

Министерство науки и высшего образования Российской Федерации
Ярославский государственный университет им. П.Г. Демидова

Н. В. Тимофеева

Алгебраические структуры

Часть 1

Учебное пособие

Ярославль
ЯрГУ
2021

УДК 512.5(075.8)
ББК В144я73
Т41

*Рекомендовано
Редакционно-издательским советом университета
в качестве учебного издания. План 2021 года*

Рецензенты:
кафедра «Высшая математика» ЯГТУ;
А.В. Ястребов, д-р пед. наук, проф.,
профессор кафедры математического анализа,
теории и методики обучения математике ЯГПУ им. К. Д. Ушинского

Тимофеева, Надежда Владимировна.

Т 41 **Алгебраические структуры. Часть 1** : учебное пособие /
Н.В. Тимофеева; Яросл. гос. ун-т им. П.Г. Демидова. – Яро-
славль : ЯрГУ, 2021. – 80 с.

ISBN 978-5-8397-1213-3

Пособие включает следующие разделы общей алгебры: множества и операции, моноиды и полугруппы, группы, кольца. Его целью является изложение общеалгебраических знаний, предусмотренных требованиями математической подготовки по специальности «Компьютерная безопасность». Пособие также полезно студентам магистратуры, изучающим курс «Фундаментальные алгебраические структуры». Кроме того, оно подойдёт для систематизации общеалгебраических знаний и справок по включённым в него разделам.

Предназначено для студентов математического факультета, изучающим общую алгебру.

УДК 512.5(075.8)
ББК В144я73

ISBN 978-5-8397-1213-3

© ЯрГУ, 2021

Оглавление

Введение	5
Глава 1. Множества, операции, арности	7
1.1 Множества и отображения	7
1.1.1 Первые понятия	7
1.1.2 Отношения и их виды. Эквивалентность и разбиение. Операции	12
1.2 Структуры алгебры (общие замечания)	16
Глава 2. группоиды, моноиды и полугруппы	17
2.1 Группоид. Полугруппа. Моноид	17
2.2 Гомоморфизмы и изоморфизмы группоидов, моноидов и полугрупп.	
Конгруэнция. Теоремы о гомоморфизме	19
2.3 Специальные элементы	21
Глава 3. Группы	23
3.1 Начальные знания о группах	23
3.1.1 Первые понятия	23
3.1.2 Циклические подгруппы и группы	25
3.1.3 Таблица Кэли и теорема Кэли	28
3.2 Подгруппы. Нормальность и факторгруппы. Гомоморфизмы и действия	29
3.2.1 Смежные классы относительно подгруппы. Теорема Лагранжа	29
3.2.2 Действие группы на множестве	30
3.2.3 Нормальная подгруппа. Факторгруппа	34
3.2.4 Ядро и образ гомоморфизма групп. Теорема о гомоморфизме для групп	36
3.2.5 Свойства нормальных подгрупп. Теоремы об изоморфизмах для групп	37
3.3 Образующие элементы группы. Свободная группа. Задание группы образующими и определяющими соотношениями	39
3.4 Прямое произведение групп. Разложение группы в прямое произведение	41
3.5 Конечно порождённые абелевы группы	44
3.5.1 Строение конечных абелевых групп	44
3.5.2 Строение конечно порождённых абелевых групп	47
3.6 Силовские подгруппы конечной группы. Теоремы Силова	48
3.6.1 Центр группы. Внутренние автоморфизмы группы. Централизаторы и уравнение классов	48
3.6.2 p -группы и теоремы Силова	50

3.7 Коммутаторы в группе. Коммутант	53
3.8 Разрешимые группы	54
Глава 4. Кольца	57
4.1 Кольца. Подкольца и идеалы. Факторкольца и гомоморфизмы	57
4.1.1 Понятие кольца	57
4.1.2 Образующие идеала	59
4.1.3 Обрыв возрастающих цепей идеалов в кольце главных идеалов	61
4.1.4 Условия конечности в кольцах	61
4.1.5 Прямое произведение колец. Разложение кольца в прямую сумму идеалов	63
4.1.6 Характеристика кольца с единицей	64
4.1.7 Обратимые элементы кольца. Тела и поля	65
4.1.8 Факторкольцо	67
4.1.9 Гомоморфизмы колец	68
4.2 Некоторые результаты из теории коммутативных колец	69
4.2.1 Область целостности	69
4.2.2 Поле частных целостного кольца	70
4.2.3 Простые и максимальные идеалы	71
4.2.4 Евклидовы кольца	74
4.3 Элементы теории делимости в областях целостности	75
4.3.1 Простые и неприводимые элементы области целостности	75
4.3.2 Факториальные кольца	76
Заключение	78
Литература	79

Введение

Основное содержание современной алгебры составляет исследование алгебраических систем, т. е. множеств с операциями. В данном пособии основное внимание уделено замкнутости изложения и единому подходу к изучению различных алгебраических систем. Это позволит всюду, где возможно, добиться максимальной предсказуемости развития сюжета. Пособие написано с целью сделать изучение алгебры по возможности простым, а её результаты – как можно более естественными и интуитивно приемлемыми.

Читателю полезно внимательно разбирать доказательства всех утверждений: в них расставлены акценты, помогающие понять причины тех или иных математических явлений. Примеры, кроме иллюстративной функции, несут ещё эвристическую нагрузку, часто предваряя введение новых понятий или формулировку достаточно общих результатов. Как правило, примеры выбраны очень простыми и максимально прозрачными. Некоторые из примеров содержат пропуски фрагментов, оставленных читателю для самостоятельной проработки. Эти пропуски нетрудно заполнить, используя приёмы рассуждений из предшествующего текста. Упражнения, включённые в текст, очень лёгкие. Их решение призвано показать технику доказательств в алгебре и дать необходимый навык ведения рассуждений на достаточном уровне математической строгости. Приёмы, демонстрируемые в доказательствах утверждений (теорем, предложений, лемм), затем «работают» в упражнениях и входят далее в качестве стандартных шагов в последующие рассуждения. Поэтому решать упражнения и разбирать примеры по мере их появления в тексте пособия очень полезно: это сэкономит усилия по изучению последующего материала. Степень подробности изложения рассуждений снижается при продвижении к концу каждой главы. Пособие рассчитано на активное сотрудничество со стороны читателя, хотя трудных (предполагающих применение неожиданных приёмов, либо сложных, либо трудоёмких) заданий в пособии нет.

Предполагается, что читатель свободно владеет основными понятиями теории многочленов над полями вещественных и комплексных чисел и основами теории векторных пространств, а также вычислениями в кольце целых чисел.

В качестве исходного материала для конструирования примеров мы будем часто использовать некоторые классические множества, обозначения которых являются традиционными. Это

- \mathbb{N} – натуральные числа $1, 2, 3, \dots, n, \dots$,
- \mathbb{N}_0 – целые неотрицательные числа $0, 1, 2, \dots, n, \dots$
- \mathbb{Z} – целые числа,
- \mathbb{Q} – рациональные числа,
- \mathbb{R} – вещественные (или действительные) числа,
- \mathbb{C} – комплексные числа.

В процессе работы будут введены и подробно описаны (вместе с «живущими» на них структурами) близкие к ним объекты, возможно, в той или иной мере уже знакомые читателю:

- $\mathbb{Z}[i]$ – целые гауссовы числа,
- $\mathbb{Q}[i]$ – рациональные комплексные числа,
- \mathbb{H} – кватернионы Гамильтона.

Также нам необходимы *кванторы*:

- \forall – *квантор общности*: этот символ имеет значение «для любого»,
- \exists – *квантор существования*: этот символ имеет значение «существует»,

логические связки:

- $\&$ (\wedge) – *и (знак конъюнкции)*,
- \vee – *или (знак дизъюнкции)*,

знаки импликации \Rightarrow , \Leftarrow

и знак эквиваленции \Leftrightarrow .

Пример 0.0.1. Примеры использования логической символики.

Формула	Прочтение
$A \Rightarrow B$	из A следует B (A влечёт B)
$A \Leftarrow B$	из B следует A (B влечёт A)
$A \Leftrightarrow B$	A эквивалентно B (A выполнено тогда и только тогда, когда выполнено B)

Глава 1

Множества, операции, аксиомы

Эта глава носит обзорный характер и содержит сведения, в основном известные читателю. Они приведены со справочными целями, а также с целью фиксации терминов и обозначений.

1.1 Множества и отображения

1.1.1 Первые понятия

В качестве *множества* мы будем рассматривать совокупность объектов, обладающих некоторым фиксированным признаком. Этот признак присущ объектам, принадлежащим рассматриваемому множеству, и не присущ объектам, не принадлежащим ему. Такое понимание множества восходит к основателю теории множеств Г. Кантору: «Под множеством мы понимаем объединение в одно целое определенных, вполне различных объектов нашей интуиции или нашей мысли».

Объект, принадлежащий множеству, называется *элементом* этого множества. Мы будем обозначать множества заглавными буквами латинского алфавита A, B, C, \dots, X, Y, Z , элементы – строчными буквами латинского алфавита a, b, c, \dots, x, y, z .

Например, можно рассматривать множество натуральных чисел, множество людей с рыжими волосами или множество автомобилей красного цвета в данном городе.

Понятно, что можно рассматривать множество, не содержащее ни одного элемента; такое множество называется *пустым*, и для него используют символ \emptyset . Запись $X = \emptyset$ означает, что X – пустое множество.

Описываемый подход к понятию множества является достаточным для всех дальнейших построений, однако он не безупречен с точки зрения логики. Это позволяет увидеть следующий

Парадокс Рассела.

Предположим, что все множества заданы одновременно. Пусть Q – множество всех множеств, не содержащих себя в качестве элемента. Содержит ли Q себя в качестве элемента?

Если это не так ($Q \notin Q$), то по определению множества Q получим $Q \in Q$ – противоречие. Если, наоборот, $Q \in Q$, то по определению множества Q будем иметь $Q \notin Q$ – снова противоречие.

Таким образом, в рамках «наивного» подхода к теории множеств невозможно считать все множества заданными одновременно.

Выход из данной ситуации вполне естественен – последовательное построение множеств разных «уровней». На каждом этапе построения доступна совокупность уже введенных в рассмотрение множеств, на базе которых формируются новые множества. При этом никакая совокупность множеств не может быть элементом себя самой. Точное описание этой конструкции проводится в подробных курсах математической логики

и выходит далеко за рамки данного пособия.

Множества X и Y называются *равными* (обозначение: $X = Y$), если они совпадают по составу, т. е. всякий элемент множества X принадлежит множеству Y , а всякий элемент множества Y принадлежит множеству X . Формально это можно записать так:

$$X = Y \Leftrightarrow (\forall x \in X \ x \in Y) \ \& \ (\forall y \in Y \ y \in X).$$

Множество X есть *подмножество* множества Y (обозначение: $X \subset Y$), если всякий элемент множества X принадлежит множеству Y . Это определение записывается так:

$$X \subset Y \Leftrightarrow \forall x \in X \ x \in Y.$$

Очевидно, любое множество является подмножеством в себе самом.

Множество X есть *собственное подмножество* множества Y (обозначение: $X \subsetneq Y$), если X – подмножество в Y и $X \neq Y$. Это определение записывается так:

$$X \subsetneq Y \Leftrightarrow (X \subset Y) \ \& \ (X \neq Y).$$

Пересечением $A \cap B$ множеств A и B называется множество

$$A \cap B = \{x \in A \mid x \in B\} = \{x \in B \mid x \in A\} = \{x \mid x \in A \ \& \ x \in B\}.$$

Объединением $A \cup B$ множеств A и B называется множество

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Дизъюнктное объединение $A \sqcup B$ имеет место, если $A \cap B = \emptyset$.

Замечание 1.1.1. Пересечение и объединение могут быть естественно определены для любых серий множеств. Серии множеств могут быть конечными или бесконечными.

Замечание 1.1.2. Понятия пересечения и объединения могут быть определены и использоваться в более частной ситуации, когда множества A и B являются подмножествами некоторого множества U : $A \subset U \supset B$.

Теоретико-множественная разность $A \setminus B$ определяется равенством

$$A \setminus B = \{x \in A \mid x \notin B\}.$$

В частности, если $A \subset U$, то теоретико-множественная разность $U \setminus A$ носит специальное название *дополнения* подмножества A во множестве U . Мы не будем использовать специального символа для дополнения.

В различных теоретико-множественных рассуждениях бывают полезными *формулы де Моргана* для серии подмножеств $X_\alpha \subset U$ множества U , пронумерованных индексами α из множества \mathbf{A} :

$$\begin{aligned} U \setminus \bigcup_{\alpha \in \mathbf{A}} X_\alpha &= \bigcap_{\alpha \in \mathbf{A}} (U \setminus X_\alpha), \\ U \setminus \bigcap_{\alpha \in \mathbf{A}} X_\alpha &= \bigcup_{\alpha \in \mathbf{A}} (U \setminus X_\alpha). \end{aligned}$$

Определение 1.1.3. *Декартовым, или прямым, произведением* множеств A и B называется множество

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

При это множества A и B называются соответственно *первым* и *вторым прямыми сомножителями* прямого произведения $A \times B$.

Очевидно, определение декартова произведения может быть распространено на любой конечный или бесконечный набор сомножителей.

Определение 1.1.4. Соответствием между множествами A и B называется подмножество $R \subset A \times B$.

Определение 1.1.5. Соответствие $R \subset A \times B$ называется *отображением*, или *функцией*, из A в B , если для любого $a \in A$ подмножество $r(a) = \{b \in B \mid (a, b) \in R\}$ состоит из одного элемента.

Для отображения используется запись следующего вида: $r: A \rightarrow B: a \mapsto r(a)$. В таком случае подмножество R называют *графиком отображения* r .

Например, прямое произведение множеств $X \times Y$ обладает двумя «забывающими» отображениями (*проекциями на прямые сомножители*)

$$X \xleftarrow{p_1} X \times Y \xrightarrow{p_2} Y,$$

которые определяются соответствиями

$$p_1: (x, y) \mapsto x; \quad p_2: (x, y) \mapsto y.$$

Пусть $f: X \rightarrow Y$ – отображение. Тогда множество X называется *областью определения* $\text{dom } f$ отображения f , Y – *областью значений* этого отображения. Для любого $x \in X$ элемент $f(x)$ называется *образом* элемента $x \in X$. Если $y = f(x)$, то элемент $x \in X$ называется *прообразом* элемента $y \in Y$. Также говорят о *полном прообразе* элемента $y \in Y$:

$$f^{-1}(y) = \{x \in X \mid f(x) = y\}.$$

Образ подмножества $A \subset X$ при отображении $f: X \rightarrow Y$ определяется выражением

$$f(A) = \{f(a) \mid a \in A\} \subset Y,$$

а прообраз подмножества $B \subset Y$ при отображении $f: X \rightarrow Y$ – выражением

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

В частности, подмножество $f(X)$ называется *образом отображения* $f: X \rightarrow Y$ и обозначается символом $\text{im } f$.

Под *композицией* отображений $f: X \rightarrow Y$ и $g: Y \rightarrow Z$ понимают их последовательное выполнение:

$$g \circ f: X \rightarrow Z: x \mapsto g(f(x)).$$

Предостережение: читателю необходимо обратить внимание на взаимосвязь порядка выполнения отображений

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

и порядка следования их символов в записи композиции $g \circ f$.

Чтобы два отображения f, g обладали композицией $g \circ f$, необходимо и достаточно, чтобы образ первого отображения (в порядке их применения) был подмножеством области определения второго отображения, т. е. чтобы выполнялось включение

$$\text{im } f \subset \text{dom } g.$$

Иногда бывает удобно записывать композицию отображений в виде диаграммы:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow g \circ f & \downarrow g \\ & & Z \end{array}$$

Говорят, что диаграмма

$$\begin{array}{ccc} A & \xrightarrow{c} & B \\ & \searrow b & \downarrow a \\ & & C \end{array}$$

коммутативна, если $b = a \circ c$. Иногда возникают последовательности, состоящие более чем из двух отображений. Например, композицию трёх отображений можно вычислять двумя различными способами:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow g \circ f & \downarrow g \\ T & \xleftarrow{h} & Z \end{array} \quad \begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow h \circ g & \downarrow g \\ T & \xleftarrow{h} & Z \end{array}$$

Обе композиции определены всякий раз, когда определены попарные композиции $g \circ f$ и $h \circ g$, и в действительности $h \circ (g \circ f) = (h \circ g) \circ f$. Поэтому композиция трёх или более последовательных отображений не зависит от порядка расстановки скобок, и имеет смысл рассматривать, например, диаграммы вида

$$\begin{array}{ccccc} & & X_2 & \cdots & X_{n-2} \\ & \nearrow f_2 & & & \searrow f_{n-1} \\ X_1 & & & & X_{n-1} \\ & \nwarrow f_1 & & & \nearrow f_n \\ & & X_0 & & X_n \end{array}$$

Если дано отображение $f: Y \rightarrow Z$ и X – подмножество в Y , то *ограничение*

$$f|_X: X \rightarrow Z$$

отображения f на подмножество X – это индуцированное отображение

$$f|_X: X \subset Y \xrightarrow{f} Z: x \mapsto f(x).$$

Бывают полезными следующие соотношения, которые нетрудно доказать непосредственным использованием определений. Для серии подмножеств $B_\gamma \subset Y$, $\gamma \in \Gamma$ и произвольного отображения $f: X \rightarrow Y$

$$\begin{aligned} f^{-1}\left(\bigcup_{\gamma \in \Gamma} B_\gamma\right) &= \bigcup_{\gamma \in \Gamma} \{f^{-1}(y) | y \in B_\gamma\} = \bigcup_{\gamma \in \Gamma} f^{-1}(B_\gamma), \\ f^{-1}\left(\bigcap_{\gamma \in \Gamma} B_\gamma\right) &= \bigcap_{\gamma \in \Gamma} \{f^{-1}(y) | y \in B_\gamma\} = \bigcap_{\gamma \in \Gamma} f^{-1}(B_\gamma). \end{aligned}$$

Для произвольных подмножеств $A \subset X$ и $B \subset Y$ имеют место включения

$$A \subset f^{-1}f(A), \quad ff^{-1}(B) \subset B,$$

а также равенство

$$f(A \cap f^{-1}(B)) = f(A) \cap B.$$

Определение 1.1.6. Отображение $f: X \rightarrow Y$ *инъективно* (равносильно, является *вложением*), если

$$\forall x_1, x_2 \in X (x_1 \neq x_2) \Rightarrow (f(x_1) \neq f(x_2)).$$

Отображение $f: X \rightarrow Y$ *сюръективно* (равносильно, является *наложением*), если

$$\forall y \in Y \exists x \in X : y = f(x).$$

Отображение $f: X \rightarrow Y$ *биективно* (равносильно, является *взаимно однозначным*), если оно инъективно и сюръективно.

Иными словами, отображение инъективно, если оно переводит различные элементы в различные, сюръективно, если его образ совпадает с областью значений, и биективно, если выполнены оба требования. Для инъективного отображения часто используется стрелка \hookrightarrow , для сюръективного – стрелка \twoheadrightarrow . При использовании каждой из этих стрелок отдельно в тексте не указывается на инъективность (соответственно, сюръективность) отображения.

Определение 1.1.7. Отображение называется *тождественным*, если оно имеет вид

$$\text{id}_X: X \rightarrow X : x \mapsto x.$$

Иными словами, тождественное отображение – это отображение, график которого представляет собой диагональ $\text{diag}(X) = \{(x, x) \mid x \in X\} \subset X \times X$.

Тождественные отображения характеризуются следующим поведением в композиции: для любого отображения $f: X \rightarrow Y$ выполнены тождества

$$\text{id}_Y \circ f = f, \quad f \circ \text{id}_X = f.$$

Пусть отображение $f: X \rightarrow Y$ биективно, т. е. инъективно и сюръективно. В силу сюръективности для любого $y \in Y$ прообраз непуст $f^{-1}(y) \neq \emptyset$, а в силу инъективности этот прообраз состоит из единственного элемента $x \in X$ такого, что $f(x) = y$. Таким образом, взятие прообразов относительно биективного отображения f определяет отображение

$$f^{-1}: Y \rightarrow X : y \mapsto f^{-1}(y),$$

причём выражение $f^{-1}(y)$ означает прообраз элемента $y \in Y$, состоящий из единственного элемента $x \in X$. Легко заметить, что

$$f \circ f^{-1} = \text{id}_Y, \quad f^{-1} \circ f = \text{id}_X. \quad (1.1.1)$$

Определение 1.1.8. Отображение $g: Y \rightarrow X$ называется *двусторонним обратным* к отображению $f: X \rightarrow Y$, если для отображений f и g выполнены тождества

$$f \circ g = \text{id}_Y, \quad g \circ f = \text{id}_X. \quad (1.1.2)$$

Понятно, что отображение, обладающее двусторонним обратным, биективно. Итак, имеем следующее

Предложение 1.1.9. Отображение $f: X \rightarrow Y$ биективно тогда и только тогда, когда оно обладает двусторонним обратным.

Отображение, обладающее двусторонним обратным, называется *обратимым*. Встречаются ситуации, когда для пары отображений $f: X \rightarrow Y$ и $g: Y \rightarrow X$ выполнено только одно из соотношений (1.1.2).

Определение 1.1.10. Отображение $g: Y \rightarrow X$ называется *сечением* отображения $f: X \rightarrow Y$, если для него выполнено соотношение

$$f \circ g = \text{id}_Y.$$

Например, для любого $x_2 \in X_2$ отображение $s_{x_2}: X_1 \rightarrow X_1 \times X_2: x_1 \mapsto (x_1, x_2)$ является сечением проекции $p_1: X_1 \times X_2 \rightarrow X_1$. Существуют и другие сечения этой же проекции.

1.1.2 Отношения и их виды. Эквивалентность и разбиение. Операции

Определение 1.1.11. *Бинарным отношением* на множестве X называется соответствие $R \subset X \times X$. Если $(x_1, x_2) \in R$, то говорят, что элемент x_1 *находится в отношении* R к элементу x_2 .

Замечание 1.1.12. Иногда наравне с записью $(x_1, x_2) \in R$ используют запись $x_1 R x_2$. В последнем случае часто вместо буквенного обозначения бинарного отношения (в нашем случае это R) используют какой-либо символ, обозначающий данное бинарное отношение. Например, традиционно используют запись $x = y$ для равенства чисел и запись $l \parallel m$ для параллельности прямых.

Теперь обратимся к бинарным отношениям специальных видов. Бинарные отношения, упоминаемые далее, могут не определять отображений.

Определение 1.1.13. Бинарное отношение $R \subset X \times X$

- *рефлексивно*, если $R \supset \text{diag}(X) = \{(x, x) | x \in X\}$;
- *симметрично*, если $(x_1, x_2) \in R \Rightarrow (x_2, x_1) \in R$;
- *транзитивно*, если $(x_1, x_2) \in R \& (x_2, x_3) \in R \Rightarrow (x_1, x_3) \in R$.

Бинарное отношение $R \subset X \times X$ называется *эквивалентностью*, или *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

Эквивалентностями являются равенство чисел, равенство векторов, параллельность прямых (если совпавшие прямые тоже считать параллельными), подобие треугольников в евклидовом пространстве.

Пусть на множестве X задано отношение эквивалентности \sim . Тогда для каждого элемента $x \in X$ можно рассмотреть подмножество $[x] := \{x' \in X | x' \sim x\}$. Это подмножество называется *классом эквивалентности* элемента $x \in X$. Очевидно, что состав класса эквивалентности $[x]$ может измениться, если рассмотреть на том же множестве X новое отношение эквивалентности, отличное от отношения \sim .

Определение 1.1.14. Подмножества $X_i \in X, i \in I$, множества X составляют *разбиение*, если

- подмножества $X_i, i \in I$ *составляют покрытие* множества X , т. е. $\bigcup_{i \in I} X_i = X$ и
- подмножества $X_i, i \in I$ *попарно не пересекаются*, т. е. для любых $i, j \in I, i \neq j$, выполнено $X_i \cap X_j = \emptyset$.

Предложение 1.1.15. *Задание отношения эквивалентности на множестве X определяет его разбиение на классы эквивалентности. Обратно, задание разбиения множества X определяет отношение эквивалентности на нём.*

Доказательство. Пусть на множестве X задано отношение эквивалентности \sim ; тогда каждый элемент $x \in X$ принадлежит классу $[x]$. Таким образом, классы эквивалентности составляют покрытие множества X . Предположим, что элемент x принадлежит двум классам $[x] \ni x \in [\bar{x}]$. Тогда, выбрав произвольный элемент $x' \in [x]$ и используя определение класса эквивалентности, мы можем записать

$$\left. \begin{array}{l} x' \in [x] \Leftrightarrow x' \sim x \\ x \in [\bar{x}] \Leftrightarrow x \sim \bar{x} \end{array} \right| \Rightarrow x' \sim \bar{x} \Leftrightarrow x' \in [\bar{x}]. \quad (1.1.3)$$

Импликация после вертикальной черты верна по транзитивности отношения \sim . Поскольку (1.1.3) выполнено для произвольного $x' \in [x]$, то $[x] \subset [\bar{x}]$. Поменяв ролями классы

$[x]$ и $[\bar{x}]$, приходим к равенству $[x] = [\bar{x}]$. Итак, классы эквивалентности, имеющие непустое пересечение, совпадают. Таким образом, различные классы эквивалентности попарно не пересекаются, т. е. классы эквивалентности составляют разбиение.

Обратно, пусть задано разбиение множества $X = \bigsqcup_{i \in I} X_i$. Определим на множестве X отношение \sim

$$x \sim x' \Leftrightarrow \exists i \in I : x \in X_i \ni x' \quad (1.1.4)$$

и убедимся в том, что \sim – отношение эквивалентности. Поскольку для всякого элемента $x \in X$ выполнено $x \sim x$, то отношение \sim рефлексивно. Если $x \sim x'$, то два элемента x, x' принадлежат одному подмножеству X_i ; тогда, разумеется, $x' \sim x$. Отсюда заключаем, что отношение \sim симметрично. Наконец, пусть $x \sim x'$, откуда x, x' принадлежат одному подмножеству X_i . Пусть также $x' \sim x''$; тогда x', x'' принадлежат одному подмножеству X_j . Поскольку $X_i \ni x' \in X_j$ и подмножества $X_i, i \in I$, составляют разбиение, то $i = j$ и потому x, x', x'' принадлежат одному подмножеству X_i . Отсюда заключаем, что $x \sim x''$, что доказывает транзитивность отношения \sim . \square

Итак, любое отношение эквивалентности \sim , введённое на множестве X , разбивает это множество на классы $[x]$ эквивалентных элементов. Тогда можно рассмотреть новое множество X/\sim , элементами которого являются классы $[x]$. Множество X/\sim называют *фактормножеством* множества X по отношению эквивалентности \sim . Имеется отображение $X \twoheadrightarrow X/\sim : x \mapsto [x]$.

Пример 1.1.16. Пусть X – множество всех ненулевых векторов в \mathbb{R}^2 . Назовём два вектора $v_1, v_2 \in X$ *коллинеарными* ($v_1 \parallel v_2$), если они линейно зависимы. Итак,

$$v_1 \parallel v_2 \Leftrightarrow \exists \alpha, \beta \in \mathbb{R} : (\alpha, \beta) \neq (0, 0) \& \alpha v_1 + \beta v_2 = 0.$$

Понятно, что отношение \parallel есть эквивалентность. Тогда фактормножество X/\parallel обладает биекцией на множество точек окружности $S^1 = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$. (*Упражнение: опишите явно эту биекцию!*)

Пример 1.1.17. Пусть X – множество ненулевых векторов $n + 1$ -мерного k -векторного пространства k^{n+1} , а отношение коллинеарности определим как

$$v_1 \parallel v_2 \Leftrightarrow \exists \alpha, \beta \in k : (\alpha, \beta) \neq (0, 0) \& \alpha v_1 + \beta v_2 = 0.$$

Множество точек n -мерного *проективного пространства* \mathbb{P}_k^n – это фактормножество X/\parallel . В частности, из предыдущего примера имеем биекцию $\mathbb{P}_{\mathbb{R}}^1 \simeq S^1$.

Теперь рассмотрим отображение множеств $f: X \rightarrow Y$ и связанное с ним отношение эквивалентности \sim_f на области определения $\text{dom } f = X$:

$$x \sim_f x' \Leftrightarrow f(x) = f(x').$$

Это отношение эквивалентности приводит к фактормножеству X/\sim_f и биекции

$$X/\sim_f \simeq \text{im } f : [x] \mapsto f(x).$$

Таким образом, мы приходим к разложению (*факторизации*) произвольного отображения $f: X \rightarrow Y$ в композицию сюръективного и инъективного отображений

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow \hat{f} & \nearrow f \\ & \text{im } f & \end{array}$$

Введено отображение $\hat{f}: X \rightarrow \text{im } f : x \mapsto f(x)$. Оно отличается от отображения f только областью значений (при этом область определения и образ отображения \hat{f} такие же, каковы соответственно область определения и образ отображения f).

Указанное разложение приводит к простому, но очень важному результату.

Теорема 1.1.18 (теорема о факторизации). Пусть отображения $\varphi: X \rightarrow Y$ и $\psi: X \rightarrow Z$ таковы, что индуцированные ими отношения эквивалентности

$$\begin{aligned}\sim_\varphi &= \{(x, x') \in X \times X \mid \varphi(x) = \varphi(x')\}, \\ \sim_\psi &= \{(x, x') \in X \times X \mid \psi(x) = \psi(x')\}\end{aligned}$$

удовлетворяют включению $(\sim_\varphi) \subseteq (\sim_\psi)$. Тогда существует отображение $\chi: \text{im } \varphi \rightarrow Z$, включаемое в коммутативную диаграмму

$$\begin{array}{ccc} X & \xrightarrow{\psi} & Z \\ & \searrow \hat{\varphi} & \nearrow \chi \\ & \text{im } \varphi & \end{array}$$

Определение 1.1.19. n -местным (n -арным) отношением R , заданным на множествах M_1, M_2, \dots, M_n , называется подмножество их декартова произведения

$$R \subseteq M_1 \times M_2 \times \dots \times M_n.$$

При этом количество сомножителей n называется *арностью* отношения R . Отношение арности 2 называется *бинарным*, отношение арности 3 – *тернарным*.

Факт связи n -ки элементов $(m_1, m_2, \dots, m_n) \in M_1 \times M_2 \times \dots \times M_n$ отношением R обозначается $R(m_1, m_2, \dots, m_n)$ или $(m_1, m_2, \dots, m_n) \in R$.

Факт связи объектов $m_1 \in M_1$ и $m_2 \in M_2$ бинарным отношением $R \subset M_1 \times M_2$ (его называют *соответствием* между множествами M_1 и M_2) обычно обозначают с помощью инфиксной записи: $m_1 R m_2$. Одноместные (унарные) отношения соответствуют свойствам или атрибутам; обычно для таких случаев терминология отношений не используется.

Универсальное отношение — это отношение, связывающее все элементы заданных множеств, т. е. отношение, совпадающее с декартовым произведением: $R = M_1 \times M_2 \times \dots \times M_n$. Нуль-отношение — отношение, не связывающее никакие элементы, т. е. пустое множество: $R = \emptyset \subset M_1 \times M_2 \times \dots \times M_n$.

Отношение $R \subseteq M_1 \times M_2 \times \dots \times M_n \times M_{n+1}$ называется функциональным, если из выполнения $R(m_1, \dots, m_n, x)$ и $R(m_1, \dots, m_n, y)$ следует, что $x = y$.

Наиболее распространённые в языке математики отношения — это бинарные отношения над одним множеством $R \subseteq M^2$. Наиболее часто используются бинарные отношения, обладающие специальными свойствами:

- *симметричностью*: $a R b \Rightarrow b R a$
или *антисимметричностью* $a R b \wedge b R a \Rightarrow a = b$,
- *рефлексивностью*: $a R a$
или *антирефлексивностью* $\neg(a R a)$,
- *транзитивностью*: $a R b \wedge b R c \Rightarrow a R c$
или *антитранзитивностью* $a R b \wedge b R c \Rightarrow \neg a R c$,
- *связностью*: $a \neq b \Rightarrow a R b \vee b R a$.

В зависимости от набора свойств бинарных отношений формируются некоторые широко используемые их виды:

- *отношение эквивалентности* — всякое рефлексивное, транзитивное и симметричное отношение;
- *отношение предпорядка* — рефлексивное и транзитивное;
- *отношение частичного порядка* — рефлексивное, транзитивное и антисимметричное;
- *отношение строгого порядка* — антирефлексивное, транзитивное, антисимметричное;
- *отношение линейного порядка* — связное, рефлексивное, антисимметричное.

Важную роль играет

- *отношение равенства* — отношение эквивалентности, выполненное только для двух совпадающих элементов.

Пример 1.1.20. Отношение делимости, например на множестве \mathbb{Z} целых чисел, состоит из пар вида $(x, y) \in \mathbb{Z}$ таких, что x делит y нацело. Оно обычно обозначается символом $|$ («делит»), например, $2|6$. Это отношение транзитивно и рефлексивно.

Пример 1.1.21. Пример тернарного (трёхместного) отношения — образование пифагоровой тройки тремя целыми числами:

$$(x, y, z) \in PT \Leftrightarrow x^2 + y^2 = z^2.$$

Пример 1.1.22. Более свободный набор свойств бинарных отношений применяется в теории графов: неориентированный граф может быть определён как множество вершин с симметричным бинарным отношением над ним, а ориентированный граф — как множество вершин с произвольным бинарным отношением над ним.

Определение 1.1.23. q -арной операцией на непустом множестве X называется отображение

$$\diamond: \underbrace{X \times \cdots \times X}_q \rightarrow X : (x_1, \dots, x_q) \mapsto \diamond(x_1, \dots, x_q),$$

если $q \in \mathbb{N}$, и отображение $\omega: \{\cdot\} \rightarrow X, \cdot \mapsto \omega \in X$, если $q = 0$. Здесь символом $\{\cdot\}$ обозначено множество, состоящее из одного элемента. При этом число q называется *арностью* операции \diamond .

При $q = 0$ получается *нульарная* операция; она представляет собой указание во множестве X некоторого выделенного элемента. Например, на множестве целых чисел одна нульарная операция выделяет нуль 0 , а другая — единицу 1 .

При $q = 1$ имеем *унарную* операцию; это функция одной переменной на множестве X со значениями в нём же. Например, на множестве целых чисел имеется операция

$$-: \mathbb{Z} \rightarrow \mathbb{Z} : n \mapsto -n.$$

При $q = 2$ получим *бинарную* операцию. Таковы, например, привычные операции сложения и умножения чисел.

Определение 1.1.24. Бинарная операция $\circ: X \times X \rightarrow X$ называется *коммутативной*, если для любых $x_1, x_2 \in X$ выполнено равенство $x_1 \circ x_2 = x_2 \circ x_1$.

Определение 1.1.25. Бинарная операция $\circ: X \times X \rightarrow X$ называется *ассоциативной*, если для любых $x_1, x_2, x_3 \in X$ выполнено равенство $(x_1 \circ x_2) \circ x_3 = x_1 \circ (x_2 \circ x_3)$.

Пример 1.1.26. Сложение и умножение вещественных чисел являются ассоциативными и коммутативными операциями. Умножение квадратных матриц любого размера, не превосходящего 2, ассоциативно, но не коммутативно.

Определение 1.1.27. Множества M и N называются *равномощными*, если существует биективное отображение $M \xrightarrow{\sim} N$.

1.2 Структуры алгебры (общие замечания)

Понятие алгебраической системы возникло из общности конструкций, характерных для различных общеалгебраических структур, таких как группы и кольца. В частности, таковы конструкции подсистемы (обобщающей понятия подгруппы и подкольца соответственно), гомоморфизма, изоморфизма, факторсистемы (обобщающей соответственно конструкции факторгруппы и факторкольца). Эта общность формализуется и изучается в самостоятельном разделе общей алгебры — *универсальной алгебре*. В этом направлении получен ряд содержательных результатов, характерных для любых алгебраических систем. Например, такова теорема о гомоморфизме, которая в случае алгебраической системы без заданных отношений — алгебры — уточняется до теорем об изоморфизме, известных из теории групп и теории колец. Этот сюжет будет подробно рассмотрен в следующих главах.

Алгебраическая система в универсальной алгебре — это непустое множество G (*носитель*) с заданным на нём набором операций и отношений; этот набор называется *сигнатурой*. Алгебраическая система с пустым множеством отношений называется *алгеброй*, а система с пустым множеством операций — *моделью*.

В математике с той или иной степенью строгости также используется понятие «алгебраической структуры». В частности, у Бурбаки в статье «Архитектура математики» оно понимается как множество, наделённое операциями; при этом множество, наделённое отношениями (наличие которых возможно для алгебраической системы), уже рассматривается как математическая структура другого рода — структура порядка. Однако и не все алгебраические структуры описываются алгебраическими системами без дополнительных конструкций. Даже для определения таких классических структур, как модуль над кольцом (каковым является, например, векторное пространство над полем) или алгебра над полем, в универсальной алгебре используются такие искусственные конструкции, как определение для каждого элемента кольца (поля) унарной операции умножения на этот элемент.

Множество можно считать вырожденной алгебраической системой с пустым набором операций и отношений.

Для алгебр любого типа *гомоморфизм* — это отображение однотипных алгебр, сохраняющее все операции. *Изоморфизм* — это обратимый (т. е. биективный) гомоморфизм. Поэтому всякий раз, говоря о гомоморфизме (соответственно, изоморфизме), уточняют, о гомоморфизме (соответственно, изоморфизме) каких алгебр идёт речь: гомоморфизме групп, гомоморфизме колец и т. п. Гомоморфизм $f: A \rightarrow A$ алгебры A в себя называют *эндоморфизмом* алгебры A . Изоморфизм $f: A \xrightarrow{\sim} A$ алгебры A на себя называют *автоморфизмом* алгебры A (опять же в обоих случаях необходимо указывать тип алгебры).

Глава 2

Группоиды, моноиды и полугруппы

2.1 Группоид. Полугруппа. Моноид

Определение 2.1.1. *Группоид* – это непустое множество S с одной бинарной операцией $*$.

Например, любое ненулевое множество вещественных чисел с бинарной операцией

$$(a, b) \mapsto \max(a, b)$$

является группоидом.

Определение 2.1.2. *Полугруппа* – это непустое множество S с одной ассоциативной бинарной операцией $*$.

Например, полугруппой будет такое множество:

$$S = \{n \in \mathbb{N} \mid n \geq n_0\},$$

если в качестве операции выбрать обычное умножение.

Упражнение 2.1.3. Образуем ли полугруппу то же множество относительно сложения?

Если бинарная операция – умножение, то полугруппу называют *мультипликативной*, если бинарная операция – сложение, то полугруппу называют *аддитивной*. Бинарная операция может быть определена абстрактным образом, а элементы полугруппы могут не быть числами. Вместе с тем говорят о мультипликативной или аддитивной формах записи полугруппы и бинарной операции в ней. Как правило, аддитивная форма записи подразумевает коммутативность бинарной операции, а мультипликативная форма записи – нет.

Может случиться, что в полугруппе (S, \circ) имеется такой элемент $e \in S$, что для всех $s \in S$ выполнено $e \circ s = s \circ e = s$.

Определение 2.1.4. Элемент e полугруппы (S, \circ) такой, что для всех $s \in S$ выполнено $e \circ s = s \circ e = s$, называется *нейтральным* (относительно бинарной операции \circ).

Например, натуральные числа \mathbb{N} образуют полугруппы относительно операции сложения $+$ и операции умножения \cdot . Однако полугруппа (\mathbb{N}, \cdot) содержит нейтральный элемент 1, а полугруппа $(\mathbb{N}, +)$ нейтрального элемента не содержит. Вместе с тем последняя ситуация может быть исправлена добавлением нуля: $(\mathbb{N} \cup \{0\}, +)$ – полугруппа с нейтральным элементом 0.

Определение 2.1.5. *Моноидом* называется полугруппа, обладающая нейтральным элементом.

Таким образом, моноидами среди приведённых примеров являются: натуральные числа относительно умножения, натуральные числа с нулём относительно сложения, целые числа относительно сложения.

Пусть M – моноид, $a \in M$.

Предложение 2.1.6. *Значение выражения $a^n := aa \dots a$ не зависит от порядка выполнения операций.*

Доказательство. Докажем предложение по индукции. Очевидно, утверждение тривиально верно для произведения, состоящего из одного сомножителя a . Предположим, что оно также верно для произведений, состоящих не более чем из $n-1$ сомножителя. Тогда, используя ассоциативность операции \cdot , рассмотрим выражение $a \cdot a^{n-1} = a \cdot (a^i \cdot a^{n-i-1}) = (a \cdot a^i) \cdot a^{n-i-1} = a^{i+1} \cdot a^{n-i-1} = a^{i+1} \cdot (a \cdot a^{n-i-2}) = a^{i+2} \cdot a^{n-i-2} = \dots = a^{n-1} \cdot a$. \square

Упражнение 2.1.7. Докажите, что значение произведения $a_1 a_2 \dots a_n$ элементов $a_i \in M$, $i = 1, \dots, n$, моноида M не зависит от порядка выполнения операций.

Зафиксируем непустое множество A , которое будем называть *алфавитом*, а его элементы – *буквами*. Назовём *словом* над алфавитом A любую конечную последовательность (кортеж) $a_1 a_2 \dots a_n$ букв $a_i \in A$, $i = 1, \dots, n$. При этом буквы, имеющие различные номера, могут совпадать. Пустое слово будем обозначать символом e . Мы будем обозначать множество всех слов над алфавитом A символом W_A . Поскольку длины слов не ограничены, множество W_A бесконечно даже в том случае, когда алфавит A конечен.

Определение 2.1.8. *Конкатенацией, или сцеплением, слов $a_1 a_2 \dots a_n$ и $a'_1 a'_2 \dots a'_m$ над алфавитом A называется слово $a_1 a_2 \dots a_n a'_1 a'_2 \dots a'_m$.*

По определению, конкатенация является ассоциативной бинарной операцией на множестве всех слов над алфавитом A . При этом пустое слово ведёт себя следующим образом: для любого $a_1 a_2 \dots a_n \in W_A$ выполнены равенства $a_1 a_2 \dots a_n e = a_1 a_2 \dots a_n$, $e a_1 a_2 \dots a_n = a_1 a_2 \dots a_n$, $ee = e$. Таким образом, пустое слово e является нейтральным элементом относительно конкатенации на множестве W_A всех слов над алфавитом A . Итак, мы имеем следующее

Предложение 2.1.9 (конструкция свободного моноида). *Множество W_A всех слов над алфавитом A с операцией конкатенации составляет моноид.*

Определение 2.1.10. Моноид предложения 2.1.9 называется *свободным моноидом*, порождаемым алфавитом A . Буквы алфавита A называются *порождающими элементами*, или *образующими*, свободного моноида W_A .

Пример 2.1.11. *Свободный моноид с одной образующей* состоит из элементов

$$e, a, aa, \dots, \underbrace{a \dots a}_n, \dots$$

Замечание 2.1.12. Понятно, что в свободном моноиде с одной образующей конкатенация коммутативна:

$$\underbrace{a \dots a}_n \underbrace{a \dots a}_m = \underbrace{a \dots a}_m \underbrace{a \dots a}_n = \underbrace{a \dots a}_{n+m}$$

для любых целых неотрицательных n, m . Однако если рассматривать алфавит, состоящий из двух или более букв, то, например, слова $a_1 a_1 a_2$ и $a_1 a_2 a_1$ будут различными. Поэтому свободный моноид над алфавитом, состоящим более чем из одной буквы, некоммутативен.

2.2 Гомоморфизмы и изоморфизмы группоидов, моноидов и полугрупп. Конгруэнция. Теоремы о гомоморфизме

Пусть M – непустое множество, \circ – бинарная операция на множестве M .

Определение 2.2.1. Отношение эквивалентности \sim на группоиде (M, \circ) называется *конгруэнцией*, если для любых пар $a_1 \sim a_2$ и $b_1 \sim b_2$, $a_i, b_i \in M$, $i = 1, 2$, выполнено $a_1 \circ b_1 \sim a_2 \circ b_2$. В этом случае говорят, что эквивалентность \sim *согласована с бинарной операцией* \circ .

Предложение 2.2.2 (конструкция факторгруппоида). *Конгруэнция \sim на группоиде (M, \circ) наделяет фактормножество M/\sim индуцированной бинарной операцией.*

Доказательство. Достаточно убедиться в том, что для любых классов $[a], [b] \in M/\sim$ и любых представителей $a' \in [a]$ и $b' \in [b]$ класс $[a'b']$ не зависит от выбора представителей a', b' . Действительно, $a \sim a'$ и $b \sim b'$; тогда $ab \sim a'b'$, что и требовалось. \square

Теперь рассмотрим два группоида $(M, *)$ и (N, \circ) .

Определение 2.2.3. Отображение $f: M \rightarrow N$ называется *гомоморфизмом группоидов*, если оно сохраняет бинарную операцию, т. е. для любых $m_1, m_2 \in M$ выполнено

$$f(m_1 * m_2) = f(m_1) \circ f(m_2).$$

Биективный гомоморфизм группоидов называется *изоморфизмом группоидов*.

Определение 2.2.4. *Подгруппоидом* группоида $(M, *)$ называется подмножество $S \subseteq M$, замкнутое относительно бинарной операции $*$, т. е. такое, что для любых $s_1, s_2 \in S$ выполнено $s_1 * s_2 \in S$.

Понятно, что подгруппоид является группоидом и отображение вложения подгруппоида $S \hookrightarrow M: s \mapsto s$ является (инъективным) гомоморфизмом группоидов.

Определение 2.2.5. *Образом* гомоморфизма группоидов $f: (M, *) \rightarrow (N, \circ)$ называется подмножество

$$\text{im } f = \{f(m) | m \in M\} \subseteq N.$$

Предложение 2.2.6 (образ гомоморфизма как подгруппоид). *Образ $\text{im } f$ гомоморфизма группоидов $f: M \rightarrow N$ является подгруппоидом группоида N .*

Доказательство. Рассмотрим два произвольных элемента $f(m_1), f(m_2) \in \text{im } f$. Тогда

$$f(m_1) \circ f(m_2) = f(m_1 * m_2) \in \text{im } f.$$

\square

Теорема 2.2.7 (о ядре гомоморфизма группоидов). *Любой гомоморфизм группоидов*

$$f: M \rightarrow N$$

определяет отношение эквивалентности на области определения $\ker f \subset M \times M$, являющееся конгруэнцией и задаваемое следующим образом:

$$(m_1, m_2) \in \ker f \Leftrightarrow f(m_1) = f(m_2).$$

Обратно, задание на группоиде M любой конгруэнции R наделяет фактормножество M/R структурой группоида и определяет индуцированный гомоморфизм группоидов

$$f_R: M \rightarrow M/R.$$

При этом $\ker f_R = R$.

Доказательство. Убедимся в том, что $\ker f$ – конгруэнция. Для этого выберем $(m_1, m'_1) \in \ker f$ и $(m_2, m'_2) \in \ker f$. Это означает, что $f(m_1) = f(m'_1)$ и, соответственно, $f(m_2) = f(m'_2)$. Тогда, формируя композиции, имеем $f(m_1) \circ f(m_2) = f(m'_1) \circ f(m'_2)$. Учитывая гомоморфность отображения f , получим

$$f(m_1 * m_2) = f(m_1) \circ f(m_2) = f(m'_1) \circ f(m'_2) = f(m'_1 * m'_2).$$

По определению отношения $\ker f$ это означает, что $(m_1 * m_2, m'_1 * m'_2) \in \ker f$.

Теперь пусть R – конгруэнция на группоиде M . Рассмотрим фактормножество M/R и определим на нём бинарную операцию \circ следующим образом: для двух классов $[m_1], [m_2] \in M/R$ положим $[m_1] \circ [m_2] = [m_1 * m_2]$. Поскольку R – конгруэнция, то для $(m_1, m'_1) \in R$ и для $(m_2, m'_2) \in R$ имеем $(m_1 * m_2, m'_1 * m'_2) \in R$, откуда следует, что операция \circ определена корректно, и построен группоид $(M/R, \circ)$. Далее рассмотрим отображение $f_R: M \rightarrow M/R: m \mapsto [m]$. По определению бинарной операции \circ , это отображение является гомоморфизмом группоидов: $f(m_1 * m_2) = [m_1 * m_2] = [m_1] \circ [m_2] = f(m_1) \circ f(m_2)$.

Наконец, поскольку элементы m и m' принадлежат одному классу $[m]$ тогда и только тогда, когда $(m, m') \in R$, то $R = \ker f$. Это завершает доказательство теоремы. \square

Определение 2.2.8. Конгруэнция, определённая в теореме 2.2.7, называется *ядром* гомоморфизма группоидов $f: M \rightarrow N$.

Теорема 2.2.9 (о гомоморфизме для группоидов). *Любой гомоморфизм группоидов $f: M \rightarrow N$ обладает разложением в композицию гомоморфизмов согласно коммутативной диаграмме:*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow & & \uparrow \\ M/\ker f & \xrightarrow{\sim} & \operatorname{im} f \end{array}$$

Доказательство. Необходимо доказать изоморфизм группоидов $M/\ker f \simeq \operatorname{im} f$. Для этого рассмотрим отображение $M/\ker f \rightarrow \operatorname{im} f: [m] \mapsto f(m)$. Поскольку все элементы группоида M , принадлежащие одному классу $[m]$ относительно отношения $\ker f$, отображаются в один и тот же элемент $f(m)$, то это отображение определено корректно. Поскольку определено обратное к нему отображение $\operatorname{im} f \rightarrow M/\ker f: f(m) \mapsto [m]$, то оба отображения представляют собой взаимно обратные биекции. Сохранение операции, поставленное для всех $m, m' \in M$ соответствием $[m] \circ [m'] \mapsto f(m) \circ f(m')$, показывает, что оба отображения суть взаимно обратные изоморфизмы. \square

Определение 2.2.10. Группоид $(M/\sim, \circ)$, построенный в предложении 2.2.2, называется *факторгруппоидом* группоида (M, \circ) относительно конгруэнции \sim .

Пусть $S, *$ и T, \circ – полугруппы.

Определение 2.2.11. Отображение полугрупп $f: S \rightarrow T$ называется *гомоморфизмом полугрупп*, если оно сохраняет бинарную операцию, т. е. для любых $s_1, s_2 \in S$ выполнено $f(s_1 * s_2) = f(s_1) \circ f(s_2)$. Гомоморфизм полугрупп $f: S \rightarrow T$ называется *изоморфизмом полугрупп*, если он биективен.

Определение 2.2.12. Подполугруппой полугруппы $(S, *)$ называется подмножество $T \subseteq S$, замкнутое относительно бинарной операции $*$.

Понятно, что подполугруппа является полугруппой и отображение вложения подполугруппы $T \hookrightarrow S: t \mapsto t$ является (инъективным) гомоморфизмом полугрупп.

Определение 2.2.13. Отображение моноидов $f: M \rightarrow N$ называется *гомоморфизмом моноидов*, если оно сохраняет бинарную операцию

$$\forall m_1, m_2 \in M \quad f(m_1 * m_2) = f(m_1) \circ f(m_2)$$

и переводит нейтральный элемент $e_M \in M$ в нейтральный элемент e_N , т. е. $f(e_M) = e_N$.

Упражнение 2.2.14. Если $f: M \rightarrow N$ – сюръективное отображение моноидов, то из требования сохранения операции следует, что $f(e_M) = e_N$. Докажите это.

Определение 2.2.15. *Подмоноидом* моноида $(M, *, e)$ называется подмножество $S \subseteq M$, замкнутое относительно бинарной операции $*$ и содержащее нейтральный элемент e .

Очевидно, подмоноид является моноидом и отображение вложения подмоноида

$$S \hookrightarrow M: s \mapsto s$$

является (инъективным) гомоморфизмом моноидов.

Если $(M, *)$ – группоид с ассоциативной бинарной операцией $*$ и конгруэнция R задана на нём, то факторгруппоид M/R тоже наделён ассоциативной бинарной операцией, т. е. представляет собою полугруппу, называемую *факторполугруппой* полугруппы M относительно конгруэнции R . Теорема о гомоморфизме для полугрупп формулируется и доказывается совершенно аналогично теореме о гомоморфизме для группоидов.

Если $(M, *, e)$ – моноид с нейтральным элементом e и конгруэнция R задана на нём, то $[e]$ – нейтральный элемент факторгруппоида M/R (убедитесь в этом!) и тем самым факторгруппоид становится моноидом, который называется *фактормоноидом* моноида M относительно конгруэнции R . Теорема о гомоморфизме для моноидов формулируется аналогично теореме о гомоморфизме для моноидов (сформулируйте её и проверьте, что доказательство переносится дословно, если заметить, что все стрелки диаграммы переводят нейтральный элемент в нейтральный элемент).

2.3 Специальные элементы

Соглашение 2.3.1. Если не оговорено противное, далее бинарную операцию на элементах a, b мы будем обозначать выражением ab (опуская символы $*$, \circ и т. п.).

Пусть S – группоид.

Предложение 2.3.2 (единственность нейтрального элемента). *Если в группоиде S существует нейтральный элемент, то он единственен.*

Доказательство. Предположим противное: пусть e и e' – два нейтральных элемента. Тогда $e = ee' = e'$. \square

Пусть M – моноид с нейтральным элементом e .

Определение 2.3.3. Элемент $a_L^{-1} \in M$ называется *левым обратным* элемента $a \in M$, если $a_L^{-1}a = e$. Элемент $a \in M$, для которого существует левый обратный, называется *обратимым слева*. Элемент $a_R^{-1} \in M$ называется *правым обратным* элемента $a \in M$, если $aa_R^{-1} = e$. Элемент $a \in M$, для которого существует правый обратный, называется *обратимым справа*. Элемент $a^{-1} \in M$ называется *двусторонним обратным* (или просто *обратным*) элемента $a \in M$, если $a^{-1}a = aa^{-1} = e$. Элемент $a \in M$, для которого существует двусторонний обратный, называется *обратимым*.

Теорема 2.3.4 (равенство левого и правого обратных элементов). *Если бинарная операция в моноиде M ассоциативна, то левый обратный и правый обратный элемента a совпадают всякий раз, когда они существуют.*

Доказательство. Доказательство поставляется цепочкой равенств:

$$a_L^{-1} = a_L^{-1}e = a_L^{-1}(aa_R^{-1}) = (a_L^{-1}a)a_R^{-1} = ea_R^{-1} = a_R^{-1}.$$

□

Замечание 2.3.5. Читателю полезно обратить внимание на то, что в доказательстве используется ассоциативность бинарной операции.

Аналогичным образом нетрудно доказать, что обратный элемент для данного обратимого элемента единственен.

Упражнение 2.3.6. Докажите это!

Пример 2.3.7. Читателю хорошо известно, что в моноиде квадратных матриц над полем (и над любым коммутативным кольцом!) $\text{Mat}_k(n)$ относительно матричного умножения левая обратная данной матрицы совпадает с её правой обратной, если только левая и правая обратная матрицы существуют. Более того, если некоторая матрица A' является левой обратной данной матрицы A , то A' является также и правой обратной для A . И наоборот, если некоторая матрица A'' является правой обратной некоторой матрицы A , то A'' является также и левой обратной для A .

Упражнение 2.3.8. Пусть элемент m моноида M обладает обратным элементом, равным m^{-1} , а элемент n того же моноида – обратным элементом, равным n^{-1} . Найдите элементы, обратные к mn и к nm .

Однако справедлив более сильный результат.

Предложение 2.3.9. Если в моноиде M с нейтральным элементом e каждый элемент a обратим слева (соответственно, справа), то каждый элемент также обратим и справа (соответственно, слева), причём левый и правый обратные каждого элемента совпадают.

Доказательство. Приведём доказательство для случая, когда дана обратимость справа (для обратимости слева доказательство аналогично). Пусть $a \in M$, и $ax = e$ для некоторого $x \in M$. Также $xy = e$ для некоторого $y \in M$. Имеем цепочку равенств

$$xa = xae = xa(xy) = x(ax)y = xy = e,$$

т. е. x является двусторонним обратным для a .

□

Глава 3

Группы

3.1 Начальные знания о группах

3.1.1 Первые понятия

Определение 3.1.1. *Группой* называется непустое множество G с бинарной операцией $*$ (эту операцию называют *групповой операцией* или *композицией*), удовлетворяющей следующим аксиомам:

- операция ассоциативна: $\forall a, b, c \in G \ a * (b * c) = (a * b) * c$,
- существует нейтральный элемент: $\exists e \in G : \forall a \in G \ a * e = e * a = a$,
- все элементы обратимы: $\forall a \in G \ \exists a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$.

Обратимые элементы ассоциативного моноида образуют группу.

Если пользоваться языком универсальной алгебры, то в группе имеется одна бинарная операция $*$, одна унарная операция $(\)^{-1}$ и одна нульарная операция – указание нейтрального элемента. Эти операции связаны соотношениями, приведёнными в аксиомах определения 2.2.10.

Предложение 3.1.2 (уравнения в группе). *В группе $(G, *)$ уравнение вида $a * x = b$ при любых $a, b \in G$ разрешимо единственным образом. Уравнение вида $x * a = b$ при любых $a, b \in G$ также разрешимо единственным образом.*

Доказательство. Мы докажем первое утверждение; второе утверждение доказывается аналогично. Домножим левую и правую части уравнения $a * x = b$ слева на a^{-1} . Получим

$$a^{-1} * (a * x) = a^{-1} * b,$$

откуда, используя ассоциативность операции $*$, получим

$$a^{-1} * (a * x) = (a^{-1} * a) * x = e * x = x = a^{-1} * b.$$

Из этого вычисления также следует, что любой элемент $x \in G$, удовлетворяющий уравнению $a * x = b$, равен $a^{-1} * b$. \square

Упражнение 3.1.3. Докажите второе утверждение предложения 3.1.2.

Групповая операция может иметь любую природу. Например, множество целых чисел \mathbb{Z} образует группу относительно операции обычного сложения $+$, а нейтральным элементом в ней является ноль 0. В этой группе групповая операция коммутативна.

Определение 3.1.4. Группу с бесконечным множеством элементов называют *бесконечной*, или *группой бесконечного порядка*. Группу, состоящую из конечного числа элементов, называют *конечной*, или *группой конечного порядка*. *Порядком группы G* (обозначение: $|G|$) называют число элементов в ней, если группа конечная. Если группа бесконечная, то говорят, что её *порядок бесконечен* (обозначение: $|G| = \infty$).

Определение 3.1.5. Группа $(G, *, e)$ называется *абелевой*, или *коммутативной*, если групповая операция $*$ коммутативна, т. е. к трём аксиомам определения 2.2.10 добавлена (четвёртая) аксиома

- групповая операция $*$ коммутативна: $\forall a, b \in G \ a * b = b * a$.

В зависимости от способа определения групповой операции используются две различных формы записи групп:

аддитивная, когда групповой операцией в данной группе G является сложение $+$: $(a, b) \mapsto a + b$, в качестве нейтрального элемента выступает нуль (и/или нейтральный элемент обозначается символом 0), а в качестве обратного выступает *противоположный элемент* $-a$;

мультипликативная, когда групповая операция в данной группе G записывается как умножение \cdot : $(a, b) \mapsto ab$, а нейтральный элемент e и обратный a^{-1} для каждого элемента $a \in G$ обозначаются обычным образом.

При этом аддитивная форма записи применяется, как правило, для абелевых групп. Мультипликативная форма записи может использоваться для групп любого вида с операцией любой природы.

Пример 3.1.6. Целые числа \mathbb{Z} составляют группу относительно сложения $+$ с нейтральным элементом 0. Эта группа, очевидно, абелева.

Пример 3.1.7. Параллельные переносы вдоль аффинной прямой составляют группу Trans^1 относительно композиции (последовательного выполнения). В качестве нейтрального элемента выступает тождественное преобразование, а в качестве переноса, обратного переносу на вектор a , — перенос на вектор $-a$. В векторных обозначениях композиция двух переносов на векторы a и b записывается в виде переноса на вектор $a + b$. Аналогичная картина возникает, если рассмотреть группу Trans^n параллельных переносов n -мерного аффинного пространства.

Пример 3.1.8. Группа *кватернионных единиц* \mathbf{H} состоит из 8 элементов $\pm 1, \pm i, \pm j, \pm k$, умножение которых подчинено соотношениям:

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik, \quad (3.1.1)$$

а нейтральным элементом является элемент 1. Читателю предлагается убедиться в том, что умножение, определяемое соотношениями (3.1.1), ассоциативно и поэтому действительно наделяет множество $\mathbf{H} = \{\pm 1, \pm i, \pm j, \pm k\}$ структурой группы. Очевидно, эта группа неабелева.

Пример 3.1.9. Группа \mathbb{Q}^* ненулевых рациональных чисел, группа \mathbb{R}^* ненулевых вещественных чисел и группа \mathbb{C}^* ненулевых комплексных чисел имеют умножение в качестве групповых операций и число 1 в качестве нейтрального элемента. Поскольку умножение чисел коммутативно, эти группы абелевы.

Пример 3.1.10. Группа \mathbb{H}^* ненулевых кватернионов Гамильтона представляет собой множество вида

$$\mathbb{H}^* = \{a + bi + cj + dk \mid (a, b, c, d) \in \mathbb{R}^4 \setminus \{0\}\},$$

а умножение определяется так же, как для многочленов от трёх некоммутирующих переменных i, j, k , умножение которых подчиняется правилам (3.1.1) умножения в группе **H** кватернионных единиц. При этом

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

Очевидно, эта группа неабелева.

Пример 3.1.11. Множество $\text{Mat}_k(m, n)$ матриц размеров $m \times n$ над полем k образует абелеву группу относительно сложения.

Пример 3.1.12. Множество $\text{GL}_k(n)$ невырожденных квадратных матриц размера n над полем k образует группу относительно матричного умножения. При $n \geq 2$ эта группа неабелева (докажите!).

Пусть $(G, *)$ и (H, \circ) – группы.

Определение 3.1.13. Отображение $f: G \rightarrow H$ называется *гомоморфизмом групп*, если оно сохраняет групповую операцию, т. е.

$$\forall g_1, g_2 \in G \quad f(g_1 * g_2) = f(g_1) \circ f(g_2).$$

Биективный гомоморфизм групп называется *изоморфизмом групп*.

Определение 3.1.14. *Подгруппой* группы G называется подмножество $H \subseteq G$, замкнутое относительно групповой операции и взятия обратного элемента, т. е. обладающее свойствами:

- 1) $\forall h_1, h_2 \in H \quad h_1 h_2 \in H$,
- 2) $\forall h \in H \quad h^{-1} \in H$.

Для подгруппы H в группе G используется обозначение $H \leq G$ или $H < G$.

Читателю следует обратить внимание на то, что из определения подгруппы следует, что подгруппа всегда содержит нейтральный элемент.

Упражнение 3.1.15. Опишите явно все подгруппы в группе **H** кватернионных единиц (см. пример 3.1.8).

Теорема 3.1.16 (критерий подгруппы). *Подмножество H группы G является в ней подгруппой тогда и только тогда, когда для любых элементов $h_1, h_2 \in H$ выполнено $h_1 h_2^{-1} \in H$.*

Доказательство. Это несложное упражнение для читателя. □

Упражнение 3.1.17. Докажите, что пересечение любого набора подгрупп в группе G является в ней подгруппой.

Пример 3.1.18. Группа D_3 симметрий правильного треугольника изоморфна группе S_3 перестановок трёх символов.

3.1.2 Циклические подгруппы и группы

Пусть G – группа, записываемая мультипликативно, и $g \in G$ – её произвольный элемент. Обозначим символом g^n n -кратную композицию $gg \dots g$ для любого натурального числа n . Понятно, что $(g^{-1})^n = (g^n)^{-1}$, и тогда положим $g^{-n} := (g^{-1})^n = (g^n)^{-1}$. Также положим по определению $g^0 := e$.

Определение 3.1.19. Подмножество $\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\} \subseteq G$ является подгруппой в группе G и называется (циклической) подгруппой, порождённой элементом a . Сам элемент a называется образующей, или порождающим элементом, циклической подгруппы $\langle a \rangle$.

В зависимости от структуры группы G и выбора элемента a подгруппа $\langle a \rangle$ может быть как конечной, так и бесконечной.

Определение 3.1.20. Если подгруппа $\langle a \rangle$ бесконечна, то говорят, что a – элемент бесконечного порядка или что a имеет бесконечный порядок в группе G . Если подгруппа $\langle a \rangle$ конечна, то говорят, что a – элемент конечного порядка или что a имеет конечный порядок в группе G . Порядком элемента a в группе G называется порядок порождённой им подгруппы $\langle a \rangle$. Порядок элемента a в группе G обозначается символом $\text{ord}_G(a)$.

Замечание 3.1.21. Порядок элемента a в группе G можно определить следующим равносильным способом. Если для $n \in \mathbb{N} \cup 0$ все a^n различны в группе G , то a – элемент бесконечного порядка. В противном случае $\text{ord}_G(a) = \min\{n \mid a^n = e\}$.

Определение 3.1.22. Циклической называется группа G , совпадающая с одной из своих циклических подгрупп. Соответственно, на циклические группы естественным образом переносятся понятия образующей, а также конечного и бесконечного порядка.

Порядок циклической группы совпадает с порядком её образующей.

Пример 3.1.23. Группа $(\mathbb{Z}, +)$ целых чисел по сложению (здесь используется не мультипликативная, а аддитивная запись!) совпадает со своей циклической подгруппой $\langle 1 \rangle$ и потому является циклической. Очевидно, она имеет бесконечный порядок.

Пример 3.1.24. Группа (Rot_n, \circ) вращений правильного n -угольника (групповая операция – композиция вращений) также является циклической. В качестве её образующей можно выбрать вращение на угол, имеющий радианную меру $2\pi/n$ (в любом из двух возможных направлений). Группа Rot_n конечна и имеет порядок, равный n .

Пример 3.1.25. Группа $(\mathbb{Z}_n, +)$ классов вычетов по модулю n (групповая операция – сложение по модулю n) является циклической. В качестве её образующей можно выбрать класс единицы.

Теорема 3.1.26 (классификация циклических групп). Бесконечная циклическая группа изоморфна группе $(\mathbb{Z}, +)$. Конечная циклическая группа порядка n изоморфна группе $(\mathbb{Z}_n, +)$.

Доказательство. Если группа $\langle a \rangle$ бесконечна, то для любых различных $m, n \in \mathbb{Z}$ элементы a^m и a^n также различны. Поэтому можно рассмотреть отображение логарифмирования

$$\log: G \rightarrow \mathbb{Z} : a^n \mapsto n.$$

Понятно, что \log переводит произведение $a^m a^n = a^{m+n}$ в $m+n$, т. е. оно является гомоморфизмом групп (группа $\langle a \rangle$ записывается мультипликативно, а \mathbb{Z} – аддитивная группа). Отображение $\text{pot}: \mathbb{Z} \rightarrow \langle a \rangle : n \mapsto a^n$ (естественно назвать его потенцированием), как нетрудно проверить, является взаимно обратным к отображению логарифмирования:

$$\text{pot} \circ \log: \langle a \rangle \xrightarrow{\log} \mathbb{Z} \xrightarrow{\text{pot}} \langle a \rangle : a^n \mapsto n \mapsto a^n \Rightarrow \text{pot} \circ \log = \text{id}_{\langle a \rangle};$$

$$\log \circ \text{pot}: \mathbb{Z} \xrightarrow{\text{pot}} \langle a \rangle \xrightarrow{\log} \mathbb{Z} : n \mapsto a^n \mapsto n \Rightarrow \log \circ \text{pot} = \text{id}_{\mathbb{Z}}.$$

Пусть теперь $\langle a \rangle$ – конечная циклическая группа порядка n ; это, в частности, означает, что порядок её образующей равен n . Согласно определению порядка элемента в группе,

для $0 \leq i, j \leq n-1$ при $i \neq j$ выполнено $g^i \neq g^j$, т. е. определено отображение логарифмирования $\log: \langle g \rangle \rightarrow \mathbb{Z}_n: g^i \mapsto i$. Поскольку $\log(g^i g^j) = \log g^{i+j} = i+j = \log g^i + \log g^j$, то \log – гомоморфизм групп. Отображение потенцирования $\text{pot}: \mathbb{Z}_n \rightarrow \langle g \rangle: i \mapsto g^i$ является двусторонним обратным отображением для \log (Упражнение: докажите это!). \square

Предложение 3.1.27 (критерий циклическости конечной группы). *Конечная группа G является циклической тогда и только тогда, когда она содержит элемент $g \in G$, порядок которого $\text{ord}_G(g)$ равен порядку $|G|$ группы G .*

Доказательство. Действительно, группа G является циклической тогда и только тогда, когда она совпадает с одной из своих циклических подгрупп. Образующая этой циклической подгруппы имеет порядок, равный $|G|$. \square

Далее мы будем использовать следующее обозначение: если m, n – целые числа, то их наибольший общий делитель будем обозначать символом (m, n) . В частности, если числа m и n взаимно просты, то $(m, n) = 1$. Напомним, что функция Эйлера φ ставит в соответствие каждому натуральному числу n количество натуральных чисел, взаимно простых с n и не превосходящих n . В частности, $\varphi(1) = 1$ и $\varphi(p) = p-1$, если число p является простым.

Лемма 3.1.28 (характеризация образующих конечной циклической группы). *Пусть g – образующая конечной циклической группы, имеющей порядок n . Элемент g^ℓ является образующей группы G тогда и только тогда, когда $(\ell, n) = 1$.*

Доказательство. Пусть $(\ell, n) = 1$. Тогда существуют $u, v \in \mathbb{Z}$ такие, что $\ell u + nv = 1$. Отсюда $g^{\ell u} g^{nv} = g$. Поскольку $G = \langle g \rangle$ имеет порядок n , то $g^n = e$, и тогда $g^{\ell u} = g$. Таким образом, образующая g получается как степень элемента g^ℓ и, следовательно, все элементы группы G также являются степенями элемента g^ℓ . Таким образом, g^ℓ также является образующей группы G . Пусть теперь $\langle g^\ell \rangle = \langle g \rangle$; тогда найдётся такое $u \in \mathbb{N}$, что $g^{\ell u} = g$. Отсюда $\ell u - 1 = nv$ для некоторого $v \in \mathbb{Z}$. Это означает, что $(\ell, n) = 1$. \square

Теорема 3.1.29 (основная теорема о циклических группах). (1) *Всякая подгруппа H циклической группы G является циклической группой.* (2) *Порядок любой подгруппы H конечной циклической группы G является делителем порядка группы G .* (3) *Если n – порядок циклической группы G и ℓ – натуральный делитель числа n , то в группе G существует единственная подгруппа H , имеющая порядок, равный ℓ .* (4) *Для каждого натурального числа d , являющегося делителем порядка n группы G , количество элементов группы G , имеющих порядок, равный d , равно $\varphi(d)$, где $\varphi(d)$ – значение функции Эйлера от числа d .*

Доказательство. Поскольку группа G является циклической, то она имеет вид $\langle g \rangle$. Зафиксируем какую-нибудь образующую g группы G .

(1) Если $|H| = 1$, то утверждение очевидно. В противном случае заметим, что подгруппа H содержит хотя бы одну положительную степень образующей g , т. е. существует $n \in \mathbb{N}$ такое, что $g^n \in H$. Действительно, предположим, что это не так. Тогда, поскольку $|H| > 1$, существует хотя бы один элемент вида $g^{-n} \in H$, $n \in \mathbb{N}$. Но элемент g^n , обратный к элементу g^{-n} , тоже принадлежит подгруппе H .

Теперь рассмотрим подмножество $\{n \in \mathbb{N} | g^n \in H\} \subseteq \mathbb{N}$ и в нём выберем наименьший элемент $s = \min\{n \in \mathbb{N} | g^n \in H\}$. Очевидно, что он существует. Теперь возьмём произвольный элемент подгруппы H ; он имеет вид g^t .

Утверждается, что число s является делителем числа t . В противном случае $t = sq + r$, где $q \in \mathbb{Z}$, $r \in \mathbb{N}$ и $0 < r < s$, что противоречит выбору числа s . Итак, все элементы подгруппы H имеют вид $g^{sq} = (g^s)^q$, $q \in \mathbb{Z}$. Понятно, что все элементы вида $(g^s)^q$, $q \in \mathbb{Z}$, принадлежат подгруппе H . Итак, $H = \langle g^s \rangle$.

(2) Подгруппа H циклической группы $G = \langle g \rangle$, будучи циклической, имеет вид $H = \langle g^s \rangle$, где $s = \min\{n \in \mathbb{N} \mid g^n \in H\}$. Пусть $\text{ord}_G g = |G| = n$. Тогда, в силу конечности группы G , существуют такие $t \in \mathbb{N}$, что $(g^s)^t = e = g^n$. Пусть $\ell = \min\{t \in \mathbb{N} \mid (g^s)^t = e\}$. Таким образом, $s\ell \equiv 0 \pmod n$, откуда заключаем, что $s\ell = n$.

(3) Поскольку ℓ – делитель числа n , то $n/\ell \in \mathbb{N}$. Подгруппа $H = \langle g^{n/\ell} \rangle < G$ имеет порядок, равный ℓ . Теперь предположим, что существует подгруппа $H' < G$, также имеющая порядок, равный ℓ . Поскольку $G = \langle g \rangle$, то H' тоже является циклической. Таким образом, существует $s \in \mathbb{N}$ такое, что $H' = \langle g^s \rangle$, причём $s\ell \equiv 0 \pmod n$. Тогда найдётся $r \in \mathbb{Z}$ такое, что $s = nr/\ell$. Таким образом, $g^s = g^{nr/\ell}$, откуда $H' < H$. Поскольку $|H'| = |H|$, то $H' = H$.

(4) Согласно (3), для любого натурального делителя $d \mid n$ в группе G существует единственная подгруппа H , имеющая порядок, равный d . Поэтому все элементы группы G , имеющие порядок, равный d , суть образующие единственной подгруппы H , имеющей порядок d . Имеем $H = \langle g^{n/d} \rangle$. Элемент $g^{sn/d}$ – другая образующая подгруппы H в том и только в том случае, когда $(s, d) = 1$. При этом будут получаться различные образующие, если и только если $s < d$. Таким образом, применив лемму 3.1.28, получаем число элементов порядка d в группе G , равное $\varphi(d)$. \square

Упражнение 3.1.30. Докажите, что в циклической группе, имеющей порядок, больший двух, число образующих чётно.

Упражнение 3.1.31. Пусть G – циклическая группа порядка n с образующей g . Найдите и докажите необходимое и достаточное условие включения $\langle g^s \rangle \subseteq \langle g^r \rangle$.

3.1.3 Таблица Кэли и теорема Кэли

Пусть G – конечная группа порядка n , записываемая мультипликативно. Перенумеруем её элементы каким-либо способом: g_1, g_2, \dots, g_n . Тогда все композиции в группе G можно записать в виде таблицы умножения, или *таблицы Кэли*, следующего вида:

	g_1	g_2	\dots	g_n
g_1			\dots	
g_2			\dots	
\vdots	\vdots	\vdots	\ddots	\vdots
g_n			\dots	

Условимся о том, что произведение $g_i g_j$ находится на пересечении i -й строки и j -го столбца. Заметим, что внутренняя часть таблицы (т. е. совокупность ячеек, расположенных правее вертикальной двойной черты и ниже горизонтальной двойной черты) ввиду однозначной разрешимости уравнений в группе (предложение 3.1.2) обладает следующим комбинаторным свойством:

каждый элемент встречается в каждой строке и в каждом столбце таблицы только по одному разу. Такая таблица размера $n \times n$ называется *латинским квадратом*.

В частности, выбрав какой-либо (произвольный) элемент $g \in G$, в соответствующей ему строке таблицы обнаружим gg_1, gg_2, \dots, gg_n . Вычислив значения этих произведений в группе G , получим соответственно $g_{\gamma(1)}, g_{\gamma(2)}, \dots, g_{\gamma(n)}$, и тем самым получим перестановку индексов, соответствующую умножению слева на элемент g :

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

В частности, если $g_1 = e$ – нейтральный элемент группы G , то ему соответствует тождественная перестановка:

$$g \mapsto \varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Наконец, последовательное умножение слева сначала на элемент g , а затем на элемент g' приводит к последовательному применению к ряду индексов $(1 \ 2 \ \dots \ n)$ сначала перестановки γ (соответствующей элементу g), а затем перестановки γ' (соответствующей элементу g'). Следовательно, построенное соответствие сохраняет композицию: $g'g \mapsto \gamma' \circ \gamma$. Таким образом, имеется гомоморфизм групп $G \rightarrow S_n$ группы G в симметрическую группу (группу перестановок) n элементов. Поскольку каждая из строк таблицы не повторяется, то построенный гомоморфизм групп инъективен. Таким образом, доказана

Теорема 3.1.32 (теорема Кэли о вложении конечной группы в симметрическую группу). *Всякая конечная группа G обладает гомоморфным вложением в подходящую симметрическую группу.*

3.2 Подгруппы. Нормальность и факторгруппы. Гомоморфизмы и действия

3.2.1 Смежные классы относительно подгруппы. Теорема Лагранжа

Пусть G – группа, H – подгруппа в ней.

Определение 3.2.1. *Левым смежным классом* элемента $g \in G$ в группе G относительно подгруппы H называется подмножество

$$gH = \{gh \mid h \in H\}.$$

Правым смежным классом элемента $g \in G$ в группе G относительно подгруппы H называется подмножество

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

Лемма 3.2.2 (разбиение на смежные классы). (1) *Левые смежные классы в группе G относительно подгруппы H образуют разбиение.* (2) *Правые смежные классы в группе G относительно подгруппы H образуют разбиение.*

Доказательство. Докажем, что любые два различных левых смежных класса не пересекаются (для правых смежных классов доказательство аналогично). Пусть g_1H и g_2H – два смежных класса. Пусть $g_1h_1 = g_2h_2$. Отсюда имеем $g_1 = g_2h_2h_1^{-1}$, и поэтому $g_1 \in g_2H$ и, вместе с тем, $g_1H \subseteq g_2H$. Аналогично, $g_2 = g_1h_1h_2^{-1}$, и поэтому $g_2 \in g_1H$ и отсюда $g_2H \subseteq g_1H$. Поменяв ролями g_1 и g_2 , заключаем, что $g_1H = g_2H$. \square

Лемма 3.2.3 (равномощность смежных классов). *Все (левые и правые) смежные классы в группе G относительно подгруппы H равномощны.*

Доказательство. Биекция для левого класса имеет вид: $H \rightarrow gH : h \mapsto gh$. Для правого класса доказательство аналогично. \square

Объединив леммы 3.2.2 и 3.2.3 в случае конечной группы, получим следующий результат.

Теорема 3.2.4 (теорема Лагранжа). *Если G – конечная группа, H – её подгруппа, тогда порядок $|H|$ подгруппы H является делителем порядка $|G|$ группы G . Справедливо равенство*

$$|G| = |H|[G : H],$$

в котором символ $[G : H]$ означает число (левых или правых) смежных классов группы G относительно подгруппы H .

Замечание 3.2.5. Поскольку все левые и правые смежные классы содержат поровну элементов, количество левых смежных классов группы G относительно подгруппы H равно количеству правых смежных классов той же группы относительно той же подгруппы.

Упражнение 3.2.6. Докажите, что порядок любого элемента конечной группы G является делителем порядка группы G .

Упражнение 3.2.7. Докажите, что любая группа, порядок которой является простым числом, является циклической.

Следствие 3.2.8. Для цепочки подгрупп $K < H < G$ конечной группы G имеем равенство

$$[G : K] = [G : H][H : K].$$

Доказательство. Итак, применим теорему Лагранжа трижды: для $K < G$, для $H < G$ и для $K < H$.

$$\begin{aligned} |G| &= [G : K]|K|, \\ |G| &= [G : H]|H| = [G : H][H : K]|K|. \end{aligned}$$

Сравнив правые части полученных равенств, получим требуемое равенство. \square

Определение 3.2.9. Число $[G : H]$ левых (правых) смежных классов группы G относительно её подгруппы H называется *индексом подгруппы H в группе G* .

3.2.2 Действие группы на множестве

Пусть X – множество; его элементы мы будем называть *точками*. Пусть S_X – множество биективных отображений множества X на себя. Это множество наделено структурой группы относительно композиции.

Определение 3.2.10. Группа S_X называется *симметрической группой* множества X .

Пример 3.2.11. Если X – множество из n элементов $X = \{1, 2, \dots, n\}$, то $S_X = S_n$ – группа перестановок n символов (симметрическая группа на n символах).

Определение 3.2.12. Действием группы G на множестве X называется гомоморфизм групп

$$\alpha: G \rightarrow S_X.$$

Таким образом, действие α для каждого элемента $g \in G$ определяет биективное отображение $\alpha(g): X \rightarrow X: x \mapsto \alpha(g)(x)$. Поскольку α – гомоморфизм групп, для действия композиции элементов группы имеем композицию их действий $\alpha(gg') = \alpha(g) \circ \alpha(g')$ и тождественное преобразование для нейтрального элемента $\alpha(e) = \text{id}_X$.

Более того, определение действия группы на множестве можно сформулировать следующим равносильным образом.

Определение 3.2.13. Действием группы G на множестве X называется отображение $\hat{\alpha}: G \times X \rightarrow X$, удовлетворяющее аксиомам:

1. Для нейтрального элемента $e \in G$ отображение $\hat{\alpha}_e$ – тождественное отображение;
2. Для любых двух элементов $g, g' \in G$ выполнено правило композиции $\hat{\alpha}_{gg'} = \hat{\alpha}_g \circ \hat{\alpha}_{g'}$.

Упражнение 3.2.14. Докажите, что из аксиом действия группы следует, что для любого элемента $g \in G$ справедливо $\hat{\alpha}_{g^{-1}} = \hat{\alpha}_g^{-1}$.

Упражнение 3.2.15. Докажите, что для любого $g \in G$ и естественной биекции

$$X \xrightarrow{\sim} g \times X : x \mapsto (g, x)$$

индуцированное отображение $\hat{\alpha}_g : X \rightarrow g \times X \xrightarrow{\sim} X$ биективно.

Определение 3.2.16. Орбитой точки $x \in X$ при действии $\hat{\alpha} : G \times X \rightarrow X$ группы G на множестве X называется образ $G(x) := \hat{\alpha}(G \times x)$.

Пример 3.2.17. Пусть X – множество точек евклидовой плоскости, $G = S^1$ – группа вращений относительно начала координат. Каждое вращение на угол $\phi \in [0, 2\pi)$ может быть интерпретировано как точка на окружности, имеющая полярную координату (полярный угол), равную ϕ . При этом композиции вращений соответствует сумма соответствующих им полярных углов. В этом смысле окружность S^1 наделена структурой группы, а группа вращений плоскости изоморфна группе S^1 . При действии группы S^1 вращениями плоскости получим следующее: орбиты всех точек, отличных от центра вращения (начала координат), представляют собой концентрические окружности с центром в начале координат. Орбита начала координат состоит из единственной точки – самого начала координат.

Пример 3.2.18. Пусть \mathbb{A}_k^n – n -мерное аффинное пространство над полем k . Как известно, аффинное пространство состоит из множества точек и n -мерного k -векторного пространства, связанных известным набором аксиом. Пусть X – множество точек аффинного пространства \mathbb{A}_k^n , V_n – ассоциированное векторное пространство аффинного пространства \mathbb{A}_k^n . Тогда имеет место действие $\tau : V_n \times X \rightarrow X : (v, \dot{x}) \mapsto \dot{x} + v$, ставящее в соответствие каждому вектору $v \in V_n$ и каждой точке $\dot{x} \in X$ точку $\dot{x} + v$, полученную параллельным переносом точки \dot{x} на вектор $v \in V_n$. При этом выполнены аксиомы:

1. Для любой точки $\dot{x} \in X$ $\dot{x} + 0 = \dot{x}$.
2. Для любой точки $\dot{x} \in X$ и для любых векторов $v, v' \in V_n$ выполнено $\dot{x} + (v + v') = (\dot{x} + v) + v'$.
3. Для любых точек $\dot{x}, \dot{x}' \in X$ существует вектор $v \in V_n$ такой, что $\dot{x}' = \dot{x} + v$.
4. Для любых точек $\dot{x}, \dot{x}' \in X$ вектор $v \in V_n$, описанный в п. 3, единственен.

Таким образом, структура аффинного пространства предполагает действие группы векторов на множестве точек, причём это действие обладает специальными свойствами, описанными в пп. 3 и 4, к которым мы ещё вернёмся. Орбитой каждой точки $\dot{x} \in X$ является всё множество X .

Соглашение 3.2.19. Пусть действие $\hat{\alpha} : G \times X \rightarrow X$ группы G на множестве X фиксировано. Тогда будем использовать сокращённое обозначение $g(x)$ вместо $\hat{\alpha}(g, x)$.

Определение 3.2.20. Действие $\hat{\alpha} : G \times X \rightarrow X$ группы G на множестве X называется *свободным*, если для любых различных $g, h \in G$ и любой точки $x \in X$ выполнено $g(x) \neq h(x)$.

Это означает, что при свободном действии невозможна ситуация $g(x) = x$ при $g \neq e$.

Определение 3.2.21. Точка $x \in X$ называется *неподвижной точкой* элемента $g \in G$ при действии $\hat{\alpha} : G \times X \rightarrow X$, если выполнено $g(x) = x$.

Свободное действие – это действие без неподвижных точек.

Определение 3.2.22. Действие $\hat{\alpha}: G \times X \rightarrow X$ группы G на множестве X называется *транзитивным*, если для любых точек $x, y \in X$ найдётся элемент $g \in G$ такой, что $g(x) = y$.

Иначе говоря, действие транзитивно, если любая его орбита совпадает со всем множеством X . Образно говоря, транзитивное действие сдвигает каждую точку в каждую точку (подходящим элементом группы для каждой пары точек).

Рассмотрим ограничение любого действия $\hat{\alpha}: G \times X \rightarrow X$ на любую из его орбит:

$$\hat{\alpha}|_{G(x)}: G \times G(x) \rightarrow G(x).$$

Действие $\hat{\alpha}|_{G(x)}$ транзитивно.

Транзитивное и свободное действие называют *регулярным*.

В частности, n -мерное аффинное пространство над полем k – это множество (точек), на котором аддитивная группа n -мерного k -векторного пространства действует транзитивно и свободно, т. е. регулярно (*Упражнение:* проверьте, что требования транзитивности и свободы действия гарантируют выполнение пп. 3 и 4 примера 3.2.18. Обратная импликация очевидна. Таким образом, это определение равносильно классическому определению аффинного пространства, обычно приводимому в книгах по геометрии, с аксиомами 1–4 примера 3.2.18).

Пример 3.2.23. Действие группы на себе левыми сдвигами определяется отображением

$$\lambda: G \times G \rightarrow G: (g, x) \mapsto gx.$$

Очевидно, оно регулярно. При этом действие каждого из элементов $g \in G$, отличного от нейтрального, не сохраняет групповую операцию $(gx)(gx') \neq g(xx')$ и поэтому не является гомоморфизмом групп.

Пример 3.2.24. Пусть $H < G$ – подгруппа. Действие группы левыми сдвигами на множестве её левых смежных классов по подгруппе H определяется отображением

$$\lambda_H: G \times \{gH\} \rightarrow \{gH\}: (g', gH) \mapsto g'gH.$$

Определение 3.2.25. Действие $\hat{\alpha}: G \times X \rightarrow X$ группы G на множестве X называется *эффективным*, если для любых двух элементов $g, h \in G$, $g \neq h$, существует точка $x \in X$ такая, что $g(x) \neq h(x)$.

Образно говоря, при эффективном действии каждый неединичный элемент сдвигает с места хотя бы одну точку.

Предложение 3.2.26. Орбиты любого действия группы $\hat{\alpha}: G \times X \rightarrow X$ образуют разбиение множества X .

Доказательство. Введём бинарное отношение \sim на множестве X : $x \sim x'$, если найдётся $g \in G$ такой, что $x' = g(x)$. Очевидно, это отношение рефлексивно. При этом, очевидно, $x = g^{-1}(x')$ и, тем самым, отношение \sim симметрично. Пусть, наконец, $x \sim x'$ и $x' \sim x''$, т. е. существуют $g, g' \in G$ такие, что $x' = g(x)$ и $x'' = g'(x')$. Тогда $x'' = g'(x') = g'g(x)$, т. е. $x \sim x''$, и \sim есть эквивалентность. В каждый класс относительно этого отношения эквивалентности входят точки одной орбиты и только они: $x \sim x'$ тогда и только тогда, когда $x' \in G(x)$. \square

Определение 3.2.27. Стабилизатором, или стационарной подгруппой, точки $x \in X$ при действии $\hat{\alpha}: G \times X \rightarrow X$ называется подгруппа $G_x = \{g \in G \mid g(x) = x\}$.

Понятно, что действие $\hat{\alpha}$ является свободным тогда и только тогда, когда стабилизаторы всех точек $x \in X$ тривиальны: $G_x = \{e\}$.

В частности, действие группы на себе левыми сдвигами транзитивно, эффективно и свободно. Действие группы G на множестве её левых смежных классов по подгруппе H транзитивно.

Теорема 3.2.28 (об орбите и стабилизаторе). *Пусть G – конечная группа, действующая на множестве X . Тогда порядок $|G|$ равен произведению порядка стабилизатора любой точки x на мощность её орбиты:*

$$|G| = |G_x| \cdot |G(x)|.$$

Доказательство. Рассмотрим стабилизатор $G_x < G$ и запишем для него теорему Лагранжа:

$$|G| = |G_x| \cdot [G : G_x].$$

Биекция множества левых смежных классов группы G относительно стабилизатора G_x на множество точек её орбиты устанавливается естественным соответствием: $gG_x \mapsto g(x)$. Действительно, для любого $h \in G_x$ имеем $gh(x) = g(h(x)) = g(x)$, т. е. все элементы одного и того же смежного класса действуют на точку x одинаковым образом. Обратно, пусть $g(x) = g'(x)$. Тогда $x = g^{-1}g(x) = g^{-1}g'(x)$, т. е. $g^{-1}g' \in G_x$. Отсюда следует, что $g' \in gG_x$, т. е. элементы g, g' принадлежат одному левому смежному классу относительно G_x . \square

Введём следующее обозначение для множества точек, неподвижных при действии элементом $g \in G$:

$$X^g := \{x \in X \mid g(x) = x\}.$$

Поскольку, как мы видели, действие группы G на множестве X индуцирует на нём отношение эквивалентности, приводящее к разбиению множества X на орбиты, то естественно образовать фактормножество X/G , представляющее собой множество орбит рассматриваемого действия.

Определение 3.2.29. Подмножество $Y \subseteq X$ называется G -инвариантным, если для любой точки $y \in Y$ выполнено $G(y) \subseteq Y$.

Теорема 3.2.30 (лемма Бёрнсайда). *Пусть конечная группа G действует на конечном множестве X . Тогда*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

Доказательство. Перепишем сумму в правой части утверждения теоремы в виде

$$\sum_{g \in G} |X^g| = |\{(g, x) \in G \times X \mid gx = x\}| = \sum_{x \in X} |G_x|.$$

По теореме об орбите и стабилизаторе $|G_x| = |G|/|G(x)|$. Итак, мы будем доказывать эквивалентное равенство

$$|X/G| = \sum_{x \in X} \frac{1}{|G(x)|}.$$

Заметим, что для любого разбиения множества G в объединение G -инвариантных подмножеств $X = \bigcup_{i \in I} Y_i$ из того, что теорема верна для каждого отдельного подмножества Y_i , следует её истинность для всего множества X . Поэтому достаточно доказать теорему для ограничения действия группы на одну орбиту.

Теорема в этом (транзитивном) случае принимает вид

$$1 = \sum_{x \in X} \frac{1}{|G(x)|},$$

причём $X = G(x)$, т. е. становится очевидным тождеством. \square

Определение 3.2.31. G -пространством называется множество X с фиксированным на нём действием α группы G .

Пусть (X, α) и (Y, β) – G -пространства.

Определение 3.2.32. G -эквивариантным отображением, или G -морфизмом, или морфизмом G -пространств называется такое отображение G -пространств $f: X \rightarrow Y$, что для каждого $g \in G$ коммутативна диаграмма

$$\begin{array}{ccc} X & \xrightarrow{g} & X \\ f \downarrow & & \downarrow f \\ Y & \xrightarrow{g} & Y \end{array}$$

Биективное G -эквивариантное отображение называют *изоморфизмом G -пространств*.

Пусть X и Y равномощны. Отождествив их каким-либо способом, мы можем считать, что все биекции из множества X в множество Y биективны перестановкам из группы S_X . Поэтому изоморфизм G -пространств часто называют *подстановочным изоморфизмом*, а сами G -пространства (X, α) и (Y, β) – *подстановочно эквивалентными G -пространствами*.

Соглашение 3.2.33. Если действие α транзитивно, то G -пространство (G, α) мы тоже будем называть транзитивным.

Следующий результат позволяет изучать действия группы на множестве её смежных классов вместо её конкретного действия на некотором множестве произвольной природы.

Теорема 3.2.34 (структура транзитивного действия). *Транзитивное G -пространство подстановочно эквивалентно действию группы G левыми сдвигами на множестве её левых смежных классов относительно стабилизатора любой из точек.*

Доказательство. Выберем (произвольную) точку $x \in X$ и рассмотрим разбиение $G = \bigcup gG_x$ группы G в объединение левых смежных классов относительно стабилизатора G_x точки x . Элементы g выбраны по одному из каждого смежного класса. Определим отображение f множества X во множество левых смежных классов вида gG_x следующим образом. Выбранной точке $x \in X$ поставим в соответствие класс $f(x) = eG_x$. Тогда для каждого $x' \in X$ в силу транзитивности действия существует $g' \in G$ такой, что $x' = g'x$, и тогда положим $f(x') = g'G_x$. Понятно, что f – G -эквивариантная биекция множества X на множество левых смежных классов вида gG_x . Это завершает доказательство. \square

3.2.3 Нормальная подгруппа. Факторгруппа

Определение 3.2.35. Подгруппа N *нормальна* в группе G , если для каждого элемента $g \in G$ его левый смежный класс по подгруппе N совпадает с его правым смежным классом, т. е. $gN = Ng$. Также нормальную подгруппу иногда называют *нормальным делителем*, или *инвариантной подгруппой*. Обозначение нормальной подгруппы: $N \triangleleft G$.

Очевидно, что в абелевой группе любая подгруппа нормальна.

Любая группа G содержит, как минимум, две нормальные подгруппы; это $\{e\}$ и G . Группа, не содержащая других нормальных подгрупп, называется *простой*. Таковы, например, все группы простых порядков (*упражнение*: докажите, что такие группы циклические) и знакопеременные группы A_n при $n \geq 5$ (доказательство этого факта весьма трудоёмко и здесь приведено не будет).

Пример 3.2.36. В симметрической группе S_3 имеются всего три нормальные подгруппы: тривиальная $\{e\}$, знакопеременная (она же – группа чётных перестановок) $A_3 \cong \mathbb{Z}_3$ и, наконец, сама группа S_3 . Аналогичная ситуация имеет место для симметрических групп S_n при $n \geq 5$ (однако, разумеется, знакопеременные группы A_n при $n \geq 3$ устроены гораздо сложнее, чем A_3 ; они нециклические и неабелевы): $\{e\}$, A_n , S_n . В группе S_4 имеется следующий набор нормальных подгрупп: $\{e\}$, $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ (так называемая *четверная группа Клейна*), A_4 и S_4 .

Замечание 3.2.37. Из того, что в цепочке подгрупп $L < M < N$ подгруппа L нормальна в M , а M нормальна в N , не следует, что L нормальна в N .

Заметим, что равенство $gN = Ng$ можно переписать в равносильной форме $N = gNg^{-1}$. Рассмотрев действие группы G на себе сопряжениями

$$G \times G \rightarrow G : (g, g') \mapsto gg'g^{-1},$$

видим, что подгруппа H неподвижна (как подмножество; каждый из её элементов может перемещаться) тогда и только тогда, когда она нормальна. Поэтому нормальные подгруппы называют инвариантными.

Замечание 3.2.38. Равенство левого и правого смежных классов $gN = Ng$ для любого элемента $g \in G$ означает следующее:

- для любого $n \in N$ существует $n' \in N$ такой, что $gn = n'g$;
- для любого $n \in N$ существует $n'' \in N$ такой, что $ng = gn''$.

Можно сказать, что нормальная подгруппа *перестановочна в целом* с любым элементом группы G .

Нормальная подгруппа обладает следующим замечательным свойством.

Предложение 3.2.39 (существование факторгруппы). *На множестве смежных классов группы G относительно её нормальной подгруппы $N \triangleleft G$ определена индуцированная бинарная операция, наделяющая это множество структурой группы.*

Доказательство. Под произведением смежных классов g_1N и g_2N понимают следующее множество:

$$(g_1N)(g_2N) = \{g_1n_1g_2n_2 \mid n_1, n_2 \in N\}.$$

Понятно, что произведение смежных классов относительно подгруппы в общем случае не является смежным классом относительно той же подгруппы. Однако если N – нормальная подгруппа, то существует $n'_1 \in N$ такой, что $n_1g_2 = g_2n'_1$, откуда

$$g_1n_1g_2n_2 = g_1g_2n'_1n_2 \in g_1g_2N.$$

Таким образом, $(g_1N)(g_2N) = g_1(Ng_2)N = g_1g_2NN \subseteq g_1g_2N$. Это включение определяет бинарную операцию для смежных классов относительно подгруппы N . Эта бинарная операция, очевидно, ассоциативна. Также $(g^{-1}N)(gN) \subseteq g^{-1}gN = eN$ и $(gN)(g^{-1}N) \subseteq gg^{-1}N = eN$. Наконец, для любого $g \in G$ имеем $(gN)(eN) = gN$ и $(eN)(gN) = e(gN) = gN$. Таким образом, на множестве смежных классов относительно подгруппы N действительно определена индуцированная структура группы. \square

Определение 3.2.40. Группа смежных классов, построенная в предложении 3.2.39, называется *факторгруппой* группы G относительно нормальной подгруппы N и обозначается G/N .

Замечание 3.2.41. Важно, что для определения бинарной операции на смежных классах относительно подгруппы N необходима её перестановочность в целом с любым элементом группы G . Поэтому бинарная операция определена только для смежных классов относительно нормальной подгруппы.

С формированием факторгруппы группы G относительно её нормальной подгруппы $N \triangleleft G$ связан гомоморфизм групп $\phi: G \rightarrow G/N: g \mapsto gN$.

Упражнение 3.2.42. Докажите, что любая подгруппа индекса 2 в любой группе G является в этой группе нормальной подгруппой.

3.2.4 Ядро и образ гомоморфизма групп. Теорема о гомоморфизме для групп

Определение 3.2.43. *Ядром* гомоморфизма групп $f: G \rightarrow G'$ называется подмножество

$$\ker f := \{g \in G \mid f(g) = e\}.$$

Упражнение 3.2.44. Докажите, что $\ker f \triangleleft G$.

В контексте групп символ $\ker f$ всюду понимается как обозначение подгруппы (к связи этой подгруппы с соответствующей конгруэнцией мы ещё вернёмся).

Определение 3.2.45. *Образом* гомоморфизма групп $f: G \rightarrow G'$ называется подмножество

$$\operatorname{im} f := \{f(g) \mid g \in G\}.$$

Упражнение 3.2.46. Докажите, что $\operatorname{im} f < G'$.

Замечание 3.2.47. Образ гомоморфизма групп может не быть нормальной подгруппой в области значений G' (приведите пример гомоморфизма групп, образ которого не является нормальным делителем).

Итак, пусть $f: G \rightarrow G'$ – гомоморфизм групп. Выясним, каким образом ядро отображения f , рассматриваемого как гомоморфизм группоидов (т. е. как конгруэнция) связано с ядром гомоморфизма f групп как подгруппой (т. е. с подгруппой $\ker f$). Пусть $\ker f = \{g \in G \mid f(g) = e\}$. Тогда для двух элементов $g_1, g_2 \in G$, имеющих в G' равные образы $f(g_1) = f(g_2)$, имеем $e = f(g_1)f(g_2)^{-1} = f(g_1g_2^{-1})$, т. е. $g_1g_2^{-1} \in \ker f$. По аналогичной причине $g_2^{-1}g_1 \in \ker f$. Понятно, что $g \in \ker f$ влечёт $(hg, h) \in K_f$ для всех $h \in G$. Итак, имеем отображение множеств

$$\Delta: G \times G \rightarrow G: (g_1, g_2) \mapsto g_1g_2^{-1},$$

причём образ конгруэнции K_f при этом отображении равен $\ker f$, т. е. включается в коммутативную диаграмму

$$\begin{array}{ccc} K_f & \hookrightarrow & G \times G \\ \downarrow & & \downarrow \Delta \\ \ker f & \hookrightarrow & G \end{array}$$

Поскольку K_f – конгруэнция, то из $(g_1, g_2) \in K_f$ следует, что для любого $h \in g$ выполнено $(hg_1, hg_2) \in K_f$. Тогда для образов при отображении Δ будем иметь: из $g_1g_2^{-1} \in \ker f$ следует $h(g_1g_2^{-1})h^{-1} \in \ker f$. Отсюда и из сюръективности ограничения $\Delta|_{K_f}$ имеем нормальность подгруппы $\ker f$.

Поэтому теорема о гомоморфизме для групп может быть сформулирована следующим образом.

Теорема 3.2.48 (о гомоморфизме для групп). *Любой гомоморфизм групп $f: G \rightarrow G'$ обладает разложением в композицию согласно коммутативной диаграмме*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow & & \uparrow \\ G/\ker f & \xrightarrow{\sim} & \operatorname{im} f \end{array}$$

В частности, теорема о гомоморфизме для групп позволяет перечислить факторгруппы и гомоморфизмы данной группы, используя перечень её нормальных подгрупп (для несложных подгрупп это позволяет решить задачу полностью, поскольку нетрудно перечислить нормальные подгруппы) и, соответственно, сделать вывод о существовании (или отсутствии) нетривиальных гомоморфизмов между двумя данными группами.

Упражнение 3.2.49. Опишите все гомоморфизмы группы D_3 симметрий правильного треугольника в группы, порядки которых не больше чем $|D_3|$.

3.2.5 Свойства нормальных подгрупп. Теоремы об изоморфизмах для групп

Определение 3.2.50. *Произведением подгрупп A и B группы G называется подмножество*

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

Если группа G абелева, то произведение любых двух её подгрупп является подгруппой. В произвольной ситуации произведение подгрупп может не быть подгруппой.

Предложение 3.2.51 (нормальность при пересечениях и произведениях). *Пусть G – произвольная группа, $A < G$ – подгруппа, $H \triangleleft G \triangleright K$ – две нормальные подгруппы. Тогда (1) $A \cap H \triangleleft A$, (2) $AH = \{ah \mid a \in A, h \in H\} < G$, (3) $K \cap H \triangleleft G$, (4) $KH \triangleleft G$.*

Доказательство. (1) Для любого $a \in A$ и любого $h \in A \cap H$ имеем $aha^{-1} \in A$ и $aha^{-1} \in H$ (поскольку $H \triangleleft G$). Таким образом, $a(A \cap H)a^{-1} = A \cap H$. (2) Для любых $a_1, a_2 \in A$ и любых $h_1, h_2 \in H$ воспользуемся критерием подгруппы, вычислив

$$(a_1 h_1)(a_2 h_2)^{-1} = a_1 h_1 h_2^{-1} a_2^{-1} = a_1 a_2^{-1} h'$$

для подходящего $h' \in H$. Здесь мы воспользовались совпадением левого и правого смежных классов относительно нормальной подгруппы H , благодаря которому $h_1 h_2^{-1} a_2^{-1} = a_2^{-1} h'$. (3) Для любого $g \in G$ и для любого $h \in K \cap H$ имеем, в силу нормальности подгрупп K и H , $ghg^{-1} \in K \cap H$, т. е. $g(K \cap H)g^{-1} \subseteq K \cap H$, откуда $g(K \cap H)g^{-1} = K \cap H$ для всех $g \in G$. (4) Для любого $g \in G$ имеем $gKHg^{-1} = (gKg^{-1})(gHg^{-1}) \subseteq KH$, откуда $gKHg^{-1} = KH$ для всех $g \in G$. \square

Определение 3.2.52. *Полным прообразом подмножества $S \subset T'$ при отображении $f: T \rightarrow T'$ называется подмножество*

$$f^{-1}(S) = \{t \in T \mid f(t) \in S\}.$$

Полезно заметить, что полным прообразом элемента $f(g) \in G'$ при гомоморфизме групп $f: G \rightarrow G'$ является смежный класс $g\ker f$.

Предложение 3.2.53 (образ и прообраз подгруппы и нормальной подгруппы). *Пусть $f: G \rightarrow G'$ – гомоморфизм групп. Тогда (1) для любой подгруппы $A < G$ выполнено равенство $f^{-1}f(A) = A \cdot \ker f$, (2) для любой нормальной подгруппы $B \triangleleft G'$ её полный прообраз нормален: $f^{-1}B \triangleleft G$. Если к тому же гомоморфизм f сюръективен, то (3) для любой подгруппы $B < G'$ выполнено $f(f^{-1}(B)) = B$, (4) для любой нормальной подгруппы $A \triangleleft G$ её образ также нормален $f(A) \triangleleft G'$.*

Доказательство. (1) $f^{-1}f(a) = a \ker f$, откуда

$$f^{-1}f(A) = \bigcup_{a \in A} f^{-1}f(a) = \bigcup_{a \in A} a \ker f = A \cdot \ker f.$$

(2) Для любого $b \in B$ и любого $g \in G$ имеем $f(g)bf(g)^{-1} \in B$. Тогда для любого из образов bk , $k \in \ker f$, элемента b значение выражения $g(bk)g^{-1}$ принадлежит множеству $f^{-1}(f(g)bf(g)^{-1}) \subset f^{-1}B$. Доказательство пп. (3) и (4) предлагается читателю в качестве упражнения. \square

Теорема 3.2.54 (первая теорема об изоморфизме для групп). *Пусть $\phi: G \rightarrow G'$ – гомоморфизм групп, A – подгруппа в группе G . Тогда*

$$\phi(A) \cong A/(A \cap \ker \phi).$$

Доказательство. То, что $A \cap \ker \phi \triangleleft A$, доказано в п. 1 предложения 3.2.51. Рассмотрим коммутативную диаграмму

$$\begin{array}{ccccc} \ker \phi & \xhookrightarrow{\quad} & G & \xrightarrow{\quad \phi \quad} & G' \\ \uparrow & & \uparrow & & \uparrow \\ A \cap \ker \phi & \xhookrightarrow{\quad} & A & \xrightarrow{\quad \psi \quad} & \phi(A) \end{array}$$

в которой гомоморфизм $\psi: A \rightarrow \phi(A)$ индуцирован ограничением $\phi|_A$. Тогда

$$\ker \psi = \{a \in A \mid \phi(a) = e\} = \{a \in A \mid \psi(a) = e\} = A \cap \ker \phi.$$

Применив теорему о гомоморфизме к гомоморфизму ψ , получим $\phi(A) \cong A/(A \cap \ker \phi)$. \square

Следствие 3.2.55 (ограничение факторизации на подгруппу). *Если $H \triangleleft G$ и $A < G$, то $H \triangleleft AH$, $A \cap H \triangleleft A$, $AH/H \cong A/(A \cap H)$.*

Доказательство. Рассмотрим гомоморфизм групп $\phi: G \rightarrow G/H$. По предложению 3.2.53, $\phi^{-1}\phi(A) = A \cdot \ker \phi = AH$. Так как $\phi\phi^{-1}\phi(A) = \phi(A)$, то $\phi\phi^{-1}\phi(A) = \phi(AH) = \phi(A)$. Дважды применив первую теорему об изоморфизме для групп, получим

$$\phi(A) \cong A/(A \cap \ker \phi) = A/(A \cap H)$$

и

$$\phi(A) \cong AH/(AH \cap \ker \phi) = AH/(AH \cap H) = AH/H.$$

\square

Теорема 3.2.56 (вторая теорема об изоморфизме для групп). *Пусть $\phi: G \rightarrow G'$ – сюръективный гомоморфизм групп и $H \triangleleft G$, тогда $\phi(H) \triangleleft G'$ и имеет место изоморфизм $G'/\phi(H) \cong G/(H \cdot \ker \phi)$.*

Доказательство. Нормальность образа $\phi(H) \triangleleft G'$ является результатом п. (4) предложения 3.2.53. Рассмотрим гомоморфизм $\phi_0: G' \rightarrow G'/\phi(H)$ и композицию

$$\begin{array}{ccc} G & \xrightarrow{\quad \phi \quad} & G' \\ & \searrow \psi & \downarrow \phi_0 \\ & & G'/\phi(H) \end{array}$$

По теореме о гомоморфизме для групп, применённой к гомоморфизму ψ , имеем изоморфизм факторгрупп $G'/\phi(G') \cong G/\ker \psi$. Докажем, что $\ker \psi = H \cdot \ker \phi$. Действительно, $g \in \ker \psi$ тогда и только тогда, когда $\phi(g)\phi(H) = \phi(H)$, т. е. тогда и только тогда, когда $\phi(g) \in \phi(H)$, т. е. $g \in \phi^{-1}\phi(H) = H \cdot \ker \phi$. \square

Следствие 3.2.57 (правило сокращения для факторгрупп). Пусть $N \triangleleft G \supset H$, причём $N < H$. Тогда $H/N \triangleleft G/N$, причём имеет место изоморфизм

$$G/H \cong \frac{G/N}{H/N}.$$

Доказательство. Заметим, что H/N – образ подгруппы H при сюръективном гомоморфизме $\phi: G \rightarrow G/N$, и тогда

$$\frac{G/N}{\phi(H)} = \frac{G/N}{H/N}.$$

Применив вторую теорему об изоморфизме для групп, получим

$$\frac{G/N}{\phi(H)} \cong \frac{G}{H \cdot \ker \phi}.$$

Поскольку $N < H$, имеем $H \cdot \ker \phi = HN = H$. □

3.3 Образующие элементы группы. Свободная группа. Задание группы образующими и определяющими соотношениями

Определение 3.3.1. Подмножество M группы G называется *порождающим подмножеством*, или *множеством (системой) образующих* группы G , если каждый элемент $g \in G$ обладает представлением в виде композиции конечного числа элементов из M и обратных к ним: $g_1^{m_1} \dots g_s^{m_s}$, $g_i \in M$, $m_i \in \mathbb{Z}$, $i = 1, \dots, s$, $s \in \mathbb{N}$. Сами элементы множества M называются *порождающими элементами*, или *образующими*, группы G . При этом говорят, что группа G *порождается* подмножеством M . Для записи факта порождения группы G её подмножеством M используют запись $G = \langle M \rangle$.

Замечание 3.3.2. Очевидно, что любая группа порождается множеством всех своих элементов, т. е. $G = \langle G \rangle$.

Пример 3.3.3. Как и любая циклическая группа, группа \mathbb{Z} целых чисел может быть задана одной образующей \mathbb{Z} :

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle.$$

Пример 3.3.4. Группа D_n (n -я диэдральная группа) симметрий правильного n -угольника состоит из n вращений на углы $2\pi\ell/n$, $\ell = 0, \dots, n-1$, и осевых симметрий относительно n осей, которыми обладает правильный n -угольник. Таким образом, n -я диэдральная группа имеет порядок, равный $2n$. Заметим, что «двуугольник» с группой симметрии D_2 понимается в условном смысле: его можно мыслить как часть плоскости, ограниченную двумя равными дугами равных окружностей; эта часть плоскости имеет два угла, её симметриями являются повороты на 0 и π , а также осевые симметрии относительно хорды, соединяющей углы, и относительно её серединного перпендикуляра. Группа D_n порождается, например, двумя образующими следующего вида: поворотом r на $2\pi/n$ и любой из осевых симметрий t .

Замечание 3.3.5. В одной и той же группе можно выбирать разные системы образующих, которые могут иметь различные мощности.

Определение 3.3.6. Группа G называется *конечно порождённой*, если она допускает задание конечной системой образующих.

Пример 3.3.7. Мультипликативная группа поля рациональных чисел $\mathbb{Q} \setminus 0, \cdot$ не является конечно порождённой.

Пусть теперь A – множество, которое мы условимся называть *алфавитом*, а его элементы a_1, a_2, \dots – *буквами*.

Определение 3.3.8. *Групповым словом* над алфавитом A называется выражение $w = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$, $a_i \in A$, $\varepsilon_i \in \{\pm 1\}$, $i = 1, \dots, n$, $n \in \mathbb{N}$. Также рассматривается *пустое слово* e , не содержащее ни одной буквы. Множество всех групповых слов над алфавитом A обозначается символом W_A .

Определение 3.3.9. *Подсловом* слова $a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ называется любое слово вида $a_i^{\varepsilon_i} \dots a_{i+t}^{\varepsilon_{i+t}}$.

Определение 3.3.10. Слова w и w' называются *эквивалентными* (обозначение: $w \sim w'$), если они либо совпадают, либо отличаются последовательными вставкой/удалением одного или нескольких подслов вида aa^{-1} , $a^{-1}a$.

Пример 3.3.11. Слова $a_1a_2a_3^{-1}a_3a_3^{-1}a_1a_4a_5^{-1}$ и $a_1bcc^{-1}ba_2a_3^{-1}a_1a_4a_5^{-1}$ эквивалентны. Слова *abracadabra* и *aaaaabbcdrr* не эквивалентны.

На множестве групповых слов W_A определена операция конкатенации

$$a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} \circ b_1^{\delta_1} \dots b_m^{\delta_m} = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} b_1^{\delta_1} \dots b_m^{\delta_m},$$

причём на фактормножестве W_A / \sim она индуцирует структуру группы. Пусть $[w]$ – класс слов, эквивалентных слову w . Тогда $[w][w'] = [w \circ w']$, $[a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}]^{-1} = [a_n^{-\varepsilon_n} \dots a_1^{-\varepsilon_1}]$, $[e]$ – нейтральный элемент.

Определение 3.3.12. *Свободной группой* над алфавитом A называется группа классов эквивалентных групповых слов над алфавитом A с операцией, индуцированной конкатенацией на словах. Свободную группу над алфавитом A будем обозначать символом F_A .

Для группы G с выбранной в ней системой образующих M зафиксируем биекцию

$$A \xrightarrow{\sim} M : a \mapsto m.$$

Эта биекция индуцирует сюръективный гомоморфизм групп

$$ev : F_A \rightarrow G : a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} \mapsto m_1^{\varepsilon_1} \dots m_n^{\varepsilon_n}.$$

Выражение $m_1^{\varepsilon_1} \dots m_n^{\varepsilon_n}$ вычисляет значение слова $a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ в группе G , поэтому имеет смысл назвать этот гомоморфизм *гомоморфизмом вычисления*.

Определение 3.3.13. Любую систему образующих R для ядра $\ker ev$ данного гомоморфизма вычисления $ev : F_A \rightarrow G$ называют *множеством определяющих соотношений* в группе G относительно системы образующих M . Итак, $\ker ev = \langle R \rangle$.

Определение 3.3.14. Группа G называется *конечно определённой*, если она допускает выбор конечной системы образующих M , для которой множество определяющих соотношений R может быть выбрано также конечным.

Итак, группа G задаётся данными $\langle M | R \rangle$, которые называются *генетическим кодом* группы G .

Пример 3.3.15. Циклическая группа порядка n задаётся генетическим кодом $\langle a \mid (a^n, e) \rangle$.

Пример 3.3.16. Диэдральная группа D_n задаётся генетическим кодом

$$\langle a, b \mid (a^n, e), (b^2, e), ((ab)^2, e) \rangle.$$

Пример 3.3.17. Симметрическая группа S_n порождена транспозициями $g_i = (i, i + 1)$, $i = 1, \dots, n - 1$. Тогда определяющие соотношения для такого задания симметрической группы имеют вид

$$\begin{aligned} (g_i^2, e), \quad i = 1, \dots, n - 1, \\ (g_i g_j, g_j g_i), \quad i, j = 1, \dots, n - 1, \quad |i - j| > 1 \quad (n > 3), \\ (g_i g_{i+1} g_i, g_{i+1} g_i g_{i+1}), \quad i = 1, \dots, n - 2 \quad (n > 2). \end{aligned}$$

Понятно, что одна и та же группа допускает разные задания.

Переход от одного задания группы G к другому осуществляется *преобразованиями Титце* четырёх типов. К ним относятся:

1. Добавление нового соотношения, выражаемого через старые.
2. Ввод новой образующей, выражаемой через старые.
3. Исключение соотношения, выражаемого через остальные.
4. Исключение образующей, выражаемой через остальные.

Пусть даны два генетических кода $\langle M_1 | R_1 \rangle$ и $\langle M_2 | R_2 \rangle$. Проблема изоморфизма, или проблема Дэна, состоит в следующем: *выяснить, изоморфны ли группы $\langle M_1 | R_1 \rangle$ и $\langle M_2 | R_2 \rangle$* . Задача проверки истинности высказывания *алгоритмически неразрешима*, если для неё принципиально не существует алгоритма, дающего ответ «истинно/ложно» для любого набора допустимых входных данных за конечное число шагов работы алгоритма.

В классе всех конечно определённых групп проблема Дэна алгоритмически неразрешима.

3.4 Прямое произведение групп. Разложение группы в прямое произведение

Пусть G, \circ и $H, *$ – группы.

Определение 3.4.1. (Внешним) *прямым произведением* групп G, \circ и $H, *$ называется группа со множеством элементов $G \times H = \{(g, h) | g \in G, h \in H\}$, бинарной операцией $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$, нейтральным элементом $e = (e_G, e_H)$ и правилом обращения $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Замечание 3.4.2. Иными словами, структура группы на прямом произведении индуцируется групповыми структурами сомножителей.

С конструкцией внешнего прямого произведения связаны четыре гомоморфизма групп:

- два вложения подгрупп

$$\begin{aligned} i_G: G \hookrightarrow G \times H, \quad g \mapsto (g, e_H), \\ i_H: H \hookrightarrow G \times H, \quad h \mapsto (e_G, h). \end{aligned}$$

- две проекции на сомножители

$$\begin{aligned} p_G: G \times H \longrightarrow G, \quad (g, h) \mapsto g, \\ p_H: G \times H \longrightarrow H, \quad (g, h) \mapsto h. \end{aligned}$$

Понятно, что каждое из этих вложений является сечением одноимённой проекции:

$$p_G \circ i_G = \text{id}_G, \quad p_H \circ i_H = \text{id}_H.$$

Также имеем

$$\begin{aligned} \ker p_G &= \{(e_G, h) | h \in H\} = i_H(H), \\ \ker p_H &= \{(g, e_H) | g \in G\} = i_G(G). \end{aligned}$$

Заметим следующее:

- образы обоих вложений являются нормальными подгруппами в $G \times H$:

$$G \cong i_G(G) \triangleleft G \times H \triangleright i_H(H) \cong H;$$

- $G = i_G(G)i_H(H)$, причём элементы, взятые по одному из каждой подгруппы $i_G(G)$ и $i_H(H)$, коммутируют:

$$\forall g \in G \forall h \in H \quad (g, e_H) \cdot (e_G, h) = (g, h) = (e_G, h) \cdot (g, e_H);$$

- пересечение подгрупп $i_G(G)$ и $i_H(H)$ тривиально: $i_G(G) \cap i_H(H) = \{e\}$;
- каждый элемент (g, h) группы $G \times H$ обладает единственным разложением

$$(g, h) = (g, e_H) \cdot (e_G, h), \quad g \in G, \quad h \in H.$$

Это означает, что для каждого элемента $(g, h) \in G \times H$ элементы $g \in G$ и $h \in H$ определены единственным образом.

Конструкция внешнего прямого произведения позволяет использовать произвольные (абстрактные) группы в качестве сомножителей. Однако часто аналогичная структура возникает, когда группа изоморфна прямому произведению некоторых своих подгрупп, если эти подгруппы рассматривать как абстрактные группы. С точки зрения алгебраической структуры внутреннее и внешнее прямые произведения не различаются.

Определение 3.4.3. Группа G является (внутренним) прямым произведением своих подгрупп H_1 и H_2 , если:

- любые элементы $h_1 \in H_1$ и $h_2 \in H_2$ (взятые из различных подгрупп) коммутируют: $h_1 h_2 = h_2 h_1$;
- каждый элемент $g \in G$ обладает однозначным разложением $g = h_1 h_2$, где $h_1 \in H_1$ и $h_2 \in H_2$.

Теорема 3.4.4 (разложение группы в прямое произведение двух подгрупп). *Группа G является прямым произведением своих подгрупп H_1 и H_2 (т. е. $G = H_1 \times H_2$) тогда и только тогда, когда каждый элемент $g \in G$ представим в виде конечного произведения элементов из объединения $H_1 \cup H_2$, причём выполнены следующие условия:*

1. Подгруппы H_1 и H_2 имеют тривиальное пересечение: $H_1 \cap H_2 = \{e\}$;
2. Обе подгруппы являются нормальными подгруппами в группе G :

$$H_1 \triangleleft G \triangleright H_2;$$

3. Элементы, взятые по одному из каждой подгруппы H_i , $i = 1, 2$, коммутируют:

$$\forall h_1 \in H_1 \forall h_2 \in H_2 \quad h_1 h_2 = h_2 h_1.$$

Доказательство. Пусть группа G является прямым произведением своих подгрупп $G = H_1 H_2$, и пусть существует элемент $h \neq e$ такой, что $h \in H_1 \cap H_2$. Выберем произвольные элементы $h_1 \in H_1$ и $h_2 \in H_2$. Тогда имеем два различных представления элемента $h_1 h_2$ в виде произведения: $h_1 h_2 = (h_1 h)(h^{-1} h_2)$, что противоречит определению прямого произведения подгрупп. Для доказательства нормальности подгруппы H_1 рассмотрим сопряжение её произвольного элемента \hat{h}_1 произвольным элементом $g \in G$ (при этом учтём, что элемент g обладает разложением $g = h_1 h_2$ и что элементы подгруппы H_1 перестановочны с элементами подгруппы H_2): $g \hat{h}_1 g^{-1} = h_1 h_2 \hat{h}_1 h_2^{-1} h_1^{-1} = h_1 \hat{h}_1 h_2 h_2^{-1} h_1^{-1} = h_1 \hat{h}_1 h_1^{-1} \in H_1$. Нормальность подгруппы H_2 доказывается аналогично.

Пусть группа G содержит две подгруппы $H_1 < G > H_2$ такие, что каждый элемент $g \in G$ представим в виде конечного произведения элементов из объединения $H_1 \cup H_2$, причём выполнены условия 1 – 3. Поскольку элементы подгруппы H_1 коммутируют с элементами подгруппы H_2 , то любое произведение вида $h_1^{(1)} h_2^{(1)} h_1^{(2)} h_2^{(2)} \dots h_1^{(s)} h_2^{(s)}$, в котором $h_i^{(j)} \in H_i$, $i = 1, 2$, $j = 1, \dots, s$, можно переписать в виде $h_1^{(1)} h_2^{(1)} h_1^{(2)} h_2^{(2)} \dots h_1^{(s)} h_2^{(s)} = h_1^{(1)} h_1^{(2)} \dots h_1^{(s)} h_2^{(1)} h_2^{(2)} \dots h_2^{(s)} = \hat{h}_1 \hat{h}_2$, где $\hat{h}_i \in H_i$, $i = 1, 2$. \square

Замечание 3.4.5. Аналогично можно определить прямое произведение любого семейства групп и доказать аналогичную теорему о группе, представимой в виде прямого произведения некоторого семейства своих подгрупп. Доказательство легко распространяется на этот случай.

Определение 3.4.6. Группа G является (*внутренним*) *прямым произведением* своих подгрупп $H_\iota < G$, $\iota \in I$, если:

- любые элементы двух различных подгрупп $h_\iota \in H_\iota$ и $h_\nu \in H_\nu$, $\iota \neq \nu$, коммутируют: $h_\iota h_\nu = h_\nu h_\iota$;
- каждый элемент $g \in G$ обладает однозначным разложением $g = \prod_{\iota \in I} h_\iota$, где $h_\iota \in H_\iota$ и произведение содержит конечное число неединичных сомножителей.

Теорема 3.4.7 (разложение группы в прямое произведение семейства подгрупп). *Группа G является прямым произведением своих подгрупп H_ι , $\iota \in I$, тогда и только тогда, когда каждый элемент $g \in G$ представим в виде конечного произведения элементов из объединения $\bigcup_{\iota \in I} H_\iota$, причём выполнены следующие условия:*

1. Для любого $\iota \in I$ подгруппы H_ι и $\prod_{v \in I, v \neq \iota} H_v$ имеют тривиальное пересечение:

$$H_\iota \cap \bigcup_{v \in I, v \neq \iota} H_v = \{e\};$$

2. Все подгруппы H_ι , $\iota \in I$, являются нормальными подгруппами в группе G ;
3. Элементы любых двух различных подгрупп H_ι , H_ν , $\iota, \nu \in I$, $\iota \neq \nu$, коммутируют:

$$\forall h_\iota \in H_\iota \forall h_\nu \in H_\nu, \quad h_\iota h_\nu = h_\nu h_\iota.$$

Следующий результат, хорошо известный читателю, является прямым следствием теоремы о разложении группы.

Следствие 3.4.8 (китайская теорема об остатках для групп классов вычетов). *Пусть n – натуральное число и $n = m_1 m_2 \dots m_s$ – его разложение на попарно взаимно простые множители. Тогда имеет место изоморфизм групп*

$$\mathbb{Z}_n \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_s}.$$

Упражнение 3.4.9. Прямое произведение циклических групп является циклической группой тогда и только тогда, когда порядки сомножителей попарно взаимно просты. Докажите часть «только тогда» (часть «тогда» составляет содержание следствия).

Замечание 3.4.10. В том случае, когда группа записывается аддитивно, вместо произведения её подгрупп говорят об их сумме, а вместо прямого произведения \times – о прямой сумме \oplus .

3.5 Конечно порождённые абелевы группы

В этом разделе мы получим структурную теорему о конечных абелевых группах и сформулируем без доказательства теорему о конечно порождённых абелевых группах.

3.5.1 Строение конечных абелевых групп

Теорема 3.5.1 (существование элемента простого порядка, являющегося делителем порядка группы). Пусть G – конечная абелева группа и p – простой делитель её порядка. Тогда группа G содержит элемент порядка p .

Доказательство. Доказательство проводится индукцией по порядку группы G . В случае $|G| = 1$ теорема тривиально верна. Предположим, что она верна для групп, имеющих порядки меньшие чем $|G|$. Очевидно, что в группе G существует элемент (какого-нибудь) простого порядка, скажем, равного q . Действительно, по теореме о циклических группах, если $\text{ord } x = m$ и q – простой множитель в m , то $x^{m/q}$ имеет порядок, равный q . Если $q = p$, то искомым элемент найден. Итак, пусть y – элемент порядка q .

В противном случае рассмотрим факторгруппу $G^* = G/\langle y \rangle$. Тогда $|G^*| = |G|/q$ и при этом p – делитель числа $|G^*|$. По предположению индукции, группа G^* содержит элемент \bar{g} порядка p . Для соответствующего ему смежного класса имеем $(g\langle y \rangle)^p = g^p\langle y \rangle = \langle y \rangle$ и, следовательно, $g^p \in \langle y \rangle$. Отсюда либо $g^p = e$, либо $\text{ord}(g^p) = q$ (поскольку q – простое число). В первом случае g – искомым элемент. Во втором случае $\text{ord } g = pq$, и тогда g^q – искомым. \square

Основной целью этого раздела является доказательство следующей теоремы.

Теорема 3.5.2 (строение конечной абелевой группы). Всякая конечная абелева группа G изоморфна прямому произведению циклических групп, порядки которых равны степеням простых делителей порядка $|G|$ группы G , т. е.

$$G \cong \mathbb{Z}_{p_1^{\ell_1}} \times \mathbb{Z}_{p_2^{\ell_2}} \times \cdots \times \mathbb{Z}_{p_s^{\ell_s}}, \quad (3.5.1)$$

где p_i , $i = 1, \dots, s$, – простые числа. Разложение (3.5.1) единственно с точностью до перестановки сомножителей.

Лемма 3.5.3 (выделение примарного сомножителя в конечной абелевой группе). Пусть G – конечная абелева группа, имеющая порядок $p^n m$, где p – простое число и m не делится на p . Тогда группа G представима в виде прямого произведения $G \cong H \times K$, где

$$\begin{aligned} H &= \{x \in G \mid x^{p^n} = e\}, \\ K &= \{x \in G \mid x^m = e\}. \end{aligned}$$

Более того, $|H| = p^n$.

Доказательство. Понятно, что H и K – подгруппы в группе G . Поскольку G абелева, достаточно показать, что $G = HK$ и $H \cap K = \{e\}$. Поскольку p^n и m взаимно просты, то найдутся $s, t \in \mathbb{Z}$ такие, что $sm + tp^n = 1$. Тогда для любого элемента $x \in G$ выполнено $x = x^{ms} \cdot x^{p^{nt}}$. Отсюда имеем $(x^{ms})^{p^n} = x^{|G|s} = e$ и $(x^{p^{nt}})^m = x^{|G|t} = e$, т. е. $x^{ms} \in H$ и $x^{p^{nt}} \in K$. Итак, $G = HK$.

Пусть $x \in H \cap K$. Тогда $x^{p^n} = e = x^m$ и, следовательно, $\text{ord } x$ является общим делителем чисел p^n и m . Поскольку эти числа взаимно просты, то $\text{ord } x = 1$, т. е. $x = e$.

Для доказательства того, что $|H| = p^n$, заметим, что

$$p^n m = |HK| = \frac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K|,$$

и достаточно убедиться в том, что число p не является делителем числа $|K|$. В противном случае в подгруппе K нашёлся бы элемент x порядка p (теорема 3.5.1), и тогда число $p = |\langle x \rangle|$ было бы делителем числа m (поскольку в подгруппе K все элементы удовлетворяют уравнению $x^m = e$), что противоречит предположению о взаимной простоте чисел p^n и m . \square

Итак, пусть

$$|G| = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$$

– стандартное разложение порядка группы G на простые множители. Считаем, что $p_i \neq p_j$ при $i \neq j$. Введём обозначение

$$G(p_i) := \{x \in G \mid x^{p_i^{n_i}} = e\}.$$

По индукции, применив лемму 3.5.3, имеем прямое разложение:

$$G = G(p_1) \times G(p_2) \times \dots \times G(p_r), \quad |G(p_i)| = p_i^{n_i}, \quad i = 1, \dots, r.$$

Лемма 3.5.4 (выделение циклического сомножителя максимального порядка в примарной абелевой группе). Пусть G – абелева группа, имеющая порядок p^n , $a \in G$ – элемент максимального порядка в группе G . Тогда группа G изоморфна прямому произведению $G \cong \langle a \rangle \times K$.

Доказательство. Индукция по n . При $n = 1$ группа G является циклической, и $G \cong \langle a \rangle \times \{e\}$. Предположим, что лемма верна для групп, имеющих порядки, равные p^k , $k < n$. Выберем элемент a максимального порядка p^m в группе G . Тогда $x^{p^m} = e$ для всех элементов $x \in G$. Будем считать, что $G \neq \langle a \rangle$ (иначе доказывать нечего). Теперь среди элементов группы G , не принадлежащих подгруппе $\langle a \rangle$, выберем элемент b минимального порядка и докажем, что $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Прежде убедимся в том, что $\text{ord } b = p$. Поскольку $b \in G$ и $|G| = p^n$, то $\text{ord } b = p^m$ для некоторого $m \leq n$. Тогда $\text{ord } b^p = (\text{ord } b)/p = p^{m-1}$. При этом $\text{ord } b$ – наименьший из порядков всех элементов множества $G \setminus \langle a \rangle$. Тогда $b^p \in \langle a \rangle$. Отсюда для любого i имеем $\text{ord } a^i \leq p^{m-1}$. Таким образом, a^i не является образующей подгруппы $\langle a \rangle$, и числа i и p^m имеют неединичный общий делитель, т. е. $i = pj$ для некоторого j . Итак, $b^p = a^{pj} = a^i$.

Рассмотрим элемент $c = a^{-j}b$. Понятно, что $c \notin \langle a \rangle$ (в противном случае с необходимостью $b \in \langle a \rangle$). Также $c^p = a^{-pj}b^p = e$. Таким образом, найден элемент $c \notin \langle a \rangle$ такой, что $\text{ord } c = p$. Поскольку элемент b был выбран как элемент подмножества $G \setminus \langle a \rangle$, имеющий наименьший порядок, то с необходимостью $\text{ord } b = \text{ord } c = p$.

Теперь покажем, что из $\text{ord } b = p$ следует $\langle a \rangle \cap \langle b \rangle = \{e\}$. Предположим противное: найдутся $i > 0$ и $j > 0$ такие, что $b^i = a^j$. Тогда либо $\text{ord } b^i = p$, либо $\text{ord } b^i = 1$. В первом случае найдётся натуральное u такое, что $b = (b^i)^u = (a^j)^u \in \langle a \rangle$, что противоречит выбору элемента b . Во втором случае $b^i = a^j = e$, и $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Теперь рассмотрим факторгруппу $\bar{G} = G/\langle b \rangle$. Для элемента $x \in G$ будем обозначать символом \bar{x} его образ в \bar{G} . Если $\text{ord } \bar{a} < \text{ord } a = p^m$, то $\bar{a}^{p^{m-1}} = \bar{e}$. Это означает, что $(a\langle b \rangle)^{p^{m-1}} = a^{p^{m-1}}\langle b \rangle = \langle b \rangle$, так что $a^{p^{m-1}} \in \langle a \rangle \cap \langle b \rangle = \{e\}$. Это противоречит факту $\text{ord } a = p^m$. Поэтому $\text{ord } \bar{a} = \text{ord } a = p^m$, и \bar{a} – элемент максимального порядка в группе \bar{G} .

По индукции $\bar{G} \cong \langle \bar{a} \rangle \times \bar{K}$ для некоторой подгруппы $\bar{K} < \bar{G}$. Пусть K – полный прообраз подгруппы \bar{K} относительно гомоморфизма на факторгруппу $G \twoheadrightarrow \bar{G}$. Покажем, что $\langle a \rangle \cap K = \{e\}$. Пусть $x \in \langle a \rangle \cap K$ и, соответственно, $\bar{x} \in \langle \bar{a} \rangle \cap \bar{K} = \{\bar{e}\}$. Таким образом, $x \in \langle a \rangle \cap \langle b \rangle = \{e\}$.

Наконец, покажем, что $G = \langle a \rangle K$. Выберем произвольный элемент $g \in G$. Поскольку группа G конечна, то существует натуральное ℓ такое, что $g^\ell \in \langle a \rangle$. Выберем наименьшее возможное из таких ℓ , т. е. такое, что $g^{\ell-1} \notin \langle a \rangle$. Тогда $g = gg^{\ell-1}g^{-(\ell-1)} = g^\ell g^{-(\ell-1)}$. При этом $g^\ell \in \langle a \rangle$, а $g^{-(\ell-1)} \in K$. Таким образом, разложение $G \cong \langle a \rangle \times K$ доказано. \square

Лемма 3.5.4 и индукция по n приводят к следующему результату.

Лемма 3.5.5 (разложение примарной абелевой группы в прямое произведение циклических групп). *Пусть G – конечная абелева группа, порядок которой равен p^n , где p – простое число. Тогда G изоморфна прямому произведению циклических групп.*

Факторы $G(p_i)$ определяются единственным образом, поскольку они содержат в себе элементы, порядки которых равны степеням простых чисел p_i , $i = 1, \dots, r$. Для завершения доказательства теоремы о конечных абелевых группах остаётся доказать единственность разложения каждой из групп $G(p_i)$ в прямое произведение циклических групп.

Лемма 3.5.6 (единственность разложения примарной абелевой группы в произведение циклических). *Пусть G – конечная абелева группа и $|G| = p^n$. Если имеют место два разложения $G \cong H_1 \times H_2 \times \dots \times H_m$ и $G \cong K_1 \times K_2 \times \dots \times K_n$, где все H_i , $i = 1, \dots, m$, и все K_j , $j = 1, \dots, n$, – нетривиальные циклические группы и $|H_1| \geq |H_2| \geq \dots \geq |H_m|$ и $|K_1| \geq |K_2| \geq \dots \geq |K_n|$, то $m = n$ и $|H_i| = |K_i|$, $i = 1, \dots, n$.*

Доказательство. Индукция по n . При $n = 1$ лемма тривиально верна. Предположим, что она верна для всех абелевых групп, имеющих порядки меньше чем $|G|$. Для любой абелевой группы L подмножество $L^p := \{x^p \mid x \in L\}$ является подгруппой в группе L . Следовательно, для подгруппы $G^p < G$ имеют место разложения $G^p \cong H_1^p \times H_2^p \times \dots \times H_m^p$ и $G^p \cong K_1^p \times K_2^p \times \dots \times K_{n'}^p$, где m' – наибольшее целое i такое, что $|H_i| > p$ и n' – наибольшее целое j такое, что $|K_j| > p$. Такой выбор m' и n' гарантирует отсутствие тривиальных прямых сомножителей в записи обоих разложений для G^p .

Поскольку $|G^p| < |G|$, по предположению индукции имеем $m' = n'$ и $|H_i^p| = |K_i^p|$, $i = 1, \dots, n'$. Принимая во внимание естественные равенства $|H_i| = p|H_i^p|$, $i = 1, \dots, n'$, получим $|H_i| = |K_i|$, $i = 1, \dots, n'$. Остаётся доказать, что количество сомножителей H_i порядка p равно количеству сомножителей K_j порядка p , т. е. убедиться в том, что $m - n' = n - n'$. Для порядков обоих разложений группы G имеем

$$|H_1| \cdot |H_2| \cdot \dots \cdot |H_m| p^{m-n'} = |G| = |K_1| \cdot |K_2| \cdot \dots \cdot |K_n| p^{n-n'},$$

где $|H_i| = |K_i|$, $i = 1, \dots, n'$. Отсюда заключаем, что $m - n' = n - n'$, и $m = n$. \square

Пример 3.5.7. Все абелевы группы порядка 8 разбиваются на 3 класса: 1) циклические; такие группы содержат элементы порядков 2, 4, 8; 2) изоморфные прямому произведению $\mathbb{Z}_4 \times \mathbb{Z}_2$; такие группы содержат элементы порядков 2 и 4, но не содержат элементов порядка 8; 3) изоморфные произведению $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$; такие группы содержат элементы порядка 2, но не содержат элементов порядков 4 и 8. Группы одного класса изоморфны, группы разных классов – нет.

Упражнение 3.5.8. Используя теорему о конечных абелевых группах, опишите и обоснуйте классификацию абелевых групп порядка 72. Почему группы, принадлежащие разным классам, неизоморфны?

Теорема о конечных абелевых группах имеет важное следствие.

Следствие 3.5.9 (существование подгруппы порядка, равного делителю порядка группы). *Если число t является делителем порядка $|G|$ конечной абелевой группы G , то в группе G существует подгруппа, имеющая порядок t .*

Доказательство. Рассмотрим канонические разложения чисел $|G|$ и t :

$$|G| = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}, \quad t = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}.$$

Для единообразия обозначений мы считаем, что $n_i > 0$, $0 \leq l_i \leq n_i$, $i = 1, \dots, s$. Тогда искомая подгруппа определяется прямым произведением подгрупп $G'(p_i)$ в тех сомножителях $G(p_i)$ в разложении группы G , для которых $l_i \neq 0$. Зафиксируем $p = p_i$ с таким свойством и опишем процедуру выделения $G'(p)$. Группа $G(p)$ порядка p^n изоморфна прямому произведению циклических подгрупп

$$G(p) \cong \mathbb{Z}_{p^{i_1}} \times \dots \times \mathbb{Z}_{p^{i_t}}, \quad i_1 \geq \dots \geq i_t, \quad i_1 + \dots + i_t = n.$$

Тогда для выделения в группе $G(p)$ подгруппы $G'(p)$ порядка p^l достаточно указать (любое) разбиение $l = j_1 + \dots + j_t$ такое, что $0 \leq j_v \leq i_v$, $v = 1, \dots, t$. Искомая подгруппа имеет вид

$$G'(p) \cong \mathbb{Z}_{p^{j_1}} \times \dots \times \mathbb{Z}_{p^{j_t}}, \quad j_1 + \dots + j_t = l.$$

□

3.5.2 Строение конечно порождённых абелевых групп

В определении 3.3.1 порождающего подмножества группа G не подразумевается абелевой. Пусть группа G конечно порождена, и $M = \{g_1, \dots, g_k\}$ – конечное множество её образующих. Образующие могут входить в представление элемента g в любом порядке с возможными повторениями. Если группа G абелева, то можно зафиксировать какой-либо порядок образующих элементов, и каждый $g \in G$ приобретает представление в виде монома $g_1^{i_1} \dots g_k^{i_k}$, $i_u \in \mathbb{Z}$, $u = 1, \dots, k$.

Определение 3.5.10. *Кручением группы G называется подмножество её элементов, имеющих конечные порядки. Обозначение: $\text{tors } G$.*

Упражнение 3.5.11. Докажите, что в абелевой группе G её кручение $\text{tors } G$ является подгруппой.

Зафиксируем натуральное число k .

Определение 3.5.12. *Конечно порождённой свободной абелевой группой называется группа, образованная всеми мономами вида $g_1^{n_1} \dots g_k^{n_k}$, где $n_i \in \mathbb{Z}$, $i = 1, \dots, k$. Групповая операция определяется умножением мономов:*

$$(g_1^{n_1} \dots g_k^{n_k}) \circ (g_1^{n'_1} \dots g_k^{n'_k}) = g_1^{n_1+n'_1} \dots g_k^{n_k+n'_k}.$$

Число k называется *рангом* свободной абелевой группы.

Можно доказать, что изоморфные абелевы группы имеют равные ранги. В этой работе мы не будем этого делать.

Упражнение 3.5.13. Докажите, что свободная абелева группа ранга k изоморфна прямому произведению $\underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_k$.

Пусть G – конечно порождённая абелева группа, $T = \text{tors } G$ – её подгруппа кручения. Можно доказать, что подгруппа кручения в конечно порождённой абелевой группе конечно порождена и, следовательно, конечна, а факторгруппа G/T – конечно порождённая свободная абелева группа, изоморфная некоторой подгруппе $F < G$. Тогда $G = FT$ и $F \cap T = \{e\}$, откуда $G = F \times T$.

Имеет место следующая теорема, подробное доказательство которой мы рассматривать не будем, ограничившись приведёнными выше мотивировками.

Теорема 3.5.14 (о конечно порождённых абелевых группах). *Всякая конечно порождённая абелева группа G изоморфна прямому произведению конечного набора циклических групп:*

$$G \cong \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_k \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}.$$

3.6 Силовские подгруппы конечной группы. Теоремы Силова

3.6.1 Центр группы. Внутренние автоморфизмы группы. Централизаторы и уравнение классов

Пусть G – группа, $g \in G$.

Определение 3.6.1. Элемент $g' \in G$ называется *сопряжённым* элемента g , если существует элемент $h \in G$ такой, что $g' = hgh^{-1}$. При этом говорят, что *элемент h' получен сопряжением элементом g .*

Пример 3.6.2. В группе S_3 сопряжение элементом (13) переводит цикл (12) в цикл (23).

Рассмотрим действие группы на себе сопряжениями:

$$\text{conj}: G \times G \rightarrow G : (g, h) \mapsto hgh^{-1}.$$

Заметим, что если элемент h коммутирует со всеми элементами группы G (такой элемент называется *центральным*), то он неподвижен относительно этого действия, и его орбита состоит из одной точки.

Определение 3.6.3. *Центром* группы G называется подмножество

$$Z(G) = \{h \in G \mid \forall g \in G \quad gh = hg\}.$$

Упражнение 3.6.4. Докажите, что центр $Z(G)$ – нормальная подгруппа в группе G .

Рассмотрим композицию

$$c_g: G \hookrightarrow G \times G \xrightarrow{\text{conj}} G : h \mapsto (g, h) \mapsto hgh^{-1}.$$

Упражнение 3.6.5. Докажите, что композиция c_g осуществляет эндоморфизм (см. п. 1.2) группы G .

Упражнение 3.6.6. Докажите, что эндоморфизм c_g группы G имеет двусторонний обратный $(c_g)^{-1} = c_{g^{-1}}$, т. е. c_g – автоморфизм группы G .

Определение 3.6.7. Изоморфизм вида $c_g: G \xrightarrow{\sim} G$ называется *внутренним автоморфизмом* группы G .

Понятно, что внутренние автоморфизмы группы G образуют группу $\text{Inn } G$ относительно композиции

$$c_g \circ c_h = c_{gh}. \quad (3.6.1)$$

Предложение 3.6.8. *Имеет место изоморфизм групп*

$$\text{Inn } G \cong G/Z(G).$$

Доказательство. Согласно правилу композиции (3.6.1), имеет место сюръективный гомоморфизм групп $\gamma: G \twoheadrightarrow \text{Inn } G$. Его ядро образовано теми и только теми элементами группы G , сопряжения которыми действуют тождественно на всех элементах группы G :

$$g \in \ker \gamma \Leftrightarrow \forall h \in G \quad ghg^{-1} = h.$$

Но это означает, что $gh = hg$ для всех элементов $h \in G$, т. е. $g \in Z(G)$. Теорема о гомоморфизме для групп приводит к искомому изоморфизму. \square

Определение 3.6.9. Подмножества $M \subset G \supset N$ в группе G *сопряжены*, если существует элемент $g \in G$ такой, что $N = c_g(M)$.

Замечание 3.6.10. Поскольку c_g – гомоморфизм, то $c_g(M)$ является подгруппой всякий раз, когда M – подгруппа. При этом, как уже упоминалось, нормальные подгруппы инвариантны относительно сопряжений.

Определение 3.6.11. *Классом сопряжённости* элемента $h \in G$ называется его орбита относительно действия con группы G на себе сопряжениями, т. е.

$$cl(h) = \{ghg^{-1} \mid g \in G\}.$$

Определение 3.6.12. *Централизатором* элемента $h \in G$ называется подмножество

$$C(h) = \{g \in G \mid gh = hg\}.$$

Нетрудно проверить, что централизатор любого элемента группы G является подгруппой в G (*упражнение для читателя!*).

Теорема 3.6.13 (мощность класса сопряжённости). *Для каждого элемента g конечной группы G выполнено равенство*

$$|cl(g)| = [G : C(g)]. \quad (3.6.2)$$

Доказательство. Соответствие $x C(g) \mapsto xgx^{-1}$ поставляет отображение множества левых смежных классов относительно $C(g)$ в класс сопряжённости элемента g . Пусть $xgx^{-1} = x'gx'^{-1}$. Отсюда $x'^{-1}xg = gx'^{-1}x$, т. е. $x'^{-1}x \in C(g)$, и $x \in x'C(g)$. Таким образом, отображение инъективно. Его сюръективность следует сразу из конструкции соответствия. Итак, $|cl(g)| = [G : C(g)]$. \square

Суммируя равенства (3.6.2) по всем классам сопряжённости в группе G , получим

Следствие 3.6.14 (уравнение классов).

$$|G| = \sum |cl(g)| = \sum [G : C(g)],$$

где суммирование выполняется по подмножеству элементов $g \in G$, взятых по одному из каждого класса сопряжённости.

3.6.2 p -группы и теоремы Силова

Определение 3.6.15. Конечная группа порядка p^k , где p – простое число, $k \geq 1$, называется p -группой.

Теорема 3.6.16 (центр p -группы). Пусть G – p -группа. Тогда её центр $Z(G)$ содержит более одного элемента.

Доказательство. Заметим, что элемент является центральным тогда и только тогда, когда его класс сопряжённости состоит из единственного элемента:

$$a \in Z(G) \Leftrightarrow cl(a) = \{a\}.$$

Тогда уравнение классов можно переписать, выделив классы центральных элементов:

$$|G| = |Z(G)| + \sum [G : C(g)], \quad (3.6.3)$$

где суммирование ведётся по классам сопряжённости, соответствующим нецентральным элементам. При этом по теореме Лагранжа $[G : C(g)] = |G|/|C(g)|$, т. е. каждое из слагаемых под знаком суммирования в (3.6.3) кратно p . Таким образом, $|Z(G)|$ также кратно p и поэтому $|Z(G)| > 1$. \square

Следствие 3.6.17 (группа порядка p^2). Группа порядка p^2 , где p – простое число, абелева.

Доказательство. Применив теорему о центре p -группы, заключаем, что либо $Z(G) = p^2$, либо $Z(G) = p$. В первом случае $Z(G) = G$, и G – абелева группа. Во втором случае $Z(G)$ – циклическая подгруппа, пусть $Z(G) = \langle z \rangle$. Факторгруппа $G/Z(G)$ имеет простой порядок, равный p . Значит, она тоже циклическая. Пусть $gZ(G)$ – её циклическая образующая. Тогда все элементы группы G имеют вид $g^s z^t$, $0 \leq s, t \leq p-1$. Рассмотрим произведение двух элементов $g^s z^t$ и $g^u z^v$ и воспользуемся центральностью элементов z^t и z^v :

$$(g^s z^t)(g^u z^v) = g^s(z^t g^u)z^v = g^s g^u z^t z^v = g^u g^s z^v z^t = g^u(g^s z^v)z^t = g^u(z^v g^s)z^t = (g^u z^v)(g^s z^t).$$

Таким образом, все элементы группы G коммутируют, т. е. $Z(G) = G$. \square

Теорема 3.6.18 (первая теорема Силова). Пусть G – конечная группа и p – простое число. Если некоторая степень p^k является делителем $|G|$ порядка группы G , то в группе G существует хотя бы одна подгруппа, порядок которой равен p^k .

Доказательство. Доказательство индукцией по $|G|$. При $|G| = 1$ теорема тривиально верна. Предположим, что она верна для всех групп, имеющих порядки строго меньшие, чем $|G|$. Если группа G имеет собственную подгруппу $H < G$ и число p^k является делителем её порядка $|H|$, то, по предположению индукции, в подгруппе H имеется подгруппа порядка p^k .

Предположим, что p^k не является делителем порядка ни одной из собственных подгрупп группы G . Рассмотрим уравнение классов в виде

$$|G| = |Z(G)| + \sum [G : C(g)],$$

где суммирование ведётся по представителям классов сопряжённости нецентральных элементов и при этом из каждого класса взято по одному представителю. Поскольку $|G| = |C(g)|[G : C(g)]$ и при этом p^k – делитель числа $|G|$, но по предположению p^k не является делителем числа $|C(g)|$, то p^k является делителем числа $[G : C(g)]$ для каждого $g \notin Z(G)$. Из уравнения классов заключаем, что p – делитель порядка центра $|Z(G)|$. По теореме 3.5.1 (существование элемента простого порядка, являющегося делителем

порядка абелевой группы), применённой к $Z(G)$, в $Z(G)$ существует элемент x такой, что $\text{ord}_{Z(G)}(x) = \text{ord}_G(x) = p$. Таким образом, поскольку элемент x является центральным, то $\langle x \rangle \triangleleft G$, и можно рассмотреть факторгруппу $G/\langle x \rangle$. Тогда p^{k-1} является делителем её порядка $|G/\langle x \rangle|$. По предположению индукции, в факторгруппе $G/\langle x \rangle$ существует подгруппа H порядка p^{k-1} .

Итак, имеется сюръективный гомоморфизм групп $\phi: G \twoheadrightarrow G/\langle x \rangle$ и подгруппа $H < G/\langle x \rangle$. Тогда её полный прообраз $\phi^{-1}(H)$ является подгруппой и представляет собой объединение смежных классов по подгруппе $\langle x \rangle$: $\phi^{-1}(H) = \bigcup_{g \in H} g\langle x \rangle$. Так как $|H| = p^{k-1}$ и $|\langle x \rangle| = p$, то $|\phi^{-1}(H)| = p^k$. \square

Следствие 3.6.19 (теорема Коши). *Пусть G – конечная группа, p – простой делитель её порядка $|G|$. Тогда в группе G существует элемент порядка p .*

Доказательство. По первой теореме Силова, если p^k – делитель числа $|G|$, то в группе G имеется подгруппа порядка p^k . Остаётся положить $k = 1$; тогда существует подгруппа простого порядка p . Она является циклической; искомый элемент – её циклическая образующая. \square

Определение 3.6.20. Пусть G – конечная группа, p – простой делитель её порядка $|G|$. Если $|G|$ делится на p^k , но не делится на p^{k+1} , $k \geq 1$, то всякая подгруппа порядка p^k в группе G называется *силовской p -подгруппой* группы G .

Определение 3.6.21. *Нормализатор* подгруппы H в группе G называется подмножество

$$N(H) := \{g \in G \mid gHg^{-1} = H\}.$$

Упражнение 3.6.22. Проверьте, что $N(H)$ является подгруппой в группе G .

Лемма 3.6.23. Пусть H – p -подгруппа конечной группы G , $C := \{K_1 = K, K_2, \dots, K_n\}$ – множество всех подгрупп, сопряжённых с некоторой силовской p -подгруппой $K < G$, и $S = S_C$ – группа перестановок множества C . Рассмотрим действие группы G на множестве C , заданное гомоморфизмом групп

$$\tau: G \rightarrow S: g \mapsto (K_i \mapsto gK_i g^{-1}),$$

и его ограничение на подгруппу $H < G$. Тогда из равенства $|H(K_i)| = 1$ следует включение $H < K_i$.

Доказательство. Условие $|H(K_i)| = 1$ означает, что для всех $g \in H$ группа K_i неподвижна: $gK_i g^{-1} = K_i$. Таким образом, $g \in N(K_i)$. Покажем теперь, что все элементы в нормализаторе $N(K_i)$, имеющие порядки, равные степеням числа p , и только они принадлежат подгруппе K_i .

Пусть $x \in N(K_i)$ и $\text{ord } x = p^k$, $k \geq 1$. Нетрудно проверить, что произведение $\langle x \rangle K_i$ является подгруппой в группе G (упражнение!). Предположим, что $x \notin K_i$. Тогда $\langle x \rangle \not\subset K_i$, т. е. существует $m > 1$ такое, что $\langle x^m \rangle = \langle x \rangle \cap K_i$. Поскольку $\text{ord } x = p^k$, то m – делитель числа p^k , т. е. $m = p^l$ для некоторого l , $1 \leq l < k$. Вместе с тем очевидно, что $\langle x \rangle K_i = K_i \cup xK_i \cup \dots \cup x^{m-1}K_i$ – объединение непересекающихся подмножеств мощности $|K_i|$, так что если $|K_i| = p^n$, то $|\langle x \rangle K_i| = p^{n+l} > p^n$ вопреки тому, что K_i – силовская подгруппа. Следовательно, поскольку H – p -группа и $H \subset N(K_i)$, имеем $H < K_i$. \square

Теорема 3.6.24 (вторая теорема Силова). *Пусть H – p -подгруппа конечной группы G . Тогда H содержится в одной из силовских p -подгрупп группы G .*

Доказательство. Согласно лемме 3.6.23, достаточно убедиться в том, что $|H(K_i)| = 1$, где K_i – одна из силовских p -подгрупп, сопряжённых с данной силовской p -подгруппой K . Рассмотрим отображение

$$f: \{gN(K) | g \in G\} \rightarrow C: gN(K) \mapsto gKg^{-1}.$$

Легко проверить, что f – биекция. Таким образом, число

$$|C| = |\{gN(K) | g \in G\}| = \frac{|G|}{|N(K)|} = \frac{|G|/|K|}{|N(K)|/|K|} = \frac{|G|/|K|}{[N(K) : K]} \quad (3.6.4)$$

не делится на p , так как $|G|/|K|$ не делится на p (поскольку K – силовская p -подгруппа). Орбиты элементов множества C под действием элементов группы $\tau(H)$ составляют разбиение множества C . Мощности орбит являются делителями числа $|\tau(H)|$, т. е. они являются и делителями числа $|H|$. Поскольку H – p -группа, то мощности орбит её действия являются степенями числа p . Если каждая из этих мощностей больше 1, то их сумма $|C|$ делится на p вопреки доказанному. \square

Теорема 3.6.25 (третья теорема Силова). *Пусть N – число силовских p -подгрупп в группе G . Тогда $N \equiv 1 \pmod{p}$. Все силовские p -подгруппы конечной группы G сопряжены между собой.*

Доказательство. Пусть K – силовская p -подгруппа группы G и

$$C = \{K = K_1, K_2, \dots, K_n\}$$

– множество всех подгрупп, сопряжённых с группой K . Покажем, что $n \equiv 1 \pmod{p}$. Как и в доказательстве второй теоремы Силова, для любого i мощность орбиты $K(K_i)$ равна степени числа p . При этом $|K(K_i)| = 1$ тогда и только тогда, когда $K < K_i$. Поэтому имеем $|\tau(K)(K_1)| = 1$ и $|\tau(K)(K_i)| = p^{h_i}$, где $i > 1$. Поскольку орбиты действия τ подгруппы K задают разбиение множества C , то $n = |C| \equiv 1 \pmod{p}$.

То, что число n является делителем порядка $|G|$ группы G , следует из (3.6.4).

Теперь докажем, что $n = N$, т. е. каждая силовская p -подгруппа группы G принадлежит множеству C . Предположим противное: найдётся силовская p -подгруппа H такая, что $H \notin C$. Поскольку орбиты под действием $\tau(H)$ составляют разбиение множества C , то $|C| = \sum_{part} |H(K_i)|$, где символ \sum_{part} означает суммирование по разбиению, в котором слагаемых столько же, сколько подмножеств в разбиении. Так как $H \notin C$, то в рассматриваемом разбиении нет орбиты, мощность которой равна 1. Таким образом, $|C| \equiv 0 \pmod{p}$, что противоречит доказанному выше. \square

Следствие 3.6.26. *Силовская p -подгруппа конечной группы G является нормальной подгруппой тогда и только тогда, когда она является единственной силовской p -подгруппой группы G .*

Пример 3.6.27. В группе S_3 , состоящей из $6 = 3 \cdot 2$ элементов, имеются силовские подгруппы для $p = 3$ и $p = 2$. Силовских 2-подгрупп три: $\langle(12)\rangle$, $\langle(23)\rangle$, $\langle(13)\rangle$, и они сопряжены. Единственная силовская 3-подгруппа – это $A_3 = \langle(123)\rangle$.

Пример 3.6.28. В группе A_4 , состоящей из $12 = 3 \cdot 2^2$ элементов, имеется единственная силовская 2-подгруппа V_4 (*упражнение:* убедитесь, что это действительно так) и четыре сопряжённых 3-подгруппы (*упражнение:* укажите, какие это подгруппы и какими элементами осуществляется сопряжение).

Теорема 3.6.29. *Пусть G группа порядка pq , где p и q – простые числа, $p < q$ и p не является делителем числа $q - 1$. Тогда G – циклическая группа.*

Доказательство. Пусть H – силовская p -подгруппа, K – силовская q -подгруппа группы G . По третьей теореме Силова, число силовских p -подгрупп равно $1 + kp$ и является делителем числа pq . Поэтому возможны следующие варианты: $1 + kp = 1$, $1 + kp = p$, $1 + kp = q$, $1 + kp = pq$. Поскольку p не является делителем числа $q - 1$, то $k = 0$. Итак, H – единственная силовская p -подгруппа.

Аналогично число силовских q -подгрупп равно $1 + lq$ и является делителем числа pq , откуда получаем варианты: $1 + lq = 1$, $1 + lq = p$, $1 + lq = q$, $1 + lq = pq$. При условии, что $p < q$, возможно $l = 0$. Значит, K – единственная силовская q -подгруппа в G . Поэтому $H \triangleleft G \triangleright K$. Обе подгруппы являются циклическими, поскольку они имеют конечные порядки. Поскольку их порядки взаимно просты, то эти подгруппы имеют тривиальное пересечение. Остаётся убедиться в том, что подгруппы H и K коммутируют; тогда $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

Итак, пусть $H = \langle x \rangle$ и $K = \langle y \rangle$. Поскольку обе подгруппы являются нормальными в G , имеем $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in Ky^{-1} = K$ и $xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in xH = H$. Отсюда имеем $xyx^{-1}y^{-1} \in H \cap K = \{e\}$ и, следовательно, $xy = yx$. \square

3.7 Коммутаторы в группе. Коммутант

Пусть G – группа.

Определение 3.7.1. Выражение $[g_1, g_2] := g_1g_2g_1^{-1}g_2^{-1}$ называется *коммутатором* элементов $g_1, g_2 \in G$.

Замечание 3.7.2. Понятно, что

- $[g, f]^{-1} = [f, g]$ для любых $f, g \in G$;
- $[g, f] = e$ тогда и только тогда, когда $gf = fg$;
- $[g, f]fg = gf$ для любых $f, g \in G$.

Определение 3.7.3. *Коммутантом* группы G (обозначение: $K(G)$) называется подгруппа группы G , порождённая множеством коммутаторов всех элементов группы G .

Теорема 3.7.4 (универсальность коммутанта). *Коммутант $K(G)$ – наименьшая нормальная подгруппа группы G , факторгруппа по которой абелева.*

Доказательство. Во-первых, каждый элемент коммутанта есть произведение конечного числа коммутаторов. Поскольку сопряжение сохраняет произведения, то

$$q[f_1, g_1] \dots [f_s, g_s]q^{-1} = (q[f_1, g_1]q^{-1}) \dots (q[f_s, g_s]q^{-1})$$

для любого $q \in G$, и далее достаточно проверить следующее тождество для одного коммутатора:

$$q[f, g]q^{-1} = [q, [f, g]][f, g].$$

Отсюда имеем $qK(G)q^{-1} \subset K(G)$, что и доказывает нормальность коммутанта.

Во-вторых, для доказательства коммутативности факторгруппы $G/K(G)$ выберем произвольные $g, h \in G$ и рассмотрим произведение смежных классов

$$(gK(G))(hK(G)) = g(K(G)h)K(G) = ghK(G) = hg[g, h]K(G) = hgK(G) = (hK(G))(gK(G)),$$

что и доказывает коммутативность факторгруппы $G/K(G)$.

В-третьих, пусть нормальная подгруппа $H \triangleleft G$ такова, что G/H абелева. Рассмотрим любые два смежных класса g_1H и g_2H и их коммутатор $[g_1H, g_2H] = [g_1, g_2]H$. Поскольку факторгруппа G/H абелева, то $[g_1H, g_2H] = eH$. Отсюда заключаем, что любой коммутатор $[g_1, g_2] \in H$. Отсюда $K(G) < H$. \square

Замечание 3.7.5. Понятно, что $K(G) = \{e\}$ тогда и только тогда, когда группа G абелева.

Упражнение 3.7.6. Вычислите коммутанты следующих групп:

1. D_3 – группа симметрий правильного треугольника;
2. D_4 – группа симметрий квадрата;
3. \mathbf{H} – группа кватернионных единиц.

3.8 Разрешимые группы

Определение 3.8.1. *Нормальным рядом* в группе G называется последовательность подгрупп

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G_n = G,$$

в которой каждая предыдущая группа нормальна в последующей. Число n называется *длиной* нормального ряда, а факторгруппы G_i/G_{i-1} – его *факторами*.

Далее мы будем использовать сокращённое обозначение G_\bullet для последовательности подгрупп, если прежде она была описана.

Определение 3.8.2. *Разрешимой* называется группа G , обладающая нормальным рядом конечной длины, факторы которого абелевы.

Замечание 3.8.3. Любая абелева группа разрешима.

Теорема 3.8.4 (разрешимость подгруппы). *Подгруппа разрешимой группы разрешима.*

Доказательство. Пусть $K < G$ (подгруппа K может не быть нормальной!). Рассмотрим в ней последовательность подгрупп

$$\{e\} < K \cap G_1 < K \cap G_2 < \cdots < K \cap G_{n-1} < K. \quad (3.8.1)$$

В зависимости от ситуации, несколько первых членов последовательности (3.8.1) могут оказаться тривиальными. Последовательность является нормальным рядом в K (*упражнение*: обоснуйте это!). Тогда определены факторгруппы $(K \cap G_i)/(K \cap G_{i-1})$. Убедимся в том, что эти факторгруппы абелевы, вычислив коммутатор произвольной пары смежных классов $g_1(K \cap G_{i-1})$ и $g_2(K \cap G_{i-1})$:

$$g_1(K \cap G_{i-1})g_2(K \cap G_{i-1})g_1^{-1}(K \cap G_{i-1})g_2^{-1}(K \cap G_{i-1}) = g_1g_2g_1^{-1}g_2^{-1}(K \cap G_{i-1}).$$

Поскольку ряд G_\bullet является нормальным рядом с абелевыми факторами, то для коммутатора смежных классов элементов g_1, g_2 в факторгруппе G_i/G_{i-1} имеем $g_1g_2g_1^{-1}g_2^{-1}G_{i-1} = G_{i-1}$, т. е. $g_1g_2g_1^{-1}g_2^{-1} \in G_{i-1}$. Поскольку $g_1g_2g_1^{-1}g_2^{-1} \in K$, имеем $g_1g_2g_1^{-1}g_2^{-1}(K \cap G_{i-1}) = K \cap G_{i-1}$. \square

Теорема 3.8.5 (разрешимость факторгруппы). *Факторгруппа разрешимой группы разрешима.*

Доказательство. Пусть теперь $K \triangleleft G$, причём группа G разрешима и имеет нормальный ряд G_\bullet с абелевыми факторами. В факторгруппе G/K рассмотрим последовательность подгрупп

$$\{eK\} < G_1K/K < \cdots < G_iK/K < \cdots < G/K.$$

По следствию 3.2.55 первой теоремы об изоморфизмах для групп имеем

$$G_iK/K \cong G_i/(K \cap G_i).$$

Для доказательства нормальности ряда $G_\bullet K/K$ выберем произвольные $gkK \in G_i K/K$ и $hk'K \in G_{i-1} K/K$ и вычислим $gkK(hk'K)(gkK)^{-1} = ghg^{-1}K \in G_{i-1} K/K$. Поскольку смежный класс коммутатора в факторгруппе равен коммутатору смежных классов сомножителей, то из того, что для любых $g_1, g_2 \in G_i$ выполнено $g_1 g_2 g_1^{-1} g_2^{-1} \in G_{i-1}$, следует, что образ этого коммутатора в $G_i K/K$ принадлежит подгруппе $G_{i-1} K/K$. Таким образом, факторы ряда $G_\bullet K/K$ абелевы. \square

Теорема 3.8.6 (разрешимость расширения). *Если группа G имеет разрешимый нормальный делитель, факторгруппа по которому разрешима, то и группа G разрешима.*

Доказательство. Пусть $H \triangleleft G$, и группы H и G/H разрешимы. Рассмотрим их нормальные ряды:

$$\begin{aligned} \{e\} \triangleleft H_1 \triangleleft \cdots \triangleleft H_\ell = H, \\ \{eH\} \triangleleft \overline{K}_1 \triangleleft \cdots \triangleleft \overline{K}_m = G/H. \end{aligned}$$

Пусть K_i – полный прообраз подгруппы $\overline{K}_i < G/H$ относительно гомоморфизма групп $G \twoheadrightarrow G/H$. Убывающей индукцией по i , $i = 1, \dots, m$, убеждаемся в том, что для последовательных прообразов также справедливо условие $K_{i-1} \triangleleft K_i$, причём $K_i/K_{i-1} \cong \overline{K}_i/\overline{K}_{i-1}$ (Упражнение!). Тогда имеем следующий нормальный ряд для группы G :

$$\{e\} \triangleleft H_1 \triangleleft \cdots \triangleleft H_\ell = H \triangleleft K_1 \triangleleft \cdots \triangleleft K_{m-1} \triangleleft K_m = G.$$

Его факторы изоморфны факторам рядов H_\bullet и \overline{K}_\bullet и, следовательно, абелевы. \square

Теорема 3.8.7 (гомоморфизм в абелеву группу). *Разрешимая группа обладает нетривиальным гомоморфизмом в абелеву группу.*

Доказательство. Поскольку G обладает нормальным рядом $G_\bullet : \{e\} \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G$ с абелевыми факторами, то гомоморфизм $G \twoheadrightarrow G/G_{n-1}$ – искомый. \square

Введём индуктивно последовательные коммутанты группы G :

$$K^0 G := G, \quad K^1 G := K(G), \quad \dots, \quad K^s G := K(K^{s-1} G).$$

Теорема 3.8.8 (критерий разрешимости). *Группа G разрешима тогда и только тогда, когда существует такое $n \in \mathbb{N}$, что $K^n G = \{e\}$.*

Доказательство. Понятно, что цепь последовательных коммутантов образует нормальный ряд с абелевыми факторами. Обратно, пусть группа G обладает нормальным рядом $G_\bullet : G \triangleright G_{s-1} \triangleright \cdots \triangleright \{e\}$, факторы которого абелевы. В частности, G/G_{s-1} – абелева группа и, следовательно, по теореме 3.7.4 об универсальности коммутанта $G_{s-1} > K^1 G$. Пусть теперь доказано, что $G_{s-i} > K^i G$. Поскольку факторгруппа G_{s-i}/G_{s-i-1} абелева, то $G_{s-i-1} > K(G_{s-i}) > K(K^i G)$. Из равенства $G_0 = \{e\}$ следует, что $K^s G = \{e\}$. \square

Теорема 3.8.9 (собственность коммутанта разрешимой группы). *Если неединичная группа G разрешима, то $K(G) \neq G$.*

Доказательство. Поскольку G неединичная и разрешимая, то она обладает непостоянным гомоморфизмом $f: G \rightarrow A$ в абелеву группу A . Таким образом, $K(G) \subseteq \ker f$. Если $K(G) = G$, то $K(G) = G = \ker f$, и f – постоянный гомоморфизм (противоречие). \square

Пример 3.8.10. Группа S_3 разрешима. Её нормальный ряд имеет вид

$$\{1\} \triangleleft A_3 \triangleleft S_3.$$

Здесь A_3 – группа чётных перестановок трёх элементов.

Пример 3.8.11. Группа S_4 разрешима. Её нормальный ряд имеет вид

$$\{1\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4.$$

Здесь A_4 – группа чётных перестановок четырёх элементов, V_4 – четверная группа Клейна. Ряд можно уплотнить:

$$\{1\} \triangleleft \{e, (12)(34)\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4.$$

Пример 3.8.12. Группа порядка p^n , где p – простое число, $n \in \mathbb{N}$, разрешима. Действительно, при $n = 1$ имеем группу простого порядка. Она является циклической и, следовательно, разрешимой. Предположим, что разрешимы все группы, имеющие порядки, равные p^ℓ , $\ell < n$. В группе порядка p^n имеется нетривиальный центр $Z(G) \triangleleft G$. Поскольку $Z(G)$ – абелева группа, то она разрешима. Факторгруппа $G/Z(G)$ имеет порядок p^ℓ для некоторого $\ell < n$, и, следовательно, она разрешима по предположению. Таким образом, группа G разрешима.

Глава 4

Кольца

4.1 Кольца. Подкольца и идеалы. Факторкольца и гомоморфизмы

4.1.1 Понятие кольца

Определение 4.1.1. *Кольцом* называется непустое множество R с двумя бинарными операциями (обычно их называют *сложением* $+: R \times R \rightarrow R: (x, y) \mapsto x + y$ и *умножением* $\cdot: R \times R \rightarrow R: (x, y) \mapsto xy$) такими, что

- $(R, +)$ – абелева группа, нейтральный элемент которой называется *нулём* кольца R и обозначается символом 0 ,
- умножение *дистрибутивно* относительно сложения, т. е. выполнены условия:

$$\begin{aligned} \text{дистрибутивность для левого сомножителя} \quad & \forall x, y, z \in R \quad (x + y)z = xz + yz, \\ \text{дистрибутивность для правого сомножителя} \quad & \forall x, y, z \in R \quad x(y + z) = xy + xz. \end{aligned}$$

Если кольцо $(R, +, \cdot)$ содержит элемент, нейтральный по умножению, то такой элемент называется *единицей* кольца R , а само кольцо – *кольцом с единицей*, или *унитарным кольцом*. Если умножение \cdot коммутативно, ассоциативно и т. п., то кольцо называется соответственно *коммутативным*, *ассоциативным* и т. п.

Пример 4.1.2. 1. Целые числа \mathbb{Z} образуют ассоциативное коммутативное кольцо с единицей 1 .

2. Вещественные числа \mathbb{R} образуют ассоциативное коммутативное кольцо с единицей 1 .

3. Квадратные матрицы $\text{Mat}_{\mathbb{R}}(n)$ размера n с вещественными элементами образуют ассоциативное кольцо с единицей (единица этого кольца – это единичная матрица E) относительно обычных матричных операций сложения и умножения. При $n \geq 2$ кольцо $\text{Mat}_{\mathbb{R}}(n)$ некоммутативно.

Упражнение 4.1.3. В определении кольца с единицей не требуется, чтобы $1 \neq 0$. Что можно сказать о кольце, в котором $1 = 0$?

Пример 4.1.4. 1. Пусть V_3 – множество векторов трёхмерного евклидова пространства с обычным векторным сложением $+$ и векторным умножением

$$[-, -]: V_3 \times V_3 \rightarrow V_3: (v_1, v_2) \mapsto [v_1, v_2],$$

известным читателю из аналитической геометрии. Векторное умножение антикоммутативно: $[v, v] = 0$ для любого вектора $v \in V_3$. Тогда $(V_3, +, [-, -])$ – неассоциативное антикоммутативное кольцо.

2. Матрицы $\text{Mat}_{\mathbb{R}}(n)$ размера n с вещественными элементами, обычным матричным сложением и умножением, определённым по правилу

$$[-, -]: \text{Mat}_{\mathbb{R}}(n) \times \text{Mat}_{\mathbb{R}}(n) \rightarrow \text{Mat}_{\mathbb{R}}(n) : (A, B) \mapsto [A, B] = AB - BA,$$

образуют неассоциативное антикоммутативное кольцо.

3. Матрицы $\text{Mat}_{\mathbb{R}}(n)$ размера n с вещественными элементами, обычным матричным сложением и умножением, определённым по правилу

$$\{-, -\}: \text{Mat}_{\mathbb{R}}(n) \times \text{Mat}_{\mathbb{R}}(n) \rightarrow \text{Mat}_{\mathbb{R}}(n) : (A, B) \mapsto \{A, B\} = \frac{1}{2}(AB + BA),$$

образуют неассоциативное коммутативное кольцо, единицей которого по-прежнему будет E .

Соглашение 4.1.5. Если не оговорено противное, далее всюду символ $\text{Mat}_{\mathbb{R}}(n)$ будет означать кольцо матриц с обычными матричными сложением и умножением.

Упражнение 4.1.6. Что можно сказать об антикоммутативном кольце с единицей?

Определение 4.1.7. *Подкольцом* кольца R называется подгруппа S абелевой группы $(R, +)$, замкнутая относительно умножения:

$$\forall s, s' \in S \quad ss' \in S.$$

Пример 4.1.8. Целые числа \mathbb{Z} образуют подкольцо в кольце \mathbb{Q} рациональных чисел.

Пример 4.1.9. Матрицы, в которых все элементы i -й строки равны нулю, образуют подкольцо в кольце $\text{Mat}_{\mathbb{R}}(n)$. Аналогичный вывод справедлив для матриц, в которых все элементы j -го столбца равны нулю.

Замечание 4.1.10. Понятно, что пересечение подколец является подкольцом.

Определение 4.1.11. *Левым идеалом* кольца R называется подгруппа I_L абелевой группы $(R, +)$, замкнутая относительно умножения слева на элементы кольца:

$$\forall x \in I_L \quad \forall r \in R \quad rx \in I_L.$$

Правым идеалом кольца R называется подгруппа I_R абелевой группы $(R, +)$, замкнутая относительно умножения справа на элементы кольца:

$$\forall x \in I_R \quad \forall r \in R \quad xr \in I_R.$$

Двусторонним идеалом кольца R называется подгруппа I абелевой группы $(R, +)$, замкнутая относительно внешнего умножения слева и справа:

$$\forall x \in I \quad \forall r \in R \quad rx \in I \ \& \ xr \in I.$$

Замечание 4.1.12. Понятно, что левый (правый, двусторонний) идеал является подкольцом, однако обратная импликация в общем случае неверна.

Определение 4.1.13. *Суммой* подколец (соответственно, левых идеалов, правых идеалов, двусторонних идеалов) S_1 и S_2 называется подмножество

$$S_1 + S_2 = \{s_1 + s_2 \mid s_i \in S_i, \ i = 1, 2\}.$$

Замечание 4.1.14. Понятно, что сумма подколец (соответственно, левых идеалов, правых идеалов, двусторонних идеалов) является подкольцом (соответственно, левым идеалом, правым идеалом, двусторонним идеалом).

Определение 4.1.15. Пересечением подколец (соответственно, левых идеалов, правых идеалов, двусторонних идеалов) S_1 и S_2 называется подмножество

$$S_1 \cap S_2 = \{s \in R \mid s \in S_i, \ i = 1, 2\}.$$

Замечание 4.1.16. Понятно, что пересечение подколец (соответственно, левых идеалов, правых идеалов, двусторонних идеалов) является подкольцом (соответственно, левым идеалом, правым идеалом, двусторонним идеалом).

Замечание 4.1.17. Понятия суммы и пересечения подколец (соответственно, левых идеалов, правых идеалов, двусторонних идеалов) можно обобщить для любого, даже бесконечного, семейства подколец (соответственно, левых идеалов, правых идеалов, двусторонних идеалов). Сумма подколец (соответственно, левых идеалов, правых идеалов, двусторонних идеалов) $S_i, i \in J$, определяется как множество

$$\sum_{i \in J} S_i = \left\{ \sum_{u=1}^{\ell} s_{i_u} \mid i_u \in J, \ell \in \mathbb{N} \right\}.$$

Таким образом, сумма подколец (соответственно, левых идеалов, правых идеалов, двусторонних идеалов) – это множество всех таких сумм элементов, взятых по одному из каждого S_i , что в каждой сумме элементов количество ненулевых слагаемых конечно. Пересечение любого семейства подколец (соответственно, левых идеалов, правых идеалов, двусторонних идеалов) определяется как пересечение соответствующих подмножеств.

Упражнение 4.1.18. Приведите пример ситуации, когда пересечение левого и правого идеалов не является двусторонним идеалом (*Указание:* используйте кольцо матриц над каким-нибудь числовым кольцом).

Определение 4.1.19. Кольцо R называется *простым*, если в нём нет ненулевых собственных двусторонних идеалов.

Пример 4.1.20. Можно доказать, что кольцо матриц, например с рациональными элементами, просто. Доказательство этого результата будет дано во второй части в разделе, посвящённом алгебрам над полем.

Соглашение 4.1.21. Далее мы будем работать исключительно с ассоциативными кольцами. Поэтому факт ассоциативности кольца в дальнейшем тексте упоминаться не будет.

4.1.2 Образующие идеала

Пусть R – кольцо, $I \subset R$ – левый (соответственно, правый) идеал. Выберем произвольный элемент $p \in R$.

Определение 4.1.22. Множество

$$\{rp + kp \mid r \in R, k \in \mathbb{Z}\}$$

называется *главным левым идеалом*, порождённым элементом p . Множество

$$\{pr + kp \mid r \in R, k \in \mathbb{Z}\}$$

называется *главным правым идеалом*, порождённым элементом p . В том случае, когда кольцо R коммутативно, эти идеалы совпадают и называются *главным идеалом*, порождённым элементом p . Этот идеал обозначаются символом (p) .

Замечание 4.1.23. Главный левый идеал, порождённый элементом p – это наименьший по включению левый идеал в R , содержащий элемент p . Соответственно, главный правый идеал, порождённый элементом p – это наименьший по включению правый идеал, содержащий элемент p .

Замечание 4.1.24. Если кольцо R содержит единицу 1 , то, поскольку $kp = (k \cdot 1)p = p(k \cdot 1)$, главные левый и правый идеалы, порождённые p , можно записать в виде $Rp = \{rp \mid r \in R\}$ и $pR = \{pr \mid r \in R\}$ соответственно.

Замечание 4.1.25. Всякий идеал, содержащий элемент p , содержит и главный идеал, им порождённый.

Пусть теперь M – некоторое подмножество в кольце R .

Так как пересечение произвольного семейства левых идеалов кольца R также является левым идеалом кольца R , то для всякого подмножества M кольца R существует наименьший по включению левый идеал, его содержащий: это пересечение всех левых идеалов, содержащих подмножество M . То же самое верно для правых и двусторонних идеалов.

Определение 4.1.26. Если кольцо R не содержит единицы, то

- *левый идеал, порождённый множеством M* , – это подмножество элементов вида

$$r_1 m_1 + \dots + r_n m_n + k_1 m'_1 + \dots + k_s m'_s, \\ m_i, m'_j \in M, r_i \in R, k_j \in \mathbb{Z}, i = 1, \dots, n, j = 1, \dots, s, n \in \mathbb{N};$$

- *правый идеал, порождённый множеством M* , – это подмножество элементов вида

$$m_1 r_1 + \dots + m_n r_n + k_1 m'_1 + \dots + k_s m'_s, \\ m_i, m'_j \in M, r_i \in R, k_j \in \mathbb{Z}, i = 1, \dots, n, j = 1, \dots, s, n \in \mathbb{N};$$

- *двусторонний идеал, порождённый множеством M* , – это подмножество элементов вида

$$\sum_{i=1}^n r_i m_i r'_i + \sum_{j=1}^s k_j r''_j m'_j + \sum_{l=1}^t k'_l m''_l r'''_l + \sum_{u=1}^w k''_u m'''_u, \\ m_i, m'_j, m''_l, m'''_u \in M, r_i, r'_i, r''_j, r'''_l \in R, k_j, k'_l, k''_u \in \mathbb{Z}, \\ i = 1, \dots, n, j = 1, \dots, s, \ell = 1, \dots, t, u = 1, \dots, w, n, s, t, w \in \mathbb{N}.$$

Если кольцо R коммутативно, то для данного множества M левый, правый и двусторонний идеалы совпадают и обозначаются символом (M) .

Определение 4.1.27. Для кольца R с единицей *левый идеал, порождённый множеством M* , – это подмножество элементов вида

$$r_1 m_1 + \dots + r_n m_n, \quad m_i \in M, r_i \in R, i = 1, \dots, n, n \in \mathbb{N},$$

правый идеал, порождённый множеством M , – это подмножество элементов вида

$$m_1 r_1 + \dots + m_n r_n, \quad m_i \in M, r_i \in R, i = 1, \dots, n, n \in \mathbb{N},$$

двусторонний идеал, порождённый множеством M , – это подмножество элементов вида

$$r_1 m_1 r'_1 + \dots + r_n m_n r'_n, \quad m_i \in M, r_i \in R, i = 1, \dots, n, n \in \mathbb{N}.$$

Определение 4.1.28. Пусть левый (соответственно, правый, двусторонний) идеал I кольца R порождён подмножеством M . Тогда M называется *множеством*, или *системой*, образующих левого (соответственно, правого, двустороннего) идеала I , а элементы подмножества M называются *образующими* левого (соответственно, правого, двустороннего) идеала I .

Замечание 4.1.29. Понятие системы образующих идеала близко к понятию базиса векторного пространства. Однако для произвольного идеала в произвольном кольце разные системы образующих могут иметь разные мощности. Также в произвольном идеале произвольного кольца не всегда бывает целесообразно (и не всегда возможно!) выбрать не только R -линейно независимую (т. е. не допускающую нетривиальных равных нулю R -линейных комбинаций), но и минимальную систему образующих (т. е. систему, из которой невозможно удалить ни один элемент так, чтобы порождаемый ею идеал остался неизменным).

Определение 4.1.30. Идеал, допускающий конечную систему образующих, называется *конечно порождённым*.

4.1.3 Обрыв возрастающих цепей идеалов в кольце главных идеалов

Определение 4.1.31. *Кольцом главных идеалов* называется область целостности, в которой всякий идеал является главным.

Теорема 4.1.32. *В кольце главных идеалов возрастающая цепочка идеалов не может быть бесконечной.*

Доказательство. Пусть R – кольцо главных идеалов и

$$(a_1) \subsetneq (a_2) \subsetneq \dots \subsetneq R$$

– возрастающая цепь идеалов. Рассмотрим объединение всех собственных идеалов этой цепи $I = \bigcup_i (a_i)$. Множество I является подгруппой и является устойчивым относительно умножения на элементы кольца R . Таким образом, I – идеал. Поскольку R – кольцо главных идеалов, идеал I является главным; пусть $I = (c)$. Пусть $c \in (a_m)$; тогда $I \subset (a_m)$ и, следовательно, $I = (a_m)$. Итак, (a_m) – последний собственный идеал в цепи $\{(a_i)\}$. \square

4.1.4 Условия конечности в кольцах

Определение 4.1.33. *Условие обрыва возрастающих цепей (ОВЦ) левых* (соответственно, *правых, двусторонних*) *идеалов* заключается в следующем: всякая строго возрастающая цепь левых (соответственно, правых, двусторонних) идеалов кольца R

$$I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_s \subsetneq \dots$$

не может быть бесконечной. Кольцо, удовлетворяющее условию ОВЦ для левых (соответственно, правых, двусторонних) идеалов, называется *нётеровым слева* (соответственно, *нётеровым справа, нётеровым*).

Определение 4.1.34. *Условие обрыва убывающих цепей (ОУЦ) левых* (соответственно, *правых, двусторонних*) *идеалов* заключается в следующем: всякая строго убывающая цепь левых (соответственно, правых, двусторонних) идеалов кольца R

$$I_1 \supsetneq I_2 \supsetneq \dots \supsetneq I_s \supsetneq \dots$$

не может быть бесконечной. Кольцо, удовлетворяющее условию ОУЦ для левых (соответственно, правых, двусторонних) идеалов, называется *артиновым слева* (соответственно, *артиновым справа, артиновым*).

Пример 4.1.35. Кольца, обладающие конечным набором идеалов, нётеровы и артиновы. Таковы любое поле K , кольца $K[x]/(x^s)$, $s > 1$, $K[x, y]/(x^s, y^t)$, $s, t \geq 1$.

Упражнение 4.1.36. Докажите, что каждое из колец примера 4.1.35 содержит конечное число идеалов и, следовательно, является и артиновым, и нётеровым.

Пример 4.1.37. Кольцо целых чисел \mathbb{Z} нётерово, но не артиново. Действительно, все идеалы в нём имеют вид $n\mathbb{Z} = (n)$, $n \in \mathbb{N}$, а по основной теореме арифметики целых чисел для любого натурального числа, большего 1, существует единственное разложение на простые множители: $n = p_1^{s_1} \dots p_l^{s_l}$. Тогда наиболее длинная строго возрастающая цепь собственных идеалов с началом в (n) имеет вид:

$$(n) \subsetneq (p_1^{s_1-1} \dots p_l^{s_l}) \subsetneq (p_1^{s_1-2} \dots p_l^{s_l}) \subsetneq \dots \subsetneq (p_2^{s_2} \dots p_l^{s_l}) \subsetneq (p_2^{s_2-1} \dots p_l^{s_l}) \subsetneq \dots \subsetneq (p_l^{s_l}) \subsetneq \dots \subsetneq (p_l).$$

Однако в кольце \mathbb{Z} существуют бесконечные строго убывающие цепи идеалов, например, такие:

$$(n) \supsetneq (n^2) \supsetneq (n^3) \supsetneq \dots \supsetneq (n^s) \supsetneq \dots,$$

где $n \neq 1$, $s \in \mathbb{N}$.

Теорема 4.1.38 (критерий нётеровости кольца). *Кольцо R нётерово слева (соответственно, справа) тогда и только тогда, когда каждый его левый (соответственно, правый) идеал конечно порождён.*

Доказательство. Пусть кольцо R нётерово слева, т. е. любая строго возрастающая цепь левых идеалов в нём имеет конечную длину. Пусть I – левый идеал, не допускающий конечной системы образующих. Пусть $\{m_1, \dots, m_s, \dots\}$ – такая бесконечная последовательность в I , что m_{s+1} не принадлежит левому идеалу, порождённому элементами m_1, \dots, m_s (такая последовательность существует для идеала, не допускающего конечной системы образующих). Пусть I_s – левый идеал, порождённый m_1, \dots, m_s . Тогда имеем бесконечную строго возрастающую цепь левых идеалов $I_1 \subsetneq \dots \subsetneq I_s \subsetneq \dots$, что противоречит предположению о том, что кольцо R нётерово слева.

Пусть все левые идеалы кольца R конечно порождены. Предположим, что существует бесконечная строго возрастающая цепь левых идеалов

$$I_1 \subsetneq \dots \subsetneq I_s \subsetneq \dots \quad (4.1.1)$$

Тогда $I = \bigcup_{s=1}^{\infty} I_s$ – идеал. Поскольку I конечно порождён, то выберем некоторую конечную систему его образующих m_1, \dots, m_t . Для каждого i , $i = 1, \dots, t$, существует $s(i)$ такое, что $m_i \in I_{s(i)}$. Тогда для всех $s > \max\{s(i) \mid i = 1, \dots, t\}$ выполнено включение $I \subset I_s$. Это означает, что строго возрастающая цепь (4.1.1) не может быть бесконечной. \square

Следующий результат мы приведём ввиду его важности, однако доказательство пока опустим.

Теорема 4.1.39 (теорема Гильберта о базисе). *Если R – коммутативное нётерово кольцо, то кольцо многочленов $R[x]$ также является нётеровым.*

Следствие 4.1.40. *Если R – коммутативное нётерово кольцо, то кольца многочленов $R[x_1, \dots, x_n]$ являются нётеровыми для любых $n \in \mathbb{N}$.*

Замечание 4.1.41. Кольцо многочленов $R[x_1, \dots]$ от бесконечного набора переменных содержит бесконечную строго возрастающую цепь идеалов

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

и потому не является нётеровым.

4.1.5 Прямое произведение колец. Разложение кольца в прямую сумму идеалов

Пусть $(R_1, \uplus, *)$ и (R_2, \oplus, \circ) – кольца.

Определение 4.1.42. (Внешним) прямым произведением колец $(R_1, \uplus, *)$ и (R_2, \oplus, \circ) называется кольцо со множеством элементов $R_1 \times R_2$ и бинарными операциями, определёнными покомпонентно:

$$(r_1, r_2) + (r'_1, r'_2) = (r_1 \uplus r'_1, r_2 \oplus r'_2), \quad (r_1, r_2) \cdot (r'_1, r'_2) = (r_1 * r'_1, r_2 \circ r'_2).$$

Замечание 4.1.43. Понятно, что аддитивная группа $(R_1 \times R_2, +)$ прямого произведения колец представляет собой прямую сумму аддитивных групп сомножителей $(R_1, \uplus) \times (R_2, \oplus)$. Её нуль – это $0 = (0_1, 0_2)$.

Замечание 4.1.44. Если кольцо R_1 содержит единицу 1_1 , а кольцо R_2 – единицу 1_2 , то легко проверить, что кольцо $R_1 \times R_2$ содержит единицу $(1_1, 1_2)$.

Соглашение 4.1.45. Далее, поскольку путаница исключена, мы будем для всех колец использовать стандартные обозначения для бинарных операций ($+$ для сложения, \cdot для умножения), а в обозначениях нуля 0 и единицы 1 опускать индексы.

Заметим, что всякий раз, когда оба сомножителя представляют собою ненулевые кольца, прямое произведение содержит элементы вида $(r_1, 0)$ и $(0, r_2)$, обладающие следующим свойством:

$$(r_1, 0) \neq 0, \quad (0, r_2) \neq 0, \quad (r_1, 0)(0, r_2) = 0.$$

Определение 4.1.46. *Левым делителем нуля* в кольце R называется такой отличный от нуля элемент $s \in R \setminus 0$, что существует отличный от нуля элемент $t \in R \setminus 0$ такой, что $st = 0$. *Правым делителем нуля* в кольце R называется такой отличный от нуля элемент $s \in R \setminus 0$, что существует отличный от нуля элемент $t \in R \setminus 0$ такой, что $ts = 0$. Если кольцо R коммутативно, то говорят просто о *делителе нуля*.

Таким образом, кольца, являющиеся прямыми произведениями (а также многие другие кольца!), содержат делители нуля.

Пример 4.1.47. Согласно китайской теореме об остатках для колец вычетов, имеется изоморфизм колец $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ для любых простых чисел p, q (теорема верна и для составных взаимно простых оснований, но нам сейчас достаточно этого случая). Тогда элементы $n \bmod p \in \mathbb{Z}_p \setminus 0$ и $m \bmod q \in \mathbb{Z}_q \setminus 0$ являются делителями нуля в прямом произведении $\mathbb{Z}_p \times \mathbb{Z}_q$. Их образы $nq \bmod pq \in \mathbb{Z}_{pq} \setminus 0$ и $mp \bmod pq \in \mathbb{Z}_{pq} \setminus 0$ являются делителями нуля в кольце \mathbb{Z}_{pq} .

Пример 4.1.48. В матричном кольце $\text{Mat}_{\mathbb{Q}}(2)$ элементы

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{и} \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

являются соответственно левым и правым делителями нуля.

Вложение каждого из сомножителей $i_j : R_j \hookrightarrow R_1 \times R_2$, $j = 1, 2$, является гомоморфизмом колец, а его образ $\text{im } i_j$ – двусторонним идеалом в произведении $R_1 \times R_2$. Соответствующие идеалы $I_1 = R_1 \times 0 = i_1(R_1)$ и $I_2 = 0 \times R_2 = i_2(R_2)$ имеют в $R = R_1 \times R_2$ нулевое пересечение. В такой ситуации говорят, что *кольцо R разложено в прямое произведение своих двусторонних идеалов $I_1 = R_1 \times 0$ и $I_2 = 0 \times R_2$* .

Определение 4.1.49. Кольцо R является *прямой суммой подколец $R_i \subset R$, $i = 1, \dots, s$* , если

- $R = \bigoplus_{i=1}^s R_i$ – разложение аддитивной группы $(R, +)$ кольца R в прямую сумму аддитивных подгрупп $(R_i, +) < (R, +)$;
- если $a \in R_i$, $b \in R_j$, $i \neq j$, то $ab = 0$.

Упражнение 4.1.50. Для каждого $j = 1, \dots, s$ рассмотрим гомоморфизм колец $i_j: R_j \hookrightarrow \bigoplus_{i=1}^s R_i : r \mapsto (0, \dots, 0, r, 0, \dots, 0)$, ставящий $r \in R_j$ на j -е место. Тогда обозначим его образ $\text{im } i_j = \bar{R}_j$. Докажите, что \bar{R}_j – двусторонний идеал в прямой сумме $\bigoplus_{i=1}^s R_i$.

Пусть теперь I_i – двусторонние идеалы в R , $i = 1, \dots, s$. Читателю известно, что их сумма

$$\sum_{i=1}^s I_i = \{i_1 + \dots + i_s \mid i_j \in I_j, j = 1, \dots, s\}$$

является идеалом в кольце R .

Определение 4.1.51. Сумма идеалов $\sum_{i=1}^s I_i$ *прямая*, если выполнено одно из трёх эквивалентных условий:

1. Для любого $x \in \sum_{i=1}^s I_i$ разложение $x = x_1 + \dots + x_s$, $x_j \in I_j$, $j = 1, \dots, s$, единственно;
2. Для любого $j = 1, \dots, s$ выполнено $I_j \cap \sum_{u \neq j} I_u = 0$;
3. Если $x_1 + \dots + x_s = 0$ для $x_j \in I_j$, $j = 1, \dots, s$, то $x_1 = x_2 = \dots = x_s = 0$.

Упражнение 4.1.52. Пусть $R = \bigoplus_{i=1}^r R_i$ – разложение аддитивной группы кольца R в прямую сумму подгрупп. Докажите, что это разложение есть прямая сумма подколец тогда и только тогда, когда каждое из R_i , $i = 1, \dots, r$, есть двусторонний идеал в R .

Упражнение 4.1.53. Прямое произведение колец $R = \times_{j=1}^r R_j$ обладает разложением в прямую сумму идеалов $I_j = i_j(R_j)$, $j = 1, \dots, r$. Докажите это. Обратно, если кольцо R обладает разложением в прямую сумму идеалов J_j , $j = 1, \dots, r$, то существует изоморфизм колец $\phi: R \rightarrow \times_{j=1}^r J_j$ такой, что $\phi|_{J_j} = i_j$, $j = 1, \dots, r$.

Упражнение 4.1.54 (китайская теорема об остатках). Если коммутативное кольцо R обладает разложением в сумму своих идеалов $R = I + J$, то имеет место изоморфизм колец

$$\frac{R}{I \cap J} \cong \frac{R}{I} \times \frac{R}{J}.$$

Указание: имитируйте доказательство китайской теоремы об остатках для групп классов вычетов.

4.1.6 Характеристика кольца с единицей

Пусть R – кольцо с единицей 1.

Определение 4.1.55. Если порядок $\text{ord } 1$ элемента 1 в аддитивной группе $(R, +)$ конечен, то *характеристика* $\text{chr } R$ кольца R считается равной $\text{ord } 1$. Если порядок $\text{ord } 1$ элемента 1 в аддитивной группе $(R, +)$ бесконечен, то *характеристика* $\text{chr } R$ кольца R считается равной 0.

Пример 4.1.56. Кольцо вычетов \mathbb{Z}_n , $n \in \mathbb{N}$, имеет характеристику, равную n . Кольца \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} имеют нулевую характеристику.

Замечание 4.1.57. Если одно кольцо является подкольцом другого, то характеристики обоих колец совпадают.

Предложение 4.1.58. Характеристика кольца, не содержащего делителей нуля, является простым числом либо равна нулю.

Доказательство. Докажем, что кольцо, характеристика которого является составным числом, содержит делители нуля. Пусть $\text{chr } R = mn$, $m, n > 1$. Тогда справедливо равенство

$$\underbrace{(1 + \dots + 1)}_n \underbrace{(1 + \dots + 1)}_m = \underbrace{1 + \dots + 1}_{mn} = 0.$$

Поскольку каждый из множителей отличен от нуля, то оба множителя являются делителями нуля. \square

4.1.7 Обратимые элементы кольца. Тела и поля

В этом параграфе мы считаем, что кольцо R содержит единицу 1.

Замечание 4.1.59. Говоря об обратимых элементах кольца, имеют в виду элементы, обратимые относительно операции умножения (поскольку относительно сложения элементы кольца образуют абелеву группу и, соответственно, любой элемент обратим по сложению). Напомним, что по теореме 2.3.4 если бинарная операция ассоциативна (а это так по соглашению 4.1.21), то левый и правый обратные данного элемента равны, если они существуют. В частности, в кольцах матриц левая и правая обратные для данной матрицы совпадают.

Определение 4.1.60. Группа обратимых элементов кольца R – это множество

$$\text{Unit } R = \{u \in R \mid \exists u^{-1} : u^{-1}u = 1\}.$$

Пример 4.1.61. Очевидно, $\text{Unit } \mathbb{Z} = \{\pm 1\}$, а $\text{Unit } \mathbb{R} = \mathbb{R} \setminus 0$.

Упражнение 4.1.62. Найдите все обратимые элементы в кольце целых гауссовых чисел

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}, i^2 = -1\}.$$

Упражнение 4.1.63. Найдите все обратимые элементы в кольце

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

Упражнение 4.1.64. Что можно сказать об идеале I в кольце R , содержащем хотя бы один обратимый элемент?

Пример 4.1.65. Рассмотрим кольцо матриц $\text{Mat}_R(n)$, элементы которых принадлежат коммутативному кольцу R , и охарактеризуем обратимые элементы этого матричного кольца. Для любой матрицы $A \in \text{Mat}_R(n)$ её *присоединённая* матрица определяется формулой $A^\# = (a_{st}^\#)$, где $a_{st}^\# = A_{ts}$ (читателю следует обратить внимание на изменение порядка следования индексов!). Символ A_{ts} означает алгебраическое дополнение элемента a_{ts} матрицы A . Из правила разложения определителя по строке (столбцу) следует тождество

$$AA^\# = (\det A)E,$$

где $\det A$ – определитель матрицы A . Отсюда видно, что матрица A обратима тогда и только тогда, когда её определитель $\det A \in R$ является обратимым элементом кольца R . При этом $A^{-1} = (\det A)^{-1}A^\#$.

Пример 4.1.66. *Формальным степенным рядом* над кольцом A от одной переменной x называется бесконечная сумма $\sum_{i=0}^{\infty} a_i x^i$, где $a_i \in A$. Поскольку кольцо A предполагается произвольным, вопрос о сходимости и функциональном значении таких рядов не ставится. Формальные степенные ряды допускают почленное сложение и вычитание

$$\sum_{i=0}^{\infty} a_i x^i \pm \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i \pm b_i) x^i,$$

а также умножение

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} \left(\sum_{u=0}^i a_u b_{i-u}\right) x^i,$$

индуцированные соответствующими операциями в кольце A . Таким образом, формальные степенные ряды от переменной x над кольцом A образуют кольцо, которое обозначается символом $A[[x]]$. При этом A естественно вложено в кольцо $A[[x]]$ как подкольцо посредством гомоморфизма колец

$$i: A \hookrightarrow A[[x]] : a \mapsto a + \sum_{i=1}^{\infty} 0x^i.$$

Пусть кольцо A содержит единицу 1 , тогда она же будет единицей кольца $A[[x]]$. Выясним, когда ряд $\sum_{i=1}^{\infty} a_i x^i$ является обратимым элементом кольца $A[[x]]$.

Итак, пусть

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} \left(\sum_{u=0}^i a_u b_{i-u}\right) x^i = 1.$$

приравнивая коэффициенты при соответствующих степенях переменной x , получим бесконечную систему уравнений

$$\begin{aligned} a_0 b_0 &= 1, \\ a_1 b_0 + a_0 b_1 &= 0, \\ a_2 b_0 + a_1 b_1 + a_0 b_2 &= 0, \\ &\dots\dots\dots \\ a_i b_0 + a_{i-1} b_1 + \dots + a_u b_{i-u} + \dots + a_0 b_i &= 0, \\ &\dots\dots\dots \end{aligned}$$

Эту систему можно разрешить относительно коэффициентов b_i , $i \in \mathbb{N}_0$, до любого наперёд указанного i , двигаясь в порядке возрастания индекса, тогда и только тогда, когда $a_0 \in \text{Unit } A$. Для каждого b_i получим его выражение через b_u , $0 \leq u \leq i-1$.

$$\begin{aligned} b_0 &= a_0^{-1}, \\ b_1 &= -a_0^{-1} a_1 b_0, \\ b_2 &= -a_0^{-1} (a_2 b_0 + a_1 b_1), \\ &\dots\dots\dots \\ b_i &= -a_0^{-1} (a_i b_0 + a_{i-1} b_1 + \dots + a_u b_{i-u} + \dots + a_1 b_{i-1}), \\ &\dots\dots\dots \end{aligned}$$

Определение 4.1.67. *Телом* называется ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим. *Полем* называется коммутативное ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Пример 4.1.68. Полями являются следующие известные читателю кольца:

- \mathbb{Q} – кольцо рациональных чисел,
- \mathbb{R} – кольцо вещественных чисел,

- \mathbb{C} – кольцо комплексных чисел,
- \mathbb{Z}_p – кольцо классов вычетов по простому модулю p (важно, что p – простое число!).

Пример 4.1.69. Кватернионы Гамильтона – это элементы \mathbb{R} -линейной оболочки

$$\mathbb{H} = \langle 1, i, j, k \rangle_{\mathbb{R}} = \{a \cdot 1 + b \cdot i + c \cdot j + d \cdot k \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1\},$$

в которой элементы $1, i, j, k$ линейно независимы. Единица $1 = 1 + 0i + 0j + 0k$ совпадает с единицей поля \mathbb{R} . Элемент $z = a \cdot 1 + b \cdot i + c \cdot j + d \cdot k$ называется *кватернионом*. Умножение кватернионов \mathbb{R} -билинейно и определяется соотношениями:

$$\begin{aligned} ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik, \\ i^2 = j^2 = k^2 = -1. \end{aligned}$$

Нетрудно проверить (*упражнение!*), что умножение кватернионов ассоциативно. Очевидно, вещественные числа \mathbb{R} и комплексные числа \mathbb{C} составляют подкольца в кольце \mathbb{H} . На кольце кватернионов имеется естественное отображение (сохраняющее операции!), аналогичное комплексному сопряжению на поле комплексных чисел:

$$\sigma: \mathbb{H} \rightarrow \mathbb{H}: z = a \cdot 1 + b \cdot i + c \cdot j + d \cdot k \mapsto \bar{z} = a \cdot 1 - b \cdot i - c \cdot j - d \cdot k.$$

Кватернион \bar{z} называется *сопряжённым* кватерниону z . Это отображение оставляет неподвижным подкольцо вещественных чисел $\mathbb{R} \subset \mathbb{H}$.

Непосредственно проверяется, что $z\bar{z} = \bar{z}z = a^2 + b^2 + c^2 + d^2$, и поэтому любой ненулевой кватернион обратим:

$$z^{-1} = \frac{\bar{z}}{z\bar{z}}.$$

Таким образом, кольцо кватернионов является телом.

Упражнение 4.1.70. Охарактеризуйте все идеалы в теле.

Упражнение 4.1.71. Поскольку \mathbb{H} – некоммутативное кольцо, то в общем случае решения уравнений $ax = b$ и $xa = b$ различны. Действительно, для первого уравнения $x = a^{-1}b$, а во втором $x = ba^{-1}$. В таком случае говорят, что в кольце \mathbb{H} левое и правое деления различны. Решите оба уравнения при $a = 1 + j$, $b = j + k$.

4.1.8 Факторкольцо

Пусть R – ассоциативное кольцо, I – двусторонний идеал в нём. Рассмотрим факторгруппу R/I аддитивной группы кольца R по её подгруппе I и исследуем поведение умножения на смежных классах. Выбрав два произвольных смежных класса $r_1 + I$ и $r_2 + I$, получим

$$(r_1 + I)(r_2 + I) = r_1r_2 + r_1I + Ir_2 + I^2.$$

Читателю полезно обратить внимание на порядок следования сомножителей во втором и третьем слагаемых, поскольку кольцо R не предполагается коммутативным. Поскольку идеал I устойчив как относительно левого, так и относительно правого внешних умножений, то имеют место включения

$$r_1I \subset I \supset Ir_2.$$

Очевидно, $I^2 \subset I$, и поэтому произведение $(r_1 + I)(r_2 + I)$ является подмножеством однозначно определённого смежного класса $r_1r_2 + I$. Это показывает, что факторгруппа наделена также индуцированным умножением, наделяющим её структурой кольца.

Определение 4.1.72. Факторкольцом кольца R по его двустороннему идеалу I называется факторгруппа R/I его аддитивной группы по её подгруппе $(I, +) < (R, +)$ с умножением смежных классов, индуцированным умножением в кольце R .

Замечание 4.1.73. Если R – коммутативное кольцо, то в нём все идеалы двусторонние. Поэтому в случае коммутативного кольца R факторкольца определены относительно любых идеалов в R .

Замечание 4.1.74. Если R – коммутативное кольцо, то его любое факторкольцо, очевидно, будет коммутативным. Если R содержит единицу 1, то факторкольцо R/I содержит единицу $1 + I$.

4.1.9 Гомоморфизмы колец

Определение 4.1.75. Отображение колец $f: R \rightarrow R'$ называется *гомоморфизмом колец*, если f – гомоморфизм их аддитивных групп и при этом f сохраняет умножение, т. е.

$$\forall r_1, r_2 \in R \quad f(r_1 r_2) = f(r_1) f(r_2).$$

Изоморфизмом колец называется биективный гомоморфизм колец.

Определение 4.1.76. Ядром гомоморфизма колец $f: R \rightarrow R'$ называется подгруппа

$$\ker f = \{r \in R \mid f(r) = 0\} < R.$$

Образом гомоморфизма колец $f: R \rightarrow R'$ называется подгруппа

$$\operatorname{im} f = \{f(r) \mid r \in R\} < R'.$$

Пример 4.1.77. Если R/I – факторкольцо кольца R , то имеется естественный гомоморфизм $\varphi: R \rightarrow R/I: r \mapsto r + I$. Его ядро равно $\ker \varphi = I$, а образ – $\operatorname{im} \varphi = R/I$.

Предложение 4.1.78. Ядро $\ker f$ гомоморфизма колец $f: R \rightarrow R'$ является двусторонним идеалом в кольце R . Образ $\operatorname{im} f$ гомоморфизма колец $f: R \rightarrow R'$ является подкольцом в кольце R' .

Упражнение 4.1.79. Докажите предложение 4.1.78.

Замечание 4.1.80. Понятно, что инъективный гомоморфизм колец осуществляет изоморфизм области определения на образ гомоморфизма.

Пример 4.1.81. Рассмотрим вложение $i_{nn}: \operatorname{Mat}_k(n-1) \hookrightarrow \operatorname{Mat}_k(n)$ матричных колец над полем k , определяемое приписыванием к матрице $A \in \operatorname{Mat}_k(n-1)$ n -й строки и n -го столбца, состоящих из нулей. Тогда гомоморфизм i_{nn} осуществляет изоморфизм $\operatorname{Mat}_k(n-1) \cong \operatorname{im} i_{nn}$.

Теорема 4.1.82 (теорема о гомоморфизме для колец). Любой гомоморфизм колец $f: R \rightarrow R'$ обладает разложением в композицию согласно коммутативной диаграмме

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \widehat{f} \downarrow & & \uparrow j \\ R/\ker f & \xrightarrow{\sim} & \operatorname{im} f \end{array}$$

где $\widehat{f}: R \rightarrow R/\ker f: r \mapsto r + \ker f$ – гомоморфизм на факторкольцо.

Доказательство. Во-первых, для аддитивных групп колец имеем аналогичный результат (теорема о гомоморфизме для групп). Во-вторых, все отображения в диаграмме сохраняют умножение, т. е. являются гомоморфизмами колец. \square

Следствие 4.1.83. *Ненулевой гомоморфизм тела в любое кольцо инъективен.*

Доказательство. Ядро любого гомоморфизма колец $\kappa : K \rightarrow R$, есть двусторонний идеал в K . Поскольку K – тело, то в нём имеется только два двусторонних идеала: (0) и $(1) = K$. Вариант $\ker \kappa = K$ поставяет нулевой гомоморфизм. \square

Пример 4.1.84. Рассмотрим отображение

$$\alpha: \mathbb{C} \rightarrow \text{Mat}_{\mathbb{R}}(2) : a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Читателю предлагается проверить, что это отображение является гомоморфизмом колец. Поскольку \mathbb{C} – поле, этот гомоморфизм инъективен.

Пример 4.1.85. Имеет место вложение тела кватернионов \mathbb{H} в кольцо матриц $\text{Mat}_{\mathbb{C}}(2)$, определяемое образами \mathbb{R} -базисных элементов $1, j, k, \ell$ (чтобы не возникло путаницы с мнимой единицей i поля \mathbb{C} , кватернионные мнимые единицы обозначены другими символами так, что $\mathbb{H} = \langle 1, j, k, \ell \rangle_{\mathbb{R}}$):

$$\mathbb{H} \hookrightarrow \text{Mat}_{\mathbb{C}}(2) : 1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; j \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; k \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \ell \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Образ произвольного кватерниона легко вычислить, используя продолжение описанного соответствия по \mathbb{R} -линейности на всё \mathbb{R} -векторное пространство \mathbb{H} . Читателю предлагается убедиться в том, что полученное отображение является гомоморфизмом колец.

Замечание 4.1.86. Обычно образ идеала при гомоморфизме не является идеалом. Если гомоморфизм сюръективен, то образ идеала – идеал (*упражнение!*). В частности, при гомоморфизме кольца на факторкольцо каждый идеал переходит в идеал.

Упражнение 4.1.87. Докажите, что если $f: A \rightarrow B$ – гомоморфизм колец и I – произвольный идеал в кольце B , то его полный прообраз $f^{-1}I = \{a \in A \mid f(a) \in I\}$ является идеалом (левым, правым или двусторонним, в зависимости от того, каков идеал I).

4.2 Некоторые результаты из теории коммутативных колец

4.2.1 Область целостности

Определение 4.2.1. *Областью целостности, или целостным кольцом, называется ненулевое коммутативное кольцо с единицей, не содержащее делителей нуля.*

Пример 4.2.2. Кольцо целых чисел \mathbb{Z} , любое поле K и кольцо полиномов $K[x]$ над полем K являются областями целостности.

Предложение 4.2.3. *Конечная область целостности является полем.*

Доказательство. Пусть R – область целостности, состоящая из конечного множества элементов. Если R состоит только из нулевого 0 и единичного 1 элементов, то $R \simeq \mathbb{Z}_2$, и теорема доказана. Иначе выберем в кольце R произвольный ненулевой и неединичный элемент $a \neq 0$ и рассмотрим последовательность его натуральных степеней a^n , $n \in \mathbb{N}$. Поскольку R – конечное множество, то найдутся $i, s \in \mathbb{N}$ такие, что $a^i = a^{i+s}$. Отсюда $a^i(a^s - 1) = 0$. Поскольку R – область целостности и $a \neq 0$, то $a^s = 1$ для некоторого $s \geq 2$ (если $s = 1$, то $a = 1$, что противоречит выбору a). Итак, a – обратимый элемент; его обратный равен $a^{-1} = a^{s-1}$. \square

Замечание 4.2.4. Приведённое доказательство не использует коммутативности умножения в кольце R . Поэтому мы доказали гораздо более общий результат: *конечное кольцо с единицей, не содержащее делителей нуля, является телом.*

Пример 4.2.5. \mathbb{Z}_p , где p – простое число, является полем. Действительно, выберем ненулевой класс вычетов $\bar{r} \in \mathbb{Z}_p$ и его представитель $r \in \mathbb{Z}$. Поскольку p – простое число, числа r и p взаимно просты. Тогда найдутся $u, v \in \mathbb{Z}$ такие, что $ru + pv = 1$. Для классов в \mathbb{Z}_p будем иметь $\bar{r}\bar{u} = \bar{1}$.

Упражнение 4.2.6. Докажите, что $\mathbb{Z}_3[i] = \{\bar{a} + i\bar{b} \mid \bar{a}, \bar{b} \in \mathbb{Z}_3, i^2 = -\bar{1}\}$ – поле и вычислите обратный для элемента $\bar{2} + i$ в этом поле.

4.2.2 Поле частных целостного кольца

Конструкция поля частных области целостности воспроизводит построение рациональных чисел на базе целых чисел.

Пусть R – целостное кольцо. Рассмотрим его декартов квадрат $R \times R$ (здесь не предполагается структуры прямого произведения колец, а используется лишь множество элементов!). Элементы множества $R \times R$ будем называть *R -дробями* и записывать в виде $\frac{r}{s} \in R \times R$ или $r/s \in R \times R$. Назовём дроби r/s и r'/s' *эквивалентными*, если выполнено равенство $rs' = sr'$ (произведение вычисляется в R). Класс эквивалентных дробей будем обозначать символом $[r/s]$.

Предложение 4.2.7. Сложение и умножение классов дробей, определяемые формулами

$$\left[\frac{r}{s}\right] + \left[\frac{r'}{s'}\right] = \left[\frac{rs' + sr'}{ss'}\right], \quad (4.2.1)$$

$$\left[\frac{r}{s}\right] \cdot \left[\frac{r'}{s'}\right] = \left[\frac{rr'}{ss'}\right], \quad (4.2.2)$$

не зависят от выбора их представителей, используемых в вычислениях.

Доказательство. Выберем по два представителя каждого класса: $[r/s] = [\bar{r}/\bar{s}]$ и $[r'/s'] = [\bar{r}'/\bar{s}']$. Это означает, что $r\bar{s} - \bar{r}s = 0$ и $r'\bar{s}' = \bar{r}'s'$. Выполнив сложение согласно (4.2.1), получим две дроби:

$$\frac{rs' + sr'}{ss'} \text{ и } \frac{\bar{r}\bar{s}' + \bar{s}\bar{r}'}{\bar{s}\bar{s}'}$$

Остаётся проверить их эквивалентность; с учётом равенств $r\bar{s} - \bar{r}s = 0$ и $r'\bar{s}' = \bar{r}'s'$

$$(rs' + sr')\bar{s}\bar{s}' - ss'(\bar{r}\bar{s}' + \bar{s}\bar{r}') = 0.$$

Доказательство независимости произведения классов от выбора представителей предлагается читателю. \square

Определение 4.2.8. Множество классов R -дробей со сложением и умножением, определяемыми (4.2.1, 4.2.2), называется *полем частных* области целостности R и обозначается символом $Q(R)$.

Любое целостное кольцо R обладает гомоморфизмом (колец) в своё поле частных $Q(R)$: $\varphi: R \rightarrow Q(R) : r \mapsto [r/1]$. Понятно, что этот гомоморфизм инъективен, и поэтому часто говорят, что *область целостности вкладывается в своё поле частных*. Среди всех полей F , в которые существуют вложения данной области целостности R , поле частных $Q(R)$ занимает особое положение.

Теорема 4.2.9 (универсальное свойство поля частных области целостности). *Каждое вложение области целостности R в поле F пропускается через вложение R в её поле*

частных $Q(R)$. Иначе говоря, любой инъективный гомоморфизм колец $f: R \rightarrow F$, где F – поле, разлагается в композицию согласно коммутативной диаграмме

$$\begin{array}{ccc} R & \xrightarrow{f} & F \\ & \searrow \varphi \quad \nearrow i & \\ & Q(R) & \end{array}$$

где $i: Q(R) \hookrightarrow F$ – вложение поля частных $Q(R)$ в поле F в качестве подполя.

Замечание 4.2.10. Из теоремы следует, что поле частных $Q(R)$ области целостности R – это наименьшее по включению из всех подполей, содержащих R как подкольцо. Отсюда понятно, что такое минимальное поле определено однозначно с точностью до изоморфизма.

Доказательство. Пусть $r \in R$ – произвольный ненулевой элемент. Тогда $f(r) \neq 0$, и элемент $f(r)$ обратим в поле F . Определим отображение $i: Q(R) \rightarrow F$ по правилу:

$$i\left(\left[\frac{r}{s}\right]\right) = f(r)f(s)^{-1}.$$

Убедимся в том, что образ класса дробей, определённый таким способом, не зависит от выбора представителя этого класса. Пусть $[r/s] = [\bar{r}/\bar{s}]$, т. е. $r\bar{s} - s\bar{r} = 0$. Тогда $f(r)f(\bar{s}) - f(s)f(\bar{r}) = 0$, откуда $f(r)f(s)^{-1} = f(\bar{r})f(\bar{s})^{-1}$, т. е.

$$i\left(\left[\frac{r}{s}\right]\right) = i\left(\left[\frac{\bar{r}}{\bar{s}}\right]\right).$$

Очевидно, $i \circ \varphi = i|_R = f$, что и завершает доказательство. \square

Пример 4.2.11. Пусть $R = K[x]$ – кольцо многочленов от одной переменной x над полем K . Тогда его поле частных $Q(K[x])$ – это *поле рациональных дробей*, или *поле рациональных функций*, переменной x над полем K . Оно обозначается символом $K(x)$.

Упражнение 4.2.12. Докажите, что поле частных кольца целых гауссовых чисел $\mathbb{Z}[i]$ есть

$$\mathbb{Q}[i] = \{q_1 + iq_2 \mid q_j \in \mathbb{Q}, j = 1, 2\}.$$

4.2.3 Простые и максимальные идеалы

Пусть R – ненулевое коммутативное кольцо.

Определение 4.2.13. Собственный идеал $I \subset R$ называется *простым*, если всякий раз из $xy \in I$ следует, что либо $x \in I$, либо $y \in I$.

Понятие простого идеала родственно понятию простого числа: если число $p \in \mathbb{Z}$ является простым, то идеал $(p) = \{pn \mid n \in \mathbb{Z}\}$ прост (проверьте выполнение импликации, данной в определении, самостоятельно!)

Теорема 4.2.14 (факторкольцо по простому идеалу). Пусть R – коммутативное кольцо с единицей 1. Идеал $I \subset R$ является простым тогда и только тогда, когда факторкольцо R/I является областью целостности.

Доказательство. Пусть R/I – область целостности. Тогда для любых смежных классов $r_1 + I, r_2 + I \in R/I$ справедлива импликация

$$(r_1 + I)(r_2 + I) = 0 + I \Rightarrow r_1 + I = 0 + I \vee r_2 + I = 0 + I.$$

Равенство $r+I = 0+I$ означает в точности, что $r \in I$. Вместе с тем $(r_1+I)(r_2+I) \subset r_1r_2+I$. Поэтому мы приходим к цепочке

$$(r_1 + I)(r_2 + I) = 0 + I \Leftrightarrow r_1r_2 \in I \Rightarrow r_1 \in I \vee r_2 \in I,$$

в которой последняя импликация и означает простоту идеала I .

Обратно, пусть I – простой идеал, т. е. для любых элементов $r_1, r_2 \in R$ выполнена импликация

$$r_1r_2 \in I \Rightarrow r_1 \in I \vee r_2 \in I.$$

Тогда для смежных классов относительно идеала I будем иметь

$$(r_1 + I)(r_2 + I) = 0 + I \Rightarrow r_1 + I = 0 + I \vee r_2 + I = 0 + I.$$

Это означает отсутствие делителей нуля в факторкольце R/I . Поскольку I – простой идеал, то он собственный. Таким образом, R/I – область целостности. \square

Определение 4.2.15. Собственный идеал $I \subset R$ называется *максимальным*, если для идеала $J \subset R$ всякий раз из $I \subset J \subset R$ следует, что либо $I = J$, либо $J = R$.

Например, если K – поле, то в нём имеется только два идеала; это (0) и $(1) = K$. Очевидно, что в поле нулевой идеал (0) максимален.

Замечание 4.2.16. Максимальность идеала I в точности означает, что для любого $r \in R \setminus I$ идеал, порождённый подмножеством $I \cup \{r\}$, совпадает со всем кольцом R . Если R – коммутативное кольцо с единицей 1 , то максимальность идеала I равносильна выполнению условия $\langle I \cup \{r\} \rangle \ni 1$ для любого элемента $r \in R \setminus I$. Иначе говоря, для любого $r \in R \setminus I$ существует $s \in R$ такой, что $rs + I \ni 1$.

Теорема 4.2.17 (факторкольцо по максимальному идеалу). *Пусть R – коммутативное кольцо с единицей 1 . Идеал I является максимальным тогда и только тогда, когда факторкольцо R/I является полем.*

Доказательство. Пусть R/I – поле. Это означает, что для любого $r+I \in R/I$ существует обратный элемент, т. е. $r'+I \in R/I$ такой, что $rr'+I = 1+I$. Отсюда понятно, что $1 \in rr'+I$. Значит, идеал I вместе с любым элементом $r \notin I$ порождает всё кольцо R , т. е. I – максимальный идеал.

Обратно, пусть I – максимальный идеал. Следовательно, для любого элемента $r \notin I$ существует такой элемент $s \in R$, что $rs + I \ni 1$, откуда для смежных классов получим $(r+I)(s+I) = 1+I$, т. е. класс $s+I$ является обратным класса $r+I$. Таким образом, R/I – поле. \square

Следствие 4.2.18. *Максимальный идеал прост.*

Доказательство. Поскольку поле является областью целостности, то из того, что для любого максимального идеала $\mathfrak{m} \subset R$ факторкольцо R/\mathfrak{m} является полем. Оно также является областью целостности, и потому идеал \mathfrak{m} прост. \square

Определение 4.2.19. Полином $f \in K[x]$ ненулевой степени *неприводим над полем K* , если в любом представлении $f = gh$, где $g, h \in K[x]$, один из сомножителей имеет степень, равную 0 .

Напомним, что степень корректно определена только для ненулевых полиномов. Не существует такого целого числа, которое можно было бы приписать нулевому полиному в качестве его степени так, чтобы степень сохраняла мультипликативность.

Замечание 4.2.20. В факторкольце кольца главных идеалов все идеалы главные (но могут существовать делители нуля).

Предложение 4.2.21. Кольцо $K[x]$, где K – поле, является кольцом главных идеалов.

Доказательство. Пусть $I \subset K[x]$ – идеал. Необходимо доказать, что он допускает представление в виде $I = (f)$ для некоторого подходящего полинома f . Выберем среди всех ненулевых полиномов, принадлежащих идеалу I , тот, который имеет наименьшую степень. Пусть это полином f ; убедимся в том, что $I = (f)$. Для этого возьмём произвольный ненулевой многочлен $g \in I$ и выполним деление с остатком полинома g на полином f : $g = qf + r$, где $q \in K[x]$ – неполное частное, $r \in K[x]$ – остаток. При этом либо $\deg r < \deg f$, либо $r = 0$. Поскольку f имеет наименьшую степень среди всех ненулевых полиномов идеала I , то вариант $\deg r < \deg f$ невозможен, и поэтому $r = 0$. \square

Предложение 4.2.22 (идеал, порождённый неприводимым полиномом). Пусть K – поле. Полином $f(x) \in K[x]$ неприводим тогда и только тогда, когда идеал $(f(x))$ максимален.

Доказательство. Пусть f – полином, неприводимый над полем K , и предположим, что идеал $(f) \subset K[x]$ не является максимальным. Это означает, что существует идеал $J \subset K[x]$ такой, что $(f) \subsetneq J \subsetneq K[x]$. Известно (предложение 4.2.21), что кольцо $K[x]$ является кольцом главных идеалов. Таким образом, найдётся полином $h \in K[x]$ такой, что $J = (h)$. Поскольку $(f) \subset (h)$, заключаем, что $f = gh$ для некоторого $g \in K[x]$. Так как f – неприводимый полином, то один из сомножителей f либо h имеет нулевую степень. Если $\deg g = 0$, то g – обратимый элемент кольца $K[x]$, откуда $(f) = (h) = J$, что противоречит предположению. Если, наоборот, $\deg h = 0$, то h – обратимый элемент кольца $K[x]$, откуда $(h) = J = K[x]$. Опять же получено противоречие с предположением.

Пусть теперь $(f) \subset K[x]$ – максимальный идеал, и предположим, что полином f обладает представлением $f = gh$ таким, что $\deg g \neq 0$ и $\deg h \neq 0$. Тогда имеем цепочку вложений $(f) \subset (h) \subset K[x]$:

1. Поскольку g – непостоянный полином, имеем $(f) \subsetneq (h)$.
2. Вместе с тем h – тоже непостоянный полином, и потому $(h) \subsetneq K[x]$.

Выводы 1 и 2 противоречат предположению о максимальной идеала (f) . \square

Пример 4.2.23. В кольце целых чисел \mathbb{Z} максимальными идеалами являются все простые идеалы: если p – простое число, тогда идеал $(p) = p\mathbb{Z}$ максимален. Например, чётные числа образуют максимальный идеал, а числа, кратные 4 – образуют идеал, но не максимальный – этот идеал содержится в идеале чётных чисел.

Пример 4.2.24. В кольце многочленов $K[X, Y]$, где K – алгебраически замкнутое поле, максимальные идеалы имеют вид $I_{a,b} = \{f \in K[X, Y] \mid f(a, b) = 0\}$, $a, b \in K$.

Определение 4.2.25. Коммутативное кольцо R , в котором имеется единственный максимальный идеал, называется *локальным* кольцом.

Упражнение 4.2.26. Докажите, что кольца вычетов вида \mathbb{Z}_{p^n} , где p – простое число, являются локальными (Указание: кольца \mathbb{Z}_{p^n} являются факторкольцами кольца \mathbb{Z} , и, следовательно, в них все идеалы главные).

Пример 4.2.27. Кольцо формальных степенных рядов $K[[X]]$ над полем K – локальное кольцо. Необратимые элементы в нём – в точности те, которые не содержат свободного члена. Они образуют идеал. Он – единственный максимальный идеал в этом кольце.

4.2.4 Евклидовы кольца

Определение 4.2.28. Область целостности R называется *евклидовым кольцом*, если на множестве его ненулевых элементов определена функция

$$N: R \setminus 0 \rightarrow \mathbb{N}_0,$$

называемая *нормой*, такая, что для любых $a \in R$ и $b \in R \setminus 0$ существуют $q, r \in R$ такие, что $a = bq + r$, где либо $r = 0$, либо $N(r) < N(b)$.

Замечание 4.2.29. Свойство кольца «быть евклидовым» означает возможность деления с остатком в этом кольце. При этом q называется *неполным частным*, а r – *остатком* при делении a на b . Пусть кольцо R допускает алгоритм деления с остатком. Тогда можно имитировать деление с остатком, имитируя алгоритм Евклида в кольце целых чисел, до тех пор, пока в остатке не получится 0:

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\dots\dots\dots \\ r_{n-2} &= r_{n-1}q_n. \end{aligned}$$

Тогда последний ненулевой остаток r_{n-1} – это наибольший общий делитель δ элементов a и b . Двигаясь снизу вверх и выполняя последовательные подстановки, получим представление δ в виде $\delta = as + bt$, $s, t \in R$. Таким образом, в произвольном евклидовом кольце можно реализовать обычный и расширенный алгоритмы Евклида, если известен алгоритм, позволяющий вычислять неполное частное и остаток.

Пример 4.2.30. 1. \mathbb{Z} – кольцо целых чисел, $N(n) = |n|$ для любого $n \in \mathbb{Z} \setminus 0$.

2. $K[x]$ – кольцо полиномов от переменной x над полем K , $N(f) = \deg f$ для любого $f \in K[x] \setminus 0$.

Теорема 4.2.31. *Евклидово кольцо является кольцом главных идеалов.*

Доказательство. Рассмотрим любой ненулевой идеал $I \subset R$. Поскольку множество \mathbb{N}_0 вполне упорядочено, то среди всех элементов подмножества $I \setminus 0$ существует элемент, имеющий наименьшую норму; пусть таков элемент $a \in I \setminus 0$. Поскольку R – евклидово кольцо, то для любого элемента $b \in R$ и, в частности, для любого $b \in I$ можно выполнить деление с остатком на a . Получим $b = aq + r$, причём либо $N(r) < N(a)$, либо $r = 0$. Поскольку $r = b - aq \in I$, первое невозможно в силу выбора a как элемента с наименьшей нормой в $I \setminus 0$. Таким образом, любой элемент $b \in I$ делится на a , т. е. $I \subset (a)$. Так как $a \in I$, то $(a) \subset I$. Отсюда $I = (a)$. \square

Пример 4.2.32. Докажем, что кольцо целых гауссовых чисел

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}, i^2 = -1\}$$

– евклидово кольцо с нормой $N(a + ib) = a^2 + b^2$.

Мы будем использовать поле частных кольца $\mathbb{Z}[i]$ всякий раз, когда это будет необходимо. Понятно, что $Q(\mathbb{Z}[i]) = \mathbb{Q}[i]$. Для двух целых гауссовых чисел $a, b \in \mathbb{Z}[i]$ пусть $\sigma + i\tau = a/b$ – их частное в $\mathbb{Q}[i]$. Тогда найдутся ближайшие целые $s, t \in \mathbb{Z}$ такие, что $|s - \sigma| \leq 1/2$ и $|t - \tau| \leq 1/2$. Положим $\alpha := \sigma - s$ и $\beta := \tau - t$. Тогда

$$a = b(s + \alpha + i(t - \beta)) = b(s + it) + b(\alpha + i\beta) = bq + r,$$

где $q = s + it \in \mathbb{Z}[i]$, $r = a - bq \in \mathbb{Z}[i]$. Осталось оценить норму остатка r :

$$N(r) = |b^2|(\alpha^2 + \beta^2) \leq |b^2|/2 = N(b)/2.$$

Итак, $N(r) < N(b)$, и $\mathbb{Z}[i]$ – евклидово кольцо.

4.3 Элементы теории делимости в областях целостности

4.3.1 Простые и неприводимые элементы области целостности

Пусть R – область целостности.

Определение 4.3.1. Будем говорить, что элемент $a \in R$ *делит* элемент $b \in R$, если существует элемент $h \in R$ такой, что $b = ah$. Обозначение: $a|b$.

Непосредственно легко проверить, что

- отношение делимости транзитивно: если $a|b$ и $b|c$, то $a|c$;
- если $a|b$ и $a|c$, то $a|(b+c)$ и $a|(b-c)$;
- обратимые элементы делят все ненулевые элементы области целостности R .

Определение 4.3.2. Элементы $a \in R$ и $b \in R$ называются *ассоциированными*, если $a|b$ и $b|a$. Обозначение: $a \sim b$.

Замечание 4.3.3. Нетрудно проверить, что ассоциированность является отношением эквивалентности.

Упражнение 4.3.4. Элементы a и b ассоциированы тогда и только тогда, когда $a = bu$, где u — обратимый элемент. Докажите.

Определение 4.3.5. Ненулевой элемент a называется *простым*, если

- элемент a не является обратимым элементом кольца R ;
- всякий раз из того, что $a|bc$, следует, что $a|b$ или $a|c$.

Определение 4.3.6. Ненулевой элемент a называется *неприводимым*, если

- элемент a не является обратимым элементом кольца R ;
- из того, что $a = bc$, следует, что b обратим или c обратим.

Теорема 4.3.7 (простота влечёт неприводимость). *Из простоты элемента области целостности следует его неприводимость.*

Доказательство. Пусть a — простой элемент. Предположим, что он не является неприводимым, т. е. найдутся такие $b, c \in R$, не являющиеся обратимыми, что $a = bc$. Тогда $a|bc$, но $a \nmid b$ и $a \nmid c$, что противоречит простоте элемента a . \square

Замечание 4.3.8. Однако в произвольной области целостности из неприводимости простота не следует. Пусть $R = \mathbb{Z}[\sqrt{-3}]$, элемент $a = 2$ неприводим в этом кольце. Для доказательства найдём все разложения вида $2 = (b_1 + b_2\sqrt{-3})(c_1 + c_2\sqrt{-3})$. Получим $b_1 = \pm 1$, $b_2 = 0$, $c_1 = \pm 2$, $c_2 = 0$, т. е. множитель $b_1 + b_2\sqrt{-3} = \pm 1$ обратим. Однако элемент $a = 2$ не является простым: из того, что $2|(1 + \sqrt{-3})(1 - \sqrt{-3})$, не следует, что элемент 2 делит хотя бы один из сомножителей; действительно, $2 \nmid (1 \pm \sqrt{-3})$.

Теорема 4.3.9 (в КГИ неприводимый прост). *В кольце главных идеалов понятия простоты и неприводимости равносильны.*

Доказательство. Необходимо показать, что в кольце главных идеалов любой неприводимый элемент прост.

Во-первых, докажем, что идеал (a) , порождённый неприводимым элементом a , максимален. Рассуждение совершенно аналогично доказательству предложения 4.2.22. Предположим противное: пусть существует собственный идеал $I \supsetneq (a)$. Поскольку R — кольцо

главных идеалов, то $I = (q)$ для некоторого $q \in I$. Тогда $q|a$, т. е. существует $u \in R$ такой, что $a = qu$. Поскольку элемент a неприводим, заключаем, что либо q – обратимый элемент, либо u – обратимый элемент. В первом случае $I = R$, что противоречит предположению о том, что идеал I собственный. Во втором случае $I = (a)$, что противоречит предположению о том, что $I \supsetneq (a)$. Таким образом, идеал (a) максимален.

Во-вторых, максимальный идеал прост (следствие 4.2.18). Итак, (a) – простой идеал.

В-третьих, покажем, что если идеал (a) прост, то элемент a является простым. Предположим противное: пусть существуют $b, c \in R$ такие, что $a|bc$, но $a \nmid b$ и $a \nmid c$. Из этих предположений имеем $(bc) \subset (a)$, но $(b) \not\subset (a)$ и $(c) \not\subset (a)$. Поскольку идеал (a) прост, то из $bc \in (a)$ следует, что либо $b \in (a)$, либо $c \in (a)$, т. е. либо $(b) \subset (a)$, либо $(c) \subset (a)$. Противоречие. \square

4.3.2 Факториальные кольца

Здесь мы рассмотрим класс коммутативных колец, в которых реализуется аналог основной теоремы арифметики, хорошо известной читателю.

Теорема 4.3.10 (основная теорема арифметики целых чисел). *Всякое целое число, отличное от нуля и ± 1 , обладает единственным, с точностью до выбора порядка следования и знаков сомножителей, разложением в произведение простых чисел.*

Определение 4.3.11. Элемент a области целостности R обладает однозначным разложением на неприводимые множители при выполнении следующих условий:

- существуют неприводимые элементы $p_1, \dots, p_m \in R$ такие, что $a = \prod_{i=1}^m p_i$;
- если $a = \prod_{i=1}^n q_i$ – некоторое представление элемента a в виде произведения неприводимых q_i , $i = 1, \dots, n$, то $n = m$ и при подходящем изменении порядка нумерации сомножителей $q_i \sim p_i$, $i = 1, \dots, n$.

Определение 4.3.12. Факториальным кольцом называется область целостности, в которой каждый ненулевой необратимый элемент обладает однозначным разложением на неприводимые множители.

Пример 4.3.13. Поле является факториальным кольцом, поскольку в нём каждый ненулевой элемент обратим и, соответственно, условие определения факториального кольца выполнено тривиально.

Теорема 4.3.14. Кольцо главных идеалов факториально.

Доказательство. Докажем существование разложения на неприводимые множители для любого ненулевого необратимого элемента a в кольце главных идеалов R . Предположим, что элемент a таким разложением не обладает. Если a неприводим, то он обладает разложением, состоящим из одного множителя, что противоречит предположению. Иначе элемент a представим в виде произведения двух необратимых множителей $a = a_1 b_1$, и $(a) \subsetneq (a_1)$. По предположению хотя бы один из сомножителей a_1, b_1 не имеет разложения на неприводимые; пусть таков, например, a_1 . Далее опять же $a_1 = a_2 b_2$ и т. д. Приходим к бесконечной возрастающей цепи идеалов $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$, что противоречит конечности возрастающих цепей идеалов в кольцах главных идеалов (теорема 4.1.32). Таким образом, существование разложения ненулевого необратимого элемента кольца главных идеалов на неприводимые доказано.

Теперь докажем единственность разложения. Если a – неприводимый элемент, то для него утверждение о единственности разложения верно. Предположим, что утверждение о единственности разложения верно для элементов, представимых в виде произведений n неприводимых множителей, и докажем его для $n + 1$ множителя. Рассмотрим

два разложения:

$$a = p_1 \dots p_n p_{n+1} = q_1 \dots q_s q_{s+1}. \quad (4.3.1)$$

В кольце главных идеалов неприводимый элемент прост; поэтому p_{n+1} делит хотя бы один из сомножителей $q_1 \dots q_s q_{s+1}$, скажем $p_{n+1} | q_{s+1}$. Поскольку q_{s+1} неприводим и, следовательно, прост, то $q_{s+1} = up_{n+1}$, где $u \in \text{Unit } R$. Выполнив подстановку этого равенства в (4.3.1), приходим к равенству $p_1 \dots p_n = uq_1 \dots q_s$. По предположению индукции $n = s$ и после подходящей перенумерации сомножителей $p_i \sim q_i$, $i = 1, \dots, n$. Также нами доказано, что $p_{n+1} \sim q_{n+1}$, что завершает доказательство теоремы. \square

Замечание 4.3.15. В факториальных кольцах корректно определены (с точностью до ассоциированности) понятия наибольшего общего делителя и наименьшего общего кратного любого конечного набора элементов, а также понятие взаимной простоты элементов. Они повторяют аналогичные понятия, например, в кольце целых чисел.

Упражнение 4.3.16 (лемма о совместной делимости). Докажите, что, если элемент N факториального кольца R делится на каждый из элементов a_1, \dots, a_k , причём эти элементы попарно взаимно просты, тогда N делится на их произведение.

Упражнение 4.3.17. Докажите, что, если $N^n = a_1 \dots a_k$, причём элементы a_1, \dots, a_k попарно взаимно просты, тогда каждое из них имеет вид $a_i = u_i b_i^n$, где $u_i \in R$, $i = 1, \dots, k$.

Упражнение 4.3.18. Докажите, что любую дробь a/b , составленную из элементов факториального кольца R , можно записать в несократимом виде, то есть существуют взаимно простые элементы $p \in R$ и $q \in R$ (однозначно определённые с точностью до ассоциирования), такие что $a/b = p/q$.

Упражнение 4.3.19 (теорема Гаусса). Пусть R – факториальное кольцо. Докажите, что если дробь $a/b \in Q(R)$ является корнем многочлена

$$x^n + c_{n-1}x^{n-1} + \dots + c_0 \in R[x]$$

со старшим коэффициентом, равным 1, тогда $a/b \in R$, то есть $b|a$ в кольце R . (Данное свойство кольца называется *целозамкнутостью*).

Заключение

В данном пособии изучались основные понятия и наиболее важные результаты о полугруппах, моноидах, группах и кольцах. Читатель, наверное, заметил, что часть возникающих сюжетов является общей для рассмотренных алгебраических объектов. Это гомоморфизмы, изоморфизмы и теоремы о гомоморфизмах. Другая же часть сюжетов носит специфический характер для своего типа алгебраических систем. Например, такие теоремы Силова в теории групп или любые теоремы об областях целостности. Такие сюжеты составляют содержательное богатство конкретных алгебраических теорий, скажем теории групп или коммутативной алгебры.

Обширный пласт алгебраической теории, посвящённый модулям над кольцами, алгебрам и, в частности, расширениям полей, остался вне рамок данной работы. Освещение этих содержательно богатых, плодотворных в приложениях и эстетически привлекательных разделов алгебры является делом будущего.

Литература

- [1] Бурбаки, Н. Архитектура математики / Н. Бурбаки; пер. с фр. Д.Н. Ленского // Математическое просвещение (математика, её преподавание, приложения и история) / ред. И.Н. Бронштейн. – М. : Физматгиз, 1960. № 5. – URL: <http://egamath.narod.ru/Math/Bourbaki.htm> (дата обращения: 05.03.2021).
- [2] Глухов, М.М. Алгебра : учебник : в 2 т. Т. 1 / М.М. Глухов, В.П. Елизаров, А.А. Нечаев. – М. : Гелиос АРВ, 2003. – 336 с.
- [3] Глухов, М.М. Алгебра: учебник : в 2 т. Т. 2 / М.М. Глухов, В.П. Елизаров, А.А. Нечаев. – М. : Гелиос АРВ, 2003. – 416 с.
- [4] Зуланке, Р. Алгебра и геометрия : в 3 т. Т. 1 : Введение / Р. Зуланке, А.Л. Онищик. – М. : МЦНМО, 2004. – 408 с.
- [5] Кострикин, А.И. Введение в алгебру. Основы алгебры: учебник для вузов / А.И. Кострикин. – М. : Физматлит, 1994. – 320 с.
- [6] Кострикин, А.И. Введение в алгебру. Часть III : Основные структуры алгебры : учебник для вузов / А.И. Кострикин. – М. : Физико-математическая литература, 2001. – 272 с.
- [7] Скорняков, Л. А. Элементы общей алгебры / Л. А. Скорняков. – М. : Наука, 1983. – 272 с.
- [8] Скорняков, Л. А. Общая алгебра / Л. А. Скорняков, О. В. Мельников, В. Н. Ремесленников [и др.]; под общ. ред. Л. А. Скорнякова. – М. : Наука, 1990. – Т. 1. – 592 с. – (Справ. мат. б-ка).
- [9] Дурнев, В.Г. Алгоритмические проблемы в комбинаторной теории групп : учеб.-метод. пособие / В.Г. Дурнев, О.В. Зеткина. – Ярославль : ЯрГУ, 2019. – 54 с. – URL: <http://www.lib.uniya.ac.ru/edocs/iuni/20190203.pdf> (дата обращения: 14.04.2021).
- [10] Gallian, J. A. Contemporary Abstract Algebra. – Ninth Ed. / J. A. Gallian. – Boston : Cengage Learning, 2017. – 631 p.

Учебное издание

Тимофеева Надежда Владимировна

Алгебраические структуры. Часть I

Учебное пособие

Редактор, корректор Л. Н. Селиванова
Компьютерный набор, вёрстка Н. В. Тимофеева

Подписано в печать 23.09.21. Формат 60 × 84 1/8
Усл. печ. л. 9,3. Уч.-изд. л. 6,0. Тираж 23 экз.
Заказ .

Оригинал-макет подготовлен
в редакционно-издательском отделе ЯрГУ.

Ярославский государственный университет
им. П. Г. Демидова

150003, Ярославль, ул. Советская, 14.