 8 обладает двумя различными представлениями в виде произведения простых неассоциированных множителей:

$$8 = 2 \cdot 2 \cdot 2 = (1 + \sqrt{-7}) \cdot (1 - \sqrt{-7}).$$

В отличие от предыдущего кольца в кольце $\langle \{a + b\sqrt{-7} \mid a, b \in \mathbb{Z}\}; +, \cdot \rangle$ число 8 имеет два разложения, в которых даже число простых множителей различно.

Доказательство в обоих случаях опирается на множество обратимых элементов этих колец (и, соответственно, отношение ассоциированности). Найти же множество обратимых элементов помогает мультипликативное свойство квадрата модуля комплексного числа.

Найдем обратимые элементы кольца:

$$\langle \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}; +, \cdot \rangle.$$

Для этого сначала вычислим квадрат модуля комплексного числа $a + b\sqrt{-3}$:

$$|a + b\sqrt{-3}|^2 = (\sqrt{a^2 + 3b^2})^2 = a^2 + 3b^2.$$

Поскольку модуль комплексного числа обладает свойством мультипликативности,

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|,$$

этим же свойством обладает и квадрат модуля.

Пусть теперь $a + b\sqrt{-3}$ — обратимый элемент нашего кольца. Это значит, что существует такое число $c + d\sqrt{-3}$, что

$$(a + b\sqrt{-3}) \cdot (c + d\sqrt{-3}) = 1.$$

Вычислим квадрат модуля от левой и правой частей:

$$|(a + b\sqrt{-3})(c + d\sqrt{-3})|^2 = |1|^2.$$

Отсюда

$$|a + b\sqrt{-3}|^2 \cdot |c + d\sqrt{-3}|^2 = 1,$$

следовательно,

$$(a^2 + 3b^2)(c^2 + 3d^2) = 1.$$

Уравнение $a^2 + 3b^2 = 1$ с неизвестными a, b имеет только два целочисленных решения: $(1, 0)$ и $(-1, 0)$. Это значит, что в кольце $\langle \{a + b\sqrt{-3} | a, b \in \mathbb{Z}\}; +, \cdot \rangle$ только два обратимых элемента: 1 и -1 .

Следовательно, числа 2 и $1 \pm \sqrt{-3}$ неассоциированы, они отличаются более чем на множитель ± 1 .

Однако может случиться, что эти числа не простые в рассматриваемом кольце.

Покажем, что число 2 простое, т. е.

$$2 = ab \Rightarrow a \in K^* \text{ или } b \in K^*.$$

Из равенства

$$2 = (a + b\sqrt{-3}) \cdot (c + d\sqrt{-3})$$

следует

$$|a + b\sqrt{-3}|^2 \cdot |c + d\sqrt{-3}|^2 = 4.$$

Уравнение $a^2 + 3b^2 = 2$ с неизвестными a, b не имеет решения в целых числах, а это значит, что число 2 в кольце $\langle \{a + b\sqrt{-3} | a, b \in \mathbb{Z}\}; +, \cdot \rangle$ является простым.

Аналогично устанавливается, что и числа $1 \pm \sqrt{-3}$ тоже простые. Таким образом, произведения

$$2 \cdot 2 = (1 - \sqrt{-3}) \cdot (1 + \sqrt{-3})$$

действительно являются различными разложениями числа 4 на простые неассоциированные множители.

Точно таким же приемом устанавливается, что

$$(\langle \{a + b\sqrt{-7} \mid a, b \in \mathbb{Z}\}; +, \cdot \rangle)^* = \{1, -1\}$$

и, соответственно,

$$2 \cdot 2 \cdot 2 = (1 + \sqrt{-7}) \cdot (1 - \sqrt{-7}) —$$

это два существенно различных разложения числа 8 на простые множители.

5.5. Свойства колец

Уже был отмечен ряд свойств кольца целых чисел: там выполняются теорема о делении с остатком и основная теорема арифметики, каждая пара чисел имеет НОД и НОК.

Некоторая связь между этими свойствами проглядывается (например, существование наибольшего общего делителя и наименьшего общего кратного можно доказать, опираясь на теорему о делении с остатком, но можно и с помощью основной теоремы арифметики).

Однако пока мы не сможем уверенно сказать, следует ли из основной теоремы арифметики теорема о делении с остатком (или, наоборот, основная теорема действительно не является основной и из нее не следует теорема о делении с остатком).

Доказательства этих и других утверждений опирались на некоторые специфические свойства кольца \mathbb{Z} , например, на вполне упорядоченность его положительной части, дискретность порядка и т. п. Произвольное кольцо может быть и неупорядоченным вовсе, и недискретным.

В этой и последующих темах будет выяснена связь между перечисленными фактами. На самом деле, из теоремы о делении с остатком следует основная теорема арифметики, а обратное утверждение неверно, т. е. основная теорема *слабее* теоремы о делении с остатком.

Начнем обсуждение не с теорем, а с некоторого промежуточного места, связанного с понятием однопорядоченного идеала.

Оказывается, из теоремы о делении с остатком следует однопорядоченность идеалов (а обратное утверждение неверно), и из одно-

порожденности идеалов следует аналог основной теоремы арифметики (обратное снова неверно).

Таким образом, между двумя арифметическими теоремами расположено понятие кольца, в котором все идеалы однопороденные. Такое кольцо называется *кольцом главных идеалов*. Это значит, что для каждого идеала H кольца K существует элемент d из K такой, что $(d) = H$. Связь между главными идеалами и отношением делимости в кольце отмечалась и ранее, но для колец главных идеалов эта связь наиболее плодотворна.

В поле всего два идеала: нулевой и единичный — и оба главные. Так что поле является кольцом главных идеалов. Любое конечное целостное кольцо образует поле, поэтому все конечные целостные кольца — это кольца главных идеалов.

В кольце целых чисел каждая аддитивная подгруппа является идеалом, а поскольку в бесконечной циклической группе каждая подгруппа циклическая, кольцо целых чисел является кольцом главных идеалов.

Приведем пример кольца, содержащего неглавные идеалы. Рассмотрим множество $\mathbb{Z}[x]$ всех многочленов от одной переменной x с целыми коэффициентами. Обычные школьные операции сложения и умножения многочленов превращают $\mathbb{Z}[x]$ в кольцо. Множество I , состоящее из всех многочленов с четным свободным членом, образует идеал. Идеал I порождается элементами $x, 2$:

$$I = (x, 2) = (x) + (2).$$

Если бы идеал I был главным, то для некоторого многочлена $d(x)$

$$(d(x)) = (x, 2).$$

Отсюда, в частности, следует, что $d(x) \mid x$ и $d(x) \mid 2$.

Наибольший общий делитель $d(x)$ у многочленов x и 2 есть — это 1 (или -1). Однако этот делитель даже не содержится в идеале I , поэтому

$$(1) \neq (x, 2).$$

Следовательно, многочлена $d(x)$, порождающего идеал I , не существует, I — неглавный идеал.

Пример неглавного идеала оправдывает применение термина «идеал».

В данном случае «идеальный» — это антоним слова «материальный». Неглавный идеал ведет себя в точности как главный, т. е. как множество кратных некоторого элемента, но элемента этого на самом деле не существует, порождающий элемент *идеальный*.

В школьном курсе математики встречаются многочлены и от двух переменных с действительными коэффициентами. Множество

всех таких многочленов обозначим символом $R[x, y]$. С обычными школьными операциями сложения и умножения множество $R[x, y]$ образует кольцо. Подмножество, состоящее из многочленов с нулевым свободным членом, образует идеал I_1 , и идеал этот неглавный. Действительно, I_1 порождается элементами x, y :

$$I_1 = (x, y),$$

и состоит из всех многочленов с нулевым свободным членом. Снова есть многочлен, который делит оба порождающих элемента многочлена, но этот делитель не входит в идеал I_1 , и

$$(1) \neq (x, y).$$

Чуть позже мы увидим значение этого факта: из-за существования неглавного идеала следует, что деление с остатком в кольце $R[x, y]$ невозможно.

Пусть K — кольцо главных идеалов; обозначим символом $|$ отношение делимости в этом кольце, а символом \sim — соответствующую ему ассоциированность.

Из определения главного идеала получаем (для любых элементов a, b из K):

$$a | b \Leftrightarrow (a) \supset (b), \quad a \sim b \Leftrightarrow (a) = (b).$$

Таким образом, отношение делимости на фактор-множестве K/\sim изоморфно представляется отношением включения на множестве главных идеалов кольца K .

Рассмотрим решетку идеалов кольца главных идеалов. В любом кольце пересечение любого числа идеалов является идеалом. В кольце главных идеалов пересечение идеалов будет главным идеалом. Порождающий элемент пересечения идеалов $(a) \cap (b)$ является точной верхней гранью множества $\{a, b\}$ в смысле делимости, т. е. он наименьшее общее кратное элементов a и b . Наименьшее общее кратное обозначают символом $[a, b]$.

Таким образом, элемент $n = [a, b]$ — НОК элементов a, b , если:

- 1) $a | n$ и $b | n$;
- 2) если $a | x$ и $b | x$, то $n | x$.

Первое условие означает, что n — общее кратное; второе, что n — наименьшее (в смысле делимости) общее кратное.

Такого рода определение имеет существенный недостаток: не видно, почему такой объект должен существовать. На самом деле: наименьшее общее кратное для каждой пары элементов найдется далеко не в каждом кольце.

Однако в кольце главных идеалов любые два элемента обладают наименьшим общим кратным.

Дело в том, что пересечение двух идеалов является наибольшим идеалом, содержащимся в двух идеалах (a) и (b) одновременно, а элемент n , порождающий $(a) \cap (b)$, является наименьшим в смысле делимости, делящимся на a и b . Иначе говоря,

$$(n) = (a) \cap (b).$$

Число элементов, для которых существует НОК, может быть и больше двух. В пересечении может участвовать любое число идеалов, поэтому в кольце главных идеалов для любого множества элементов существует наименьшее общее кратное.

Точную нижнюю грань в смысле делимости множества $\{a, b\}$ называют наибольшим общим делителем элементов a и b . Наибольший общий делитель обозначают символом (a, b) .

Итак, элемент $d = (a, b)$ — наибольший общий делитель элементов a, b , если:

- 1) $d|a$ и $d|b$;
- 2) если $x|a$ и $x|b$, то $x|d$.

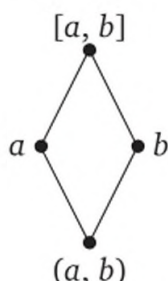
Как и в любом кольце, в кольце главных идеалов сумма двух идеалов $(a) + (b)$ снова является идеалом. Это наименьший идеал, содержащий идеалы (a) и (b) . В кольце главных идеалов все идеалы главные, поэтому и сумма идеалов снова будет главным идеалом. Пусть d — порождающий элемент главного идеала $(a) + (b)$, тогда

$$(d) = (a) + (b).$$

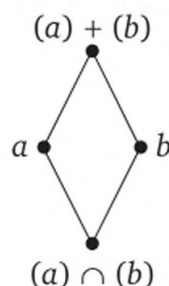
Другими словами, в кольце главных идеалов любые два элемента обладают наибольшим общим делителем.

Итак, в кольце главных идеалов пересечению идеалов соответствует НОК, а сумме — НОД.

Графы отношения делимости в K и отношения включения идеалов кольца K изоморфны (точнее, инверсно изоморфны: для совпадения картинок одну из них нужно повернуть на 180°).



Отношение делимости



Отношение включения

Число элементов, для которых найдется НОД, может быть любым — конечным или даже бесконечным.

Сумма любого числа идеалов в кольце главных идеалов будет главным идеалом. Более того, зная, как выглядят элементы из суммы идеалов, получаем дополнительно представление для НОД.

В кольце K главных идеалов для любого (может быть, и бесконечного) множества элементов S существует НОД d , причем найдутся такие элементы a_1, a_2, \dots, a_n из S и элементы u_1, u_2, \dots, u_n из K , что

$$d = a_1 u_1 + a_2 u_2 + \dots + a_n u_n.$$

Два элемента из кольца принято называть *взаимно простыми*, если у них нет общих делителей, кроме делителей единицы.

Если a, b — взаимно простые элементы в кольце главных идеалов K , то

$$au + bv = 1$$

для некоторых u, v из K . Если, наоборот, $au + bv = 1$, то любой общий делитель a, b является делителем единицы, а идеал $(a) + (b)$, как содержащий единицу, совпадает со всем кольцом K .

В кольце главных идеалов K два элемента a, b взаимно просты тогда и только тогда, когда найдутся такие элементы u, v из K , что

$$au + bv = 1.$$

В кольце главных идеалов K два элемента a, b взаимно просты тогда и только тогда, когда

$$(a) + (b) = K.$$

Ситуацию можно обобщить на идеалы произвольного кольца K : два идеала I_1 и I_2 взаимно просты, если $I_1 + I_2 = K$.

Кольцо K разлагается в прямое произведение своих идеалов A и B , если A и B взаимно просты и имеют нулевое пересечение.

Заметим, что существование НОД (и НОК) может опираться на другие факты.

Например, в кольце $\mathbb{Z}[x]$ многочленов с целыми коэффициентами есть неглавные идеалы, поэтому проведенные рассуждения для него не годятся. Однако каждые два многочлена с целочисленными коэффициентами все-таки обладают НОД и НОК.

В кольце $\mathbb{R}[x, y]$ тоже есть неглавные идеалы, но и там каждые два многочлена обладают НОД и НОК.

Из критерия взаимной простоты следует, в частности, что если $d = (a, b)$ тогда и только тогда, когда $a = a_1 d$, $b = b_1 d$, то $(a_1, b_1) = 1$. Тогда элемент $a_1 b_1 d$ является наименьшим общим кратным элементов a, b .

Отсюда следует, что в кольце главных идеалов НОД и НОК элементов a и b связаны соотношением

$$(a, b) \cdot [a, b] = ab.$$

С помощью этого равенства можно найти НОК, если НОД уже найден.

Обратим внимание на максимальные идеалы кольца. Мы уже видели, что идеал, порожденный простым элементом, может оказаться не максимальным. Но только не в кольце главных идеалов.

Если K — кольцо главных идеалов, то идеал I является максимальным в K тогда и только тогда, когда I порождается простым элементом.

Поскольку максимальность идеала непосредственно связана со свойством фактор-кольца «быть полем», получаем: *если K — кольцо главных идеалов, то фактор-кольцо K/I является полем тогда и только тогда, когда I порождается простым элементом.*

Рассмотрим возрастающую цепочку

$$I_1 \subset I_2 \subset I_3 \dots \subset I_i \subset \dots$$

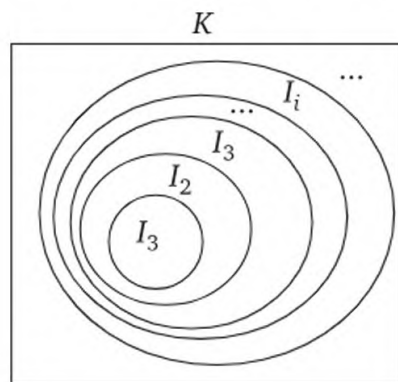
идеалов кольца K . Пусть I — объединение этой цепочки:

$$I = \bigcup_{n=1}^{\infty} I_n.$$

Если элементы x, y принадлежат I , то они оба лежат в некотором идеале. Но это значит, что объединение возрастающей цепочки идеалов само является идеалом.

В кольце главных идеалов все идеалы главные, поэтому будет главным и объединение возрастающей цепочки идеалов. Как только порождающий элемент этого главного идеала окажется в некотором звене цепочки, так цепочка и оборвется.

В кольце главных идеалов возрастающие цепочки идеалов обрываются на конечном шаге. Заметим, что однопорожденность идеалов для обрыва возрастающих цепочек вовсе не является необходимым условием. Для этого достаточно лишь конечной порожденности идеалов.



Цепь идеалов

Если в кольце K все идеалы конечно порождены, то все возрастающие цепочки идеалов обрываются на конечном шаге.

Действительно, объединение идеалов снова является идеалом, а конечная порожденность этого объединения означает, что как только в цепочке окажутся все порождающие этого объединения, так цепочка и оборвется (точнее, стабилизируется — все идеалы цепочки с некоторого места совпадают).

Условие конечной порожденности идеалов является и *необходимым* для обрыва возрастающей цепочки идеалов.

Идеал бесконечно порожден, если он наименьший идеал, содержащий некоторое бесконечное множество M , причем никаким конечным множеством множество M заменить нельзя. Если I — бесконечно порожденный идеал кольца K , то можно указать бесконечную строго возрастающую цепочку идеалов кольца K .

Итак, *все возрастающие цепочки идеалов кольца K обрываются на конечном шаге тогда и только тогда, когда все идеалы кольца K конечно порождены.*

Среди колец особое место занимают кольца многочленов $K[x]$ над данным кольцом. Что можно сказать о кольце $K[x]$, если K — кольцо главных идеалов?

Простое трансцендентное расширение $K[x]$ кольца K (оно же кольцо многочленов от одного переменного) сохраняет свойства целостности кольца. Кольцо многочленов $K[x]$ над целостным кольцом K само целостное.

Естественно, возникает вопрос: сохраняется ли при таком расширении свойство «быть кольцом главных идеалов»?

Ответ на этот вопрос отрицательный: нет, не сохраняется.

Соответствующий пример уже получен ранее: кольцо целых чисел \mathbb{Z} является кольцом главных идеалов, но в кольце многочленов $\mathbb{Z}[x]$ существуют неглавные идеалы.

Свойство «быть кольцом главных идеалов» при простом трансцендентном расширении кольца, вообще говоря, не сохраняется.

Слова «вообще говоря» здесь потому, что это свойство иногда может случайно и сохраниться.

Рассмотрим кольцо многочленов $\mathbf{R}[x]$ от одного переменного с действительными коэффициентами.

Пусть I — ненулевой идеал в кольце $\mathbf{R}[x]$ и $f(x)$ — ненулевой многочлен наименьшей степени, принадлежащий идеалу I .

Возьмем произвольный многочлен $g(x)$ из идеала I . По теореме о делении с остатком для многочленов найдутся такие многочлены $q(x)$ и $r(x)$ из $\mathbf{R}[x]$, что

$$g(x) = f(x) \cdot q(x) + r(x),$$

где $r(x)$ тождественно равен нулю или $\deg r(x) < \deg f(x)$.

Поскольку $r(x)$ принадлежит нашему идеалу I , ненулевым многочленом $r(x)$ быть не может. Следовательно, многочлен $g(x)$ делится на $f(x)$, а это значит, что в кольце многочленов $\mathbf{R}[x]$ над полем действительных чисел все идеалы главные.

Никаких особых свойств действительных чисел здесь не потребовалось: теорема о делении с остатком верна для кольца многочленов $P[x]$ над любым полем P .

В кольце многочленов $P[x]$ над полем P все идеалы главные.

Поле — это частный случай кольца главных идеалов. Таким образом, по крайней мере в одной серии частных случаев свойство однопорожденности (главности) идеалов сохраняется.

В кольце главных идеалов любая пара элементов имеет НОД и НОК.

Кольцо целых чисел обладает таким же свойством, но доказательство существования НОД и НОК обычно опирается не на свойства идеалов кольца \mathbf{Z} , а на *теорему о делении с остатком*.

Отметим, что из теоремы о делении с остатком как раз и следует однопорожденность всех идеалов кольца \mathbf{Z} .

Теорема о делении с остатком гарантирует, что для любых целых чисел a, b ($b \neq 0$) существуют такие целые числа q, r , что

$$a = bq + r, \text{ где } 0 \leq r < |b|.$$

Аналогичная теорема выполняется в кольце многочленов $P[x]$ с коэффициентами из поля P , только роль модуля числа играет степень многочлена.

В том и другом случае на основе теоремы о делении с остатком действует *алгоритм Евклида* для нахождения НОД, поэтому кольцо, в котором выполняется теорема о делении с остатком, называют *евклидовым кольцом*.

Дадим точное определение евклидова кольца.

Целостное кольцо K *евклидово*, если существует отображение $\varepsilon : K \setminus \{0\} \rightarrow \mathbf{Z}_0$, причем для любых a, b из K ($b \neq 0$) найдутся такие элементы q, r , что

$$a = bq + r,$$

где $r = 0$ или $\varepsilon(r) < \varepsilon(b)$.

В кольце целых чисел евклидовость реализуется отображением $\varepsilon : x \mapsto |x|$. Эта функция случайно определена на всем кольце \mathbf{Z} , включая и нуль, но так будет не для всех евклидовых колец.

В кольце многочленов с действительными (или рациональными, или из любого поля) коэффициентами деление с остатком тоже возможно. Функцией, реализующей евклидовость, в этом случае будет степень многочлена (уже не определенная для нулевого многочлена).

Каждое целостное кольцо вложимо в поле, наименьшее из таких полей, — это поле частных. Элементы поля частных евклидова кольца можно представить в виде суммы целой и дробной частей. Дробная часть (правильная дробь) над евклидовым кольцом — это элемент $\frac{a}{b}$, для которого $\varepsilon(a) < \varepsilon(b)$.

Формально можно говорить о правильных дробях и над неевклидовым кольцом, например над кольцом $\mathbf{Z}[x]$ или $\mathbf{R}[x, y]$, с помощью той же степени многочленов, но в этом случае далеко не каждый элемент из поля частных удастся представить в виде целой и дробной частей.

Поле частных кольца целых гауссовых чисел

$$\mathbf{Z}[i] = \langle \{a + bi \mid a, b \in \mathbf{Z}\}; +, \cdot \rangle$$

является поле гауссовых чисел

$$\mathbf{Z}(i) = \langle \{a + bi \mid a, b \in \mathbf{Q}\}; +, \cdot \rangle.$$

Действительно, частное от деления двух элементов из $\mathbf{Z}[i]$ принадлежит $\mathbf{Z}(i)$:

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i.$$

Поскольку $\mathbf{Z}(i)$ содержит \mathbf{Q} — поле частных кольца \mathbf{Z} , каждый элемент из $\mathbf{Z}(i)$ принадлежит полю частных кольца $\mathbf{Z}(i)$.

Покажем, что кольцо $\mathbf{Z}[i]$ целых гауссовых чисел евклидово, а функцией ε , реализующей евклидовость для этого кольца, является квадрат модуля комплексного числа:

$$\varepsilon(a + bi) = a^2 + b^2.$$

Пусть u и v — два целых гауссова числа, $v \neq 0$. Частное w_1 от деления u на v является гауссовым числом:

$$w_1 = \frac{u}{v} = \alpha + \beta i,$$

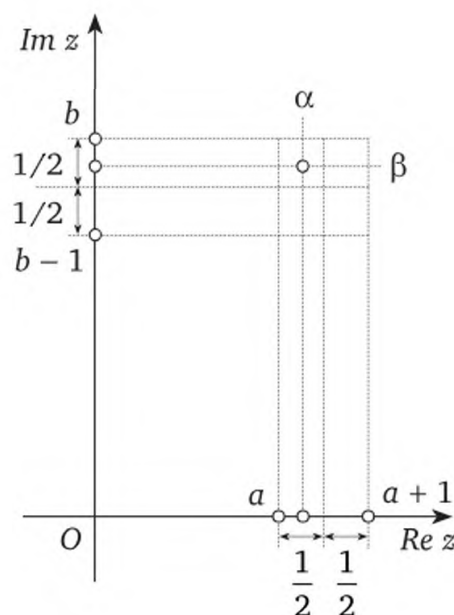
где α, β — рациональные числа. Если α, β оказались целыми, то деление состоялось нацело и остаток

$$r = u - wv$$

от деления u на v равен нулю. Если это не так, то возьмем ближайшие к α, β целые числа.

Например, на рисунке число $\alpha + \beta i$ расположено внутри полос,

$$a < \operatorname{Re} z < a + 1, \quad b - 1 < \operatorname{Im} z < b.$$



Деление с остатком в кольце $\mathbb{Z}[i]$

Пусть a — ближайшее целое число к α , а b — ближайшее целое число к β . Это значит, что в любом случае:

$$|a - \alpha| \leq \frac{1}{2} \text{ и } |b - \beta| \leq \frac{1}{2}.$$

Обозначим $w = a + bi$. Поскольку $u - w_1 v = 0$, запишем:

$$u - wv = u - w_1 v + (w_1 - w)u = (w_1 - w)u.$$

Отсюда следует, что

$$|u - wv|^2 = |(w_1 - w)u|^2 = |w_1 - w|^2 \cdot |u|^2 = |w_1 - w|^2 \cdot \varepsilon(u).$$

Оценим теперь квадрат модуля разности $w_1 - w$:

$$|w_1 - w|^2 = (a - \alpha)^2 + (b - \beta)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1.$$

Итак, если остаток от деления u на v

$$r = u - wv$$

отличен от нуля, то $\varepsilon(r) < \varepsilon(u)$.

Кольцо целых гауссовых чисел евклидово.

Аналогичным образом, используя тот же прием, можно показать, что из неравенства

$$\left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 < 1$$

следует евклидовость кольца, состоящего из чисел вида $a + b\sqrt{-2}$, где $a, b \in \mathbb{Z}$. Функция, реализующая евклидовость, в этом кольце та же самая — квадрат обычного модуля комплексного числа $a + b\sqrt{2}i$:

$$\varepsilon(a + b\sqrt{2}i) = a^2 + 2b^2.$$

Отметим, что для чисел $a + b\sqrt{-3}$ с целыми a, b этот «фокус» уже не даст результата. Впрочем, и никакой другой прием не удастся: кольцо $\langle \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}; +, \cdot \rangle$ неевклидово.

Нулевой идеал любого кольца является главным. Если H — ненулевой идеал евклидова кольца, то элемент d из H с наименьшим значением евклидовой функции является порождающим для H . Действительно, для любого элемента h из H найдутся такие q и r , что

$$h = dq + r,$$

где $r = 0$ или $\varepsilon(r) < \varepsilon(b)$. Поскольку остаток

$$r = h - dq$$

тоже принадлежит идеалу H , возможность этого «или» исключена: остаток может быть только нулевым. Итак, $r = 0$, следовательно, элемент d делит h . Идеал H главный.

Иначе говоря, в евклидовом кольце все идеалы главные (говорят еще: «евклидово кольцо является кольцом главных идеалов»).

Этот факт применяется, как правило, для получения отрицательных результатов, т. е. в следующей формулировке: кольцо, содержащее неглавный идеал, неевклидово.

Наличие неглавного идеала в $\mathbb{Z}[x]$ означает, что невозможно придумать схему деления для многочленов с целыми коэффициентами, аналогичную схеме деления уголком многочленов с действительными или рациональными коэффициентами. Нет такой схемы, да и не будет никогда. Процедуру деления многочленов иногда называют алгоритмом деления. Если нет самого деления, то нет и алгоритма.

В кольце многочленов от одного переменного с целыми коэффициентами невозможно определить алгоритм деления с остатком.

В школьном курсе математики появляются и многочлены от двух переменных, но деление с остатком в множестве $\mathbb{R}[x, y]$ не рассматривается.

Это не случайно. Существование неглавного идеала в $\mathbb{R}[x, y]$ означает, что схемы деления (с остатком) многочлена от двух переменных на другой многочлен от двух переменных, подобной схеме деления для многочленов от одной переменной, не существует.

В кольце многочленов от двух переменных с действительными коэффициентами невозможно определить алгоритм деления с остатком.

Евклидовы кольца обладают всеми свойствами колец главных идеалов. Более того, НОД в евклидовом кольце не просто всегда существует — его можно найти с помощью алгоритма Евклида (если в этом кольце есть алгоритмы для арифметических операций и вычисления функции, реализующей евклидовость).

Доказательства существования НОД и НОК в кольце главных идеалов, рассмотренные в предыдущем пункте темы, являются косвенными: они не дают никаких указаний, как практически найти эти элементы.

Существует, однако, и конструктивное доказательство этих фактов.

Все, что было ранее сказано о кольце целых чисел, почти без изменений переносится на произвольные евклидовы кольца. Обозначим тем же символом $\text{Rest}(x, y)$ остаток от деления элемента x на ненулевой элемент y (точнее, один из остатков, так как в определении евклидовости не требовалось единственность частного и остатка). Если a, b произвольные и оба ненулевые элементы из евклидова кольца, то

$$\begin{aligned} r_1 &= \text{Rest}(a, b); & 0 \leq f(r_1) < f(b), & (a, b) = (b, r_1); \\ r_2 &= \text{Rest}(b, r_1); & 0 \leq f(r_2) < f(r_1), & (b, r_1) = (r_1, r_2); \\ r_3 &= \text{Rest}(r_1, r_2); & 0 \leq f(r_3) < f(r_2), & (r_1, r_2) = (r_2, r_3); \\ & \dots\dots\dots \\ r_{i+1} &= \text{Rest}(r_{i-1}, r_i); & 0 \leq f(r_{i+1}) < f(r_i), & (r_{i-1}, r_i) = (r_i, r_{i+1}). \\ & \dots\dots\dots \end{aligned}$$

Снова появляется строго убывающая цепочка целых неотрицательных чисел:

$$f(b) > f(r_1) > f(r_2) > f(r_3) > \dots > f(r_i) > \dots \geq 0,$$

которая непременно оборвется через конечное число шагов.

В евклидовом кольце любая пара ненулевых элементов обладает наибольшим общим делителем и наименьшим общим кратным.

Наибольший общий делитель двух элементов из евклидова кольца равен последнему ненулевому остатку в алгоритме Евклида, примененному к этим элементам.

Если a, b — элементы евклидова кольца K и $d = (a, b)$, то в K существуют элементы u, v такие, что

$$au + bv = d,$$

причем элементы u, v можно найти с помощью неполных частных алгоритма Евклида.

Наименьшее общее кратное $[a, b]$ двух элементов a, b из евклидова кольца вычисляется по формуле

$$[a, b] = \frac{ab}{(a, b)}.$$

Таким образом, вычислив с помощью алгоритма Евклида НОД (a, b) , найдем и $[a, b]$.

Отметим также, что неслучайно множество максимальных идеалов и идеалов, порожденных простыми числами, в кольце \mathbb{Z} совпадают.

В евклидовом кольце K элемент p является простым тогда и только тогда, когда идеал (p) — максимальный в K .

Так называемая *основная теорема арифметики* обычно формулируется для натуральных чисел и означает, что каждое натуральное число, большее единицы, является произведением простых чисел, и такое представление единственно (с точностью до порядка множителей). Система натуральных чисел не является кольцом, поэтому для возможности переноса этого факта на произвольные кольца сформулируем основную теорему арифметики для кольца целых чисел.

Каждое целое число, отличное от 0, 1, -1, является простым или произведением простых чисел, причем представление в виде произведения простых единственно с точностью до порядка и ассоциированности множителей.

«С точностью до порядка и ассоциированности множителей» означает, что если какое-то число имеет два разложения

$$p_1 \cdot p_2 \cdot \dots \cdot p_n = q_1 \cdot q_2 \cdot \dots \cdot q_m$$

в виде произведения простых чисел p_i и q_j , то $n = m$ и при подходящем изменении нижних индексов множители p_i и q_j ассоциированы.

Например, число 12 можно представить в виде

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot (-3) \cdot (-2),$$

но эти два разложения отличаются лишь порядком простых множителей и их ассоциированностью.

Для перехода в произвольное целостное кольцо K заметим, что множество $\{1, -1\}$ — это мультипликативная группа \mathbb{Z}^* кольца \mathbb{Z} . Выполнимость основной теоремы в целостном кольце K означает, что для любого ненулевого и необратимого элемента a из целостного кольца K существует единственное с точностью до порядка множителей и ассоциированности множителей представление a в виде произведения простых элементов:

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_n.$$

Кольца, в которых выполняется основная теорема арифметики, называют *гауссовыми* (или *факториальными*). Термин «гауссово кольцо» предложил Р. Дедекин¹ в честь своего учителя Карла Фридриха Гаусса².

Кольцо целых чисел, кольцо многочленов с коэффициентами из поля — все это примеры гауссовых колец.

Примером негауссова кольца является, например, числовое кольцо

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}.$$

В этом кольце число 4 имеет два существенно различных представления:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3}).$$

Как в кольце целых чисел, так и в кольце многочленов от одного переменного с коэффициентами из поля выполняется теорема о делении с остатком, поэтому там все идеалы главные. В этом и кроется причина их гауссовости.

Покажем, что *каждое кольцо главных идеалов является гауссовым*.

Если элемент a из целостного кольца является составным, но не имеет представления в виде произведения простых элементов кольца, то можно указать цепочку неассоциированных элементов

$$a, a_1, a_2, a_3, \dots,$$

в которой каждый новый элемент делит предыдущий. Но тогда цепочка идеалов

$$(a) \subset (a_1) \subset (a_2) \subset (a_3) \subset \dots$$

неограниченно возрастает.

Напомним, что в кольце главных идеалов все возрастающие цепочки идеалов обрываются на конечном шаге. Следовательно, в кольце главных идеалов каждый составной элемент обладает представлением в виде произведения простых элементов.

Для гауссовости кольца этого мало; нужно еще, чтобы представление в виде произведения простых элементов было *единственным* (с точностью до ассоциированности и порядка множителей).

Если

$$p_1 \cdot p_2 \cdot \dots \cdot p_n = q_1 \cdot q_2 \cdot \dots \cdot q_m —$$

¹ Юлиус Вильгельм Рихард Дедекин (*Dedekind*; 1831—1916) — немецкий математик, известный работами по общей алгебре и основаниям действительных чисел.

² Карл Фридрих Гаусс (*Gauß*, 1777—1855) — немецкий математик, с 1807 г. — профессор Геттингенского университета и директор Геттингенской астрономической обсерватории.

два представления элемента в виде произведения простых элементов, то для доказательства единственности достаточно показать (например, индукцией по числу множителей в разложении), что хотя бы одно из q_i делится на p_1 . Для этого, естественно, надо начать с двух множителей, причем не обязательно простых.

Пусть элементы a и b из кольца главных идеалов взаимно просты, $(a, b) = 1$. По критерию взаимной простоты для некоторых u, v из нашего кольца $au + bv = 1$. Умножив левую и правую части этого равенства на элемент c из кольца, получаем следующее утверждение: *если a, b, c — элементы кольца главных идеалов, то*

$$a \mid bc, (a, b) = 1 \Rightarrow a \mid c.$$

В кольце целых чисел это утверждение называется *теоремой Евклида о делимости*.

Заметим, что в идеальной формулировке теорема Евклида о делимости принимает следующий вид: *если a, b, c — элементы из кольца K главных идеалов, то*

$$(a) \supset (bc), (a) + (b) = K \Rightarrow (a) \supset (c).$$

Поскольку простые элементы кольца либо ассоциированы, либо взаимно просты, из теоремы Евклида о делимости следует, что *если $q \mid p_1 p_2$, где q, p_1, p_2 — простые элементы, то элемент q ассоциирован с p_1 или с p_2* .

Теперь индукцией по числу множителей p_i получается утверждение: *если*

$$q \mid p_1 p_2 \dots p_n,$$

где q, p_i — простые элементы из кольца главных идеалов, то для некоторого i элементы q и p_i ассоциированы.

Для произвольного целостного кольца такое утверждение *неверно*.

Например, в кольце $\mathbb{Z}[\sqrt{-3}]$, состоящем из чисел вида $a + b\sqrt{-3}$, где a, b — целые числа, число

$$(1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$$

делится на 2, но ни один из этих множителей с двойкой не ассоциирован.

Назовем идеал I целостного кольца K *простым*, если фактор-кольцо K/I целостное. Поскольку гомоморфный образ ассоциативно-коммутативного кольца является ассоциативно-коммутативным, свойство простоты идеала связано лишь с появлением делителей нуля.

Идеал I целостного кольца K *прост*, если фактор-кольцо K/I без делителей нуля.

Элемент, отличный от нуля и делителя единицы, из целостного кольца называется простым, если он не имеет нетривиального разложения на множители. Фактор-кольцо по идеалу, порожденному простым элементом, может оказаться непростым.

Например, число 2 является простым элементом в кольце $\mathbb{Z}[\sqrt{-3}]$, но фактор-кольцо $\mathbb{Z}[\sqrt{-3}]/(2)$ содержит делители нуля:

$$\left[(2) + (1 + \sqrt{-3}) \right] \cdot \left[(2) + (1 - \sqrt{-3}) \right] = (2) + 4 = (2),$$

т. е. идеал (2) не простой в кольце $\mathbb{Z}[\sqrt{-3}]/(2)$.

Однако в любом целостном кольце идеал, порожденный составным элементом, не прост. Действительно, если $p = ab$ — нетривиальное разложение элемента из кольца K на множители, то $I + a$ и $I + b$ — делители нуля в кольце K/I :

$$(I + a)(I + b) = I + ab = I + p = I,$$

и идеал (p) не прост.

Непростой идеал, порожденный простым элементом, был указан в кольце с неоднозначным разложением на множители. Это неслучайно. В гауссовом кольце¹ понятия «простой элемент» и «простой идеал» имеют естественную связь.

Если в кольце K каждый элемент, отличный от нулевого и делителя нуля, имеет не более одного представления в виде произведения простых множителей, то для каждого p из K идеал (p) простой тогда и только тогда, когда элемент p простой. В одну сторону утверждение уже доказано, причем для произвольного целостного кольца.

Предположим, что в кольце K каждый составной элемент имеет не более одного разложения, а p — простой элемент в кольце K . Пусть I — идеал, порожденный элементом p , и в фактор-кольце K/I есть делители нуля. Пусть это будут элементы $I + a$ и $I + b$:

$$(I + a)(I + b) = I + ab = I.$$

Это значит, что $ab \in (p)$ и, следовательно, $p \mid ab$. Из однозначной разложимости составного элемента следует, что $p \mid a$ или $p \mid b$, поэтому $I + a = I$ или $I + b = I$.

Предположим, что в целостном кольце K каждый простой элемент p порождает простой идеал. Это означает, что из равенства

$$[(p) + a] \cdot [(p) + b] = (p) + ab = (p)$$

следует, что $(p) + a = (p)$ или $(p) + b = (p)$.

¹ И даже в кольце, в котором для каждого элемента существует не более одного представления в виде произведения простых.

То же самое на языке деления означает: если $p \mid ab$, то $p \mid a$ или $p \mid b$.

Последнее предложение — это следствие из теоремы Евклида о делимости. Из этого следствия уже получается единственность представления составного элемента в виде произведения простых.

Таким образом, если в целостном кольце каждый простой элемент порождает простой идеал, то каждый составной элемент имеет не более одного представления в виде произведения простых элементов.

Возвратимся вновь к кольцам главных идеалов.

Индукцией по числу простых множителей в разложении элемента их кольца главных идеалов получаем утверждение о единственности разложения, а вместе с существованием и следующее предложение: *кольцо главных идеалов является гауссовым.*

Евклидово кольцо является кольцом главных идеалов, а это значит, что и *евклидово кольцо является гауссовым.*

Эти два факта можно записать иначе: если в кольце K есть элементы с неоднозначным разложением на простые множители, то K содержит неглавные идеалы. Или, другими словами, кольцо с неоднозначным разложением на простые множители не является евклидовым: если нет однозначного разложения на простые множители, то нет и теоремы о делении с остатком. Естественно, что если нет теоремы о делении, то нет и алгоритма деления.

Если в кольце K есть элементы с неоднозначным разложением на простые множители, то в K нельзя определить алгоритм деления с остатком.

Поскольку евклидово кольцо является кольцом главных идеалов, а то, в свою очередь, гауссовым, получаем: в кольце целых гауссовых чисел все идеалы главные, и кольцо целых гауссовых чисел является гауссовым.

Заметим, что в отличие от целых чисел, где все подкольца являются идеалами, в кольце $\mathbb{Z}[i]$ ситуация существенно иная — каждое ненулевое подкольцо, порожденное элементом a , не совпадает с главным идеалом (a) .

Алгоритм деления в кольце целых гауссовых чисел можно без изменений (с той же самой функцией — квадрат модуля, реализующий евклидовость) перенести на кольцо $\mathbb{Z}[\sqrt{-2}]$, состоящее из чисел вида $a + b\sqrt{-2}$, где a, b — целые.

В числовом кольце $\mathbb{Z}[\sqrt{-2}]$ можно определить деление с остатком. Поэтому все идеалы в кольце $\mathbb{Z}[\sqrt{-2}]$ главные, а каждый элемент из $\mathbb{Z}[\sqrt{-2}] \setminus (1, -1, 0)$ можно представить, и единственным образом (с точностью до порядка и ассоциированности сомножителей), в виде произведения простых элементов этого кольца.

Еще раз обратим внимание на связь между максимальными идеалами и идеалами, порожденными простыми элементами.

В гауссовом кольце, не являющемся кольцом главных идеалов, идеал, порожденный простым элементом, не обязательно является максимальным. Например, фактор-кольцо

$$\frac{\mathbb{Z}[x]}{(x^2 + 1)}$$

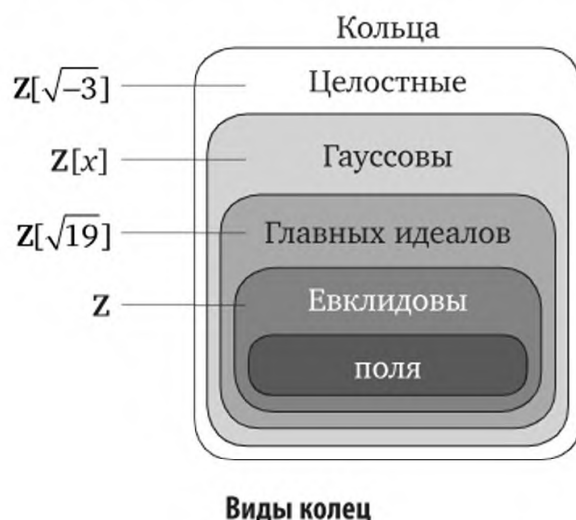
кольца многочленов с целыми коэффициентами по идеалу, порожденному простым элементом — многочленом $x^2 + 1$, изоморфно кольцу целых гауссовых чисел, которое не является полем, поэтому идеал $(x^2 + 1)$ не максимальный в $\mathbb{Z}[x]$.

Ранее уже появился пример того, что в негауссовом кольце простой элемент может порождать непростой идеал.

Если целостное кольцо K не является гауссовым, то фактор-кольцо $K/(p)$ по идеалу, порожденному простым элементом p , может оказаться нецелостным.

Отметим, что основная теорема арифметики — это следствие теоремы о делении с остатком. Существование гауссовых, но не евклидовых колец означает, что основная теорема *слабее* теоремы о делении с остатком.

Связь между различными видами колец изображена на схеме.



Каждое новое множество колец является *собственным* подмножеством предыдущего.

Существуют нецелостные кольца. Нарушения целостности могут быть различными. Например, кольцо матриц некоммутативно, а с наличием делителей нуля получается двойное нарушение. Кольцо классов вычетов \mathbb{Z}_m по составному модулю m ассоциативное и коммутативное, но с делителями нуля. Тело кватернионов ассоциативное и без делителей нуля, но некоммутативное. И матричное кольцо, и кольцо \mathbb{Z}_m , где m составное, и кольцо кватернионов — все это примеры нецелостных колец. По традиции не считается целостным и кольцо, состоящее из одного нуля, — нулевое кольцо.

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$$

является числовым, следовательно, целостным. Однако в кольце $\mathbb{Z}[\sqrt{-3}]$ есть числа с неоднозначным разложением на простые множители, поэтому оно негауссово.

Кольцо $\mathbb{Z}[x]$ гауссово, но в нем есть неглавные идеалы.

Числовое кольцо $\mathbb{Z}[\sqrt{19}] = \{a + b\sqrt{19} \mid a, b \in \mathbb{Z}\}$ образует кольцо главных идеалов, но не является евклидовым¹.

Кольцо \mathbb{Z} целых чисел, кольцо целых гауссовых чисел $\mathbb{Z}[i]$, числовое кольцо $\{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$, $+$ \cdot — все это примеры евклидовых колец, не являющихся полями.

Для существования НОД и НОК вовсе не обязательна теорема о делении с остатком. Алгоритм Евклида или однопорожденность идеалов — это лишь достаточные, но не необходимые условия.

Собрав в степени одинаковые простые множители в представлении элемента из гауссова кольца K , мы получим представление элемента a из $K \setminus (\{0\} \cup K^*)$ в канонической форме

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n},$$

где α_i — целые положительные числа.

Такая каноническая форма единственна (с точностью до ассоциированности и порядка множителей). Благодаря единственности канонической формы любой делитель элемента a в гауссовом кольце имеет вид

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n},$$

где $0 \leq \beta_i \leq \alpha_i$, $i = 1, 2, \dots, n$.

Такую форму элемента, в которой участвуют и нулевые показатели степеней, принято называть *полуканонической*.

Используя полуканоническую форму, можно любые два ненулевых элемента гауссова кольца записать с одним и тем же набором простых множителей:

$$\begin{aligned} a &= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}; \\ b &= p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n}, \end{aligned}$$

где $0 \leq \beta_i$, $0 \leq \alpha_i$, $i = 1, 2, \dots, n$.

Тогда

$$\begin{aligned} (a, b) &= p_1^{\min\{\alpha_1, \beta_1\}} \cdot p_2^{\min\{\alpha_2, \beta_2\}} \cdot \dots \cdot p_n^{\min\{\alpha_n, \beta_n\}}; \\ [a, b] &= p_1^{\max\{\alpha_1, \beta_1\}} \cdot p_2^{\max\{\alpha_2, \beta_2\}} \cdot \dots \cdot p_n^{\max\{\alpha_n, \beta_n\}}. \end{aligned}$$

¹ Впервые это заметил в 1949 г. израильско-американский математик Теодор Сэмюэль Моцкин (Motzkin, 1908—1970).

Эти формулы аналогичны школьным формулам для нахождения НОД и НОК целых чисел.

Заметив, что для любых целых чисел

$$\max\{\alpha, \beta\} + \min\{\alpha, \beta\} = \alpha + \beta,$$

получаем, что в гауссовом кольце любые два элемента a, b имеют наибольший общий делитель (a, b) и наименьшее общее кратное $[a, b]$, причем

$$(a, b)[a, b] = ab.$$

Число элементов, для которых разыскивается (a, b) и $[a, b]$, может быть и больше двух. Кроме того, если в гауссовом кольце пара элементов порождает неглавный идеал, то НОД (a, b) не принадлежит идеалу, порожденному элементами a, b . Но тогда (a, b) не будет иметь и линейного представления, которое всегда есть в кольце главных идеалов.

Таким образом, в гауссовом кольце K для любого конечного множества элементов S существует НОД d , однако не для каждого элемента a, b найдутся такие элементы u, v из K , что

$$d = au + bv.$$

Пока без доказательства отметим, что кольца многочленов $\mathbf{Z}[x]$ и $\mathbf{R}[x, y]$, указанные ранее в качестве примера колец с неглавными идеалами, являются гауссовыми.

Для существования разложения составного элемента в произведение простых необходимо и достаточно, чтобы возрастающая цепочка главных идеалов обрывалась на конечном шаге.

Что же означает *единственность* разложения на языке идеалов?

Заметим сначала, что если p — простой элемент кольца K , то, по определению, между идеалами (p) и K нет промежуточных главных идеалов.

Пусть a — элемент кольца K — является произведением двух простых элементов, $a = p_1 p_2$, и (x) — промежуточный главный идеал между идеалами (a) и (p_2) , т. е.

$$(a) \subset (x) \subset (p_2).$$

Тогда $x|a$ и $p_2|x$, что означает:

$$a = xk = (p_2 m)k = p_1 p_2.$$

По закону сокращения, $mk = p_1$. Поскольку p_1 — простой элемент, то либо m , либо k является делителем единицы. Если k — делитель единицы, то $(x) = (a)$. Если m — делитель единицы, то $(x) = (p_2)$. Это

значит, что (x) — ненастоящий промежуточный идеал или, иначе говоря, между идеалами (a) и (p_2) промежуточных идеалов нет.

Итак, если $a = p_1 p_2$ — разложение элемента в простые, то цепочка главных идеалов

$$(a) \subset (p_2) \subset K$$

плотная, в ней нельзя разместить промежуточные идеалы. Конечно, таким же свойством обладает и цепочка

$$(a) \subset (p_1) \subset K.$$

В общем виде ситуация та же. Если $a = p_1 p_2 \dots p_n$ — представление элемента в виде произведения простых элементов, то цепочка главных идеалов

$$(a) \subset (p_2 \cdot \dots \cdot p_n) \subset (p_3 \cdot \dots \cdot p_n) \subset \dots \subset (p_n) \subset K$$

плотная: в нее нельзя вставить ни одного промежуточного главного идеала. В этой цепочке каждый идеал, кроме K , является максимальным главным идеалом в следующем.

Таким образом, существование представления составного элемента a в виде произведения простых равносильно существованию плотной цепочки главных идеалов, идущей от идеала, порожденного элементом a , до всего кольца K .

Поясним единственность представления поучительным примером.

Пусть $K = \mathbb{Z}$ — кольцо целых чисел, $a = 6 = 2 \cdot 3 = 3 \cdot 2$, и, соответственно, возникают две плотные цепочки идеалов:

$$6\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z};$$

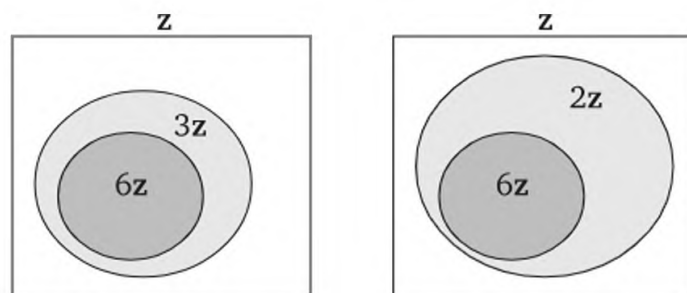
$$6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}.$$

Поскольку цепочка состоит из идеалов, можно рассмотреть фактор-кольца:

$$2\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \text{ и } \mathbb{Z}/3\mathbb{Z}, 3\mathbb{Z}/6\mathbb{Z}.$$

Фактор-кольцо $2\mathbb{Z}/6\mathbb{Z}$ изоморфно кольцу классов вычетов \mathbb{Z}_3 , т. е. кольцу $\mathbb{Z}/3\mathbb{Z}$, а фактор-кольцо $3\mathbb{Z}/6\mathbb{Z}$ изоморфно кольцу $\mathbb{Z}/2\mathbb{Z}$. Таким образом, хотя цепочки эти различны, но они имеют одну и ту же длину и определяют одно и то же множество фактор-колец.

Две плотные цепочки с одинаковыми фактор-кольцами называются изоморфными. Для целых чисел единственность представления составного числа $a > 1$ в виде произведения простых означает, что все плотные цепочки главных идеалов, соединяющих главный идеал (a) и кольцо \mathbb{Z} , изоморфны.



Плотные цепочки

Никаких особых свойств целых чисел для такого заключения не требуется. Это значит, что целостное кольцо K является гауссовым тогда и только тогда, когда для каждого ненулевого элемента a из $K \setminus K^*$ между идеалом (a) и кольцом K существует плотная цепочка главных идеалов и все такие цепочки изоморфны.

Конечно, такой критерий носит чисто теоретический характер и более интересен не для того, чтобы узнать, гауссово кольцо или нет, а наоборот, какими интересными свойствами гауссово кольцо обладает.

Ранее уже появлялись необходимые и достаточные условия и существования разложения, и его единственности. Соберем эти условия вместе.

Целостное кольцо K является гауссовым тогда и только тогда, когда все возрастающие цепочки главных идеалов в K обрываются; каждый идеал в K , порожденный простым элементом, является простым.

Первое условие гарантирует существование представления составного элемента в виде произведения простых, а второе — единственность такого разложения.

При простом трансцендентном расширении кольца K , т. е. при переходе к кольцу многочленов $K[x]$ из рассмотренных свойств колец (целостность, евклидовость, однопорожденность идеалов), всегда сохраняется только целостность. Два других свойства, вообще говоря, не сохраняются.

Есть, однако, важный частный случай простого трансцендентного расширения кольца K , когда сохраняются все три кольцевых свойства. Этот счастливый случай возникает тогда, когда K — поле.

Контрольные задания

1. Докажите, что кольцо K является прямым произведением своих подколец A и B тогда и только тогда, когда пересечение подколец A и B состоит из одного нуля, множество совпадает со всем K и для каждого a из A и каждого b из B произведение ab равно нулю.

2. Докажите, что в кольце главных идеалов любые два элемента обладают наименьшим общим кратным.

3. Докажите, что в гауссовом кольце K для любого конечного множества элементов S существует наибольший общий делитель d , однако, не для любых элементов a, b найдутся такие элементы u, v из K , что $d = au + bv$.
4. Докажите, что в гауссовом кольце, не являющемся кольцом главных идеалов, идеал, порожденный простым элементом, не обязательно является максимальным.
5. Докажите, что в евклидовом кольце K элемент p является простым тогда и только тогда, когда идеал (p) — максимальный в K .
6. Докажите, что в евклидовом кольце все идеалы главные.
7. Докажите, что кольцо целых чисел неразложимо в прямое произведение.
8. Докажите, что любое поле неразложимо в прямое произведение.
9. Докажите, что существуют неизоморфные кольца с ненулевым умножением, состоящие из четырех элементов.
10. Докажите, что множество конечных десятичных дробей образует кольцо.

Тема 6

МНОГОЧЛЕНЫ

Основные понятия: многочлен, корень, сопряженность, автоморфизм, приводимые и неприводимые многочлены, гауссовость, кратные неприводимые множители и кратные корни, производная многочлена, границы корней многочлена, формулы Виета, система многочленов Штурма. гауссовость, нетеровость, действие подстановки на многочлен от нескольких переменных, словарное упорядочение, высший член, основные симметрические многочлены.

Основные факты: при простом трансцендентном расширении кольца сохраняются целостность, нетеровость и гауссовость, и, вообще говоря, не сохраняются евклидовость и одно-порожденность идеалов; поле комплексных чисел алгебраически замкнуто, подкольцо симметрических многочленов порождается основными симметрическими многочленами. задача разложения многочлена с рациональными коэффициентами на неприводимые множители алгоритмически разрешима, задача отделения действительных корней многочлена с действительными коэффициентами алгоритмически разрешима.

На простое трансцендентное расширение $K[x]$ кольца K можно смотреть как на теоретико-кольцевую операцию: каждому кольцу K ставится в соответствие однозначно определенное (с точностью до изоморфизма) кольцо $K[x]$, оно же кольцо многочленов над K . В предыдущих темах уже было показано, что простое трансцендентное расширение существует для любого кольца.

Кольцо коэффициентов K может обладать различными свойствами. Оно может быть целостным, гауссовым, кольцом главных идеалов и т. п.

Какие кольцевые свойства сохраняются при простом трансцендентном расширении?

6.1. Многочлены над целостными кольцами

Заметим сначала, что если кольцо K ассоциативно, то его простое трансцендентное расширение $K[x]$ тоже ассоциативно.

Если кольцо K коммутативно, то его простое трансцендентное расширение $K[x]$ тоже коммутативно.

Если кольцо K с единицей, то его простое трансцендентное расширение $K[x]$ тоже с единицей.

Для целостного кольца коэффициентов неравенство

$$\deg(f(x) \cdot g(x)) \leq \deg f(x) + \deg g(x)$$

превращается в точное равенство

$$\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x).$$

Но это означает, в частности, что произведение многочленов со степенями снова является остепененным многочленом.

Иначе говоря, если кольцо K без делителей нуля, то его простое трансцендентное расширение $K[x]$ тоже без делителей нуля.

Напомним, что ассоциативно-коммутативное кольцо без делителей нуля называется целостным кольцом.

Собирая все проведенные наблюдения вместе, получаем: *простое трансцендентное расширение целостного кольца является целостным кольцом.*

Итак, целостность кольца при простом трансцендентном расширении кольца сохраняется. Что же можно сказать о сохранении других свойств целостных колец: евклидовости, однопорожденности (или конечной порожденности) идеалов, гауссовости?

В евклидовом кольце каждый идеал является главным. Указав хотя бы один неглавный идеал, мы тем самым устанавливаем, что функции ϵ , реализующей евклидовость, не существует.

Пример такого кольца и такого идеала уже был указан, а именно идеал, порожденный элементами x и 2 , в кольце многочленов с целыми коэффициентами неглавный.

Кольцо \mathbb{Z} — кольцо главных идеалов, а в $\mathbb{Z}[x]$ существуют неглавные идеалы. Следовательно, свойство «быть кольцом главных идеалов» при простом трансцендентном расширении кольца, вообще говоря, не сохраняется.

Кольцо, в котором найдутся неглавные идеалы, неевклидово.

Кольцо $\mathbb{Z}[x]$ многочленов с целыми коэффициентами не является евклидовым.

Этот пример означает, что *простое трансцендентное расширение евклидова кольца не обязательно является евклидовым кольцом.*

Или, другими словами, евклидовость при переходе от кольца K к его простому трансцендентному расширению $K[x]$, вообще говоря, не сохраняется.

Аналогично *простое трансцендентное расширение кольца главных идеалов не обязательно является кольцом главных идеалов.*

Оказалось, что теорема о делении с остатком, даже если она и имела место в кольце коэффициентов, не обязательно будет выполняться в кольце многочленов.

Тем интереснее будут частные случаи, когда она все-таки выполняется.

Многочлен называется *нормированным*, если коэффициент его старшего члена равен единице (напомним, что в ненулевом кольце единица и нуль не совпадают, поэтому, в частности, нормированный многочлен не является нулевым).

Если K — произвольное целостное (не обязательно евклидово) кольцо, а делитель является нормированным многочленом, то теорема о делении с остатком выполняется. Евклидовой функцией можно считать степень многочлена.

Если

$$\begin{aligned}f(x) &= a_0x^n + a_1x^{n-1} + \dots + a_n, \\g(x) &= x^m + b_0x^{m-1} + \dots + b_m,\end{aligned}$$

где $a \neq 0$ и $n \geq m$, то

$$\deg(f(x) - g(x) \cdot a_0x^{n-m}) < \deg f(x)$$

и, таким образом, индукцией по степени делимого получается следующее утверждение: для любого многочлена $f(x)$ и нормированного $g(x)$ с коэффициентами из целостного кольца K существуют многочлены $q(x)$ и $r(x)$ из $K[x]$ такие, что

$$f(x) = g(x) \cdot q(x) + r(x),$$

где $r(x) = 0$ или $\deg r(x) < \deg g(x)$.

Доказательство этого утверждения методом математической индукции, а именно индукцией по степени многочлена $f(x)$, фактически воспроизводит известную из школьного курса схему деления уголком:

$$\begin{array}{r|l} f(x) & g(x) \\ \vdots & q(x) \\ \hline r(x) & \end{array}$$

В частности, в кольце многочленов над произвольным целостным кольцом можно произвести деление с остатком любого многочлена на нормированный многочлен $x - \alpha$ *первой степени*.

В этом случае нет необходимости оформлять деление уголком. Как коэффициенты частного, так и остаток можно получить с помощью простых *рекуррентных* формул.

Раскрыв скобки в правой части тождества

$$\begin{aligned}& a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = \\&= (x - \alpha)(b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-2}x + b_{n-1}) + r,\end{aligned}$$

а затем, приведя подобные члены и приравняв коэффициенты у одинаковых степеней переменного, получаем:

$$\begin{aligned} b_0 &= a_0; \\ 12b_i &= \alpha \cdot b_{i-1} + a_i \quad (\text{для } i = 1, 2, \dots, n-1); \\ 12r &= \alpha \cdot b_{n-1} + a_n. \end{aligned}$$

Эти формулы называют схемой Горнера¹.

Вычисления по схеме Горнера обычно выполняют в виде таблицы.

	a_0	a_1	...	a_{i-1}	a_i	...	a_n
α	b_0	$\alpha \cdot b_0 + a_1$...	b_{i-1}	$\alpha \cdot b_{i-1} + a_i$...	$\alpha \cdot b_{n-1} + a_n$

В верхней строке этой таблицы расположены коэффициенты делимого $f(x)$. О делителе $(x - \alpha)$ в схеме напоминает символ α , стоящий возле начала второй строки.

В первых n клетках второй строки находятся коэффициенты частного $q(x)$ от деления $f(x)$ на $(x - \alpha)$. В последней клетке второй строки расположен остаток от деления $f(x)$ на $(x - \alpha)$.

Многочлен $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ может быть разложен по степеням линейного двучлена $(x - \alpha)$:

$$12f(x) = b_0(x - \alpha)^n + b_1(x - \alpha)^{n-1} + \dots + b_{n-1}(x - \alpha) + b_n.$$

Остаток от деления $f(x)$ на $(x - \alpha)$ равен b_n . Если частное от этого деления разделить снова на $(x - \alpha)$, то получим b_{n-1} . Новое частное снова разделим на $(x - \alpha)$, в результате получится b_{n-2} .

Продолжим и далее эти деления промежуточных частных, в результате найдем все коэффициенты разложения многочлена по степеням $(x - \alpha)$.

Эти вычисления оформляют обычно в виде треугольной таблицы.

	a_0	a_1	...	a_i	...	a_{n-2}	a_{n-1}	a_n
α	a_0	...						b_n
α	a_0	...					b_{n-1}	
α	a_0	...				b_{n-2}		
α	a_0			
...								
α	a_0	b_1						
α	b_0							

¹ Вильямс Джордж Горнер (Horner, 1768—1837) — английский математик-алгебраист. Вместе со схемой деления многочлена на линейный нормированный многочлен опубликовал в 1819 г. и способ приближенного вычисления действительных корней многочлена (известный, впрочем, еще китайцам в XII в.).

Разложение многочлена по степеням $(x - \alpha)$ можно получить и другим способом.

Определим сначала формальную производную $f'(x)$ многочлена

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

по правилу

$$f'(x) \stackrel{\text{опр}}{=} a_0 \cdot n \cdot x^{n-1} + a_1 \cdot (n-1) \cdot x^{n-2} + \dots + a_{n-2} \cdot 2 \cdot x + a_{n-1}.$$

Кольцо, над которым определяется производная, — произвольное целостное (если его характеристика нулевая, то все свойства производной, известной из анализа, переносятся буквально без изменений). В случае положительной характеристики придется учитывать, что если степень n одночлена x^n кратна этой характеристике, то производная этого одночлена равна нулю.

В любом случае производная будет обладать обычными свойствами производной:

$$\begin{aligned}(f(x) + g(x))' &= f'(x) + g'(x), \\ (f(x) \cdot g(x))' &= f'(x) \cdot g(x) + f(x) \cdot g'(x).\end{aligned}$$

В частности,

$$(k(x - \alpha)^m)' = km(x - \alpha)^{m-1}.$$

Используя эти тождества, последовательно вычислим производные многочлена, разложенного по степеням $(x - \alpha)$:

$$\begin{aligned}f(x) &= b_0 n(x - \alpha)^{n-1} + b_1 (n-1)(x - \alpha)^{n-2} + \dots + b_{n-1}; \\ f''(x) &= b_0 n(n-1)(x - \alpha)^{n-2} + b_1 (n-1)(n-2)(x - \alpha)^{n-3} + \dots + 2b_{n-2}; \\ &\dots \dots \dots \\ f^{(n)}(x) &= b_0 \cdot n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1.\end{aligned}$$

Подставив в каждую из производных элемент α вместо x , получим равенства

$$\begin{aligned}f'(\alpha) &= b_{n-1}; \\ f''(\alpha) &= 2b_{n-2}; \\ &\dots \dots \dots \\ f^{(i)}(\alpha) &= 2 \cdot 3 \cdot \dots \cdot i \cdot b_{n-i} = i! \cdot b_{n-i}; \\ &\dots \dots \dots \\ f^{(n)}(\alpha) &= n! \cdot b_0.\end{aligned}$$

Из этих равенств можно выразить коэффициенты b_j разложения многочлена $f(x)$ по степеням $(x - \alpha)$, и, таким образом:

$$f(x) = \sum_{i=0}^n \frac{f^{(i)}(a)}{i!} (x-a)^i.$$

Полученная формула является частным случаем ряда Тейлора¹ разложения функции в степенной ряд.

Еще раз особо отметим, что кольцо коэффициентов целостное, но не обязательно поле. Например, если K — кольцо многочленов от переменного y , то в $K[x]$ деление на нормированный многочлен всегда выполнимо. Если же делитель является нормированным многочленом первой степени, то деление можно осуществить с помощью схемы Горнера.

Разделим, например, по схеме Горнера многочлен $x^3 - y^3$ на $x - y$:

	1	0	0	$-y^3$
y	1	y	y^2	0

Получили разложение многочлена $x^3 - y^3$ на множители:

$$x^3 - y^3 = (x - y)(x^2 + yx + y^2) + 0.$$

Результат выполненного деления был известен заранее (это формула, известная школьникам средних классов).

Выполним еще одно деление с остатком, но уже с неизвестным заранее результатом. Разделим с помощью схемы Горнера многочлен $F(x)$ на $G(x)$:

$$F(x) = x^3 + y^3 + z^3 + 3xyz;$$

$$G(x) = x + y + z.$$

Здесь коэффициентами многочленов $F(x)$ и $G(x)$ являются многочлены от переменных y, z :

	1	0	$3yz$	$y^3 + z^3$
$-y - z$	1	$-y - z$	$(y + z)^2 + 3yz$	0

Остаток при делении оказался равным нулю, т. е. $G(x) \mid F(x)$:

$$(x^3 + y^3 + z^3 + 3xyz) = (x + y + z)[x^2 + (-y - z)x + (y + z)^2 + 3yz].$$

Вернемся от примеров к общим соображениям. Схему Горнера можно было записать развернуто в следующем виде:

¹ Брук Тейлор (Taylor, 1685—1731) — английский математик и философ, член Лондонского королевского общества (с 1712 г.) и его ученый секретарь (с 1714 г.). Разложение функции в степенной ряд Тейлор опубликовал в 1715 г. (нашел в 1712 г.).

	a_0	a_1	a_2	\dots	a_i	\dots	a_n
α		αb_0	αb_1	\dots	αb_{i-1}	\dots	
	b_0	$\alpha b_0 + a_1$	$\alpha b_1 + a_2$		$\alpha b_{i-1} + a_i$		$\alpha b_{n-1} + a_n$

Такая развернутая схема содержит промежуточные вычисления (и в случае необходимости легче найти ошибку в вычислениях).

Важнее, однако, то, что схему в таком виде легко обобщить на случай произвольного нормированного многочлена (впрочем, и ненормированного тоже, только тогда коэффициенты многочленов должны быть взяты из поля).

Такую обобщенную схему деления многочленов называют *схемой Яковкина*¹.

Для нахождения частного от деления многочлена

$$a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

на многочлен

$$x^m + b_1x^{m-1} + \dots + b_{m-1}x + b_m$$

по схеме Яковкина коэффициенты многочленов располагают в прямоугольной таблице следующим образом.

В верхней строке располагаются коэффициенты делимого (*f*-строка), а в первом столбце — коэффициенты делителя, начиная со второго, взятые с противоположными знаками (*g*-столбец).

Сама таблица заполняется сверху вниз и слева направо, подобно развернутой схеме Горнера.

Результаты (частное и остаток) появятся в самой нижней строке таблицы Яковкина.

$f \backslash g$	a_0	a_1	\dots	a_{n-1}	a_n
$-b_1$					
\dots					
$-b_{m-1}$					
$-b_m$					
	$q(x)$				$r(x)$

¹ Михаил Владимирович Яковкин — русский математик. Схема, обобщающая схему Горнера, опубликована им в 1954 г.

Сначала в самую нижнюю строку просто переносится a_0 . Старший коэффициент частного c_0 равен a_0 . Затем умножаем элементы g -столбца на c_0 и записываем эти произведения внутри таблицы под a_1, a_2, \dots, a_n .

Складываем все элементы a_1 -столбца и получаем следующий коэффициент частного — число c_1 .

Теперь умножаем элементы g -столбца на c_1 и записываем эти произведения внутри таблицы под элементами a_2, a_3, \dots, a_n .

Складываем все элементы a_2 -столбца и получаем следующий коэффициент частного — c_2 . Продолжаем далее до тех пор, пока новая строка произведений на c_m элементов столбца не достигнет своим последним элементом правого края таблицы. Сложив элементы в последних столбцах, получим коэффициенты остатка.

Рассмотрим небольшой числовой пример, иллюстрирующий схему Яковкина.

Разделим многочлен

$$f(x) = 2x^5 + 3x^4 + 4x^3 - 5x^2 + 6x + 7$$

на многочлен

$$g(x) = x^3 - 2x^2 + x - 3.$$

	2	3	4	-5	6	7
2		4	-2	6		
-1			14	-7	21	
3				32	-16	48
	2	7	16	24	11	55

После того как коэффициенты промежуточной строки достигли последнего столбца, коэффициенты остатка получаются простым сложением всех элементов соответствующих столбцов (в одном столбце находятся коэффициенты подобных членов).

Из таблицы Яковкина следует, что

$$f(x) = g(x) \cdot (2x^2 + 7x + 16) + (24x^2 + 11x + 55).$$

Если $b_0 = 1$, а многочлен $g(x)$ линейный, то схема Яковкина превращается в развернутую схему Горнера.

Справедливости ради отметим, что схема Яковкина не получила такого широкого распространения, как схема Горнера (а после внедрения вычислительной техники уже и не получит).

Под многочленом $f(x)$ можно понимать и целую рациональную функцию, определенную в K со значением в K .

Итак, вместо x в многочлен $f(x)$ можно поставить любой элемент кольца — в результате снова получится элемент кольца. Полный

прообраз нуля при таком отображении называется множеством корней многочлена, а элемент этого множества — *корнем*.

Другими словами, α (возможно, элемент надкольца кольца коэффициентов) — корень многочлена $f(x)$, если $f(\alpha) = 0$.

Подставляя в левую и правую части вместо x элемент α и используя связь между понятиями алгебраического многочлена и многочлена-функции, получаем, что остаток от деления многочлена $f(x)$ с коэффициентами из целостного кольца на двучлен $x - \alpha$ равен $f(\alpha)$.

Этот факт в честь автора называют *теоремой Безу*¹. Используя символ $\text{Rest}(a, b)$ для записи остатка от деления a на b , теорему Безу можно записать короче:

$$\text{Rest}(f(x), x - \alpha) = f(\alpha).$$

Теперь если многочлен разделился нацело на $(x - \alpha)$, то это значит, что $f(\alpha) = 0$. Верно и обратное, т. е. элемент α из целостного кольца K является корнем многочлена $f(x)$ с коэффициентами из K тогда и только тогда, когда $f(x)$ делится на двучлен $(x - \alpha)$.

В краткой, символической записи это утверждение имеет вид

$$f(\alpha) = 0 \Leftrightarrow (x - \alpha) \mid f(x).$$

Особо отметим, что теорема Безу выполняется для многочленов $f(x)$ с коэффициентами из целостного кольца K (не обязательно поля). Например, таким кольцом K может быть кольцо многочленов от переменных y, z , и чтобы узнать, делится ли многочлен

$$F(x) = x^3 + y^3 + z^3 + 3xyz$$

на

$$G(x) = x + y + z,$$

можно также использовать теорему Безу:

$$G(x) \mid F(x) \Leftrightarrow F(-y - z) = 0.$$

Вычислить значение $F(-y - z)$ и убедиться, что оно точно равно нулю, нетрудно (не сложнее, чем разделить $F(x)$ на $G(x)$ по схеме Горнера).

Вернемся от примера к общим результатам. Индукцией по степени многочлена $f(x)$, используя теорему Безу и отсутствие делителей нуля в кольце многочленов над целостным кольцом, получаем следующее утверждение: *число различных корней многочлена с ко-*

¹ *Этьенн Безу* (Bezout, 1730—1783) — французский математик, с 1763 г. — преподаватель математики в училище для гардемарин, а с 1768 г. — в Королевском артиллерийском корпусе.

коэффициентами из целостного кольца не превышает степени этого многочлена.

Корень α называют k -кратным (или корнем кратности k), если

$$(x - \alpha)^k \mid f(x),$$

но $(k + 1)$ -я степень $(x - \alpha)$ уже не делит $f(x)$.

Число различных корней многочлена степени n не превышает n , даже если считать каждый корень столько раз, какова его кратность.

Обобщить последнее утверждение на произвольные кольца коэффициентов не удастся.

Отсутствие делителей нуля в последнем наблюдении существенно. Например, в кольце \mathbb{Z}_8 классов вычетов по модулю 8 многочлен второй степени $x^2 - 1$ имеет четыре корня.

При некоммутативном умножении приходится говорить о двух частных и двух остатках — правом и левом соответственно.

Однако о корнях многочлена и их числе можно говорить и для некоммутативного кольца коэффициентов. Тот же многочлен $x^2 - 1$, рассматриваемый над телом кватернионов, имеет более двух корней. Это значит, что роль коммутативности умножения существенна. В теле кватернионов все свойства области целостности, кроме коммутативности, выполнены.

Многочлен $f(x)$ изображает некоторую функцию, определенную в кольце K со значением в K .

Как обычно, можно определить сумму и произведение многочленов-функций:

$$(f + g)(x) = f(x) + g(x);$$

$$(f \cdot g)(x) = f(x) \cdot g(x).$$

Множество многочленов-функций также образует кольцо K_1 с введенными операциями сложения и умножения. Это кольцо содержит в качестве подкольца кольцо коэффициентов K , но K_1 не всегда совпадает с простым трансцендентным расширением кольца K .

Говорят, что многочлены равны в алгебраическом смысле, если у них совпадают все коэффициенты при одинаковых степенях переменного. Понятно, что из равенства в алгебраическом смысле двух многочленов $f(x)$ и $g(x)$ следует и их функциональное равенство: значения $f(x)$ и $g(x)$ равны в каждой точке.

Число различных корней многочлена с коэффициентами из целостного кольца не превышает степени этого многочлена, поэтому если многочлен

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$$

имеет более чем n корней, то это означает, что f — многочлен без степени, т. е. нулевой, и, следовательно, $a_0 = a_1 = \dots = a_n = 0$.

Это значит, что если два многочлена степени n совпадают как функции в $(n + 1)$ -й точке, то коэффициенты этих многочленов равны.

Другими словами, коэффициенты многочлена $f(x)$ степени n полностью задаются значениями функции $y = f(x)$ в $(n + 1)$ -й точке.

Следовательно, если два многочлена $f(x)$ и $g(x)$ с коэффициентами из целостного кольца K имеют степень n и значения этих многочленов совпадают для $(n + 1)$ различных значений x , то для всех элементов a из K

$$f(a) = g(a).$$

Если целостное кольцо K бесконечно, то для многочлена n -й степени всегда можно указать $(n + 1)$ различных элементов из K , поэтому над бесконечным кольцом два многочлена, совпадающие как функции, равны в алгебраическом смысле.

Таким образом, установлено, что многочлены над бесконечным целостным кольцом равны в алгебраическом смысле тогда и только тогда, когда они равны в функциональном смысле.

Для такого кольца понятия простого трансцендентного расширения и понятия кольца многочленов как функций от одного переменного совпадают.

Бесконечность кольца коэффициентов существенно использовалась в доказательстве последнего утверждения, однако это не отнимает надежды, что существует другое доказательство, не использующее бесконечность этого кольца.

Надежда эта несбыточна — это свойство обойти нельзя.

Действительно, простое трансцендентное расширение любого кольца (и конечного тоже) бесконечно. Однако число всевозможных функций, в том числе и представимых многочленами, определенных на конечном множестве и со значениями в этом конечном множестве, конечно. Следовательно, для конечных целостных колец различные в алгебраическом смысле многочлены могут совпадать как функции.

Зададимся практическим вопросом: пусть известно, что $f(x)$ — многочлен степени $(n - 1)$, а функция $y = f(x)$ в различных n точках x_i принимает значения y_i ($i = 1, 2, \dots, n$).

Как найти коэффициенты многочлена $f(x)$?

Можно считать, что задача поставлена несколько иначе. Дана функция $y = f(x)$, и нам известны ее значения в n точках. Спрашивается, нельзя ли эту функцию представить некоторым многочленом степени n , т. е. указать такой многочлен, график которого пройдет через эти точки? Из предыдущего следует, что ответ на такой

степени многочлена число операций для вычисления коэффициентов растет слишком быстро.

Практически более удобен другой способ.

Многочлен

$$f(x) = \sum_{i=1}^n \frac{(x-x_1)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_n)}{(x_i-x_1)\dots(x_i-x_{i-1})(x_i-x_{i+1})\dots(x_i-x_n)} y_i$$

в честь его автора называют интерполяционным¹ многочленом Лагранжа.

Непосредственная проверка показывает, что интерполяционный многочлен Лагранжа $f(x)$ является многочленом степени не выше $(n-1)$ и для всех $i = 1, 2, \dots, n$

$$f(x_i) = y_i.$$

Таким образом, этот многочлен решает задачу нахождения многочлена $(n-1)$ -й степени по заданным n значениям.

Найдем, например, интерполяционный многочлен $f(x)$ пятой степени по заданным шести значениям:

$$f(1)=2, f(2)=3, f(3)=5, f(4)=7, f(5)=11, f(6)=13.$$

После раскрытия скобок и приведения подобных членов в многочлене Лагранжа получаем:

$$f(x) = -\frac{3}{40}x^5 + \frac{5}{4}x^4 - \frac{187}{24}x^3 + \frac{91}{4}x^2 - \frac{437}{15}x + 15.$$

6.2. Теория делимости в кольце многочленов

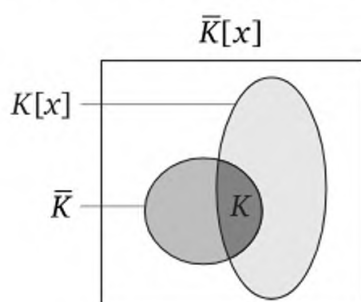
Поле — это лишь частный случай целостного кольца. Однако любое целостное кольцо K является подкольцом поля \bar{K} частных кольца K . При изучении кольца $K[x]$ многочленов над целостным кольцом K полезно иметь в виду, что это кольцо всегда содержится в кольце многочленов $\bar{K}[x]$ с коэффициентами из поля.

Поле является тривиальным образом евклидовым кольцом: любая функция годится для реализации евклидовости — в поле остаток от деления на ненулевой элемент всегда равен нулю.

Как и во всяком евклидовом кольце, в поле все идеалы главные (в поле всего два идеала — (0) и (1) , и оба главные).

¹ От лат. *interpolatio* — «обновление, переделывание». В первоначальном понимании — восстановление функции (приближенное или точное) по известным ее значениям.

Как и всякое кольцо главных идеалов, поле является гауссовым кольцом. В гауссовом кольце если элемент x отличен от нуля и делителя единицы, то ... (впрочем, не имеет значения, каким свойством обладает элемент x : в поле таких элементов просто нет).



Кольцо многочленов над полем частных

Самое важное для кольца многочленов над полем — то, что все эти кольцевые свойства *сохраняются*.

Конечно, в данной цепочке из трех звеньев (евклидовость, однопорядочность идеалов, гауссовость) решающим звеном является первое — евклидовость. Ухватившись за него, можно вытянуть всю цепь, так как евклидово кольцо является кольцом главных идеалов, а оно, в свою очередь, гауссово. Это значит, что хотя в общем случае евклидовость при простом трансцендентном расширении кольца K не сохраняется, но для поля коэффициентов природа сделала исключение.

Итак, покажем, что *кольцо многочленов над полем евклидово*.

Функцией, реализующей евклидовость, будет степень многочлена. Это значит, что для любых многочленов $f(x)$, $g(x)$ с коэффициентами из поля P :

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n;$$

$$g(x) = b_0x^m + b_1x^{m-1} + \dots + b_{m-1}x + b_m,$$

где $a_0 \neq 0$ и $b_0 \neq 0$, т. е. $\deg f(x) = n$ и $\deg g(x) = m$, существуют такие многочлены $q(x)$ и $r(x)$ с коэффициентами из этого же поля, что

$$f(x) = g(x)q(x) + r(x),$$

где $r(x)$ — нулевой многочлен или $\deg r(x) < \deg g(x)$.

Если $m = 0$, то и доказывать нечего (в этом случае многочлен $g(x)$ — ненулевой элемент в поле и, следовательно, делитель единицы).

Итак, пусть $\deg g(x) > 0$.

Многочлен

$$g_1(x) = \frac{1}{b_0} g(x)$$

нормирован, а для нормированного многочлена-делителя деление с остатком со степенью в качестве евклидовой функции выполняется над любым целостным кольцом.

Записав соответствующее равенство и отдав коэффициент $\frac{1}{b_0}$ частному, получим результат деления $f(x)$ на $g(x)$ в кольце $P[x]$. Это значит, что простое трансцендентное расширение поля является евклидовым кольцом.

Впрочем, доказательство евклидовости $P[x]$ можно было провести и не ссылаясь на уже рассмотренный ранее случай с нормированным делителем.

Если $n \geq m$, то

$$f(x) - g(x) \cdot \frac{a_0}{b_0} x^{n-m} = 0$$

(в этом случае все закончено) или

$$\deg \left(f(x) - g(x) \cdot \frac{a_0}{b_0} x^{n-m} \right) < \deg f(x).$$

Рассуждение далее можно провести индукцией по степени делимого $f(x)$. Такое доказательство полностью воспроизводит известную из школьного курса математики схему деления уголком:

$$\begin{array}{r|l} f(x) & g(x) \\ \vdots & q(x) \\ \hline r(x) & \end{array}$$

В отличие от рассмотренного ранее случая с целостным кольцом, здесь многочлен $g(x)$ произвольный, а не обязательно нормированный.

Доказательство существования частного и остатка конструктивно, а это значит, что если есть алгоритмы арифметических действий в поле коэффициентов, то, соответственно, возникает алгоритм деления для многочленов с коэффициентами из этого поля.

Например, алгоритмически разрешима задача нахождения частного и остатка для многочленов с рациональными коэффициентами.

Все алгоритмы действий над рациональными числами основаны на алгоритмах для целых чисел. Поэтому алгоритм деления был бы более естественен для многочленов с целыми коэффициентами. Однако в $\mathbb{Z}[x]$ вообще нельзя определить евклидову функцию, поэтому не существует алгоритма деления для многочленов от одного переменного с целочисленными коэффициентами.

Начинаем вытягивать цепь умозаключений, ухватившись за решающее звено — евклидовость.

В евклидовом кольце все идеалы главные. Поэтому кольцо многочленов над полем является кольцом главных идеалов.

В частности, главным идеалом будет идеал, порожденный n многочленами $f_1(x), f_2(x), \dots, f_n(x)$. Поскольку идеал, порожденный любым числом элементов, в кольце главных идеалов состоит из всевозможных сумм кратных этих элементов, получаем, что для каждого n многочленов $f_1(x), f_2(x), \dots, f_n(x)$ с коэффициентами из поля P существуют такие многочлены $u_1(x), u_2(x), \dots, u_n(x)$ из $P[x]$, что

$$u_1(x) \cdot f_1(x) + u_2(x) \cdot f_2(x) + \dots + u_n(x) \cdot f_n(x) = d(x),$$

где $d(x) = (f_1(x), f_2(x), \dots, f_n(x))$.

Для $n = 2$ можно выразиться точнее: для каждого двух многочленов $f(x), g(x)$ с коэффициентами из поля P существуют такие многочлены $u(x), v(x)$ из $P[x]$, что

$$u(x) \cdot f(x) + v(x) \cdot g(x) = (f(x), g(x)),$$

где $\deg v(x) < \deg f(x), \deg u(x) < \deg g(x)$.

Это свойство позволяет найти многочлены $u(x)$ и $v(x)$ методом неопределенных коэффициентов.

Впрочем, многочлены $u(x)$ и $v(x)$ можно найти, используя неполные частные алгоритма Евклида, примененного к нахождению $(f(x), g(x))$. Все свойства цепных дробей, членами которых являются целые числа, полностью переносятся и на цепные дроби, заполненные многочленами с коэффициентами из поля.

Теперь рассмотрим отдельно случай конечного кольца коэффициентов.

Покажем, что *любая функция от одного переменного, определенная над конечным целостным кольцом со значениями в этом кольце, является многочленом.*

Если конечное кольцо K содержит n элементов, то число различных многочленов степени меньше n равно числу всевозможных отображений множества K в K .

Отсюда и следует, что если K — конечное целостное кольцо, состоящее из n элементов, то каждое отображение $f: K \rightarrow K$ можно единственным образом представить многочленом степени не выше $(n - 1)$.

Впрочем, вместо слов «конечное целостное кольцо» можно сказать лишь одно слово «поле», так как каждое конечное целостное кольцо является полем.

Итак, каждая функция $y = f(x)$ со значениями из n -элементного поля может быть единственным образом представлена многочленом степени не выше $(n - 1)$.

Подведем первые итоги.

При простом трансцендентном расширении кольца сохраняется целостность, но, вообще говоря, не сохраняется ни евклидовость, ни однопорозжденность идеалов.

Важным свойством кольца является гауссовость (факториальность). Кольцо гауссово, если каждый его элемент, отличный от нуля и делителя единицы, является либо простым, либо произведением простых, причем представление в виде простых единственно (с точностью до порядка множителей и ассоциированности).

Чтобы говорить о свойстве гауссовости, нужно сначала договориться о простых элементах в кольце многочленов.

Простые элементы в кольце многочленов, отличные от простых элементов кольца коэффициентов, принято называть *неприводимыми многочленами*.

Кольцо многочленов с коэффициентами из целостного кольца снова является целостным кольцом, поэтому можно говорить о делимости в этом кольце.

В поле P необратимым элементом является лишь нуль, группа $(P[x])^*$ обратимых элементов кольца $P[x]$ многочленов над полем P совпадает с мультипликативной группой P^* поля P . Это значит, что

$$(P[x])^* = \{f(x) \mid \deg f(x) = 0\}.$$

Отношение делимости в целостном кольце является отношением предпорядка на самом кольце и одновременно отношением порядка на фактор-множестве по отношению ассоциированности.

В кольце $P[x]$ многочленов над полем P два многочлена ассоциированы тогда и только тогда, когда они отличаются ненулевым множителем из P .

Многочлены ненулевой степени, играющие роль простых элементов в кольце многочленов с коэффициентами из поля, называют *неприводимыми многочленами*.

Итак, многочлен $f(x)$ неприводим, если:

- 1) $\deg f(x) > 0$;
- 2) $f(x) = a(x) \cdot b(x) \Rightarrow \deg a(x) = 0$ или $\deg b(x) = 0$.

Многочлен ненулевой степени, не являющийся неприводимым, называется *приводимым*. Точнее, многочлен $f(x)$ приводим, если

$$f(x) = a(x) \cdot b(x),$$

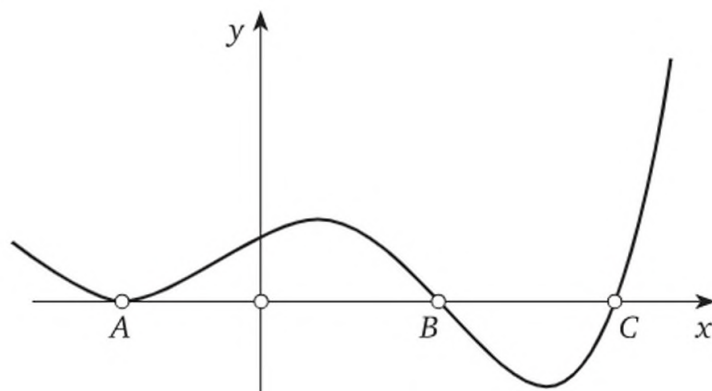
где $\deg a(x) > 0$ и $\deg b(x) > 0$.

Непосредственно из определения неприводимости следует, что все многочлены первой степени над любым полем неприводимы. Число многочленов первой степени в кольце $P[x]$ над бесконечным полем бесконечно.

Если поле P конечно, то число многочленов любой фиксированной (в том числе и первой) степени в $P[x]$ будет конечным. Однако, повторяя почти дословно рассуждение Евклида, примененное для доказательства бесконечности множества простых чисел, получаем, что и над конечным полем существует бесконечно много неприводимых многочленов. Итак, *над любым полем существует бесконечно много неприводимых многочленов.*

Наличие бесконечного числа неприводимых многочленов над конечным полем и одновременно лишь конечного числа многочленов степени, не превышающей данного числа n , означает, что *над конечным полем существуют неприводимые многочлены, степень которых превышает любое наперед заданное натуральное число.*

Рассмотрим многочлен $f(x)$ с действительными коэффициентами. Точки пересечения графика функции $y = f(x)$ с осью абсцисс — это корни многочлена $f(x)$. Данное пересечение может выглядеть по-разному.



Корни многочлена в точках A, B, C

В одном случае линия графика пересекает ось абсцисс под некоторым ненулевым углом (т. е. касательная в этой точке не параллельна оси абсцисс), а в другом случае ось абсцисс является одновременно и касательной, проведенной в точку корня.

Во втором случае корень многочлена является одновременно и корнем его производной. В то же время касание графика многочлена оси абсцисс сигнализирует нам о кратном корне многочлена.

Например, на рисунке, изображающем график многочлена, в точке A — кратный корень, а в точках B, C, возможно, простые корни многочлена (или корни нечетной кратности).

Итак, если многочлен $f(x)$ имеет кратный корень s , то число s является и корнем его производной $f'(x)$. Этот факт, впрочем, можно сформулировать в гораздо большей общности, и не только для многочленов с действительными коэффициентами. Можно даже уточнить это утверждение, не просто отметив кратность корня, а указав эту кратность точно.

Напомним, что производную многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n,$$

где a_i — элементы из произвольного поля ($i = 0, 2, \dots, n$), можно было определить чисто формально, положив по определению

$$f'(x) \stackrel{\text{опр}}{=} na_0x^{n-1} + (n-1)a_1x^{n-2} + \dots + a_{n-1}.$$

Все обычные свойства производной будут выполнены, формулы для вычисления производной суммы и произведения двух многочленов, а также производная суперпозиции будут точно такими же.

Единственное, в чем нельзя теперь быть уверенным, это то, что степень производной в точности на единицу меньше степени многочлена (в поле конечной характеристики некоторые члены после такого «дифференцирования» могут исчезнуть). Поэтому самые главные замечания касаются все-таки полей нулевой характеристики.

Неприводимый k -кратный множитель многочлена $f(x)$ с коэффициентами из поля нулевой характеристики является $(k-1)$ -кратным множителем его производной.

Чтобы это увидеть, достаточно вычислить производную многочлена

$$f(x) = [p(x)]^k \cdot q(x),$$

где $q(x)$ не делится на $p(x)$. Вычисляем

$$\begin{aligned} f'(x) &= p'(x) \cdot [p(x)]^{k-1} \cdot q(x) + [p(x)]^k \cdot q'(x) = \\ &= [p(x)]^{k-1} (p'(x) \cdot q(x) + p(x) \cdot q'(x)). \end{aligned}$$

Многочлен

$$p'(x) \cdot q(x) + p(x) \cdot q'(x)$$

не делится на $p(x)$. Действительно, слагаемое $p(x) \cdot q'(x)$ делится на $p(x)$, но ни один из многочленов $p'(x)$, $q(x)$ не делится на $p(x)$.

Корню многочлена соответствует линейный (и поэтому неприводимый) множитель.

Следовательно, корень кратности k многочлена $f(x)$ с коэффициентами из поля нулевой характеристики является $(k-1)$ -кратным корнем многочлена $f'(x)$.

В частности, простой корень многочлена не является корнем его производной. Этот факт для многочленов из $\mathbf{R}[x]$ можно было заранее предсказать, опираясь лишь на геометрические свойства графика многочлена.

Итак, многочлен с коэффициентами из поля нулевой характеристики не имеет кратных корней тогда и только тогда, когда он взаимно прост со своей производной.

Отметим, что для любого поля (в том числе и с положительной характеристикой) из взаимной простоты со своей производной следует отсутствие кратных корней многочлена.

Производная и наибольший делитель находятся с помощью арифметических операций поля, т. е. если $f(x)$ принадлежит $P[x]$, то и его производная $f'(x)$, и наибольший общий делитель $(f(x), f'(x))$ многочлена и его производной снова находятся в кольце $P[x]$. Поэтому если многочлен $f(x)$ с коэффициентами из поля P не имеет кратных корней в P , то он не имеет кратных корней в любом расширении поля P .

Многочлен с коэффициентами из поля нулевой характеристики не имеет кратных корней тогда и только тогда, когда он взаимно прост со своей производной.

Простое трансцендентное расширение кольца главных идеалов не обязательно является кольцом главных идеалов, т. е. свойство однопорядковности идеалов при переходе к кольцу многочленов сохраняется не всегда.

Однако однопорядковность идеалов — это лишь частный случай конечной порождаемости. Для конечно порожденных идеалов ситуация меняется. Кольцо, в котором каждый идеал конечно порожден, называется *нетеровым кольцом*¹.

Другими словами, каждая возрастающая цепочка идеалов нетерова кольца

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_i \subseteq \dots$$

обрывается на конечном шаге.

Пусть идеал I в кольце многочленов $K[x]$ бесконечно порожден, $f_i(x)$ — его порождающие многочлены и $a_i x^{n_i}$ — старшие члены этих многочленов.

Удаляя, если потребуется, лишние многочлены, можно считать, что для каждого i многочлен $f_i(x)$ не принадлежит идеалу, порожденному всеми предшествующими многочленами $f_k(x)$:

$$f_i(x) \notin (f_1(x), f_2(x), \dots, f_{i-1}(x)).$$

Более того, можно выбрать так эти многочлены, что каждый $f_i(x)$ будет многочленом наименьшей степени, не входящим в идеал, порожденный предшественниками.

¹ Эмми Амали Нётер (Noether, 1882—1935) — немецкий математик, внештатный профессор Геттингенского университета (1922—1933), образно выражаясь, «мать современной алгебры».

Тогда степени многочленов $f_i(x)$ не убывают:

$$n_1 \leq n_2 \leq \dots \leq n_i \leq \dots$$

Предположим, что a_i выражается через a_1, a_2, \dots, a_{i-1} :

$$a_i = a_1 b_1 + a_2 b_2 + \dots + a_{i-1} b_{i-1}.$$

Тогда старший член многочлена

$$g(x) = b_1 f_1(x) x^{n_i - n_1} + b_2 f_2(x) x^{n_i - n_2} + \dots + b_{i-1} f_{i-1}(x) x^{n_i - n_{i-1}}$$

равен $a_i x^{n_i}$, и, следовательно, многочлен $f_i(x) - g(x)$ не принадлежит идеалу

$$(f_1(x), f_2(x), \dots, f_{i-1}(x)),$$

но

$$\deg(f_i(x) - g(x)) < \deg(f_i(x)).$$

Полученное противоречие означает, что в кольце $K[x]$ нет бесконечно порожденных идеалов. Это значит, что *простое трансцендентное расширение нетерова кольца снова является нетеровым кольцом*.

Итак, к сохраняющимся при переходе к кольцу многочленов свойствам добавилось еще одно — конечная порожденность идеалов.

Нетеровость кольца $K[x_1, x_2, \dots, x_n]$ над нетеровым кольцом K означает, в частности, что *любая система алгебраических уравнений с коэффициентами из K равносильна своей конечной подсистеме*. Этот факт по имени автора называют *теоремой Гильберта¹ о базисе*.

Подведем итоги.

При простом трансцендентном расширении два свойства (целостность и нетеровость) сохраняются, а два (евклидовость и однопорожденность идеалов) не сохраняются.

Остается разобраться лишь со свойством гауссовости (факториальности).

6.3. Сохранение гауссовости при переходе к кольцу многочленов

Гауссовость кольца — однозначность представления ненулевого и отличного от делителя единицы элемента в виде произведения простых множителей — является еще одним случаем сохранения кольцевого свойства при простом трансцендентном расширении.

¹ Доказана Д. Гильбертом в 1890 г.

Главная цель этого пункта — доказать утверждение, сформулированное в названии. Опорным пунктом доказательства является факт, что кольцо многочленов с коэффициентами из поля является гауссовым, а каждое целостное кольцо изоморфно вложено в поле. Кроме того, потребуется одно свойство гомоморфизма гауссовых колец.

Напомним, что фактор-кольцу целостного кольца вовсе не обязательно быть полем и даже целостным кольцом. Например, все кольца классов вычетов по составному модулю содержат делители нуля. Однако если модуль — простое число p , то фактор-кольцо \mathbb{Z}_p является полем.

Кольцо \mathbb{Z} , правда, не просто гауссово кольцо, оно и кольцо главных идеалов, и даже евклидово.

Оказалось, что свойство сохранения целостности (т. е. непоявление делителей нуля) при переходе к гомоморфному образу является общим для всех гауссовых колец.

Если кольцо K гауссово, а p — простой элемент в K , то фактор-кольцо $K/(p)$ целостное.

Действительно, из равенства

$$((p) + x)((p) + y) = (p) + xy = (p)$$

следует, что p делит xy . Из гауссовости кольца K следует, что p делит x или p делит y . На языке сравнений это означает, что

$$xy \equiv 0(\text{mod}(p)) \Rightarrow x \equiv 0(\text{mod}(p)) \text{ или } y \equiv 0(\text{mod}(p)).$$

Следовательно, фактор-кольцо $K/(p)$ не содержит делителей нуля.

Одного этого важного утверждения о гауссовых кольцах для достижения поставленной цели недостаточно.

Вспользуемся идеей, принадлежащей К. Гауссу. Для этого введем вспомогательное понятие *примитивного многочлена*.

Пусть K — гауссово кольцо. В гауссовом кольце любое конечное множество элементов обладает наибольшим общим делителем и наименьшим общим кратным. Если a_1, a_2, \dots, a_n — некоторое конечное множество элементов из K , а d — их наибольший общий делитель, то разделив каждый элемент a_i на d , мы получим множество взаимно простых (в совокупности) элементов.

Многочлен из $K[x]$ называют *примитивным*, если его коэффициенты в совокупности взаимно просты.

Если $f(x)$ — произвольный многочлен положительной степени из $K[x]$, то, вынеся наибольший общий делитель его коэффициентов за скобку, мы получим представление многочлена

$$f(x) = d \cdot f_1(x),$$

где d — элемент из K , а $f_1(x)$ — примитивный многочлен.

Представление многочлена в таком виде не однозначно, так как сам элемент d определяется с точностью до ассоциированности.

Однако эта ассоциированность — единственное, что может нарушить однозначность такого представления. Раскрыв скобки в представлении и используя ассоциированность наибольших общих делителей, получим, что если

$$d_1 \cdot f_1(x) = d \cdot f_2(x),$$

где $f_1(x)$ и $f_2(x)$ — оба примитивные, то эти многочлены ассоциированы в K (как ассоциированы d_1 и d_2).

Кольцо K целостное, поэтому для него существует поле частных P .

Исследуемое кольцо $K[x]$ содержится в кольце $P[x]$. Так как P — поле, то кольцо $P[x]$ является гауссовым; в нем каждый многочлен положительной степени можно представить в виде произведения неприводимых многочленов. Такое представление единственно с точностью до порядка и ассоциированности множителей.

Пусть теперь $f(x)$ — многочлен из $P[x]$. Каждый коэффициент этого многочлена является отношением двух элементов из K . Приведем эти дроби к общему знаменателю и вынесем знаменатель за скобку. В скобках останется многочлен из $K[x]$. У этого многочлена вынесем за скобку наибольший делитель его коэффициентов и в результате получим представление многочлена

$$f(x) = \frac{a}{b} \cdot f_1(x),$$

где a, b — взаимно простые элементы из K , а $f_1(x)$ — примитивный многочлен из $K[x]$.

Элемент $\frac{a}{b}$ в таком представлении называют *содержанием*, а $f_1(x)$ — *примитивной частью* многочлена $f(x)$.

Если многочлен имеет два представления в виде произведения содержания и примитивной части,

$$\frac{a}{b} \cdot f_1(x) = \frac{a_1}{b_1} \cdot f_2(x),$$

то

$$ab_1 \cdot f_1(x) = a_1b \cdot f_2(x),$$

где элементы ab_1 и a_1b принадлежат K и, следовательно, ассоциированы в K . Но тогда a делит a_1b и a взаимно просто с b , значит, a делит a_1 . По той же причине a_1 делит a . Элементы a и a_1 (аналогично b и b_1) ассоциированы.

Итак, если P — поле частных гауссова кольца, то представление каждого многочлена положительной степени из $P[x]$ в виде произведения содержания и примитивной части единственно с точностью до ассоциированности множителей.

Отсюда, в частности, следует, что если в таком представлении $b = 1$, то и любое другое представление этого же многочлена будет иметь целое (т. е. принадлежащее K) содержание.

Следующий факт вошел в историю математики как *лемма Гаусса*: *произведение примитивных многочленов является примитивным многочленом.*

Для доказательства леммы Гаусса предположим, что в кольце K найдется простой элемент p , который делит все коэффициенты многочлена-произведения.

Поскольку элемент p — простой в кольце K , то фактор-кольцо $K/(p)$ целостное. Переход к кольцу многочленов целостность сохраняет, поэтому кольцо $K/(p)[x]$ тоже целостное. При переходе от кольца $K[x]$ к кольцу $K/(p)[x]$ многочлен-произведение превратится в нулевой, а следовательно, и один из множителей должен быть нулевым многочленом в $K/(p)[x]$, т. е. не примитивным над K .

В лемме Гаусса речь идет о двух многочленах. Индукцией это утверждение распространяется на любое число множителей.

Если P — поле частных гауссова кольца K и многочлен с коэффициентами из K разлагается на множители над K , то это же разложение можно считать разложением над полем P . Другими словами, если многочлен из $K[x]$ приводим над кольцом K , то он приводим над полем частных этого кольца.

Покажем, что и обратное верно: если многочлен $f(x)$ из $K[x]$ приводим над полем P , то он приводим и над кольцом K .

Предположим, что над полем P многочлен $f(x)$ обладает нетривиальным разложением на множители:

$$f(x) = s(x) \cdot t(x),$$

где степени многочленов $s(x)$ и $t(x)$ ненулевые.

Представим многочлены $s(x)$ и $t(x)$ в виде произведения содержания и примитивной части, затем перемножим их содержания и примитивные части. В результате благодаря лемме Гаусса получим представление многочлена $f(x)$, у которого содержание принадлежит K . Следовательно, по единственности такого представления и содержание многочлена $s(x)t(x)$ тоже находится в K . Но это означает, что если P — поле частных гауссова кольца K , то многочлен с коэффициентами из K приводим над K тогда и только тогда, когда он приводим над P .

С помощью поля частных P можно получить разложение многочлена $f(x)$ на неприводимые множители над K . Пусть $f(x)$ — многочлен из $K[x]$ и

$$f(x) = p_1(x) \cdot p_2(x) \cdot \dots \cdot p_m(x) —$$

его разложение на множители, неприводимые над полем P . Представим каждый множитель $p_i(x)$ в виде содержания и примитивной части, а затем перемножим все содержания. В результате получится произведение примитивных неприводимых над K многочленов (тех же степеней и даже ассоциированных в K) и некоторого элемента d из K .

Разложив элемент d на произведение простых элементов кольца K , мы получим в результате разложение многочлена $f(x)$ на простые множители. В этом разложении многочленная и содержательная части имеют единственное (с точностью до порядка и ассоциированности множителей) представление.

Иначе говоря: *простое трансцендентное расширение гауссова кольца является гауссовым кольцом.*

В частности, кольцо $\mathbb{Z}[x]$ многочленов с целыми коэффициентами тоже гауссово. Напомним, что в этом кольце есть неглавные идеалы. Таким образом, существует гауссово кольцо, не являющееся евклидовым кольцом. *Из гауссовости не следует евклидовость.*

То же самое можно сформулировать на языке школьного курса математики: *теорема о делении с остатком не является следствием основной теоремы арифметики.*

Напомним, что обратное верно: *основная теорема арифметики — это следствие теоремы о делении с остатком.* Разумеется, речь идет не только о кольце целых чисел.

Итак, над любым полем многочлен положительной степени можно разложить в произведение неприводимых множителей.

Эти множители существенно зависят от поля коэффициентов. Например, многочлен $x^2 - 2$ с рациональными коэффициентами не имеет рациональных корней, т. е. он неприводим над полем \mathbb{Q} .

Однако в поле действительных чисел этот многочлен уже имеет корень, поэтому он приводим над полем \mathbb{R} . Впрочем, так далеко расширять поле \mathbb{Q} для этой цели нет необходимости: уже множество

$$P = \{a + b\sqrt{2} \mid a \in \mathbb{Q}, b \in \mathbb{Q}\}$$

является полем, содержащим поле рациональных чисел \mathbb{Q} и корень многочлена $x^2 - 2$.

Аналогично многочлен $x^2 + 1$ не имеет корней в поле \mathbb{R} действительных чисел, но имеет их в поле \mathbb{C} комплексных чисел.

Иначе говоря, многочлен $f(x)$ с коэффициентами из поля P может не иметь корней в поле коэффициентов, однако имеет корень в полевом расширении поля P .

В двух предыдущих примерах многочлены были неприводимы над полем коэффициентов. Пусть коэффициенты неприводимого над P многочлена $f(x)$ принадлежат полю P , а ни один из корней этому полю не принадлежит. Однако поле P можно расширить таким образом, что расширение уже будет содержать по крайней мере один из корней многочлена $f(x)$. Иначе говоря, для каждого поля P и неприводимого многочлена $f(x)$ с коэффициентами из P существует поле P_1 — расширение поля P , содержащее корень многочлена $f(x)$.

В качестве такого поля P_1 можно взять фактор-кольцо $P[x]/(f(x))$. Действительно, из максимальности идеала $(f(x))$ в кольце $P[x]$ следует, что это фактор-кольцо является полем. Пересечение идеала $(f(x))$ и поля коэффициентов состоит только из одного нуля, поэтому фактор-кольцо содержит изоморфную копию

$$\{(f(x)) + a \mid a \in P\}$$

поля P . Тогда переписанный в терминах элементов этой копии многочлен $f(X)$ имеет корнем $(f(x)) + x$:

$$f((f(x)) + x) = (f(x)),$$

а идеал $(f(x))$ играет роль нуля в фактор-кольце.

Поскольку кольцо $P[x]$ гауссово, многочлен $f(x)$ является произведением неприводимых над P многочленов, каждый корень которых является корнем многочлена $f(x)$.

Это значит, что слово «неприводимый» в предыдущем утверждении можно удалить: для каждого поля P и многочлена $f(x)$ с коэффициентами из P существует поле P_1 — расширение поля P , содержащее корень многочлена $f(x)$.

В честь автора это утверждение называют *теоремой Кронекера*¹.

Расширение поля коэффициентов многочлена $f(x)$, содержащее все корни этого многочлена, называют *полем разложения многочлена $f(x)$* .

Многочлен степени n может иметь самое большее n различных корней, поэтому в результате не более n расширений поля коэффициентов многочлена $f(x)$ появится поле, которое содержит все корни этого многочлена.

Иначе говоря, для каждого многочлена с коэффициентами из поля существует поле разложения этого многочлена.

¹ Леопольд Кронекер (Kronecker, 1823—1891) — немецкий математик, иностранный член Петербургской академии наук (с 1872 г.), член Берлинской академии наук (с 1861 г.), с 1883 г. — профессор Берлинского университета. Теорема о существовании корня многочлена в некотором расширении поля коэффициентов доказана им в 1882 г.

Если поставить вопрос проще: нельзя ли произвольное поле вложить в некоторое более широкое поле, то ответ, по существу, был уже получен ранее: да, можно.

Каждое целостное кольцо изоморфно вложимо в поле частных; вложимо в поле и кольцо многочленов $K[x]$ над целостным кольцом K . Поле частных $K[x]$ кольца многочленов $K[x]$ называют *полем рациональных дробей*. Это поле обозначают символом $K(x)$. Многочлен можно считать представляющим некоторую функцию над кольцом коэффициентов, поэтому рациональная дробь тоже представляет функцию над K . Обычно ее называют *дробно-рациональной функцией* или просто *рациональной функцией*. Точнее говоря, функция вида

$$s(x) = \frac{f(x)}{g(x)},$$

где $f(x)$ и $g(x)$ — многочлены с коэффициентами из некоторого поля и $g(x)$ ненулевой, называется *дробно-рациональной*. В частности, все функции, представляемые многочленами, являются рациональными функциями, говорят: «целая рациональная функция».

Можно считать, что многочлены, участвующие в представлении рациональной функции, взаимно просты, так как в противном случае дробь $\frac{f(x)}{g(x)}$ можно сократить.

Рациональная дробь $\frac{f(x)}{g(x)}$ называется *правильной*, если $\deg f < \deg g$.

Используя линейное разложение наибольшего общего делителя взаимно простых многочленов, получаем, что каждую правильную рациональную дробь

$$\frac{f(x)}{g_1(x)g_2(x)},$$

где g_1, g_2 взаимно просты, можно представить в виде суммы двух дробей:

$$\frac{f(x)}{g_1(x)g_2(x)} = \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)}.$$

Поскольку степени дополняющих множителей в линейном разложении единицы ограничены степенями многочленов $g_1(x), g_2(x)$, то представление правильной рациональной дроби

$$\frac{f(x)}{g_1(x)g_2(x)},$$

где $g_1(x), g_2(x)$ взаимно просты, в виде суммы двух *правильных* дробей

$$\frac{f(x)}{g_1(x)g_2(x)} = \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)}$$

единственно.

Это утверждение обобщается на произвольное число множителей в знаменателе. Точнее, каждую правильную рациональную дробь

$$\frac{f(x)}{g_1(x)g_2(x)\dots g_n(x)},$$

где $g_1(x), g_2(x), \dots, g_n(x)$ попарно взаимно просты, можно представить, и единственным образом, в виде суммы правильных дробей:

$$\frac{f(x)}{g_1(x)g_2(x)\dots g_n(x)} = \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} + \dots + \frac{f_n(x)}{g_n(x)}.$$

Свойства кольца многочленов над полем и свойства кольца целых чисел во многом схожи. Главное сходство состоит в том, что оба эти кольца евклидовы: в каждом из них выполняется теорема о делении с остатком.

Из выполнения теоремы о делении с остатком и следует однопорочность идеалов и гауссовость.

Но для целых чисел не эти следствия были самыми важными. Важнейшим следствием теоремы о делении с остатком была возможность представления каждого натурального числа в систематической записи, т. е. в позиционной аддитивно-мультипликативной системе исчисления.

Для многочленов это свойство, хотя и не играет такой значительной роли, как для чисел, но тоже выполняется.

Зафиксируем $g(x)$ произвольный многочлен положительной степени из $P[x]$. Используя теорему о делении с остатком, можно представить любой многочлен $f(x)$ из $P[x]$ в виде

$$f(x) = q_m(x)g^m(x) + q_{m-1}(x)g^{m-1}(x) + \dots + q_1(x)g(x) + q_0(x),$$

где для всех $i = 0, 1, \dots, m$ многочлен $q_i(x)$ нулевой или $\deg q_i(x) < \deg g(x)$.

Теперь в произвольной дроби

$$\frac{f(x)}{g^n(x)}$$

можно числитель представить в $g(x)$ -ичном систематическом виде:

$$\frac{f(x)}{g(x)} = \frac{q_m(x)g^m(x) + q_{m-1}(x)g^{m-1}(x) + \dots + q_0(x)}{g^n(x)}.$$

Если $m \geq n$, то в представлении этой дроби выделится целая часть, а для $m < n$ появится представление дробной части:

$$\begin{aligned} \frac{q_m(x)g^m(x) + q_{m-1}(x)g^{m-1}(x) + \dots + q_0(x)}{g^n(x)} &= \\ = \frac{q_m(x)}{g^{n-m}(x)} + \frac{q_{m-1}(x)}{g^{n-m+1}(x)} + \dots + \frac{q_1(x)}{g^{n-1}(x)} + \frac{q_0(x)}{g^n(x)}. \end{aligned}$$

Если многочлен $p(x)$ неприводим, то дробь вида

$$\frac{q(x)}{p^k(x)},$$

где $\deg q(x) < \deg g(x)$, называют *простейшей дробью*.

Кольцо $P[x]$ гауссово, т. е. каждый многочлен $g(x)$ можно представить в виде произведения степеней неприводимых многочленов

$$g(x) = p_1^{\alpha_1}(x) \cdot p_2^{\alpha_2}(x) \cdot \dots \cdot p_m^{\alpha_m}(x).$$

Все множители $p_1^{\alpha_1}(x), p_2^{\alpha_2}(x), \dots, p_m^{\alpha_m}(x)$ попарно взаимно просты, и, следовательно, правильная дробь $\frac{f(x)}{g(x)}$ имеет представление

$$\frac{f(x)}{g(x)} = \frac{f(x)}{p_1^{\alpha_1}(x)p_2^{\alpha_2}(x)\dots p_n^{\alpha_n}(x)} = \frac{f_1(x)}{p_1^{\alpha_1}(x)} + \frac{f_2(x)}{p_2^{\alpha_2}(x)} + \dots + \frac{f_n(x)}{p_n^{\alpha_n}(x)}.$$

Каждое слагаемое теперь можно представить в виде простейших дробей. Таким образом, каждая правильная рациональная дробь с коэффициентами из поля имеет представление в виде суммы простейших дробей.

Напомним, что многочлен первой степени всегда неприводим. Найти представление дроби $\frac{f(x)}{(x-a)^k}$ в виде суммы простейших дробей можно с помощью схемы Горнера. Для этого достаточно разложить числитель дроби по степеням $(x-a)$, а затем произвести почленное деление:

$$\begin{aligned} \frac{f(x)}{(x-a)^k} &= \frac{b_m(x-a)^m + b_{m-1}(x-a)^{m-1} + \dots + b_0}{(x-a)^n} = \\ &= \frac{b_m}{(x-a)^{n-m}} + \frac{b_{m-1}}{(x-a)^{n-m+1}} + \frac{b_0}{(x-a)^n}. \end{aligned}$$

6.4. Многочлены над числовыми полями

Общие соображения о многочленах над целостными кольцами и полями, разумеется, остаются верными и для числовых полей. Особенностью исследования многочленов с числовыми ко-

эффициентами являются многочисленные вопросы технического характера: вычисление корней многочлена с заданной точностью, определение числа корней в заданном интервале и другие сходные проблемы. Принципиально важным свойством наибольшего числового поля — поля комплексных чисел — является его алгебраическая замкнутость.

Числовым полем называют любое подполе поля комплексных чисел. Число различных числовых полей превышает мощность континуума, но сейчас имеются в виду вовсе не все числовые поля, а всего лишь *три* поля:

- наибольшее (поле \mathbb{C});
- наименьшее (поле \mathbb{Q});
- промежуточное (поле \mathbb{R}).

Таким образом, под словами «числовое поле» будут пониматься основные числовые поля школьного курса математики и вузовского курса математического анализа.

Начнем обсуждение с промежуточного поля — *поля действительных чисел*.

Над полем действительных чисел множество многочленов с операциями сложения и умножения на число образует векторное пространство.

Свойство базиса этого пространства связано с комбинаторной задачей разбиения множества из n элементов на k смежных классов.

Рассмотрим множество $\mathbf{R}_n[x]$ многочленов с действительными коэффициентами, степень которых не превышает данное число n . Степень нулевого многочлена считается равной $-\infty$, поэтому множество $\mathbf{R}_n[x]$ содержит и нулевой многочлен.

Поскольку

$$\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\},$$

множество $\mathbf{R}_n[x]$ замкнуто относительно сложения, и поэтому образует векторное пространство.

Точнее, если n — целое неотрицательное число, то множество

$$\mathbf{R}_n[x] = \{a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \mid a_i \in \mathbf{R}\}$$

образует векторное пространство над полем \mathbf{R} и $\dim \mathbf{R}_n[x] = n + 1$.

Естественным базисом для пространства $\mathbf{R}_n[x]$ является система многочленов

$$1, x, x^2, \dots, x^n.$$

Эта система линейно независима, и любой многочлен естественным образом линейно выражается через нее.

Для линейной независимости этой системы на самом деле достаточно того, что все степени многочленов в системе различны. Иначе говоря, система $f_1(x), f_2(x), \dots, f_m(x)$, состоящая из многочленов попарно различных степеней, линейно независима.

В m -мерном векторном пространстве любая система, состоящая из m линейно независимых векторов, образует базис пространства. Поэтому любая система многочленов $f_0(x), f_1(x), \dots, f_n(x)$ таких, что $\deg f_i(x) = i$, образует базис пространства $\mathbf{R}_n[x]$.

Это замечание означает, в частности, что произвольный многочлен $f(x)$ степени $\leq n$ можно представить единственным образом в виде

$$f(x) = \sum_{i=0}^n a_i f_i(x),$$

где $f_i(x)$ — многочлены i -й степени.

Рассмотрим систему из $n + 1$ многочлена следующего вида:

$$\begin{aligned} p_0(x) &= 1; \\ p_1(x) &= x; \\ p_2(x) &= x(x-1); \\ &\dots\dots\dots \\ p_k(x) &= x(x-1)(x-2)\dots[x-(k-1)]; \\ &\dots\dots\dots \\ p_n(x) &= x(x-1)(x-2)\dots[x-(n-1)]. \end{aligned}$$

Поскольку $\deg p_i(x) = i$, многочлены $p_i(x)$ образуют базис пространства $\mathbf{R}_n[x]$.

Числом $s(n, k)$ Стирлинга¹ первого рода называют коэффициент при степени x^k в многочлене

$$x(x-1)(x-2)\dots[x-(n-1)].$$

Другими словами,

$$x(x-1)(x-2)\dots(x-n+1) = \sum_{k=0}^n s(n, k) \cdot x^k.$$

Поэтому числа Стирлинга первого рода — это коэффициенты при степенях x в многочлене $p_n(x)$.

Непосредственно из определения числа $s(n, k)$ следует, что если $k > n$, то $s(n, k) = 0$. Для любого неотрицательного n число $s(n, n) = 1$, а для положительных n число $s(n, 0) = 0$.

¹ Джеймс Стирлинг (Stirling, 1692—1770) — шотландский математик, член Лондонского королевского общества (с 1729 г.), его основные результаты опубликованы в 1730 г. в работе «Метод разностей».

Из равенств коэффициентов при степенях неизвестного в левой и правой частях равенства

$$p_n(x) = p_{n-1}(x)(x - n + 1)$$

получаются следующие формулы для вычисления чисел Стирлинга первого рода:

$$s(n, k) = s(n-1, k-1) - (n-1) \cdot s(n-1, k).$$

Напомним, что числом Стирлинга второго рода называют число всех разбиений n -элементного множества на k смежных классов.

Число Стирлинга второго рода обозначают символом $S(n, k)$. Числа Стирлинга второго рода для небольших значений n и k можно найти непосредственно по определению, а следующие числа Стирлинга второго рода тоже вычисляются с помощью рекуррентных соотношений:

$$S(n, k) = S(n-1, k-1) + k \cdot S(n-1, k).$$

Из определения чисел Стирлинга первого рода, следует, что $s(n, k)$ — элементы матрицы перехода от базиса $1, p_1(x), p_2(x), \dots, p_n(x)$ к базису $1, x, x^2, \dots, x^n$.

Числа Стирлинга второго рода, наоборот, равны элементам матрицы перехода от базиса x^i к базису $p_i(x)$. Иначе говоря, для каждого $n \geq 0$

$$x^n = \sum_{i=0}^n S(n, i) p_i(x).$$

Итак, числа Стирлинга первого и второго рода являются элементами взаимно обратных матриц, и связь между числами Стирлинга первого и второго рода выражается следующей формулой:

$$\sum_{i=k}^n s(n, i) \cdot S(i, k) = \begin{cases} 1, & \text{если } k = n, \\ 0, & \text{если } k \neq n. \end{cases}$$

Это соотношение, выражающее связь между числами Стирлинга, принято называть свойством ортогональности чисел Стирлинга первого и второго рода.

Под словом «многочлен» будем понимать далее только многочлен положительной степени.

Поле P называется алгебраически замкнутым, если каждый многочлен с коэффициентами из P имеет корень в P .

Если поле P алгебраически замкнуто, то каждый ненулевой многочлен с коэффициентами из P можно представить в виде произведения многочленов первой степени.

Другими словами, над алгебраически замкнутым полем неприводимыми являются лишь многочлены первой степени.

Например, поле рациональных чисел не алгебраически замкнуто: многочлен $x^2 - 2$ не имеет рациональных корней.

Не алгебраически замкнуто и поле действительных чисел.

Отвлечемся на время от числовых полей и посмотрим: может быть, какое-нибудь конечное поле алгебраически замкнуто?

Ни одно из конечных полей не является алгебраически замкнутым, так как над любым конечным полем существуют неприводимые многочлены, степень которых превышает любое наперед заданное натуральное число. Впрочем, чтобы показать незамкнутость конечного поля, достаточно привести пример многочлена степени больше единицы, не имеющего линейного множителя.

Начнем поиск такого многочлена с двухэлементного поля \mathbb{Z}_2 .

Многочлен $x^2 + x + 1$ не имеет корней в поле классов вычетов \mathbb{Z}_2 по модулю 2. Это значит, что поле \mathbb{Z}_2 не алгебраически замкнуто. Посмотрим внимательней на устройство неприводимого многочлена. Многочлен $x^2 + x + 1$ в \mathbb{Z}_2 имеет вид

$$(x-0)(x-1)+1,$$

а элементы 0, 1 исчерпывают все кольцо \mathbb{Z}_2 . Поэтому $x^2 + x + 1$ и не имеет линейных множителей с коэффициентами из этого поля.

Эту идею можно реализовать в любом конечном поле.

Если конечное поле P состоит из q элементов,

$$P = \{a_1, a_2, \dots, a_q\},$$

то многочлен

$$g(x) = (x - a_1)(x - a_2) \dots (x - a_q) + 1$$

степени n не имеет корней в поле P и, следовательно, поле P не является алгебраически замкнутым.

Многочлен, корнями которого являются все элементы конечного поля, можно построить еще проще.

Ненулевые элементы группы образуют группу по умножению. Порядок этой группы равен $q - 1$, и по следствию теоремы Лагранжа каждый ненулевой элемент поля удовлетворяет тождеству $x^{q-1} - 1 = 0$. Но тогда тождеству

$$x(x^{q-1} - 1) = 0$$

удовлетворяет любой элемент поля. Это значит, что многочлен $g(x)$, не имеющий корней в конечном поле, имеет вид

$$g(x) = x^q - x + 1.$$

Итак, ни поле рациональных чисел, ни поле действительных чисел, ни одно конечное поле не является алгебраически замкнутыми.

После таких примеров возникают естественные сомнения: а существуют ли вообще алгебраически замкнутые поля?

Алгебраически замкнутые поля существуют.

Алгебраически замкнутым полем является, например, наибольшее числовое поле — поле комплексных чисел \mathbb{C} .

Иначе говоря, *каждый многочлен с комплексными коэффициентами имеет по крайней мере один корень, принадлежащий полю \mathbb{C} .*

Этот факт вошел в историю науки под названием «Основная теорема алгебры»¹.

Для начала рассмотрим случай, когда корень можно просто вычислить.

Пусть $ax^2 + bx + c$ — многочлен второй степени с комплексными коэффициентами. В вопросе о поисках корня многочлена можно считать коэффициент положительным.

Итак, $a > 0$. Разделим левую и правую части уравнения на a , выделим полный квадрат и представим полученное выражение в виде разности квадратов:

$$ax^2 + bx + c = \left[x + \frac{b}{2a} \right]^2 - \left(\left(\frac{b}{2a} \right)^2 - \frac{c}{a} \right) = \left[x + \frac{b}{2a} \right]^2 - \left(\sqrt{\left(\frac{b}{2a} \right)^2 - \frac{c}{a}} \right)^2.$$

Отсюда следует, что уравнение $ax^2 + bx + c = 0$ равносильно совокупности уравнений

$$\begin{cases} x + \frac{b}{2a} - \sqrt{\left(\frac{b}{2a} \right)^2 - \frac{c}{a}} = 0, \\ x + \frac{b}{2a} + \sqrt{\left(\frac{b}{2a} \right)^2 - \frac{c}{a}} = 0. \end{cases}$$

Из этих двух уравнений получаем известные из школьного курса математики формулы

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

В поле комплексных чисел можно извлечь корень любой степени из любого числа, поэтому *квадратный многочлен с комплексными коэффициентами всегда имеет два корня (может быть, кратных).*

¹ Первое безупречное доказательство этого факта принадлежит К. Ф. Гауссу (1799), поэтому иногда утверждение об алгебраической замкнутости поля комплексных чисел называют *теоремой Гаусса*.

Далее мы можем считать, что многочлен

$$f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n,$$

существование корня у которого мы хотим доказать, нормированный и не имеет кратных корней.

Множество корней ненулевого многочлена с коэффициентами из поля конечно. Это значит, что все корни находятся внутри некоторого круга с центром в начале координат.

Радиус этого круга можно оценить (правда, весьма грубо) с помощью коэффициентов многочлена. Пусть

$$M = \max(|a_1|, \dots, |a_{n-1}|, |a_n|).$$

Покажем, что тогда все корни многочлена $f(x)$ лежат внутри круга с центром в точке O и радиусом $r = 1 + M$.

Если $|x| > r$, то

$$\begin{aligned} & |a_1x^{n-1} + \dots + a_{n-1}x + a_n| \leq |a_1x^{n-1}| + \dots + |a_{n-1}x| + |a_n| = \\ & = |a_1| \cdot |x|^{n-1} + \dots + |a_{n-1}| \cdot |x| + |a_n| \leq M \cdot (|x|^{n-1} + |x|^{n-2} + \dots + |x| + 1) = \\ & = M \frac{|x|^n - 1}{|x| - 1} < \frac{M}{|x| - 1} |x|^n < |x|^n. \end{aligned}$$

Из неравенства

$$|x^n| > |a_1x^{n-1} + \dots + a_{n-1}x + a_n|$$

следует, в частности, что для такого x выполняется неравенство $f(x) \neq 0$.

Более того, те же рассуждения показывают, что для любого действительного $k > 0$, если $|x| > 1 + kM$, выполняется неравенство

$$|x^n| > k|a_1x^{n-1} + \dots + a_{n-1}x + a_n|.$$

Проведенное наблюдение называют *леммой о модуле старшего члена*. Эта лемма означает, в частности, что для достаточно больших значений модуля x значение

$$|a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n|$$

будет больше наперед заданного числа.

Кроме того, отношение

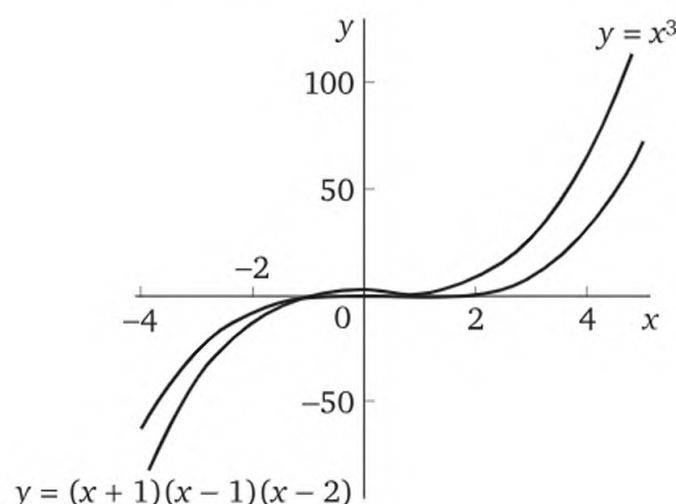
$$\frac{|a_1x^{n-1} + \dots + a_{n-1}x + a_n|}{|x^n|}$$

становится и остается с некоторого места меньше любого положительного числа. Иначе говоря,

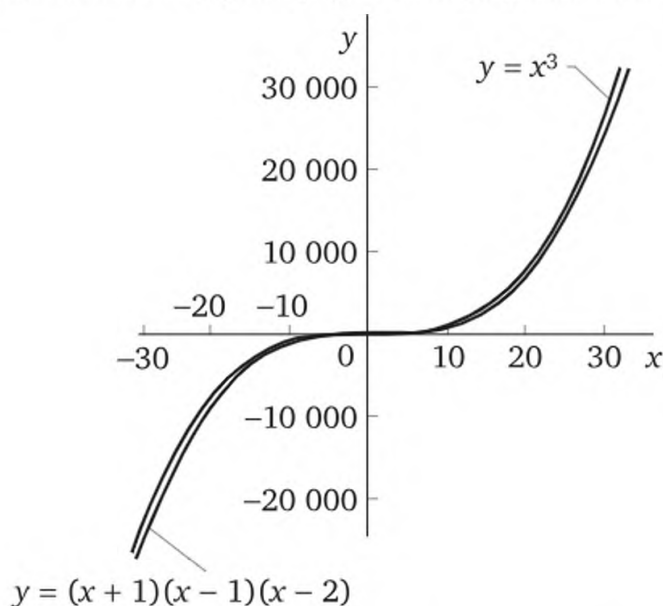
$$\lim_{|x| \rightarrow \infty} \frac{|a_1 x^{n-1} + \dots + a_{n-1} x + a_n|}{|a_0 x^n|} = 0.$$

Это значит, что при неограниченном увеличении модуля аргумента x график функции $y = |f(x)|$ асимптотически приближается к графику $y = |a_0 x^n|$. На рисунках изображены графики функций

$$y = (x+1)(x-1)(x-2) \text{ и } y = x^3.$$



Если на небольшом интервале эти графики еще отчетливо различимы, то при увеличении модуля аргумента графики почти сливаются.



Покажем теперь, что если все коэффициенты многочлена $f(x)$ действительные, то он имеет по крайней мере один комплексный корень.

Если $f(x)$ — многочлен нечетной степени и

$$M = \max(|a_1|, \dots, |a_{n-1}|, |a_n|) + 1,$$

то $f(-M) < 0$, а $f(M) > 0$. Функция $y = f(x)$ непрерывна и, следовательно, в интервале $(-M, M)$ обращается в нуль.

Таким образом, *многочлен нечетной степени с действительными коэффициентами имеет по крайней мере один действительный корень.*

Далее проведем доказательство методом математической индукции, а именно индукцией по степени двойки в разложении числа n — степени многочлена $f(x)$. Коэффициенты $f(x)$ — действительные числа.

Точнее, пусть $n = 2^m q$, где q нечетное, и ведем индукцию по m .

База индукции: $m = 0$, тогда n нечетное и $f(x)$ имеет корень. База доказана.

Шаг индукции. Пусть $m > 0$ и для всех для $m - 1$ утверждение верно.

Воспользуемся тем, что для любого многочлена над любым полем существует поле разложения этого многочлена.

В частности, наш многочлен $f(x)$ имеет n корней x_1, x_2, \dots, x_n , лежащих в некотором расширении P поля \mathbb{C} . Теперь только остается показать, что хотя бы один из этих корней принадлежит полю \mathbb{C} .

Пусть c — произвольное действительное число. Для $i \neq j$ определим

$$y_{ji}(c) = y_{ij}(c) = cx_i x_j + x_i + x_j.$$

Многочлен

$$g(x) = \prod_{1 \leq i < j < n} (x - y_{ij}(c))$$

имеет степень $k = \frac{n(n-1)}{2}$, в каноническое разложение числа k число 2 входит с показателем $m - 1$.

Теперь воспользуемся утверждением, доказательство которого будет приведено в следующей теме: *любое симметрическое выражение от корней многочлена принадлежит полю коэффициентов этого многочлена.*

Коэффициенты многочлена $g(x)$ являются симметрическими (т. е. выдерживающими любые подстановки x_i) выражениями от корней, поэтому коэффициенты $g(x)$ — действительные числа.

По индуктивному предположению имеем, что при любом c из \mathbb{R} многочлен

$$g(x) = \prod_{1 \leq i < j < n} (x - y_{ij}(c))$$

имеет по крайней мере один комплексный корень.

Число корней многочлена $g(x)$ равно k , поэтому среди любых различных $k + 1$ чисел c_1, c_2, \dots, c_{k+1} непременно найдутся два значения числа c (для определенности пусть это будут c_1 и c_2) такие, что $y_{ij}(c_1) = u, y_{ij}(c_2) = v$ — оба комплексные.

Но тогда пара (x_i, x_j) является решением системы уравнений

$$\begin{cases} c_1 x_i x_j + x_i + x_j = u, \\ c_2 x_i x_j + x_i + x_j = v. \end{cases}$$

Решение этой системы сводится к нахождению корней квадратного уравнения с комплексными коэффициентами, а такое уравнение всегда имеет комплексные корни. Следовательно, x_i, x_j принадлежат полю \mathbb{C} .

Шаг индукции доказан. Доказательство утверждения закончено.

Итак, показано, что *многочлен с действительными коэффициентами всегда имеет по крайней мере один комплексный корень.*

Теперь осталось перейти к основному полю, т. е. к полю комплексных чисел. Пусть

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n —$$

многочлен с комплексными коэффициентами. Рассмотрим второй многочлен:

$$f_1(x) = x^n + \bar{a}_1 x^{n-1} + \dots + \bar{a}_{n-1} x + \bar{a}_n,$$

коэффициенты которого комплексно сопряжены с коэффициентами многочлена $f(x)$.

Пусть $s(x) = f(x) \cdot f_1(x)$. Возьмем сопряжение $s(x)$:

$$\begin{aligned} \overline{s(x)} &= (x^n + a_1 x^{n-1} + \dots + a_n)(x^n + \bar{a}_1 x^{n-1} + \dots + \bar{a}_n) = \\ &= (\bar{x}^n + \bar{a}_1 \bar{x}^{n-1} + \dots + \bar{a}_n)(\bar{x}^n + a_1 \bar{x}^{n-1} + \dots + a_n) = s(\bar{x}). \end{aligned}$$

Это значит, что коэффициенты многочлена $s(x)$ совпадают со своими сопряженными и, следовательно, все эти коэффициенты — действительные числа. Любой многочлен с действительными коэффициентами имеет комплексный корень, имеет его и $s(x)$. Пусть x_1 — комплексный корень многочлена $s(x)$.

Поскольку \mathbb{C} — поле, там нет делителей нуля, поэтому из равенства

$$f(x_1) \cdot f_1(x_1) = 0$$

следует $f(x_1) = 0$ или $f_1(x_1) = 0$.

В первом случае цель достигнута.

Если же выпал второй вариант, то возьмем сопряжение левой и правой частей равенства $f_1(x_1) = 0$.

Отображение, переводящее каждое комплексное число в сопряженное, является автоморфизмом поля комплексных чисел, оставляющим поле действительных чисел неподвижным.

Но это значит, что $\overline{f_1(x_1)} = f(\overline{x_1})$ и, следовательно, $f(\overline{x_1}) = 0$.

Итак, в любом случае многочлен с комплексными коэффициентами имеет по крайней мере один комплексный корень.

Поле комплексных чисел алгебраически замкнуто.

В частности, получено полное описание всех неприводимых над полем \mathbf{C} многочленов.

Над полем комплексных чисел неприводимыми являются только многочлены первой степени.

Пусть теперь

$$f(z) = a_0 z^n + a_1 z^{n-1} + \dots + a_{n-1} z + a_n —$$

это многочлен n -й степени с комплексными коэффициентами, т. е. $a_k = u_k + v_k i$ для $k = 0, 1, \dots, n$ и $u_k, v_k \in \mathbf{R}$.

Если комплексное число z имеет вид $z = x + yi$, где x, y — действительные числа, то, подставив в многочлен $f(x)$ вместо коэффициентов a_k и переменного z их выражения в алгебраической форме, после раскрытия скобок и группировки получим алгебраическую форму для $f(z)$:

$$f(z) = U(x, y) + V(x, y) \cdot i,$$

где $U(x, y), V(x, y)$ — многочлены с действительными коэффициентами от переменных x и y .

Многочлены $U(x, y), V(x, y)$ являются непрерывными функциями от двух действительных переменных x, y . Непрерывной функцией будет и функция — модуль многочлена

$$|f(z)| = \sqrt{U^2(x, y) + V^2(x, y)}.$$

Функция $w = f(z)$ обращается в нуль одновременно с функцией $w = |f(z)|$. Последняя является действительной функцией от двух переменных, и ее можно представить наглядно в виде графика.

Основная теорема алгебры имеет наглядную геометрическую интерпретацию; она означает, что если многочлен степени n не имеет кратных корней, то график модуля этого многочлена соприкасается с координатной плоскостью в точности в n точках.

Например, на рисунке изображен фрагмент графика функции

$$w = |0,1z^4 - 0,2i \cdot z + 1|.$$

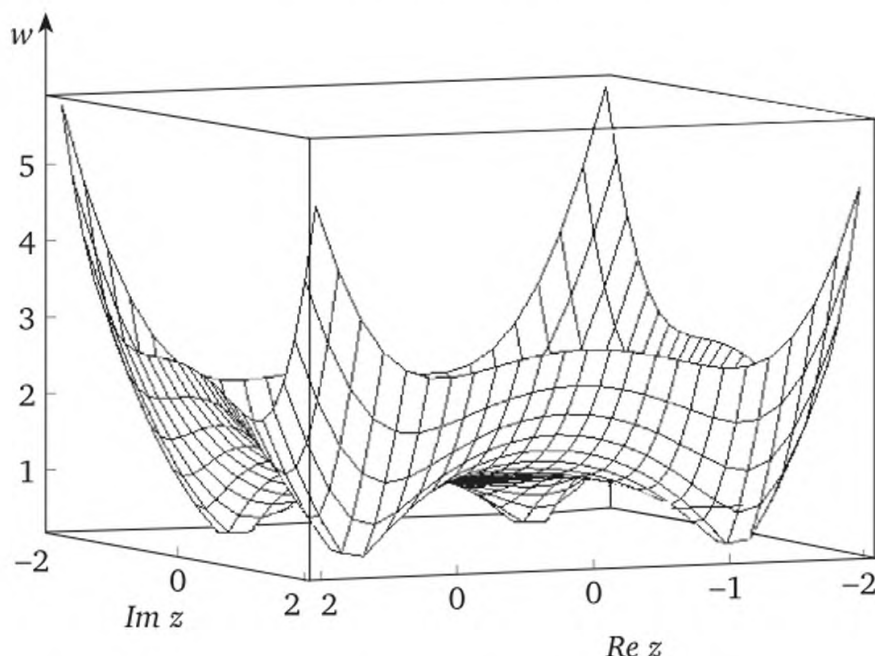
Отметим, что корни многочлена $0,1z^4 - 0,2iz + 1$ приближенно равны:

$$z_1 = 1,410526327 + 1,262336581i;$$

$$z_2 = -1,410526327 + 1,262336581i;$$

$$z_3 = -1,094259005 - 1,262336581i;$$

$$z_4 = 1,094259005 - 1,262336581i.$$



По свисающим вниз четырем выпуклостям графика, касающимся координатной плоскости, видно местонахождение корней многочлена

Лемма о модуле старшего члена многочлена означает, что для каждого положительного числа M существует положительное r такое, что

$$|z| > r \Rightarrow |f(z)| > M.$$

Это значит, что если провести плоскость через точку M на оси Ow параллельно плоскости $\text{Im } z \text{ } O \text{ } \text{Re } z$, то эта плоскость рассекает график $w = |f(z)|$ на две части, причем часть, расположенная вне круга с центром в начале координат и радиусом r , целиком находится выше этой плоскости (и поэтому вне этого круга уж точно не будет касаться координатной плоскости).

То, что оценка эта слишком груба, показывает приведенный графический пример. Все корни рассматриваемого многочлена находятся внутри квадрата

$$-2 < \text{Re } z < 2,$$

$$-2 < \text{Im } z < 2,$$

поэтому вне круга с центром в начале координат и радиусом $2\sqrt{2}$ корней у многочлена нет. «Ловушка для корней», полученная с по-

мощью леммы о модуле старшего члена, значительно больше — это круг, радиус которого больше числа

$$M = \max(|-0,2:0,1|, |1:0,1|) + 1 = \\ = \max(2, 10) + 1 = 11.$$

Приведенное рассуждение является чистым доказательством существования. Лишь утверждение о существовании корня многочлена второй степени было конструктивным — с явным указанием, как можно найти этот корень.

Этот конструктивизм можно продолжить до уравнений третьей и четвертой степеней.

Приведем сначала несколько общих соображений о многочленах с комплексными коэффициентами.

Нахождение корней двучленного уравнения $x^n = g$ называют *извлечением корня n -й степени из g* .

В поле комплексных чисел такая операция для ненулевого g дает n значений, поэтому запись $\sqrt[n]{g}$ обозначает один из этих n корней.

Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n.$$

Говорят, что уравнение $f(x) = 0$ разрешимо в радикалах, если корни многочлена $f(x)$ выражаются через коэффициенты a_0, a_1, \dots, a_n с помощью сложения, умножения, вычитания, деления и извлечения корня.

Например, любое двучленное уравнение разрешимо в радикалах, и, таким образом, существуют разрешимые в радикалах уравнения любой степени. Многочлены первой и второй степеней разрешимы в радикалах. Про первую степень и говорить нечего, а многочлен второй степени $x^2 + bx + c$ сводится к двучленному многочлену с помощью подстановки

$$x = y - \frac{b}{2}.$$

Эта подстановка уничтожает член первой степени, остаются лишь старший и свободный члены, т. е. уравнение становится двучленным.

Аналогично с помощью подстановки

$$x = y - \frac{a_1}{n}$$

многочлен

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n$$

приводится к многочлену

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n$$

не содержащему члена с $(n - 1)$ -й степенью переменного.

Такая подстановка, правда, не делает многочлен степени выше третьей двучленным, однако в дальнейшем для решения вопроса о разрешимости уравнения в радикалах можно считать, что многочлен n -й степени уже преобразован к такому виду, т. е. он не имеет члена с $(n - 1)$ -й степенью переменного.

Для уравнений третьей и четвертой степеней такой договор существенно ускоряет решение.

Итак, возьмем многочлен третьей степени без квадратного члена и соответствующее уравнение

$$x^3 + px + q = 0.$$

Пусть x_0 — корень многочлена, u, w — новые неизвестные, сумма которых равна x_0 , т. е. $x_0 = u + w$ и, следовательно,

$$(u + w)^3 + p(u + w) + q = 0. \quad (*)$$

Равенство $(*)$ накладывает условие лишь на сумму неизвестных. Чтобы найти u, w , нужно второе уравнение. В качестве этого второго уравнения удобно взять

$$3uw + p = 0.$$

Тогда уравнение $(*)$ принимает вид

$$u^3 + w^3 + q = 0,$$

а исходное уравнение становится равносильно системе

$$\begin{cases} u^3 + w^3 = -q, \\ uw = -\frac{p}{3} \end{cases}$$

из двух уравнений с двумя неизвестными.

Систему можно решить, возведя левую и правую части второго уравнения в куб, и получить, таким образом, систему-следствие:

$$\begin{cases} u^3 + w^3 = -q, \\ u^3w^3 = -\frac{p^3}{27}. \end{cases}$$

Нахождение неизвестных u, w теперь сводится к поиску корней кубо-квадратного уравнения:

$$z^6 + qz^3 - \frac{p^3}{27} = 0.$$

Решим это уравнение как квадратное с неизвестным z^3 . Произведя вычисления, получаем: корни многочлена $x^3 + px + q$ выражаются следующей формулой:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \quad (**)$$

Эта формула была опубликована Джироламо Кардано¹ со ссылкой на автора — Тарталью². По традиции, однако, их принято называть не формулами Тартальи, а *формулами Кардано*.

Наличие формулы для вычисления корней означает, в частности, что *любое уравнение третьей степени разрешимо в радикалах*.

После этого принципиального, но теоретического замечания сделаем несколько наблюдений технического характера.

Квадратный радикал в формуле Кардано, взятый сначала со знаком плюс, а потом со знаком минус, — это два квадратных корня из числа

$$\frac{q}{4} + \frac{p^3}{27}.$$

Чтобы получить все корни третьей степени из числа g , можно взять одно из значений $\sqrt[3]{g}$ и умножить его на все корни $\varepsilon_0, \varepsilon_1, \varepsilon_2$ третьей степени из единицы.

Напомним, что на комплексной плоскости числа $\varepsilon_0, \varepsilon_1, \varepsilon_2$ лежат в вершинах правильного треугольника, вписанного в окружность единичного радиуса с центром в начале координат, причем одна из вершин треугольника — единица. Иначе говоря,

$$\varepsilon_0 = 1, \quad \varepsilon_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \quad \varepsilon_2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

Из ненулевого числа извлекаются три различных корня третьей степени, поэтому формула (**) дает девять различных чисел x .

Но многочлен третьей степени имеет лишь три корня (да и то если считать каждый корень столько раз, какова его кратность). Это значит, что формула Кардано неточна: она лишь указывает (со значительным излишеством) множество чисел, среди которых заведомо содержатся корни кубического многочлена.

¹Джироламо Кардано (Cardano, 1501—1576) — итальянский математик, философ и врач. С 1534 г. — профессор медицины в Милане и Болонье. Формула для вычисления корней кубического уравнения опубликована им в 1545 г. в книге «*Artis magna sive de rebus algebraicis liber unus*» («Великое искусство, или об алгебраических вещах в одной книге»).

²Николо Фонтана по прозвищу Тарталья (Tartaglia — Заука, 1500—1557) — итальянский математик, с 1535 г. — профессор математики в Вероне. Формулу для нахождения корней кубического уравнения Тарталья по секрету сообщил Д. Кардано в 1539 г.

Конечно, можно найти все девять чисел и с помощью проверки отсеять лишние, но в таких вычислениях нет необходимости.

Если одно из значений u_0 найдено, то соответствующее ему значение w_0 должно удовлетворять равенству

$$u_0 w_0 = -\frac{p}{3}.$$

Произведение двух различных корней третьей степени из единицы $\varepsilon_i, \varepsilon_j$ (где $i < j$) равно единице тогда и только тогда, когда $i = 1, j = 2$. Поэтому после выбора w_0 этому равенству будут удовлетворять лишь пары

$$u_0 \varepsilon_1, w_0 \varepsilon_2;$$

$$u_0 \varepsilon_2, w_0 \varepsilon_1.$$

После этих уточнений о корнях кубического уравнения можно сказать более определенно: корни многочлена $x^3 + px + q$ выражаются следующими формулами:

$$x_0 = u_0 + w_0;$$

$$x_1 = -\frac{u_0 + w_0}{2} + \frac{(u_0 - w_0)\sqrt{3}}{2}i;$$

$$x_2 = -\frac{u_0 + w_0}{2} - \frac{(u_0 - w_0)\sqrt{3}}{2}i,$$

где u_0 — одно из значений

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \text{ а } w_0 = -\frac{p}{3u_0}.$$

Рассмотрим отдельно случай, когда многочлен третьей степени с рациональными коэффициентами имеет рациональные корни.

Если коэффициенты p, q рациональные и оба корня (и квадратный, и кубический) извлекаются нацело, то корни многочлена имеют вид

$$x_0 = a;$$

$$x_1 = a + b\sqrt{3}i;$$

$$x_2 = a - b\sqrt{3}i,$$

где a — рациональное число, равное $\frac{u_0 + w_0}{2}$.

Заметим, что многочлен с такими корнями имеет рациональные коэффициенты, причем

$$\frac{q}{4} + \frac{p^3}{27}$$

является квадратом рационального числа, а

$$-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

кубом рационального числа.

Таким образом, при решении кубического уравнения с рациональными коэффициентами по формулам Кардано все извлекаемые корни являются рациональными числами тогда и только тогда, когда корни уравнения имеют вид

$$a, a + b\sqrt{3} \cdot i, a - b\sqrt{3} \cdot i,$$

где a, b — рациональные.

Перейдем к обсуждению уравнений четвертой степени. Для решения вопроса о разрешимости (или неразрешимости) в радикалах уравнения четвертой степени можно сразу считать, что многочлен, стоящий в его левой части, нормирован и не содержит члена с кубом неизвестного, т. е. уравнение имеет вид

$$x^4 + px^2 + qx + r = 0.$$

Многочлен можно попытаться представить в виде разности квадратов

$$x^4 + px^2 + qx + r = (x^2 + u)^2 - (2ux^2 - qx + u^2 - r),$$

где u — вспомогательное неизвестное, причем $u \neq 0$.

Многочлен $2ux^2 - qx + u^2 - r$ с неизвестным x является полным квадратом тогда и только тогда, когда его дискриминант равен нулю:

$$q^2 - 4 \cdot 2u(u^2 - r) = 0.$$

Это уравнение третьей степени с неизвестным u принято называть кубической резольвентой¹ данного уравнения четвертой степени.

Если один из корней резольвенты равен нулю, то в исходном уравнении $q = 0$ и представление его в виде суммы двух квадратов не представляет трудностей:

$$x^4 + px^2 + qx + r = \left(x^2 + \frac{p}{2}\right)^2 - \left(\sqrt{r - \frac{p^2}{4}}\right)^2.$$

¹ От лат. *resolventa* — «разрешающая». Название введено Ж. Л. Лагранжем в 1808 г.

Если же u_0 — ненулевой корень кубической резольвенты, то снова получаем представление исходного уравнения в виде разности двух квадратов:

$$x^4 + px^2 + qx + r = (x^2 + u_0)^2 - \left[\sqrt{2u_0} \left(x - \frac{q}{4u_0} \right) \right]^2.$$

Теперь остается лишь решить совокупность, состоящую из двух квадратных уравнений. Решение уравнения четвертой степени путем сведения его к решению уравнения третьей степени впервые было предложено итальянским математиком Людовико Феррари¹.

Отметим, что если формулами Кардано еще можно как-то воспользоваться для практических вычислений, то окончательные формулы для уравнения четвертой степени совершенно бесполезны для практических вычислений.

Подводя итоги, отметим лишь самое главное: *уравнения третьей и четвертой степеней разрешимы в радикалах.*

Разумеется, в радикалах разрешимы уравнения первой и второй степеней. А вот уравнения пятой степени и выше разрешимы в радикалах не всегда. Разрешимость уравнения зависит от свойств группы автоморфизмов поля, содержащего корни уравнения. Каждый такой автоморфизм должен оставлять поле коэффициентов неподвижным.

Поле \mathbb{C} комплексных чисел алгебраически замкнуто, поэтому многочлен с действительными коэффициентами степени n имеет n комплексных корней, если каждый корень считать столько раз, какова его кратность. Это означает, что многочлен можно представить в виде произведения линейных множителей с коэффициентами из поля \mathbb{C} . Если все эти коэффициенты оказались случайно действительными числами, то мы получим представление многочлена из $\mathbb{R}[x]$ в виде произведения неприводимых множителей из $\mathbb{R}[x]$.

Что делать, если среди множителей оказались многочлены с недействительными коэффициентами? Покажем сначала, что *комплексные корни многочлена с действительными коэффициентами сопряжены.*

Отображение, переводящее каждое комплексное число в комплексно сопряженное, является автоморфизмом поля комплексных чисел, оставляющим подполе действительных чисел неподвижным.

Пусть α — комплексный, но не действительный корень многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n,$$

¹ Людовико Феррари (Ferrari, 1522—1565) — итальянский математик, ученик (в современной терминологии — аспирант) Дж. Кардано. В 1540—1556 гг. заведовал кафедрой математики в Миланском университете, а затем преподавал математику в Болонье. Формулы Феррари были опубликованы вместе с формулами Кардано в книге Дж. Кардано «Великое искусство...».

тогда

$$a_0\alpha^n + a_1\alpha^{n-1} + \dots + a_{n-1}\alpha + a_n = 0.$$

Возьмем сопряжение левой и правой части этого равенства, получим:

$$\overline{a_0\alpha^n + a_1\alpha^{n-1} + \dots + a_{n-1}\alpha + a_n} = 0,$$

откуда

$$a_0\bar{\alpha}^n + a_1\bar{\alpha}^{n-1} + a_{n-1}\bar{\alpha} + a_n = 0.$$

Следовательно, $f(\bar{\alpha}) = 0$.

Теоретически можно ожидать, что, например, один из комплексных корней сопряжен сразу с несколькими другими действительными корнями. Однако в действительности это не так.

Покажем методом математической индукции, а именно индукцией по степени многочлена $f(x)$, что *недействительные корни многочлена положительной степени с действительными коэффициентами можно объединить в пары комплексно сопряженных корней*.

Если $f(x)$ — многочлен первой степени, то у него вообще нет действительных корней. Поэтому база индукции начинается с многочлена второй степени.

База индукции. Степень многочлена $f(x)$ равна двум. У такого многочлена всего два корня, и если они недействительные, то сопряжены. База индукции доказана.

Шаг индукции. Пусть многочлен $f(x)$ с действительными коэффициентами имеет степень $n > 2$. По индуктивному предположению у всех многочленов положительной степени, меньшей n , с действительными коэффициентами недействительные корни распадаются на пары комплексно сопряженных.

Пусть $\alpha = a + bi$ и $\bar{\alpha} = a - bi$ — два комплексных корня многочлена $f(x)$ с действительными коэффициентами ($b \neq 0$, поэтому $\bar{\alpha} \neq \alpha$). По теореме Безу многочлен $f(x)$ делится и на $(x - \alpha)$, и на $(x - \bar{\alpha})$, и, следовательно,

$$f(x) = (x - \alpha)(x - \bar{\alpha})f_1(x).$$

Степень многочлена $f_1(x)$ равна $(n - 2)$, но вдруг среди его коэффициентов попадают недействительные числа.

Покажем, что нет, не попадутся.

Коэффициенты многочлена

$$(x - \alpha)(x - \bar{\alpha}) = x^2 - 2bx + (a^2 + b^2) —$$

действительные числа. Деление многочлена на многочлен осуществляется с помощью полевых операций: сложения, вычитания, ум-

ножения и деления. Поэтому коэффициенты многочлена $f_1(x)$ тоже действительные.

По индуктивному предположению множество всех комплексных корней многочлена $f_1(x)$ распадается на пары комплексно сопряженных корней.

Добавим к этим парам нашу парочку $\bar{\alpha}, \alpha$, получим доказываемое утверждение.

Каждая пара комплексно сопряженных корней дает многочлен второй степени с действительными коэффициентами, делящий многочлен $f(x)$. Каждый «холостяк» — действительный корень β многочлена — предоставляет для $f(x)$ линейный множитель $x - \beta$.

Таким образом, каждый многочлен положительной степени с действительными коэффициентами можно представить в виде произведения многочленов с действительными коэффициентами первой и второй степеней.

Иначе говоря, над полем действительных чисел все многочлены степени выше второй приводимы.

«Спаривание» комплексно сопряженных корней может помочь еще в одном вопросе. Если многочлен

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

не имеет действительных корней, то все его корни комплексные и они разбиваются на пары комплексно сопряженных. Общее число корней многочлена $f(x)$ четно; разделим их на два множества: один класс пусть составит половина корней x_1, x_2, \dots, x_k , а другая половина — $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_k$ — состоит из сопряжений элементов первой. Положим

$$g_1(x) = (x - x_1)(x - x_2)\dots(x - x_k);$$

$$g_2(x) = (x - \bar{x}_1)(x - \bar{x}_2)\dots(x - \bar{x}_k).$$

Тогда

$$f(x) = a_0 \cdot g_1(x) \cdot g_2(x)$$

и многочлены $g_1(x)$ и $g_2(x)$ имеют комплексные коэффициенты, причем коэффициенты при одинаковых степенях x сопряжены. Следовательно, если выделить в многочлене $g_1(x)$ действительную и мнимую части, то соответствующее представление для многочлена $g_2(x)$ получается сопряжением.

Но это означает, что если многочлен

$$f(x) = a_0x^n + \dots + a_{n-1}x + a_n$$

с действительными коэффициентами не имеет действительных корней, то существуют такие многочлены $u(x)$ и $v(x)$ с действительными коэффициентами, что

$$f(x) = a_0[u(x) + i \cdot v(x)] \cdot [u(x) - i \cdot v(x)].$$

Перемножим многочлены в правой части и получим

$$f(x) = a_0(u^2(x) + v^2(x)).$$

Предположим теперь, что наш многочлен положителен при всех действительных значениях аргумента. Тогда коэффициент a_0 его старшего члена больше нуля и, следовательно, $\sqrt{a_0}$ — тоже действительное число.

Это значит, что *каждый* многочлен $f(x)$ с действительными коэффициентами и *положительный* при всех действительных x можно представить в виде суммы квадратов двух многочленов:

$$f(x) = (\sqrt{a_0} \cdot u(x))^2 + (\sqrt{a_0} \cdot v(x))^2.$$

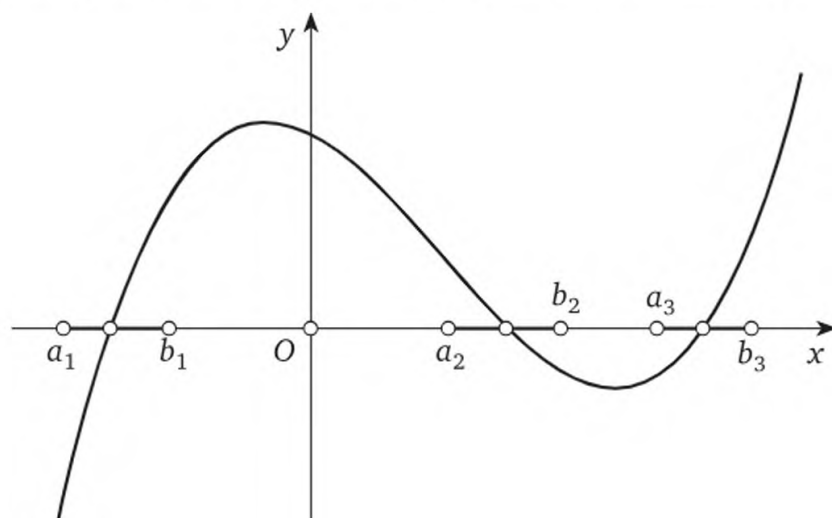
Зная точно, что корни многочлена существуют, попробуем определить круг поиска этих корней. Слово «круг» здесь вовсе не для красного словца, а понимается буквально.

Можно указать на комплексной плоскости круг, содержащий все корни многочлена. Если же указать круги (или прямоугольники), содержащие в точности по одному корню многочлена, то комплексные корни будут отделены (друг от друга).

Пока нас интересуют лишь действительные корни многочлена с действительными коэффициентами.

Если известно, что интервал $[a; b]$ содержит в точности один действительный корень многочлена $f(x)$ с действительными коэффициентами, то вычислить этот корень можно с любой точностью разными способами (например, методом дихотомии — последовательным делением этого интервала пополам). Главное, чтобы корень в интервале был один, т. е. отделен от других корней.

Нахождение отрезков, каждый из которых содержит в точности один корень, называют отделением действительных корней.



Отделение действительных корней

Например, на рисунке изображен график многочлена, имеющего в точности три действительных корня, и корни эти отделены (друг от друга): корень x_i — единственный в отрезке $[a_i, b_i]$, а интервалы

$$(-\infty, a_1), (b_1, a_2), (b_2, a_3), (b_3, +\infty)$$

уже не содержат ни одного корня многочлена, и, таким образом, корни многочлена отделены.

Аналогичную задачу можно поставить и для комплексных корней многочлена с комплексными коэффициентами. Отделение корней будет состоять в нахождение кругов на комплексной плоскости, каждый из которых содержит в точности один корень.

Образно говоря, отделение корней — это предоставление каждому корню отдельной квартиры; квартира комплексного корня — это круг или прямоугольник на координированной комплексной плоскости, а квартира действительного корня — это отрезок на оси.

Для начала заметим, что общая (коммунальная) квартира для корней многочлена — это интервал $(-A, A)$, где A — число, превышающее максимальный модуль корня (а если речь идет о комплексных корнях многочлена, то это круг с центром в начале координат и радиусом A).

В соответствии с леммой о модуле старшего члена в качестве числа A для многочлена

$$x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

можно взять число, равное

$$1 + \max\{|a_1|, |a_2|, \dots, |a_n|\}.$$

Этим общим замечанием о местонахождении комплексных корней и ограничимся, сосредоточив далее свое внимание только на действительных корнях многочлена с действительными коэффициентами.

Интервал $(-A, A)$, как правило, слишком велик. Например, если все коэффициенты многочлена $f(x)$ неотрицательны, то ясно, что число нуль является верхней границей корней — ни одно положительное число корнем такого многочлена быть не может, поэтому для поимки корней этого многочлена достаточно половины интервала $(-A, A)$, а именно $(-A, 0)$.

Используя разложение Тейлора для многочлена $f(x)$ по степеням $(x - a)$,

$$f(x) = \sum_{i=0}^n \frac{f^{(i)}(a)}{i!} (x - a)^i,$$

получаем оценку верхней границы положительных корней многочлена.

Число a является верхней границей положительных корней многочлена $f(x)$, если $f(a) > 0$ и $f^{(i)}(a) \geq 0$.

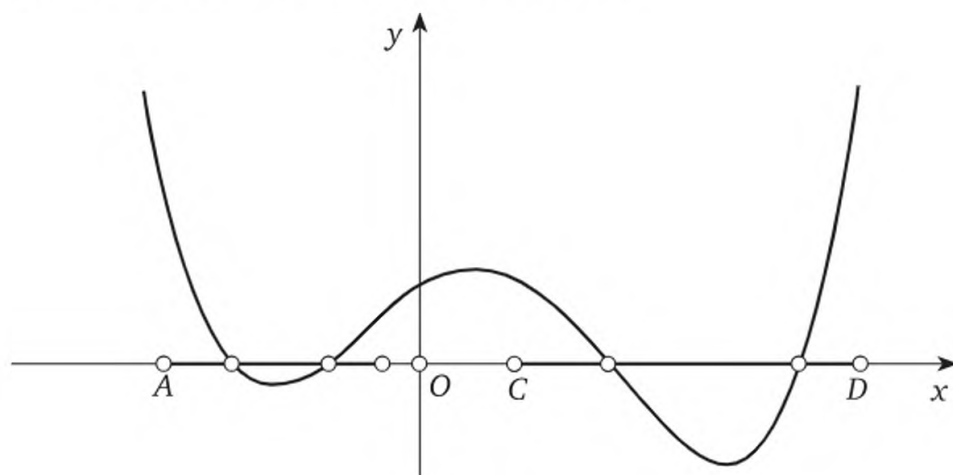
Эту границу впервые нашел еще Исаак Ньютон.

Знак многочлена и его производных в точке a совпадает со знаком коэффициентов разложения по степеням $(x - a)$, поэтому метод Ньютона удобно использовать совместно со схемой Горнера.

Если при делении $f(x)$ на $(x - a)$ все коэффициенты частного и остаток являются неотрицательными числами, то все последующие коэффициенты будут тоже неотрицательные (и в их вычислении уже нет необходимости).

Оценка Ньютона позволяет уточнить лишь верхнюю границу положительных корней (ВГПК) многочлена.

Однако для полноты картины следует найти и нижнюю границу положительных корней (НГПК), а также верхнюю и нижнюю границы отрицательных корней (ВГОК и НГОК).



Верхние и нижние границы корней

На рисунке изображен многочлен $f(x)$, имеющий в точности четыре корня. Точка A является нижней границей отрицательных корней, а точка B — верхней границей положительных корней. Аналогично C — это нижняя, а D — верхняя граница положительных корней многочлена $f(x)$. Для нахождения всех четырех границ корней достаточно уметь находить лишь одну — ВГПК.

Действительно, если многочлен $f(x)$ имеет степень n и M_0 — ВГПК многочлена $f(x)$, M_1 — ВГПК многочлена

$$x^n f\left(\frac{1}{x}\right),$$

M_2 — ВГПК многочлена $f(-x)$, M_3 — ВГПК многочлена

$$x^n f\left(-\frac{1}{x}\right),$$

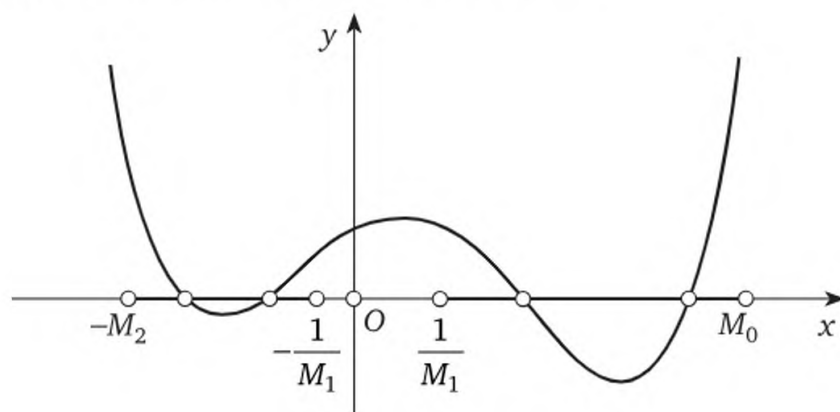
то все отрицательные корни многочлена $f(x)$ принадлежат интервалу

$$\left(-M_2; -\frac{1}{M_1}\right),$$

а все положительные — интервалу

$$\left(\frac{1}{M_1}; M_0\right).$$

В обозначениях предыдущего утверждения число M_2 является нижней границей отрицательных корней, а $-\frac{1}{M_1}$ — их верхней границей. Аналогично к ВГПК (M_0) добавилась нижняя граница положительных корней — число $\frac{1}{M_1}$. Таким образом, с помощью метода Ньютона можно найти верхние и нижние границы и положительных, и отрицательных корней многочлена.



Границы корней

Однако знания верхней и нижней границ положительных и отрицательных корней для вычисления самих корней недостаточно.

Во-первых, наличие границ вовсе не дает гарантии, что корни там вообще есть. Во-вторых, если корней несколько, то для успешного отделения необходимо точно знать, сколько корней многочлена содержится в данном интервале.

Число корней может вовсе не совпадать с числом общих точек графика многочлена и оси абсцисс: у многочлена могут быть и кратные корни.

Впрочем, задача отделения кратных корней многочлена алгоритмически разрешима: разделив многочлен $f(x)$ на наибольший делитель $(f(x), f'(x))$ этого многочлена и его производной, получим многочлен без кратных корней, имеющий то же самое множество корней, что и $f(x)$.

В силу этого замечания можно считать с самого начала, что многочлен не имеет кратных корней и, в частности, что каждая точка пересечения его графика с осью абсцисс изображает в точности один корень.

Сформулируем задачу, которую осталось решить.

Дан многочлен $f(x)$ с действительными коэффициентами без кратных корней, и нам нужно определить, сколько корней этого многочлена содержится в заданном числовом интервале.

Есть несколько способов для решения этой задачи. Самым первым из них был получен метод Штурма¹.

Вычисления методом Штурма используют специальный набор многочленов, полученных из данного многочлена $f(x)$.

Многочлены $f_0(x), f_1(x), \dots, f_m(x)$ из $\mathbf{R}[x]$ образуют систему Штурма, если:

- 1) соседние многочлены не имеют общих корней;
- 2) $f_m(x)$ не имеет действительных корней;
- 3) $\alpha \in \mathbf{R}$ и $f_i(\alpha) = 0$, то $f_{i-1}(\alpha)$ и $f_{i+1}(\alpha)$ имеют разные знаки;
- 4) $\alpha \in \mathbf{R}$ и $f_0(\alpha) = 0$, то произведение $f_0(x) \cdot f_1(x)$ меняет знак с минуса на плюс, когда x , возрастая, проходит через точку α .

После такого неконструктивного определения сразу же возникает вопрос: существует ли для многочлена $f(x)$ хотя бы одна система многочленов Штурма?

Покажем сначала, что *система многочленов Штурма существует для любого многочлена $f(x)$ без кратных корней*.

Пусть $f_0(x) = f(x)$ и $f_1(x) = f'(x)$. Проверим, что свойства многочленов Штурма, в которых участвует $f_1(x)$, выполняются.

Многочлен $f_1(x)$ участвует в первом и последнем свойствах.

Первое свойство: соседние многочлены не имеют общих корней. Если бы многочлены $f_0(x)$ и $f_1(x)$ обладали общим корнем, то это означало бы, что $f(x)$ имеет кратный корень, а по нашему договору это не так.

Рассмотрим четвертое условие. Пусть действительное число α является корнем многочлена $f(x)$, т. е. $f_0(\alpha) = 0$. Невозможность общих корней у соседних многочленов означает, что α не может быть корнем многочлена $f_1(x)$. Это значит, что многочлен $f_1(x)$ в некоторой окрестности точки α сохраняет знак, а многочлен $f_0(x)$ меняет знак.

Если выбрать окрестность достаточно малую, то функция $y = f(x)$ в этой окрестности будет изменяться строго монотонно. Если $y = f(x)$ строго убывает, то она изменяет знак с плюса на минус, а $f_1(x) < 0$. Если $y = f(x)$ строго возрастает, то она изменяет знак с минуса на плюс и $f_1(x) > 0$.

В любом случае четвертое свойство выполняется.

¹ Жак Шарль Франсуа Штурм (Sturm, 1803—1855) — французский математик, иностранный член-корреспондент Петербургской академии наук (1836), учитель гимназии в Женеве до 1830 г.

Построим остальные многочлены Штурма.

Для этого с помощью алгоритма Евклида найдем наибольший общий делитель многочленов $f_0(x)$ и $f_1(x)$.

Поскольку эти многочлены взаимно просты, то последним ненулевым остатком в алгоритме Евклида будет многочлен ненулевой степени, т. е. действительное ненулевое число.

При выполнении алгоритма Евклида можно умножать промежуточные остатки на любое ненулевое число: наибольший общий делитель в результате таких умножений тоже будет умножен на некоторое число, но НОД и определен с точностью до ассоциированности, т. е. с точностью до любого ненулевого числового множителя.

Иначе говоря, промежуточные умножения наибольшего делителя не испортят.

Умножим все промежуточные остатки при нахождении $(f_0(x), f_1(x))$ алгоритмом Евклида на -1 . Таким образом, результаты вычислений будут иметь вид

$$\begin{aligned} f_2(x) &= -\text{Rest}(f_0(x), f_1(x)); \\ f_3(x) &= -\text{Rest}(f_1(x), f_2(x)); \\ &\dots\dots\dots \\ f_i(x) &= -\text{Rest}(f_{i-2}(x), f_{i-1}(x)); \\ &\dots\dots\dots \\ f_{m-1}(x) &= -\text{Rest}(f_{m-3}(x), f_{m-2}(x)); \\ f_m(x) &= -\text{Rest}(f_{m-2}(x), f_{m-1}(x)); \\ f_{m+1}(x) &= -\text{Rest}(f_{m-1}(x), f_m(x)) = 0. \end{aligned} \tag{*}$$

Многочлен $f_m(x)$ в этом ряду имеет нулевую степень, т. е. является ненулевым действительным числом.

Покажем, что многочлены $f_0(x), f_1(x), f_2(x), \dots, f_m(x)$ удовлетворяют всем свойствам системы многочленов Штурма.

Второе свойство многочленов Штурма для наших многочленов выполнено, так как $\deg f_m(x) = 0$.

Свойство многочленов «не иметь общих корней» пока было проверено лишь для $f_0(x)$ и $f_1(x)$. Заметим, что если в вычислениях по алгоритму Евклида для поиска наибольшего общего делителя двух многочленов $f_0(x)$ и $f_1(x)$ удалить часть первых равенств, то оставшиеся вычисления

$$\begin{aligned} f_i(x) &= -\text{Rest}(f_{i-2}(x), f_{i-1}(x)); \\ &\dots\dots\dots \\ f_{m-1}(x) &= -\text{Rest}(f_{m-3}(x), f_{m-2}(x)); \\ f_m(x) &= -\text{Rest}(f_{m-2}(x), f_{m-1}(x)); \\ f_{m+1}(x) &= -\text{Rest}(f_{m-1}(x), f_m(x)) = 0; \\ &\dots\dots\dots \end{aligned}$$

будут представлять собой тоже алгоритм Евклида, но примененный теперь для поиска наибольшего делителя многочленов $f_{i-2}(x)$ и $f_{i-1}(x)$. Окончательным результатом алгоритма будет, естественно, тот же самый многочлен $f_m(x)$, равный наибольшему делителю $(f_0(x), f_1(x))$.

Иначе говоря,

$$(f_0(x), f_1(x)) = (f_{i-1}(x), f_{i-2}(x))$$

для любого $i > 2$. Это означает, что если многочлен $f(x)$ не имеет кратных корней, то многочлены $f_i(x)$ и f_{i+1} из (*) не имеют общих корней для всех $i = 1, 2, \dots, m-1$.

Итак, первые два свойства многочленов Штурма для многочленов, полученных из алгоритма Евклида, примененного к многочлену и его производной (с обращением знаков остатков), выполняются.

Заметим, что обращение знаков остатков пока и не потребовалось: оно нужно лишь для выполнения свойства (3).

Переходим к третьему свойству. Связь между многочленами $f_{i-1}(x)$ и $f_{i+1}(x)$ выражается тождеством

$$f_{i-1}(x) = f_i(x)q(x) - f_{i+1}(x).$$

Подставив вместо x число, являющееся корнем многочлена $f_i(x)$, получим равенство

$$f_{i-1}(x) = -f_{i+1}(x),$$

причем в виду свойства (1) $f_{i-1}(x) \neq 0$ и $f_{i+1}(x) \neq 0$. Третье свойство системы многочленов Штурма доказано.

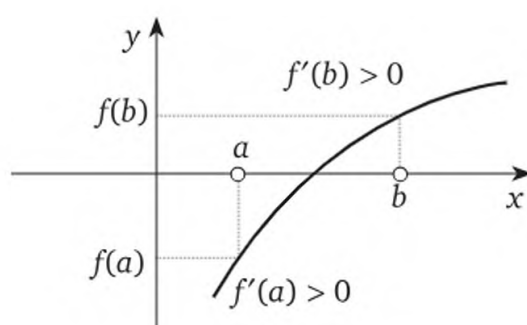
Итак, $f_0(x), f_1(x), \dots, f_m(x)$ образуют систему многочленов Штурма.

Пусть теперь дана конечная система ненулевых действительных чисел a_1, a_2, \dots, a_m . Запишем только знаки этих чисел, т. е. последовательность

$$\varepsilon_1, \varepsilon_2, \dots, \varepsilon_m,$$

где $\varepsilon \in \{+, -\}$. Нас будут интересовать даже не числа и не знаки этих чисел, а лишь смена знаков в последовательности $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_m$, число пар $\varepsilon_i, \varepsilon_{i+1}$, где $\varepsilon_i, \varepsilon_{i+1}$ различны.

Рассмотрим поведение графика многочлена $f(x)$ вблизи его корня. Около корня можно указать такую окрестность: пусть это будет интервал $[a, b]$, в котором наш многочлен будет только убывать или только возрастать, а на концах интервала имеет различные знаки. Напомним, что многочлен $f(x)$ по условию вообще не имеет кратных корней, а касание графика оси абсцисс происходит лишь в случае корня четной кратности.



Прохождение корня на возрастании $f(x)$

Возникают два возможных случая.

Первый случай: многочлен проходит корень при возрастании функции $y = f(x)$.

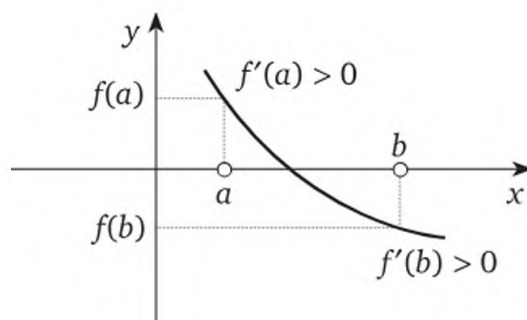
Второй случай: корень появляется при убывании многочлена.

Первый случай. Многочлен $f(x)$ в точке a отрицателен и возрастает, т. е. $f(a) < 0$ и $f'(a) > 0$, в конце интервала многочлен также возрастает, но значение его уже положительно: $f(b) > 0$ и $f'(a) > 0$.

Запишем только знаки этих многочленов $\operatorname{sgn} f(x)$ и $\operatorname{sgn} f'(x)$ для $x = a$, $x = b$. Число смен знаков в точке a обозначим символом $W(a)$, т. е. $W(a) = 1$, а число смен знаков в точке b — соответственно символом $W(b)$, т. е. $W(b) = 0$.

x	$\operatorname{sgn} f(x)$	$\operatorname{sgn} f'(x)$	$W(x)$
a	—	+	1
b	+	+	0

Аналогичная ситуация возникает и тогда, когда функция $y = f(x)$ убывает в окрестности корня.



Прохождение корня на убывании $f(x)$

Тогда ее производная отрицательна, а многочлен меняет знак с плюса на минус. В этом случае:

x	$\operatorname{sgn} f(x)$	$\operatorname{sgn} f'(x)$	$W(x)$
a	+	—	1
b	—	—	0

Итак, мы взяли в интервале $[a, b]$ в точности один корень и видим, что $W(a) > W(b)$ и $W(a) - W(b) = 1$.

Но смена знака у многочлена на концах интервала как раз и сигнализирует о наличии корня в этом интервале. Так что если знак многочлена сменился при прохождении интервала, а знак производной остался прежним, т. е.

$$W(a) - W(b) = 1,$$

то это сигнал о существовании *по крайней мере одного* корня в интервале $[a, b]$.

«По крайней мере один» — это слабо сказано: корней в интервале может оказаться гораздо больше, их может быть любое нечетное число, не превышающее степень многочлена. Иначе говоря, информации о корнях многочлена $f(x)$ из $W(b) - W(a) = 1$ получается мало, но и для ее извлечения используется совсем немного сведений об этом многочлене (да и то, по существу, избыточно — для существования корня достаточно лишь смены знака у самого многочлена). При этом если многочлен $f(x)$ не изменяет знака на концах интервала $[a, b]$, то это еще вовсе не значит, что он не имеет там корней.

Оказывается, что с помощью подсчета смены знаков *во всех* многочленах Штурма в точках a, b можно получить полную информацию о числе корней многочлена $f(x)$, лежащих в интервале (a, b) .

Пусть $f_0(x), f_1(x), \dots, f_m(x)$ — система многочленов Штурма и c — произвольное действительное число. Рассмотрим последовательность

$$f_0(c), f_1(c), \dots, f_m(c).$$

Уберем из нее все нулевые значения, запишем только знаки оставшихся чисел и обозначим символом $W(c)$ число перемен знаков в полученной последовательности плюсов и минусов.

На примере двух многочленов Штурма $f_0(x)$ и $f_1(x)$ мы уже увидели, что если $a < b$, то число потерь знаков уменьшилось, т. е. $W(a) > W(b)$, а число корней многочлена $f(x)$ не меньше $W(a) - W(b)$. Короче говоря, число действительных корней многочлена $f(x)$ в интервале (a, b) не меньше числа потерь перемен знаков при переходе от a к b .

Это свойство функции W сохранится и тогда, когда мы возьмем все многочлены системы Штурма, и именно тогда будет получена точная информация: число потерь перемен знаков при переходе от числа a к числу b равно числу корней многочлена в этом интервале.

Если действительные числа a и b ($a < b$) не являются корнями многочлена $f(x)$ без кратных корней, то число действительных кор-

ней многочлена $f(x)$ в интервале $(a; b)$ равно числу потерь перемен знаков в системе Штурма этого многочлена при переходе от a к b .

Именно этот результат и доказан Ж. Штурмом¹ в 1829 г.

Зная интервалы, содержащие в точности по одному действительному корню многочлена, можно уже с помощью вычислительной техники найти их значения с наперед заданной точностью.

Если мы пожелаем бы найти комплексный корень $a + bi$ многочлена $f(x)$, то, преобразуя $f(a + bi)$ в алгебраическую форму, получили бы два уравнения с действительными коэффициентами: одно — с неизвестным a для поиска действительной части комплексного корня, второе — с неизвестным b для нахождения коэффициента при мнимой части.

В первом и втором уравнениях будут интересны только действительные решения. Таким образом, умения находить действительные корни достаточно для нахождения всех корней многочлена.

Отделив действительные корни, можно сужать их интервалы, делая, таким образом, их «квартиры» все более тесными, а числовые значения корней все более точными.

Аналогичная картина будет и с комплексными корнями.

Отделение комплексных корней будет означать получение каждым корнем отдельного прямоугольника. Уменьшение длины и ширины этого прямоугольника будет, соответственно, давать все более точное значение действительной и мнимой частей комплексного корня многочлена.

Рассмотрим небольшой пример. Применим метод Штурма к многочлену

$$f(x) = x^6 - 3x^5 - 3x^4 + 11x^3 - 3x^2 - 3x + 1.$$

Вычислим производную многочлена, т. е. найдем $f_1(x)$:

$$f_1(x) = f'(x) = 6x^5 - 15x^4 - 12x^3 + 33x^2 - 6x - 3.$$

Поскольку нас будет интересовать лишь смена знаков в системе многочленов Штурма, все промежуточные многочлены можно умножать и делить на любые положительные числа. Разделим $f_1(x)$ на 3, получим:

$$f_1(x) = 2x^5 - 5x^4 - 4x^3 + 11x^2 - 2x - 1.$$

¹ Распространена легенда о том, что Ж. Штурм так гордился своей теоремой, что, начиная ее доказывать, обычно говорил: «А сейчас, господа, докажем теорему, имя которой я имею честь носить». Вторая (и более правдоподобная) история связана с именем французского математика *Эвариста Галуа* (Galois, 1811—1832). В начале 1830 г., когда статья Штурма еще не вышла из печати, Э. Галуа, услышав впервые на учебном занятии формулировку теоремы Штурма, сразу же (на спор с преподавателем) доказал ее.

Аналогично многочлен $f_2(x)$, равный $-\text{Rest}(f_0(x), f_1(x))$, умножим на 4, тогда

$$f_2(x) = 9x^4 - 18x^3 - 3x^2 + 12x - 3.$$

Многочлен $f_3(x)$, умноженный на 3, имеет вид

$$f_3(x) = 16x^3 - 24x^2 + 4,$$

а многочлен $f_4(x)$, умноженный на 8, становится многочленом

$$f_4(x) = 78x^2 - 78x + 15.$$

Многочлен $f_5(x)$ умножим на 13 и получим

$$f_5(x) = 144x - 72.$$

И, наконец, $f_6(x)$ — это положительное число, и можно считать, что $f_6(x) = +1$.

Соберем все многочлены Штурма в таблицу и вычислим перемены знаков при $x = -\infty$, $x = 0$, $x = +\infty$.

Поскольку в бесконечности многочлен ведет себя почти как старший член, для вычисления знаков $x = -\infty$ и $x = +\infty$ достаточно оценить знак старшего члена.

$+\infty$	0	$-\infty$	x
+	+	+	$f(x) = x^6 - 3x^5 - 3x^4 + 11x^3 - 3x^2 - 3x + 1$
+	-	-	$f_1(x) = 2x^5 - 5x^4 - 4x^3 + 11x^2 - 2x - 1$
+	-	+	$f_2(x) = 9x^4 - 18x^3 - 3x^2 + 12x - 3$
+	+	-	$f_3(x) = 16x^3 - 24x^2 + 4$
+	+	+	$f_4(x) = 78x^2 - 78x + 15$
+	-	-	$f_5(x) = 144x - 72$
+	+	+	$f_6(x) = +1$
0	4	6	$W(x)$

Результаты вычислений показывают, что общее число действительных корней

$$W(-\infty) - W(+\infty) = 6 - 0 = 6.$$

Число отрицательных корней

$$W(-\infty) - W(0) = 6 - 4 = 2,$$

а положительных —

$$W(0) - W(+\infty) = 4 - 0 = 4.$$

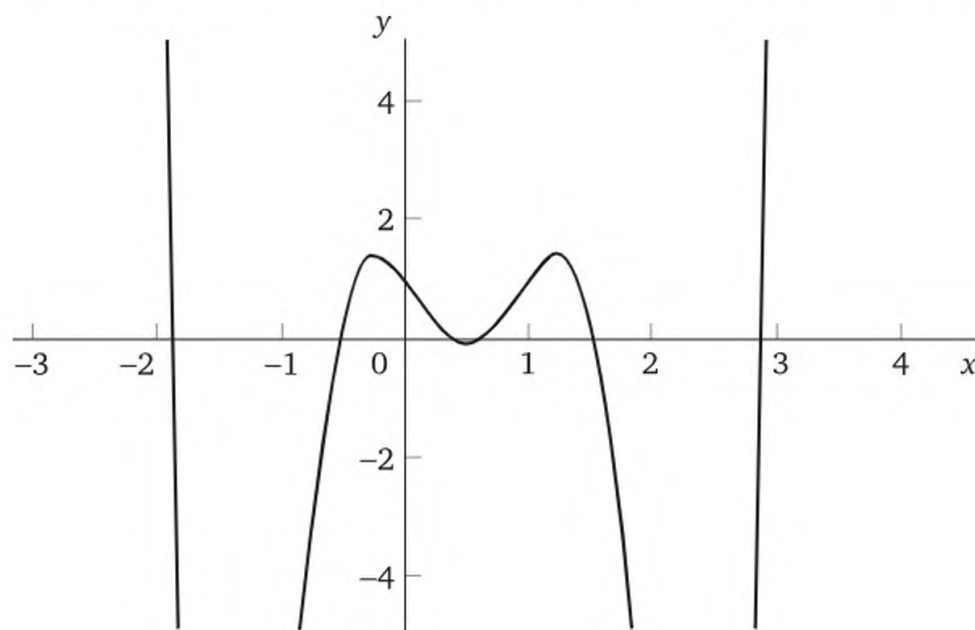
«Бесконечностью» для нашего многочлена является число 12, левее числа -12 корней у этого многочлена нет, как нет их правее $+12$.

Разделив отрезок $(-12; 0)$ пополам, с помощью многочленов Штурма обнаружим, что оба корня находятся в интервале $(-6; 0)$. Повторное деление также не позволит разделить корни. Только подсчет знаков для интервала $(-2; -1)$ дает первое разделение: один отрицательный корень принадлежит интервалу $(-2; -1)$, а второй — интервалу $(-1; 0)$.

Действуя аналогичным образом для положительного направления оси абсцисс, выясняем, что в каждом из интервалов $(1; 2)$ и $(2; 3)$ содержится в точности по одному корню и два корня оказались в отрезке $(0; 1)$. Теперь уже простым делением отрезка $(0; 1)$ пополам, обнаружив смену знака многочлена при прохождении $x = 0,5$, делаем окончательный вывод. Корни многочлена $f(x)$ содержатся по одному в интервалах:

$$(-2; -1); (-1; 0); (0; 0,5); (0,5; 1); (1; 2); (2; 3).$$

Отделение действительных корней закончено. Фрагмент графика функции $y = f(x)$ наглядно подтверждает проведенные вычисления.



$$f(x) = x^6 - 3x^5 - 3x^4 + 11x^3 - 3x^2 - 3x + 1$$

В школьном курсе математики многочлены и их корни рассматриваются над полем действительных чисел. Однако если иррациональные корни для учащихся являются привычными, то появление иррациональных коэффициентов у многочлена, как правило, вызывает внутренний дискомфорт. Иначе говоря, по существу, школьными объектами являются не многочлены из $\mathbf{R}[x]$, а многочлены над полем рациональных чисел.

Теперь рассмотрим задачу разыскания рациональных корней многочлена с целыми коэффициентами. Сначала сделаем замечание о целых корнях.

Все целые корни многочлена с целыми коэффициентами являются делителями свободного члена.

Действительно, если

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

и α — целый корень многочлена $f(x)$, то свободный член является суммой целых чисел, каждое из которых делится на α :

$$a_n = (-a_0\alpha^n) + (-a_1\alpha^{n-1}) + \dots + (-a_{n-1}\alpha).$$

Таким образом, для поиска целых корней многочлена $f(x)$ с целыми коэффициентами можно просто испытать все делители свободного члена многочлена.

Для проверки того, является ли кандидат в корни действительно таковым, удобно использовать схему Горнера. Если число c окажется корнем, то схема Горнера, кроме информации об удаче, предоставит и коэффициенты частного от деления $f(x)$ на $x - c$.

В случае успеха (нахождения корня c) следует этот успех закрепить, расширяя захваченный плацдарм: возможно, что c является k -кратным корнем, тогда степень многочлена $f(x)$ будет понижена до числа $\deg f(x) - k$.

Первыми кандидатами в корни многочлена являются числа 1 и -1 , так как эти числа делят любое целое число.

Если ни $f(1)$, ни $f(-1)$ не равны нулю, то полученные числа можно использовать для предварительного отсеивания кандидатов в корни.

Пусть α — целый корень многочлена $f(x)$. Тогда

$$f(x) = (x - \alpha)q(x),$$

где $q(x)$ — многочлен с целыми коэффициентами. Подставим в оба члена этого равенства вместо x единицу и получим:

$$f(1) = (1 - \alpha)q(1).$$

Отсюда следует, что если α — целый корень многочлена с целыми коэффициентами, то число $\frac{f(1)}{1 - \alpha}$ целое.

Вместо x в равенство можно поставить -1 , и тогда получим, что если α — целый корень многочлена с целыми коэффициентами, то число $\frac{f(-1)}{1 + \alpha}$ целое.

Перейдем теперь к поиску (и отсеvu) рациональных корней многочлена с целыми коэффициентами.

Если несократимая дробь $\frac{p}{q}$ является рациональным корнем многочлена

$$a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

с целыми коэффициентами, то p делит a_n , а q делит a_0 .

Действительно, из равенства

$$a_0p^n + a_1p^{n-1}q + \dots + a_{n-1}pq^{n-1} + a_nq^n = 0$$

следует, что q делит a_0p^n и, следовательно, по теореме Евклида о делимости делит a_0 . По аналогичной причине p делит a_n .

Итак, задача нахождения рациональных корней многочлена с рациональными коэффициентами в принципе решена. Эти корни находятся среди элементов конечного множества, которое легко строится по данному многочлену. Достаточно сделать коэффициенты исследуемого многочлена целыми, а затем перебрать всевозможные варианты числителей и знаменателей — кандидатов в корни — и непосредственным испытанием (например, с помощью схемы Горнера) проверить, кто из кандидатов действительно является корнем. С помощью схемы Горнера определяется и кратность полученного корня.

Если многочлен нормированный, то поиск рациональных корней сводится к поиску лишь целых корней, так как все рациональные корни нормированного многочлена с целыми коэффициентами являются целыми.

Если многочлен ненормированный, т. е. коэффициент a_0 старшего члена отличен от единицы, то вычисления могут и затянуться, особенно если делителей у свободного члена и коэффициента старшего члена оказалось слишком много.

Первыми кандидатами в корни многочлена являются числа 1 и -1 : они делят любое целое число.

В случае удачи (одно из этих чисел или оба оказались корнями), последовательно деля многочлен на $x - 1$ (или $x + 1$), определим кратность корня и одновременно понизим степень исследуемого многочлена.

Если же корнями многочлена являются не только 1 и -1 , то либо в самом начале, либо в ходе вычислений деление на $x - 1$ (или $x + 1$) закончится ненулевым остатком.

Однако эту неудачу легко обратить в полезное улучшение дальнейших вычислений, предлагая последующим кандидатам в корни предварительное и легкое для вычислителя испытание.

Пусть $\frac{p}{q}$ — корень многочлена $f(x)$ степени n , тогда по теореме Безу

$$f(x) = \left(x - \frac{p}{q}\right)g(x),$$

где многочлен $g(x)$ имеет степень $(n - 1)$, а коэффициенты его можно вычислить по схеме Горнера.

При вычислении коэффициентов придется последовательно производить умножение на $\frac{p}{q}$, поэтому все эти коэффициенты, начиная со второго, имеют вид дробей, знаменатели которых являются степенями q . Умножим левую и правую части равенства на число q^n . Тогда все коэффициенты многочлена $q^{n-1} \cdot g(x)$ после раскрытия скобок становятся целыми числами, а равенство принимает вид

$$q^n \cdot f(x) = (xq - p)[q^{n-1} \cdot g(x)]. \quad (*)$$

Подставим в тождество $(*)$ вместо x единицу и получим:

$$q^n \cdot f(1) = (q - p)[q^{n-1} \cdot g(k)].$$

Поскольку q и p взаимно просты, НОД $(q^n, q - p) = 1$. Следовательно, по теореме Евклида о делимости число $f(1)$ делится на $(q - p)$.

Если в тождество $(*)$ вместо x подставить -1 , то получим, что число $p + q$ должно делить $f(-1)$.

Таким образом, если несократимая дробь $\frac{p}{q}$ — рациональный корень многочлена $f(x)$ с целыми коэффициентами, то числа $\frac{f(1)}{p - q}$ и $\frac{f(-1)}{p + q}$ — целые числа.

Полученное свойство является лишь необходимым условием свойства «быть корнем».

Если это условие не выполнено, то претендент в корни точно корнем не будет. Однако выполнение этого условия не дает еще полной гарантии, что корень найден; окончательным решением вопроса будет вычисление значения многочлена в этой точке.

Рассмотрим пример нахождения рациональных корней многочлена. Пусть

$$f(x) = x^5 - 5x^4 + 13x^3 - 22x^2 + 27x - 20.$$

Коэффициент старшего члена у $f(x)$ равен единице, поэтому рациональные корни многочлена целые. Это значит, что в выражении $\frac{p}{q}$ для корня $q = 1$. Числа 1 и -1 не являются корнями $f(x)$:

$$f(1) = -6, \quad f(-1) = -88.$$

Теперь проверим на свойство «быть корнем» числа α из множества

$$\{2, -2, 4, -4, 5, -5, 10, -10, 20, -20\}.$$

Сначала испытаем этих кандидатов на целостность чисел $\frac{f(1)}{\alpha-1}$ и $\frac{f(-1)}{\alpha+1}$.

Результаты испытания оформим в виде таблицы. Если для некоторого α соответствующее число целое, то поставим букву «ц» (целое) и перейдем к следующей проверке этого же α . Если кандидат α проверку не прошел, то ставим букву «н» (не целое), а в графе «Примечание» сразу пишем: «Не корень». Для кандидатов, прошедших обе проверки, пишем в последней графе: «Корень?». С помощью схемы Горнера для таких α ставим окончательный эксперимент.

Заполняем ведомость испытаний:

Кандидат в корни α	$\frac{-6}{\alpha-1}$	$\frac{-88}{\alpha+1}$	Примечание
2	ц	н	Не корень
-2	ц	ц	Корень?
4	ц	н	Не корень
-4	н		Не корень
5	н		Не корень
-5	ц	ц	Корень?
10	н		Не корень
-10	н		Не корень
20	н		Не корень
-20	н		Не корень

Таким образом, лишь два числа (-2 и -5) выдержали «отборочный тур» и допускаются к основному и окончательному экзамену. Однако ни то, ни другое число этот экзамен не выдерживают:

$$f(-2) = -378, \quad f(-5) = -8580.$$

Таким образом, многочлен

$$f(x) = x^5 - 5x^4 + 13x^3 - 22x^2 + 27x - 20$$

рациональных корней не имеет¹.

¹ Над полем рациональных чисел многочлен $f(x)$ имеет разложение $(x^2 - 3x + 4)(x^3 - 2x^2 + 3x - 5)$, и у этого многочлена лишь один действительный корень, приближенно равный 1,843734.

Число возможных кандидатов в корни может оказаться слишком велико, и испытание на принадлежность чисел $\frac{f(1)}{p-q}$ и $\frac{f(-1)}{p+q}$ множеству \mathbb{Z} мало поможет делу.

Однако в действительности роль единицы здесь может выполнять любое целое число k , т. е. в удачу можно превращать любую неудачу с целым кандидатом в корни. Заметим сначала, что если числа p и q взаимно просты, то p не делится на q , т. е. для любого целого числа k выполняется неравенство $p - kq \neq 0$.

Быстрому отбору некорней существенно может помочь следующий факт.

Если несократимая дробь $\frac{p}{q}$ — корень многочлена $f(x)$ с целыми коэффициентами, то для любого целого числа k число $\frac{f(k)}{p - qk}$ целое.

Действительно, если $\frac{p}{q}$ — корень многочлена $f(x)$, то

$$f(x) = \left(x - \frac{p}{q}\right)g(x),$$

где коэффициенты многочлена $g(x)$ — это дроби, знаменатели которых являются степенями q . Умножим левую и правую части равенства на q^n . Тогда

$$q^n \cdot f(x) = (xq - p)q^{n-1} \cdot g(x),$$

где $q^{n-1} \cdot g(x)$ — многочлен с целыми коэффициентами. Подставим в это равенство $x = k$ и получим:

$$q^n \cdot f(k) = (kq - p)[q^{n-1} \cdot g(k)].$$

Любой общий делитель t чисел q^n и $(kq - p)$ делит и число p , а поскольку p и q взаимно просты, то $t = 1$. Это значит, что

$$(q^n, kq - p) = 1.$$

По теореме Евклида о делимости число $f(k)$ делится на $(kq - p)$.

Утверждение доказано; предыдущее замечание — это просто частные случаи последнего наблюдения, а именно для $k = 1$ и $k = -1$.

Нахождение рациональных корней многочлена позволяет найти все его неприводимые множители первой степени.

В поле комплексных чисел нахождение разложения многочлена на произведение неприводимых множителей заканчивалось нахождением линейных множителей.

Разложением на линейные множители над полем комплексных чисел, по существу, решалась задача о разложении многочлена

с действительными коэффициентами над полем действительных чисел.

Однако в отличие от поля комплексных чисел или поля действительных чисел задача разложения многочлена на неприводимые множители над полем рациональных чисел не заканчивается нахождением линейных множителей.

Связь между многочленами с коэффициентами из гауссова кольца и многочленами с коэффициентами из поля частных этого кольца означает, в частности, что многочлен с целыми коэффициентами приводим над полем рациональных чисел тогда и только тогда, когда он приводим над кольцом целых чисел.

Вопрос о неприводимости над кольцом целых чисел решается проще, чем для поля рациональных чисел, хотя бы потому, что для целых чисел есть возможность перехода к конечному гомоморфному образу — кольцу классов вычетов.

Если многочлен

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

приводим над кольцом целых чисел:

$$f(x) = g(x)s(x),$$

то при переходе к кольцу Z_m возникает разложение образа многочлена $f(x)$.

Отсюда следует, что если многочлен $f(x)$ неприводим над некоторым полем Z_p , то его прообраз неприводим над кольцом целых чисел, а следовательно, неприводим и над полем Q .

Заметим сначала, что над любым конечным полем существует бесконечно много неприводимых многочленов. Действительно, если $p_1(x), p_2(x), \dots, p_m(x)$ — все многочлены, неприводимые над полем P , то любой неприводимый множитель многочлена

$$p_1(x)p_2(x)\dots p_m(x) + 1$$

отличен от каждого $p_i(x)$.

Поскольку для фиксированного n над конечным полем существует лишь конечное число многочленов степени $\leq n$, бесконечность множества неприводимых многочленов означает, что степени этих многочленов не ограничены.

Для любого натурального n над полем Z_p , а следовательно, и над полем Q найдется неприводимый многочлен степени, большей числа n .

Впрочем, несложно явно указать неприводимый многочлен, степень которого в точности равна n .

В качестве такого многочлена годится $f(x) = x^n - p$, где p — простое число. Предположим, что, вопреки утверждению, этот многочлен приводим, т. е.

$$f(x) = g_1(x) \cdot g_2(x),$$

где оба многочлена $g_1(x)$, $g_2(x)$ имеют ненулевую степень. Каждый из этих множителей $g_1(x)$, $g_2(x)$ является произведением линейных множителей вида $(x - c_i)$, где c_i — корни n -й степени из p .

Отсюда следует, что модуль свободного члена каждого из множителей имеет вид $\sqrt[n]{p^k}$, где $k < n$.

Все такие числа являются иррациональными.

Этот пример можно значительно обобщить с помощью критерия Эйзенштейна¹.

Пусть многочлен

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

с целыми коэффициентами такой, что все его коэффициенты, кроме первого, делятся на некоторое простое число p , а свободный член (делясь на p) не делится на p^2 . Допустим далее, что этот многочлен приводим над \mathbb{Z} .

От кольца \mathbb{Z} перейдем к кольцу \mathbb{Z}_p и, соответственно, от кольца $\mathbb{Z}[x]$ к $\mathbb{Z}_p[x]$. Многочлен $f(x)$ превратится в многочлен a_0x^n .

Поскольку \mathbb{Z}_p является полем, то кольцо $\mathbb{Z}_p[x]$ гауссово, значит, каждый многочлен из $\mathbb{Z}_p[x]$ имеет единственное представление в виде произведения неприводимых многочленов. Поэтому если многочлен a_0x^n над \mathbb{Z}_p разложим на множители, то эти множители имеют вид bx^k . Свободный член каждого такого многочлена, записанного с целыми коэффициентами, сравним с нулем по модулю p , следовательно, свободный член $f(x)g(x)$ делится на p^2 .

Иначе говоря, многочлен

$$a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

с целыми коэффициентами неприводим над полем рациональных чисел, если существует такое простое число p , что:

- 1) a_0 не делится на p ;
- 2) все остальные коэффициенты делятся на p ;
- 3) a_n не делится на p^2 .

По традиции это достаточное условие неприводимости называют критерием. Из критерия Эйзенштейна снова следует, что над

¹ Фердинанд Готхольд Макс Эйзенштейн (Eisenstein, 1823—1852) — немецкий математик, приват-доцент Берлинского университета (с 1847 г.), член Берлинской академии наук (1852 г.). В 29 лет Эйзенштейн заболел туберкулезом, от которого и умер.

полем рациональных чисел существуют неприводимые многочлены любой степени, например многочлен $x^n + p$, где p — простое число, неприводим над полем \mathbb{Q} для любого натурального n .

Критерий Эйзенштейна не является необходимым условием неприводимости.

Например, неприводимый над полем \mathbb{Q} многочлен $x^2 + 1$ не удовлетворяет условию Эйзенштейна. Правда, заменой переменного x на двучлен $y + 1$ получаем многочлен

$$f(x) = y + 2y + 2.$$

Этот многочлен $f(x)$ уже удовлетворяет условию Эйзенштейна, следовательно, многочлен $f(x)$ неприводим, а значит, неприводим и многочлен $x^2 + 1$.

С помощью таких подстановок можно применить критерий Эйзенштейна и в других случаях.

Например, корни многочлена $x^n - 1$ расположены в вершинах правильного n -угольника, вписанного в окружность с центром в начале координат. Одним из корней является единица, поэтому после деления многочлена $x^n - 1$ на $x - 1$ получим уравнение

$$x^{n-1} + x^{n-2} + \dots + x + 1 = 0,$$

корни которого изображают остальные вершины n -угольника.

Это уравнение называют *уравнением деления круга* (а многочлен в левой части, соответственно, — *многочленом деления круга*).

Непосредственно к многочлену уравнения деления круга критерий Эйзенштейна неприменим, однако многочлен $f(x)$ приводим или неприводим одновременно с многочленом $f(x + 1)$. Используя равенство

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1}$$

и формулу бинома Ньютона

$$(x+1)^p = \sum_{i=0}^n \binom{n}{i} x^i = 1 + px + \frac{p(p-1)}{2} x^2 + \dots + px^{p-1} + x^p,$$

устанавливаем, что для многочлена $f(x)$ условия критерия Эйзенштейна выполнены.

Следовательно, если p — простое число, то многочлен уравнения деления круга

$$x^{p-1} + x^{p-2} + \dots + x + 1$$

неприводим над полем рациональных чисел.

Может появиться подозрение, что на самом деле критерий Эйзенштейна действительно является критерием, только слегка зама-

скированным: если многочлен $f(x)$ неприводим, то для подходящего целого a многочлен $f(x + a)$ уже будет удовлетворять условию критерия Эйзенштейна.

К сожалению, это не так.

Например, к многочлену $f(x) = x^4 - 10x^2 + 1$ непосредственно критерий Эйзенштейна неприменим. Неприменим он к этому $f(x)$ и при любой подстановке $x + a$ вместо x (где a — любое целое число). После такой подстановки свободным членом многочлена останется число 1, которое не делится ни на какое простое число.

И все-таки этот многочлен $f(x)$ неприводим.

Рациональных корней у этого многочлена нет, значит, нет и линейных множителей. Найдем корни этого биквадратного уравнения:

$$x^2 = \sqrt{5 \pm 2\sqrt{6}} = \sqrt{(\sqrt{2} \pm \sqrt{3})^2},$$

откуда

$$x_1 = \sqrt{2} + \sqrt{3}, \quad x_2 = \sqrt{2} - \sqrt{3}, \quad x_3 = -\sqrt{2} - \sqrt{3}, \quad x_4 = -\sqrt{2} + \sqrt{3}.$$

Возможный делитель второй степени имеет вид

$$(x - x_i)(x - x_j),$$

но ни один набор x_i, x_j не дает многочлена с рациональными коэффициентами. Это значит, что многочлен $f(x)$ не имеет множителей ни первой, ни второй степени с рациональными коэффициентами или, короче говоря, *неприводим над полем рациональных чисел*.

Таким образом, *существуют неприводимые над полем рациональных чисел многочлены $f(x)$ с целыми коэффициентами такие, что для любого целого a к многочлену $f(x + a)$ неприменим критерий Эйзенштейна*.

Пусть $f(x)$ — многочлен с рациональными коэффициентами и мы желаем найти его разложение на неприводимые над полем рациональных чисел множители.

Найдем НОД многочлена $f(x)$ и его производной $f'(x)$ и разделим на него данный $f(x)$. Тем самым мы отделим все кратные множители $f(x)$, и полученный многочлен имеет те же самые неприводимые множители, что и $f(x)$: эти множители однократные.

Найдя рациональные корни многочлена (а затем определив их кратности), можно найти все неприводимые множители первой степени данного многочлена. Однако уже поиски неприводимых делителей второй степени могут вызвать затруднения.

Здесь можно попытаться свести задачу к вычислениям в гомоморфных образах.

Доказательство критерия Эйзенштейна, а еще раньше — леммы Гаусса основано на переходе от кольца коэффициентов к его гомоморфному образу.

Точнее говоря, если K_1 — гомоморфный образ кольца K при гомоморфизме φ , то φ можно продолжить до гомоморфизма φ_1 кольца $K[x]$ на кольцо $K_1[x]$. Если в кольце $K[x]$ многочлен раскладывается на множители, то можно попытаться найти такое кольцо K_1 , в котором многочлен будет уже разложим на нетривиальные множители.

Особую ценность представляет случай, когда K_1 — конечное целостное кольцо. Впрочем, все конечные целостные кольца являются полями, так что K_1 в таком случае должно быть полем.

После этого общего замечания вернемся к нашим числовым полям и кольцам.

Рассмотрим в качестве кольца K кольцо целых чисел \mathbb{Z} . Нам уже известно, что вопрос, не является ли данный многочлен с рациональными коэффициентами приводимым над полем рациональных чисел, сводится к вопросу о приводимости над кольцом целых чисел многочлена с целыми коэффициентами.

Если многочлен $f(x)$ приводим, то делитель этого многочлена можно найти простым перебором вариантов (степень делителя — строго меньше степени $f(x)$, а коэффициенты многочлена — целые числа, которые можно предварительно упорядочить, например, по абсолютной величине). Хуже будет, если многочлен неприводим. Тогда поиски делителя таким спросом будут продолжаться вечно и безрезультатно.

Попытаемся свести вопрос о неприводимости такого многочлена над \mathbb{Z} к вопросу о неприводимости его образа над конечным полем.

Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n —$$

многочлен с целыми коэффициентами. Тогда для простого числа p , не делящего a_0 , многочлен

$$F(x) = [a_0]x^n + [a_1]x^{n-1} + \dots + [a_{n-1}]x + [a_n]$$

с коэффициентами из поля \mathbb{Z}_p имеет ту же степень n .

Если $f(x)$ приводим над кольцом \mathbb{Z} , т. е.

$$f(x) = g(x) \cdot s(x),$$

то при переходе к кольцу $\mathbb{Z}_p[x]$ многочлены $g(x)$ и $s(x)$ превратятся в многочлены таких же степеней.

Таким образом, если многочлен $f(x)$ приводим над кольцом целых чисел, то образ этого многочлена $f(x)$ приводим над некоторым кольцом \mathbb{Z}_p .

Если образ $f(x)$ многочлена $f(x)$ с целыми коэффициентами имеет такую же степень, что и $f(x)$, и неприводим в кольце $\mathbb{Z}_p[x]$, то $f(x)$ неприводим над кольцом \mathbb{Z} и, следовательно, над полем \mathbb{Q} .

Итак, для неприводимости многочлена с целыми коэффициентами над полем \mathbb{Q} достаточно, чтобы этот многочлен, сохранив свою степень, оказался неприводимым над некоторым полем классов вычетов \mathbb{Z}_p .

Для любого натурального n в кольце многочленов $\mathbb{Z}_p[x]$ содержится лишь конечное число многочленов степени n . Поэтому неприводимость (как и приводимость) данного многочлена над \mathbb{Z}_p можно проверить с помощью конечного числа испытаний.

Например, многочлен

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

рассматриваемый над полем \mathbb{Z}_2 , не делится ни на один из многочленов:

$$x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1,$$

поэтому он неприводим над \mathbb{Z}_2 . Отсюда следует, что любой многочлен шестой степени с целыми нечетными коэффициентами неприводим над полем рациональных чисел.

Возвращаемся к общей ситуации. Снова многочлен $f(x)$ — это многочлен с целыми коэффициентами степени n , а $f(x)$ — его гомоморфный образ той же степени при переходе от кольца \mathbb{Z} к полю \mathbb{Z}_p .

Если $f(x)$ неприводим, то и $f(x)$ неприводим.

Обратное утверждение неверно: если многочлен $f(x)$ приводим в кольце \mathbb{Z}_p , то его прообраз $f(x)$ может оказаться как приводимым, так и неприводимым над кольцом \mathbb{Z} .

Иначе говоря, если $f(x)$ неприводим над \mathbb{Z} , то его образ $F(x)$ может оказаться приводимым. Однако если образ неприводим, то и $f(x)$ неприводим. Кольца \mathbb{Z}_p конечные, и можно надеяться, что, перебирая различные простые числа p , в случае неприводимости многочлена $f(x)$ через конечное число шагов обнаружим неприводимый $F(x)$. Если бы это было так, то вопрос о неприводимости многочлена с целыми коэффициентами можно было решить простым перебором гомоморфных образов.

К сожалению, это не так — есть многочлены, неприводимые над кольцом \mathbb{Z} , но приводимые над каждым \mathbb{Z}_p .

Рассмотрим пример такого многочлена.

Многочлен

$$f(x) = x^4 - 10x^2 + 1$$

имеет четыре действительных корня:

$$-\sqrt{3}-\sqrt{2}, \sqrt{3}+\sqrt{2}, -\sqrt{3}+\sqrt{2}, \sqrt{3}-\sqrt{2}.$$

Группируя парами множители разложения

$$f(x) = (x + \sqrt{3} + \sqrt{2}) \cdot (x - \sqrt{3} - \sqrt{2}) \cdot (x + \sqrt{3} - \sqrt{2}) \cdot (x - \sqrt{3} + \sqrt{2}),$$

можно представить $f(x)$ в виде произведения многочленов над полями $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ и $\mathbb{Q}[\sqrt{6}]$:

$$f(x) = (x^2 - 2\sqrt{2}x - 1) \cdot (x^2 + 2\sqrt{2}x - 1);$$

$$f(x) = (x^2 - 2\sqrt{3}x + 1) \cdot (x^2 + 2\sqrt{3}x + 1);$$

$$f(x) = (x^2 - 5 - \sqrt{6}) \cdot (x^2 - 5 + \sqrt{6}).$$

Ни одно из этих разложений не является разложением над \mathbb{Q} , так как все уравнения:

$$x^2 = 2, \quad x^2 = 3, \quad x^2 = 6 \text{ —}$$

не имеют решений в поле рациональных чисел.

Таким образом, многочлен

$$f(x) = x^4 - 10x^2 + 1$$

неприводим над полем \mathbb{Q} (и, следовательно, неприводим над кольцом \mathbb{Z}).

Покажем, что для любого простого p этот многочлен приводим в поле классов \mathbb{Z}_p .

Для $p = 2$ многочлен $f(x)$ превращается в приводимый многочлен

$$f(x) = x^4 - 10x^2 + 1 \equiv x^4 + 1 \equiv (x^2 + 1)(x^2 + 1) \pmod{2}.$$

Пусть теперь число p простое нечетное.

Группа \mathbb{Z}_p^* циклическая, порядок ее $(p - 1)$ — число четное. Пусть g — порождающий этой группы, $\mathbb{Z}_p^* = \text{gr}(g)$.

Предположим теперь, что элемент g^k из \mathbb{Z}_p^* является квадратом некоторого элемента u из \mathbb{Z}_p^* , т. е. $u^2 = g^k$. Пусть $u = g^m$, тогда

$$g^{2m} = g^k,$$

следовательно,

$$2m \equiv k \pmod{p-1}.$$

Отсюда следует, что число k четное.

В то же время, если $k = 2s$, то

$$g^k = g^{2s} = (g^s)^2.$$

Итак, в циклической группе $\text{gr}(g)$ четного порядка элемент g^k является квадратом тогда и только тогда, когда k четное.

Предположим, что уравнения $x^2 = a$ и $x^2 = b$ не имеют решения в этой группе. Это значит, что оба эти элемента являются нечетными степенями элемента g . Но тогда элемент ab — это четная степень элемента g , и уравнение $x^2 = ab$ уже имеет решение.

Отсюда, в частности, следует, что по крайней мере одно из трех уравнений:

$$x^2 = 2, \quad x^2 = 3, \quad x^2 = 6 —$$

непрерывно разрешимо в \mathbb{Z}_p (если неразрешимы два первых, то разрешимо третье).

Если x_1 — решение уравнения $x^2 = 2$ в группе \mathbb{Z}_p^* , то многочлен $f(x)$ получает разложение

$$f(x) = (x^2 - 2x_1x - 1) \cdot (x^2 + 2x_1x - 1) \pmod{p}.$$

Если x_2 — решение уравнения $x^2 = 3$ в группе \mathbb{Z}_p^* , то

$$f(x) = (x^2 - 2x_2x + 1) \cdot (x^2 + 2x_2x + 1) \pmod{p}.$$

И, наконец, если x_3 — решение уравнения $x^2 = 6$, то

$$f(x) = (x^2 - 5 - x_3) \cdot (x^2 - 5 + x_3) \pmod{p}.$$

Таким образом, многочлен $f(x) = x^4 - 10x^2 + 1$ приводим над любым полем \mathbb{Z}_p .

Следуя этому образцу, можно построить и бесконечную серию подобных многочленов, но сейчас важен сам печальный факт: существуют многочлены с целыми коэффициентами, неприводимые над полем рациональных чисел, но приводимые над кольцом вычетов \mathbb{Z}_p по любому простому модулю p . Это значит, что простым перебором вариантов с конечными полями задачу о приводимости над \mathbb{Z} данного произвольного многочлена с целыми коэффициентами не решить.

Сделаем замечание общего характера.

Алгебра A называется *финитно аппроксимируемой* относительно некоторого свойства $P(x, y, \dots, z)$ своих элементов, если для каждого элемента x_0, y_0, \dots, z_0 из A , не обладающих свойством P , найдется конечный гомоморфный образ $\varphi(A)$ алгебры A такой, что $\varphi(x_0), \varphi(y_0), \dots, \varphi(z_0)$ продолжают не обладать свойством P и в $\varphi(A)$.

Точнее говоря, для такого φ

$$P(x, y, \dots, z) = \text{Л} \Rightarrow P(\varphi(x_0), \varphi(y_0), \dots, \varphi(z_0)) = \text{Л}.$$

Если конечно определенная алгебра A финитно аппроксимируема относительно некоторого свойства, то проблема распознавания, обладают ли произвольно выбранные элементы этим свойством, алгоритмически разрешима.

Решение задачи о конкретном наборе элементов выглядит так.

Начнем выписывать элементы, не обладающие свойством P , и одновременно строить список элементов, этим свойством обладающих.

Не обладающие свойством элементы находятся в некотором конечном гомоморфном образе этой алгебры. Начнем перечислять гомоморфные образы алгебры A , а в каждом образе — наборы элементов, не обладающих свойством P .

Для элементов, обладающих свойством, можно устроить другой поиск, последовательно выписывая наборы элементов алгебры A , обладающие рассматриваемым нужным свойством.

В зависимости от того, в каком списке окажется интересующий нас данный набор элементов, и будет зависеть решение вопроса, обладают эти элементы свойством P или нет. Такое рассуждение в честь его первооткрывателя принято называть *методом МакКинси*¹.

Если бы кольцо многочленов с целыми коэффициентами было финитно аппроксимируемо *относительно неприводимости*, то задачу разложения на множители можно было бы решить, последовательно перебирая конечные гомоморфные образы кольца коэффициентов.

Существование многочленов, приводимых над любым конечным полем и неприводимых над кольцом целых чисел, означает, что методом МакКинси решить проблему разложения многочлена с целочисленными коэффициентами на множители не удастся.

Но алгоритм распознавания неприводимости над кольцом целых (а следовательно, и над полем рациональных) чисел все-таки существует.

Многочлен с целыми коэффициентами, неприводимый над кольцом целых чисел, неприводим и над полем рациональных чисел. Кроме того, многочлен k -й степени полностью определяется значениями в $(k + 1)$ -й точке.

Используя эти два факта, можно найти не только линейные неприводимые множители многочлена с рациональными коэффициентами.

Метод, по существу, состоит в выявлении кандидатов на такой множитель и последующей проверке. Как и для линейных множителей, подбор кандидатов основан на свойствах делимости целых чисел; поэтому сразу же умножением на общий знаменатель сделаем все коэффициенты исследуемого многочлена целыми числами.

Пусть

$$f(x) = a_0 p^n + a_1 p^{n-1} q + \dots + a_{n-1} p q^{n-1} + a_n q^n —$$

¹ Джеймс Оскар МакКинси (McKinsey, 1889—1937) — американский математик.

многочлен степени n с целочисленными коэффициентами и нам нужно найти многочлен $g(x)$ степени меньше n с целыми коэффициентами, делящий $f(x)$. Если такого $g(x)$ не существует, то многочлен $f(x)$ неприводим.

Если

$$f(x) = g_1(x) \cdot g_2(x),$$

то степень по крайней мере одного из множителей не превышает половины степени многочлена $f(x)$.

Поэтому можно считать, что $\deg g(x) = k \leq \left\lfloor \frac{n}{2} \right\rfloor$, и, таким образом, записать многочлен $g(x)$ с не определенными пока коэффициентами:

$$g(x) = c_0 x^k + c_1 x^{k-1} + \dots + c_{k-1} x + c_k.$$

Кандидаты на роль свободного члена c_k — это делители свободного члена a_n многочлена $f(x)$, а коэффициент старшего члена c_0 должен делить a_0 — коэффициент старшего члена многочлена $f(x)$.

Отметим, что для $k = 1$ именно перебором всех вариантов с последующей проверкой (и некоторыми промежуточными испытаниями) определялись рациональные корни многочлена и, соответственно, линейные множители.

Для нахождения всех $(k + 1)$ коэффициентов многочлена $g(x)$ — возможного делителя многочлена $f(x)$ — нужна система из $(k + 1)$ уравнений.

Возьмем $(k + 1)$ различных целых чисел m_i и подставим каждое из них в исходный многочлен $f(x)$. Поскольку

$$f(m_i) = g(m_i) \cdot q(m_i) —$$

это разложение целого числа $f(m_i)$ в произведение целых множителей, то число $g(m_i)$ является делителем $f(m_i)$.

Выбрав для каждого $i = 1, 2, \dots, k + 1$ по одному из делителей числа $f(m_i)$, получим систему линейных уравнений для нахождения коэффициентов многочлена $g(x)$. Впрочем, коэффициенты многочлена $g(x)$ можно найти и с помощью интерполяционного многочлена Лагранжа. В любом случае, мы получим лишь возможный делитель многочлена $f(x)$.

Действуя так же и далее, обнаружим все возможные варианты значений для c_i , т. е. всех кандидатов в делители исходного многочлена. Затем уже непосредственным делением проверим, какой из полученных многочленов действительно делит $f(x)$.

Если ни один из построенных кандидатов в делители многочлена $f(x)$ делителем все-таки не является, то многочлен $f(x)$ неприводим.

Идея такого способа разложения многочлена над полем \mathbb{Q} на неприводимые множители принадлежит Леопольду Кронекеру¹.

Отметим, что метод Кронекера годится не только для многочленов с целочисленными коэффициентами. По существу, рассуждения Кронекера означают, что алгоритмическая разрешимость задачи разложения на простые множители наследуется при переходе к простому трансцендентному расширению, т. е. если в кольце K алгоритмически разрешима задача разложения на простые множители, то она алгоритмически разрешима и в кольце $K[x]$.

Задача разложения целого числа на множители алгоритмически разрешима. Поэтому задача разложения многочлена с одним переменным и целыми коэффициентами на неприводимые множители алгоритмически разрешима.

Однако разложимость над кольцом целых чисел и разложимость над полем рациональных чисел тесно связаны между собой. Поэтому предыдущее утверждение можно записать иначе: задача разложения многочлена с одним переменным и рациональными коэффициентами на неприводимые множители алгоритмически разрешима.

Рассмотрим пример нахождения методом Кронекера разложения многочлена на неприводимые множители. Пусть

$$f(x) = x^5 - 5x^4 + 13x^3 - 22x^2 + 27x - 20.$$

Этот многочлен нам уже знаком: ранее мы попытались найти рациональные корни $f(x)$, но оказалось, что таких корней у многочлена $f(x)$ нет. Это значит, что у многочлена нет и множителей первой степени.

Еще до поиска рациональных корней было ясно, что если многочлен $f(x)$ приводим, то один из его множителей — обозначим его $g(x)$ — имеет степень не выше второй:

$$g(x) = c_0x^2 + c_1x + c_2.$$

Линейных множителей у многочлена $f(x)$ нет, поэтому если такой $g(x)$ существует, то $\deg g(x) = 2$, т. е. $c_0 \neq 0$. Кроме того, c_0 должен делить коэффициент старшего члена многочлена $f(x)$, следовательно, $c_0 = 1$.

Свободный член c_2 — опять же в предположении существования многочлена $g(x)$ — должен делить число $f(0) = 20$.

Для нахождения c_2 и c_1 придадим переменному x еще одно значение, например $x = 2$. Тогда $g(2)$ должно быть делителем числа $f(2) = -2$.

¹ Цитируемый результат Л. Кронекер опубликовал в 1882 г.

Начинаем перебирать варианты возможных значений $g(0)$ и $g(2)$, т. е. составляем системы уравнений вида

$$\begin{cases} c_2 = a, \\ 4 + 2c_1 + c_2 = b, \end{cases}$$

где $a \in \{1, -1, 2, -2, 4, -4, 5, -5, 10, -10, 20, -20\}$, $b \in \{1, -1, 2, -2\}$. Для каждого решения такой системы составляем многочлен $g(x)$ и делим $f(x)$ на $g(x)$. Если a , принимаяющие последовательно свои значения, соединять с каждым возможным значением b , то на 19-й проверке деление произойдет без остатка, а именно только система

$$\begin{cases} c_2 = 4, \\ 4 + 2c_1 + c_2 = 2, \end{cases} \quad (*)$$

доставляет делитель многочлена $f(x)$. Действительно, решая систему (*), получаем $c_1 = -3$ и, соответственно, многочлен

$$g(x) = x^2 - 3x + 4.$$

Этот $g(x)$ делит многочлен $f(x)$:

$$f(x) = (x^2 - 3x + 4)(x^3 - 2x^2 + 3x - 5).$$

Итак, многочлен $f(x)$ приводим. У него нет линейных множителей, поэтому оба многочлена —

$$x^2 - 3x + 4 \text{ и } x^3 - 2x^2 + 3x - 5$$

неприводимы. Это значит, что получено окончательное разложение многочлена $f(x)$ на неприводимые множители. Этот пример наглядно показывает, что практическая ценность метода Кронекера невелика¹. Можно сказать, что нам еще повезло: многочлен $f(x)$ оказался приводимым, поэтому более половины необходимых проверок не потребовалось.

В случае неприводимости $f(x)$ пришлось бы рассмотреть все 48 вариантов и лишь после последней неудачи сказать: «Многочлен неприводим».

Даже для сравнительно небольших степеней многочлена число проверок может оказаться столь большим, что ручное разложение многочлена на множители (или доказательство его неприводимости) может потребовать нереально большого времени.

К счастью, для вычислительной техники препятствием для вычислений является как раз нереально большая степень многочлена (хотя сами вычисления могут потребовать многочасовой работы).

¹ Метод Кронекера был значительно усовершенствован в 1959 г. русским математиком М. В. Яковкиным.

Например, наш многочлен

$$f(x) = x^5 - 5x^4 + 13x^3 - 22x^2 + 27x - 20$$

компьютер раскладывает на неприводимые множители в доли секунды.

Несколько секунд требуется вычислительной технике, чтобы выяснить, что многочлен

$$x^{1000} - 5x^4 + 13x^3 - 22x^2 + 27x - 20,$$

степень которого в 200 раз больше предыдущего, является неприводимым над полем \mathbb{Q} .

Если 1000 заменить на 10 000 000, то неприводимость многочлена такой степени выяснится через несколько часов работы машины. И лишь степень многочлена, равная 100 000 000, для современной техники слишком большая: компьютер просто отказывается от попытки разложить многочлен такой степени на множители.

Определим кольцо от n переменных x_1, x_2, \dots, x_n с коэффициентами из кольца K по правилу

$$K[x_1, x_2, \dots, x_{n-1}, x_n] = (K[x_1, x_2, \dots, x_{n-1}])[x_n],$$

т. е. взяв в качестве кольца коэффициентов кольцо многочленов от $(n - 1)$ переменного. Используя свойства кольца, можно раскрыть скобки и собрать подобные одночлены.

Это же кольцо называют *кратным трансцендентным расширением кольца K* .

6.5. Многочлены от нескольких переменных

Все свойства кольца, которые сохраняются при присоединении одного переменного, сохраняются и при кратном расширении кольца. В частности, сохраняются свойства целостности, гауссовости и нетеровости.

Другими словами, кольцо многочленов $K[x_1, x_2, \dots, x_n]$ над целостным кольцом K является целостным кольцом; кольцо многочленов $K[x_1, x_2, \dots, x_n]$ над гауссовым кольцом K является гауссовым кольцом; кольцо многочленов $K[x_1, x_2, \dots, x_n]$ над нетеровым кольцом K является нетеровым кольцом.

Последнее означает, что любая система алгебраических уравнений с n неизвестными и коэффициентами из поля равносильна своей конечной подсистеме.

Два многочлена $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$ с коэффициентами из бесконечного целостного кольца равны в функциональном смысле тогда и только тогда, когда они равны в алгебраическом смысле.

Свойства евклидовости и однопорожденности идеалов колец не сохраняются при простом (однократном) трансцендентном расширении кольца. Отсюда следует, что если $n > 1$, то:

1) кольцо многочленов $K[x_1, x_2, \dots, x_n]$ над любым ненулевым кольцом K не является евклидовым кольцом;

2) кольцо многочленов $K[x_1, x_2, \dots, x_n]$ над любым ненулевым кольцом K не является кольцом главных идеалов;

3) не существует алгоритма деления для многочленов от двух и более переменных.

Отметим, что кратное расширение можно получить, не присоединяя один элемент за другим, а присоединив их все сразу. Точнее, кратное трансцендентное расширение кольца K является полугрупповой алгеброй прямого произведения мультипликативно записанных моноидов, изоморфных аддитивному моноиду натуральных чисел.

Такое определение открывает новые возможности. Можно взять прямое произведение любого числа моноидов, считая, что в образовании каждого элемента участвует лишь конечное прямых сомножителей. Поэтому можно говорить о составном трансцендентном расширении $K[M]$ кольца K с помощью переменных из множества M . Если K конечно или счетно, а M бесконечно, то мощность $K[M]$ равна мощности M .

Напомним, что каждое целостное кольцо изоморфно вложено в поле, а каждое поле — в более широкое поле.

Более широкое поле, содержащее поле P , может оказаться изоморфным полю P . Например, если P — это поле рациональных дробей от счетного числа переменных $x_1, x_2, \dots, x_n, \dots$, то поле $P(y)$ изоморфно полю P .

Однако, используя теорему Кантора о неограниченности мощностей, всегда можно указать новое, более широкое поле, существенно отличающееся от исходного. Иначе говоря, *каждое поле изоморфно вложено в неизоморфное ему поле*.

И все-таки важнейшим трансцендентным расширением для нас является случай конечного числа переменных.

Рассмотрим особо и случай конечного кольца коэффициентов.

Если K — конечное целостное кольцо, а $y = f(x_1, x_n, \dots, x_n)$ — функция от n переменных, определенная над K со значениями в K , то $f(x_1, x_n, \dots, x_n)$ является многочленом от n переменных.

Действительно, число различных функций от n переменных, определенных в K со значениями в K , в точности равно числу функций, представимых различными многочленами над K .

Функции от n переменных, определенные над двухэлементным полем Z_2 , со значениями в этом поле принято называть *булевыми функциями*.

Для кольца Z_2 утверждение о представимости любой функции над конечным кольцом в виде многочлена принимает следующий

вид: каждую булеву функцию $y = f(x_1, x_2, \dots, x_n)$ можно представить в виде многочлена с коэффициентами из \mathbb{Z}_2 .

Многочлен, представляющий булеву функцию, в честь его автора называют *полиномом Жегалкина*¹.

Одночлены в многочлене от одной переменной можно упорядочить по возрастанию или убыванию степеней. Для многочлена от нескольких переменных такое упорядочение не годится — в нем может оказаться несколько одночленов одной и той же степени; более того, все одночлены, входящие в многочлен, могут оказаться одной степени. В таком случае многочлен называется *однородным* (или *формой*). Каждый многочлен $f(x_1, x_2, \dots, x_n)$ можно представить в виде суммы форм. Можно упорядочить эти формы, например, по убыванию степеней, однако проблема упорядочения многочленов внутри формы остается.

Упорядочить одночлены можно все сразу, не проводя никаких предварительных упорядочений по форме. Такой порядок — по алфавиту — издавна используется при составлении словарей.

Уточним это понятие.

Пусть M — множество произвольных символов, которые назовем *буквами*, а M , соответственно, — *алфавитом*. Среди символов поместим и символ пробела, например \square . Любую конечную цепочку букв назовем *словом*.

Упорядочение слов в словаре называют *словарным* (или *лексикографическим*²) упорядочением. Текст в словаре идет сверху вниз, одно слово расположено *выше* или *ниже* другого, поэтому словарное упорядочение является упорядочением *по высоте*.

Словарное упорядочение является продолжением упорядочения алфавита. Пусть алфавит $M = \{\square, a, b, c, \dots, d\}$ упорядочен по высоте, причем символ пробела расположен *ниже* всех остальных символов. Возьмем два слова в этом алфавите:

$$U = x_1 x_2 x_3 \dots x_n,$$

$$W = y_1 y_2 y_3 \dots y_m,$$

где $x_i, y_j \in M$.

Слово U в словаре будет расположено *выше* слова W , если

$$x_1 = y_1, x_2 = y_2, \dots, x_{k-1} = y_{k-1},$$

но x_k выше y_k .

¹ Иван Иванович Жегалкин (1869—1947) — русский математик, профессор Московского университета (1902—1911 гг. и с 1917 г.), автор первой русской монографии по теории множеств («Трансфинитные числа», 1907). Представление булевых функций многочленами от n переменных обнаружено им в 1927 г.

² От греч. $\lambda\epsilon\gamma\iota\chi\omicron\varsigma$ — «относящийся к слову» и $\gamma\rho\alpha\phi\omega$ — «пишу».

Таким образом, словарное упорядочение определяется по первым различным символам.

Одночлены от переменных x_1, x_2, \dots, x_n тоже являются словами (с коммутирующими буквами и дополнительной буквой — ненулевым коэффициентом).

Таким образом, слово $U = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ выше слова $W = x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}$, если первое ненулевое число в последовательности

$$\alpha_1 - \beta_1, \alpha_2 - \beta_2, \dots, \alpha_n - \beta_n$$

положительно.

Это действительно упорядочение, т. е. рефлексивное, транзитивное и антисимметричное отношение на множестве слов. Более того, это отношение связно и, следовательно, является отношением *линейного* порядка. Каждая убывающая цепь слов обрывается на конечном шаге, поэтому лексикографический порядок является *вполне упорядочением*.

Иначе говоря, в лексикографическом упорядочении каждое непустое подмножество слов имеет наименьший элемент.

Поскольку словарное упорядочение является линейным порядком, одночлены любого многочлена от нескольких переменных можно единственным образом упорядочить по высоте. Самый первый член такого упорядочения в ненулевом многочлене принято называть *высшим членом многочлена*.

Если в многочлене всего одно переменное, то понятия высшего и старшего членов совпадают. В упорядочении «по возрасту» было свойство, не раз используемое в различных рассуждениях: если кольцо коэффициентов целостное, то старший член произведения многочленов является произведением старших членов.

Это свойство с естественным изменением в терминологии переносится на кольцо многочленов от нескольких переменных над целостным кольцом: высший член произведения многочленов является произведением высших членов.

Действительно, если одночлены многочленов $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$ упорядочены по высоте:

$$f(x_1, x_2, \dots, x_n) = Ax_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} + \dots + Bx_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n} + \dots;$$

$$g(x_1, x_2, \dots, x_n) = Cx_1^{\gamma_1} x_2^{\gamma_2} \dots x_n^{\gamma_n} + \dots + Dx_1^{\delta_1} x_2^{\delta_2} \dots x_n^{\delta_n} + \dots,$$

то одночлен $ACx_1^{\alpha_1+\gamma_1} x_2^{\alpha_2+\gamma_2} \dots x_n^{\alpha_n+\gamma_n}$ будет выше всех остальных членов произведения.

Результатом действия подстановки

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}$$

на многочлен $f(x_1, x_2, \dots, x_n)$ называют многочлен

$$\alpha f(x_1, x_2, \dots, x_n) = f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)}).$$

Говорят, что многочлен f *выдерживает* подстановку α , если $\alpha f = f$.

Если многочлен от n переменных выдерживает *все* подстановки степени n , то этот многочлен называют *симметрическим*. Итак, многочлен $f(x_1, x_2, \dots, x_n)$ симметрический, если для любой подстановки α из S_n

$$f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)}) = f(x_1, x_2, \dots, x_n).$$

Чтобы узнать, является ли данный многочлен от n переменных симметрическим, нет необходимости проверять действие на него каждой из $n!$ подстановок степени n . Поскольку симметрическая группа S_n порождается транспозициями, перемещающими соседние символы, достаточно лишь $(n - 1)$ проверок.

Многочлен $f(x_1, x_2, \dots, x_n)$ является симметрическим, если он выдерживает все транспозиции $(i \ i + 1)$, где $i = 1, 2, \dots, n - 1$.

Однако число испытаний на симметричность можно снизить до двух, так как симметрическая группа S_n порождается всего лишь двумя элементами: $(1 \ 2)$ и $(1 \ 2 \dots n)$.

Таким образом, многочлен $f(x_1, x_2, \dots, x_n)$ является симметрическим, если:

$$f(x_2, x_1, x_3, \dots, x_{n-1}, x_n) = f(x_1, x_2, x_3, \dots, x_{n-1}, x_n);$$

$$f(x_2, x_3, \dots, x_{n-1}, x_n, x_1) = f(x_1, x_2, x_3, \dots, x_{n-1}, x_n).$$

Менее чем двумя проверками для $n > 2$ обойтись нельзя. При $n > 2$ группа S_n нециклическая, поэтому даже если многочлен $f(x_1, x_2, \dots, x_n)$ выдержал какую-нибудь неединичную подстановку, то наверняка найдется подстановка из S_n , которая этот многочлен изменит.

Простейшим симметрическим многочленом будет многочлен, состоящий из одного свободного члена: он, конечно, «выдержит» все подстановки переменных, которых в нем попросту нет.

Рассмотрим менее тривиальный пример, а именно серию симметрических многочленов степеней $1, 2, \dots, n$:

$$\sigma_1(x_1, \dots, x_n) = x_1 + x_2 + \dots + x_n = \sum_{i_1 \leq i_1 \leq n} x_{i_1};$$

$$\sigma_2(x_1, \dots, x_n) = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n = \sum_{1 \leq i_1 < i_2 \leq n} x_{i_1} x_{i_2};$$

$$\sigma_3(x_1, \dots, x_n) = x_1 x_2 x_3 + x_1 x_3 x_4 + \dots + x_{n-2} x_{n-1} x_n = \sum_{1 \leq i_1 < i_2 < i_3 \leq n} x_{i_1} x_{i_2} x_{i_3};$$

.....

$$\sigma_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k};$$

$$\sigma_n(x_1, \dots, x_n) = x_1 x_2 \dots x_n.$$

Многочлены $\sigma_i(x_1, \dots, x_n)$ называют основными (или элементарными, или простейшими) симметрическими многочленами.

Тайна происхождения основных симметрических многочленов (и предпочтение именно этих многочленов, например, суммам i -х степеней переменных) проясняется следующим фактом.

Коэффициенты нормированного многочлена от одной переменной с точностью до знака являются значениями основных симметрических многочленов от корней многочлена.

О «точности до знака» можно сказать точнее.

Знаки значений симметрических многочленов от корней многочлена просто чередуются, а именно: если многочлен

$$x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

имеет корни x_1, x_2, \dots, x_n , где каждый корень считается столько раз, какова его кратность, то:

$$\begin{aligned} a_1 &= -(x_1 + x_2 + \dots + x_n); \\ a_2 &= (x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n); \\ a_3 &= - \sum_{i_1 < i_2 < i_3} x_{i_1} x_{i_2} x_{i_3}; \\ &\dots\dots\dots \\ a_k &= (-1)^k \cdot \sum_{i_1 < i_2 < \dots < i_k} x_{i_1} x_{i_2} \dots x_{i_k}; \\ &\dots\dots\dots \\ a_n &= (-1)^k \cdot x_1 x_2 \dots x_n \end{aligned}$$

или то же самое, но короче:

$$a_k = (-1)^k \cdot \sigma_k(x_1, x_2, \dots, x_n).$$

В честь автора эти формулы называют *формулами Виета*¹.

Для доказательства формул Виета достаточно раскрыть скобки в произведении

$$x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = (x - x_1)(x - x_2) \dots (x - x_n),$$

привести подобные члены и приравнять коэффициенты у одинаковых степеней x у многочленов в левой и правой частях равенства.

¹ Франсуа Виет (Viète, 1540—1603) — французский математик. Разработал почти всю элементарную алгебру и первым ввел буквенные обозначения для коэффициентов в уравнениях. Среди своих алгебраических открытий сам Виет особенно ценил установление зависимости между корнями и коэффициентами уравнений.

Для вопроса о корнях требование нормированности многочлена несущественно — корни многочлена от нормирования не меняются.

Но формулы Виета несложно записать и для произвольного многочлена: корни x_1, x_2, \dots, x_n многочлена

$$a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

(где каждый корень считается столько раз, какова его кратность) связаны следующими соотношениями:

$$\frac{a_k}{a_0} = (-1)^k \cdot \sigma_k(x_1, x_2, \dots, x_n).$$

Если $f(x_1, x_2, \dots, x_m)$ — произвольный многочлен, а $s_i(x_1, x_2, \dots, x_n)$ — симметрические многочлены ($i = 1, 2, \dots, m$), то

$$f(s_1(x_1, x_2, \dots, x_n), s_2(x_1, x_2, \dots, x_n), \dots, s_m(x_1, x_2, \dots, x_n)) —$$

тоже симметрический многочлен. Другими словами, подстановка симметрических многочленов в произвольный многочлен является симметрическим многочленом.

Поскольку нулевой многочлен и многочлен нулевой степени тоже симметрические, это утверждение равносильно тому, что сумма, разность и произведение симметрических многочленов снова являются симметрическими многочленами.

Иначе говоря, множество симметрических многочленов образует подкольцо.

Для изучения объекта в первую очередь полезно найти порождающие элементы.

Подкольцо симметрических многочленов порождается элементарными симметрическими многочленами.

Этот факт носит название *основной теоремы о симметрических многочленах*.

Доказательство основной теоремы можно провести методом математической индукции, а именно индукцией по высоте высшего члена многочлена $f(x_1, x_2, \dots, x_n)$.

Низший возможный член многочлена — это свободный член (равный нулю или ненулевой). В свободном члене вообще нет переменных, поэтому формально он является симметрическим многочленом. База индукции доказана.

Шаг индукции. Симметрический многочлен $f(x_1, x_2, \dots, x_n)$ состоит не из одного свободного члена, и пусть

$$W = Ax_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} —$$

его высший член. По индуктивному предположению для всех симметрических многочленов с высшим членом ниже, чем одночлен W , утверждение теоремы верно.

ном ниже W , следует истинность предложения и для многочлена $f(x_1, x_2, \dots, x_n)$.

Впрочем, то, что цепочка промежуточных многочленов непременно оборвется, можно увидеть и из простых арифметических соображений.

Если многочлен $f_2(x_1, x_2, \dots, x_n)$ состоит не из одного свободного члена, то его высший член имеет вид

$$Bx_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n},$$

где $\alpha_2 \geq \beta_1 \geq \beta_2 \geq \dots \geq \beta_n$.

Таким же свойством будут обладать все высшие члены промежуточных многочленов. Число всевозможных наборов целых неотрицательных чисел $(\gamma_1, \gamma_2, \dots, \gamma_n)$ таких, что

$$\alpha_2 \geq \gamma_2 \geq \gamma_1 \geq \dots \geq \gamma_n,$$

конечно, поэтому через конечное число шагов будет получен многочлен, состоящий из одного свободного члена.

Доказательство основной теоремы подсказывает и алгоритм нахождения конкретного представления симметрического многочлена от основных симметрических многочленов. Выпишем сначала выражения возможных высших членов всех промежуточных многочленов, начиная с данного многочлена $f_2(x_1, x_2, \dots, x_n)$.

В результате мы получим искомого выражения от элементарных симметрических многочленов с пока неопределенными коэффициентами. Найдем эти коэффициенты, придав наборы значений переменным x_1, x_2, \dots, x_n и решив получившуюся систему уравнений.

Симметрический многочлен является суммой однородных симметрических многочленов различных степеней. Однородный от элементарных симметрических многочленов после раскрытия скобок тоже превращается в однородный многочлен.

Поэтому целесообразно искать выражение от элементарных симметрических многочленов для каждого слагаемого отдельно. Для однородного симметрического многочлена степени k возможности для промежуточного высшего члена

$$x_1^{\gamma_1} x_2^{\gamma_2} \dots x_n^{\gamma_n}$$

еще более ограничены. К условию $\alpha_2 \geq \gamma_2 \geq \gamma_1 \geq \dots \geq \gamma_n$ в этом случае добавляется еще одно:

$$\gamma_2 + \gamma_1 + \dots + \gamma_n = k.$$

Рассмотрим пример нахождения представления симметрического многочлена через элементарные симметрические многочлены.

Пусть

$$f(x, y, z) = x^3 + y^3 + z^3.$$

Элементарные симметрические многочлены от трех переменных — это

$$\sigma_1(x, y, z) = x + y + z;$$

$$\sigma_2(x, y, z) = xy + xz + yz;$$

$$\sigma_3(x, y, z) = xyz.$$

Многочлен $f(x, y, z)$ однородный, его высший член — x^3 . Построим сначала последовательности целых неотрицательных — возможных показателей у высших членов, а затем соответствующие одночлены от σ_i .

Оформим эти поиски в виде таблицы.

В первом столбце нам нужен, по существу, лишь один элемент — высший член исходного многочлена. По его системе показателей заполняем второй столбец, а по второму столбцу строим третий.

Высший член от x_i	Показатели высшего члена	Одночлен от σ_i
x^3	3, 0, 0	$A\sigma_1^3\sigma_2^0\sigma_3^0$
	2, 1, 0	$B\sigma_1^2\sigma_2^1\sigma_3^0$
	1, 1, 1	$C\sigma_1^1\sigma_2^1\sigma_3^1$

Итак,

$$x^3 + y^3 + z^3 = A\sigma_1^3 + B\sigma_1^2\sigma_2 + C\sigma_1\sigma_2\sigma_3.$$

Коэффициенты у высших членов совпадают, поэтому $A = 1$. Остается найти коэффициенты B и C . Придадим значения переменным x, y, z и вычислим при этих значениях $\sigma_i(x, y, z)$ и $f(x, y, z)$. Результаты вычислений оформим в виде второй таблицы:

x	y	z	$x + y + z$	$xy + xz + yz$	xyz	$x^3 + y^3 + z^3$
1	1	1	3	3	1	3
1	1	-2	0	-3	-2	-6

В результате получена система уравнений для B и C :

$$\begin{cases} 27 + 9B + C = 3, \\ -2C = -6. \end{cases}$$

Решаем систему $B = 3, C = 3$ и получаем окончательное решение вопроса:

$$x^3 + y^3 + z^3 = \sigma_1^3 - 3\sigma_1^2\sigma_2 + 3\sigma_1\sigma_2\sigma_3.$$

Вернемся к общей картине. На ситуацию с симметрическими многочленами можно взглянуть и с иной точки зрения.

В кольце $K[x_1, x_2, \dots, x_n]$ рассмотрим подкольцо S , порожденное основными симметрическими многочленами σ_i . Основная теорема о симметрических многочленах решает *проблему вхождения* в подкольцо S : многочлен f принадлежит S тогда и только тогда, когда f симметрический. Проверка симметричности состоит в ответе на вопрос, выдерживает или нет многочлен подстановки $(1\ 2)$ и $(1\ 2\ \dots\ n)$.

Кроме ответа на вопрос, входит или нет многочлен в подкольцо S , можно получить и представление этого многочлена в порождающих σ_i .

Если $a\sigma_1\sigma_2\dots\sigma_n$ — одночлен от σ_i , то после замены σ_i многочленами от x_1, x_2, \dots, x_n по показателям степеней x_i в высшем члене полученного многочлена можно однозначно восстановить исходный одночлен $a\sigma_1\sigma_2\dots\sigma_n$. Поэтому ненулевой многочлен $f(\sigma_1, \sigma_2, \dots, \sigma_n)$ остается ненулевым и после замены σ_i на их выражения через x_1, x_2, \dots, x_n .

Отсюда следует, что каждый симметрический от переменных x_i многочлен имеет единственное представление в виде многочлена от σ_i .

Но каждый многочлен $f(x_1, x_2, \dots, x_n)$ также имеет единственное представление от переменных x_i . Отображение $x_i \rightarrow \sigma_i, i = 1, 2, \dots, n$ при неподвижных элементах из K можно продолжить до отображения всего кольца $K[x_1, x_2, \dots, x_n]$ на кольцо $K[\sigma_1, \sigma_2, \dots, \sigma_n]$, причем это отображение взаимно однозначно и сохраняет операции. Иначе говоря, *кольцо симметрических многочленов $K[\sigma_1, \sigma_2, \dots, \sigma_n]$ изоморфно кольцу $K[x_1, x_2, \dots, x_n]$.*

Естественно, что можно взять симметрические многочлены от σ_i , в результате снова получится кольцо, изоморфное исходному кольцу многочленов, и т. д. Таким образом, в кольце многочленов от нескольких переменных содержится бесконечная убывающая цепочка подколец, изоморфных кольцу $K[x_1, x_2, \dots, x_n]$.

Наконец обсудим вопрос, как строить симметрические многочлены.

Пусть $x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ — произвольный одночлен от переменных x_i . *Моногенным* симметрическим многочленом, порожденным одночленом $x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$, (или *орбитой* этого одночлена) называется сумма всех одночленов, полученных из $x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ всеми перестановками переменных. Такой многочлен обозначают символом $S(x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n})$. Например, для $n = 3$

$$S(x_1x_2^2x_3^3) = x_1x_2^2x_3^3 + x_1x_2^3x_3^2 + \\ + x_1^2x_2x_3^3 + x_1^2x_2^3x_3 + x_1^3x_2x_3^2 + x_1^3x_2^3x_3.$$

Число одночленов в моногенном многочлене зависит от числа переменных. Например, если $n = 4$, то

$$S(x_1 x_2^2 x_3^3) = S(x_1 x_2^2 x_3^3 x_4^0)$$

состоит не из шести, а из 24 одночленов. Элементарные симметрические многочлены являются орбитами одночленов вида $x_1 x_2 \dots x_k$,

$$\sigma_k(x_1, x_2, \dots, x_n) = S(x_1 x_2 \dots x_k).$$

Число одночленов в элементарном симметрическом многочлене σ_k равно числу сочетаний из n элементов по k , т. е.

$$\frac{n!}{(n-k)! \cdot k!}.$$

Стоит отметить, что набор простейших симметрических многочленов вовсе не является единственной системой порождающих (вместе с кольцом коэффициентов) подкольца симметрических многочленов. Слово «простейшие» для них на первый взгляд и не подходит.

Первое, что приходит в голову в разговоре о простейших симметрических многочленах, — это орбита $S(f(x))$ простейшего многочлена k -й степени, а таковым является, конечно, многочлен $f(x) = x^k$.

Многочлен

$$S(x_1^k) = x_1^k + x_2^k + \dots + x_n^k$$

называют k -й *степенной суммой* от n переменных.

Степенная сумма

$$s_k = x_1^k + x_2^k + \dots + x_n^k$$

k -й степени является симметрическим многочленом и, следовательно, по основной теореме о симметрических многочленах выражается через простейшие. Сначала можно непосредственно проверить следующие рекуррентные соотношения:

$$\begin{aligned} s_1 &= 1 \cdot \sigma_1; \\ s_2 &= \sigma_1 s_1 - 2\sigma_2; \\ s_3 &= \sigma_1 s_2 - \sigma_2 s_1 + 3\sigma_3; \\ s_4 &= \sigma_1 s_3 - \sigma_2 s_2 + \sigma_3 s_1 - 4\sigma_4; \\ s_5 &= \sigma_1 s_4 - \sigma_2 s_3 + \sigma_3 s_2 - \sigma_4 s_1 + 5\sigma_5; \\ s_6 &= \sigma_1 s_5 - \sigma_2 s_4 + \sigma_3 s_3 - \sigma_4 s_2 + \sigma_5 s_1 - 6\sigma_6; \\ s_7 &= \sigma_1 s_6 - \sigma_2 s_5 + \sigma_3 s_4 - \sigma_4 s_3 + \sigma_5 s_2 - \sigma_6 s_1 + 7\sigma_7; \\ &\dots \end{aligned}$$

Индукцией по k можно проверить эту закономерность в общем виде: для любого натурального $k \leq n$ между простейшими симметрическими многочленами и k -ми степенными суммами от n переменных существует следующая зависимость:

$$s_k = (-1)^{k+1} \cdot \sigma_k + \sum_{i=1}^{k-1} (-1)^{k+1} \sigma_i s_{k-i}.$$

Эти формулы для рекуррентных выражений степенных сумм называют в честь автора *формулами Ньютона*¹.

Из формул Ньютона можно последовательно получить выражения степенных сумм через простейшие симметрические многочлены:

$$\begin{aligned} s_1 &= \sigma_1; \\ s_2 &= \sigma_1^2 - 2\sigma_2; \\ s_3 &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3; \\ s_4 &= \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3 - 4\sigma_4; \\ s_5 &= \sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1\sigma_2^2 + 5\sigma_1^2\sigma_3 - 5\sigma_2\sigma_3 - 5\sigma_1\sigma_4 + 5\sigma_5; \\ &\dots\dots\dots \end{aligned}$$

Впрочем, и без приведенных примеров было ясно, что поскольку степенная сумма является однородным многочленом k -й степени, произвольный одночлен от σ_i , входящий в многочлен, представляющий s_k , будет иметь вид

$$\sigma_1^{\lambda_1} \sigma_2^{\lambda_2} \dots \sigma_n^{\lambda_n},$$

где $1 \cdot \lambda_1 + 2 \cdot \lambda_2 + \dots + n \cdot \lambda_n = k$. Для $i > k$ коэффициентами в таком разложении могут быть только нули. В выражениях для s_1, s_2, s_3, s_4, s_5 действительно содержатся одночлены только такого вида.

Значительно сложнее догадаться о коэффициентах, с которыми эти одночлены входят в формулу для выражения s_k . Впрочем, если знать тайну этих коэффициентов, то, используя формулы Ньютона, уже можно доказать индукцией по k : для любого натурального $k \leq n$ между простейшими симметрическими многочленами и k -ми степенными суммами от n переменных существует следующая зависимость:

$$s_k = \sum_{\lambda_1 + 2\lambda_2 + \dots + k\lambda_k = k} (-1)^{k-(\lambda_1 + \lambda_2 + \dots + \lambda_k)} \frac{k! (\lambda_1 + \lambda_2 + \dots + \lambda_k - 1)!}{\lambda_1! \lambda_2! \dots \lambda_k!} \sigma_1^{\lambda_1} \sigma_2^{\lambda_2} \dots \sigma_k^{\lambda_k}.$$

Приведенную формулу называют *формулой Варинга*².

Если поле коэффициентов P имеет нулевую характеристику, то в этом поле уравнение $px = a$ имеет решение для любого нату-

¹ Формулы Ньютона опубликованы в 1707 г.

² Формулы для выражения s_k содержатся в работе Э. Варинга «Аналитические этюды об алгебраических уравнениях и свойствах кривых» (1762).

рального n и любого элемента a из P . В этом случае формулу Варинга можно записать в следующем виде:

$$\frac{S_k}{k} = \sum_{\lambda_1 + 2\lambda_2 + \dots + k\lambda_k = k} (-1)^{k - (\lambda_1 + \lambda_2 + \dots + \lambda_k)} \frac{(\lambda_1 + \lambda_2 + \dots + \lambda_k - 1)!}{\lambda_1! \lambda_2! \dots \lambda_k!} \sigma_1^{\lambda_1} \sigma_2^{\lambda_2} \dots \sigma_k^{\lambda_k}.$$

Для поля нулевой характеристики с помощью формул Ньютона можно получить выражение простейших симметрических многочленов через степенные суммы s_1, s_2, \dots, s_n :

$$\sigma_1 = s_1;$$

$$\sigma_2 = \frac{1}{2}(s_1\sigma_1 - s_2) = \frac{1}{2}(s_1^2 - s_2);$$

$$\sigma_3 = \frac{1}{3}(s_3 - s_2\sigma_1 + s_1\sigma_2) = \frac{1}{6}(s_1^3 - 3s_1s_2 + 2s_3);$$

$$\dots\dots\dots$$

Проверку можно продолжить и убедиться, что каждый простейший симметрический многочлен можно выразить через первые n степенных сумм.

Но это значит, что первые n степенных сумм вместе с кольцом коэффициентов порождают подкольцо симметрических многочленов: если K — целостное кольцо нулевой характеристики, то

$$K[\sigma_1, \sigma_2, \dots, \sigma_n] = K[s_1, s_2, \dots, s_n].$$

Таким образом, в качестве порождающих элементов подкольца симметрических многочленов можно было взять более естественные на первый взгляд степенные суммы. Однако менее естественные простейшие симметрические многочлены имеют одно неоспоримое преимущество, связанное с их происхождением, т. е. с формулами Виета.

Из основной теоремы о симметрических многочленах и формул Виета получается важное следствие: *симметрическое выражение от корней многочлена принадлежит полю коэффициентов этого многочлена.*

6.6. Дискриминант и результат

Рассмотрим два применения этой теоремы. Оба применения связаны с задачами, уже получившими свое решение (каждый раз с помощью алгоритма Евклида), но новый подход окажется более легко обобщаемым на случай кольца (а не поля) коэффициентов.

Первая задача связана с кратными корнями многочлена, вторая — со взаимной простотой двух многочленов.

Задача о кратных корнях многочлена $f(x)$ с коэффициентами из целостного кольца K характеристики нуль легко решается.

Многочлен $f(x)$ имеет кратные корни тогда и только тогда, когда он не взаимно прост со своей производной. Вычислить наибольший делитель многочлена $f(x)$ и его производной можно в кольце $\bar{K}[x]$ многочленов над \bar{K} — полем частных кольца K .

Есть, однако, и другой путь, известный (в частном случае) даже школьникам. Рассмотрим эту школьную ситуацию подробно.

Пусть

$$f(x) = ax^2 + bx + c —$$

многочлен второй степени. Этот многочлен имеет кратные корни тогда и только тогда, когда его *дискриминант*

$$D = b^2 - 4ac$$

равен нулю.

Утверждение о дискриминанте и кратных корнях квадратного многочлена связано с формулой для нахождения корней этого многочлена. Можно ли так определить понятие дискриминанта для многочлена, степени больше двух, что его свойство (равенство нулю тогда и только тогда, когда многочлен имеет корни) сохранилось? Возникает еще один вопрос: возможно ли это сделать без формулы для нахождения корней?

Сначала рассмотрим ситуацию с многочленом второй степени более тщательно. Пусть x_1, x_2 — корни этого многочлена. Тогда они совпадают тогда и только тогда, когда $x_1 - x_2 = 0$. Выражение $x_1 - x_2$ несимметрично, однако симметрию легко внести, сохранив главное свойство этого выражения. Многочлен $x + bx + c$ имеет кратные корни тогда и только тогда, когда выражение

$$(x_1 - x_2)^2$$

равно нулю. Такое D уже симметрично, поэтому его можно выразить через основные симметрические многочлены, а те, в свою очередь, — через коэффициенты a, b многочлена. Чтобы остаться в кольце (а не в поле) коэффициентов, нужно вспомнить, что в выражении основных симметрических многочленов через корни многочлена будет присутствовать множитель $\frac{1}{a}$.

Наибольшую степень этого множителя здесь видно непосредственно. Эта степень равна двум. Поэтому, чтобы остаться в кольце коэффициентов, следует умножить $(x_1 - x_2)^2$ на a^2 .

Итак,

$$D = a^2 \cdot (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = a^2 \left(\frac{b^2}{a^2} - 4 \frac{c}{a} \right) = b^2 - 4ac.$$

Тайна дискриминанта нормированного многочлена второй степени раскрыта — это просто квадрат разности его корней (с ненулевым множителем, убирающим знаменатели в его выражении через коэффициенты многочлена).

После этого наблюдения несложно обобщить понятие дискриминанта на случай произвольного нормированного многочлена.

Пусть $f(x)$ — многочлен с коэффициентами из целостного кольца K нулевой характеристики:

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a,$$

где $a_0 \neq 0$; x_1, x_2, \dots, x_n — корни этого многочлена. Среди этих корней встретятся равные тогда и только тогда, когда выражение

$$\prod_{1 \leq i < j \leq n} (x_i - x_j)^2$$

равно нулю.

Переменное x_1 входит в это произведение в степени $2n - 2$, поэтому для того, чтобы это произведение осталось в кольце коэффициентов многочлена, достаточно умножить его на a_0^{2n-2} .

Выражение

$$D(f) = a_0^{2n-2} \cdot \prod_{1 \leq i < j \leq n} (x_i - x_j)^2$$

называют *дискриминантом*¹ многочлена $f(x)$.

Понятие дискриминанта введено Джеймсом Сильвестром².

Точно так же, как и в случае квадратного многочлена, $f(x)$ имеет кратные корни тогда и только тогда, когда его дискриминант $D(f)$ равен нулю.

Дискриминант $D(f)$ является симметричным выражением от корней многочлена $f(x)$, поэтому по основной теореме о симметрических многочленах он выражается через основные симметрические многочлены, а те, в свою очередь, выражаются по формулам Виета через коэффициенты многочлена $f(x)$. Иначе говоря, *дискриминант нормированного многочлена принадлежит кольцу коэффициентов этого многочлена*.

С помощью основной теоремы о симметрических многочленах и формул Виета дискриминант многочлена может быть вычислен без нахождения корней многочлена.

Найдем, например, дискриминант нормированного многочлена третьей степени. Если x_1, x_2, x_3 — корни многочлена

$$f(x) = ax^3 + bx^2 + cx + d,$$

¹ От лат. *discriminare* — «разделять, различать».

² Джеймс Джозеф Сильвестр (Sylvester, 1814—1897) — английский математик, иностранный член-корреспондент Петербургской академии наук (с 1872 г.).

то

$$D(f) = a^4 \cdot (x_1 - x_2)^2 \cdot (x_1 - x_3)^2 \cdot (x_2 - x_3)^2.$$

Используя алгоритм нахождения представления симметрического многочлена через основные симметрические многочлены, можно получить выражение D через коэффициенты многочлена. Это выражение и входит составной частью в формулу Кардано.

Дискриминант многочлена $ax^3 + bx^2 + cx + d$ равен

$$b^2c^2 - 4b^3d - 4c^2a + 18abcd - 27a^2d^2.$$

При нахождении корней многочлена n -й степени можно считать, что коэффициент у одночлена x^{n-1} равен нулю. Именно это уравнение рассматривается для нахождения корней методом Кардано. В такой ситуации выражение дискриминанта упрощается (все члены, содержащие коэффициент a , исчезают).

Дискриминант многочлена $x^3 + px + q$ равен

$$-4p^3 - 27q^2.$$

В формуле Кардано выражение под квадратным корнем отличается лишь числовым множителем:

$$-4p^3 - 27q^2 = -108 \left(\frac{q^2}{4} + \frac{p^3}{27} \right).$$

Это значит, что и формулы Кардано в случае нулевого дискриминанта дают, по крайней мере, два равных корня.

Практическое вычисление дискриминанта многочлена степени выше второй можно упростить, используя *определитель Вандермонда*:

$$\Delta = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix} = \prod_{n \geq i > j \geq 1} (x_i - x_j).$$

Определитель не изменяется при транспонировании его матрицы, а это значит, что произведение

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}$$

равно дискриминанту нормированного многочлена.

Если, как обычно, S_k обозначает сумму k -х степеней элементов x_1, x_2, \dots, x_n , то дискриминант равен

$$D = \begin{vmatrix} n & S_1 & \dots & S_{n-1} \\ S_1 & S_2 & \dots & S_n \\ S_2 & S_3 & \dots & S_{n+1} \\ \cdot & \cdot & \cdot & \cdot \\ S_{n-1} & S_n & \dots & S_{2n-2} \end{vmatrix}.$$

Используя формулы для вычисления S_i , теперь можно получить выражение для D .

Напомним, что дискриминант является произведением квадратов. Если $D < 0$, то это значит, что многочлен имеет комплексный (недействительный) корень. Однако многочлен с действительными коэффициентами вместе с комплексным корнем $a + bi$ имеет корнем и сопряженное с корнем число $a - bi$. Кроме того, многочлен имеет нечетную степень, и, следовательно, всегда имеет по крайней мере один действительный корень.

Если дискриминант многочлена третьей степени меньше нуля, то один из корней многочлена действительный, а два — сопряженные комплексные.

Непосредственным вычислением можно поверить, что и обратное утверждение тоже верно: если один из корней многочлена третьей степени действительный, а два — сопряженные комплексные, то дискриминант многочлена отрицательный.

Оба эти утверждения можно собрать вместе: *дискриминант многочлена третьей степени меньше нуля тогда и только тогда, когда один из корней многочлена — действительное число, а два других — сопряженные комплексные.*

Если $D = 0$, то это значит, что многочлен имеет кратные корни. Совпадение двух комплексных (недействительных) корней невозможно: в таком случае общее число корней будет не меньше четырех. Иначе говоря, *если дискриминант многочлена третьей степени равен нулю, то все корни многочлена действительные и по крайней мере два из них совпадают.*

Разумеется, верно и обратное утверждение — равенство двух корней означает, что дискриминант многочлена нулевой.

Таким образом, *дискриминант многочлена третьей степени равен нулю тогда и только тогда, когда все корни многочлена действительные и по крайней мере два из них совпадают.*

Наконец, дискриминант кубического многочлена может оказаться положительным.

Поскольку случаи отрицательного и нулевого дискриминанта рассмотрены полностью, то для положительного D осталась лишь последняя возможность.

Дискриминант многочлена третьей степени больше нуля тогда и только тогда, когда все корни многочлена действительные и различные.

Заметим, что само числовое выражение дискриминанта для получения этих свойств многочлена с действительными коэффициентами и не потребовалось. Однако в частном случае для неполного кубического уравнения зависимость между дискриминантом и корнями многочлена можно было установить из формул Кардано, уже существенно используя выражение для дискриминанта.

Рассмотрим систему алгебраических уравнений с коэффициентами из поля P , т. е. систему

[illegible]

где $f_i(x_1, x_2, \dots, x_n)$ — многочлены, а число m необязательно конечно. Впрочем, теорема Гильберта о базисе (т. е. нетеровость кольца $P[x_1, x_2, \dots, x_n]$) означает, что любая система алгебраических уравнений равносильна своей конечной подсистеме, поэтому m можно всегда считать натуральным числом.

В курсе линейной алгебры уже рассматривался частный случай таких систем, а именно системы линейных уравнений, т. е. случай, когда

$$\deg f_i(x_1, x_2, \dots, x_n) = 1.$$

Основным методом решения произвольной системы линейных уравнений является метод Гаусса, состоящий в последовательном исключении неизвестных.

Метод последовательного исключения неизвестных, с помощью которого решение системы алгебраических уравнений от n неизвестных сводится к решению системы от $n - 1$ одного неизвестного, применим и для произвольной системы алгебраических уравнений.

Чтобы это увидеть, достаточно показать, что систему из двух уравнений с двумя неизвестными

$$\begin{cases} f(x, y) = 0, \\ g(x, y) = 0 \end{cases} \quad (*)$$

МОЖНО СВЕСТИ К РЕШЕНИЮ ОДНОГО УРАВНЕНИЯ С ОДНИМ НЕИЗВЕСТНЫМ.

Поскольку $P[x, y] = (P[x])[y]$, каждый многочлен $s(x, y)$ от переменных x, y является многочленом от y , коэффициенты которого — многочлены от x :

$$s(x, y) = S(y) = c_0(x)y^k + c_1(x)y^{k-1} + \dots + c_k(x).$$

В частности, многочлены из нашей системы имеют такой же вид:

$$\begin{aligned} f(x, y) &= F(y) = a_0(x)y^n + a_1(x)y^{n-1} + \dots + a_n(x); \\ g(x, y) &= G(y) = b_0(x)y^m + b_1(x)y^{m-1} + \dots + c_m(x). \end{aligned}$$

Многочлен $a_0(x)$ ненулевой, поэтому степень многочлена $F(y)$ равна n . Аналогично $b_0(x)$ ненулевой, и степень $G(y)$ равна m .

Поскольку $P[x]$ является лишь кольцом, но не полем, кольцо $(P[x])[y]$ неевклидово: теорема о делении с остатком там не выполняется. Однако она выполняется для нормированного многочлена $G(y)$, а если этот многочлен не нормирован, то для многочленов $[b_0(y)]^{n-m+1}F(y)$ и $G(y)$:

$$[b_0(x)]^{n-m+1}F(y) = G(y)Q(y) + R(y),$$

где $Q(y), R(x) \in (P[x])[y]$ и $\deg R(y) < \deg G(y)$.

Многочлен $R(y)$ выражается через многочлены системы (*):

$$R(y) = [b_0(x)]^{n-m+1}F(y) - G(y)Q(y),$$

значит, $R(y)$ является следствием системы (*). Не все решения уравнения $R(y) = r(x, y)$ являются решениями системы (*): если $b_0(x)$ обращается в нуль, то степень многочлена $F(y)$ на самом деле строго меньше n .

В любом случае решение системы (*) сводится к решению двух систем:

$$\begin{cases} r(x, y) = 0, \\ g(x, y) = 0, \\ b_0(x) \neq 0; \end{cases} \quad (s_1)$$

$$\begin{cases} f(x, y) = 0, \\ b_1(x)y^{m-1} + \dots + b_m(x) = 0, \\ b_0(x) = 0. \end{cases} \quad (s_2)$$

Сумма степеней всех уравнений системы (s_i) по y строго меньше такой же суммы системы (*).

Таким образом, применяя индукцию по степени y , получаем следующее утверждение: *одно из неизвестных в системе, состоящей из двух алгебраических уравнений с двумя неизвестными, можно исключить.*

Теперь индукцией по числу m уравнений получаем: *одно из неизвестных в системе, состоящей из m алгебраических уравнений с двумя неизвестными, можно исключить.*

Рассмотрим два многочлена степени n и m :

$$\begin{aligned} f(x) &= a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n; \\ g(x) &= b_0x^m + b_1x^{m-1} + \dots + b_{m-1}x + b_m. \end{aligned}$$

Для определенности будем считать, что $n \geq m$. Многочлены $f(x)$ и $g(x)$ имеют общий корень тогда и только тогда, когда они не взаимно просты, т. е.

$$\deg(f(x), g(x)) > 0.$$

Кольцо многочленов с коэффициентами из поля является гауссовым, а в каждом гауссовом кольце любая пара элементов a, b обладает НОД (a, b) и НОК $[a, b]$, причем

$$(a, b)[a, b] = ab.$$

Поскольку $\deg f(x) \cdot g(x) = n + m$, а $\deg(f(x), g(x)) > 0$, из равенства

$$(f(x), g(x)) \cdot [f(x), g(x)] = f(x) \cdot g(x)$$

следует: $\deg[f(x), g(x)] < n + m$.

Это значит, что существуют такие многочлены $u(x)$ и $v(x)$ из того же кольца $P[x]$, что

$$[f(x), g(x)] = u(x) \cdot g(x) = v(x) \cdot f(x),$$

причем $\deg u(x) < n$, $\deg v(x) < m$.

Пусть

$$\begin{aligned} u(x) &= c_1 x^{n-1} + c_2 x^{n-2} + \dots + c_{n-1} x + c_n; \\ v(x) &= d_1 x^{m-1} + d_2 x^{m-2} + \dots + d_{m-1} x + d_m. \end{aligned}$$

Равенство

$$u(x)g(x) = v(x) \cdot f(x)$$

означает, что коэффициенты при равных степенях неизвестного в левой и правой частях равенства совпадают.

k	Коэффициент x^k в $v(x) f(x)$	Коэффициент x^k в $u(x) g(x)$
$n + m - 1$	$a_0 d_1$	$b_0 c_1$
$n + m - 2$	$a_1 d_1 + a_0 d_2$	$b_1 c_1 + b_0 c_2$
$n + m - 3$	$a_2 d_1 + a_1 d_2 + a_0 d_3$	$b_2 c_1 + b_1 c_2 + b_0 c_3$
...		
n	$a_n d_1 + a_{n-1} d_1 + \dots + a_{n-m+1} d_m$	$\dots b_m c_{n-m} + \dots + b_0 c_n$
	$a_{n-1} d_1 + \dots + a_{n-m+2} d_m$	$b_m c_{n-m+1} + \dots + b_1 c_n$
...		
1	$a_n d_{m-1} + a_{n-1} d_m$	$b_m c_{n-1} + b_{m+1} c_n$
0	$a_n d_m$	$b_m c_n$

Равенство коэффициентов приводит к системе однородных линейных уравнений с неизвестными, $c_1, c_2, \dots, c_n, d_1, d_2, \dots, d_m$. Коэффициенты в уравнениях при неизвестных расположим в таблице (не выписывая нули).

Неизвестные										
c_1	c_2	c_3	...	c_{n-1}	c_n	d_1	d_2	...	d_{m-1}	d_m
a_0			...			$-b_0$...		
a_1	a_0		...			$-b_1$	$-b_0$...		
...	a_1	a_0	$-b_1$...		
a_{m-1}	...	a_1	...			$-b_{m-1}$		
a_m	a_{m-1}			$-b_m$	$-b_{m-1}$...		
a_{m+1}	a_m	a_{m-1}	...				$-b_m$...		
...	a_{m+1}	a_m		
a_n	...	a_{m+1}		
	a_n		
		a_n	$-b_0$	
			$-b_1$	$-b_0$
			$-b_1$
			$-b_{m-1}$...
			...	a_n	a_{n-1}			...	$-b_m$	$-b_{m-1}$
			...		a_n			...		$-b_m$

Система однородных линейных уравнений имеет ненулевое решение тогда и только тогда, когда ее определитель равен нулю. Матрицу коэффициентов при неизвестных в этой системе «для красоты» можно транспонировать, а затем умножить на число -1 последние n строк. Определитель будет иметь коэффициент $(-1)^n$, который не изменит его равенство (или неравенство) нулю. Итак, многочлены

$$a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n, b_0x^m + b_1x^{m-1} + \dots + b_{m-1}x + b,$$

где a_i, b_i из целостного кольца и a_0 или b_0 отличны от нуля, имеют общий корень тогда и только тогда, когда определитель $(n + m)$ -го порядка

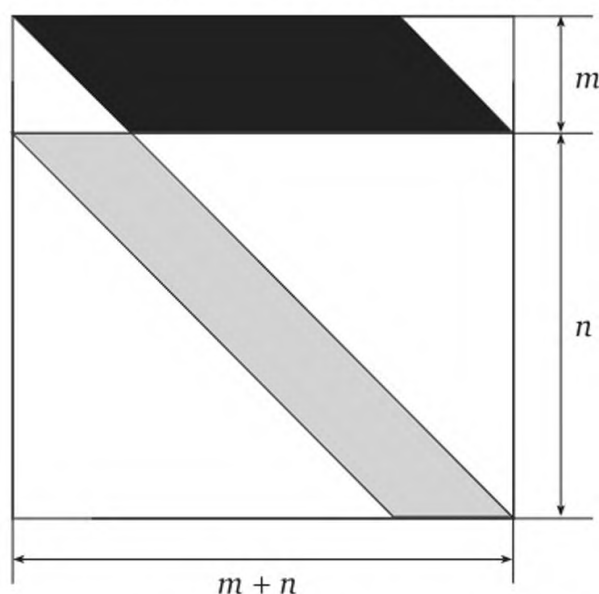
$$\left| \begin{array}{cccccccc}
 a_0 & a_1 & \dots & a_n & 0 & 0 & \dots & 0 \\
 0 & a_0 & a_1 & \dots & a_n & 0 & 0 & \dots & 0 \\
 \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
 0 & 0 & \dots & 0 & a_0 & a_1 & \dots & \dots & a_n \\
 b_0 & b_1 & \dots & \dots & \dots & b_m & 0 & \dots & 0 \\
 0 & b_0 & b_1 & \dots & \dots & \dots & b_m & 0 & \dots & 0 \\
 \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
 0 & 0 & \dots & 0 & b_0 & b_1 & \dots & \dots & \dots & b_m
 \end{array} \right| \left. \begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \end{array} \right\} \begin{array}{l} m \text{ строк} \\ \\ \\ n \text{ строк} \end{array}$$

равен нулю.

Полученный определитель обозначают символом $R(f, g)$ и называют *результантом*¹ многочленов f и g .

Сам определитель такого вида называют *определителем Сильвестра*.

На рисунке схематически изображен результат многочленов $f(x)$ и $g(x)$. Имеется в виду, что $\deg f(x) = n$, $\deg g(x) = m$.



Для наглядности коэффициенты многочленов раскрашены в разные цвета. Чтобы получить результат, на главную диагональ квадратной матрицы нанизываются старшими членами m строк коэффициентов многочлена $f(x)$. Эти строки на рисунке выделены черным цветом (если смотреть на них издали, то они сливаются в черный параллелограмм). Затем, снова цепляясь за главную диагональ, но теперь уже свободными членами, располагаются n строк коэффициентов многочлена $g(x)$ (на рисунке они выделены серым цветом и сливаются в серый параллелограмм). На остальных (белых) местах матрицы стоят нули.

¹ От лат. *resultantis* — «отражающийся».

Для примера найдем результат многочленов

$$f(x) = a_0x^3 + a_1x^2 + a_2x + a_3 \text{ и } g(x) = b_0x^2 + b_1x + b_2:$$

$$R(f, g) = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{pmatrix} =$$

$$= b_0a_1^2b_2^2 - 2b_0^2a_1b_2a_3 - b_2^2a_1b_1a_0 + b_0^3a_3^2 + 3b_0a_0b_1a_3b_2 - b_1b_0a_2a_1b_2 - \\ - b_0^2b_1a_2a_3 + b_1^2a_0a_2b_2 + b_0a_1b_1^2a_3 - a_0b_1^3a_3 + b_2b_0^2a_2^2 - 2b_0a_2b_2^2a_0 + a_0^2b_2^3.$$

Отметим, что предложения «многочлены $f(x)$ и $g(x)$ имеют общий корень» и «многочлены $g(x)$ и $f(x)$ имеют общий корень» означают одно и то же. Следовательно, f и g должны входить симметричным образом и в выражение для результата. В действительности это не совсем так.

Если $(n + m) \times (n + m)$ -матрицу сначала заполнить коэффициентами многочлена $g(x)$, а затем лишь коэффициентами $f(x)$, то получится $R(g, f)$, который отличается от $R(f, g)$ лишь расположением строк. Это значит, что $R(g, f)$ отличается от $R(f, g)$ лишь множителем вида $(-1)^k$, где k — число перемен строк в $R(f, g)$, необходимых для получения $R(g, f)$ (или k — число такой же четности).

Впрочем, число k можно вычислить точно.

Если $f(x)$, $g(x)$ — многочлены с коэффициентами из целостного кольца и $\deg f(x) = n$, $\deg g(x) = m$, то

$$R(f, g) = (-1)^{nm} \cdot R(g, f).$$

Это означает, что $R(f, g)$ и $R(g, f)$ оба равны нулю и матрицу результата можно заполнять в любом порядке.

Для того чтобы многочлены $f(x)$ и $g(x)$ с коэффициентами из целостного кольца были не взаимно просты, необходимо, чтобы результат $R(f, g)$ был равен нулю.

Равенство нулю результата без оговорок о старших коэффициентах многочленов является лишь *необходимым*, но не *достаточным* условием. Действительно, если $a_0 = b_0$, то результат равен нулю, даже если у многочленов нет общих корней.

Результат можно использовать для исключения неизвестного из системы алгебраических уравнений.

Общий случай (произвольного числа уравнений и произвольного числа неизвестных) снова сводится к системе из двух уравнений с двумя неизвестными:

$$\begin{cases} f(x, y) = 0, \\ g(x, y) = 0. \end{cases} \quad (s)$$

Каждый многочлен $s(x, y)$ от переменных x, y является многочленом от переменной x , а коэффициентами этого многочлена являются многочлены от y :

$$s(x, y) = S(x) = c_0(y) \cdot y^k + c_1(y) \cdot y^{k-1} + \dots + c_k(y).$$

В частности, многочлены из системы (s) имеют такой же вид:

$$f(x, y) = F(x) = a_0(y)x^n + a_1(y)x^{n-1} + \dots + a_n(y);$$

$$g(x, y) = G(x) = b_0(y)x^m + b_1(y)x^{m-1} + \dots + c_m(y).$$

Многочлен $a_0(y)$ ненулевой, поэтому степень многочлена $F(x)$ равна n . Аналогично $b_0(y)$ ненулевой, и степень $G(x)$ равна m .

Система (s) принимает вид

$$\begin{cases} F(x) = 0, \\ G(x) = 0. \end{cases} \quad (S)$$

Если (x_0, y_0) — решение системы (s), то x_0 — общий корень многочленов $F(x)$ и $G(x)$ и, следовательно, результат этих многочленов $R(F, G)$ равен нулю. В этом результате членами матрицы являются многочлены от неизвестного y , и результат $R(F, G)$ имеет вид

$$\begin{vmatrix} a_0(y) & a_1(y) & \dots & a_n(y) & & & \\ & a_0(y) & a_1(y) & \dots & a_n(y) & & \\ \cdot & & \cdot & & \cdot & & \cdot \\ & & & a_0(y) & a_1(y) & \dots & a_n(y) \\ b_0(y) & b_1(y) & \dots & b_m(y) & & & \\ & b_0(y) & b_1(y) & \dots & b_m(y) & & \\ \cdot & & \cdot & & \cdot & & \cdot \\ & & & b_0(y) & b_1(y) & \dots & b_m(y) \end{vmatrix}.$$

В этом определителе, как обычно для результата, в первых m строках располагаются коэффициенты многочлена $F(x)$, а в нижних n строках находятся коэффициенты многочлена $G(x)$. И те и другие заполняют свои строки не полностью, на всех оставшихся местах строк стоят нули.

Но это значит, что y_0 является корнем уравнения

$$R(F, G) = 0.$$

Таким образом, решение системы из двух алгебраических уравнений с коэффициентами из целостного кольца и двумя неизвестными можно свести к решению одного уравнения $R(F, G) = 0$ с одним неизвестным, а затем к решению систем из двух алгебраических уравнений с одним неизвестным.

Другими словами, с помощью результата одно из неизвестных в системе, состоящей из двух алгебраических уравнений, можно исключить.

Теперь отметим следующее обстоятельство.

Дискриминант многочлена появился как симметрическое выражение от корней многочлена. Происхождение результата иное, но связь между результатом и дискриминантом должна быть не переменна.

Дело в том, что многочлен $f(x)$ имеет кратные корни тогда и только тогда, когда он не взаимно прост со своей производной, но одновременно тогда и только тогда, когда его дискриминант равен нулю. Таким образом,

$$D(f) = 0 \Leftrightarrow R(f, f') = 0.$$

Вычисления показывают, что действительно результат многочлена и его производной оказался дискриминантом, умноженным, правда, на старший член многочлена $f(x)$ и на -1 . Поскольку старший член всегда в таких случаях отличен от нуля, равенство (или неравенство) нулю дискриминанта или результата многочлена и его производной будет происходить одновременно.

Для многочлена $f(x) = ax^2 + bx + c$ эта связь тоже имеет место:

$$R(f, f') = -ab^2 + 4ac = -a \cdot D(f).$$

Если $f(x) = ax^4 + bx^3 + cx^2 + d$, то результат $f(x)$ многочлена и его производной имеет вид

$$\begin{aligned} & a(-4d^3b^3 - 27d^4a^2 + c^2b^2d^2 - 4c^3b^2e + 144cb^2ae^2 + 144d^2a^2ec + \\ & + 256e^3a^3 - 6d^2aeb^2 - 27b^4e^2 - 4c^3ad^2 + 16c^4ae - \\ & - 128c^2a^2e^2 + 18d^3acb - 80dac^2be + 18dcb^3e - 192da^2e^2b). \end{aligned}$$

Здесь выражение в скобках — это в точности дискриминант $f(x)$, т. е. в этом случае

$$R(f, f') = a \cdot D(f).$$

Таким образом, для многочленов второй, третьей и четвертой степеней видна простая связь между дискриминантом и результатом этого многочлена:

$$D(f) = k(-a_0) \cdot R(f, f').$$

В этом равенстве коэффициент k для многочленов второй и третьей степеней равен 1, а для четвертой степени $k = 1$. Чтобы доказать, что такое равенство выполняется для любого многочлена с коэффициентами из целостного кольца и разгадать тайну коэф-

коэффициента k , нужно другое определение результата, более близкое к определению дискриминанта. Дискриминант определялся с помощью симметрических многочленов. Для решения поставленной задачи нужно определить результат аналогичным образом — через симметрические многочлены.

Пусть два многочлена

$$\begin{aligned}f(x) &= a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n; \\g(x) &= b_0x^m + b_1x^{m-1} + \dots + b_{m-1}x + b_m.\end{aligned}$$

соответственно степеней n , m , и x_1, x_2, \dots, x_n — корни многочлена $f(x)$; y_1, y_2, \dots, y_m — корни многочлена $g(x)$.

Произведение

$$g(x_1) \cdot g(x_2) \cdot \dots \cdot g(x_n)$$

будет равно нулю тогда и только тогда, когда хотя бы один из корней многочлена $g(x)$ совпадает с некоторым x_i . Это произведение является симметрическим относительно корней многочлена $f(x)$ и, следовательно, выражается с помощью полевых операций через коэффициенты $f(x)$. Наивысшей степенью элемента x_1 в этом произведении будет число m , поэтому, чтобы остаться в кольце коэффициентов, достаточно множителя a_0^m . Выражение

$$a_0^m g(x_1) \cdot g(x_2) \cdot \dots \cdot g(x_n)$$

и будет результатом $R(f, g)$ многочленов f и g .

Поскольку это выражение симметрично относительно x_i , а множитель a_0^m исключит появление дробей, новый $R(f, g)$, так же как и старый, является элементом кольца коэффициентов данных многочленов.

В новый результат (опять же, как и в старый) многочлены f и g входят не совсем симметрично: выражение всегда совпадает с

$$a_0^m g(x_1) \cdot g(x_2) \cdot \dots \cdot g(x_n).$$

Чтобы убедиться, что мы пока еще на правильном пути, нужно увидеть, что эти два произведения отличаются лишь множителем $(-1)^{nm}$.

Для каждого x_i

$$g(x_i) = b_0(x_i - y_1)(x_i - y_2) \dots (x_i - y_m),$$

поэтому

$$a_0^m \cdot g(x_1) \cdot g(x_2) \cdot \dots \cdot g(x_n) = a_0^m \cdot b_0^n \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (x_i - y_j).$$

В то же время

$$b_0^n \cdot f(y_1) \cdot f(y_2) \dots f(y_m) = b_0^n \cdot a_0^m \prod_{\substack{1 \leq j \leq n \\ 1 \leq i \leq m}} (y_j - x_i).$$

В каждом случае произведение включает nm сомножителей вида $(x_i - y_j)$, поэтому и для нового результата выполняется старое свойство (появление коэффициентами при смене мест многочленов).

Точнее, для любых многочленов $f(x)$ и $g(x)$ с коэффициентами из целостного кольца если $\deg f(x) = n$, $\deg g(x) = m$, то

$$R(f, g) = (-1)^{nm} \cdot R(g, f).$$

Это наблюдение позволяет считать в дальнейшем, что $\deg f(x) \geq \deg g(x)$. Если коэффициенты многочленов $f(x)$ и $g(x)$ заставить изменяться, то соответственно будет изменяться и результат $R(f, g)$. При такой точке зрения $R(f, g)$ является однородным многочленом степени n от переменных b_0, b_1, \dots, b_m , и он же — однородный многочлен степени m от переменных a_0, a_1, \dots, a_n .

И, конечно, на результат можно смотреть как на однородный многочлен степени mn от переменных $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$.

Обозначим матрицу результата через T :

$$T = \begin{pmatrix} a_0 & a_1 & \dots & a_n & & & & \\ & a_0 & a_1 & \dots & a_n & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & & & b_m & & \\ & b_0 & b_1 & \dots & & & b_m & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & b_0 & b_1 & \dots & b_m \end{pmatrix}.$$

Итак, наша ближайшая цель — показать, что старый результат $R_1(f, g)$ (равный $|T|$) и новый $R_2(f, g)$ (в виде произведения разностей корней многочленов) совпадают и в том случае, когда ни один из x_i не равен ни одному y_j .

На оба результата (и старый, и новый) можно смотреть как на многочлены от переменных $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m$.

Эти переменные изменяются: при некоторых их значениях многочлены имеют кратные корни, а при некоторых — нет. Пусть значения переменных таковы, что все x_i различны.

Тогда определитель

$$|S| = \begin{vmatrix} x_1^{n-1} & x_2^{n-1} & \dots & x_{n-1}^{n-1} & x_n^{n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ x_1^2 & x_2^2 & \dots & x_{n-1}^2 & x_n^2 \\ x_1 & x_2 & \dots & x_{n-1} & x_n \\ 1 & 1 & 1 & 1 & 1 \end{vmatrix}$$

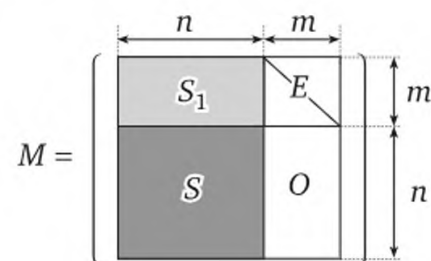
n -го порядка отличен от нуля (это слегка измененный определитель Вандермонда).

Матрица определителя $R_1(f, g)$ имеет размеры бóльшие, чем у матрицы S . Расширим матрицу S до нужных размеров, не слишком испортив при этом значение определителя.

Построим матрицу M следующим образом. Сначала припишем сверху еще t степеней x_i . Получится прямоугольная $(t+n) \times n$ -матрица. Пополним ее еще t столбцами так, чтобы рядом с новыми степенями расположилась единичная $t \times t$ -матрица, а строки матрицы S дополним нулями:

$$|M| = \begin{vmatrix} x_1^{n-1+m} & \dots & x_n^{n-1+m} & 1 & 0 & 0 & \dots & 0 \\ x_1^{n-2+m} & \dots & x_n^{n-2+m} & 0 & 1 & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_1^n & \dots & x_n^n & 0 & 0 & \dots & 0 & 1 \\ x_1^{n-1} & \dots & x_n^{n-1} & 0 & 0 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_1 & & x_n & 0 & 0 & \dots & 0 & 0 \\ 1 & \dots & 1 & 0 & 0 & \dots & 0 & 0 \end{vmatrix}.$$

На рисунке показано строение матрицы M . Она состоит из четырех подматриц: S — $n \times n$ -матрица, E — $t \times t$ -матрица, O — $n \times t$ -матрица и S_1 — $t \times n$ -матрица.



Для наглядности отдельные подматрицы матрицы M выделим цветом.

Непосредственным вычислением устанавливается, что

$$|M| = (-1)^{mn} |S|.$$

Вычислим произведение матриц T и M . Обе матрицы квадратные, одного размера, поэтому TM тоже $(n + m) \times (n + m)$ -матрица:

$$TM = \begin{pmatrix} x_1^{m-1}f(x_1) & x_2^{m-1}f(x_2) & \dots & x_n^{m-1}f(x_n) & a_0 & a_1 & \dots & a_{m-1} \\ x_1^{m-2}f(x_1) & x_2^{m-2}f(x_2) & \dots & x_n^{m-2}f(x_n) & 0 & a_0 & \dots & a_{m-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ f(x_1) & f(x_2) & \dots & f(x_n) & 0 & \dots & 0 & a_0 \\ x_1^{n-1}g(x_1) & x_2^{n-1}g(x_2) & \dots & x_n^{n-1}g(x_n) & b_0 & b_1 & \dots & b_{m-1} \\ x_1^{n-2}g(x_1) & x_2^{n-2}g(x_2) & \dots & x_n^{n-2}g(x_n) & 0 & b_0 & \dots & b_{m-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_1^{n-m}g(x_1) & x_2^{n-m}g(x_2) & \dots & x_n^{n-m}g(x_n) & 0 & 0 & \dots & b_0 \\ x_1^{n-m-1}g(x_1) & x_2^{n-m-1}g(x_2) & \dots & x_n^{n-m-1}g(x_n) & 0 & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g(x_1) & g(x_2) & \dots & g(x_n) & 0 & \dots & \dots & 0 \end{pmatrix}.$$

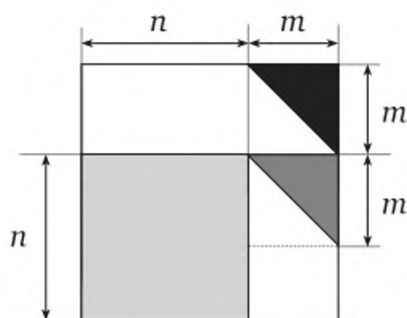
В первых $n - m$ столбцах матрицы TM расположены значения многочленов f и g в точках x_1, x_2, \dots, x_n . Поскольку x_i является корнем многочлена $f(x)$, левый верхний угол, расположенный на первых m строках и n столбцах матрицы TM , сплошь заполняется нулями, т. е. эта матрица имеет вид

$$TM = \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 & a_1 & \dots & a_{m-1} \\ 0 & 0 & \dots & 0 & 0 & a_0 & \dots & a_{m-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & a_0 \\ x_1^{n-1}g(x_1) & x_2^{n-1}g(x_2) & \dots & x_n^{n-1}g(x_n) & b_0 & b_1 & \dots & b_{m-1} \\ x_1^{n-2}g(x_1) & x_2^{n-2}g(x_2) & \dots & x_n^{n-2}g(x_n) & 0 & b_0 & \dots & b_{m-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_1^{n-m}g(x_1) & x_2^{n-m}g(x_2) & \dots & x_n^{n-m}g(x_n) & 0 & 0 & \dots & b_0 \\ x_1^{n-m-1}g(x_1) & x_2^{n-m-1}g(x_2) & \dots & x_n^{n-m-1}g(x_n) & 0 & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g(x_1) & g(x_2) & \dots & g(x_n) & 0 & \dots & \dots & 0 \end{pmatrix}.$$

Это тоже клетчатая матрица. В ее левом верхнем углу находится $m \times n$ -матрица, сплошь заполненная нулями, в правом верхнем — треугольная $m \times m$ -матрица (на поясняющем рисунке она выделена черным треугольником), ниже этой треугольной — вторая треугольная того же размера (на рисунке этот треугольник светлее), ниже которой в оставшихся элементах столбцов стоят одни нули.

Наконец, в нижнем левом углу матрицы TM находится $n \times n$ -матрица, полученная из матрицы S умножением i -го столбца на $g(x_i)$.

На рисунке эта квадратная подматрица выделена светло-серым цветом.



Вычисляем определитель клетчатой матрицы:

$$|TM| = (-1)^{mn} a_0^m g(x_1)g(x_2)\dots g(x_n) |S| = a_0^m g(x_1)g(x_2)\dots g(x_n) |M| = |T| \cdot |M|.$$

В рассматриваемом случае $|M| \neq 0$, поэтому

$$|T| = a_0^m g(x_1)g(x_2)\dots g(x_n),$$

т. е. результат в старом смысле совпал с новым результатом. Правда, доказательство этого совпадения опирается на то, что все корни многочлена $f(x)$ различны.

Ограничение это несущественно. И старый, и новый результаты являются многочленами от одних и тех же переменных над бесконечным целостным кольцом, поэтому из того, что они совпадают при некотором конечном числе различных наборов переменных (это число зависит от числа переменных и степени многочленов), следует их совпадение в алгебраическом смысле.

Таким образом, если

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n,$$

$$g(x) = b_0 x^m + b_1 x^{m-1} + \dots + b_{m-1} x + b_m —$$

многочлены степеней n, m соответственно с коэффициентами бесконечного целостного кольца, x_1, x_2, \dots, x_n — корни многочлена $f(x)$, то

$$a_0^m g(x_1)g(x_2)\dots g(x_n) = \begin{vmatrix} a_0 & a_1 & \dots & a_n & & & & \\ & a_0 & a_1 & \dots & a_n & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & & & b_m & & \\ & b_0 & b_1 & \dots & & & b_m & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & b_0 & b_1 & \dots & b_m \end{vmatrix}.$$

Новое определение результата позволяет подтвердить обнаруженную связь между дискриминантом и результатом многочлена и его производной для произвольных многочленов с коэффициентами из целостного кольца нулевой характеристики (и заодно раскрыть тайну коэффициента k).

Пусть $f(x)$ — такой многочлен степени n и a_0 — коэффициент его старшего члена, а x_1, x_2, \dots, x_n — его корни.

Тогда

$$f(x) = a_0(x - x_1)(x - x_2)\dots(x - x_n),$$

а производная многочлена

$$f'(x) = a_0 \sum_{k=1}^n (x - x_1)\dots(x - x_{k-1})(x - x_{k+1})\dots(x - x_n).$$

Для каждого $i = 1, 2, \dots, n$

$$f'(x_i) = a_0(x_i - x_1)\dots(x_i - x_{i-1})(x_i - x_{i+1})\dots(x_i - x_n).$$

По новому представлению результата получаем:

$$\begin{aligned} R(f, f') &= a_0^{n-1} f'(x_1) f'(x_2) \dots f'(x_n) = \\ &= a_0^{n-1} a_0^n \prod_{k=1}^n (x_k - x_1) \dots (x_k - x_{k-1})(x_k - x_{k+1}) \dots (x_k - x_n). \end{aligned}$$

Для каждой пары различных индексов i, j в этом произведении находится в точности по одному множителю $(x_i - x_j)$ и $(x_j - x_i)$. В множестве из n элементов содержится $\frac{n(n-1)}{2}$ двухэлементных подмножеств. Это число и дает разгадку тайны коэффициента ± 1 , появляющегося в выражении дискриминанта через результат.

Если $f(x) = a_0 x^n + \dots + a_n$ — многочлен с коэффициентами из целостного кольца ($a_0 \neq 0$), то

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} \cdot a_0 \cdot D(f).$$

Контрольные задания

1. Докажите, что свойство целостности при трансцендентном простом расширении кольца сохраняется.
2. Докажите, что свойство евклидовости при трансцендентном простом расширении кольца, вообще говоря, не сохраняется.
3. Докажите, что свойство однопорочности идеалов при трансцендентном простом расширении кольца, вообще говоря, не сохраняется.
4. Докажите, что свойство нетеровости при трансцендентном простом расширении кольца сохраняется.

5. Докажите, что свойство гауссовости при трансцендентном простом расширении кольца сохраняется.
6. Докажите, что каждую булеву функцию от n переменных можно представить многочленом от n переменных.
7. Докажите, что подкольцо симметрических многочленов изоморфно исходному кольцу всех многочленов.
8. Докажите, что уравнения степени не выше четвертой разрешимы в радикалах.
9. Докажите, что если в кольце K алгоритмически разрешима задача разложения на простые множители, то она алгоритмически разрешима и в кольце многочленов с коэффициентами из K .
10. Докажите, что поле комплексных чисел алгебраически замкнуто.

Тема 7

СТРОЕНИЕ ПОЛЕЙ

Основные понятия: расширение, подполе, простое расширение, составное расширение, алгебраическое расширение, конечное расширение, конечномерное векторное пространство, алгебраический над полем элемент, минимальный многочлен, степень алгебраического элемента, алгебраические и трансцендентные числа, алгебраическая иррациональность.

Основные факты: простое алгебраическое расширение поля является конечным и алгебраическим расширением; составное алгебраическое расширение просто; существуют алгебраические расширения, не являющиеся простыми расширениями; все классические задачи древности на построение циркулем и линейкой неразрешимы.

Если поле P_1 — подполе поля P_2 , то P_2 называют расширением P_1 . Например, любое числовое поле является расширением поля рациональных чисел, а каждое поле характеристики p — это расширение поля классов вычетов \mathbb{Z}_p по простому модулю. Расширение поля с помощью присоединения одного элемента называют *простым расширением*.

7.1. Простые расширения полей

Пусть P — подполе поля S и a — произвольный элемент из S . Наименьшее подполе поля S , содержащее множество $P \cup \{a\}$, называют *простым расширением* поля P с помощью элемента a . Обозначается простое расширение символом $P(a)$.

Ситуацию можно обобщить. Если a_1, a_2, \dots, a_m — конечное множество элементов из S , то наименьшее подполе поля S , содержащее множество $P \cup \{a_1, a_2, \dots, a_m\}$, называют *конечно порожденным расширением* поля P и обозначают символом $P(a_1, a_2, \dots, a_m)$. Таким образом, простое расширение поля является *однопорожденным расширением*.

Наименьшее подкольцо поля S , содержащее подполе P и элемент a , называют *простым кольцевым расширением* и обозначают символом $P[a]$. Подкольцо $P[a]$ состоит из всех элементов из S , которые можно получить из элементов из P и элемента a с помощью

кольцевых операций (сложения, умножения и вычитания). Для получения подполя $P(a)$ нужна еще одна операция (деление на ненулевой элемент), поэтому $P(a) \supset P[a]$.

Простое полевое расширение $P(a)$ содержит все элементы поля S , которые можно получить с помощью полевых операций.

Простое расширение $P(a)$ совпадает с множеством элементов вида

$$\frac{f(a)}{g(a)},$$

где $f(x)$, $g(x)$ — многочлены с коэффициентами из поля P и $g(a) \neq 0$.

Действительно, во-первых, множество таких элементов является подполем поля S ; во-вторых, это множество содержит и подполе P , и элемент a ; наконец, в-третьих, это множество содержится в любом подполе, содержащем $P \cup \{a\}$.

Если элемент a из поля S является корнем некоторого ненулевого многочлена с коэффициентами из подполя P , то a называют алгебраическим над P элементом.

Если a — алгебраический над P элемент, то простое расширение $P(a)$ поля P называют простым алгебраическим расширением поля P .

Теорема Кронекера означает, что для любого поля P и любого многочлена $f(x)$ из $P[x]$ существует расширение $P_1 \supset P$, содержащее элемент a — корень многочлена $f(x)$. В поле P_1 возьмем подполе $P(a)$.

Другими словами, для любого поля P и любого многочлена $f(x)$ из $P[x]$ существует простое алгебраическое расширение $P(a)$ поля P с помощью элемента a — корня многочлена $f(x)$.

Если элемент a из поля S не является корнем никакого ненулевого многочлена с коэффициентами из подполя P , то a называют трансцендентным¹ над P элементом.

Если a — трансцендентный над P элемент, то простое расширение $P(a)$ поля P называют простым трансцендентным расширением поля P .

Как и для любого простого расширения, каждый элемент из простого трансцендентного расширения $P(a)$ можно представить в виде

$$\frac{f(a)}{g(a)},$$

где $f(x)$, $g(x)$ из $P[x]$ и $g(a) \neq 0$.

Если $f(x)$ и $f_1(x)$ — различные многочлены, а $f(a) = f_1(a)$, то a будет корнем ненулевого многочлена. Следовательно, если a транс-

¹ От лат. *transcendens*, род. падеж *transcendentis* — «выходящий за пределы».

цендентный, то каждый элемент из $P[a]$ имеет единственное представление в виде

$$a_0 a^n + a_1 a^{n-1} + \dots + a_{n-1} a + a_n,$$

где $n \in \mathbb{Z}_0$ и $a_i \in P$.

Иначе говоря, для трансцендентного элемента a кольцо $P[a]$ изоморфно кольцу многочленов $P[x]$ (впрочем, кольцо многочленов $K[x]$ именно так и определялось — как простое трансцендентное расширение кольца K). Из изоморфизма колец $P[a]$ и $P[x]$ следует, что *если элемент a — трансцендентный над полем P , то простое трансцендентное расширение $P(a)$ поля P изоморфно полю рациональных дробей $P(x)$* .

Таким образом, простое трансцендентное расширение поля — это частный случай простого трансцендентного расширения кольца и в некотором смысле оно является знакомым и частично изученным объектом.

Для алгебраических расширений это пока не так, поэтому обратим внимание на них.

Элемент a — алгебраический над полем P — может являться корнем нескольких многочленов с коэффициентами из P . Многочлен $f(x)$ из $P[x]$ такой, что $f(a) = 0$ и $f(x)$ наименьшей степени с таким свойством, называют *минимальным многочленом для элемента a* .

Минимальный многочлен алгебраического элемента неприводим. Действительно, если

$$f(x) = f_1(x) \cdot f_2(x),$$

где $\deg f_i(x) < \deg f(x)$, то $f_1(a) = 0$ или $f_2(a) = 0$, что противоречит минимальности степени $f(x)$.

Пусть $s(x)$ — минимальный многочлен элемента a и $t(x)$ — многочлен, корнем которого тоже является элемент a . Многочлен $s(x)$ неприводим, а НОД многочленов $s(x)$ и $t(x)$ отличен от делителя единицы. Это означает, что $s(x)$ делится на $t(x)$.

Итак, *любой многочлен, корнем которого является алгебраический элемент a , делится на минимальный многочлен этого элемента*.

В частности, если $g(x)$ — другой минимальный многочлен элемента a , то $g(x)$ тоже делится на $f(x)$; следовательно, *минимальный многочлен алгебраического элемента определен с точностью до ассоциированности*.

Это позволяет ввести следующее понятие.

Степенью элемента, алгебраического над P , называют степень его минимального над P многочлена.

Если многочлен $w(x)$ не обращается в нуль при x , равном a , то это значит, что минимальный многочлен $s(x)$ не делит $w(x)$. Из непри-

водимости минимального многочлена следует, что любой многочлен, корнем которого не является алгебраический элемент, взаимно прост с минимальным многочленом этого элемента.

Таким образом, если $s(x)$ — минимальный многочлен алгебраического элемента a , то для каждого многочлена $t(x)$ из $P[x]$ элемент a не обращает $t(x)$ в нуль тогда и только тогда, когда $(s(x), t(x)) = 1$.

Представление простого расширения $P(a)$ в виде множества

$$\left\{ \frac{f(a)}{g(a)} \mid f(x), g(x) \in P[x], g(a) \neq 0 \right\}$$

для простого алгебраического расширения является слишком избыточным, даже если договориться рассматривать только несократимые дроби

$$\frac{f(x)}{g(x)}.$$

Каждый элемент из $P(a)$ имеет бесконечно много представлений в таком виде. Убрать излишние представления можно. Сначала заметим, что если n — степень минимального для a многочлена (т. е. n — степень элемента a), то степени многочленов $f(x)$ и $g(x)$, участвующих в представлении элемента из $P(a)$, можно считать строго меньшими n .

Если $s(x)$ — минимальный многочлен для a , то для любого $f(x)$ из $P[x]$

$$f(x) = s(x) \cdot q(x) + r(x),$$

где $q(x), r(x)$ принадлежат $P[x]$ и $r(x) = 0$ или $\deg r(x) < \deg s(x)$. Но

$$f(a) = s(a) \cdot q(a) + r(a) = r(a).$$

Итак, если степень алгебраического над P элемента a равна n , то простое расширение $P(a)$ совпадает с множеством элементов вида

$$\frac{f(a)}{g(a)},$$

где $f(x), g(x)$ — многочлены с коэффициентами из поля P , $g(a) \neq 0$, $\deg f(x) < n$ и $\deg g(x) < n$.

Многочлены, степень которых строго меньше n , можно записать явно и, таким образом, уточнить последнее наблюдение: если степень алгебраического над P элемента a равна n , то простое расширение $P(a)$ совпадает с множеством элементов вида

$$\left\{ \frac{a_0 x^{n-1} + \dots + a_{n-1}}{b_0 x^{n-1} + \dots + b_{n-1}} \mid a_1, \dots, a_{n-1}, b_1, \dots, b_{n-1} \in P, b_0 x^{n-1} + \dots + b_{n-1} \neq 0 \right\}.$$

Однако и в этом (гораздо более экономном) представлении элементов из $P(a)$ есть излишества. На самом деле все элементы из $P(a)$ можно записать без знаменателей.

Пусть снова $s(x)$ — минимальный многочлен алгебраического над P элемента a . Если $g(x)$ из $P[x]$, то $g(a) \neq 0$ тогда и только тогда, когда $g(x)$ и $s(x)$ взаимно просты.

Поскольку кольцо $P[x]$ является кольцом главных идеалов, взаимная простота этих многочленов означает, что существуют такие многочлены $u(x)$ и $v(x)$ из $P[x]$, что

$$u(x)s(x) + v(x)g(x) = 1.$$

Отсюда

$$u(a)s(a) + v(a)g(a) = 1,$$

следовательно, $v(a)g(a) = 1$ и

$$\frac{1}{g(a)} = v(a).$$

Каким бы здесь ни получился многочлен $v(x)$, степень его, как и раньше, можно считать не превышающей $(n - 1)$.

Если степень алгебраического над P элемента a равна n , то простое расширение $P(a)$ совпадает с множеством элементов вида

$$\{a_0x^{n-1} + a_1x^{n-2} + \dots + a_{n-1} \mid a_0, \dots, a_{n-1} \in P\}.$$

Знаменатели дробей были действительно последним излишеством в этой истории; иначе говоря, больше уже ничего улучшить нельзя: если степень алгебраического над P элемента a равна n , то каждый элемент из простого алгебраического расширения $P(a)$ имеет единственное представление в виде

$$a_0a^{n-1} + a_1a^{n-2} + \dots + a_{n-1}a + a_n.$$

Задачу нахождения этого многочлена $v(x)$ такого, что

$$\frac{1}{g(a)} = v(a)$$

называют освобождением от алгебраической иррациональности в знаменателе дроби $\frac{1}{g(a)}$ (говорят еще «уничтожение иррациональности»).

Иррациональностью здесь является элемент a — корень неприводимого многочлена $s(x)$. Если многочлен $g(x)$ делится на $s(x)$, то a — корень $g(x)$, т. е. $g(a) = 0$. Следовательно, $s(x)$ не делит $g(x)$, поэтому

взаимно прост с ним. Взаимная простота означает, что существуют такие многочлены $u(x)$, $v(x)g(x)$ с коэффициентами из того же поля, что и коэффициенты многочленов $g(x)$, $s(x)$, что

$$u(x)s(x) + v(x)g(x) = 1.$$

Подставим в это тождество вместо x элемент a и получим $g(a) \cdot v(a) = 1$. Отсюда

$$\frac{1}{g(a)} = v(a).$$

Найти многочлен $v(x)$ такой, что

$$u(x)s(x) + v(x)g(x) = 1,$$

можно с помощью алгоритма Евклида.

Каждый промежуточный остаток $r_i(x)$ в алгоритме Евклида имеет вид

$$r_i(x) = u_i(x)s(x) + v_i(x)g(x),$$

поэтому такой же вид примет и последний ненулевой остаток, равный наибольшему общему делителю.

Задача освобождения от алгебраической иррациональности встречается в школьном курсе математики, но решается она там иначе. Рассмотрим школьный пример. Требуется освободиться от иррациональности в знаменателе дроби

$$\frac{1}{1 + \sqrt{2}}.$$

Здесь $a = \sqrt{2}$, т. е. $s(x) = x^2 - 2$, $g(x) = 1 + x$. Многочлен $v(x)$ в школьном курсе находится не с помощью алгоритма Евклида. Там для решения этой задачи умножают числитель и знаменатель дроби на $1 - \sqrt{2}$, в результате чего иррациональность в знаменателе дроби исчезнет:

$$\frac{1}{1 + \sqrt{2}} = \frac{(1 - \sqrt{2})}{(1 + \sqrt{2})(1 - \sqrt{2})} = \frac{1 - \sqrt{2}}{1 - 2} = -1 + \sqrt{2}.$$

Как возник этот множитель $1 - \sqrt{2}$ и что нам делать в общем случае для произвольных взаимно простых многочленов $s(x)$ и $g(x)$?

Все корни одного и того же неприводимого многочлена называют сопряженными. Если многочлен имеет степень n , то существует в точности n взаимно сопряженных элементов. Например, числа $\sqrt{2}$ и $-\sqrt{2}$ — корни многочлена $(x^2 - 2)$, поэтому сопряжены. Выраже-

ние $1 - \sqrt{2}$ — это результат подстановки в многочлен $(1 + x)$ сопряженного с числом $\sqrt{2}$ числа $-\sqrt{2}$.

В общем случае этот прием принимает следующий вид.

Пусть a_1, a_2, \dots, a_n — все корни неприводимого многочлена $s(x)$, а многочлен $g(x)$ взаимно прост с многочленом $s(x)$, и нам требуется освободиться от иррациональности в знаменателе дроби

$$\frac{1}{g(a_1)}.$$

Умножим числитель и знаменатель этой дроби на произведение значений многочлена $g(x)$ во всех остальных корнях $s(x)$:

$$\frac{1}{g(a_1)} = \frac{g(a_2)g(a_3)\dots g(a_n)}{g(a_1)g(a_2)g(a_3)\dots g(a_n)}.$$

В выражении $g(a_1)g(a_2)\dots g(a_n)$ можно устраивать любые перестановки элементов a_i — выражение от этого не изменится. По следствию из основной теоремы о симметрических многочленах и формул Виета любое симметрическое выражение от корней многочлена $s(x)$ принадлежит тому же полю, что и коэффициенты многочлена $s(x)$. Таким образом,

$$g(a_1)g(a_2)\dots g(a_n) \in P.$$

Иррациональности в знаменателе дроби $\frac{1}{g(a_1)}$ больше нет.

Итак, школьный способ освобождения от алгебраической иррациональности в знаменателе дроби является применением основной теоремы о симметрических многочленах и формул Виета.

Рассмотрим еще один пример школьного типа, но уж с более осмысленных позиций. Избавимся от иррациональности в знаменателе дроби

$$\frac{1}{1 - \sqrt[3]{2}}.$$

Здесь

$$g(x) = 1 - x;$$

$$s(x) = x^3 - 2 = x^2 + 0 \cdot x^2 + 0 \cdot x + (-2).$$

Если a_1, a_2, a_3 — все три корня многочлена $s(x)$, то

$$\begin{aligned} g(a_1)g(a_2)g(a_3) &= (1 - a_1)(1 - a_2)(1 - a_3) = \\ &= 1 - (a_1 + a_2 + a_3) + (a_1a_2 + a_1a_3 + a_2a_3) - a_1a_2a_3 = 1 - 0 + 0 - [-(-2)] = -1; \\ g(a_1)g(a_2) &= (1 - a_1)(1 - a_2) = 1 - (a_1 + a_2) + a_1a_2. \end{aligned}$$

Поскольку $a_2 + a_3 + \sqrt[3]{2} = 0$, получаем $a_2 + a_3 = -\sqrt[3]{2}$. Из равенства $a_2 a_3 \sqrt[3]{2} = 2$ следует:

$$a_2 a_3 = \frac{2}{\sqrt[3]{2}} = \sqrt[3]{4}.$$

Поэтому

$$g(a_1)g(a_1) = 1 + \sqrt[3]{2} + \sqrt[3]{4}.$$

Итак,

$$\frac{1}{1 - \sqrt[3]{2}} = \frac{1 + \sqrt[3]{2} + \sqrt[3]{4}}{(1 - \sqrt[3]{2})(1 + \sqrt[3]{2} + \sqrt[3]{4})} = \frac{1 + \sqrt[3]{2} + \sqrt[3]{4}}{-1} = -1 - \sqrt[3]{2} - \sqrt[3]{4}.$$

Кроме этих двух способов уничтожения иррациональности есть еще один прием, не использующий ни алгоритм Евклида, ни теорему о симметрических многочленах.

Пусть a — корень неприводимого многочлена $s(x)$, многочлен $g(x)$ не делится на $s(x)$ и требуется освободиться от иррациональности в знаменателе дроби $\frac{1}{g(a)}$.

Каждый элемент из $P(a)$ можно представить единственным образом в виде линейной комбинации степеней $1, a, a^2, \dots, a^{n-1}$ с коэффициентами из P . Это значит, что

$$\frac{1}{g(a)} = a_0 a^n + a_1 a^{n-1} + \dots + a_{n-1} a + a_n,$$

где a_i — пока что неопределенные коэффициенты. Это уравнение с неизвестными a_i равносильно уравнению

$$(a_0 a^n + a_1 a^{n-1} + \dots + a_{n-1} a + a_n) \cdot g(a) = 1.$$

Раскрыв скобки, приведя подобные члены и воспользовавшись алгебраическим равенством многочленов, мы получим систему из n линейных уравнений от n неизвестных.

В рассмотренном ранее примере это означало: заранее было известно, что

$$\frac{1}{1 - \sqrt[3]{2}} = a + b\sqrt[3]{2} + c\sqrt[3]{4},$$

и задача состояла только в нахождении коэффициентов разложения a, b, c .

Это уравнение с неизвестными a, b, c равносильно уравнению

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})(1 - \sqrt[3]{2}) = 1,$$

откуда, раскрыв скобки, получаем:

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} - a\sqrt[3]{2} - b\sqrt[3]{4} - 2c = 1.$$

Приведем подобные члены:

$$(a - 2c) + (b - a)\sqrt[3]{2} + (c - b)\sqrt[3]{4} = 1.$$

Используя единственность такого представления, получаем систему уравнений

$$\begin{cases} a - 2c = 1, \\ -a + b = 0, \\ -b + c = 0. \end{cases}$$

Система эта имеет единственное решение $(-1, -1, -1)$, и, соответственно,

$$\frac{1}{1 - \sqrt[3]{2}} = -1 - \sqrt[3]{2} - \sqrt[3]{4}.$$

Сделаем еще несколько замечаний, связанных с тем, что в простом алгебраическом расширении поля не нужны дробные выражения.

Если a — алгебраический над P элемент, то $P(a) = P[a]$.

В трансцендентном расширении от знаменателей дробей избавиться не удастся. Поэтому если a — трансцендентный над P элемент, то $P(a) \neq P[a]$.

Поскольку каждый элемент или алгебраический, или трансцендентный, то эти два предложения можно собрать в одно: *элемент a является алгебраическим над полем P тогда и только тогда, когда $P(a) = P[a]$.*

Наконец, обратим внимание на следующее.

Когда мы говорим « a — один из корней многочлена $f(x)$ », то a никаким особым образом не выделяется. Само собой подразумевается, что в рассматриваемой ситуации все корни неприводимого многочлена *равноправны*. Это действительно так.

Если a и b — два корня неприводимого над полем P многочлена $f(x)$, то простые алгебраические расширения $P(a)$ и $P(b)$ изоморфны.

Для этого изоморфизма достаточно поставить в соответствие элементу a элемент b , каждый элемент из P оставить на месте и продолжить это отображение так, чтобы сохранялись операции сложения и умножения. Теорема о строении простого алгебраического расширения гарантирует, что это соответствие действительно будет взаимно однозначным отображением.

Если P_1 и P_2 — два расширения одного поля P , то обычно представляют интерес не просто изоморфизм между полями P_1 и P_2 ,

а изоморфизм, оставляющий поле P неподвижным. Такой изоморфизм называют P -изоморфизмом. Если P_1 и P_2 совпадают, то P -изоморфизм превращается в P -автоморфизм.

Если элементы a и b сопряжены над полем P , то поля $P(a)$ и $P(b)$ P -изоморфны.

7.2. Конечные расширения полей

Расширение S поля P является векторным пространством над полем P . Элементы из S удобно называть векторами, а элементы из P — скалярами. Если размерность этого пространства конечна, то S называют конечным расширением поля P . Вместо слова «размерность» чаще говорят «степень расширения», при этом используется обозначение $[S : P]$, т. е.

$$[S : P] = \dim_P S.$$

Обычно точное значение бесконечной степени не называют, например, редко пишут

$$[\mathbb{R} : \mathbb{Q}] = \aleph,$$

да и говорить о континуальной степени не принято.

Наблюдения, сделанные в предыдущем пункте данной темы, означают, что простое алгебраическое расширение является конечным расширением.

Если степень алгебраического элемента a равна n , то элементы $1, a, a^2, \dots, a^{n-1}$ являются порождающими элементами векторного пространства $P(a)$. Единственность представления каждого элемента из $P(a)$ в виде

$$a_0 a^{n-1} + a_1 a^{n-2} + \dots + a_{n-1} a + a_n$$

означает, что простое алгебраическое расширение $P(a)$ является конечным расширением поля P и элементы $1, a, a^2, \dots, a^{n-1}$ образуют базис пространства $P(a)$.

В n -мерном векторном пространстве любая система из $(n + 1)$ векторов образует линейно зависимую систему. Например, $(n + 1)$ степеней $1, b, b^2, \dots, b^n$ любого элемента b линейно зависимы. Это значит, что конечное расширение является алгебраическим расширением.

Из того, что конечное расширение является алгебраическим, а простое расширение — конечным, получаем: простое алгебраическое расширение является алгебраическим расширением.

Зависимость между различными видами расширений показана на рисунке.



Пока для нас неясно, являются ли эти подмножества собственными. Существует ли конечное расширение, не являющееся простым алгебраическим расширением, и существует ли алгебраическое расширение, не являющееся конечным? Позднее мы увидим, что ответ на первый вопрос отрицательный (нет, не существует), а на второй — положительный (да, существует).

Для любого неприводимого многочлена $f(x)$ с коэффициентами из поля P существует простое алгебраическое расширение $P(a)$, где a — корень многочлена $f(x)$. Если над полем есть неприводимые многочлены любой степени, то существуют и конечные расширения любой степени. Например, для любого натурального n существует расширение поля \mathbb{Q} степени n .

Для алгебраически замкнутого поля нетривиальных конечных расширений не найдется. Над полем действительных чисел неприводимыми могут быть лишь многочлены первой и второй степени, поэтому все конечные расширения поля \mathbb{R} имеют степень 1 или 2. В первом случае это само \mathbb{R} , во втором — поле \mathbb{C} комплексных чисел.

Для изоморфизма двух простых алгебраических расширений полей $\mathbb{Q}(a)$ и $\mathbb{Q}(b)$ поля \mathbb{Q} необходимо, чтобы их размерности как векторных пространств над \mathbb{Q} совпадали. Однако равенства степеней чисел a, b может оказаться недостаточно. При изоморфизме полей простое подполе переходит в простое подполе. Поэтому если поля $\mathbb{Q}(a)$ и $\mathbb{Q}(b)$ изоморфны, то при этом изоморфизме подполе поля \mathbb{Q} переходит на себя, но у поля \mathbb{Q} нет нетривиальных автоморфизмов и оно при изоморфизме своих расширений просто остается на месте.

Уравнение $x^2 - 2 = 0$ имеет решение в поле $\mathbb{Q}(\sqrt{2})$, но неразрешимо в поле $\mathbb{Q}(\sqrt{3})$. Это значит, что эти два поля неизоморфны. Любое поле нулевой характеристики является расширением поля рацио-

нальных чисел, поэтому для изоморфизма двух конечных расширений P_1 и P_2 поля нулевой характеристики P необходимо, но недостаточно равенства степеней $[P_1 : P] = [P_2 : P]$.

Свойство конечности расширения транзитивно: конечное расширение конечного расширения само является конечным расширением.

Точнее говоря, если поле P_2 — конечное расширение поля P_1 , а поле P_1 — конечное расширение поля P , то P_2 — конечное расширение поля P .

Этот факт можно уточнить: если $P_2 \supset P_1 \supset P$ — последовательные расширения поля P , то

$$[P_2 : P] = [P_2 : P_1] \cdot [P_1 : P].$$

В векторном пространстве размерности n найдутся подпространства любой размерности, меньшей n . Для конечных расширений поля мы видим, что это не так.

Если $P \subset P_1 \subset P_2$ — последовательные расширения поля P , то размерность $\dim_P P_1$ промежуточного расширения является делителем основной размерности $\dim_P P_2$.

Каждое подпространство конечномерного векторного пространства само конечномерно. Поэтому обратное утверждение тоже верно. Таким образом, если $P \subset P_1 \subset P_2$ — последовательные расширения поля P , то P_2 является конечным расширением поля P тогда и только тогда, когда P_2 — конечное расширение поля P_1 и P_1 — конечное расширение поля P .

Конечное поле является конечным расширением своего простого подполя. Простое конечное подполе состоит из p элементов, где p — простое число. При этом n -мерное векторное пространство является прямой суммой n одномерных векторных пространств, а одномерное векторное пространство состоит в точности из стольких же элементов, что и его поле скаляров. Это значит, что конечное поле состоит из p^n элементов, где p — простое натуральное число.

Вновь вернемся к произвольным полям и рассмотрим конечно порожденное расширение $P(a_1, a_2, \dots, a_m)$ поля P . Если каждый элемент a_1, a_2, \dots, a_m алгебраичен над P , то в цепочке расширений

$$P \subset P(a_1) \subset P(a_1, a_2) \subset \dots \subset P(a_1, a_2, \dots, a_{m-1}) \subset P(a_1, a_2, \dots, a_m)$$

каждое новое расширение является конечным расширением предыдущего.

Это значит, что если все a_i — алгебраические элементы над полем P , то конечно порожденное расширение $P(a_1, a_2, \dots, a_m)$ является конечным (поэтому алгебраическим) расширением.

Трансцендентность хотя бы одного элемента a_i над P , естественно, лишает свойства алгебраичности поля $P(a_1, a_2, \dots, a_m)$ над P .

Итак, конечно порожденное расширение $P(a_1, a_2, \dots, a_m)$ поля P является конечным расширением поля P тогда и только тогда, когда каждый элемент a_i алгебраический над полем P .

Поэтому конечно порожденное расширение $P(a_1, a_2, \dots, a_m)$ поля P является алгебраическим расширением поля P тогда и только тогда, когда каждый элемент a_i алгебраический над P .

Пусть $P \subset P_1 \subset P_2$, причем P_2 — алгебраическое расширение P_1 , а P_1 — алгебраическое расширение поля P . Если элемент c из P_2 алгебраический над P_1 , то найдется многочлен

$$a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

с коэффициентами a_i из поля P , корнем которого является элемент c . Элементы a_i алгебраические над P , поэтому расширение $P(a_1, a_2, \dots, a_m)$ конечно над полем P .

Итак, $P(a_1, a_2, \dots, a_m)$ образует конечное расширение поля P , а $P(a_1, a_2, \dots, a_m, c)$ — конечное расширение поля $P(a_1, a_2, \dots, a_m)$. Отсюда следует, что свойство алгебраичности расширения тоже транзитивно: алгебраическое расширение алгебраического расширения само является алгебраическим.

Или то же самое, но более точно, если $P \subset P_1 \subset P_2$, причем P_2 — алгебраическое расширение P_1 , а P_1 — алгебраическое расширение поля P , то P_2 — алгебраическое расширение поля P .

Мы уже заметили ранее, что если элемент a алгебраический над полем P , то кольцевое и полевое расширения поля P с помощью элемента a совпадают: $P[a] = P(a)$. Это свойство легко обобщается на случай произвольного конечного числа присоединяемых элементов.

Если a_1, a_2, \dots, a_n — конечное множество алгебраических над полем P элементов, то $P[a_1, a_2, \dots, a_n] = P(a_1, a_2, \dots, a_n)$.

Верно и обратное утверждение: если P — поле и $P[a_1, a_2, \dots, a_n] = P(a_1, a_2, \dots, a_n)$, то все элементы a_1, a_2, \dots, a_n алгебраические над полем P .

Присоединение хотя бы одного трансцендентного элемента нарушает алгебраичность расширения, и, таким образом, если P — поле, то

$$P[a_1, a_2, \dots, a_n] = P(a_1, a_2, \dots, a_n)$$

тогда и только тогда, когда все элементы a_1, a_2, \dots, a_n алгебраические над полем P .

Простое алгебраическое расширение поля P является конечным расширением P .

Если P_1 — конечное расширение конечного поля P , то P_1 тоже конечно. Конечная мультипликативная группа любого поля циклическая, $P_1^* = \text{гр}(a)$ для некоторого a из P_1 . Отсюда $P_1 = P(a)$, т. е.

каждое конечное расширение конечного поля является простым алгебраическим расширением. Можно представить это иначе: если a_1, a_2, \dots, a_n — конечное число алгебраических над конечным полем P элементов, то найдется такой элемент a , что $P(a_1, a_2, \dots, a_n) = P(a)$.

Это свойство не является привилегией лишь конечных полей: для любого поля P полевое присоединение конечного числа алгебраических элементов можно заменить присоединением всего лишь одного элемента.

Чтобы это увидеть, достаточно показать, что два-порожденное алгебраическое расширение $P(a, b)$ поля P можно представить как простое алгебраическое расширение, т. е. существует третий элемент c такой, что $P(c) = P(a, b)$. Этот третий элемент называется *примитивным элементом*, а сам факт его существования — *теоремой о примитивном элементе*.

Поскольку эта теорема верна для конечных полей, можно считать, что расширяемое поле P бесконечно.

Итак, бесконечное поле P расширили с помощью двух алгебраических элементов a, b и получили составное алгебраическое расширение $P(a, b)$.

Пусть $f(x)$ — минимальный многочлен для элемента a , а $g(x)$ — минимальный многочлен для b . Минимальный многочлен неприводим, поэтому $f(x)$ и $g(x)$ не имеют кратных корней. Пусть $a = a_1, a_2, \dots, a_n$ — все корни многочлена $f(x)$, а $b = b_1, b_2, \dots, b_m$ — все корни многочлена $g(x)$. Поскольку поле P бесконечно, в P найдется элемент такой элемент k , что

$$k \neq \frac{a - a_i}{b_j - b},$$

где $i \neq 1, j \neq 1$.

Элемент $c = a + kb$ и есть искомый, т. е. $P(a, b) = P(c)$. Включение $P(c) \subset P(a, b)$ следует непосредственно из определения расширения. Для доказательства обратного включения обратим внимание на то, что коэффициенты многочлена

$$f_1(x) = f(c - kx)$$

принадлежат кольцу $P(c)$, а

$$(f_1(x), f(x)) = x - b.$$

Поскольку поиск наибольшего общего делителя не выводит за пределы поле коэффициентов, это значит, что b принадлежит $P(c)$. Отсюда следует, что и $a = c - kb$ тоже принадлежит $P(c)$, поэтому $P(a, b) \subset P(c)$.



Расширения полей (уточненная схема)

Итак, теперь уже для любого поля P : если a, b — алгебраические элементы над полем P , то существует такой элемент c , что $P(a, b) = P(c)$.

Из теоремы о примитивном элементе следует, что класс конечных расширений совпадает с классом простых алгебраических расширений.

Это значит, что на схеме, иллюстрирующей связь между различными видами расширений, вовсе не три множества, а не более двух. На рисунке приведена уточненная схема.

Теперь остается неясным лишь одно: может ли алгебраическое расширение *не быть* простым алгебраическим?

Поле разложения многочлена встречалось нам раньше. Существование поля разложения для любого многочлена над любым полем (теорема Кронекера) явилось опорным фактом для доказательства основной теоремы алгебры. Поле разложения в той ситуации подробно не изучалось, достаточно было факта его существования.

Для каждого поля P и каждого многочлена $f(x)$ с коэффициентами из поля P существует поле P_1 , содержащее изоморфную копию поля P и все корни многочлена $f(x)$.

Поскольку отделение кратных корней не выводит за пределы поля коэффициентов, с самого начала можно считать, что многочлен $f(x)$, поле разложения которого строится, не имеет кратных корней.

Если a_1, a_2, \dots, a_n — все различные корни многочлена $f(x)$ из $P[x]$, то поле разложения многочлена $f(x)$ — это поле $P(a_1, a_2, \dots, a_n)$.

Поскольку все a_i алгебраические над P , поле разложения многочлена с коэффициентами из поля P является конечным расширением поля P .

Конечное расширение алгебраично, поэтому поле разложения многочлена с коэффициентами из поля P является алгебраическим расширением поля P .

Многочлен $f(x)$ можно разложить на неприводимые множители и строить поле разложения постепенно, присоединяя сначала корни одного неприводимого множителя, затем второго и т. д.

Поскольку сопряженные элементы приводят к P -изоморфным простым алгебраическим расширениям, получаем, что два поля разложения одного и того же многочлена $f(x)$ над полем P являются P -изоморфными. Этот изоморфизм оставляет поле коэффициентов P неподвижным, а множество корней многочлена $f(x)$ отображает взаимно однозначно на себя.

Для более детального изучения объекта рассмотрим теперь P -автоморфизмы поля разложения многочлена с коэффициентами из поля P .

Поскольку P -изоморфизм полей разложения многочлена $f(x)$ лишь переставляет корни $f(x)$, а автоморфизм — это изоморфизм на себя, получаем, что каждый P -автоморфизм поля разложения неприводимого над P многочлена $f(x)$ переставляет корни многочлена $f(x)$.

Верно и обратное утверждение. Любая перестановка корней неприводимого над полем P многочлена продолжается до P -автоморфизма поля разложения этого многочлена.

7.3. Алгебраические расширения

Алгебраическое над полем рациональных чисел \mathbb{Q} комплексное число называют алгебраическим числом.

Иначе говоря, число a алгебраическое, если существуют рациональные числа a_1, a_2, \dots, a_n , не все равные нулю и такие, что

$$a^n + a_1 a^{n-1} + \dots + a_{n-1} a + a_n = 0.$$

Множество всех алгебраических чисел обозначают буквой A .

Ситуацию можно обобщить. Если P — подполе поля S , то символом $A_S(P)$ обозначим множество всех элементов из S , алгебраических над P . Тогда $A = A_{\mathbb{C}}(\mathbb{Q})$.

Число, не являющееся алгебраическим, называют трансцендентным.

Заметим сначала, что трансцендентных чисел значительно больше, чем алгебраических.

Множество алгебраических чисел счетно, а множество трансцендентных чисел несчетно.

Если a, b — два алгебраических числа, то $\mathbb{Q}(a, b)$ является конечным расширением поля \mathbb{Q} , а в конечное расширение алгебраично над \mathbb{Q} . Это означает, в частности, что множество алгебраических чисел образует поле.

Пусть a_1, a_2, \dots, a_n принадлежат A и b — корень многочлена

$$a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n.$$

Поле $P = \mathbb{Q}(a_1, a_2, \dots, a_n)$ является конечным расширением поля \mathbb{Q} , а $P(b)$ — это конечное расширение поля P . Таким образом, в поле $\mathbb{Q}(a_1, a_2, \dots, a_n, b)$ все элементы принадлежат множеству A . В частности, $b \in A$. Это значит, что поле алгебраических чисел алгебраически замкнуто.

Те же самые доводы позволяют доказать и значительно более общий факт: для любого поля S и его подполя P множество $A_S(P)$ является полем. Если S алгебраически замкнуто, то и $A_S(P)$ тоже алгебраически замкнуто.

Заметим, что последнее утверждение значительно расширяет круг алгебраически замкнутых полей.

Поскольку поле комплексных чисел алгебраически замкнуто, любое числовое поле содержится в некотором алгебраически замкнутом числовом поле.

Снова вернемся к полю A алгебраических чисел. Каждый элемент из A по определению является алгебраическим над \mathbb{Q} , т. е. A — это алгебраическое расширение поля \mathbb{Q} . Если бы это расширение было конечным степени n , то любое алгебраическое число имело степень, не превышающую n . Однако это не так. Для каждого натурального n существует неприводимый над полем \mathbb{Q} многочлен с рациональными коэффициентами. Поэтому множество алгебраических чисел является алгебраическим, но неконечным расширением поля \mathbb{Q} .

Таким образом, схему с видами расширений полей уже не улучшить. В этой схеме в действительности всего два класса расширений, причем второй класс (алгебраические расширения) строго больше первого.

Заметим, что пересечение алгебраически замкнутых числовых полей снова является алгебраически замкнутым полем. Таким образом, наименьшее алгебраически замкнутое поле \bar{P} , содержащее данное поле P , определено однозначно. Поле \bar{P} называют алгебраическим замыканием поля P . В момент построения поля A алгебраических чисел мы уже обратили внимание на то, что можно говорить о пополнении алгебраическими элементами любого поля, и это пополнение является полем, и полем алгебраически замкнутым. Иначе говоря, каждое числовое поле имеет алгебраическое замыкание.

На самом деле, это верно не только для числовых полей.

По теореме Кронекера для каждого поля P и каждого многочлена $f(x)$ из $P[x]$ положительной степени найдется P_1 — расширение поля P , содержащее корень многочлена $f(x)$.

При доказательстве теоремы Кронекера многочлену $f(x)$ ставится в соответствие элемент x , затем в кольце $P[x]$ рассматривается идеал, порожденный многочленом $f(x)$. При этом можно считать, что многочлен $f(x)$ неприводим (в случае приводимости можно воспользоваться разложением $f(x)$ на неприводимые множители). Вер-

немся к этому доказательству, причем не будем считать заранее, что многочлен $f(x)$ неприводим. Это допущение может усложнить (и, честно говоря, ухудшить) доказательство. Однако это новое, ухудшенное доказательство легко распространить на общий случай. Общий случай — это когда рассматривается произвольное множество многочленов.

Итак, $f(x)$ — произвольный, не обязательно неприводимый многочлен. Пусть I — идеал, порожденный многочленом $f(x)$. Идеал I не совпадает с кольцом $P[x]$, более того, он не содержит ни одного ненулевого элемента из P . Действительно, из равенства

$$f(x)g(x) = c,$$

где $c \neq 0$, следует, что $\deg f(x) = 0$.

Отсюда следует, что если два элемента a, b из поля P сравнимы по модулю идеала I :

$$a \equiv b \pmod{I},$$

то $a = b$. Поэтому множество $\{I + a \mid a \in P\}$ образует в кольце $P[x]/I$ подполе, изоморфное полю P . Перепишав коэффициенты данного многочлена с учетом этого обстоятельства (т. е. заменив каждый коэффициент a_i на смежный класс $I + a_i$), непосредственным вычислением убеждаемся, что класс $I + x$ является корнем этого многочлена.

Фактически цель почти достигнута: кольцо $P[x]/I$ содержит поле, изоморфное полю коэффициентов, и корень многочлена $f(x)$. Не хватает лишь малого: $P[x]/I$ — не поле.

Фактор-кольцо K/I целостного кольца является полем тогда и только тогда, когда I максимальный, а для максимальности идеала в кольце главных идеалов (таковым является кольцо многочленов $P[x]$) достаточно простоты его порождающего элемента. Но от простоты порождающего мы сейчас и отказались. Воспользуемся другой идеей, а именно аксиомой выбора в формулировке Цорна.

Напомним, что, по лемме Цорна, если в частично упорядоченном множестве M каждая линейно упорядоченная цепочка имеет верхнюю грань, то в M существует максимальный элемент.

Множеством M сейчас будет множество всех собственных идеалов в $P[x]$, содержащих идеал I и имеющих нулевое пересечение с P . Объединение любой возрастающей цепочки таких идеалов снова является идеалом с теми же свойствами, т. е. условие леммы Цорна выполнено. Пусть I_1 — максимальный идеал из нашего множества M . Если I_1 не является максимальным идеалом в кольце $P[x]$, то найдется собственный идеал I_2 , включающий в себя идеал I_1 . Тогда, по определению, I_1 — пересечение $I_2 \cap P \neq \{0\}$, но если ненулевой элемент из поля содержится в идеале, то и единица поля

тоже попадает в этот идеал и, следовательно, $I_2 = P[x]$. Идеал I_2 не-собственный.

Значит, I_1 максимальный, поэтому фактор-кольцо $P[x]/I_1$ — поле, и это поле содержит изоморфную копию поля P , а смежный класс $I_1 + x$ является корнем многочлена $f(x)$.

Итак, теорема Кронекера доказана для произвольного многочлена $f(x)$.

Эта произвольность дорого обошлась: ссылка на лемму Цорна усложнила (и ухудшила¹) доказательство.

Однако при таком подходе несложно обобщить теорему Кронекера на произвольное множество многочленов.

Разумеется, для конечного множества многочленов нет никакой необходимости в лемме Цорна. Воспользовавшись теоремой Кронекера (с обычным доказательством) несколько раз, можно установить, что для каждого поля P и каждого конечного множества многочленов $f_i(x)$ с коэффициентами из P существует расширение поля P , содержащее корни всех многочленов $f_i(x)$.

Возьмем теперь бесконечное множество многочленов, а именно все многочлены с коэффициентами из $P[x]$. Каждому многочлену $f(x)$ поставим в соответствие символ x_f и рассмотрим кольцо многочленов $K = P[x_f]$, где пробегает все кольцо $P[x]$.

Пусть I — идеал в K , порожденный многочленами $f(x_f)$. Тогда пересечение $I \cap P$ состоит из одного нуля. Действительно, если

$$f_1(x_{f_1})g_1 + f_2(x_{f_2})g_2 + \dots + f_m(x_{f_m})g_m = c,$$

где $c \neq 0$, а g_i — многочлены из K , то, взяв расширение поля P , в котором содержатся все корни многочленов $f_i(x)$, получим равенство $0 = c$.

Применяя лемму Цорна, устанавливаем существование максимального в кольце K идеала I_1 , содержащего идеал I и имеющего нулевое пересечение с P . Фактор-кольцо $P[x]/I_1$ будет полем, содержащим корни всех многочленов с коэффициентами из поля P .

Для каждого поля P существует поле P_1 , содержащее корни всех многочленов с коэффициентами из P .

Теперь ту же процедуру можно проделать и для поля P_1 . В результате получится поле P_2 , содержащее корни всех многочленов с коэффициентами из поля P_1 , затем появится поле P_3 и т. д.

В результате имеется возрастающая цепочка полей:

$$P \subset P_1 \subset P_2 \subset \dots \subset P_n \subset \dots$$

¹ Странные следствия аксиомы выбора набрасывают тень сомнения на любой результат, доказываемый с ее помощью.

$$\bar{P} = \bigcup_{i=1}^{\infty} P_i$$

возрастающей цепочки полей само является полем. Из того, что в цепочке полей

$$P = P_0 \subset P_1 \subset P_2 \subset \dots \subset P_n \subset \dots$$

каждое подполе P_i содержит корни всех многочленов с коэффициентами из подполя P_{i-1} ($i = 1, 2, \dots$), следует алгебраическая замкнутость поля \bar{P} .

Как следствие этих наблюдений, мы получаем утверждение, которое по имени автора называют *теоремой Штейница*¹.

Для каждого поля существует алгебраическое замыкание.

Заметим, что если S — алгебраическое замыкание поля P , то и поле $A_S(P)$ тоже алгебраически замкнуто. Но множество $A_S(P)$ — это лишь первый «этаж» бесконечноэтажного «небоскреба», построенного при доказательстве теоремы Штейница. Это значит, что, построив эту башню полей до конца (до алгебраического замыкания исходного поля), мы видим с ее высоты, что в этом случае, кроме первого этажа, ничего делать не нужно.

Пусть \bar{P} — алгебраическое замыкание поля P . Если над полем P существуют неприводимые многочлены степени, большей любого данного натурального числа, то \bar{P} является алгебраическим, но не простым алгебраическим расширением.

Над конечным полем существуют неприводимые многочлены любой степени, поэтому алгебраическое замыкание конечного поля бесконечно. Таким образом, *каждое алгебраически замкнутое поле бесконечно*.

Если поле P находится внутри поля K , то оно является расширением поля P . Теоретически можно представить, что это расширение является комбинацией цепочки (может быть, бесконечной) алгебраических и трансцендентных расширений.

Однако на деле ситуация проще — в действительности такая цепочка состоит всего из двух звеньев: одно расширение трансцендентное, а второе — алгебраическое.

Точнее, имеет место следующая теорема, впервые также установленная Э. Штейницем: *каждое расширение K поля P является алгебраическим расширением чисто трансцендентного расширения K поля P .*

Пусть S — некоторая максимальная алгебраически независимая над P система элементов из поля K . Тогда $T = P(S)$ — чисто транс-

¹ Эрнст Штейниц (Steinitz, 1871—1916) — немецкий математик.

цендентное расширение поля P . Если $a \in K$, то система $\{a, S\}$ не будет алгебраически независимой над P , т. е. существует ненулевой многочлен $f(x_1, x_2, \dots, x_{n+1})$ с коэффициентами из поля P такой, что

$$f(a, a_1, \dots, a_n) = 0$$

для некоторых элементов a_1, \dots, a_n из S . Запишем многочлен f по убывающим степеням a и получим

$$b_0(a_i)a^m + b_1(a_i)a^{m-1} + \dots + b_m(a_i) = 0.$$

Поскольку элементы из S алгебраически независимы над P , степень многочлена f относительно x_1 отлична от нуля. Следовательно, элемент a алгебраичен над T .

7.4. Разрешимость алгебраических уравнений в радикалах

Пусть рациональное число d не является точным квадратом, т. е. уравнение $x^2 = d$ не имеет решения в рациональных числах.

Используя теорему о строении простого алгебраического расширения поля или непосредственную проверку, можно установить, что множество чисел вида $a + b\sqrt{d}$, где a, b — рациональные числа, образует числовое поле.

Это поле $\mathbf{Q}(\sqrt{d})$ называют *простым квадратичным расширением поля \mathbf{Q}* с помощью элемента \sqrt{d} .

Ситуация легко обобщается (и тоже можно обойтись без общей теоремы о строении простых алгебраических расширений). Вместо поля \mathbf{Q} рациональных чисел можно взять любое числовое поле.

Множество чисел вида $a + b\sqrt{d}$, где a, b принадлежат произвольному числовому полю, также образует числовое поле.

Если P — числовое поле, а элемент d не является точным квадратом в P , то множество

$$\{a + b\sqrt{d} \mid a, b \in P\}$$

обозначают символом $P(\sqrt{d})$ и называют *простым квадратичным расширением поля P* с помощью элемента \sqrt{d} .

Каждый элемент из простого квадратичного расширения $P(\sqrt{d})$ имеет единственное представление в виде $a + b\sqrt{d}$, где $a, b \in P$.

Элементы $a + b\sqrt{d}$ и $a - b\sqrt{d}$ из $P(\sqrt{d})$ являются корнями одного и того же многочлена

$$x^2 - 2ax + (a^2 - b^2d)$$

с коэффициентами из поля P и неприводимого над P .

Таким образом, $a + b\sqrt{d}$ и $a - b\sqrt{d}$ сопряжены над P .

Отображение, переводящее каждый элемент $a + b\sqrt{d}$ в сопряженный $a - b\sqrt{d}$, является автоморфизмом поля $P(\sqrt{d})$, оставляющим подполе P неподвижным.

Говорят, что корни многочлена

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0$$

выражаются в квадратных радикалах (или уравнение $f(x) = 0$ разрешимо в квадратных радикалах), если корни этого многочлена выражаются через его коэффициенты $a_0, a_1, \dots, a_{n-1}, a_n$ с помощью операций сложения, умножения, вычитания, деления и извлечения квадратного корня.

Алгебраическое уравнение $f(x) = 0$ разрешимо в квадратных радикалах, если от его поля коэффициентов P до поля разложения многочлена $f(x)$ можно протянуть цепочку простых квадратичных расширений.

Слово «цепочка» в этом утверждении, как обычно, означает линейно упорядоченное множество. В данном случае это множество подполей, вложенных друг в друга. Наименьшим из них является поле P , а наибольшим — поле разложения многочлена $f(x)$.

Набор операций $\{+, -, *, /, \sqrt{}\}$ представляет интерес в связи с геометрическими задачами на построение с помощью циркуля и линейки.

Для того чтобы циркулем и линейкой можно было построить отрезок x , длина которого является выражением $f(a, b, \dots, c)$ от длин a, b, \dots, c данных отрезков, необходимо и достаточно, чтобы в выражении $f(a, b, \dots, c)$ использовались только операции сложения, вычитания, умножения, деления и извлечения квадратного корня.

Пытаясь решить классические задачи древности, французский математик Пьер Вантцель¹ доказал следующую теорему.

Корни многочлена третьей степени выражаются в квадратных радикалах через коэффициенты многочлена тогда и только тогда, когда один из корней принадлежит полю коэффициентов.

Достаточность условия устанавливается тривиально. Если корень α многочлена

$$x^3 + a_1x^2 + a_2x + a_3 \tag{*}$$

принадлежит полю коэффициентов, то по теореме Безу

$$x^3 + a_1x^2 + a_2x + a_3 = (x - \alpha)(x^2 + b_2x + b_3),$$

а уравнение второй степени разрешимо в квадратных радикалах.

¹ Пьер Лоран Вантцель (Wantzell, 1814—1848) — французский математик, по специальности инженер мостов и дорог. Теорему о кубических уравнениях Вантцель доказал в 1837 г. С 1838 г. Вантцель преподавал в Политехнической школе, Школе мостов и дорог и еще в нескольких учебных заведениях Парижа. Скончался Вантцель в возрасте 33 лет от переутомления.

Более интересна обратная ситуация — необходимость условия. Предположим, что ни один из корней не принадлежит полю коэффициентов, но уравнение все-таки разрешимо в квадратных радикалах.

Это значит, что, по крайней мере один из корней многочлена (*) выражается через его коэффициенты с помощью полевых операций и извлечения квадратного корня. Но тогда коэффициенты многочлена —

$$x^2 + b_2x + b_3,$$

следовательно, и его корни тоже имеют аналогичные выражения. Таким образом, для каждого корня исходного многочлена можно протянуть цепочку простых квадратичных расширений от его поля коэффициентов P до поля, содержащего этого корень.

Пусть x_1 — корень многочлена (*), имеющий цепочку наименьшей длины:

$$P = P_0 < P_1 < \dots < P_k,$$

где $k > 0$ и каждое P_i является простым квадратичным расширением P_{k-1} и $x_1 \in P_k$.

Пусть $P_k = P_{k-1}(\sqrt{d})$, где d — элемент из P_{k-1} , а уравнение $x^2 = d$ не имеет решения в поле P_{k-1} . Тогда $x_1 = a + b\sqrt{d}$, где a, b — элементы из поля P_{k-1} . Элемент $x_2 = a - b\sqrt{d}$ из P_k является вторым корнем многочлена (*). Цепочка для корня x_2 имеет длину k . По формулам Виета имеем:

$$x_1 + x_2 + x_3 = a_1,$$

откуда

$$x_3 = a_1 - (x_1 + x_2) = a_1 - 2a.$$

Элементы a_1, a принадлежат полю P_{k-1} , следовательно, $x_3 \in P_{k-1}$, т. е. цепочка у корня x_3 оказывается короче минимальной. Полученное противоречие означает, что самая короткая цепочка в действительности состоит всего из одного звена — поля P , и соответствующий корень принадлежит полю коэффициентов. Утверждение доказано.

Сделаем одно замечание о приведенном доказательстве. По существу, речь в нем шла о числе квадратных корней в записи корней многочлена, а рассуждение Вантцеля означает, что символ квадратного корня либо вообще не появляется в выражении для корня многочлена, либо появляется в точности один раз.

С помощью своей теоремы П. Вантцель в той же работе 1837 г. получил решение трех из четырех классических задач на построение с помощью циркуля и линейки.

Под названием «классические задачи» имеют в виду следующие проблемы:

- построить с помощью циркуля и линейки ребро куба, объем которого в два раза больше данного (*задача об удвоении куба*);
- с помощью циркуля и линейки разделить угол на три равные части (*задача о трисекции угла*);
- построить с помощью циркуля и линейки квадрат, площадь которого равна площади данного круга (*задача о квадратуре круга*);
- разделить окружность на n равных частей (*задача о построении правильного многоугольника*).

В истории человечества немного задач, проверенных временем так, как классические задачи.

Решение этих задач на построение безуспешно пытались получить в течение многих столетий как профессионалы, так и математики-любители. В XVIII в. число таких любительских решений, представляемых в Парижскую академию наук, превысило пределы разумного, и академия приняла постановление: «...Отныне и впредь не рассматривать представляемых решений задач удвоения куба, трисекции угла, квадратуры круга»¹. Постановление академии, впрочем, было поспешным: до окончательного решения задач об удвоении куба и трисекции угла должно было пройти еще более полувека, а задаче о квадратуре круга предстояло оставаться без решения еще более 100 лет.

В то же время предположение о том, что решения этих задач отрицательны, т. е. требуемое построение невозможно, появилось задолго до постановления академии.

Удвоение куба, тройное сечение угла, недоступные обычной геометрии, и квадратура круга, немыслимая для любой геометрии, были объектом бесполезных поисков древних.

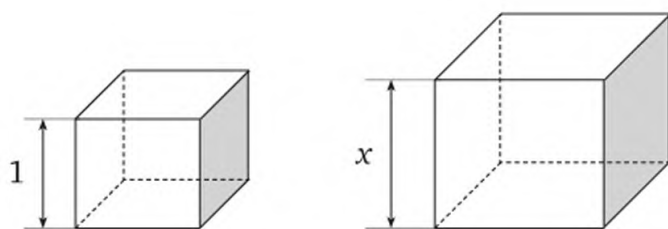
Вольтер², «Философские письма»

Действительно, все перечисленные классические задачи имеют отрицательное решение: требуемые построения невозможны.

Рассмотрим сначала задачу об удвоении куба. Длину ребра данного куба можно считать единичной, и задача об удвоении куба сводится к построению отрезка $\sqrt[3]{2}$.

¹ «Решения и постановления Парижской академии наук» (1775).

² Вольтер (Voltaire — псевдоним, настоящие имя и фамилия Мари Франсуа Аруэ (Arouet, 1694—1778) — французский писатель, философ, историк. Член Французской академии (1746). «Философские письма» опубликованы в 1733 г. [Цит. по: «История бесконечности», гл. XIX].



Задача об удвоении куба

Непосредственной проверкой можно убедиться, что многочлен $x^3 - 2$ не имеет рациональных корней, поэтому по теореме Вантцеля следует: задача об удвоении куба с помощью циркуля и линейки неразрешима.

В задаче о трисекции угла требуется с помощью циркуля и линейки разделить данный угол на три равные части, т. е. построить *трисектрису*. Для некоторых частных случаев такое построение возможно. Например, чтобы разделить на три части угол в 180° , нужно построить угол в 60° , а это угол при вершине правильного треугольника.

Чтобы разделить угол в 90° , нужно построить угол в 30° , а для этого достаточно угол в 60° разделить пополам. Аналогичным образом произойдет трисекция угла в 45° , $22,5^\circ$ и вообще угла $\frac{180^\circ}{2^n}$ (где n — любое натуральное число).

Возможно, что своему возникновению задача обязана прямой аналогии с делением отрезка на равные части, тем более что деление отрезка пополам и построение биссектрисы угла очень похожи. Деление отрезка на три равные части не представляет никаких трудностей, также легко разделить отрезок и на n частей. Видимо, первоначально задача с делением угла была задачей общего вида — разделить угол на n частей, но непреодолимые трудности возникли уже при $n = 3$.

Будем считать, что нам даны два отрезка — единичный e и отрезок a , равный $\cos 3\alpha$. Тогда задача о трисекции угла сводится к построению отрезка x , равного $\cos \alpha$.

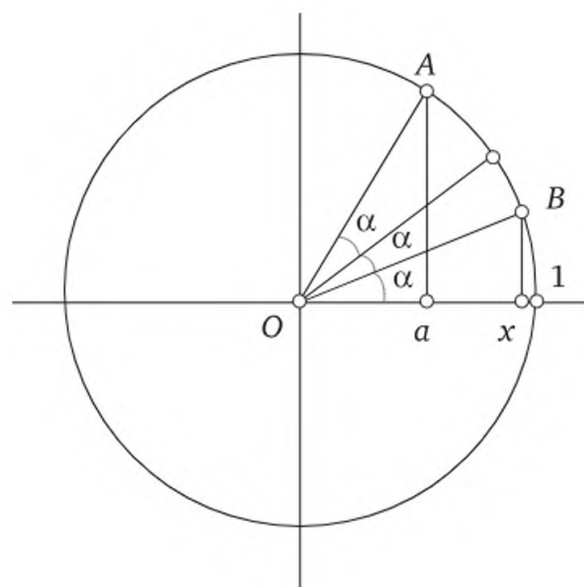
С помощью формулы для косинуса суммы получим формулу для косинуса тройного угла:

$$\cos 3\alpha = 4\cos^3 \alpha - 3\cos \alpha.$$

При этих обозначениях возникает уравнение для x :

$$a = 4x^3 - 3x.$$

Возможность построения трисектрисы теперь зависит от числа a . Например, при $a = 0$ (тогда $3\alpha = 90^\circ$) или при $a = \frac{\sqrt{2}}{2}$ (тогда $3\alpha = 45^\circ$) корни уравнения можно построить с помощью циркуля и линейки.



Задача о трисекции угла

Попробуем разделить на три части угол, равный 60° . В этом случае $a = \frac{1}{2}$ и уравнение для x примет вид

$$4x^3 - 3x - \frac{1}{2} = 0.$$

Это уравнение не имеет рациональных корней, поэтому по теореме Вантцеля ни один из корней этого уравнения не выражается через коэффициенты с помощью арифметических операций и извлечения квадратного корня.

Следовательно, разделить угол в 60° с помощью циркуля и линейки невозможно. *Задача о трисекции угла с помощью циркуля и линейки в общем случае неразрешима.*

В течение столетий, начиная с древнейших времен, исключительной популярностью пользовалась задача о квадратуре круга.

Перевод ее на язык данных и искомых отрезков несложен. По условию дан отрезок a , и требуется построить такой отрезок x , что квадрат со стороной x имеет такую же площадь, что и круг радиуса a . Это значит, что x удовлетворяет уравнению $x^2 = \pi a^2$.

Чтобы построить отрезок x , достаточно получить πa . Среднее геометрическое двух отрезков легко строится с помощью циркуля и линейки. Таким образом, задача о квадратуре круга — это задача о спрямлении окружности, т. е. построении отрезка, равного $2\pi a$. При $a = 1$ эта длина составляет 2π .

То, что проблема квадратуры круга сводится к задаче о спрямлении окружности, т. е. к поиску основания — отрезка, равного π , и что в этом-то и состоит вся трудность задачи, в средние века была известно даже в гуманитарной среде.

Как геометр, напрягший все старанья,
Чтобы измерить круг, схватить умом
Искомое не может основанья...

Данте¹, «Божественная комедия»

Каждое число, которое можно получить из единицы с помощью арифметических операций и извлечения квадратного корня, является корнем многочлена с рациональными коэффициентами.

Другими словами, циркулем и линейкой при данном единичном отрезке можно построить лишь алгебраические числа (да и то далеко не все).

В 1882 г. Фердинанд Линдеманн² доказал, что число π трансцендентно и, следовательно, окружность не спрямляема с помощью циркуля и линейки: *задача о квадратуре круга неразрешима*.

Пусть $n = 7$, т. е. рассмотрим задачу о построении правильного семиугольника.

Корни седьмой степени из единицы расположены в вершинах правильного семиугольника, вписанного в единичную окружность, если число z находится в вершине и $z \neq 1$, то z является корнем уравнения

$$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0.$$

Это возвратное уравнение, и делением левой и правой частей на z^3 , и последующей подстановкой $z = x + \frac{1}{x}$ оно сводится к уравнению

$$x^3 + x^2 - 2x - 1 = 0.$$

Полученное уравнение с неизвестным x (следовательно, и исходное с z) не имеет рациональных корней, поэтому по теореме Вантцеля *построить правильный семиугольник с помощью циркуля и линейки невозможно*.

Доказательство невозможности построения правильного семиугольника с помощью циркуля и линейки было получено еще в 1796 г. К. Гауссом. Тогда же он обнаружил, что с помощью циркуля и линейки можно построить правильный семнадцатиугольник³ — резуль-

¹ Данте Алигьери (Dante Alighieri, 1265—1321) — итальянский поэт. Вершина творчества Данте — поэма «Комедия», названная потомками «Божественной». Форма поэмы восходит к традиционному жанру видения; она изображает странствие поэта по загробному миру и состоит из трех частей: «Ад», «Чистилище» и «Рай» [Цит. по: «Рай», XXXIII, строфа 133 /пер. М. Лозинского].

² Фердинанд Карл Луис Линдеманн (Lindemann, 1852—1939) — немецкий математик, профессор Кенигсбергского (с 1883 г.) и Мюнхенского (с 1893 г.) университетов.

³ Наивысшим математическим достижением в своей жизни Гаусс считал решение задачи о построении правильных многоугольников.

тат, как сам автор правильно оценил, не уступающий по значимости классическим результатам древних.

В 1801 г. К. Гаусс полностью решил задачу о построении правильного n -угольника, доказав, что правильный n -угольник можно построить с помощью циркуля и линейки тогда и только тогда, когда значение функции Эйлера от n является степенью двойки, $\varphi(n) = 2^n$.

Выясним, например, можно или нельзя построить правильный тринадцатигульник. Все натуральные числа, меньшие простого числа p , взаимно просты с ним: для простого p таких чисел найдется $p - 1$. Поэтому для числа 13 найдется 12 чисел, меньших 13 и взаимно простых с ним. Число 12 — это не степень двойки, следовательно, правильный тринадцатигульник с помощью циркуля и линейки построить нельзя.

Число 17 тоже простое; число натуральных чисел, меньших семнадцати и взаимно простых с ним, равно 16, а $16 = 2^4$. Значит, семнадцатигульник построить можно. По той же причине возможно построение 257-угольника и 65 537-угольника.

Если p — простое число, то $\varphi(p) = p - 1$. Таким образом, если простое число $p = 2^n + 1$, то $\varphi(p) = 2^n$.

Напомним, что числа вида

$$F_n = 2^{2^n} + 1$$

называют числами Ферма и при $n = 0, 1, 2, 3, 4$ соответствующие числа Ферма 3, 5, 17, 257, 65 537 являются простыми.

Кроме этих чисел пока (2021 г.) не известно ни одного простого числа F_n .

Правильный n -угольник можно построить с помощью циркуля и линейки тогда и только тогда, когда n имеет вид

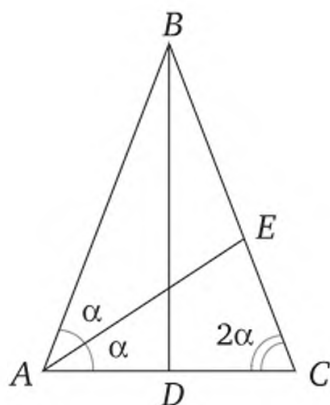
$$n = 2^k \cdot p_1 \cdot p_2 \cdot \dots \cdot p_s,$$

где p_1, p_2, \dots, p_s — различные простые числа Ферма.

Если вдруг окажется, что существует лишь конечное число простых чисел Ферма, то число правильных n -угольников с нечетным n , которые можно построить с помощью циркуля и линейки, тоже будет конечным. Если к тому же выяснится, что при $n > 4$ число F_n всегда составное, т. е. простых чисел Ферма всего пять, то таких n -угольников будет в точности 31.

По существу, классическими задачами на построение являются также и задачи, связанные с построением треугольника.

Легко построить треугольник по трем сторонам, чуть сложнее построить треугольник по трем медианам или трем высотам. Самый трудный случай возникает для трех данных биссектрис. Эта задача непроста даже для равнобедренного треугольника, т. е. тогда, когда две биссектрисы треугольника равны.



К построению треугольника по биссектрисам

Пусть в равнобедренном треугольнике ABC известны длины биссектрис AE и BD :

$$AE = a, \quad BD = b.$$

Построение треугольника ABC сводится к построению угла α . Точнее, треугольник ABC можно построить с помощью циркуля и линейки тогда и только тогда, когда можно построить α (значит, и $\sin \alpha$).

Найдем площадь треугольника ABC двумя способами:

$$S_{\triangle ABC} = \frac{1}{2} AC \cdot BD = \frac{1}{2} \cdot (2b \cdot \operatorname{ctg} 2\alpha) \cdot b;$$

$$S_{\triangle ABC} = S_{\triangle ACE} + S_{\triangle ABE} = \frac{1}{2} a \cdot 2b \cdot \operatorname{ctg} 2\alpha \cdot \sin \alpha + \frac{1}{2} \cdot a \cdot \sin \alpha \cdot \frac{b}{\sin 2\alpha}.$$

Отсюда получаем уравнение

$$\frac{1}{2} \cdot (2b \cdot \operatorname{ctg} 2\alpha) \cdot b = \frac{1}{2} a \cdot 2b \cdot \operatorname{ctg} 2\alpha \cdot \sin \alpha + \frac{1}{2} \cdot a \cdot \sin \alpha \cdot \frac{b}{\sin 2\alpha},$$

что равносильно

$$\frac{2ab \cdot \cos 2\alpha}{\sin 2\alpha} \cdot \frac{b}{a} = \frac{2ab \cdot \cos 2\alpha \cdot \sin \alpha}{\sin 2\alpha} + \sin \alpha \cdot \frac{ab}{\sin 2\alpha}.$$

Пусть $\frac{b}{a} = k$; разделив обе части уравнения на (явно ненулевое) число $\frac{ab}{\sin 2\alpha}$, получим уравнение с параметром k :

$$2 \cdot \cos 2\alpha \cdot k = \cos 2\alpha \cdot \sin \alpha + \sin \alpha.$$

Преобразуем

$$2(1 - 2\sin^2 \alpha)k = (1 - 2\sin^2 \alpha)\sin \alpha + \sin \alpha.$$

Обозначим $y = \sin \alpha$, тогда уравнение принимает вид

$$2k(1 - 2y^2) = 2y(1 - 2y^2) + y,$$

что равносильно

$$4y^3 - 4ky^2 - 3y + 2k.$$

При некоторых рациональных значениях k это уравнение имеет корень, который выражается в квадратных радикалах. Например, если $k = 1$, то многочлен

$$4y^3 - 4y^2 - 3y + 2 = (2y - 1)(2y^2 - y - 2)$$

имеет рациональный корень $y = \frac{1}{2}$ и треугольник построить можно. Впрочем, это было ясно и без уравнения; при $k = 1$ треугольник равносторонний, тогда угол $\alpha = 30^\circ$ и его синус, равный $\frac{1}{2}$, известен априори.

Отметим, что два других корня этого многочлена, а именно

$$y_{2,3} = \frac{1 \pm \sqrt{17}}{4},$$

в нашей задаче лишние: углов с такими синусами не существует.

Менее очевидно, что при соотношении биссектрис, равном $k = \frac{1}{2}$, треугольник тоже можно построить с помощью циркуля и линейки. В этом случае уравнение для $y = \sin \alpha$ имеет вид

$$4y^3 - 1 - 2y^2 - 3y + 1 = 0.$$

Этот многочлен имеет корень $y = 1$, но α с таким синусом не подходит: треугольника с углом в 180° не существует. Но один из двух остальных корней многочлена

$$4y^3 - 2y^2 - 3y + 1 = (y - 1)(4y^2 + 2y - 1)$$

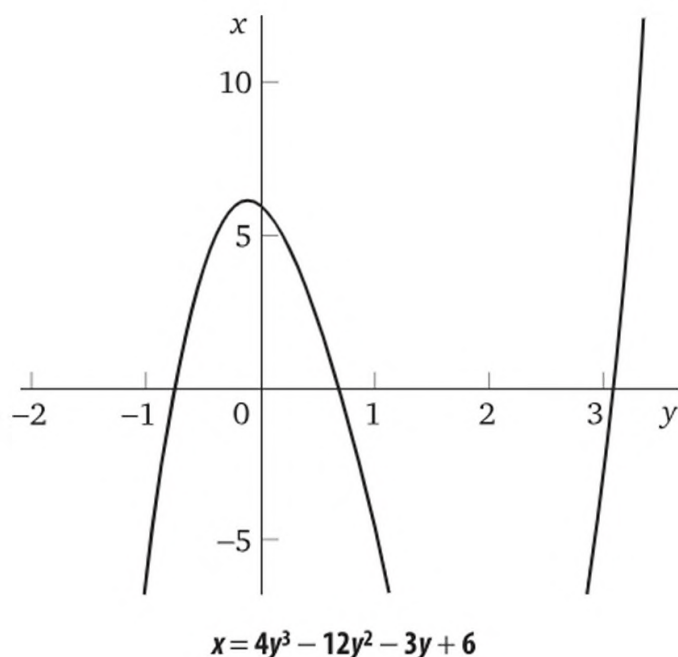
подходит в качестве решения:

$$0 < \frac{-1 + \sqrt{5}}{4} < 1.$$

При $k = 3$ многочлен принимает вид

$$4y^3 - 12y^2 - 3y + 6.$$

У него есть действительный корень, удовлетворяющий условию задачи, т. е. лежащий в интервале $(0; 1)$, так как $f(0) > 0$, $f(1) < 0$.



Однако по критерию Эйзенштейна этот многочлен неприводим над полем рациональных чисел, поэтому у него нет рациональных корней. По теореме Вантцеля его корни нельзя выразить в квадратных радикалах через коэффициенты уравнения.

Это значит, что $\sin \alpha$ и, следовательно, равнобедренный треугольник ABC с отношением биссектрис $1 : 3$ построить циркулем и линейкой не удастся.

Отметим, что при соотношении биссектрис $3 : 1$ многочлен

$$g(x) = 12y^3 - 4y^2 - 9y + 2$$

также неприводим и имеет даже два действительных корня, удовлетворяющих условиям задачи. Действительно, $g(0) > 0$ и $g(1) > 0$, а производная $g'(y) = 36y^2 - 8y - 9$ обращается в нуль внутри интервала $(0; 1)$:

$$g'(0) < 0,$$

$$g'(1) > 0.$$

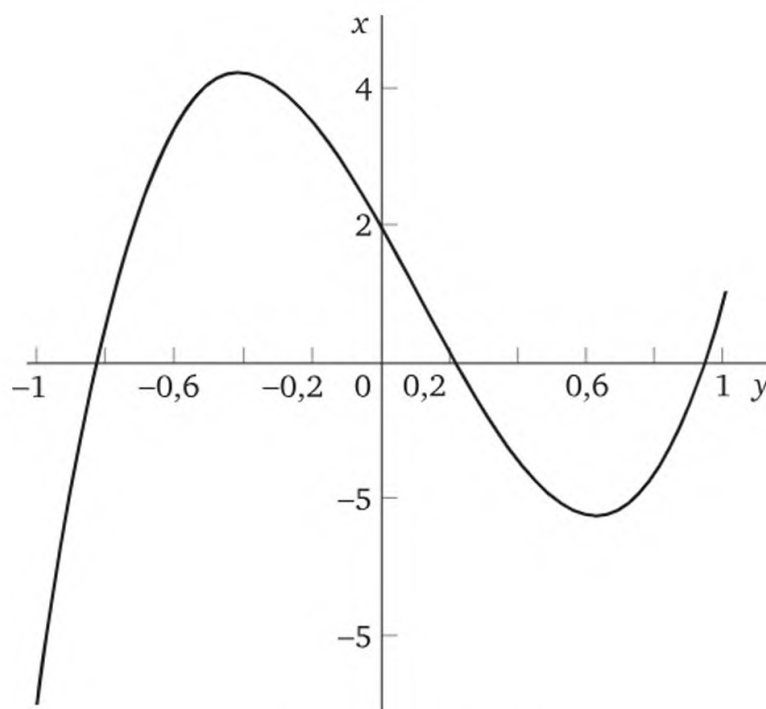
Вид графика функции $x = g(y)$ наглядно подтверждает эти вычисления.

Это значит, что существуют два различных равнобедренных треугольника с таким соотношением биссектрис, но построить ни один из них с помощью циркуля и линейки не удастся.

Подведем главный итог: *задача о построении треугольника по трем биссектрисам с помощью циркуля и линейки в общем случае неразрешима.*

Вместо квадратных корней можно рассмотреть корни любой степени, т. е. рассмотреть *простые радикальные расширения полей.*

Здесь есть одна особенность. Квадратных корней из числа два, но когда мы присоединяем один корень второй степени к полю, то второй, противоположный, автоматически окажется в этом же поле. Для корней более высоких степеней так может не получиться. Но все корни n -й степени из числа можно получить из одного корня путем умножения его на корни n -й степени из единицы. Поле $P(\epsilon^m \sqrt[n]{a})$, где ϵ пробегает все множество корней n -й степени из единицы, называют *простым радикальным расширением* поля P .



$$g(x) = 12x^3 - 4x^2 - 9x + 2$$

Поле K называют *радикальным расширением* поля P , если существует цепочка полей

$$P = P_1 \subset P_2 \subset \dots \subset P_n = K,$$

каждое из которых является простым радикальным расширением предыдущего.

Алгебраическое уравнение $f(x) = 0$ с коэффициентами из поля P разрешимо в радикалах, если поле разложения многочлена $f(x)$ является радикальным расширением поля P .

Иначе говоря, от поля коэффициентов P до поля разложения многочлена $f(x)$ можно протянуть возрастающую цепочку простых радикальных расширений.

Рассматриваемые поля имеют характеристику нуль, поэтому являются бесконечными. Простым перебором существования (или несуществования) такой цепочки установить невозможно.

Оказывается, что искомую возрастающую цепочку вложенных друг в друга бесконечных полей с заданными свойствами можно точно представить убывающей цепочкой подгрупп некоторой конечной группы. Тайну этой связи можно раскрыть сразу: речь идет о *группе автоморфизмов* поля разложения многочлена, оставляющих поле коэффициентов неподвижным.

Обратим внимание на одну особенность поля разложения многочлена.

Конечное расширение P_1 поля P называют *нормальным расширением*, если каждый неприводимый над P многочлен, имеющий в P_1 хотя бы один корень, содержит в P_1 все свои корни.

Поле P_1 тогда и только будет нормальным расширением поля P , когда P_1 является полем разложения некоторого многочлена над P .

Нормальное расширение поля P является простым алгебраическим расширением.

Пересечение нормальных расширений является нормальным расширением.

Если поле P_1 нормально над полем P , а поле L — промежуточное между P и P_1 , то P_1 является нормальным расширением поля L .

Наименьшее поле, содержащее два нормальных расширения, само является нормальным расширением.

Рассмотрим теперь автоморфизмы нормального расширения, оставляющие исходное поле неподвижным.

Если элемент α алгебраический степени n над полем P , расширение $P(\alpha)$ является нормальным, а $\alpha_2, \alpha_3, \dots, \alpha_n$ — элементы, сопряженные с элементом α , то каждый неединичный автоморфизм поля $P(\alpha)$, оставляющий поле P неподвижным, однозначно определяется отображением $\alpha \mapsto \alpha_i$.

Пусть поле K является расширением поля P . Множество всех автоморфизмов поля K , оставляющих поле P неподвижным, образует группу.

Эта группа называется *группой Галуа* и обозначается символом $G(K, P)$.

Если числовое поле L является нормальным расширением своего подполя P , то группа Галуа конечна и имеет порядок, равный $\dim_p L$.

Следующий факт вошел в историю науки как *основная теорема теории Галуа*.

Если числовое поле K является нормальным расширением поля P , то соответствие, сопоставляющее каждому промежуточному полю S группу Галуа $G(K, S)$ поля K над полем S , является инверсным изоморфизмом между структурой $L(K, P)$ всех промежуточных полей и структурой $L(G(K, P))$ всех подгрупп группы Галуа $G(K, P)$.

Отдельные замечания можно сделать о нормальных делителях группы Галуа и соответствующих фактор-группах.

Соответствие Галуа между структурой подгрупп группы Галуа $L(G(K, P))$ и структурой $L(K, P)$ промежуточных полей сопоставляет каждому нормальному делителю N группы Галуа $G(K, P)$ промежуточное, нормальное над P поле S , причем группа $G(S, P)$ изоморфна фактор-группе

$$G(K, P) / N.$$

Если элемент a из поля P не является m -й степенью в поле P , а ε — первообразный корень m -й степени из единицы, то группа Галуа $G(P(\varepsilon^m \sqrt[m]{a}), P)$ является циклической.

Если группа Галуа поля разложения K некоторого многочлена над полем P циклическая, то K является простым радикальным расширением поля P .

Каждое радикальное расширение поля содержится в некотором нормальном радикальном расширении этого поля.

Если P_1 — поле разложения неприводимого над полем P многочлена $f(x)$ и уравнение $f(x) = 0$ разрешимо в радикалах, то группа Галуа $G(P_1, P)$ разрешима.

Если группа Галуа поля разложения K некоторого многочлена над полем P разрешима, то существует радикальное расширение поля P , содержащее поле K .

Таким образом, возрастающая цепочка простых радикальных расширений полей, соединяющая поле коэффициентов P и поле разложения многочлена K , существует тогда и только тогда, когда в группе Галуа $G(K, P)$ существует цепочка нормальных делителей

$$G(K, P) = G_0 > G_1 > \dots > G_n = E,$$

в которой каждая фактор-группа G_i / G_{i+1} циклическая ($i = 0, 1, \dots, n - 1$).

Группы с таким свойством называют *разрешимыми*. В предыдущих темах простейшие свойства и примеры разрешимых групп уже были, но уместно их напомнить (и применить в свете новых фактов).

Симметрические группы степени ≤ 4 разрешимы.

Подгруппа разрешимой группы разрешима.

Следовательно, подгруппы симметрических групп степени не выше четвертой разрешимы.

Каждое уравнение степени не более четырех имеет разрешимую группу Галуа и поэтому разрешимо в радикалах.

Если бы мы не знали к этому моменту ни формул для корней квадратного уравнения, ни формул Кардано, ни метода Феррари, то сейчас могли бы все равно уверенно сказать, что формулы для выражения корней этих уравнений через их коэффициенты суще-

ствуют. Более того, можно заранее предсказать вид формулы — какие там извлекаются корни и сколько раз.

Ответ нам подсказывают ряды разрешимости в группах S_1, S_3, S_4 .

Группа A_5 проста. Если $n \geq 5$, то группа S_n неразрешима. Это значит, что если группа Галуа уравнения степени пятой и выше является симметрической, то корни этого уравнения нельзя выразить в радикалах через коэффициенты многочлена и, в частности, общей формулы для выражения решений таких уравнений не существует.

Например, если многочлен $f(x)$ степени n с коэффициентами из поля \mathbb{Q} и неприводимый над \mathbb{Q} имеет в точности $n - 2$ действительных корня, то группа Галуа многочлена $f(x)$ совпадает с S_n .

Рассмотрим числовой пример. Многочлен

$$f(x) = x^5 - px + p,$$

где p — простое число, по критерию Эйзенштейна неприводим над \mathbb{Q} . Найдем число действительных корней этого многочлена.

Вычисляем систему многочленов Штурма:

$$f_1(x) = 5x^4 - p;$$

$$f_2(x) = \frac{4}{5}px - p;$$

$$f_3(x) = p - \frac{3125}{256}.$$

Приближенно

$$f_3(x) = p - 12,2.$$

Найдем число перемен знаков в системе многочленов Штурма от $-\infty$ до $+\infty$:

x	$x^5 - px + p$	$5x^4 - p$	$\frac{4}{5}px - p$	$p - \frac{3125}{256}$	$W(x)$
$-\infty$	—	+	—	?	3
$+\infty$	+	+	+	?	0

При $p \geq 13$ в таблице вместо знака «?» стоит символ «+» и многочлен

$$x^5 - px + p$$

имеет три действительных корня. Поэтому его группа Галуа совпадает с S_5 и, следовательно, неразрешима. Это значит, что при $p \geq 13$ уравнение

$$x^5 - px + p = 0$$

неразрешимо в радикалах.

Заметим, что и для простых $p < 13$ группа Галуа многочлена

$$x^5 - px + p$$

тоже совпадает со всей симметрической группой пятой степени. Это значит, что уравнение

$$x^5 - px + p = 0$$

неразрешимо в радикалах для любого простого числа p .

Поставить вместо простого p в этот многочлен произвольное натуральное число a нельзя. Например, многочлен

$$x^5 - 32x + 32$$

имеет линейный множитель

$$x^5 - 32x + 32 = (x - 2)(x^4 + 2x^3 + 4x^2 + 8x - 16)$$

и соответствующее уравнение разрешимо в радикалах.

В наше время — время всепроникающей электронной техники — особое значение имеют конечные поля.

7.5. Конечные поля

Конечные поля относятся к числу алгебраических систем, изученных наиболее полно и имеющих довольно прозрачное строение.

Одно из замечательных свойств конечных полей состоит в том, что над конечным полем нет всюду определенных функций, кроме многочленов. Если же функция над конечным полем не является всюду определенной, то ее можно представить в виде рациональной дроби.

В настоящее время конечные поля нашли широкое применение в теории кодирования, а функции над конечными полями — в криптографии.

Число элементов в конечном поле может быть любым натуральным числом, или это число обладает особым свойством? Если выполняется это «или», то для любого ли такого особого числа m найдется поле из m элементов? Как устроена решетка подполей конечного поля и его группа автоморфизмов? На все эти вопросы есть ответы.

Кольцо классов вычетов \mathbb{Z}_p по простому модулю p является полем. Это значит, что для каждого простого числа p существует поле из p элементов.

Выясним, существуют ли другие конечные поля.

Пусть P — конечное поле из q элементов. Тогда характеристика поля P ненулевая и является простым числом (в противном случае в P появятся делители нуля).

Аддитивная подгруппа H , порожденная единицей, состоит из p элементов, а ее множество замкнуто относительно умножения, т. е. образует подкольцо кольца P . Подкольцо H изоморфно полю классов вычетов \mathbb{Z}_p .

Итак, если конечное поле P существует, то его характеристика — простое число и это поле является расширением поля \mathbb{Z}_p .

Уточним теперь вид числа q .

Пусть размерность векторного пространства P над \mathbb{Z}_p равна n . Каждое n -мерное пространство изоморфно n -мерному арифметическому пространству строк. Число различных таких строк (размещений по n элементов из p с повторениями) равно p^n .

Таким образом, число элементов в конечном поле равно p^n , где p — простое, а n — некоторое натуральное число.

Остается показать, что поле такого порядка действительно всегда существует.

Если $f(x)$ — неприводимый над полем \mathbb{Z}_p многочлен степени n , то простое алгебраическое расширение $\mathbb{Z}_p(g)$ содержит в точности p^n элементов.

Таким образом, для существования нужного поля достаточно показать, что для любого натурального n существует неприводимый над полем \mathbb{Z}_p многочлен.

Оказалось, что можно указать еще один замечательный многочлен с коэффициентами из поля \mathbb{Z}_p .

Размерность P как векторного пространства над \mathbb{Z}_p конечна, поэтому каждый элемент из P является корнем некоторого многочлена с коэффициентами из \mathbb{Z}_p . Перемножив эти многочлены и отделив кратные корни, можно построить многочлен, среди корней которого будут все элементы поля P . Впрочем, многочлен, корнями которого являются элементы из P , можно указать явно.

Множество P^* ненулевых элементов поля образует группу по умножению.

Любой элемент группы, возведенный в степень, равную порядку группы, превращается в единицу. Поэтому для любого ненулевого элемента x из P выполняется равенство $x^{q-1} = 1$. Умножим левую и правую части равенства на x и получим тождество (для любого x из поля P): $x^q = x$.

Итак, если конечное поле P , состоящее из q элементов, существует, то каждый элемент этого поля является корнем многочлена $x^q - x$, причем коэффициенты этого многочлена принадлежат полю \mathbb{Z}_p , которое входит как подполе в поле P .

В действительности слово «если» из предыдущей фразы можно убрать.

Пусть P_1 — поле разложения многочлена $x^{p^n} - x$ над \mathbb{Z}_p . Поле P_1 содержит \mathbb{Z}_p в качестве подполя и множество M всех корней многочлена $f(x)$.

Производная $f'(x)$ многочлена $f(x)$ равна -1 , так как $p^n \equiv 0 \pmod{p}$. Отсюда следует, что многочлен $f(x)$ взаимно прост со своей производной, а это значит, что многочлен $f(x)$ не имеет кратных корней и, следовательно, число элементов в M в точности равно p^n .

Используя формулу бинома Ньютона и тот факт, что при $k \neq 0$ и $k \neq p^n$ число

$$\binom{p^n}{k} = \frac{p^n(p^n-1)\dots(p^n-k+1)}{1 \cdot 2 \cdot \dots \cdot k}$$

всегда делится на p , получаем тождество (для любых элементов x, y из P_1):

$$(x \pm y)^{p^n} = x^{p^n} \pm y^{p^n}.$$

Кроме того, $(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n}$, а для ненулевого элемента b

$$\left(\frac{a}{b}\right)^{p^n} = \frac{a^{p^n}}{b^{p^n}}.$$

Все это означает, что множество M замкнуто относительно сложения, вычитания, умножения и деления на ненулевой элемент и поэтому образует поле. Иначе говоря, поле разложения многочлена $x^{p^n} - x$ над полем \mathbb{Z}_p и есть M .

Существование поля из p^n элементов доказано: для каждого простого p и любого натурального n существует поле из p^n элементов.

Поле разложения многочлена единственно с точностью до изоморфизма. Поэтому конечное поле полностью определяется числом своих элементов.

По этой причине конечное поле из q элементов принято обозначать символом F_q ¹.

В честь автора конечное поле F_q называют полем Галуа, обозначают его еще и символом $GF(q)$, что означает **GaloisField** из q элементов.

Существование поля порядка p^n означает, что для любого натурального n существует неприводимый над полем \mathbb{Z}_p многочлен $f(x)$.

Можно указать даже место поиска многочлена $f(x)$. Все неприводимые над \mathbb{Z}_p многочлены любой степени, не превышающей число n , — это в точности неприводимые над \mathbb{Z}_p множители многочлена $x^{p^n} - x$.

Итак, пусть

$$f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n —$$

неприводимый над \mathbb{Z}_p многочлен степени n , а $I = (f(x))$ — идеал, порожденный многочленом $f(x)$, в кольце $\mathbb{Z}_p[x]$.

¹ F — первая буква слова *Field* (поле), а q — число элементов в этом поле.

Тогда фактор-кольцо $\mathbb{Z}_p[x]/I$ образует поле. Это поле содержит изоморфную копию поля \mathbb{Z}_p и элемент $I + x$ является корнем многочлена

$$f(X) = X^n + (I + a_1)X^{n-1} + \dots + (I + a_{n-1})X + (I + a_n).$$

С точностью до изоморфизма поле $\mathbb{Z}_p[x]/I$ и есть искомое поле $\mathbb{Z}_p(g)$.

Если g — корень многочлена $f(x)$, то элементы $1, g, g^2, \dots, g^{n-1}$ образуют базис векторного пространства $\mathbb{Z}_p(g)$ над \mathbb{Z}_p . Это значит, что каждый элемент из $\mathbb{Z}_p(g)$ можно представить, и единственным образом, в виде линейной комбинации

$$b_0 + b_1g + \dots + b_{n-1}g^{n-1},$$

где b_i принадлежат \mathbb{Z}_p .

Сложение таких комбинаций сводится к сложению в поле \mathbb{Z}_p , а при построении таблицы умножения следует лишь учесть, что

$$g^n = -a_1g^{n-1} - \dots - a_{n-1}g - a_n.$$

Отметим, что $\mathbb{Z}_p(g)$ — линейная алгебра над \mathbb{Z}_p , поэтому таблица умножения в $\mathbb{Z}_p(g)$ полностью определяется таблицей умножения базисных элементов: $1, g, g^2, \dots, g^{n-1}$.

Построим, например, поле P , состоящее из восьми элементов. Для этого сначала разложим многочлен $x^8 - x$ на неприводимые множители над полем \mathbb{Z}_2 :

$$x^8 - x = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1)x.$$

В этом разложении оказались два многочлена третьей степени. Любой из них годится для наших целей.

Заметим, что расширение любого конечного P с помощью одного корня одного из неприводимых многочленов автоматически захватывает и остальные корни этого многочлена, и корни всех других многочленов такой же (или меньшей) степени.

Итак, пусть $f(x) = x^3 + x + 1$, а g — корень этого многочлена. Тогда поле P состоит из линейных комбинаций элементов $1, g, g^2$:

$$P = \{a + bg + cg^2 \mid a, b, c \in \mathbb{Z}_p\}.$$

Сложение таких комбинаций происходит по правилу

$$(a_1 + b_1g + c_1g^2) + (a_2 + b_2g + c_2g^2) = (a_1 + a_2) + (b_1 + b_2)g + (c_1 + c_2)g^2.$$

При умножении линейных комбинаций (в частности, базисных элементов) используем равенство $g^3 = -1 - g$.

Для поля \mathbb{Z}_2 , впрочем, $-1 - g = 1 + g$. Например:

$$g^2g^2 = g^4 = g^3g = (-1 - g)g = -g - g^2 = g + g^2.$$

Итак, поле из восьми элементов построено. При желании можно выписать его таблицы Кэли для сложения и умножения.

Вспомним теперь, что поле P — это соединение двух групп: аддитивной $\langle P; + \rangle$ и мультипликативной $\langle P^*; \cdot \rangle$.

В конечном поле строение этих групп несложное. Особенно просто устроена мультипликативная группа.

Пусть P — конечное поле и $|P|$ — его порядок, равный p^n .

Аддитивная группа $\langle P; + \rangle$ — это группа векторного пространства над \mathbb{Z}_p , и она изоморфна прямой n -й степени группы $\langle \mathbb{Z}_p; + \rangle$:

$$\langle P; + \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p.$$

Все элементы аддитивной группы имеют порядок p , поэтому если поле P не совпадает с \mathbb{Z}_p , то группа $\langle P; + \rangle$ нециклическая.

В отличие от аддитивной группы (которая порождается одним элементом лишь в полях \mathbb{Z}_p), мультипликативная группа конечного поля всегда циклическая, так как все конечные мультипликативные группы любого поля порождаются одним элементом.

В поле P мультипликативную группу P^* составляют все его ненулевые элементы, т. е. порядок $|P^*|$ мультипликативной группы поля P равен $p^n - 1$. Итак, в поле P найдется такой элемент g , что

$$P \setminus \{0\} = \{1, g, g^2, \dots, g^{p^n-2}\}.$$

Если циклическая группа $\text{gr}(g)$ имеет порядок m , то элемент g^k порождает эту группу тогда и только тогда, когда k и m взаимно просты. Таким образом, в конечном поле P порядка p^n содержится в точности $\varphi(p^n - 1)$ элементов, каждый из которых порождает группу $\langle P^*; \cdot \rangle$.

Порождающий элемент g мультипликативной группы P может быть выбран в качестве присоединяемого элемента, т. е. $P = \mathbb{Z}_p(g)$. Действительно, степени элемента g — это все ненулевые элементы из P , а $0 = g - g$.

Впрочем, этот же факт можно рассмотреть с иной точки зрения.

Каждый элемент конечного расширения поля \mathbb{Z}_p является корнем многочлена с коэффициентами из \mathbb{Z}_p , и степень этого многочлена не превышает число n . Не будет исключением и порождающий элемент g мультипликативной группы P^* поля P .

Если k — наименьшая степень многочлена $f(x)$ над \mathbb{Z} , корнем которого является элемент g , то элементы $1, g, g^2, \dots, g^{k-1}$ еще линейно независимы над полем \mathbb{Z}_p , а элементы $1, g, g^2, \dots, g^{k-1}, g^k$ уже линейно зависимы. Поэтому

$$g^k = a_0 + a_1 g + \dots + a_{k-1} g^{k-1}, \quad (*)$$

где a_0, a_1, \dots, a_{k-1} — элементы из \mathbb{Z}_p .

Из минимальности выбора числа k следует, что многочлен

$$f(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$$

неприводим, поэтому простое алгебраическое расширение $\mathbb{Z}_p(g)$ поля \mathbb{Z}_p с помощью g — корня многочлена $f(x)$ — имеет над \mathbb{Z}_p размерность k . Поле $\mathbb{Z}_p(g)$ содержится в поле P .

С помощью равенства (*) можно получить все остальные степени элемента g . Поскольку g — порождающий элемент группы P^* , эти остальные степени вместе с уже имеющимися — $1, g, g^2, \dots, g^{k-1}$ — дадут все ненулевые элементы поля P . Поэтому $\mathbb{Z}_p(g) = P$, а $k = n$.

Многочлен $x^{p^n} - x$ не имеет кратных корней, следовательно, и каждый его неприводимый множитель степени n имеет n различных корней. Каждый порождающий мультипликативной группы поля является корнем одного из таких многочленов-множителей. Число различных порождающих циклической группы порядка p^n равно $\varphi(p^n - 1)$. Кроме того, если один из корней неприводимого многочлена степени n оказался порождающим мультипликативной группы поля $FG(p^n)$, то и все остальные корни этого многочлена тоже будут порождающими. Если k — число неприводимых над \mathbb{Z}_p многочленов степени n , корни которых оказались порождающими циклической группы $\langle P^*; \cdot \rangle$, то¹

$$kn = \varphi(p^n - 1).$$

Следовательно, общее число неприводимых над \mathbb{Z}_p многочленов степени n не меньше числа

$$\frac{\varphi(p^n - 1)}{n}.$$

Это число для некоторых p^n действительно равно числу неприводимых многочленов степени n над полем \mathbb{Z}_p (например, для рассмотренного ранее поля из восьми элементов), но, вообще говоря, эта оценка грубовата. Дело в том, что не каждый корень минимального многочлена обязан быть порождающим мультипликативной группы поля.

Например,

$$\frac{\varphi(2^{12} - 1)}{12} = \frac{\varphi(4095)}{12} = \frac{\varphi(3^2 \cdot 5 \cdot 7 \cdot 13)}{12} = \frac{6 \cdot 4 \cdot 6 \cdot 12}{12} = 144,$$

но в действительности число неприводимых над \mathbb{Z}_2 многочленов степени 12 равно 335. Это значит, что поле $FG(2^{12})$ можно представить

¹ Отсюда, в частности, следует, что для любого простого p и любого натурального n число $\frac{\varphi(p^n - 1)}{n}$ целое.

как расширение поля \mathbb{Z}_p с помощью любого из 12 корней 191 многочлена, и этот корень не будет порождающим мультипликативной группы ненулевых элементов этого поля.

Точное значение числа неприводимых многочленов степени m над полем \mathbb{Z}_p равно

$$\frac{1}{m} \sum_{d|m} \mu(d) p^{\frac{m}{d}},$$

где $\mu(n)$ — функция Мебиуса¹: $\mu(1) = 1$, и если p_i — различные простые числа и $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$, где $\alpha_i \geq 1$, то

$$\mu(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}) = \begin{cases} 0, & \text{если существует } i \text{ такой, что } \alpha_i > 1, \\ (-1)^k, & \text{если все } \alpha_i = 1. \end{cases}$$

Для строения поля важную роль играет устройство *решетки подполей*. Как и для любой алгебры, в исследовании поля одной из первостепенных задач является описание *автоморфизмов* поля.

Пусть P — конечное поле порядка p^n и H — его подполе. Порядок k подполя H является делителем числа p^n , поэтому $k = p^m$, где $m \leq n$.

Поле P является расширением подполя H , и значит, P образует векторное пространство над H конечной размерности s . Каждое такое пространство изоморфно s -мерному арифметическому пространству строк. Число различных таких строк (размещений по s элементов из k с повторениями) равно k^s , т. е. $(p^m)^s = p^n$.

Таким образом, число элементов в подполе конечного поля порядка p^n равно p^m , где m делит n . При этом для каждого делителя m числа n в поле P найдется подполе порядка p^m .

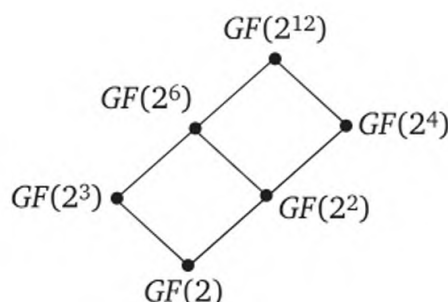
Действительно, многочлен $f(x) = x^{p^n} - x$ делится на $g(x) = x^{p^m} - x$ и, следовательно, поле разложения H многочлена $g(x)$ содержится в поле разложения многочлена $f(x)$.

Порядок H равен p^m , а это значит, что для каждого m — делителя числа n — в поле порядка p^n найдется подполе порядка p^m .

Мультипликативная группа каждого подполя является подгруппой мультипликативной группы поля, но в циклической группе порядка t существует в точности одна подгруппа порядка q для каждого q — делителя числа t . Единственная подгруппа дает единственное подполе.

Для каждого m — делителя числа n — в поле порядка p^n найдется единственное подполе порядка p^m . Это все означает, что решетка подполей поля $GF(p^n)$ элементов изоморфна решетке делителей числа n .

¹ Август Фердинанд Мебиус (Möbius, 1790—1868) — немецкий математик, получивший в основном результаты в геометрии; в 1858 г. установил существование односторонних поверхностей (лист Мебиуса). Функция $\mu(n)$ введена А. Мебиусом в 1832 г.



Решетка подполей поля $GF(2^{12})$

Например, шести делителям числа 12 соответствуют шесть подполей поля $GF(p^{12})$.

Полное описание алгебры включает исследование ее полугруппы эндоморфизмов и группы автоморфизмов. Эндоморфизмов, отличных от изоморфизмов, не имеет любое поле, в том числе и конечное.

Любой автоморфизм α поля оставляет на месте нейтральные элементы. Поэтому $\alpha(1) = 1$, а тогда для любого натурального n выполняется тождество

$$\alpha(n \cdot 1) = n \cdot 1.$$

Следовательно, любой автоморфизм оставляет простое подполе неподвижным. В конечном поле характеристики p простым подполем является \mathbb{Z}_p . Элементы из \mathbb{Z}_p не перемещаются при любом автоморфизме, в частности группа $\text{Aut}(\mathbb{Z}_p)$ единичная.

Посмотрим, как устроена группа автоморфизмов конечного поля P из p^n элементов при $n > 1$. Отображение $\varphi: x \mapsto x^p$ сохраняет операции и, следовательно, является (кольцевым) гомоморфизмом. При этом гомоморфизме единица переходит в единицу, т. е. отображение ненулевое. У полей любой ненулевой гомоморфизм является изоморфизмом.

Поле P конечно, следовательно, φ — отображение *на* (биекция), т. е. автоморфизм.

Этот автоморфизм называют *автоморфизмом Фробениуса*¹. Для любого натурального $m < n$ в поле P не выполняется тождество $x^{p^m} = x$, поэтому и сам автоморфизм Фробениуса нетождественный, все n степеней этого автоморфизма ($1 \leq k \leq n$)

$$\varphi^k(x) = \underbrace{((x^p)^p \dots)^p}_k = x^{p^k}$$

¹ Фердинанд Георг Фробениус (Frobenius, 1849—1917) — немецкий математик, профессор Цюрихского политехникума (1875—1892), Берлинского университета (с 1892 г.). В 1877 г. Ф. Фробениус доказал теорему, из которой следует, что поле комплексных чисел — наибольшая из возможных числовых систем.

различны. Тожество $x^{p^n} = x$ означает, что $\varphi^n = \varepsilon$. Итак, циклическая группа, порожденная автоморфизмом Фробениуса, состоит в точности из n элементов.

Покажем, что других автоморфизмов в группе $\text{Aut}(P)$ нет.

Пусть элемент α — корень неприводимого над \mathbb{Z}_p многочлена $f(x)$ степени n и $\alpha_2, \alpha_3, \dots, \alpha_n$ — остальные корни этого многочлена. Все эти корни принадлежат полю P , равному $\mathbb{Z}_p(\alpha)$ — простому алгебраическому расширению поля \mathbb{Z}_p . Поэтому любой автоморфизм, оставляющий поле \mathbb{Z}_p неподвижным, однозначно определяется отображением $\alpha \mapsto \alpha_i$ ($i = 2, 3, \dots, n$). Число таких отображений равно n , значит, порядок $\text{Aut}(P)$ тоже равен n .

Отсюда следует, что других автоморфизмов, кроме степеней автоморфизма Фробениуса, у конечного поля нет.

Группа автоморфизмов конечного поля $GF(p^n)$ найдена.

$\text{Aut}(GF(p^n))$ — это циклическая группа порядка n , порожденная автоморфизмом $x \mapsto x^p$ и состоящая из отображений вида $x \mapsto x^{p^i}$.

Отметим попутно, что если α — один из корней минимального многочлена, то все корни этого многочлена имеют вид α^{p^i} , где $i = 0, 1, \dots, n-1$.

Кроме того, из биективности отображения $x \mapsto x^{p^n}$ следует, что для любого натурального n уравнение $x^{p^n} = a$ в поле характеристики p имеет в точности одно решение для любого элемента a .

Особый интерес представляют квадратные двучленные уравнения над конечным полем.

Как и в поле классов вычетов по простому модулю, для произвольного конечного поля определяются квадратичные вычеты и невычеты.

Пусть a — ненулевой элемент конечного поля $GF(p^m)$. Если уравнение $x^2 = a$ имеет решение в поле $GF(p^m)$, то a называют *квадратичным вычетом*. В противном случае, т. е. тогда, когда не существует такого элемента b , что $a = b^2$, элемент a называется *квадратичным невычетом*.

Если g — порождающий мультипликативной группы ненулевых элементов этого поля, то каждый ненулевой элемент этого поля имеет вид g^k . Сравнение

$$2x \equiv k \pmod{2^m - 1}$$

имеет решение для любого целого числа k . Это означает, что уравнение $g^k = x^2$ в поле $GF(2^m)$ имеет решение для любого k , поэтому все ненулевые элементы из $GF(2^m)$ являются квадратичными вычетами.

Если p — нечетное число, то сравнение

$$2x \equiv k \pmod{p^m - 1}$$

имеет решение тогда и только тогда, когда число k четное. Это значит, что четные степени порождающего элемента являются квадратичными вычетами, а нечетные степени — квадратичными невычетами.

Таким образом, в поле $GF(p^m)$ содержится $\frac{p^m-1}{2}$ квадратичных вычетов и ровно столько же квадратичных невычетов.

Одно из важнейших применений конечных полей — это теория кодирования.

7.6. Первоначальное представление о теории кодирования

Систему условных символов для передачи, обработки и хранения различной информации называют кодом¹.

Кодированием принято называть алгоритм отождествления множества символов одного кода с множеством символов другого кода. Необходимость кодирования возникает прежде всего из потребности приспособить форму сообщения к данному каналу связи или устройству, предназначенному для преобразования или хранения информации.

Передаваемую информацию могут исказить помехи в используемой сети. Возникает естественная проблема: как выяснить, нет ли в полученных данных ошибок, и как с наибольшей вероятностью обнаруженные ошибки исправить.

В этой теме обсуждаются элементарные методы решения этих двух задач — обнаружение ошибки (детектирование) и исправление ошибки (корректирование).

При передаче информации можно использовать всего два символа, например ноль и единицу.

Пусть \mathbf{Z}_2^n — арифметическое n -мерное векторное пространство над полем \mathbf{Z}_2 . Векторы из \mathbf{Z}_2^n будем записывать в виде строк без скобок и разделяющих запятых, т. е. в виде слов вида $\alpha_1\alpha_2\dots\alpha_n$, где $\alpha \in \{0, 1\}$. Такое слово, по существу, является функцией, определенной на множестве $\{1, 2, \dots, n\}$ со значениями в множестве $\{0, 1\}$. Носителем слова называется полный прообраз единицы, т. е. множество номеров его единичных букв.

Нулем назовем слово $\mathbf{0}$, состоящее из n нулей, а единицей — слово $\mathbf{1}$, состоящее из n единиц. Носитель нуля — пустое множество, а носителем единицы является все множество $\{1, 2, \dots, n\}$. Пространство \mathbf{Z}_2^n с покомпонентным умножением превращается в булево кольцо, и в этом кольце (и, соответственно, в булевой решетке) $\mathbf{0}$ является нулевым элементом, а $\mathbf{1}$ — единичным.

¹ От лат. *codex* — «свод законов».

Число элементов в носителе слова, т. е. число единиц в записи вектора x , обозначают символом $\|x\|$ и называют *нормой* (или *весом*) *Хэмминга*. Норма Хэмминга обладает всеми свойствами, обычными для модулей векторов евклидовых пространств (для любых x, y из Z_2^n):

- 1) $\|x\| \geq 0$;
- 2) $\|x\| = 0 \Leftrightarrow x = 0$;
- 3) $\|x + y\| \leq \|x\| + \|y\|$.

Точно так же, как в евклидовом пространстве, определим с помощью нормы метрику в Z_2^n , полагая *расстоянием* Хэмминга $\rho(x, y)$ между векторами x, y норму разности этих векторов:

$$\rho(x, y) = \|x - y\|.$$

Поскольку сложение в Z_2 совпадает с вычитанием, $\rho(x, y) = \|x + y\|$.

Расстояние между векторами (в таком контексте их удобнее называть *точками*) равно числу элементов в пересечении носителей этих векторов. Из свойств нормы¹ следуют обычные свойства метрики (для любых x, y, z из Z_2^n):

- 1) $\rho(x, y) = \rho(y, x)$;
- 2) $\rho(x, y) \geq 0$;
- 3) $\rho(x, y) = 0 \Leftrightarrow x = y$;
- 4) $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$.

Свойство 4) имеет обычный геометрический смысл для треугольника с вершинами x, y, z и называется 4) так же, как в геометрии, *неравенством треугольника*.

Так же, как в геометрии, норма вектора x равна расстоянию от x до нулевого вектора — точки, изображающей начало координат:

$$\|x\| = \rho(x, 0).$$

Число векторов, норма которых равна m , равно числу m -элементных подмножеств множества из n элементов. Это число равно $\binom{n}{m}$ — числу сочетаний из n по m .

Отображение, переводящее каждый вектор x в вектор $x + \alpha$, сохраняет расстояние

$$\rho(x, y) = \rho(x + \alpha, y + \alpha).$$

Образно говоря, параллельный перенос на вектор α является движением. В частности, все расстояния между точками фигуры M — подмножества множества Z_2^n — при параллельном переносе (т. е. при переходе к фигуре $M + \alpha$) сохраняются.

¹ Или из свойств пересечения множеств.

Аналогию с элементарной геометрией можно продолжить и далее. Определим *сферу* и *шар* Хэмминга с центром в точке α и радиусом r по правилам:

- сфера: $(\alpha, r) = \{x \in \mathbb{Z}_2^n \mid \rho(x, \alpha) = r\}$;
- шар: $(\alpha, r) = \{x \in \mathbb{Z}_2^n \mid \rho(x, \alpha) \leq r\}$.

Поскольку при параллельном переносе все расстояния между точками фигуры сохраняются, все сферы и все шары одного и того же радиуса состоят из одинакового числа элементов.

Число точек в сфере с центром в точке 0 и радиусом r равно числу векторов нормы k , т. е. равно $\binom{n}{k}$. Каждый шар радиуса r является объединением сфер с тем же центром и радиусами $k = 0, 1, \dots, r$. Поэтому число точек в шаре радиуса r равно

$$\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{k} + \dots + \binom{n}{r}.$$

Подмножество V векторного пространства \mathbb{Z}_2^n называют кодом.

В реальности код возникает как образ отображения некоторого пространства $\mathbb{Z}_2^{n_1}$ в пространство \mathbb{Z}_2^n , где $n_1 < n$. Отображение принято называть *передачей*, а результаты передачи — *сообщениями*. Таким образом, V — это все сообщения, которые могут поступить при передаче. В процессе передачи возможные помехи могут исказить передаваемые слова, и в результате будет принято слово с *ошибками*, т. е. в некоторых местах полученного слова вместо символа 1 будет стоять символ 0 или вместо 0 появится 1.

Говорят, что код $V = \{a_1, a_2, \dots, a_m\}$ обнаруживает t ошибок, если в любом кодовом слове a_i изменение t или менее символов приводит к слову, не принадлежащему множеству V .

Если при передаче получено слово с ошибками, то при наличии канала обратной связи можно сделать запрос, чтобы повторить передачу и исправить ошибки.

Если в слове a сделано в точности k ошибок, то ошибочное слово a_1 находится от истинного слова на расстоянии k . Это значит, что если в слове сделано t или менее ошибок, то слово останется внутри шара с центром в точке a и с радиусом t .

Таким образом, возможность кода обнаружить t ошибок равносильна тому, что каждый шар Хэмминга, центром которого является произвольное кодовое слово, а радиус равен t , не содержит никакой другой кодовой точки. Иначе говоря, код V обнаруживает t ошибок тогда и только тогда, когда расстояние Хэмминга между двумя любыми точками из V строго больше t .

Возможность кода V исправить t ошибок равносильна тому, что все шары Хэмминга, центрами которых являются кодовые слова из V , а радиусы равны t , не имеют общих точек.

Другими словами, код V способен исправить t ошибок тогда и только тогда, когда расстояние Хэмминга между двумя любыми точками из V строго больше $2t$.

Если расстояние между каждой парой кодовых слов строго больше $2t$, то слово, переданное с t ошибками, принадлежит одному из шаров радиусом t с центром в кодовой точке, и это слово естественно декодировать как центр этого шара¹.

Отсюда следует, что основной характеристикой кода V является минимальное расстояние $d(V)$ между его точками.

Код V может обнаружить t ошибок, если $d(V) > t$, и исправить k ошибок, если $d(V) > 2k$.

Параллельный перенос не изменяет расстояния между точками, поэтому для любого множества V и каждого вектора a

$$d(V + a) = d(V).$$

Это значит, что, имея один код с нужными свойствами, можно получить еще несколько кодов с такими же возможностями обнаружения и исправления ошибок.

Можно получить новый код из данного V и другим способом. Запишем все элементы из V в столбик в виде матрицы

$$\begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_m \end{pmatrix}$$

и сделаем любую перестановку *столбцов* этой матрицы. Новые строки полученной матрицы представляют новый код V_1 . Все расстояния между новыми элементами останутся прежними; не изменится и минимальное расстояние: $d(V) = d(V_1)$. Два кода, отличающиеся лишь такой перестановкой, называют *эквивалентными*.

Максимальное число таких точек пространства \mathbf{Z}_2^n , что расстояние между каждой парой из них строго больше d , принято обозначать символом $A(n, d)$.

Пусть V_k — произвольное k -элементное подмножество из \mathbf{Z}_2^n . Наибольшее возможное значение числа $d(V_k)$ обозначают символом $d(k, n)$.

Числа $A(n, d)$ и $d(k, n)$ являются корректирующими способностями кода.

Если значение n задано, то при построении конкретного кода главная задача состоит в том, чтобы эти способности оказались реализованными.

¹ Говорят «декодирование по максимуму правдоподобия».

Другими словами, основными задачами теории кодирования являются:

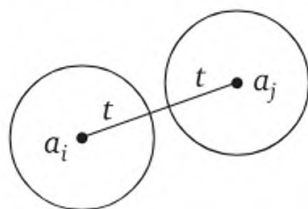
- 1) для данных n, t найти набор из $A(n, 2t + 1)$ кодовых слов;
- 2) для данного n найти такой набор V из k кодовых слов, чтобы $d(V) = d(k, n)$.

Под словами «найти набор» имеется в виду не просто задание кода V списком или перечисляющим алгоритмом, а указание простого алгоритма, решающего проблему вхождения в V .

Отметим, что функции $A(n, d)$ и $d(k, n)$ связаны простым соотношением

$$A(n, d(k, n)) = k.$$

Для того чтобы код V позволял исправлять t ошибок, необходимо и достаточно, чтобы все окрестности ошибок, т. е. все шары Хэмминга с центрами в кодовых словах и с радиусами t , не пересекались.



Шары Хэмминга не пересекаются

Число точек в шаре радиуса t равно

$$\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{t},$$

поэтому

$$|V| \cdot \left(\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{t} \right) \leq |\mathbb{Z}_2^n| = 2^n.$$

Отсюда получается верхняя оценка для $A(n, 2t + 1)$ — максимального числа таких шаров (следовательно, и элементов из V):

$$A(n, 2t + 1) \leq \frac{2^n}{1 + \binom{n}{1} + \dots + \binom{n}{t}}.$$

Это неравенство называют *границей Хэмминга*.

Код, при котором непересекающиеся шары Хэмминга полностью заполняют все пространство \mathbb{Z}_2^k , называется *совершенным* или *плотно упакованным*. В этом случае неравенство Хэмминга превращается в равенство, правая часть которого является *границей плотной упаковки*.

Можно оценить число $A(n, 2t + 1)$ и снизу. Окружим каждую точку кода V , исправляющего t ошибок, шаром радиусом $2t$. Поскольку $d(V) > 2t$, каждый такой шар содержит в точности одну кодовую точку. Каждый шар содержит

$$\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{2t}$$

точек. Если бы объединение таких шаров не совпадало с \mathbb{Z}_2^n , то нашлась бы по крайней мере одна точка, удаленная от любого кодового слова на расстояние, большее $2t$, что противоречит максимальной $A(n, 2t + 1)$. Следовательно, объединение всех шаров совпадает с \mathbb{Z}_2^n . Эти шары могут иметь и общие точки, поэтому число всех элементов во всех шарах не меньше общего числа элементов в \mathbb{Z}_2^n :

$$A(n, 2t + 1) \cdot \left(1 + \binom{n}{1} + \dots + \binom{n}{2t} \right) \geq |\mathbb{Z}_2^n| = 2^n,$$

откуда

$$A(n, 2t + 1) \geq \frac{2^n}{1 + \binom{n}{1} + \dots + \binom{n}{2t}}.$$

Эту оценку называют границей Варшамова — Гилберта. Таким образом,

$$\frac{2^n}{1 + \binom{n}{1} + \dots + \binom{n}{t}} \geq A(n, 2t + 1) \geq \frac{2^n}{1 + \binom{n}{1} + \dots + \binom{n}{2t}}.$$

Например, для $t = 1, n = 15$

$$\frac{2^{15}}{1 + 15} \geq A(15, 3) \geq \frac{2^{15}}{1 + 15 + \frac{15(15-1)}{2}},$$

что дает очень грубую оценку¹:

$$2048 \geq A(15, 3) \geq 271.$$

Код V называется *линейным*, если V образует подпространство пространства \mathbb{Z}_2^n . Поскольку умножение на скаляр в \mathbb{Z}_2^n носит чисто формальный характер, для линейности кода достаточно замкнутости V по сложению. Другими словами, код V линейный, если он является подгруппой группы $\langle \mathbb{Z}_2^n; + \rangle$.

¹ На самом деле $A(15, 3) = 2048$.

По этой причине линейный код называют еще и *групповым*¹.

Пусть x — ненулевой элемент из линейного кода V — имеет наименьшую норму k в V . Если y — любой другой элемент из V , то $x + y$ тоже принадлежит V и, следовательно,

$$\rho(x, y) = \|x + y\| \geq k.$$

Это значит, что для линейного кода V наименьшее расстояние $d(V)$ между элементами V равно наименьшей норме ненулевого элемента:

$$d(V) = \min\{\|x\| \mid x \in V \setminus \{0\}\}.$$

Таким образом, для нахождения $d(V)$ линейного кода достаточно вычислить $|V| - 1$ норм элементов, а не

$$\frac{|V| \cdot (|V| - 1)}{2}$$

расстояний между элементами, что необходимо для произвольного кода V .

Как подпространство, так и подгруппа полностью задаются своим порождающим множеством. Порождающие векторы линейного кода V , выписанные в столбик, один под другим, образуют матрицу, которую называют *порождающей* для V . Естественно, что имеет смысл выписывать не просто порождающие, а базисные векторы для V .

Итак, линейный код полностью задается порождающей матрицей, в которой строки можно считать линейно независимыми. Верно и обратное утверждение: любая $(k \times n)$ -матрица с элементами из \mathbb{Z}_2 (и линейно независимыми строками) определяет линейный код V размерности k .

Итак, если A — порождающая $(r \times n)$ -матрица кода V , то элемент x из \mathbb{Z}_2^n принадлежит множеству V тогда и только тогда, когда x является линейной комбинацией строк матрицы A . Поскольку в поле \mathbb{Z}_2 всего лишь два элемента, линейная комбинация — это просто сумма некоторых векторов. Линейная независимость системы из r векторов для поля \mathbb{Z}_2 означает, что любая сумма векторов этой системы не равна нулевому вектору.

Если $\text{rank}(A) = r$, т. е. строки матрицы A линейно независимы, то V образует подпространство размерности r . Линейный код, образующий подпространство размерности r в пространстве \mathbb{Z}_2^n , называют (n, r) -кодом.

Две матрицы порождают один и тот же код, если строки одной матрицы линейно выражаются через строки другой.

¹ Так будет только для пространства над полем \mathbb{Z}_2 .

Если проделать перестановку столбцов порождающей матрицы кода V , то эта же перестановка произойдет во всех кодовых словах, т. е. новая матрица порождает код, эквивалентный коду V .

Линейный код V является, в частности, подгруппой аддитивной группы $\langle \mathbb{Z}_2; + \rangle$, поэтому число элементов в V делит $|\mathbb{Z}_2^n| = 2^n$. Следовательно, число элементов в V равно 2^k .

Если k — размерность линейного кода, который исправляет t ошибок, то неравенство Хэмминга принимает вид

$$2^k \leq \frac{2^n}{1 + \binom{n}{1} + \dots + \binom{n}{t}},$$

что равносильно

$$k \leq n - \log_2 \left(1 + \binom{n}{1} + \dots + \binom{n}{t} \right).$$

Граница Варшамова — Гилберта позволяет оценить размерность линейного кода, исправляющего t ошибок, снизу:

$$2^k \geq \frac{2^n}{1 + \binom{n}{1} + \dots + \binom{n}{2t}},$$

что равносильно

$$k \geq n - \log_2 \left(1 + \binom{n}{1} + \dots + \binom{n}{2t} \right).$$

Каждое подпространство арифметического конечномерного векторного пространства является множеством решений некоторой системы однородных линейных уравнений. Эта система полностью задается своей матрицей B коэффициентов уравнений. Эту матрицу называют *проверочной* матрицей линейного кода. Размерность V линейного кода равна числу свободных неизвестных в задающей системе линейных уравнений, поэтому

$$\text{rank}(B) = n - \dim V.$$

Естественно, можно считать, что строки проверочной матрицы B и строки матрицы A , порождающей (n, k) -код V , линейно независимы. В этом случае проверочная матрица B имеет $(n - k)$ строк и n столбцов.

Если B — проверочная $(n - k) \times n$ -матрица (n, k) -кода V , то элемент x из \mathbb{Z}_2^n принадлежит множеству V тогда и только тогда, когда $Bx^T = \mathbf{0}$, где $\mathbf{0}$ — нулевой вектор-столбец из пространства столбцов \mathbb{Z}_2^{n-k} .

Иначе говоря, линейный код V — это ядро линейного отображения пространства столбцов Z_2^n в пространство столбцов Z_2^{n-k} , заданного $(n - k) \times n$ -матрицей B .

Находится проверочная матрица обычным для линейной алгебры приемом: разысканием ортогонального дополнения для подпространства, заданного порождающими векторами. Два вектора $x = \alpha_1\alpha_2\ldots\alpha_n$ и $y = \beta_1\beta_2\ldots\beta_n$ назовем *ортогональными*, если

$$\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots + \alpha_n\beta_n = 0.$$

То, что пространство Z_2^n неевклидово, т. е. скалярное произведение здесь не совсем обычно (вектор может оказаться ортогональным самому себе), нисколько не мешает достижению поставленной цели. Как и в евклидовом пространстве, подпространство H^\perp разыскивается как множество решений системы однородных линейных уравнений, и $H^{\perp\perp} = H$.

Код V^* , порожденный проверочной матрицей кода V , называют *двойственным* к коду V . Проверочной матрицей кода V^* можно взять порождающую матрицу для V .

Пусть V — групповой (n, k) -код с $(n - k) \times n$ -матрицей M в качестве проверочной, т. е.

$$V = \{x \in Z_2^n \mid Mx^T = 0\}.$$

Пусть вектор $x = \alpha_1\alpha_2\ldots\alpha_n$ принадлежит V . Тогда

$$xM^T = 0.$$

Распишем произведение xM^T по столбцам m_1, m_2, \ldots, m_n матрицы M и получим, что линейная комбинация столбцов с коэффициентами из множества $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ равна нулевому вектору:

$$\alpha_1m_1 + \alpha_2m_2 + \ldots + \alpha_nm_n = 0 \quad (*)$$

Эта комбинация на самом деле является просто суммой векторов. Число ненулевых слагаемых в этой сумме равно числу ненулевых α_i в записи вектора x , т. е. равно норме вектора $\|x\|$.

Если любая система из $r - 1$ столбца матрицы M линейно независима, то равенство $(*)$ становится возможным только тогда, когда $\|x\| \geq r$ и, следовательно, $d(V) \geq r$.

Если же каждая система из $(r - 1)$ столбца матрицы M линейно независима, но существует линейно зависимая система из r столбцов, то $d(V) = r$.

Итак, возможности определения (*детектирования*) и исправления (*корректирования*) числа ошибок линейного кода можно оценить по его проверочной матрице. Особенно проста эта оценка для случая $r = 2$.

Два ненулевых вектора из \mathbf{Z}_2^n линейно зависимы (коллинеарны) тогда и только тогда, когда они равны. Это значит, что если все столбцы проверочной матрицы кода V отличны от нуля и различны, то $d(V) \geq 3$ и код V способен исправить не менее одной ошибки.

Пусть B — проверочная $(n - k) \times n$ -матрица линейного (n, k) -кода V . Аддитивная группа $\langle \mathbf{Z}_2^n; + \rangle$ распадается на смежные классы по подгруппе V :

$$\mathbf{Z}_2^n = (V + b_0) + (V + b_1) + \dots + (V + b_{s-1}).$$

Число

$$s = [\mathbf{Z}_2^n : V] = \frac{2^n}{2^k} = 2^{n-k} —$$

индекс подгруппы V в \mathbf{Z}_2^n .

Любой вектор из \mathbf{Z}_2^n , лежащий в смежном классе, отличном от V , ошибочный и не принадлежит множеству V . Иначе говоря, все векторы, не принадлежащие множеству V , сдвинуты на вектор ошибки.

Этим вектором ошибки является представитель смежного класса. В качестве представителя класса V выберем $b_0 = \mathbf{0}$. Тогда если вектор принадлежит коду V , то его вектор ошибки равен нулю.

Верно и обратное утверждение, а это значит, что вектор является кодовым словом тогда и только тогда, когда его вектор ошибки равен нулю. Носитель вектора ошибки показывает, какие именно символы в данном слове ошибочны.

Впрочем, знание носителя вектора ошибки даже излишне: с помощью вектора ошибки b_i , где $i \in \{2, 3, \dots, s - 1\}$, можно не только узнать, что данный вектор x ошибочен, но и исправить все ошибки, заменив вектор x на вектор $x + b_i$.

Вектор yB^T называют синдромом вектора y .

Вектор является кодовым словом тогда и только тогда, когда его синдром равен нулю.

Пусть y — вектор с ошибками, т. е. $yB^T \neq \mathbf{0}$, и кроме того $y = x + b_i$, где x из V , а $i \in \{2, 3, \dots, s - 1\}$. Тогда

$$(x + y)B^T = xB^T + yB^T = yB^T.$$

Это значит, что все элементы, имеющие один и тот же вектор ошибки (т. е. лежащие в одном смежном классе по подгруппе V), имеют один и тот же синдром.

Верно и обратное утверждение, следовательно,

$$\text{синдром } a = \text{синдром } b \Leftrightarrow a \equiv b \pmod{V}.$$

Знание смежного класса, которому принадлежит вектор ошибки, еще не определяет сам этот вектор. Если считать, что вероятность

большого числа ошибок меньше вероятности меньшего их числа, то в качестве представителя смежного класса целесообразно выбрать векторы с наименьшей нормой. Представитель в классе V уже выбран — это нулевой вектор.

Представителей смежных классов с минимальной нормой принято называть *лидерами* (или *ведущими элементами*) класса.

Если в каждом смежном классе в точности один лидер, то с помощью таблицы лидеров и их синдромов можно теперь декодировать любое слово x .

Лидер	b_2	$b_3,$...	b_{s-1}
Синдром лидера	b_2B^T	b_3B^T	...	$b_{s-1}B^T$

Для этого сначала вычисляем синдром xB^T этого вектора. Если синдром нулевой, то $x \in V$. Если $xB^T \neq 0$, то найдется такой номер $i \in \{2, 3, \dots, s-1\}$, что $xB^T = b_iB^T$. Тогда $x + b_i$ — исправленный вектор.

В некотором смежном классе может оказаться несколько лидеров, тогда состоится лишь детектирование ошибки без ее исправления.

Рассмотрим один важный пример линейного кода и декодирования по синдрому.

Пусть $n = 2^k - 1$, где k — натуральное число больше единицы, и линейное отображение $\varphi: \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^k$ задается $(n \times k)$ -матрицей M , строки которой состоят из всех ненулевых векторов пространства \mathbb{Z}_2^k , т. е. (для всех элементов x из \mathbb{Z}_2^n)

$$\varphi(x) = xM.$$

Ядро φ образует линейный код V :

$$V = \text{Ker } \varphi = \{x \in \mathbb{Z}_2^n \mid \varphi(x) = 0\}.$$

Таким образом, получаем $(n, n-k)$ -код V . Матрица M^T является проверочной для V :

$$V = \{x \in \mathbb{Z}_2^n \mid xM^T = 0\}.$$

Все столбцы проверочной матрицы M^T различны, поэтому $d(V) \geq 3$, т. е. V является кодом, исправляющим одну ошибку. Число элементов в таком коде равно

$$\frac{|\mathbb{Z}_2^n|}{|\mathbb{Z}_2^k|} = \frac{2^n}{2^k} = 2^{n-k}.$$

Посмотрим на оценку Хэмминга $A(n, 3)$ при $n = 2^k - 1$:

$$A(n, 3) \geq \frac{2^n}{1+n} = \frac{2^n}{1+2^k-1} = 2^{n-k}.$$

Таким образом, число различных кодовых слов из V в точности равно числу различных шаров Хэмминга с радиусом 1.

Оценка становится точной. Этот код совершенный.

Совершенный код длины $2^k - 1$, исправляющий одну ошибку, называют двоичным (или бинарным) кодом Хэмминга.

Если V — двоичный код Хэмминга, то фактор-пространство \mathbb{Z}_2^n / V изоморфно пространству \mathbb{Z}_2^k .

Представителями смежных классов пространства \mathbb{Z}_2^n по подпространству V можно выбрать элементы пространства \mathbb{Z}_2^k . По существу, они и будут играть роль лидеров.

Проверочной матрицей бинарного кода Хэмминга является матрица M^T , столбцы которой состоят из всех ненулевых векторов пространства \mathbb{Z}_2^k , расположенных, вообще говоря, совершенно произвольно.

Расположим эти столбцы в M^T (а в матрице M — строки) не произвольно, а таким образом, чтобы каждый столбец M^T (соответственно, строка в M) изображал двоичную запись своего номера. Например, для $n = 7, k = 3$ матрица M будет иметь вид

$$M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Теперь если вектор x содержит ошибочный символ в i -м месте, то синдром xM равен i -й строке матрицы M . Прочитав эту строку как число в двоичной записи, получаем номер ошибочного символа в векторе x .

Параллельный перенос множества не изменяет расстояний между точками этого множества. Поэтому если V — двоичный код Хэмминга, то и все смежные классы $V + b$ также образуют совершенные коды.

Оказалось, что существуют совершенные коды V с $d(V) = 3$, не являющиеся смежными классами по коду Хэмминга (и более того, не переводимые друг в друга параллельными переносами).

В коде V^* , двойственном бинарному (n, m) -коду Хэмминга, содержится 2^m элементов, причем все ненулевые векторы имеют одну и ту же норму, равную

$$\frac{n+1}{2} = 2^{m-1}.$$

Код, у которого все попарные расстояния между элементами равны, называется эквидистантным. Код V^* эквидистантный.

Рассмотрим арифметическое n -мерное векторное пространство \mathbb{Z}_2^n над полем \mathbb{Z}_2 . Циклическим сдвигом вектора $a = \alpha_0\alpha_1\ldots\alpha_{n-1}$ из \mathbb{Z}_2^n называют вектор

$$a_1 = \alpha_{n-1}\alpha_0\alpha_1\ldots\alpha_{n-2}.$$

Код называется *циклическим*, если вместе с каждым вектором он содержит и его циклический сдвиг.

Сдвиг вектора лучше всего описать с помощью группового кольца \mathbb{Z}_2G циклической группы $G = \langle x; x^n \rangle$. Каждому вектору $a = \alpha_0\alpha_1\ldots\alpha_{n-1}$ из \mathbb{Z}_2^n поставим в соответствие элемент

$$a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$$

из кольца \mathbb{Z}_2G .

Элемент $a(x)$ имеет вид многочлена, и сложение этих многочленов обычное (соответствует сложению в \mathbb{Z}_2^n), однако при умножении необходимо учитывать, что $x^n = 1$.

Кольцо \mathbb{Z}_2G изоморфно фактор-кольцу $\mathbb{Z}_2[x]/(x^n - 1)$, и элементами его действительно являются все многочлены над \mathbb{Z}_2 степени, строго меньшей n .

Поскольку алгебры $\langle \mathbb{Z}_2^n; + \rangle$ и $\langle \mathbb{Z}_2G; + \rangle$ изоморфны, будем теперь под n -мерными векторами понимать элементы из \mathbb{Z}_2G (называя их и векторами, и многочленами в зависимости от ситуации).

Код V является линейным тогда и только тогда, когда множество V замкнуто относительно сложения.

Циклический сдвиг осуществляется простым умножением элемента $a(x)$ на x :

$$\begin{aligned} a(x)x &= a_0x + a_1x^2 + \ldots + a_{n-2}x^{n-1} + a_{n-1}x^n = \\ &= a_{n-1} + a_0x + a_1x^2 + \ldots + a_{n-2}x^{n-1}. \end{aligned}$$

Двойной сдвиг осуществляется умножением на x^2 , тройной — на x^3 и т. д. Другими словами, если код V циклический, то для любого натурального k и любого $a(x)$ из V элемент $a(x)x^k$ снова принадлежит V . Пусть

$$f(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1} —$$

произвольный элемент из \mathbb{Z}_2G . Тогда

$$\begin{aligned} a(x) \cdot f(x) &= a(x)(b_0 + b_1x + \ldots + b_{n-1}x^{n-1}) = \\ &= a(x)b_0 + b_1 \cdot a(x)x + \ldots + b_{n-1} \cdot a(x)x^{n-1}. \end{aligned}$$

Если код V циклический, то каждое слагаемое полученной суммы снова принадлежит V , а если V к тому же и линейный, то и вся сумма находится в V .

Таким образом, линейный код является циклическим тогда и только тогда, когда он замкнут относительно умножения на любой элемент из \mathbb{Z}_2G .

Заметим, что кольцо \mathbb{Z}_2G ассоциативно-коммутативное с единицей и характеристикой $\text{char } \mathbb{Z}_2G = 2$. Операции сложения и вычитания в этом кольце совпадают.

Иначе говоря, непустое подмножество этого кольца, замкнутое относительно сложения, является подкольцом, а если оно к тому же замкнуто относительно умножения на элементы из \mathbb{Z}_2G , то — идеалом.

Таким образом, если линейный код является циклическим, то он является идеалом в \mathbb{Z}_2G .

Любой идеал кольца \mathbb{Z}_2G замкнут относительно сложения, поэтому каждый идеал образует линейный циклический код.

Кольцо $\mathbb{Z}_2[x]$ евклидово (поэтому в нем каждый идеал главный). В фактор-кольце

$$\mathbb{Z}_2[x]/(x^n - 1)$$

тоже выполняется теорема о делении с остатком (наличие делителей нуля и ограниченность степени многочлена не мешают доказательству существования частного и остатка). Как обычно, из теоремы о делении с остатком следует, что в этом кольце все идеалы главные.

Это значит, что линейный циклический код V как идеал является 1-порожденным, т. е. состоит из всевозможных кратных одного элемента.

Циклический код является линейным, поэтому он имеет порождающую и проверочную матрицы. Если

$$g(x) = g_0 + g_1x + \dots + g_mx^m —$$

многочлен степени m (где $m < n$), порождающий циклический код, то многочлены

$$g(x), xg(x), x^2g(x), \dots, x^{n-m-1}g(x)$$

являются кодовыми, степень каждого из них не больше $(n - 1)$ и они линейно независимы.

Следовательно, матрица M ,

$$M = \begin{pmatrix} g(x) \\ xg(x) \\ \dots \\ x^{n-m-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \dots & g_m & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{m-1} & g_m & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_m \end{pmatrix},$$

составленная из коэффициентов этих многочленов, порождает циклический код $(g(x))$.

Матрицей Адамара¹ H_n называют такую квадратную $(n \times n)$ -матрицу с элементами $+1$ и -1 из поля действительных чисел, что ее строки попарно ортогональны. Например:

$$H_1 = (1), \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Если $H_n = (a_{ij})$ — матрица Адамара, то для всех i, j из $\{1, 2, \dots, n\}$

$$\sum_{k=1}^n a_{ik} a_{jk} = \begin{cases} 0, & \text{если } i \neq j, \\ n, & \text{если } i = j. \end{cases}$$

Это значит, что условие попарной ортогональности строк такой матрицы равносильно равенству

$$H_n H_n^T = nE.$$

Сумма любых двух элементов строк матрицы Адамара равна 0 или 2. Пусть матрица Адамара содержит по крайней мере три строки. Тогда каждое слагаемое в сумме

$$\sum_{k=1}^n (a_{1k} + a_{2k})(a_{2k} + a_{3k})$$

равно 4, -4 или 0, и, следовательно, эта сумма делится на четыре. Раскроем скобки в каждом слагаемом суммы и получим:

$$\begin{aligned} & \sum_{k=1}^n (a_{1k} + a_{2k})(a_{2k} + a_{3k}) = \\ & = \sum_{k=1}^n a_{1k} a_{2k} + \sum_{k=1}^n a_{2k}^2 + \sum_{k=1}^n a_{1k} a_{3k} + \sum_{k=1}^n a_{2k} a_{3k} = \sum_{k=1}^n a_{2k}^2 = n. \end{aligned}$$

Таким образом, если $n > 2$ и H_n — матрица Адамара, то n делится на 4.

По виду матриц H_1, H_2, H_4 можно усмотреть некоторую закономерность образования H_2, H_4 . Эта закономерность продолжается и далее, т. е. если H_n — матрица Адамара порядка n , то матрица

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix} —$$

тоже матрица Адамара порядка $2n$.

¹ Жак Соломон Адамар (Hadamard, 1865—1963) — французский математик, иностранный член-корреспондент (1922) и иностранный почетный член (1929) АН СССР.

Таким образом, для любого m существует¹ матрица Адамара порядка 2^m .

Впрочем, на эту же закономерность можно взглянуть чуть иначе, и тогда прием получения новых матриц Адамара становится более общим.

Если $H_k, H_n = (a_{ij})$ — две матрицы Адамара, то матрица

$$H_{kn} = (a_{ij}H_k) —$$

тоже матрица Адамара порядка kn .

Заменим в H_n в каждой строке элемент $+1$ на 0 , а -1 — на 1 . Тогда множество строк V полученной матрицы образует код. Из того, что скалярное произведение любых двух строк матрицы Адамара H_n равно нулю, следует, что любые две строки H_n совпадают в точности в $\frac{n}{2}$ местах и отличаются знаками в остальных. Это означает, что расстояние между любыми кодовыми словами из V равно в точности $\frac{n}{2}$.

Таким образом, из каждой матрицы Адамара порядка n в \mathbb{Z}_2^n можно построить эквидистантный код V , содержащий n элементов, причем $d(V) = \frac{n}{2}$.

На этом завершается обзор основных структур и фундаментальных результатов абстрактной алгебры.

Следующие темы посвящаются использованию вычислительной техники для решения конкретных задач символьных вычислений.

Одним из лучших современных пакетов символьных математических вычислений, пригодным для этих целей, является пакет *Maple*.

В этом пакете возможно достаточно детальное компьютерное исследование довольно сложных алгебраических объектов, какими являются, например, группы подстановок.

Контрольные задания

1. Докажите, что составное алгебраическое расширение поля — конечно.
2. Докажите, что в конечном расширении размерности n существует алгебраический элемент степени n .
3. Докажите, что составное алгебраическое расширение является алгебраическим.
4. Докажите, что размерность промежуточного расширения является делителем основной размерности.
5. Докажите, что множество алгебраических чисел образует поле, и это поле алгебраически замкнуто.

¹ Есть предположение, что матрица Адамара существует для любого порядка, кратного четырем.

6. Докажите, что конечное расширение поля — алгебраично.
7. Докажите, что множество алгебраических чисел является алгебраическим, но не конечным расширением поля \mathbb{Q} .
8. Докажите, что для каждого поля P и каждого многочлена $f(x)$ с коэффициентами из поля P существует поле P_1 , содержащее изоморфную копию поля P и все корни многочлена $f(x)$.
9. Докажите, что для каждого поля существует алгебраическое замыкание этого поля.
10. Докажите, что для каждого поля P существует расширение P_1 такое, что поля P и P_1 не изоморфны.

Тема 8

КОМПЬЮТЕРНОЕ ИССЛЕДОВАНИЕ ГРУПП

Основные понятия: подгруппа, смежный класс, индекс, гомоморфизм, изоморфизм, мономорфизм, группа подстановок, ядро гомоморфизма, нормальный делитель, фактор-группа, естественный гомоморфизм, коммутант, центр, нижний центральный ряд.

Основные факты: для групп подстановок и конечных групп небольших порядков с помощью компьютера можно определить порядок, наличие или отсутствие тождеств, найти копредставление подгрупп и фактор-групп, проверить подгруппу на нормальность, вычислить коммутант, центр и члены нижнего центрального ряда, найти силовские подгруппы.

В системе компьютерной алгебры *Maple* исследование групп осуществляется с помощью пакета *Group Theory*. Чтобы исследовать группу подстановок, нужно сначала войти в этот пакет. Вход осуществляется командой *with(group)*.

Если поставить в конце команды точку с запятой, то машина покажет команды для решения теоретико-групповых задач:

```
> with(group);  
[DerivedS, LCS, NormalClosure, RandElement, SnConjugates,  
Sylow, areconjugate, center, centralizer, core, cosets, cosrep,  
derived, elements, groupmember, grouporder, inter, invperm,  
isabelian, isnormal, issubgroup, mulperms, normalizer, orbit,  
parity, permrep, pres, transgroup];
```

Для непосредственного использования теоретико-групповых команд удобнее воспользоваться командой *?group*.

Согласно теореме Кэли, любую конечную группу можно изоморфно представить в виде группы подстановок.

Сейчас мы рассмотрим назначение и особенности использования машинных команд, предназначенных для исследования групп подстановок, т. е., по существу, команд для изучения конечных групп.

8.1. Исследование групп подстановок

Группа подстановок — это подгруппа симметрической группы S_n . Симметрическая группа состоит из всевозможных взаимно

однозначных отображений множества $\{1, 2, \dots, n\}$ на себя. Число n принято называть *степенью* подстановки.

Если группа, например S_n , уже задана, то любой набор ее элементов порождает некоторую подгруппу, в данном случае — группу подстановок степени n . Наоборот, любую подгруппу группы S_n можно задать ее порождающим множеством.

Итак, для задания группы подстановок H достаточно указать ее порождающие, т. е. некоторые элементы из S_n . Если m — наибольшее число, фигурирующее в подстановках, то степень подстановок из H не меньше m . Однако степень может быть и больше m ; в этом случае все символы, превышающие m , подстановки из H оставляют неподвижными.

Это значит, что для корректного задания группы подстановок H необходимо указать степень ее подстановок и порождающие элементы. Именно это и проделывается в пакете *Group Theory* с помощью команды *permgrou*.

Рассмотрим пример применения команды *permgrou*. Пусть группа подстановок H состоит из подстановок степени 7 и порождается подстановками $(1\ 2\ 3\ 4\ 5)$, $(4\ 5)$ $(6\ 7)$. Машинное задание этой группы выглядит так:

```
> with(group):  
> H := permgrou(7, {[[1, 2, 3, 4, 5]], [[4, 5], [6, 7]]}):
```

Особенности записи для машины состоят в том, что каждый цикл подстановки и дополнительно сама подстановка окружены квадратными скобками, а вместо пробелов, разделяющих перемещаемые символы, используются запятые. Запятые разделяют как отдельные подстановки, так и циклы в подстановке.

После выполнения этой команды под символом H (и если в дальнейшем не будет придано другое значение букве H) машина в течение всего сеанса в *Maple* будет понимать именно эту группу подстановок.

Заметим, что после выхода из *Maple* в сохраненном файле эта информация (включая и вход в пакет *Теория групп*) будет потеряна и ее придется ввести заново, т. е. нажать клавишу *Enter* на всех командных строках файла.

Следует отметить еще, что видимый результат работы команды ввода группы подстановок (если в конце ее поставить точку с запятой) не зависит от входа в пакет *Group Theory*. Однако если этот вход не состоялся, т. е. отсутствует команда *with(group)*, то ни одной теоретико-групповой задачи с символом H техника решить не сможет — она просто будет переписывать поставленный вопрос другим цветом.

Для задания группы подстановок необходимо, чтобы ее порождающие уже были представлены в виде произведения независимых циклов. Найти такое представление для подстановки

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n-1) & \alpha(n) \end{pmatrix}$$

можно с помощью машинной команды

```
convert ([α(1), α(2), ..., α(n - 1), α(n)], 'disjcyc').
```

Для выполнения этой команды входить в пакет *Group Theory* обязательно:

```
> convert ([8, 7, 6, 5, 4, 1, 2, 3], 'disjcyc');
```

```
[[1, 8, 3, 6], [2, 7], [4, 5]]
```

Полученный результат означает, что

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix} = (1836)(27)(45).$$

Обратный переход от циклового представления подстановки α к представлению α второй строкой —

$[\alpha(1), \alpha(2), \dots, \alpha(n-1), \alpha(n)]$ —

осуществляется командой `convert (α, 'permlist', n)`, где n — степень подстановки. Проверим только что проведенные вычисления циклового представления:

```
> convert ([[1, 8, 3, 6], [2, 7], [4, 5]], 'permlist', 8);
```

```
[8, 7, 6, 5, 4, 1, 2, 3]
```

Если группа подстановок порождается подстановками, часть которых задана с помощью вторых строк, то их придется предварительно конвертировать в нужный вид. Например:

```
> with(group):
> G := permgroup (5, {convert ([4, 3, 2, 5, 1], 'disjcyc'),
  convert ([5, 4, 3, 2, 1], 'disjcyc'),
  > [[1, 2, 3]]});
```

```
G := permgroup (5, {[[1, 2, 3]], [[1, 4, 5], [2, 3]], [[1, 5], [2, 4]]})
```

Самая большая (по включению и по порядку, т. е. по числу элементов) группа подстановок степени n — это сама симметрическая группа S_n . Группа S_n может быть порождена всего лишь двумя элементами (говорят «2-порожденная группа»), а в качестве порождающих элементов можно взять подстановки $(1\ 2)$ и $(1\ 2\ 3\ \dots\ n)$.

Например, для задания группы S_4 достаточно указать в качестве порождающих элементов подстановки $(1\ 2)$ и $(1\ 2\ 3\ 4)$:

```
> with(group):
> S[4] := permgroup(4, {[[1, 2]], [[1, 2, 3, 4]]});
```

$$S_4 := \text{permgroup}(4, \{[[1, 2]], [[1, 2, 3, 4]]\})$$

Современной компьютерной технике, к сожалению, нельзя доверять безоговорочно. Лучше каждый полученный компьютерный результат тут же проверить. Например, нам известно, что группа S_4 состоит из 24 элементов (а произвольная симметрическая группа содержит $n!$ элементов). Поэтому для контроля, верно ли машина поняла команду о вводе группы S_4 , можно просто узнать порядок этой группы.

Порядок группы вычисляется с помощью команды *grouporder*.

Вычислим, например, порядок группы S_4 (после знака *#* пишется невыполняемая команда, например комментарий):

```
> with(group):
> S[4] := permgroup(4, {[[1, 2]], [[1, 2, 3, 4]]}): # задание
группы  $S_4$ 
> grouporder(S[4]); # вычисление порядка  $S_4$ 
```

24

Если бы команда *with(group)* отсутствовала, то результатом работы было бы безынформативное сообщение

$$\text{grouporder}(\text{permgroup}(4, \{[[1, 2]], [[1, 2, 3, 4]]\})).$$

Если требуется вычислить лишь порядок данной группы подстановок, а для дальнейших символьных вычислений сама группа не потребуется, то ее порядок можно найти, не вводя специального обозначения. Например,

```
> with(group):
> grouporder(permgroup(10, {[[1, 2]], [[1, 2, 3, 4, 5, 6, 7,
8, 9, 10]]}));
```

3628800

Как и ожидалось, порядок группы S_{10} равен $10!$.

Порядок элемента — это порядок подгруппы, порожденной данным элементом.

Таким образом, команда

$$\text{grouporder}(\text{permgroupe}(m, \{\alpha\})),$$

где m — натуральное число, а α — подстановка степени $\leq m$, вычисляет порядок подстановки α .

Впрочем, для небольших подстановок порядок нетрудно найти и без вычислительной техники.

Если подстановка α образует единственный цикл длины k , то при возведении α в степени

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^i, \dots$$

единичная подстановка получится впервые только на k -м шаге. Это значит, что *порядок цикла равен его длине*.

Каждую подстановку можно представить в виде произведения независимых циклов. Поскольку независимые циклы не имеют общих элементов, они перестановочны. Следовательно, порядок такого произведения равен НОК порядков этих циклов. Таким образом, если подстановка α является произведением независимых циклов длин n_1, n_2, \dots, n_m соответственно, то порядок подстановки α равен $\text{НОК}[n_1, n_2, \dots, n_m]$.

Например, пусть подстановка α принадлежит симметрической группе S_{20} и образует цикл длины 12:

$$\alpha = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12).$$

Порядок α равен длине цикла, т. е. 12. Сделаем машинную проверку:

```
> with(group):  
> grouporder(permgroupe(20, {[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10,  
11, 2]]})));
```

12

Вместо числа 20 в рассмотренном примере подходит любое число, не меньшее 12. Порядок цикла не превышает его степени, т. е. числа символов, перемещаемых подстановками. Для произведения циклов так будет не всегда.

Найдем, например, порядок подстановки β , принадлежащей S_{17} и имеющей вид

$$\beta = (1\ 2\ 3\ 4\ 5)\ (6\ 7\ 8\ 9\ 10\ 11\ 12)\ (13\ 14)\ (15\ 16\ 17).$$

Предвосхищая машинный результат, можно заранее сказать, что порядок подстановки β равен

$$\text{НОК}[5, 7, 2, 3] = 210.$$

Действительно,

```
> with(group):  
> grouporder(permgroupe (17, {[[1, 2, 3, 4, 5], [6, 7, 8, 9, 10,  
11, 12],  
[13, 14], [15, 16, 17]]})));
```

210

Может оказаться, что степень подстановки слишком велика для машинного вычисления, а длины независимых циклов из разложения подстановки известны. В таком случае НОД чисел — длин циклов — можно вычислить с помощью машины. В рассмотренном примере числа, правда, невелики; однако проверим. Для вычисления наибольшего общего делителя чисел нам придется войти в пакет «Теория чисел» — *Number Theory*. Вход в этот пакет осуществляется командой *with(numtheory)*. Итак,

```
> with(numtheory):  
> ilcm(5, 7, 2, 3);
```

210

Стоит отметить, что машинный алгоритм вычисления порядка группы подстановок не совсем совершенен: время вычисления существенно зависит от степени подстановки (а не от фактически перемещаемых символов). Так, вычисление на машине порядка единичной группы $\{e\}$ по команде

```
> with(group):  
> grouporder(permgroupe (10^7, {[[]]}));
```

1

продолжается несколько минут, а команда

```
> with(group): grouporder(permgroupe (10^8, {[[]]}));
```

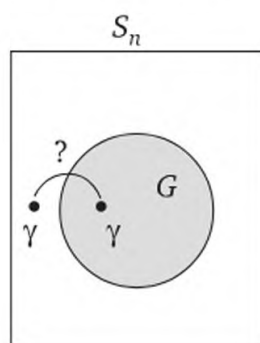
для современной версии пакета математических символьных вычислений компьютерной алгебры вообще невыполнима (число 100 000 000 для современной машины слишком большое):

```
> with(group): grouporder(permgroupe (10^8, {[[]]}));
```

Error, (in convert / plist) object too large

При исследовании группы подстановок G , являющейся подгруппой группы S_n , может возникнуть вопрос, принадлежит или нет подстановка γ из S_n подгруппе G . Другими словами, возникает *проблема вхождения* в G .

Заметим, \ что для произвольных (бесконечных) групп проблема даже вхождения в фиксированную конечно порожденную подгруппу может не иметь алгоритмического решения.



Проблема вхождения

В то же время для конечного объекта любую алгоритмическую задачу можно решить простым перебором вариантов.

Машинная команда *groupmember* (γ, G) решает проблему вхождения элемента γ в подгруппу G .

Если $\gamma \in G$, то результатом работы команды является слово *true*, а если $\gamma \notin G$, то — слово *false*. Например:

```
> with(group):
> G := permgroup(7, {[[1, 2, 3, 4, 5]], [[4, 5], [6, 7]]}):
> groupmember([1, 3, 5], [2, 4], [6, 7], H);
```

true

```
> groupmember([1, 3, 4, 2], G);
```

false

Полученный результат означает, что подстановка $(1\ 3\ 5)\ (2\ 4)\ (6\ 7)$ принадлежит

$$G = \text{gp}(1\ 2\ 3\ 4\ 5), (4\ 5)\ (6\ 7)),$$

а подстановка $(1\ 3\ 4\ 2)$ — не принадлежит.

Элементы, заведомо принадлежащие подгруппе, получить несложно. Любая подгруппа G любой группы замкнута относительно умножения:

$$\alpha \in G, \beta \in G \Rightarrow \alpha\beta \in G.$$

Поэтому любые произведения степеней порождающих элементов снова принадлежат этой же подгруппе.

Вычисление произведения $\alpha\beta$ двух подстановок α и β с помощью техники происходит с помощью команды *mulperms*(α, β). Например:

```
> with(group):
> mulperms([[1, 2, 3, 4, 5], [6, 7], [8, 9]],
  [[1, 6, 8], [2, 3, 4, 5], [7, 9]]);

[[1, 3, 5, 6, 9], [2, 4], [7, 8]].
```

В результате получено равенство

$$(1\ 2\ 3\ 4\ 5)\ (6\ 7)\ (8\ 9) \cdot (1\ 6\ 8)\ (2\ 3\ 4\ 5)\ (7\ 9) = (1\ 3\ 5\ 6\ 9)\ (2\ 4)\ (7\ 8).$$

Если подстановки заданы вторыми строками, то при умножении необходимо их конвертирование. Например, умножение

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 2\ 3\ 4)$$

в машинном варианте имеет вид

```
> with(group):
> mulperms(convert([4, 3, 2, 5, 1], 'disjycyc'),
  convert([5, 4, 3, 2, 1], 'disjycyc'));

[[1, 2, 3, 4]]
```

Результат произведения можно было сразу записать в том же виде, в каком были заданы множители:

```
> with(group):
> convert(mulperms(convert([4, 3, 2, 5, 1], 'disjycyc'),
  convert([5, 4, 3, 2, 1], 'disjycyc')),
  'permlist', 5);

[2, 3, 4, 1, 5]
```

Вместе с каждым своим элементом α подгруппа содержит и его обратный — α^{-1} . Найти подстановку α^{-1} , обратную для α , записанную в виде произведения независимых циклов, несложно вручную: достаточно записать все элементы циклов в обратном порядке. Например, пусть

$$\alpha = (1\ 2\ 3\ 4\ 5)\ (6\ 7\ 8)\ (9\ 10),$$

тогда

$$\alpha^{-1} = (5\ 4\ 3\ 2\ 1)\ (8\ 7\ 6)\ (10\ 9).$$

Найти обратную подстановку можно и машинной командой *invperm*(α):

```
> with(group):
> invperm([[1, 2, 3, 4, 5], [6, 7, 8], [9, 10]]);
```

[[1, 5, 4, 3, 2], [6, 8, 7], [9, 10]]

Как и для умножения, подстановка для этой команды должна иметь представление в виде произведения независимых циклов. Если она задана второй строкой, то ее нужно предварительно конвертировать в циклическое представление.

Найдем, например, подстановку, обратную для подстановки

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}.$$

```
> with(group):
> invperm(convert([8, 7, 6, 5, 4, 1, 2, 3], 'disjcyc'));
```

[[1, 6, 3, 8], [2, 7], [4, 5]]

Обратную подстановку можно записать в том же виде, в каком была задана исходная, т. е. второй строкой:

```
> with(group):
> convert(invperm(convert([8, 7, 6, 5, 4, 1, 2, 3],
  'disjcyc')), 'permlist', 8);
```

[6, 7, 8, 5, 4, 3, 2, 1]

Из того, что группа $G = \text{gr}(a_1, a_2, \dots, a_n)$ замкнута относительно умножения и взятия обратного, следует, в частности, что значение любого слова $w(a_i, a_i^{-1})$ от порождающих и их обратных снова принадлежит группе G .

Значение этого слова вычисляется машинной командой

convert(w , 'disjcyc', G).

Особенности синтаксиса видны из следующего примера:

```
> with(group):
> G := permgroup(5, {a = [[1, 2], [3, 4]],
  b = [[1, 2, 3, 4, 5]], c = [[1, 2, 3]]}):
> convert([a, b, 1/c, 1/a, b, b, c], 'disjcyc', G);
```

[[2, 4, 5]]

В примере группа G порождается элементами a, b, c , а значение слова

$$abc^{-1}a^{-1}b^2c$$

оказалось равным подстановке $(2\ 4\ 5)$.

Заметим, что порядок этой подстановки равен трем, следовательно, в этой группе выполняется равенство¹

$$123(abc^{-1}a^{-1}b^2c)^3 = 1.$$

Рассмотрим еще один пример. Подстановка

$$\beta = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10\ 11\ 12)(13\ 14)(15\ 16\ 17),$$

как было уже отмечено, имеет порядок 210, т. е., в частности, $\beta^{210} = e$.

Сделаем машинную проверку этого равенства с помощью команды `convert... 'disjсyc'`:

```
> with(group):
> G := permgroup(17, {a = [[1, 2, 3, 4, 5],
  [6, 7, 8, 9, 10, 11, 12], [13, 14], [15, 16, 17]]}):
> convert([a$210], 'disjсyc', G);
```

[]

Если нас интересует какой-нибудь случайный элемент из группы подстановок G , то можно воспользоваться командой

$$\text{RandElement}(G).$$

В качестве демонстрации найдем пару случайных элементов из группы G , порожденной подстановками $(1\ 2\ 3\ 4\ 5)$, $(4\ 5)(6\ 7)$:

```
> with(group):
> G := permgroup(7, {[[1, 2, 3, 4, 5]], [[4, 5], [6, 7]]}):
> a := RandElement(G);
```

$$a := [[1, 3, 5], [2, 4], [6, 7]]$$

```
> b := RandElement(G);
```

$$b := [[1, 3, 2]]$$

Машина указывает элементы

$$a = (1\ 3\ 5)(2\ 4)(6\ 7), b = (1\ 3\ 2).$$

¹ Здесь и в дальнейшем в аналогичном контексте символ 1 обозначает единицу группы, а не перемещаемый символ.

Тут может возникнуть вопрос: не совпадает ли наша группа G со всей симметрической группой S_7 ?

Если это так, то никакой машины для решения нашей задачи не требуется: любая подстановка на семи символах будет принадлежать нашей подгруппе.

Ответить на поставленный вопрос несложно. Порядок S_7 равен $7! = 5040$.

Какой же порядок имеет подгруппа $\text{gr}((1\ 2\ 3\ 4\ 5), (4\ 5)\ (6\ 7))$?

Машина сообщает, что он равен всего лишь 120:

```
> with(group):  
> grouporder(permgroupe(7, {[[1, 2, 3, 4, 5]], [[4, 5], [6, 7]]}));
```

120

Таким образом, группа G содержит далеко не все подстановки на семи символах.

Мы можем произвести проверку машинных вычислений, проведенных пакетом символьных вычислений, с помощью этого же пакета. Для конечных подгрупп (и вообще конечных подалгебр) выполняется аналог теоремы Кронекера — Капелли¹: элемент β принадлежит подгруппе $\text{gr}(\alpha_1, \alpha_2, \dots, \alpha_n)$ тогда и только тогда, когда

$$|\text{gr}(\alpha_1, \alpha_2, \dots, \alpha_n)| = |\text{gr}(\alpha_1, \alpha_2, \dots, \alpha_n, \beta)|.$$

Итак, проверим, действительно ли элементы

$$a = (1\ 3\ 5)\ (2\ 4)\ (6\ 7) \text{ и } b = (1\ 3\ 2)$$

принадлежат подгруппе

$$H = \text{gr}((1\ 2\ 3\ 4\ 5), (4\ 5)\ (6\ 7)):$$

```
> with(group):  
> grouporder(permgroupe(7, {[[1, 2, 3, 4, 5]], [[4, 5], [6, 7]]}));
```

120

```
> grouporder(permgroupe(7, {[[1, 2, 3, 4, 5]], [[4, 5],  
[6, 7]], [[1, 3, 2]]}));
```

120

¹ По теореме Кронекера — Капелли вектор β принадлежит подпространству, порожденному $\alpha_1, \alpha_2, \dots, \alpha_n$, тогда и только тогда, когда $\text{pr}(\alpha_1, \alpha_2, \dots, \alpha_n) = \text{pr}(\alpha_1, \alpha_2, \dots, \alpha_n, \beta)$, а последнее равенство равносильно совпадению размерностей этих подпространств. С помощью этой теоремы решается проблема вхождения для подпространств конечномерного векторного пространства.

Порядок подгруппы не изменился после присоединения этих элементов к системе порождающих группы G , следовательно, они действительно входят в эту подгруппу.

Проверим теперь тем же способом, что $(1\ 3\ 4\ 2)$ не входит в подгруппу G :

```
> with(group):
> grouporder(permgroupe(7, {[[1, 2, 3, 4, 5]], [[4, 5], [6, 7]],
  [[1, 2, 3]], [[1, 3, 4, 2]]}));
```

240

Порядок подгруппы изменяется; следовательно, присоединение нового элемента изменяет подгруппу: элемент $(1\ 3\ 4\ 2)$ действительно не принадлежит подгруппе G .

Отметим, что числа 120 и 240 являются делителями порядка всей группы S_7 , равного 5040, как и должно быть по теореме Лагранжа.

Иногда представляет интерес не только вопрос о количестве элементов в группе G , но и сами эти элементы. Команда

elements(G)

позволяет удовлетворить наше любопытство:

```
> with(group):
> H:= permgroupe(4, {[[1, 2, 3]], [[1, 2, 4]]}):
> grouporder(H);
```

12

```
> elements(H);
```

```
{[], [[1, 2, 3]], [[1, 2, 4]], [[1, 4, 3]], [[1, 2], [3, 4]], [[1, 4], [2, 3]],
[[2, 4, 3]], [[1, 3], [2, 4]], [[2, 3, 4]], [[1, 3, 2]], [[1, 3, 4]], [[1, 4, 2]]}
```

Машина выписала все четные подстановки на четырех символах. Это значит, что группа H совпадает со знакопеременной группой A_4 .

Все элементы группы можно найти другим способом: с помощью разложения группы на смежные классы по единичной подгруппе.

8.2. Подгруппы конечной группы

Каждую группу G можно разложить на правые (или левые) смежные классы по подгруппе H . Соответствующие разложения имеют вид

$$G = Hg_1 + Hg_2 + \dots + Hg_m;$$

$$G = u_1H + u_2H + \dots + u_mH.$$

Сама подгруппа H образует отдельный класс (правый и левый одновременно); обычно в качестве представителя H берут единственный элемент.

Число правых смежных классов равно числу левых и называется *индексом* подгруппы H в группе G . Обозначают индекс символом $|G : H|$.

Представители *правых* смежных классов группы G по подгруппе H находятся с помощью команды $\text{cosets}(G, H)$. Найдем, например, разложение группы S_5 по подгруппе S_4 :

```
> with(group):
> S[5] := permgroup(5, {[[1, 2]], [[1, 2, 3, 4, 5]]}):
> S[4] := permgroup(5, {[[1, 2, 3]], [[1, 2, 3, 4]]}):
> cosets(S[5], S[4]);
```

```
{[], [[1, 2, 3, 4, 5]], [[2, 3, 4, 5]], [[3, 4, 5]], [[4, 5]]}
```

Полученный результат означает, что

$$S_5 = S_4(1\ 2\ 3\ 4\ 5) + S_4(2\ 3\ 4\ 5) + S_4(3\ 4\ 5) + S_4(4\ 5).$$

Из равенства $(Hg)^{-1} = g^{-1}H$ следует, что в качестве представителей *левых* смежных классов можно взять обращения представителей *правых*. В рассматриваемом примере

$$S_5 = (5\ 4\ 3\ 2\ 1)S_4 + (5\ 4\ 3\ 2)S_4 + (5\ 4\ 3)S_4 + (4\ 5)S_4.$$

Разложение по единичной подгруппе E состоит из одноэлементных классов, поэтому команда $\text{cosets}(G, E)$ действует точно так же, как команда $\text{elements}(G)$.

Например, найдем все элементы группы $G = S_3$ двумя способами:

```
> with(group):
> G := permgroup(3, {[[1, 2]], [[1, 2, 3]]}):
> E := permgroup(3, {[[]]}):
> elements(G);
```

```
{[], [[1, 2]], [[1, 2, 3]], [[1, 3, 2]], [[2, 3]], [[1, 3]]}
```

```
> cosets(G, E);
```

```
{[], [[1, 2]], [[1, 2, 3]], [[1, 3, 2]], [[2, 3]], [[1, 3]]}
```

Если H группа подстановок степени n , а α — произвольная подстановка той же степени, то подстановку α можно представить в виде

$$\alpha = hq,$$

где h — элемент из H , а q — представитель правого смежного класса по H .

Элементы h и q находятся с помощью команды

$$\text{cosrep}(\alpha, H).$$

Пусть, например, H — симметрическая группа S_4 , а $\alpha = (1\ 4\ 5)$ — подстановка из группы S_5 . Найдем описанное представление для подстановки α :

```
> with(group):  
> H := permgroup(5, {[[1, 2]], [[1, 2, 3, 4]]}):  
> cosrep([1, 4, 5], H);
```

$$[[[1, 3, 2]], [[1, 2, 3, 4, 5]]]$$

Это значит, что

$$(1\ 4\ 5) = (1\ 3\ 2)(1\ 2\ 3\ 4\ 5),$$

где подстановка $(1\ 2\ 3)$ принадлежит H , а $(1\ 2\ 3\ 4\ 5)$ — представитель из правостороннего разложения группы S_5 по подгруппе H .

То, что машина не ошиблась, видно сразу: подстановка $(1\ 2\ 3)$ не перемещает элемент 5 (и, следовательно, принадлежит подгруппе H , равной S_4), а $(1\ 2\ 3\ 4\ 5)$ — действительно один из представителей правых смежных классов, найденных ранее.

Для нахождения разложения элемента α с представителем *левого* смежного класса найдем сначала разложение для α^{-1} с представителем правого класса, а затем воспользуемся равенством

$$\alpha^{-1} = q^{-1}h^{-1}.$$

Например,

```
> with(group):  
> H := permgroup(5, {[[1, 2]], [[1, 2, 3, 4]]}):  
> cosrep([5, 4, 1], H);
```

$$[[[1, 4]], [[4, 5]]]$$

Таким образом, $(1\ 4\ 5)^{-1} = (1\ 4)(4\ 5)$, откуда $(1\ 4\ 5) = (4\ 5)(1\ 4)$, где $(4\ 5)$ — представитель *левого* смежного класса по подгруппе H , а элемент $(4\ 5)$ принадлежит H .

Теорема Лагранжа означает, что *если в конечной группе из n элементов найдется подгруппа из t элементов, то t делит n .*

Утверждение, обратное теореме Лагранжа, имеет следующий вид: *если число t является делителем n , то в конечной группе из n элементов найдется подгруппа порядка t .*

Это утверждение неверно.

Например, знакопеременная группа A_4 четвертой степени имеет порядок 12, но не содержит подгрупп порядка шесть.

Все элементы A_4 были только что выписаны.

Как может быть устроена группа порядка шесть?

В группе четного порядка обязательно содержится элемент второго порядка. Если все элементы такой группы имеют второй порядок, то два различных элемента порождают подгруппу, состоящую из четырех элементов. Эта подгруппа изоморфна V_4 — четверной группой Клейна. Поскольку 4 не делит 6, в группе шестого порядка (обозначим ее символом G_6) обязательно содержится элемент порядка 3. Пусть a — элемент второго порядка, а b — элемент третьего порядка из группы G_6 . В G_6 четыре элемента $1, a, b, b^2$ различны. Поскольку порядок подгруппы должен делить порядок группы, отсюда следует, что любая группа порядка шесть порождается двумя элементами: один элемент имеет порядок два, другой — порядок три.

Если эти элементы перестановочны, то порождаемая ими группа изоморфна циклической группе шестого порядка.

Если же эти элементы не перестановочны, то получается симметрическая группа третьей степени S_3 .

Итак, неизоморфных групп порядка шесть всего две: циклическая шестого порядка и симметрическая третьей степени¹.

Среди выписанных элементов группы A_4 нет ни цикла длины шесть, ни произведения циклов длин два и три. Это значит, что в A_4 нет элементов шестого порядка, а следовательно, нет и циклических подгрупп порядка шесть.

Группа S_3 содержит три элемента второго порядка, которые вместе с единицей не образуют подгруппу, так как любая пара различных транспозиций является циклом длины три, т. е. *пятым элементом*.

В группе A_4 содержатся тоже три элемента второго порядка:

$$(1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4).$$

Однако подгруппа, порожденная этими тремя подстановками, состоит из четырех элементов. Это и есть четверная группа Клейна V_4 , так как произведение любых двух различных элементов из этой тройки дает третий элемент. Однако можно даже и не проверять, а просто спросить машину, не порождают ли эти три элемента подгруппу порядка четыре:

```
> with(group):  
> grouporder(permgroupe(7, [[1, 2], [3, 4]], [[1, 4], [2, 3]],  
  [[1, 3], [2, 4]]));
```

¹ Это утверждение, разумеется, сразу же следует из теорем Силова, но здесь просто нет необходимости прибегать к столь сильным средствам.

Это значит, что вместе с единицей (четвертым элементом) эти три подстановки действительно образуют подгруппу.

Итак, ни циклическая шестого порядка, ни группа S_3 не содержатся в группе A_4 . Несмотря на то, что число 6 делит 12, в A_4 — группе порядка 12 — нет подгрупп шестого порядка.

Существует ли группа порядка меньше 12, для которой обращение теоремы Лагранжа не выполняется?

Нет, A_4 — это наименьшая группа с таким свойством.

Это утверждение сразу следует из теорем Силова, однако его нетрудно получить и непосредственно.

По теореме Лагранжа, в группе простого порядка нет подгрупп, кроме тривиальных. Поэтому для групп порядка 2, 3, 5, 7, 11 утверждение, обратное теореме Лагранжа, выполняется. Выполняется оно и для любой конечной циклической группы.

Оно будет верным и в группе порядка p^2 , где p — простое число. Если такая группа нециклическая¹, то она содержит элементы только порядка p (а если циклическая, то порядка p и порядка p^2), так что для групп порядка 4 и групп порядка 9 обращение теоремы Лагранжа тоже верно.

Число 10 четное, поэтому в группе порядка 10 есть элемент порядка 2; причем все элементы в такой группе имеют порядок 2 не могут (в противном случае там появится четверная группа Клейна V_4 , но число 4 не делит 10). Это значит, что в этой группе есть элемент пятого порядка, т. е. обращение теоремы Лагранжа для этой группы тоже выполняется.

Остается рассмотреть лишь группы восьмого порядка. Если в нециклической группе восьмого порядка G_8 все элементы имеют порядок два, то пара различных элементов порождает подгруппу порядка четыре. Если же не все элементы в нециклической G_8 имеют порядок два, то этот другой порядок может быть равен только четырем.

Таким образом, для всех групп порядка, не превышающего числа 11, обращение теоремы Лагранжа выполняется.

Пересечение подгрупп снова является подгруппой, поэтому множество подгрупп образует решетку. Для исследования этой решетки достаточно уметь находить порождающие элементы пересечения двух подгрупп.

Пакет *Maple* имеет соответствующую команду, а именно

$$\text{inter}(G, H).$$

Умея находить пересечение двух подгрупп, можно выяснить, не входит ли одна подгруппа в другую, так как (для любых множеств A, B)

$$A \subseteq B \Leftrightarrow A \cap B = A.$$

¹ Группа порядка p^2 всегда абелева.

Впрочем, в пакете *Maple* есть специальная команда для узнавания, входит ли подгруппа A в подгруппу B .

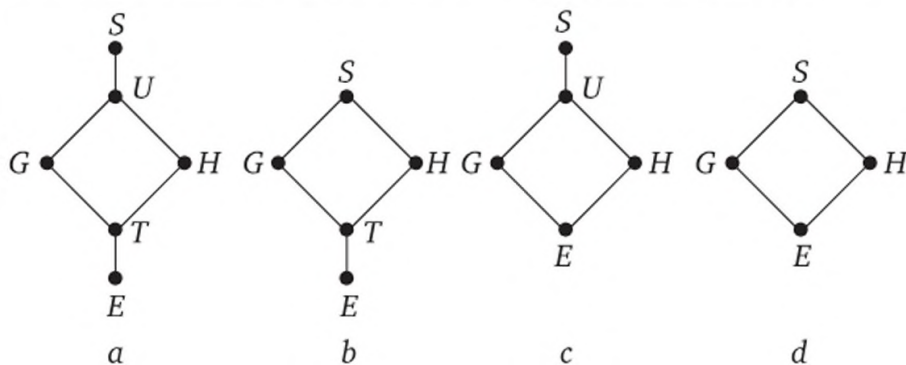
Результатом действия команды

$$\text{issubgroup}(A, B)$$

является слово *true*, если A — подгруппа группы B , и слово *false*, если это не так.

Пусть в симметрической группе S находятся две подгруппы G и H , и нас интересует их взаимное расположение, а именно: как связаны их множества, не входит ли одна подгруппа в другую.

Если $G \cap H = T$, а $\text{gr}(G, H) = U$, то заранее известно лишь, что $E \subseteq T$, а $U \subseteq S$. Если к тому же установлено, что ни одна из групп G , H не является подгруппой другой, то фрагмент графа решетки подгрупп может иметь вид одной из следующих конфигураций:



Покажем на конкретном примере, как можно выяснить действительное положение вещей. Пусть в группе $S = S_8$ содержатся две подгруппы G и H , заданные своими порождающими:

$$G = \text{gr}((1\ 2\ 3\ 4), (1\ 2), (5\ 6\ 7), (5\ 6)),$$

$$H = \text{gr}((3\ 2\ 4\ 5\ 6), (5\ 6\ 7\ 8), (5\ 6)).$$

Саму группу S также зададим двумя стандартными порождающими:

$$(1\ 2) \text{ и } (1\ 2\ 3\ 4\ 5\ 6\ 7).$$

Выясним сначала, сравнимы ли подгруппы G и H по отношению включения, т. е. не является ли одна из групп подгруппой другой:

```
> with(group):
> S := permgroup(8, {[[1, 2]], [[1, 2, 3, 4, 5, 6, 7, 8]]}):
> G := permgroup(8, {[[1, 2, 3, 4]], [[1, 2]],
  [[5, 6, 7]], [[5, 6]]}):
> H := permgroup(8, {[[3, 2, 4, 5, 6]], [[5, 6, 7, 8]], [[5, 6]]}):
> issubgroup(G, S);
```

true

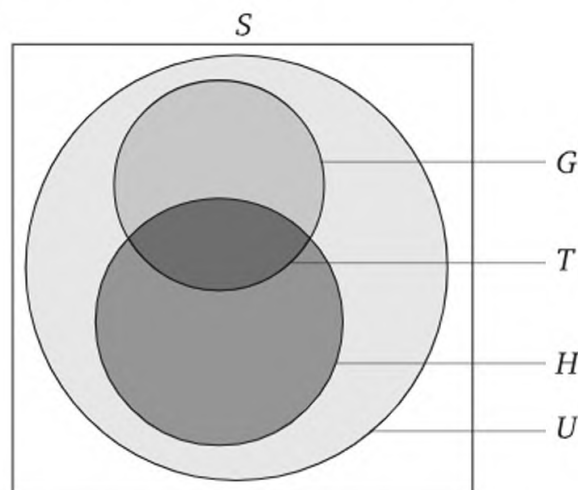
```
> issubgroup(G, H);
```

false

```
> issubgroup(H, G);
```

false

Факт, что группа G является подгруппой группы S , конечно, можно было и не проверять — эта команда присутствует здесь лишь для дополнительной проверки работоспособности пакета.



Решетка подгрупп

Однако то, что ни G не является подгруппой в H , ни H в G , — уже совсем не очевидный факт. Машина сообщает, что множества G и H расположены примерно так, как на прилагаемом рисунке.

Таким образом, фрагмент графа решетки подгрупп группы S — это действительно один из перечисленных на схеме вариантов a, b, c, d .

Остается выяснить, какой именно из четырех вариантов верный. Найдем сначала порождающие подгруппы T :

```
> with(group):  
> G := permgroup(8, {[[1, 2, 3, 4]], [[1, 2]], [[5, 6, 7]],  
  [[5, 6]]}):  
> H := permgroup(8, {[[3, 2, 4, 5, 6]], [[5, 6, 7, 8]],  
  [[5, 6]]}):  
> T := inter(G, H);
```

```
T := permgroup(8, {[[5, 6, 7]], [[3, 4]], [[6, 7]], [[2, 3]]})
```

Итак, порождающие подгруппы T найдены:

$$T = \text{gr}((5\ 6\ 7), (3\ 4), (6\ 7), (2\ 3)).$$

Подгруппа T отлична от единичной, так что варианты c, d на схеме, изображающей граф решетки, отпадают.

Порождающие элементы для группы $U = \text{gr}(G, H)$ искать не нужно — это просто объединение множеств порождающих элементов подгрупп G и H :

$$U = \text{gr}((1\ 2\ 3\ 4), (1\ 2), (5\ 6\ 7), (5\ 6)), (3\ 2\ 4\ 5\ 6), (5\ 6\ 7\ 8), (5\ 6)).$$

Остается лишь выяснить, не совпадает ли группа U со всей группой S .

Узнать это можно с помощью той же команды *issubgroup*: если $D = S$, то результатом команды *issubgroup*(S, D) будет слово *true*. Проверим:

```
> with(group):
> S := permgroup(8, {[[1, 2]], [[1, 2, 3, 4, 5, 6, 7, 8]]}):
> U := permgroup(8, {[[1, 2, 3, 4]], [[1, 2]], [[5, 6, 7]],
    [[5, 6]],
    [[3, 2, 4, 5, 6]], [[5, 6, 7, 8]]}):
> issubgroup(G, S);

true
```

Итак, группа U совпадает со всей группой S . Это значит, что из четырех предложенных версий фрагментов решетки подгрупп в действительности имеет место вариант *b*.

Чтобы еще отчетливее представить получившуюся картину, узнаем число элементов в фигурантах ситуации, т. е. найдем порядки подгрупп G , H и T (и вычислим заодно, на всякий случай, для контроля компьютера, порядки подгрупп U и S , хотя эти последние нам уже известны: они оба равны $8! = 40\ 320$):

```
> with(group):
> S := permgroup(8, {[[1, 2]], [[1, 2, 3, 4, 5, 6, 7, 8]]}):
> U := permgroup(8, {[[1, 2, 3, 4]], [[1, 2]], [[5, 6, 7]],
    [[5, 6]],
    [[3, 2, 4, 5, 6]], [[5, 6, 7, 8]]}):

> G := permgroup(8, {[[1, 2, 3, 4]], [[1, 2]], [[5, 6, 7]],
    [[5, 6]]}):
> H := permgroup(8, {[[3, 2, 4, 5, 6]], [[5, 6, 7, 8]],
    [[5, 6]]}):
> T := inter(G, H):
> grouporder(G);

144

> grouporder(H);

5040
```



```
> grouporder(T);
```

36

```
> grouporder(U);
```

40 320

```
> grouporder(S);
```

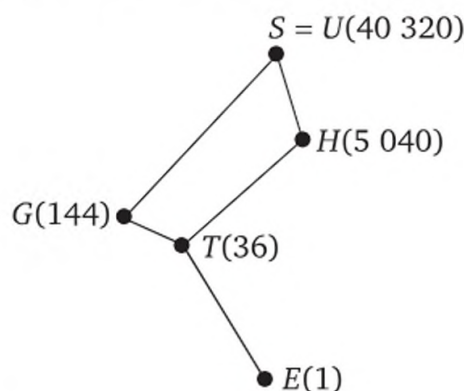
40 320

Порядки всех подгрупп найдены. Обратим внимание на то, что в соответствии с теоремой Лагранжа в каждом случае порядок подгруппы делит порядок своей надгруппы: $T < G$ и $|T| = 36$ делит число $|G| = 144$, $T < H$ и $|T|$ делит $|H| = 5040$, наконец, числа $|H|$ и $|G|$ делят порядок всей группы — число 40 320.

С учетом порядков подгрупп картинку теперь можно изобразить точнее, указав у каждой группы ее порядок и поместив группы большего порядка на более высоком уровне.

Новая картинка потеряла былую красоту, она уже не так симметрична, но зато частично отражает и глубины погружения одной подгруппы в другую (теперь граф напоминает не решетку, а скорее схему *созвездия*).

Длины отрезков, соединяющих подгруппы, хотя и приблизительно, но лучше старой картинки (вариант *b*) соответствуют индексам подгрупп — более короткие отрезки изображают меньшие индексы.



Граф отношения включения подгрупп

Правда, совершенно точно отобразить ситуацию затруднительно, так как наибольший индекс в этой конфигурации равен 280, а наименьший — четырем:

$$|S : G| = 280, |G : T| = 4.$$

Важную роль в группе S_n всех подстановок степени n играет знакопеременная подгруппа A_n состоящая из всех четных подстановок.

Узнать является ли подстановка α четной можно с помощью команды

$$\text{parity}(\alpha).$$

Результатом действия этой команды будет значение функции $\text{sgn}(\alpha)$ — знак подстановки. Напомним, что

$$\text{sgn } \alpha = \begin{cases} 1, & \text{если } \alpha \text{ — четная,} \\ -1, & \text{если } \alpha \text{ — нечетная.} \end{cases}$$

Например, подстановка $(1\ 2\ 3)$ четная, так как ее можно представить в виде четного произведения транспозиций:

$$(1\ 2\ 3) = (1\ 2)(1\ 3),$$

а подстановка $(1\ 2\ 3\ 4)$ нечетная, потому что

$$(1\ 2\ 3\ 4) = (1\ 2)(1\ 3)(1\ 4).$$

Таким образом, $\text{sgn}(1\ 2\ 3) = 1$, $\text{sgn}(1\ 2\ 3\ 4) = -1$.
Проверим на компьютере:

```
> with(group):  
> parity([[1, 2, 3]]);
```

1

```
> parity([[1, 2, 3, 4]]);
```

-1

С помощью такой же команды, но уже обращенной к группе G , состоящей из подстановок степени n , можно выяснить, является ли G подгруппой знакопеременной группы A_n .

Например, результат следующих вычислений:

```
> with(group):  
> G1 := permgroup(4, {[[1, 2, 3]], [[2, 3, 4]]}):  
> parity(G1);
```

1

```
> G2 := permgroup(4, {[[1, 2]], [[3, 4]]}):  
> parity(G2);
```

-1

означает, что группа $G1$ состоит только из четных подстановок, следовательно, $G1 \leq A_n$, а группа $G2$ содержит и нечетные подстановки, поэтому не содержится в A_n .

8.3. Подгруппы с особыми свойствами

Два элемента a, b группы G называют *сопряженными*, если существует такой элемент c , что

$$b = c^{-1}ac.$$

Заметим, что сопряжение можно писать и по-другому: cas^{-1} , так как c^{-1} — это элемент той же группы. Часто пользуются символикой: $c^{-1}ac = a^c$ (или $cas^{-1} = a^c$).

Важную роль в решетке подгрупп группы играют нормальные подгруппы. Подгруппа N нормальна в группе G , если N замкнута относительно взятия сопряженного:

$$x \in N, g \in G \Rightarrow g^{-1}xg \in N;$$

пишут: $N \triangleleft G$.

Если H — подгруппа группы G , а g — некоторый фиксированный элемент из G , то множество

$$G^{-1}Hg = \{g^{-1}hg \mid h \in H\}$$

тоже образует подгруппу. Эту подгруппу называют *сопряжением* подгруппы H .

Таким образом, подгруппа N нормальна, если она содержит все свои сопряжения (для любого g из группы G):

$$g^{-1}Ng \subseteq N.$$

Наименьший нормальный делитель группы G , содержащий подгруппу (или просто подмножество) H , называют *нормальным замыканием* подгруппы (подмножеством) H и обозначают символом $\langle H \rangle^G$.

Нормальное замыкание порождается сопряжениями всех элементов из H :

$$\langle H \rangle^G = \text{gp}(\{h^g \mid h \in H, g \in G\}).$$

Подгруппа является нормальным делителем в G тогда и только тогда, когда она совпадает со своим нормальным замыканием в G .

Как и любая группа подстановок, нормальное замыкание определено, если найдены его групповые порождающие элементы.

Команда

$$\text{NormalClosure}(H, G)$$

выдает в качестве результата множество порождающих (как подгруппы) для нормального замыкания $\langle H \rangle^G$. При этом H должна

быть подгруппой группы G . Если это не так, то поступит сообщение об ошибке.

Найдем нормальное замыкание N группы

$$H = \text{gr}((1\ 2\ 3), (1\ 5\ 6))$$

в группе

$$G = \text{gr}((1\ 2), (1\ 2\ 3\ 4\ 5\ 6)).$$

Сразу же вычислим и порядки всех этих групп (хотя и до вычислений ясно, что порядок G равен $6! = 720$):

```
> with(group):
> H := permgroup(6, {[[1, 2, 3]], [[1, 5, 6]]}):
> grouporder(H);
```

60

```
> G := permgroup(6, {[[1, 2]], [[1, 2, 3, 4, 5, 6]]}):
> grouporder(G);
```

720

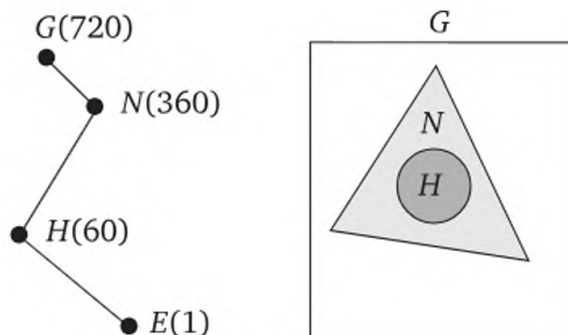
```
> N := NormalClosure(H, G); grouporder(N);
N := permgroup(6, {[[1, 2, 3]], [[1, 5, 6]], [[2, 3, 4]]})
```

360

Таким образом, подгруппа H не была нормальной, но ее нормальное замыкание —

$$N = \text{gr}((1\ 2\ 3), (1\ 5\ 6), (2\ 3\ 4)) \text{ —}$$

это еще не вся группа G . Связь между этим тремя подгруппами на графе отношения порядка и на диаграмме Эйлера — Венна представлена на рисунке.



N — нормальное замыкание подгруппы H

Вычисление, выполненное техникой, можно проверить с помощью той же техники. Машинная команда

isnormal(A, B)

выдает слово *true*, если *B* — нормальный делитель группы *A*, и слово *false*, если *B* не нормальна в *A*:

```
> with(group):
> H := permgroup(6, {[[1, 2, 3]], [[1, 5, 6]]}):
> G := permgroup(6, {[[1, 2]], [[1, 2, 3, 4, 5, 6]]}):

> N := permgroup(6, {[[1, 2, 3]], [[1, 5, 6]], [[2, 3, 4]]}):
> isnormal(G, H);

false

> isnormal(G, N);
```

true

Пусть *G* — группа, а *H* — ее подгруппа. Может случиться, что *H*, не являясь нормальной во всей группе *G*, является нормальным делителем некоторой промежуточной подгруппы. Наибольшая такая подгруппа называется *нормализатором H в G*. Обозначается нормализатор символом $N_G(H)$.

Такое определение не гарантирует существования объекта — наибольший элемент может не существовать даже в конечном упорядоченном множестве. Однако нормализатор можно определить иначе, конструктивно. Множество

$$\{x \in G \mid x^{-1}Hx = H\}$$

как раз и образует наибольшую подгруппу группы *G*, в которой *H* является нормальным делителем.

Подгруппа *H* группы *G* будет нормальным делителем в *G* тогда и только тогда, когда нормализатор *H* в *G* совпадает с *G*.

Найти порождающие элементы нормализатора $N_G(H)$ позволяет команда

normalizer(G, H).

Найдем нормализатор *NR* подгруппы *H* в группе *G* из предыдущего примера. Чтобы оценить размеры нормализатора, найдем его порядок. Кроме того, проверим машину дополнительным вопросом, не является ли подгруппа *H* нормальным делителем в *NR* (ответ на этот вопрос известен заранее: да, является).

```

> with(group):
> H := permgroup(6, {[[1, 2, 3]], [[1, 5, 6]]}):
> G := permgroup(6, {[[1, 2]], [[1, 2, 3, 4, 5, 6]]}):
> NR := normalizer(G, H); grouporder(NR);
NR := permgroup(6, {[[1, 2, 3]], [[1, 5, 6]], [[5, 6]]})

```

120

```

> isnormal(NR, H);

```

true

Число различных сопряжений подгруппы H в группе G равно индексу нормализатора $N_G(H)$ в группе G :

$$|\{g^{-1}Hg \mid g \in G\}| = |G : N_G(H)|.$$

В предыдущем примере порядок нормализатора равен 120. Всего в группе содержится 720 элементов, значит, индекс нормализатора равен шести и в группе G содержится шесть различных сопряжений группы H .

Пересечение всех сопряжений подгруппы H в группе G является наибольшим нормальным делителем группы G , содержащимся в H . Представление группы G подстановками правых смежных классов по подгруппе H (правыми сдвигами) является точным (изоморфизмом) тогда и только тогда, когда этот нормальный делитель образует единичную подгруппу.

Ответ на вопрос о порождающих элементах наибольшего нормального делителя группы G , содержащегося в подгруппе H , дается с помощью команды

$\text{core}(H, G)$.

Найдем наибольший нормальный делитель группы $G = ((1\ 2), (1\ 2\ 3\ 4\ 5\ 6))$, содержащийся в подгруппе $H = ((1\ 2\ 3), (1\ 5\ 6))$.

```

>with(group):
> H := permgroup(6, {[[1, 2, 3]], [[1, 5, 6]]}):
> G := permgroup(6, {[[1, 2]], [[1, 2, 3, 4, 5, 6]]}):
> core(H, G);

```

$\text{permgroup}(6, \{\})$

Оказалось, что в подгруппе H нет нетривиальных нормальных делителей группы G ; пересечение всех сопряжений подгруппы H в группе G тривиально, поэтому представление группы G подстановками правых смежных классов по подгруппе H будет точным.

Рассмотрим еще один пример нахождения ядра гомоморфизма группы G на группу правых сдвигов по подгруппе H .

Пусть

$$G = \text{gr}((1\ 2\ 3\ 4), (1\ 2), (5\ 6\ 7), (5\ 6)),$$

а H — ее подгруппа, порожденная элементами

$$(5\ 6), (2\ 3), (5\ 6\ 7), (2\ 3\ 4).$$

Найдем наибольший нормальный делитель группы G , содержащийся в H :

```
> with(group):
> G := permgroup(8, {[[1, 2, 3, 4]], [[1, 2]], [[5, 6, 7]],
  [[5, 6]]}):
> H := permgroup(8, {[[5, 6]], [[2, 3], [5, 6, 7]], [[2, 3, 4]]}):
> CR := core(H, G);
```

$$CR := \text{permgroup}(8, \{[[5, 6]], [[6, 7]]\})$$

```
> grouporder(G);
```

144

```
> grouporder(H);
```

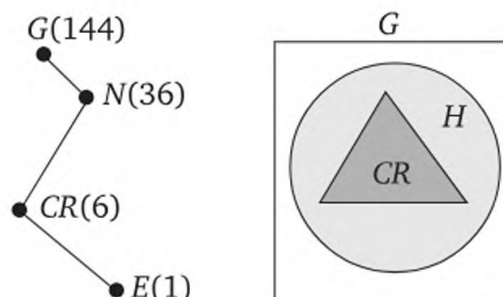
36

```
> grouporder(CR);
```

6

В подгруппе H находится нетривиальный нормальный делитель CR группы G . Подгруппа CR — это пересечение всех сопряжений H в группе G . Между CR и подгруппой H , возможно, находятся промежуточные подгруппы, но ни одна из них (в том числе и сама H) не будет нормальной в G .

Ситуация схематично отображена на прилагаемом рисунке.



CR — наибольший нормальный делитель группы G , содержащийся в H

Представление этой группы G сдвигами правых смежных классов по подгруппе H будет неточным.

Правда, в нашем примере неточность представления (и, таким образом, нетривиальность ядра) можно было установить, используя лишь значения порядков группы G и подгруппы H .

Действительно, индекс подгруппы H в G равен $\frac{144}{36} = 4$, и если бы представление было точным, число 144 являлось бы делителем $4! = 24$.

Рассмотрим еще один вопрос, связанный с нормальностью и ненормальностью подгруппы.

Свойство быть подгруппой транзитивно: подгруппа подгруппы является подгруппой. Можно ли здесь поставить прилагательное «нормальной»?

Точнее говоря, верно ли, что нормальный делитель нормального делителя тоже является нормальным делителем во всей группе?

Ответ на этот вопрос отрицательный.

С помощью техники соответствующий пример легко обнаружить. В группе S_4 подгруппа

$$K = \{e, (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\}$$

абелева, поэтому любая ее неединичная подгруппа, например, $H = \{e, (1\ 2)(3\ 4)\}$, образует нетривиальный нормальный делитель.

Однако H не является нормальным делителем во всей группе S_4 . Продемонстрируем с помощью машины истинность этих утверждений (для контроля самой машины, проверив заодно и порядки всех групп):

```
> with(group):
> S := permgroup(4, {[[1, 2]], [[1, 2, 3, 4]]}):
> K := permgroup(4, {[[1, 2], [3, 4]], [[3, 1], [2, 4]]}):
> H := permgroup(4, {[[1, 2], [3, 4]]}):
> grouporder(G);
```

24

```
> grouporder(K);
```

4

```
> grouporder(H);
```

2

```
> isnormal(S, K);
```

true

```
> isnormal(K, H);
```

true

```
> isnormal(S, H);
```

false

Итак, $K \triangleleft A_4 \triangleleft S_4$ но K — не нормальная подгруппа в группе S_4 .

Множество всех элементов группы перестановочных с каждым элементом из M образует подгруппу, называемую *централизатором* M в группе G . Обозначают централизатор множества M в группе G символом $Z_G(M)$. Таким образом,

$$Z_G(M) = \{g \in G \mid (\forall x \in M)[gx = xg]\}.$$

Находится централизатор $Z_G(M)$ с помощью машинной команды

centralizer(G, M).

Число различных сопряжений элемента x в группе G равно индексу централизатора x в группе G :

$$|\{g^{-1}xg \mid g \in G\}| = |G : Z_G(x)|.$$

Найдем, например, централизатор элемента $(1\ 2\ 3)$ в группе S_4 :

```
> with(group):
```

```
> Z := centralizer(permgroupe(4, {[[1, 2]], [[1, 2, 3, 4]]},  
  {[[1, 2, 3]]}));
```

$Z := \text{permgroupe}(4, \{[[1, 3, 2]]\})$

```
> grouporder(Z);
```

3

Группа S_4 содержит 24 элемента, поэтому индекс подгруппы Z в S_4 равен $\frac{24}{3} = 8$.

Следовательно, число различных сопряжений подстановки $(1\ 2\ 3)$ равно восьми.

Заметим, что если бы нас интересовало только это число сопряжений, а не централизатор элемента, то вычисления можно было оформить двумя командами: вход в пакет и вычисление индекса:

```
> with(group):  
> grouporder(permgroupe(4, {[[1, 2]], [[1, 2, 3, 4]]})) /  
  grouporder(centralizer  
(permgroupe(4, {[[1, 2]], [[1, 2, 3, 4]]}), {[[1, 2, 3]]}));
```

8

Как узнать, сопряжены или нет две подстановки α и β ?

Представим каждую из них в виде произведения независимых циклов. Если подстановки одинаково устроены, т. е. наборы длин циклов у подстановок α и β совпадают, то α и β сопряжены во всей симметрической группе S_n . Если же устройство их различно, то они не сопряжены в S_n .

Например, подстановки $(1\ 2\ 3)(4\ 5)$ и $(1\ 4)(2\ 3\ 6)$ сопряжены в группе S_6 , а подстановка $(1\ 2\ 3)(4\ 5\ 6)$ с ними не сопряжена.

Число подстановок, имеющих одинаковое цикловое устройство с подстановкой α и принадлежащих подгруппе G , находится с помощью команды

$$SnConjugates(G, \alpha).$$

Вычислим, например, число всех подстановок на шести символах, имеющих тот же тип циклов, что и подстановка $(1\ 2\ 3)(4\ 5)$, т. е. найдем число подстановок вида $(a\ b\ c)(d\ e)$, где все буквы различны.

```
> with(group):
> S[6] := permgroup(6, {[[1, 2]], [[1, 2, 3, 4, 5, 6]]}):
> SnConjugates(S[6], [[1, 2, 3], [4, 5]]);
```

Все эти 120 подстановок сопряжены с подстановкой в группе S_6 . Проверим работу машины, вычислив это же число другим способом:

```
> with(group):
> S[6] := permgroup(6, {[[1, 2]], [[1, 2, 3, 4, 5, 6]]}):
> Z := centralizer(S[6], {[[1, 2, 3], [4, 5]]}):
> grouporder(S[6])/grouporder(Z);
```

120

Число подстановок такого же циклического типа, что и подстановка $(1\ 2\ 3)(4\ 5)$, попавших, например, в группу

$$G = \text{gr}((1\ 2\ 3), (4\ 5\ 6), (5\ 6)),$$

состоящую всего лишь из 18 элементов, естественно, гораздо меньше:

```
> with(group):
> G := permgroup(6, {[[1, 2, 3]], [[4, 5, 6]], [[5, 6]]}):
> grouporder(G);
```

18

```
> SnConjugates(G, [[1, 2, 3], [4, 5]]);
```

6

Значительные трудности с решением вопроса о сопряженности двух элементов при ручных вычислениях возникнут в группе подстановок H , не совпадающей со всей симметрической группой.

Разумеется, если α и β не сопряжены во всей симметрической группе, то тем более они не сопряжены ни в какой подгруппе.

Иначе говоря, *различно устроенные подстановки не сопряжены никогда*.

Однако подстановки из подгруппы H могут иметь одинаковое строение и все-таки не быть сопряженными: сопрягающий элемент, содержащийся во всей S_n , не попал в H .

Узнать, сопряжены или нет два элемента α и β в группе подстановок G , можно с помощью команды `areconjugate(G, α , β)`.

Рассмотрим пример на тестирование сопряженности в группе подстановок, отличной от симметрической группы. Пусть группа $G = ((1\ 2\ 3), (4\ 5\ 6), (5\ 6))$ и подстановки

$$a = (1\ 2\ 3)\ (4\ 5),\ b = (1\ 2\ 3)\ (5\ 6),\ c = (1\ 3\ 2)\ (5\ 6)$$

принадлежат этой группе.

Проверим сначала, что они действительно являются элементами группы G , а затем выясним, нет ли среди этих трех подстановок сопряженных (заметим предварительно, что a, b, c циклически устроены одинаково, поэтому любые две из них сопряжены во всей группе S_6):

```
> with(group):
> G := permgroup(6, {[[1, 2, 3]], [[4, 5, 6]], [[5, 6]]}):
> groupmember([[1, 2, 3], [4, 5]], G);

true

> groupmember([[1, 3, 2], [5, 6]], G);

true

> groupmember([[1, 3, 2], [5, 6]], G);

true

> areconjugate(G, [[1, 2, 3], [4, 5]], [[1, 2, 3], [5, 6]]);

true

> areconjugate(G, [[1, 2, 3], [4, 5]], [[1, 3, 2], [5, 6]]);

false

> areconjugate(G, [[1, 2, 3], [5, 6]], [[1, 3, 2], [5, 6]]);

false
```


Оказалось, что подстановки a и b сопряжены в G , а подстановки a и c — нет. Подстановки b и c тоже не сопряжены.

Последнюю проверку можно было и не проводить: отношение сопряженности является эквивалентностью, поэтому два элемента, сопряженные третьему, сопряжены.

Пример показывает, что одинаково устроенные подстановки могут быть как сопряженными, так и не сопряженными в группе подстановок, отличной от всей симметрической группы.

Сколько же всего элементов, сопряженных с подстановкой a , содержится в G ?

Вычислив индекс централизатора $Z_G(a)$, ответим на этот вопрос:

```
> with(group):
> G := permgroup(6, {[[1, 2, 3]], [[4, 5, 6]], [[5, 6]]}):
> Z := centralizer(G, {[[1, 2, 3], [4, 5]]}):
> grouporder(G)/grouporder(Z);
```

3

Чтобы найти все подстановки, сопряженные с a , достаточно взять ее сопряжения с помощью представителей правых смежных классов группы G по подгруппе $Z_G(a)$. Разыщем представителей правых смежных классов:

```
> with(group):
> G := permgroup(6, {[[1, 2, 3]], [[4, 5, 6]], [[5, 6]]}):
> Z := centralizer(G, {[[1, 2, 3], [4, 5]]}):
> cosets(G, Z);
```

{[], [[4, 5, 6]], [[5, 6]]}

Таким образом, правостороннее разложение группы G по подгруппе $Z = Z_G(a)$ имеет вид

$$G = Z + Z(4\ 5\ 6) + Z(5\ 6).$$

Следовательно, все подстановки, сопряженные с подстановкой $(1\ 2\ 3)(4\ 5)$, — это:

$$e^{-1} \cdot (1\ 2\ 3)(4\ 5) \cdot e = (1\ 2\ 3)(4\ 5);$$

$$(6\ 5\ 4) \cdot (1\ 2\ 3)(4\ 5) \cdot (4\ 5\ 6) = (1\ 2\ 3)(5\ 6);$$

$$(5\ 6) \cdot (1\ 2\ 3)(4\ 5) \cdot (5\ 6) = (1\ 2\ 3)(4).$$

Может возникнуть вопрос: а не выполняется ли в группе подстановок какое-нибудь нетривиальное тождество? В частности, не является ли данная группа абелевой?

Абелевость группы подстановок G проверяет команда

$isabelian(G)$.

Если группа G абелева, то на выходе появляется слово *true*, а если неабелева — *false*. Выясним, являются ли абелевыми две группы подстановок:

$$P = \text{gr}((1\ 2), (1\ 2\ 3\ 4)\ (9\ 10)),$$

$$H = \text{gr}((1\ 2\ 3), (3\ 2\ 1)\ (4\ 5\ 6\ 7)):$$

```
> with(group):  
> P := permgroup(10, {[[1, 2]], [[1, 2, 3, 4], [9, 10]]}):  
> H := permgroup(8, {[[1, 2, 3]], [[3, 2, 1], [4, 5, 6, 7]]}):  
> isabelian(P);
```

false

```
> isabelian(G);
```

true

Группа P оказалась неабелевой, а группа H — абелевой.

Заметим, что свойство неабелевости группы имеет некоторые градации, т. е. неабелевость неабелевости рознь.

Напомним, что элемент $xux^{-1}y^{-1}$ называют коммутатором элементов x, y . Коммутант часто обозначают символом $[x, y]$. Подгруппа группы G , порожденная всевозможными коммутаторами, называется коммутантом (или производной) группы G . Обозначают коммутант G символом $[G, G]$ или символом, напоминающим производную: G' .

Группа G абелева тогда и только тогда, когда ее коммутант равен единичной подгруппе.

Образно выражаясь, чем больше коммутант группы, тем дальше от абелевости изучаемая группа. Самый большой возможный коммутант — это вся группа G (а когда коммутант единичный — самый малый из возможных, то группа G и становится абелевой).

Иначе говоря, мало сказать «группа неабелева». Хотелось бы знать, сколь далека она от абелевости, т. е. вычислить ее коммутант. Порождающие элементы коммутанта группы подстановок G вычисляет машинная команда

$derived(G)$.

Вычислим коммутанты групп P и H .

Мы уже знаем, что группа H абелева, поэтому ее коммутант является единичной подгруппой, т. е. содержит всего одну, единичную подстановку.

Коммутант группы P точно не равен единице, а какой он именно, сейчас узнаем. Чтобы выяснить, сколь велик коммутант по сравнению со всей группой, вычислим порядки всех групп-участников этого примера:

```
> with(group):
> P := permgroup(10, {[[1, 2]], [[1, 2, 3, 4], [9, 10]]}):
> grouporder(P);
```

48

```
> H := permgroup(8, {[[1, 2, 3]], [[3, 2, 1], [4, 5, 6, 7]]}):
> grouporder(H);
```

12

```
> K[1] := derived(P); grouporder(K[1]);
K1 := permgroup(10, {[[]], [[1, 3, 2]], [[2, 4, 3]]})
```

12

```
> K[2] := derived(H); grouporder(K[2]);
K2 := permgroup(8, {[[]]})
```

1

Итак, группа P содержит 48 элементов, а ее коммутант, группа K_1 , имеет порядок 12. Таким образом, группа P неабелева, но не совпадает со своим коммутантом.

Группа H состоит из 12 элементов, и ее коммутант, группа K_2 , как и ожидалось, равен единичной подгруппе.

Для исследований свойств многочленов важным теоретико-групповым свойством является разрешимость.

Напомним, что группа G разрешима, если ряд последовательных коммутантов

$$G' = [G, G], G'' = [G', G''], \dots, G^{(m)} = [G^{(m-1)}, G^{(m-1)}], \dots$$

доходит до единичной подгруппы. Длина этого ряда называется степенью разрешимости группы (говорят: « m -ступенно разрешимая группа»).

Абелева группа — это разрешимая группа первой степени.

Разрешимую группу второй степени называют метабелевой. Группа G метабелева, если ее коммутант является абелевой группой (т. е. в G есть нетривиальный абелевый нормальный делитель, фактор-группа по которому тоже абелева).

Найти порождающие ряда последовательных коммутантов группы G (и таким образом выяснить, разрешима или нет данная группа) можно с помощью команды

$$\text{DerivedS}(G).$$

Результатом ее действия будут порождающие элементы каждого из последовательных коммутантов (начиная с нулевой производной — самой группы G).

Проверим, является ли разрешимой группа $G = \text{gr}((1\ 2), (1\ 2\ 3\ 4)\ (9\ 10))$:

```
> with(group):
> G := permgroup(10, {[[1, 2]], [[1, 2, 3, 4], [9, 10]]}):
> DerivedS(G);
```

$$[\text{permgroup}(10, \{[[1, 2]], [[1, 2, 3, 4], [9, 10]]\}),$$

$$\text{permgroup}(10, \{[], [[1, 3, 2]], [[2, 4, 3]]\}),$$

$$\text{permgroup}(10, \{[], [[1, 4], [2, 3]], [[1, 2], [3, 4]]\}),$$

$$\text{permgroup}(10, \{[]\})]$$

Группа G оказалась 3-ступенно разрешимой: ее третий коммутант достиг единицы. Первый коммутант $[G, G] = K_1$ состоит из 12 элементов. Производная группы K_1 — подгруппа $[K_1, K_1]$ — порождается подстановками $(1\ 4)\ (2\ 3)$ и $(1\ 2)\ (3\ 4)$. Без обращения к технике видно, что $[K_1, K_1]$ — это четверная группа Клейна V_4 . Эта группа абелева, и естественно, что ее коммутант (третий в последовательности для исходной группы) превращается в единичную подгруппу.

Напомним определение простого коммутатора и нильпотентности.

Простой коммутатор длины 2 — это $[x_1, x_2] = x_1 x_2 x_1^{-1} x_2^{-1}$. Индукцией по n полагаем:

$$[x_1, x_2, \dots, x_{n-1}, x_n] = [[x_1, x_2, \dots, x_{n-1}], x_n].$$

Группа G называется *нильпотентной*, если все простые коммутаторы длины n равны единице, т. е. в группе G выполняется тождество

$$[x_1, x_2, \dots, x_{n-1}, x_n] = 1.$$

Другими словами, группа G нильпотентна, если убывающая цепочка подгрупп

$$G = G_0 > G_1 > G_2 > \dots > G_k > \dots,$$

порожденных простыми коммутаторами достигает единичной подгруппы. Эта цепочка подгрупп называется *нижним центральным рядом* (*Lower Central Series* — *LCS*).

Найти нижний центральный ряд группы (и таким образом узнать, нильпотентна или нет данная группа) можно с помощью команды

$$LCS(G).$$

Эта команда выдает в качестве результата порождающие подгруппы, порожденных простыми коммутаторами, начиная с коммутаторов «единичной длины», т. е. просто элементов самой группы G .

Проверим, не является ли нильпотентной группа $G = \text{gr}((1\ 2), (1\ 2\ 3\ 4)\ (9\ 10))$:

```
> with(group):
> G := permgroup(10, {[[1, 2]], [[1, 2, 3, 4], [9, 10]]}):
> LCS(G);
```

```
[permgroup(10, {[[1, 2]], [[1, 2, 3, 4], [9, 10]]}),
```

```
permgroup(10, {[[], [[1, 3, 2]], [[2, 4, 3]]})]
```

Выясняется, что нижний центральный ряд оборвался после первого же шага, не достигнув единичной группы. Группа G не нильпотентна.

Чуть ранее было установлено, что группа G разрешима. Таким образом, свойство нильпотентности сильнее свойства разрешимости: *из нильпотентности следует разрешимость, а обратное утверждение неверно.*

Роль силовских подгрупп в связи со свойством нильпотентности обсуждалась в третьей теме.

Силовские p -подгруппы группы G для данного простого p сопряжены в G , поэтому они все изоморфны.

Следовательно, для того чтобы иметь ясное представление об устройстве силовских p -подгрупп для данного p , достаточно найти какую-нибудь силовскую p -подгруппу.

Найти какую-нибудь силовскую p -подгруппу группы H можно с помощью команды

$$Sylow(H, p).$$

Найдем силовские p -подгруппы группы

$$G = \text{gp}((1\ 2), (1\ 2\ 3\ 4)\ (9\ 10)).$$

Чтобы узнать значения простых p , нам необходимо иметь разложение порядка группы G на простые множители. Такое разложение осуществляется в пакете *Number Theory*. Поэтому после задания группы G войдем в пакет «Теория чисел» и разложим число $|P|$ на простые множители:

```
> with(group):  
> G := permgroup(10, {[[1, 2]], [[1, 2, 3, 4], [9, 10]]}):  
> with(numtheory): ifactor(grouporder(G));
```

$$(2)^4(3)$$

Итак, порядок группы G оказался равным 48 (что, впрочем, сейчас не самое главное), а в каноническое разложение порядка входят лишь простые числа 2 и 3.

Это значит, что в группе G содержатся силовские 2-подгруппы (порядка 16) и силовские 3-подгруппы (порядка 3).

Найдем порождающие элементы для одного экземпляра каждого типа:

```
> with(group):  
> G := permgroup(10, {[[1, 2]], [[1, 2, 3, 4], [9, 10]]}):  
> Sylow(G, 2);
```

```
permgroup(10, {[[1, 2], [3, 4], [9, 10]], [[3, 4]], [[1, 3], [2, 4]], [[9, 10]]})
```

```
> Sylow(G, 3);
```

$$\text{permgroup}(10, \{[[2, 3, 4]]\})$$

Все силовские подгруппы сопряжены в группе G , а число различных сопряжений подгруппы H равно индексу нормализатора $N_G(H)$. Поэтому число различных силовских p -подгрупп для фиксированного p равно индексу нормализатора какой-нибудь силовской p -подгруппы.

Найдем индекс нормализатора силовской 2-подгруппы и индекс нормализатора силовской 3-подгруппы группы G из рассматриваемого примера:

```
> with(group):  
> G := permgroup(10, {[[1, 2]], [[1, 2, 3, 4], [9, 10]]}):  
> grouporder(G)/grouporder(normalizer(G, Sylow(G, 2)));
```

$$3$$

```
> grouporder(G)/grouporder(normalizer(G, Sylow(G, 3)));
```

$$4$$

Число силовских 2-подгрупп в группе G равно трем, а число силовских 3-подгрупп — четырем. Полученные числа согласуются с теоремой Силова, согласно которой число силовских p -подгрупп делит порядок всей группы, а при делении на число p дает в остатке единицу.

Может возникнуть желание увидеть не одну, а все силовские p -подгруппы группы H .

Если команду $Sylow(H, p)$ повторять снова и снова, то машина выдаст (вообще говоря, с повторениями) все силовские p -подгруппы группы H .

Найдем таким способом все четыре силовские 3-подгруппы группы

$$G = \text{grp}((1\ 2), (1\ 2\ 3\ 4)\ (9\ 10)):$$

```
> with(group):
> G := permgroup(10, {[[1, 2]], [[1, 2, 3, 4], [9, 10]]}):
> Sylow(G, 3);
```

```
permgroup(10, {[[2, 3, 4]]})
```

```
> Sylow(G, 3);
```

```
permgroup(10, {[[1, 2, 3]]})
```

```
> Sylow(G, 3);
```

```
permgroup(10, {[[1, 4, 3]]})
```

```
> Sylow(G, 3);
```

```
permgroup(10, {[[1, 4, 2]]})
```

Если силовская p -подгруппа группы G единственна, то все ее сопряжения совпадают, а это значит, что она нормальна в G . Если для каждого простого числа p -делителя порядка G в группе G найдется единственная силовская p -подгруппа, то каждая силовская подгруппа нормальна в G . Но тогда группа G является прямым произведением своих силовских подгрупп и, следовательно, нильпотентна.

Группа G из приведенного примера не является нильпотентной, поэтому заранее было ясно, что по крайней мере одна из силовских p -подгрупп содержится в G не в единственном экземпляре.

В то же время информация о том, что одна из силовских p -подгрупп не единственна, означает, что группа точно не нильпотентна и ее нижний центральный ряд не достигает единицы. Каждая неединичная группа имеет по крайней мере два нормальных делителя — это сама группа и ее единичная подгруппа. Эти нормальные делители называются *тривиальными*.

Группа, не имеющая нетривиальных нормальных делителей, называется *простой*.

Просто перебрав нормальные замыкания всех циклических подгрупп группы G , можно выяснить, проста G или нет.

Покажем, что A_5 — знакопеременная группа пятой степени — простая группа.

Для этого достаточно увидеть, что нормальное замыкание произвольного неединичного элемента из A_5 совпадает со всей A_5 . Неединичный элемент x из A_5 , представленный в виде произведения независимых циклов, может иметь вид $(a\ b\ c)$, или $(a\ b)\ (c\ d)$, или $(a\ b\ c\ d\ e)$. Вместо буквенных символов можно поставить и конкретные (но различные) числа: если для каких-то конкретных чисел наше утверждение о нормальном замыкании окажется верным, то и для любых других оно тоже будет верным (все передвигаемые символы равноправны).

Возьмем, например, подстановки $(1\ 2\ 3\ 4\ 5)$, $(1\ 2\ 3)$ и $(1\ 2)\ (3\ 4)$ и найдем порядки их нормальных замыканий в A_5 . Напомним, что сама A_5 содержит 60 элементов:

```
> with(group):
> S := permgroup(5, {[[1, 2, 3]], [[2, 3, 4]], [[3, 4, 5]]}):
> grouporder(NormalClosure(permgroup(5, {[[1, 2, 3, 4, 5]]}), S));
```

60

```
> grouporder(NormalClosure(permgroup(5, {[[1, 2, 3]]}), S));
```

60

```
> grouporder(NormalClosure(permgroup(5, {[[1, 2], [3, 4]]}), S));
```

60

Все эти замыкания совпадают с группой A_5 , поэтому группа A_5 проста.

Аналогично с помощью техники можно установить, что и A_6 , и A_7 , и вообще A_n для конкретного $n > 4$ проста. Однако машина бессильна показать, что на самом деле это утверждение верно для любого $n > 4$.

Прежде чем доказать это утверждение, рассмотрим вопрос о порождающих элементах групп A_n . Симметрическая группа порождается всего двумя элементами. Сколько же порождающих имеет знакопеременная группа? Эта группа порождается произведениями пар транспозиций, а каждая такая пара представима в виде произведения тройных циклов:

$$\begin{aligned}(ab)(cd) &= (abc)(adc), \\ (ab)(ac) &= (abc).\end{aligned}$$

В множестве из n элементов содержится

$$\frac{n(n-1)(n-2)}{6}$$

трехэлементных подмножеств, и это число с возрастанием n увеличивается чрезвычайно быстро.

Попробуем подойти к проблеме «с другого бока».

Группа A_2 — это просто единичная группа, группа A_3 циклическая, т. е. однопорожденная. Поскольку A_n нормальна в S_n , все сопряжения любого элемента, а следовательно, и все нормальные замыкания в S_n элементов из A_n содержатся в A_n . Более того, для $n \geq 5$ все группы A_n просты, поэтому нормальные замыкания будут совпадать со всей группой A_n . Впрочем, эти совпадения начинаются уже с A_3 : неединичные элементы из A_3 сопряжены в S_3 .

Рассмотрим теперь ситуацию с группой A_4 , а именно: возьмем нормальное замыкание N цикла $(1\ 2\ 3)$ в S_4 и вычислим порядок N :

```
> with(group):
> S := permgroup(4, {[[1, 2]], [[1, 2, 3, 4]]}):
> G := permgroup(4, {[[1, 2, 3]]}):
> N := NormalClosure(G, S);

N := permgroup(4, {[[1, 2, 3]], [[2, 3, 4]]})
> grouporder(N);
```

12

Оказалось, что подгруппа N содержит 12 элементов из группы A_4 , порядок которой как раз и равен 12. Итак,

$$A_4 = \text{gr}((1\ 2\ 3), (2\ 3\ 4)).$$

Сделаем ту же процедуру для группы A_5 и получим:

```
> with(group):
> S := permgroup(5, {[[1, 2]], [[1, 2, 3, 4, 5]]}):
> G := permgroup(5, {[[1, 2, 3]]}):
> N := NormalClosure(G, S);

N := permgroup(5, {[[3, 4, 5]], [[1, 2, 3]], [[2, 3, 4]]})
> grouporder(N);
```

60

Вычисление порядка группы N сейчас было даже излишним: в силу простоты группы A_5 заранее было ясно, что $N = A_5$. Другое дело порождающие элементы:

$$A_5 = \text{gr}((1\ 2\ 3), (2\ 3\ 4), (3\ 4\ 5)).$$

Нетрудно уловить и общую закономерность: знакопеременная группа n -й степени имеет $n - 2$ порождающих:

$$A_n = \text{gr}((1\ 2\ 3), (2\ 3\ 4), \dots, (n-3\ n-2\ n-1), (n-2\ n-1\ n)).$$

Сделаем контрольный эксперимент. Найдем таким же способом порождающие группы A_{10} :

```
> with(group):
> S := permgroup(10, {[[1, 2]], [[1, 2, 3, 4, 5, 6, 7,
    8, 9, 10]]}):
> G := permgroup(10, {[[1, 2, 3]]}):
> N := NormalClosure(G, S);

N := permgroup(10, {[[5, 6, 7]], [[1, 2, 3]], [[8, 9, 10]],
    [[7, 8, 9]], [[6, 7, 8]], [[2, 3, 4]], [[3, 4, 5]], [[4, 5, 6]]})
```

Эксперимент удался: группа A_5 действительно имеет восемь порождающих указанного вида.

Впрочем, число порождающих элементов для группы A_n можно и уменьшить. Например, если n нечетно, то цикл длины n и тройной цикл порождают группу A_n , т. е. для нечетного n

$$A_n = \text{gr}((1\ 2\ 3\ \dots\ n), (1\ 2\ 3)).$$

Для $n = 3$ это утверждение очевидно: A_3 как раз и порождается одним тройным циклом. Проверим эту гипотезу сначала для $n = 5$:

```
> with(group):
> S := permgroup(5, {[[1, 2, 3, 4, 5]], [[1, 2, 3]]}):
> grouporder(S);
```

60

Такую проверку выдерживают и другие конкретные группы. Проведем снова контрольный эксперимент, например, для $n = 13$. Группа A_{13} имеет порядок $\frac{13!}{2} = 311351040$:

```
> with(group):
> S := permgroup(13, {[[1, 2, 3, 4, 5, 6, 7, 8, 9,
    10, 11, 12, 13]], [1, 2, 3]]}):
> grouporder(S);
```

311351040

С помощью компьютерных экспериментов и команды *NormalClosure* можно найти и другие интересные виды порождающих для A_n

с нечетным n . Например, для нечетного n группа A_n порождается двумя циклами длины n :

$$A_n = \text{gr}((1\ 2\ 3\ 4\ \dots\ n), (2\ 1\ 3\ 4\ \dots\ n)),$$

что забавно напоминает знаменитую игру в пятнадцать.

Проверим это утверждение для $n = 15$:

```
> with(group):
> S := permgroup(15, {[[1, 2]], [[1, 2, 3, 4, 5, 6, 7, 8, 9,
10, 11, 12, 13, 14, 15]]}):
> G := permgroup(15, {[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,
13, 14, 15]]}):
> N := NormalClosure(G, S);
```

```
N := permgroup(15, {[[2, 1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]],
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]]})
```

```
> grouporder(N);
```

653837184000

```
> 15!/2;
```

653837184000

Если n четное, то небольшая поправка большого и малого циклов также дает два порождающих симметрической группы, а именно для четных $n > 2$

$$A_n = \text{gr}((1\ 2\ 3\ 4\ \dots\ n-1), (1\ 2\ n)).$$

Например, для $n = 4$ группа, порожденная такими подстановками, действительно имеет нужный порядок, т. е. 12:

```
> with(group):
> G := permgroup(4, {[[1, 2, 3]], [[1, 2, 4]]}):
> grouporder(G);
```

12

Сделаем контрольный эксперимент сразу для степени побольше, например для $n = 20$. Предварительно заметим, что $|A_{20}| = \frac{20!}{2} = 1\ 216\ 451\ 004\ 088\ 320\ 000$:

```
> with(group):
> G := permgroup(20, {[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,
13, 14, 15, 16, 17, 18, 19]],
```

```
[[1, 2, 20]]}):  
> grouporder(G);
```

1 216 451 004 088 320 000

Универсальным (т. е. не зависящим от четности или нечетности степени подстановок) порождающим множеством знакопеременной группы для любого $n > 2$ будет, например, множество

$$\{(1\ 2\ 3), (1\ 2\ 4), \dots, (1\ 2\ n)\}.$$

Продемонстрируем это свойство на примерах: $n = 4$, $n = 5$, $n = 10$:

```
> with(group):  
> grouporder(permgroupe(4, {[[1, 2, 3]], [[1, 2, 4]]}));
```

12

```
> grouporder(permgroupe(5, {[[1, 2, 3]], [[1, 2, 4]],  
  [[1, 2, 5]]}));
```

60

```
> grouporder(permgroupe(10, {[[1, 2, 3]], [[1, 2, 4]],  
  [[1, 2, 5]], [[1, 2, 6]], [[1, 2, 7]], [[1, 2, 8]],  
  [[1, 2, 9]], [[1, 2, 10]]}));
```

1 814 400

```
> 10!/2;
```

1 814 400

Покажем теперь, что для любого $n > 4$ группа A_n проста.

Уже отмечено, что циклы длины 3 порождают группу A_n . Пусть N — нормальный делитель группы A_n и α — неединичная подстановка из N , перемещающая наименьшее число символов. Если $\alpha = (abc)$, то рассмотрим две подстановки:

$$\sigma_1 = \begin{pmatrix} a & b & c & d & e & \dots \\ u & v & w & d & e & \dots \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} a & b & c & d & e & \dots \\ u & v & w & e & d & \dots \end{pmatrix},$$

в которых элементы, стоящие на месте многоточий, остаются неподвижными. Одна из подстановок σ_1, σ_2 принадлежит группе A_n . Обозначим эту подстановку символом σ . Тогда

$$\gamma_1 = \sigma^{-1}\alpha\sigma = (uvw) —$$

элемент из N . Следовательно, вместе с α нормальный делитель N содержит и все порождающие элементы группы A_n , т. е. $N = A_n$.

Предположим теперь, что α не является тройным циклом, но разложение α содержит цикл, длина которого не меньше трех:

$$\alpha = (abc\dots)\dots$$

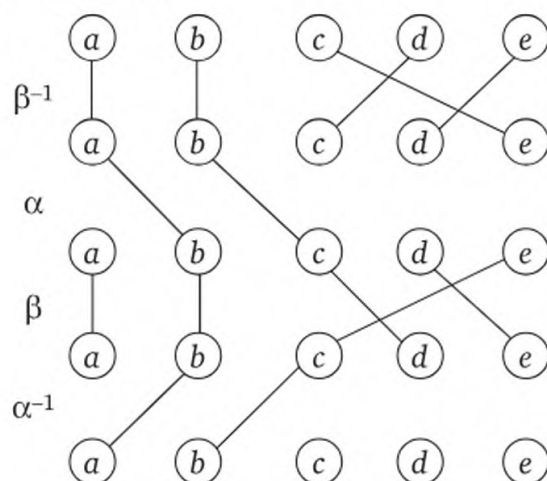
Поскольку α четная, она должна перемещать по крайней мере еще два символа, например d, e . Если $\beta = (c d e)$, то коммутатор

$$\gamma = \beta^{-1}\alpha\beta\alpha^{-1}$$

принадлежит N . Эта подстановка не равна единице, так как

$$\beta^{-1}\alpha\beta(b) \neq \alpha(b).$$

Подстановка γ оставляет на месте все символы, которые оставляет α , и $\gamma(a) = a$. Все это наглядно видно на фрагменте графа, изображающего подстановку γ .



Итак, если подстановка α содержит в своем разложении цикл длины не менее трех, то α — это просто тройной цикл.

Если α является произведением независимых транспозиций

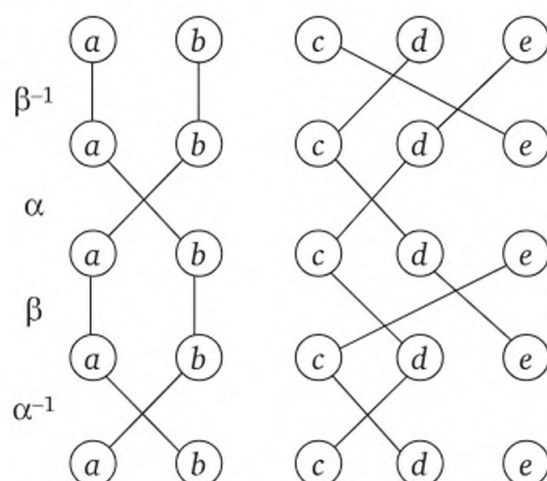
$$\alpha = (ab)(cd)\dots,$$

то снова тот же коммутатор неединичен и, оставляя неподвижными все перемещаемые символы α , дополнительно не трогает символы a, b .

Снова получено противоречие с выбором α , а это значит, что подстановка α может быть только тройным циклом. Следовательно, $N = A_n$. Группа A_n проста.

Отметим, что теперь появляется не одна, а целая бесконечная серия групп, для которых обращение теоремы Лагранжа неверно. Действительно, для $n > 4$ порядок группы A_n всегда четный, однако

подгруппы индекса 2 там нет, подгруппа индекса 2 является нормальным делителем, а A_n проста.



Пусть теперь G — произвольная группа. Как узнать, проста или нет эта группа?

Группа непроста, если она содержит нетривиальную нормальную подгруппу. Однако группа может содержать не просто нормальные, а характеристические или даже вполне характеристические подгруппы.

Если группа абелева и непростого порядка, то она точно непроста (а если простого порядка, то проста). Таким образом, проблема простоты для абелевой группы решается легко.

Если группа G неабелева (т. е. не совпадает со своим центром), но центр ее неединичен, то G имеет нетривиальную характеристическую подгруппу¹ — центр $Z(G)$, и, следовательно, G непроста.

Группу с самым маленьким, т. е. единичным, центром образно называют *группой без центра*.

Разыскивается центр группы G с помощью машинной команды

$$\text{center}(G).$$

Для примера найдем центр симметрической группы S_4 :

```
> with(group):
> center(permgrou(4, {[[1, 2]], [[1, 2, 3, 4]]}));

permgrou(4, {})
```

Группа S_4 оказалась группой без центра.

Группа $G = \text{gr}((1\ 2\ 3), (3\ 2\ 1)\ (4\ 5), (5\ 6))$ — пример группы с центром.

¹ Центр группы — характеристическая, но не всегда вполне характеристическая подгруппа, т. е. центр может и не выдержать некоторый эндоморфизм группы.

Действительно:

```
> with(group):  
> G := permgroup(6, {[[1, 2, 3]], [[3, 2, 1], [4, 5]], [[5, 6]]}):  
> grouporder(G);
```

18

```
> Z := center(G); grouporder(Z);
```

```
Z := permgroup(6, {[[1, 2, 3]])
```

3

Таким образом, простоту группы S_4 с помощью ее центра установить не удалось, а группа

$$G = \langle (1\ 2\ 3), (3\ 2\ 1)\ (4\ 5), (5\ 6) \rangle$$

точно не проста: она содержит даже не просто нормальную, а характеристическую подгруппу.

Как проверить, содержит ли данная группа G какую-нибудь вполне характеристическую подгруппу?

Любая вербальная подгруппа группы G является вполне характеристической в G . Например, таковыми являются все производные группы (члены последовательности коммутантов), а также группы, порожденные значениями слов — простых коммутаторов, т. е. все члены нижнего центрального ряда.

Первым членом и производного ряда, и LCS является коммутант группы G , и он точно нормален в группе G .

Правда, для абелевой группы коммутант опять ничего не даст, как и центр. В этом случае какая-нибудь искомая подгруппа будет слишком мала.

Уже заметили, что задача «проста или не проста» для абелевой группы несложна, и можно считать, что испытываемая на простоту группа G неабелева.

Правда, если группа неабелева, то может случиться, что ни центр, ни коммутант не дадут нужной информации.

Центр может оказаться слишком мал (т. е. единичный), а коммутант, напротив, слишком велик (совпадающий со всей группой G).

Если испытываемая на простоту неабелева группа G действительно проста, то так и будет: $Z(G) = E$, а $[G, G] = G$.

Вернемся, однако, к группе S_4 . Ее центр не помог решить проблему простоты (или непростоты) этой группы. Обратимся за помощью к коммутанту:

```
> with(group):  
> S[4] := permgroup(4, {[[1, 2]], [[1, 2, 3, 4]]}):  
> K := derived(S[4]);
```

```
K := permgroup(4, {[[], [[2, 4, 3]], [[1, 3, 2]]})
```


Коммутант найден. Он порождается четными подстановками, поэтому наверняка не совпадает со всей группой S_4 . Определить истинные его размеры несложно:

```
> with(group):
> grouporder(permgroupe(4, {[[[2, 4, 3]], [[1, 3, 2]]]}));
```

12

Порядок коммутанта $[S_4, S_4]$ оказался в точности равен порядку A_4 . Коммутант находится в A_4 , и, следовательно, $[S_4, S_4] = A_4$.

Заметим, что и для любого $n > 2$ коммутант группы S_n равен A_n .

Действительно, группа A_n порождается циклами длины три, а те, в свою очередь, являются коммутаторами:

$$(abc) = (ab) \cdot (bc) \cdot (ab) \cdot (bc).$$

Таким образом, для любого $n > 2$ группы S_n не просты, и более того, все эти группы содержат по крайней мере одну вполне характеристическую подгруппу.

8.4. Фактор-группы

Фактор-группа G/N группы G по нормальному делителю N состоит из смежных классов по N

$$G/N = \{Ng \mid g \in G\},$$

с умножением, определенным по представителям, т. е.

$$Nx \cdot Ny \stackrel{\text{опр}}{=} Nxy.$$

Найти представителей правых смежных классов (а для нормальных подгрупп представители правых классов одновременно представляют и левые классы) можно с помощью команды

$$\text{cosets}(G, N).$$

Таким образом, получают представители элементов фактор-группы G/N .

Фактор-группа конечной группы, разумеется, сама конечна, поэтому может быть представлена как группа подстановок, степень которых не превышает степени группы G . Пока машинной команды для нахождения порождающих элементов фактор-группы в пакете компьютерной алгебры нет, поэтому в каждом конкретном случае нахождение группы подстановок, изоморфно представляющей данную фактор-группу, является маленькой творческой задачей.

В предыдущих темах был пример ручного нахождения фактор-группы. Проверим полученный результат машинными вычислениями.

Итак, найдем с помощью пакета *Maple* фактор-группу S_4 / V_4 группы S_4 по четверной группе Клейна V_4 :

```
> with(group):
> S[4] := permgroup(4, {[[1, 2]], [[1, 2, 3, 4]]}):
> V[4] := permgroup(4, {[[1, 2], [3, 4]], [[1, 3], [2, 4]]}):
> cosets(S[4], V[4]);
```

```
{[], [[2, 3]], [[3, 4]], [[2, 4, 3]], [[2, 3, 4]], [[2, 4]]}
```

Отметим, что представителями смежных классов оказались элементы группы S_3 , записанной на символах 2, 3, 4. Точнее говоря, множество

$$\{e, (2\ 3), (3\ 4), (2\ 4\ 3), (2\ 3\ 4), (2, 4)\}$$

образует подгруппу в S_4 , и эта подгруппа изоморфна S_3 .

Это значит, что группа S_4 совпадает с комплексом $S_3 K$ (но не является прямым их произведением, так как S_3 — ненормальная подгруппа в S_4). Однако наша подгруппа S_3 не содержит ни одного неединичного элемента из K . Это значит, что S_4 является *полупрямым произведением* S_3 и K :

$$S_4 = K \rtimes S_3.$$

Итак, мы снова нашли фактор-группу S_4 / K и снова выяснили внутреннее строение группы S_4 .

Заметим, что если заранее известно, что группа раскладывается в полупрямое (или даже в прямое) произведение, то фактор-группу по «нормальной части» легко найти и вручную — это просто второй (вообще говоря, ненормальный) дополняющий множитель.

Для произвольной группы G фактор-группа $G / Z(G)$ по ее центру изоморфна группе $\text{Inn}(G)$ внутренних автоморфизмов группы G . Таким образом, отыскание группы $\text{Inn}(G)$ сводится к нахождению $Z(G)$ группы G и описанию фактор-группы $G / Z(G)$.

Если группа G без центра (т. е. $Z(G) = E$), то она изоморфна своей группе внутренних автоморфизмов. Например, такими будут все простые неабелевы группы. Впрочем, S_n при $n > 2$ не проста, но тоже без центра, например:

```
> with(group):
> G := permgroup(3, {[[1, 2]], [[1, 2, 3]]}):
> Z := center(G);
```

$$Z := \text{permgroup}(3, \{\})$$

```
> G := permgroup(4, {[[1, 2]], [[1, 2, 3, 4]]}):
> Z := center(G);
```

```
Z := permgroup(4, {})
```

Рассмотрим менее тривиальный пример. Найдём группу внутренних автоморфизмов группы $G = \text{gr}((1\ 2)\ (4\ 3), (1\ 2\ 5)\ (3\ 4))$.

Сначала вычислим порядок группы и её центр:

```
> with(group):
> G := permgroup(5, {[[1, 2], [4, 3]], [[1, 2, 5], [3, 4]]}):
> grouporder(G);
```

12

```
> Z := center(G);
```

```
Z := permgroup(5, {[[3, 4]]})
```

Группа содержит 12 элементов, а центром является циклическая подгруппа второго порядка. Следовательно, порядок фактор-группы $G/Z(G)$ равен $\frac{12}{2} = 6$. Фактор-группа по центру не может быть циклической, значит, $G/Z(G)$ нециклическая. Нециклическая группа шестого порядка всего одна, это S_3 — симметрическая группа третьей степени.

Итак, группа $\text{Inn}(G)$ найдена. Группа внутренних автоморфизмов группы G изоморфна S_3 .

8.5. Исследование абстрактной группы

Абстрактной группой обычно называют группу, заданную порождающим множеством и определяющими соотношениями. Такое задание называют *копредставлением* (или *представлением*) группы.

Если группа конечна, то её можно изоморфно представить в виде группы подстановок и в дальнейшем при её изучении воспользоваться машинными командами, рассмотренными в предыдущей теме. С бесконечными группами дело, как правило, обстоит значительно сложнее, но в некоторых случаях вычислительная техника все-таки может помочь.

Как и для групп подстановок, исследование произвольной абстрактной группы осуществляется с помощью пакета *Group Theory*. Чтобы исследовать группу, нужно сначала войти в этот пакет. Вход осуществляется командой *with(group)*.

Список машинных команд, применимых для групп, заданных копредставлением, значительно беднее, чем для групп подстановок. Выделим эти команды из общего перечня пакета *Group Theory*:

cosets, cosrep, grelgroup, grouporder, isnormal, permrep, pres, subgrel.

Далее рассмотрим особенности и методику их применения для исследования произвольной абстрактной группы.

Если группа G задана копредставлением, т. е. порождающим множеством a_1, a_2, \dots, a_n и определяющими соотношениями $R_1(a_i) = 1, R_2(a_i) = 1, \dots, R_k(a_i) = 1$, то пишут:

$$G = \langle a_1, a_2, \dots, a_n; R_1(a_i) = 1, R_2(a_i) = 1, \dots, R_k(a_i) = 1 \rangle.$$

Распространена также укороченная запись без символов равенства и единиц:

$$G = \langle a_1, a_2, \dots, a_n; R_1(a_i), R_2(a_i), \dots, R_k(a_i) \rangle.$$

Если определяющее соотношение первоначально имело вид $U = W$, то его можно переписать в виде $UW^{-1} = 1$. Например, четвертая группа Клейна V_4 задается копредставлением

$$V_4 = \langle a, b; a^2 = 1, b^2 = 1, ab = ba \rangle,$$

что удобнее для ручного исследования, но для машины это копредставление должно быть преобразовано в следующее:

$$V_4 = \langle a, b; a^2, b^2, aba^{-1}b^{-1} \rangle.$$

Для компьютерного задания группы

$$G = \langle a_1, a_2, \dots, a_n; R_1(a_i), R_2(a_i), \dots, R_k(a_i) \rangle$$

компьютерная команда имеет вид

$$\text{grelgroup}(\{a_1, a_2, \dots, a_n\}, \{R_1(a_i), R_2(a_i), \dots, R_k(a_i)\}).$$

Например, копредставление циклической группы порядка n , порожденной элементом a , имеет вид $\langle a; a^n \rangle$. Для компьютера n должно быть конкретным (и не очень большим; число $n = 100\,000\,000$ для современной техники уже недоступно).

Пусть, например, группа $G = \langle a; a^5 \rangle$ циклическая пятого порядка. Тогда она вводится в компьютер следующим образом:

```
> with(group):
> K := relgroup({a}, {[a, a, a, a, a]});
```

$$K := \text{grelgroup}(\{a\}, \{[a, a, a, a, a]\})$$

Для задания соотношения a^n можно не записывать n раз символ a , а воспользоваться командой $\$n$:

```
> with(group):
> K := relgroup({a}, {[a$5]});
```

$$K := \text{grelgroup}(\{a\}, \{[a, a, a, a, a]\})$$

Символ \$ при записи определяющего соотношения можно использовать несколько раз. Например, зададим группу $H = \langle a, b; a^{-10}b^4a^{-13}b^5 \rangle$:

```
> with(group):
> H := relgroup({a, b}, {[1/a$10, b$4, 1/a$13, b$5]});
H := relgroup({a, b}, [[1/a, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, b, b,
b, b, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, 1/a, b, b, b, b, b]]).
```

Если порядок циклической группы больше 10^8 , то машина сразу сообщает, что это число слишком большое. Интересно, что копредставление нециклической группы порядка, значительно больше 10^8 , и даже заведомо бесконечной группы (например, как только что введенная группа H с одним определяющим соотношением) машина принимает для обработки (хотя эта обработка часто ей недоступна).

Машина может отказаться от работы в момент задания группы. Причем против задания, например, бесконечной циклической группы $G_1 = \langle a \rangle$ или бесконечной группы диэдра $G_2 = \langle a, b; a^2, b^2 \rangle$ техника ничего против не имеет, а циклическая группа $G_3 = \langle a; a^{100\,000\,000} \rangle$ для нее «слишком большой объект»:

```
> with(group):
> G[1] := relgroup({a}, {});
G1 := relgroup({a}, {});
> G[2] := relgroup({a, b}, {[a, a], [b, b]});
G2 := relgroup({a, b}, {[a, a], [b, b]});
> G[3] := relgroup({a}, {[a$100000000]}):
```

Error, object too large

Особенность командной записи в одну строку сказывается и на изображении отрицательных степеней в определяющих соотношениях. Например, копредставление четверной группы Клейна

$$V_4 = \langle a, b; a^2, b^2, aba^{-1}b^{-1} \rangle$$

в машинном варианте выглядит так:

```
> with(group):
> V[4] := relgroup({a, b}, {[a, a], [b, b], [a, b, 1/a, 1/b]});
```


$$V_4 := \text{grelgroup} \left(\{a, b\}, \left\{ [a, a], [b, b], \left[a, b, \frac{1}{a}, \frac{1}{b} \right] \right\} \right).$$

Порождающие элементы группы можно обозначать латинскими буквами с большими индексами. Та же группа Клейна

$$\langle a_1, a_2; a_1^2, a_2^2, a_1 a_2 a_1^{-1} a_2^{-1} \rangle$$

в машинной записи имеет следующий вид:

```
> with(group):
> V[4] := grelgroup({a[1], a[2]}, {[a[1], a[1]], [a[2], a[2]],
[a[2], a[2], 1/a[1], 1/a[2]]});
```

$$V_4 := \text{grelgroup} \left(\{a_1, a_2\}, \left\{ [a_1, a_1], [a_2, a_2], \left[a_2, a_2, \frac{1}{a_1}, \frac{1}{a_2} \right] \right\} \right).$$

Более того, при задании группы с порождающими a_2, a_3, \dots, a_n можно использовать одни индексы без букв (кроме индекса «1», так как он применяется при изображении обратного элемента).

Таким образом, следующий пример — это тоже группа Клейна:

```
> with(group):
> V[4] := grelgroup({2, 3}, {[2, 2], [3, 3], [2, 3, 1/2, 1/3]});
```

$$V_4 := \text{grelgroup} \left(\{2, 3\}, \left\{ [2, 2], \left[2, 3, \frac{1}{2}, \frac{1}{3} \right], [3, 3] \right\} \right).$$

Команда $\text{grouporder}(G)$ применима и для группы G , заданной ко-представлением.

Пусть, например:

$$G = \langle a, b; a^2 b a b^4 = 1, b^2 a b a^4 = 1 \rangle.$$

Найдем ее порядок:

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
> grouporder(G);
```

144

Группа G конечна и содержит 144 элемента.

Машина в некоторых случаях может определить и бесконечный порядок. Группа диэдра

$$G = \langle x, y: x^2, y^2 \rangle$$

и группа с одним соотношением

$$H = \langle a, b; a^{-10} b^4 a^{-13} b^5 \rangle —$$

обе бесконечны, и машинная проверка это подтверждает:

```
> with(group):  
> G := relgroup({x, y}, {[x, x], [y, y]});  
> grouporder(G);
```

∞

```
> H := relgroup({a, b}, {[1/a$10, b$4, 1/a$13, b$5]}):  
> grouporder(H);
```

∞

В некоторых случаях бесконечность группы легко определить и без вычислительной техники. Если комбинаторное копредставление группы имеет особый вид, то вопрос о порядке такой группы упрощается.

Например, если число определяющих соотношений группы строго меньше числа порождающих, то эта группа бесконечна (в пакете *Maple* эта информация заложена; после вопроса о порядке для таких групп компьютер сразу выдает символ бесконечности).

Если копредставление группы G распадается на представления двух неединичных подгрупп, то группа G образует свободное произведение этих подгрупп.

Точнее говоря, группа G — свободное произведение своих подгрупп (пишут: $G = A * B$), если G обладает копредставлением, полученным из представлений групп A, B теоретико-множественным объединением:

$$A * B = \langle \text{порождающие } A, \text{ порождающие } B;$$

$$\text{соотношения } A, \text{ соотношения } B \rangle.$$

В свободном произведении $G = A * B$ содержатся подгруппы, изоморфные множителям (можно считать, что это сами группы A, B): они порождают группу G , и пересечение этих подгрупп единично.

Если множители A, B неединичны, то свободное произведение всегда бесконечно.

Таким образом, вопрос о порядке группы, разложимой в свободное произведение, сводится к вопросу о нетривиальности подгрупп — множителей (или к вопросу о порядке одного из этих множителей, если второй — единичная подгруппа).

В самой общей ситуации группа G порождается двумя своими подгруппами A и B , но их пересечение $D = A \cap B$ неединично.

Поэтому более сильной конструкцией, чем свободное произведение, является свободное произведение с объединением. В таком случае в группе A содержится подгруппа U , а в группе B — подгруп-

па W , причем U и W изоморфны. Пусть φ — изоморфизм между подгруппами U и W , переводящий каждый порождающий u_j подгруппы U в порождающий w_j подгруппы W . Если группа G является свободным произведением групп A и B с объединенными подгруппами U и W при склеивающем изоморфизме φ , т. е.

$$G = A *_U B = A *_W B,$$

то G обладает копредставлением, полученным из представлений групп A, B теоретико-множественным объединением представлений A и B и пополненным равенствами вида $\varphi(u_i) = w_j$:

$$A *_U B = \langle \text{порождающие } A, \text{ порождающие } B;$$

$$\text{соотношения } A, \text{ соотношения } B, \varphi(u_i) = w_j \rangle.$$

Если группа U — собственная подгруппа группы A , а W — собственная подгруппа группы B , то свободное произведение с объединением $A *_U B$ всегда бесконечно.

Таким образом, вопрос о порядке группы, разложимой в обобщенное свободное произведение, сводится к вопросу о совпадении объединяемой подгруппы с одним из множителей (или к вопросу о порядке наибольшего по включению множителя, если наименьший множитель содержится в большем).

Свойство конечно определенной группы называется *марковским*¹, если:

- 1) существует группа, обладающая этим свойством;
- 2) существует группа, не обладающая этим свойством, такая, что и все ее надгруппы тоже не обладают этим свойством.

Марковское свойство алгоритмически неразлично. Это значит, что не существует алгоритма для узнавания, обладает ли группа данным свойством.

Поскольку свойство «иметь конечный порядок» является марковским, задача вычисления порядка для всех конечно определенных групп алгоритмически неразрешима.

Это означает, в частности, что не для каждой конечно определенной группы машина всегда будет выдавать результат.

Действительно, для некоторых (иногда конечных, и даже не очень больших) порядков компьютер конечный результат не выдает. Он может считать очень долго, не останавливаясь (и это может означать, что порядок исследуемой группы бесконечен или конечен, но для машины слишком велик), может зависнуть или,

¹ Андрей Андреевич Марков (1903—1979) — русский математик, член-корреспондент АН СССР (с 1953 г.).

прекратив вычисления, сообщить, что программа будет закрыта. Например, вычисляя порядок группы

$$H = \langle x, y : x^2, y^3 \rangle$$

с помощью *Maple*, верный результат получить не удастся. Проработав некоторое время, машина сообщает, что программа выполнила недопустимую операцию и будет закрыта.

Отметим, что для человека вычисление порядка группы H никаких трудностей не представляет: группа H разложима в свободное произведение неединичных групп и поэтому бесконечна.

Это значит, что «узнавания» свободных произведений в пакете *Maple* пока нет.

При этом порядок группы

$$G = \langle x, y : x^4, y^4, x^2y^{-2} \rangle,$$

разложимой в свободное произведение с объединенной подгруппой (и поэтому бесконечной), компьютер определяет быстро и точно, т. е. обобщенное произведение он «узнал»:

```
> with(group):
> G := grelgroup({x, y}, {[x, x, x, x], [y, y, y, y],
  [x, x, 1/y, 1/y]}):
> grouporder(G);
```

∞

Следует иметь в виду одно интересное обстоятельство. Пытаясь решить непосильную для него задачу о порядке группы, компьютер может поступить «чисто по-человечески»: только для того, чтобы от него отстали, он просто выдает неверный результат.

Часто этим результатом является символ ∞ или 1, поэтому именно к машинному сообщению о бесконечности или тривиальности группы следует относиться недоверчиво.

Для группы G , заданной копредставлением, важной проблемой является нахождение копредставления подгруппы, заданной порождающим множеством. Дело в том, что хотя сама группа G имеет в копредставлении и порождающие элементы, и определяющие соотношения, подгруппа H группы G уже будет задана *только порождающими*.

Естественно, что для полного описания подгруппы H нужны дополнительно и соотношения между этими (или какими-либо другими) ее порождающими.

Пусть $H = \text{гр}(h_1, h_2, \dots, h_m)$ — подгруппа группы $G = \text{гр}(a_1, a_2, \dots, a_n)$. Таким образом, h_i — это слова в алфавите $a_1, \dots, a_n, a_1^{-1}, \dots, a_n^{-1}$, $h_i = w(a_j)$ для $i = 1, 2, \dots, m$.

Находится копредставление подгруппы H группы G с помощью двух команд. Первой командой

$$\text{subgrel}(\{h_1 = w(a_j), h_2 = w(a_j), \dots, h_m = w(a_j)\}, G)$$

вводится информация о подгруппе H , второй командой

$$\text{pres}(H)$$

строится копредставление подгруппы H .

Пусть группа G задана копредставлением

$$G = \langle a, b : a^2bab^3 = 1, b^2aba^3 = 1 \rangle.$$

Рассмотрим в ней подгруппу $H = \text{gr}(a^2)$, порожденную элементом a^2 .

Ясно, что подгруппа H циклическая, но порядок ее неизвестен. Может быть, она совпадает со всей группой, но также возможно, что H сжимается в единицу. Чтобы иметь полную информацию о группе H , найдем ее копредставление:

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$3], [b, b, a, b, a$3]}):
> H := subgrel({x=[a, a]}, G):
> pres(H);
```

$$\text{grelgroup}(\{x\}, \{[x, x, x, x, x, x, x]\})$$

Представление для H найдено,

$$H = \langle x; x^7 = 1 \rangle.$$

Обе команды для нахождения копредставления подгруппы можно объединить в одну. Найдем, например, в группе

$$G = \langle a, b; a^2bab^4 = 1, b^2aba^4 = 1 \rangle$$

представление подгруппы H , порожденной элементами ab и b^2 . Поинтересуемся заодно, не совпадает ли эта подгруппа со всей группой G . Для этого просто вычислим порядок подгруппы H и порядок подгруппы G :

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
> H := pres(subgrel({x=[a, b], y=[b, b]}, G));
```

$$H := \text{grelgroup}\left(\{x, y\}, \left\{\left[x, x, y, y, \frac{1}{x}, y, y, \frac{1}{x}, \frac{1}{x}, y\right], \left[x, y, y, \frac{1}{x}, \frac{1}{x}, \frac{1}{y}, x, x, y, y, \frac{1}{x}, y, y, \frac{1}{x}, \frac{1}{x}, \frac{1}{y}, x, x, y, y, \frac{1}{x}, \frac{1}{x}, \frac{1}{y}\right]\right\}\right)$$


```
> grouporder(G); grouporder(H);
```

144

72

Итак, H — собственная подгруппа группы G , и H имеет копредставление

$$H = \langle x, y; x^2y^2x^{-1}y^2x^{-2}y, xy^2x^{-2}y^{-1}x^2y^2, (xy)^2yx^{-1}y^2x^{-2}y^{-1}x^2y^{-2}x^{-2}y^{-1} \rangle.$$

Отметим, что с задачей машина справилась потому, что группа G конечная. Нахождение копредставления подгрупп конечного индекса для техники тоже, как правило, не вызывает затруднений.

Например, группа

$$G = \langle a, b; a^2 = 1, b^2 = 1 \rangle$$

является свободным произведением неединичных групп, поэтому бесконечна. Найдем копредставление подгруппы H , порожденной элементом ab :

```
> with(group):
> G := grelgroup({a, b}, {[a, a], [b, b]}):
> H := subgrel({x=[a, b, a, b]}, G):
> pres(H);
```

$$\text{grelgroup}(\{x\}, \{[]\})$$

Это значит, что подгруппа H , порожденная элементом $x = ab$, в группе

$$G = \langle a, b; a^2 = 1, b^2 = 1 \rangle$$

имеет копредставление $H = \langle x \rangle$.

Отметим, что подгруппа H нормальна в G , ее индекс равен 2.

Множество соотношений у подгруппы H пустое (равенство $1 = 1$ тривиальное, оно выполняется в любой группе). Порождающий элемент x , на который не наложено никаких соотношений, кроме тривиальных, называется свободным порождающим.

Группы, которые можно записать без определяющих соотношений, называют свободными группами. Свободную группу можно задать копредставлением

$$F_r = \langle x_1, x_2, \dots, x_r \rangle.$$

Порождающие x_1, x_2, \dots, x_r при таком представлении свободны, а их число называют рангом свободной группы, т. е. группа F_r — это свободная группа ранга r .

Группа $\langle x \rangle$ — свободная ранга 1 (она же бесконечная циклическая группа). Свободная группа ранга r является свободным произведением r бесконечных циклических групп.

Заметим, что у свободной группы могут быть и несвободные порождающие. Например (в аддитивной записи) бесконечная циклическая группа $Z = \langle \mathbb{Z}; + \rangle$ свободно порождается элементом 1 (или -1). Однако ту же группу можно породить двумя элементами, например $Z = \text{гр}(2, 3)$, причем ни один из этих порождающих не лишний. После удаления любого из них получается уже собственная подгруппа группы Z . Элементы 2 и 3 порождают группу целых чисел Z , но порождают ее *несвободно*.

Действительно, в мультипликативной записи бесконечная циклическая группа с такими порождающими элементами имеет копредставление

$$P = \langle a, b; a^3b^{-2}, aba^{-1}b^{-1} \rangle.$$

Здесь роль двойки играет элемент a . Элемент b исполняет роль тройки из аддитивной записи.

Вместо двойки и тройки можно взять любые два взаимно простых числа. Более того, для любого натурального $n > 1$ можно подобрать n натуральных в совокупности взаимно простых чисел так, что любые $n - 1$ из них не взаимно просты. Это означает, что для любого $n > 1$ свободная группа ранга 1 может порождаться системой из n элементов и ни один элемент из этой системы нельзя удалить.

Вопросы, связанные со свободными группами, компьютер, вообще говоря, решать не отказывается. Найдем для примера копредставление подгруппы

$$H = \text{гр}(b, aba^{-1}, a^2ba^{-2})$$

в свободной группе $G = \langle a, b \rangle$:

```
> with(group):
> G := relgroup({a, b}, {}):
> H := subgrel({x = [b], y = [a, b, 1/a],
  z = [a, a, b, 1/a, 1/a]}, G):
> H := pres(H);
```

$$H := \text{relgroup}(\{x, y, z\}, \{\}).$$

Результат вычислений означает, что подгруппа H сама свободна, а элементы aba^{-1} , b , a^2ba^{-2} — ее свободные порождающие. Отметим, что ранг подгруппы H равен трем, т. е. превышает ранг исходной группы. Более того, по образцу порождающих элементов для H можно построить в свободной группе второго ранга подгруппу, которая

свободна, и ранг этой подгруппы равен любому наперед заданному натуральному числу или даже бесконечен (счетный).

В начале XX в. было установлено, что любая подгруппа свободной группы сама свободна¹. Это значит, что произвольные порождающие подгруппы свободной группы можно всегда заменить новыми, свободными от определяющих соотношений.

Задача нахождения свободных порождающих конечно порожденной подгруппы свободной группы имеет алгоритмическое решение, но в пакете *Maple* этот алгоритм пока не реализован.

Чтобы найти порядок элемента g группы G , достаточно вычислить порядок подгруппы $\text{gr}(g)$, порожденной этим элементом. Этот порядок появится в качестве показателя степени в представлении группы.

Найдем порядки порождающих элементов в группе

$$G = \langle a, b; a^2bab^4 = 1, b^2aba^4 = 1 \rangle:$$

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
> A := subgrel({a = [a]}, G):
> pres(A);
```

```
grelgroup({a}, {[a, a, a, a, a, a, a, a, a, a, a, a, a, a, a]})
```

```
> B := subgrel({b = [b]}, G):
> pres(B);
```

```
grelgroup({b}, {[b, b, b, b, b, b, b, b, b, b, b, b, b, b, b]})
```

Итак, подгруппы, порожденные каждым из порождающих элементов в отдельности, имеют порядки 16.

Это означает, что порядок каждого из порождающих равен 16 и, соответственно, в группе G подгруппы, порожденные каждым из порождающих в отдельности, имеют копредставления:

$$\text{gr}(x) = \langle x; x^{16} = 1 \rangle,$$

$$\text{gr}(y) = \langle y; y^{16} = 1 \rangle.$$

Поинтересуемся порядком коммутатора порождающих, т. е. найдем порядок подгруппы

```
C = gr(aba-1b-1):
> C := subgrel({c = [a, b, 1/a, 1/b]}, G):
> pres(C);
```

```
grelgroup({c}, {[c, c, c]})
```

¹ Доказано немецким математиком *Отто Шрейером* (Schreier, 1901—1929) в 1927 г.

Порядок коммутатора оказался равен трем. Это означает, в частности, что коммутатор отличен от единицы и, следовательно, исследуемая группа неабелева.

Конечно порожденная группа абелева, если коммутаторы всех ее порождающих равны единице.

Таким образом, с помощью команд *subgrel*, *pres* и *grelgroup* в конечное число шагов можно выяснить, не является ли группа абелевой.

Точно так же, вычисляя значения более сложных коммутаторных выражений от элементов группы, можно выяснить, не является ли группа нильпотентной или разрешимой (и вообще выполняется или нет в ней данное тождество). Отметим, что для бесконечной группы такое исследование может оказаться невыполнимым.

Существуют конечно определенные группы с неразрешимой проблемой равенства, т. е. группы, для которых не существует алгоритма для узнавания, равно ли произвольное слово от порождающих группы единице этой группы или нет. Компьютер для исследования такой группы бессилен. Невозможно так же для произвольной конечно определенной группы по единому алгоритму узнать, абелева эта группа или нет, нильпотентна или нет, разрешима или нет и т. д.

К счастью, для конечных групп все эти задачи всегда разрешимы. Более того, достаточно воспользоваться теоремой Кэли и представить исследуемую группу в виде группы подстановок. Для групп подстановок простым перебором вариантов в конечное число шагов можно ответить на любой вопрос.

Для групп подстановок абелевость (и разрешимость) выясняются с помощью одной команды. Несложно устанавливается и нильпотентность или ненильпотентность конечной группы.

Если группа G задана копредставлением, а $H = \text{гр}(h_1, h_2, \dots, h_m)$ — ее подгруппа, введенная в компьютер командой

$$\text{subgrel}(\{h_1 = w(a_j), h_2 = w(a_j), \dots, h_m = w(a_j)\}, G),$$

то машинная команда

$$\text{cosets}(H)$$

выдает систему представителей правых смежных классов группы G по подгруппе H .

Рассмотрим сначала пример, результат которого нам известен заранее (и, таким образом, проверим работу техники). Пусть группа

$$G = \langle a, b: a^2bab^4 = 1, b^2aba^4 = 1 \rangle,$$

а ее подгруппа $H = \text{гр}(ab, b^2)$. Из предыдущего мы уже знаем, что группа H имеет копредставление

$$H = \langle x, y; x^2y^2x^{-1}y^2x^{-2}y, xy^2x^{-2}y^{-1}x^2y^2, (xy)^2yx^{-1}y^2x^{-2}y^{-1}x^2y^{-2}x^{-2}y^{-1} \rangle,$$

где $x = ab$, $y = b^2$. Кроме того, известны порядки G и H : $|G| = 144$, а $|H| = 72$. По теореме Лагранжа число смежных классов G по H равно $\frac{144}{72} = 2$. Выполним машинную проверку:

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
> H := subgrel({x=[a, b], y=[b, b]}, G):
> cosets(H);
```

$\{[], [a]\}$

Смежных классов действительно оказалось два, и правостороннее разложение группы G по H имеет вид

$$G = H + Ha.$$

Впрочем, как и любая подгруппа индекса два, подгруппа H нормальна в группе G , поэтому ее левостороннее разложение имеет таких же представителей:

$$G = H + aH.$$

Рассмотрим еще один пример такого рода. Пусть группа G та же самая, а $A = \text{gr}(a)$. Порядок H равен 16, поэтому число смежных классов в разложении группы G по подгруппе A равно $\frac{144}{16} = 9$.

Проверим, что индекс действительно равен девяти, и заодно найдем представителей этих классов:

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
> A := subgrel({x=[a]}, G):
> cosets(A);
```

$\{[], [b, b], [b], [b, a], [b, a, b], [b, a, b, b], [b, a, b, b, b],$
 $[b, a, a, b], [b, b, b, a, b, a]\}$

Итак, правостороннее разложение группы G по A получено:

$$G = A + Ab^2 + Ab + Aba + Abab + Abab^2 + Abab^3 + Aba^2b + Ab^3aba.$$

Как выяснить, нормальна подгруппа A в группе G или нет, обсудим позже, а пока отметим, что команда $elements(G)$ для группы, заданной порождающим множеством и определяющими соотношениями, не действует.

Однако можно обойтись и без этой команды, а просто разложить группу единичной подгруппе. Найдем для примера все элементы

диэдральной группы D_4 из восьми элементов (в пакете *Maple* букву D запрещается использовать для обозначения объектов, поэтому пусть в машинной обработке $D_4 = G$):

```
> with(group):
> G := grelgroup({a, b}, {[a, a], [b, b], [a, b, a, b, a,
  b, a, b]}):
> E := subgrel({x=[]}, G):
> cosets(E);
```

```
{[], [a, b, a, b], [a, b, a], [a, b, a, b, a], [a, b, a, b, a, b], [a, b], [a], [b]}
```

Элементы группы D_4 найдены; выпишем их в том же порядке, что указал компьютер:

$$D_4 = \{1, (ab)^2, aba, (ab)^2a, (ab)^3, ab, a, b\}.$$

Команда *cosrep* работает и для абстрактной группы, более того, возможности ее расширены.

Если для групп подстановок речь шла о разложении одной, а именно симметрической группы S_n по подгруппе H , то для групп, заданных копредставлением, эта команда применима к любой группе G и ее подгруппе H .

Если группа G задана командой *grelgroup*, а подгруппа H уже определена в группе G указанием *subgrel*, то команда *cosrep*(α , H , G) укажет копредставление α в виде $\alpha = hg$, где h — элемент из H , а g — представитель правого смежного класса по H .

Заметим, что такое представление для каждого элемента из G при фиксированной системе представителей правых смежных классов единственно. В частности, $\alpha = 1$ тогда и только тогда, когда $h = 1$ и $g = 1$.

Таким образом, если G и H зафиксированы, то, выполняя команду *cosrep*(α , H , G), компьютер решает проблему тождества в группе G . Это значит, что для группы G с неразрешимой проблемой тождества команда *cosrep* будет выдавать результат не для любого элемента α .

Чтобы узнать, абелева группа или нет, достаточно вычислить значения коммутаторов ее порождающих. Сделать это можно с помощью команды *cosrep*.

Однако в классе всех конечно определенных групп свойство абелевости алгоритмически нераспознаваемо¹. Поэтому заведомо не для каждой группы команда *cosrep* будет выдавать результат даже для конечного набора элементов конкретных элементов — коммутаторов порождающих.

¹ Свойство абелевости является марковским.

Рассмотрим сначала действие этой команды, когда результат легко предугадать. Пусть группа $G = \langle a \rangle$ бесконечная циклическая, порожденная элементом a , $H = \text{гр}(a^5)$ — ее подгруппа, порожденная элементом a^5 . Найдем представление элемента a^{23} . Заранее ясно, что

$$a^{24} = a^{5 \cdot 4 + 4} = (a^5)^4 \cdot a^4 = x^4 \cdot a^3.$$

Видим, что машина тоже не ошиблась:

```
> with(group):
> G := grelgroup({a}, {}):
> H := subgrel({x = [a$5]}, G):
> cosrep([a$24], H, G);
```

$$[[x, x, x, x], [a, a, a]]$$

Рассмотрим второй, более сложный пример. Пусть G — свободная группа ранга два, $G = \langle a, b \rangle$, а ее подгруппа $H = \text{гр}(aba^{-1}, b, a^2)$. Найдем представление элемента $ababa^{-1}b$:

```
> with(group):
> G := grelgroup({a, b}, {}):
> H := subgrel({x = [a, b, 1/a], y = [b], z = [a, a]}, G):
> cosrep([a, b, a, b, 1/a, b], H, G);
```

$$\left[\left[x, z, y, \frac{1}{z}, x \right], [a] \right].$$

Представление найдено. В обозначениях $x = aba^{-1}$, $y = b$, $z = a^2$ получено равенство

$$ababa^{-1}b = xzyx^{-1}xa.$$

Проконтролировать машинный результат несложно, для этого достаточно вместо x , y , z подставить их выражения и произвести вычисления. Проверим машину:

$$xzyx^{-1}xa = aba^{-1} \cdot a^2 \cdot b \cdot a^{-2} \cdot aba^{-1} \cdot a = ababa^{-1}b.$$

Как видим, ошибок нет и сейчас.

Рассмотрим теперь действие команды *cosrep* для конечной группы. Пусть

$$G = \langle a, b; a^2bab^4 = 1, b^2aba^4 = 1 \rangle,$$

ее подгруппа $A = \text{гр}(a)$ и элемент $b^{-5}ab^5$:

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
```

```
> A := subgrel({a = [a]}, G):
> cosrep([1/b$5, a, b$5], A, G);
```

$$\left[\left[\frac{1}{a} \right], [b, b] \right].$$

Итак, в группе G выполняется равенство

$$b^{-5}ab^5 = a^{-1} \cdot b^2.$$

Это равенство не противоречит предыдущим машинным вычислениям. Элемент b^2 действительно содержится в системе представителей правых смежных классов по подгруппе A (то, что a^{-1} принадлежит A , в проверке и не нуждается: A — подгруппа, поэтому она замкнута относительно взятия обратного элемента). Правда, равенство может оказаться ошибочным по другой причине: вдруг соотношение

$$b^{-5}ab^5 \cdot b^{-2}a = 1$$

в группе G не выполняется? Если это равенство не является следствием определяющих соотношений, то группа

$$G1 = \langle a, b; a^2bab^4 = 1, b^2aba^4 = 1, b^{-5}ab^5 \cdot b^{-2}a \rangle$$

не совпадает с группой G и содержит меньшее количество элементов. Проверим, так ли это:

```
> with(group):
> G1 := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4],
  [1/b$5, a, b$3, a]}):
> grouporder(G1);
```

144

Порядок группы $G1$ в точности равен порядку группы G , поэтому равенство

$$b^{-5}ab^5 = a^{-1} \cdot b^2$$

на самом деле выполняется в группе G .

Равенство $b^{-5}ab^5 = a^{-1} \cdot b^2$ означает, в частности, что сопряжение элемента из A не попало в подгруппу A (представителем которой является единичный элемент, а не b^2), поэтому группа A ненормальна в группе G .

Впрочем, в пакете *Maple* нормальность или ненормальность подгруппы можно выяснить и непосредственно.

Если группа G задана командой *grelgroup*, а в ней с помощью указания *subgrel* определена подгруппа H , то по машинной команде

$$isnormal(H)$$

можно выяснить, нормальна H в группе G или нет. Если H — нормальный делитель в G , то результатом действия команды будет слово *true*, если же нет, то слово *false*.

Для группы

$$G = \langle a, b; a^2bab^4 = 1, b^2aba^4 = 1 \rangle$$

мы уже из косвенных соображений определили, что подгруппа $H = \text{гр}(ab, b^2)$ нормальна в G , а подгруппа $A = \text{гр}(a)$ ненормальна. Проверим это машинными вычислениями:

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
> H := subgrel({x = [a, b], y = [b, b]}, G):
> isnormal(H);
```

true

```
> A := subgrel({a = [a]}, G):
> isnormal(A);
```

false

Если группа абелева, то все подгруппы в ней нормальны. Существуют и неабелевы группы, обладающие такими же свойствами.

Наименьшей по числу элементов такой группой является группа G , состоящая из восьми элементов тела кватернионов:

$$1, -1, i, -i, j, -j, k, -k.$$

Это множество замкнуто относительно умножения, поэтому образует группу, которая называется *группой кватернионов*.

Попробуем найти копредставление этой группы из восьми элементов. Сначала заметим, что

$$(-1)^2 = 1, i^2 = -1, j^2 = -1, k^2 = -1, ij = -ji = k.$$

Из этих равенств видно, что элементы i, j порождают эту группу. Из первых трех соотношений следует:

$$i^4 = 1, i^2 = j^2.$$

Из равенства $ij = -ji$ умножением справа на $i^{-1}j$ получается соотношение

$$iji^{-1}j = 1.$$

Покажем, что эти четыре соотношения являются определяющими для группы G . Для этого вычислим порядок группы с таким копредставлением:

```

> with(group):
> G := relgroup({i, j}, {[i$4], [i, i, 1/j, 1/j], [i, j, 1/i, j]});


$$G := \text{relgroup}\left(\{i, j\}, \left\{\left[i, j, \frac{1}{i}, j\right], [i, i, i, i], \left[i, i, \frac{1}{j}, \frac{1}{j}\right]\right\}\right)$$


> grouporder(G);

```

8

Итак, группа кватернионов имеет копредставление

$$G = \langle i, j; i^4, i^2 j^{-2}, i j i^{-1} j \rangle$$

Равенство $ij = -ji$ как будто означает, что группа G неабелева. Но вдруг в этой группе выполняется и равенство $-ji = ji$? Если такое равенство выполнится, то это будет означать, что группа G абелева.

Окончательным решением вопроса будет факт неединичности коммутатора порождающих элементов:

```

> with(group):
> G := relgroup({i, j}, {[i$4], [i, i, 1/j, 1/j], [i, j, 1/i, j]}):
> K := subrel({x = [i, j, 1/i, 1/j]}, G):
> pres(K);

```

$$\text{relgroup}(\{x\}, \{[x, x]\})$$

Порядок коммутатора оказался равным двум, т. е. он отличен от единицы: группа G неабелева.

Покажем, что, несмотря на неабелевость, все подгруппы нормальны в G .

Порядок G равен восьми, поэтому по теореме Лагранжа собственная подгруппа состоит из двух или четырех элементов. Если H содержит четыре элемента, то ее индекс равен двум и, следовательно, она нормальна в G . Таким образом, интерес представляют лишь двухэлементные подгруппы. Среди элементов $1, -1, i, -i, j, -j, k, -k$ лишь -1 имеет порядок два. В наших порождающих это элемент i^2 (он же j^2).

Итак, остается проверить на нормальность в G всего одну подгруппу $H = \text{gr}(i^2)$. Проверяем:

```

> with(group):
> G := relgroup({i, j}, {[i$4], [i, i, 1/j, 1/j], [i, j, 1/i, j]}):
> isnormal(subrel({x = [i, i]}, G));

```

true

Итак, единственная сомнительная подгруппа H тоже нормальна в G .

В этих двух примерах исходные группы были конечны. Рассмотрим ситуацию с бесконечной группой. В свободной группе $G = \langle a, b \rangle$ возьмем две подгруппы:

$$A = \text{гр}(b, aba^{-1}, a^2ba^{-2}),$$

$$B = \text{гр}(ab, b^2, a^2) —$$

и проверим их на нормальность:

```
> with(group):
> G := grelgroup({a, b}, {}):
> A := subgrel({x = [b], y = [a, b, 1/a],
  z = [a, a, b, 1/a, 1/a]}, G):
> isnormal(A);
```

false

```
> B := subgrel({x = [a, b], y = [b, b], z = [a, a]}, G):
> isnormal(B);
```

true

Итак, подгруппа B нормальна в G , а подгруппа A — нет.

Представление группы в виде порождающего множества с определяющими соотношениями является особенно удобным, когда требуется получить копредставление фактор-группы.

Пусть группа G задана своим копредставлением

$$G = \langle a_1, a_2, \dots, a_n; R_1(a_i), R_2(a_i), \dots, R_k(a_i) \rangle.$$

Предположим далее, что $h_1(a_i), h_2(a_i), \dots, h_s(a_i)$ — произвольное множество элементов из G , записанных в порождающих a_i , а N — нормальное замыкание этого множества в G .

Тогда фактор-группа G/B имеет копредставление

$$G/B = \langle a_1, a_2, \dots, a_n; R_1(a_i), R_2(a_i), \dots, R_k(a_i), \\ h_1(a_i), h_2(a_i), \dots, h_s(a_i) \rangle.$$

Рассмотрим конкретные примеры отыскания фактор-групп.

Только что было установлено, что подгруппа $B = \text{гр}(ab, b^2, a^2)$ нормальна в группе $G = \langle a, b \rangle$, и, следовательно, можно говорить о фактор-группе G/B . Выясним, чем является эта фактор-группа. Сначала найдем ее порядок:

```
> with(group):
> grouporder(grelgroup({a, b}, {[a, b], [b, b], [a, a]}));
```

Группа, порядок которой простое число, единственна. Эта группа циклическая. Таким образом, фактор-группа G/B — это циклическая порядка 2, и ее можно задать копредставлением

$$G/B = \langle x; x^2 \rangle.$$

Если же появится желание увидеть, какой именно смежный класс является порождающим элементом в фактор-группе (множестве смежных классов по B), то это желание легко выполнимо с помощью команды `cosets`:

```
> with(group):
> G := grelgroup({a, b}, {}):
> B := subgrel({x = [a, b], y = [b, b], z = [a, a]}, G):
> cosets(B);
```

$$\{[], [a]\}$$

Итак, $G/B = \{B, Ba\}$, и таблица умножения этой группы имеет вид

\cdot	B	Ba
B	B	Ba
Ba	Ba	B

Результат $Ba \cdot Ba = B$ получается следующим образом. По определению фактор-группы

$$Ba \cdot Ba = Ba^2.$$

Элемент a^2 принадлежит подгруппе B , следовательно, $Ba^2 = B$.

Два элемента x, y из одного смежного класса по подгруппе N называют *сравнимыми по модулю N* . Пишут:

$$x \equiv y \pmod{N}.$$

В предыдущем вычислении a^2 равен единице по mod N :

$$a^2 \equiv 1 \pmod{N}.$$

Рассмотрим пример с конечной группой.

Мы уже узнали, что в группе кватернионов

$$G = \langle i, j; i^4, i^2 j^{-2}, i j i^{-1} j \rangle$$

подгруппа $N = \langle i^2 \rangle$ нормальна в G . Найдем фактор-группу $G_1 = G/N$. Копредставление этой фактор-группы

$$G_1 = \langle i, j; i^4, i^2 j^{-2} i j i^{-1} j, i^2 \rangle,$$

и эта фактор-группа состоит из четырех элементов. Проверим на всякий случай:

```
> with(group):
> G[1] := grelgroup({i, j}, {[i$4], [i, i, 1/j, 1/j],
  [i, j, 1/i, j], [i, i]}):
> grouporder(G[1]);
```

4

Теперь остается выяснить, что эта за группа. Заметим, что в нашем случае это несложно проделать ручными вычислениями: равенство $i^4 = 1$ является следствием равенства $i^2 = 1$, поэтому его из списка соотношений можно удалить. Из равенств $i^2 j^{-2}$ и $i^2 = 1$ следует, что $j^2 = 1$, и т. д.

Так легко будет не всегда, поэтому рассмотрим машинное решение вопроса.

Найдем сначала представителей правых смежных классов по подгруппе N в G :

```
> with(group):
> G := grelgroup({i, j}, {[i$4], [i, i, 1/j, 1/j],
  [i, j, 1/i, j]}):
> N := subgrel({y = [i, i]}, G):
> cosets(N);
```

$$\left\{ [], [i], [i, j], \left[i, j, \frac{1}{i} \right] \right\}.$$

Представители правых смежных классов найдены — это элементы $1, i, ij, ij i^{-1}$. Найдем теперь порядки неединичных элементов. Порядок нужно искать по модулю подгруппы N , т. е. надо найти наименьшую степень элемента, которая равна единице по модулю N , т. е. принадлежит N . Это значит, что представитель смежного класса, содержащий этот элемент, должен быть равным единице.

Вычисляем степени представителей правых смежных классов по подгруппе N . Элемент i^2 принадлежит подгруппе N , так что его порядок в фактор-группе G/N равен двум.

Посмотрим, не равен ли единице по модулю подгруппы N элемент $(ij)^2$. Для этого воспользуемся командой *cosrep*:

```
> with(group):
> G := grelgroup({i, j}, {[i$4], [i, i, 1/j, 1/j],
  [i, j, 1/i, j]}):
> N := subgrel({y = [i, i]}, G):
> cosrep([i, j, i, j], N, g);
```

$$[[y, y, y], []]$$

Представитель $(ij)^2$ оказался равным единице, а это значит, что

$$(ij)^2 \equiv 1(\text{mod } N).$$

Итак, элемент ij тоже имеет порядок два в фактор-группе G/N .

Становится ясно, что G/N нециклическая: в циклической группе для каждого делителя k порядка группы существует в точности одна подгруппа порядка k . Другими словами, нам заранее известно, что порядок элемента iji^{-1} не может быть равным четырем, а это значит, что этот порядок равен двум. Однако проверим:

```
> with(group):
> G := grelgroup({i, j}, {[i $4], [i, i, 1/j, 1/j],
  [i, j, 1/i, j]}):
> N := subgrel({y = [i, i]}, G):
> cosrep([i, j, 1/i, i, j, 1/i], N, G);
```

[[y], []]

Представитель элемента $(iji^{-1})^2$ действительно оказался равен единице: порядок этого элемента по mod N равен двум,

$$(iji^{-1})^2 \equiv 1(\text{mod } N).$$

Ранее было замечено, что группа, в которой выполняется тождество $x^2 = 1$, абелева. Таким образом, сейчас мы уже точно знаем, что фактор-группа G/N — это четверная группа Клейна V_4 и ее копредставление имеет вид

$$\langle a, b, a^2 = 1, b^2 = 1, ab = ba \rangle,$$

где $a = Ni$, $b = Nij$.

Если бы эрудиция нас подвела и мы не узнали клейновскую группу, то мы продолжали бы вычисления далее, т. е. выясняли, не абелева ли группа G/N :

```
> with(group):
> G := grelgroup({i, j}, {[i $4], [i, i, 1/j, 1/j],
  [i, j, 1/i, j]}):
> N := subgrel({y = [i, i]}, G):
> cosrep([i, i, j, 1/i, 1/j, 1/i], N, G);
```

$$\left[\begin{bmatrix} 1 \\ y \end{bmatrix}, [] \right].$$

Да, эта группа абелева, так как представитель коммутатора по модулю N равен единице:

$$i \cdot ij \cdot i^{-1} \cdot (ij)^{-1} \equiv 1(\text{mod } N).$$

Вычисления (с «двойным запасом прочности¹») закончены: фактор-группа G/N — это четверная группа Клейна.

В качестве второго примера рассмотрим бесконечную исходную группу G .

В бесконечной группе

$$G = \langle a, b; a^2 = 1, b^2 = 1 \rangle$$

возьмем нормальное замыкание N элемента (ab) , т. е. $N = \langle (ab)^3 \rangle^G$.

Тогда фактор-группа $G_1 = G/N$ имеет копредставление

$$G_1 = \langle a, b; a^2, b^2, (ab)^3 \rangle.$$

Поинтересуемся порядком полученной группы:

```
> with(group):
> G[1] := relgroup({a, b}, {[a, a], [b, b], [a, b, a, b, a, b]}):
> grouporder(G[1]);
```

6

Группа G_1 состоит из шести элементов, а таких групп всего две — циклическая шестого порядка и симметрическая группа третьей степени S_3 . Какая именно группа сейчас перед нами?

Сначала выясним, как устроен нормальный делитель N и как сильно он отличается от подгруппы H , порожденной элементом $(xy)^3$. Для этого найдем индекс H в G :

```
> with(group):
> G := relgroup({a, b}, {[a, a], [b, b]}):
> cosets(subgroup({y = [a, b, a, b, a, b]}, G));
```

$\{[], [a], [a, b], [a, b, a], [a, b, a, b], [a, b, a, b, a]\}$

Оказалось, что $|G:H| = |G:N|$. Поскольку $H \subset N$, отсюда следует $H = N$, т. е. подгруппа, порожденная множеством, совпадает с нормальным замыканием этого множества. Другими словами, подгруппа H уже нормальна в G .

Начнем искать порядки элементов $a, ab, aba, abab, ababa$ по модулю $H = \text{gr}((ab)^3)$. Если среди них окажется элемент шестого порядка, то группа G/N циклическая. Поэтому вполне возможно, что исследование группы G/N закончится раньше, чем мы найдем порядки всех этих элементов. Впрочем, оно закончится раньше, даже если эта группа нециклическая.

Итак, начинаем.

¹ «Запас прочности» здесь даже тройной: нециклическая группа порядка p^2 , где p простое, является прямым произведением двух циклических групп порядка p .

Элемент a имеет порядок два в исходной группе G , поэтому

$$a^2 = 1 \equiv 1(\text{mod } H).$$

Элемент $(ab)^3$ принадлежит подгруппе H , следовательно,

$$(ab)^3 \equiv 1(\text{mod } H).$$

Порядок элемента ab в фактор-группе равен трем.

Посмотрим теперь, каков порядок aba . Может быть, он равен двум?

Проверяем:

```
> with(group):  
> G := grelgroup({a, b}, {[a, a], [b, b]}):  
> H := subgrel({x = [a, b, a, b, a, b]}, G):  
> cosrep([a, b, a, a, b, a], H, G);
```

[[], []]

Да, квадрат этого элемента сравним с единицей по mod N ,

$$(aba)^2 \equiv 1(\text{mod } H),$$

т. е. порядок элемента aba в фактор-группе G/N действительно равен двум.

Теперь мы точно знаем, как устроена группа G/N .

В циклической группе для каждого натурального делителя m порядка всей группы найдется в точности один элемент порядка m . Наличие сразу двух различных элементов второго порядка в группе G/N означает, что группа эта нециклическая и, следовательно, группа G/N изоморфна группе S_3 .

8.6. Копредставления и группы подстановок

По теореме Кэли каждую конечную группу порядка n можно изоморфно представить группой подстановок степени n . Степень подстановок в некоторых случаях можно значительно понизить.

Если H — неединичная подгруппа группы G , не содержащая нетривиального нормального делителя группы G , то группу G можно изоморфно представить правыми сдвигами правых смежных классов по подгруппе H . Степень этих подстановок равна индексу $|G:H|$.

Если же в подгруппе H найдется неединичный нормальный делитель N группы G , то это представление будет лишь гомоморфным. Таким образом, авторский вариант теоремы Кэли — это всего лишь частный случай общей ситуации, когда подгруппа $H = E$.

Таким образом, для использования теоремы Кэли или ее обобщения нужно сначала задать подгруппу H группы G . Задается H , как и раньше, командой *subgrel*. Если h_1, h_2, \dots, h_k — порождающие элементы для H , то по команде

$$\text{permrep}(H)$$

компьютер выдает представление этих порождающих в виде подстановок степени, равной индексу $|G : H|$. Подгруппа, порожденная этими подстановками, является гомоморфным образом группы G , а если в H нет неединичного нормального делителя всей группы, то этот гомоморфизм становится изоморфизмом.

Найдем для примера копредставление группы

$$G = \langle a, b : a^2bab^4 = 1, b^2aba^4 = 1 \rangle$$

подстановками правых смежных классов по некоторой подгруппе H .

Группа G содержит 144 элемента. Если буквально следовать теореме Кэли, то нужно взять единичную подгруппу и получить множество сдвигов этой единичной подгруппы в группе G . В результате получится копредставление группы G группой подстановок на 144 символах:

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
> E := subgrel({y=[]}, G):
> permrep(E);
```

$$\text{permgroup}(144, \{a = [[1, 2, 3, 16, 25, 108, 131, 42,$$

$$43, 93, 94, 95, 12, 13, 14, 15],$$

$$[4, 5, 33, 41, 20, 116, 121, 97, 135, 76, 77, 105, 37, 38, 39, 40],$$

$$[6, 48, 49, 139, 30, 87, 138, 124, 125, 109, 110, 102, 52, 53, 54, 55],$$

$$[7, 47, 56, 86, 115, 140, 31, 32, 126, 127, 128, 129, 22, 58, 59, 60],$$

$$[8, 51, 61, 113, 114, 17, 18, 91, 92, 29, 136, 137, 64, 65, 66, 67],$$

$$[9, 63, 68, 144, 104, 83, 84, 50, 44, 130, 23, 24, 71, 72, 73, 74],$$

$$[10, 11, 75, 82, 34, 28, 96, 57, 45, 134, 101, 143, 78, 79, 80, 81],$$

$$[19, 90, 85, 141, 112, 98, 142, 35, 36, 132, 133, 106, 107, 118, 119, 120],$$

$$[21, 117, 122, 69, 70, 26, 27, 99, 100, 111, 62, 46, 103, 88, 89, 123]],$$

$$b = [[1, 9, 10, 69, 76, 125, 126, 92, 43, 44, 45, 46, 5, 6, 7, 8],$$

[2, 22, 23, 124, 66, 36, 37, 100, 93, 115, 68, 55, 18, 19, 20, 21],
 [3, 4, 31, 35, 89, 79, 51, 52, 94, 135, 59, 120, 27, 28, 29, 30],
 [11, 12, 88, 91, 73, 133, 129, 53, 134, 25, 26, 67, 84, 85, 86, 87],
 [13, 48, 99, 128, 81, 40, 118, 144, 108, 109, 123, 56, 57, 97, 98, 24],
 [14, 90, 102, 39, 130, 114, 75, 60, 131, 132, 139, 121, 63, 64, 101, 32],
 [15, 96, 106, 113, 140, 70, 71, 41, 42, 80, 141, 137, 58, 103, 104, 105],
 [16, 17, 77, 78, 49, 50, 117, 107, 95, 65, 33, 34, 110, 74, 111, 112],
 [38, 136, 122, 54, 142, 82, 83, 127, 116, 61, 62, 138, 119, 143, 72, 47]]))

Работать, конечно, можно и с таким копредставлением — машину не смутит большим числом символов. Однако попытаемся найти другое представление той же группы, более приемлемое для человека-вычислителя.

Возьмем в G подгруппу H , порожденную элементом a , и найдем копредставление группы G сдвигами правых смежных классов по H :

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
> H := subgrel({a = [a]}, G):
> permrep(H);
```

```
permgrou(9, {a = [[2, 3, 7, 6, 5, 9, 8, 4]], b = [[1, 2, 7, 8, 3, 4, 5, 6]]})
```

Получено представление группы подстановками всего на девяти символах. Конечно, такое представление больше подходит для ручной работы.

Возникает вопрос: является ли это представление точным?

К сожалению, нет, это представление неточно, и нам это известно уже до машинной проверки. Порядки порождающих элементов a, b этой группы мы нашли раньше — они оба равны 16.

Порядки подстановок $(2\ 3\ 7\ 6\ 5\ 9\ 8\ 4)$ и $(1\ 2\ 7\ 8\ 3\ 4\ 5\ 6)$ равны восьми; отображение, указанное компьютером, не взаимно однозначно — это не изоморфизм, а всего лишь гомоморфизм. Впрочем, в этом печальном факте можно убедиться и непосредственно:

```
> with(group):
> S := permgrou(9, {[[2, 3, 7, 6, 5, 9, 8, 4]],
  [[1, 2, 7, 8, 3, 4, 5, 6]]}):
> grouporder(S);
```

Представление неточно: в подгруппе $H = \text{gr}(a)$ содержится неединичный нормальный делитель N всей группы G . Индекс N в G равен 72, и, следовательно, порядок N равен двум. Группа $H = \text{gr}(a)$ циклическая порядка 16, поэтому $N = \text{gr}(a^8)$.

Проверим, на всякий случай, так ли это, т. е. выясним, действительно ли $\text{gr}(a^8)$ нормальна в группе G :

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
> N := subgrel({x = [a$8]}, G):
> isnormal(N);
```

true

То, что представление неточно, можно было сказать сразу, как только мы увидели степень подстановок — число 9. На девяти символах невозможно построить подстановку порядка 16. Для такой подстановки нужно как минимум 16 символов. Кроме того, степень представляющей подстановки должна делить порядок исходной группы — в нашем случае это число 144. Таким образом, можно надеяться лишь на понижение степени лишь до чисел 16 или 48.

Прделаем еще один эксперимент на понижение степени представляющих подстановок. Возьмем в G подгруппу $H1 = \text{gr}(aba^{-1}b^{-1})$, порожденную коммутатором порождающих элементов:

```
> with(group):
> G := grelgroup({a, b}, {[a, a, b, a, b$4], [b, b, a, b, a$4]}):
> H1 := subgrel({x=[a, b, 1/a, 1/b]}, G):
> permrep(H1);
```

```
permgrou(48, {a = [[1, 2, 5, 16, 32, 24, 19, 38, 39, 40, 41, 6, 7, 13, 14, 15],
[3, 23, 17, 18, 9, 44, 35, 42, 48, 21, 22, 31, 27, 10, 28, 4],
[8, 37, 34, 20, 36, 43, 30, 25, 26, 33, 46, 47, 45, 11, 12, 29]],
b = [[1, 4, 11, 30, 32, 26, 27, 44, 39, 42, 43, 12, 7, 8, 9, 10],
[2, 3, 21, 25, 31, 14, 38, 47, 40, 48, 23, 29, 18, 19, 15, 20],
[5, 6, 22, 13, 37, 46, 28, 45, 41, 16, 17, 24, 33, 34, 35, 36]]})
> grouporder(permrep(H1));
```

144

Представление группой подстановок на 48 символах оказалось точным: порядки представления подстановками и порядок самой группы совпадают. Тайна такой точности проста — в подгруп-

пе H нет нормального делителя группы G , кроме единичного (H содержит всего три элемента, в ней нет собственных подгрупп, а сама она ненормальна).

Полученное представление группы G (любое — на 144 или на 48 перемещаемых символах) дает возможность полного исследования этой группы. Например, машинными командами для групп подстановок проверяется, что группа G разрешима (точнее, метабелева), но не нильпотентна, коммутант ее состоит из девяти элементов, а центр — из двух элементов:

```
> with(group):
> G := permgroup(48, {[[1, 2, 5, 16, 32, 24, 19, 38, 39, 40,
    41, 6, 7, 13, 14, 15],
    [3, 23, 17, 18, 9, 44, 35, 42, 48, 21, 22, 31, 27, 10, 28, 4],
    [8, 37, 34, 20, 36, 43, 30, 25, 26, 33, 46, 47, 45, 11, 12, 29]],
    [[1, 4, 11, 30, 32, 26, 27, 44, 39, 42, 43, 12, 7, 8, 9, 10],
    [2, 3, 21, 25, 31, 14, 38, 47, 40, 48, 23, 29, 18, 19, 15, 20],
    [5, 6, 22, 13, 37, 46, 28, 45, 41, 16, 17, 24, 33, 34, 35, 36]]}):

> DerivedS(G);

[permgroup(48, {[[1, 2, 5, 16, 32, 24, 19, 38, 39, 40, 41, 6, 7, 13, 14, 15],
    [3, 23, 17, 18, 9, 44, 35, 42, 48, 21, 22, 31, 27, 10, 28, 4],
    [8, 37, 34, 20, 36, 43, 30, 25, 26, 33, 46, 47, 45, 11, 12, 29]],
    [[1, 4, 11, 30, 32, 26, 27, 44, 39, 42, 43, 12, 7, 8, 9, 10],
    [2, 3, 21, 25, 31, 14, 38, 47, 40, 48, 23, 29, 18, 19, 15, 20],
    [5, 6, 22, 13, 37, 46, 28, 45, 41, 16, 17, 24, 33, 34, 35, 36]]}),
    permgroup(48, {[[1, 35, 47], [2, 42, 45], [4, 36, 40], [6, 23, 30],
    [7, 25, 17], [8, 31, 24], [10, 38, 34], [12, 16, 21], [13, 26, 18],
    [15, 46, 44], [20, 39, 28], [22, 32, 29]], [[1, 35, 47], [3, 43, 41],
    [5, 48, 11], [6, 30, 23], [7, 25, 17], [9, 14, 33], [10, 34, 38], [12, 21, 16],
    [15, 44, 46], [19, 37, 27], [20, 39, 28], [22, 32, 29]]}),
    permgroup(48, {[]})]

> LCS(G);

[permgroup(48, {[[1, 2, 5, 16, 32, 24, 19, 38, 39, 40, 41, 6, 7, 13, 14, 15],
    [3, 23, 17, 18, 9, 44, 35, 42, 48, 21, 22, 31, 27, 10, 28, 4],
```



```

[8, 37, 34, 20, 36, 43, 30, 25, 26, 33, 46, 47, 45, 11, 12, 29]],
[[1, 4, 11, 30, 32, 26, 27, 44, 39, 42, 43, 12, 7, 8, 9, 10],
[2, 3, 21, 25, 31, 14, 38, 47, 40, 48, 23, 29, 18, 19, 15, 20],
[5, 6, 22, 13, 37, 46, 28, 45, 41, 16, 17, 24, 33, 34, 35, 36]]}),
permgroup(48, {[[]], [[1, 35, 47], [2, 45, 42], [3, 41, 43], [4, 40, 36],
[5, 11, 48], [7, 25, 17], [8, 24, 31], [9, 33, 14], [13, 18, 26],
[19, 27, 37], [20, 39, 28], [22, 32, 29]], [[1, 47, 35], [2, 45, 42],
[4, 40, 36], [6, 30, 23], [7, 17, 25], [8, 24, 31], [10, 34, 38],
[12, 21, 16], [13, 18, 26], [15, 44, 46], [20, 28, 39], [22, 29, 32]]}])
> grouporder(center(G));

2

> grouporder(derived(G));

```

9

Взаимная простота порядков центра и коммутанта означает, в частности, что их пересечение тривиально, а подгруппа порядка 18, ими порожденная, является их прямым произведением.

Важнее, однако, другое. Поскольку $144 = 9 \cdot 16$, а числа 16 и 9 взаимно просты, получаем, что вся группа G разложима в полупрямое произведение своего коммутанта K (он же — силовская 3-подгруппа) и силовской 2-подгруппы P :

$$G = K \rtimes P.$$

Можно заранее сказать, что это полупрямое произведение не является прямым. Если бы оно было прямым, то группа G была бы нильпотентной, но нижний центральный ряд (LCS) этой группы единичной подгруппы не достиг.

Только по виду подстановок, порождающих коммутант, можно заметить, что коммутант является прямым произведением двух циклических групп порядков 3.

Выясним, как устроена группа P :

```

> with(group):
> G := permgroup(48, {[[1, 2, 5, 16, 32, 24, 19, 38, 39, 40,
41, 6, 7, 13, 14, 15],
[3, 23, 17, 18, 9, 44, 35, 42, 48, 21, 22, 31, 27, 10, 28, 4],

```

```
[8, 37, 34, 20, 36, 43, 30, 25, 26, 33, 46, 47, 45, 11, 12, 29]],
[[1, 4, 11, 30, 32, 26, 27, 44, 39, 42, 43, 12, 7, 8, 9, 10],
[2, 3, 21, 25, 31, 14, 38, 47, 40, 48, 23, 29, 18, 19, 15, 20],
[5, 6, 22, 13, 37, 46, 28, 45, 41, 16, 17, 24, 33, 34, 35, 36]]):
> P := Sylow(G, 2);
```

```
P := permgroup(48, {[[1, 6, 27, 2, 25, 34, 48, 26, 39,
16, 9, 40, 29, 46, 3, 8],
[4, 32, 15, 43, 24, 35, 23, 37, 42, 7, 38, 11, 13, 28, 21, 33],
[5, 18, 20, 12, 14, 36, 22, 44, 41, 31, 47, 30, 19, 45, 17, 10]]})
```

Итак, силовская 2-подгруппа группы G содержит элемент порядка 16 и сама состоит из 16 элементов. Это значит, что эта группа циклическая.

Соберем все эти копредставления вместе. Коммутант K группы G можно задать копредставлением

$$K = \langle x, y; x^3 = 1, y^3 = 1, xy = yx \rangle,$$

а группу P — копредставлением

$$P = \langle z; z^6 = 1 \rangle.$$

Элементы x, y, z можно интерпретировать подстановками:

```
x = [[1, 35, 47], [2, 42, 45], [4, 36, 40], [6, 23, 30], [7, 25, 17], [8, 31, 24],
[10, 38, 34], [12, 16, 21], [13, 26, 18],
[15, 46, 44], [20, 39, 28], [22, 32, 29]],
y = [[1, 35, 47], [3, 43, 41], [5, 48, 11], [6, 30, 23], [7, 25, 17], [9, 14, 33],
[10, 34, 38], [12, 21, 16], [15, 44, 46], [19, 37, 27],
[20, 39, 28], [22, 32, 29]],
z = [[1, 6, 27, 2, 25, 34, 48, 26, 39, 16, 9, 40, 29, 46, 3, 8],
[4, 32, 15, 43, 24, 35, 23, 37, 42, 7, 38, 11, 13, 28, 21, 33],
[5, 18, 20, 12, 14, 36, 22, 44, 41, 31, 47, 30, 19, 45, 17, 10]].
```

Элементы x, y, z — это новые порождающие группы G , представленной подстановками. В этих порождающих внутреннее строение группы G более прозрачно.

Правда, полупрямое произведение неоднозначно задается своими множителями: надо еще знать, как именно действует группа P сопряжениями на K . Для этого достаточно увидеть, какими элементами из K являются сопряжения порождающих x, y .

Попробуем это выяснить, используя команду *convert*:

```
> with(group):
> G := permgroup(48, {x = [[1, 35, 47], [2, 42, 45],
[4, 36, 40], [6, 23, 30],
[7, 25, 17], [8, 31, 24], [10, 38, 34], [12, 16, 21],
[13, 26, 18], [15, 46, 44], [20, 39, 28], [22, 32, 29]],
y = [[1, 35, 47], [3, 43, 41], [5, 48, 11], [6, 30, 23],
[7, 25, 17], [9, 14, 33], [10, 34, 38], [12, 21, 16], [15, 44, 46],
[19, 37, 27], [20, 39, 28], [22, 32, 29]],
z = [[1, 6, 27, 2, 25, 34, 48, 26, 39, 16, 9, 40, 29, 46, 3, 8],
[4, 32, 15, 43, 24, 35, 23, 37, 42, 7, 38, 11, 13, 28, 21, 33],
[5, 18, 20, 12, 14, 36, 22, 44, 41, 31, 47, 30, 19, 45, 17, 10]]}):
> convert([z, x, 1/z, y, x], 'disjycyc', G);
```

[]

```
> convert([z, y, 1/z, x], 'disjycyc', G);
```

[]

Получено, что $zxz^{-1}yx = 1$ и $zyz^{-1}x = 1$, что равносильно

$$zxz^{-1} = x^{-1}y^{-1} \text{ и } zyz^{-1} = x^{-1}.$$

Прозрачные, т. е. ясно указывающее на внутреннее строение группы G , соотношения получены:

$$K = \langle x, y, z; x^3 = 1, y^3 = 1, xy = yx, z^6 = 1, zxz^{-1} = x^{-1}y^{-1}, zyz^{-1} = x^{-1} \rangle.$$

Рассмотрим еще один пример представления группы подстановками. Пусть G — группа кватернионов:

$$G = \langle i, j; i^4, i^2j^{-2}, iji^{-1}j \rangle.$$

Группа G состоит из восьми элементов, но каждая подгруппа этой группы нормальна. Поэтому группу G можно изоморфно представить только подстановками не ниже восьмой степени.

Таким образом, придется взять единичную подгруппу E в G и разыскать копредставление группы сдвигами смежных классов по E :

```
> with(group):
> G := grelgroup({i, j}, {[i, i, i, i], [i, i, 1/j, 1/j],
[i, j, 1/i, j]}):
> E := subgrel({e = []}, G):
> permrep(E);
```

```
permgroup(8, {j = [[1, 5, 3, 7], [2, 6, 4, 8]], i = [[1, 2, 3, 4], [5, 8, 7, 6]]})
```

Теперь, имея копредставление группы G в виде группы подстановок, мы можем найти ее коммутант, центр и вообще ответить на любой вопрос относительно этой интересной группы. Вообще-то нам заранее известно, что группа, порядок которой — степень простого числа, является нильпотентной и, следовательно, разрешимой. Это значит, в частности, что и центр такой группы неединичен. Неединичен и коммутант, если эта группа неабелева.

Группа кватернионов неабелева, поэтому центр ее отличен от всей группы, а коммутант неединичен. Проверяем:

```
> with(group):
> G := permgroup(8, {[[1, 5, 3, 7], [2, 6, 4, 8]],
  [[1, 2, 3, 4], [5, 8, 7, 6]]});
> derived(G);

permgroup(8, {[], [[1, 3], [2, 4], [5, 7], [6, 8]]})

> center(G);

permgroup(8, {[], [[1, 3], [2, 4], [5, 7], [6, 8]]})
```

Оказалось, что центр группы кватернионов совпадает с ее коммутантом. Коммутант (он же центр) — циклическая группа второго порядка, поэтому коммутант коммутанта равен единице. Группа кватернионов метабелева.

Группа второго порядка в группе кватернионов единственная — $\text{gr}(i^2)$. Так что если нас интересует фактор-группа $G / Z(G)$ по центру, ее представление нам известно заранее:

$$G / Z(G) = \langle i, j; i^4, i^2 j^{-2}, i j i^{-1} j, i^2 \rangle.$$

Ранее уже было установлено, что это представление четверной группы Клейна V_4 . Знание того, что факторизация происходит по центру группы, сейчас значительно ускоряет дело. Фактор-группа неабелевой группы по ее центру не может быть циклической.

Фактор-группа $G / Z(G)$ состоит из четырех элементов и нециклическая, следовательно, это прямое произведение двух циклических групп порядка два, т. е. четверная группа Клейна V_4 .

Заметим, что в группе G не содержится подгруппы, изоморфной четверной группе Клейна. Там всего лишь один элемент второго порядка (-1) , а в группе Клейна таковых три. Наконец, вспомним, что фактор-группа группы G по ее центру изоморфна группе $\text{Inn}(G)$ внутренних автоморфизмов группы G . Таким образом, попутно найдена и группа внутренних автоморфизмов группы кватернионов: она изоморфна четверной группе Клейна.

Каждая конечно порожденная неединичная и нециклическая абелева группа разложима в прямое произведение циклических групп. Если группа к тому же конечна, то эти циклические сомножи-

тели можно выбрать так, что их порядками будут степени простых чисел (такая группа уже не разложима в прямое произведение). Набор этих порядков называют *инвариантами* абелевой группы. Инварианты зависят только от самой группы и не зависят от способа нахождения разложения.

Как найти эти инварианты?

Конечная абелева группа является прямым произведением своих силовских p -подгрупп, так что нахождение инвариантов сводится к нахождению разложения на прямые множители p -групп. Если p -группа представлена подстановками, то такое разложение несложно найти вручную; подстановка имеет порядок p^k тогда и только тогда, когда в ее разложении есть цикл длины p^k .

Таким образом, для нахождения разложения абелевой группы в прямое произведение неразложимых циклических групп достаточно представить эту группу подстановками и найти ее силовские p -подгруппы для каждого простого p — делителя порядка группы. Заранее видна чисто техническая трудность: в абелевой группе все подгруппы нормальны, поэтому в изоморфном представлении подстановки будут иметь степень, равную порядку группы, и уменьшить эту степень нельзя.

Рассмотрим конкретный пример разыскания инвариантов конечной абелевой группы. Пусть группа G задана копредставлением

$$G = \langle a, b, c; a^5 b^5 c^2, a^{11} b^8 c^5, a^{17} b^5 c^8, aba^{-1}b^{-1}, aca^{-1}c^{-1}, bcb^{-1}b^{-1} \rangle.$$

Наличие в копредставлении группы всех коммутаторов порождающих элементов говорит о том, что группа G абелева; а то, что она конечна, еще нужно проверить:

```
> with(group):
> G := grelgroup({a, b, c}, {[a$5, b$5, c$2],
[a$11, b$8, c$5], [a$17, b$5, c$8],
[a, b, 1/a, 1/b], [a, c, 1/a, 1/c], [b, c, 1/b, 1/c]}):
> grouporder(G);
```

18

Проверили: группа G содержит 18 элементов. Теперь представим группу подстановками правых смежных классов по подгруппе H . В качестве H , как уже было сказано, сейчас можно взять лишь единичную подгруппу:

```
> with(group):
> G := grelgroup({a, b, c}, {[a$5, b$5, c$2],
[a$11, b$8, c$5], [a$17, b$5, c$8],
[a, b, 1/a, 1/b], [a, c, 1/a, 1/c], [b, c, 1/b, 1/c]}):
> E := subgreL({y = []}, G):
> G1 := permrep(E);
```



```

G1 := permgroup(18, {a = [[1, 2, 7, 8, 9, 10], [3, 12, 16, 14, 11, 4],
                        [5, 15, 13, 17, 18, 6]],
b = [[1, 4, 5, 8, 16, 17], [2, 3, 15, 9, 14, 18],
      [6, 7, 12, 13, 10, 11]],
c = [[1, 6, 3, 8, 13, 14], [2, 5, 12, 9, 17, 11],
      [4, 7, 15, 16, 10, 18]]})

```

Представление найдено. Заметим, что мы только сейчас узнали точные значения порядков исходных порождающих a , b , c : они все равны шести.

Теперь роль данной группы G играет ее изоморфная копия — группа $G1$.

Поскольку $18 = 2 \cdot 3^2$, группа $G1$ содержит единственную силовскую 2-подгруппу (обозначим ее буквой A) и единственную силовскую 3-подгруппу; пусть этот будет подгруппа B . Группа $G1$ является прямым произведением подгрупп A и B :

$$G1 = A \times B.$$

Группа A содержит всего два элемента, поэтому можно сразу сказать, что A циклическая; один из неразложимых множителей (и, соответственно, один инвариант группы G) найден.

Переходим к исследованию группы B :

```

> with(group):
> G1 := permgroup(18, {[[1, 2, 7, 8, 9, 10],
[3, 12, 16, 14, 11, 4], [5, 15, 13, 17, 18, 6]],
[[1, 4, 5, 8, 16, 17], [2, 3, 15, 9, 14, 18],
[6, 7, 12, 13, 10, 11]],
[[1, 6, 3, 8, 13, 14], [2, 5, 12, 9, 17, 11],
[4, 7, 15, 16, 10, 18]]}):
> B := Sylow(G1, 3);

B := permgroup(18, {[[1, 7, 9], [2, 8, 10], [3, 16, 11], [4, 12, 14],
[5, 13, 18], [6, 15, 17]], [[1, 16, 5], [2, 14, 15],
[3, 18, 9], [4, 17, 8], [6, 10, 12], [7, 11, 13]]})

```

Оказалось, что в группе B порядки порождающих элементов равны трем; поэтому и все неединичные элементы этой группы тоже третьего порядка. Здесь нет элемента девятого порядка, эта группа нециклическая. Таким образом, группа B — это прямое произведение двух циклических групп третьего порядка.

Инварианты группы G_1 (она же группа G) найдены — это $(2, 3, 3)$; группа G является прямым произведением циклической группы порядка два и двух циклических групп порядка три. Получено новое, *улучшенное копредставление* группы G :

$$G = \langle x; x^2 \times \langle y; y^3 \times \langle z; z^3 \rangle = \\ = \langle x, y, z; x^2 = 1, y^3 = 1, z^3 = 1, xy = yx, xz = zx, zy = yz \rangle.$$

В конкретной ситуации сама данная группа может случайно оказаться неразложимой циклической или даже единичной. Естественно, что в таком случае представление группы подстановками становится излишним.

Рассмотрим примеры такого рода.

Пусть абелева группа G_1 имеет копредставление

$$G_1 = \langle a, b, c; a^5 b^5 c^3, a^5 b^6 c^5, a^8 b^7 c^9, aba^{-1}b^{-1}, aca^{-1}c^{-1}, bcb^{-1}b^{-1} \rangle.$$

Найдем ее разложение в произведение циклических групп. Проверим сначала, конечна ли она:

```
> with(group):
> G[1] := grelgroup({a, b, c}, {[a$5, b$5, c$3],
[a$5, b$6, c$5], [a$8, b$7, c$9],
[a, b, 1/a, 1/b], [a, c, 1/a, 1/c], [b, c, 1/b, 1/c]}):
> grouporder(G[1]);
```

31

Проверка закончилась, а вместе с ней окончилось и изучение группы G_1 .

Группа G_1 имеет простой порядок, следовательно, она циклическая. Улучшенное копредставление группы G_1 имеет вид

$$G_1 = \langle x; x^{31} \rangle.$$

Теперь исследуем группу

$$G_2 = \langle a, b, c; a^2 b^3 c^4, a^5 b^5 c^6, a^2 b^6 c^9, aba^{-1}b^{-1}, aca^{-1}c^{-1}, bcb^{-1}b^{-1} \rangle.$$

Как и раньше, сначала найдем порядок G_2 :

```
> with(group):
> G[2] := grelgroup({a, b, c}, {[a$2, b$3, c$4],
[a$5, b$5, c$6], [a$2, b$6, c$9],
[a, b, 1/a, 1/b], [a, c, 1/a, 1/c], [b, c, 1/b, 1/c]}):
> grouporder(G[2]);
```

1

Оказалось, что группа G_2 единичная.

Отметим, что единичность G_2 (и нетривиальность G и G_1) можно было установить иными средствами.

Напомним, что новые порождающие абелевой группы можно найти с помощью элементарных преобразований строк и столбцов соответствующей матрицы. После приведения этой матрицы к диагональному виду по диагонали с точностью до знака будут стоять порядки ее циклических прямых множителей.

Поэтому если число определяющих соотношений, отличных от коммутаторов, абелевой группы A на n порождающих равно n , то группа A бесконечна тогда и только тогда, когда определитель, составленный из показателей степеней в этих соотношениях, равен нулю.

Если группа A конечна, то ее порядок равен абсолютной величине этого определителя.

Сделаем такую проверку для групп G , G_1 и G_2 .

Для этого нам потребуется пакет «Линейная алгебра» — *LinearAlgebra*. Вход в этот пакет осуществляется командой

with(LinearAlgebra).

Матрица A соответствует набору показателей степеней в соотношениях абелевой группы G , матрица B соответствует группе G_1 , а матрица C — группе G_2 :

> *with(LinearAlgebra):*

> $A = \begin{bmatrix} 5 & 5 & 2 \\ 11 & 8 & 5 \\ 17 & 5 & 8 \end{bmatrix};$

> *Determinant(A);*

18

> $B = \begin{bmatrix} 5 & 5 & 3 \\ 5 & 6 & 5 \\ 8 & 7 & 9 \end{bmatrix};$

> *Determinant(B);*

31

> $C = \begin{bmatrix} 2 & 3 & 4 \\ 5 & 5 & 6 \\ 2 & 6 & 9 \end{bmatrix};$

> *Determinant(C);*

-1

Вычисления подтвердили полученные ранее результаты:

$$|G|=18, |G_1|=31, |G_2|=1.$$

Кроме порядков групп, с помощью матриц можно определить и групповые инварианты. Элементарными преобразованиями строк и столбцов, используя в качестве скаляров только целые числа, матрицы A, B, C , можно преобразовать соответственно в диагональные матрицы матриц A_1, B_1, C_1 , где по диагонали будут расположены нужные нам числа:

$$A_1 = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix};$$

$$B_1 = \begin{bmatrix} 31 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

$$C_1 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Рассмотрим еще один пример абелевой группы. Пусть группа G_3 задана копредставлением

$$G_3 = \langle a, b, c; a^4b^7c^3, a^2b^3c^2, a^6b^{10}c^5, aba^{-1}b^{-1}, aca^{-1}c^{-1}, bcb^{-1}b^{-1} \rangle.$$

Матрица T , соответствующая этому копредставлению, имеет вид

$$T = \begin{bmatrix} 4 & 7 & 3 \\ 2 & 3 & 2 \\ 6 & 10 & 5 \end{bmatrix}.$$

Вычисляем определитель этой матрицы и узнаем, что группа G_3 бесконечна:

```
> with(LinearAlgebra):
> T =  $\begin{bmatrix} 4 & 7 & 3 \\ 2 & 3 & 2 \\ 6 & 10 & 5 \end{bmatrix}$ :
> Determinant(T);
```

0

Отметим, что бесконечность группы G_3 можно было узнать и непосредственно в пакете «Теория групп»:

```

> with(group):
> G[3] := grelgroup({a, b, c}, {[a$4, b$7, c$3],
[a$2, b$3, c$2], [a$6, b$10, c$5],
[a, b, 1/a, 1/b], [a, c, 1/a, 1/c], [b, c, 1/b, 1/c]}):
> grouporder(G[3]);

```

∞

Вернемся к матрице T , представляющей группу G_3 . Разрешенными элементарными преобразованиями матрица T превращается в диагональную матрицу

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Это значит, что в группе G_3 два порождающих равны единице (т. е. их можно просто выбросить из системы порождающих), а один имеет бесконечный порядок. Группа G_3 бесконечная циклическая.

Отметим, что изучение устройства группы G_3 легко проводится без машины, вручную, и без приведения матрицы T к диагональному виду. Из равенств

$$a^4 b^7 c^3 = 1;$$

$$a^2 b^3 c^2 = 1$$

следует, что $b = c$, а это значит, что представление группы G_3 имеет вид

$$G_3 = \langle a, b; a^2 b^5, aba^{-1}b^{-1} \rangle.$$

Введем новый порождающий элемент $d = ab^2$. Тогда $b = d^{-2}$, $a = d^5$. Следовательно, наша группа бесконечная циклическая: $G_3 = \langle d \rangle$.

Каждая конечная группа изоморфно представима группой подстановок — подгруппой симметрической группы.

Группа подстановок задается своими порождающими элементами. Если известно копредставление всей симметрической группы, то можно найти копредставление и подгруппы. Поэтому особый интерес представляют копредставления самих симметрических групп.

Симметрическая группа второй степени — это циклическая группа второго порядка, ее копредставление имеет вид

$$S_2 = \langle a; a^2 \rangle.$$

Копредставление группы S_3 было найдено ранее для двух порождающих второго порядка (т. е. как фактор-группы группы диэдра):

$$S_3 = \langle a, b; a^2, b^2, (ab)^3 \rangle.$$

Конечно, элементами второго порядка (транспозициями) порождается любая симметрическая группа, однако каждая симметрическая группа обладает и системой всего из двух порождающих:

$$S_n = \text{гр}(a = (123\dots n), b = (12)).$$

Это значит, что симметрическая группа S_n для $n > 2$ является фактор-группой свободного произведения двух групп: циклической порядка два и циклической порядка n . Фрагмент копредставления для такой группы имеет вид

$$S_n = \langle a, b; a^n, b^2, \dots \rangle.$$

Остается только раскрыть тайну многоточия (разумеется, множество соотношений на месте многоточия не пусто: группа $\langle a, b; a^n, b^2 \rangle$ бесконечна, в то время как группа S_n конечна).

Найдем сначала определяющие соотношения группы S_3 в стандартных порождающих:

$$a = (123), b = (12).$$

Порядки этих порождающих равны соответственно трем и двум, и, таким образом, часть нового копредставления группы S_3 уже есть:

$$S_3 = \langle a, b; a^3, b^2, \dots \rangle.$$

Индекс подгруппы $A = \text{гр}(a)$ в группе S_3 равен двум, и элемент b не принадлежит A . Это значит, что

$$S_3 = A + Ab = \{e, a, a^2\} \cup \{b, ab, a^2b\}.$$

При этом левостороннее разложение S_3 по A имеет вид

$$S_3 = A + bA = \{e, a, a^2\} \cup \{b, ba, ba^2\}.$$

Отсюда следует, что

$$\{b, ab, a^2b\} = \{b, ba, ba^2\}.$$

Поскольку группа S_3 неабелева, из равенства множеств следует равенство элементов

$$\begin{aligned} ab &= ba^2, \\ a^2b &= ba. \end{aligned}$$

Эти соотношения в S_3 выполняются. Возможно, что именно они — недостающие определяющие соотношения. Это будет действительно так, если группа

$$\langle a, b; a^3, b^2, ab = ba^2, a^2b = ba \rangle$$

содержит ровно столько же элементов, что и S_3 .

Проверяем:

```
> with(group):
> grouporder(grelgroup({a, b}, {[a, a, a], [b, b],
[a, b, 1/a^2, 1/b], [a, a, b, 1/a, 1/b]}));
```

6

Представление для группы S_3 получено:

$$S_3 = \langle a, b; a^3, b^2, ab = ba^2 \rangle.$$

Возможно, что здесь есть лишние соотношения. Попробуем убрать одно из них:

```
> with(group):
> grouporder(grelgroup({a, b}, {[a, a, a], [b, b],
[a, b, 1/a^2, 1/b]}));
```

6

Попытка удалась, окончательное копредставление группы S_3 получено:

$$S_3 = \langle a, b; a^3, b^2, ab = ba^2 \rangle.$$

Отметим, что если третье соотношение переписать в виде

$$b^{-1}ab = a^2,$$

то сразу становится очевидным разложение группы S_3 в полупрямое произведение группы A и группы $B = \langle b \rangle$:

$$S_3 = A \rtimes B.$$

Найдем теперь порождающие элементы и определяющие соотношения знакопеременной группы A_5 (эта группа тоже замечательна в своем роде). Мы уже знаем, что порядок A_5 равен 60 и она состоит из четных подстановок на пяти символах.

Группа S_4 порождается элементами

$$a = (1234), b = (12).$$

Копредставление для группы S_4 имеет вид

$$S_4 = \langle a, b; a^4, b^2, \dots \rangle.$$

Теперь остается, как и в предыдущем случае, найти недостающие соотношения, скрытые пока знаком многоточия.

Применение прежнего способа, связанного с разложением симметрической группы в полупрямое произведение знакопеременной

группы и циклической группы, здесь затруднено тем, что группа A_4 нециклическая и ее копредставление нам пока не известно.

Попробуем найти недостающие соотношения экспериментальным путем. Используя команду *convert*, мы можем получать равенства, заведомо верные в нашей группе. Присоединив эти равенства к уже имеющимся соотношениям, с помощью вычисления порядка группы проверим затем, не является ли получившаяся группа именно группой S_4 (а не ее гомоморфным прообразом).

Сначала просто найдем порядок элемента ab :

```
> with(group):
> G := permgroup(7, {a = [[1, 2, 3, 4]], b = [[1, 2]]}):
> convert([a, b], 'disjunc', G);
```

[[2, 3, 4]]

Подстановка, изображающая элемент ab , — это цикл длины три, поэтому порядок ab равен трем. Число соотношений в искомом копредставлении увеличивается:

$$S_4 = \langle a, b; a^4, b^2, (ab)^3, \dots \rangle.$$

Этих трех соотношений достаточно для задания группы S_4 , если группа

$$G = \langle a, b; a^4, b^2, (ab)^3 \rangle,$$

как и S_4 , содержит 24 элемента.

Проверяем:

```
> with(group):
> G := relgroup({a, b}, {[a, a, a, a],
  [b, b], [a, b, a, b, a, b]}):
> grouporder(G);
```

24

Проверка получилась: группа G содержит 24 элемента; копредставление симметрической группы четвертой степени получено:

$$S_4 = \langle a, b; a^4, b^2, (ab)^3 \rangle.$$

Переходим к поиску копредставления S_5 . Группа S_5 порождается элементами

$$a = (12345), \quad b = (12),$$

а ее копредставление имеет вид

$$S_5 = \langle a, b; a^5, b^2, \dots \rangle.$$

Снова начнем поиск недостающих соотношений с определения порядка элемента ab :

```
> with(group):
> G := permgroup(5, {a = [[1, 2, 3, 4, 5]], b = [[1, 2]]}):
> convert([a, b], 'disjycyc', G);
```

```
[[2, 3, 4, 5]]
```

Итак,

$$S_5 = \langle a, b; a^5, b^2, (ab)^4, \dots \rangle.$$

Маловероятно, что этих соотношений будет достаточно. Действительно, вычислительный эксперимент с группой, содержащей только эти три соотношения, тянется подозрительно долго; возможно, что порядок группы с такими соотношениями бесконечен или же конечен, но значительно больше желаемого числа 120.

Поиск еще соотношения. Найдем, например, порядок коммутатора $aba^{-1}b^{-1}$:

```
> with(group):
> G := permgroup(5, {a = [[1, 2, 3, 4, 5]], b = [[1, 2]]}):
> convert([a, b, 1/a, 1/b], 'disjycyc', G);
```

```
[[1, 5, 2]]
```

Появилось еще одно равенство из группы S_5 :

$$(aba^{-1}b^{-1})^3 = 1.$$

Заметим, что порядок элемента b равен двум, поэтому элемент $b^{-1} = b$ и найденное соотношение равносильно соотношению

$$(aba^{-1}b)^3 = 1.$$

Проверим, не хватит ли полученных соотношений для искомого копредставления:

```
> with(group):
> G := relgroup({a, b}, {[a, a, a, a, a],
[b, b], [a, b, a, b, a, b, a, b],
[a, b, 1/a, b, a, b, 1/a, b, a, b, 1/a, b]}):
> grouporder(G);
```

```
120
```

Соотношений хватило: получено нужное нам число 120 — порядок группы S_5 . Копредставление группы S_5 получено:

$$S_5 = \langle a, b; a^5, b^2, (ab)^4, (aba^{-1}b)^3 \rangle.$$

Рассмотрим теперь свойства симметрической группы степени больше пяти:

$$S_n = \langle a, b; a^n, b^2, \dots \rangle.$$

Порядок элемента ab в этой группе несложно вычислить вручную:

$$(123\dots n) \cdot (12) = (23\dots n),$$

поэтому всегда $(ab)^{n-1} = 1$.

Коммутатор порождающих элементов тоже можно вычислить в самом общем виде:

$$(123\dots n)(12) \cdot (n\dots 321)(12) = (1n2).$$

Итак,

$$S_n = \langle a, b; a^n, b^2, (ab)^{n-1}, (aba^{-1}b)^3, \dots \rangle.$$

Заметим сразу, что для $n > 5$ этого недостаточно. Поможет окончательному нахождению копредставления¹ группы S_n знание порядков коммутаторов степеней a и элемента b , т. е. значения порядков элементов вида

$$a^k b a^{-k} b,$$

где k принимает значения от 2 до n .

Знакопеременная группа A_2 состоит из одной единицы. Группа A_3 циклическая третьего порядка, ее можно представить как $\langle x; x^3 \rangle$. Найдем копредставление группы A_4 . Для этого воспользуемся тем, что представление всеобъемлющей группы S_4 у нас уже есть:

$$S_4 = \langle a, b; a^4, b^2, (ab)^3 \rangle.$$

В группе подстановок эти элементы интерпретируются так:

$$a = (1234), \quad b = (12).$$

Теперь нам нужно выразить порождающие группы A_4 через элементы a, b . Подстановки, изображающие a, b , обе нечетные, поэтому элементы ba и ab соответствуют четным подстановкам, т. е. элементам из A_4 . Проверим, не порождается ли подгруппа A_4 этими двумя подстановками. Для начала найдем эти подстановки (хотя это несложно сделать и вручную), а затем определим порядок подгруп-

¹ То, что этого будет действительно достаточно, доказал еще в 1897 г. Элиаким Гастингс Мур (Moore, 1862—1932) — американский математик, один из основателей (1894) и президент (1900—1902) американского математического общества.

пы $\text{gr}(ba, ab)$. Если он окажется равным 12 — порядку группы A_4 , — то эти элементы действительно порождают A_4 :

```
> with(group):
> G := permgroup(4, {a = [[1, 2, 3, 4]], b = [[1, 2]]}):
> convert([b, a], 'disjcyc', G);
```

[[1, 3, 4]]

```
> convert([a, b], 'disjcyc', G);
```

[[2, 3, 4]]

```
> grouporder (permgroup(5, {[[1, 3, 4]], [[2, 3, 4]]})):
```

12

Итак, группа A_4 — это подгруппа $\text{gr}(ba, ab)$ в группе

$$S_4 = \langle a, b; a^4, b^2, (ab)^3 \rangle.$$

Для получения копредставления A_4 теперь остается лишь воспользоваться компьютерными командами *subgrel* и *pres* для нахождения копредставления подгрупп:

```
> with(group):
> G := grelgroup({a, b}, {[a, a, a, a], [b, b],
[a, b, a, b, a, b]}):
> H := subgrel({x = [b, a], y = [a, b]}, G):
> pres(H);
```

$\text{grelgroup}(\{x, y\}, [y, x, y, x], [y, y, y], [x, y, x, y], [x, x, x])$

Копредставление для знакопеременной группы четвертой степени найдено:

$$A_4 = \langle x, y; (yx)^2, y^3, (xy)^2, x^3 \rangle.$$

Результат, полученный компьютером, можно улучшить. Элементы $ухух$ и $хуху$ сопряжены, поэтому одно из этих соотношений можно удалить.

На всякий случай сделаем после удаления проверку (после выбрасывания лишнего соотношения порядок должен остаться прежним, равным 12):

```
> with(group):
> grouporder(grelgroup({x, y}, {[x, x, x], [y, y, y],
[x, y, x, y]})):
```

12

Итак, окончательное копредставление нашей группы имеет вид

$$A_4 = \langle x, y; x^3, y^3, (xy)^2 \rangle.$$

Переходим к обследованию знакопеременной группы пятой степени.

Вспомним, что группа A_5 — замечательная в своем роде. Во-первых, это наименьшая неабелева простая группа. Во-вторых, именно из-за ее простоты алгебраические уравнения степени пятой и выше не имеют общих формул для нахождения корней и вообще не всегда разрешимы в радикалах.

Для отыскания копредставления группы A_5 воспользуемся найденным ранее копредставлением группы S_5 :

$$S_5 = \langle a, b; a^4, b^2, (ab)^4, (aba^{-1}b)^3 \rangle.$$

В группе подстановок эти элементы интерпретируются так:

$$a = (12345), \quad b = (12).$$

Теперь нам нужно выразить порождающие группы A_5 через элементы a, b . Подстановка a четная, поэтому она принадлежит подгруппе A_5 . Возьмем еще сопряжение a с помощью элемента b и посмотрим, не породят ли они вдвоем всю группу A_5 :

```
> with(group):
> G := permgroup(5, {a = [[1, 2, 3, 4, 5]], b = [[1, 2]]}):
> convert([b, a, b], 'disjunc', G);

[[1, 3, 4, 5, 2]]

> A := permgroup(5, {[[1, 3, 4, 5, 2]], [[1, 2, 3, 4, 5]]}):
> grouporder(A);
```

60

Эти элементы в самом деле оказались порождающими:

$$A_5 = \text{gp}(a, bab).$$

Используя копредставление группы S_5 и порождающие для A_5 , найдем теперь копредставление группы A_5 :

```
> with(group):
> G := grelgroup({a, b}, {[a, a, a, a, a], [b, b],
[a, b, a, b, a, b, a, b],
[a, b, 1/a, b, a, b, 1/a, b, a, b, 1/a, b]}):
> H := subgrel({x=[a], c=[b, a, b]}, G):
> pres(H);
```

$$\text{grelgroup} \left(\{a, c\}, \left\{ [a, a, a, a, a], [c, c, c, c, c], [c, a, c, a], \right. \right. \\ \left. \left. \left[a, \frac{1}{c}, a, \frac{1}{c}, a, \frac{1}{c} \right], [a, c, a, c] \right\} \right).$$

Снова невооруженным глазом видно лишнее соотношение: из двух равенств $(ac)^2 = 1$ и $(ca)^2 = 1$ одно можно удалить. Удаляем и делаем проверку с помощью порядка группы (он должен быть равен 60):

```
> with(group):
> grouporder(grelgroup({a, c}, {[a, a, a, a, a],
[c, c, c, c, c], [a, c, a, c],
[a, 1/c, a, 1/c, a, 1/c]})))
```

60

Представление замечательной группы A_5 получено:

$$A_5 = \langle a, c; a^5, c^5, (ac)^2, (ac^{-1})^3 \rangle.$$

Посмотрим второе решение этой же задачи, не связанное с копредставлением всей симметрической группы. В предыдущей теме были показаны порождающие системы знакопеременных групп, состоящие из циклов длины три.

В частности, группу A_5 можно породить тремя подстановками:

$$A_5 = \text{gr}(a = (123), b = (124), c = (125)).$$

Тогда

$$ab = (123) \cdot (124) = (14)(23);$$

$$bc = (124) \cdot (125) = (15)(24);$$

$$ac = (123) \cdot (125) = (15)(23).$$

Часть искомых соотношений уже есть:

$$a^3 = 1, b^3 = 1, c^3 = 1, (ab)^2 = 1, (bc)^2 = 1, (ac)^2 = 1.$$

Являются ли эти соотношения определяющими? Это выяснит машина:

```
> with(group):
> grouporder(grelgroup({a, b, c}, {[a$3], [b$3],
[c$3], [a, b, a, b],
[a, c, a, c], [b, c, b, c]})))
```

60

Итак, этими соотношениями задается группа порядка 60, т. е. A_5 . Знакопеременная группа пятой степени имеет представление

$$A_5 = \langle a, b, c; a^3 = 1, b^3 = 1, c^3 = 1, (ab)^2 = 1, (bc)^2 = 1, (ac)^2 = 1 \rangle.$$

Новое представление, безусловно, симметричнее полученного ранее, а главное — оно легко переносится на общий случай.

Для $n > 2$ группа A_n порождается элементами $a_k = (1\ 2\ k)$, где $k = 3, 4, \dots, n$. Если $k \neq m$, то

$$(12k) \cdot (12m) = (1m) \cdot (2k),$$

т. е. все попарные произведения этих порождающих имеют порядок два.

Следовательно, фрагмент копредставления группы A_n имеет вид

$$A_n = \langle a_3, a_4, \dots, a_n; a_i^3, (a_i a_j)^2, \dots \rangle,$$

где $i, j \in \{3, 4, \dots, n\}$, $i \neq j$.

Оказывается, что это вовсе не фрагмент копредставления, а *полное копредставление* знакопеременной группы¹.

Для группы A_4 было получено именно такое представление. Для контроля проверим это утверждение для $n = 6$ и $n = 7$. Заметим сначала, что группа A_6 имеет порядок $\frac{6!}{2} = 360$, а порядок группы A_7 равен

$\frac{7!}{2} = 2520$. Тогда:

`> with(group):`

```
> grouporder(grelgroup({a, b, c, d}, {[a$3],
[b$3], [c$3], [d$3], [a, b, a, b],
[a, c, a, c], [a, d, a, d], [b, c, b, c],
[b, d, b, d], [c, d, c, d]}));
```

360

```
> grouporder(grelgroup({a, b, c, d, e},
{[a$3], [b$3], [c$3], [d$3], [e$3], [a, b, a, b], [a, c, a, c],
[a, d, a, d], [a, e, a, e], [b, c, b, c], [b, d, b, d], [b, e,
b, e], [c, d, c, d], [c, e, c, e], [d, e, d, e]}));
```

2520

Рассмотрим теперь пример отыскания копредставления некоторой произвольной группы подстановок. Пусть эта группа порождается подстановками

$$a = (1245), \quad b = (45)(36).$$

¹ Впервые доказано также Э. Г. Муром в 1897 г.

Сначала найдем порядок этой группы — он наверняка потребуется в дальнейших вычислениях. Заодно выясним, абелева ли данная группа. В случае абелевости она является прямым произведением силовских p -подгрупп, которые, разумеется, тоже абелевы. Исходная задача значительно упрощается:

```
> with(group):
> G := permgroup(6, {[[1, 2, 4, 5]], [[4, 5], [3, 6]]}):
> grouporder(G);
```

48

```
> isabelian(G);
```

false

Группа содержит 48 элементов, и она неабелева. Найдем порядок произведения порождающих и порядок их коммутатора:

```
> with(group):
> G := permgroup(6, {a = [[1, 2, 4, 5]], b = [[4, 5], [3, 6]]}):
> convert([a, b], 'disjycyc', G);
```

[[1, 2, 5], [3, 6]]

```
> convert([a, b, 1/a, b], 'disjycyc', G);
```

[[2, 5, 4]]

Итак, группа G имеет копредставление:

$$G = \langle a, b; a^4, b^2, (ab)^6, (aba^{-1}b^{-1})^3, \dots \rangle.$$

Вычислительный эксперимент, продолжающийся подозрительно долго, показывает, что этих соотношений, видимо, недостаточно: за многоточием действительно что-то находится. Найдем еще какое-нибудь соотношение, например, выясним порядок элемента $aba^{-2}b^{-1}$:

```
> with(group):
> G := permgroup(6, {a = [[1, 2, 4, 5]], b = [[4, 5], [3, 6]]}):
> convert([a, b, 1/a, 1/a, b], 'disjycyc', G);
```

[[1, 4]]

Порядок элемента оказался равен двум. Пополним множество соотношений равенством

$$(aba^{-2}b^{-1})^2 = 1$$

и снова проведем контрольное испытание.

Итак, вычисляем порядок группы, заданной новыми соотношениями; если порядок окажется равным 48, то определяющие соотношения группы найдены:

```
> with(group):
> G := relgroup({a, b}, {[a$4], [b$2],
[a, b, a, b, a, b, a, b, a, b, a, b],
[a, b, 1/a, 1/b, a, b, 1/a, 1/b, a, b, 1/a, 1/b],
[a, b, 1/a, 1/a, b, a, b, 1/a, 1/a, b]}):
> grouporder(G);
```

48

Вычисления окончены, исследуемая группа G задается копредставлением:

$$G = \langle a, b; a^4, b^2, (ab)^6, (aba^{-1}b^{-1})^3, (aba^{-2}b^{-1})^2 \rangle.$$

Найденное копредставление позволяет находить копредставления фактор-групп и подгрупп группы G , но мало что говорит о строении самой группы G . Попробуем заменить это копредставление другим, более прозрачным.

Группа G неабелева, поэтому ее коммутант отличен от единицы, а центр — от всей группы. Найдем коммутант и центр группы G , а затем попытаемся с помощью этих заведомо нормальных подгрупп описать строение группы G . Сейчас нам придется вернуться к исходному заданию группы G в виде группы подстановок:

```
> with(group):
> G0 := permgroup(6, {[[1, 2, 4, 5]], [[4, 5], [3, 6]]}):
> K := derived(G0);
```

$$K := \text{permgroup}(6, \{[], [[1, 4, 5]], [[1, 2, 5]]\})$$

```
> grouporder(K);
```

12

```
> Z := center(G0);
```

$$Z := \text{permgroup}(6, \{[[3, 6]]\})$$

Коммутант K и центр Z группы найдены; в коммутанте содержится 12 элементов, а в центре — всего 2. Символы, перемещаемые подгруппами K и Z , различны, поэтому их пересечение единично. Для других групп это может быть по-другому или не так очевидно, поэтому сделаем машинную проверку:

```
> with(group):
> K := permgroup(6, {[[1, 4, 5]], [[1, 2, 5]]}):
```

```
> Z := permgroup(6, {[[3, 6]]}):
> inter(Z, K);
```

$\text{permgroup}(6, \{\})$

Действительно, $Z \cap K = E$. Отсюда следует, что подгруппа $S = \text{gr}(Z, K)$ является их прямым произведением:

$$S = Z \times K.$$

Теперь для того, чтобы найти копредставление подгруппы S , достаточно знать копредставление коммутанта K .

В коммутанте всего 12 элементов, и найти его копредставление значительно легче, чем исходной группы. Пусть $x = (1\ 4\ 5)$, $y = (1\ 2\ 5)$. Тогда

$$xy = (1\ 4\ 5) \cdot (1\ 2\ 5) = (1\ 4) \cdot (2\ 5).$$

Проверим, является ли группа

$$\langle x, y; x^3, y^3, (xy)^2 \rangle$$

нашим коммутантом:

```
> with(group):
> grouporder(grelgroup({x, y}, {[x$3], [y$3], [x, y, x, y]})):
```

Ответ получен: да, является.

Пусть $z = (3, 6)$. Тогда представление подгруппы S имеет вид

$$\begin{aligned} S &= \langle x, y; x^3, y^3, (xy)^2 \rangle x \langle z; z^2 \rangle = \\ &= \langle x, y; z; x^3 = 1, y^3 = 1, (xy)^2 = 1, z^2 = 1, xz = zx, zy = yz \rangle. \end{aligned}$$

Но S — это еще не вся группа G . Попробуем теперь с помощью копредставления подгруппы S получить копредставление всей группы.

Обе группы Z и K нормальны в группе G , поэтому и S нормальна в G .

Посмотрим, не раскладывается ли группа G в полупрямое (или даже прямое) произведение, одним из множителей которого является подгруппа S .

Для этого сначала найдем систему представителей правых смежных классов группы G по подгруппе S :

```
> with(group):
> G := permgroup(6, {[[1, 2, 4, 5]], [[4, 5], [3, 6]]}):
> S := permgroup(6, {[[1, 4, 5]], [[1, 2, 5]], [[3, 6]]}):
> cosets(G, S);
```

$$\{[], [[4, 5]]\}$$

Подгруппа $A = \text{gr}((4\ 5))$ имеет единичное пересечение с подгруппой S , но ненормальна в группе G :

```
> with(group):
> G := permgroup(6, {[[1, 2, 4, 5]], [[4, 5], [3, 6]]}):
> A := permgroup(6, {[[4, 5]]}):
> inter(S, A);
```

$\text{permgroup}(6, \{\})$

```
> isnormal(G, A);
```

false

Итак, группа G разложима в полупрямое произведение:

$$G = S \rtimes A.$$

Пусть $t = (4\ 5)$, тогда наша группа порождается элементами x, y, z, t . Копредставления групп подгрупп S и A нам известны. Остается узнать, как действуют сопряжения элементом t на элементы x, y, z .

Сразу заметим, что на z — элемент центра — t никак не действует:

$$tzt^{-1} = z.$$

Для элементов x и y проведем вычислительные эксперименты, т. е. поищем элементы из подгруппы S , равные txt^{-1} и tyt^{-1} . В начале вычислений проверим, не допущена ли где ранее ошибка, т. е. действительно ли группа $\text{gr}(x, y, z, t)$ совпадает с исходной группой G . Поскольку все подстановки x, y, z, t принадлежат исходной группе, достаточно вычислить порядок $\text{gr}(x, y, z, t)$: если все верно, то он должен равняться 48:

```
> with(group):
> G := permgroup(6, {x = [[1, 4, 5]], y = [[1, 2, 5]],
z = [[3, 6]], t = [[4, 5]]}):
> grouporder(G);
```

48

```
> convert([t, x, 1/t, x], 'disjсyc', T);
```

[]

```
> convert([t, y, 1/t, x, y, y], 'disjсyc', T);
```

[]

Результаты сопряжений элементов x, y с помощью элемента t стали известны:

$$txt^{-1} = x^{-1}, \quad tyt^{-1} = y^{-2}x^{-1}.$$

Теперь можно написать новое, улучшенное копредставление группы:

$$G = \langle x, y; z, t; x^3 = 1, y^3 = 1, (xy)^2 = 1, z^2 = 1, xz = zx, \\ zy = yz, tz = zt, txt^{-1} = x^{-1}, tyt^{-1} = y^{-2}x^{-1} \rangle.$$

Контрольные задания

1. Задайте группу подстановок на девяти символах с помощью двух порождающих элементов и найдите с помощью пакета *Maple* порядок этой группы.

2. Задайте группу подстановок на девяти символах с помощью двух порождающих элементов и определите с помощью пакета *Maple* является ли эта группа.

3. Задайте группу подстановок на девяти символах с помощью двух порождающих элементов и с помощью пакета *Maple* найдите центр группы из задания 1.

4. Задайте группу подстановок на девяти символах с помощью двух порождающих элементов и с помощью пакета *Maple* найдите коммутант этой группы.

5. Задайте группу подстановок на девяти символах с помощью двух порождающих элементов и определите с помощью пакета *Maple* является ли эта группа разрешимой.

6. Задайте группу подстановок на девяти символах с помощью двух порождающих элементов и определите с помощью пакета *Maple* является ли эта группа нильпотентной.

7. Задайте абстрактную группу на двух порождающих с тремя определяющими соотношениями и найдите с помощью пакета *Maple* порядок этой группы (примечание: можно не справиться с такой задачей, в этом случае поэкспериментируйте с соотношениями группы).

8. Конечную группу из задания 7 с помощью пакета *Maple* представьте подстановками множества самой группы.

9. Конечную группу из задания 7 с помощью пакета *Maple* представьте подстановками правых смежных классов по подгруппе.

10. Задайте группу подстановок на девяти символах с помощью двух порождающих элементов и с помощью пакета *Maple* найдите копредставление этой группы.

Тема 9

КОМПЬЮТЕРНОЕ ИССЛЕДОВАНИЕ КОЛЕЦ

Основные понятия: кольцо, целостное кольцо, идеал, главный идеал, сумма идеалов, евклидовость, простые и составные элементы целостного кольца, гомоморфизм, ядро гомоморфизма, фактор-кольцо, многочлен, корень многочлена, границы корней, интерполяционный многочлен, группа Галуа многочлена.

Основные факты: для колец целых чисел, гауссовых целых чисел, колец многочленов от одной и нескольких переменных с помощью компьютера можно определить простоту (неприводимость) или не простоту (приводимость) элементов, находить разложение на простые (неприводимые) множители, для многочленов от одной переменной вычислять корни и находить группу Галуа, находить представления рациональных алгебраических функций в виде суммы простейших дробей, интерполировать многочленами таблично заданные функции.

В отличие от групповых задач, команды, связанные с изучением колец целых чисел, колец классов вычетов, колец многочленов от одной и нескольких переменных, более просты в применении. Часто значение команды понятно из ее названия, а ее применение доступно учащемуся средней общеобразовательной школы. Поэтому сейчас мы ограничимся лишь основными вопросами, возникающими при исследовании колец.

Как и раньше, основной целью сейчас является иллюстрация машинными вычислениями теоретических положений, рассмотренных ранее.

9.1. Машинные вычисления в кольце целых чисел

В системе компьютерной алгебры *Maple* исследование целых чисел осуществляется с помощью пакета *Number Theory*. Вход осуществляется командой *with(numtheory)*.

Если поставить в конце команды точку с запятой, то машина покажет команды для решения теоретико-числовых задач:

```
> with(numtheory):  
[GIgcd, bigomega, cfrac, cfracpol, cyclotomic, divisors,  
factorEQ, factorset, fermat, imagunit, index, integral basis,
```



```
> prevprime(97);
```

89

Занумеруем простые числа в порядке возрастания: $p_1 = 2$, $p_2 = 3$, $p_4 = 5$,

По команде

```
ithprime(n)
```

выдается n -е простое число. Например, миллионное простое число равно 15 485 863:

```
> ithprime(1000000);
```

15 485 863

Распределение простых чисел в ряде натуральных чисел описывается функцией $\pi(n)$, равной числу простых чисел, не превышающих натуральное n (вообще-то эта функция определена на всем множестве положительных действительных чисел, но в пакете *Maple* ее область определения ограничена). Формулы для выражения функции $\pi(n)$ до сих пор не получено (вполне возможно, что таковой вообще не существует), но известно, что асимптотически она приближается к функции $\frac{x}{\ln x}$. Это значит, что

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Этот предел пакет *Maple* пока вычислять не умеет, но для конкретных и достаточно больших значений n мы можем сравнить значения этих двух функций:

```
> pi(10000000000);
```

455052511

```
> x := 10000000000: y := 10000000000.: pi(x)/(y/log(y));
```

1.047797128

Разложение числа на множители, нахождение множества простых делителей числа натурального числа, а также множества всех делителей числа видно из следующих примеров (буква i в начале команды — от сокращения слова *integer* — целое):

```
> ifactor(987654321);
```

(3)² (17)² (379721)

```
> factorset(987654321);
```

```
{3, 17, 379721}
```

```
> divisors(987654321);
```

```
{1, 3, 9, 17, 51, 153, 289, 867, 2601, 379721, 1139163, 3417489,  
6455257, 19365771, 58097313, 109739369, 329218107, 987654321}
```

В кольце целых гауссовых чисел $\mathbb{Z}[i]$ выполняется аналог основной теоремы арифметики, поэтому каждое целое гауссово число, отличное от делителя единицы и нуля, является либо простым, либо произведением простым, причем такое представление единственно с точностью до ассоциированности и порядка множителей.

Множество делителей единицы в кольце $\mathbb{Z}[i]$ — это множество $\{1, -1, i, -i\}$, а простыми являются такие числа $a + bi$, для которых $a^2 + b^2$ нечетное простое.

Для выполнения команд, связанных с целыми гауссовыми числами, необходимо войти в подпакет «*Gaussian Integers*»:

Например, число 2 непростое:

```
> with(GaussInt):
```

```
> GPrime(2);
```

```
false
```

```
> GPrime(1 + 4*I);
```

```
true
```

```
> GPrime(3 + 7*I);
```

```
false
```

```
> GIfactor(2);
```

```
(-I) (1 + I)2
```

Два простых числа p и $p + 2$ древние греки называли *близнецами*. Близнецы могут быть очень большими, и вполне возможно, что множество близнецов бесконечно. Близнецы встречаются довольно часто. Поиск пары близнецов в интервале $[a, a + b]$ для достаточно больших чисел b быстро приводит к успеху. Например, в интервале $[10^{30}, 10^{30} + 10\,000]$ содержится даже две пары близнецов:

```
> a:= 10^30: b:= 10000:
```

```
for i from nextprime(a) to a + b
```

```
by 2 do if isprime(i) and isprime(i + 2)
```

```
then print(i):
```

[illegible] $10^{100} + 87\,079$ и $10^{100} + 87\,081$.

612

Действительно, первые пять чисел F_n ($n = 0, 1, 2, 3, 4$) простые. Однако существует ли хотя бы еще одно простое число F_n , пока неизвестно. С помощью следующей программы при $a = 20$ сразу проверяется простота уже известной пятерки и одновременно выясняется, что в интервале $[655\,378, 10\,315\,652]$ простых чисел Ферма нет:

```
>k := 0: a := ____
for i from 1 to a
by 1 do
if i sprime(2^(2^i) + 1)
then print(i):
print(2^(2^i) + 1):
k := k + 1: print(k):
print(____):
else fi od;
```

Простые числа Ферма связаны с задачей построения правильного n -угольника с помощью циркуля и линейки: такое построение возможно тогда и только тогда, когда в каноническое разложение числа n входят лишь число 2 и простые числа Ферма. Таким образом, для конкретного n команда

$ifactor(phi(n))$

позволяет узнать, можно или нельзя построить правильный n -угольник с помощью циркуля и линейки.

Еще в 1742 г. было замечено¹, что каждое четное число больше двух можно представить в виде суммы двух простых чисел. Вычислительная техника позволяет найти такое представление для сравнительно больших чисел. Например:

$$10^{600} = 4091 + (10^{600} - 4091).$$

Можно заметить, что число таких представлений для конкретного n не просто ненулевое, а увеличивается с возрастанием n :

```
> a := ____ : k := 0:
for i from 2 to a by 1
do if isprime(i) and isprime(a - i)
then k := k + 1:
else fi od; print(k);
```

Например, число 10 можно представить тремя способами, 100 — 12-ю, для 1 000 число способов равно 56, для 10 000 — 254, для 100 000 — 1 620, а для 1 000 000 — 10 804. Несмотря на заметное

¹ Замечено петербургским академиком Христианом Гольдбахом (Goldbach, 1690—1754). Обсуждаемое наблюдение вошло в историю науки под названием проблемы Гольдбаха.

увеличение таких представлений с увеличением n , пока нет доказательства, что для любого четного n найдется хотя бы одно такое представление (как нет контрпримера, опровергающего предположение Гольдбаха).

До сих пор неизвестно, конечно или бесконечно множество простых чисел вида $n^2 + 1$. Найти числа вида $n^2 + 1$ в интервале $[1, n^2 + 1]$ для достаточно больших значений n можно с помощью программы:

```
> n := ____ :
for i from 1 to n
by 1 do
if isprime(i*i + 1) then print(i*i + 1):
else fi od;
```

Встречаются такие числа не так уж часто, например, в интервале $[1, 10^{10}]$ их меньше чем одно на пять миллионов:

```
> n := 100000: k := 0:
for i from 1 to n by 1
do if isprime(i*i + 1)
then k := k + 1:
else fi od;
print(k): print(100000^2 + 1);
```

6656

37607912018

Перестанут ли простые числа вида $n^2 + 1$ вообще попадаться с какого-то места натурального ряда или множество таких чисел бесконечно, пока (2021 г.) неизвестно. Теорема о делении с остатком реализуется с помощью команд, действие которых хорошо видно из приводимых примеров:

```
> irem(132049, 11, 'q');
```

5

```
> q;
```

12004

```
> iquo(102, 7, 'r');
```

14

```
> r;
```

4

```
> 11*12004 + 5;
```

132049

Напомним, что кольцо целых чисел не единственное, в котором выполняется теорема о делении с остатком. Кольцо целых гауссовых чисел $\mathbb{Z}[i]$ тоже евклидово. Аналогичными командами находят частное и остаток для чисел в $\mathbb{Z}[i]$:

```
> with(GaussInt):
```

```
> GIquo(2011+5*I, 10+6*I, 'r');
```

148 - 88I

```
> r;
```

3 - 3I

```
> GIrem(2011+5*I, 10+6*I, 'q');
```

3 - 3I

```
> q;
```

148 - 88I

```
> (10+6*I)*(148 - 88*I)+(3 - 3*I);
```

2011 + 5I

Среди двухместных числовых функций, определенных на множестве целых чисел, в теории делимости важнейшую роль играют наибольший общий делитель (a, b) и наименьшее общее кратное $[a, b]$. Машинные команды представляют собой кальку с русского на английский сокращений НОД и НОК:

gcd — *greatest common divisor*;

lcm — *least common multiple*.

Начинаются эти команды с буквы *i*, как и команда разложения на множители (без этой буквы и команда разложения на множители, и команды *nod* и *nok* машиной будут поняты как относящиеся к многочленам). Итак, НОД целых чисел a, b находится командой

igcd(a, b),

а НОК — командой

ilcm(a, b).

Наибольший общий делитель не просто всегда существует — он обладает линейным разложением. Это разложение тоже можно найти, решив соответствующее неопределенное уравнение в целых числах:

```
> igcd(10, 15, 20, 45);
```

5

```
> ilcm(12, 18, 20);
```

180

```
> isolve(10*a + 15*b + 20*c + 45*d = 5, {a, b, c, d});  
{b = a, c = b, d = 1 + a + 2c, a = -4 - 6a - 2b - 9c}
```

Подставив значения для свободных переменных в этом уравнении, получим конкретное разложение наибольшего общего делителя:

```
> isolve({10*a + 15*b + 20*c + 45*d = 5, c = 0, b = 1, d = 0},  
{a, b, c, d});
```

$\{c=0, b=1, d=0, a=-1\}$.

Если речь идет всего лишь о паре целых чисел, то можно найти линейное разложение наибольшего общего делителя

$$(a, b) = ua + vb$$

с помощью специальной команды

```
igcdex(a, b, 'u', 'v');
```

Найдем, например, линейное разложение для чисел 100 и 1255:

```
> igcdex(100, 1255, 'u', 'v');
```

5

```
> u;
```

113

```
> v;
```

-9

```
> 100*113 - 9*1255;
```

5

Наибольший общий делитель и наименьшее общее кратное есть у любой пары элементов из евклидова кольца. Например, у пары целых гауссовых чисел есть и НОД, и НОК. Как и в любом кольце главных идеалов, наибольший общий делитель целых гауссовых чисел обладает линейным разложением:

```
> with(GaussInt):
> a: = 2011 + 5*I: b: = 10 + 6*I:GIgcd(a, b);
```

$1 + I$

```
> GILcm(a, b);
```

$3982 + 16098I$

```
> GIgcdex(a, b, 'u', 'v');
```

$1 + I$

```
> u;
```

$2 - 3I$

```
> v;
```

$-31 + 621I$

```
> a*u + b*v;
```

$1 + I$

Ранее в связи с изучением мультипликативной группы кольца классов вычетов по модулю n появилась функция $\varphi(n)$ — функция Эйлера, равная числу натуральных чисел, меньших n и взаимно простых с n .

Давно замечено¹ для сравнительно больших числовых интервалов, что функция Эйлера $\varphi(n)$ при $n > 1$ принимает каждое свое значение *не менее двух раз*. Пока не доказано и не опровергнуто, что так будет всегда.

Машинные команды позволяют вычислить функцию Эйлера, а также в некотором смысле взять обратную (многозначную) функцию $\varphi^{-1}(n)$:

```
> phi(9876);
```

3288

```
> invphi(3288);
```

[4115, 6584, 8230, 9876]

¹ Гипотеза носит название «проблема Кармайкла».

С помощью «обращения» функции Эйлера можно обнаружить, как изменяется число совпадений значений $\varphi(n)$, всегда оставаясь не меньше двух. В следующем примере $a = 10$, $b = 20$:

```
> for i from a to b
do if invphi(i) <> [] then
print(invphi(i))
else fi od;
```

[11, 22]

[13, 21, 26, 28, 36, 42]

[17, 32, 34, 40, 48, 60]

[19, 27, 38, 54]

[25, 33, 44, 50, 66]

Можно расширить возможности поиска совпадений функции Эйлера в различных точках. Придав конкретные значения a , b в программе:

```
> a:= __: b:= __: k:= 0:
for i from 2 to a
do if phi(i)=b
then k := k + 1
else fi od ; : print(k):
```

можно вычислить число решений уравнения $\varphi(x) = b$ для x из интервала $[1, a]$. По результатам вычислений видно, что в конкретных случаях число совпадений этой функции значительно больше двух.

Найдем число совпадений значений функции Эйлера (от 2 до b) на таком интервале (а заодно посмотрим и решения соответствующего уравнения):

```
> with(numtheory):
a := __: b := __:
for i from 2 to b by 1 do
print(__):print (i): print(__):
for j from 1 to a by 1
do if phi(j) = i then print(j):
else fi od; od;
```

Техника позволяет исследовать функцию изменения расстояния до ближайшего совпадения $\varphi(n)$, среднее число совпадений на интервале и т. п.

Классическими числовыми функциями натурального аргумента являются число $\tau(n)$ и сумма $\sigma(n)$ натуральных делителей числа n . Например:


```
> tau(123456789101112);
```

32

```
> sigma(10000000000);
```

24987792457

Функция $\sigma(n)$ приобретает особое значение при изучении совершенных и дружественных чисел. Число называется совершенным (красивым), если оно совпадает с суммой своих собственных делителей.

Например, числа 6, 28, 496, 8128 совершенные. Школа Пифагора приписывала числам мистические свойства. В частности, красивым числам отдавалась роль спасителей (а именно: «красота спасет мир»). Естественно, возник вопрос о конечности или бесконечности такой красоты. Другими словами, еще два с половиной тысячелетия назад был поставлен вопрос: конечно или бесконечно множество совершенных чисел? Ответа на этот вопрос нет до сих пор.

Во времена Евклида были известны всего лишь первые четыре совершенных числа. Даже сейчас, во время машинных вычислений, когда становятся доступными для экспериментов числа с миллионами и миллиардами цифр, вопрос о совершенных числах, по существу, продвинулся недалеко. Древние знали четыре числа, а сейчас их известно меньше пяти десятков, но главный вопрос — конечно или бесконечно — остается без ответа.

Все найденные пока совершенные числа являются четными, поэтому неизвестно даже, существуют ли нечетные совершенные числа.

Задав значения a, b в программе:

```
> k := 0 : a := ____ : b := ____ :  
for i from a to a + b by 1 do  
if sigma(i) - i = i  
and irem(i, 2) > 0  
then print(i): k := k + 1:  
else fi od;  
print(k):
```

можно попытаться найти все нечетные совершенные числа из промежутка $[a, b]$.

Вообще говоря, *Maple* предназначен для точных вычислений с числами, в десятичной записи которых число цифр не превышает 268 435 456, однако в действительности пакет *Number Theory* надежно работает лишь с числами, число цифр которых меньше 10^7 . Кроме того, действие некоторых числовых функций еще более ограничено, например, функция $\sigma(x)$ определена лишь для чисел, не превышающих 10^{10} . Несмотря на эти ограничения, техника

позволяет непосредственно убедиться, что в интервале $[1, 10^{2\,000\,000}]$ нет ни одного нечетного совершенного числа.

Убрав из программы требование нечетности числа i , можно найти все совершенные числа из интервала $[1, 10^{2\,000\,000}]$:

```
>k := 0:
for i from 1 to 10**2000000
by 1 do
if sigma(i) - i = i
then print(i): k := k + 1:
length(i):
print(k):
print(_____):
else fi od;
```

В программу вставлена команда, определяющая число цифр в десятичной записи k -го совершенного числа. Последнее (36-е) совершенное число из этого интервала имеет 1 791 864 цифр.

Четное число a совершенно тогда и только тогда, когда $a = 2^{n-1} \cdot p$, где p — простое число вида $2^n - 1$. Простое число вида $M_n = 2^n - 1$ называют *числом Мерсенна*. Вопрос о мощности множества четных совершенных чисел сводится к вопросу о мощности множества чисел Мерсенна.

В течение последних десятилетий нахождение каждого нового числа Мерсенна было связано, как правило, с появлением очередного поколения вычислительной техники и являлось демонстрацией возможностей этой новой техники. Все числа Мерсенна, начиная с 13-го, были найдены только с помощью вычислительной техники.

Программа

```
> k := 0:
for i from 1 to 10^3000000
by 1 do
if isprime(2^i - 1)
then print(i):
print(2^i - 1):
print(length(i)):
k := k + 1: print(k):
print(_____):
else fi od;
```

позволяет найти 36 чисел Мерсенна, лежащих в интервале $[1, 10^{1\,000\,000}]$. Заметим, что команда

mersenne(n)

быстрее проверяет число n на простоту, однако диапазон ее действия существенно меньше.

Одновременно с задачей о совершенных числах появилась и задача о дружественных числах. Два числа называют дружественными, если сумма собственных делителей каждого из них равна другому числу.

Пока неизвестно, конечно или бесконечно множество пар дружественных чисел. Исторически так случилось, что пары дружественных (даже не очень больших) чисел находились с трудом. После первой пары (220 и 284), известной древним грекам, до нахождения следующих трех пар прошло более двух тысяч лет. Однако вычислительная техника позволяет сравнительно легко находить все пары дружественных чисел в достаточно большом отрезке натурального ряда:

```
> k := 0;
for i from 2 to 10^1000000
by 1 do
if sigma(sigma(i) - i) = sigma(i)
and i < sigma(i) - i
then k := k + 1:
print(i):
print(sigma(i) - i):
print(k): print(____):
else fi od;
```

Если убрать условие $i < \sigma(i) - i$, то программа заодно выдаст и все совершенные числа из этого интервала (а каждую дружественную пару выведет дважды).

Пока не найдено ни одной пары дружественных чисел разной четности (но нет и доказательства того, что в такой паре оба числа должны быть непременно одной четности). Можно попытаться поискать пару разной четности в интервале $[a, b]$:

```
> with(numtheory):
a := __: b := __:
k := 0:
for i from a to b by 1 do
if sigma(sigma(i) - i) = sigma(i)
and i < sigma(i) - i
and irem(sigma(i) - i - i, 2) > 0
then k := k + 1:
print(i): print(sigma(i) - i):
print(k):
print(____):
else fi od;
```

Вычисления по программе для $a = 100\,000$ показывают, что отношение чисел в дружественной паре колеблется, то приближаясь к единице, то чуть удаляясь от нее.

```
> a := __:
for i from 1 to a by 1 do
```

```

if sigma(sigma(i) - i) = sigma(i)
and i < sigma(i) - i then
print(evalf(i/(sigma(i) - i))):
else fi od;

```

0.7746478873

0.9785123967

0.8960328317

0.9022286125

0.9786432161

0.9896831245

0.8417266187

0.9391833189

0.8282950423

0.9990446620

0.9430740038

0.7943925234

0.8987940944

Аналогичным образом можно рассмотреть функцию, равную расстоянию между парами, среднюю плотность пар на отрезке $[a, b]$ и т. п.

9.2. Машинные вычисления в кольце классов вычетов

Арифметические действия: сложение, вычитание и умножение — в кольце Z_m классов вычетов по модулю m производятся с добавлением в конце команды символа $\text{mod}(m)$. Для вычисления по модулю вход в пакет *Number Theory* необязателен. Разумеется, тот же ответ получится, если результат в целых числах просто разделить на m :

```
>123456^789 + 987654*123 - 12345 mod(101);
```

26

```
> irem(123456^789 + 987654*123 - 12345, 101);
```

26

Кроме арифметических действий, в кольце классов вычетов по модулю m можно извлекать корни любой степени. Команда

$$mroot(a, n, m)$$

выдает одно из решений сравнения $x^n \equiv a \pmod{m}$. Проведем вычислительный эксперимент и проверим его результат:

```
> mroot(13, 17, 97);
```

80

```
> 80^17 mod(97);
```

13

Таким образом, получено

$$90^{17} \equiv 12 \pmod{97}.$$

Вычисления в поле классов вычетов \mathbb{Z}_p естественно продолжают-ся в кольце многочленов $\mathbb{Z}_p[x]$ над полем. В частности, можно найти разложение многочлена с коэффициентами из конечного поля на неприводимые множители. Разложим, например, многочлен

$$x^5 + 9x^4 + 8x^3 + 13x^2 + 11x - 8$$

на множители над полем \mathbb{Z}_{17} и над полем \mathbb{Z}_{19} :

```
> f := x^5 + 9*x^4 + 8*x^3 + 13*x^2 + 11*x - 8:
> Factor(f)mod 17;
```

$$(x+16)^2(x+15)^3$$

```
> Factor(f)mod 19;
```

$$(x+16)(x^4+12x^3+6x^2+12x+9).$$

По китайской теореме об остатках если числа m_1, m_2, \dots, m_n попарно взаимно просты, то для любых целых чисел c_1, c_2, \dots, c_n система сравнений

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}, \\ \dots\dots\dots \\ x \equiv c_n \pmod{m_n} \end{cases}$$

имеет единственное решение по модулю $m_1 \cdot m_2 \cdot \dots \cdot m_n$.

Китайская теорема означает, что задача «найти число, которое при делении на m_i дает соответственно остатки c_i », всегда имеет решение, если m_i попарно взаимно просты.

Для двух таких сравнений и взаимно простых модулей команда

$$mcombine(m_1, c_1, m_2, c_2)$$

находит это решение по модулю $m_1 \cdot m_2$. Применим эту команду и сразу проверим машинные вычисления другой машинной командой:

```
> mcombine(15, 1, 16, 2);
```

226

```
> 226 mod(15);
```

1

```
> 226 mod(16);
```

2

Мультипликативная группа $\langle \mathbb{Z}_p^*; \cdot \rangle$ кольца классов вычетов по простому модулю циклическая. Это значит, что по простому модулю p существует первообразный элемент, т. е. элемент, все степени которого полностью исчерпывают множество \mathbb{Z}_p^* . Для простого числа p команда

$$primroot(p)$$

выдает (наименьший положительный) первообразный элемент по модулю p .

Найдем первообразный по модулю 97 и сразу проверим результат другой командой. Порядок первообразного по модулю p должен равняться $p - 1$. Порядок натурального числа n по модулю p вычисляется по команде

$$order(n, p).$$

Проверим заодно, не является ли какое-нибудь число меньше пяти тоже первообразным корнем:

```
> primroot(97);
```

5

```
> order(5, 97);
```

96

```
> order(4, 97); order(3, 97); order(2, 97);
```

24

48

48

Оказалось, что 5 — это действительно наименьшее положительное число, порождающее по модулю 97 группу \mathbf{Z}_{97}^* .

Группы $\langle \mathbf{Z}_{p-1}; + \rangle$ и $\langle \mathbf{Z}_p^*; \cdot \rangle$ имеют одинаковый порядок и обе циклические. Такие группы изоморфны. Изоморфизм продолжает отображение порождающего одной группы в порождающий элемент другой группы. Точнее, если g — порождающий (первообразный) элемент группы $\langle \mathbf{Z}_p^*; \cdot \rangle$, то соответствие $i \mapsto g^i$, переводящее каждое целое число i в степень порождающего элемента g^i , является изоморфизмом.

Таким образом, каждое целое число a , не кратное p , сравнимо по модулю $p - 1$ с некоторой степенью g^i . Число i в этом равенстве называют *индексом* числа a при основании g по модулю p и пишут

$$i = \text{ind}_g a.$$

Машинная команда

$$mlog(a, g, p)$$

выдает индекс i числа a при основании g по модулю p . Это значит, что

$$a \equiv g^i \pmod{p}.$$

Первообразный элемент по модулю 97 только что был вычислен. Найдем при этом основании индекс какого-нибудь числа и сразу же проверим эти вычисления:

```
> mlog(1000, 5, 97);
```

9

```
> 1000 mod (97);
```

30

```
> 5^9 mod(97);
```

30

Вычисление порядка числа по простому модулю позволяет до вычисления назвать длину периода обыкновенной дроби после об-

ращения ее в десятичную. Длина периода дроби $\frac{a}{b}$, где $1 \leq a < b$, $(a, b) = (g, b) = 1$, после обращения ее в g -ичную систематическую дробь равна порядку числа g по модулю b .

Найдем, например, длину периода дроби $\frac{1}{17}$ и сразу проверим результат с помощью команды

pdexpand(a/b).

Эта команда выдает все цифры периода дроби $\frac{a}{b}$. Командой

convert(PDEXPAND[c], rational)

десятичную дробь снова свернем в обыкновенную:

> order(10, 17);

16

> pdexpand(1/17);

PDEXPAND(1, 0, [], [0, 5, 8, 8, 2, 3, 5, 2, 9, 4, 1, 1, 7, 6, 4, 7])

> convert(PDEXPAND(1, 0, [], [0, 5, 8, 8, 2, 3, 5, 2, 9, 4, 1, 1, 7, 6, 4, 7]), rational);

$\frac{1}{17}$.

Прежде чем перейти к обсуждению особенностей обработки кольца многочленов, приведем список основных команд из пакета «Теория чисел».

9.3. Машинные вычисления в кольце многочленов

Под словом «полином» понимается далее алгебраический многочлен, т. е. целая рациональная функция конечной ненулевой степени.

С помощью команды

?polynomials

можно увидеть сводку основных машинных операций над полиномами. Входа в особый пакет для работы с многочленами, как правило, не требуется. Лишь для отдельных задач возникает необхо-

димось применения пакета «Полиномиальные инструментальные средства». Это вход осуществляется командой

with(PolynomialTools).

Выполнить действия над многочленами, т. е. раскрыть скобки при умножении, а затем привести подобные члены в выражении f можно с помощью команды

expand(f).

Например, раскроем скобки и приведем подобные члены в выражении

$$f(x) = (2 - x)(1 + x^2)(x - 3)^3 + (x - 1)(x + 2):$$

```
> f := (2 - x)*(1 + x^2)*(x - 3)^3 + (x - 1)*(x + 2):  
> expand(f);
```

$$92x^3 - 98x^2 + 82x - 56 + 11x^5 - 46x^4 - x^6.$$

При такой случайной записи одночленов в многочлене может представлять интерес команда

degree(f, x)

для нахождения степени многочлена $f(x)$, которую, впрочем, можно применить и до приведения многочлена к стандартному виду — сумме одночленов. Например:

```
> f := (2 - x)*(1 + x^2)*(x - 3)^14 + (x - 1)*(x + 2):  
> degree(f, x);
```

17

Расположить одночлены в многочлене в порядке возрастания степеней, не приводя его к стандартному виду, можно с помощью команды

taylor(f, x = a, n).

Эта команда вообще применима к любой неограниченно дифференцируемой функции от переменного x . Результатом действия команды является разложение функции по степеням $x - a$; число n указывает число членов ряда Тейлора.

Напомним, что разложение функции $f(x)$ находится по формуле

$$f(x) = \sum_{i=0}^{\infty} \frac{f^{(i)}(a)}{i!} (x - a)^i.$$

Для многочлена $f(x)$ такое разложение обрывается через конечное число шагов, равное $\deg f(x) + 1$.

Команда $\text{taylor}(f, x = a, n)$ для многочленов действует точно так же, как

$$\text{series}(f, x = a, n).$$

Для многочлена (или выражения, которое станет многочленом после преобразований) число n равно степени многочлена, увеличенной на единицу.

Рассмотрим два примера. В одном примере разложим многочлен по степеням $x - 0$ и получим в результате упорядочение одночленов по возрастанию степеней. Во втором упражнении найдем двумя способами разложение многочлена (также еще не оформленного окончательно) по степеням $x - a$:

```
> f := (2 - x)*(1 + x^2)*(x - 3)^3 + (x - 1)*(x + 2):
> taylor(f, x = 0, degree(f, x) + 1);
```

$$-56 + 82x - 98x^2 + 92x^3 - 46x^4 + 11x^5 - x^6$$

```
> f := (2 - x)*(1 + x^2)*(x - 3) + (x - 1)*(x + 2):
> taylor(f, x = 1, degree(f, x) + 1);
```

$$-4 + 5(x - 1) + 3(x - 1)^2 + (x - 1)^3 - (x - 1)^4$$

```
> series(f, x = 1, degree(f, x) + 1);
```

$$-4 + 5(x - 1) + 3(x - 1)^2 + (x - 1)^3 - (x - 1)^4.$$

Группировка слагаемых в многочлене p от нескольких переменных по степеням переменной z осуществляется командой

$$\text{collect}(p, z).$$

Сгруппируем сначала члены по степеням x , а затем по степеням y :

```
> p := x*(x + 1) + y*(x + 1) + (y^2 + 2)*x^2;
```

$$p := x(1 + x) + y(1 + x) + (y^2 + 2)x^2$$

```
> collect(p, x);
```

$$(3 + y^2)x^2 + y(1 + y)x + y$$

```
> collect(p, y);
```

$$x^2y^2 + y(1 + x) + x(1 + x) + 2x^2$$

Может случиться, что до выполнения вычислений и приведения подобных членов в многочлене f нас могут интересовать лишь отдельные детали этого многочлена. На вопрос, с каким коэффициентом входит в многочлен одночлен x^n , отвечает команда

$$\text{coeff}(f, x, n).$$

Найдем, например, коэффициенты у одночленов x^5 и x^{15} в многочлене f из предыдущего примера:

```
> f := (2 - x)*(1 + x^2)*(x - 3)^4 + (x - 1)*(x + 2)^2;  
> coeff ( f, x, 5);
```

$$-79$$

```
> coeff ( f, x, 15);
```

$$0$$

О коэффициенте при 15-й степени x можно было и не спрашивать: то, что он будет нулевым, было ясно с самого начала, так как $\deg f(x) = 7$.

Эти же команды применимы к многочленам от нескольких переменных:

```
> f := (2 - x)*(y + x^2)*(y^2 - z);  
> coeff ( f, x, 2);
```

$$2y^2 - 2z$$

```
> coeff ( f, y, 1);
```

$$-(2-x)z$$

```
> degree( f, x); degree( f, y); degree( f, z);
```

$$3$$

$$3$$

$$1$$

Командой

$$\text{nops}(f)$$

можно выяснить количество слагаемых в выражении с одной переменной, т. е. в многочлене, который получится после выполнения предписанных действий, и, в частности, в самом еще не обработанном выражении f :

```
> f := (2 - x)*(z + x^2)*(x^2 - 3)^4 + (x - z)*(x + 2)^2 + 1:
> nops( f );
```

3

```
> nops(expand( f ));
```

22

В многочлене f , уже записанном как сумма одночленов, командой

$op(k, f)$

можно узнать k -е слагаемое. Если многочлен f еще не представлен в виде суммы одночленов, то можно предварительно воспользоваться командой $expand(f)$ для такого представления:

```
> f := (2 - x)*(1 + x^2)*(x - 3)^4 + (x - 1)*(x + 2)^2 + 1:
> expand(f);
```

$$230x^4 - 374x^3 + 381x^2 - 297x + 159 + 14x^6 - 79x^5 - x^7$$

```
> op(6, expand(f));
```

$14x^6$

```
> op(3, expand(f));
```

$381x^2$

С помощью той же команды можно исследовать и многочлен от нескольких переменных:

```
> f := (2 - x)*(z + x^2)*(x^2-3)^4 + (x - z)*(x + 2)^2 + 1:
> op(10, expand( f ));
```

$-217x^2z$

```
> op(22, expand( f ));
```

$12x^9$

```
> f3 := 3*x[1]^5*x[2]^2*x[3]^3 + 4*x[1]*x[2]^2*x[3]^2 +
x[1]^4*x[2]*x[3]^4 + x[1]^4*x[2]^2*x[3]^2+10;
```

$$f := 3x_1^5x_2^2x_3^3 + 4x_1x_2^2x_3^2 + x_1^4x_2x_3^4 + x_1^4x_2^2x_3^2 + 10$$

```
> op(4, f3);
```

$x_1^4x_2^2x_3^2$

```
> degree(f 3);
```

10

Командой

$op(f)$

выдаются все одночлены, входящие в многочлен f . Правда, для получения действительно одночленов необходимо привести многочлен к стандартному виду

```
> f := (2 - x)*(1+x^2)*(x- 3)^4+(x- 1)*(x+2)^2+1:
> op( f );
```

$(2-x)(1+x^2)(x-3)^4, (x-1)(x+2)^2, 1$

```
> op(expand( f ));
```

$230x^4, -374x^3, 381x^2, -297x, 159, 14x^6, -79x^5, -x^7$

```
> f := (2 - x)*(y^2 + x^2) + (x - y)*(x + 2)^2 + 1:
> op(expand( f ));
```

$2y^2, 6x^2, -xy^2, 4x, -yx^2, -4yx, -4y, 1.$

Если $f(x_1, x_2, \dots, x_n)$ — функция от переменных x_i и g_1, g_2, \dots, g_n — набор функций (некоторые из них или даже все могут совпадать с f), то команда

$subs(x_1 = g_1, x_2 = g_2, \dots, x_n = g_n, f)$

вычисляет суперпозицию $f(g_1, g_2, \dots, g_n)$. В частности, если g_i — константы, то будет вычислено значение f в точке:

```
> f := (2 - x)*(1 + x^2)*(x - 3) + (x - 1)*(x + 2)^2 + 1:
> subs(x = 5, f );
```

41

```
> subs(x = a, expand( f ));
```

$5a-9+6a^3-4a^2-a^4$

```
> subs(x = (x - a), expand( f ));
```

$5x-5a-9+6(x-a)^3-4(x-a)^2-(x-a)^4$

```
> f := x*x + y^3 + z;
```

$f := x^2 + y^3 + z$

```
> subs(x = f, y = f, z = 2, f) ;
```

$$(x^2 + (x^2 + y^3 + 2)^3 + 2)^2 + (x^2 + y^3 + 2)^3 + 2$$

```
> f := (2 - x)*(1 + x^2)*(x - 3) + (x - 1)*(x + 2)^2 + 1:
> subs(x = 5, f);
```

$$41$$

```
> subs(x = a, expand(f));
```

$$5a - 9 + 6a^3 - 4a^2 - a^4$$

```
> subs(x = (x - a), expand(f));
```

$$5x - 5a - 9 + 6(x - a)^3 - 4(x - a)^2 - (x - a)^4.$$

Впрочем, значение многочлена (и вообще любой функции) в точке можно найти и другими способами:

```
> f := z^2*x^3 + 6*z^2*x^2 + 9*z^2*x - z^2*y*x^2 -
6*z^2*y*x - 9*z^2*y;
> s := value(Eval(f, {x = 10, y = 20, z = 30}));
```

$$s := -1\,521\,000$$

Рассмотрим еще пару примеров таких вычислений. Первый пример многочлена над числовым множеством:

```
> f := z^2*x^3 + 6*z^2*x^2 + 9*z^2*x - z^2*y*x^2:
> Eval(f, x=5);
```

$$(z^2x^3 + 6z^2x^2 + 9z^2x - z^2yx^2) \Big|_{x=5}$$

```
> value(%);
```

$$320z^2 - 25z^2y,$$

а второй — над кольцом вычетов по модулю 10:

```
> Eval(x^7 + x + 1, x = 1) mod 10;
```

$$3$$

```
> Eval(x^2 + y, {x = 3, y = 2});
> value(%);
```

$$11$$

Кольцо многочленов от одного переменного над полем является евклидовым кольцом — в нем выполняется теорема о делении с остатком. Прежде чем выполнять деление, можно выяснить, не равен ли остаток от деления нулю, а уж затем с помощью команд

$$\text{rem}(f, g, x, 'q'); q$$

определить частное. Впрочем, команда

$$\text{quo}(f, g, x)$$

выдает частное сразу:

```
> divide(x^5 - 1, x- 1, 'q');
true
> q;
x^4 + x^3 + x^2 + x + 1
> f := x^5 + x^4 + x^3 + x - 1;
x^5 + x^4 + x^3 + x - 1
> g := x^3 + x^2 - x + 1;
x^3 + x^2 - x + 1
> divide(f, g, 'q');
false
> rem(f, g, x, 'q');
-3 + 3x - 3x^2
> q;
x^2 + 2
> rem(f, g, x, 'q');
-3 + 3x - 3x^2
> quo(f, g, x);
x^2 + 2.
```

9.4. Дифференцирование и интегрирование

В кольце функций (в том числе и полиномиальных), кроме арифметических операций, важны операции дифференцирования и ин-

тегрирования. Производная функции f по переменной x вычисляется по команде

$$\text{diff}(f, x).$$

Для вычисления n -й производной предназначена команда

$$\text{diff}(f, x\$n).$$

Перед вычислением производной с помощью команды

$$\text{diff}(f, x\$n)$$

можно просто записать поставленную задачу.

Найдем для примера частные производные f'_x, f'_y, f'_z функции

$$f(x, y, z) := (2 - z)(1 + x^2)(y - 3) + (x - 1)(y + 2)^2 + 1.$$

Производную функции f по переменной x сначала выпишем в виде постановки задачи:

$$> f := (2 - z) * (1 + x^2) * (y - 3) + (x - 1) * (y + 2)^2 + 1;$$

$$f := (2 - z)(1 + x^2)(y - 3) + (x - 1)(y + 2)^2 + 1$$

$$> g := \text{Diff}(f, x);$$

$$g := \frac{\partial}{\partial x}((2 - z)(1 + x^2)(y - 3) + (x - 1)(y + 2)^2 + 1)$$

$$> g := \text{diff}(f, x);$$

$$g := 2(2 - z)x(y - 3) + (y + 2)^2$$

$$> s := \text{diff}(f, y);$$

$$s := (2 - z)(1 + x^2) + 2(x - 1)(y + 2)$$

$$> t := \text{diff}(f, z);$$

$$t := -(1 + x^2)(y - 3)$$

Теперь найдем производные высших порядков для той же функции:

$$> g1 := \text{Diff}(f, x\$2); g2 := \text{Diff}(f, x, y);$$

$$g3 := \text{Diff}(f, x\$2, y); g4 := \text{Diff}(f, x\$2, y\$2);$$

$$g1 := \frac{\partial^2}{\partial x^2} f; g2 := \frac{\partial^2}{\partial x \partial x} f; g3 := \frac{\partial^3}{\partial y \partial x^2} f; g4 := \frac{\partial^4}{\partial y^2 \partial x^2} f$$

```
> f := (2 - z)*(1 + x^2)*(y - 3) + (x - 1)*(y + 2)^2 + 1;
> g1 := diff ( f, x$2); g2 := diff ( f, x, y);
g3 := diff ( f, x$2, y); g4 := diff ( f, x$2, y$2);
```

$$g1 := 2 (2 - z) (y - 3)$$

$$g2 := 2 (2 - z) x + 2 y + 4$$

$$g3 := 4 - 2 z$$

$$g4 := 0$$

Рассмотрим одно из важнейших применений оператора дифференцирования — нахождение экстремальных точек функции. Возьмем полиномиальную функцию от трех переменных

$$f(x, y, z) = -x^2 - y^2 - z^2 - x + xy + 2z$$

и найдем сначала ее критические точки. Для этого вычислим первые производные по каждой из переменных, приравняем эти производные к нулю и решим полученную систему уравнений:

```
> f := -x*x - y*y - z*z - x + x*y + 2*z;
f 1 := diff ( f, x); f 2 := diff ( f, y); f 3 := diff ( f, z);
solve({f 1 = 0, f 2 = 0, f 3 = 0}, {x, y, z});
```

$$f := -x^2 - y^2 - z^2 - x + xy + 2z$$

$$f1 := -2x - 1 + y$$

$$f2 := -2y + x$$

$$f3 := -2z + 2$$

$$\left\{ x = \frac{-2}{3}, y = \frac{-1}{3}, z = 1 \right\}.$$

Критическая точка найдена, с помощью матриц Гессе¹ определим ее характер. Для этого придется войти в подпакеты «Студент (Векторное числение)» и «Линейная алгебра»:

```
> with(Student [VectorCalculus]):
T := Hessian (f, [x, y, z]); T1 := Hessian (f, [x, y]);
```

$$T := \begin{bmatrix} -2 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & -2 \end{bmatrix}; T1 := \begin{bmatrix} -2 & 1 \\ 1 & -2 \end{bmatrix}$$

¹ Людвиг Отто Гессе (Hesse, 1811—1874) — немецкий математик, член Баварской академии наук (1868 г.), профессор Политехнической школы в Мюнхене (с 1869 г.). Понятие определителя Гессе (гессиана) введено в 1844 г.

```
> with (linalg): det (T1); det (T);
```

3

-6

Числа -2, 3, -6 образуют знакопеременную последовательность, следовательно, в точке $\left(\frac{-2}{3}, \frac{-1}{3}, 1\right)$ функция достигает максимального значения. Вычислим это значение:

```
> f:= -x*x - y*y - z*z - x + x*y + 2*z;
> subs(x = -2/3, y = -1/3, z = 1, f);
```

$\frac{4}{3}$

Напомним, что это не единственный способ определения характера экстремальной точки. Можно было просто вычислить характеристический многочлен гессиана T и найти его корни — собственные значения матрицы T :

```
> with(LinearAlgebra): CharacteristicPolynomial(T, x);
```

$6 + x^3 + 6x^2 + 11x$

```
> eigenvals(T);
```

-3, -2, -1

Все собственные значения матрицы T отрицательны, а это значит, что исследуемая точка является точкой максимума.

Отметим, что максимум полиномиальной функции f можно было найти с помощью команд

$\text{maximize}(f)$ или $\text{maximize}(f, \text{location})$.

Аналогично командами

$\text{minimize}(f)$ $\text{minimize}(f, \text{location})$

определяются минимальные значения функции f .

Проверим наши вычисления:

```
> f:= -x*x - y*y - z*z - x + x*y + 2*z;
> maximize( f );
```

$\frac{4}{3}$

> *maximize(f, location);*

$$\frac{4}{3}, \left\{ \left[\left\{ x = \frac{-2}{3}, y = \frac{-1}{3}, z = 1 \right\}, \frac{4}{3} \right] \right\}$$

Для вычисления неопределенного интеграла $\int f(x)dx$ используется команда

$$\text{int}(f, x).$$

По команде

$$\text{int}(f, x = a \dots b)$$

вычисляется определенный интеграл $\int_a^b f(x)dx$.

Перед вычислением можно записать интеграл в стандартном виде. Для примера запишем, а потом вычислим интегралы $\int_1^2 \cos x e^x dx$ и $\int_1^2 \cos x e^x dx$ сначала в аналитическом, а затем в числовом виде:

> *Int(cos(x)*exp(x), x);*

$$\int \cos x e^x dx$$

> *int(cos(x)*exp(x), x);*

$$\frac{1}{2}\cos(x)e^x + \frac{1}{2}\sin(x)e^x$$

> *Int(cos(x)*exp(x), x=1...2);*

$$\int_1^2 \cos x e^x dx$$

> *int(cos(x)*exp(x), x = 1...2);*

$$\frac{1}{2}\cos(1)e - \frac{1}{2}\sin(1)e + \frac{1}{2}\cos(2)e^2 + \frac{1}{2}\sin(2)e^2$$

> *int(cos(x)*exp(x), x = 1...2.);*

$$-0.05606592515$$

Значением предела интегрирования может быть и бесконечность (*infinity*), т. е. вычислить можно и значение несобственного интеграла. Например:

> Int(1 / (x^2), x = 1...infinity);

$$\int_1^{\infty} \frac{1}{x^2} dx$$

> int(1 / (x^2), x=1...infinity);

1

Подынтегральная функция может зависеть не только от одного переменного. При интегрировании функции

$$f(x, y, z) = -x^2 - y^2 - z^2 - x + xy + 2z$$

по одной из переменных остальные переменные будут восприниматься техникой как параметры:

> f := -x*x - y*y - z*z - x + x*y + 2*z;
> int(f, x);

$$(2-z)(y-3)\left(\frac{1}{3}x^3 + x\right) + (y+2)^2\left(\frac{1}{2}x^2 - x\right) + x$$

> int(f, z);

$$(1+x^2)(y-3)\left(2z - \frac{1}{3}z^2\right) + (x-1)(y+2)^2z + z$$

Рассмотрим пример дифференцирования и интегрирования не-полиномиальных функций:

> f := (sin(x)) ^ cos(Log(y));

$$f := \sin(x)^{\cos(\ln(y))}$$

> f [1] := Diff (f, x);

$$f_1 := \frac{\partial}{\partial x} \sin(x)^{\cos(\ln(y))}$$

> f [1] := diff ((sin(x)) ^ cos(Log(y)), x);

$$f := \sin(x)^{\cos(\ln(x))} \left(-\frac{\sin(\ln(x)) \ln(\sin(x))}{x} + \frac{\cos(\ln(x)) \cos(x)}{\sin x} \right)$$

> int(f [1], x);

$$\sin(x)^{\cos \ln(x)}$$

> int(f [1], x);

$$\sin(x)^{\cos \ln(x)}$$


```
> int(1 / log(x^2), x);
```

$$\int \frac{1}{\ln(x^2)} dx$$

Последний интеграл не берется в элементарных функциях; свою беспомощность компьютер демонстрирует тем, что просто переписывает задание синим цветом.

Однако есть еще возможность вычислить этот интеграл приближенно. Попробуем преобразовать подынтегральную функцию в многочлен с помощью команды

```
convert(f, polinom),
```

а затем проинтегрировать:

```
> f := 1 / log;  
> convert(f, polinom);
```

Error, unrecognized conversion

Не вышло, машина не всесильна. Есть еще вариант: команда

```
taylor(f, x = a, n)
```

должна выдать n членов разложения f в ряд Тейлора при $x = a$. Итак, разложим функцию f в ряд Тейлора:

```
> taylor(f, x = 1, 5);
```

Error, does not have a taylor expansion, try series()

Снова не получилось. Но на этот раз техника советует для разложения в ряд воспользоваться другой командой —

```
series(f, x = a, n).
```

На этот раз все получается. Появившийся ряд можно проинтегрировать:

```
> f1 := series(f, x = 1, 3);
```

$$f1 := \frac{1}{2}(x-1)^{-1} + \frac{1}{4} - \frac{1}{24}(x-1) + \frac{1}{48}(x-1)^2 + O((x-1)^3)$$

```
> int(f1, x);
```

$$\frac{1}{2}\ln(x-1) + \frac{1}{4}(x-1) - \frac{1}{48}(x-1)^2 + \frac{1}{144}(x-1)^3 + O((x-1)^4).$$

Кратные интегралы вычисляются повторным применением команды *int*. Продемонстрируем ее применение на примерах. По команде

value(%)

вычисляется значение предыдущего выражения:

> *Int(Int(x*y + x ^ 3, y), y);*

$$\iint xy + x^3 dy dy$$

> *value(%);*

$$\frac{1}{6}xy^3 + \frac{1}{2}x^3y^2$$

> *Int(Int(Int(x ^ 2*y ^ 2 + z ^ 3, x = 1.. 2), y = 3.. 4), z = 5.. 6);*

$$\int_5^6 \int_3^4 \int_1^2 x^2 y^2 + z^3 dx dy dz$$

> *value(%);*

$$\frac{7075}{36}.$$

Под интегрированием понимают также решение дифференциальных уравнений. Общее решение дифференциального уравнения *f* находится по команде

dsolve(f).

Найдем, например, общий интеграл линейного дифференциального уравнения второго порядка с правой частью:

$$y'' + 4y' - 5y = (16 - 12x)e^{-x} :$$

> *f := diff (y(x), x\$2) + 4*diff (y(x), x) - 5*y(x) = (16 - 12*x)*exp(-x);*

$$f = \left(\frac{d^2}{dx^2} y(x) \right) + 4 \left(\frac{d}{dx} y(x) \right) - 5y(x) = (16 - 12x)e^{-x}$$

> *dsolve(f);*

$$y(x) = e^{(-5x)} - C2 + e^x - C1 + \frac{1}{8}(-13 + 12x)e^{(-x)}.$$

Для демонстрации особенностей машинного решения задачи Коши также достаточно одного примера. Найдем частное решение дифференциального уравнения $y'' + y' + y = 4e^x$, удовлетворяющее начальным условиям: $y(0) = 4$; $y'(0) = -3$:

```
> dsolve({diff (y(x), x$2) + diff (y(x), x) + y(x) = 4*exp(x),
y(0) = 4, D(y) (0) = -3}, y(x));
```

$$y(x) = -2e^{\left(-\frac{x}{2}\right)} \sin\left(\frac{\sqrt{3}x}{2}\right) \sqrt{3} + \frac{8}{3}e^{\left(-\frac{x}{2}\right)} \cos\left(\frac{\sqrt{3}x}{2}\right) + \frac{4}{3}e^x.$$

Наконец, рассмотрим образец решения системы дифференциальных уравнений. Найдем сначала общее решение системы дифференциальных уравнений

$$\begin{cases} y'(x) + y(x) - x = z(x), \\ z'(x) = 2y(x) \end{cases}$$

машинным способом, а затем разыщем решение системы при начальных условиях $y(0) = 1$, $z(1) = 1$:

```
> dsolve({diff (y(x), x) + y(x) - x = z(x),
diff (z(x), x) = 2*y(x)});
```

$$\left\{ y(x) = \frac{1}{2}e^x - C_2 - e^{(-2x)} - C_1 - \frac{1}{2}, z(x) = e^x - C_2 + e^{(-2x)} - C_1 - \frac{1}{2} - x \right\}$$

```
> dsolve({diff (y(x), x) + y(x) - x = z(x),
diff (z(x), x) = 2*y(x), y(0) = 1, z(1) = 1});
```

$$\begin{cases} y(x) = \frac{1}{2} \frac{e^x (3e^{(-2)} + 5)}{2e + e^{(-2)}} + \frac{1}{2} \frac{e^{(-2x)} (-5 + 6e)}{2e + e^{(-2)}} - \frac{1}{2}, \\ z(x) = \frac{e^x (3e^{(-2)} + 5)}{2e + e^{(-2)}} - \frac{1}{2} \frac{e^{(-2x)} (-5 + 6e)}{2e + e^{(-2)}} - \frac{1}{2} - x \end{cases}.$$

Важной задачей в кольце функций от одного действительного переменного является интерполяция произвольной функции многочленом. Интерполяционный многочлен $f(x)$, который для различных значений x_i принимает заданные значения y_i , можно найти по машинной команде

$$\text{interp}([x_1, x_2, \dots, x_n], [y_1, y_2, \dots, y_n], x).$$

Найдем, например, интерполяционный многочлен $f(x)$ пятой степени по заданным шести значениям:

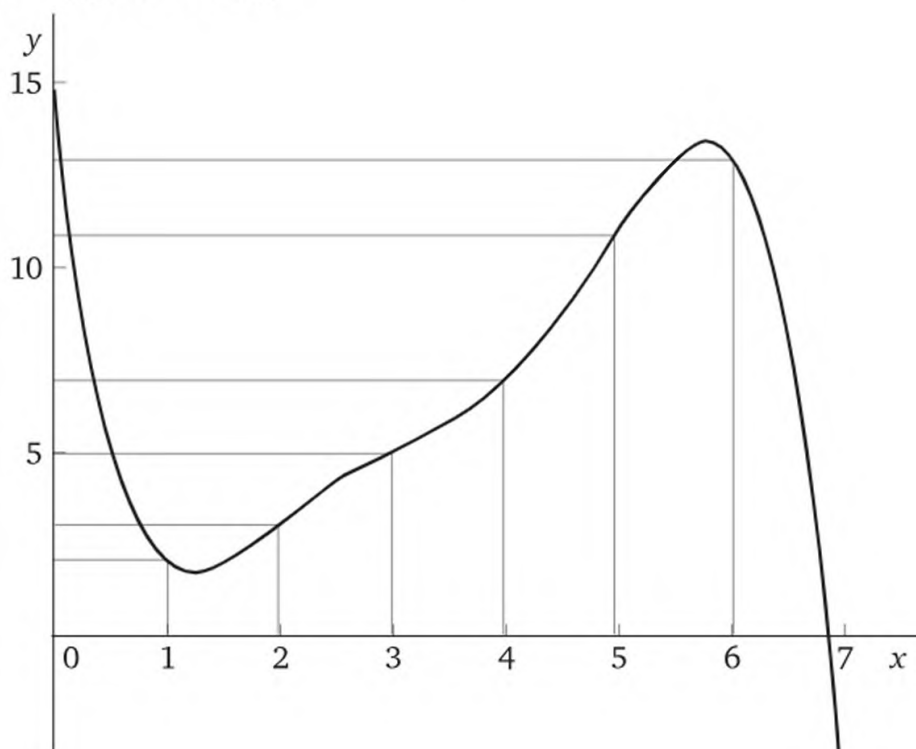
$$f(1) = 2, f(2) = 3, f(3) = 5, f(4) = 7, f(5) = 11, f(6) = 13.$$

Для наглядности сразу же с помощью машины построим график этого многочлена и непосредственно убедимся, что коэффициенты интерполяционного многочлена найдены верно:

```
> f := interp([1, 2, 3, 4, 5, 6], [2, 3, 5, 7, 11, 13], x);
```

$$f(x) = -\frac{3}{40}x^5 + \frac{5}{4}x^4 - \frac{187}{24}x^3 + \frac{91}{4}x^2 - \frac{437}{15}x + 15$$

```
> plot(f, x= 0..7);
```



Команда

$$linterp([x_1, x_2, \dots, x_n], [y_1, y_2, \dots, y_n], x) \bmod p$$

позволяет найти интерполяционный многочлен по значениям в данных точках с коэффициентами из конечного поля \mathbf{Z}_p классов вычетов по простому модулю p .

Например, для той же функции, но теперь уже не над числовым полем, а над полем \mathbf{Z}_{17} , получаем:

```
> Interp([1, 2, 3, 4, 5, 6], [2, 3, 5, 7, 11, 13], x) mod 17;
```

$$8x^5 + 14x^4 + 10x^2 + 6x + 15.$$

Напомним, что любая функция (от любого числа переменных) над конечным полем является *многочленом*.

Например, таковыми являются показательная функции и обратная к ней функция дискретного логарифмирования.

Рассмотрим числовой пример полиномиального представления показательной функции и функции дискретного логарифмирования над полем \mathbb{Z}_{17} .

Число 3 является первообразным по модулю 17. Вычислим все значения показательной функции

$$y \equiv 3^x \pmod{17}$$

и этим заодно проверим, что число 3 действительно является порождающим элементом циклической группы \mathbb{Z}_{17}^* :

```
> p := 17:
for i from 1 to p - 1 by 1 do
  print(irem(3^i, p)) : od;
```

39101351511161487412261

Теперь по этим точкам построим интерполяционный полином:

```
> X := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]:
> Y := [3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1]:
> f := Interp(X, Y, x);
```

$$f := 10x^{15} + 14x^{14} + 4x^{13} + 4x^{12} + 9x^{11} + 11x^{10} + 5x^9 + \\ + 5x^8 + 2x^7 + 12x^6 + 12x^5 + 11x^4 + 6x^3 + 13x^2 + 4x.$$

Многочлен, представляющий показательную функцию, найден. Сделаем на всякий случай проверку:

```
> p := 17: for i from 1 to p - 1 by 1 do
  print(irem((eval(f, x = i)), p)): od;
```

39101351511161487412261

Проверка подтвердила найденный результат.

Найдем теперь многочлен для обратной, т. е. логарифмической, функции

$$y \equiv \text{ind}_3 x \pmod{16}.$$

Для этого достаточно в командах поменять местами символы X и Y:

```
> Y := [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]:
> X := [3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1]:
> f1 := Interp(X, Y, x):
```

$$f1 := 10x^{15} + 16x^{14} + 3x^{13} + 11x^{12} + 14x^{11} + 12x^{10} + 13x^9 + \\ + 9x^8 + 5x^7 + 6x^6 + 4x^5 + 7x^4 + 15x^3 + 2x^2 + 8x.$$

Аналогичным образом можно найти полиномиальное представление для обращения дискретной экспоненты над любым конечным полем.

Обращение дискретной экспоненты над любым конечным полем является целой алгебраической функцией.

Для составного m в кольце \mathbb{Z}_m не каждая функция имеет полиномиальное представление. Число таких функций меньше числа всех функций над \mathbb{Z}_m , равного m^m .

Однако вполне может оказаться, что именно дискретное логарифмирование всегда можно выразить в виде некоторого многочлена.

Покажем, что это не так; например, с помощью техники увидим, что функция

$$y \equiv \text{ind}_2 x \pmod{\varphi(9)}$$

неполиномиальна над кольцом \mathbb{Z}_9 .

Слова «покажем» и «увидим» могут иметь в компьютерной алгебре не совсем обычный смысл. «Увидит» интересующее нас явление вычислительная техника, работая в пакете системы компьютерной математики *Maple*.

Нам лишь следует предварительно убедиться, что предложенная для этой работы программа работает корректно и поставленную задачу — увидеть все — действительно выполняет. Таким образом, доказательством математического утверждения явится *опыт*, а точнее, такой машинно-вычислительный эксперимент, который невозможно воспроизвести вручную.

Приступаем непосредственно к решению нашей задачи.

Число 2 — действительно первообразный элемент по модулю 9, и мультипликативная группа \mathbb{Z}_9^* составляет множество $\{2, 4, 8, 7, 5, 1\}$.

Неполиномиальность функции

$$y \equiv \text{ind}_2 x \pmod{6}$$

означает, что не существует многочлена $f(x)$ над \mathbb{Z}_9 такого, что

$$f(2) = 1, f(4) = 2, f(8) = 3, f(7) = 4, f(5) = 5, f(1) = 6.$$

Поскольку в \mathbb{Z}_9 выполняется тождество $x^8 = x^2$, все многочлены над \mathbb{Z}_9 степени выше седьмой редуцируются к многочленам седьмой степени. Число различных таких многочленов (которые вовсе не обязательно различны как функции) равно

$$9^8 = 43\,046\,721.$$

Составим программу (назовем ее *PROG 1*) для непосредственного перебора всех многочленов $f(x)$ степени не выше седьмой и вычисления второй строки таблицы значений.

X	0	1	2	3	4	5	6	7	8
$f(x)$	$f(0)$	$f(1)$	$f(2)$	$f(3)$	$f(4)$	$f(5)$	$f(6)$	$f(7)$	$f(8)$

Предложим технике сравнить полученную строку с некоторой заранее данной строкой Y и в случае совпадения выведем на экран соответствующий многочлен $f(X)$ и надпись «Полином найден». В работе программы используются операции над матрицами, поэтому, кроме вхождения в пакет «Теория чисел», придется войти в пакет «Линейная алгебра»:

PROG 1

```
> with(numtheory): with(linalg):
> m := 9 :
for j1 from 1 to m do : for j2 from 1 to m do :
for j3 from 1 to m do : for j4 from 1 to m do :
for j5 from 1 to m do : for j6 from 1 to m do :
for j7 from 1 to m do : for j8 from 1 to m do :
f := j1*x^7 + j2*x^6 + j3*x^5 + j4*x^4 + j5*x^3 + j6*x^2 + j7*
x + j8:
f := modp1(ConvertIn( f, x), 9);
for i from 0 to 9 do
a(i) := irem((eval(f, x = i)), m) : od :
X := matrix(1, 9, [a(0), a(1), a(2), a(3), a(4), a(5), a(6),
a (7), a(8)])):
if norm(evalm(X - Y)) = 0 then print('Полином_найден') :
print('f (x)' = f ) else fi od : od : od : od : od : od : od :
od :
```

Проверим сначала работу этой программы, предложив ей в качестве контрольного примера найти многочлен $f(x) = x$, т. е. положив

$$Y = [0, 1, 2, 3, 4, 5, 6, 7, 8].$$

Результатом начала работы по программе

$$Y := \text{matrix}(1, 9, [0, 1, 2, 3, 4, 5, 6, 7, 8]):$$

PROG 1

являются, в частности, многочлены:

$$\begin{aligned} &x, \\ &3x^3 + 7x, \\ &6x^3 + 4x, \\ &3x^4 + 5x^2 + x, \\ &3x^4 + 3x^3 + 6x^2 + 7x, \end{aligned}$$

$$\begin{aligned}
&3x^4 + 5x^3 + 6x^2 + 4x, \\
&6x^4 + 3x^2 + x, \\
&6x^4 + 3x^3 + 3x^2 + 7x, \\
&7x + 7x^2 + x^3 + x^4 + x^5 + x^6 + x^7.
\end{aligned}$$

Проверим правильность проведенных вычислений; для этого покажем, например, что в нашем кольце функция

$$y = 7x + 7x^2 + x^3 + x^4 + x^5 + x^6 + x^7$$

действительно тождественно совпадает с функцией $y = x$:

```

> with(numtheory): with(Linalg):
> f1 := x^7 + x^6 + x^5 + x^4 + x^3 + 7*x^2 + 7*x:

> m := 9: for i from 0 to m - 1 by 1 do
a(i) := irem((eval(f1, x = i)), m) : od:
X := matrix(1, 9, [a(0), a(1), a(2), a(3), a(4), a(5), a(6),
a(7), a(8)]);

```

$$X = [0, 1, 2, 3, 4, 5, 6, 7, 8].$$

Проверка состоялась. Кроме того, тождество

$$x^7 \equiv 3x + 2x^2 + 8x^3 + 8x^4 + 8x^5 + 8x^6 \pmod{9}$$

позволяет теперь понизить степень любого многочлена над кольцом \mathbb{Z}_9 до шестой степени и ниже.

Таким образом, число всех полиномиальных функций над \mathbb{Z}_9 не превышает числа $9^7 = 4\,782\,969$. Уменьшив возможную степень многочлена в *PROG 1*, мы ускорим работу по этой программе в девять раз. Поэтому внесем в *PROG 1* соответствующие изменения и в результате получим программу:

PROG 2

```

> with(numtheory):with(Linalg):
m := 9 :
for j1 from 1 to m do : for j2 from 1 to m do :
for j3 from 1 to m do : for j4 from 1 to m do :
for j5 from 1 to m do : for j6 from 1 to m do :
for j7 from 1 to m do :
f := j1*x^6 + j2*x^5 + j3*x^4 + j4*x^3 + j5*x^2 + j6*x + j7 :
f := modp1(ConvertIn(f, x), 9):
for i from 0 to 9 do
a(i) := irem((eval(f, x = i)), m) : od :
X := matrix(1, 9, [a(0), a(1), a(2), a(3), a(4), a(5), a(6),
a(7), a(8)]):
if norm(evalm(X - Y)) = 0 then print('Полином_найден') :
print('f(x)' = f) else fi od : od : od : od : od : od : od :

```

Программу *PROG 2* также можно проверить контрольными примерами и убедиться, что и она безошибочно выдает любой наперед заданный многочлен (кроме него, и другие, тождественно с ним равные).

Внесем теперь в *PROG 2* самые важные для нас изменения, а именно будем искать многочлен $f(x)$, у которого фрагмент таблицы значений имеет вид

X	2	4	8	7	5	1
$f(x)$	1	2	3	4	5	6

Сразу же введем и соответствующую матрицу Y . Итак:

PROG 3

```
> with(numtheory): with(linalg):
> Y := matrix(1, 6, [1, 2, 3, 4, 5, 6]):
m := 9 :
for j1 from 1 to m do : for j2 from 1 to m do :
for j3 from 1 to m do : for j4 from 1 to m do :
for j5 from 1 to m do : for j6 from 1 to m do :
for j7 from 1 to m do :
f := j1*x^6 + j2*x^5 + j3*x^4 + j4*x^3 + j5*x^2 + j6*x + j7 :
X := matrix(1, 6, [irem((eval(f, x = 2)), 9), irem((eval(f,
x = 4)), 9), irem((eval(f, x = 8)), 9),
irem((eval(f, x = 7)), 9), irem((eval(f, x = 5)), 9),
irem((eval(f, x = 1)), 9)]):
if norm(evalm(X - Y)) = 0 then print('полином_найден'):
print('f(x)' = f):
break else fi od: od: od: od: od: od: od:
```

После этого начинаем вычислительный эксперимент, результаты которого проверяет вычислительная техника без участия человека.

Полное время работы по программе *PROG 3* для вычислительной техники средних возможностей (*Intel Pentium 4*, CPU 3.01 ГГц, 2,00 ГБ ОЗУ) составляет около 20 000 с. За это время машина находит выражения всех 4 782 969 многочленов шестой степени с коэффициентами из кольца Z_9 , вычисляет значения этих многочленов в указанных шести точках, собирает эти значения в матрицу X и сравнивает X с заданной матрицей Y (т. е. производит более 30 млн арифметических операций).

Ни один из этих 4 782 969 многочленов не совпадает с функцией $y = \text{ind}_2 x$, поэтому работа программы не прерывается до самого конца, команда «*break*» не используется, и после окончания работы надпись «Полином_найден» на экране не появляется.

Это значит, что дискретный логарифм над кольцом Z_9 не представляется полиномом.

9.5. Корни многочленов и связанные с ними задачи

Найти рациональные корни многочлена $f(x)$ и их кратность можно с помощью команды

$$\text{roots}(f).$$

Например, многочлен $f(x)$ имеет корень 3 кратности 2, корень -1 кратности 2 и однократный (простой) корень -2 :

```
> f := x^5 - 2*x^4 - 10*x^3 + 8*x^2 + 33*x + 18;  
> roots( f );
```

$$[[3, 2], [-2, 1], [-1, 2]]$$

Тот же результат можно получить с помощью команды

$$\text{solve}(S, \{W\}),$$

где S — система уравнений или неравенств, содержащих неизвестные из множества W :

```
> f := x^5 - 2*x^4 - 10*x^3 + 8*x^2 + 33*x + 18;  
> solve( f = 0, x );
```

$$-2, -1, -1, 3, 3$$

Ответ будет еще нагляднее, если многочлен разложить на множители над полем рациональных чисел:

```
> f := x^5 - 2*x^4 - 10*x^3 + 8*x^2 + 33*x + 18;  
> factor( f );
```

$$(x+2)(x+1)^2(x-3)^2.$$

Команда

$$\text{realroot}(f, \epsilon)$$

позволяет найти действительные корни многочлена с точностью до ϵ . Определим интервалы, содержащие корни многочлена f , и заодно разложим этот многочлен на множители, чтобы точно знать, что это за корни:

```
> f := 4 + 24*x + 32*x^2 - 24*x^3 - 35*x^4 + 6*x^5 + 9*x^6;  
> realroot( f, 1/100 );
```

$$\left[\left[\frac{181}{128}, \frac{91}{64} \right], \left[\frac{-43}{128}, \frac{-21}{64} \right], \left[\frac{-91}{64}, \frac{-181}{128} \right] \right]$$


```
> factor( f );
```

$$(3x+1)^2(x^2-2)^2.$$

Разложение многочлена на неприводимые множители зависит от поля коэффициентов. Поле коэффициентов для многочлена с рациональными коэффициентами по умолчанию является поле рациональных чисел \mathbf{Q} . Поле \mathbf{R} действительных чисел (*real*), поле \mathbf{C} комплексных чисел (*complex*) или конечное поле \mathbf{Z}_p классов вычетов по простому модулю p указываются в команде разложения на множители.

Найдем, например, разложение многочлена f над полем рациональных чисел, затем над полем действительных чисел и над полем комплексных чисел. Наконец, разложим этот же многочлен на неприводимые множители над конечным полем из 11 элементов:

```
> f := -4 + 4*x + 3*x^4 - 3*x^5 - 1*x^6 + 1*x^7;
> factor( f );
```

$$(x^2-2)^2(1+x^2)(x-1)$$

```
> factor( f, real );
```

$$(x+1.414213562)^2(x-1.)(x-1.414213562)^2(x^2+1.00000000000)$$

```
> factor( f, complex);
```

$$(x+1.414213562)^2(x+1.00000000000I)(x^2+1.00000000000I)$$

$$(x-1.)(x-1.414213562)^2$$

```
> factor( f ) mod (11);
```

$$(x+9)(x^2+1)(x^2+8)^2.$$

Кольцо многочленов $P[x]$ с коэффициентами из поля P является кольцом главных идеалов (и даже евклидовым). Поэтому каждая пара многочленов $f(x)$, $g(x)$ имеет НОД и НОК, принадлежащие этому же кольцу $P[x]$.

В системе компьютерной алгебры *Maple* команда

$$\gcd(f, g)$$

для нахождения НОД многочленов f и g с числовыми коэффициентами составлена из первых букв слов *greatest common divisor* (наибольший общий делитель), т. е. соответствует русскому сокращению НОД.

Аналогично командой

$$\operatorname{lcm}(f, g),$$

составленной из первых букв слов *least common multiple* (наименьшее общее кратное), находится НОК (f, g) — наименьшее общее кратное многочленов.

Наименьшее общее кратное двух многочленов компьютер выдает в виде произведения на дополняющий множитель второго многочлена в записи $lcm(f, g)$. Таким образом, результаты команд $lcm(f, g)$ и $lcm(g, f)$ различны, если $f \neq g$. Разумеется, команда

$expand(s),$

раскрывающая скобки, все уравнивает.

Рассмотрим пример нахождения НОД и НОК многочленов:

$$f(x) = x^6 - 11x^5 + 46x^4 - 92x^3 + 99x^2 - 81x + 54,$$

$$g(x) = x^5 - 9x^4 + 29x^3 - 45x^2 + 54x - 54.$$

Вычисления сделаем двумя способами и проверим результат:

$> f := x^6 - 11*x^5 + 46*x^4 - 92*x^3 + 99*x^2 - 81*x + 54:$

$> g := x^5 + 29*x^3 - 9*x^4 - 45*x^2 + 54*x - 54:$

$> gcd(f, g);$

$$x^3 - 9x^2 + 27x - 27$$

$> lcm(f, g);$

$$(x^3 - 2x^2 + x - 2)(x^5 - 9x^4 + 29x^3 - 45x^2 + 54x - 54)$$

$> lcm(g, f);$

$$(x^2 + 2)(x^6 - 11x^5 + 46x^4 - 92x^3 + 99x^2 - 81x - 54).$$

Оказалось, что НОД (с точностью до числового ненулевого множителя) равен

$$x^3 - 9x^2 + 27x - 27,$$

а НОК —

$$(x^3 - 2x^2 + x - 2) \cdot g(x) = (x^2 + 2) \cdot f(x).$$

Представление НОК в виде произведения может оказаться и ненужным, тогда с помощью команды $expand$ можно сразу получить стандартное представление многочлена. Возьмем второе из представлений НОК многочленов f и g и сразу найдем его стандартное представление:

$> f := x^6 - 11*x^5 + 46*x^4 - 92*x^3 + 99*x^2 - 81*x + 54:$

$> g := x^5 + 29*x^3 - 9*x^4 - 45*x^2 + 54*x - 54:$

$> expand(lcm(f, g));$

$$x^8 - 11x^7 + 48x^6 - 114x^5 + 191x^4 - 265x^3 + 252x^2 - 162x + 108.$$

В кольце главных идеалов для любых элементов a, b выполняется равенство

$$(a, b) \cdot [a, b] = ab.$$

Проверим это тождество для нашего примера, не показывая промежуточных результатов, а лишь демонстрируя окончательное решение:

```
> f := x^6 - 11*x^5 + 46*x^4 - 92*x^3 + 99*x^2 - 81*x + 54:
> g := x^5 + 29*x^3 - 9*x^4 - 45*x^2 + 54*x - 54:
> a := expand(gcd(f, g)*lcm(g, f)):
> b := expand(f*g):
> a - b;
```

0

Пример совпадения этих двух произведений в кольце многочленов можно значительно обобщить.

Возьмем два произвольных многочлена: f степени не выше шестой и g степени не выше пятой. Машинным вычислением проверяется связь между наибольшим общим делителем и наименьшим общим кратным:

```
> f := a0*x^6 + a1*x^5 + a2*x^4 + a3*x^3 + a4*x^2 + a5*x + a6:
> g := b0*x^5 + b1*x^3 + b2*x^4 + b3*x^2 + b4*x + b5:
> a := expand(gcd(f, g)*lcm(g, f)):
> b := expand(f*g):
> a - b;
```

0

Если $d(x)$ — наибольший общий делитель многочленов $f(x)$ и $g(x)$ с коэффициентами, то в кольце $P[x]$ найдутся многочлены $u(x)$ и $v(x)$ такие, что

$$f(x) \cdot u(x) + g(x) \cdot v(x) = d(x).$$

Это равенство называется линейным разложением НОД.

Чтобы найти линейное разложение, можно левую и правую части равенства сократить на $d(x)$. Тогда исходные многочлены будут заменены на взаимно простые:

$$f_0(x) = \frac{f(x)}{d(x)}, \quad g_0(x) = \frac{g(x)}{d(x)},$$

а разложение будет иметь вид

$$f_0(x) \cdot u(x) + g_0(x) \cdot v(x) = 1.$$

Степени многочленов $u(x)$ $v(x)$ можно оценить сверху —

$$\deg u(x) < \deg g_0(x),$$

$$\deg v(x) < \deg f_0(x),$$

поэтому при разыскании линейного разложения вручную можно воспользоваться методом неопределенных коэффициентов.

Попробуем найти этим методом линейное разложение НОД многочленов:

$$f_0(x) = x^3 - 2x^2 + x - 2,$$

$$g_0(x) = x^2 + 2.$$

Сначала проверим, что эти многочлены действительно взаимно просты:

```
> f [0] := x^3 - 2*x^2 + x - 2:
> g [0] := x^2 + 2:
> gcd ( f [0], g[0] );
```

1

Теперь составим многочлен $s(x)$, в котором с неопределенными пока коэффициентами участвуют искомые многочлены-множители:

$$s(x) = (x^3 - 2x^2 + x - 2)(a_0x + a_1) + (x^2 + 2)(b_0x^2 + b_1x + b_2).$$

Теперь нужно раскрыть скобки в выражении для s , затем собрать одинаковые степени переменного x и приравнять все коэффициенты, кроме свободного члена, к нулю. Выражение для свободного члена приравнивается к единице. Заранее известно, что получившаяся система уравнений имеет решение, и оно единственно.

Скобки в многочлене s раскрываются с помощью команды *expand(s)*. Команда *collect(s, x)* собирает одинаковые степени переменного x и одновременно упорядочивает многочлен по убыванию степеней x . Однако для решения нашей задачи можно просто командой

$$\text{coeff}(s, x, n)$$

выписать коэффициенты у одночленов x^n из многочлена $s(x)$, составить систему уравнений с искомыми неопределенными коэффициентами и решить ее, используя команду *solve*:

```
> f [0] := x^3 - 2*x^2 + x - 2:
> g [0] := x^2 + 2:
> s := f [0]*(a0*x + a1) + g[0]*(b0*x^2 + b1*x + b2):
> solve({coeff (s, x, 0) = 1, coeff (s, x, 1) = 0,
coeff (s, x, 2) = 0, coeff (s, x, 2) = 0,
```

$\text{coeff}(s, x, 3) = 0, \text{coeff}(s, x, 4) = 0\},$
 $\{a0, a1, b0, b1, b2\});$

$$\left\{ b0 = \frac{-1}{6}, b2 = \frac{5}{6}, b1 = 0, a1 = \frac{1}{3}, a0 = \frac{1}{6} \right\}.$$

Коэффициенты искоемых множителей линейного разложения

$$f_0(x) \cdot u(x) + g_0(x) \cdot v(x) = 1$$

найденны:

$$u(x) = \frac{1}{6}x + \frac{1}{3}, \quad v(x) = -\frac{1}{6}x^2 + \frac{5}{6}.$$

Сделаем, на всякий случай, проверку:

```
> f [0] := x^3 - 2*x^2 + x - 2;
> g [0] := x^2 + 2;
> u := 1/6*x + 1/3;
> v := -1/6*x^2 + 0*x + 5/6;
> expand ( f [0]*u + g [0]*v);
```

1

Поскольку НОД (и НОК) определены с точностью до ассоциированности, т. е. до ненулевого числового множителя, можно «для красоты» оба найденных многочлена умножить на 6. Тогда:

$$\begin{aligned} u(x) &= x + 2, \\ v(x) &= -x^2 + 5, \\ f_0(x) \cdot u(x) + g_0(x) \cdot v(x) &= 6. \end{aligned}$$

Вернемся к многочленам $f(x)$ и $g(x)$ из первого примера:

$$\begin{aligned} f(x) &= x^6 - 11x^5 + 46x^4 - 92x^3 + 99x^2 - 81x + 54, \\ g(x) &= x^5 - 9x^4 + 29x^3 - 45x^2 + 54x + 54. \end{aligned}$$

Эти многочлены не взаимно просты, поэтому для нахождения линейного разложения наибольшего общего делителя сначала разделим каждый на их наибольший общий делитель:

```
> f := x^6 - 11*x^5 + 46*x^4 - 92*x^3 + 99*x^2 - 81*x + 54;
> g := x^5 - 9*x^4 + 29*x^3 - 45*x^2 + 54*x - 54;
> f [0] := quo ( f, gcd ( f, g), x);
```

$$f_0 := x^3 - 2x^2 + x - 2$$

```
> g [0] := quo ( g, gcd ( f, g), x);
```

$$g_0 := x^2 + 2.$$

Получились уже знакомые нам многочлены f_0 и g_0 . Это значит, что искомое представление наибольшего общего делителя в «красивом варианте» (т. е. без дробных коэффициентов) имеет вид

$$f(x) \cdot (x+2) + g(x) \cdot (x^2+5) = 6(x^3 - 9x^2 + 27x - 27).$$

Рассмотренный способ нахождения линейного разложения наибольшего общего делителя не единственный.

Понятие цепной дроби можно ввести в любом евклидовом кольце K и точно так же, как в кольце целых чисел, использовать их свойства для решения неопределенных уравнений в кольце K .

Если элементы a, b из евклидова кольца взаимно просты, то обыкновенную дробь $\frac{a}{b}$ можно представить в виде цепной дроби:

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \dots \frac{1}{q_{n-1} + \frac{1}{q_n}}}}.$$

Обыкновенную дробь $\frac{P_i}{Q_i}$, получившуюся в результате «сворачивания» начального куска цепной дроби, называют *подходящей*.

С помощью команды

$$\text{cfrac}(f)$$

рациональная дробь f получает представление в виде цепной дроби. Для вычисления цепной дроби необходимо войти в пакет «Теория чисел». Командой

$$\text{nthconver}(f, n)$$

вызывается n -я подходящая дробь. Можно отдельно найти числитель и знаменатель подходящей дроби. Команда

$$\text{nthnumer}(f, n)$$

выдает числитель n -й подходящей дроби для цепной дроби f , а по команде

$$\text{nthdenom}(f, n)$$

вычисляется знаменатель n -й подходящей дроби.

Особенности таких поисков (точно таких же, как в кольце целых чисел) видны из примера:

```
> with(numtheory):
> f := 11*x^5 - 46*x^4 + 92*x^3 - 99*x^2 + 81*x - 54 - x^6;
```

$$f := 11x^5 - 46x^4 + 92x^3 - 99x^2 + 81x + 54 - x^6$$

```
> g := x^5 + 29*x^3 - 9*x^4 - 45*x^2 + 54*x - 54;
```

$$g := x^5 - 29x^3 - 9x^4 - 45x^2 + 54x - 54$$

```
> a := cfrac (f / g);
```

$$a := -x + 2 + \frac{1}{x + 2 + \frac{1}{\frac{1}{6}x - \frac{1}{3}}}$$

```
> nthconver(a, 2);
```

$$\frac{-\frac{1}{6}x^3 + \frac{1}{3}x^2 - \frac{1}{6}x + \frac{1}{3}}{\frac{1}{6}x^2 + \frac{1}{3}}$$

```
> nthnumer(a, 2);
```

$$-\frac{1}{6}x^3 + \frac{1}{3}x^2 - \frac{1}{6}x + \frac{1}{3}$$

```
> nthdenom(a, 2);
```

$$\frac{1}{6}x^2 + \frac{1}{3}.$$

Каждая подходящая дробь несократима, и, начиная с $i = 1$, числители и знаменатели двух последовательных подходящих дробей связаны равенством

$$\begin{vmatrix} P_{i-1} & P_i \\ Q_{i-1} & Q_i \end{vmatrix} = (-1)^i.$$

Последняя подходящая дробь — это (с точностью до ассоциированности) исходная обыкновенная дробь $\frac{a}{b}$. Поэтому $P_n = a$, $Q_n = b$.

Тогда

$$\begin{vmatrix} a & P_{n-1} \\ b & Q_{n-1} \end{vmatrix} = (-1)^n.$$

Отсюда

$$aQ_{n-1}(-1)^n + bP_{n-1}(-1)^{n+1} = 1.$$

Таким образом, для решения неопределенного уравнения

$$f_0(x) \cdot u(x) + g_0(x) \cdot v(x) = 1,$$

где «неизвестными» являются многочлены $u(x)$ и $v(x)$, достаточно разложить обыкновенную дробь $\frac{f_0(x)}{g_0(x)}$ в цепную и воспользоваться свойствами числителя и знаменателя подходящих дробей.

Найдем многочлены $u(x)$ и $v(x)$ с помощью разложения обыкновенной дроби $\frac{f_0(x)}{g_0(x)}$ в цепную дробь:

```
> f[0] := x^3 - 2*x^2 + x - 2;
> g[0] := x^2 + 2;
> with(numtheory):
> a := cfrac( f[0] / g[0] );
```

$$a := x - 2 + \frac{1}{-x - 2 + \frac{1}{-\frac{1}{6}x + \frac{1}{3}}}.$$

Видно, что длина полученной цепной дроби, изображающей обыкновенную дробь $\frac{f_0(x)}{g_0(x)}$, равна двум. Это значит, что числитель второй подходящей дроби с точностью до числового множителя равен f_0 , а знаменатель равен g_0 . Проверяем:

```
> f[0] := x^3 - 2*x^2 + x - 2;
> g[0] := x^2 + 2;
> with(numtheory):
> a := cfrac(f[0] / g[0]);
> nthnumer (a, 2);
```

$$\frac{1}{6}x^3 - \frac{1}{3}x^2 + \frac{1}{6}x - \frac{1}{3}$$

```
> nthdenom(a, 2);
```

$$\frac{1}{6}x^2 + \frac{1}{3}$$

С точностью до числового множителя появились исходные многочлены.

Чтобы найти $u(x)$ и $v(x)$, нужно сначала определить числитель и знаменатель предпоследней подходящей дроби:

```
> f[0] := x^3 - 2*x^2 + x - 2;
> g[0] := x^2 + 2;
```

```
> with(numtheory):
> a := cfrac(f[0] / g[0]):
> nthnumer (a, 1);
```

$$-x^2 + 5$$

```
> nthdenom(a, 1);
```

$$-x - 2$$

Для окончательного решения теперь достаточно умножить многочлен, изображающий знаменатель первой подходящей дроби, на поправочный коэффициент $(-1)^1 = -1$.

Чтобы в линейном разложении НОД находились исходные многочлены $f_0(x)$ и $g_0(x)$, а не ассоциированные с ними, множитель $\frac{1}{6}$ можно переместить в многочлены $u(x)$ и $v(x)$ или просто умножить левую и правую части равенства на число 6.

Отметим, что все предыдущие способы вычислений скорее ручные, чем машинные. При таких вычислениях видна вся теоретическая основа явления, а техника используется лишь для рутинных преобразований. Однако техника может сразу назвать ответ без промежуточных результатов. Для нахождения НОД двух многочленов $f(x)$, $g(x)$ и его линейного разложения

$$(f(x), g(x) = f(x)u(x) + g(x)v(x)$$

используется машинная команда

$$gcdex(f, g, x, 'u', 'v').$$

Проверим наши машинно-ручные вычисления еще раз:

```
> with(numtheory):
> f := x^6 - 11*x^5 + 46*x^4 - 92*x^3 + 99*x^2 - 81*x + 54:
> g := x^5 + 29*x^3 - 9*x^4 - 45*x^2 + 54*x - 54:
> gcdex(f, g, x, 'u', 'v');
```

$$-27 + x^3 - 9x^2 + 27x$$

```
> u; v;
```

$$\frac{1}{6}x + \frac{1}{3}$$

$$-\frac{x^2}{6} + \frac{5}{6}$$

```
> # проверка
> expand (f*u+g*v);
```

$$-27 + x^3 - 9x^2 + 27x$$

Кольцо многочленов от нескольких переменных над полем тоже гауссово, поэтому в этом кольце любая пара многочленов тоже имеет НОД и НОК. Правда, в таком кольце есть неглавные идеалы, поэтому НОД уже не обладает линейным разложением.

Найдем НОД и НОК двух многочленов от трех переменных и для контроля разложим эти многочлены на неприводимые множители:

```
> f := z^2*x^3 + 6*z^2*x^2 + 9*z^2*x - z^2*y*x^2 -
6*z^2*y*x - 9*z^2*y;
> g := z*x^4 + 9*z*x^3 + 27*z*x^2 + 27*z*x - z*y*x^3 -
9*z*y*x^2 - 27*z*y*x - 27*z*y;
> gcd( f, g);
```

$$(x-y)z(x+3)^2$$

```
> lcm( f, g);
```

$$z^2(x-y)(x+3)^3$$

```
> factor(g); factor( f );
```

$$(x-y)z(x+3)^3$$

$$(x-y)z^2(x+3)^2$$

Функцию, представленную в виде отношения двух многочленов

$$y = \frac{w(x)}{s(x)},$$

принято называть дробно-рациональной (или просто рациональной). Если $\deg w < \deg s$, то функция называется *правильной*. Каждая рациональная функция является суммой многочлена и правильной функции.

Дробно-рациональная функция вида

$$y = \frac{g(x)}{[f(x)]^k},$$

где $f(x)$ — неприводимый многочлен, а $\deg f(x) < \deg g(x)$, называется *элементарной* (или простейшей) *дробью*.

Каждая правильная рациональная функция может быть представлена в виде суммы элементарных дробей.

Неприводимость или приводимость многочлена зависит от исходного поля, поэтому и свойство элементарности дроби также зависит от поля коэффициентов.

Многочлен первой степени неприводим над любым полем, поэтому если знаменатель дроби имеет вид $(x-a)^k$, то элементарная дробь в представлении для $\frac{g(x)}{(x-a)^k}$ будет иметь вид

$$\frac{g(x)}{(x-a)^k}$$

$$\frac{b}{(x-a)^k},$$

где b — элемент из поля коэффициентов. Такое представление можно найти, используя разложение многочлена $g(x)$ по степеням $(x-a)$.

Вручную такое разложение проще всего найти с помощью схемы Горнера; однако машинная команда

$$\text{convert}(f, \text{horner}, x)$$

лишь осуществляет расстановку скобок для вычисления значения многочлена с наименьшим числом операций. Например:

```
> f := 6*x^6 + 5*x^5 - 4*x^4 + 3*x^3 - 2*x^2 + 8*x - 9;
```

$$f := 6x^6 + 5x^5 - 4x^4 + 3x^3 - 2x^2 + 8x - 9$$

```
> f := convert(f, horner, x);
```

$$f := -9 + (8 + (-2 + (3 + (-4 + (5 + 5x)x)x)x)x)x$$

Разложение многочлена по степеням $(x-a)$ в машинном варианте дает любая из двух команд:

$$\text{taylor}(g, x = a, n)$$

или

$$\text{series}(g, x = a, n),$$

где n — число членов ряда.

Для многочлена такое представление будет точным, если число членов ряда равно степени многочлена $g(x)$, увеличенной на единицу, т. е. $\deg g(x) + 1$. Степень многочлена g определяет команда $\text{degree}(g)$.

Представим в виде суммы простейших дробей дробь

$$\frac{4x^4 - 3x^3 + 2x^2 - x + 10}{(x-2)^7}.$$

Для этого разложим многочлен, стоящий в числителе, по степеням $(x-2)$:

```
> f := 4*x^4 - 3*x^3 + 2*x^2 + 10;
```

```
> f1 := taylor ( f, x = 2, degree ( f ) + 1);
```

$$f1 := 58 + 100(x-2) + 80(x-2)^2 + 29(x-2)^3 + 4(x-2)^4$$

> f 1 / (x- 2)^7;

$$\frac{58+100(x-2)+80(x-2)^2+29(x-2)^3+4(x-2)^4}{(x-2)^7}$$

После этого вычисления несложно закончить вручную:

$$\frac{f1(x)}{(x-2)^7} = \frac{58}{(x-2)^7} + \frac{100}{(x-2)^6} + \frac{80}{(x-2)^5} + \frac{29}{(x-2)^4} + \frac{4}{(x-2)^3}.$$

Впрочем, можно обойтись и без ручных вычислений. В системе компьютерной алгебры *Maple* есть универсальная команда для представления дробно-рациональной функции в виде суммы элементарных дробей.

По команде

$$\text{convert}(d, \text{parfrac}, x)$$

компьютер выдает представление дробно-рациональной функции $d(x)$ в виде суммы элементарных дробей (если речь идет о символьных вычислениях, то неприводимость понимается над полем рациональных чисел, а если вычисления числовые, т. е. приближенные, то над полем действительных чисел).

Проверим наши машинно-ручные вычисления:

> f := 4*x^4 - 3*x^3 + 2*x^2 + 10;
> convert(f/(x - 2)^7, parfrac, x);

$$58 \frac{1}{(x-2)^7} + \frac{100}{(x-2)^6} + \frac{80}{(x-2)^5} + \frac{29}{(x-2)^4} + \frac{4}{(x-2)^3}.$$

Если многочлены $f(x)$ и $g(x)$ взаимно просты, то линейное разложение нормального делителя принимает вид

$$f(x) \cdot u(x) + g(x) \cdot v(x) = 1.$$

где $u(x)$ и $v(x)$ принадлежат тому же кольцу многочленов, что $f(x)$ и $g(x)$.

Разделив левую и правую части этого равенства на $f(x) \cdot g(x)$, получим

$$\frac{1}{f(x)g(x)} = \frac{u(x)}{g(x)} + \frac{v(x)}{f(x)}.$$

Если $f(x)$ и $g(x)$ неприводимы над рассматриваемым полем, то дроби $\frac{u(x)}{g(x)}$ и $\frac{v(x)}{f(x)}$ будут простейшими.

В этом случае с помощью нахождения разложения правильной дроби

$$\frac{1}{f(x) \cdot g(x)}$$

можно найти линейное разложение НОД многочленов $f(x) \cdot d(x)$ и $g(x) \cdot d(x)$.

Например, многочлены

$$\begin{aligned} f(x) &= x^4 - x^3 + x^2 + 1, \\ g(x) &= x^3 - 3x^2 + 1 \end{aligned}$$

неприводимы над полем рациональных чисел: команда *factor* (*d*), выдающая разложение многочлена $d(x)$ над полем рациональных чисел, оставляет эти многочлены неизменными:

```
> f := x^4 - x^3 + x^2 + 1;
> factor ( f );
```

$$x^4 - x^3 + x^2 + 1$$

```
> g := x^3 - x^2 - 2*x^2 + 1;
> factor ( g );
```

$$x^3 - 3x^2 + 1.$$

Для таких многочленов быстрый способ нахождения линейного разложения НОД подходит:

```
> f := x^4 - x^3 + x^2 + 1;
> g := x^3 - x^2 - 2*x^2 + 1;
> convert (1/ (f *g), preface, x);
```

$$\frac{1}{109} \frac{28-10x+16x^2+13x^3}{x^4-x^3+x^2+1} - \frac{1}{109} \frac{-81-10x+13x^2}{x^3-3x^2+1}.$$

Таким образом, если

$$u(x) = -\frac{1}{109}(-81-10x+13x^2),$$

$$v(x) = \frac{1}{109}(28-10x+16x^2+13x^3),$$

то

$$f(x) \cdot u(x) + g(x) \cdot v(x) = 1.$$

Многочлен $f_0(x) = x^3 - 2x^2 + x - 2$ приводим над полем рациональных чисел:

```
> f [0] := x^3 - 2*x^2 + x - 2;
> factor ( f[0] );
```

$$(x-2)(x^2+1).$$

Поэтому при представлении дроби

$$\frac{1}{f_0(x) \cdot g_0(x)}$$

в виде суммы простейших дробей в знаменателях появятся не $f_0(x)$, а многочлены $(x-2)$ и (x^2+1) . Однако их нетрудно снова собрать вместе, достаточно выполнить сложение этих дробей.

Найдем снова линейное разложение НОД многочленов

$$\begin{aligned} f_0(x) &= x^3 - 2x^2 + x - 2, \\ g_0(x) &= x^2 + 2 \end{aligned}$$

теперь уже с помощью разложения рациональной функции

$$\frac{1}{f_0(x) \cdot g_0(x)}$$

в сумму простейших дробей. Для сложения дробей воспользуемся командой

$$\text{simplify}(F),$$

предназначенной для упрощения выражений:

```
> f [0] := x^3 - 2*x^2 + x - 2;
> g[0] := x^2 + 2;
> convert(1/(f[0] * g[0]), parfrac, x);
```

$$\frac{1}{30} \frac{1}{x-2} - \frac{1}{5} \frac{x+2}{x^2+1} + \frac{1}{6} \frac{(x+2)}{x^2+2}$$

```
> simplify(1/30*1/(x-2) - 1/5*(x+2)/(x^2+1));
```

$$-\frac{1}{6} \frac{x^2-5}{(x-2)(x^2+1)}$$

Полученный результат означает, что

$$\frac{1}{f_0(x) \cdot g_0(x)} = -\frac{1}{6} \frac{x^2-5}{(x-2)(x^2+1)} + \frac{1}{6} \frac{(x+2)}{x^2+2}.$$

Отсюда следует, что линейное разложение НОД многочленов f_0 и g_0 получено:

$$\frac{1}{6}(x+2) \cdot f_0(x) - \frac{1}{6}(x^2-5) \cdot g_0(x) = 1.$$

Разложение дроби в сумму простейших основано на том, что кольцо многочленов от одного переменного является кольцом главных идеалов.

Поскольку в кольце многочленов от нескольких переменных содержатся неглавные идеалы, не каждую дробь из $P(x, y)$ удастся представить в виде суммы простейших.

С рациональными функциями связана еще одна задача — освобождение от иррациональности в знаменателе.

Задачу нахождения такого многочлена $v(x)$, что

$$\frac{1}{g(\alpha)} = v(\alpha),$$

где α — корень неприводимого многочлена $f(x)$, называют освобождением от алгебраической иррациональности в знаменателе дроби $\frac{1}{g(\alpha)}$ (говорят еще «уничтожение иррациональности»).

Многочлены $f(x)$, $g(x)$ взаимно простые, иначе $g(\alpha) = 0$.

Найти нужный многочлен $v(x)$ можно с помощью линейного разложения НОД

$$u(x)f(x) + v(x)g(x) = 1.$$

Например, такое разложение уже было найдено ранее для многочленов

$$\begin{aligned} f_0(x) &= x^3 - 2x^2 + x - 2, \\ g_0(x) &= x^2 + 2, \end{aligned}$$

из него получаем

$$v := \frac{28}{109} - \frac{10}{109}\alpha + \frac{16}{109}\alpha^2 + \frac{13}{109}\alpha^3.$$

Освободиться от иррациональности можно и другим, более прямым способом.

Командой

$$\text{alias}(\alpha = \text{RootOf}(f))$$

символом α обозначим корень многочлена f , затем с помощью команды

$$\text{subs}(x = \alpha, g)$$

подставим в $g(x)$ элемент α вместо x . После этого команда

$$\text{evala}(\text{Expand}(1/g1))$$

произведет вычисления по модулю идеала, порожденного многочленом $f(x)$, в кольце $\mathbf{Q}[x]$:

```
> f := x^4 - x^3 + x^2 + 1; g := x^3 - x^2 - 2*x^2 + 1;
> gcd(f, g);
```

$$1$$

```
> alias(alpha = RootOf(f));
> g1 := subs(x = alpha, g);
```

$$g1 := \alpha^3 - 3\alpha^2 + 1$$

```
> evala(Expand(1/g1));
```

$$\frac{28}{109} - \frac{10}{109}\alpha + \frac{16}{109}\alpha^2 + \frac{13}{109}\alpha^3.$$

Рассмотрим еще два примера уничтожения иррациональности. С помощью команды

$$\text{rationalize}(s)$$

освободимся от иррациональности в знаменателях дробей

$$\frac{1}{\sqrt{2} + \sqrt{5} + \sqrt{3}} \text{ и } \frac{1}{\sqrt[3]{2} + \sqrt[3]{3} + 1}:$$

```
> s1 := 1/(sqrt(2) + sqrt(5) + sqrt(3));
```

$$s1 := \frac{1}{\sqrt{2} + \sqrt{5} + \sqrt{3}}$$

```
> rationalize(s1);
```

$$\frac{1}{12}(\sqrt{2} + \sqrt{3} - \sqrt{5})\sqrt{2}\sqrt{3}$$

```
> expand( %);
```

$$\frac{\sqrt{3}}{6} + \frac{\sqrt{2}}{4} - \frac{\sqrt{2}\sqrt{3}\sqrt{5}}{12}$$

```
> s2 := 1/(2^(1/3) + 1 + 3^(1/3));
```

$$s2 := \frac{1}{2^{(1/3)} + 1 + 3^{(1/3)}}$$

```
> expand(rationalize(s2));
```

$$\frac{2^{(2/3)}}{6} + \frac{2^{(1/3)}}{3} - \frac{1}{3} - \frac{3^{(1/3)}2^{(1/3)}}{3} + \frac{3^{(1/3)}2^{(2/3)}}{6} + \frac{3^{(2/3)}}{3} - \frac{3^{(2/3)}2^{(2/3)}}{6}.$$

Корни многочлена $f(x)$ выражаются через его коэффициенты с помощью полевых операций и извлечения корней различных степеней тогда и только тогда, когда группа Галуа этого многочлена разрешима.

В случае, когда такое выражение существует, говорят: уравнение $f(x) = 0$ разрешимо в радикалах. Техника позволяет выяснить, разрешимо или нет в радикалах уравнение степени не выше девятой.

Из того, что подгруппа разрешимой группы разрешима, и из разрешимости группы S_4 следует, что уравнения, степень которых не выше четвертой, разрешимы в радикалах.

Впрочем, можем провести численный эксперимент и убедиться в этом непосредственно. Покажем, например, что уравнение

$$x^4 - 5x + 1 = 0$$

разрешимо в радикалах. Для исследования группы Галуа многочлена f , которая появляется по команде

$galois(f),$

придется войти в пакет «Теория групп»:

```
> f := x^4 - 5*x + 1:
> galois( f );
```

«4T5», {“S(4)”}, “-”, 24, {“(1 4)”, “(2 4)”, “(3 4)”}

```
> with(group):
> G := permgroup(4, {[[1, 4]], [[2, 4]], [[3, 4]]}):
> DerivedS(G);
```

$permgroup(4, \{[[1, 4]], [[2, 4]], [[3, 4]]\}),$

$permgroup(4, \{[], [[1, 3, 4]], [[2, 3, 4]]\}),$

$permgroup(4, \{[], [[1, 2], [3, 4]], [[1, 3], [2, 4]]\}),$

$permgroup(4, \{[]\})]$

По команде $galois$ машина выдала:

1) имя группы (в нашем случае — 4T5, что означает «четырежды транзитивная группа степени 5»);

2) симметрическую группу S_4 , подгруппой которой является данная группа Галуа;

3) знак четности («+» — четная, «-» — нечетная), наша группа нечетная;

4) порядок группы;

5) порождающие элементы группы Галуа.

Ряд последовательных коммутантов группы Галуа нашего уравнения дошел до единичной подгруппы, а это значит, что уравнение разрешимо в радикалах.

Посмотрим теперь, разрешимо ли уравнение

$$x^5 - 5x + 1 = 0$$

в радикалах:

```
> f:= x^5 - 5*x+ 1:
> galois(f);

«5T5», {«S(5)»}, «-», 120, {«(1 5)», «(2 5)», «(3 5)», «(4 5)»}

> with(group):
> G := permgroup(5, {[[4, 5]], [[3, 5]], [[1, 5]], [[2, 5]]}):
> group[DerivedS](G);
```

[permgroup (5, {[[1, 2]], [[1, 2, 3, 4, 5]]}),

permgroup (5, {[[], [[1, 2, 3]], [[2, 4, 3]], [[3, 5, 4]]})]

Ряд последовательных коммутантов группы G не дошел до единичной подгруппы. Это значит, что группа G неразрешима и, следовательно, уравнение

$$x^5 - 5x + 1 = 0$$

неразрешимо в радикалах.

Рассмотрим еще несколько поучительных примеров:

```
> f := x^8 + 6*x*x + 1:
> G := galois(f);

G := "8T39", {"[2^3]S(4)"}, "+", 192, {"(1 2 3) (4 6 5)",
"(1 6) (2 3 5 4)", "(1 8) (2 3) (4 5) (6 7)",
"(2 8) (1 3) (4 6) (5 7)", "(4 8) (1 5) (2 6) (3 7)"}

```

```
> with(group):
> group[DerivedS](permgroup(8, G[5]));

[permgroup(8, {[[1, 6], [2, 3, 5, 4]], [[1, 2, 3], [4, 6, 5]],
[[1, 8], [2, 3], [4, 5], [6, 7]], [[2, 8], [1, 3], [4, 6], [5, 7]]},
```

```

[[4, 8], [1, 5], [2, 6], [3, 7]])),
permgroup(8, {[], [[1, 2, 4], [3, 6, 5]], [[1, 5, 3], [2, 4, 6]],
[[1, 3], [2, 8], [4, 6], [5, 7]], [[1, 8], [2, 3], [4, 5], [6, 7]])),
permgroup(8, {[], [[1, 6], [2, 5]], [[1, 6], [3, 4]],
[[1, 2], [3, 8], [4, 7], [5, 6]], [[1, 7], [2, 4], [3, 5], [6, 8]])),
permgroup(8, {[], [[1, 6], [2, 5], [3, 4], [7, 8]])),
permgroup(8, {[[]}])

```

Ряд последовательных коммутантов достиг единичной подгруппы, а это значит, что уравнение

$$x^8 + 6x^2 + 1 = 0$$

разрешимо в радикалах.

Для следующего многочлена нет необходимости искать ряд коммутантов. Группа Галуа многочлена оказалась однопороченной, а все циклические группы абелевы и, следовательно, разрешимы:

```

> f := x^6 + x^5 + x^4 + x^3 + x^2 + x + 1:
> G := galois(f);

```

```

G := «6T1», {«3[x]2», «C(6)»}, «-», 6, {«(1 2 3 4 5 6)»}

```

Таким образом, уравнение

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

разрешимо в радикалах.

Решение системы алгебраических уравнений с помощью последовательного исключения переменных сводится к нахождению корней одного многочлена с одним переменным.

Исключение переменных в системе алгебраических уравнений осуществляется с помощью результата. Результат — это определитель специального вида, поэтому для его вычисления необходимо войти в пакет «Линейная алгебра». Если мы желаем исключить переменное x из системы уравнений, содержащей многочлены $f(x, y)$ и $g(x, y)$, то вызываем результат командой

```

sylvester(f, g, x).

```

Исключим переменное x из системы

$$\begin{cases} x^2 - xy + y^2 - 3 = 0, \\ x^2y + xy^2 - 6 = 0, \end{cases}$$

а затем найдем рациональные значения неизвестного y (разложив результат $S(y)$ на множители над полем комплексных чисел, можно убедиться, что остальные корни y этого многочлена действительные):

```
> f := x*x - x*y + y*y - 3:
> g := x*x*y + x*y*y - 6:
> with(linalg):
> S := sylvester( f, g, x);
```

$$S := \begin{bmatrix} 1 & -y & y^2-3 & 0 \\ 0 & 1 & -y & y^2-3 \\ y & y^2 & -6 & 0 \\ 0 & y & y^2 & -6 \end{bmatrix}$$

```
> f := det(S);
```

$$f := 36 + 3y^6 - 12y^4 - 36y + 9y^2$$

```
> roots(36 + 3*y^6 - 12*y^4 - 36*y + 9*y^2, y);
```

```
[[1, 1], [2, 1]]
```

```
> factor(f, complex);
```

$$\begin{aligned} & 3 \cdot (y + 1.833915327 + 0.7449244634 I) \times \\ & \times (y + 1.833915327 - 0.7449244634 I) \times \\ & \times (y - 0.3339153268 + 1.191567210 I) \times \\ & \times (y - 0.3339153268 - 1.191567210 I) (y - 1.) (y - 2.) \end{aligned}$$

Есть и второй способ вычисления результата и, соответственно, исключения одного из переменных из системы алгебраических уравнений:

```
> f := x*x - x*y + y*y - 3:
> g := x*x*y + x*y*y - 6:
> r1 := evala(Resultant(f, g, x));
```

$$36 + 3y^6 - 12y^4 - 36y + 9y^2$$

```
> r2 := evala(Resultant(f, g, y));
```

$$3x^6 - 12x^4 + 9x^2 - 36x + 36$$

```
> roots(r1);
```

```
[[1, 1], [2, 1]]
```



```
>roots(r2);
```

```
[[1, 1], [2, 1]]
```

Приближенные значения решений системы из алгебраических уравнений с двумя неизвестными можно получить и непосредственным применением команды *solve*:

```
> f := x*x - x*y + y*y - 3.:\n> g := x*x*y + x*y*y - 6.:\n> solve({f, g}, {x, y});
```

```
{x = 2., y = 1.}, {x = 1., y = 2.},
```

```
{x = -1.833915327 + 0.7449244634 I, y = 0.3339153268 + 1.191567210 I},
```

```
{x = 0.3339153269 + 1.191567210 I, y = -1.833915327 + 0.7449244634 I},
```

```
{x = 0.3339153269 - 1.191567210 I, y = -1.833915327 - 0.7449244634 I},
```

```
{x = -1.833915327 - 0.7449244634 I, y = 0.3339153268 - 1.191567210 I}.
```

Контрольные задания

1. Задайте числовой интервал в окрестности числа 10^{100} и с помощью пакета *Maple* найдите ближайшую к нему пару близнецов.
2. С помощью пакета *Maple* найдите простые числа, ближайшие к числу 10^{100} .
3. С помощью пакета *Maple* найдите простые числа Мерсенна, ближайшие к числу 10^{100} .
4. С помощью пакета *Maple* найдите простые числа, ближайшие к числу 10^{100} .
5. Задайте многочлен с целыми коэффициентами шестой степени и с помощью пакета *Maple* найдите его разложение на неприводимые множители над полем \mathbb{Z}_{19} .
6. Задайте многочлен с целыми коэффициентами шестой степени и с помощью пакета *Maple* найдите его разложение на неприводимые множители над полем \mathbb{Q} .
7. Задайте многочлен с целыми коэффициентами шестой степени и с помощью пакета *Maple* отделите его действительные корни.
9. Задайте многочлен с целыми коэффициентами шестой степени и с помощью пакета *Maple* найдите группу Галуа этого многочлена.
10. Задайте алгебраическое уравнение шестой степени и с помощью пакета *Maple* выясните, разрешимо ли оно в ардикалах.

Глоссарий алгебры

Абелева группа — группа с коммутативной операцией.

Аксиома выбора — в любом множестве смежных классов можно выбрать по одному представителю из каждого класса.

Алгебра — множество с операциями.

Алгебраическая система — множество с операциями и отношениями.

Алгебраическая форма комплексного числа z — представление комплексного числа в виде $z = a + bi$, где a, b — действительные числа, а i — мнимая единица.

Алгебраическое дополнение элемента a_{ij} — дополнительный минор элемента a_{ij} , взятый со знаком $(-1)^{i+j}$; обозначается символом A_{ij} , т. е. $A_{ij} = (-1)^{i+j}M_{ij}$.

Аргумент числа z — полярный угол точки z . Аргумент обозначается символом $\text{Arg } z$, или по модулю 2π — символом $\arg z$.

Арифметическое m -мерное векторное пространство над полем P — декартова степень P^m с операциями сложения и умножения на скаляр, выполняемыми покомпонентно.

Базис векторного пространства — линейно независимая система порождающих, и он же — максимальная линейно независимая система векторов этого пространства.

Биекция — взаимно однозначное отображение на все множество.

Бинарное отношение на множестве M — подмножество декартова квадрата M^2 .

Булеан $P(M)$ — множество подмножеств множества M .

Вектор — элемент векторного пространства.

Векторное пространство над полем P — алгебра L с двумя операциями, внутренней (сложением) и внешней (умножением на скаляр), причем алгебра $\langle L; + \rangle$ является абелевой группой, и для каждого α, β из L , и каждого a, b из P :

- 1) $a(\alpha + \beta) = a\alpha + a\beta$;
- 2) $(a + b)\alpha = a\alpha + b\alpha$;
- 3) $a(b\alpha) = (ab)\alpha$;
- 4) $1 \cdot \alpha = \alpha$.

Вершина системы линейных неравенств ранга r — решение системы, которое обращает в равенства ее r неравенств с линейно независимыми левыми частями.

Выпуклая оболочка множества M — наименьшее выпуклое множество, содержащее данное множество M .

Выпуклая оболочка множества S из действительного пространства L — множество, состоящее из всех линейных комбинаций

$$k_1\alpha_1 + k_2\alpha_2 + \dots + k_m\alpha_m,$$

где $\alpha_i \in S$, $k_i \geq 0$, $k_1 + k_2 + \dots + k_m = 1$.

Выпуклое подмножество S из действительного векторного пространства L — подмножество, обладающее свойством

$$\alpha, \beta \in S \Rightarrow [\alpha, \beta] \subset S.$$

Гауссова кольцо — целостное кольцо, в котором выполняется аналог основной теоремы арифметики.

Главный идеал — идеал, порожденный одним элементом.

Гомоморфизм — отображение, сохраняющее операции и отношения.

Группа — моноид, в котором каждый элемент обратим.

Группа абелева с коммутативной операцией, в абелевой группе выполняется тождество $[x_1, x_2] = 1$.

Группа кватернионов — мультипликативная группа на множестве $\{1, i, j, k, -1, -i, -j, -k\}$.

Группа нильпотентная — группа в которой выполняется тождество

$$[x_1, x_2, \dots, x_{n-1}, x_n] = 1,$$

где $[x_1, x_2, \dots, x_{n-1}, x_n]$ — простой коммутатор.

Группа разрешимая — группа в которой ряд последовательных коммутаторов обрывается на единичной подгруппе.

Действительная часть комплексного числа z — число a в алгебраической форме $z = a + bi$. Принято обозначение $a = \operatorname{Re} z$.

Действительное векторное пространство — векторное пространство над полем действительных чисел.

Декартов квадрат множества M — множество

$$M^2 = M \times M = \{(a, b) | a \in M, b \in M\}.$$

Декартово произведение множеств A, B — множество

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

Дефект отображения f — размерность $\operatorname{Ker} f$ — ядра этого отображения.

Дополнительный минор элемента a_{ij} — определитель M_{ij} матрицы, оставшейся после вычеркивания в данной квадратной матрице i -й строки и j -го столбца.

Евклидово кольцо — целостное кольцо, в котором выполняется теорема о делении с остатком.

Евклидово пространство — действительное векторное пространство со скалярным умножением.

Знак подстановки — функция не симметрической группе со значениями в $\{1, -1\}$, заданная правилом (для каждой σ из S_n):

$$\operatorname{sgn} \sigma = \begin{cases} 1, & \text{если } \sigma \text{ — четная,} \\ -1, & \text{если } \sigma \text{ — нечетная.} \end{cases}$$

Знакопеременная группа — множество A_n четных подстановок с операцией умножения.

Идеал кольца K — непустое подмножество в K , замкнутое относительно вычитания и умножения на элементы из K .

Идемпотент — элемент x , совпадающий со своим квадратом: $x^2 = x$.

Изоморфизм — взаимно однозначное отображение, сохраняющее операции и отношения.

Инвариантное подмножество линейного оператора f — подмножество, содержащее вместе с каждым элементом x и его образ $f(x)$.

Квантор существования — символ \exists логической операции; читается: *существует*.

Кольцо — аддитивно записанная абелева группа с умножением, дистрибутивным относительно сложения.

Кольцо булево — ассоциативное, идемпотентное кольцо с единицей.

Кольцо главных идеалов — целостное кольцо, в котором все идеалы однопорожждены.

Кольцо идемпотентное — кольцо, в котором выполняется тождество $x^2 = x$.

Кольцо классов вычетов — факторкольцо.

Кольцо целостное — ассоциативное, коммутативное кольцо без делителей нуля.

Кольцо целых чисел \mathbb{Z} — наименьшее кольцо, содержащее полукольцо целых неотрицательных чисел.

Коммутатор простой длины n — $[x_1, x_2, \dots, x_{n-1}, x_n]$. Для $n = 2$ по определению: $[x_1, x_2] = x_1 x_2 x_1^{-1} x_2^{-1}$. Для $n > 2$ полагаем:

$$[x_1, x_2, \dots, x_{n-1}, x_n] \stackrel{\text{опр}}{=} [[x_1, x_2, \dots, x_{n-1}], x_n].$$

Коммутант группы G — подгруппа $[G, G]$ группы G , порожденная всеми коммутаторами элементов из G .

Конгруэнция — эквивалентность, согласованная с операциями и отношениями алгебраической системы.

Крамеровская система линейных уравнений — система из n линейных уравнений с n неизвестными и с ненулевым определителем матрицы системы.

Линейная алгебра — векторное пространство над полем, в котором задано умножение, перестановочное с умножением на скаляр и дистрибутивное относительно сложения.

Линейная комбинация векторов $\alpha_1, \alpha_2, \dots, \alpha_n$ — вектор $\beta = k_1\alpha_1 + k_2\alpha_2 + \dots + k_n\alpha_n$.

Линейно независимая система векторов S — ни один из векторов из системы S линейно не выражается через остальные векторы системы.

Линейное выражение вектора β через векторы $\alpha_1, \alpha_2, \dots, \alpha_n$ — вектор β является линейной комбинацией векторов $\alpha_1, \alpha_2, \dots, \alpha_n$.

Линейно независимая система векторов $\alpha_1, \alpha_2, \dots, \alpha_n$ — ни один из векторов системы линейно не выражается через остальные.

Линейное отображение — отображение векторного пространства, сохраняющие операции сложения и умножения на скаляр.

Линейный оператор — линейное отображение векторного пространства в себя.

Максимальная подсистема системы векторов $\alpha_1, \alpha_2, \dots, \alpha_n$ — максимальная линейно независимая подсистема.

Матрица линейного отображения (оператора) — матрица, составленная из скаляров разложения образов векторов базиса.

Матрица над кольцом K — двумерный массив, заполненный элементами из кольца K .

Минор k -го порядка матрицы — определитель квадратной подматрицы k -го порядка.

Мнимая часть комплексного числа z — число b в алгебраической форме $z = a + bi$. Принято обозначение $b = \text{Im } z$.

Модель — множество с отношениями.

Модуль комплексного числа z — расстояние от точки z до начала координат.

Моноид — полугруппа с нейтральным элементом.

Нетерово кольцо — целостное кольцо, в котором все идеалы конечно порождены. В нетеровом кольце возрастающая цепочка идеалов обрывается на конечном шаге.

Нечетная подстановка — подстановка, которую можно представить в виде нечетного числа транспозиций.

Норма вектора α из евклидова пространства — число $\|\alpha\| = \sqrt{(\alpha, \alpha)}$.

Нормальный делитель (нормальная подгруппа) группы G — подгруппа N , для которой каждый правый смежный класс совпадает с левым классом:

$$Nx = xN$$

для каждого x из G .

Нормированный вектор — вектор, норма которого равна единице.

Образ пространства L при линейном отображении f — множество $f(L) = \{f(x) \mid x \in L\}$.

Обратная матрица матрицы A — такая матрица A^{-1} , что $AA^{-1} = E$. Обратную матрицу можно вычислить по формуле

$$A^{-1} = \frac{1}{|A|} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}.$$

Общезначимая формула — формула алгебры предикатов, истинная при любой интерпретации.

Определитель квадратной матрицы A — элемент $|A|$ из исходного кольца, вычисляемый по правилу

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \dots \cdot a_{n\sigma(n)}.$$

Ортогональность векторов α и β — равенство нулю их скалярного произведения, $(\alpha, \beta) = 0$; пишут $\alpha \perp \beta$.

Ортонормированность — система $\alpha_1, \alpha_2, \dots, \alpha_m$ ортонормированна, когда

$$(\alpha_i, \alpha_j) = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j. \end{cases}$$

Основная теорема алгебры — поле комплексных чисел алгебраически замкнуто.

Основная теорема арифметики — каждое целое число, отличное от 0, 1, -1, является либо простым, либо произведением простых; причем такое представление единственно с точностью до порядка и ассоциированности множителей.

Основная теорема о линейной зависимости — если каждый вектор линейно независимой системы $\alpha_1, \alpha_2, \dots, \alpha_k$ линейно выражается через векторы системы $\beta_1, \beta_2, \dots, \beta_m$, то $m \geq k$.

Основная теорема о симметрических многочленах — подкольцо симметрических многочленов порождается простейшими симметрическими многочленами.

Отношение порядка — рефлексивное, транзитивное и антисимметричное отношение.

Отношение линейного порядка (цепь) — связное отношение порядка.

Отношение эквивалентности — рефлексивное, транзитивное и симметричное отношение.

Отображение — то же, что и *функция*.

Подалгебра — алгебры A — непустое подмножество множества A , образующее с операциями A такого же типа и класса, что и A .

Подгруппа — непустое подмножество группы, замкнутое относительно умножения и взятия обратного элемента.

Подкольцо — непустое подмножество кольца, замкнутое относительно вычитания и умножения.

Подпространство векторного пространства — непустое подмножество H из векторного пространства, замкнутое относительно сложения и умножения на скаляр.

Поле — ассоциативно-коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Поле действительных чисел \mathbb{R} — непрерывное поле, содержащее поле рациональных чисел \mathbb{Q} .

Поле комплексных чисел — наименьшее поле, содержащее как подполе поле действительных чисел и решение уравнения $x^2 + 1 = 0$.

Поле рациональных чисел \mathbb{Q} — поле частных кольца целых чисел.

Поле частных целостного кольца K — наименьшее поле, содержащее кольцо K как подалгебру.

Полугруппа — алгебра с одной ассоциативной операцией.

Полукольцо — алгебра $A = \langle A; \oplus, \otimes \rangle$ с двумя операциями, причем $A = \langle A; \oplus \rangle$ — коммутативная полугруппа с сокращением, а операция (\otimes) — дистрибутивна относительно \oplus .

Представление группы — задание группы с помощью порождающего множества и определяющих соотношений.

Произведение матриц

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1k} \\ b_{21} & b_{22} & \dots & b_{2k} \\ \dots & & & \\ b_{n1} & b_{n2} & \dots & b_{nk} \end{pmatrix} —$$

матрица

$$C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1k} \\ c_{21} & c_{22} & \dots & c_{2k} \\ \dots & & & \\ c_{m1} & c_{m2} & \dots & c_{mk} \end{pmatrix},$$

элементы которой имеют вид

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj}.$$

Простейший симметрический многочлен — многочлен

$$\sigma_k(x_1, x_2, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}.$$

Размерность пространства L — число элементов в базисе векторного пространства L ; обозначают символом $\dim L$.

Ранг матрицы — ранг системы векторов-столбцов (или векторов-строк) этой матрицы.

Ранг отображения f — размерность образа $f(L)$ пространства L при линейном отображении f .

Ранг системы векторов S — число элементов в максимальной линейно независимой подсистеме векторов данной системы.

Ранг системы векторов $\alpha_1, \alpha_2, \dots, \alpha_n$ — число элементов в максимальной линейно независимой подсистеме.

Решетка — упорядоченное множество, в котором каждая пара элементов имеет точную верхнюю и точную нижнюю грани.

Решетка булева — дистрибутивная решетка с дополнениями.

Сигнатура алгебраической системы — символы для обозначений операций и отношений системы.

Сигнатура алгебры — символы для обозначений операций алгебры.

Симметрическая группа — множество S_n всех биекций множества из n элементов на себя с операцией умножения.

Симметрическая разность множеств A и B — $(A \setminus B) \cup (B \setminus A)$.

Симметрический многочлен — многочлен, выдерживающий все перестановки своих переменных.

Система действительных чисел \mathbf{R} — наименьшее непрерывное поле, содержащее поле рациональных чисел в качестве подполя.

Скаляр — элемент из P — поля скаляров векторного пространства.

След матрицы — сумма диагональных элементов матрицы.

Собственное значение линейного оператора A — такой скаляр λ , что $xA = \lambda x$ для некоторого ненулевого вектора x . Вектор x называют *собственным вектором* линейного оператора A .

Собственный вектор — вектор, порождающий одномерное инвариантное подпространство. Ненулевой вектор x является собственным вектором линейного оператора A , если $xA = \lambda x$ для некоторого скаляра λ из P . Скаляр λ называют *собственным значением* собственного вектора x .

Степень нильпотентности группы — наименьшая длина простого коммутатора в тождестве нильпотентности.

Степень разрешимости группы — длина ряда последовательных коммутаторов.

Тело — ассоциативное кольцо, в котором каждый ненулевой элемент обратим.

Тело кватернионов — четырехмерная действительная линейная алгебра с базисом $1, i, j, k$:

$$i^2 = j^2 = -1, \quad ij = -ji = k.$$

Тип алгебраической системы — набор местностей операций и отношений системы.

Тип алгебры — набор местностей операций алгебры.

Транспозиция — подстановка, перемещающая в точности два символа.

Факторгруппа — группа, состоящая из смежных классов по нормальной подгруппе с операцией, определенной по представителям.

Факторкольцо — кольцо, состоящее из смежных классов по идеалу с операцией, определенной по представителям.

Факормножество — множество, состоящее из смежных классов.

Формула первой ступени — формула алгебра предикатов, у которой кванторы навешены только на предметные переменные.

Фундаментальный набор решений системы однородных линейных уравнений — решения, образующие базис пространства решений системы.

Функциональное отношение (функция, отображение) — бинарное отношение, в котором каждый элемент имеет не более одного образа.

Функция — то же, что и *функциональное отношение*.

Функция Эйлера $\varphi(n)$ равна числу натуральных чисел, не превышающих n и взаимно простых с n .

Характеристика кольца — аддитивный порядок единичного элемента.

Характеристика поля — то же, что и характеристика кольца.

Характеристический многочлен матрицы A — многочлен

$$f(\lambda) = |A - \lambda E|.$$

Характеристическое уравнение матрицы A — уравнение

$$f(\lambda) = |A - \lambda E| = 0.$$

Характеристическое уравнение линейного оператора — характеристическое уравнение матрицы этого оператора.

Центр группы — множество элементов группы, перестановочных со всеми элементами группы.

Центр кольца — множество элементов кольца, перестановочных со всеми элементами кольца.

Цепь (цепочка) — линейно упорядоченное множество.

Циклическая группа — группа, порожденная одним элементом.

Цорна лемма — если каждая цепь частично упорядоченного множества имеет верхнюю грань, то каждый элемент множества не превышает некоторого максимального элемента из этого же множества.

Четная подстановка — подстановка, которую можно представить в виде четного числа транспозиций.

Эквивалентные системы векторов — каждый вектор одной системы линейно выражаются через векторы другой.

Элементарная теория — аксиоматическая теория, все аксиомы которой являются формулами первой степени.

Элементарное преобразование второго типа — замена одного из уравнений системы на сумму этого уравнения с другим, умноженным на любой элемент из поля коэффициентов. Аналогичное преобразование системы векторов, строк или столбцов матрицы.

Элементарное преобразование первого типа — умножение левой и правой частей одного из уравнений системы на ненулевой элемент из поля коэффициентов. Аналогичное преобразование системы векторов, строк или столбцов матрицы.

Ядро гомоморфизма — полный прообраз нейтрального элемента.

Ядро линейного отображения $f : L \rightarrow L_1$ — полный прообраз нулевого элемента θ из образа L_1 :

$$\text{Ker } f = f^{-1}(\theta) = \{x \in L \mid f(x) = \theta\}.$$

Библиографический список

1. *Виноградов, И. М.* Основы теории чисел / И. М. Виноградов. — Москва : Издательство Юрайт, 2020.
2. *Далингер, В. А.* Информатика и математика. Решение уравнений и оптимизация в Mathcad и Maple : учебник и практикум для вузов / В. А. Далингер, С. Д. Симонженков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020.
3. *Журавлев, Ю. И.* Дискретный анализ. Основы высшей алгебры : учебное пособие для академического бакалавриата / Ю. И. Журавлев, Ю. А. Флеров, М. Н. Вялый. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019.
4. Информатика и математика : учебник и практикум для академического бакалавриата / Т. М. Беляева [и др.] ; под редакцией В. Д. Элькина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019.
5. *Кашапова, Ф. Р.* Высшая математика. Общая алгебра в задачах : учебное пособие для академического бакалавриата / Ф. Р. Кашапова, И. А. Кашапов, Т. Н. Фоменко. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2018.
6. *Ларин, С. В.* Алгебра: многочлены : учебное пособие для академического бакалавриата / С. В. Ларин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019.
7. *Ларин, С. В.* Алгебра и теория чисел. Группы, кольца и поля : учебное пособие для академического бакалавриата / С. В. Ларин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019.
8. *Палий, И. А.* Дискретная математика и математическая логика : учебное пособие для вузов / И. А. Палий. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020.

Приложение

1. Основные команды пакета Maple для работы с группами подстановок

Команда	Действие
<i>with(group)</i>	Вход в пакет «Теория групп»
<i>areconjugate</i> (<i>G</i> , <i>a</i> , <i>b</i>)	Определяет, сопряжены или нет подстановки <i>a</i> и <i>b</i> в группе подстановок <i>G</i>
<i>center</i> (<i>G</i>)	Находит центр группы подстановок <i>G</i>
<i>centralizer</i> (<i>G</i> , { <i>M</i> })	Находит централизатор множества подстановок <i>M</i> в группе <i>G</i>
<i>convert</i> (<i>α</i> , 'permlist', <i>n</i>)	Записывает вторую строку подстановки $\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha & (1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix},$ заданной в виде произведения независимых циклов
<i>convert</i> ([<i>α</i> (1), <i>α</i> (2), ..., <i>α</i> (<i>n</i>)], 'disjycs')	Записывает подстановку $\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha & (1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix},$ в виде произведения независимых циклов
<i>convert</i> ([<i>w</i> (<i>a_i</i>)], 'disjycs', <i>G</i>)	Вычисляет значение слова <i>w</i> (<i>a_i</i>) в группе подстановок $G := \text{permgroupp}(n, \{a1 = u_1, a2 = u_2, \dots\})$ степени <i>n</i> , порожденной подстановками <i>u₁</i> , <i>u₂</i> , ...
<i>core</i> (<i>H</i> , <i>G</i>)	Находит порождающие элементы наибольшей нормальной подгруппы, содержащейся в подгруппе данной группы подстановок (если <i>H</i> — подгруппа группы <i>G</i> , то <i>coreN</i> — это ядро гомоморфизма группы <i>G</i> в группу правых сдвигов правостороннего разложения <i>G</i> по <i>H</i>)
<i>cosets</i> (<i>G</i> , <i>H</i>)	Находит полную систему представителей правых смежных классов группы <i>G</i> по подгруппе <i>H</i>
<i>cosrep</i> (<i>a</i> , <i>H</i>)	Находит представление элемента <i>a</i> группы <i>G</i> в виде произведения элемента из подгруппы <i>H</i> , умноженного на представитель правого смежного класса по этой подгруппе

Команда	Действие
<i>derived</i> (<i>G</i>)	Находит производную подгруппу (коммутант) группы подстановок <i>G</i>
<i>DerivedS</i> (<i>G</i>)	Находит ряд производных (коммутантов) группы подстановок <i>G</i>
<i>elements</i> (<i>G</i>)	Находит элементы группы подстановок <i>G</i>
<i>groupmember</i> (<i>a</i> , <i>G</i>)	Определяет, входит ли подстановка <i>a</i> в группу подстановок <i>G</i>
<i>grouporder</i> (<i>G</i>)	Вычисляет порядок группы <i>G</i> подстановок (или группы <i>G</i> , заданной порождающими элементами и определяющими соотношениями)
<i>inter</i> (<i>A</i> , <i>B</i>)	Находит порождающие элементы пересечения двух групп подстановок <i>A</i> и <i>B</i>
<i>invperm</i> (<i>a</i>)	Находит подстановку, обратную для подстановки <i>a</i>
<i>isabelian</i> (<i>G</i>)	Определяет, не является ли группа подстановок <i>G</i> абелевой
<i>isnormal</i> (<i>G</i> , <i>H</i>)	Определяет, не является ли подгруппа <i>H</i> нормальным делителем в группе <i>G</i>
<i>issubgroup</i> (<i>H</i> , <i>G</i>)	Определяет, является ли группа подстановок <i>H</i> подгруппой группы подстановок <i>G</i>
<i>LCS</i> (<i>G</i>)	Находит нижний центральный ряд (<i>Lower Central Series</i>) группы подстановок <i>G</i>
<i>mulperms</i> (<i>a</i> , <i>b</i>)	Находит произведение <i>ab</i> подстановок <i>a</i> и <i>b</i> , представленных в виде произведения непересекающихся циклов
<i>NormalClosure</i> (<i>H</i> , <i>G</i>)	Находит порождающие элементы нормального замыкания подгруппы <i>H</i> в группе подстановок <i>G</i>
<i>normalizer</i> (<i>G</i> , <i>H</i>)	Находит порождающие элементы нормализатора подгруппы <i>H</i> в группе подстановок <i>G</i>
<i>orbit</i> (<i>G</i> , <i>i</i>)	Вычисляет орбиту (множество точек) точки <i>i</i> в группе подстановок <i>G</i>
<i>parity</i> (<i>a</i>)	Определяет четность подстановки <i>a</i>
<i>parity</i> (<i>G</i>)	Определяет четность группы подстановок <i>G</i> (четность равна +1, если все подстановки из <i>G</i> четные, и -1, если не все подстановки четные)
<i>permgroupe</i> (<i>n</i> , { <i>a</i> , <i>b</i> , ...})	Задаёт группу подстановок степени <i>n</i> с порождающими подстановками <i>a</i> , <i>b</i> , ...
<i>RandElement</i> (<i>G</i>)	Находит случайно выбранный элемент из группы подстановок <i>G</i>

Команда	Действие
$SnConjugates(G, a)$	Находит число подстановок, сопряженных с подстановкой a в группе G
$Sylow(G, p)$	Находит порождающие элементы силовой p -подгруппы группы подстановок G
$transgroup(\langle nTm \rangle, 'names')$	Определяет вид группы (имя) m -кратно транзитивных групп подстановок на n символах
$transgroup(\langle nTm \rangle, 'order', 'parity', 'generators')$	Определяет порядок, четность и порождающие элементы m -кратно транзитивных групп подстановок степени n
$transgroup([n, m], 'names', 'parity')$	Определяет вид группы (имя) и четность m -кратно транзитивных групп подстановок степени n
$transgroup(m, 'number')$	Определяет число m -кратно транзитивных групп подстановок
$transgroup(m, 'number', 'order')$	Определяет число m -кратно транзитивных групп подстановок и их порядки
$type(a, 'disjyc'(n))$	Проверяет правильность записи подстановки a степени n в виде произведения независимых циклов

2. Основные команды пакета Maple для работы с абстрактными группами

Команда	Действие
$with(group)$	Вход в пакет «Теория групп»
$cosets(G, H)$	Находит полную систему представителей правых смежных классов для подгруппы группы подстановок или группы, заданной порождающими и определяющими соотношениями
$cosrep(a, H)$	Находит представление элемента a группы G в виде произведения элемента из подгруппы H , умноженного на представитель правого смежного класса по этой подгруппе
$grelgroup(\{a_1, a_2, \dots\}, \{R_1(a_i), R_2(a_i), \dots\})$	Задаёт группу порождающими элементами a_1, a_2, \dots и определяющими соотношениями $R_1(a_i), R_2(a_i), \dots$
$grouporder(G)$	Вычисляет порядок группы G подстановок (или группы G , заданной порождающими элементами и определяющими соотношениями)
$isnormal(G, H)$	Определяет, не является ли подгруппа H нормальным делителем в группе G
$permrep(H)$	Находит представление группы G , заданной порождающими элементами и определяющими соотношениями, подстановками правых смежных классов по подгруппе H

Команда	Действие
$pres(H)$	Находит комбинаторное представление для подгруппы H , порожденной данными элементами, в группе G , заданной комбинаторным представлением
$subgrel(\{x = [a], y = [b], \dots\}, G)$	Находит определяющие соотношения в порождающих x, y, \dots для подгруппы, порожденной элементами a, b, \dots в группе G , заданной порождающими элементами и определяющими соотношениями

3. Основные команды пакета Maple для работы с целыми числами

Команда	Действие
$with(numtheory)$	Вход в пакет «Теория чисел»
$bigomega(n)$	Вычисляет количество простых делителей целого числа n , считая каждый делитель столько раз, какова его кратность
$cfrac(f)$	Выдает представление рационального выражения f от одной переменной в виде цепной дроби
$cfrac(x)$	Представляет действительное число x в виде цепной дроби (с десятью дробными частями)
$cfrac(x, n)$	Представляет действительное число x в виде цепной дроби (с n дробными частями)
$cfrac(x, n, 'quotients')$	Выдает n частных представления действительного числа x в виде цепной дроби
$cfrac(x, 'periodic')$	Для действительного x , представимого в виде периодической цепной дроби, выдает допериодическую часть и период
$cfrac(x, 'periodic')$	Для действительного x , представимого в виде периодической цепной дроби, выдает частные допериодической части и периода
$cfracpol(f)$	Выдает десять частных представления рационального корня многочлена f с рациональными коэффициентами
$cfracpol(f, n)$	Выдает $n + 1$ частное из представления в виде цепной дроби корня многочлена f с рациональными коэффициентами
$divisors(n)$	Выдает множество всех делителей целого числа n
$factorEQ(m, d)$	Если $\mathbf{Z}[\sqrt{d}]$ — евклидово, то выдает разложение на множители в кольце $\mathbf{Z}[\sqrt{d}]$ числа m из этого кольца
$factorial(n)$	Выдает $n!$ для целого неотрицательного n

Команда	Действие
<i>factorset</i> (<i>n</i>)	Выдает множество простых делителей целого числа <i>n</i>
<i>fermat</i> (10, 'w'): <i>w</i>	Выдает <i>n</i> -е число Ферма $2^{2^m} + 1$ вместе с его простыми делителями для $n < 22$
<i>fermat</i> (<i>n</i>)	Выдает <i>n</i> -е число Ферма $2^{2^m} + 1$ для $n < 22$
<i>Glgcd</i> (<i>a</i> + <i>b</i> * <i>I</i> , <i>c</i> + <i>d</i> * <i>I</i> , 'r')	Находит наибольший общий делитель двух целых гауссовых чисел $a + bi$, $c + di$
<i>Gllcm</i> (<i>a</i> + <i>b</i> * <i>I</i> , <i>c</i> + <i>d</i> * <i>I</i> , 'r')	Находит наименьшее общее кратное двух целых гауссовых чисел $a + bi$, $c + di$
<i>GIquo</i> (<i>a</i> + <i>b</i> * <i>I</i> , <i>c</i> + <i>d</i> * <i>I</i> , 'r')	Выдает частное от деления целых гауссовых чисел $a + bi$, $c + di$; остаток от деления равен <i>r</i>
<i>Glrem</i> (<i>a</i> + <i>b</i> * <i>I</i> , <i>c</i> + <i>d</i> * <i>I</i> , 'q')	Выдает остаток от деления целых гауссовых чисел $a + bi$, $c + di$; частное от деления равно <i>q</i>
<i>ifactor</i> (<i>a</i>)	Выдает канонические формы числителя и знаменателя рационального числа <i>a</i>
<i>ifactors</i> (<i>a</i>)	Выдает канонические формы числителя и знаменателя рационального числа <i>a</i> в виде коэффициента (1 или -1) и простых делителей с указанием их кратностей
<i>igcd</i> (<i>a</i> , <i>b</i>)	Вычисляет НОД (<i>a</i> , <i>b</i>)
<i>ilcm</i> (<i>a</i> , <i>b</i>)	Вычисляет НОК [<i>a</i> , <i>b</i>]
<i>imagunit</i> (<i>m</i>)	Указывает решение сравнения $x^2 \equiv -1 \pmod{m}$ или сообщает, что решения не существует
<i>index</i> (<i>x</i> , <i>g</i> , <i>m</i>)	Вычисляет индекс (дискретный логарифм) целого числа <i>x</i> по основанию <i>g</i> и по модулю <i>m</i> или сообщает, что таковой не существует
<i>invphi</i> (<i>n</i>)	Показывает список целых чисел m_i таких, что $\phi(m_i) = n$; список может быть и пустым — []
<i>iquo</i> (<i>a</i> , <i>b</i>)	Вычисляет частное от деления <i>a</i> на <i>b</i>
<i>irem</i> (<i>a</i> , <i>b</i>)	Вычисляет Rest (<i>a</i> , <i>b</i>)
<i>isolve</i> (<i>S</i>)	Находит целочисленные решения системы уравнений <i>S</i> с несколькими переменными
<i>isprime</i> (<i>n</i>)	Выясняет, просто или нет целое число <i>n</i>
<i>issqfree</i> (<i>n</i>)	Выясняет, свободно или нет целое число <i>n</i> от квадратов (т. е. верно ли, что в каноническом разложении числа <i>n</i> все простые множители однократные)
<i>ithprime</i> (<i>n</i>)	Выдает <i>n</i> -е простое число

Команда	Действие
$\text{jacobi}(a, b)$	Вычисляет символ Якоби $\left(\frac{a}{b}\right)$ для целого a и положительного нечетного b
$L(a, p)$	Вычисляет символ Лежандра $\left(\frac{a}{p}\right)$ для целого a и простого нечетного p
$\text{lambda}(m)$	Определяет порядок наибольшей циклической мультипликативной группы по модулю m
$\text{legendre}(a, p)$	Вычисляет символ Лежандра $\left(\frac{a}{p}\right)$ для целого a и простого нечетного p
$\text{mcombine}(a, r1, b, r2)$	Реализует китайскую теорему об остатках, т. е. указывает решение системы сравнений $\begin{cases} x \equiv r1(\text{mod } a), \\ x \equiv r2(\text{mod } b), \end{cases}$ или сообщает, что эта система несовместна
$\text{mersenne}([n])$	Вычисляет n -е число Мерсенна
$\text{mersenne}(n)$	Выясняет, просто или нет n -е число Мерсенна
$\text{mipolys}(n, p),$	Вычисляет число различных неприводимых многочленов степени n над полем \mathbb{Z}_p
$\text{mipolys}(n, p, m),$	Вычисляет число различных неприводимых многочленов степени n над полем из p^m элементов
$\text{mlog}(x, g, m)$	Вычисляет дискретный логарифм (индекс) целого числа x по основанию g и по модулю m или сообщает, что таковой не существует
$\text{mobius}(n)$	Вычисляет функцию Мебиуса $\mu(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}) = \begin{cases} 0, & \text{если } (\exists i)[\alpha_i > 1], \\ (-1)^k, & \text{если все } \alpha_i = 1 \end{cases}$
$\text{mroot}(a, n, m)$	Выдает решение сравнения $x^n \equiv a(\text{mod } m)$ или сообщает, что такого решения не существует
$\text{msqrt}(a, m)$	Выдает решение сравнения $x^2 \equiv a(\text{mod } m)$ или сообщает, что такого решения не существует
$n!$	Выдает $n!$ для целого неотрицательного n
$\text{nextprime}(n)$	Вычисляет наименьшее простое число, которое больше натурального числа n
$\text{nthconver}(\text{ЦД}, n)$	Вычисляет n -ю подходящую дробь цепной дроби ЦД

Команда	Действие
$nthdenom(\text{ЦД}, n)$	Вычисляет знаменатель n -й подходящей дроби ЦД
$nthnumer(\text{ЦД}, n)$	Вычисляет числитель n -й подходящей дроби ЦД
$nthpow(m, n)$	Вычисляет наибольшее натуральное число a такое, что a^n делит целое число n
$order(a, m)$	Вычисляет порядок целого числа a по модулю m или сообщает, что такого не существует
$pdexpand(a)$	Показывает цифры допериодической части и периода после обращения рационального числа a в десятичную дробь
$phi(n)$	Вычисляет функцию Эйлера $\varphi(n)$
$pi(n)$	Вычисляет значение функции $\pi(n)$, равное числу натуральных простых чисел, не превышающих n
$pprimroot(g, m)$	Вычисляет первообразный элемент по модулю m , превышающий число g , или сообщает, что такого нет
$prevprime(n)$	Вычисляет наибольшее простое число, которое меньше натурального числа n
$primroot(m)$	Вычисляет наименьший положительный первообразный элемент по модулю m или сообщает, что такого нет
$quadres(a, p)$	Вычисляет обобщенный символ Лежандра $\left(\frac{a}{p}\right)$, равный 1, если сравнение $x^2 \equiv a \pmod{p}$ имеет решение, и равный -1 , если сравнение несовместно
$rootsunity(p, m)$	Для простого p и целого m выдает все решения сравнения $x^p \equiv 1 \pmod{m}$; одним из корней всегда является 1
$safeprime(n)$	Вычисляет такое наименьшее простое число p , большее n , что $\frac{p-1}{2}$ тоже простое (и, таким образом, команда иллюстрирует постулат Бертрана, доказанный П. Л. Чебышевым)
$sigma(n)$	Выдает сумму натуральных делителей целого числа n
$sq2factor(a)$	Выдает разложение на множители в кольце $\mathbb{Z}[\sqrt{2}]$ числа a из этого кольца
$sum2sqr(n)$	Показывает все варианты представления целого неотрицательного числа в виде суммы двух квадратов; если такого представления не существует, то список пуст — []

Команда	Действие
$\text{tau}(n)$	Выдает число натуральных делителей целого числа n
$\text{thue}(F, [x, y])$	Выдает целочисленные решения системы уравнений или системы неравенств F с двумя неизвестными x, y

4. Основные команды пакета Maple для работы с многочленами

Команда	Действие
$\text{with}(\text{numtheory})$	Вход в пакет «Теория чисел»
$\text{with}(\text{PolynomialTools})$	Вход в пакет «Полиномиальные инструментальные средства»
$\text{cfraction}(f)$	Представляет функцию $f(x)$ в виде цепной дроби
$\text{coeff}(f, x, n)$	Определяет коэффициент одночлена x^n в многочлене f от нескольких переменных
$\text{coeff}(f, x)$	Вычисляет коэффициент при x в многочлене f от нескольких переменных
$\text{coeff}(f, x^n)$	Вычисляет коэффициенты при x^n в многочлене f от нескольких переменных
$\text{coeffs}(f, x, 't')$	Вычисляет коэффициенты многочлена f от нескольких переменных, относящиеся к переменной x (или списку переменных) с опцией 't', задающей имя переменной
$\text{collect}(f, x)$	Группирует слагаемые в многочлене f от нескольких переменных по степеням переменной x
$\text{combine}(f, x)$	Преобразует выражение f к более компактному виду, объединяет выражения (команда, обратная команде expand)
$\text{convert}(d, \text{parfrac}, x)$	Выдает представление дробно-рациональной функции d в виде суммы элементарных дробей
$\text{convert}(f, \text{horner}, x)$	Осуществляет расстановку скобок для вычисления значения многочлена с наименьшим числом операций
$\text{convert}(f, \text{polinom})$	Преобразует функцию f в многочлен
$\text{degree}(f, x)$	Указывает степень многочлена $f(x)$ по переменной x
$\text{diff}(f, x\$n)$	Вычисляет n -ю производную по переменной x функции f от нескольких переменных
$\text{Diff}(f, x\$n)$	Показывает естественную запись n -ю производной по переменной x функции f от нескольких переменных

Команда	Действие
$\text{diff}(f, x)$	Вычисляет первую производную по переменной x функции f от нескольких переменных
$\text{discrim}(f, x)$	Вычисляет дискриминант многочлена f по переменной x
$\text{DistDeg}(f, x) \bmod p$	Вычисляет неприводимые множители многочлена $f(x)$ над полем \mathbb{Z}_p
$\text{divide}(f, g, 'q')$	Выясняет, делится ли многочлен f на многочлен g , в случае делимости частное равно q
$\text{dsolve}(\{f, W\})$	Находит частное решение дифференциального уравнения f при заданных условиях W
$\text{dsolve}(f)$	Находит общее решение дифференциального уравнения f
$\text{expand}(f)$	Раскрывает скобки при умножении, а затем приводит подобные члены в выражении
$\text{factor}(f, \text{complex})$	Находит разложение на линейные множители над полем комплексных чисел многочлена f с комплексными коэффициентами
$\text{factor}(f)$	Находит разложение на множители, сокращает подобные члены в алгебраической дроби
$\text{fixdiv}(f, x)$	Вычисляет фиксированный делитель для многочлена $f(x)$ с целыми коэффициентами, т. е. находит наибольшее целое число, которое делит $f(m)$ для любого целого m
$\text{galois}(f)$	Вычисляет группу Галуа неприводимого многочлена f степени ≤ 9
$\text{gcd}(f, g)$	Находит наибольший общий делитель многочленов f и g
$\text{gcdex}(f, g, x, 'u', 'v')$	Вычисляет наибольший общий делитель $(f(x), g(x))$ многочленов $f(x)$ и $g(x)$ и его линейное разложение $(f(x), g(x)) = f(x) u(x) + g(x) v(x)$
$\text{Hessian}(f, [x_1, x_2, \dots, x_n])$	Вычисляет гессиан n -го порядка для функции f от переменных x_1, x_2, \dots, x_m , где $n \leq m$
$\text{linterp}([x_1, x_2, \dots, x_n], [y_1, y_2, \dots, y_n], x) \bmod p$	Находит интерполяционный многочлен по значениям y_i в данных точках x_i с коэффициентами из конечного поля \mathbb{Z}_p
$\text{Int}(f, x = a..b)$	Показывает естественную запись определенного интеграла $\int_a^b f(x) dx$

Команда	Действие
$\text{int}(f, x = a..b)$	Вычисляет определенный интеграл $\int_a^b f(x)dx$
$\text{int}(f, x = a..\text{infinity});$	Вычисляет несобственный определенный интеграл $\int_a^{\infty} f(x)dx$
$\text{Int}(f, x)$	Показывает естественную запись неопределенного интеграла $\int f(x)dx$
$\text{int}(f, x)$	Вычисляет неопределенный интеграл $\int f(x)dx$
$\text{int}(\text{int}(f, y), x);$	Вычисляет неопределенный интеграл $\iint f(x, y)dydx$
$\text{int}(\text{int}(\text{int}(f(x, y, z), x = a1..a2), y = b1..b2), z = c1..c2)$	Вычисляет определенный интеграл $\int_{c1}^{c2} \int_{b1}^{b2} \int_{a1}^{a2} f(x, y, z)dx dy dz$
$\text{interp}([x_1, x_2, \dots, x_n], [y_1, y_2, \dots, y_n], x)$	Вычисляет интерполяционный многочлен $f(x)$, которой для различных значений x_i принимает заданные значения y_i
$\text{irredik}(p)$	Выясняет, имеет ли многочлен f неприводимые множители
$\text{lcm}(f, g)$	Находит наименьшее общее кратное многочленов f, g
$\text{maximize}(f)$	Вычисляет максимальное значение функции f
$\text{maximize}(f, \text{location})$	Вычисляет максимальное значение функции f с указанием точки максимума
$\text{MinimalPolynomial}(a, n)$	Вычисляет многочлен степени $\leq n$, корень которого приближенно равен числу a
$\text{minimize}(f)$	Вычисляет минимальное значение функции f
$\text{minimize}(f, \text{location})$	Вычисляет минимальное значение функции f с указанием точки минимума
$\text{nops}(f)$	Определяет количество слагаемых в выражении f с одной переменной
$\text{normal}(f)$	Нормализует рациональное выражение f , сокращает общие множители и приводит к общему знаменателю
$\text{nthdenom}(f, n)$	Находит знаменатель n -й подходящей дроби для цепной дроби f
$\text{nthnumer}(f, n)$	Находит числитель n -й подходящей дроби для цепной дроби f

Команда	Действие
$op(k, f)$	Определяет k -е слагаемое в многочлене f , записанном как сумма одночленов
$powmod(f, n, g, x)$	Вычисляет $f(x)^n \bmod g(x)$ для целого n
$proot(f, n)$	Вычисляет n -ю степень многочлена f с рациональными коэффициентами
$psqrt(f)$	Вычисляет квадратный корень многочлена f с рациональными коэффициентами
$quo(f, g, x, 'r')$	Вычисляет частное от деления многочлена f на многочлен g ; многочлен r — остаток от деления
$randpoly([x, y, \dots, z])$	Выдает случайный многочлен $f(x, y, \dots, z)$ с целыми коэффициентами из интервала $[-99 \dots 99]$ и степени меньше 6
$randpoly(x)$	Выдает случайный многочлен $f(x)$ с целыми коэффициентами из интервала $[-99 \dots 99]$ и степени меньше 6
$Randprime(n, x) \bmod p$	Выдает случайный неприводимый многочлен степени n с переменной x над конечным полем \mathbb{Z}_p
$rationalize(s)$	Освобождает от иррациональности знаменатель дроби s
$realroot(f)$	Вычисляет интервалы, в которых находятся действительные корни многочлена f
$rem(f, g, x, 'q')$	Вычисляет остаток от деления многочлена f на многочлен g ; многочлен q — частное от деления
$resultant(f, g, x)$	Вычисляет результат многочленов $f(x, y)$ и $g(x, y)$
$Resultant(f, g, x) \bmod p$	Вычисляет результат многочленов $f(x, y)$ и $g(x, y)$ с коэффициентами из поля \mathbb{Z}_p
$roots(f)$	Вычисляет рациональные корни многочлена $f(x)$ и определяет их кратность
$series(f, x = a, n)$	Находит первые n членов разложения функции в ряд Тейлора по степеням $(x - a)$
$simplify(f, x)$	Упрощает выражение $f(x)$
$solve(S, \{W\})$	Находит решение системы уравнений или неравенств S , содержащих неизвестные из множества W
$sturm(f, x, a, b)$	Определяет число действительных корней многочлена $f(x)$ с действительными коэффициентами в интервале (a, b)

Окончание таблицы

Команда	Действие
$sturmseg(f, x)$	Выдает систему многочленов Штурма для многочлена $f(x)$
$subs(x = \alpha, f)$	Символом α обозначается корень многочлена f
$subs(x_1 = g_1, \dots, x_n = g_n, f)$	Вычисляет суперпозицию $f(g_1, g_2, \dots, g_n)$
$sylvester(f, g, x)$	Вычисляет результат многочленов $f(x, y)$ и $g(x, y)$
$taylor(f, x = a, n)$	Находит первые n членов разложения функции в ряд Тейлора по степеням $(x - a)$
$value(\%)$	Вычисляет значение предыдущего выражения

Наши книги можно приобрести:

Учебным заведениям и библиотекам:
в отделе по работе с вузами
тел.: (495) 744-00-12, e-mail: vuz@urait.ru

Частным лицам:
список магазинов смотрите на сайте urait.ru
в разделе «Частным лицам»

Магазинам и корпоративным клиентам:
в отделе продаж
тел.: (495) 744-00-12, e-mail: sales@urait.ru

Отзывы об издании присылайте в редакцию
e-mail: gred@urait.ru

Новые издания и дополнительные материалы доступны
на образовательной платформе «Юрайт» urait.ru,
а также в мобильном приложении «Юрайт.Библиотека»

Учебное издание

Горюшкин Александр Петрович

АБСТРАКТНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

Учебник для вузов

Формат 70×100 ¹/₁₆.
Гарнитура «Charter». Печать цифровая.
Усл. печ. л. 53,61

ООО «Издательство Юрайт»
111123, г. Москва, ул. Плеханова, д. 4а.
Тел.: (495) 744-00-12. E-mail: izdat@urait.ru, www.urait.ru