

# **Конспект семинаров по курсу «Основы высшей алгебры и теории кодирования»**

Гущин Д. Д.  
МФТИ

2021  
Апрель

# Оглавление

<b>Глава 1. Предварительные сведения</b>	<b>4</b>
1.1 Базовые понятия из курса дискретного анализа . . . . .	5
1.1.1 Отношение эквивалентности . . . . .	5
1.1.2 Отображения . . . . .	7
1.2 База теории чисел . . . . .	10
1.2.1 Алгоритм Евклида . . . . .	10
1.2.2 Линейные диофантовы уравнения . . . . .	12
1.2.3 Основная теорема арифметики . . . . .	13
1.2.4 Функция Эйлера . . . . .	14
<b>Глава 2. Общая теория групп</b>	<b>15</b>
2.1 Основы теории групп . . . . .	16
2.1.1 Полугруппа, моноид, группа . . . . .	16
2.1.2 Естественные примеры групп . . . . .	18
2.1.3 Подгруппы, классы смежности . . . . .	19
2.1.4 Циклические группы . . . . .	22
2.2 Симметрическая группа . . . . .	24
2.2.1 Перестановки . . . . .	25
2.2.2 Цикловое разложение . . . . .	26
2.2.3 Сопряженные элементы . . . . .	27
2.2.4 Знакопеременная группа . . . . .	29
2.3 Морфизмы и конструкции. Часть 1 . . . . .	30
2.3.1 Нормальные подгруппы . . . . .	30
2.3.2 Прямое произведение групп . . . . .	32
2.3.3 Гомоморфизмы: определение, ядра . . . . .	33
2.3.4 Изоморфизмы, эндоморфизмы, автоморфизмы . . . . .	34
2.4 Морфизмы и конструкции. Часть 2 . . . . .	36
2.4.1 Фактор-группы . . . . .	37
2.4.2 Теорема о гомоморфизмах . . . . .	38
2.4.3 Группа преобразований . . . . .	40
2.4.4 Группа автоморфизмов . . . . .	41
2.4.5 Внутренние автоморфизмы . . . . .	41
2.5 Геометрические и комбинаторные группы. Коммутант . . . . .	43
2.5.1 Порождающие и соотношения . . . . .	43
2.5.2 Конечно-порожденные абелевы группы . . . . .	45
2.5.3 Группа Диэдра . . . . .	46
2.5.4 Группы симметрий и группы вращений . . . . .	46
2.5.5 Коммутант . . . . .	47
2.6 Связь с теорией чисел . . . . .	48
2.6.1 Мультипликативная группа вычетов . . . . .	48
2.6.2 Первобразный корень . . . . .	49
2.6.3 Малая теорема Ферма и теорема Эйлера . . . . .	49

2.6.4	Китайская теорема об остатках . . . . .	50
2.6.5	Квадратичные вычеты . . . . .	51
2.7	Действия групп . . . . .	53
2.7.1	Действия групп: определение . . . . .	54
2.7.2	Орбита, стабилизатор . . . . .	55
2.7.3	Теорема Кэли . . . . .	56
2.7.4	Лемма Бернсайда . . . . .	57
<b>Глава 3.</b>	<b>Общая теория колец и полей</b>	<b>59</b>
3.1	Основы теории колец . . . . .	60
3.1.1	Кольцо: определение и свойства . . . . .	60
3.1.2	Обратимые элементы кольца, делители нуля, область целостности . . . . .	61
3.1.3	Кольцо многочленов и кольцо функций . . . . .	62
3.1.4	Нильпотенты, идемпотенты . . . . .	63
3.1.5	Подкольцо и прямая сумма колец . . . . .	63
3.2	Поля, идеалы и многочлены. Часть 1 . . . . .	65
3.2.1	Поле: определение, характеристика, простое подполе . . . . .	65
3.2.2	Гомоморфизмы колец . . . . .	66
3.2.3	Ядра гомоморфизмов колец и идеалы . . . . .	67
3.2.4	Факторкольца . . . . .	69
3.3	Поля, идеалы и многочлены. Часть 2 . . . . .	72
3.3.1	Делимость в кольце многочленов и главные идеалы . . . . .	72
3.3.2	Корни многочлена . . . . .	74
3.3.3	Цикличность мультиликативной группы конечного поля . . . . .	75
3.3.4	Максимальный идеал. Теорема о максимальном идеале . . . . .	76
3.3.5	Поле частных. Поле рациональных функций . . . . .	77
3.3.6	Расширение полей . . . . .	79
3.4	Евклидовы и факториальные кольца . . . . .	81
3.4.1	Евклидово кольцо: определение и свойства . . . . .	82
3.4.2	Простой идеал . . . . .	84
3.4.3	Ассоциированные и неприводимые элементы . . . . .	85
3.4.4	Факториальное кольцо: определение, свойства . . . . .	89
3.5	Конечные поля . . . . .	90
3.5.1	Векторные пространства . . . . .	91
3.5.2	Поле разложения . . . . .	92
3.5.3	Конечные поля: существование и единственность . . . . .	94
3.5.4	Под поля в конечных полях . . . . .	96
3.5.5	Автоморфизмы конечных полей. Автоморфизм Фробениуса . . . . .	97

## От автора

Это конспект семинаров по курсу «Основ высшей алгебры и теории кодирования». В связи с этим в пособии есть свои плюсы и минусы. Вы найдете внутри решения некоторых интересных задач, но часть теоретических утверждений останутся без доказательств. Специфика этого пособия заключается в том, что оно заточено под определенный курс, который читается на Физтехе. Может так быть, что при чтении вы наткнетесь на сложную тему или приведенные доказательства не будут понятны. В этом случае попробуйте обратиться к другой литературе.

Все книги, которые были использованы при верстке и которые рекомендуются к прочтению, указаны в конце каждого раздела. Если я забыл указать какой-то материал, который явно используется в этой методичке, то приношу свои извинения: это точно не специально, и вы можете написать об этой оказии на [dmckg1999@gmail.com](mailto:dmckg1999@gmail.com), чтобы я добавил необходимые ссылки. Несмотря на отсутствие новизны в материале ниже, он оформлен заметками автора. Автор надеется, что они облегчат чтение материала.

В конце каждого раздела вы можете найти 10 задач, которые читатель должен суметь решить после прочтения соответствующего раздела и, возможно, рекомендуемой литературы. После этих задач всегда идет одна бонусная. Вряд ли вы сможете решить ее с первого раза, но при глубоком погружении в материал и бонусные задачи можно и стоит решать.

Приношу благодарность тем ученикам групп Б05-008, Б05-004, Б05-002, Б05-006, которые при прохождении курса смогли вычитывать методическое пособие и находить в нем ошибки.

Также участие в проведении курса было бы невозможно без кафедры «Математических основ управления» и лично лектора этого курса — Михаила Николаевича Вялого, конспект лекций которого легли в основу этого методического пособия.

Если в процессе чтения вы находите опечатки или ошибки разного рода, то пожалуйста пишите о них на [dmckg1999@gmail.com](mailto:dmckg1999@gmail.com).

*Гущин Д. Д.*

# **Глава 1.**

## **Предварительные сведения**

## 1.1 Базовые понятия из курса дискретного анализа

Эта глава сделана для удобства читателей. В ней представлены основные определения и факты из курса дискретного анализа, которые необходимо помнить для более спокойного изучения курса высшей алгебры.

**Ключевые слова:** бинарное отношение, отношение эквивалентности, класс эквивалентности, отображение, композиция отображений.

### 1.1.1 Отношение эквивалентности

Начнем с некоторых понятий теории множеств. Здесь мы вспомним, что такое бинарные отношения и, в частности, что такое отношения эквивалентности.

**Определение 1.1.1.** Пусть  $A$  — произвольное множество. Тогда **бинарное отношение** — это подмножество  $R$  декартового произведения  $A \times A$ .

**Замечание.**  $A \times A \stackrel{\text{def}}{=} \{(a_1, a_2) : a_1, a_2 \in A\}$ .

Как видите, бинарное отношение показывает, какие упорядоченные пары элементов сравнимы, а какие — нет. Бывают и более общие случаи  $n$ -арных отношений, которые нам не интересны в курсе, поэтому мы про них не будем рассказывать. Здесь мы использовали определенный символ для декартового произведения множеств. Позже мы еще встретимся с этим символом и переопределим его для множеств. Будьте готовы к этому. И не пугайтесь, когда увидите этот знак между двух групп.

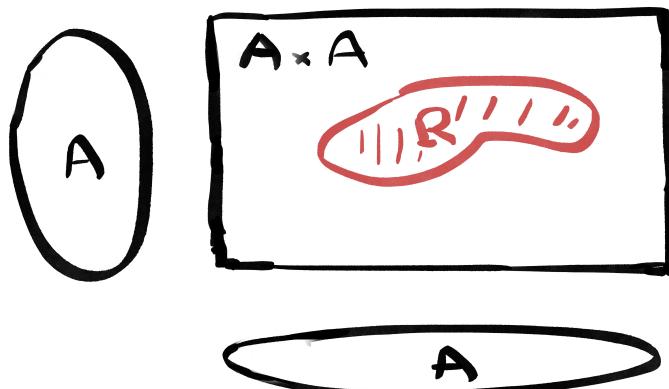


Рис. 1.1: Бинарное отношение

Перейдем к бинарному отношению, которое встречается чаще всего.

**Определение 1.1.2. Отношение эквивалентности** — это бинарное отношение, которое удовлетворяет трём аксиомам:

1.  $\forall a \in A : (a, a) \in R$  (рефлексивность);
2.  $\forall a, b \in A : (a, b) \in R \Rightarrow (b, a) \in R$  (симметричность);
3.  $\forall a, b, c \in A : (a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$  (транзитивность).

**Замечание.** Для более простого обозначения пишут обычно не  $(a, b) \in R$ , а  $aRb$ . В случае отношения эквивалентности само отношение часто обозначают «тильдой», то есть эквивалентность элементов  $a, b$  записывают так:  $a \sim b$ .

Зачем мы задаем отношение эквивалентности? Если попробовать посмотреть, какие элементы эквивалентны между собой, то мы заметим, что они образуют некоторые подмножества, которые не пересекаются между собой. Четырех этих подмножеств есть формальное название.

**Определение 1.1.3.** Пусть на множестве  $A$  задано отношение эквивалентности  $R$ . Тогда **классом эквивалентности** называются множество элементов  $b$  эквивалентных фиксированному элементу  $a$ , то есть

$$K_a = \{b : b \in A, (a, b) \in R\}.$$

Из определения может быть еще непонятно, как между собой соотносятся разные классы эквивалентности. А на самом деле суть в том, что классы эквивалентности могут либо совпадать, либо не пересекаться. Больше им альтернатив не дано. Давайте докажем это.

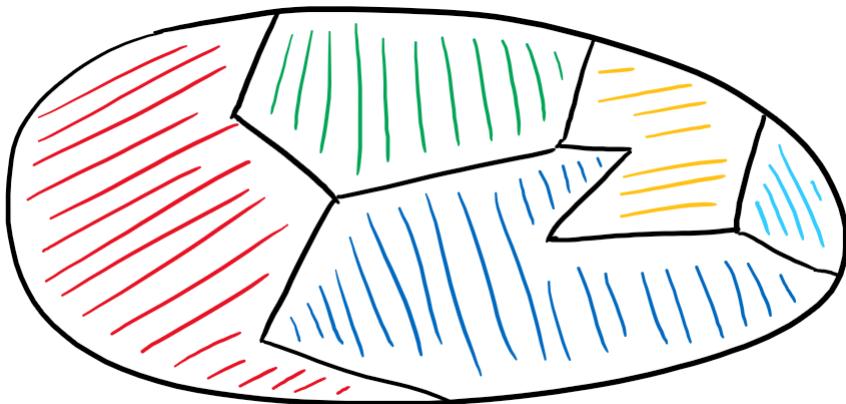


Рис. 1.2: Разбиение множества на классы эквивалентности

**Утверждение 1.1.4.** Пусть на множестве  $A$  задано отношение эквивалентности  $R$ . Тогда классы  $K_a$  и  $K_b$  пересекаются тогда и только тогда, когда  $K_a = K_b$ .

*Доказательство.* Заметим, что по рефлексивности каждый из классов эквивалентности не пуст, так что из того, что они совпадают с очевидностью следует, что их пересечение не пусто. Следовательно, нам остается доказать в прямую сторону это утверждение.

Предположим, что  $c \in K_a \cap K_b$ . Покажем, что каждый из классов содержится в другом, откуда будет следовать, что они совпадают. Пусть  $K_a \not\subseteq K_b$ , тогда существует такой элемент  $d \in K_a \setminus K_b$ , то есть элемент не эквивалентный  $b$ . Заметим, что  $d \sim c$ , так как  $c \in K_a$ . А кроме этого  $c \sim b$ , так как  $c \in K_b$ . По транзитивности получается, что  $d \sim b$ , что противоречит нашему предположению.

Получается, что каждый из классов лежит содержится в другом, что дает нам искомую импликацию. ■

Итак, всякий раз, как в курсе будут встречаться отношения эквивалентности, мы тут же будем вспоминать о классах эквивалентности, которые будут использоваться в дальнейших наших рассуждениях. При этом впоследствии мы не будем использовать обозначение  $K_a$ , а будем просто писать  $K$ , подразумевая, что не важно, какой представитель в этом классе выбирать. Иногда это будет заводить нас в фантомный тупик, так как придется доказывать корректность того или иного определения, которая будет возникать от того, что мы можем указывать различные представители в классах эквивалентности. Однако не переживайте: с опытом придет понимание, в какие моменты и почему необходимо доказательство корректности некоторых определений.

## 1.1.2 Отображения

Не менее важное понятие, которое раскроется, когда мы будем обсуждать перестановки и позже — группы преобразований, — это отображение. Оно представляет из себя правило, по которому производится сопоставление элементам одного множества элементов другого множества. Это неформальное определение, которое мы часто будем вспоминать.

Для тех же, кто скрупулезно вчитывается в текст и ищет формалистики, мы выпишем формальное определение отображения ниже. Однако в отличие от неформального определения выше мы никогда не будем явно обращаться к тому, что ниже.

**Определение 1.1.5. Отображение** — это  $\varphi \subseteq X \times Y$ , которое удовлетворяет свойствам:

O1.  $\forall x \in X \exists y \in Y: (x, y) \in \varphi$  (всюду определенность);

O2.  $\forall x \in X \forall y_1, y_2 \in Y: (x, y_1) \in \varphi, (x, y_2) \in \varphi \Rightarrow y_1 = y_2$  (однозначность).

**Замечание.** Отметим, что здесь и далее мы будем считать, что  $\text{Dom } \varphi = X$ , то есть отображение является всюду определенной функцией. Бывают и другие нотации, но они имеют смысл, когда отображения рассматриваются под лупой, а не используются как инструмент.

**Замечание.** По классике мы будем писать не  $\varphi \subseteq X \times Y$ , а  $\varphi: X \rightarrow Y$ .

С отображениями связаны отношения эквивалентности, которые мы рассматривали ранее. Как? Рассмотрим отображение  $\varphi: X \rightarrow Y$ . Зададим отношения эквивалентности, согласованное с этим отображением, а именно:

$$\forall x_1, x_2 \in X: x_1 \sim x_2 \Leftrightarrow \varphi(x_1) = \varphi(x_2)$$

Класс такой эквивалентности обычно называют *слоем*. Также он всегда является прообразом одноэлементного множества из  $\text{Im } \varphi$ .

**Упражнение.** Проверить, что  $x_1 \sim x_2 \Leftrightarrow \varphi(x_1) = \varphi(x_2)$  отношение эквивалентности на  $X$ .

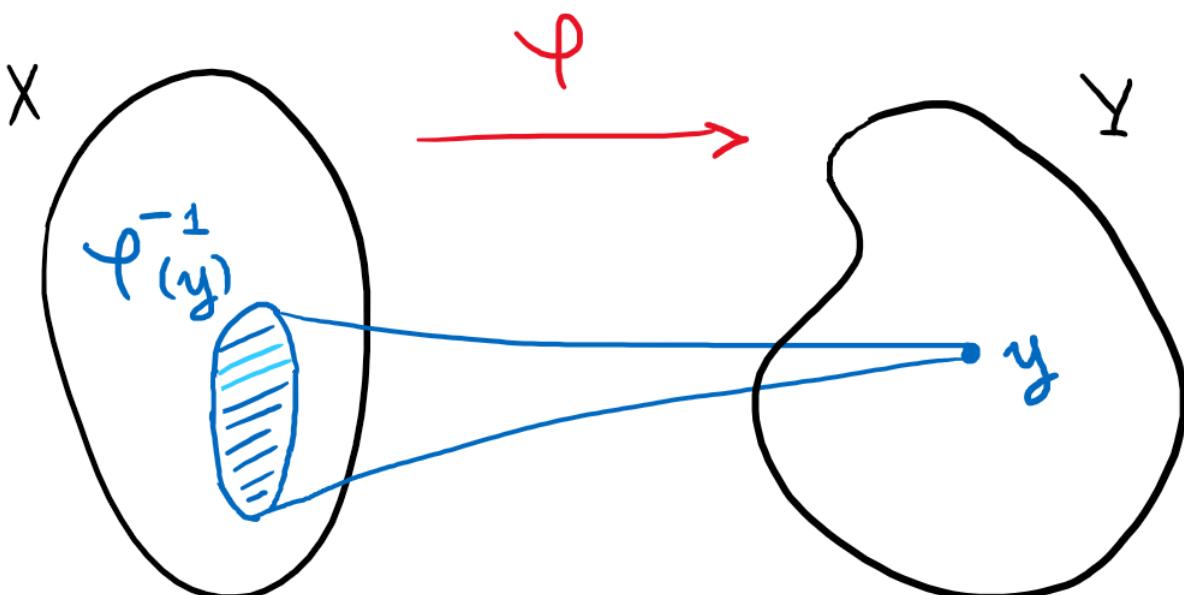


Рис. 1.3: Слой отображения  $\varphi$

Отображение  $\varphi$  можно представлять различными способами. Мы разберем несколько из них, которые мы часто неосознанно будем использовать.

*Список.* Если отображение  $\varphi$  задано на конечном множестве, то можно попробовать указать, какие элементы куда переходят.

**Пример 1.1.6.** Предположим, что  $\varphi: X \rightarrow X$ , где  $X = \{0, 1, 2, 3\}$ . Можем описать это отображение так

$$\varphi: 0 \rightarrow 0, 1 \rightarrow 2, 2 \rightarrow 0, 3 \rightarrow 2.$$

*Формула.* Это самый привычный вам способ, когда мы можем записать отображение с помощью формулы, подразумевая, что в нее можно подставить любой элемент области определения.

**Пример 1.1.7.** Отображение  $\varphi(x) = 2x, x \in \mathbb{R}$ .

*Двудольный граф.* Также если дано отображение  $\varphi: X \rightarrow Y$ , мы можем схематично обозначить каждое из множеств и с помощью стрелок показывать, какие элементы куда переходят.

*Орграф.* Наверное самым полезным представлением будет представление отображение в виде орграфа. В этом виде мы обозначаем элементы множества через точки, а стрелками указываем, кто и куда переходит. При этом у каждой точки из  $X$  исходящая степень равна 1.

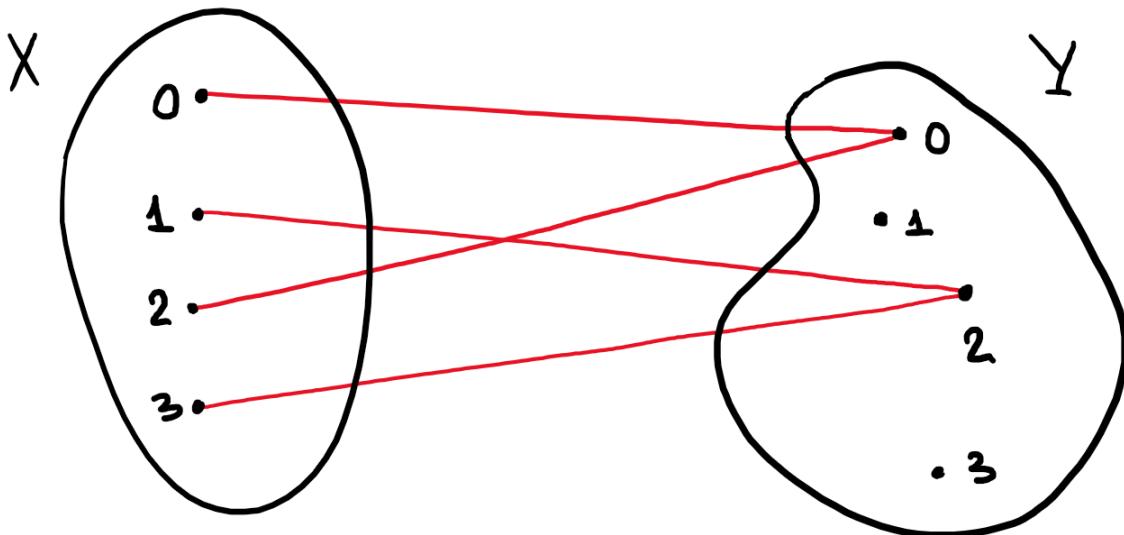


Рис. 1.4: Отображение  $\varphi$  из примера 1.1.6 в виде двудольного графа

Почему нам будет интересно такое представление? Дело в том, что для биективных отображений (перестановок), где  $X = Y$ , орграф представляет из себя набор циклов. Циклов в смысле замкнутого ориентированного пути. Здесь мы имеем в виду конечно, что петля может существовать и она является циклом длины 1.

**Пример 1.1.8.** Отображение  $\psi$ , заданное ниже, представляет из себя перестановку на 4 элементах, которую можно разложить в два цикла:  $(012)$  и  $(3)$ . Такие разложения мы в скором времени учтем и будем использовать для алгебраических целей. В данном случае итоговая перестановка имеет вид

$$\psi = (012)(3).$$

Последнее, что надо обозначить в этом разделе — *композицию отображений*. Если даны два отображения  $f: X \rightarrow Y$ ,  $g: Y \rightarrow Z$ , то их композицией будем называть отображение  $g \circ f: X \rightarrow Z$ , которое определяется следующим образом

$$\forall x \in X: (g \circ f)(x) \stackrel{\text{def}}{=} g(f(x)).$$

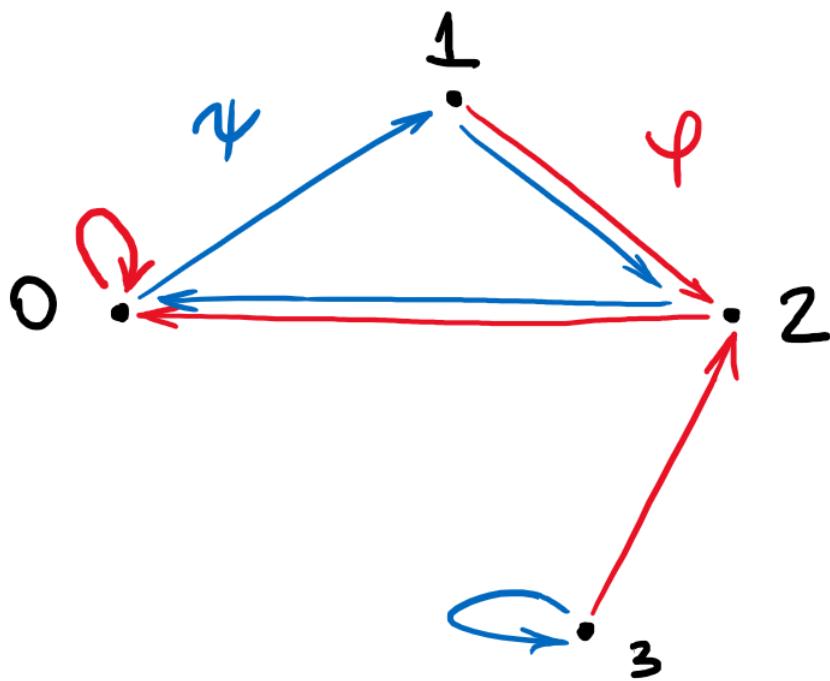


Рис. 1.5: Отображения  $\varphi$  и  $\psi$

Обратим сразу ваше внимание на то, что первое применяемое отображение в композиции пишется с правой стороны, а не с левой стороны. Не путайте!

Здесь нам понадобится следующее утверждение.

**Утверждение 1.1.9.** Пусть  $f$  — биекция,  $g$  — биекция. Тогда  $g \circ f$  — биекция.

*Доказательство.* В силу сюръективности  $g$  у каждого  $z \in Z$  есть прообраз в  $Y$ , а так как  $f$  тоже сюръективно, то и у любого  $y \in Y$  есть свой прообраз, так что сюръективность композиции здесь очевидна. Остается показать, что элементы не могут «склеиться» под действием двух инъектививных отображений, так что композиция так же инъективна. ■

Помимо этого нам может понадобится следующее утверждение, которое поможет доказывать биективность отображения очень быстро.

**Утверждение 1.1.10.** Если  $X$  — конечное множество, то для  $\varphi: X \rightarrow X$  эквивалентны следующие альтернативы:

1.  $\varphi$  — биекция;
2.  $\varphi$  — сюръекция;
3.  $\varphi$  — инъекция.

Итак, мы вспомнили, что такое отношение эквивалентности и как оно связано с отображениями. Кроме этого мы обсудили разные представления отображений и сформулировали утверждения, которые впоследствии понадобятся при работе с перестановками.

## Рекомендуемая литература

- [1] Сабурова Н. Ю. — Множества, отношения, функции — Архангельск: Арханг. гос. тех. ун-т, 2008.

- [2] Верещагин Н. К., Шень А. — Лекции по математической логике и теории алгоритмов. Ч. 1. Начала теории множеств — 4-е изд., доп. — М.: МЦНМО, 2012. — Глава 1, §1-7.
- [3] Курош А. Г. — Лекции по общей алгебре. — М.: Физ.-мат. лит., 1962. — Глава первая, §1, 2, 3.
- [4] Городенцев А. Л. — Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 1, §1.
- [5] Кострикин А. И. — Введение в алгебру: В 3-х ч. — Четвертое издание, стереотип. — М.: МЦНМО, 2020. — Глава 1, §5, 6.

## 1.2 База теории чисел

Теория чисел очень сильно связана с теорией групп. Более того, некоторые теоремы как одной, так и другой областей доказываются в одну строчку, если рассматривать теорему на языке другой теории. Ниже мы дадим пару страниц основ в теории чисел, которые стоит помнить независимо от понимания теории групп. Однако впоследствии из этих простых утверждений и групповых свойств мы сможем получить интересные результаты.

**Ключевые слова:** делимость целых чисел, наибольший общий делитель, соотношение Безу, расширенный алгоритм Евклида, линейные диофантовые уравнения, простое число, основная теорема арифметики, функция Эйлера.

### 1.2.1 Алгоритм Евклида

Начинается эта теория с того, что мы умеем не только складывать целые числа, но и умножать. Одна из самых важных аксиом целых чисел звучит неформально так: мы можем любое целое число разделить на другое целое число с остатком. Формально это условие задается следующей формулой:

$$\forall a, b \in \mathbb{Z}: \exists q, r \in \mathbb{Z}: a = q \cdot b + r, \quad r = 0 \vee 1 \leq r < |b|.$$

Здесь число  $r$  называется *остатком*, а число  $q$  — *частным*.

**Замечание.** Глубокий смысл, зачем мы в формуле выше отделили случай  $r = 0$  от других, станет очевиден только после того, как мы рассмотрим евклидовы кольца. Пока что можете считать, что этот случай объясняется необходимостью в следующем определении.

**Определение 1.2.1.** Если при делении  $a$  на  $b$  мы получили в остатке ноль, то мы будем говорить, что  $a$  *делится на*  $b$  или  $b$  *делит*  $a$ . При этом будем писать  $b \mid a$ .

Мы знаем, что любые два целых числа делятся на 1. Следовательно, множество общих делителей двух целых чисел всегда непусто. Мы можем рассмотреть наибольший (по модулю) из общих делителей двух чисел. Он очевидно называется *наибольший общий делитель*. Мы его будем обозначать через  $\text{НОД}(a, b)$  или просто  $(a, b)$ . Нам будут полезны следующие две теоремы.

**Теорема 1.2.2** (соотношение Безу). Если  $(a, b) = d$ , то существуют  $u, v \in \mathbb{Z}$ , что  $au + bv = d$ .

**Теорема 1.2.3.** У любых двух целых чисел  $a, b$  существует и единственен (с точностью до знака) наибольший общий делитель. Он делится на любой общий делитель  $a, b$ .

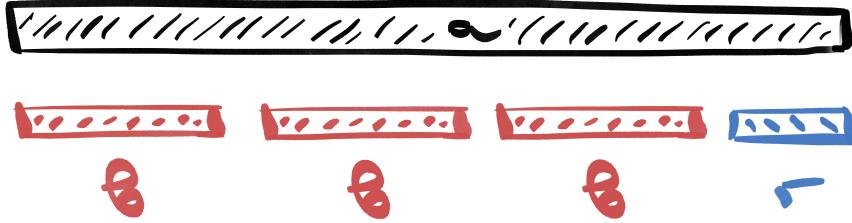


Рис. 1.6: Наглядная иллюстрация деления с остатком

Вторая теорема следует из первой, но обе важны. Мы будем параллельно доказывать эти теоремы, используя *расширенный алгоритм Евклида*. Опишем его.

**Шаг 1.** На вход алгоритма мы подаем два числа  $a, b$ . Без ограничения общности будем считать, что они положительны, так как

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

Кроме того, мы можем считать, что  $a > b$ . Каждой такой паре  $a, b$  мы можем сопоставить их сумму в качестве характеристики, которая будет уменьшаться хотя бы на единицу каждым шагом нашего алгоритма. Это автоматически будет означать, что алгоритм в какой-то момент прервется.

**Шаг 2.** Вначале мы проверяем, делится ли  $a$  на  $b$ . Если да, то мы говорим, что число  $b$  и есть искомое число (проверьте, что это так). Иначе мы делаем шаг алгоритма.

Шаг алгоритма Евклида будет выглядеть так: от пары  $a, b$  мы перейдем к паре  $b, r$ , где  $r$  — остаток при делении числа  $a$  на  $b$ . То есть число  $r$  определяется из равенства

$$a = q \cdot b + r, \quad r = 0 \vee 1 \leq r < |b|.$$

Повторяем этот шаг до тех пор, пока первое число не будет делится на второе.

**Упражнение.** Покажите, что если  $r_{k-1} = q_k \cdot r_k + r_{k+1}$ , то

$$\forall d \in \mathbb{Z}: d \mid (r_{k-1}, r_k) \Leftrightarrow d \mid (r_k, r_{k+1}).$$

Из этого упражнения следует, что множество общих делителей не меняется при процедуре, описанной выше. И при этом в конце мы имеем дело с двумя кратными числами. Из этого автоматически следует утверждение теоремы выше.

**Шаг 3.** Теперь мы хотим получить соотношение Безу. Для этого мы должны заметить, что между парами  $r_{k+1}, r_k$  и  $r_k, r_{k-1}$  имеется линейная связь, с помощью которой мы можем подниматься наверх по нашей системе равенств. Как это происходит?

Допустим, что мы смогли выразить наибольший общий делитель через  $r_k, r_{k+1}$ , то есть

$$\exists \alpha_{k+1}, \beta_{k+1}: d = \alpha_{k+1}r_k + \beta_{k+1}r_{k+1}.$$

Мы знаем, что  $r_{k+1} = r_{k-1} - q_k r_k$ . Подставим это выражение в равенство выше:

$$d = \alpha_{k+1}r_k + \beta_{k+1}r_{k+1} = \alpha_{k+1}r_k + \beta_{k+1}(r_{k-1} - q_k r_k) = \beta_{k+1}r_{k-1} + (\alpha_{k+1} - q_k \beta_{k+1})r_k,$$

то есть  $\alpha_k = \beta_{k+1}$ ,  $\beta_k = \alpha_{k+1} - q_k \beta_{k+1}$ .

Получается, что мы можем подниматься по нашей системе равенств наверх и итоге мы получим равенство, где слева будет  $d$ , а справа — линейная комбинация  $a$  и  $b$ , что доказывает соотношение Безу.

**Пример 1.2.4.** Найдем НОД(28, 22). Спускаемся по алгоритму Евклида

$$\begin{aligned} 28 &= 22 + 6, \\ 22 &= 3 \cdot 6 + 4, \\ 6 &= 4 + 2, \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

Получается, что  $(28, 22) = 2$ . Теперь по третьему шагу находим выражение для наибольшего общего делителя:

$$\begin{aligned} 2 &= 4 - 2 = 4 - (6 - 4) = 2 \cdot 4 - 6 = 2 \cdot (22 - 3 \cdot 6) - 6 = \\ &= 2 \cdot 22 - 7 \cdot 6 = 2 \cdot 22 - 7 \cdot (28 - 22) = -7 \cdot 28 + 9 \cdot 22. \end{aligned}$$

Чтобы показать практическую необходимость в этом алгоритме, мы покажем, как с помощью него можно решать линейные диофантовы уравнения.

## 1.2.2 Линейные диофантовы уравнения

На самом деле диофантовых уравнений очень много (все они подразумевают поиск решения в целых числах). И некоторые из них настолько просты в записи, насколько сложны в решении (вспомнить, чего стоит одна Великая Теорема Ферма). Мы же разберем один простой класс этих уравнений: линейные диофантовы уравнения от двух переменных:

$$ax + by = c.$$

Если у чисел  $a, b, c$  есть общий делитель, то разделим на него все числа. Тогда без ограничения общности, мы можем считать, что у них нет общего неединичного делителя. Теперь предположим, что  $(a, b) = d \neq 1$  и при этом число  $c$  не делится на  $d$ . Тогда какие бы целые  $x, y$  мы не подбирали, решением это являться не будет, а следовательно, множество решений пусто.

Теперь предположим, что  $(b, c) = t \neq 1$  и при этом  $(a, t) = 1$ . Тогда мы автоматически получаем, что  $x$  всегда делится на  $t$ . Сделаем замену  $x = t \cdot x'$ . И придет к случаю, когда любые два коэффициента взаимно просты. Такую систему мы и научимся дальше решать.

Для начала заметим, что из соотношения Безу для чисел  $a, b$  следует существование решения у линейного диофантового уравнения:

$$a \cdot (uc) + b \cdot (vc) = (au + bv) \cdot c = 1 \cdot c = c.$$

Давайте обозначим частное решение через  $x_0$  и  $y_0$ . Посмотрим на общее решение нашего уравнения:

$$ax + by = c.$$

Мы можем вычесть из общего решения частное и получить:

$$a(x - x_0) + b(y - y_0) = 0 \Leftrightarrow a(x - x_0) = -b(y - y_0),$$

так как  $a, b$  взаимно просты, то мы можем сказать, что разница  $x - x_0$  должна делиться на  $b$ , то есть  $x - x_0 = bt$ , где  $t \in \mathbb{Z}$ . При подстановке в уравнение получаем, что тогда  $y - y_0 = -at$ . И видим, что при этом подходящее для пары число  $y$  однозначно восстанавливается и тоже является целым. Следовательно, общее решение имеет вид:

$$x = x_0 + bt, \quad y = y_0 - at, \quad t \in \mathbb{Z}.$$

**Пример 1.2.5.** Решите диофантово уравнение  $23x - 33y = 2$ .

Для этого сначала находим частное решение с помощью расширенного алгоритма Евклида:

$$(33, 23) = (23, 10) = (10, 3) = (3, 1) = 1 \Rightarrow 23 \cdot 23 - 33 \cdot 16 = 2 \Rightarrow x_0 = 23, y_0 = 16.$$

И из выкладок выше получаем общее решение и ответ:

$$x = 23 + 33t, \quad y = 16 + 23t, \quad t \in \mathbb{Z}.$$

### 1.2.3 Основная теорема арифметики

В этом разделе мы сформулируем важную теорему, которая показывает, что делимость хоть и сложнее сложения чисел, но тоже имеет свои атомы, которые интересны как с теоретической, так и с прикладных точек зрения.

**Определение 1.2.6.** Целое число  $p$  называется **простым**, если из  $d | p$  следует, что  $d = \pm 1$  или  $d = \pm p$ .

**Замечание.** Так как мы рассматриваем целые числа, то в определении стоит плюс–минус. Если бы мы заменили целые числа, на натуральные, то этих знаков не было бы. И суть здесь не только в знаках, но и в том, какие элементы мы можем обратить по умножению, не выходя из множества целых чисел (например,  $(-1) \cdot (-1) = 1$ ).

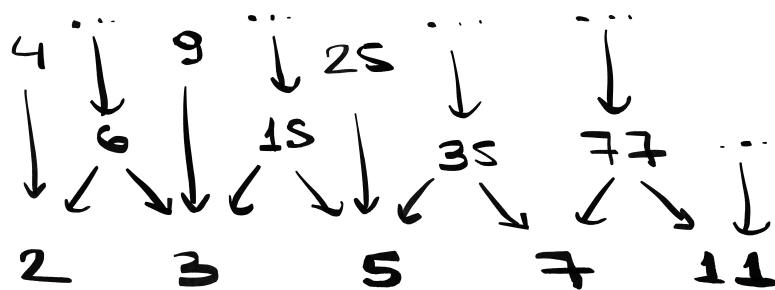


Рис. 1.7: Наглядная иллюстрация деления с остатком

**Теорема 1.2.7 (основная теорема арифметики).** Любое целое число раскладывается в произведение простых единственным образом до их порядка и множителя  $\pm 1$ .

Заметьте, что эта теорема утверждает, что такое разложение существует и единственно. Однако никто нам само разложение не предоставляет. И это важно, так как поиск разложения на простые множители — это очень важная задача, сложность решения которой непосредственно связано с качеством шифрования систем связи в мире.

Мы про криптографию в курсе говорить не будем, но эта теорема нам понадобится, когда мы столкнемся с функцией Эйлера.

## 1.2.4 Функция Эйлера

Эта функция будет связывать порядки некоторых двух групп, так что знакомство с ней важно для понимания.

**Определение 1.2.8.** Пусть  $n \in \mathbb{N}$ . **Функция Эйлера от числа  $n$**  — это число натуральных чисел, не больших чем  $n$  и взаимно простых с ним. Это число обозначают  $\varphi(n)$ .

Легко понять, что  $\varphi(n) = n - 1$  тогда и только тогда, когда число  $n$  просто. Также легко понять, что если  $n$  — это степень простого числа  $p$ , то есть  $n = p^m$ , то  $\varphi(n) = p^m - p^{m-1}$ . Этот опыт можно обобщить и получить общую формулу для функции Эйлера.

**Теорема 1.2.9.** Пусть  $n = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$ , где разложение выбрано так, чтобы  $p_i$  не равнялось  $p_j$ , когда  $i \neq j$ . Тогда

$$\varphi(n) = (p_1^{m_1} - p_1^{m_1-1})(p_2^{m_2} - p_2^{m_2-1}) \cdots (p_s^{m_s} - p_s^{m_s-1}) = n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

## Рекомендуемая литература

- [1] Виноградов И. М. — Основы теории чисел. — М.-Л., Гостехиздат, 1952. — Глава 1, §1, 2, 5, 6; Глава 2, §4.
- [2] Дэвенпорт Г. — Высшая арифметика. Введение в теорию чисел. — Изд. "Наука" 1965 — Глава I, II.
- [3] Городенцев А. Л. — Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 2, §2.
- [4] Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Разделы 1.

## **Глава 2.**

# **Общая теория групп**

## 2.1 Основы теории групп

В этой лекции мы обсудим первые понятия теории групп. Начнем с самого простого и базового в нашем курсе — с ответа на вопрос: «Что такое группа?» В частности мы разберем пару примеров естественных групп, появляющихся в комплексном анализе, а также в геометрии. Потом мы обсудим, что такое подгруппы и циклические группы, увидим, что в любой группе можно найти циклическую подгруппу. В заключение мы обсудим, что такое порядок элемента, и поймем, почему он делит порядок группы.

**Ключевые слова:** бинарная операция, полугруппа, моноид, группа, группа вычетов, группа корней из единицы, абелева группа, подгруппа, смежные классы, индекс подгруппы, теорема Лагранжа, циклическая группа, порождающий, порядок элемента.

### 2.1.1 Полугруппа, моноид, группа

Как мы увидим ниже, группы появляются естественно в задачах, но их не всегда легко исследовать. Поэтому важно помнить разные свойства групп и держать в голове структуру их построения, чтобы благодаря ей, получать разные интересующие нас свойства.

По сути в течение всего курса мы будем исследовать множества с введенными бинарными операциями (бывают еще тернарные операции или операции  $n$ -арные, но мы про них упоминать в курсе не будем).

**Определение 2.1.1.** Бинарной операцией на множестве  $S$  будем называть отображение

$$\circ: S \times S \rightarrow S.$$

**Пример 2.1.2.** В школе учат тому, как складывать и вычитать числа  $x, y \in \mathbb{Z}$ . С того времени вы должны помнить, что сумма и разность целых чисел — это целое число. Это в точности и означает, что операции  $+, -$  являются бинарными операциями на этом множестве.

**Пример 2.1.3.** Кроме этого, вполне вероятно, что вам рассказывали о конъюнкции, дизъюнкции, импликации на дискретном анализе. Каждая из этих операций является бинарной операцией в смысле определения выше на множестве из нуля и единице или на множестве последовательностей длины  $n$  из нулей и единиц.

Как показывает практика, бинарная операция нам дана для того, чтобы мы «перемножали» или «складывали» элементы множества. Но такие действия интересны только в том случае, если мы можем что-то преобразовать и вычислить с помощью них, так что обычно требуют, чтобы бинарная операция удовлетворяла некоторому набору аксиом, благодаря которым исследование алгебраического объекта облегчается.

Начнем с самого простого алгебраического объекта.

**Определение 2.1.4.** Пару  $(S, \circ)$  из множества  $S$  и бинарной операции на нем будем называть **полугруппой**, если выполнена следующая аксиома

$$S1. \forall x, y, z \in S \mapsto x \circ (y \circ z) = (x \circ y) \circ z \text{ (ассоциативность).}$$

**Пример 2.1.5.** Множество  $S$  произвольной природы можно наделить, например, следующей полугрупповой операцией:

$$\forall x, y \in S \mapsto x \circ y = x.$$

Аксиома П1 выполняется, так как каждое из произведения, которые там стоят, представляет из себя левый множитель, то есть  $x$ . Именно поэтому, это множество образует полугруппу. Эта полугруппа называется **полугруппой правых единиц**. Смысл такого названия станет понятен чуть позже.

**Пример 2.1.6.** Более типичным примером полугруппы будет пара  $(\mathbb{N}, +)$ .

**Пример 2.1.7.** Если мы рассмотрим какое-то множество  $S \subseteq \mathbb{Q}$ , то это множество будет образовывать полугруппу с операцией  $\max$ , которая определяется естественным образом.

Можно заметить, что в последнем примере, если множество  $S$  содержит свой инфимум, то мы можем сказать, что

$$\forall x \in S \mapsto \max(x, \inf S) = \max(\inf S, x) = x.$$

Это свойство очень похоже на свойство нуля на множестве действительных чисел. Оно появляется много где, поэтому и имеет смысл следующее определение.

**Определение 2.1.8.** Пара  $(M, \circ)$  из множества и бинарной операции называется **моноидом**, если выполнены следующие аксиомы

M1.  $\forall x, y, z \in M \mapsto x \circ (y \circ z) = (x \circ y) \circ z$  (ассоциативность);

M2.  $\exists e \in M : \forall x \in M \mapsto x \circ e = e \circ x = x$  (нейтральный элемент).

Моноиды уже чаще встречаются в разных областях математики (например, у них есть необычное применение в теории реализации языков программирования). Они не сильно отличаются от полугрупп, так как, во-первых, моноид всегда является полугруппой, а во-вторых, полугруппу всегда формально можно расширить до моноида.

**Утверждение 2.1.9.** Если полугруппа  $(S, \circ)$  не является моноидом, то пара  $(S \cup \{e\}, \circ)$  с формальным элементом  $e$ , который умножается как нейтральный элемент, является моноидом.

**Пример 2.1.10.** Можно заметить, что в  $\mathbb{N}$  нет нейтрального элемента по сложению. Так что его можно добавить туда, тогда мы получим моноид, который своей аддитивной структурой является не чем иным как  $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ .

**Пример 2.1.11.** В разных областях математики всплывают такие понятия, как языки. Их обычно задают следующим образом. Зафиксируем какое-то непустое множество  $\Lambda$  и обозначим за  $\Lambda^n$  последовательности длины  $n$  из букв из множества  $\Lambda$  (обычно их пишут подряд  $\alpha_1 \alpha_2 \dots \alpha_n$  и называют словами). Тогда множеством всех слов будет

$$\Lambda^* = \left( \bigcup_{n=1}^{\infty} \Lambda^n \right) \cup \{\lambda\},$$

где последнее слагаемое  $\lambda$  является тем самым «пустым словом», которое при конкатенации (приписывании рядом двух слов) со словом  $u$  дает само же слово  $u$ . Как мы видим, в этом слово и воплощается идея о том, что мы можем полугруппу дополнить до моноида.

В тех же рациональных числах мы можем увидеть, что не просто существует нейтральный элемент по сложению (ноль), но и у любого элемента есть такой, который при сложении даст нейтральный. Такой элемент называется *обратным элементом* и он дополняет аксиоматику центрального понятия первой трети курса — группы.

**Определение 2.1.12.** Пара  $(G, \circ)$ , состоящая из множества  $G$  и бинарной операции на нем, называется **группой**, если выполнены следующие аксиомы

G1.  $\forall x, y, z \in G \mapsto x \circ (y \circ z) = (x \circ y) \circ z$  (ассоциативность);

G2.  $\exists e \in G : \forall x \in G \mapsto x \circ e = e \circ x = x$  (нейтральный элемент);

G3.  $\forall a \in G \exists b \in G: a \circ b = b \circ a = e$  (обратный элемент).

**Замечание.** Мощность группы принято называть ее *порядком*.

**Замечание.** Как мы видим, чтобы определить обратный, необходимо знать, что такое нейтральный элемент, поэтому без аксиомы G2 аксиома G3 особого смысла не имеет.

**Замечание.** Обычно обратный элемент к элементу  $a$  обозначают элементом  $a^{-1}$ .

**Замечание.** Стоит обратить внимание на то, что по определению бинарная операция замкнута, то есть ее результат лежит в том же множестве, что и те два элемента, к которым мы ее и применяли. С другой стороны, не всегда это так, операции можно определять более общим способом. В таких случаях стоит отдельно проверять замкнутость (иногда это свойство выписывают в качестве нулевого).

Примеров групп настолько много, что можно хоть посвятить все оставшиеся занятия изучению их. Однако у нас нет столько времени, так что мы приведем далее некоторые базовые группы, которые естественно возникают при изучении высшей математики. Их не стоит запоминать, но обратите внимание на то, почему соответствующие пары являются группами: чаще всего за этим стоит некоторое важное свойство.

## 2.1.2 Естественные примеры групп

Начнем с простых числовых групп, с которыми вы сталкивались еще в школе.

**Пример 2.1.13.** Числовые множества  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  с привычным для нас сложением являются группами. Такие группы называют *аддитивными*.

**Пример 2.1.14.** Множества  $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$  являются также группами относительно умножения. Эти группы называют *мультипликативными*.

Разница между аддитивными группами и мультипликативными группами становится видна только тогда, когда начинаешь изучать кольца: в них уже есть две операции, которые традиционно и называют аддитивной и мультипликативной операцией. Сейчас же относитесь к этим понятиям как к научному соглашению, которые при этом никаких новых свойств группе не прибавляют.

**Пример 2.1.15.** Еще один важный класс групп, которые рассматриваются в основах теории чисел, — это группы вычетов. Они определяются так: берем множество  $\overline{0, n - 1}$  и определяем сложение и умножение как обычное сложение и умножение соответственно, но после которого берется остаток по модулю  $n$ .

Можно заметить, что  $(\overline{0, n - 1}, +)$  становится тогда группой. Эту группу называют *аддитивной группой вычетов* и обозначают  $\mathbb{Z}_n$  или  $\mathbb{Z}/n\mathbb{Z}$ .

А вот по умножению мы не сразу получаем группу. Достаточно заметить, что у нуля нет обратного по умножению, так что его стоит точно выбросить. Общая теория говорит, что помимо нуля надо выбросить все элементы, которые не взаимно просты с  $n$ . Тогда оставшиеся элементы будут образовывать группу (это следует из Алгоритма Евклида), которая и называется *мультипликативной группой вычетов*. Она обычно обозначается  $\mathbb{Z}_n^*$  или  $(\mathbb{Z}/n\mathbb{Z})^*$ .

Имеют место также комплексные группы, с которыми вы можете встретиться при изучении комплексного анализа, групп Ли или алгебраической топологии. Отметим, что при базовом изучении комплексных чисел вводятся такие понятия как модуль, сопряженное комплексные числа, формула Эйлера и прочее — мы считаем, что вы с ними знакомы.

**Пример 2.1.16.** Вспомним, что геометрически  $\mathbb{C}$  можно изобразить как плоскость  $\mathbb{R}^2$ . Тогда множество комплексных чисел по модулю равных единице образуют единичную окружность с центром в  $(0; 0)$ . Эти комплексные числа по умножению замкнуты и образуют группу, как легко проверить. Будем ее обозначать так:

$$\mathbb{T} = (\{z \in \mathbb{C}: |z| = 1\}, \times).$$

В англоязычном мире эту группу принято называть *group of unit complex numbers*. В русскоязычной литературе какого-то каноничного названия нет.

**Замечание.** Группу  $\mathbb{T}$  можно встретить в разных областях высшей математики и теоретической физики. Часто ее обозначают по-другому: либо  $U(1)$ , либо  $SO(2)$ .

Мы практически не будем залезать на территорию дифференциальной геометрии, а скорее потратим большую часть времени осмысливая дискретные группы, которые иногда можно представить на плоскости.

**Пример 2.1.17.** В  $\mathbb{T}$  есть много групп конечного порядка. Например, мы можем рассмотреть множество комплексных чисел, которые в  $n$ -й степени дают единицу. Оказывается, они образуют группу. Будем ее обозначать через  $\mu_n$ .

Элементы этой группы легко перечислить:

$$z^n = 1 \Leftrightarrow z = e^{i\varphi}, \varphi = 0, 1 \cdot \frac{2\pi}{n}, 2 \cdot \frac{2\pi}{n}, \dots, (n-1) \cdot \frac{2\pi}{n} \Leftrightarrow z = \zeta_k = e^{i\frac{2\pi k}{n}}, k \in \overline{0, n-1}.$$

Можно удостовериться, что во всех примерах выше множители (или слагаемые) можно было переставлять между собой. Это свойство очень важно с алгебраической точки зрения, так что отдельно выделяют следующий класс групп.

**Определение 2.1.18.** Абелевой группой называют группу  $(G, \circ)$ , которая удовлетворяет следующей аксиоме

G4.  $\forall a, b \in G \mapsto a \circ b = b \circ a$  (коммутативность).

На самом деле не все группы абелевы. А если говорить совсем честно, то практически все группы, которые представляют научные интерес сейчас, неабелевы. С одним из классов неабелевых групп — групп перестановок — мы познакомимся ближе на следующей лекции, а сейчас приведем простой пример неабелевой группы, с которой вы работаете на курсе линейной алгебры.

**Пример 2.1.19.** Пусть  $n > 1, n \in \mathbb{N}$ , тогда обозначим за  $GL(n, \mathbb{R})$  множество обратимых матриц размера  $n \times n$  над полем  $\mathbb{R}$  (что такое поле, будет ясно, когда дойдем до них). Эти матрицы образуют группу относительно умножения. Эта группа не абелева. Например,  $n = 2$ :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

### 2.1.3 Подгруппы, классы смежности

Как и во многих других разделах высшей математики, свойства группы могут наследоваться некоторыми подмножествами в  $G$ , из-за чего последние тоже становятся группами.

**Определение 2.1.20.** Пусть  $H$  является подмножеством в  $G$ , где последнее множество образует группу с операцией  $\circ$ . Подмножество  $H$  называется **подгруппой**, если  $(H, \circ)$  — группа.

**Замечание.** С формальной точки зрения надо понимать, что операции  $\circ$  на  $H$  и на  $G$  будут разными, так как по определению операция  $\circ$  изначально было отображением из  $G \times G$  в  $G$ , а впоследствии мы уже подразумевали, что эта операция действует из  $H \times H$  в  $H$ . Так что формально их стоит обозначать по-разному и говорить, что вторая операция есть ни что иное, как ограничение первой на подмножество  $H$ .

**Замечание.** Подгруппа  $H$  в группе  $G$  обычно обозначается так:  $H < G$ .

**Пример 2.1.21.** Можно заметить, что в силу естественности соответствующих числовых аддитивных групп имеет место следующее вложение

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}.$$

**Пример 2.1.22.** Аналогично, вспоминая предыдущий подраздел, мы можем привести пример следующего ряда вложенных друг в друга групп (меньшая будет подгруппой большей)

$$\mu_{n_1} < \mu_{n_1 \cdot n_2} < \mu_{n_1 \cdot n_2 \cdot n_3} < \dots < \mathbb{T},$$

где  $n_i$  — произвольные натуральные числа.

**Пример 2.1.23.** В множестве  $\mathbb{Z}$  подгруппой будет  $2\mathbb{Z}$  — множество четных чисел.

Как можно заметить из последнего примера, все множество  $\mathbb{Z}$  разбивается на два непересекающихся подмножества: четные и нечетные числа. В более общем случае можно написать следующее равенство

$$\mathbb{Z} = n\mathbb{Z} \sqcup (n\mathbb{Z} + 1) \sqcup \dots \sqcup (n\mathbb{Z} + n - 1), \quad (2.1)$$

где под  $n\mathbb{Z}$  мы подразумеваем множество чисел, делящихся на  $n$ , а знак между ними является обычным объединением с дополнительным условием — никакие два множества не пересекаются (в народе такого представление называют разбиением множества  $\mathbb{Z}$  по остатку от деления числа на  $n$ ).

Такие разбиения будут очень интересны нам, поэтому выделим для них отдельное определение.

**Определение 2.1.24.** Пусть заданы группа  $(G, \cdot)$  и подгруппа  $H$  в ней. Будем называть **левыми смежными классами** подмножества следующего вида

$$gH = \{gh : h \in H\},$$

а **правыми смежными классами** подмножества следующего вида

$$Hg = \{hg : h \in H\}.$$

**Замечание.** До обсуждения нормальных групп мы будем под смежными классами всегда подразумевать левые смежные классы. В силу симметричности этих понятий все утверждения, которые мы сформулируем дальше, также могут быть написаны и для правых смежных классов.

**Замечание.** Множество левых смежных классов обозначается через  $G/H$ , а правых —  $H\backslash G$ . Мощности обоих множеств обозначаются через  $[G : H]$  и называются **индексом подгруппы**. Как мы увидим дальше, индекс подгруппы зависит только от  $G$  и  $H$ , но не от того, какие смежные классы мы рассматриваем, поэтому это определение корректно.

Для начала поймем, сколько же элементов в этих смежных классах? Представим, что какие-то два элемента одного смежного класса совпадают

$$gh_1 = gh_2 \Rightarrow h_1 = h_2, \quad (2.2)$$

то есть получается, что  $|gH| = |H| = |Hg|$ .

Помимо этого, чтобы у нас было разбиение как в (2.1), необходимо, чтобы различные смежные классы не пересекались. Оказывается, что это утверждение можно доказать.

**Утверждение 2.1.25.** Пусть заданы группа  $(G, \cdot)$  и подгруппа  $H$  в ней. Левые смежные классы  $g_1H$  и  $g_2H$  имеют непустое пересечение тогда и только тогда, когда они совпадают.

*Доказательство.* В обратную сторону утверждение очевидно, так как следует из теоретико-множественных выкладок.

В прямую сторону будем доказывать следующим образом: предположим, что если какие-то два класса пересекаются, то каждый лежит в другом классе, а значит, они совпадают. Для этого напишем, что

$$g_1H \cap g_2H \neq \emptyset \Rightarrow \exists h_1, h_2 \in H: g_1h_1 = g_2h_2 \Rightarrow g_1 = g_2 \cdot (h_2h_1^{-1}).$$

Так как  $H$  — подгруппа, то она замкнута относительно взятия обратного и относительно произведение, так что мы показали, что  $g_1 \in g_2H$ , откуда немедленно следует

$$\forall h \in H: g_1h = g_2(h_2h_1^{-1}h) \in g_2H \Rightarrow g_1H \subseteq g_2H.$$

В силу симметричности выкладок относительно индексов  $g_1$  и  $g_2$  мы можем сказать, что имеет место и обратное вложение, так что множества совпадают и утверждение доказано. ■

**Следствие 2.1.26.** Если ввести отношение  $R_H$  на группе  $G$ , которое говорит, что элемент  $g_1$  лежит или не лежит в смежном классе  $g_2H$ , то это будет отношением эквивалентности.

*Доказательство.* Действительно, рефлексивность очевидна. Симметричность следует из того, что  $g_1H \ni g_1$ , а транзитивность — из

$$\begin{cases} g_1H \cap g_2H \neq \emptyset, \\ g_2H \cap g_3H \neq \emptyset, \end{cases} \Rightarrow \begin{cases} g_1H = g_2H, \\ g_2H = g_3H, \end{cases} \Rightarrow g_1H = g_2H = g_3H.$$

■

Собирая воедино следствие выше и рассуждения из (2.2), мы можем закончить доказательство следующей важной теоремы.

**Теорема 2.1.27 (Лагранжа).** Пусть  $H$  — подгруппа в конечной группе  $G$ . Тогда

$$[G : H] = \frac{|G|}{|H|}. \quad (2.3)$$

Эта теорема очень важна, так как мы теперь понимаем, что порядок подгруппы обязан делить порядок группы. Следовательно, количество различных подгрупп, которые могут существовать резко сокращается.

**Пример 2.1.28.** Рассмотрим произвольную группу  $G$  простого порядка. Так как порядок любой подгруппы должен делить порядок группы, то в ней подгруппа либо может быть тривиальной (то есть  $\{e\}$ ), либо может совпадать со всей группой. Других вариантов нет. В таких случаях говорят, что в группе нет нетривиальных собственных подгрупп.

**Пример 2.1.29.** Геометрически легко заметить, что  $\mu_k < \mu_n$  тогда и только тогда, когда  $k$  делит  $n$ . При этом по теореме Лагранжа мы знаем, что есть  $|\mu_n|/|\mu_k| = n/k$  смежных классов по этой подгруппе, а значит, они исчерпываются следующим списком

$$\mu_k, e^{i\frac{2\pi \cdot 1}{k}} \cdot \mu_k, e^{i\frac{2\pi \cdot 2}{k}} \cdot \mu_k, \dots, e^{i\frac{2\pi \cdot (k-1)}{k}} \cdot \mu_k.$$

Почти никогда не верно, что если порядок  $G$  делится на число  $k$ , то в группе есть подгруппа такого порядка. Чаще всего подгрупп немногие. Однако есть простые (с точки зрения познания) группы, которые удовлетворяют этому свойству. О них мы и поговорим дальше.

## 2.1.4 Циклические группы

Мы уже пару раз столкнулись с циклической группой, но вы можете еще не догадываться об этом. Чтобы лучше понять, что такое циклическая группа, заглянем внутрь ее.

Пусть есть не нейтральный элемент  $g \in G$ . Рассмотрим его степени (произведение этого элемента на самого себя), в том числе и обратные к этому элементы

$$\dots, g^{-4}, g^{-3}, g^{-2}, g^{-1}, e, g^1, g^2, g^3, g^4, \dots$$

Предположим, что никакие два элемента в этом ряду не равны. Чтобы перемножать какие-то элементы, достаточно брать сумму их показателей. Кроме того, пусть в этой группе нет других элементов. Таким образом, мы завершили построение бесконечной циклической группы. В ней элемент  $g$  называется *порождающим*. И обозначается она обычно  $C_\infty$ .

**Пример 2.1.30.** Заметим, что  $(\mathbb{Z}, +)$  — это бесконечная циклическая группа с порождающим  $g = +1$ . Соответствие между этими группами можно построить так

$$\varphi: (\mathbb{Z}, +) \rightarrow C_\infty, \quad \varphi: k \mapsto g^k.$$

Такие соответствия мы позже будем рассматривать и будем называть их изоморфизмами.

Чтобы построить *конечные циклические группы*, можно предположить, что  $g^n = e$  для некоторого заранее фиксированного  $n \in \mathbb{N}$ . В таком случае получается группа, которая обычно обозначается  $C_n$ .

**Пример 2.1.31.** По аналогии с предыдущим примером мы можем рассмотреть следующий изоморфизм между аддитивной группой вычетов и циклической группой того же порядка

$$\varphi: \mathbb{Z}_n \rightarrow C_n, \quad \varphi: k \mapsto g^k.$$

На самом деле элемент  $g \in G$  в произвольной группе может порождать некоторую подгруппу. Для этого необходимо рассмотреть все его степени (включая отрицательные).

**Пример 2.1.32.** Рассмотрим  $2 \in \mathbb{Z}_4$ . Можем заметить, что всевозможные «степени» этой двойки ограничиваются  $\{0, 2\}$ , то есть получается подгруппа, которая является  $C_2$ .

В связи с этим вводят следующее определение.

**Определение 2.1.33.** Если элемент  $g \in G$  в степени  $n \in \mathbb{N}$  дает нейтральный элемент, но ни при каком  $m \in \overline{1, n-1}$  не дает нейтральный, то  $n$  называют *порядком элемента  $g$* .

**Замечание.** Порядок  $g$  обычно обозначают  $\text{ord } g$ .

**Замечание.** Если в любой натуральной степени элемент  $g$  дает не нейтральные элемент, то говорят, что порядок бесконечен и пишут  $\text{ord } g = +\infty$ .

**Пример 2.1.34.** Допустим, что порядок элемента  $g \in G$  равен 104 и необходимо найти порядок элемента  $g^{39}$ . В таком случае мы можем воспользоваться изоморфизмом, описанным в примере 2.1.31 и переформулировать задачу на языке вычетов: сколько раз минимально необходимо сложить 39 с самим собой, чтобы получить 0 по модулю 104? Ответ легко посчитать: 8.

**Пример 2.1.35.** Докажем, что если порядок элемента  $a$  равен  $n$ , то все элементы  $e, a, \dots, a^{n-1}$  различные. Для этого предположим противное, то есть что существуют такие  $i$  и  $j$ , что  $a^i = a^j$ . Пусть  $i > j$ , тогда  $a^{i-j} = e$ , откуда получаем противоречие с определением.

По аналогии можно показать, что в бесконечной циклической группе все элементы  $a^i$  различные, так как иначе бы мы получили бы конечную циклическую группу.

Порядок элемента соотносится с циклическими группами следующим образом.

**Утверждение 2.1.36.** Пусть элемент  $g$  порождает подгруппу  $H$  в группе  $G$ . Тогда  $|H| = \text{ord } g$ .

**Следствие 2.1.37.** Порядок элемента всегда делит порядок группы.

**Пример 2.1.38.** Если группа  $G$  имеет простой порядок, то любой элемент  $g \neq e$  порождает ее. Чтобы показать это, заметим, что порядок элемента делит порядок группы, откуда следует, что порядок элемента  $g$  равен  $|G|$ . По примеру 2.1.35 мы знаем, что среди степеней элемента  $g$  есть  $\text{ord } g$  различных элементов, то есть все элементы группы. Откуда получается, что подгруппа, порожденная элементом  $g$ , является всей группой  $G$ .

**Утверждение 2.1.39.** Докажем, что если  $\text{ord } g = n < +\infty$ , то  $a^m = e$  тогда и только тогда, когда  $m$  делится на  $n$ .

*Доказательство.* В обратную сторону утверждение очевидно:

$$a^m = a^{kn} = (a^n)^k = e^k = e.$$

В прямую сторону мы предположим противное: пусть  $m = nk + r$ , где  $r \in \overline{1, n - 1}$ . Тогда заметим, что

$$e = a^m = a^{nk+r} = (a^n)^k \cdot a^r = a^r,$$

что противоречит доказанному в примере 2.1.35. ■

Давайте на примере поймем, как решаются уравнения в циклических группах. Позже мы увидим, что в разных алгебраических структурах можно записывать знакомые нам уравнения и получать неожиданные решения.

**Пример 2.1.40.** Решим уравнение  $x^4 = e$  в группе  $C_{12}$ . Заметим, что любой элемент в  $C_{12}$  есть не что иное, как  $g^i$ , а значит:

$$e = x^4 = g^{4i} \Leftrightarrow 4i:12 \Leftrightarrow i = 0, 3, 6, 9,$$

то есть в группе 4 решения этого уравнения. Отметим, что не у всех элементов, являющихся решением уравнения, порядок равен 4 (например,  $\text{ord } g^6 = 2$ ).

**Пример 2.1.41.** Решим уравнение  $x^5 = e$  в группе  $C_{12}$ . Для этого проведем такие же выкладки, как и выше и увидим, что в качестве решения подходит только нейтральный элемент.

**Пример 2.1.42.** Решим уравнение  $x^8 = e$  в группе  $C_{12}$ . Распишем по аналогии равенства выше и получим, что  $g^i$  является решением тогда и только тогда, когда  $8i$  делится на 12, то есть при  $i = 0, 3, 6, 9$ . При этом ни один из этих элементов не имеет порядок, равный 8.

Таким образом, мы получили, что циклические группы неразрывно связаны с подгруппами, порождаемыми одними элементами группы. В случае абелевых групп этот факт позволяет достаточно быстро прийти к их классификации, а в некоммутативном случае классификации как таковой нет, но какие-то дальнейшие шаги можно сделать, изучив теоремы Силова.

## Домашнее задание

**Задача 2.1.1.** Образуют ли группу по умножению: 1) все действительные числа; 2) все действительные числа без 0; 3) все положительные действительные числа; 4) все натуральные числа?

**Задача 2.1.2.** Докажите, что в группе: а) существует ровно один нейтральный элемент; б) у каждого элемента ровно один обратный элемент; в)  $(a^{-1})^{-1} = a$  и  $e^{-1} = e$ .

**Задача 2.1.3.** Сформулируйте критерий обратимости вычета по модулю  $n$  и докажите его.

**Задача 2.1.4.** Докажите, что если  $H_1$  и  $H_2$  — подгруппы в  $G$ , то  $H_1 \cap H_2$  тоже подгруппа.

**Задача 2.1.5.** В группе  $(\mathbb{Q}, +)$  рациональных чисел по сложению рассмотрим подгруппу  $G$ , порожденную числами  $1/2, 1/6, 1/7$  (наименьшую подгруппу, которая содержит все эти числа). Верно ли, что числа  $1/9$  и  $-7/27$  принадлежат одному классу смежности по подгруппе  $G$ ?

**Задача 2.1.6.** (а) Верно ли, что всякий корень 35-й степени из единицы (то есть  $x \in \mu_{35}$ ) является кубом некоторого корня 35-й степени из единицы? (б) Тот же вопрос про корни 36-й степени из единицы.

**Задача 2.1.7.**  $C_{360}$  — циклическая группа порядка 360. Найти число решений уравнения  $x^k = e$  и количество элементов порядка  $k$  в группе  $C_{360}$  при а)  $k = 7$ ; б)  $k = 12$ ; в)  $k = 48$ . Сколько в  $C_{360}$  порождающих элементов?

**Задача 2.1.8.** Уравнение  $x^{12} = e$  имеет 14 решений в группе  $G$ . Доказать, что группа  $G$  не является циклической.

**Задача 2.1.9.** Пусть все элементы в квадрате дают нейтральный элемент. Докажите, что группа коммутативна.

**Задача 2.1.10.** Пусть  $a, b$  — произвольные элементы некоторой группы  $G$ . Доказать, что каждое из уравнений  $ax = b$  и  $ya = b$  имеет, и притом ровно одно, решение в данной группе.

**Бонусная задача.** Построить группу  $G$ , в которой уравнение  $x^{12} = e$  имеет ровно 14 решений.

## Рекомендуемая литература

- [1] Алексеев В. Б. — Теорема Абелля в задачах и решениях. — Новое изд. — М.: МЦНМО, 2017. — Глава 1, §1, 3, 4, 6, 8.
- [2] Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Разделы 1, 2.
- [3] Винберг Э. Б. — Курс Алгебры — 2-е изд., стереотип. — М.: МЦНМО, 2013. — Глава 1, §1, 2, 4, 5; Глава 4, §1, 3, 5.
- [4] Кострикин А. И. — Введение в алгебру: В 3-х ч. — Четвертое издание, стереотип. — М.: МЦНМО, 2020. — Глава 4, §1.

## 2.2 Симметрическая группа

В прошлом разделе мы много обсуждали группы и большинство их них были абелевыми. На самом деле абелевы группы — это полезный, но относительно маленький класс групп. Намного больше существует групп, которые не являются абелевыми. И так или иначе они связаны со следующими группами — группами перестановок.

**Ключевые слова:** перестановки, транспозиции, симметрическая группа, цикл, разложение перестановки в произведение независимых циклов, сопряженные элементы, коммутатор, знакопеременная группа.

## 2.2.1 Перестановки

Здесь и далее мы будем предполагать, что  $S$  — это конечное множество из  $n$  элементов, например,  $\overline{1, n}$ . Перестановкой в общем случае называют взаимно однозначное соответствие конечного множества в себя. Мы же зафиксируем множество, на котором будем рассматривать перестановку.

**Определение 2.2.1.** Перестановкой будем называть биекцию  $\sigma: S \rightarrow S$ .

Перестановки обычно записываются с помощью таблицы из двух строк, где в первой строке пишут элементы множества  $S$ , а во второй строке — элементы, в которые переходят первые, то есть

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

**Пример 2.2.2.** Среди перестановок часто нам будут встречаться *транспозиции*. Это перестановки, которые оставляют все элементы на месте, кроме двух. Оставшиеся же два элемента транспозиция меняет местами:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & 3 & \dots & j & \dots & i & \dots & n \end{pmatrix}.$$

**Пример 2.2.3.** Перестановка из примера 1.1.8 будут записываться так

$$\psi = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 3 \end{pmatrix}.$$

**Пример 2.2.4.** Еще среди перестановок выделяются  *тождественная перестановка и циклы*. Первая перестановка представляет из себя биекцию  $\text{id}(i) = i$  (ее еще обозначают через  $\text{id}_S$ , чтобы подчеркнуть, на каком множестве она задана). Циклами же называют перестановки, которые некоторые элементы оставляют на месте, а остальные же переводят циклически между собой, то есть

$$c = \begin{pmatrix} \dots & i_1 & \dots & i_2 & \dots & i_3 & \dots & i_k & \dots \\ \dots & i_2 & \dots & i_3 & \dots & i_4 & \dots & i_1 & \dots \end{pmatrix}.$$

Как мы чуть дальше увидим, они называются циклами не просто так, а имеют под этим веское основание (можете вспомнить пример 1.1.8).

**Пример 2.2.5.** Заметим, что группа  $S_n$  почти всегда (при  $n \geq 3$ ) не абелева. А именно, мы можем рассмотреть следующие две перестановки (в случае  $n > 3$  все оставшиеся элементы, кроме первых трех, остаются на месте при действии каждой перестановки):

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Заметим, что чтобы найти композицию двух перестановок, можно склеить первую строчку первой перестановки со второй строчкой второй перестановки. Тогда получим, что в первой строчке написано  $i$ , во второй —  $\sigma_2(i)$ , а в третьей —  $\sigma_1(\sigma_2(i))$ .

**Пример 2.2.6.** Найдем композицию  $\psi$  из примера 1.1.8 и перестановки элементов 1, 3:

$$\psi \circ \tau = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 2 & 1 \\ 1 & 3 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 0 & 2 \end{pmatrix}.$$

Как мы знаем, у любой биекции есть обратное отображение, которое тоже является биекцией. А также, как мы писали в примере 2.2.4, существует тождественная перестановка. В совокупности с ассоциативностью композиции как бинарной операции мы получаем, что выполнено следующее утверждение

**Утверждение 2.2.7.** Множество перестановок на  $S$  с композицией образует группу.

**Замечание.** Эту группу обозначают через  $S_n$  (или  $\mathfrak{S}_n$ ) и называют **симметрической группой**.

**Пример 2.2.8.** Чему равен порядок симметрической группы  $S_n$ ? Заметим, что любая перестановка  $\sigma$  задается своей второй строкой, то есть набором элементов  $\sigma(i)$ . Отсюда получается, что элемент 1 мы можем перевести в  $n$  элементов, элемент 2 в  $(n - 1)$  элементов и т. д. В итоге  $|S_n| = n!$ .

Исходя из последнего утверждения, мы можем смотреть на перестановки как на элементы какой-то группы и рассуждать о них в ключе теории групп. Чтобы понять, как находить порядки перестановок, обсудим, что такое цикловое разложение перестановок в независимые циклы.

## 2.2.2 Цикловое разложение

Весь этот подраздел мы будем обсуждать циклы и все, что с ними связано. Например, мы увидим, как просто найти класс сопряженности в группе перестановок.

**Определение 2.2.9.** **Цикл** — перестановка  $c$ , для которой существует такой набор  $\{i_t\}_{t=1}^k = I$ , что выполняются два условия:

- $\forall t \in \overline{1, k-1}: \sigma(i_t) = i_{t+1}, \sigma(i_k) = i_1;$
- $\forall j \in S \setminus I: \sigma(j) = j.$

**Замечание.** *Длиной цикла* называют количество элементов в  $I$ , то есть число  $k$ .

**Замечание.** Легко заметить, что определение корректно и это действительно перестановка. Также видно, что  $\text{ord } c = k$ , то есть длина цикла равна его порядку. Такой цикл принято обозначать через

$$c = (i_1 \ i_2 \ i_3 \ \dots \ i_k) = |i_1 \ i_2 \ i_3 \ \dots \ i_k\rangle.$$

**Замечание.** Чисто комбинаторно циклы можно описать следующим образом: орграф, который задает перестановку содержит не более одного цикла, отличного от петли (может быть и ноль в случае тождественной перестановки, ее мы будем считать циклом длины 1).

**Пример 2.2.10.** Покажем, что, если  $c$  — цикл длины  $k$ , перестановка  $c^m$  является циклом тогда и только тогда, когда  $(m, k) = 1$ . Для этого заметим, что подгруппа  $H$ , порожденная этим циклом, является циклической группой  $C_k$ . Отсюда следует, что  $(m, k) = 1$  необходимо и достаточно для того, чтобы  $c^m$  имело порядок  $k$ . Кроме того мы можем сказать, что если  $c^m$  является набором циклов, то все эти циклы имеют одинаковую длину (в силу симметрии), откуда получаем, что  $c^m$  в таком случае имеет длину меньше  $k$ . Видно, что это означает, что  $c^m$  является единственным циклом длины  $k$ , что и завершает доказательство.

Если цикл  $c_1$  действует на множестве  $I_1$  (множество не неподвижных точек этого цикла), а цикл  $c_2$  — на множестве  $I_2$ , то эти циклы называются *независимыми* тогда и только тогда, когда  $I_1 \cap I_2 = \emptyset$ .

Среди всех утверждений про циклы самым важным является следующее.

**Теорема 2.2.11.** Любую перестановку  $\sigma \in S_n$  можно представить в виде произведения независимых циклов:

$$\sigma = c_1 \circ c_2 \circ \dots \circ c_t,$$

притом это разложение единствено с точностью до перестановки этих  $t$  циклов.

**Замечание.** Этот вид называется **разложением перестановки в произведение независимых циклов**.

В связи с этой теоремой часто говорят о *циклическом типе* перестановки, подразумевая под ним невозрастающую последовательность длин циклов, входящих в цикловое разложение. Как мы дальше увидим, циклический тип неразрывно связан с сопряженностью перестановок. А сейчас давайте поймем как по циклическому типу узнать порядок перестановки.

**Утверждение 2.2.12.** Если  $\sigma \in S_n$  имеет циклический тип  $(l_1, \dots, l_t)$ , то  $\text{ord } \sigma = \text{НОК}(l_1, \dots, l_t)$ .

### 2.2.3 Сопряженные элементы

Сейчас мы обсудим важную групповую конструкцию, которая очень важна для понимания структуры групп, но суть ее будет очевидна только после того, как мы пройдем практически всю теорию групп этого курса. При этом на примере перестановок мы увидим, как сопряжение связано с разложением на независимые циклы.

**Определение 2.2.13.** Пусть  $g, h \in G$ . Будем говорить, что элемент  $a$  **сопряжен элементу  $h$  посредством элемента  $g$** , если  $a = ghg^{-1}$ .

**Замечание.** Элемент  $ghg^{-1}$  обычно обозначается посредством  $h^g$ .

**Упражнение.** Покажите, что сопряженность является отношением эквивалентности.

По понятным причинам *классом сопряженности* называется множество попарно сопряженных элементов.

**Пример 2.2.14.** Пусть группа  $G$  абелева. Покажем, что классы сопряженности одноэлементны. Для этого выпишем следующие равенства:

$$h = e \cdot h = (gg^{-1})h = ghg^{-1},$$

отсюда и следует искомое.

**Замечание.** Заметим, что равенство  $ghg^{-1} = h$  эквивалентно равенству  $ghg^{-1}h^{-1} = e$  и равенству  $gh = hg$ . Как мы знаем, последнее равенство называется коммутативностью элементов  $g$  и  $h$ , а второе равенство показывает, что *коммутатор* элементов  $g$  и  $h$  равен нейтральному элементу. Позже нам еще встретятся коммутаторы.

**Пример 2.2.15.** Найдем элемент, полученный сопряжением перестановки  $(12)(345)$  посредством элемента  $(1345)$ . Введем обозначения:  $\sigma = (12)(345)$ ,  $\tau = (1345)$ . И найдем композицию

$$\tau \circ \sigma \circ \tau^{-1} = (1345) \circ (12)(345) \circ (1543) = (145)(23).$$

Отметим, что циклический тип перестановки  $\sigma^\tau$  совпадает с циклическим типом перестановки  $\sigma$ . Оказывается это не случайность, а вполне явное свойство симметрической группы.

**Теорема 2.2.16.** Для сопряженности перестановок необходимо и достаточно, чтобы они имели одинаковый циклический тип.

**Пример 2.2.17.** Заметим, что у сопряженных элементов совпадают порядки (если они конечны). Для того чтобы показать это, отметим:

$$h^n = e \Rightarrow (h^g)^n = (h^g)^n = (ghg^{-1})^n = ghg^{-1} \cdot ghg^{-1} \cdots ghg^{-1} = gh^n g^{-1} = (h^n)^g = e^g = e,$$

$$(ghg^{-1})^n = e \Rightarrow gh^n g^{-1} = e \Rightarrow h^n = g^{-1}g = e.$$

Из последних двух строчек с формулами следует, что порядки сопряженных элементов должны делить друг друга, из чего мы заключаем, что они совпадают.

**Пример 2.2.18.** Укажем в группе  $S_6$  две не сопряженные перестановки, которые имеют одинаковый порядок. Это будут  $\sigma_1 = (12)(3456)$  и  $\sigma_2 = (1234)(5)(6)$ . Можно заметить, что  $\text{ord } \sigma_1 = \text{НОК}(2, 4) = 4 = \text{НОК}(4, 1, 1) = \text{ord } \sigma_2$ , но при этом у этих перестановок разные цикловые типы, так что они не сопряжены.

**Утверждение 2.2.19.** Покажем, что два цикла  $\sigma_1, \sigma_2 \in S_n$  коммутируют тогда и только, когда они независимы или когда  $\sigma_1 = \sigma_2^s$ , притом  $\text{ord } \sigma_1 = \text{ord } \sigma_2 = r$ ,  $(r, s) = 1$ .

*Доказательство.* Отметим, что коммутативность двух циклов есть ни что иное, как равенство  $\sigma_1 = \sigma_2^{\sigma_2}$ . А мы знаем, как устроена сопряженная перестановка.

Если  $I_1 \cap I_2 \neq \emptyset$ , то циклы независимы и все доказано. Иначе допустим, что есть элемент  $i_1$  такой, что  $\sigma_2(i_1) = i_1$  (если второй цикл не сопряжен с первым, то такой элемент обязан быть). В таком случае  $i_2 = \sigma_1(i_1)$  тоже неподвижен относительно второго отображения — докажем это:

$$i_1 = \sigma_2^{-1}(i_1) \Rightarrow \sigma_2(\sigma_1(\sigma_2^{-1}(i_1))) = \sigma_2(\sigma_1(i_1)) = \sigma_2(i_2) = \sigma_1(i_1) = i_2 \Rightarrow \sigma_2(i_2) = i_2.$$

Продолжая по индукции, мы покажем, что все элементы цикла  $\sigma_1$  будут неподвижны относительно второго цикла, что противоречит предположению об отсутствии независимости этих циклов. Следовательно, во второй цикл входят все элементы первого, а значит, в силу симметрии они сопряжены, откуда и получается искомая зависимость. ■

**Пример 2.2.20.** Найдем все перестановки из  $S_4$ , которые коммутируют с  $\tau = (12)(34)$ . Мы знаем, что если  $\sigma$  коммутирует с  $\tau$ , то  $\tau^\sigma = \tau$ , то есть

$$(\sigma(1)\sigma(2))(\sigma(3)\sigma(4)) = (12)(34).$$

Как видим, циклический тип у перестановок совпадает, поэтому нам нужно сделать так, чтобы сами циклы тоже совпадали. Для этого разберем несколько случаев:

1.  $\sigma(1) = 1$ , тогда обязательно  $\sigma(2) = 2$ , а оставшиеся два элемента могут переходить куда угодно, то есть получаем два варианта:  $\sigma_1 = (1)(2)(34)$ ,  $\sigma_2 = \text{id}$ ;
2.  $\sigma(1) = 2$ , тогда обязательно  $\sigma(2) = 1$ , и по аналогии имеем:  $\sigma_3 = (12)(34)$ ,  $\sigma_4 = (12)$ ;
3. если  $\sigma(1) = 3$ , то  $\sigma(2) = 4$  и мы имеем два варианта в зависимости от того, куда оставшиеся два элемента переходят:  $\sigma_5 = (13)(24)$ ,  $\sigma_6 = (1324)$ ;
4. если  $\sigma(1) = 4$ , то  $\sigma(2) = 3$  и получается, что есть два варианта:  $\sigma_7 = (14)(23)$ ,  $\sigma_8 = (1423)$ .

## 2.2.4 Знакопеременная группа

Назовем перестановку *четной*, если ее можно представить в виде произведения четного числа транспозиций. Если ее можно представить в виде нечетного числа транспозиций, то перестановка называется *нечетной*. Смысл этих понятий раскрывается в следующем наборе упражнений.

**Упражнение.** Количество инверсий для перестановки  $\sigma \in S_n$  называется число таких пар  $(i, j), i < j$ , что  $\sigma(i) > \sigma(j)$ . Покажите, что у  $\sigma$  и  $\tau \circ \sigma$  разная четность числа инверсий, если  $\tau$  — транспозиция.

**Упражнение.** Покажите, что четные перестановки замкнуты относительно взятие композиции и обращения.

**Следствие 2.2.21.** Четные перестановки образуют подгруппу в  $S_n$ . Эту подгруппу называют **знакопеременной группой** и обозначают ее через  $A_n$ .

### Домашнее задание

**Задача 2.2.1.** Найти порядок элемента  $\sigma \in S_n$ , где

1.  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 7 & 1 & 2 & 5 & 6 & 10 & 9 & 8 \end{pmatrix}, n = 10;$
2.  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 5 & 4 & 1 & 6 & 2 & 3 & 9 & 8 & 11 & 12 & 10 \end{pmatrix}, n = 12;$
3.  $\sigma = (123435)(6789), n = 9.$

**Задача 2.2.2.** Доказать, что в группе  $S_8$  нет элементов порядка 56.

**Задача 2.2.3.** Найти порядок перестановки  $(123)(4567)(89)$  и количество сопряженных ей перестановок в группе  $S_9$ . Является ли эта перестановка четной?

**Задача 2.2.4.** а) Доказать, что все элементы порядка 11 сопряжены в  $S_{11}$ . б) Порождают ли перестановки порядка 11 группу  $S_{11}$ ?

**Задача 2.2.5.** Решите уравнение в  $S_9$ :

1.  $x \circ (14)(23)(7869) = (123)(456)(789);$
2.  $x^2 \circ (14)(23)(7869) = (123)(456)(789).$

**Задача 2.2.6.** Постройте некоммутативную группу минимального порядка.

**Задача 2.2.7.** Найдите все классы сопряженности в  $S_{11}$ , которые содержат перестановку порядка 12.

**Задача 2.2.8.** Доказать, что число элементов, сопряженных с элементом  $a$  в группе  $G$ , равно индексу  $N(a)$  в группе  $G$ , т. е. числу смежных классов по подгруппе  $N(a)$  — нормализатору элемента  $a$ :

$$N(a) = \{g \in G : ag = ga\}.$$

**Задача 2.2.9.** Какие классы сопряженности в  $S_n$  распадаются на несколько классов сопряженности в  $A_n$ ? Перечислите классы сопряженных элементов с указанием числа элементов в каждом классе для групп а)  $A_3$ ; б)  $A_4$ .

**Задача 2.2.10.** Перестановкой  $\sigma \in S_n$  называется *инволютивной* (или просто *инволюцией*), если  $\sigma^2 = \text{id}$ . Покажите, что

- перестановка инволютивна тогда и только тогда, когда в ее цикловом типе встречаются только циклы длины 1 и циклы длины 2;
- любой цикл  $\tau \in S_n$  длины не меньше 3 является композицией двух инволюций.

**Бонусная задача.** Найдите все нормальные подгруппы в  $S_4$ .

## Рекомендуемая литература

- [1] Алексеев В. Б. — Теорема Абеля в задачах и решениях. — Новое изд. — М.: МЦНМО, 2017. — Глава 1, §15.
- [2] Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Разделы 1, 2, 4.
- [3] Шень А. — Перестановки — М.: МЦНМО, 2020.
- [4] Городенцев А. Л. — Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 3, §10; Глава 4, §15.
- [5] Кострикин А. И. — Введение в алгебру: В 3-х ч. — Четвертое издание, стереотип. — М.: МЦНМО, 2020. — Глава 1, §8.

## 2.3 Морфизмы и конструкции. Часть 1

Так, мы уже изучили разные примеры групп, однако большинство групп строятся из приведенных так же, как из кирпичей строят дом. И теперь необходимо понять как из «pine» и «apple» сделать «pineapple». На пути к этому мы с вами познакомимся с нормальными подгруппами, которые очень важны в понимании этой теории. Советую всем, кто первый раз столкнулся с этим материалом, внимательно приглядеться к нормальным группам.

Кроме того, мы с вами изучим гомоморфизмы, то есть отображения, которые сохраняют групповую операцию. С помощью них мы сможем находить связь между разными группами, описывая одни через свойства других.

**Ключевые слова:** нормальная подгруппа, класс сопряженности, прямое произведение, гомоморфизм, ядро гомоморфизма, изоморфизм, изоморфизмы числовых множеств, эндоморфизмы, автоморфизмы.

### 2.3.1 Нормальные подгруппы

Ранее мы уже узнали, что такое подгруппы и что такие классы смежности. Мы видели, что классы смежности разбивают группу на непересекающиеся подмножества. Хочется, чтобы на этих подмножествах мы могли установить какую-то структуру, заимствованную из изначальной группы. Как это сделать? Оказывается, что в общем случае очень непросто, а в частном — вполне реально

**Определение 2.3.1.** Будем называть подгруппу  $H < G$  *нормальной подгруппой*, если для любого элемента  $g \in G$  левый смежный класс этого элемента совпадает с правым, то есть  $gH = Hg$ .

**Замечание.** Равенство в определении надо понимать как равенство множеств, то есть неверно считать, что для всех  $g \in G, h \in H$  будет выполнено, что  $gh = hg$ . Но при этом правильно будет говорить, что для любого  $h_1 \in H$  найдется такой  $h_2 \in H$ , что  $gh_1 = h_2g$ .

**Замечание.** Нормальную подгруппу обозначают так:  $H \triangleleft G$ .

**Пример 2.3.2.** Пусть  $H < G$  и при этом  $G$  абелева. Тогда можем заметить, что все элементы коммутируют, а значит,  $gH = Hg$  для любого  $g \in G$ . Отсюда автоматически получается, что  $H$  нормальна в  $G$ . То есть в абелевой группе все подгруппы нормальны.

**Пример 2.3.3.** Самая простая не нормальная подгруппа — это подгруппа, порожденная транспозицией в  $S_3$ . Например, возьмем  $H = \{\text{id}, (12)\}$ , и посмотрим на левые и правые смежные классы:

$$(13) \circ H = \{(13), (123)\} \neq H \circ (13) = \{(13), (132)\}.$$

**Замечание.** На последнем примере можно увидеть, что если левые классы смежности образовывали разбиение группы, то в совокупности и левые, и правые классы смежности никакого разбиения уже не задают хотя бы по тому, что есть пересекающиеся и не совпадающие классы.

Нормальные подгруппы хороши следующим важным свойством.

**Утверждение 2.3.4.** Пусть  $H \triangleleft G$ . Тогда для любых элементов  $g_1, g_2 \in G$  выполняется, что  $(g_1H) \circ (g_2H) = (g_1g_2)H$ .

**Замечание.** Выше использована следующая нотация:  $A \circ B = \{a \circ b : a \in A, b \in B\}$ .

Кроме того, имеет место следующее важное свойство, которое обычно забывают:

$$\forall g_2 \in g_1H \mapsto g_2H = g_1H.$$

В связи с этим, когда мы в перспективе захотим обсуждать введение операции на классах смежности, то нам можно будет брать представителей классов смежности и перемножать их с другими представителями, а потом брать класс смежности по получаемому элементу. Более подробно эту часть повествования мы разберем в следующем разделе при обсуждении фактор-групп.

Для нормальных подгрупп можно сформулировать следующий важный критерий, который позволяет легче проверять их наличие.

**Утверждение 2.3.5.** Пусть  $H$  подгруппа в  $G$ . Тогда эквивалентны следующие свойства:

1.  $H$  нормальна в  $G$ ;
2. для любого  $g \in G$  верно, что  $gHg^{-1} \subseteq H$ ;
3. для любого  $g \in G$  верно, что  $gHg^{-1} = H$ ;
4. множества  $G/H$  и  $H\backslash G$  совпадают;
5. вместе с каждым элементом  $H$  содержит весь класс сопряженности.

**Пример 2.3.6.** Докажем, что подгруппа, порожденная некоторым классом сопряженных элементов группы  $G$ , является нормальным делителем группы  $G$ .

Распишем все по определению. Что такое класс сопряженности? Это следующее множество:

$$\forall g \in G \mapsto K_g = \{hgh^{-1} : h \in G\}.$$

Что значит: группа  $H$  порождена некоторым классом элементов? Это значит, что в ней лежат всевозможные комбинации элементов из класса. Поэтому если наша подгруппа  $H$  порождена классом сопряженных элементов  $K_g$ , то

$$\forall h \in H \mapsto \exists \alpha_1, \dots, \alpha_m \in G : h = \alpha_1 g \alpha_1^{-1} \cdot \alpha_2 g \alpha_2^{-1} \cdot \dots \cdot \alpha_m g \alpha_m^{-1},$$

и наоборот:

$$\forall \alpha_1, \dots, \alpha_m \in G \mapsto \exists h \in H : h = \alpha_1 g \alpha_1^{-1} \cdot \alpha_2 g \alpha_2^{-1} \cdot \dots \cdot \alpha_m g \alpha_m^{-1}.$$

Но тогда вместе с любым элементом  $h$  группы  $H$  также будет содержаться все сопряженные с ним. Почему? А вот почему:

$$\begin{aligned} \forall k \in G, h \in H \mapsto khk^{-1} &= k\alpha_1 g \alpha_1^{-1} \cdot \alpha_2 g \alpha_2^{-1} \cdot \dots \cdot \alpha_m g \alpha_m^{-1} k^{-1} = \\ &= k\alpha_1 g \alpha_1^{-1} k^{-1} \cdot k\alpha_2 g \alpha_2^{-1} k^{-1} \cdot \dots \cdot k^{-1} \cdot k\alpha_m g \alpha_m^{-1} k^{-1} = \beta_1 g \beta_1^{-1} \cdot \beta_2 g \beta_2^{-1} \cdot \dots \cdot \beta_m g \beta_m^{-1}, \end{aligned}$$

где  $\beta_i = k \cdot \alpha_i$ . А из этого уже напрямую следует то, что это нормальная подгруппа, т.к.

$$\forall d \in G, h' \in H \mapsto d^{-1} h' d \in H \Rightarrow d \cdot d^{-1} h' d = h' d \in dH \Rightarrow Hd \subseteq dH \Rightarrow Hd = dH.$$

**Пример 2.3.7.** Докажите, что если элементы  $x, y$  сопряжены в конечной группе, то наименьший порядок нормальной подгруппы, содержащей  $x$ , равен наименьшему порядку нормальной подгруппы, содержащей  $y$ .

Если элементы сопряжены, то их классы сопряженности совпадают, то есть  $K_x = K_y$ . Заметим, что все комбинации из этого классы должны лежать в наименьшей подгруппе, содержащей оба этих элемента. Тем более, мы показали выше, что класс сопряженности порождает нормальную подгруппу. Следовательно, в обоих случаях мы получаем подгруппу  $\langle K_x \rangle = \langle K_y \rangle$ . Из равенства групп следует очевидное равенство их порядков.

### 2.3.2 Прямое произведение групп

Дальше будет конструкция, которая позволяет из двух групп  $G_1$  и  $G_2$  делать одну группу с наследованием групповых операций. Дадим определение.

**Определение 2.3.8.** Пусть даны две группы:  $(G_1, \cdot)$ ,  $(G_2, \circ)$ . Будем называть **прямым произведением групп** пару  $(G_1 \times G_2, \otimes)$  из декартового произведения  $G_1$  на  $G_2$  (как множеств) и бинарной операции  $\otimes$ , определенной следующим образом:

$$\otimes : (G_1 \times G_2) \times (G_1 \times G_2) \rightarrow G_1 \times G_2, \quad (g_1, h_1) \otimes (g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2).$$

**Замечание.** Здесь мы используем обозначение  $\otimes$ , чтобы не повторяться, но без намека на тензорное произведение (точно так же, как используем  $\times$  без намека на векторное произведение). Как говорят, все совпадения случайны.

**Замечание.** Между тем, мы дальше будем использовать обозначение  $G_1 \times G_2$ , подразумевая произведение двух групп в том смысле, что мы определили выше. Такое переопределение имеет смысл, так как декартово произведение нам в практических задачах не встретиться.

Основное важное утверждение, поясняющее введенное понятие, будет таким.

**Утверждение 2.3.9.** Произведение групп  $G_1 \times G_2$  является группой.

*Доказательство.* Замкнутость и ассоциативность следует из определения, так что нам необходимо показать только выполнимость  $G2$ ,  $G3$ . Для этого заметим, что

$$(g, h) \otimes (e_{G_1}, e_{G_2}) = (e_{G_1}, e_{G_2}) \otimes (g, h) = (g, h),$$

$$(g, h) \otimes (g^{-1}, h^{-1}) = (e_{G_1}, e_{G_2}) = (g^{-1}, h^{-1}) \otimes (g, h).$$

■

**Следствие 2.3.10.** Произведение двух абелевых групп — абелева группа.

Здесь надо отметить следующее: если говорить формально, то  $(G_1 \times G_2) \times G_3$  является группой, отличной от группы  $G_1 \times (G_2 \times G_3)$ . Однако между ними можно построить изоморфизм (говоря короче, их можно отождествить), из-за чего мы не будем различать эти группы и будем их записывать одинаково:  $G_1 \times G_2 \times G_3$ .

### 2.3.3 Гомоморфизмы: определение, ядра

Наконец мы добрались до отображений, которые интересны нам в рамках той теории, которую мы изучаем. Ведь не можем мы просто сравнивать множества по количеству элементов. Нам необходимо еще учитывать их операции. Для этого мы и вводим следующее определение.

**Определение 2.3.11.** Пусть даны две группы  $(G_1, \cdot)$  и  $(G_2, \circ)$ . Тогда отображение  $\varphi: G_1 \rightarrow G_2$  будет называть **гомоморфизмом**, если оно сохраняет операцию:

$$\forall g, h \in G_1 \mapsto \varphi(g \cdot h) = \varphi(g) \circ \varphi(h).$$

**Замечание.** Свойство, записанное формулой, обычно называют коротко так: «отображение сохраняет групповую операцию».

**Пример 2.3.12.** Будет ли гомоморфизмом аддитивных групп умножение на 2 в целых числах? Ответ: да, так как можно проверить, что отображение  $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$  будет сохранять операцию:

$$\varphi(x + y) = 2(x + y) = 2x + 2y = \varphi(x) + \varphi(y).$$

**Пример 2.3.13.** Заметим, что в группе  $C_n$  возведение в  $k$ -ую степень тоже будет являться гомоморфизмом. При этом, например, если  $k = n$ , то образом гомоморфизма будет только  $\{e\}$ .

**Определение 2.3.14.** Пусть задан гомоморфизм  $\varphi: G_1 \rightarrow G_2$ . **Образом гомоморфизма** называется

$$\text{Im } \varphi = \{x \in G_2 \mid \exists y \in G_1 : \varphi(y) = x\}.$$

**Определение 2.3.15.** Пусть задан гомоморфизм  $\varphi: G_1 \rightarrow G_2$ . **Ядром гомоморфизма** называется  $\varphi^{-1}(e_{G_2})$ , или иначе:

$$\text{Ker } \varphi = \{x : \varphi(x) = e_{G_2}\}.$$

**Упражнение.** Найдите ядра гомоморфизмов в задачах 2.3.12 и 2.3.13.

**Пример 2.3.16.** Из группы  $S_k$  можно построить инъективный гомоморфизм в группу  $S_n$ , если  $k \leq n$ . Для этого заметим, что перестановки  $\sigma \in S_k$  мы можем рассматривать как перестановку на первых  $k$  элементах из  $n$  доступных, то есть

$$\varphi: S_k \hookrightarrow S_n, \sigma \mapsto \sigma(k+1)(k+2)\dots(n).$$

Можно заметить, что этот гомоморфизм инъективен, откуда следует, что ядро нулевое, то есть  $\text{Ker } \varphi = \{\text{id}\}$ .

**Пример 2.3.17.** Возьмем  $\mathbb{Z}/n\mathbb{Z}$  и  $k$  — делитель числа  $n$ . Тогда отображение  $\varphi: i \mapsto ki$  будет являться гомоморфизмом, как легко проверить. Видно, что если  $\varphi(i) = 0$ , то  $ki$  делится на  $n$ , а значит,  $i$  делится на  $n/k$ . Далее можно показать, что  $\ker \varphi = \{0, n/k, \dots, (k-1)n/k\}$ .

В предыдущем примере видно, что ядро является циклической подгруппой порядка  $k$  в группе  $\mathbb{Z}/n\mathbb{Z}$ . Мы увидим еще много похожих примеров, когда ядра гомоморфизмов мы где-то уже встречали. Но одним из самых важных явлений, которые вы могли упустить, будет следующий факт.

**Теорема 2.3.18.** (a) Ядро любого гомоморфизма  $\varphi: G_1 \rightarrow G_2$  будет являться нормальной подгруппой в  $G_1$ . (b) Для любой нормальной подгруппы  $H$  в группе  $G_1$  мы найдем такую группу  $G_2$  и гомоморфизм между ними, что  $\ker \varphi = H$ .

**Пример 2.3.19.** Пусть  $\varphi: G \rightarrow G$  — инъективный гомоморфизм групп. Про элементы  $x, y$  известно, что они принадлежат одному классу смежности по ядру гомоморфизма  $\varphi$ . Следует ли из этого, что  $x = y$ ? Проверим.

Для этого заметим, что из инъективности гомоморфизма следует, что ядра нулевое, то есть  $\ker \varphi = \{e\}$ . Отсюда следует, что все классы смежности по ядру одноэлементны, а значит,  $x = y$ .

Эта теорема фактически говорит нам о том, что можно не различать нормальные подгруппы и ядра гомоморфизмов. Это буквально одно и тоже (с точки зрения теории категорий).

Мы же далее рассмотрим специальные гомоморфизмы, которые важны сами по себе, так как наполняют неизбежно речь любого алгебраиста: например, все группы однозначно рассматриваются с точностью изоморфизма. Или, например, некоторые исключительные изоморфизмы групп могут намного больше сказать о той алгебре, которую мы изучаем, чем пробы исследователей классифицировать группы.

## 2.3.4 Изоморфизмы, эндоморфизмы, автоморфизмы

Начнем с простого. Будем называть гомоморфизм групп **изоморфизмом**, если он биективен.

И тут начинается расцвет той скрытой информации о группах, которые мы изучали. Мы можем заметить множество изоморфизмов между ними.

**Пример 2.3.20.** Рассмотрим циклическую группу порядка  $n$  и аддитивную группу вычетов по модулю  $n$ . Построим изоморфизм следующим образом:

$$\varphi: C_n \rightarrow \mathbb{Z}/n\mathbb{Z}, g^i \mapsto i.$$

Более того, мы можем вспомнить группу корней  $n$ -й степени из единицы в комплексных числах, которую мы обозначали через  $\mu_n$ . Так оказывается она тоже изоморфна группам выше. Например,

$$\psi: \mu_n \rightarrow \mathbb{Z}/n\mathbb{Z}, \zeta_k \mapsto k.$$

**Упражнение.** Введем отношение изоморфности: пара  $(G_1, G_2)$  удовлетворяет ему тогда и только тогда, когда можно построить изоморфизм  $\varphi: G_1 \rightarrow G_2$ . Покажите, что это отношение является отношением эквивалентности.

**Замечание.** В силу последнего упражнения принято говорить, что *группы изоморфны*, если существует изоморфизм между ними (неважно, откуда он идет).

**Замечание.** Если  $G_1$  изоморфно  $G_2$ , то пишут  $G_1 \cong G_2$ .

Можно еще привести разные изоморфизмы попроще.

**Пример 2.3.21.** Группы  $S_2$  и  $C_2$  изоморфны, так как между ними мы можем построить отображение, которое нейтральный элемент переводит в нейтральный элемент другой группы, а другой элемент переводит в не нейтральный элемент второй группы, то есть

$$\varphi: S_2 \rightarrow C_2, \text{id} \rightarrow e, (12) \rightarrow g.$$

**Пример 2.3.22.** Бесконечная циклическая группа  $C_\infty$  изоморфна аддитивной группе целых чисел  $(\mathbb{Z}, +)$ . Для этого изоморфизма достаточно отобразить порождающий элемент  $g$  в 1 — порождающий элемент в  $(\mathbb{Z}, +)$ .

**Пример 2.3.23.** Приведем пример двух неизоморфных групп одинакового порядка. Возьмем  $C_4$  и  $C_2 \times C_2$ . Заметим, что в одной группе есть элемент порядка 4, а в другой — нет. Следовательно, это не изоморфные группы.

**Пример 2.3.24.** Докажем, что группа всех действительных чисел по сложению изоморфна группе положительных действительных чисел по умножению. Для этого рассмотрим следующее отображение

$$\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_+, \cdot), x \mapsto e^x.$$

Из свойств экспоненты, которую традиционно рассматривают на математическом анализе, следует, что это отображение является гомоморфизмом. При этом легко проверить, что этот гомоморфизм биективен, а значит, является изоморфизмом.

Следующий класс гомоморфизмов, который стоит отдельно рассмотреть — это гомоморфизмы группы  $G$  в себя, то есть **эндоморфизмы**.

**Пример 2.3.25.** В примерах 2.3.12 и 2.3.13 были разобраны эндоморфизмы соответствующих групп.

Нам будут интересны биективные эндоморфизмы, которые называют **автоморфизмами**. Как вы понимаете, это по сути изоморфизмы в из группы в саму себя.

**Пример 2.3.26.** Рассмотрим  $C_p$ , где  $p$  — простое число. Пусть  $\varphi: C_p \rightarrow C_p$  действует возвещением элемента в степень  $k$ , где  $k \in \overline{1, p - 1}$ . Тогда это отображение — автоморфизм.

**Пример 2.3.27.** В любой группе есть так называемый тривиальный автоморфизм, который действует тождественно на элементах группы, то есть  $\varphi(g) = g$ .

**Пример 2.3.28.** Отображение  $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $a \mapsto -a$  является автоморфизмом аддитивной группы целых чисел. Мы можем даже представить действие этого изоморфизма как поворот оси абсцисс на  $180^\circ$  вокруг начала координат.

Автоморфизмы отражают внутреннюю симметрию группы и позволяют получать разные свойства из этого. Относительно скоро, мы сможем увидеть действие автоморфизмов и поймем, почему их называют симметриями групп.

## Домашние задачи

**Задача 2.3.1.** (a) Покажите, что подгруппа индекса 2 всегда нормальна. Из этого следует нормальность  $A_n$  в  $S_n$ . (b) Множество элементов группы  $G$ , перестановочные (коммутирующие) со всеми элементами группы называется **центром группы**  $G$  (обозначается через  $Z(G)$ ). Докажите, что центр — подгруппа, и более того, нормальная подгруппа в  $G$ .

**Задача 2.3.2.** Докажите, что пересечение любого числа нормальных подгрупп является нормальной подгруппой.

**Задача 2.3.3.** Пусть  $\varphi: G_1 \rightarrow G_2$  — гомоморфизм. а) Докажите, что  $\varphi(e_{G_1}) = e_{G_2}$ . б) Докажите, что для любого элемента  $g \in G_1$  выполнено:  $\varphi(g^{-1}) = \varphi(g)^{-1}$ . в) Докажите, что при этом  $\varphi$  — инъективный гомоморфизм тогда и только тогда, когда для любого элемента  $g \in G_1$  верно, что  $\varphi(g)$  и  $g$  имеют одинаковые порядки.

**Задача 2.3.4.** Существует ли гомоморфизм группы  $S_9$ , ядром которого является подгруппа  $G$ , состоящая из перестановок, которые элемент 1 переводят в себя?

**Задача 2.3.5.** Для каких групп отображение  $x \rightarrow x^{-1}$  является гомоморфизмом?

**Задача 2.3.6.** Верны ли равенства: 1)  $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ ; 2)  $\mathbb{Z}_2 \times \mathbb{Z}_4 \cong \mathbb{Z}_8$ ? 3) Когда  $\mathbb{Z}_n \times \mathbb{Z}_m$  изоморфно  $\mathbb{Z}_{nm}$ ?

**Задача 2.3.7.** Доказать, что если порядок абелевой группы  $G$  равен  $nm$ , где  $(n, m) = 1$ , то  $G$  изоморфна прямому произведению групп порядков  $n$  и  $m$ .

**Задача 2.3.8.** Найти порядок элемента  $(2, 5)$  в прямом произведении циклических групп  $C_{16} \times C_{12}$ .

**Задача 2.3.9.** Существует ли сюръективный гомоморфизм а)  $C_{24} \times C_{18}$  на  $C_{16}$ ; б)  $C_{25} \times C_{18}$  на  $C_{15}$ ?

**Задача 2.3.10.** Пусть  $\varphi: G_1 \rightarrow G_2$  — сюръективный гомоморфизм. а) Докажите, что, если  $G_1$  — коммутативная группа, то и  $G_2$  тоже коммутативная. б) Докажите, что обратное не верно в общем случае.

**Бонусная задача.** Постройте некоммутативную группу порядка 8, все подгруппы которой нормальны.

## Рекомендаемая литература

- [1] Алексеев В. Б. — Теорема Абеля в задачах и решениях. — Новое изд. — М.: МЦНМО, 2017. — Глава 1, §5, 7, 10, 13.
- [2] Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Разделы 3, 4.
- [3] Городенцев А. Л. — Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 4, §15.
- [4] Винберг Э. Б. — Курс Алгебры — 2-е изд., стереотип. — М.: МЦНМО, 2013. — Глава 4, §5, 6; Глава 10, §1.
- [5] Кострикин А. И. — Введение в алгебру: В 3-х ч. — Четвертое издание, стереотип. — М.: МЦНМО, 2020. — Глава 4, §2.

## 2.4 Морфизмы и конструкции. Часть 2

В этом разделе мы с вами продолжим развивать теорию, начатую ранее. Для начала мы на множестве смежных классов определим операцию, согласованную с групповой операцией, что даст нам новую группу. Далее мы вернемся к гомоморфизмам и сформулируем теорему о гомоморфизмах. В продолжение занятия нас встретят две интересные и важные группы: группа автоморфизмов и группа внутренних автоморфизмов. В последнем случае мы сможем дополнить наши знания сопряжения новыми интересными фактами.

**Ключевые слова:** фактор-группы, аддитивная группа вычетов, теоремы о гомоморфизме, группа преобразований, группа вращений куба, группа Диэдра, группа автоморфизмов, группа внутренних автоморфизмов.

## 2.4.1 Фактор-группы

Вспомним утверждение 2.3.4. В нем говорится, что перемножая классы смежности по нормальной подгруппе, мы получаем класс, который определяется двумя различными представителями исходных классов. Отсюда следует, что мы можем ввести операцию произведения двух смежных классов:

$$(g_1H) \circ (g_2H) = (g_1g_2)H.$$

**Утверждение 2.4.1.** Введенная операция корректно определена на  $G/H$ , то есть не зависит от тех  $g_1$  и  $g_2$ , которые мы выбираем из классов смежности. Более того,  $(G/H, \circ)$  — это группа.

**Замечание.** Пару  $(G/H, \circ)$  называют **фактор-группой**.

На фактор-группу можно смотреть немного с другой стороны. Мы же знаем, что такое  $G/H$ , и есть сюръективное отображение, которое каждому элементу сопоставляет его класс смежности:

$$p: G \rightarrow G/H, \quad g \mapsto gH.$$

Введенная операция на классах смежности определена так, чтобы, во-первых, отображение  $p$  было гомоморфизмом, а во-вторых, чтобы  $\text{Ker } p = H$ . Итак, мы можем задавать фактор-группу не через классы смежности, а через отображение  $p$  с заданными условиями (это отображение называется **фактор-отображением**). Такой подход соответствует с тем, что называется универсальным свойством в теории категорий.

**Пример 2.4.2.** Рассмотрим подгруппу  $n\mathbb{Z}$  в  $(\mathbb{Z}, +)$ . Как мы знаем, множество смежных классов выглядит так:

$$\mathbb{Z}/n\mathbb{Z} = \{i + n\mathbb{Z}: i \in \overline{0, n-1}\}.$$

Определяя фактор-группу, мы получаем знакомую нам аддитивную группу вычетов по модулю  $n$ . Фактор-отображение в данном случае сопоставляет каждому целому числу его остаток по модулю  $n$ .

**Пример 2.4.3.** Подгруппа  $A_n$  нормальна в  $S_n$ , так как это подгруппа индекса 2. Отсюда следует, что мы можем по ней профакторизовать:

$$S_n/A_n \cong (\{\pm 1\}, \cdot).$$

**Пример 2.4.4.** Докажем, что нормальная подгруппа индекса  $k$  содержит все элементы, порядки которых взаимно просты с  $k$ . Обозначим подгруппу через  $H$ . По условию мы получаем, что порядок  $G/H$  равен  $k$ . Посмотрим на образ элемента  $g \in G$  при фактор-отображении  $p(g)$  лежит в  $G/H$  и поэтому порядок  $p(g)$  делит порядок группы, то есть  $k$ . Как мы знаем, при гомоморфизме сохраняется операция, откуда можно получить, что  $\text{ord } p(g) | \text{ord } g = n$ . Следовательно, порядок  $p(g)$  делит наибольший общий делитель чисел  $n$  и  $k$ , то есть равен 1, что означает, что  $g$  лежит в  $\text{Ker } p = H$ .

**Пример 2.4.5.** Построим гомоморфизм  $\varphi$  аддитивной группы рациональных чисел  $(\mathbb{Q}, +)$ , ядром которого является подгруппа целых чисел  $(\mathbb{Z}, +)$ . Для этого рассмотрим каноническое отображение

$$p: (\mathbb{Q}, +) \rightarrow (\mathbb{Q}, +)/(\mathbb{Z}, +).$$

Знаем, что по определению ядром гомоморфизма  $p$  будет аддитивная группа целых чисел, что нам и нужно было.

**Пример 2.4.6.** Пусть  $G$  — абелева группа и  $H$  — подгруппа всех ее элементов конечного порядка. Тогда в фактор-группе  $G/H$  все неединичные элементы имеют бесконечный порядок.

## 2.4.2 Теорема о гомоморфизмах

Мы подобрались к одной из ключевых теорем теории групп, которая является неким аналогом метода математической индукции для теории групп. Без шуток. Многие средней трудности теоремы доказываются с использованием индукции по размерности или порядку рассматриваемого алгебраического объекта и часто для индукционного перехода используют понятие фактор-пространства (или в нашем случае, фактор-группы).

К вышесказанному можно добавить, что теоремы о гомоморфизмах продолжают тенденцию, начатую во подразделе о гомоморфизмах: мы лишний раз убедимся, что нормальные подгруппы и ядра гомоморфизмов — это один объект, который мы можем называть по-разному точно так же, как и многие объекты можно описывать на разных языках мира.

Приступим к формулировке теорем о гомоморфизмах.

**Теорема 2.4.7.** (первая теорема о гомоморфизмах) Пусть  $\varphi: G_1 \rightarrow G_2$  — гомоморфизм. Тогда существует канонический гомоморфизм между двумя группами:

$$G_1 / \text{Ker } \varphi \cong \text{Im } \varphi.$$

*Доказательство.* Биективность отображения следует из того, что если  $\varphi: g \mapsto h$ , то  $g \cdot \text{Ker } \varphi = \varphi^{-1}(h)$ . При этом отображение  $\psi: g \text{Ker } \varphi \mapsto \varphi(g)$  будет заимствовать гомоморфность у  $\varphi$ , так как ядро — нормальная подгруппа элементов, которые переходят в нейтральный элемент. ■

**Пример 2.4.8.** Покажем, что  $(\mathbb{R}, +)/(\mathbb{Z}, +) \cong \mathbb{T}$ . Для этого рассмотрим гомоморфизм:

$$\varphi: (\mathbb{R}, +) \rightarrow \mathbb{T}, \quad x \mapsto e^{2\pi i x}.$$

Видно, что  $\text{Im } \varphi = \mathbb{T}$ , а  $\text{Ker } \varphi = (\mathbb{Z}, +)$ . По первой теореме о гомоморфизмах получаем искомое.

Для второй теоремы о гомоморфизмах мы докажем промежуточное утверждение.

**Утверждение 2.4.9.** Пусть  $H, N$  — подгруппы в  $G$ , притом  $N$  нормальна в ней. Тогда имеют место три предложения:

- (1)  $H \cdot N$  — подгруппа в  $G$ ;
- (2)  $N \cap H \triangleleft H$ ;
- (3)  $N \triangleleft H \cdot N$ .

**Замечание.** Здесь  $H \cdot N \stackrel{\text{def}}{=} \{hn: h \in H, n \in N\}$ .

*Доказательство.* (1) Для доказательства этого факта воспользуемся критерием подгруппы и покажем, что это множество замкнуто относительно взятия обратного и произведения. Отметим, что в обоих случаях будет важна нормальность подгруппы  $N$ , так что это свойство, которое нельзя убрать из формулировки утверждения.

Начнем с замкнутости: для любых  $h_1, h_2 \in H$ ,  $n_1, n_2 \in N$  покажем, что  $h_1 n_1 h_2 n_2 \in H \cdot N$ . Для этого заметим, что  $n_1 h_2 \in N h_2 = h_2 N$ , откуда мы можем заключить, что существует такой  $n_3$ , что  $n_1 h_2 = h_2 n_3$ . Следовательно,

$$h_1 n_1 h_2 n_2 = h_1 h_2 n_3 n_2 = (h_1 h_2)(n_3 n_2) \in H \cdot N.$$

Теперь покажем замкнутость этого множества относительно взятия обратного: пусть  $h \in H$ ,  $n \in N$ . Тогда  $(hn)^{-1} = n^{-1}h^{-1} \in N h^{-1} = h^{-1}N$ . Из последней формулы следует, что существует такой  $n_2 \in N$ , что

$$n^{-1}h^{-1} = h^{-1}n_2 \in H \cdot N.$$

Итак, мы показали верность обоих пунктов эквивалентных определению подгруппы, так что можем на этом остановиться.

(2) Для доказательства этого факта мы рассмотрим канонический гомоморфизм:

$$p: G \rightarrow G/N.$$

Мы знаем, что  $H$  подгруппа в  $G$ , откуда легко получить, что  $p(H)$  будет подгруппой в  $G/N$ . Поэтому мы можем ограничить наше отображение на  $H$  и получим

$$p|_H: H \rightarrow p(H).$$

Это отображение с очевидностью наследует гомоморфность отображения  $p$ . Следовательно, его ядро является нормальной подгруппой в  $H$ , что доказывает искомое утверждение, так как

$$\text{Ker } p|_H = \text{Ker } p \cap H = N \cap H.$$

(3) Здесь мы воспользуемся опять критерием нормальности подгруппы и вспомним, что

$$\forall g \in G: gNg^{-1} \subseteq N.$$

Отсюда следует, что и для всех элементов из  $H \cdot N$  это будет так. Заметим еще, что  $N \subseteq H \cdot N$ , что завершает доказательство. ■

Теперь с помощью последнего утверждения мы можем сформулировать следующую теорему.

**Теорема 2.4.10.** (вторая теорема о гомоморфизмах) Пусть  $H, N$  — подгруппы в  $G$ , притом  $N$  нормальна в ней. Тогда имеет место изоморфизм:

$$(H \cdot N)/N \cong H/(H \cap N).$$

*Доказательство.* Рассмотрим гомоморфизм из доказательства последнего утверждения:

$$p|_H: H \rightarrow p(H).$$

По первой теореме о гомоморфизме мы уже имеем

$$H/(H \cap N) \cong p(H),$$

поэтому остается показать, что

$$p(H) = (H \cdot N)/N.$$

Для этого покажем включение в обе стороны. Во-первых, образ  $H$  при отображении  $p$  состоит из классов смежности вида  $hN$ , что очевидно лежит в  $(H \cdot N)/N$ , так как  $H \subseteq H \cdot N$ . Отсюда автоматически следует, что  $p(H) \subseteq (H \cdot N)/N$ . Во-вторых, все элементы  $(H \cdot N)/N$  имеют вид  $(hn)N = hN = p(h) \in p(H)$ , что показывает включение в другую сторону и завершает доказательство. ■

**Пример 2.4.11.** Пусть  $H$  — это подгруппа в  $S_n$ , содержащая нечетную перестановку. Тогда по второй теореме о гомоморфизме мы можем сказать, что

$$H/(H \cap A_n) \cong (HA_n)/A_n = S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}.$$

**Пример 2.4.12.** Пусть  $n, m \in \mathbb{Z}$  и  $d$  — наибольший общий делитель  $m$  и  $n$ , а  $l$  — наименьшее общее кратное этих же двух чисел. Тогда

$$d\mathbb{Z}/n\mathbb{Z} = (m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} \cong m\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}) = m\mathbb{Z}/l\mathbb{Z}.$$

Для доказательства третьей теоремы сформулируем вспомогательное утверждение.

**Утверждение 2.4.13.** Пусть  $G$  — группа, в которой мы выделили две нормальные подгруппы  $N, K$ , такие что  $K \subseteq N$ . Тогда  $N/K$  — нормальная подгруппа в  $G/K$ .

И последняя теорема о гомоморфизмах.

**Теорема 2.4.14.** (третья теорема о гомоморфизмах) Пусть  $G$  — группа, в которой мы выделили две нормальные подгруппы  $N, K$ , такие что  $K \subseteq N$ . Тогда имеет место следующий изоморфизм:

$$(G/K)/(N/K) \cong G/N.$$

*Доказательство.* Воспользуемся первой теоремой о гомоморфизмах для следующего гомоморфизма:

$$\varphi: G/K \rightarrow G/N, \quad gK \mapsto gN.$$

■

На этом заканчивается список теорем о гомоморфизмах. И мы переходим к важным группам, которые ранее мы не успели обсудить.

### 2.4.3 Группа преобразований

Когда мы говорили о симметрической группе, то для ее определения мы фиксировали некоторое множество и рассматривали перестановки на нем. При этом рассматриваемое множество было конечно. А что будет если это множество будет бесконечно?

Оказывается, что даже над бесконечными множествами мы можем задавать конечные группы. А позже окажется, что все практически все группы, которые мы можем задать, имеют некоторые представления как группы преобразований. Следовательно, изучение таких групп полезно, так как оно ведет к лучшему пониманию свойств групп и выражению этих свойств в геометрических и комбинаторных свойствах объектов, над которыми мы и рассматриваем наши группы.

Пусть фиксировано множество  $X$ . Будем обозначать через  $S(X)$  — множество биекций из  $X$  в себя. Понятно, что  $S(X)$  — это группа относительно композиции.

**Определение 2.4.15.** Множество  $G \subseteq S(X)$  называется **группой преобразований**, если  $G$  вместе с композицией образует подгруппу.

**Замечание.** Часто  $X$  — это некоторый алгебраический или геометрический объект. В таком случае обычно рассматривают те подгруппы, которые сохраняют свойства  $X$  (например, если  $X$  — метрическое пространство, то рассматривают группы преобразований, которые сохраняют метрику).

**Пример 2.4.16.** Мы можем смотреть на преобразования пространства  $\mathbb{R}^3$ , которые переводят кубик в себя. Если при этом мы остановимся на тех преобразованиях, которые сохраняют расстояния между точками, а также углы между векторами, то мы получим **группу вращений кубика**.

**Пример 2.4.17.** Можем посмотреть на преобразования плоскости, которые переводят правильный  $n$ -угольник в себя, сохраняя расстояния между вершинами. Этую группу называют **группой Диэдра** и обозначают через  $D_n$ .

## 2.4.4 Группа автоморфизмов

Одной из самых важных групп преобразований над алгебраическим объектом является **группа автоморфизмов** некоторой группы. Ее обозначают через  $\text{Aut}(G)$  и включают в нее все отображения  $\varphi \in S(G)$ , которые являются автоморфизмами. Легко показать, что это действительно будет группой преобразований.

Следующий пример показывает, что знание каких-то автоморфизмов может привести к получению свойств самой группы.

**Пример 2.4.18.** Пусть дана конечная группа  $G$  с автоморфизмом  $\varphi \in \text{Aut}(G)$  порядка 2. Докажем, что если этот автоморфизм имеет одну неподвижную точку (то есть нейтральный элемент), то группа  $G$  абелева и  $\varphi(g) = g^{-1}$  для всех  $g \in G$ .

Для этого заметим, что для различных элементов  $a, b \in G$  верно, что  $\varphi(b^{-1}a) \neq b^{-1}a$ . Отсюда после преобразований при использовании простых свойств гомоморфизма получаем, что

$$\varphi(a)a^{-1} \neq \varphi(b)b^{-1}.$$

Следовательно,  $\psi: a \mapsto \varphi(a)a^{-1}$  инъективно, а значит, биективно. Откуда заключаем, что все элементы  $g \in G$  представимы в виде  $g = \varphi(a)a^{-1}$ . Остается посмотреть, что происходит с таким элементом при действии нашим автоморфизмом:

$$\varphi(g) = \varphi^2(a)\varphi(a^{-1}) = a\varphi(a)^{-1} = (\varphi(a)a^{-1})^{-1} = g^{-1}.$$

Мы доказали, что  $\varphi$  есть ни что иное, как автоморфизм обращения элемента. Тогда мы можем записать, что

$$ab = \varphi(a^{-1})\varphi(b^{-1}) = (\varphi(ba))^{-1} = ba,$$

что и доказывает абелевость группы  $G$ .

## 2.4.5 Внутренние автоморфизмы

Из всех автоморфизмов над группой  $G$  выделяются следующие:

$$\varphi_g: h \mapsto ghg^{-1},$$

где  $g$  — некоторый элемент группы  $G$ . Говорят, что  $\varphi_g$  действует на элемент  $h$  сопряжением. Можно заметить, что  $\varphi_g \circ \varphi_k = \varphi_{gk}$ . Кроме того  $(\varphi_g)^{-1} = \varphi_{g^{-1}}$ , откуда автоматически следует, что множество автоморфизмов описанного выше вида является подгруппой в  $S(X)$ . Отсюда следует, что это некоторая группа преобразований. Ее называют **группой внутренних автоморфизмов** и обозначают через  $\text{Int}(G)$  (или  $\text{Inn}(G)$ ).

**Утверждение 2.4.19.** Внутренний автоморфизм является автоморфизмом.

**Доказательство.** Необходимо показать биективность отображения и выполнение условия сохранения операции. Первое следует из следующих рассуждений:

$$\varphi_g(x) = \varphi_g(y) \Leftrightarrow x = y, \quad \forall x \in G: g^{-1}xg \in \varphi_g^{-1}(x).$$

Для второго мы можем выписать еще один ряд формул:

$$\varphi_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi_g(x) \cdot \varphi_g(y).$$

■

**Следствие 2.4.20.**  $\text{Int}(G) < \text{Aut}(G)$ .

**Пример 2.4.21.** Докажем, что в любой группе элементы  $gh$  и  $hg$  имеют одинаковые порядки. Для этого заметим, что  $\varphi_g(hg) = gh$ . Так как  $\varphi_g \in \text{Aut}(G)$ , то этот гомоморфизм сохраняет порядки элементов, откуда и следует искомое утверждение.

## Домашнее задание

**Задача 2.4.1.** Предположим, что построен гомоморфизм  $\varphi$  аддитивной группы рациональных чисел  $(\mathbb{Q}, +)$ , ядром которого является подгруппа целых чисел  $(\mathbb{Z}, +)$ . Проверьте, что  $(\mathbb{Q}, +)/\ker \varphi$  бесконечна, но все ее элементы имеют конечный порядок.

**Задача 2.4.2.** Укажите такую абелеву группу  $G$  и две такие ее изоморфные подгруппы  $H_1, H_2$ , что фактор-группы  $G/H_1$  и  $G/H_2$  неизоморфны.

**Задача 2.4.3.** Докажите следующие изоморфизмы: а)  $(\mathbb{C}, +)/(\mathbb{R}, +) \cong (\mathbb{R}, +)$ ; б)  $(\mathbb{C}^*, \cdot)/(\mathbb{R}^*, \cdot) \cong \mathbb{T}$ ; в)  $\mathbb{T}/\mu_n \cong \mathbb{T}$ .

**Задача 2.4.4.** Пусть даны  $G, N$  — группа и нормальная подгруппа в ней. При этом  $(|N|, |G/N|) = 1$ . Докажите, что тогда  $N$  — единственная подгруппа порядка  $|N|$ .

**Задача 2.4.5.** Пусть  $G$  — группа вращений трехмерного куба, а  $H_v$  — ее подгруппа, состоящая из тех вращений, которые оставляют вершину  $v$  на месте. Указать повороты на  $90^\circ$  и  $180^\circ$  из одного смежного класса по подгруппе  $H_v$ .

**Задача 2.4.6.** В группе симметрий тетраэдра найти подгруппы изоморфные а)  $D_3$ ; б)  $C_4$ . В группе вращений тетраэдра найти подгруппы изоморфные в)  $C_2$ ; г)  $C_3$ .

**Задача 2.4.7.** а) Докажите, что группа автоморфизмов циклической группы абелева. б) Найти порядок группы автоморфизмов циклической группы порядка 12. в) Является ли эта группа циклической?

**Задача 2.4.8.** Докажите, что подгруппа  $\text{Int}(G)$  внутренних автоморфизмов группы  $G$  нормальна в группе  $\text{Aut}(G)$  всех автоморфизмов  $G$ .

**Задача 2.4.9.** Докажите, что  $G/Z(G) \cong \text{Int}(G)$ .

**Задача 2.4.10.** а) Докажите, что количество элементов в классе сопряженности является делителем порядка группы. б) Докажите, что количество внутренних автоморфизмов (то есть автоморфизмов вида  $x \mapsto g x g^{-1}$ ) конечной группы делит порядок группы.

**Бонусная задача.** а) Найти порядок группы  $G = \text{Aut}(C_3 \times C_3)$  автоморфизмов прямого произведения двух циклических групп  $C_3$ . б) Постройте сюръективный гомоморфизм  $\text{Aut}(C_3 \times C_3) \rightarrow S_4$ .

## Рекомендуемая литература

- [1] Алексеев В. Б. — Теорема Абеля в задачах и решениях. — Новое изд. — М.: МЦНМО, 2017. — Глава 1, §2, 9, 11.
- [2] Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Раздел 4.
- [3] Городенцев А. Л. — Алгебра. Численник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 4, §15, 16.
- [4] Кострикин А. И. — Введение в алгебру: В 3-х ч. — Четвертое издание, стереотип. — М.: МЦНМО, 2020. — Глава 4, §2.

## 2.5 Геометрические и комбинаторные группы. Коммутант

Мы изучили достаточно подробно ту базовую теорию, которая позволяет работать с группами. Теперь настало время расширить множество классов групп, которые мы знаем. При этом мы увидим, что группы можно задавать или абстрактным способом, или с помощью каких-либо геометрических интерпретаций (например, как группу движений какого-либо объекта в пространстве).

**Ключевые слова:** порождающие, соотношения, группа кватернионов, свободная группа, конечно-порожденные абелевы группы, группа Диэдра, группа симметрий куба, группа симметрий ромба, коммутант.

### 2.5.1 Порождающие и соотношения

Мы уже говорили о порождающих в связи с циклическими группами. Сейчас же мы будем обобщать тот случай, и пользуясь теми конструкциями, которые мы ранее изучили, будем понимать, как можно задавать группы.

**Определение 2.5.1.** Будем говорить, что  $S \subseteq G$  **порождает группу  $G$** , если любой элемент  $g \in G$  можно представить в виде комбинации элементов из  $S$  и обратных к ним. При этом совокупность элементов из  $S$  называется **порождающими**.

**Замечание.** Если  $S$  порождает  $G$ , то пишут, что  $G = \langle S \rangle$ .

**Пример 2.5.2.** Любая циклическая группа порождается по определению некоторым элементом  $g$ . В конечном случае кроме этого элемента порождающими будут так же элементы  $g^m$ , где  $m$  взаимно просто с порядком группы. Отсюда следует, что количество порождающих в группе  $C_n$  равно  $\varphi(n)$ .

**Пример 2.5.3.** Рассмотрим группу  $S_n$ . Мы знаем, что любую перестановку можно разложить в произведение циклов. Менее тривиальное утверждение состоит в том, что любой цикл мы можем представить в виде произведений транспозиций  $(i \ i+1)$ . Отсюда следует, что

$$S_n = \langle (12), (23), (34), \dots, (n-1 \ n) \rangle.$$

**Пример 2.5.4.** Есть очень важное в механике векторное пространство, элементы которого называются **кватернионами**. Формально это — четырехмерное вещественное пространство, элементы которого записываются (по аналогии с комплексными числами) в виде

$$\mathbf{x} = x_0 + x_1 \cdot i + x_2 \cdot j + x_3 \cdot k,$$

где  $i, j, k$  — это формальные величины, которые перемножаются по правилам:

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j.$$

Нам будут интересны группа из восьми кватернионов, которую обозначают обычно  $Q_8$ . Ее состав:

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

Это множество образует мультиликативную группу. Легко заметить, что это неабелева группа, так что она не циклическая. Следовательно, чтобы породить такую группу надо взять, как минимум, два элемента этой группы. Далее простая арифметика подсказывает, что

$$Q_8 = \langle i, j \rangle = \langle j, k \rangle = \langle k, i \rangle.$$

Что есть важного в примерах выше? В них есть *соотношения*, которые определяются группой. То есть нам недостаточно просто указать, какие элементы порождают группу. Помимо этого необходимо еще показать, какие комбинации дают нейтральный элемент группы  $G$ . Попробуем обобщить эту конструкцию.

Возьмем множество  $S$  (здесь будем считать, что оно конечно, хотя в общем случае оно может быть произвольной мощности). В примере 2.1.11 мы рассматривали множество слов, которые мы можем получить над алфавитом  $\Lambda$ . Будем считать, что  $\Lambda = S \sqcup S^{-1}$ , где  $S^{-1}$  состоит из формальных обратных элементов к элементам из  $S$ .

Нельзя просто взять множество слов и называть группой. Мы видели, что это моноид, но обратимость нам еще никто не обещал даже если мы рассматриваем множество слов над  $S \sqcup S^{-1}$ . Чтобы обратимость появилась, будем рассматривать не множество слов, а класс эквивалентных слов (почувствуйте аналогию с определением векторов на аналитической геометрии), где эквивалентность выглядит следующим образом:

$$\begin{aligned} \forall \omega_1, \omega_2 \in \Lambda^*: \omega_1 \sim \omega_2 \Leftrightarrow \exists u, v \in \Lambda^*, \exists g \in S: \omega_1 = uv, \omega_2 = ug^{-1}v \vee \\ \vee \omega_1 = uv, \omega_2 = ug^{-1}gv \vee \omega_1 = ugg^{-1}v, \omega_2 = uv \vee \omega_1 = ug^{-1}gv, \omega_2 = uv. \end{aligned}$$

**Замечание.** Не пугайтесь формулы выше. Суть этой эквивалентности в том, что мы можем сокращать на пары  $gg^{-1}$  и  $g^{-1}g$ , которые увидим в слове.

**Утверждение 2.5.5.**  $(\Lambda^*/\sim, \circ)$  — группа.

Если множество  $S$  имеет порядок  $n$ , то говорят, что оно порождает **свободную группу ранга  $n$**  и пишут  $\langle S \rangle = F_n$ . Как легко заметить, при  $n = 1$  эта группа  $F_1 \cong \mathbb{Z}$ . При  $n > 1$  она будет неабелевой. При этом свободная группа натурального ранга всегда бесконечна. А мы стремимся к тому, чтобы с помощью этой конструкции описать все группы. Так как же ограничить группу? Ответ прост: с помощью соотношений. Сформулируем важную для формализма теорему.

**Теорема 2.5.6.** (Нильсона-Шрайера) Любая подгруппа свободной группы свободна.

**Замечание.** Ранг подгруппы не обязан быть меньше ранга группы. Он даже может быть равен бесконечности.

**Утверждение 2.5.7.** Любая конечно-порожденная группа является фактор-группой свободной группы.

**Доказательство.** Пусть  $G$  порождается элементами  $g_1, \dots, g_n$ . Определим следующий гомоморфизм  $\varphi: F_n \rightarrow G$ , который переводит порождающие свободной группы в  $g_i$ ,  $i \in \overline{1, n}$ . Так как  $g_i$  порождали группу  $G$ , этот гомоморфизм сюръективен, а значит,  $\text{Im } \varphi = G$ . По первой теореме о гомоморфизме получаем, что

$$G = \text{Im } \varphi \cong F_n / \text{Ker } \varphi.$$

■

Суммируя теорему Нильсона-Шрайера и последнее утверждение, мы получаем, что есть свободная нормальная подгруппа  $H$  в  $F_n$ , фактор по которой дает группу  $G$ . Так как эта подгруппа свободна, то есть набор элементов  $\omega_i \in H$ , порождающих подгруппу. Далее под *соотношением* мы будем подразумевать

$$\omega_i = e.$$

Если для группы заданы порождающие элементы и соотношения на них, то пишут обычно

$$G = \langle g_1, \dots, g_n | \omega_1 = e, \dots, \omega_m = e \rangle.$$

**Пример 2.5.8.** Циклическая группа порядка  $n$  — это  $C_n = \langle g | g^n = e \rangle$ .

**Пример 2.5.9.** Чтобы получить конечно-порожденные абелевы группы, необходимо взять свободную группу  $F_n$  с порождающими  $e_1, \dots, e_n$  и наложить на них соотношения, среди которых будут и соотношения вида:

$$e_i e_j e_i^{-1} e_j^{-1} = e,$$

то есть коммутатор любых двух базисных элементов равен нейтральному элементу.

**Пример 2.5.10.** Группу  $Q_8$  можно задать следующим образом

$$Q_8 = \langle (-1), i, j, k | (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle.$$

Далее мы рассмотрим простой случай абелевых групп и поймем, как можно классифицировать конечно-порожденные абелевы группы. После чего мы рассмотрим отдельно геометрические группы и укажем для них порождающие множества с соотношениями.

## 2.5.2 Конечно-порожденные абелевы группы

Теория начинается с того, что если мы позволим коммутировать элементы  $\Lambda = S \sqcup S^{-1}$  друг с другом, то мы из свободной группы  $F_n$  получим группу изоморфную  $\mathbb{Z}^n$ . Более того, имеет место следующее утверждение, похожее на теорему Нильсона-Шрайера.

**Утверждение 2.5.11.** Любая подгруппа  $\mathbb{Z}^n$  изоморфна  $\mathbb{Z}^m$ , где  $0 \leq m \leq n$ .

**Следствие 2.5.12.** В бесконечной циклической группе любая нетривиальная подгруппа изоморфна бесконечной циклической группе.

Обычно, чтобы отдельно показать, что мы рассматриваем абелевы группы, произведение групп  $G_1$  и  $G_2$  записывают через  $G_1 \oplus G_2$ . Мы здесь будем придерживаться таких нотаций.

**Теорема 2.5.13.** Конечно-порожденная абелева группа  $G$  разлагается в сумму

$$G = \bigoplus_{i=1}^m C_{q_i}^{m_i},$$

где  $q_i$  — это либо  $\infty$ , либо степень простого числа.

**Пример 2.5.14.** Покажем, что абелева группа порядка 26 всегда циклична. Для этого представим эту группу в виде суммы циклических групп:

$$G \cong C_2 \oplus C_{13} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{13}.$$

Видно, что  $(1, 1)$  является порождающим этой группы.

**Пример 2.5.15.** Сколько существует абелевых групп порядка 24? В разложении выше применительно к группе порядка 24 все  $q_i$  являются степенями простых чисел, а значит, они могут равняться: 3, 2, 4, 8. Простой перебор показывает, что есть 3 неизоморфных группы:

$$C_2 \oplus C_2 \oplus C_2 \oplus C_3, \quad C_2 \oplus C_4 \oplus C_3, \quad C_8 \oplus C_3.$$

Как мы позже увидим, конечно-порожденные абелевы группы возникают в теории делимости целых чисел.

### 2.5.3 Группа Диэдра

Мы уже обсуждали, что такое группа преобразований и в частности, что такое *группа Диэдра*. Здесь же мы хотим отдельно отметить, что

$$D_n \cong \langle r, s | r^n = e, s^2 = e, (sr)^2 = e \rangle,$$

что следует из того, что группа Диэдра порождается наименьшим поворотом и симметрией.

Менее очевидное утверждение, что если  $s_i$  и  $s_{i+1}$  — это симметрии относительно осей, отличающихся на минимальный угол, то они порождают группу Диэдра, то есть

$$D_n \cong \langle s_1, s_2 | s_1^2 = s_2^2 = (s_1 s_2)^n = e \rangle.$$

Эту группу интересно исследовать на предмет простых конструкций, которые мы ранее изучали. Например, вполне очевидно, что порядок группы Диэдра равен  $2n$ . При этом в этой группе есть группа поворотов изоморфная  $C_n$ . Можем заметить, что это подгруппа индекса 2, так что она нормальна в  $D_n$ .

**Пример 2.5.16.** Найдем всевозможные подгруппы в  $D_n$ . Понятно, что если  $m$  делит  $n$ , то в  $D_n$  есть подгруппа, изоморфная  $D_m$ . Это следует напрямую из геометрии действия группы Диэдра. Кроме того, очевидно, что при тех же ограничениях на  $m$  мы можем найти подгруппу, изоморфную  $C_m$  (подгруппу вращений).

Есть также и маленькие подгруппы, которые порождаются симметриями. Они все изоморфны  $C_2$ .

Остается заметить, что если у нас в подгруппе есть несколько симметрий, то композиция двух дает поворот, а значит мы автоматически получаем какую-то подгруппу Диэдра в этой группе. Следовательно, в группе Диэдра нет больше подгрупп, кроме тех, что перечислены выше.

### 2.5.4 Группы симметрий и группы вращений

Группа Диэдра описывает симметрию правильного многоугольника. Но ведь есть еще пла-тоновы тела — очень симметричные объекты в пространстве. Мы можем посчитать их симметрии? Оказывается: да, можем. Более того, если мы посмотрим на группы симметрий, то поймем, почему так мало симметричных тел. Такой подход и позволил математику Шлефли классифицировать правильные многогранники в  $n$ -мерном пространстве.

**Пример 2.5.17.** Сколько существует вращений у куба? Для подсчета заметим, что любую вершину куба мы можем перевести в любую другую. При этом есть 3 варианта, как мы можем разместить эту вершину в углу куба. Следовательно, количество вращений равно произведению этих двух чисел, то есть  $8 \cdot 3 = 24$ .

Мы можем искать группы вращений и симметрий не обязательно у правильного многогранника или многоугольника.

**Пример 2.5.18.** Рассмотрим ромб. Легко заметить, что в нем группа симметрий уже не будет переводить любую вершину в любую другую вершину. Получается, что есть всего 4 симметрии ромба. А что это за группа? Понятно, что она изоморфна либо  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ , либо  $\mathbb{Z}_4$ . Но какую выбрать? Ответ: первую группу, так как видно, что любая симметрия ромба имеет порядок 2.

**Замечание.** Интересный факт: если мы берем квадрат и немного сжимаем вершин, то получаем ромб, группа симметрий которого меньше группы симметрий квадрата. Отсюда автоматически следует, что в группе симметрий квадрата есть подгруппа изоморфная  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

## 2.5.5 Коммутант

И напоследок рассмотрим одну важную конструкцию. Для ее введения определим отдельно **коммутатор** двух элементов:

$$[x, y] \stackrel{\text{def}}{=} xyx^{-1}y^{-1}.$$

**Определение 2.5.19.** Подгруппа, порожденная коммутаторами, называется **коммутантом**.

**Замечание.** Коммутант группы  $G$  обозначаются через  $G'$  или  $[G, G]$ .

Как можно легко заметить, коммутатор двух элементов очень сильно связан с перестановкой этих двух переменных местами:

$$xy = [x, y]yx.$$

Можно предположить, что коммутант будет обладать какими-то хорошими свойствами, связанными с коммутативностью. Однако вряд ли вы, если не сталкивались с этим понятием ранее, можете представить себе, насколько это хорошая подгруппа.

**Утверждение 2.5.20.** Коммутант группы  $G$  является нормальной подгруппой.

**Пример 2.5.21.** Если группа  $G$  абелева, то ее коммутант тривиален  $G' = \{e\}$ .

**Пример 2.5.22.** Найдем коммутант для группы  $S_3$ . Для этого вспомним, что обратная к транспозиции — это транспозиция. А в  $S_3$  произведение двух транспозиций есть цикл длины 3. Следовательно,

$$[(12), (13)] = ((12)(13))^2 = ((132))^2 = (123).$$

При этом можно заметить, что коммутатор двух перестановок — это четная перестановка. Откуда получается, что мы не можем получить ничего больше  $A_3$ . Следовательно,  $S'_3 = A_3$ .

## Домашнее задание

**Задача 2.5.1.** Пусть  $G$  — группа, порожденная элементами  $a$  и  $b$ , для которых выполняются соотношения  $ab = ba$ ,  $a^2 = b^2$ ,  $a^4b^4 = e$ . Найдите порядок группы. Является ли группа циклической?

**Задача 2.5.2.** Задайте с помощью порождающих и соотношений группу  $A_4$ .

**Задача 2.5.3.** а) Пусть  $G_1 = \langle S_1 | R_1 \rangle$ ,  $G_2 = \langle S_2 | R_2 \rangle$ ,  $G_1 \times G_2 = \langle S_3 | R_3 \rangle$ . Выразите  $S_3$  и  $R_3$  через  $S_1$  и  $S_2$ . б) С помощью полученного в первом пункте выражения докажите еще раз, что  $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ , если  $(n, m) = 1$ .

**Задача 2.5.4.** При каких  $n$  группа Диэдра  $D_n$  изоморфна  $\mathbb{Z}_2 \oplus \mathbb{Z}_n$ .

**Задача 2.5.5.** Какие из перечисленных групп ниже будут изоморфны

$$D_8, \quad D_4 \times \mathbb{Z}_2, \quad Q_8 \times \mathbb{Z}_2?$$

**Задача 2.5.6.** Склейм две равнобокие пирамиды по квадратным основаниям (получим почти правильный октаэдр). Найдите группу вращений и группу симметрий получившейся фигуры.

**Задача 2.5.7.** Доказать, что а) группа вращений трехмерного куба изоморфна группе  $S_4$ ; б) группа симметрий куба изоморфна группе  $S_4 \times \mathbb{Z}_2$ .

**Задача 2.5.8.** Найти коммутант группы а)  $D_n$ ; б)  $S_4$ .

**Задача 2.5.9.** Найти коммутант групп а)  $A_4$ ; б)  $Q_8$ .

**Задача 2.5.10.** Докажите, что фактор-группа  $G/H$  абелева тогда и только тогда, когда  $H$  содержит коммутант группы  $G$ .

**Бонусная задача.** Найти коммутант группы невырожденных верхнетреугольных матриц  $n \times n$ .

## Рекомендуемая литература

- [1] Алексеев В. Б. — Теорема Абеля в задачах и решениях. — Новое изд. — М.: МЦНМО, 2017. — Глава 1, §1, 6, 12.
- [2] Журавлёв Ю. И., Флёрков Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Раздел 5.
- [3] Городенцев А. Л. — Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 4, §15, 16.
- [4] Смирнов Е. Ю. — Группы отражений и правильные многогранники. — 2-е изд., испр. и доп. — М.: МЦНМО, 2018. — Лекция 1, 2½.
- [5] Винберг Э. Б. — Курс Алгебры — 2-е изд., стереотип. — М.: МЦНМО, 2013. — Глава 4, §4.

## 2.6 Связь с теорией чисел

Сейчас мы отступим от общей теории групп и покажем, как связана та теория, которую мы уже изучили, с теорией групп.

**Ключевые слова:** мультипликативная группа вычетов, первообразный корень, малая теорема Ферма, теорема Эйлера, китайская теорема об остатках, мультипликативность функции Эйлера, квадратичный вычет, критерий Эйлера, символ Лежандра.

### 2.6.1 Мультипликативная группа вычетов

Для начала покажем, какие есть мультипликативные группы вычетов. Чтобы вычет  $a$  был обратимым по умножению, должен существовать такой  $x$ , что выполнено равенство

$$a \cdot x = 1 \pmod{n}.$$

**Утверждение 2.6.1.** Вычет обратим тогда и только тогда, когда он взаимно прост с модулем.

Так как обратимость на языке делимости означает взаимную простоту  $a$  и  $n$ , остается только проверить, что этого достаточно, чтобы построить группу.

**Утверждение 2.6.2.** Обозначим через  $\mathbb{Z}_n^*$  множество вычетов по модулю  $n$ , которые взаимно просты с  $n$ . Тогда  $(\mathbb{Z}_n^*, \cdot)$  — группа.

**Замечание.** Эту группу называют **мультипликативной группой вычетов по модулю  $n$** . Обозначают ее обычно просто  $\mathbb{Z}_n^*$ . И как легко заметить, в этой группе ровно  $\varphi(n)$  чисел.

**Пример 2.6.3.** Найдем вычет, обратный 13 в мультипликативной группе кольца  $\mathbb{Z}/109\mathbb{Z}$ .

Для этого заметим, что достаточно решить следующее диофантово уравнение:

$$13x - 109y = 1.$$

Так что с помощью расширенного алгоритма Евклида находим частное решение:

$$(109, 13) = (13, 5) = (5, 3) = (3, 2) = (2, 1) = 1 \Rightarrow 1 = 42 \cdot 13 - 109 \cdot 5 \Rightarrow 13^{-1} = 42 \pmod{109}.$$

Также можно заметить, что так как  $\varphi(n) = n - 1$  тогда и только тогда, когда  $n$  — простое число, то множество  $\mathbb{Z}_n^*$  совпадает с  $\mathbb{Z}_n \setminus \{0\}$ , только если  $n$  — простое число. Это свойство нам еще понадобится, когда мы будем работать с полями.

## 2.6.2 Первообразный корень

Мы оставим без доказательства следующее важное свойство.

**Теорема 2.6.4.** Мультипликативная группа вычетов по простому модулю  $n$  циклична.

**Замечание.** Порождающий мультипликативной группы вычетов по модулю  $n$  обычно называют **первообразным корнем**.

Что мы можем вынести сразу из этого свойства? Мы знаем, что в мультипликативной группе по простому модулю будет  $n - 1$  элемент. Так что количество порождающих будет равно  $\varphi(n - 1)$ . Притом если нам дан хотя бы один первообразный корень, то мы можем найти все оставшиеся.

**Пример 2.6.5.** Найдем первообразные корни по модулю 11. Легко проверить, что 2 будет таким корнем:

$$\begin{aligned} 2^2 &= 4, & 2^3 &= 8, & 2^4 &= 5, & 2^5 &= 10, & 2^6 &= 9, \\ 2^7 &= 7, & 2^8 &= 3, & 2^9 &= 6, & 2^{10} &= 1. \end{aligned}$$

Мы знаем, что  $|\mathbb{Z}_n^*| = 10$ , так что порождающих в этой группе ровно  $\varphi(10) = 4$ . И их все мы можем получить при возведении числа 2 в степень взаимно простую с 10, то есть первообразными корнями будут:

$$2^1 = 2, \quad 2^3 = 8, \quad 2^7 = 7, \quad 2^9 = 6.$$

Ниже при обсуждении квадратичных вычетов мы будем с вами использовать свойство цикличности мультипликативной группы вычетов.

## 2.6.3 Малая теорема Ферма и теорема Эйлера

Сейчас мы сформулируем две теоремы на языке теории чисел, которые звучат сложно, однако являются тривиальными следствиями той теории, которую мы до этого изучали.

**Теорема 2.6.6 (малая теорема Ферма).** Если  $p$  — простое число,  $a \in \mathbb{N}$  не делится на него, то

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Доказательство.* Если  $a$  не делится на  $p$ , то этому числу соответствует ненулевой вычет  $r$ , который с очевидностью лежит в  $\mathbb{Z}_p^*$ . По свойствам группы мы знаем, что порядок  $r$  делит порядок мультипликативной группы вычетов по модулю  $n$ , а значит:

$$r^{|\mathbb{Z}_p^*|} \equiv a^{p-1} \equiv 1 \pmod{n}.$$

■

Сразу покажем на примере, как можно применять эту теорему.

**Пример 2.6.7.** Вычислите  $12^{257} \pmod{17}$ :

$$12^{257} = (12^{17-1})^{16} \cdot 12 \equiv 1^{16} \cdot 12 = 12 \pmod{17}.$$

**Пример 2.6.8.** Делится ли  $25^{54} - 1$  на 107?

Посчитаем вычет этого выражения по модулю 107:

$$25^{54} - 1 = 5^{108} - 1 \equiv 5^2 - 1 = 24 \pmod{107}.$$

Так как вычет не равен нулю, то и выражение из условия не делится.

Теперь перейдем к более сложной теореме.

**Теорема 2.6.9** (Эйлера). Если  $(a, n) = 1$ , то  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

*Доказательство.* Аналогично доказательству малой теоремы Ферма с отличием в том, что тут надо помнить, что  $|\mathbb{Z}_n^*| = \varphi(n)$ . ■

Отметим, что теоремы очень красивы и полезны, так как помогают перейти от поиска остатка числа  $a^m$  по модулю  $n$  к поиск остатка числа  $m$  по модулю  $\varphi(n)$ . Решение этой задачи обычно проще, чем путь в лоб: возвести в степень.

## 2.6.4 Китайская теорема об остатках

Несмотря на красоту двух теорем выше, они не позволяют решить общую задачу: что делать, когда число  $a$  не взаимно просто с  $n$ , а мы хотим найти остаток числа  $a^m$  по модулю  $n$ ? Для решения этой более общей задачи мы покажем, как с помощью теории конечно-порожденных абелевых групп, переводить одни линейные условия в теории чисел в другие условия на этом же языке.

**Теорема 2.6.10** (Китайская теорема об остатках). Пусть  $m_1, m_2, \dots, m_s$  — взаимно простые попарно числа. Обозначим через  $M$  произведение всех этих чисел. Утверждается, что между множеством вычетов  $r$  по модулю  $M$  и множеством упорядоченных вычетов  $r_1, \dots, r_s$  по модулям  $m_1, \dots, m_s$  имеется такая биекция, что множество решений уравнения

$$x \equiv r \pmod{M}$$

и множество решений системы

$$\begin{cases} x \equiv r_1 \pmod{m_1}, \\ x \equiv r_2 \pmod{m_2}, \\ \dots \\ x \equiv r_s \pmod{m_s} \end{cases}$$

совпадает.

Как и обещали, доказательство такое же короткое, как и длинная теория групп в разделах выше.

*Доказательство.* Мы знаем, что

$$\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \dots \oplus \mathbb{Z}_{m_s}.$$

Искомая биекция появляется из этого изоморфизма. ■

Замечательно то, что КТО (так часто сокращают название китайской теоремы об остатках) работает в две стороны и бывает полезна при переводе условий в обе стороны. Покажем это на примере.

**Пример 2.6.11.** Найдем остаток  $14^{25}$  при делении на 35. Заметим, что 14 и 35 не взаимно просты, так что мы не можем просто применить теорему Эйлера. Однако КТО подсказывает нам, что для нахождения остатка достаточно найти остатки по модулю 7 и по модулю 5. Это легко сделать:

$$14^{25} \equiv 0 \pmod{7}, \quad 14^{25} \equiv 14 \pmod{5}.$$

Далее нам остается только подобрать такой остаток по модулю 35, который даст 0 при делении на 7 и 14 при делении на 5. Китайская теорема об остатках при этом утверждает об единственности и существования такого решения. Получаем, что

$$14^{25} \equiv 14 \pmod{35}.$$

**Пример 2.6.12.** Найдем такие целые числа, которые дают остаток 1 при делении на 14 и при делении на 25. Заметим, что формально эти условия записываются так:

$$n \equiv 1 \pmod{14}, \quad n \equiv 1 \pmod{25}.$$

Как видно, из записи число 1 подходит в качестве решения. А из КТО следует, что все решения имеют вид  $n = n_0 + 14 \cdot 25 \cdot t$ , где  $t$  — некоторое целое число, то есть все числа, которые дают остаток 1 при делении на 350. Это и есть искомый ответ.

**Пример 2.6.13.** Решим систему уравнений

$$\begin{cases} x \equiv 2 \pmod{39}, \\ x \equiv -2 \pmod{29}. \end{cases}$$

Можно пойти двумя путями: сказать, что первое уравнение эквивалентно  $x = 2 + 39a$ , а второе —  $x = -2 + 29b$ . И дальше решить линейное диофантово уравнение.

Мне кажется, что это слишком просто, поэтому мы схитрим: прибавим в левой части 39 двенадцать раз, получим:

$$\begin{cases} x + 12 \cdot 39 \equiv 2 \pmod{39}, \\ x + 12 \cdot 39 \equiv -2 + 4 = 2 \pmod{29} \end{cases}$$

По КТО мы можем перейти к уравнению:

$$x + 12 \cdot 39 - 2 \equiv 0 \pmod{1131} \Rightarrow x = -466 + 1131 \cdot t, t \in \mathbb{Z}.$$

Покажем, какой еще интересный факт мы можем достать из КТО.

**Утверждение 2.6.14** (мультипликативность функции Эйлера). Если  $(n, m) = 1$ , то  $\varphi(nm) = \varphi(n) \cdot \varphi(m)$ .

*Доказательство.* Заметим, что китайская теорема об остатках говорит нам, что число  $a$  лежит в мультипликативной группе вычетов  $\mathbb{Z}_{nm}^*$  тогда и только тогда, когда  $a$  лежит в мультипликативных группах  $\mathbb{Z}_n^*$  и  $\mathbb{Z}_m^*$ . ■

**Замечание.** По сути изоморфизм между аддитивными группами можно опустить до изоморфизма мультипликативных групп вычетов. Это свойство подводит нас ближе к таким алгебраическим объектам, которые уже содержат несколько операций, которые между собой как-то связаны.

## 2.6.5 Квадратичные вычеты

Мы научились перекладывать линейные условия с языка теории чисел на язык теории групп. А что будет, если мы рассмотрим более сложные условия? Оказывается, что дальше теория развивается примерно с таким же пессимизмом, как и теория разрешимости многочленов в радикалах. Оказывается, что уже для поиска решений квадратного уравнений необходима большая теория, с которой мы сейчас и познакомимся.

**Определение 2.6.15.** Элемент  $a \in \mathbb{Z}_n$  называется **квадратичным вычетом**, если существует  $x$ , такой что  $x^2 \equiv a \pmod{n}$ . Остальные элементы называются **квадратичными невычетами**.

Может показаться, что уравнение имеет всегда два решения, как и в вещественных числах, и в комплексных числах. Однако простой пример  $\mathbb{Z}_8$  показывает, что это не так:

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}.$$

Достаточно очевидно, что множество квадратичных вычетов не совпадает со всем множеством вычетов в общем случае: 3 является квадратичным невычетом по модулю 4.

**Пример 2.6.16.** Решим уравнение  $x^2 - 1 \equiv 0 \pmod{143}$ . Для этого сначала воспользуемся КТО и найдем решения

$$x^2 \equiv 1 \pmod{11}, \quad x^2 \equiv 1 \pmod{13}.$$

Как мы позже увидим при работе с полями, при простом  $n$  уравнение выше не может иметь больше двух корней, а ими будут, легко проверить, 1 и  $-1$ . Следовательно, мы приходим к системе

$$\begin{cases} x \equiv \pm 1 \pmod{11}, \\ x \equiv \pm 1 \pmod{13}. \end{cases}$$

При выборе знаков мы получаем систему, которая решается единственным образом в  $\mathbb{Z}_{143}$ , так что можно либо решить честно такую систему, либо угадать решение:  $x = 1, 12, 131, 142$ .

Мы остановимся на случае, когда  $n$  — простое число (будем его обозначать через  $p$ ). Случай  $p = 2$  тривиален, так что будем предполагать, что  $p > 2$  везде далее.

**Утверждение 2.6.17.** В  $\mathbb{Z}_p$  есть ровно  $\frac{p-1}{2}$  ненулевых квадратичных вычетов.

**Доказательство.** Для начала заметим, что  $i^2 \equiv (p-i)^2 \pmod{p}$ , так что больше, чем  $\frac{p-1}{2}$ , мы получить не можем. Далее предположим, что

$$i^2 \equiv j^2 \pmod{p} \Leftrightarrow (i-j)(i+j) \equiv 0 \pmod{p}.$$

Отсюда в силу простоты числа  $p$  следует, что либо  $i-j$ , либо  $i+j$  делится на  $p$ . Но этому условию удовлетворяют только пары  $i = j$  или  $i = p-j$ . ■

**Утверждение 2.6.18.** Ненулевые квадратичные вычеты образуют подгруппу в  $\mathbb{Z}_p^*$ .

**Доказательство.** Так как  $p$  простое, то любой ненулевой вычет обратим, а значит:

$$(x^{-1})^2 \equiv a^{-1} \pmod{p},$$

то есть вместе с любым  $a$  квадратичным вычетом будет и обратный к нему по умножению элемент лежать в мультиликативной группе.

Произведение квадратичных вычетов тоже будет являться квадратичным вычетом:

$$x^2 \equiv a \pmod{p}, \quad y^2 \equiv b \pmod{p} \Rightarrow (xy)^2 \equiv a \cdot b \pmod{p}.$$

По критерию подгруппы это будет подгруппа в мультиликативной группе вычетов по модулю  $p$ . ■

Самый важный критерий квадратичного вычета звучит следующим образом.

**Теорема 2.6.19** (критерий Эйлера). Имеется критерий для ненулевого квадратичного вычета по модулю  $p$ :

1.  $a$  — квадратичный вычет тогда и только тогда, когда  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ;

2.  $a$  — квадратичный невычет тогда и только тогда, когда  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ .

**Доказательство.** Так как мультиликативная группа вычетов циклична, то все элементы являются степенями порождающего  $g$ . Легко заметить, что порождающий в степени  $k$  дает квадратичный вычет тогда и только тогда, когда  $k$  четное. При этом  $g^{\frac{p-1}{2}} = -1$ . Из этих двух свойств и следует искомое. ■

**Замечание.** Число  $0, 1, -1$  называют **символом Лежандра** для числа  $a$  по модулю  $p$ , если  $a = 1$ ,  $a$  — квадратичный вычет (не равный 1),  $a$  — квадратичный невычет соответственно.

Его обычно обозначают через  $\left(\frac{a}{p}\right)$ .

## Домашнее задание

**Задача 2.6.1.** а) Найти порядок мультиPLICATивной группы  $\mathbb{Z}_{72}^*$ .  
б) Решите уравнение  $17x \equiv 9 \pmod{72}$ .

**Задача 2.6.2.** Решите линейное диофантово уравнение:

$$33x + 23y = 4.$$

**Задача 2.6.3.** Найдите все первообразные корни по модулю 29.

**Задача 2.6.4.** Найдите наибольший порядок элемента мультиPLICATивной группы  $\mathbb{Z}_{72}^*$ .

**Задача 2.6.5.** Вычислите а)  $10^{111} \pmod{121}$ ; б)  $26^{21^{100500}} \pmod{14}$ .

**Задача 2.6.6.** Решить систему сравнений:

$$\begin{cases} 21x \equiv 13 \pmod{34}, \\ 7x \equiv 2 \pmod{73}. \end{cases}$$

**Задача 2.6.7.** Решить систему сравнений:

$$\begin{cases} x \equiv 1 \pmod{33}, \\ x \equiv -1 \pmod{23}. \end{cases}$$

**Задача 2.6.8.** Докажите, что множество решений сравнения  $x^2 \equiv 1 \pmod{n}$  образует подгруппу в  $\mathbb{Z}/n\mathbb{Z}$ .

**Задача 2.6.9.** а) Найдите сумму всех квадратичных вычетов по модулю 73. б) Найдите произведение всех квадратичных вычетов по модулю 103.

**Задача 2.6.10.** а) Покажите, что если  $p = 8k \pm 1$ , то  $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ . б) Покажите, что если  $p = 8k \pm 3$ , то  $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ . в) Исходя из полученного, вычислите  $\left(\frac{2}{p}\right)$ ,  $p > 2$ .

**Бонусная задача.** При каких целых  $n$  мультиPLICATивная группа  $\mathbb{Z}_n^*$  будет циклична?

## Рекомендуемая литература

- [1] Виноградов И. М. — Основы теории чисел. — М.-Л., Гостехиздат, 1952. — Глава 3, 4, 5, 6.
- [2] Дэвенпорт Г. — Высшая арифметика. Введение в теорию чисел. — Изд. "Наука" 1965 — Глава II, III.

## 2.7 Действия групп

В этот раз мы с вами расширим понимание групп преобразований за счет представлений некоторых известных нам групп. Нас ожидает теория, которая объяснит, как с помощью абстрактных групп мы можем решать вполне комбинаторные и геометрические задачи.

**Ключевые слова:** действие группы, орбита, стабилизатор, левые и правые сдвиги, теорема Кэли, лемма Бернсайда.

## 2.7.1 Действия групп: определение

Мы можем вспомнить, что группа преобразований — это подгруппа группы  $S(X)$ . Это полезное определение. Однако мы знакомы с разными классами групп в отсутствии их какого-либо представления внутри  $S(X)$ . Так как же мы можем его получить? Именно для ответа на подобные вопросы мы с вами и тратили некоторые время на знакомство с морфизмами и конструкциями.

**Определение 2.7.1.** Будем говорить, что задано *действие группы  $G$  на множестве  $X$* , если задан гомоморфизм  $\varphi: G \rightarrow S(X)$ .

**Замечание.** Как вы можете заметить, действие задается гомоморфизмом, так что оно не однозначно определено парой  $G$  и  $X$ .

**Замечание.** Чтобы не нагромождать формулы излишними буквами, часто вместо  $\varphi(g)(x)$  пишут  $gx$  или  $g(x)$ , подразумевая, что само действие задано где-то выше. Однако если на одном множестве мы можем задать несколько действий, то лучше использовать обычную нотацию, чтобы было понятно, какое из действий мы выбрали.

**Пример 2.7.2.** Предположим, что  $X \neq \emptyset$ , а  $G$  — произвольная группа. Тогда существует *тривиальное действие группы  $G$* , где  $\varphi: g \mapsto \text{id}_X$  для любого  $g \in G$ .

Конечно нельзя не вспомнить о важном классе симметрических групп.

**Пример 2.7.3.** Можем рассмотреть множество  $X = \overline{1, n}$ . Тогда по определению  $S_n = S(X)$ , а значит, у нас задано действие симметрической группы на  $n$ -элементном множестве.

Интересно, что за счет перестановок мы можем порождать и не столь тривиальные примеры действий, как выше.

**Пример 2.7.4.** Пусть у нас  $X = 2^{\overline{1, n}}$ , то есть  $X$  — это множество подмножеств  $n$ -элементного множества. Тогда мы можем задать действие группы  $S_n$  следующим образом:

$$\forall \sigma \in S_n, A \subseteq \overline{1, n}: \quad \sigma(A) = \{\sigma(x): x \in A \subseteq \overline{1, n}\}.$$

То есть произвольное множество  $A$  чисел от 1 до  $n$  будет переходить в множество образов своих чисел при действии на них перестановкой  $\sigma$ .

**Пример 2.7.5.** Как мы знаем, у нас есть интересная группа внутренних автоморфизмов:

$$\text{Int } G \triangleleft \text{Aut } G \triangleleft S(G).$$

Таким образом, мы можем говорить о *действии группы на себя сопряжениями*. При этом у вас элемент  $g$  действует на элемент  $h$ , переводя его в элемент  $ghg^{-1}$ .

**Пример 2.7.6.** Мы можем рассмотреть множество многочленов от  $n$ -переменных. Тогда группа  $S_n$  будет действовать на эти многочлены перестановкой переменных.

Геометрические интерпретации очень важны в этой науке. На следующем примере мы увидим, что, как и в случае с теорией чисел, геометрия позволяет получить нетривиальные групповые свойства.

**Пример 2.7.7.** Рассмотрим группу вращений куба. Мы знаем, что эта группа изоморфна  $S_4$ , так что можно считать, что эта группа действует на куб вращениями. Кроме того, мы знаем, что пары противоположных граней переходят в пары противоположных граней, так что

группа вращений действует на парах противоположных граней перестановкой. Следовательно, геометрический взгляд на группу вращений позволяет сказать, что мы имеем гомоморфизм  $\varphi: S_4 \rightarrow S_3$ . При этом видно, что все перестановки мы можем получить с помощью вращений вокруг главной диагонали и вращений вокруг оси, проходящей через середины ребер. Следовательно, этот гомоморфизм сюръективен. Видно, что ядро  $\varphi$  состоит из четырех вращений и можно посчитать, какие это будут вращения: они будут образовывать четверную группу Клейна  $V_4$  в  $S_4$ . Отсюда мы получаем, что

$$S_4/V_4 \cong S_3.$$

**Замечание.** Говорят, что действие группы *точное*, если ядро гомоморфизма  $\varphi$  тривиально. В последнем примере действие  $S_4$  вращениями на кубике точно, а действие  $S_4$  на перестановках пар граней уже не точно.

## 2.7.2 Орбита, стабилизатор

Как и ранее мы сталкивались с особыми конструкциями и группами в связи с какими-то задачами, так и тут есть своя терминология, которая используется при решении задач.

**Определение 2.7.8.** Пусть задано действие группы  $G$  на множестве  $X$ . Тогда **орбита точки  $x \in X$**  — это множество таких  $y$ , которые мы можем получить из  $x$  при действии элементами  $g \in G$ , то есть

$$Gx = \text{Orb}(x) = \{gx: g \in G\}.$$

**Замечание.** Орбиты образуют непересекающиеся классы эквивалентностей. Так что принадлежность одной орбите означает, что есть  $g \in G$ , переводящий один элемент в другой.

**Замечание.** Если орбита покрывает все множество  $X$ , то есть единственна, то говорят, что действие *транзитивно*. По сути это значит, что мы можем не отличать точки множества  $X$  относительно действия нашей группой.

**Определение 2.7.9.** Пусть задано действие группы  $G$  на множестве  $X$ . Тогда **стабилизатор точки  $x \in X$**  — это такие элементы группы  $G$ , которые оставляют точку  $x$  на месте, то есть

$$G_x = \text{Stab}(x) = \{g: gx = x\}.$$

Часто в прикладных задачах стабилизатор и орбиту легко посчитать, а за счет следующего утверждения мы можем получить порядок группы из найденных множеств.

**Утверждение 2.7.10.** Пусть задано действие конечной группы  $G$  на множестве  $X$ . Тогда для любой точки  $x \in X$  верно, что

$$|G| = |\text{Stab}(x)| \cdot |\text{Orb}(x)|.$$

**Пример 2.7.11.** Найдем порядок группы симметрий тетраэдра, не находя саму группу. Для этого заметим, что действие группой симметрий транзитивно на вершинах тетраэдра, а следовательно,  $|\text{Orb}(x)| = 4$  для любой вершины  $x \in X$ . Кроме того, имеется ровно 6 симметрий в группе, оставляющих вершину на месте (столько же, сколько есть симметрий правильного треугольника). Следовательно, итоговый порядок группы симметрий тетраэдра равен 24.

**Замечание.** В последнем примере можно заменить тетраэдр на произвольный  $n$ -мерный симплекс и можно получить, что его группа симметрий имеет порядок  $n!$  (и далее можно показать, что эта группа действительно совпадает с группой  $S_n$ ).

**Пример 2.7.12.** Группа вращений куба действует транзитивно на вершинах, а значит, орбита имеет порядок 8. Чтобы найти стабилизатор заметим, что вращение, оставляющее на месте вершину есть ни что иное, как вращение вокруг главной диагонали. Таких вращений всего 3. Отсюда получаем, что группа вращений куба имеет порядок 24.

Мы уже заметили с вами, что симметрическая группа возникает то тут, то там. Однако следующий пункт закрепит за этой группой центральное значение в теории конечных групп.

### 2.7.3 Теорема Кэли

Мы уже видели действия группы на самой себе. Например, с помощью сопряжения. Однако это действие не всегда является точным, а значит, мы не можем задать группу как группу каких-то внутренних автоморфизмов. Однако не стоит отчаиваться, ведь мы сейчас покажем еще два действия, которые уже будут точными. И они уже помогут нам сформулировать и доказать интересную теорему.

**Пример 2.7.13.** Группа  $G$  может действовать на себе с помощью левых сдвигов. Что это означает? В группе задано умножение. А давайте мы определим действие  $\lambda: G \rightarrow S(G)$  следующим образом:

$$\lambda(g)(h) \stackrel{\text{def}}{=} g \cdot h.$$

Видно, что это отображение будет являться гомоморфизмом, так как умножение в группе ассоциативно.

Имеется аналог — правые сдвиги:

$$\rho(g)(h) \stackrel{\text{def}}{=} h \cdot g^{-1}.$$

**Упражнение.** Почему при левых сдвигах мы умножаем на  $g$ , а при правых на  $g^{-1}$ ?

**Замечание.** Действие элементом  $g$  задает биекцию, которое не обязано быть гомоморфизмом, так что не стоит удивляться, что при сдвигах нейтральный элемент переходит не в нейтральный, да и гомоморфности, тем более, никакой нет.

**Теорема 2.7.14 (Кэли).** Любая конечная группа  $G$  изоморфна некоторой подгруппе  $S_n$  при некотором  $n$ .

**Доказательство.** Рассмотрим действие группы  $G$  на себе левыми сдвигами. Легко заметить, что это действие точно, а значит:

$$G \cong \text{Im } \lambda < S_{|G|}.$$

■

**Замечание.** Интересна задача поиска такого минимального  $n$  для группы  $G$ , чтобы она была подгруппой  $S_n$ . Как видно, минимальное  $n$  будет не больше порядка группы, однако достаточно легко привести пример группы, у которой такое минимальное  $n$  будет намного меньше.

Несмотря на свою универсальность, сама по себе теорема Кэли практически бесполезна, хотя левые сдвиги возникают в теории групп Ли, так что их стоит запомнить.

Ниже мы увидим, как получать комбинаторные следствия из той небольшой теории, которую мы описали выше.

## 2.7.4 Лемма Бернсайда

В комбинаторных задачах иногда говорят: найти количество объектов с точностью до группы симметрий. И на самом деле это важная задача, так как мы часто имеем дело с нефиксированными геометрическими объектами. В связи с этим бывает полезно считать количество орбит действия (далее будем обозначать это число через  $\#$ орбит).

**Теорема 2.7.15** (лемма Бернсайда). Пусть задано действие конечной группы  $G$  на множестве  $X$ . Обозначим через  $X_g$  множество таких точек, которые остаются на месте при действии элементом  $g$ , то есть

$$X_g \stackrel{\text{def}}{=} \{x : gx = x\}.$$

Тогда имеет место равенство

$$\# \text{орбит} = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

Намного легче понять на примере, как пользоваться этой леммой, чем доказать ее и пытаться понять обозначение вне практики. Так что посмотрим на пару примеров использования леммы Бернсайда.

**Пример 2.7.16.** Найдем количество различных раскрасок граней куба в два цвета. Различными мы будем считать те раскраски, которые не получаются друг из друга при помощи поворота куба.

Для начала стоит вспомнить все вращения куба: тождественное вращение, вращение на 90 градусов в количестве 6 штук, 3 вращения на 180 градусов относительно оси, проходящей через центр грани, 6 вращений на 180 градусов вокруг оси, проходящей через центры противоположных ребер, и еще 8 вращений на 120 градусов. Будем все эти вращения обозначать через  $s_0, s_1, s_2, s_3, s_4$  (исходя из их типа). Рассмотрим каждый тип и поймем, сколько раскрасок остаются на месте при действии соответствующим поворотом.

Стоит отметить, что важно понять, на каком множестве мы действуем нашими перестановками. В этой задаче  $X$  — это множество упорядоченных шестерок цветов, в которые мы раскрашиваем грани (сами грани мы можем упорядочить в любом порядке). Видно, что тогда орбиты — это множество раскрасок, которые не различимы для нас, так как получаются друг из друга при помощи вращения.

Приступим к перебору типов вращений.

1. При тождественном вращении любая раскраска с фиксированными гранями переходит в себя же, так что  $|X_{s_0}| = 2^6$ .
2. При вращении на 90 градусов все боковые грани должны иметь одинаковый цвет, чтобы раскраска перешла в себя, так что  $|X_{s_1}| = 2^3$ .
3. При вращении на 180 градусов, относительно оси, соединяющей центры противоположных граней, видно, что есть 2 пары противоположных боковых граней, которые должны иметь одинаковый цвет, и еще по одной грани сверху и снизу, так что  $|X_{s_2}| = 2^4$ .
4. При повороте на 180 градусов, относительно оси, соединяющей центры противоположных ребер, появляются три пары граней, которые будут иметь одинаковую раскраску, то есть  $|X_{s_3}| = 2^3$ .
5. И при вращении на 120 градусов вокруг главной диагонали грани бьются на 2 группы, а значит,  $|X_{s_4}| = 2^2$ .

Осталось воспользоваться леммой Бернсайда:

$$\# \text{орбит} = \frac{1}{24} (1 \cdot 2^6 + 6 \cdot 2^3 + 3 \cdot 2^4 + 6 \cdot 2^3 + 8 \cdot 2^2) = 10.$$

## Домашнее задание

**Задача 2.7.1.** Найдите порядок группы вращений додекаэдра.

**Задача 2.7.2.** Докажите, что  $\text{Stab}(x)$  является нормальной подгруппой в  $G$  тогда и только тогда, когда любой элемент  $g \in \text{Stab}(x)$  оставляет на месте не только  $x$ , но и любой элемент  $\text{Orb}(x)$ .

**Задача 2.7.3.** а) Докажите, что ядро действия группы  $G$  суть пересечение всех  $\text{Stab}(x)$ .  
б) Найдите ядро действия группы  $G$  на фактор-группу  $G/H$  с помощью сопряжений.

**Задача 2.7.4.** Найдите число различных раскрасок ребер трехмерного куба в два цвета. Две раскраски считаются различными, если нельзя добиться совпадения цветов ребер вращениями куба.

**Задача 2.7.5.** Найдите количество различных раскрасок 10 бусинок в три цвета, нанизанных на круглую ниточку.

**Бонусная задача.** Докажите, что при  $n \neq 6$  верно, что  $\text{Aut } S_n = \text{Inn } S_n$ .

## Рекомендуемая литература

- [1] Журавлёв Ю. И., Флёрков Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Раздел 6.
- [2] Кострикин А. И. — Введение в алгебру: В 3-х ч. — Четвертое издание, стереотип. — М.: МЦНМО, 2020. — Глава 1, §8.
- [3] Винберг Э. Б. — Курс Алгебры — 2-е изд., стереотип. — М.: МЦНМО, 2013. — Глава 10, §3.
- [4] Городенцев А. Л. — Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 4, §15.

# **Глава 3.**

## **Общая теория колец и полей**

## 3.1 Основы теории колец

Мы переходим к рассмотрению новых алгебраических объектов. Основное отличие колец и полей от групп в том, что они имеют уже не одну операцию.

После конструкций групп любые другие алгебраические объекты намного легче изучать, так как некоторые конструкции абсолютно повторяют конструкции теории групп (например, подкольцо определяется очень похожим образом, как и подгруппа). Между тем, эта теория развивалась неспроста, так как с помощью взгляда на некоторые объекты со стороны теории колец мы сможем дополнить свое понимание их свойств.

**Ключевые слова:** кольцо, обратимый элемент, группа обратимых элементов, делитель нуля, область целостности, кольцо многочленов, кольцо функций, логарифмическое свойство степени многочлена, нильпотент, идемпотент, подкольцо, прямая сумма колец.

### 3.1.1 Кольцо: определение и свойства

Начнем мы конечно с самого базового, а именно: определим тот алгебраический объект, который будем дальше изучать.

**Определение 3.1.1.** Тройку  $(R, +, \cdot)$  из множества и двух бинарных операций на нем мы будем называть **кольцом**, если выполнены следующие аксиомы:

R1. пара  $(R, +)$  является абелевой группой (аддитивная группа кольца);

R2.  $\forall a, b, c \in R: a \cdot (b + c) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c$  (двухсторонняя дистрибутивность).

**Замечание.** Так как по определению кольцо обладает аддитивной группой, то там есть нейтральный элемент по сложению. Как и в простых примерах, которые мы разберем дальше, в общем случае этот элемент кольца называется **нулем** и обозначается через 0.

**Замечание.** По очевидным причинам первую операцию называют *сложением в кольце*, а вторую — *умножением в кольце*. Теперь вы можете понять, почему в прошлой главе мы встречали группы, которые называли аддитивными или мультиплекативными.

Далее мы перечислим свойства колец, которые будем использовать при работе в следующих разделах. При этом в самой общей ситуации кольцо представляет именно ту тройку, которую мы описали выше, но исследование некоммутативных, а тем более неассоциативных колец, сопряжено с огромной трудностью, так что мы практически не будем их касаться в основной части нашего курса.

R3. Кольцо называется *ассоциативным кольцом*, если умножение ассоциативно (это означает, что пара  $(R, \cdot)$  образует уже полугруппу).

R4. Кольцо называется *коммутативным*, если умножение коммутативно.

R5. Кольцо называется *кольцом с единицей*, если в кольце есть 1, которая является нейтральным элементом по умножению (если кольцо еще и ассоциативно, то тогда пара  $(R, \cdot)$  — это уже монOID).

**Замечание.** Везде далее мы будем считать, что кольцо ассоциативно и  $0 \neq 1$ .

**Пример 3.1.2.** Типичными примерами очень хороших колец являются числовые кольца: целые числа, рациональные числа, вещественные числа, комплексные числа. Во всех этих случаях мы имеем дело с ассоциативным коммутативным кольцом с единицей.

**Пример 3.1.3.** Множество  $n\mathbb{Z}$ ,  $n \geq 2$ , целых чисел кратных  $n$  образует ассоциативное коммутативное кольцо. Но в отличие от просто целых чисел, в этом кольце уже нет единицы.

**Пример 3.1.4.** Простым примером некоммутативного кольца является множество матриц размера  $n \times n$  с вещественными коэффициентами, где  $n \geq 2$ . Кольцо матриц обычно обозначается либо  $M(n, \mathbb{R})$ , либо  $\text{Mat}(n, \mathbb{R})$  (мы будем придерживаться последней нотации). Обратите внимание, что матрицы квадратные, иначе произведение двух матриц не было бы определено.

Надо понимать, что есть много свойств числовых колец, которые выполняются в общем случае. Мы не будем сейчас тратить время на доказательство этих тривиальных свойств, но оставим любознательному читателю их в качестве задач.

**Замечание.** Под элементом  $(-x)$  мы традиционно будем подразумевать обратный по сложению элемент к  $x$ . Исходя из этого обозначения мы можем понять, что такая разница элементов  $x$  и  $y$ :

$$x - y \stackrel{\text{def}}{=} x + (-y).$$

### 3.1.2 Обратимые элементы кольца, делители нуля, область целостности

В этом подразделе будем считать, что нам задано коммутативное кольцо с единицей  $R$ . Среди элементов кольца есть те, которые имеют обратный по умножению. Выделим их.

**Определение 3.1.5.** Элемент  $x \in R$  называется **обратимым**, если существует такой элемент  $y \in R$ , что  $xy = yx = 1$ .

**Замечание.** Обычно говорят, что элемент обратим с какой-то стороны. И в некоммутативных кольцах эта разница может быть чувствительной. Однако в нашем курсе такие случаи не будут интересны в дальнейшем, так что мы остановимся на том определении, которое дали выше.

Множество обратимых элементов кольца обычно обозначается через  $R^*$ . С обратимыми элементами кольца связана замечательная теорема, отражающая необходимость в таком обозначении и связь с уже встретившимися нам случаями.

**Теорема 3.1.6.** Пара  $(R^*, \cdot)$  является группой.

**Доказательство.** По определению элемент 1 обратен сам себе, так что он лежит во множестве  $R^*$ . Легко проверить, что обратный элемент к обратному тоже обратим и из-за этого лежит в  $R^*$ . А также обратный для  $xy$  — это элемент  $y^{-1}x^{-1}$ , а значит, множество  $R^*$  замкнуто относительно произведения своих элементов и образует группу. ■

**Замечание.** Группу  $(R^*, \cdot)$  называют **группой обратимых элементов кольца**.

**Пример 3.1.7.** Множество  $\mathbb{Z}/n\mathbb{Z}$  является кольцом относительно обычных операций. Мы знаем, что его мультипликативная группа  $\mathbb{Z}/n\mathbb{Z}^*$  состоит из всех вычетов, взаимно простых с  $n$ .

Заметим, что если  $n$  не простое, то в  $\mathbb{Z}/n\mathbb{Z}$  есть вычеты, которые дают в произведении ноль. При этом легко проверить, что эти вычеты не обратимы. Давайте определим их.

**Определение 3.1.8.** Будем говорить, что ненулевой элемент  $x \in R$  является **делителем нуля**, если существует такой ненулевой  $y \in R$ , что  $x \cdot y = 0$ .

Делители нуля встречаются очень часто и мешают обратимости элементов, так как имеется следующая теорема.

**Утверждение 3.1.9.** Обратимый элемент  $x \in R$  никогда не является делителем нуля.

Позже нам понадобятся кольца без делителей нуля.

**Определение 3.1.10.** Кольцо, в котором выполняются R1–R5 называется **областью целостности**, если в нем нет делителей нуля.

**Пример 3.1.11.** Кольцо целых чисел является областью целостности.

**Пример 3.1.12.** Кольцо  $\mathbb{Z}/6\mathbb{Z}$  не является целостным кольцом, так как  $2 \cdot 3 \equiv 0 \pmod{6}$ .

Дальше мы разберем две конструкции, которые достаточно естественно возникают над кольцами и сами при этом являются кольцами.

### 3.1.3 Кольцо многочленов и кольцо функций

Начнем с более простого и понятного случая и ответим на вопрос: что такое многочлен над произвольным кольцом?

Везде ниже под  $R$  мы будем подразумевать коммутативное кольцо с единицей.

При вспоминании о многочленах у вас может возникнуть представление параболы или линейной функции. Это действительно графики многочленов над вещественными числами. Но имеют они смысл только в связи с тем, что  $\mathbb{R}$  — это поле характеристики ноль (что это такое, мы обсудим позже). В более общем же случае говорить о многочленах как о графиках (как мы делаем с функциями) нельзя, так что мы найдем к ним другой подход.

**Определение 3.1.13.** Будем называть **кольцом многочленов**  $R[x]$  над кольцом  $R$  множество последовательностей  $\{c_i\}_{i=0}^{\infty}$  коэффициентов из  $R$ , в которых только конечное количество  $c_i$  отлично от нуля и между которыми введены две операции:

$$\begin{aligned}\{a_i\}_{i=0}^{\infty} + \{b_i\}_{i=0}^{\infty} &\stackrel{\text{def}}{=} \{a_i + b_i\}_{i=0}^{\infty}, \\ \{a_i\}_{i=0}^{\infty} \cdot \{b_i\}_{i=0}^{\infty} &\stackrel{\text{def}}{=} \left\{ \sum_{k=0}^i a_{i-k} b_k \right\}_{i=0}^{\infty}.\end{aligned}$$

**Замечание.** Элементы кольца многочленов мы обычно записываем не через последовательность коэффициентов, а так:

$$f(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_n x^n.$$

Суть этого распределения раскрывается в следующей теореме.

**Теорема 3.1.14.**  $R[x]$  является ассоциативным коммутативным кольцом с единицей.

Одной из важных характеристик многочлена является его степень.

**Определение 3.1.15.** Степенью многочлена  $f \in R[x]$  будем называть максимальный номер его коэффициента, отличного от нуля. Обозначать будем степень через  $\deg f$ .

**Утверждение 3.1.16** (логарифмическое свойство степени многочлена). Если  $R$  является областью целостности, то для любых двух многочленов  $f, g$  не равных тождественно нулю верно

$$\deg(fg) = \deg f + \deg g.$$

Теперь скажем пару слов про другую конструкцию.

**Определение 3.1.17.** Пусть дано произвольное множество  $X$ . **Кольцом функций из  $X$  в  $R$**  называется множество всех функций из  $X$  в  $R$ , то есть  $R^X$ , с введенными покоординатными операциями:

$$(f + g)(x) \stackrel{\text{def}}{=} f(x) + g(x), \quad (f \cdot g)(x) \stackrel{\text{def}}{=} f(x) \cdot g(x).$$

И как в случае с кольцом многочленов имеет место теорема.

**Теорема 3.1.18.**  $R^X$  с введенными операциями образует кольцо.

Отметим, что кольцо функций почти всегда не является целостным кольцом. Почему? Дело в том, что в силу поточечного умножения мы можем рассматривать функции, которые не равны нулю только в одной точке, из произведения всегда рано нулевой функции, если изначальные функции различны.

### 3.1.4 Нильпотенты, идемпотенты

Сейчас мы с вами обсудим два класса элементов в кольце, которые возникают при отсутствии у кольца свойств, к которым мы привыкли в вещественных числах: обратимость всех ненулевых чисел.

**Определение 3.1.19.** Ненулевой элемент кольца называется **нильпотентным**, если существует степень  $k$ , при возведении в которую мы получаем ноль.

**Пример 3.1.20.** Квадратная матрица с нулями на диагонали и под ней является всегда нильпотентной матрицей в  $\text{Mat}(n, \mathbb{R})$ .

**Пример 3.1.21.** Вычет 2 является нильпотентным в  $\mathbb{Z}/8\mathbb{Z}$ .

**Утверждение 3.1.22.** Любой нильпотентный элемент является делителем нуля.

Еще бывает интересен следующий элемент.

**Определение 3.1.23.** Элемент  $x$  кольца называется **идемпотентом**, если  $x^2 = x$ .

**Пример 3.1.24.** В любом кольце 0 и 1 являются идемпотентами.

**Пример 3.1.25.** В кольце матриц есть матрицы, которые задают ортогональное проектирование на некоторое подпространство в  $n$ -мерном пространстве. Такие матрицы называются **проекторами** и являются идемпотентами.

### 3.1.5 Подкольцо и прямая сумма колец

Теперь обсудим два небольших сюжета, которые очень сильно похожи на аналогичные конструкции из теории групп, хотя наличие двух операций привносит свои изменения в них тоже.

**Определение 3.1.26.** Будем говорить, что  $T \subseteq R$  является **подкольцом**, если оно образует кольцо вместе с операциями, ограниченными с кольца  $R$ .

**Пример 3.1.27.** Множество  $n\mathbb{Z}$  является подкольцом в  $\mathbb{Z}$ .

Как видно из этого примера, свойство наличия единицы может исчезать при переходе от кольца к его подкольцу, хотя сложение все еще будет абелевой групповой операцией, что следует просто из определения.

**Пример 3.1.28.** Любое кольцо  $R$  является подкольцом в  $R[x]$ .

Позже мы увидим, что интересны не просто подкольца, а те из них, которые обладают интересным свойством втягиваемости. Мы их назовем идеалами и будем смотреть на них, как на аналог нормальных подгрупп в теории групп.

Последняя конструкция на сегодня — аналог прямого произведения групп.

**Определение 3.1.29.** Будем подразумевать под **прямой суммой кольц**  $R_1 \oplus R_2$  их декартово произведение с покоординатными операциями сложения и умножения.

**Замечание.** В прямой сумме кольц всегда есть делители нуля: достаточно рассмотреть два элемента  $(0_{R_1}, 1_{R_2})$  и  $(1_{R_1}, 0_{R_2})$ .

## Домашнее задание

**Задача 3.1.1.** Докажите, что в любом кольце: а)  $a \cdot 0 = 0 \cdot a = 0$ ; б)  $(-1) \cdot (-1) = 1$ ;  
в)  $a \cdot (b - c) = a \cdot b - a \cdot c$ .

**Задача 3.1.2.** а) Докажите, что в коммутативном кольце  $a^2 - b^2 = (a - b)(a + b)$ . б) Приведите пример кольца, где это равенство будет неверным.

**Задача 3.1.3.** Докажите, что в любом кольце если элемент  $a$  не является делителем нуля, то из равенства  $ax = ay$  следует, что  $x = y$ .

**Задача 3.1.4.** а) Доказать, что любой элемент кольца  $\mathbb{Z}/143\mathbb{Z}$  является суммой двух делителей нуля. б) Найти представление в виде суммы двух делителей нуля для элемента 19.

**Задача 3.1.5.** В коммутативном кольце  $R$  уравнение  $x^2 = 2$  имеет по крайней мере 3 различных решения. Докажите, что в  $R$  есть делители нуля.

**Задача 3.1.6.** а) Сколько обратимых элементов в кольце  $\mathbb{Z}/493\mathbb{Z}$ ? б) Сколько нильпотентных элементов в кольце  $\mathbb{Z}/5100\mathbb{Z}$ ?

**Задача 3.1.7.** Докажите, что в любом кольце с 1 из нильпотентности  $a$  следует обратимость  $1 - a$ .

**Задача 3.1.8.** а) Докажите, что множество нильпотентных элементов коммутативного кольца вместе с нулем образуют подкольцо. б) Приведите пример некоммутативного кольца, где не будет выполняться предыдущий пункт.

**Задача 3.1.9.** Указать пример кольца  $R_2$  и его подкольца  $R_1$ , таких что  $1_{R_1} \neq 1_{R_2}$ .

**Задача 3.1.10.** а) В каких кольцах произведения принимают одно и то же значение? б) Постройте кольцо из 21 элемента, в котором произведения принимают ровно три различных значения.

**Бонусная задача.** Найдите все обратимые элементы в гауссовых кольцах:

$$\text{а)} \mathbb{Z}[i] \stackrel{\text{def}}{=} \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\},$$

$$\text{б)} \mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b\omega : a, b \in \mathbb{Z}, \omega^2 + \omega + 1 = 0\}.$$

## Рекомендаемая литература

- [1] Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Раздел 7.
- [2] Городенцев А. Л. — Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 2, §2, 3, 4; глава 3, §9.
- [3] Винберг Э. Б. — Курс Алгебры — 2-е изд., стереотип. — М.: МЦНМО, 2013. — Глава 1, §3, 5, 8; глава 3, §1.

## 3.2 Поля, идеалы и многочлены. Часть 1

В этом и следующем разделе мы запустим параллельно два процесса: во-первых, мы познакомимся ближе с частным случаем кольца — полем, во-вторых, мы научимся строить гомоморфизмы колец (аналоги гомоморфизмов групп). Вся эта теория будет упираться в теорию конечных полей, где мы воспользуемся всем, что изучим сейчас.

**Ключевые слова:** тело, поле, кватернионы, простое подполе, характеристика, гомоморфизмы колец, ядра гомоморфизмов, идеалы, полиномиальная функция, гомоморфизм эвалюации, определитель Вандермонда, интерполяционный многочлен Лагранжа, факторкольцо, главный идеал, кольцо главных идеалов.

### 3.2.1 Поле: определение, характеристика, простое подполе

Начнем с самого простого — с определения.

**Определение 3.2.1.** Будем называть кольцо **телом**, если  $0 \neq 1$  и  $R^* = R \setminus \{0\}$ . Если при этом кольцо коммутативно, то оно называется **полем**.

**Пример 3.2.2.** Из свойств, которые мы разобрали ранее, понятно, что  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  — это поля.

**Пример 3.2.3.** Отметим еще поле  $\mathbb{Z}/p\mathbb{Z}$  (обратимость вычетов мы доказывали, когда рассматривали мультипликативную группу вычетов). При этом если бы  $p$  было не простым, то и кольцо вычетов не было бы полем как минимум, из-за того, что содержало бы делители нуля.

**Пример 3.2.4.** А вот  $\mathbb{Z}$  уже не является полем, так как в нем обратимы только  $\pm 1$ .

**Пример 3.2.5.** А кватернионы  $\mathbb{H}$  будут являться уже телом, а не полем. Они определяются как формальные комбинации четырех чисел:

$$\forall \lambda \in \mathbb{H} \exists \lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}: \lambda = \lambda_0 \cdot 1 + \lambda_1 \cdot i + \lambda_2 \cdot j + \lambda_3 \cdot k,$$

где формальные величины  $i, j, k$  определены в примере 2.5.4.

Приступим к изучению свойств поля.

Для начала заметим, что так как в поле всегда есть единица и сложение, то мы можем получить такой элемент

$$n \cdot 1 \stackrel{\text{def}}{=} 1 + \dots + 1,$$

где количество слагаемых в сумме равно  $n$  (слагаемые вида  $n \cdot 1$  называются *кратными единицами*).

Предположим, что поле конечно. Тогда в какой-то момент единицы начнут повторяться, а значит у этого элемента есть порядок по сложению, то есть существует такое  $n$ , что  $n \cdot 1 = 0$ . Можно показать, что в таком случае в силу отсутствия делителей нуля мы обязаны получить простой порядок у единицы по сложению. Также легко заметить, что это множество замкнуто не только относительно сложения, но и относительно умножения. Следовательно, мы имеем следующую теорему.

**Теорема 3.2.6.** Если  $\mathbb{F}$  — конечное поле, то множество кратных единиц образуют поле относительно тех же сложений и умножения, что и в самом поле. Притом порядок этого под поля простой.

**Замечание.** В силу последней теоремы множество кратных единиц в конечном поле называется **простым подполем**. А порядок такого под поля называется **характеристикой** и обозначается через  $\text{char } \mathbb{F}$ .

**Замечание.** Если подполе кратных единиц бесконечно, считают, что  $\text{char } \mathbb{F} = 0$ . Если поле  $\mathbb{F}$  бесконечно, но при этом множество кратных единиц в нем конечно, то видно, что мы опять приходим к первому случаю простого под поля.

**Замечание.** Можно заметить, что множество кратных единиц определено в любом кольце с единицей. Оно и там будет замкнуто относительно умножения и вычитания, а значит, будет являться подкольцом. Следовательно, корректно определена характеристика любого кольца с единицей как порядок подкольца кратных единицы.

**Пример 3.2.7.** Характеристика полей  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  равна нулю. А  $\text{char } \mathbb{Z}_p = p$ .

Основная разница между полями характеристики ноль и полями положительной характеристики заключается в том, что в одном случае есть биективное соответствие между полиномиальными функциями и многочленами, а в другом случае это соответствие не биективно. В следующем подразделе мы определим, что такое гомоморфизм колец и покажем на его примере, чем отличаются полиномиальные функции и полиномы.

### 3.2.2 Гомоморфизмы колец

Как и в случае с группами, мы можем рассматривать специальные отображения между кольцами, которые нам будут интересны.

**Определение 3.2.8.** Пусть даны два кольца  $R_1$  и  $R_2$ . Тогда отображение  $\varphi: R_1 \rightarrow R_2$  будет называться **гомоморфизмом колец**, если выполнено свойство:

$$\forall a, b \in R_1: \varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b).$$

**Замечание.** Формально говоря, выше надо указать сумму и произведение разными знаками в разных кольцах, так как они могут спокойно иметь разную природу. Однако это мелочи и, я надеюсь, что читатель сможет понять, что слева от равенства использована одна операция, а справа — другая.

**Замечание.** Как покажут примеры дальше, образ единицы не всегда является единицей. Из-за этого часто к определению добавляют и свойство сохранения единицы. В большинстве колец с хорошими свойствами это свойство будет автоматически выполнено, из-за этого мы в определении добавлять это свойство не будем.

**Замечание.** Как и в случае групп, тут мы можем использовать понятия изоморфизма, автоморфизма, эндоморфизма с соответствующим подтекстом.

**Пример 3.2.9.** Между любыми двумя кольцами существует *тривиальный гомоморфизм*, которые отображает все элементы кольца  $R_1$  в  $0_{R_2}$ .

**Пример 3.2.10.** Рассмотрим эндоморфизмы кольца  $\mathbb{Z}$ . Каждый из эндоморфизмов определяется образом единицы. Пусть тогда  $\varphi(1) = \lambda \cdot 1$ . Следовательно, мы можем записать такие равенства

$$\varphi(1) = \varphi(1) \cdot \varphi(1) \Rightarrow \lambda = \lambda^2 \Rightarrow \lambda = 0 \vee \lambda = 1.$$

В одном случае мы получаем тривиальный гомоморфизм, а во втором случае получаем тривиальный эндоморфизм. Отсюда мы можем заключить, что в группе целых чисел нет нетривиальных эндоморфизмов.

Покажем, что при любом гомоморфизме ноль сохраняется, а единица нет. Более того, в кольце, в которое строится гомоморфизм, единицы может просто не быть.

**Утверждение 3.2.11.** При гомоморфизме  $\varphi: R_1 \rightarrow R_2$  выполнено, что  $\varphi(0_{R_1}) = 0_{R_2}$ .

*Доказательство.* Мы знаем свойства нейтрального элемента и гомоморфизма, так что

$$\varphi(0_{R_1}) = \varphi(0_{R_1} + 0_{R_1}) = \varphi(0_{R_1}) + \varphi(0_{R_1}) \Rightarrow \varphi(0_{R_1}) = 0_{R_2}.$$

■

**Пример 3.2.12.** Единица действительно может переходить не только в единицу. Мы уже могли это увидеть у тривиального гомоморфизма. А теперь рассмотрим еще парочку:

$$\varphi: n\mathbb{Z} \rightarrow n\mathbb{Z}, x \mapsto x,$$

в этом отображении у вас нет единицы нигде.

**Пример 3.2.13.** Бывают также случаи, когда в  $R_1$  есть единица, но в  $R_2$  нет единицы:

$$\varphi: \mathbb{Z} \rightarrow \mathbb{Z} \oplus 2\mathbb{Z}, z \mapsto (z, 0).$$

Если заменить в последнем отображении  $2\mathbb{Z}$  на  $\mathbb{Z}_2$ , то единица в образе появится, но при этом образ  $1_{R_1}$  все еще не будет ей равен.

**Пример 3.2.14.** Можно еще рассмотреть кольца матриц, и вложить в них как-нибудь другие матрицы или просто кольцо коэффициентов:

$$\varphi: \mathbb{Z} \rightarrow \text{Mat}(2, \mathbb{Z}), z \mapsto \begin{pmatrix} z & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow 1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq E.$$

### 3.2.3 Ядра гомоморфизмов колец и идеалы

Как и в случае гомоморфизма групп, тут нам будут интересны ядра гомоморфизма колец. Притом если в теории групп мы сначала вводили нормальные подгруппы, а потом узнавали, что они не отличимы от ядер гомоморфизмов, то тут мы поступим иначе: мы сначала поймем, какими свойствами обладает ядро гомоморфизма, а потом уже определим отдельно объект, который будет являться аналогом ядра. Приступим.

**Определение 3.2.15.** Ядром гомоморфизма  $\varphi$  называется

$$\text{Ker } \varphi \stackrel{\text{def}}{=} \{x \in R_1 : \varphi(x) = 0_{R_2}\}.$$

Во-первых, заметим, что ядро замкнуто относительно взятия суммы и произведения, а также взятия обратного по сложению, так что это подкольцо в  $R_1$ . Во-вторых, мы знаем, что при умножении на ноль любой элемент кольца дает ноль, так что

$$\forall x \in R_1 \forall i \in \text{Ker } \varphi: \varphi(x \cdot i) = \varphi(x) \cdot \varphi(i) = \varphi(x) \cdot 0_{R_2} = 0_{R_2} \Rightarrow x \cdot i \in \text{Ker } \varphi.$$

Это свойство называется *левой втягиваемостью*. Бывает также и *правая втягиваемость*, которая для ядра выполняется. И эти свойства настолько важны, что мы дадим отдельно еще следующее определение.

**Определение 3.2.16.** Если у подкольца  $I \subseteq R$  есть свойство левой и правой втягиваемостей, то это подкольцо называется *двусторонним идеалом*.

**Замечание.** Если в подкольце есть свойство правой или левой втягиваемостей, то говорят, что это соответственно *левый идеал* или *правый идеал*. Однако нам такие идеалы не встретятся, кроме учебных случаев, а в коммутативном кольце между ними вообще нет разницы.

**Замечание.** Идеал в кольце мы будем обозначать так:  $I \triangleleft R$ .

**Теорема 3.2.17.** Если  $\varphi: R_1 \rightarrow R_2$  является гомоморфизмом, то  $\text{Ker } \varphi \triangleleft R_1$ .

Как следствие из последней теоремы, мы можем строить гомоморфизмы и смотреть, какие элементы остаются в ядре и таким образом получать идеалы.

**Пример 3.2.18.** Мы уже знакомы с многочленами  $R[x]$ . Однако мы привыкли смотреть на них не как на коэффициенты (какими они являются в текущих дефинициях), а как на графики. Чтобы понять, в чем связь между ними, мы введем *гомоморфизм эвалюации*:

$$\forall \alpha \in R: \text{ev}_\alpha: R[x] \rightarrow R, \text{ev}_\alpha(f) = f_0 + f_1\alpha + f_2\alpha^2 + \dots + f_n\alpha^n.$$

При этом видно, что ядром гомоморфизма эвалюации является множество полиномов, у которых *корнем является число  $\alpha$*  (в реальности все немного наоборот, мы по определению считаем, что корень многочлена — это такой  $\alpha$ , что  $\text{ev}_\alpha(f) = 0_R$ ).

Используя гомоморфизм эвалюации, мы можем сопоставить каждому многочлену *полиномиальную функцию*, с которой этот самый многочлен часто путают:

$$\forall f \in R[x] \tilde{f}: R \rightarrow R, \tilde{f}(\alpha) \stackrel{\text{def}}{=} \text{ev}_\alpha(f) = f_0 + f_1\alpha + f_2\alpha^2 + \dots + f_n\alpha^n.$$

С одной стороны такое сопоставление понятно и дает нам привычную функцию, а с другой стороны, хочется понять, в чем же разница между полиномами и полиномиальными функциями, кроме определения? Мы дадим позже ответ на этот вопрос.

Можно сразу заметить, что если кольцо  $R$  конечно, то и полиномиальных функций конечно (ровно  $|R|^{|R|}$ ). А полиномов бесконечно, так что очевидно, что в общем случае у нас сопоставление полиномам полиномиальных функций не будет биективно.

**Пример 3.2.19.** Если рассмотрим  $\mathbb{F}_2[x]$ , то есть кольцо многочленов над конечным полем  $\mathbb{F}_2$ , то уже видно, что некоторым полиномам сопоставляются одинаковые полиномиальные функции:

$$f = x^2 + x + 1, g = 1 \Rightarrow \tilde{f} = \tilde{g}.$$

При этом в школе мы привыкли, что по двум точкам в общем положении можно построить однозначно линейную функцию, а по трем точкам — параболу. Так, в какой момент появляется эта однозначность? Оказывается, что для нее достаточно иметь поле нулевой характеристики.

**Теорема 3.2.20.** Если  $\mathbb{F}$  — это поле нулевой характеристики, то сопоставление  $f \leftrightarrow \tilde{f}$  биективно.

**Доказательство.** Сюръективность отображения очевидна в силу того, что мы определяли полиномиальные функции через полиномы, так что нужно показать, что такое сопоставление инъективно. Понятно, что для этого достаточно показать, что нулевой полиномиальной функции  $\tilde{h} \equiv 0$  соответствует только нулевой полином (тут на самом деле есть еще один спрятанный гомоморфизм, но мы про него отдельно не будем говорить).

Предположим, что у нас имеется полином  $h$ , у которого полиномиальная функция тривиальная. При этом пусть  $\deg h = n - 1$ , тогда рассмотрим  $n$  различных чисел в поле  $\mathbb{F}$  (можно взять различные кратные единицы). Для всех них мы получим нулевое значение полиномиальной функции или систему:

$$\begin{cases} h_0 + h_1 \cdot 1 + \dots + h_{n-1} \cdot 1^{n-1} = 0, \\ h_0 + h_1 \cdot 2 + \dots + h_{n-1} \cdot 2^{n-1} = 0, \\ \dots \\ h_0 + h_1 \cdot n + \dots + h_{n-1} \cdot n^{n-1} = 0. \end{cases}$$

Как мы знаем из линейной алгебры, такая система имеет единственное решение, которое легко угадывается по ней. Оно тривиально. А значит, и сопоставление биективно. ■

**Замечание.** Отметим еще очень интересный факт, что суть биективности нашего сопоставления заключается в нетривиальности *определителя Вандермонда*. Также мы могли подставлять в определитель Вандермонда не кратные единицы, а произвольные элементы поля, так что это же утверждение верно в любом бесконечном поле.

**Замечание.** Надо отметить, что в общем случае  $R^R$  намного больше, чем полиномиальных функций, однако с помощью *интерполяционного многочлена Лагранжа* можно показать, что по  $n$  значениям в  $n$  различных точках можно построить единственный многочлен степени не выше  $n - 1$ , который удовлетворяет этим условиям ( $R$  конечно в этом случае должно быть полем).

Покажем, какие еще бывают примеры идеалов.

**Пример 3.2.21.** Докажем, что множество нильпотентных элементов  $\text{Nil}$  коммутативного кольца вместе с нулем образует идеал. В домашней задаче уже было показано, что это подмножество образует кольцо. Осталось показать, что выполнено свойство втягиваемости:

$$\forall i \in \text{Nil} \quad \forall x \in R: \exists k \in \mathbb{N}: i^k = 0 \Rightarrow (ix)^k = i^k \cdot x^k = 0 \cdot x^k = 0 \Rightarrow ix \in \text{Nil}.$$

Еще как и в случае с нормальными группами, мы можем пересекать идеалы и получать новые идеалы.

**Пример 3.2.22.** Пусть  $I_1, I_2 \triangleleft R$ . Тогда пересечение этих идеалов тоже идеал, так как оно замкнуто относительно вычитания и произведения, а также удовлетворяет свойству втягиваемости. Покажем последнее. По определению

$$\forall i \in I_1 \cap I_2 \quad \forall x \in R: i \in I_1 \triangleleft R \Rightarrow i \cdot x, x \cdot i \in I_1; i \in I_2 \triangleleft R \Rightarrow i \cdot x, x \cdot i \in I_2 \Rightarrow i \cdot x, x \cdot i \in I_1 \cap I_2.$$

Как видите, выкладки насколько громоздки, настолько и просты, отчего и ненужны, так что для остальных «замкнутостей» мы доказательства не будем приводить.

### 3.2.4 Факторкольца

Имея подгруппу в группе, мы строили разбиение ее на классы смежности. Тут мы тоже определим разбиение засчет двустороннего идеала внутри кольца. Для этого назовем *вычетом по модулю идеала*  $I \triangleleft R$  следующее множество

$$\forall x \in R: [x]_I = x + I.$$

**Пример 3.2.23.** Если мы рассмотрим  $n\mathbb{Z} \triangleleft \mathbb{Z}$ , то вычетом будет являться множество целых чисел, имеющих одинаковый остаток при делении на  $n$ .

**Замечание.**  $R/I$  обозначают множество вычетов по модулю идеала  $I$ .

**Определение 3.2.24.** Имея  $I \triangleleft R$ , будем называть **факторкольцом или кольцом вычетов** тройку из  $R/I$  и двух операций, определенных ниже:

$$\forall [x_1]_I, [x_2]_I \in R/I: [x_1]_I + [x_2]_I = [x_1 + x_2]_I, \quad [x_1]_I \cdot [x_2]_I = [x_1 \cdot x_2]_I.$$

**Утверждение 3.2.25.** Факторкольцо является кольцом. Если  $R$  обладало какими-то свойствами (коммутативность, существование единицы), то и  $R/I$  тоже ими обладает.

**Пример 3.2.26.** Многочлены  $x + 1$  и  $x^3 + x$  принадлежат одному классу вычетов по модулю идеала  $I$  кольца  $\mathbb{Q}[x]$  многочленов с рациональными коэффициентами. Докажем, что многочлены  $x^3 - x^2$  и  $x^6 - x^2$  также принадлежат одному классу вычетов по модулю идеала  $I$ .

Для этого скажем, что  $x, y$  образуют один класс вычетов тогда и только тогда, когда их разница лежит в  $I$ , следовательно, из условия:

$$(x^3 + x) - (x + 1) = x^3 - 1 \in I.$$

Пользуемся свойством втягиваемости и получаем искомое:

$$[x^3 - x^2]_I = [x^6 - x^2]_I \Leftrightarrow (x^6 - x^2) - (x^3 - x^2) = x^3(x^3 - 1) \in I.$$

Идеалы можно порождать каким-нибудь множеством  $S$ . В таких случаях каждый элемент идеала представляет из себя конечную линейную комбинацию элементов из  $S$  с коэффициентами из коммутативного кольца  $R$ :

$$I = \left\{ \sum_{i=1}^n c_i x_i : x_i \in S, c_i \in R, n \in \mathbb{N} \right\}.$$

**Пример 3.2.27.** Двусторонний идеал  $I$  кольца  $R$  порожден всеми элементами вида  $x^2$ ,  $x \in R$ . Докажем, что кольцо классов вычетов  $R/I$  антисимметрично:

$$\forall a, b \in R/I: ab = -ba.$$

Для этого заметим, что в идеале есть элементы

$$x^2, y^2, (x+y)^2 \in I.$$

Их линейная комбинация будет лежать в идеале:

$$(x+y)^2 - x^2 - y^2 = xy + yx \in I.$$

Но это значит, что

$$[xy + yx]_I = [0]_I \Leftrightarrow [x]_I[y]_I = -[y]_I[x]_I.$$

**Пример 3.2.28.** Найти порядок группы обратимых элементов кольца  $\mathbb{F}_7[x]/(x^2 + 3x - 5)$ .

Заметим, что  $\mathbb{F}_7$  — это поле. Поэтому все коэффициенты обратимы по умножению. Дальше отметим, что, так как мы факторизуем по квадратичному выражению, у каждого вычета есть единственный представитель вида  $ax + b$ . Нам необходимо понять, когда такой представитель обратим.

Можно заметить, что в этом факторкольце каждый вычет обратим или является делителем нуля. Следовательно, нам нужно понять, какие вычеты являются делителями нуля. Для этого заметим, что

$$x^2 + 3x - 5 = x^2 + 3x + 2 = (x+1)(x+2).$$

Так как  $\mathbb{F}_7$  — поле, мы получаем, что выражение  $ax + b$  является делителем нуля тогда и только тогда, когда оно кратно либо  $x + 1$ , либо  $x + 2$ . Таких многочленов ровно по 6 штук и еще есть нулевой вычет, так что из 49 вычетов обратимым будет только 36.

Есть особенные идеалы, которые будут выделяться наряду с другими. Одним из таких особенных идеалов является следующий.

**Определение 3.2.29.** Идеал называется **главным**, если он порожден одним элементом кольца. Кольцо, в котором все идеалы главные, называется **кольцом главных идеалов**.

**Пример 3.2.30.** Является ли кольцом главных идеалов  $\mathbb{Z}_{72}$ ? В любом идеале  $I \subseteq \mathbb{Z}_{72}$  мы можем найти минимальный элемент. Этот элемент будет порождать весь идеал, а значит,  $I$  — главный идеал и кольцо является кольцом главных идеалов.

Кольцо главных идеалов интересно тем, что все идеалы в нем легко описать. Из-за этого можно найти все факторкольца выбранного кольца, а эти факторы нужно для классификаций и прочих интересных утверждений алгебры и близких к ней областей математики. Покажем, как можно доказывать свойства в кольце главных идеалов и какие эти свойства могут быть.

**Утверждение 3.2.31.** Если  $R$  — кольцо главных идеалов, то для любой цепочки идеалов  $\{I_i\}_{i=1}^{\infty}$ ,  $I_i \subseteq I_{i+1}$ , верно, что существует такое число  $N \in \mathbb{N}$ , что для любого  $n \geq N$ ,  $I_n = I_N$ .

**Доказательство.** Объединение всех идеалов  $J = \bigcup_{i=1}^{\infty} I_i$  будет тоже идеалом. Так как  $R$  — кольцо главных идеалов,  $J$  порождается каким-то элементом  $x \in I_N$ . Тогда

$$\forall n \geq N: J = (x) \subseteq I_N \subseteq I_n \subseteq \bigcup_{i=1}^{\infty} I_i = J \Rightarrow J = I_N = I_n.$$

■

В следующем разделе мы продолжим знакомиться с гомоморфизмами и полями. А через раз мы познакомимся с евклидовыми кольцами, которые будут являться кольцами главных идеалов. И идеалы в этих кольцах будут сильно связаны с теорией чисел, так же сильно, как и теория конечно-порожденных абелевых групп во второй главе.

## Домашнее задание

**Задача 3.2.1.** Обозначим через  $\mathbb{Q}[i]$  множество комплексных чисел с рациональными мнимой и вещественной частями. Будет ли это множество полем относительно умножения и сложения комплексных чисел?

**Задача 3.2.2.** а) Существует ли нетривиальный гомоморфизм из  $\mathbb{Z}_n$  в  $\mathbb{Z}$ ? б) Можно ли найти пример двух колец с единицами  $R_1$  и  $R_2$ , таких что между ними существует нетривиальный гомоморфизм  $\varphi: R_1 \rightarrow R_2$ , и при этом  $\text{char } R_1 > 0$ ,  $\text{char } R_2 = 0$ ?

**Задача 3.2.3.** Многочлен  $f(x)$  над полем  $\mathbb{F}_5$  степени 2 принимает значение 1 в точке 1, значение 2 в точке 3 и значение 3 в точке 4. Найти  $f(x)$ .

**Задача 3.2.4.** Найдите все идеалы в кольце  $\mathbb{F}_2^{\oplus n}$  ( $n$ -ая прямая сумма полей  $\mathbb{F}_2$ ).

**Задача 3.2.5.** Сумма идеалов  $I_1 + I_2$  — это идеал, порожденный всеми суммами элементов из идеалов  $I_1, I_2$ . Аналогично, произведение идеалов  $I_1 I_2$  — это идеал, порожденный всеми произведениями элементов из  $I_1, I_2$ . Пусть  $I_1$  порожден в  $\mathbb{Q}[x]$  многочленом  $x^2 - x$ , а  $I_2$  порожден многочленом  $x^2 + x$ . Найдите  $I_1 + I_2, I_1 I_2, I_1 \cap I_2$ .

**Задача 3.2.6.** Найдите порядок элемента  $t^8$  в мультиликативной группе кольца  $\mathbb{F}_7[t]/(t^6 - 3)$ .

**Задача 3.2.7.** Найти порядок группы обратимых элементов кольца  $\mathbb{F}_3[x]/(x^2 + x + 1)$ .

**Задача 3.2.8.** Решите уравнение  $(t + 1)^2 x = t^2$  в кольце вычетов  $\mathbb{Q}[t]/(t^3 + 3t + 1)$ .

**Задача 3.2.9.** Будет ли кольцо  $R$  кольцом главных идеалов: а)  $R = \mathbb{Z}[x]$ ; б)  $R = \mathbb{F}[x, y]$ ?

**Задача 3.2.10.** Докажите, что  $\mathbb{Z}$  — это кольцо главных идеалов. Найдите в этом кольце все максимальные идеалы, то есть идеалы, которые относительно включения не содержатся ни в каком другом идеале, не совпадающем со всем кольцом.

**Бонусная задача.** Есть ли среди факторколец кольца  $\mathbb{Z}[i]$  поле а) характеристики 2; б) характеристики 3? в) Если да, то сколько элементов может быть в этом поле?

## Рекомендуемая литература

- [1] Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Раздел 7, 9.
- [2] Городенцев А. Л. — Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 2, §3, 6.
- [3] Винберг Э. Б. — Курс Алгебры — 2-е изд., стереотип. — М.: МЦНМО, 2013. — Глава 1, §3, 5; глава 3, §1; глава 9, §2.

## 3.3 Поля, идеалы и многочлены. Часть 2

Сейчас мы свяжем поля и идеалы через важную теорему о максимальном идеале. После нам предстоит немного поговорить о кольце многочленов. Так как мы еще не обсудили евклидовы кольца и конечные поля, мы не сможем сию же секунду применить все знания, которые обсудим в этом разделе. Однако на протяжении следующих двух занятий понимание сегодняшних тем будет дополняться и мы увидим, как некоторые простые понятия нарастают нетривиальными утверждениями и позволяют лучше нам понять, как же устроены как конечные поля, так и их бесконечные аналоги.

В конце раздела добавлен подраздел о поле частных, который важен для общей теории колец и полей, однако в нашем курсе он дальше сильно не раскрывается, из-за чего он и заслужил такое унизительное место в этом разделе. Для тех же, кто хочет углубить свое понимание этой конструкции, советуем ознакомиться с леммой Гаусса.

**Ключевые слова:** область целостности, деление с остатком, кольцо главных идеалов, корень многочлена, цикличность мультиплекативной группы конечного поля, максимальный идеал, теорема о максимальном идеале, поле частных, поле рациональных функций, расширение поля, алгебраический элемент, трансцендентный элемент, минимальный многочлен, алгебраически замкнутое поле.

### 3.3.1 Делимость в кольце многочленов и главные идеалы

Начнем мы с многочленов и покажем, как они сильно похожи на кольцо целых чисел. Впоследствии это будут два основных примера евклидовых колец.

**Утверждение 3.3.1.** Пусть  $R$  — область целостности. Тогда в  $R[x]$  нет делителей нуля.

**Доказательство.** Пусть есть два многочлена  $f = f_0 + \dots + f_n x^n$  и  $g = g_0 + \dots + g_m x^m$ , которые не равны нулю. Найдем их произведение

$$f \cdot g = (f_0 g_0) + (f_1 g_0 + f_0 g_1)x + \dots + (f_n g_m)x^{n+m}.$$

Мы всегда может выбрать так  $n$  и  $m$ , чтобы коэффициенты с соответствующими индексами были ненулевыми. Тогда произведение  $f_n \cdot g_m \neq 0$ , так как в  $R$  нет делителей нуля, откуда мы получаем, что степень  $f \cdot g$  не менее  $n + m$ . Следовательно, если  $\deg f > 0$  или  $\deg g > 0$ , то произведение ненулевое.

Нам остается рассмотреть случай констант, но он очевиден: произведение ненулевых констант не равно нулю, так как коэффициенты из области целостности. ■

**Следствие 3.3.2.**  $R[x]$  — это область целостности.

Уже видим, что как и целые числа, многочлены над полем образуют область целостности. Но нам нужно большее: необходимо научиться делить многочлены с остатком.

**Утверждение 3.3.3.** Пусть  $\mathbb{F}$  — поле. Тогда для любых двух многочленов  $f, g \in \mathbb{F}[x]$ ,  $g \neq 0$ , существуют единственныe два таких многочлена  $q, r \in \mathbb{F}[x]$ , что  $f = q \cdot g + r$  и либо  $r = 0$ , либо  $\deg r < \deg g$ .

*Доказательство.* Докажем с помощью метода математической индукции, используя в качестве параметра  $\deg g$ .

База индукции будет при  $\deg g = 0$ . В этом случае  $g$  — это ненулевая константа, а значит, обратимый элемент поля. Следовательно, мы можем написать, что

$$f = \left( \frac{f_0}{g_0} + \frac{f_1}{g_0}x + \dots + \frac{f_n}{g_0}x^n \right) \cdot g_0 + 0.$$

Единственность очевидно следует из явных формул выше.

Предположим, что для всех многочленов  $g$  степени  $k$  и меньше мы доказали существование и единственность частного и остатка. Тогда покажем, что для  $\deg g = k + 1$  все будет верно.

Если степень многочлена  $f$  меньше степени многочлена  $g$ , то разложение очевидно (частное — ноль, а остаток — само  $f$ ). Пусть  $n = \deg f \geq k + 1$ . Запустим вторую индукцию по степени многочлена  $f$  и будем предполагать, что для всех многочленов меньшей степени мы все доказали. При таком допущении мы можем рассмотреть следующую разницу

$$f - g \cdot \frac{f_n}{g_{k+1}}x^{n-k-1} = f_2.$$

Степень многочлена  $f_2$  строго меньше, чем степень многочлена  $f$ , так что по предположению индукции мы можем единственным образом представить его в виде  $q_2 \cdot g + r$ . Остается провести простые преобразования

$$f - g \cdot \frac{f_n}{g_{k+1}}x^{n-k-1} = q_2 \cdot g + r \Leftrightarrow f = \left( \frac{f_n}{g_{k+1}}x^{n-k-1} + q_2 \right) \cdot g + r.$$

Из единственности  $q_2$  и  $r$  следует, что частное и остаток для  $f$  тоже единственны. ■

В следующем разделе мы покажем, что в общем случае эти рассуждения позволяют построить *обобщенный алгоритм Евклида для евклидовых колец*. Однако уже сейчас мы смогли понять, что в кольце многочленов над полем можно делить с остатком. Тут важно, что  $\mathbb{F}[x]$  — кольцо многочленов над полем, тут не хватит области целостности, так как мы хотим, чтобы можно было делить на старший коэффициент многочлена  $g$ .

**Пример 3.3.4.** Разделим многочлен  $x^4 - 4x^3 + 6x^2 - 3x + 1$  на  $x^2 - x + 1$ . Обозначим первый многочлен через  $f(x)$ , а второй — через  $g(x)$ . Тогда следуя алгоритму, изложенному в последнем доказательстве, мы можем разделить  $f(x)$  на  $g(x)$ :

$$f(x) = (x^2 - 3x + 2) \cdot g(x) + 2x - 1 = q(x) \cdot g(x) + r(x).$$

Вспомним, что такое главные идеалы. В коммутативном кольце с единицей главный идеал  $I = (a)$  будет иметь вид

$$I = (a) = Ra = \{ra : r \in R\}.$$

Если же мы сделаем шаг назад и посмотрим на некоммутативное кольцо с единицей, то главные идеалы там уже не будут так красиво выглядеть:

$$I = (a) = RaR = \left\{ \sum_{i=1}^n r_i \cdot a \cdot s_i : \forall i \in \overline{1, n} \quad r_i, s_i \in R, n \in \mathbb{N} \right\}.$$

**Замечание.** До конца части про кольца и поля мы будем считать, что рассматриваемое кольцо всегда коммутативно и содержит единицу.

Нам хочется, чтобы кольцо было кольцом главных идеалов. Для чего? Чтобы мы понимали, какие факторкольца мы можем из него получить, так как спектр идеалов значительно сокращается, если мы знаем, что они всегда главные. Покажем, что многочлены над полем образуют кольцо главных идеалов, что так же, как и предыдущие рассуждения, приближают это кольцо к кольцу целых чисел.

**Утверждение 3.3.5.** Пусть  $\mathbb{F}$  — поле. Тогда  $\mathbb{F}[x]$  — кольцо главных идеалов.

*Доказательство.* Мы можем делить с остатком в кольце многочленов над полем. Следовательно, в любом идеале  $I \triangleleft \mathbb{F}[x]$  многочлен минимальной степени обязан быть единственным (с точностью до умножения на ненулевую константу) и обязан делить любой другой многочлен. Отсюда следует, что он будет порождать весь идеал, а значит,  $I$  — главный идеал. В силу общности выбора  $I$  мы получаем, что  $\mathbb{F}[x]$  — кольцо главных идеалов. ■

**Следствие 3.3.6.** Пусть  $\mathbb{F}$  — поле, а  $I$  — идеал в  $\mathbb{F}[x]$ . Тогда  $\mathbb{F}[x]/I$  будет являться кольцом главных идеалов.

*Доказательство.* С факторкольцом связано факторотображение

$$\pi: \mathbb{F}[x] \rightarrow \mathbb{F}[x]/I.$$

Можно проверить, что прообраз любого идеала  $J$  в  $\mathbb{F}[x]/I$  будет являться идеалом в  $\mathbb{F}[x]$ . Следовательно,

$$\pi^{-1}(J) = (f(x)) \Rightarrow J = (\pi(f(x))).$$

■

Посмотрим на простой пример и поймем, что бывает, если мы берем факторкольца кольца многочленов по некоторому главному идеалу (как мы теперь понимаем, других идеалов в кольце многочленов не бывает).

**Пример 3.3.7.** Проверим, является ли полем кольцо вычетов  $\mathbb{F}_7[x]/(x^4 - x^2 + 1)$ . Для этого заметим, что

$$x^4 - x^2 + 1 \equiv x^4 - x^2 - 6 = (x^2 - 3)(x^2 + 2) \pmod{7}.$$

Из разложения следует наличие делителей нуля в факторкольце, а значит, отсутствие обратимости у некоторых вычетов, отличных от нулевого. Это не поле.

А когда мы можем точно сказать, что полученное факторкольцо является полем? Ответим ниже в одном из следующих подразделов. А пока что разберемся поближе с корнями многочленов. Эта тема тоже поможет нам в понимании классификации конечных полей.

### 3.3.2 Корни многочлена

Мы уже знаем, что корнем  $\alpha$  является элемент кольца  $R$ , который обнуляет многочлен  $f$  при подстановке  $\text{ev}_\alpha(f) = 0$ . Кроме этого, мы уже начали изучать теорию делимости в кольце многочленов над полем. Покажем, как эта теория связана с корнями.

**Утверждение 3.3.8.** Пусть  $f \in \mathbb{F}[x]$ . При делении многочлена  $f(x)$  на многочлен  $(x - a)$  получается  $f(a)$ .

*Доказательство.* Мы можем разделить формально многочлен  $f(x)$  на  $(x - a)$  с остатком:

$$f(x) = q(x) \cdot (x - a) + r(x).$$

Подставим это выражение в гомоморфизм эвалюации:

$$f(a) = \text{ev}_a(f) = \text{ev}_a(q \cdot (x - a) + r) = q(a) \cdot 0 + r(a) = r,$$

последний переход имеет смысл, так как остатком при делении на линейный многочлен является константа, которая остается собой даже после подстановки  $a$  в нее.

Как видим, мы получили в остатке  $f(a)$ . ■

Мы можем говорить, что один многочлен делится на другой, если в остатке мы получаем нулевой многочлен.

**Следствие 3.3.9.**  $f(x)$  делится на  $(x - a)$  равносильно тому, что  $a$  — корень  $f(x)$ .

**Пример 3.3.10.** Найдем остаток  $x^{100} + x - 2$  при делении на  $x - 1$  в кольце  $\mathbb{R}[x]$ . Как видим, многочлен имеет вид  $(x - a)$ , а значит, необходимо подставить  $a$  в многочлен, чтобы получить остаток:

$$\text{ev}_1(x^{100} + x - 2) = 1^{100} + 1 - 2 = 0.$$

**Утверждение 3.3.11.** Пусть  $\mathbb{F}$  — поле. Тогда количество корней  $f \in \mathbb{F}[x]$  не больше  $\deg f$ .

*Доказательство.* Мы показали выше, что если есть корень  $a$ , то мы можем разделить многочлен на  $(x - a)$ . Далее по индукции показываем, что многочлен раскладывается в произведение линейных многочленов и многочлена, который не имеет ни одного корня, то есть

$$f(x) = (x - a_1)(x - a_2)(x - a_3) \dots (x - a_k) \cdot g(x),$$

где  $g(x)$  не имеет корней.

Можем показать, что больше корней нет, так как делителей нуля нет. Остается только воспользоваться логарифмическим свойством степени многочлена. ■

Отлично, с многочленами разобрались и обсудили немного их. Теперь вернемся к полям и увидим, как факторкольца многочленов легко описываются за счет знания свойств многочлена, по которому мы факторизуем.

### 3.3.3 Цикличность мультипликативной группы конечного поля

Этот подраздел имеет одно назначение: доказать интересное свойство мультипликативной группы конечного поля.

**Теорема 3.3.12.** Мультипликативная группа конечного поля циклическая.

*Доказательство.* Пусть в поле  $\mathbb{F}$  будет  $n + 1$  элемент. Из теоремы Лагранжа мы знаем, что у обратимых элементов порядки являются делителями  $n$ . Рассмотрим такой делитель  $d$ . Если есть хотя бы один элемент  $\alpha$  такого порядка, то их ровно  $\varphi(d)$ . Почему?

Возьмем  $\alpha$  и возведем во все степени от нуля до  $d-1$ . Мы получим  $d$  различных элементов поля, которые являются корнями многочлена  $f_d(x) = x^d - 1$ . Так как этот многочлен мы рассматриваем над полем, то в нем не более  $d$  корней, а значит, все корни представлены уже выше как степени элемента  $\alpha$ . Остается заметить, что только  $\varphi(d)$  степеней  $\alpha$  будут иметь порядок  $d$ , так как для этого необходимо и достаточно, чтобы показатель  $\alpha$  был взаимно прост с  $d$ .

В комбинаторике доказывается формула

$$n = \sum_{d|n} \varphi(d).$$

Используя эту формулу, мы можем показать, что среди порядков обязаны встречаться все делители  $n$ , а значит, оно само тоже должно быть, так что есть элемент порядка  $n$ , то есть элемент порождающий всю мультиликативную группу. ■

**Замечание.** Порождающий элемент мультиликативной группы конечного поля, как и в случае вычетов, называется *первообразным корнем* или *примитивным корнем*.

**Пример 3.3.13.** Решим уравнение

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \equiv 0 \pmod{29}.$$

Для этого заметим, что  $x = 1$  не является корнем этого уравнения, а следовательно, мы можем домножить многочлен слева на  $(x - 1)$  и в множестве корней появится только 1. Получим:

$$x^7 \equiv 1 \pmod{29}.$$

Далее заметим, что  $\mathbb{Z}_{29}$  является полем, а значит, в нем есть примитивный элемент. Проверяем, что 2 является таким. По уравнению видно, что решением являются все степени примитивного корня, показатели которых кратны 4. Как итог, в ответе будут:

$$2^4 \equiv 16, 2^8 \equiv 24, 2^{12} \equiv 7, 2^{16} \equiv 25, 2^{20} \equiv 23, 2^{24} \equiv 20 \pmod{29}.$$

Как видите, цикличность может помогать решать нелинейные уравнения над полем. Позже мы познакомимся с новыми полями, и над ними мы тоже сможем достаточно легко решать простые нелинейные уравнения.

### 3.3.4 Максимальный идеал. Теорема о максимальном идеале

Сейчас мы введем максимальный идеал и покажем, как свойство максимальности связано с свойствами факторкольца.

**Определение 3.3.14.** Пусть  $I \triangleleft R$ . Будем говорить, что  $I$  **максимальный идеал**, если не существует такого идеала  $J \triangleleft R$ , что  $I \subsetneq J \subsetneq R$ .

Перед основной теоремой этого раздела докажем простое свойство поля.

**Утверждение 3.3.15.** В поле  $\mathbb{F}$  имеется всего два идеала:  $\{0\}$  и  $\mathbb{F}$ .

**Доказательство.** Рассмотрим произвольный идеал  $I$ . Если он содержит только 0, то все доказано. Пусть теперь в нем есть  $a \neq 0$ . Мы знаем, что все элементы, кроме нуля, обратимы в поле, поэтому:

$$a \cdot a^{-1} = 1 \in I.$$

Так как единица в идеале, то

$$\forall x \in \mathbb{F}: x = x \cdot 1 \in I \Rightarrow \mathbb{F} \subseteq I \subseteq \mathbb{F} \Rightarrow \mathbb{F} = I.$$

**Замечание.** Эти идеалы называются *тривиальными*.

**Следствие 3.3.16.** Если в кольце есть нетривиальный идеал, то это не поле.

А теперь основная теорема, которую нужно запомнить так же, как и первую теорему об гомоморфизме. Наизусть!

**Теорема 3.3.17.** (о максимальном идеале) Пусть  $I \triangleleft R$  и  $R$  — коммутативное кольцо с  $1 \neq 0$ . Тогда  $R/I$  поле тогда и только тогда, когда  $I$  максимальный идеал.

*Доказательство.* При факторотображении образ идеала — это идеал. Пусть  $R/I$  — поле. Тогда образ любого идеала  $J$  является идеалом в поле, но таких идеалов всего два: тривиальный из  $[0]_I$  и идеал, содержащий все поле. Следовательно, либо  $J$  совпадает с  $R$ , либо содержитя в  $I$ , что означает максимальность  $I$ .

Теперь предположим, что  $I$  максимальен. Покажем, что все элементы факторкольца, кроме нулевого, будут обратимы. Для этого рассмотрим  $y = [x]_I \in R/I$ . Так как  $[x]_I \neq [0]_I$ , то  $x$  не лежит в  $I$ , а значит,

$$I \subsetneq (I, x) \subseteq R.$$

Из максимальности  $I$  следует, что  $(I, x) = R$ . Следовательно,

$$\exists z \in (I, x) : z \cdot x = 1_R \Rightarrow [z]_I \cdot [x]_I = [1_R]_I = 1_{R/I} \Rightarrow y \in (R/I)^*.$$

В силу произвольности выбранного  $y$  мы получаем, что множество обратимых элементов совпадает с  $(R/I) \setminus \{0\}$ . А этого достаточно, чтобы сказать, что получившееся кольцо является полем. ■

**Замечание.** При факторизации по максимальному идеалу обычно говорят о *поле классов вычетов*, а не о кольце классов вычетов. Или о *факторполе*, но это слово редко встречается.

**Пример 3.3.18.** Являются ли полями следующие кольца вычетов:

$$a) \mathbb{Q}[x]/(x^3 + 1); \quad b) \mathbb{F}_3[x]/(x^3 + 2); \quad c) \mathbb{F}_7[x]/(x^3 + 3)?$$

- a) У многочлена  $x^3 + 1$  есть корень  $-1$ , поэтому этот многочлен делится на  $x + 1$ , а значит, в кольце вычетов будут делители нуля.
- б) Так как мы рассматриваем коэффициенты по модулю 3, то порождающий многочлен эквивалентен  $x^3 - 1$ , а этот многочлен мы так же легко можем разложить на множители, образы которых дадут делители нуля.
- в) Здесь все немного сложнее. А именно, если бы мы смогли разложить многочлен  $x^3 + 3$  на множители, то один из множителей обязан был бы быть линейным, а следовательно, у многочлена должен существовать корень. Далее проверяем, что у многочлена нет корней. Их, действительно, нет, и многочлен не раскладывается на произведение многочленов, откуда получаем, что он порождает максимальный идеал. По теореме о максимальном идеале мы получаем в факторе поле.

### 3.3.5 Поле частных. Поле рациональных функций

Пусть  $R$  — область целостности. Построим по этой области поле частных так же, как мы в школе по  $\mathbb{Z}$  строили  $\mathbb{Q}$ . Совет для впервые столкнувшихся с этой темой: пробуйте параллельно чтению представлять кольцо целых чисел и смотреть, что в этом примере будут те или иные конструкции.

Рассмотрим множество

$$\{(x, y) : x, y \in R, y \neq 0\} = R \times R \setminus \{0\}.$$

Элементы этого множества обычно называются *дробями* и обозначаются, как обыкновенные дроби в школе:

$$(x, y) = \frac{x}{y}.$$

Можно ввести отношение эквивалентности на этом множестве. Скажем, что

$$(x, y) \sim (z, w) \Leftrightarrow xw = zy.$$

**Лемма 3.3.19.** Введенное выше отношение является отношением эквивалентности

*Доказательство.* Рефлексивность дает верное равенство  $ab = ab$ . Симметричность следует из симметричности равенства. Остается проверить транзитивность. Для этого уже придется воспользоваться целостностью кольца  $R$ . Предположим, что  $(x, y) \sim (z, w)$  и  $(z, w) \sim (t, s)$ . По определению

$$xw = zy, \quad zs = tw \Rightarrow xtw = zyt = zxw = zsy \Rightarrow yt = sx \Rightarrow (x, y) \sim (t, s).$$

■

Раз это отношение эквивалентности, мы можем его профакторизовать:

$$Q(R) \stackrel{\text{def}}{=} (R \times R \setminus \{0\}) / \sim.$$

И на этом фактормножестве введем операции:

$$\frac{x}{y} + \frac{z}{w} \stackrel{\text{def}}{=} \frac{xw + zy}{yw}, \quad \frac{x}{y} \cdot \frac{z}{w} = \frac{xz}{yw}.$$

Оказывается, что с этими двумя операциями фактормножество становится полем. Это поле называют **полем частных кольца  $R$** . Его еще обозначают  $\text{Quot}(R)$ .

Чтобы показать, что это поле, докажем простое утверждение.

**Утверждение 3.3.20.** Отношение эквивалентности выше совпадает с отношением эквивалентности, в котором пара  $(x, y)$  эквивалентна  $(z, w)$  тогда и только тогда, когда мы можем получить из первой пары вторую домножением и сокращением на общий множитель оба числа  $x$  и  $y$ , то есть можем делать переходы:  $(a, b) \rightarrow (ka, kb)$ ,  $k \in R$  или  $(ka, kb) \rightarrow (a, b)$ ,  $k \in R$ .

*Доказательство.* Для начала нам надо показать, что новое отношение является эквивалентностью. Рефлексивность следует из того, что мы можем ни на что не домножать или домножить на единицу оба элемента. Симметричность следует из того, что мы можем как развернуть все действия, то есть заменить домножения сокращением и наоборот, поменяв при этом и порядок этих действий. А транзитивность здесь очевидна.

Далее покажем, что из первой эквивалентности следует вторая:

$$(x, y) \sim (z, w) \Rightarrow (x, y) \rightarrow (xw, yw) = (yz, yw) \rightarrow (z, w)$$

и что из второй эквивалентности следует первая:

$$(x, y) \rightarrow (kx, ky) \Rightarrow \forall z \in R, w \in R \setminus \{0\}: xz = yw \Leftrightarrow kxz = kyw.$$

Формально мы должны еще воспользоваться индукцией, но оставим этот пункт на плечах читателя. ■

**Пример 3.3.21.** Как мы знаем, из  $\mathbb{Z}$  такими махинациями мы получаем  $\mathbb{Q}$ .

**Пример 3.3.22.** Еще есть переход от многочленов  $\mathbb{F}[x]$  к  $\mathbb{F}(x) \stackrel{\text{def}}{=} Q(\mathbb{F}[x])$ , которое называют **полем рациональных функций**.

Эта конструкция позволяет перейти от области целостности к полю. Более того, видно, что  $R$  можно вложить в  $Q(R)$ , так что можно говорить, что при переходе к полю частных мы расширяем наше кольцо. А какие еще бывают расширения? Ниже мы рассмотрим расширения полей, а через раз покажем, как с помощью этих расширений получить произвольные конечные поля.

### 3.3.6 Расширение полей

Рассмотрим канонический эпиморфизм ( $I = (p(x)) \triangleleft \mathbb{F}[x]$ ):

$$\pi: \mathbb{F}[x] \rightarrow \mathbb{F}[x]/I = \mathbb{K},$$

где  $I$  — максимальный идеал. Ограничение этого эпиморфизма на простое подполе инъективно, так что  $\pi(\mathbb{F})$  — подполе в  $\mathbb{K}$ , изоморфное  $\mathbb{F}$ . Будем считать, что  $\mathbb{F} \subseteq \mathbb{K}$ .

Отметим, что при этом эпиморфизме образ  $x$  является вычетом  $[x]_I$ , то есть элементом, который удовлетворяет уравнению

$$[p_0]_I + [p_1]_I \cdot [x]_I + [p_2]_I \cdot [x]_I^2 + \dots + [p_n]_I \cdot [x]_I^n = 0 = p([x]_I).$$

Из-за этого говорят, что  $[x]_I$  — это *корень многочлена*  $p(x)$ . Если опускать формальности, то при сложении и перемножении этот элемент ведет себя именно так, как корень многочлена  $p(x)$ , поэтому и имеет смысл его называть корнем. Если мы обозначим корень через  $\alpha$ , то поле  $\mathbb{K}$  будем обозначать  $\mathbb{F}(\alpha)$ . Это обозначение очень похоже на то, что мы делали выше при определении поля частных. Тут нет двусмыслия, так как если предположить, что  $\alpha$  не является корнем никакого полинома, то  $\mathbb{F}(\alpha)$  будет минимальным полем, содержащим  $\alpha$ , и будет совпадать с полем частных от  $\mathbb{F}[x]$ .

Вся теория, изложенная выше, дана для того чтобы вы могли брать числа, которые могут являться корнями полиномов, и добавлять в поле, расширяя его. Чтобы формализовать эти идеи, дадим несколько определений.

**Определение 3.3.23.** Пусть  $\mathbb{F} \subseteq \mathbb{K}$  — два поля. Тогда  $\mathbb{K}$  — *расширение поля*  $\mathbb{F}$ . При этом если  $\mathbb{K}$  — минимальное расширение, содержащее элемент  $a$ , то мы будем писать, что  $\mathbb{K} = \mathbb{F}(a)$ .

**Замечание.** Элементы  $\mathbb{K}$  — это рациональные функции от элемента  $a$ . При этом если предполагается, что  $a$  является корнем какого-то многочлена  $p(x)$ , то любую дробь можно представить в виде многочлена от  $a$ .

Все рассуждения, которые мы оформили выше можно вылить в следующую теорему.

**Теорема 3.3.24.** Пусть  $\mathbb{F}$  — поле.  $I = (p(x)) \triangleleft \mathbb{F}[x]$  — максимальный идеал. Тогда существует расширение поля  $\mathbb{F}$  корнем  $a$  многочлена  $p(x)$ , причем  $F(a) = F[a]$ . И любое такое расширение изоморфно  $\mathbb{F}[x]/(p)$ .

**Определение 3.3.25.** Элемент  $\alpha$  в расширении  $\mathbb{K}$  для  $\mathbb{F}$  называется *алгебраическим*, если существует многочлен  $p(x) \in \mathbb{F}[x]$ , у которого  $\alpha$  — корень, то есть  $p(\alpha) = 0$ . Иначе такой элемент называется *трансцендентным*.

**Замечание.** Надо понимать, что так как  $\mathbb{K}$  расширение  $\mathbb{F}$ , то  $\mathbb{F}$  — подполе  $\mathbb{K}$ , поэтому мы можем подставлять элементы  $\mathbb{K}$  в многочлены с коэффициентами из  $\mathbb{F}$ . Так мы делаем, например, когда подставляем вещественные числа в многочлен с рациональными коэффициентами.

С алгебраическими элементами связано определенное расширение.

**Определение 3.3.26.** Если  $\mathbb{K} = \mathbb{F}(\alpha)$ , где  $\alpha$  — алгебраический элемент  $\mathbb{F}$ , то  $\mathbb{K}$  называется *алгебраическим расширением*  $\mathbb{F}$ .

**Замечание.** Отметим еще раз, что при расширении  $\mathbb{F}$  трансцендентным элементом мы получаем поле изоморфное  $\mathbb{F}(x)$ .

**Пример 3.3.27.** Найдем минимальное расширение  $\mathbb{Q}$ , где есть число  $\alpha = \sqrt{2} - \sqrt{5}$ . Обозначим это поле через  $\mathbb{K}$ . В этом расширении есть  $\alpha^2 = 7 - 2\sqrt{10}$ , то есть элемент  $\sqrt{10}$  тоже есть.

Можем преобразовать и еще раз возвести в квадрат и получить, что

$$p(\alpha) = (7 - \alpha^2)^2 - 40 = 0$$

Этот многочлен минимален по степени. Почему? На линейные множители его не разложить над  $\mathbb{Q}$ , так как тогда бы у него был корень, а мы можем легко проверить, что здесь их нет. На квадраты тоже не разложить, так как тогда получилось бы что  $\alpha$  является корнем одного из квадратов, а этого быть не может (подставьте в общий вид квадратного выражения от  $\alpha$  вид  $\alpha^2$  и приравняйте к нулю коэффициенты у всех линейно независимых элементов, тогда получите, что все коэффициенты многочлена нулевые).

**Определение 3.3.28.** Пусть  $\alpha$  — алгебраический элемент в  $\mathbb{K}$  над  $\mathbb{F}$ . Тогда **минимальным многочленом**  $\alpha$  называется многочлен  $f(x) \in \mathbb{F}[x]$  минимальной степени, который обнуляется при подстановке  $\alpha$ . При этом  $\deg f$  называется **степенью элемента**  $\alpha$  и обозначается через  $\deg_{\mathbb{F}} \alpha$ .

**Пример 3.3.29.** Пусть  $\xi = 1 + i$ . Найдем его степень над  $\mathbb{Q}$ . Заметим, что этот элемент удовлетворяет уравнению

$$x^2 - 2x + 2 = 0.$$

Над  $\mathbb{Q}$  это уравнение не раскладывается на линейные множители, так как корней в  $\mathbb{Q}$  у него нет. Следовательно, это минимальный многочлен для  $\xi$ , поэтому  $\deg_{\mathbb{Q}} \xi = 2$ .

Позже мы покажем, что минимальный многочлен существует для каждого алгебраического элемента над полем. А теперь давайте подумаем, что будет, если мы попробуем расширять наше поле до бесконечности, добавляя каждый раз новые алгебраические элементы. Оказывается, что в пределе мы имеем очень хорошее поле, над которым каждый многочлен раскладывается на линейные множители.

**Определение 3.3.30.** Будем говорить, что поле  $\mathbb{F}$  **алгебраически замкнуто**, если любой многочлен над ним имеет хотя бы один корень.

**Пример 3.3.31.**  $\mathbb{R}$  не является алгебраически замкнутым, так как  $x^2 + 1$  не имеет корней в нем.

**Пример 3.3.32.**  $\mathbb{C}$  является алгебраически замкнутым полем. Но доказательство этого факта сложно, так как основывается обязательно на непрерывных свойствах этого поля.

**Пример 3.3.33.** Любое конечное поле алгебраически не замкнуто, так как многочлен

$$f(x) = \prod_{i=1}^n (x - a_i) + 1,$$

где  $a_i$  пробегают все элементы поля, не имеет корней, что проверяется прямой подстановкой.

## Домашнее задание

**Задача 3.3.1.** Разделите многочлен  $f$  на  $g$  с остатком: а)  $f = 2x^3 + 2x^2 + x + 6$ ,  $g = x^2 + 2x + 1$ ; б)  $f = x^4 + 1$ ,  $g = x^5 + 1$ .

**Задача 3.3.2.** Являются ли полями следующие кольца вычетов:

$$a) \mathbb{Q}[x]/(x^4 + 1); \quad b) \mathbb{F}_3[x]/(x^4 + 1); \quad c) \mathbb{F}_{17}[x]/(x^4 + 1).$$

**Задача 3.3.3.** Пусть  $R$  — область целостности. Покажите, что количество корней  $f \in R[x]$  не больше  $\deg f$ .

**Задача 3.3.4.** Пусть  $\mathbb{F}$  — конечное поле,  $|\mathbb{F}^*| = n$ . Покажите, что если  $x \in \mathbb{F}^*$  не является первообразным корнем, то его порядок делит одно из чисел  $n/p_1, n/p_2, \dots, n/p_k$ , где  $p_i$  — это все простые числа, участвующие в разложении числа  $n$ .

**Задача 3.3.5.** Представьте поле из 9-ти элементов в виде факторкольца и найдите в его мультипликативной группе первообразный корень.

**Задача 3.3.6.** Покажите, что  $\text{Quot}(\mathbb{Z}[i]) = \mathbb{Q}[i]$ .

**Задача 3.3.7.** Покажите, что если  $\mathbb{F}$  — поле, то  $\text{Quot}(\mathbb{F}) \cong \mathbb{F}$ .

**Задача 3.3.8.** Докажите, что  $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$ .

**Задача 3.3.9.** Найдите такое минимальное расширение  $\mathbb{Q}$ , где есть число  $\alpha = \sqrt{2} + \sqrt{3}$ .

**Задача 3.3.10.** Пусть  $\alpha \in \mu_6$  — порождающий этой группы. Чему равна его степень над  $\mathbb{Q}$ ?

**Бонусная задача.** Докажите, что у любого поля существует алгебраически замкнутое расширение.

## Рекомендуемая литература

- [1] Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Раздел 7, 9.
- [2] Городенцев А. Л. — Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 2, §3, 4, 6.
- [3] Винберг Э. Б. — Курс Алгебры — 2-е изд., стереотип. — М.: МЦНМО, 2013. — Глава 1, §3, 5; глава 9, §2, 5.

## 3.4 Евклидовы и факториальные кольца

Ниже мы подробно обсудим евклидовы кольца. И на их примере покажем, как же важно знать о кольце то, что в нем все идеалы главные, или что в нем все простые идеалы максимальны, или что в нем все неприводимые элементы просты. Несмотря на такую тесную связь с евклидовыми кольцами, большая часть этого раздела имеет общие определения и имеет приложения за границей евклидовых колец.

В заключение мы покажем, что евклидовы кольца факториальны и объясним, что это нам дает. Даже это свойство будет указывать на большую связь между евклидовыми кольцами и теорией чисел для  $\mathbb{Z}$ .

**Ключевые слова:** евклидово кольцо, область целостности, минимальный многочлен, простой идеал, простой элемент, кольцо главных идеалов, ассоциированные элементы, неприводимые элементы, наибольший общий делитель, основная теорема арифметики, факториальное кольцо, китайская теорема об остатках.

### 3.4.1 Евклидово кольцо: определение и свойства

Мы знаем со школы, что в целых числах можно делить с остатком. Выше мы показывали, что в кольце многочленов над полем тоже это можно делать. Теперь мы обобщим эти случаи и покажем, какие общие свойства у них есть.

**Определение 3.4.1.** Пусть  $R$  — коммутативное кольцо. Отображение  $\mathcal{N}: R \rightarrow \mathbb{N}_0$ , которое мы будем называть **нормой**. Пару  $(R, \mathcal{N})$  будем называть **евклидовым кольцом**, если выполнены аксиомы:

- E1.  $\mathcal{N}(x) = 0 \Leftrightarrow x = 0$  (невырожденность);
- E2.  $\forall a, b \in R, b \neq 0 \exists q, r: a = q \cdot b + r, r = 0 \vee \mathcal{N}(r) < \mathcal{N}(b)$  (деление с остатком);
- E3.  $\forall a, b \in R \setminus \{0\}: \mathcal{N}(ab) \geq \mathcal{N}(a)$  (дополнительное свойство).

**Замечание.** Последнее свойство не всегда указывают, обобщая понятие евклидова кольца на большее количество пар. Однако многие свойства, что мы обсудим ниже не будут выполняться в таком случае, так что мы оставим определение именно в таком виде.

**Замечание.** Еще любят определять  $\mathcal{N}$  на всем кольце без нуля. При этом говорят, что нет делителей нуля, чтобы не возникало проблем с последним свойством. Мы же покажем, что при нашем определении  $R$  становится областью целостности. Отчего оба определения становятся эквивалентными.

**Пример 3.4.2.** Кольцо гауссовых целых чисел можно определить как  $\mathbb{Z}[x]/(x^2 + 1)$ , так и формально:

$$\mathbb{Z}[i] = \{a + bi: a, b \in \mathbb{Z}, i^2 + 1 = 0\}.$$

Покажем, что оно евклидово. Для этого необходимо ввести норму с целой областью значений. Возьмем:

$$\mathcal{N}(a + bi) = a^2 + b^2.$$

Достаточно просто проверяется невырожденность. Для деления с остатком вспомним, что любая точка внутри квадрата со стороной  $a$  имеет среди вершин такую, которая удалена не дальше, чем на  $a/\sqrt{2}$ . Поэтому для любых двух  $a, b \in \mathbb{Z}[i]$  мы можем нарисовать сетку из квадратов, порожденную числом  $b$  на комплексной плоскости. При этом число  $a$  попадет внутрь одного из квадратов. Остается представить число  $a$  в виде суммы вектора от нуля до ближайшей вершины и от вершины до  $a$ , что и дает искомое разложение на частное с остатком при делении на  $b$ .

Последнее свойство E3 можно в лоб доказать

$$(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2).$$

**Пример 3.4.3.** Пусть  $\mathbb{F}$  — поле. Тогда  $\mathbb{F}[x]$  является евклидовым кольцом. Однако можно заметить, что  $\deg f$  не будет нормой на этом кольце. Почему? По аксиоме E1 у нас норму ноль имеет только  $x = 0$ , однако в кольце многочленов у любой константы степень по определению считается равной нулю. Мы можем это исправить. Введем новую функцию

$$\deg' f = \begin{cases} 0, & f = 0; \\ \deg f + 1, & f \neq 0. \end{cases}$$

Это функция уже образует евклидову норму на кольце и делает из него евклидово кольцо.

Заметим, что ранее, когда мы говорили об алгоритме Евклида, то нам надо было знать только, что в целых числах можно делить. Из-за этого мы можем без изменений перенести алгоритм Евклида на евклидовые кольца. Что такое наибольший общий делитель, мы определим чуть позже, но уже сейчас мы можем вынести очень важное свойство для евклидовых колец.

**Теорема 3.4.4.** Евклидово кольцо является областью целостности.

*Доказательство.* Покажем, что нет делителей нуля. Предположим, что это не так и существуют  $a, b$ , такие что  $a \cdot b = 0$ . По свойству Е3 и Е1:

$$\mathcal{N}(a \cdot b) = \mathcal{N}(0) = 0 \geq \mathcal{N}(a), \mathcal{N}(b) \Rightarrow \mathcal{N}(a) = \mathcal{N}(b) = 0 \Rightarrow a = b = 0.$$

Теперь найдем единицу в этом кольце. Для этого найдем элемент  $x$  с наименьшей нормой и разделим на себя:

$$x = e \cdot x + r.$$

По свойству Е2 мы получаем, что  $r = 0$  и  $x = e \cdot x$ . Далее берем произвольный  $y$  в кольце:

$$y \cdot x = y \cdot ex \Rightarrow x \cdot (y - y \cdot e) = 0 \Rightarrow y = y \cdot e.$$

Получаем, что  $e$  является той самой единицей в кольце. ■

**Теорема 3.4.5.** Пусть  $(R, \mathcal{N})$  — евклидово кольцо. Тогда  $R$  — это кольцо главных идеалов.

*Доказательство.* Рассмотрим произвольный идеал  $I \triangleleft R$ . Он может содержать только ноль, тогда он очевидно им же и порождается. А может содержать ненулевой элемент  $x$ . В последнем случае множество натуральных чисел

$$\mathcal{N}(I \setminus \{0\}) = \{n : n \in \mathbb{N}, \exists x \in R \ \mathcal{N}(x) = n\}$$

непусто, а значит, имеет наименьший элемент. Пусть  $d$  имеет наименьшую ненулевую норму в  $I$ . Понятно, что  $(d) \subseteq I$ . Покажем, что верно обратное включение. Для этого возьмем произвольный элемент  $x \in I \setminus \{0\}$  и разделим с остатком на  $d$ :

$$x = q \cdot d + r.$$

Мы знаем, что в таком случае элемент  $r$  может равняться нулю или иметь норму строго меньшую, чем норма  $d$ . Однако  $r$  лежит в идеале, так как

$$r = x - q \cdot d \in I,$$

поэтому норма элемента  $r$  не может быть меньше нормы  $d$ , а следовательно,  $r = 0$  и элемент  $x$  кратен  $d$ , то есть лежит в  $(d)$ . Это в точности и дает нам обратное включение, что заканчивает доказательство теоремы. ■

**Следствие 3.4.6.** Любой идеал в  $\mathbb{F}[x]$  порожден некоторым многочленом. В случае с идеалом  $I$ , фактор по которому дает алгебраическое расширение  $\mathbb{F}[\alpha]$ , мы имеем минимальный многочлен  $m(x)$ , который обнуляется при подстановке  $\alpha$ .

Доказанная теорема имеет смысл и в прямом виде, когда мы можем пользоваться тем, что любой идеал главный. И в обратном виде, когда мы показываем, что в кольце нет главного идеала, откуда автоматически следует, что кольцо не может являться евклидовым ни при какой норме.

**Пример 3.4.7.** Докажем, что  $\mathbb{Z}[x]$  не является евклидовым. Для этого заметим, что  $(2, x)$  не является главным идеалом и содержит все многочлены, у которых свободный член является четным числом. Если бы  $f(x)$  порождал этот идеал, то у него обязательно была бы свободная часть равная  $\pm 2$ .

Если при этом степень  $f(x)$  больше нуля, то и все кратные ненулевые многочлены будут иметь ненулевую степень, однако в идеале есть многочлены нулевой степени, отличные от нуля (например,  $g(x) = 4$ ). Поэтому  $\deg f = 0$ , а значит,  $f \equiv 2$ , что сразу приводит к противоречию, так как  $h(x) = x$  лежит в  $(2, x)$ , а в  $(2)$  не лежит.

Мы нашли неглавный идеал, что доказывает, что  $\mathbb{Z}[x]$  не является евклидовым кольцом. Отметим, что кольцо коэффициентов здесь не является полем, так что мы не приходим к противоречию с тем, что мы говорили раньше.

Отлично, мы разобрались немного с определением евклидова кольца и минимальными свойствами. Теперь имеет смысл понять, какими еще свойствами обладают идеалы. Для этого мы введем новый класс идеалов и покажем, что области целостности от полей в коммутативном случае не сильно отличаются. Хотя некоторые отличия есть: посмотрите последний разобранный пример.

### 3.4.2 Простой идеал

Здесь мы будем подразумевать, что  $R$  — коммутативное кольцо с единицей.

Как понять, будет ли полем  $R/I$ ? Для этого можно проверить  $I$  на максимальность. А можно ли найти какой-то подобный критерий для областей целостности? Да, иначе бы этого вопроса тут не было бы.

Дадим, как обычно, пару определений, а потом покажем, в каком виде они эквивалентны.

**Определение 3.4.8.** Будем говорить, что **элемент  $x$  делит элемент  $y$** , если существует такой  $q \in R$ , что  $y = q \cdot x$ . Обозначается это так:  $x | y$ .

**Определение 3.4.9.** Будем говорить, что элемент  $p \in R$  **простой**, если из  $p | ab$  следует, что или  $p | a$ , или  $p | b$ .

**Определение 3.4.10.** Идеал  $I \triangleleft R$  называется **простым идеалом**, если из  $ab \in I$  следует, что  $a \in I$  или  $b \in I$ .

По определениям уже видно, что между простыми элементами и простыми идеалами должна быть связь. И она есть.

**Утверждение 3.4.11.** Элемент  $p \in R$  прост тогда и только тогда, когда  $(p)$  — это простой идеал, тогда и только тогда, когда  $R/(p)$  — это область целостности.

**Доказательство.** Докажем один переход, остальные переходы столь же очевидны. Пусть  $p \in R$  прост, тогда обозначим через  $I$  идеал, порожденный  $p$ . Предположим, что произведение  $a$  и  $b$  лежит в  $I$ , что означает делимость произведения на  $p$ . Так как  $p$  прост, то какой-то из элементов произведения должен делится на  $p$ , но это в точности означает простоту идеала  $I$ . Остальные переходы столь же просты в доказательстве, так что их оставим на совести читателя. ■

**Упражнение.** Докажите остальные переходы в утверждении выше.

**Замечание.** Отметим, что эквивалентность второго и третьего выражения имеет место быть и тогда, когда идеал порожден не одним элементом. Смотрите пример ниже.

**Пример 3.4.12.** Покажем, что в  $\mathbb{Z}[\sqrt{-6}]$  идеал  $(\sqrt{-6}, 3)$  прост и максимален. Для этого заметим, что факторкольцо по этому идеалу изоморфно  $\mathbb{Z}_3$ . Это одновременно и поле, и область целостности. Отсюда следует, что идеал был и простым, и максимальным.

После этого примера может показаться, что простые и максимальные идеалы не отличимы, хотя понятно, что область целостности и поле — это разные понятия. Но все же, чтобы развеять всяческие сомнения, покажем на другом примере, что это разные понятия.

**Пример 3.4.13.** В  $\mathbb{Z}[x]$  идеал  $x$  прост, так как факторкольцо по нему является областью целостности. Однако он не максимален, так как содержится в идеале  $(2, x)$ .

Получается, что простой идеал не всегда является максимальным идеалом. Однако в некоторых случаях все-таки может быть таким. Так в какой мере проходит эта граница между простыми и максимальными идеалами? Ответ прост и заключается в следующей теореме.

**Теорема 3.4.14.** Пусть  $R$  — это область целостности. Если идеал  $I = (p)$  прост, он максимален в множестве главных идеалов кольца.

*Доказательство.* Допустим, что идеал прост. Тогда если  $I \subsetneq J = (a)$ , то существует такой  $q \in R$ , что  $p = q \cdot a$ . В силу простоты элемента  $p$  мы имеем, что  $p \mid a$  или  $p \mid q$ . В первом случае все очевидно. А что же во втором? Представим  $q = p \cdot b$  и преобразуем равенство:

$$p = (p \cdot b) \cdot a \Leftrightarrow p \cdot (1 - b \cdot a) = 0 \Leftrightarrow a \cdot b = 1.$$

Получаем, что  $a$  обратим, откуда автоматически следует, что  $J$  совпадает с  $R$ , что доказывает максимальность идеала  $I$ . ■

**Следствие 3.4.15.** В кольцах главных идеалов идеал прост тогда и только тогда, когда он максимален.

*Доказательство.* Действительно, мы показали, что простой идеал максимален среди главных, а в КГИ это все идеалы, так что он просто максимален. В обратную же сторону мы можем опять провести рассуждения, сказав, что факторкольцо по максимальному идеалу является полем, а значит, областью целостности, а значит, все максимальные идеалы просты. ■

**Следствие 3.4.16.** Все максимальные идеалы в евклидовых кольцах просты.

**Пример 3.4.17.** Может ли пересечение двух различных максимальных идеалов содержать простой элемент? Рассмотрим опять  $\mathbb{Z}[x]$ . В нем есть два идеала:  $(2, x)$  и  $(3, x)$ . Оба идеала максимальны, так как факторкольца по ним являются полями. Что лежит в пересечении? Идеал  $(6, x)$ . А в нем есть элемент  $x$ , который является простым, так как  $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$  — область целостности. Получается, что такое может быть.

Далее мы покажем, что в евклидовых кольцах у простых элементов есть интересные свойства, которые позволяют прийти к похожему разложению, которое было в целых числах: разложению числа на простые множители. Из-за того, что мы сможем раскладывать числа на множители, мы сможем получить аналог китайской теоремы об остатках для евклидова кольца.

### 3.4.3 Ассоциированные и неприводимые элементы

Будем подразумевать, что  $R$  — область целостности. Мы уже знаем несколько классов идеалов и понимаем, что исследование идеалов колец эквивалентно исследованию его числовых свойств. Из-за этого необходимо получить несколько ответов на простые вопросы. Когда главные идеалы совпадают? Что мы можем сказать про главные идеалы, которые включены друг в друга? Как включения идеалов связаны с разложением элементов на множители?

Начнем с некоторого отношения эквивалентности, которое будет встречаться нам вплоть до конца этого раздела.

**Определение 3.4.18.** Будем говорить, что  $x$  ассоциировано  $y$ , если  $x \mid y$  и  $y \mid x$ .

**Упражнение.** Отношение ассоциированности является отношением эквивалентности на  $R$ .

Суть этого отношения раскрывается в следующем утверждении.

**Утверждение 3.4.19.** Элемент  $x$  ассоциирован с элементом  $y$  тогда и только тогда, когда существует такой  $a \in R^*$ , что  $x = a \cdot y$ .

*Доказательство.* С нулем все понятно, так что будем предполагать, что  $x$  и  $y$  ненулевые. Покажем, что из ассоциированности следует второе условие. Понятно, что имеются два равенства:

$$x = a \cdot y, \quad y = b \cdot x.$$

Но нам никто не обещает, что элементы  $a, b$  будут обратимы, но мы можем подставить одно выражение внутрь другого и получить:

$$x = (ab) \cdot x \Leftrightarrow x \cdot (1 - ab) = 0,$$

так как  $R$  — область целостности, мы можем сократить на  $x$  и получить:

$$a \cdot b = 1 \Leftrightarrow a, b \in R^*.$$

В обратную сторону видим, что  $x$  делится на  $y$ , а  $y$  делится на  $x$ :

$$y = a^{-1} \cdot x \Rightarrow x \sim y.$$

■

**Следствие 3.4.20.**  $R^*$  — это класс элементов, ассоциированных с единицей.

**Пример 3.4.21.** В  $\mathbb{Z}$  обратимы только  $\pm 1$ , так что множества ассоциированных друг с другом элементов выглядят так:  $\{x, -x\}$ .

Ассоциированность — это та точность, с которой мы можем найти порождающий у главного идеала. Почему?

**Утверждение 3.4.22.**  $a$  ассоциировано с  $b$  тогда и только тогда, когда  $(a) = (b)$ .

*Доказательство.* Элементы ассоциированы тогда и только тогда, когда каждый из них делится на другой. А это условие эквивалентно тому, что порождающий одного идеала лежит внутри другого идеала, что приводит к совпадению идеалов. ■

При всем этом мы знаем, что идеалы в евклидовом кольце всегда являются главными идеалами, так что в этом кольце легко проверить, будут ли два идеала совпадать: для этого надо сравнить порождающие с точностью до обратимого элемента.

Понимание ассоциированности дает нам возможность уже правильно определить понятие *наибольшего общего делителя в евклидовом кольце*. Если у нас имеется  $S \subseteq R$ , где  $R$  — евклидово кольцо. Идеал  $I$  порожден множеством  $S$ , следовательно, так как он главный, то существует такой  $d$ , что  $I = (d)$ . Этот  $d$  определен с точностью до ассоциированности. Этот класс ассоциированности мы будем называть наибольшим общим делителем элементов из  $S$ .

**Пример 3.4.23.** Найдем наибольший общий делитель многочленов  $f(x) = x^{84} - 1$  и  $g(x) = x^{35} - 1$  в  $\mathbb{R}[x]$ . Для этого делим многочлены с остатком до тех пор, пока не получим многочлен, на который делятся оба полинома. Таким будет

$$d(x) = x^7 - 1.$$

Из свойств алгоритма Евклида мы получаем, что  $d(x)$  должен лежать в идеале, порожденном  $f(x)$  и  $g(x)$ . И  $d(x)$  делит каждый из многочленов, откуда следует, что он действительно порождает весь идеал, порожденный двумя исходными полиномами.

Стоит отметить, что, как мы писали выше, наибольший общий делитель определен с точностью до умножения на обратимый элемент кольца, так что правильно будет говорить, что НОДом этих двух многочленов будет

$$d(x) \cdot \mathbb{R}^* = \alpha \cdot x^7 - \alpha, \alpha \in \mathbb{R} \setminus \{0\}.$$

На этом польза знания ассоциированности для евклидовых колец не заканчивается. Мы можем еще достаточно просто связать обратимость с нормой.

**Утверждение 3.4.24.** Пусть  $(R, \mathcal{N})$  — евклидово кольцо. Тогда для любых ненулевых элементов  $a, b$  равенство  $\mathcal{N}(ab) = \mathcal{N}(a)$  равносильно тому, что  $b$  — обратим.

*Доказательство.* Если элемент  $b$  обратим, то мы можем написать два равенства:

$$ab = a \cdot b, \quad a = b^{-1} \cdot ab.$$

По свойству ЕЗ получаем, что их нормы совпадают.

Обратно. Пусть их нормы совпадают. Можно разделить с остатком элемент  $a$  на  $ab$ :

$$a = q \cdot ab + r.$$

Так как элемент  $r = a \cdot (1 - qb)$ , то его норма не меньше нормы элемента  $a$ , но его норма равна норме  $ab$ , откуда следует, что  $r = 0$ . Следовательно, так как  $a$  не ноль, а  $R$  — область целостности, то  $b$  обратим. ■

**Следствие 3.4.25.** Элемент обратим тогда и только тогда, когда у него наименьшая норма.

*Доказательство.* Из доказанного для любого обратимого  $b \in R^*$ :

$$\mathcal{N}(b \cdot 1) = \mathcal{N}(1).$$

А из ЕЗ имеем:

$$\forall a \in R \setminus \{0\}: \mathcal{N}(a \cdot 1) \geq \mathcal{N}(1),$$

так что у обратимого элемента норма наименьшая и равна норме единицы. При этом если норма какого-то элемента равна норме единицы, то из  $\mathcal{N}(a \cdot 1) = \mathcal{N}(1)$  получаем, что это обратимый элемент, что доказывает искомое. ■

Мы уже определили простой элемент. Однако это определение отличается от того, к которому мы привыкли в школе: от простого элемента в кольце целых чисел. Там мы говорили, что у простого элемента есть только два делителя (он сам и единица). Тут мы уже понимаем, что делителей может быть много, поэтому нужно говорить о делимости с точностью до обратимого элемента.

**Определение 3.4.26.** Ненулевой элемент  $x$  называется **неразложимым или неприводимым**, если  $x$  необратим и в равенстве  $x = a \cdot b$  один из множителей — ассоциирован с  $x$ , а второй — обратимый элемент. Все остальные необратимые ненулевые элементы называются **разложимыми**.

**Пример 3.4.27.** В  $\mathbb{Z}$  неразложимы все простые числа.

**Пример 3.4.28.** В  $\mathbb{C}[x]$  неразложимы только линейные многочлены.

В общем случае неприводимые и простые элементы — это не одно и то же. Однако в евклидовых кольцах они совпадают.

**Утверждение 3.4.29.** Пусть  $(R, \mathcal{N})$  — евклидово кольцо.  $q$  неразложим тогда и только тогда, когда он прост.

*Доказательство.* Предположим, что  $q$  разложим, то есть  $q = a \cdot b$ , тогда  $(q) \subseteq (a)$ , откуда следует немаксимальность этого идеала, что означает его непростоту. В обратную сторону: если  $q$  неразложим, то идеал, порожденный этим элементом, будет максимальным, откуда следует, что идеал и элемент прости. ■

Нам уже встречались неприводимые многочлены.

**Утверждение 3.4.30.** Минимальный многочлен неприводим.

*Доказательство.* Мы знаем, что минимальный многочлен должен обнуляться элементом  $\alpha$ , то есть  $f(\alpha) = 0$ . Если бы этот многочлен был бы разложимым, то есть  $f(x) = g(x) \cdot h(x)$ , то при подстановке в какой-либо из многочленов  $g(x)$  или  $h(x)$  мы должны были получить ноль (в поле нет делителей нуля). Откуда получаем, что один из этих многочленов будет меньшей степени и будет обнуляться при подстановке  $\alpha$ . Это противоречит минимальности исходного полинома. ■

**Следствие 3.4.31.** Если  $\alpha$  — алгебраический элемент над  $\mathbb{F}$ , то канонический эпиморфизм  $\pi: \mathbb{F}[x] \rightarrow \mathbb{F}[\alpha]$  будет иметь ядро, порожденное минимальным многочленом.

Для полиномов небольшой степени достаточно просто сказать, является ли он приводимым или нет.

**Теорема 3.4.32.** Полином  $f(x) \in \mathbb{F}[x]$  степени  $\deg f = 2, 3$  приводим тогда и только тогда, когда он имеет корень.

*Доказательство.* Если полином имеет корень  $a$ , то он делится на  $x - a$ , так что он приводим. Если же он приводим, то у одного из множителей степень обязана быть многочленом первой степени, который будет обязательно иметь корень в поле  $\mathbb{F}$ . ■

**Пример 3.4.33.** Найдем все многочлены степени не больше 4 в  $\mathbb{F}_2[x]$ , которые являются неприводимыми. Разобьем поиски на два случая: многочлен степени 4 и степени меньше 4.

Во втором случае мы знаем, что для неприводимости достаточно, чтобы не было корней у многочлена. Поэтому мы получаем, что неприводим многочлен  $f(x)$  тогда и только тогда, когда

$$f_0 = 1, \quad f_1 + f_2 + f_3 = 0 \pmod{2}.$$

Откуда мы можем получить все возможные неприводимые многочлены степени не больше трех:

$$1 + x + x^2, \quad 1 + x + x^3, \quad 1 + x^2 + x^3.$$

У полинома четвертой степени по аналогии не должно корней, то есть

$$f_0 = 1, \quad f_1 + f_2 + f_3 = 1 \pmod{2}.$$

Помимо этого полином 4-й степени может раскладываться в произведение полиномов второй степени. Если у него нет при этом корней, то в разложении на полиномы второй степени

должны быть только неприводимые многочлены. Получается, что необходимо вычеркнуть только многочлен

$$f(x) = (1 + x + x^2) \cdot (1 + x + x^2) = 1 + x^2 + x^4.$$

Остаются следующие многочлены:

$$1 + x + x^4, \quad 1 + x^3 + x^4, \quad 1 + x + x^2 + x^3 + x^4.$$

Эти полиномы и будут дополнять список всех неприводимых степени не больше четырех.

Мы же теперь понимаем, что есть неразложимые элементы, а есть разложимые элементы. В целых числах мы могли любое число разложить на простые. А в общем евклидовом случае получиться ли так сделать? Ответ в следующем разделе. Мы введем понятие факториального кольца и обсудим общие свойства колец многочленов как факториальных колец.

### 3.4.4 Факториальное кольцо: определение, свойства

Начнем сразу с самого главного.

**Теорема 3.4.34** (основная теорема арифметики для евклидова кольца). В евклидовом кольце любой элемент можно разложить в произведение неразложимых элементов. Это разложение единственно с точностью до умножения на обратимый элемент.

Эта теорема верна не только в евклидовом кольце, так что имеет смысл дать следующее определение.

**Определение 3.4.35.** Будем говорить, что область целостности  $R$  **факториальна**, если в нем выполняется основная теорема арифметики.

**Пример 3.4.36.** Так как все евклидовы кольца факториальны, то  $\mathbb{Z}$  и  $\mathbb{F}[x]$  факториальны.

Из факториальных колец можно делать новые факториальные кольца.

**Теорема 3.4.37.** Если  $R$  факториально, то  $R[x]$  тоже факториально.

На этом связь с теорией чисел не кончается. Мы знаем, что такое НОД в евклидовых кольцах, поэтому имеет смысл понятие *взаимной простоты* двух элементов.

**Теорема 3.4.38** (китайская теорема об остатках для евклидова кольца). Если  $a, b$  взаимно просты в евклидовом кольце  $R$ , то имеет место изоморфизм

$$R/(ab) \cong R/(a) \oplus R/(b).$$

*Доказательство.* Из свойств факториальности евклидова кольца мы можем вынести, что элемент делится на два взаимно простых числа тогда и только тогда, когда он делится на их произведение. Есть отображение

$$\pi: R \rightarrow R/(a) \oplus R/(b),$$

которое каждому элементу кольца сопоставляет соответствующий вычет по идеалу  $(a)$  и  $(b)$ . Из-за свойства, описанного выше, ядро состоит ровно из тех элементов, что делятся на произведение  $ab$ , то есть  $\text{Ker } \pi = (ab)$ . Отсюда по первой теореме о гомоморфизме получаем искомый изоморфизм. ■

Видно, что и алгоритм Евклида, и основная теорема арифметики, и китайская теорема об остатках — все находит свое отражение в евклидовых кольцах и обобщает случай целых чисел. В следующем разделе мы с помощью факторкольца  $\mathbb{F}[x]/(f)$  будем расширять поля. Для этого нужно очень хорошо понимать теорию делимости многочленов, базу которой мы и разобрали выше.

## Домашнее задание

**Задача 3.4.1.** Является ли евклидовым кольцо

$$\mathbb{Z}[j] = \{a + bi : a, b \in \mathbb{Z}, j^2 + 6 = 0\}?$$

**Задача 3.4.2.** Найдите наибольший общий делитель многочленов  $x^{48} - 1$  и  $x^{20} - 1$ .

**Задача 3.4.3.** Проверьте на простоту элементы  $17, 11, 2 + 3i$  в кольце  $\mathbb{Z}(i)$ .

**Задача 3.4.4.** а) Привести пример коммутативного кольца с единицей, в котором некоторый неприводимый элемент порождает идеал, не являющийся простым. б) Привести пример коммутативного кольца с единицей, в котором некоторый простой идеал не является идеалом, порожденным простым элементом.

**Задача 3.4.5.** Найдите все неприводимые многочлены степени  $\leq 2$  в  $\mathbb{F}_3[x]$ .

**Задача 3.4.6.** Покажите, что над любым полем  $\mathbb{F}$  множество неприводимых многочленов в  $\mathbb{F}[x]$  бесконечно.

**Задача 3.4.7.** Приведите пример коммутативного кольца с единицей, в котором разложение на простые множители неоднозначно.

**Задача 3.4.8.** Докажите, что в факториальном кольце все неприводимые элементы являются простыми.

**Задача 3.4.9.** Докажите, что поле  $\mathbb{F}$  факториально.

**Задача 3.4.10.** Приведите пример не евклидова кольца главных идеалов.

**Бонусная задача.** а) *Радикалом идеала  $I$*  называется множество элементов кольца  $R$ , которые при возведении в какую-то натуральную степень  $n$  дают элемент идеала  $I$ . Докажите, что пересечение всех простых идеалов, содержащих идеал  $I$ , совпадает с радикалом идеала  $I$ . б) Покажите, что идеал совпадает со своим радикалом тогда и только тогда, когда факторкольцо по нему не будет содержать нильпотентов.

## Рекомендуемая литература

- [1] Журавлёв Ю. И., Флёров Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Раздел 10, 11.
- [2] Городенцев А. Л. — Алгебра. Учебник для студентов-математиков. Часть 1. — М.: МЦНМО, 2013. — Глава 2, §3, 4, 6.
- [3] Винберг Э. Б. — Курс Алгебры — 2-е изд., стереотип. — М.: МЦНМО, 2013. — Глава 3, §1-7, 10; глава 9, §2, 5.

## 3.5 Конечные поля

В этом разделе мы полностью классифицируем конечные поля. Для этого мы сначала покажем, какие поля точно не существуют. Потом объясним, почему поля соответствующего порядка существуют. После полной классификации конечных полей мы потратим немного бумаги и времени читателя на описание структуры конечного поля: его подполя и автоморфизмы.

**Ключевые слова:** векторное пространство, размерность пространства, расширение полей, поле разложения, бином двоешника, теорема о существовании конечного поля, теорема о кратных корнях, теорема о единственности конечного поля, подполе конечного поля, автоморфизм Фробениуса, критерий неприводимости многочлена над конечным полем.

### 3.5.1 Векторные пространства

Теория векторных пространств имеет большое значение в линейной алгебре и там она будем так же фундаментальна, как и основы теории колец в текущей главе. Между тем, мы дадим уже тут определение векторного пространства и сформулируем пару утверждений, которые понадобятся нам при классификации конечных полей. За отсутствием особого смысла обсуждать тут линейную алгебру мы оставим доказательства утверждений до момента их появления в следующих главах.

**Определение 3.5.1.** Будем говорить, что  $V$  — это **векторное пространство над  $\mathbb{F}$** , если на этом пространстве заданы две операции

$$+: V \times V \rightarrow V, \quad \cdot: \mathbb{F} \times V \rightarrow V.$$

При этом эти две операции удовлетворяют аксиомам:

V1.  $(V, +)$  — это абелева группа;

V2. выполнены две дистрибутивности:

$$\forall \alpha_1, \alpha_2 \in \mathbb{F}, v_1, v_2 \in V: \alpha_1 \cdot (v_1 + v_2) = \alpha_1 \cdot v_1 + \alpha_1 \cdot v_2, \quad (\alpha_1 + \alpha_2) \cdot v_1 = \alpha_1 \cdot v_1 + \alpha_2 \cdot v_1;$$

V3. аналог ассоциативности, но не совсем:

$$\forall \alpha, \beta \in \mathbb{F}, v \in V: \alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v;$$

V4. умножение на единицу тривиально:  $\forall v \in V: 1_{\mathbb{F}} \cdot v = v$ .

**Замечание.** Элементы  $V$  называют *векторами*, а элементы  $\mathbb{F}$  называют *скалярами*. Нейтральный элемент по сложению называется *нулевым вектором*, но обычно обозначается так же, как ноль поля  $\mathbb{F}$ .

**Замечание.** Надо отметить, что сложение является бинарной операцией в том смысле, в котором мы привыкли смотреть на них. А вот вторая операция, которую называют умножением на скаляры, не является бинарной операцией, так как область определения ее не совпадает с  $V \times V$ .

**Пример 3.5.2.**  $\mathbb{F}^n$  — это векторное пространство над  $\mathbb{F}$ , где сложение определено так, как мы привыкли: по координатно. А умножение следующее:

$$\forall v = (v_1, v_2, \dots, v_n) \in \mathbb{F}^n \quad \forall \alpha \in \mathbb{F}: \alpha \cdot v \stackrel{\text{def}}{=} (\alpha v_1, \alpha v_2, \dots, \alpha v_n).$$

**Пример 3.5.3.** Если  $\mathbb{F} \subseteq \mathbb{K}$ , то есть  $\mathbb{K}$  — расширение поля  $\mathbb{F}$ , то  $\mathbb{K}$  является векторным пространством над  $\mathbb{F}$ . При этом оно может обладать очень разными свойствами, которые могут зависеть напрямую от порядка базиса этого пространства.

Стоит отметить, что определение линейной комбинации, линейно независимой системы и базиса так же просты, как и в линейной алгебре. Так что мы опустим их и перейдем к той сути, которая будет полезна для нашей науки.

Есть много свойств этого векторного пространства, которые совпадают с аналогичными свойствами  $\mathbb{R}^n$ . Мы не будем тратить на них бумагу и время читателя, так как это суть другого курса. Нам же будет интересны два утверждения.

**Теорема 3.5.4 (о базисе).** Если  $V$  — это векторное пространство над  $\mathbb{F}$ , то в  $V$  есть базис. Количество элементов в базисе инвариантно относительно выбора базиса.

**Замечание.** Так как размерность базиса инвариантна, то говорят, что  $V$  *конечномерно*, если в базисе конечно число векторов. Иначе это — *бесконечномерное пространство*. Размерность привычно обозначают через  $\dim_{\mathbb{F}} V$ .

**Пример 3.5.5.** Можем сразу привести пример, когда важно, размерность над каким полем мы смотрим. Так, по понятным причинам,  $\dim_{\mathbb{C}} \mathbb{C} = 1$ , так как в качестве базиса мы можем взять любой обратимый элемент. Однако  $\dim_{\mathbb{R}} \mathbb{C} = 2$ , так как нам надо уже взять два элемента для базиса (например, 1 и  $i$ ).

**Пример 3.5.6.**  $\mathbb{F}[x]$  — это бесконечномерное пространство над  $\mathbb{F}$ .

**Пример 3.5.7.**  $\mathbb{R}$  является расширением  $\mathbb{Q}$ , но это расширение несчетно, так что конечно в этом векторном пространстве есть базис (смотрите *базис Гамеля*), но никто еще не видел его.

**Утверждение 3.5.8.** В конечномерном векторном пространстве  $V$  над конечным полем  $\mathbb{F}$  будет ровно  $|\mathbb{F}|^n$  элементов.

А зачем нам эта теория? Чтобы понять, сколько элементов может быть в поле.

**Теорема 3.5.9** (о количестве элементов в конечном поле). В конечном поле характеристики  $p$  всегда  $p^n$  элементов,  $n \in \mathbb{N}$ .

**Доказательство.** Как мы знаем, характеристика соответствует размерности простого подполя. Так что в  $\mathbb{F}$  есть  $\mathbb{F}_p$  как подполе. Следовательно, мы можем посмотреть на него как на векторное пространство над  $\mathbb{F}_p$ . Так как в  $\mathbb{F}$  конечное количество элементов, то мы можем посчитать размерность этого поля как  $|\mathbb{F}_p|^{\dim_{\mathbb{F}_p} \mathbb{F}} = p^n$ . ■

**Следствие 3.5.10.** Если в конечном кольце имеется  $n$  элементов и  $n$  не является степенью простого числа, то это кольцо не является полем.

**Пример 3.5.11.** Равны ли  $3^{-1}$  и  $18^{-1}$  в поле из 25 элементов? Да, так как поле из 25 элементов обязательно содержит простое подполе  $\mathbb{F}_5$ , а по модулю 5 числа 3 и 18 совпадают.

Теорема о количестве элементов в конечном поле дает нам понять, что конечные поля точно ограничиваются полями простой характеристики с размерностью  $p^n$ . А есть ли всегда такие поля? На этот вопрос мы ответим дальше. Положительно ответим.

### 3.5.2 Поле разложения

Здесь мы покажем, что алгебраические расширения полей уменьшают число неприводимых многочленов. И с помощью индукции мы можем доказать, что любой многочлен мы можем разложить на линейные множители в некотором расширении.

Мы знаем, что в отличие от полиномиальных функций полиномы мы рассматриваем как последовательности коэффициентов. Поэтому если есть вложение  $\mathbb{F} \subseteq \mathbb{K}$ , то мы можем сопоставить многочлену  $f(x) \in \mathbb{F}[x]$  соответствующий многочлен в  $\mathbb{K}[x]$ . При этом по понятным причинам в разложении на неприводимые многочлены может только увеличиться число многочленов. А можем ли мы найти такое расширение, что все неприводимые делители нашего выбранного многочлена  $p(x)$  будут линейными? Об этом ниже.

**Определение 3.5.12.** Пусть  $p(x) \in \mathbb{F}[x]$ . Тогда **полем разложения**  $p(x)$  называется такое алгебраическое расширение  $\mathbb{F} \subseteq \mathbb{K}$ , что над  $\mathbb{K}$  многочлен  $p(x)$  раскладывается на линейные множители.

**Пример 3.5.13.** Рассмотрим  $x^2 - 1 \in \mathbb{Q}[x]$ . Этот многочлен раскладывается на линейные множители над  $\mathbb{Q}$ , так что его полем разложения будет являться  $\mathbb{Q}$ .

**Пример 3.5.14.** Многочлен  $x^2 + 1 \in \mathbb{R}[x]$  не раскладывается на линейные множители, но мы знаем, что можно добавить к  $\mathbb{R}$  элемент  $i$ , получив  $\mathbb{R}(i) = \mathbb{C}$ , что позволит нам разложить многочлен на линейные множители.

**Пример 3.5.15.** Рассмотрим многочлен  $x^4 + 1 \in \mathbb{Q}[x]$ . Немного подумав, можно понять, как его стоит раскладывать на множители над  $\mathbb{R}$ :

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1).$$

Мы видим, что необходимо уже добавить элемент  $\sqrt{2}$  в поле, чтобы мы смогли на квадратичные множители разложить. Но  $\mathbb{Q}(\sqrt{2})$  нам не хватит, так как квадраты все еще не будут раскладываться на линейные множители. Поэтому добавим  $i$  в это поле. Получим  $\mathbb{Q}(\sqrt{2}, i)$  и в этом поле уже:

$$x^4 + 1 = \frac{1}{4}(\sqrt{2}x - 1 - i)(\sqrt{2}x - 1 + i)(\sqrt{2}x + 1 - i)(\sqrt{2}x + 1 + i) \in \mathbb{Q}(\sqrt{2}, i)[x].$$

Мы видим, что для простых случаев мы можем ручками посчитать такое расширение поля, в котором разложение будет единственным. Но нам этого будет недостаточно. Мы хотим, чтобы любой многочлен имел такое разложение в некотором расширении. Иначе говоря, хотим, чтобы для каждого полинома существовало поле разложения.

**Теорема 3.5.16** (о поле разложения). Для любого многочлена  $f(x) \in \mathbb{F}[x]$  существует такое алгебраическое расширение поля  $\mathbb{F}$ , над которым многочлен будет раскладываться на линейные множители, то есть у любого многочлена существует поле разложения.

*Доказательство.* Мы знаем, что кольцо многочленов над полем факториально, так что достаточно показать, что существует поле разложения для любого неприводимого многочлена. А это просто: если есть неприводимый  $f(x)$ , то мы можем добавить  $\alpha$  к полю  $\mathbb{F}$ , считая, что это корень многочлена  $f(x)$ . Тогда  $f(x)$  будет иметь хотя бы один корень в  $\mathbb{F}(\alpha)$ , что позволяет продолжить рассуждения по индукции. ■

На самом деле имеет место большее утверждение: не только у любого многочлена существует поле разложения, но и любое конечное поле является некоторым алгебраическим расширением простого поля.

**Утверждение 3.5.17.** Если поле  $\mathbb{F}$  конечно и содержит  $q = p^n$  элементов, то найдется такой неприводимый  $p(x) \in \mathbb{F}_p[x]$ , что  $\mathbb{F} \cong \mathbb{F}_p[x]/(p(x))$ .

*Доказательство.* Мы знаем, что в  $\mathbb{F}^*$  есть порождающий. Обозначим его через  $\alpha$ . Покажем, что как элементы векторного пространства над  $\mathbb{F}_p$  — простым подполем в  $\mathbb{F}$  — степени  $\alpha$  от нулевой до  $(n-1)$ -й линейно независимы.

Предположим, что это не так. Тогда существуют такие коэффициенты  $\lambda_i \in \mathbb{F}_p$ , что

$$\lambda_0 \cdot 1 + \lambda_1 \cdot \alpha + \dots + \lambda_{n-1} \cdot \alpha^{n-1} = 0.$$

Можем без ограничения общности предполагать, что  $\lambda_{n-1} \neq 0$ . Тогда выразим  $\alpha^{n-1}$  через другие  $\alpha$  меньшей степени. За счет этого выражения мы можем все степени  $\alpha$  выразить в виде линейных комбинаций первых  $n-2$  степеней. А их строго меньше, чем  $q$ , что приводит нас к противоречию.

Получается, что первые  $n$  степеней  $\alpha$  образуют базис пространства  $\mathbb{F}$  над  $\mathbb{F}_p$ . Следовательно, добавление  $\alpha^n$  превратит базис в линейно зависимую систему, а следовательно,  $\alpha$  является корнем некоторого уравнения  $n$ -й степени над  $\mathbb{F}_p$ . Легко показать, что этот многочлен будет неприводим (иначе  $\alpha$  все-таки оказался корнем некоторого уравнения меньшей степени). Это и есть многочлен  $p(x)$  из условия. Необходимый изоморфизм здесь очевиден: переводим  $\alpha$  в  $[x]_{(p(x))}$ . Оставим для читателя доказательство того, что такое отображение действительно является изоморфизмом. ■

**Упражнение.** Докажите, что отображение из доказательства выше является изоморфизмом.

**Пример 3.5.18.** Существует ли такой многочлен  $f(x) \in \mathbb{F}_2[x]$  степени 10, что в его любом поле разложения не менее  $2^{30}$  элементов? Для ответа на этот вопрос представим, что  $f$  раскладывается в произведение неприводимых многочленов степени 2, 3, 5. В таком случае, чтобы в  $\mathbb{F}_q$  он имел разложение в линейные множители, необходимо, чтобы  $q = 2^n$  и  $n$  делилось на все порядки неприводимых, входящих в  $f(x)$ . Следовательно, их должно быть не менее  $2^{30}$ .

Вам могут показаться безобидными эти утверждения. Как бы не так! Они имеют такие последствия. Давайте проследим за ними и поймем, что в конце этой дороги есть полная классификация конечных полей.

### 3.5.3 Конечные поля: существование и единственность

Как обычно, мы начнем с простого.

**Утверждение 3.5.19** (бином двоешника). Если  $\text{char } \mathbb{F} = p$ , то  $\forall x, y \in \mathbb{F}: (x + y)^p = x^p + y^p$ .

*Доказательство.* Так как поле является коммутативным кольцом, то в нем верен обычный бином Ньютона:

$$(x + y)^p = \sum_{i=0}^p C_p^i x^i y^{p-i}.$$

Заметим, что каждое  $C_p^i$  делится на  $p$ , если  $i \in \overline{1, p-1}$ . Почему? По определению в числителе биномиального коэффициента стоит выражение кратное  $p$ , а в знаменателе стоят числа, которые по модулю меньше  $p$ , которые взаимно прости с  $p$  в силу его простоты. Из-за этого, рассматривая бином Ньютона, мы можем сократить на все слагаемые, кроме крайних:

$$(x + y)^p = x^p + y^p \pmod{p}.$$

■

**Следствие 3.5.20.** По индукции мы можем заменить степень на  $q = p^n$ , то есть

$$\text{char } \mathbb{F} = p \Rightarrow \forall x, y \in \mathbb{F}: (x + y)^q = x^q + y^q.$$

Неожиданно такое простое комбинаторное утверждение приводит к вполне алгебраическим свойствам поля.

**Теорема 3.5.21** (о существовании конечного поля). Пусть  $\mathbb{K}$  — это поле разложения для  $f(x) = x^q - x \in \mathbb{F}[x]$ . При этом  $\text{char } \mathbb{F} = p$ . Тогда множество корней этого уравнения образуют подполе в  $\mathbb{K}$ .

*Доказательство.* Следствие из бинома двоешника показывает, что корни многочлена  $f(x)$  замкнуты относительно сложения. Достаточно просто проверить, что относительно умножения они тоже замкнуты. Кроме этого ноль и единица тоже удовлетворяют этому уравнению. Из этих утверждений в силу конечности поля получается, что действительно множество корней образуют подполе. ■

**Замечание.** Будем обозначать поле корней через  $\mathbb{F}_q$ .

Покажем, что существование поля определенного порядка может дать невероятное следствие для группы  $S_n$ .

**Пример 3.5.22.** Посмотрим на  $\mathbb{F}_8$ . Рассмотрим множество аффинных отображений

$$\varphi_{a,b}: \mathbb{F}_8 \rightarrow \mathbb{F}_8, \quad x \mapsto ax + b.$$

Если  $a \neq 0$ , то такое отображение биективно, а значит лежит в  $S_8$ . Всего таких отображений  $7 \cdot 8 = 56$ . Легко проверить, что композиция аффинных отображений — это аффинное отображение. Таким образом, множество аффинных отображений образует подгруппу порядка 56 в группе  $S_8$ .

А теперь, после этих рассуждений, попробуйте доказать существование подгруппы порядка 56 в  $S_8$  из общеалгебраических рассуждений. Это непросто (минимальное количество порождающих равно 4-м).

А сколько элементов в этом подполе? Понятно, что там есть все простое подполе, так как есть единица. Следовательно, в  $\mathbb{F}_q$  число элементов, кратное  $p$ . Однако могло так произойти, что некоторые элементы повторяются в разложении  $x^q - x$ . Как же с этим справиться?

Покажем, что повторяться корни не могли.

Для этого вспомним обычную производную у многочлена. Эта производная инвариантно действует на множестве многочленов, то есть переводит один многочлен в другой многочлен. Так что мы можем говорить, что это отображение из  $\mathbb{F}[x]$  в себя. Обозначим ее через  $D$ . Тогда имеет место следующая теорема.

**Теорема 3.5.23** (о кратных корнях).  $f(x) \in \mathbb{F}[x]$  не имеет кратных корней тогда и только тогда, когда  $f(x)$  и  $Df(x)$  взаимно просты.

**Следствие 3.5.24.** В поле  $\mathbb{F}_q$  ровно  $q$  корней.

*Доказательство.* Легко проверить, что

$$D(x^q - x) = q \cdot x^{q-1} - 1 = -1 \pmod{p}.$$

Видно, что производная взаимно проста с любым многочленом и с самим многочленом  $x^q - x$  тоже. Так что из утверждения выше следует, что кратных корней у многочлена нет. А так как их ровно  $q$ , то мы получаем поле из  $q$  элементов. ■

Отлично, мы показали, что для любой степени простого числа существует поле соответствующего порядка. Но может поля одного порядка будут различны. Оказывается, что нет: конечные поля одинакового порядка всегда изоморфны.

Для дальнейших рассуждений об изоморфизме полей, необходимо доказать одно из интереснейших свойств многочлена  $x^q - x$ .

**Утверждение 3.5.25.** Многочлен  $x^q - x$  делится на любой неприводимый многочлен степени  $n$  над  $\mathbb{F}_p$ .

*Доказательство.* Пусть  $f(x) \in \mathbb{F}_p[x]$  имеет степень  $n$  и неприводим. Тогда  $\mathbb{F}_p[x]/(f) = \mathbb{K}$  — это поле из  $q = p^n$  элементов. Каждый его элемент удовлетворяет уравнению  $x^q - x = 0$ . Так как корней ровно  $q$ , то мы можем сказать, что

$$x^q - x \equiv 0 \pmod{(f)},$$

что в точности означает делимость левого многочлена на правый. ■

Теперь покажем, что все поля одинаковой размерности изоморфны.

**Теорема 3.5.26** (о единственности конечного поля). Если в поле  $\mathbb{F}$  ровно  $q = p^n$  элементов, то оно изоморфно  $\mathbb{F}_q$ .

*Доказательство.* Мы знаем, что  $\mathbb{F} \cong \mathbb{F}_p[x]/(p(x))$ . При этом этот многочлен  $p(x)$  неприводим и имеет степень  $n$ , что по доказанному утверждению позволяет нам сказать, что имеет место делительность  $p(x) \mid x^q - x = h(x)$ .

Так как  $h(x)$  над  $\mathbb{F}_q$  разлагается на линейные множители, то и  $p(x)$  будет раскладываться на линейные множители над  $\mathbb{F}_q$ . Следовательно, у  $p(x)$  есть корень  $\alpha$  в этом поле. В силу неприводимости  $p(x)$  добавление к полю  $\mathbb{F}_p$  корня  $\alpha$  делает из него поле размерности  $q$ , то есть  $\mathbb{F}_q \cong \mathbb{F}_p(\alpha)$ . При этом в силу той же неприводимости  $p(x)$  мы получаем, что

$$\mathbb{F}_p[x]/(p(x)) \cong \mathbb{F}_p(\alpha) \cong \mathbb{F}_q.$$

■

**Следствие 3.5.27.** Все конечные поля одного порядка изоморфны.

**Пример 3.5.28.** Построим явно изоморфизм полей  $\mathbb{F}_5[x]/(x^2 - 2)$  и  $\mathbb{F}_5[x]/(x^2 - 3)$ . Для этого нам нужно найти в первом кольце корень для уравнения  $t^2 - 3 = 0$ . Для этого преобразуем его:

$$0 \equiv x^2 - 2 \equiv x^2 + 20x + 16 - 18 \equiv (x + 4)^2 - 3 \pmod{\mathbb{F}_5}.$$

Получается, что в первом поле корнем уравнения  $t^2 - 3$  будет  $x + 4$ . Поэтому искомый изоморфизм выглядит так (на другие элементы он продолжается по линейности):

$$\varphi([0]) = [0], \quad \varphi([1]) = [1], \quad \varphi([x]) = [x + 4].$$

Поля различного порядка не изоморфны, так как порядок поля инвариантен при изоморфизме. Это замечание оканчивает классификацию конечных полей. Давайте соединим все утверждения в одну теорему.

**Теорема 3.5.29** (о классификации конечных полях). Конечное поле  $\mathbb{F}$  обязательно имеет порядок  $q = p^n$ . И для каждого такого  $q$  существует ровно одно поле  $\mathbb{F}_q$  (с точностью до изоморфизма).

Этот подраздел оканчивается на этой высокой ноте. Следующие подразделы описывают разные свойства полей: вложение одних полей в другие поля, автоморфизмы полей.

### 3.5.4 Подполя в конечных полях

Тут мы покажем, когда поле  $\mathbb{F}_{p^k}$  мы можем вложить в  $\mathbb{F}_{p^n}$ . Для начала покажем, какое есть необходимое условие для вложения одного поля внутрь другого. После этого мы посмотрим опять на многочлен  $x^q - x$ , где  $q = p^n$  и увидим, что из разложения на неприводимые множители этого многочлена следует существование некоторых подполей в  $\mathbb{F}_q$ . Начнем.

**Утверждение 3.5.30.** Пусть  $\mathbb{F} \subseteq \mathbb{K}$  — два конечных поля. Покажем, что существует такое  $d$ , что  $|\mathbb{K}| = |\mathbb{F}|^d$ .

*Доказательство.* Если  $\mathbb{F}$  подполе, то мы можем смотреть на  $\mathbb{K}$  как на векторное пространство над  $\mathbb{F}$ . Из свойств векторного пространства следует искомое. ■

**Следствие 3.5.31.** Если  $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^n}$ , то  $k \mid n$ .

Необходимое условие получили. Покажем, что оно и достаточно.

**Теорема 3.5.32.** Неприводимый многочлен  $f(x) \in \mathbb{F}_p[x]$  является делителем  $x^q - x$  тогда и только тогда, когда  $\deg f \mid n$ .

*Доказательство.* Покажем, что любой  $f(x)$  — неприводимый делитель  $x^q - x$  имеет степень, делящую  $q$ . Для этого вспомним, что  $\mathbb{F}_q$  является полем разложения  $x^q - x$ , поэтому и для всех делителей этого многочлена поле будет являться полем разложения. Возьмем  $f(x)$ . Этот многочлен неприводим над  $\mathbb{F}_p$  и раскладывается на линейные множители над  $\mathbb{F}_q$ . Из-за этого есть такой  $\alpha \in \mathbb{F}_q$ , который является корнем  $f(x)$ . В силу неприводимости  $f(x)$  мы имеем, что  $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_q$  имеет ровно  $p^{\deg f(x)}$  корней. Из утверждения выше получаем, что  $\deg f | n$ .

Теперь в обратную сторону. Пусть  $\deg f = k | n$ . То, как мы доказывали выше, многочлен  $f(x)$  делит многочлен  $x^{p^k} - x$ . А этот многочлен уже делит многочлен  $x^q - x$ , как можно напрямую показать. Остается воспользоваться транзитивностью отношения делимости. ■

**Следствие 3.5.33.**  $\mathbb{F}_{p^k}$  можно вложить в  $\mathbb{F}_{p^n}$  тогда и только тогда, когда  $k | n$ .

*Доказательство.* Необходимость этого условия доказана. Достаточность следует из следующих рассуждений.

Найдется такой неприводимый многочлен  $p(x)$ , что  $\mathbb{F}_{p^k} \cong \mathbb{F}_p[x]/(p(x))$ . Так как степень  $\deg p = k | n$ , то этот многочлен является делителем  $x^q - x$ . Следовательно, над полем  $\mathbb{F}_{p^n}$  он раскладывается на линейные множители. Поэтому в этом поле есть корень  $\alpha$  этого многочлена, откуда мы получаем, что

$$\mathbb{F}_{p^k} \cong \mathbb{F}_p[x]/(p(x)) \cong \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}.$$

■

Итак, мы теперь знаем все, что можно знать о структуре конечных полей. Любое конечное поле имеет характеристику  $p$  и  $q = p^n$  элементов. Притом такое поле единственно. В каждом поле есть под поля, состоящие из  $p^k$  элементов, где обязательно  $k | n$ . Притом такое подполе единственно, так как это в точности решения уравнения  $x^{p^k} - x$ .

В следующем подразделе мы еще изучим группу симметрий конечного поля. И на этом уже точно полностью познаем то, как устроены конечные поля.

### 3.5.5 Автоморфизмы конечных полей. Автоморфизм Фробениуса

Здесь мы покажем, что есть автоморфизм Фробениуса определенного вида, что этот автоморфизм делает с корнями уравнения. В заключение этого подраздела будет доказательство того, что любой автоморфизм поля есть композиция автоморфизмов Фробениуса.

**Определение 3.5.34.** Пусть  $\mathbb{F}_q$  характеристики  $p$ . Будем называть отображение  $F$  **автоморфизмом Фробениуса**, если он имеет вид:

$$F: \mathbb{F}_q \rightarrow \mathbb{F}_q, \quad x \mapsto x^p.$$

Для начала покажем, что название этого отображения отражает его сущность: это автоморфизм.

**Утверждение 3.5.35.** Отображение  $F$  является автоморфизмом  $\mathbb{F}_q$ .

*Доказательство.* Нам надо показать: гомоморфность отображения и биективность. Для первого у нас все есть: надо только вспомнить бином двоешника:

$$\forall x, y \in \mathbb{F}_q: F(xy) = (xy)^p = x^p \cdot y^p, \quad F(x + y) = (x + y)^p = x^p + y^p.$$

Чтобы показать биективность, можно показать инъективность этого отображения, так как поле конечно. Для этого достаточно показать, что гомоморфизм имеет нулевое ядро:

$$\forall x \in \text{Ker } F: x^p = 0 \Rightarrow x = 0,$$

где последний переход имеет место быть, так как поле не содержит делителей нуля. ■

**Пример 3.5.36.** Пусть  $a$  — порождающий мультиликативной группы поля  $\mathbb{F}_{32}$ . Найдем наименьшую степень многочлена из  $\mathbb{F}_2[x]$ , корнями которого являются  $a^3, a^9, a^{15}$ .

Как мы знаем, у неприводимого делителя все корни будут являться степенями одного из корней, так что мы можем явно выписать все корни каждого из неприводимых делителей:

$$\begin{aligned} p_1(x) &= (x - a^3)(x - a^6)(x - a^{12})(x - a^{24})(x - a^{17}), \\ p_2(x) &= (x - a^9)(x - a^{18})(x - a^5)(x - a^{10})(x - a^{20}), \\ p_3(x) &= (x - a^{15})(x - a^{30})(x - a^{29})(x - a^{27})(x - a^{23}). \end{aligned}$$

Отлично, у нас теперь есть автоморфизм. Неожиданно он обладает очень удачным свойством, которое позволит нам не только решить пару интересных задач, но и даст нам ключ к пониманию, как выглядит произвольный автоморфизм поля  $\mathbb{F}_q$ .

**Теорема 3.5.37.** Если  $\alpha \in \mathbb{F}_{p^n}$  — это корень неприводимого над  $\mathbb{F}_p$  многочлена  $f(x)$  степени  $k$ , где  $k \mid n$ , то  $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{k-1}}$  — это все различные корни многочлена  $f(x)$ .

*Доказательство.* Заметим, что порядок группы обратимых элементов поля  $\mathbb{F}_p$  равен  $p - 1$ , поэтому для всех элементов  $\alpha$  простого подполя выполнено

$$\alpha^p = \alpha \Rightarrow \forall f(x) \in \mathbb{F}_p[x]: f(x)^p = f(x^p),$$

где последнее доказывается так же, как и бином двоешника.

Отсюда следует, что если  $\alpha$  — корень многочлена  $f(x)$ , то и  $\alpha^p$  тоже корень этого многочлена:

$$f(\alpha^p) = f(\alpha)^p = 0^p = 0.$$

Следовательно, все степени, перечисленные в условии являются корнями полинома  $f(x)$ . Но они могут совпадать. Чтобы показать, что это не так, заметим, что если в орбите действия  $F$  на  $\alpha$  ровно  $t$  элементов, то  $\alpha$  удовлетворяет уравнению  $x^{p^m} - x = 0$ , то последний многочлен должен делиться на  $f(x)$ , откуда следует, что  $t \geq k$ . Однако больше  $k$  корней у уравнения  $k$ -й степени над полем быть не может, поэтому их ровно  $k$  и они перечислены в условии. ■

**Замечание.** В этой теореме мы брали неприводимые многочлены степени, делящей  $n$ , так как мы знаем, что такие и только такие многочлены имеют корень в  $\mathbb{F}_q$ .

**Следствие 3.5.38.** Множество неподвижных точек автоморфизма Фробениуса — это в точности простое подполе  $\mathbb{F}_p \subseteq \mathbb{F}_q$ .

Представьте себе. Мы рассмотрели автоморфизм и оказалось, что действие этого автоморфизма на корнях неприводимых многочленов над  $\mathbb{F}_p$  степени  $k \mid n$  просто: он переставляет циклически эти корни. Удивительное рядом!

**Пример 3.5.39.** Укажем степени неприводимых делителей многочлена  $f(x) = x^{28} - 1 \in \mathbb{F}_3[x]$ . Заметим, что элемент  $x$  поля  $\mathbb{F}_{3^n}$  будет являться корнем этого многочлена тогда и только тогда, когда его порядок делит 28. При этом если в разложении присутствует неприводимый многочлен порядка  $d$ , то его корень встречается первый раз в  $\mathbb{F}_{3^d}$ . Поэтому для решения этой задачи необходимо находить такие  $n$ , где первый раз встречается корни нашего многочлена. Чтобы удостовериться, что найденные корни соответствуют действительно неприводимым многочленам нужной степени, мы будем их возводить в 3-ю степень и смотреть, сколько различных корней мы получаем. Формальная правильность таких действий следует из свойств автоморфизма Фробениуса.

Начнем. В поле  $\mathbb{F}_3$  мы находим два корня, которые соответствуют линейным многочленам, делящим  $f(x)$ . Так как  $f(x)$  взаимно прост со своей производной, кратных корней у него нет.

Далее в поле  $\mathbb{F}_9$  мы находим неприводимый делитель  $f(x)$ , корни которого имеют вид:  $\alpha^2$  и  $\alpha^6$ , где  $\alpha$  — порождающий элемент мультиликативной группы поля.

При подсчете мы видим, что вплоть до  $n = 6$  новых корней нет. А вот в последнем случае мы получаем четыре неприводимых делителя степени 6, корни которых мы можем выразить так с помощью порождающего  $\alpha$ :

$$\begin{aligned} p_1(x) &: \alpha^{26}, \alpha^{78}, \alpha^{234}, \alpha^{702}, \alpha^{650}, \alpha^{494}; \\ p_2(x) &: \alpha^{52}, \alpha^{156}, \alpha^{468}, \alpha^{676}, \alpha^{572}, \alpha^{260}; \\ p_3(x) &: \alpha^{104}, \alpha^{312}, \alpha^{208}, \alpha^{624}, \alpha^{416}, \alpha^{520}; \\ p_4(x) &: \alpha^{130}, \alpha^{390}, \alpha^{442}, \alpha^{598}, \alpha^{338}, \alpha^{286}. \end{aligned}$$

Но это еще не все. Мы покажем, что любой автоморфизм переводит корень неприводимого многочлена в его корень (с некоторыми уточнениями). Хотя это действие не будет циклическим, но оно будет обладать еще более удивительным свойством: действие автоморфизма будет совпадать с действием некоторой степени автоморфизма Фробениуса. Покажем это.

**Теорема 3.5.40.** Если  $\varphi: \mathbb{F}_q \rightarrow \mathbb{F}_q$  — это автоморфизм, то найдется такое  $k \in \mathbb{N}$ , что  $\varphi = F^k$ .

*Доказательство.* Для начала покажем, что автоморфизм  $\varphi$ , как и автоморфизм  $F$  имеет среди неподвижных точек все точки простого подполя. Заметим, что 0 сохраняется, так как  $\varphi$  — это гомоморфизм. Кроме этого, так как поле конечно, то единица переходит в единицу. Следовательно, для любого  $i \in \mathbb{F}_p$ :

$$\varphi(k) = \varphi(1 + 1 + \dots + 1) = 1 + \dots + 1 = k.$$

Так как все коэффициенты многочлена  $f(x) \in \mathbb{F}_p[x]$  переходят в себя, то и корень  $\alpha$  этого многочлена перейдет в какой-то другой корень. Будем считать, что  $f(x)$  — это неприводимый многочлен степени  $n$ . Тогда по доказанному выше мы получаем, что

$$\exists k \in \mathbb{N}: \varphi(\alpha) = \alpha^{p^k} = F^k(\alpha).$$

Следовательно, действие  $\varphi$  и  $F^k$  совпадает на  $\alpha$ , но тогда это действие совпадает и на  $\mathbb{F}_p(\alpha)$  как на векторном пространстве над  $\mathbb{F}_p$ . Остается заметить, что  $\mathbb{F}_p(\alpha) = \mathbb{F}_q$ . ■

**Замечание.** Как видим из доказательства выше, мы можем принять даже, что  $k$  — это некоторое натуральное число из промежутка  $\overline{0, n-1}$ .

**Пример 3.5.41.** Найдите количество нильпотентных элементов в кольце

$$\mathbb{F}_7[x]/(x^{14} + x^7 + 2) = \mathbb{F}_7[x]/(f(x)).$$

Для начала разложим  $f(x)$  на множители:

$$x^{14} + x^7 + 2 = x^{14} - 6x^7 + 9 = (x^7 - 3)^2 = (x^7 - 3^7)^2 = (x - 3)^{14} \pmod{\mathbb{F}_7}.$$

Видим, что нильпотентами будут те и только те полиномы, у которых среди корней будет 3. А их будет  $7^{13} - 1$ , так как 0 не считается нильпотентом.

Ух, на этом мы можем поставить точку в изучении конечных полей. Есть еще много интересных тем, которые относятся к алгебре, но они не относятся к этому курсу, так что мы опустим их.

## Домашнее задание

**Задача 3.5.1.** Про элементы  $x, y$  поля из 169 элементов известно, что  $x = 2y$ . Следует ли из этого равенства  $12x = 37y$ ?

**Задача 3.5.2.** а) Доказать, что в любом поле характеристики 2 уравнение  $x^2 + x + 1$  либо имеет ровно 2 различных корня, либо не имеет корней вовсе. б) Сколько решений имеет уравнение  $x^2 + x + 1$  в поле из 512 элементов?

**Задача 3.5.3.** Найдите подгруппу порядка 72 в  $S_9$ .

**Задача 3.5.4.** Найдите все гомоморфизмы  $\mathbb{F}_{81}$  в кольцо вычетов  $\mathbb{Z}_{81}$ .

**Задача 3.5.5.** Найдите наименьшее конечное поле характеристики 2, в котором многочлен  $x^{14} + 1$  раскладывается на линейные множители.

**Задача 3.5.6.** а) Элемент  $a$  порождает мультиликативную группу поля  $\mathbb{F}$  из 343 элементов. Является ли многочлен  $x^2 + ax - a + 2a^2$  неприводимым в кольце многочленов  $\mathbb{F}[x]$ ? б) Известно, что минимальный многочлен элемента  $a \in \mathbb{F}_4$  равен  $x^2 + x + 1$ . Следует ли из этого, что многочлен  $x^3 + ax^2 + a$  неприводим в кольце  $\mathbb{F}_4[x]$ ?

**Задача 3.5.7.** Укажите степени неприводимых делителей многочлена  $x^5 - 2$  из кольца  $\mathbb{F}_{67}[x]$ .

**Задача 3.5.8.** Найдите количество решений уравнения  $f(x) = 0$  в поле из  $q$  элементов. а)  $f(x) = x^{25} + x^5 + x - 1$ ;  $q = 125$ ; б)  $f(x) = x^{25} + x^5 + x - 1$ ;  $q = 625$ ; в)  $f(x) = x^{26} + x^8 + x^2 + 1$ ;  $q = 81$ .

**Задача 3.5.9.** а) Пусть  $a \in \mathbb{F}_{121}$  — корень многочлена  $x^2 - 2x + 4$  в поле из 121 элемента. Найдите всевозможные значения  $a^{12}$ . б) Тот же вопрос для многочлена  $x^2 + 6x + 4$ .

**Задача 3.5.10.** Проверьте, является ли полем кольцо вычетов  $\mathbb{F}_{11}[x]/(x^{11} - x + 1)$ .

**Бонусная задача.** а) Покажите, что количество нормированных (с коэффициентом 1 у старшей степени) неприводимых многочленов степени  $n$  над полем  $\mathbb{F}_p$  удовлетворяет формуле

$$N_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d},$$

где  $\mu(d)$  — это стандартная функция Мебиуса. б) Докажите, что из полученной формулы следует существование полей  $\mathbb{F}_q$ .

## Рекомендуемая литература

- [1] Журавлёв Ю. И., Флёрков Ю. А., Вялый М. Н. — Основы высшей алгебры и теории кодирования — Раздел 11.