К. Ю. Федоровский

Алгебра и Элементы Тензорного Анализа

Часть 1

Основные алгебраические структуры

Текст лекций для факультета ФН

Москва — 2014

Оглавление

РАЗДЕЛ 1

Алгебраические структуры. Полугруппы и группы

В курсе «Алгебра и элементы тензорного анализа» вводятся и изучаются основные алгебраические структуры (полугруппы, группы, кольца, поля, модули) и изучаются их свойства. Отдельные разделы курса посвящены тензорной алгебре и теории многочленов. Основная трудность при изучении этого курса заключается в необходимости овладения заметным «словарным запасом» за ограниченное время. Ни одно из новых понятий само по себе не является трудным, но их последовательное накопление может иногда вызвать определенные затруднения. Первый часть курса посвящена изучению основ теории групп.

Базовыми учебниками по курсу являются [1] и [2], а основным сборником задач — [3]. В качестве дополнительной литературы рекомендуются книги [4, 5, 6, 7, 8, 9].

Алгебраические операции. Пусть X — некоторое произвольное множество. В частности, качестве X можно рассматривать любое подмножество одного из следующих множеств:

- множества $\mathbb{N} = \{1, 2, \dots, \}$ всех натуральных чисел, множеств $\mathbb{Z}$ всех целых чисел, $\mathbb{Z}_+ = \{0, 1, 2, \dots \}$ всех целых неотрицательных чисел и $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$;
- множества $\mathbb{Q}$ всех рациональных чисел и множества $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$;
- множества $\mathbb{R}$ всех вещественных чисел и множества $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$;
- множества $\mathbb{C}$ всех комплексных чисел и множества $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$;
- множества $\Sigma(\Omega)$ всех подмножеств некоторого множества Ω;
- множества $T(\Omega)$ всех отображений некоторого множества Ω в себя или множества $S(\Omega)$ всех биективных отображений Ω в себя;
- множества $M_n(E)$ всех $n \times n$-матриц с элементами из некоторого числового множества E при $n \in \mathbb{N}$ и т.д.

Напомним, что $X \times X = \{(x, y) : \ x, y \in X\}$. Напомним также, что величина $|X|$ определяется следующим образом: $|X| = N$, $N \in \mathbb{N}$, если множество X состоит из N элементов и $|X| = \infty$, если X состоит из бесконечного числа элементов (в этом обозначении мы не будем различать бесконечные счетные множества и бесконечные множества, имеющие мощность континуума).

Определение. *Бинарной операцией на множестве X называется любое отображение $\tau : X \times X \to X$, определенное на всем множестве $X \times X$.*

Другими словами, если на множестве X задана *бинарная операция* τ, то любой (упорядоченной) паре (a, b) элементов $a \in X$, $b \in X$ поставлен в соответствие некоторый элемент $c = \tau(a, b)$ множества X. Аналогичным образом можно определить *унарную* операцию на X как отображение X в себя, *тернарую* операцию на X как отображение множества $X \times X \times X$ в X и так далее.

Для записи бинарных операций используют два стандартных способа: *функциональный* (при этом результат применения операции τ к элементам a и b записывается в виде $\tau(a, b)$) и *операторный* (в этом случае результат применения операции τ к элементам a и b записывается в виде $a \, \tau \, b$). Функциональную форму записи бинарных операций часто называют *префиксной*, а операторную — *инфиксной*.

Традиционно, для записи бинарных операций используют операторную форму, а в качестве символов, обозначающих операции, используют стандартные *знаки операций*, например $+$, $-$, $*$, $\cdot$, $\times$, $\circ$, $/$, $\div$, $\cup$, $\cap$ и т.д. Всюду в дальнейшем для упрощения обозначений выражение $a \cdot b$ будет записываться в виде ab.

Алгебраические структуры. На каждом множестве X можно задать много различных алгебраических операций. Множество X с заданной на нем алгебраической операцией $*$ обозначается символом $(X, *)$. Во многих случаях на множестве X целесообразно рассматривать не одну, а две, три или более различных алгебраических операций $*_1, \ldots, *_N$, $N > 1$. В этом случае используется обозначение $(X, \{*_1, \ldots, *_N\})$ или $(X, *_1, \ldots, *_N)$.

Определение. *Объект $(X, \{*_1, \ldots, *_N\})$, где X — некоторое множество, а $*_j$, $j = 1, \ldots, N$ — некоторые заданные на X алгебраические операции, называется алгебраической структурой.*

Пример 1.1. Простейшими примерами алгебраических структур являются

$$(\mathbb{Z}, +), \quad (\mathbb{Z}, \cdot), \quad (\mathbb{Q}, +), \quad (\mathbb{Q}, \cdot), \quad (\mathbb{R}, +), \quad (\mathbb{R}, \cdot), \quad (\mathbb{R}, \{+, \cdot\}),$$

где символы $+$ и $\cdot$ обозначают операции сложения и умножения, определенные на соответствующих (числовых) множествах традиционным образом.

Алгебраическими структурами будут также

$$(M_n(\mathbb{R}), +), \qquad \text{и} \quad (M_n(\mathbb{R}), \times),$$

где $+$ и $\times$ — это операции матричного сложения и умножения.

Приведем также несколько примеров алгебраических структур, заданных на стандартных множествах (таких, как $\mathbb{Z}$ или $\mathbb{R}$), но при помощи совершенно нестандартных операций:

$$(\mathbb{Z}, \diamond), \quad (\mathbb{Z}, \circ), \quad (\mathbb{R}, \circ), \quad \ldots,$$

где $x \diamond y = -x - y$, а $x \circ y = x + y + xy$.

Нам понадобится понятие замкнутости множества относительно алгебраической операции. Пусть $(X, *)$ — некоторая алгебраическая структура, а Y — некоторое подмножество X.

Определение. *Говорят, что множество Y замкнуто относительно операции $*$, если $y_1 * y_2 \in Y$ для любых $y_1, y_2 \in Y$.*

Ассоциативные и коммутативные операции. Определение бинарной операции не предполагает, что соответствующее отображение множества $X \times X$ на X обладает какими-либо особыми свойствами. Соответственно имеется неограниченная свобода в конструировании различных бинарных операций и, вместе с ними, различных алгебраических структур на X. Поэтому задача изучения свойств произвольных алгебраических структур является настолько общей, что при ее изучении практически невозможно рассчитывать на получение сколько нибудь содержательных результатов.

При изучении алгебраических структур обычно предполагают, что определяющие эту структуру бинарные операции обладают определенными свойствами. Эти свойства почти всегда обобщают хорошо известные свойства операций над числами, матрицами, множествами и другими хорошо изученными математическими объектами.

Определение. *Пусть на множестве X задана бинарная операция $*$. Она называется ассоциативной, если для любых $a, b, c \in X$ выполняется равенство*

$$(a * b) * c = a * (b * c).$$

Если для любых $a, b \in X$ выполняется равенство

$$a * b = b * a,$$

то операция $*$ называется коммутативной.

Замечание. Ассоциативность и коммутативность — это независимые свойства, поскольку существуют операции, обладающие одним из этих свойств, но не другим. В самом деле, операция умножения на множестве $M_n(\mathbb{R})$ является, как известно из курса линейной алгебры, ассоциативной, но не коммутативной. А операция $\diamond$ на множестве $\mathbb{Z}$, определенная соотношением $x \diamond y = -x - y$, является коммутативной так как для любых $x, y \in \mathbb{Z}$ имеет место равенство

$$x \diamond y = -x - y = -(x + y) = -(y + x) = -y - x = y \diamond x,$$

но не является ассоциативной, так как

$$(1 \diamond 2) \diamond 3 = (-1 - 2) \diamond 3 = -(-1 - 2) - 3 = 0 \neq 4 = 1 \diamond (2 \diamond 3).$$

1.1. Полугруппы

Пусть X — некоторое множество, а $*$ — заданная на X операция. Потребовав, чтобы операция $*$ была *ассоциативной* мы приходим к понятию одной из самых общих алгебраических структур — к понятию *полугруппы*.

Определение. *Алгебраическая структура $(X, *)$ называется полугруппой, если операция $*$ является ассоциативной.*

Если $(X, *)$ — полугруппа, а операция $*$ является коммутативной, то полугруппа $(X, *)$ называется коммутативной полугруппой.

Говорят также, что множество X *образует полугруппу (является полугруппой) относительно операции* $*$. Кроме того, обозначение $(X, *)$ используется только в том случае, когда требуется явно указать, какая операция имеется в виде. Во большинстве случаев используется простое обозначение: полугруппа X.

Простейшими примерами полугрупп являются, например, такие алгебраические структуры, как $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{R}, +)$ или $(\mathbb{R}, \cdot)$, где $+$ и $\cdot$ — это стандартные операции сложения и умножения чисел. Среди простых примеров полугрупп с нестандартными операциями можно привести, например, $(\mathbb{Z}, *)$, где $x * y = \text{НОД}(x, y)$. В то же самое время алгебраические структуры $(\mathbb{Z}, \diamond)$ и $(\mathbb{Z}, *)$ при $x * y = x^y$ не будут полугруппами, так как соответствующие операции не ассоциативны.

Полугруппами также будут $(M_n(\mathbb{R}), +)$ и $(M_n(\mathbb{R}), \cdot)$, где $+$ и $\cdot$ — это матричные операции сложения и умножения, и $(\mathfrak{M}(\Omega), \circ)$, где Ω — некоторое множество, а $\circ$ — операция композиции отображений.

Приведем еще пример *конечной* полугруппы. Для этого рассмотрим множество, состоящее из чисел $Z_n := \{0, 1, 2, \ldots, n-1\}$, где n — некоторое натуральное число. Для элементов $a, b \in Z_n$ определим операции $\oplus_n *$ и $\otimes_n$ как сложение и умножение по модулю n соответственно:

$$a \oplus_n b := (a + b) \pmod{n}, \qquad a \otimes_n b := (ab) \pmod{n}.$$

Как нетрудно проверить, в обоих случаях множество Z_n будет полугруппой относительно этих операций.

Операцию $*$ в полугруппе X часто (и традиционно) называют *умножением*. Это никак не связано в природой элементов множества X. Так, в качестве «умножения» в полугруппе $M_n(\mathbb{R})$ вещественных матриц может выступать как операция матричного сложения, так и операция матричного умножения (при этом в первом случае мы получи коммутативную полугруппу, а во втором — не коммутативную).

Если на множестве X имеется естественная операция умножения (такая, например, как операция умножения целых, рациональных, вещественных или комплексных чисел, или операция умножения матриц), то говорят, что X является *мультипликативной полугруппой* относительно этой операции. Аналогично, если на X имеется естественная операция сложения (здесь снова можно привести примеры чисел и матриц), то говорят, что X является *аддитивной полугруппой*. Например, $\mathbb{Q}$ и $M_n(\mathbb{C})$ являются одновременно мультипликативными и аддитивными полугруппами.

Единичный (нейтральный) элемент полугруппы. Понятие моноида. Пусть X — произвольная полугруппа. Дальнейшее изучение свойств полугрупповой операции $*$ связано с введением понятия единичного (или, точнее, нейтрального элемента).

Определение. *Элемент $e_L \in X$ называется левым единичным (или левым нейтральным) элементом полугруппы X, если для любого элемента $x \in X$ имеет место равенство $e_L * x = x$. Аналогично, элемент $e_R \in X$ называется правым единичным (или правым нейтральным), если $x * e_R = x$ для любого $x \in X$.*

В полугруппе $(\mathbb{R}, +)$ число 0 будет и левым и правым единичным элементом. Аналогично, в полугруппе $(\mathbb{R}, \cdot)$ левым и, одновременно, правым единичным элементом будет число 1. Оказывается, имеет место следующее свойство левых и правых единичных элементов.

Предложение. *Пусть в полугруппе X существуют левый e_L и правый e_R единичные элементы. Тогда $e_L = e_R$.*

Проверка. В самом деле, из определения левого и правого единичных элементов вытекает, что $e_R = e_L * e_R = e_L$. □

Приведем пример полугруппы, в которой не существует правого единичного элемента, но существует бесконечно много левых единичных элементов.

Пример 1.2. Множество

$$Y = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : \ a, b \in \mathbb{R} \right\}$$

является полугруппой относительно операции матричного умножения. Нетрудно проверить, что любая матрица вида

$$e_L^c = \begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$$

при $c \in \mathbb{R}$ является левым единичным элементом в Y. При этом в Y не существует ни одного правого единичного элемента (это проверяется непосредственным вычислением и оставляется в качестве *упражнения*).

Приведенное выше свойство левых и правых нейтральных элементов оправдывает введение следующего понятия:

Определение. *Элемент $e \in X$ называется единичным (или нейтральным) элементом полугруппы X, если для любого элемента $x \in X$ имеет место равенство $e * x = x * e = x$.*

Предложение. *Если в полугруппе X существует единичный элемент, то он является единственным.*

Проверка. В самом деле, пусть в некоторой полугруппе X существуют два единичных элемента, скажем e_1 и e_2. Тогда, то определению единичного элемента $e_1 = e_1 * e_2 = e_2$. □

Определение. *Полугруппа X, в которой существует единичный элемент, называется полугруппой с единицей, или моноидом.*

Пример 1.3. Пусть Ω — некоторое множество. Полугруппа $(\mathfrak{M}(\Omega), \circ)$, будет (некоммутативной) полугруппой с единицей. Единицей в этой полугруппе будет тождественное отображение id.

Кроме того, полугруппами с единицей будут такие полугруппы, как $(\Sigma(\Omega), \cup)$ и $(\Sigma(\Omega), \cap)$. Напомним, что операция операции $\cup$ и $\cap$ — это обычные операции объединения и пересечения множеств. В первом случае единицей будет пустое множество $\varnothing$, а во втором — само множество Ω.

Пример 1.4. Пусть $n > 1$ — натуральное число. Аддитивная полугруппа $M_n(\mathbb{R})$ — это коммутативный моноид (операция в этом случае — это операция матричного сложения, в единичный элемент — нулевая матрица). Мультипликативная полугруппа $M_n(\mathbb{R})$ (в этом случае рассматривается операция матричного умножения) — это некоммутативный моноид, единичным элементом в котором является единичная матрица E).

Пример 1.5. При натуральном $n > 1$ положим

$$n\mathbb{Z} := \{nk : \ k \in \mathbb{Z}\}.$$

В этом случае $n\mathbb{Z}$ является коммутативным моноидом относительно операции $+$ сложения чисел (в этом случае $e = 0$), а относительно операции $\times$ умножения чисел $n\mathbb{Z}$ является коммутативной полугруппой, но не моноидом.

Пусть X — полугруппа относительно операции $*$ и пусть Y — замкнутое относительно операции $*$ подмножество множества X. Тогда Y будет полугруппой относительно операции $*$.

Определение. *Подмножество $Y \subset X$ полугруппы X, замкнутое относительно операции $*$, называется подполугруппой полугруппы X. Подмножество $Y \subset X$ моноида X, замкнутое относительно операции $*$ и содержащее нейтральный элемент этого моноида, называется подмоноидом моноида X.*

Корректность этого определения вытекает из того, что замкнутое относительно операции $*$ подмножество полугруппы X само является полугруппой относительно операции $*$.

Например, $n\mathbb{Z}$ является мультипликативной подполугруппой и аддитивным подмоноидом в $\mathbb{Z}$.

1.1.1. Степень элемента полугруппы. Пусть X — некоторая полугруппа, и пусть $x_1, \ldots, x_n$, где $n \in \mathbb{N}$, — некоторая упорядоченная последовательность элементов из X. Используя операцию $*$ и не меняя порядка следования элементов произведения длины n можно составлять различными способами. Так, при $n = 2$ такой способ только один: $x_1 * x_2$. При $n = 3$ уже есть два разных способа составить произведение соответствующей длины: $(x_1 * x_2) * x_3$ и $x_1 * (x_2 * x_3)$, причем результат вычисления будет одним и тем же, так как операция $*$ в полугруппе ассоциативна. При $n = 4$ число таких произведений равняется пяти: $(x_1 * x_2) * (x_3 * x_4)$, $((x_1 * x_2) * x_3) * x_4$, $x_1 * (x_2 * (x_3 * x_4))$, $x_1 * ((x_2 * x_3) * x_4)$ и $(x_1 * (x_2 * x_3)) * x_4$. В качестве *упражнения* предлагается самостоятельно вычислить число ℓ_n различных способов записать произведение длины n из элементов $x_1, x_2, \ldots, x_n$ при сохранении порядка их следования. Однако, если X — полугруппа, то нет необходимости указывать, как расставлены скобки в произведении. В самом деле, имеет место следующее важное свойство ассоциативных операций.

Предложение 1.6. *Пусть X — полугруппа. Для любого натурального $n > 1$ и для любых элементов $x_1, \ldots, x_n \in X$ значение выражения $x_1 * x_2 * \cdots * x_n$ не зависит от порядка выполнения операций при его вычислении.*

Доказательство. Используем индукцию по n. При $n = 2$ доказываемое утверждение очевидно, а при $n = 3$ оно непосредственно вытекает из определения ассоциативности операции. Предположим теперь, что $n > 3$ и, что для числа сомножителей, меньшего n, утверждение справедливо. Получим из этого, что требуемое утверждение верно для произведения, содержащего n сомножителей.

Так как по предположению индукции результат вычисления произведения $m < n$ сомножителей не зависит от способа расстановки скобок, для любого натурального $m < n$ и для любых $x_1, \ldots, x_m \in X$ имеет место равенство

$$x_1 * \cdots * x_m = ((\cdots (x_1 * x_2) * \cdots) * x_{m-1}) * x_m,$$

причем способ записи (вычисления) произведения, использованный в правой части этого равенства естественно назвать *каноническим*.

Для доказательства справедливости рассматриваемого утверждения для произведения n сомножителей надо показать, что такое произведение равно соответствующему каноническому произведению независимо от способа его вычисления.

Пусть произведение $x_1 * x_2 * \cdots * x_n$ вычисляется следующим образом (здесь k — натуральное число, $1 \leqslant k \leqslant n-1$)

$$(x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_n),$$

а порядок вычисления произведений в скобках не имеет значения в силу предположения индукции (так как $k < n$ и $n - k < n$). Если $k = n - 1$, то

$$x_1 * \cdots * x_n = (x_1 * \cdots * x_{n-1}) * x_n = ((\cdots (x_1 * x_2) * \cdots) * x_{n-1}) * x_n,$$

а последнее произведение уже имеет канонический вид. При $k < n - 1$

$$(x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_n) = (x_1 * \cdots * x_k) * ((x_{k+1} * \cdots * x_{n-1}) * x_n)$$

по предположению индукции (во второй скобке порядок вычисления можно выбирать произвольно). Далее,

$$(x_1 * \cdots * x_k) * ((x_{k+1} * \cdots * x_{n-1}) * x_n) = ((x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_{n-1})) * x_n$$

в силу ассоциативности операции $*$. Еще раз применяя предположение индукции получаем, что

$$((x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_{n-1})) * x_n = (x_1 * \cdots * x_{n-1}) * x_n,$$

а последнее произведение, как уже было показано выше, равно соответствующему каноническому произведению. □

В силу только что доказанного свойства умножения в полугруппах можно использовать следующее сокращенное обозначение:

$$\prod_{k=1}^{n} x_k := x_1 * \cdots * x_n,$$

причем выражение $x_1 * \cdots * x_n$ можно понимать как каноническое произведение элементов $x_1, \ldots, x_n$, определенное при доказательстве Предложения 1.6. Разумеется, при $1 \leqslant m \leqslant n$, имеет место равенство

$$\prod_{k=1}^{n} x_k = \left(\prod_{k=1}^{m} x_k\right) * \left(\prod_{j=m+1}^{n} x_j\right), \tag{1.1}$$

Придавая естественный смысл понятиям «мультипликативный» и «аддитивный», мы будем использовать обозначения $\prod_{k=1}^{n} x_k$ и $\sum_{k=1}^{n} x_k$ в конкретных ситуациях без дополнительных пояснений и комментариев.

Определение. *Для элемента $x \in X$ полугруппы X и для натурального числа n, выражение $x^n := \prod_{k=1}^{n} x$ называется степенью элемента x. При этом x называется основанием степени, а n — показателем. В аддитивном случае используется запись nx, а соответствующий элемент называется кратным элемента x.*

Необходимо понимать, что запись nx — это не произведение n на x, а сокращенная запись выражения $\sum_{k=1}^{n} x$.

Отметим несколько простых свойств степени, которые непосредственно вытекают из формулы (1.1) и из Предложения 1.6. Пусть X — полугруппа. Для любого $x \in X$ и для любых $n, m \in \mathbb{N}$ имеют место равенства

$$x^m * x^n = x^{m+n}, \qquad (x^m)^n = x^{mn}. \tag{1.2}$$

Пусть теперь X — это моноид с единицей e. Если положить по определение, что $x^0 = e$ для любого элемента $x \in X$, то свойства (1.2) будут справедлива и при $z \in \mathbb{Z}_+$.

Для дальнейшего изучения свойств степени в полугруппах нам потребуется следующее понятие

Определение. *Элементы $x \in X$ и $y \in X$ полугруппы X называются коммутирующими (говорят также, что элементы x и y коммутируют в X), если $x * y = y * x$.*

Предложение 1.7. *Пусть элементы x и y моноида X коммутируют в X. Тогда для любого $n \in \mathbb{Z}_+$ верно равенство*

$$(x * y)^n = x^n * y^n. \tag{1.3}$$

Доказательство. Равенство (1.3) легко проверяется по индукции. В самом оно верно при $n = 0, 1$ и, из того, что $(x * y)^{n-1} = x^{n-1} * y^{n-1}$ и из равенства $x * y = y * x$ вытекает, что $y^{n-1} * x = x * y^{n-1}$ и, окончательно,

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

□

Аналогично, для произвольного набора $x_1, \ldots, x_m$ попарно коммутирующих элементов моноида X (это означает, что $x_j * x_k = x_k * x_j$ для любых $j, k \in \{1, \ldots, m\}$) и для любого $n \in \mathbb{Z}_+$ верно равенство

$$(x_1 * \cdots * x_m)^n = x_1^n * \cdots * x_m^n.$$

Обратимость элементов в полугруппах с единицей. Пусть X — моноид, и пусть e — единица в X. Мы начнем с вопроса об *односторонней обратимости* элементов в X. Другими словами, нас интересует возможность решать в X уравнения

$$a * x = e \qquad \text{и} \qquad x * a = e,$$

где $a \in X$ — некоторый фиксированный элемент.

Определение. *Элемент $a \in X$ называется обратимым слева, если найдется такой элемент $\widetilde{a}_L \in X$, что $\widetilde{a}_L * a = e$, и обратимым справа, если найдется $\widetilde{a}_R \in X$ такой, что $a * \widetilde{a}_R = e$. При этом $\widetilde{a}_L$ называется левым обратным для a, а $\widetilde{a}_R$ — правым обратным.*

Как и в случае односторонних единичных элементов тривиально проверяется следующее свойство:

Предложение. *Пусть элемент a моноида X имеет левый и правый обратные $\widetilde{a}_L$ и $\widetilde{a}_R$. Тогда $\widetilde{a}_L = \widetilde{a}_R$.*

Проверка. Для проверки этого свойства достаточно равенство $\widetilde{a}_L * a = e$ умножить справа на $\widetilde{a}_R$. В самом деле, $\widetilde{a}_L * a * \widetilde{a}_R = e * \widetilde{a}_R$, а $a * \widetilde{a}_R = e$. □

Таким образом, если элемент a обратим справа и слева, то он является обратимым и в смысле обычного определения этого понятия, которое вводится следующим образом:

Определение. *Элемент $a \in X$ называется обратимым, если существует элемент $a^{-1} \in X$ такой, что $a * a^{-1} = a^{-1} * a = e$. Этот элемент a^{-1} называется обратным для элемента a.*

Если элемент $a \in X$ обратим, а $a^{-1} \in X$ — соответствующий обратный элемент, то ясно, что a^{-1} также является обратимым элементом. Разумеется, обозначение a^{-1} для обратного элемента можно использовать только после того, как мы убедимся в его единственности. В самом деле, имеет место следующее утверждение:

Предложение. *Если элемент $a \in X$ обратим, то обратный для него элемент a^{-1} является единственным.*

Проверка. Пусть $a \in X$ и пусть $b_1 \in X$ и $b_2 \in X$ — два обратных для a элемента. Тогда $b_2 = e * b_2 = b_1 * a * b_2 = b_1 * e = b_1$. □

Операция взятия обратного элемента является операцией *инверсии*, т.е. имеет место следующее свойство:

Предложение. $(a^{-1})^{-1} = a$.

Проверка. Это непосредственно вытекает из того, что $(a^{-1})^{-1} * a^{-1} = e$ и $a^{-1}(a^{-1})^{-1} = e$. □

Пример 1.8. Обратная матрица A^{-1} (если она существует) является обратным элементом для матрицы A в мультипликативной полугруппе $M_n(\mathbb{R})$. Число $1/x$ (если $x \neq 0$) является обратным элементов для числа x — элемента мультипликативной полугруппы $\mathbb{Q}$. А обратным элементов для числа x, являющегося элементом аддитивной полугруппы $\mathbb{Q}$ будет число $-x$.

Заметим, что в общем случае элемент a моноида X может не иметь обратного элемента (в мультипликативной полугруппе $M_n(\mathbb{R})$, например, это так для любой вырожденной матрицы).

Замечание. Обратный элемент в аддитивной полугруппе традиционно называется *противоположным*. Так, число $-x$ является противоположным элементом для $x \in (\mathbb{Z}, +)$. Такая двойная терминология сложилась исторически и это приходится учитывать.

Упражнение. Привести примеры, когда элемент $a \in X$ моноида X имеет, например, левый обратный, но не имеет правого обратного.

В полугруппе X, имеющей только одностороннюю единицу (но не имеющую единицы), сформулировать определения обратимости элементов относительно односторонней единицы и привести соответствующие примеры

Имеет также место следующее свойство операции взятия обратного элемента.

Предложение. *Если X — полугруппа с единицей, $x, y \in X$ и если существуют x^{-1} и y^{-1}, то $(x * y)^{-1}$ существует и $(x * y)^{-1} = y^{-1} * x^{-1}$.*

Проверка. В самом деле, $(x*y)*(y^{-1}*x^{-1}) = x*(yy^{-1})*x^{-1} = x*e*x^{-1} = x*x^{-1} = e$, а $(y^{-1} * x^{-1}) * (xy) = y^{-1} * (x^{-1} * x) * y = y^{-1} * y = e$. □

Следствие. *Если X — моноид, то множество $U(X)$ состоящее из всех обратимых элементов моноида X является подмоноидом в X.*

Задача 1.1. Пусть

$$M_n^0(\mathbb{R}) := \left\{ A \in M_n(\mathbb{R}) \colon A = (a_{jk})_{j,k=1}^n,\ \sum_{k=1}^n a_{jk} = 0,\ j = 1 \dots n \right\}$$

при $n \in \mathbb{N}$. Требуется проверить, что множество $M_n^0(\mathbb{R})$ является полугруппой относительно обычной операции матричного умножения. Также требуется выяснить, будет ли $M_n^0(\mathbb{R})$ относительно этой операции полугруппой с единицей.

Задача 1.2. Пусть X — моноид, а $a \in X$ — произвольный (фиксированный) элемент. Определим операцию $\odot$ на S по правилу $x \odot y = x * a * y$ для произвольных $x, y \in S$. Проверить, что X является полугруппой относительно $\odot$. Доказать, что элемент a обратим в X если и только если $(X, \odot)$ является моноидом.

Задача 1.3. Проверить, что $(\mathbb{Z}, \odot)$, где операция $\odot$ определена равенством $x \odot y = x+y+xy$, является коммутативным моноидом. Найти в $(\mathbb{Z}, \odot)$ единицу и все обратимые элементы.

Задача 1.4. *Скажем, что элемент $x \in X$ полугруппы X называется идемпотентным элементом (или идемпотентом), если $x^2 = x$.*

Доказать, что любая конечная полугруппа всегда содержит идемпотент.

1.2. Понятие группы

Определение. *Полугруппа с единицей G такая, что для любого элемента $x \in G$ существует обратный элемент $x^{-1} \in G$ называется группой. Число $|G|$ называется порядком группы G.*

Другими словами, множество G с определенной на нем бинарной операцией $*$ является группой, если (1) операция $*$ является ассоциативной, (2) в G существует нейтральный элемент e относительно операции $*$ и (3) для любого $x \in G$ существует (единственный) элемент $x^{-1} \in G$ такой, что $x * x^{-1} = x^{-1} * x = e$.

Определение. *Если G — группа, то ее подмножество H называется подгруппой, если $e \in H$ и для любых элементов $x, y \in H$ выполнены условия $x * y \in H$ и $x^{-1} \in H$.*

Подгруппа H группы G называется собственной, если $H \neq \{e\}$ и $H \neq G$.

Тот факт, что группа H является подгруппой группы G обозначается символом $H \leq G$.

Термин «группа» принадлежит французскому математику Галуа, которого справедливо считать создателем теории групп в ее современном понимании. Надо заметить, что основные идеи теории групп были известны математикам (как это часто бывает с основополагающими математическими идеями) задолго до Галуа, однако их изложение носило довольно «наивный» и не вполне строгий характер. Но и после работ Галуа прошло около 50 лет, прежде чем теория групп была осознана, понята и принята математиками (это произошло в последней четверти 19 века).

Определение. *Группа G называется коммутативной, если G является коммутативной как полугруппа, т.е., если для любых элементов $x, y \in G$ справедливо равенство $x * y = y * x$.*

Замечание. Часто коммутативные группы называют также *абелевыми* (в честь норвежского математика Абеля).

Определение. *Величина $[x, y] = x*y*x^{-1}*y^{-1}$, где x и y — произвольные элементы группы G называется коммутатором элементов x и y.*

Термин «коммутатор» возник в силу следующего равенства

$$x * y = [x, y] * y * x,$$

которое справедливо для любых $x \in G$ и $y \in G$. Кроме того, элементы $x \in G$ и $y \in G$ коммутируют (т.е. $x * y = y * x$) если и только если их коммутатор $[x, y] = 1$.

Задача 1.5. Доказать, что в любой группе G коммутатор определен для любой пары элементов и обладает следующими свойствами

$$[x, y]^{-1} = [y, x], \quad [x * y, z] = x * [y, z] * x^{-1} * [x, z]$$

для любых $x, y, z \in G$.

Пример 1.9. Простейшими примерами групп являются такие алгебраические структуры, как $\mathbb{Z} = (\mathbb{Z}, +)$, $\mathbb{Q} = (\mathbb{Q}, +)$, $\mathbb{R} = (\mathbb{R}, +)$, $\mathbb{C} = (\mathbb{C}, +)$, $\mathbb{Q}^\times = (\mathbb{Q}^*, \cdot)$, $\mathbb{R}^\times = (\mathbb{R}^*, \cdot)$ и $\mathbb{C}^\times = (\mathbb{C}^*, \cdot)$. Кроме того, пусть Ω — некоторое множество. Тогда $S(\Omega)$ (совокупность всех биективных отображений множества Ω в себя) образует группу относительно операции $\circ$ композиции отображений.

Пример 1.10. Нетрудно проверить (это оставляется в качестве *упражнения*), что совокупность всех симметрий правильного плоского n-угольника (n — натуральное число) образует группу, которая традиционно обозначается символом D_n. Так, группа D_3 симметрий правильного треугольника состоит из шести отображений: из тождественного отображения, из поворотов на $120°$ и $240°$ и из симметрий относительно трех прямых, проходящих через одну из вершин треугольника и через середину противоположной стороны.

В качестве *упражнения* предлагается самостоятельно описать (геометрически) группы D_4, D_5, D_6 и D_8. Более подробно группы D_n рассматриваются ниже.

Степени элемента группы. Пусть G — некоторая, а $a \in G$. При $k \in \mathbb{N}$ обозначим $a^{-k} := (a^{-1})^k$. Таким образом понятие степени элемента определено не только для неотрицательных, но и для любых целых значений показателя. Для того, чтобы обосновать корректность такого определения степени для всех целых показателей нам необходимо проверить справедливость следующего утверждения, показывающего, что равенства (1.2) верны и при отрицательных показателях.

Предложение. *Для любого $a \in G$ и для любых $m, n \in \mathbb{Z}$ верны равенства $a^m * a^n = a^{m+n}$ и $(a^n)^m = a^{nm}$.*

Доказательство. Если $m \geqslant 0$ и $n \geqslant 0$, то соответствующее свойства степени было проверено выше, при определении степени. Пусть теперь $m < 0$, $n < 0$ и пусть $m = -m'$, $n = -n'$, $m', n' \in \mathbb{N}$. Тогда

$$a^m * a^n = (a^{-1})^{m'} * (a^{-1})^{n'} = (a^{-1})^{m'+n'} = a^{-(m'+n')} = a^{m+n}.$$

Пусть теперь $m = -m' < 0$, а $n \geqslant 0$ и пусть $n > m'$. Тогда

$$a^m * a^n = (a^{-1})^{m'} * a^n = (a^{-1} * \cdots (m' \text{ раз}) \cdots * a^{-1}) * (a * \cdots (n \text{ раз}) \cdots * a) = a^{n-m'} = a^{m+n}.$$

Остальные случаи рассматриваются аналогично. Второе равенство непосредственно вытекает из первого. □

Условия, при которых полугруппа является группой. В этом разделе мы приведем ряд простых условий, при выполнении которых полугруппа X будет группой.

В начале, по аналогии с определением обратимых элементов, по введем понятие делимости элементов в полугруппе. Скажем, что элемент $b \in X$ *делится* на $a \in X$ *слева* (соответственно, *справа*), если существует $x_L \in X$ такой, что $x_L * a = b$ (соответственно, если существует $x_R \in X$ такой, что $a * x_R = b$).

Заметим, что из делимости $b \in X$ на $a \in X$ слева или справа *не следует* единственность элементов x_L и x_R (которые естественно называть *левым и правым частными* a и b соответственно). В качестве *упражнения* предлагается привести соответствующие примеры. Однако в случае, когда любые два элемента полугруппы делятся друг на друга справа и слева, соответствующая полугруппа оказывается группой. Т.е. имеет место следующее утверждение:

Предложение 1.11. *Для того, чтобы любые два элемента полугруппы X делились друг на друга слева и справа необходимо и достаточно, чтобы X была группой.*

Доказательство. Пусть X — группа. Тогда уравнение $a*x = b$ имеет единственный корень $x = a^{-1}*b$, а уравнение $x*a = b$ имеет единственный корень $b*a^{-1}$. В самом деле, если $x*a = b$, то, домножая это равенство на a^{-1} справа, получаем $x = x*z*a^{-1} = b*a^{-1}$. Второй случай рассматривается аналогично.

Легко проверяется обратное утверждение. Пусть в полугруппе X уравнения $a*x = b$ и $x*a = b$ разрешимы для всех a и b. Тогда, в частности, для любого $a \in X$ существуют такие $x_1 \in X$ и $x_2 \in X$, что $x_1 * a = a$ и $a * x_2 = a$. Другими словами, в X существуют левая и правая единицы. Тогда, как показано выше, $x_1 = x_2 = e$ — единица в X. Далее, для любого $a \in X$ разрешимы уравнения $x * a = e$ и $a * x = e$. Это означает (см. выше), что любой элемент $a \in X$ обратим. Таким образом, X содержит единицу, а любой элемент в X обратим. Т.е. X — группа. □

Рассматривая разрешимость различных уравнений в полугруппах, мы приходим к различным интересным и важным классам полугрупп. Рассмотрим некоторые из таких классов.

Определение. *Полугруппа X называется простой, если для любых $a, b \in X$ существуют такие $x, y \in X$, что $x * a * y = b$.*

Смысл этого понятия станет ясен позднее, при изучении понятия идеала. В качестве *упражнения* предлагается проверить, что любая группа будет простой полугруппой.

Задача 1.6. Доказать, что любая простая коммутативная полугруппа является группой.

Следующий важный класс полугрупп возникает, если задаться вопросом о возможности сокращения общих множителей в равных произведениях. То, что этот вопрос имеет смысл видно из простого примера: при $\alpha, \beta, \gamma \in \mathbb{R}$ равенство $\alpha\beta = \alpha\gamma$ можно сократить на α только при $\alpha \neq 0$ (т.е. не всегда).

Определение. *Полугруппа X называется полугруппой с сокращением, если для любых $x, y, z \in X$ выполняются следующие условия:*

- *из равенства $x * y = x * z$ вытекает, что $y = z$, и*
- *из равенства $x * y = z * y$ вытекает, что $x = z$.*

Ясно, что любая группа является полугруппой с сокращением (это проверяется умножением с нужной стороны на элемент, обратный к тому, на который надо сократить). С другой стороны, мультипликативная полугруппа натуральных чисел является полугруппой с сокращением, но не группой. Однако имеет место следующее свойство полугрупп с сокращением, доказательство которого оставляется в качестве *задачи*:

Задача 1.7. Доказать, что всякая конечная полугруппа с сокращением является группой.

Кратко обсудим возможное решение этой задачи. Пусть $X = \{x_1, \ldots, x_n\}$ — конечная полугруппа, а $a \in X$. Если X — полугруппа с сокращением, то из равенства $a * x_j = a * x_k$ вытекает, что $x_j = x_k$. Следовательно, множество $\{a * x_1, \ldots, a * x_n\}$ совпадает с X. Таким образом, для любых $a, b \in X$ найдется $x_j \in X$ так что $a * x_j = b$. Аналогично решается вопрос о разрешимости в X уравнения $x * a = b$. Остается воспользоваться Предложением 1.11.

Еще одним классом полугрупп, с которым мы кратко познакомимся, является класс т.н. *регулярных* полугрупп.

Определение. *Полугруппа X называется регулярной, если для любого $a \in X$ найдется $x \in X$ такой, что $a * x * a = a$.*

Интересно отметить, что любая регулярная полугруппа обязательно содержит идемпотенты. В самом деле, пусть a и b — такие элементы регулярной полугруппы X, что $a * b * a = a$. Умножив это равенство справа на b получим $(a * b)^2 = a * b$, т.е. $a * b$ — идемпотент.

Задача 1.8. Доказать, что для любого множества Ω полугруппа $\mathfrak{M}(\Omega)$ регулярна.

Ясно, что любая группа является регулярной полугруппой (достаточно взять $x = a^{-1}$. Обратное, конечно, неверно. В качестве простого примера можно взять мультипликативную числовую полугруппу $\{0, 1\}$, которая очевидно является регулярной, но не является группой. Однако, имеет место следующий интересный факт.

Предложение 1.12. *Всякая регулярная полугруппа с сокращением является группой.*

Доказательство. Покажем, что в X есть единичный элемент. Возьмем произвольный элемент $a \in X$ и найдем $x \in X$ такой, что $a * x * a = a$. Далее, для любого $b \in X$ имеем $a * x * a * b = a * b$ и $b * a * x * a = b * a$. Применяя в этих двух равенствах правило сокращения получаем, что $(x * a) * b = b$ и $b * (a * x) = b$. Таким образом, $x * a$ — левая единица, а $a * x$ — правая. Но полугруппа, в которой существуют и левая и правая единицы является моноидом, а эти единицы совпадают. Т.е. $a * x = x * a = e$ и x — это обратный элемент для a. □

Соглашение об обозначения. В дальнейшем, если разумеется это не приведет к разночтениям и неоднозначности, мы будем записывать выражение $x * y$ в виде xy, а вместо единичного элемента группы мы часто будем использовать символ 1. При необходимости будет также использоваться и введенное выше обозначение e для единичного (нейтрального) элемента группы.

В ряде случаев нам будем удобно использовать аддитивную запись (т.е. считать, что групповая операция — это операция сложения $+$). В этом случае единичный элемент обозначается символом 0, а обратный (противоположный) элемент — символом $-x$.

1.3. Циклические группы, порядок элементов группы

Пусть G — некоторая группа. Как было показано выше (см. Предложение 1.2) для любого элемента $a \in G$ и для любого целого числа n (как положительного, так и отрицательного) определена степень a^n и выполняются соотношения (1.2).

Важную роль в теории групп играет понятие *циклической группы*. Пусть $a \in G$ — произвольный элемент группы G. В этом случае совокупность $\langle a\rangle := \{a^k \colon k \in \mathbb{Z}\}$ всех (целых) степеней элемента a образует подгруппу в группе G. В самом деле, из соотношений (1.2) вытекает, что это множество $\langle a\rangle$ замкнуто относительно умножения в G, а $e = a^0 \in \langle a\rangle$ и если $x = a^n \in \langle a\rangle$, то $x^{-1} = a^{-n} \in \langle a\rangle$.

Определение. *Подгруппа $\langle a\rangle \subset G$ называется циклической подгруппа группы G, порожденная элементом a. Группа G называется циклической, если найдется такой элемент $a \in G$, что $G = \langle a\rangle$.*

Другими словами, группа G является циклической, если существует элемент $a \in G$ такой, что для любого элемента $g \in G$ найдется число $n \in \mathbb{Z}$ такое, что $g = a^n$.

Замечание. Если G — это аддитивная группа, то циклическая подгруппа, порожденная элементом $a \in G$ состоит из всех кратных элемента a, т.е. $\langle a\rangle = \{na \colon a \in \mathbb{Z}\}$.

Пример 1.13. Одним из наиболее простых примеров циклической группы является аддитивная группа целых чисел $\mathbb{Z} = (\mathbb{Z}, +)$, которая равна $\mathbb{Z} = \langle 1\rangle$.

Легко привести пример *конечной* циклической группы. Пусть n — некоторое натуральное число. Выше была определена конечная полугруппа $Z_n = (Z_n, \oplus_n)$, где $Z_n = \{0, 1, \dots, n-1\}$, а операция $\oplus_n$ определена следующим образом $a \oplus_n b = (a + b) \pmod n$.

Легко проверить, что $Z_n = (Z_n, \oplus_n)$ является группой. В самом деле, единицей в Z_n будет элемент 0, а при $a \in Z_n$ обратным элементом к a будет элемент $(n - a) \pmod n$. Столь же легко проверяется, что Z_n — это циклическая группа, порожденная элементом 1. При этом $|Z_n| = n$.

Напомним, что на множестве $\{0, 1, \dots, n-1\}$ мы рассматривали еще и операцию $\otimes_n$, определенную равенством $a \otimes_n b = (ab) \pmod n$. Однако $(Z_n, \otimes_n)$ в общем случае является только полугруппой с единицей (моноидом), но не группой, так как содержит необратимые (относительно операции $\otimes_n$ элементы), например 0. Легко можно привести примеры необратимых элементов отличных от нуля. В самом деле, пусть $n = 8$. В этом случае выражение $4 \otimes_8 x$ принимает только два значения: 0 при $x = 0, 2, 4, 6$ и 4 при $x = 1, 3, 5, 7$. Таким образом, элемент 4 необратим относительно операции $\otimes_8$.

Интересно отметить, что существование примера ненулевого необратимого относительно операции $\otimes_n$ элемента связано с природой числа n. В самом деле, мы существенно использовали то, что число 8 *составное*. Оказывается, что имеет место следующий важный факт:

Предложение. *Пусть p — простое число, а $Z_p^* := \{1, 2, \dots, p-1\}$. Доказать, что $Z_p^\times := (Z_p^*, \otimes_p)$ является группой.*

Упражнение. Доказать предыдущее предложение и выяснить, является ли эта группа $Z_p^\times$. Если да, то найти порождающий ее элемент.

Задача 1.9. Пусть $n \geqslant 1$ — целое число. Обозначим символом $(\mathbb{Z}/n\mathbb{Z})^\times$ совокупность всех чисел из множества $\{1, \ldots, n\}$, взаимно простых с n. Т.е.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{N}\colon 1 \leqslant a \leqslant n,\ \text{НОД}(a, n) = 1\}.$$

Проверить, что $(\mathbb{Z}/n\mathbb{Z})^\times$ является группой относительно операции $\otimes_n$.

Задача 1.10. Пусть $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$. Функция $\varphi\colon \mathbb{N} \to \mathbb{N}$ называется *функцией Эйлера*. Она играет важную роль в теории чисел. Доказать, что если число $n = p_1^{k_1} \times \cdots \times p_m^{k_m}$ — это разложение числа n на простые множители, то

$$\varphi(n) = \prod_{j=1}^{m} \left(p_j^{k_j} - p_j^{k_j - 1}\right).$$

Приведем теперь пример конечной мультипликативной циклической группы. Пусть, как и раньше, $n \geqslant 1$ — натуральное число. Рассмотрим множество комплексных чисел $U_n := \{e^{2\pi i k/n}\colon k = 0, 1, \ldots, n-1\}$ с обычной операцией умножения комплексных чисел. Легко проверить, что это группа, причем циклическая. Порождающим элементом группы U_n будет число $e^{2\pi i/n}$. В частности, $U_2 = \{-1, 1\}$ — это мультипликативная группа состоящая из двух элементов.

Пример 1.14. Нетрудно проверить (это оставляется в качестве *упражнения*), что совокупность вращений плоскости, оставляющих на месте правильный n-угольник ($n \in \mathbb{N}$) с центром, совпадающим с центром вращения, образуют циклическую группу, обозначаемую C_n. Эта группа является собственной подгруппой группы D_n всех симметрий правильного n-угольника.

Упражнение. Опишите циклическая подгруппу группы $SL_2(\mathbb{Z})$, порожденную матрицей

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Одно из основных свойств циклических групп состоит в следующем:

Предложение 1.15. *Всякая подгруппа циклической группы является циклической группой.*

Доказательство. Пусть H — произвольная подгруппа циклической группы $G = \langle g \rangle$. Если $g^k \in H$, то $g^{-k} \in H$. Среди всех элементов вида $g^k \in H$ для которых $k > 0$ выберем элемент g^m, где m — это наименьшее положительное число, для которого $g^m \in H$. Запишем теперь любое целое число k в виде $k = pm + q$, $0 \leqslant q < m$. Если теперь $g^k \in H$, то $g^q = g^{k - pm} \in H$ и из минимальности m вытекает, что $q = 0$. Следовательно, $H = \langle g^m \rangle$, т.е. H является циклической группой. □

Порядок элемента группы. Пусть G — произвольная (не обязательно циклическая) группа, а $a \in G$. Для элемента a может выполняться одна из следующих двух (взаимоисключающих) ситуаций. Во-первых, все степени элемента a могут быть различны. Простейший пример — целыми степенями элемента 1 в аддитивной группе вещественных чисел $\mathbb{R}$ являются целые числа.

Во-вторых, могут найтись два таких целых числа m и n, что $a^m = a^n$. Пусть $n > m$. В этом случае получаем, что $a^{n-m} = e$ (единичный элемент в G). Например, элемент $b = 2$ группы Z_6 обладает тем свойством, что $b^1 = b^4$, откуда вытекает, что $b^3 = e$ (в самом деле, $b^4 = 8 \pmod 6 = 2$ и $b^3 = 6 \pmod 6 = 0$).

Определение. *Если $a^m \neq a^n$ при любых целых чисел $m \neq n$, то говорят, что элемент a имеет в G бесконечный порядок. Этот факт записывается в виде* $\operatorname{ord}_G a = \infty$ *или, если группа G ясна из контекста, в виде* $\operatorname{ord} a = \infty$.

Если элемент a группы G такой, что при некоторых целых $m \neq n$ имеет место равенство $a^m = a^n$, то говорят, что элемент a имеет в G конечный порядок, а натуральное число

$$\operatorname{ord}_G a = \operatorname{ord} a = \min\{p \in \mathbb{N} \colon a^p = 1\}$$

называется порядком элемента a в G.

В приведенных выше примерах, $\operatorname{ord}_{\mathbb{R}} 1 = \infty$ и $\operatorname{ord}_{Z_6} 2 = 3$.

Из определения порядка элемента непосредственно вытекает, что если $|G| < \infty$, то $\operatorname{ord}_G a < \infty$ для любого элемента a группы G. Имеют место также следующее важное свойство:

Предложение 1.16. *Для любого элемента a группы G верно равенство $\operatorname{ord}_G a = |\langle a \rangle|$. Если $\operatorname{ord}_G a = q < \infty$, то $\langle a \rangle = \{e, a, \ldots, a^{q-1}\}$ и, кроме того $a^n = e$ если и только если $n = kq$ при $k \in \mathbb{Z}$.*

Доказательство. Напомним, что $\langle a \rangle$ — это циклическая подгруппа группы G, порожденная элементом a, т.е. $\langle a \rangle = \{a^k \colon k \in \mathbb{Z}\}$. Пусть $\operatorname{ord}_G a = \infty$. Тогда, по определению элемента бесконечного порядка все целые степени элемента a различны и, следовательно, $|\langle a \rangle| = \infty$.

Пусть теперь $\operatorname{ord}_G a = q < \infty$. Тогда все элементы $e, a, a^2, \ldots, a^{q-1}$ различны, а $a^q = 1$. Далее, для произвольного $n \in \mathbb{Z}$ из равенства $n = kq + r$, где $k \in \mathbb{Z}$, а $r \in \{0, 1, \ldots, q-1\}$, вытекает, что $a^n = a^{kq+r} = (a^q)^k * a^r = a^r$. Из этого равенства непосредственно вытекают оставшиеся утверждения. □

Определение. *Пусть G — конечная группа. Число $d(G)$, равное наименьшему из натуральных чисел m таких, что $g^m = 1$ для любого элемента $g \in G$, называется периодом группы G.*

В следующей задаче предлагается выяснить простые свойства периода группы в случае конечных групп общего вида и коммутативных конечных групп.

Задача 1.11. Пусть G — конечная группа. Доказать, что период $d(G)$ группы G делит порядок $|G|$ этой группы и равен наименьшему общему кратному порядков элементов группы G. Проверить, что если группа G является коммутативной, то найдется элемент $g \in G$ такой, что $\operatorname{ord}_G g = d(G)$. Показать, что коммутативная группа G является циклической тогда и только тогда, когда $d(G) = |G|$. Выяснить, сохранятся ли два последних утверждения в случае, если группа G не будет коммутативной.

Один из основных вопросов теории групп — это вопрос о строении различных групп. Традиционно так называют вопрос о том, как могут быть устроены подгруппы рассматриваемых групп.

В случае циклических групп мы уже доказали, что любая подгруппа циклической группы является циклической. Рассмотрим вопрос о строении циклических групп более подробно.

Пусть $A = \langle a \rangle$ — аддитивная циклическая группа, порожденная элементом a. При доказательстве Предложения 1.15 было, по-существу, доказано, что если $|A| = \infty$, то подгруппы группы A — это в точности подгруппы $kA := \{kja \colon j \in \mathbb{Z}\}$ при $k \in \mathbb{N}$.

Пусть теперь $|A| = n < \infty$. Снова вспоминая доказательство Предложения 1.15 заключаем, что любая подгруппа A_1 группы A — это циклическая группа, порожденная элементом da при некотором натуральном d, причем d — это минимально возможное число с таким свойством. Пусть r — это остаток от деления n на d, т.е. $n = kd + r$ при подходящем k, а $0 \leqslant r < d - 1$. Так как $0 = na = (dk + r)a = k(da) + ra$, то $ra = -k(da) \in A_1$. Из минимальности d вытекает, что $r = 0$, т.е. n делиться на d и $A_1 = dA = \{0, da, 2da, \ldots, (k-1)da\}$. Таким образом, перебирая все делители d числа n, мы будем получать подгруппы циклической группы порядка n, причем каждому делителю числа n соответствует в точности одна подгруппа группы A.

Замечание. В (аддитивной) циклической группе $A = \langle a\rangle$ порядка n подгруппа порядка d, где d — положительный делитель числа n, совпадает с множеством $\{b \in A\colon db = 0\}$.

В самом деле, если $n = dk$, то соответствующая подгруппа имеет вид kA и, следовательно, $db = 0$ для $b \in kA$. Если, обратно, $b = ja \in A$ и $db = 0$, то $dja = 0$ и, следовательно, $dj = ns = dks$, откуда $j = ks$ и $b = s(ka) \in kA$.

Задача 1.12. Пусть G — произвольная группа, $a \in G$, и пусть $k \in \mathbb{Z}^*$. Доказать, что если $\operatorname{ord}_G a = \infty$, то $\operatorname{ord}_g a^k = \infty$, а если $\operatorname{ord}_G a = n < \infty$, то $\operatorname{ord}_G a^k = n/\operatorname{НОД}(n,k)$.

Задача 1.13. Доказать, что если $|G| = 2n < \infty$, $n \in \mathbb{N}$, то в G обязательно существует элемент g порядка 2.

1.4. Системы образующих и определяющие соотношения в группах

В этом разделе мы рассмотрим конструкцию, естественно обобщающую понятие циклической группы.

Системы образующих в группах. Пусть G — некоторая группа и пусть $A \subset G$ — некоторое подмножество ее элементов. Имеет место следующее утверждение:

Предложение 1.17. *Существует единственная подгруппа $G_A \leq G$ такая, что*

(1) $A \subset G_A$;

(2) *для любой подгруппы $G_1 \leq G$ со свойством $A \subset G_1$ имеет место $G_A \leq G_1$.*

Другими словами, G_A — это минимальная *подгруппа группы G, содержащая A.*

Доказательство. Вначале заметим, что единственность подгруппы G_A непосредственно вытекает из условия ее минимальности. Пусть, от противного, существуют две минимальные подгруппы G_A^1 и G_A^2 группы G, содержащие множество A. Тогда $G_A^1 \leq G_A^2$ и $G_A^2 \leq G_A^1$, откуда $G_A^1 = G_A^2$.

Для доказательства существования подгруппы G_A докажем вначале, что если J — некоторое множество индексов, а $G_j \leq G$, $j \in J$ — некоторый набор подгрупп группы G, то $H = \bigcap_{j\in J} G_j$ также является подгруппой в G.

В самом деле, так как единица e группы G принадлежит все подгруппам G_j при $j \in J$, то $e \in H$, откуда вытекает, что H — это моноид. Проверим замкнутость H относительно умножения. Если $a, b \in H$, то $a, b \in G_j$ для любого $j \in J$. Но тогда $ab \in G_j$ для любого $j \in J$, откуда следует, что $ab \in H$. Аналогично проверяется, что для любого элемента $a \in H$ элемент $a^{-1} \in H$. Таким образом, $H \leq G$.

Теперь для доказательства существования группы G_A необходимо применить эту конструкцию к семейству, состоящему из всех подгрупп H группы G со свойством $A \subset$. □

Определение. *Пересечение всех подгрупп H группы G со свойством $A \subset$ обозначается символом $\langle A\rangle_G$ или, если группа G ясна из контекста, $\langle A\rangle$.*

Замечание. Ясно, что $G_A = \langle A\rangle_G$.

Группа $\langle A\rangle_G$ допускает и конструктивное описание. Так, имеет место следующее утверждение:

Предложение 1.18. $\langle A\rangle = \{x_1 \times \cdots \times x_n\colon$ *где $n \in \mathbb{N}$, а $x_j \in A$ или $x_j^{-1} \in A$ при $j = 1, \ldots, n\}$.*

Доказательство. Заметим, что множество $X_A = \{x_1 \times \cdots \times x_n\colon$ где $n \in \mathbb{N}$, а $x_j \in A$ или $x_j^{-1} \in A$ при $j = 1, \ldots, n\}$является группой относительно той же операции умножения, что и исходная группа G. В самом деле, $1 \in X_A$ так как $1 = xx^{-1}$ для любого $x \in A$. Далее, если $v, w \in X_A$, то $v = v_1 \cdots v_n$, $w = w_1 \cdots w_m$, где $n, m \in \mathbb{N}$, а v_j или

v_j^{-1} и w_j или w_j^{-1} принадлежат A. Тогда $vw = v_1 \cdots w_m$, а это произведение принадлежит X_A. Аналогично, $v^{-1} = v_n^{-1} \cdots v_1^{-1}$, а это снова произведение требуемого вида. Итак, $X_A \leq G$ и $A \subset X_A$. Следовательно, $\langle A \rangle \leq X_A$ (так как $\langle A \rangle$ — это минимальная подгруппа, содержащая A).

Пусть теперь H — произвольная подгруппа группы G, содержащая множество A. Следовательно $a \in H$ и $a^{-1} \in H$ для любого $a \in A$. Следовательно, любое произведение вида $x_1 \times \cdots \times x_n$, где $x_j \in A$ или $x_j^{-1} \in A$ принадлежит H, откуда $X_A \leq H$ и, следовательно, $X_A \leq \langle A \rangle$. □

Определение. *Если $A \subset G$ — такое подмножество группы G, что $\langle A \rangle = G$, то говорят, что группа G порождена множеством A элементов. Само множество A в таком случае называется системой образующих (или порождающих) элементов группы G.*

Если $G = \langle A \rangle$ для некоторого конечного множества A, то группа G называется конечно-порожденной. В случае конечного множества $A = \{a_1, \ldots, a_n\}$ используется обозначение

$$\langle A \rangle = \langle a_1, \ldots, a_n \rangle.$$

Замечание. Каждая группа G имеет какую-то систему образующих. В самом деле, имеет место очевидное равенство $G = \langle G \rangle$.

Простым примером конечно-порожденных групп являются циклические группы.

Пример 1.19. Пусть D_n — группа движений правильного плоского n-угольника. Нам будет удобно считать, что рассматриваемый n-угольник расположен на плоскости Oxy так, что его центр совпадает с началом координат, а одна из его вершин лежит на положительной полуоси оси Ox. Выделим в этой группе два преобразования: преобразование $\mathfrak{R}$ поворота на угол $2\pi/n$ (углы отсчитываются от положительной полуоси оси Ox в направлении против часовой стрелки) и преобразование $\mathfrak{S}$ симметрии относительно оси Ox. Ясно, что $\operatorname{ord} \mathfrak{R} = n$, $\operatorname{ord} \mathfrak{S} = 2$. Кроме того, $\mathfrak{S} \neq \mathfrak{R}^k$ при любом $k = 0, 1, \ldots, n-1$, но $\mathfrak{R}\mathfrak{S} = \mathfrak{S}\mathfrak{R}^{-1}$. Заметим также, что $\mathfrak{S}\mathfrak{R}^k \neq \mathfrak{S}\mathfrak{R}^m$ при $k \neq m$. Таким образом, в группе D_n порядка $2n$ есть $2n$ различных элементов:

$$\mathrm{id}, \mathfrak{R}, \mathfrak{R}^2, \ldots, \mathfrak{R}^{n-1}; \mathfrak{S}, \mathfrak{S}\mathfrak{R}, \mathfrak{S}\mathfrak{R}^2, \ldots, \mathfrak{S}\mathfrak{R}^{n-1}.$$

Другими словами,

$$D_n = \langle \mathfrak{R}, \mathfrak{S} \rangle.$$

Так как $\mathfrak{S}$ и $\mathfrak{R}$ не коммутируют, то группа D_n не является абелевой.

Задача 1.14. Пусть G – группа, а элементы $a, b \in G$ коммутируют (т.е. $ab = ba$) и таковы, что $\text{НОД}(\operatorname{ord} a, \operatorname{ord} b) = 1$. Доказать, что в этом случае $\langle a, b \rangle = \langle ab \rangle$.

Задача 1.15. Найти порядки элементов

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{и} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

в группе $SL_2(\mathbb{Z})$. Показать, что $\langle AB \rangle$ — бесконечная циклическая подгруппа в $SL_2(\mathbb{Z})$.

Задача 1.16. Предложить какую-либо систему образующих для мультипликативной группы $\mathbb{Q}_+$ положительных рациональных чисел.

Свободные группы и определяющие соотношения в группах. Пусть $G = \langle a_1, \ldots, a_n \rangle$ — это группа, порожденная n образующими $a_1, a_2, \ldots, a_n$. Тогда каждый элемент $g \in G$ можно записать (возможно многими различными способами) в виде

$$g = a_{j_1}^{k_1} a_{j_2}^{k_2} \times \cdots \times a_{j_m}^{k_m}, \tag{1.4}$$

где $k_1, \ldots, k_m \in \mathbb{Z}$, $j_1, \ldots, j_m \in \{1, \ldots, n\}$ причем $j_s \neq j_{s+1}$ при $s = 1, 2, \ldots, k-1$ (т.е. «подобные сомножители» приведены везде, где это возможно, а представления вида $e = a_1 a_1^{-1}$ не рассматриваются).

Заметим, что если единичный элемент $e \in G$ допускает ровно одно представление вида (1.4), то и для любого элемента $g \in G$ представление вида (1.4) единственно (проверка этого простого факта оставляется в качестве *упражнения*).

Определение. *Пусть* $G = \langle a_1, \dots, a_n \rangle$. *Если при любых допустимых* $j_1, \dots, j_m$ *равенство* $a_{j_1}^{k_1} a_{j_2}^{k_2} \times \dots \times a_{j_m}^{k_m} = e$ *имеет место тогда и только тогда, когда* $k_1 = \dots = k_m = 0$, *то говорят, что группы* G *— это свободная группа ранга* n, *порожденная* n *свободными образующими.*

Пример 1.20. Приведем примеры свободных групп. Так, аддитивная группа целых чисел $\mathbb{Z}$ будет свободной группой ранга 1 (она порождается одной свободной образующей, в качестве которой выступает элемент 1).

Пример свободной группы ранга 2 строится несколько сложнее. Рассмотрим матричную группу $SL_2(\mathbb{Z}[t])$, где $\mathbb{Z}[t]$ — это совокупность всех многочленов от переменной t с целочисленными коэффициентами (проверка того факта, что $SL_2(\mathbb{Z}[t])$ является группой, оставляется в качестве простого *упражнения*). Пусть $F \leq SL_2(\mathbb{Z}[t])$ — это подгруппа, порожденная матрицами

$$a = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \qquad \text{и} \quad b = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.$$

Проверка того факта, что a и b порождают группу F свободно, оставляется к качестве простого *упражнения* на операции с матрицами.

Термин «свободная группа» объясняется тем, что образующие такой группы не связаны между собой какими-либо соотношениями. Однако во многих случаях группы порождаются образующими, которые связаны между собой различными соотношениями. Так, циклическая группа порядка n порождена одним образующим элементом g, который удовлетворяет соотношению $g^n = 1$.

Далее, порождающие элементы $\mathfrak{R}$ и $\mathfrak{S}$ группы D_n связаны, например, соотношениями $\mathfrak{R}^n = \mathrm{id}$, $\mathfrak{S}^2 = \mathrm{id}$, $\mathfrak{RS} = \mathfrak{S}\mathfrak{R}^{-1}$.

Определение. *Соотношением в группе* $G = \langle a \rangle$ *называется любое выражение вида (1.4), в котором* $g \in A \cup \{e\}$.

Предположим, что из всех соотношений, связывающих порождающие элементы некоторой группы $G = \langle A \rangle$ выбрано некоторое конечное подмножество $\rho_1, \dots, \rho_\ell$ соотношений, обладающее тем свойством, что любое соотношение в группе G может быть выведено соотношений $\rho_1, \dots, \rho_\ell$ и предположим, что ни одно из соотношений $\rho_1, \dots, \rho_\ell$ не может быть выброшено из этого множества без нарушения этого свойства.

Определение. *В таком случае говорят, что группа* G *является конечно-определенной группой, порожденной образующими* $a_1, \dots, a_n$ *и определяющими соотношениями* $\rho_1, \dots, \rho_\ell$, *и пишут*

$$G = \langle a_1, \dots, a_n | \rho_1, \dots, \rho_\ell \rangle.$$

Несколько более формальное определение *конечно-определенной* группы будет дано позднее, в качестве иллюстрации к дальнейшим теоретико-групповым конструкциям. Но для изучения примеров и решения простых задач достаточно данного выше определения.

Пример 1.21. Самым простым примером конечно-определенной группы является циклическая группа (любого конечного порядка) — она задается одним образующим элементом a и одним определяющим соотношением $a^n = e$.

Несколько более интересный пример — это группа D_3, которая задается двумя элементами $\mathfrak{R}$ и $\mathfrak{S}$ и соотношениями $\mathfrak{R}^3 = \mathfrak{S}^2 = \mathfrak{RSRS} = e$. Более общо, группа D_n задается двумя элементами $\mathfrak{R}$ и $\mathfrak{S}$ и соотношениями $\mathfrak{R}^n = \mathfrak{S}^2 = (\mathfrak{RS})^2 = e$.

Пример 1.22. Рассмотрим еще один пример. Рассмотрим два элемента, скажем, a и b и систему соотношений между ними

$$a^4 = 1, \quad b^2 = a^2, \quad bab^{-1} = a^{-1}. \tag{1.5}$$

Так как $ba = a^{-1}b = a^3b$ и так как $a^2 = b^2$, то всякий элемент вида (1.4), где $n = 2$, $a_1 = a$, а $a_2 = b$ может быть записан в виде $a^k b^m$, где $k = 0, 1, 2, 3$, а $m = 0, 1$. Таким образом, элементы a и b, связанные соотношениями (1.5), определяют некоторую группу, состоящую из 8 элементов.

1.5. Симметрическая и знакопеременная группы

Как отмечалось выше, множество $S(\Omega)$ всех биективных отображений некоторого множества Ω на себя образует группу относительно операции композиции отображений.

Определение. *Множество $S_n = S(\{1, 2, \ldots, n\})$, где $n \in \mathbb{N}$, рассматриваемое вместе с операцией композиции отображений, называется симметрической группой степени n. Элементы множества S_n называются перестановками.*

В качестве *упражнения* предлагается проверить, что $|S_n| = n!$.

Традиционно, перестановки обозначаются греческими буквами. Каждую перестановку $\pi : k \mapsto \pi(k)$, $k = 1, 2, \ldots, n$ для наглядности можно изобразить в виде $2 \times n$ матрицы

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}$$

где $k_j = \pi(j)$ — все числа из множества $\{1, 2, \ldots, n\}$ взятые по одному разу в каком-то порядке. Единичная перестановка обозначается символом $e : j \mapsto e(j) = j$, $j = 1, 2, \ldots, n$. Для перестановок определена операция *умножения*, которая определяется как композиция соответствующих отображений: произведение $\sigma\tau$ перестановок $\sigma \in S_n$ и $\tau \in S_n$ определяется как перестановка $j \mapsto \sigma(\tau(j))$, $j = 1, 2, \ldots, n$. Например, если

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \text{а} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

то произведения $\sigma\tau$ и $\tau\sigma$ вычисляются так

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

так что $\sigma\tau \neq \tau\sigma$.

Так как перестановки — это биективные отображения, то все они обратимы. В качестве *упражнения* предлагается определить перестановку, обратную произвольной перестановке $\pi \in S_n$, найти перестановки σ^{-1} и τ^{-1} и проверить при помощи непосредственного вычисления, что $\sigma\sigma^{-1} = \sigma^{-1}\sigma = 1$ и $\tau\tau^{-1} = \tau^{-1}\tau = 1$. Так как операция умножения перестановок ассоциативна и так как все перестановки обратимы, то для любой перестановки π и для любого целого числа m определена перестановка π^m.

Перестановка σ рассмотренная выше обладает тем свойством, что $\sigma : 1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1$. Перестановка τ может быть представлена в виде $\tau = \tau_1\tau_2$, где

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \quad \text{а} \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix},$$

причем перестановка τ_1 работает так $1 \mapsto 4 \mapsto 1$ (и оставляет на месте 2 и 3), а перестановка τ_2 циклически переставляет 2 и 3 и оставляет на месте 1 и 4. Для упрощения записи перестановки σ и τ естественно записать в виде (1234) и (14)(23) соответственно. При этом перестановки вида σ называются циклами длины 4, а перестановки вида τ

представляют собой произведение двух независимых (непересекающихся) циклов длины 2. В качестве упражнения предлагается вычислить, что $\sigma^2 = (13)(24)$, $\sigma^4 = e$, $\tau^2 = e$. Это представление перестановок σ и τ наталкивает нас на идею о том, что произвольная перестановка из S_n может быть разложена в произведение более простых перестановок.

Пусть $\Omega(n) := \{1, 2, \dots, n\}$ при $n \in \mathbb{N}$ и пусть $\pi \in S_n$ — некоторая перестановка. Скажем, что точки $a, b \in \Omega(n)$ являются π-эквивалентными, если $b = \pi^m(a)$ при некотором целом m. Несложно проверить, что введенное таким образом на множестве $\Omega(n)$ отношение является отношением эквивалентности (т.е. оно рефлексивно, симметрично и транзитивно). Следовательно, возникает разбиение множества $\Omega(n) = \Omega_1 \sqcup \dots \sqcup \Omega_q$ на непересекающиеся классы эквивалентности. Часто множества Ω_r называют π-*орбитами*. Это название оправдывается тем, что каждая точка $j \in \Omega(n)$ принадлежит только одному из множеств Ω_r, $r = 1, \dots, q$ и, если, $j \in \Omega_k$, то все множество Ω_k состоит из образов точки j при действии на нее степеней перестановки π:

$$\Omega_r = \{j, \pi(j), \pi^2(j), \dots, \pi^{\ell_k - 1}(j)\},$$

где ℓ_r — это наименьшее целое положительное число такое, что $\pi^{\ell_k}(j) = j$ (такое число заведомо существует, так как Ω_k — конечное множество). Перестановка

$$\pi_k := \begin{pmatrix} j & \pi(j) & \dots & \pi^{\ell_k - 2}(j) & \pi^{\ell_k - 1}(j) \\ \pi(j) & \pi^2(j) & \dots & \pi^{\ell_k - 1}(j) & j \end{pmatrix}$$

называется *циклом длины* ℓ_k. Цикл π_k оставляет на месте все точки из множества $\Omega(n) \setminus \Omega_k$. Кроме того, для любой точки $j \in \Omega_k$ имеет место равенство $\pi(j) = \pi_k(j)$. Эти два свойства дают основания называть циклы π_k при $k = 1, 2, \dots, q$ *независимыми* (или *непересекающимися*) *циклами*. Заметим еще, что $\pi_k^{\ell_k} = e$.

Итак, разбиение множества Ω на непересекающиеся классы эквивалентности по отношению π-эквивалентности порождает разложение перестановки π в произведение

$$\pi = \pi_1 \pi_2 \times \dots \times \pi_q,$$

где все циклы перестановочны друг с другом (так как все они независимы). Удобно записывать циклы в таком порядке, чтобы выполнялось неравенство

$$\ell_1 \geqslant \ell_2 \cdots \ell_p > \ell_{p+1} = \dots = \ell_q = 1.$$

Если цикл π_k имеет длину 1, то он действует как единичная перестановка и такие циклы в разложении перестановки π естественно опускать. Рассмотрим следующий пример

$$\pi \in S_8, \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (12345)(67)(8) = (12345)(67).$$

Здесь возникает проблема связанная с тем, что выражение $(12345)(67)$ может быть понято как перестановка из S_n при любом $n \geqslant 7$. Но при фиксированном n никакой неоднозначности в соответствующем разложении не возникает.

В самом деле, предположим, что существуют два различных разложения перестановки π в произведение независимых циклов:

$$\pi = \pi_1 \times \dots \times \pi_p = \alpha_1 \times \dots \times \alpha_r.$$

Пусть $j \in \Omega$ такой элемент, что $\pi(j) \neq j$. Тогда $\pi_k(j) \neq j$ и $\alpha_m(j) \neq j$ для одного (и только одного) из циклов π_* и одного (и только одного) из циклов α_*. Далее, для любого целого положительного числа s верно равенство $\pi_k^s(j) = \pi^s(j) = \alpha_m^s(j)$. Так как любой цикл однозначно определяется действием его степеней на любой не неподвижный элемент, то $\pi_k = \alpha_m$. Далее применяем индукцию по p или по r. В результате нами доказано следующее утверждение:

Предложение 1.23. *Каждая перестановка $\pi \neq e$ из S_n является произведением независимых циклов длины, большей или равной 2. Это разложение в произведение однозначно с точностью до порядка следования сомножителей.*

Введем еще одно важное понятие, связанное с перестановками. Цикл длины 2 будем называть *транспозицией*. Любая транспозиция имеет вид (ab) и оставляет на месте все символы, отличные от a и b. Из предложения 1.23 вытекает следующее утверждение

Предложение 1.24. *Каждая перестановка $\pi \in S_n$ может быть представлена в виде произведения транспозиций.*

Для **доказательства** достаточно заметить, что

$$(1, 2, \dots, m-1, m) = (1, m)(1, m-1)(1, m-2) \times \cdots \times (1, 3)(1, 2)$$

(здесь в записи циклов для удобства чтения элементы разделены запятыми). Разумеется, разложение перестановки в произведение транспозиций не является единственным. Например, в S_4 имеют место следующие разложения

$$(123) = (13)(12) = (23)(13) = (13)(24)(12)(14).$$

Более того, в общем случае имеет имеет место равенство $\sigma\tau^2 = \sigma$ для любых транспозиций σ и τ (проверка оставляется в качестве *упражнения*). Таким образом, количество транспозиций в разложении перестановки $\pi \in S_n$ зависит не только от π, но и от способа разложения.

Четность перестановок. Интересно и полезно найти величину, которая будет инвариантом разложения перестановки в произведение транспозиций. Для этого рассмотрим следующую конструкцию. Пусть $\pi \in S_n$ и пусть f — произвольная функция от n переменных. Определим

$$(\pi \circ f)(x_1, \dots, x_n) := f(x_{\pi(1)}, \dots, x_{\pi(n)}).$$

Говорят, что функция $g = \pi \circ f$ получена *действием* π на f. Например, если $\pi = (123)$, а $f(x_1, x_2, x_3) = x_1 + 2x_2^2 + 3x_3^3$, то $\pi \circ f(x_1, x_2, x_3) = x_3 + 2x_1^2 + 3x_2^3$. Из определения действия подстановки на функцию и из формулы $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$ вытекает, что если $\alpha, \beta \in S_n$, а f — произвольная функция от n переменных, то $(\alpha\beta) \circ f = \alpha \circ (\beta \circ f)$.

Определение. *Функция f от n переменных называется кососимметрической, если $\tau \circ f = -f$ для любой транспозиции $\tau \in S_n$.*

Предложение 1.25. *Пусть $\pi \in S_n$ и пусть $\pi = \tau_1 \times \cdots \times \tau_k$ — некоторое разложение π в произведение транспозиций. Тогда число $\varepsilon_\pi := (-1)^k$ полностью определяется перестановкой π и не зависит от способа ее разложения в произведение транспозиций. Кроме того, $\varepsilon_{\alpha\beta} = \varepsilon_\alpha\varepsilon_\beta$ для любых перестановок $\alpha, \beta \in S_n$.*

Определение. *Число ε_π называется четностью подстановки $\pi \in S_n$. Если $\varepsilon_\pi = 1$, то π называется четной, а если $\varepsilon_\pi = -1$, то π называется нечетной.*

Доказательство Предложения 1.25. Рассмотрим произвольную кососимметрическую функцию f от n переменных. Так как действие π на f сводится к последовательному действию на f транспозиций τ_k, τ_{k-1}, ..., τ_1, (т.е. к умножению функции f на -1, проделанному k раз), то $\pi \circ f = (-1)^k f = \varepsilon_\pi f$. Так как левая часть этого равенства зависит только от π, но не от его разложения в произведение транспозиций, то и отображение $\pi \mapsto \varepsilon_\pi$ должно полностью определяться перестановкой π (при условии, разумеется, что f не равна тождественно нулю). Осталось вспомнить, что существуют ненулевые кососимметрические функции n аргументов, например функция

$$f(x_1, \dots, x_n) = \prod_{1 \leqslant j < k \leqslant n} (x_k - x_j).$$

Для доказательства последнего утверждения теоремы заметим, что

$$\varepsilon_{\alpha\beta} f = (\alpha\beta) \circ f = \alpha \circ (\beta \circ f) = \alpha \circ (\varepsilon_\beta f) = \varepsilon_\beta(\alpha \circ f) = \varepsilon_\beta\varepsilon_\alpha f. \quad \square$$

Замечание. 1) Произведение перестановок одинаковой четности дает четную перестановку, а произведение перестановок различной четности дает нечетную перестановку.

2) Количество четных и нечетных перестановок в S_n одинаково и равно $n!/2$.

3) Множество A_n состоящее из всех *четных* перестановок степени n является подгруппой группы S_n.

Проверка утверждений этого замечания является весьма простой и оставляется в качестве *упражнения.*

Определение. *Группа A_n называется знакопеременной группой (степени n).*

Пусть некоторая перестановка $\pi \in S_n$ разложена в произведение независимых циклов длин $\ell_1, \ell_2, \ldots, \ell_m$. Тогда

$$\varepsilon_\pi = (-1)^{\sum_{k=1}^{m}(\ell_k - 1)}.$$

В самом деле, пусть $\pi = \pi_1 \times \cdots \times \pi_m$ — разложение π в произведение независимых циклов. Так как цикл π_k длины ℓ_k раскладывается в произведение $\ell_k - 1$ транспозиции, то его четность равна $(-1)^{\ell_k - 1}$. Остается перемножить эти величины для всех циклов из разложения.

1.6. Таблицы Кэли. Группа кватернионов и группа Клейна

Пусть G — некоторая конечная группа. В этом случае часто бывает удобно рассматривать таблицу, в которую записаны все попарные произведения элементов $\{g_1, \ldots, g_n\}$ группы G:

$*$	g_1	g_2	$\cdots$	g_n
g_1	g_1^2	$g_1 g_2$	$\cdots$	$g_1 g_n$
g_2	$g_2 g_1$	g_2^2	$\cdots$	$g_2 g_n$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g_n	$g_n g_1$	$g_n g_2$	$\cdots$	g_n^2

Такие таблицы часто называются *таблицами Кэли.* Основной смысл этого понятия станет ясен чуть позже (при изучении понятия изоморфизма групп).

Приведем несколько простых примеров. Таблица Кэли аддитивной циклической группы второго порядка Z_2 имеет вид

$+$	0	1
0	0	1
1	1	0

Аналогично, для группы Z_4 таблица Кэли имеет вид:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Таблицу Кэли для группы Z_2 интересно сравнить с соответствующей таблицей для мультипликативной группы $U_2 = \{1, -1\}$:

$\times$	1	-1
1	1	-1
-1	-1	1

а таблицу Кэли группы Z_4 — с мультипликативной группой из четырех элементов $\{\pm 1, \pm i\}$ (умножение здесь — это обычное умножение комплексный чисел):

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Последнюю группу обозначим символом $Q(i)$. Это не стандартное обозначение, оно похоже на обозначение группы Q_8, которая будет введена позже. Заметим, что проверка того факта, что $Q(i)$ в самом деле является группой не вызывает сложностей — все следует из того, что множество $Q(i)$ содержится в $\subset \mathbb{C}^*$ и замкнуто относительно умножения.

В то же самое время, используя таблицу Кэли можно дать другое обоснование того, что $Q(i)$ является группой. Идея такова: раз мы знаем все попарные произведения элементов множества $Q(i)$, то можем проверить все аксиомы группы (ассоциативность умножения, наличие единицы и обратимость элементов) за конечное (пусть и довольно большое) число явных вычислений.

Отметим несколько «сходных черт» групп Z_4 и $Q(i)$. В группе Z_4 есть два элемента порядка 4 (это 1 и 3), один элемент порядка 2 (это 2) и один элемент порядка 1 (это 0 — нейтральный элемент группы Z_4). В группе $Q(i)$ элементы порядка 4 — это i и $-i$, элемент порядка 2 — это -1, а элемент первого порядка — это 1 (единица группы $Q(i)$). Эти сходные черты, а на самом деле тот факт, что таблицу Кэли группы $Q(i)$ можно получить из таблицы Кэли группы Z_4 (и наоборот) при помощи простой подстановки

$$0 \leftrightarrow 1, \qquad 1 \leftrightarrow i, \qquad 2 \leftrightarrow -1, \qquad 3 \leftrightarrow -i,$$

намекает на то, что группы Z_4 и $Q(i)$ «различаются» только «формой» записи своих элементов и операции. Точное объяснение этого феномена мы дадим несколько позже, при обсуждении понятия *изоморфизма групп*.

Заметим также, что из таблицы Кэли для группы $Q(i)$ видно, что эта группа является циклической группой, порожденной элементом i.

Используем теперь таблицу Кэли для определения *группы кватернионов* Q_8. Пусть $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ — множество, состоящее из восьми элементов и пусть попарные произведения этих элементов заданы следующим образом:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Проверка того, что заданное таким образом умножение в самом деле определяет структуру мультипликативной группы на множестве Q_8 оставляется в качестве *упражнения*. Для облегчения проверки зададим это умножение не в табличном виде, а в виде нескольких легко запоминающихся правил (правила умножения на ± 1 стандартны и очевидны): $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

Заметим, что в группе Q_8 легко выделить три подгруппы, являющиеся циклическими группами четвертого порядка — это группы $Q(i)$, $Q(j)$ и $Q(k)$.

Можно легко показать, что группа Q_8 является конечно-определенной группой, порожденной элементами $a = i$ и $b = j$ и соотношениями (1.5) из Примера 1.22.

Упражнение. Определим матрицы $I, J, K \in M_2(\mathbb{C})$

$$J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Показать, что множество $\{\pm E, \pm J, \pm I, \pm K\}$ с обычной операцией матричного умножения имеет такую же таблицу Кэли, как и группа Q_8.

Пример 1.26. Таблица Кэли

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

задает на множестве $V_4 = \{e, a, b, c\}$ структуру группы, которая называется *группой Клейна*. В качестве *упражнения* предлагается проверить, что V_4 в самом деле является группой, найти порядки всех элементов в этой группе и показать, чем различаются таблицы Кэли групп V_4 и Z_4.

1.7. Основные матричные группы

Пример 1.27. Пусть $n \in \mathbb{N}$. Рассмотрим множество матриц

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \colon \det A \neq 0\}$$

и вспомним, что если матрицы A и B таковы, что $\det A \neq 0$ и $\det B \neq 0$, то и $\det AB \neq 0$. Кроме того $\det E = 1 \neq 0$ (напомним, что через E обозначается единичная матрица) и, если $\det A \neq 0$, то и определитель обратной матрицы A^{-1} также отличен от нуля. Таким образом, множество $GL_n(\mathbb{R})$ образует группу относительно операции матричного умножения. Эта группа часто называется *общей линейной группой ранга* n.

Группа $GL_n(\mathbb{R})$ содержит важную подгруппу

$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \colon \det A = 1\},$$

которую часто называют *специальной линейной группой ранга* n. Проверка того факта, что $SL_n(\mathbb{R})$ является группой относительно операции матричного умножения, оставляется читателю в качестве несложного *упражнения*.

Еще несколько примеров матричных групп можно получить, изменив в определении общей и специальной линейной групп множество, из которого берутся элементы матриц. Так возникают группы $GL_n(\mathbb{Q})$ и $GL_n(\mathbb{C})$ и их подгруппы $SL_n(\mathbb{Q})$ и $SL_n(\mathbb{C})$ соответственно.

Заметим однако, что множество матриц $GL_n(\mathbb{Z})$ не является группой, так как обратная матрица к матрице с целочисленными элементами может и не быть матрицей с целочисленными элементами. Однако, из формул для элементов обратной матрицы следует, что множество $SL_n(\mathbb{Z})$ уже будет группой относительно операции матричного умножения.

Кроме специальной линейной группы в группе $GL_n(\mathbb{R})$ выделяют так называемую *унимодулярную группу*, которая состоит из всех матриц с определителем ± 1. В группе $GL_n(\mathbb{C})$, состоящей из всех невырожденных комплексных $n \times n$-матриц, под унимодулярной группой понимается подгруппа всех матриц A таких, что $|\det A| = 1$.

Так как с каждой матрицей $A \in GL_n(\mathbb{R})$ естественным образом связывается некоторое линейное невырожденное преобразование пространства $\mathbb{R}^n$, то можно считать, что $GL_n(\mathbb{R}) \subset S(\mathbb{R}^n)$ — подгруппа группы $S(\mathbb{R}^n)$ всех биективных отображений пространства $\mathbb{R}^n$ в себя. Заметим также, что $GL_1(\mathbb{R}) = \mathbb{R}^\times$, $GL_1(\mathbb{Q}) = \mathbb{Q}^\times$, а $SL_1(\mathbb{R}) = SL_1(\mathbb{Q}) = SL_1(\mathbb{Z}) = \{1\}$.

Напомним определения основных матричных групп, естественно возникающих в линейной алгебре и в геометрии как специальные подгруппы групп преобразований аффинных, евклидовых, эрмитовых и симплектических пространств. Так возникают (всюду далее $n \in \mathbb{N}$)

- ортогональная группа $O(n) = \{A \in M_n(\mathbb{R})\colon AA^\top = A^\top A = E\}$;
- специальная ортогональная группа $SO(n) = \{A \in O(n)\colon \det A = 1\}$;
- унитарная группа $U(n) = \{A \in M_n(\mathbb{C})\colon AA^* = A^*A = E\}$;
- специальная унитарная группа $SU(n) = \{A \in U(n)\colon \det A = 1\}$;

и другие группы. Напомним также, что

$$O(1) = \{\pm 1\}, \quad SO(1) = \{1\}, \quad U(1) = \{e^{i\theta} :\ \theta \in [0, 2\pi)\}, \quad SU(1) = \{1\},$$

а также, что

$$SO(2) = \left\{ \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} :\ \phi \in [0, 2\pi) \right\} \cong U(1),$$

причем соответствующий изоморфизм задается следующим образом

$$\begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \mapsto e^{i\phi}.$$

РАЗДЕЛ 2

Основные понятия теории групп — введение

2.1. Изоморфизмы и гомоморфизмы групп

Рассмотрим следующий простой пример. Пусть D_3 — группа симметрий правильного треугольника. Хорошо известно, что она состоит из шести отображений плоскости — из трех вращений (относительно центра треугольника на углы 0, $2\pi/3$ и $4\pi/3$) и из трех симметрий относительно медиан, проведенных к каждой из сторон. Предположим, что мы пронумеровали вершины треугольника числами 1, 2 и 3. Тогда в результате описанных вращений треугольник преобразуется так, что вершины переходят одна в другую по следующим правилам:

$$(1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3), \quad (1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1), \quad (1 \mapsto 3, 3 \mapsto 2, 2 \mapsto 1)$$

а в результате соответствующий симметрий — по правилам

$$(1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2), \quad (1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1), \quad (1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3).$$

Из этого видно, что группа D_3 «похожа» на группу $S_3 = \{\mathrm{id}, (12), (23), (13), (123), (132)\}$. Более того, легко проверить, что если симметриям ϕ_1 и ϕ_2 рассматриваемого треугольника соответствуют перестановки σ_1 и σ_2 из группы S_3, то отображению $\phi_1 \circ \phi_2$ будет соответствовать перестановка $\sigma_1\sigma_2$.

Рассуждая аналогичным образом можно заметить, что группа C_n всех вращений правильного n-угольника «похожа» на циклическую подгруппу $\langle(12\cdots n)\rangle$ группы S_n. В предыдущем разделе были приведены и других примеры «похожих» групп.

Все эти примеры представляют собой частные случаи общего понятия *изоморфных* групп. Перейдем к общим определениям.

Определение. *Две группы G_1 и G_2 называются изоморфными, если существует биективное отображение $f : G_1 \to G_2$ такое, что для любых элементов $a, b \in G_1$ имеет место равенство $f(ab) = f(a)f(b)$. Факт изоморфизма групп G_1 и G_2 записывается символом $G_1 \cong G_2$. Кроме того, отображение f называется изоморфизмом групп G_1 и G_2.*

Уточним, что в равенстве $f(ab) = f(a)f(b)$ в определении изоморфизма произведение ab рассматривается относительно операции в группе G_1, а произведение $f(a)f(b)$ — относительно операции в группе G_2.

Установим основные свойства изоморфизма групп.

Предложение. *Если $f : G_1 \to G_2$ – изоморфизм групп G_1 и G_2, то $f(e_1) = e_2$, где e_j — единица группы G_j, $j = 1, 2$.*

Проверка. В самом деле, так как $ae_1 = e_1a = a$ для любого элемента $a \in G_1$, то $f(a) = f(ae_1) = f(a)f(e_1)$ и $f(a) = f(e_1a) = f(e_1)f(a)$. Следовательно, $f(e_1)$ — единица группы G_2, т.е. (напомним, что единица в группе единственна) $f(e_1) = e_2$. □

Предложение. *Если $f : G_1 \to G_2$ — изоморфизм групп G_1 и G_2, то $f(a^{-1}) = f(a)^{-1}$ для любого элемента $a \in G_1$.*

Проверка. Так как $aa^{-1} = e_1$, то $e_2 = f(e_1) = f(aa^{-1}) = f(a)f(a^{-1})$. Отсюда

$$f(a)^{-1} = f(a)^{-1}e_2 = f(a)^{-1}(f(a)f(a^{-1})) = (f(a)^{-1}f(a))f(a^{-1}) = e_2f(a^{-1}) = f(a^{-1}). \quad \square$$

Предложение. *Если $f : G_1 \to G_2$ — изоморфизм групп G_1 и G_2, то обратное отображение f^{-1} является изоморфизмом групп G_2 и G_1.*

Проверка. Так как f — биективное отображение, то и f^{-1} — биективное отображение. Проверим, что оно сохраняет операцию умножения. Рассмотрим произвольные элементы $x, y \in G_2$ и найдем такие $a, b \in G_1$, что $x = f(a)$, а $y = f(b)$. Тогда $xy = f(a)f(b) = f(ab)$ и, следовательно, $ab = f^{-1}(xy)$, т.е. $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. □

Пример 2.1. Два примера изоморфных групп были приведены в начале этого раздела. В самом деле, $S_3 \cong D_3$ и $C_n \cong \langle (12\cdots n)\rangle$.

Далее, аддитивная группа $\mathbb{R}$ вещественных чисел изоморфна мультипликативной группе $(\mathbb{R}_+^*, \times)$ положительных вещественных чисел, причем изоморфизм задается, например, функцией $\ln : \mathbb{R}_+^* \to \mathbb{R}$ (напомним, что $\ln(ab) = \ln a + \ln b$).

Изоморфизм циклических групп. Понятие изоморфизма хорошо иллюстрируется следующим важным свойством циклических групп:

Предложение 2.2. *Все циклические группы одного порядка (конечного или бесконечного) изоморфны.*

Доказательство. Пусть $\langle g\rangle$ — бесконечная циклическая группа. В этом случае все степени образующего элемента различны, т.е. $g^n \neq g^k$ при целых $n \neq k$. В самом деле, если найдутся такие целые числа n и $k < n$, что $g^n = g^k$, то $g^{n-k} = 1$. Записав произвольное целое число m в виде $m = \ell(n-k) + r$, где ℓ — целое число, а $r \in \{0, 1, \ldots, n-k-1\}$ получаем, что $g^m = g^r$, откуда $|\langle g\rangle| \leqslant n-k$.

Определим отображение f группы $\langle g\rangle$ в аддитивную группу $\mathbb{Z}$ целых чисел следующим образом: $f(g^n) = n$. Ясно, что это отображение биективно, а из свойств степени вытекает, что $f(g^n g^m) = f(g^{n+m}) = n + m$. Следовательно, построенное отображение является изоморфизмом.

Пусть теперь $G_1 = \langle g_1\rangle = \{e_1, g_1, g_1^2, \ldots, g_1^{q-1}\}$, а $G_2 = \langle g_2\rangle = \{e_2, g_2, g_2^2, \ldots, g_2^{q-1}\}$ — циклические группы конечного порядка q. Определим отображение $f\colon G_1 \to G_2$ по формуле $f(g_1^n) = g_2^n$, при $n = 0, 1, \ldots, q-1$. Так как любое $n \in \mathbb{Z}$ можно записать в виде $n = kq + r$, где $k \in \mathbb{Z}$, а $r \in \{0, 1, \ldots, q-1\}$, то

$$f(g_1^n) = f(g_1^{kq+r}) = f((g_1^q)^k g_1^r) = f(g_1^r) = g_2^r = (g_2^q)^k g_2^r = g_2^{kq+r} = g_2^n.$$

Таким образом, отображение f корректно определено и, очевидно, взаимно однозначно.

Проверим теперь свойство сохранения операции умножения при отображении f. Пусть $n, m \in \mathbb{Z}$. Так как $m + n = kq + r$, где $k \in \mathbb{Z}$, а $r \in \{0, 1, \ldots, q-1\}$, то

$$f(g_1^n g_1^m) = f(g_1^{n+m}) = f(g_1^r) = g_2^r = g_2^{n+m} = g_2^n g_2^m = f(g_1^n) f(g_1^m).$$

Итак, отображение f — это изоморфизм групп $G_1 \cong G_2$. □

Пусть $n \in \mathbb{N}$. Напомним, что ранее нами была определена конечная аддитивная группа Z_n, состоящая из элементов $\{0, 1, \ldots, n-1\}$ с операцией $a \oplus_n b = (a+b) \pmod n$ сложения чисел по модулю n. Было показано, что эта группа имеет структуру циклической группы, а в качестве образующего элемента можно взять, например, 1.

С учетом только что доказанного предложения об изоморфности циклических групп одинакового порядка, мы можем (и будем) использовать обозначение Z_n для обозначения циклической группы порядка n (без учета специфики ее элементов и операции).

Автоморфизмы и внутренние автоморфизмы групп.

Определение. *Изоморфизм $f : G \to G$ некоторой группы G на себя называется автоморфизмом группы G. Совокупность всех автоморфизмов группы G обозначается символом* $\operatorname{Aut} G$.

Предложение. *Для произвольной группы G множество* $\operatorname{Aut} G$ *образует группу относительно операции композиции отображений. При этом группа* $\operatorname{Aut} G$ *является подгруппой группы $S(G)$ всех биективных отображений группы G в себя.*

Проверка. Первым делом проверим, что композиция двух автоморфизмов ϕ и ψ группы G снова будет автоморфизмом группы G. Так как ϕ и ψ — биективные отображения, то и отображение $\phi\circ\psi$ будет биективным. Далее, пусть a и b — произвольные элементы группы G. Тогда

$$(\phi\circ\psi)(ab)=\phi(\psi(ab))=\phi(\psi(a)\psi(b))=\phi(\psi(a))\phi(\psi(b))=(\phi\circ\psi)(a)(\phi\circ\psi)(b),$$

следовательно, отображение $\phi\circ\psi$ сохраняет операцию. Итак, множество $\operatorname{Aut}G$ замкнуто относительно операции композиции. Ясно, что $\mathrm{id}\in\operatorname{Aut}G$ и для любого отображения $\phi\in\operatorname{Aut}G$ обратное отображение $\phi^{-1}\in\operatorname{Aut}G$. Следовательно, $\operatorname{Aut}G$ — группа. □

Пусть G — некоторая группа, пусть элемент $a\in G$ и пусть отображение $f_a: G\to G$ определено по формуле $f_a(x)=axa^{-1}$, $x\in G$. Тогда f_a является автоморфизмом группы G. Для проверки этого факта нам необходимо проверить, что отображение f_a биективно и обладает свойством $f_a(xy)=f_a(x)f_a(y)$ для всех $x,y\in G$. В самом деле, если $x_1,x_2\in G$ таковы, что $f_a(x_1)=f_a(x_2)$, то $ax_1a^{-1}=ax_2a^{-1}$ и, следовательно, $a^{-1}(ax_1a^{-1})a=a^{-1}(ax_2a^{-1})a$, т.е. $x_1=x_2$. Далее, для любого $y\in G$ верно равенство $y=f_a(a^{-1}ya)$. Остается заметить, что $f_a(xy)=axya^{-1}=axa^{-1}aya^{-1}=f_a(x)f_a(y)$ для всех $x,y\in G$.

Определение. *Отображение f_a, определенное выше, называется внутренним автоморфизмом группы G.*

Предложение. *Совокупность* $\operatorname{Inn}G$ *всех внутренних автоморфизмов группы G образует подгруппу в группе* $\operatorname{Aut}G$ *всех автоморфизмов G.*

Проверка. Этот факт вытекает из следующих очевидных свойств, проверка которых оставляется в качестве *упражнения*: $\mathrm{id}=f_e$ (где e – единица группы G), $(f_a)^{-1}=f_{a^{-1}}$ и $f_a\circ f_b=f_{ab}$. □

Пример 2.3. Рассмотрим несколько примеров вычисления групп $\operatorname{Aut}G$. Пусть $G=\mathbb{Q}$ — аддитивная группа рациональных чисел и пусть f — произвольный автоморфизм группы G. По определению это означает, что отображение $f\colon\mathbb{Q}\to\mathbb{Q}$ взаимно однозначно и, кроме того,

$$f(r_1+r_2)=f(r_1)+f(r_2) \tag{2.1}$$

для всех $r_1,r_2\in\mathbb{Q}$.

Для определения вида отображения f воспользуемся сначала его алгебраическим свойством (2.1). Из этого свойства вытекает, что $f(2)=f(1+1)=f(1)+f(1)=2f(1)$ и, по индукции, что $f(n)=nf(1)$ для любого $n\in\mathbb{N}$. Далее, так как $f(r)=f(r+0)=f(r)+f(0)$ для любого $r\in\mathbb{Q}$, то $f(0)=0$. Отсюда легко получаем, что для любого $n\in\mathbb{N}$ верно равенство $0=f(0)=f(n+(-n))=f(n)+f(-n)$, т.е. $f(-n)=-f(n)=(-n)f(1)$. Следовательно, $f(n)=nf(1)$ для любого $n\in\mathbb{Z}$.

Далее заметим, что

$$f(1)=f\tfrac{1}{n}+\dots+\tfrac{1}{n}=nf\tfrac{1}{n}$$

для любого $n\in\mathbb{N}$ и, следовательно, $f(1/n)=(1/n)f(1)$. Как и раньше из этого вытекает, что $f(1/n)=(1/n)f(1)$ для любого $n\in\mathbb{Z}^*$.

Остается, наконец, заметить, что $f(m/n)=(m/n)f(1)$ для любых $m\in\mathbb{Z}$ и $n\in\mathbb{Z}^*$, т.е. $f(r)=rf(1)$ для любого $r\in\mathbb{Q}$. Обозначив $a=f(1)\in\mathbb{Q}$ получаем, что наше отображение f имеет вид $f(r)=ar$.

Проверим, при каких условиях это отображение будет взаимно однозначным. Легко видеть, что необходимым и достаточным условием здесь будет $a\neq0$ (в самом деле, из равенства $ar_1=ar_2$ в этом случае вытекает, что $r_1=r_2$ и для любого $q\in\mathbb{Q}$ справедливо представление $q=a(q/a)$, причем число q/a рационально).

Итак, любой автоморфизм группы $\mathbb{Q}$ имеет вид $f(r)=ar$ при некотором $a\in\mathbb{Q}^*$. Остается заметить, что если $f_1(r)=ar$ и $f_2(r)=br$ — два автоморфизма группы $\mathbb{Q}$, то их композиция имеем вид $f_1\circ f_2(r)=f_1(f_2(r))=abr$, т.е. композиции (произведению)

отображений f_1 и f_2 соответствует произведение ab соответствующих чисел $a, b \in \mathbb{Q}^*$. Следовательно, $\operatorname{Aut}\mathbb{Q} \cong \mathbb{Q}^*$, и это — изоморфизм групп.

Аналогичные рассуждения позволяют вычислить и группу $\operatorname{Aut}\mathbb{Z}$. В самом деле, из проведенных выше рассуждений непосредственно вытекает, что любой гомоморфизм $f : \mathbb{Z} \to \mathbb{Z}$ (т.е. отображение со свойством $f(n_1 + n_2) = f(n_1) + f(n_2)$ для любых $n_1, n_2 \in \mathbb{Z}$) имеет вид $f(n) = an$, где $a = f(1) \in \mathbb{Z}$. Но, так как отображение $f(n) = an$ будет биективным отображением только если $a = \pm 1$ (проверка необходимых деталей оставляется в качестве *упражнения*), то $\operatorname{Aut}\mathbb{Z} \cong \{-1, 1\}$ (или $\operatorname{Aut}\mathbb{Z} \cong Z_2$ — циклическая группа порядка 2).

Теорема Кэли. Пусть G и H — две произвольные группы и пусть $|G| \leqslant |H|$. Говорят, что группа G может быть *реализована* как подгруппа H, если найдется такая подгруппа $H_G \leq H$, что $G \cong H_G$.

Следующее утверждение является одним из фундаментальных утверждений в теории конечных групп. Оно утверждает, что все конечные группы могут быть реализованы как некоторые подгруппы группы перестановок S_n при подходящем (возможно весьма большом) значении n.

Теорема 2.4 (теорема Кэли)**.** *Любая конечная группа порядка n изоморфна некоторой подгруппе группы S_n.*

Доказательство. Пусть G — группа и пусть $|G| = n < \infty$. Заметим, что группа $S(G)$ всех биективных отображений G на себя изоморфна группе S_n.

Для любого элемента $a \in G$ определим отображение $f_a : G \to G$ по формуле $f_a(x) = ax$, $x \in G$. Если $G = \{g_1 = e, g_2, \ldots, g_n\}$, то множество $\{ag_1, \ldots, ag_n\}$ совпадает с множеством G, элементы которого, возможно, перечислены в каком-то другом порядке. В самом деле, если $ag_j = ag_k$ для некоторых $j \neq k$, то $a^{-1}ag_j = a^{-1}ag_k$ и, следовательно, $g_j = g_k$. Но это возможно только если $j = k$ так как $g_1 \neq g_2 \neq \cdots \neq g_n$ — все элементы множества G.

Таким образом, отображение f_a — это некоторое биективное отображение G в себя, т.е. f_a — может быть задано некоторой перестановкой на n элементах.

Из определения отображения f_a вытекает, что $f_a^{-1} = f_{a^{-1}}$ и что $\mathrm{id} = f_e$. Кроме того, если $a, b \in G$ — произвольные элементы, то $f_{ab}(x) = (ab)x = a(bx) = f_a(f_b(x))$, т.е. $f_{ab} = f_a \circ f_b$. Таким образом, множество $H := \{\mathrm{id} = f_e, f_{g_2}, \ldots, f_{g_n}\}$ образует подгруппу в группе $S(G) \cong S_n$. В силу сказанного выше, отображение $a \mapsto f_a$ обладает всеми свойствами изоморфизма $G \cong H$. □

Из теоремы Кэли вытекает, что совокупность $\{S_n : n \in \mathbb{N}\}$ является «хранилищем» всех конечных групп (рассматриваемых с точностью до изоморфизма).

Заметим, однако, что группы S_n даже при небольших значениях n имеют весьма большой порядок ($|S_n| = n!$). Так, $|S_6| = 720$, а $|S_8| = 40320$. Поэтому интересным и важным является вопрос, можно ли реализовать данную конечную группу G в виде подгруппы группы S_n при $n < |G|$. Например, группа D_3 порядка 6 реализуется как S_3. В то же самое время, группа кватернионов Q_8 имеет порядок 8 и теорема Кэли гарантирует ее реализацию в виде подгруппы группы S_8.

Задача 2.1. Доказать, что группа Q_8 не может быть реализована как подгруппа группу S_n при $n \leqslant 7$.

Гомоморфизмы групп. Важное значение в теории групп играют отображения, не являющиеся взаимно однозначными, но сохраняющие групповую структуру. Введем необходимые понятия.

Определение. *Отображение $f\colon G_1 \to G_2$ группы G_1 в группу G_2 называется гомоморфизмом, если $f(ab) = f(a)f(b)$ для любых элементов $a, b \in G_1$. Гомоморфизм $f\colon G \to G$ некоторой группы G в себя называется эндоморфизмом. Совокупность всех эндоморфизмов группы G обозначается символом* $\operatorname{End} G$.

Кроме того, сюръективный гомоморфизм называется эпиморфизмом, а инъективный гомоморфизм — мономорфизмом.

Легко проверяется, что $\operatorname{End} G$ является группой относительно операции композиции отображений.

Пример 2.5. Рассмотрим отображение $F\colon G \to \operatorname{Inn} G$ некоторой группы G в ее группу внутренних автоморфизмов, определенное по правилу $F(a) = f_a$, где $f_a(x) = axa^{-1}$. Это отображение тем свойством, что для любых элементов $a, b \in G$ имеет место равенство

$$F(ab) = f_{ab} = f_a \circ f_b = F(a) \circ F(b).$$

В самом деле, $f_{ab}(x) = abxb^{-1}a^{-1} = af_b(x)a^{-1} = f_a(f_b(x))$ для любых $a, b, x \in G$.

Таким образом отображение F является гомоморфизмом групп G и $\operatorname{Inn} G$. Однако это отображение не будет, в общем случае, изоморфизмом, так как оно не обязано быть биективным. Например, если группа G коммутативна, то группа $\operatorname{Inn} G$ тривиальна, т.е. $\operatorname{Inn} G = \{\mathrm{id}\}$.

Определение. *Пусть $f\colon G_1 \to G_2$ — гомоморфизм групп G_1 и G_2. Множество $\ker f = \{x \in G_1\colon f(x) = e_2\}$ называется ядром гомоморфизма f, а множество $\operatorname{Ran} f = \{f(x)\colon x \in G_1\}$ — образом f.*

Уточним, что символ e_2 в определении ядра гомоморфизма — это единица группы G_2.

В качестве простого *упражнения* предлагается проверить, что ядро $\ker f$ гомоморфизма $f\colon G_1 \to G_2$ является подгруппой группы G_1, а образ $\operatorname{Ran} f$ — является подгруппой группы G_2. Заметим, что если $\ker f = \{e_1\}$ (т.е., если ядро тривиально), то отображение $f\colon G_1 \to \operatorname{Ran} f$ будет изоморфизмом. Таким образом, $\ker f$ является в определенном смысле мерой неинъективности отображения f.

Пример 2.6. Приведем несколько полезных примеров гомоморфизмов групп. Пусть f — отображение аддитивной группы $\mathbb{R}$ вещественных чисел в группу $SO(2)$ вращений плоскости относительно начала координат, определенное соотношением $f(\alpha) = \Phi_\alpha$, где Φ_α — поворот на угол $2\pi\alpha$ в положительном направлении. Это отображение является гомоморфизмом (проверка необходимых деталей оставляется в качестве *упражнения*). При этом $\ker f = \{2\pi n :\ n \in \mathbb{Z}\}$. Можно также сказать, что рассматриваемое отображение f является гомоморфизмом $\mathbb{R}$ *на* окружность S^1.

Далее, отображение $A \mapsto \det A$, ставящее в соответствие матрице $A \in GL_n(\mathbb{R})$ ее (ненулевой) определитель является гомоморфизмом $GL_n(\mathbb{R})$ на мультипликативную группу $\mathbb{R}^\times$ ненулевых вещественных чисел.

Еще один пример уже, фактически, возникал при вычислении групп автоморфизмов $\operatorname{Aut}\mathbb{Q}$ и $\operatorname{Aut}\mathbb{Z}$. Так, отображения $f(r) = ar$, $a, r \in \mathbb{Q}$, и $g(n) = bn$, $b, n \in \mathbb{Z}$, причем a и b фиксированы, будут гомоморфизмами групп $\mathbb{Q}$ и $\mathbb{Z}$. При этом

$$\operatorname{Ran} f = \begin{cases} \{0\}, & \text{при } a = 0; \\ \mathbb{Q}, & \text{при } a \neq 0; \end{cases}$$

а $\ker f = \{0\}$ при $a \neq 0$ и, соответственно, $\operatorname{Ran} g = b\mathbb{Z}$, а $\ker g = \{0\}$ при $b \neq 0$.

В связи с рассмотренным выше понятием гомоморфизма групп полезно иметь в виду и следующий пример: отображение $f\colon \mathbb{Z} \to \langle g\rangle_m$ аддитивной группы целых чисел в циклическую группу $\langle g\rangle_m$ порядка m, определенное по формуле $f(n) = g^n$ является гомоморфизмом рассматриваемых групп. Его ядро равно $\ker f = \{km\colon k \in \mathbb{Z}\}$.

Пример 2.7. Пусть G — произвольная группа. Выберем некоторый элемент $a \in G$ и зафиксируем его. Определим на множестве G новую операцию $\diamond$ по правилу $x \diamond y = xay$. Проверка ассоциативности операции $\diamond$ оставляется в качестве *упражнения*. Таким образом, $G_\diamond = (G, \diamond)$ является полугруппой. Проверим, что элемент a^{-1} является

единицей в $G_\diamond$. В самом деле, $x \diamond a^{-1} = a^{-1} \diamond x = x$ для любого $x \in G$ по определению операции $\diamond$. Заметим теперь, что для любого $x \in G$ выполняются равенства

$$x \diamond (a^{-1}x^{-1}a^{-1}) = (a^{-1}x^{-1}a^{-1}) \diamond x = a^{-1}.$$

Из этого следует, что любой элемент $x \in G_\diamond$ обратим в $G_\diamond$ и обратный элемент $x_\diamond$ для элемента x в $G_\diamond$ равен $a^{-1}x^{-1}a^{-1}$. Следовательно, $G_\diamond$ является группой. Можно также проверить, что группы G и $G_\diamond$ изоморфны, причем изоморфизм устанавливается при помощи отображения $f : G \to G_\diamond$, определенного соотношением $f(x) = xa^{-1}$. Проверка свойств изоморфизма для f оставляется в качестве *упражнения.*

Упражнение. Определим матрицы $I, J, K \in M_2(\mathbb{C})$

$$J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Показать, что множество $\{\pm E, \pm J, \pm I, \pm K\}$ образует группу относительно операции матричного умножения и эта группа будет изоморфна группе Q_8.

2.2. Смежные классы по подгруппе

Заметим, что если $f \in \mathrm{Hom}(G, G_1)$ — некоторый гомоморфизм групп G и G_1, а $a \in G$ — произвольный элемент, то все элементы множества $a \ker f = \{ax \colon x \in \ker f\}$ отображаются при помощи f в один элемент $f(a) \in G_1$ (проверка этого простого факта оставляется в качестве *упражнения*). Обратно, если для некоторого элемента $g \in G$ верно равенство $f(g) = f(a)$, то $f(a^{-1}g) = f(a)^{-1}f(g) = 1$, т.е. $x = a^{-1}g \in \ker f$ и, окончательно, $g = ax \in a \ker f$.

Это наблюдение оправдывает введение следующего понятия.

Определение. *Пусть $H \leq G$ — подгруппа группы G и пусть $g \in G$ — некоторый фиксированный элемент. Множество $gH = \{gh \colon h \in H\}$ называется левым смежным классом группы G по подгруппе H, а элемент g называется представителем смежного класса gH.*

Аналогично определяется *правый смежный класс* $Hg = \{hg \colon h \in H\}$. При этом левые и правые смежные классы, определяемые одним представителем, в общем случае не совпадают, т.е. $gH \neq Hg$. Подгруппы H, для которых равенство $gH = Hg$ имеет место для любого элемента $g \in G$ выделяются в специальный важный класс *нормальных* подгрупп; это понятие подробно рассматривается ниже.

Заметим, что сама подгруппа $H \leq G$ является и левым и правым смежным классом, так как $H = 1H = H1$. Однако в общем случае смежный класс gH не является подгруппой в G. В самом деле, если gH является подгруппой, то $1 \in gH$ и, следовательно, существует такой $h \in H$, что $1 = gh$. Из этого уже вытекает, что $g = h^{-1}$ и $gH = h^{-1}H = H$.

Установим следующее важное свойства смежных классов.

Предложение 2.8. *Два левых смежных класса g_1H и g_2H группы G по ее подгруппе H или совпадают или не пересекаются. Отношение $\sim_H$ на G, определенное следующим образом: $a \sim_H b$, $a, b \in G$, если $a^{-1}b \in H$, является отношением эквивалентности.*

Замечание. Аналогичное утверждение верно и для правых смежных классов.

Доказательство. Пусть два смежных класса g_1H и g_2H имеют общий элемент a. Тогда найдутся такие $h_1 \in H$ и $h_2 \in H$, что $a = g_1h_1 = g_2h_2$. Следовательно, $g_2 = g_1h_1h_2^{-1}$ и любой элемент $g_2h \in g_2H$ имеет вид $g_2h = g_1h_1h_2^{-1}h = g_1h'$, где $h' = h_1h_2^{-1}h \in H$. Отсюда вытекает, что $g_2H \subset g_1H$. Аналогично проверяется, что имеет место включение $g_1H \subset g_2H$. Итак, из предположения о том, что два смежных класса g_1H и g_2H имеют нетривиальное пересечение, вытекает, что $g_1H = g_2H$.

Проверим, что отношение $\sim_H$ на G является отношением эквивалентности. В самом деле, $a^{-1}a = 1 \in H$ и, следовательно, $a \sim_H a$ для любого $a \in G$. Далее, пусть $a \sim_H b$. Тогда $h = a^{-1}b \in H$, откуда $H \ni h^{-1} = b^{-1}a$ и, следовательно, $b \sim_H a$. И, наконец, если $a \sim_H b$ и $b \sim_H c$, то $h_1 = a^{-1}b \in H$ и $h_2 = b^{-1}c \in H$. Из этого вытекает, что $a^{-1}c = h_1h_2 \in H$ и, окончательно, $a \sim_H c$. Таким образом, отношение $\sim_H$ на G рефлексивно, симметрично и транзитивно. □

Замечание. Так как любой элемент $g \in G$ принадлежит смежному классу gH и так как смежные классы или не пересекаются или совпадают, то G распадается в сумму непересекающихся левых смежных классов по подгруппе H. Это разбиение G и определяет отношение эквивалентности $\sim_H$.

Пример 2.9. Рассмотрим в качестве примера разложение группы S_3 в объединение смежных классов по подгруппе S_2. Заметим, что $S_2 = \langle(12)\rangle$. Непосредственным вычислением проверяем, что

$$S_3 = S_2 \sqcup (13)S_2 \sqcup (23)S_2 = \{\mathrm{id}, (12)\} \sqcup \{(13), (123)\} \sqcup \{(23), (132)\}$$

и, что

$$S_3 = S_2 \sqcup S_2(13) \sqcup S_2(23) = \{\mathrm{id}, (12)\} \sqcup \{(13), (132)\} \sqcup \{(23), (123)\}.$$

Заметим, что разложения на левые и правые смежные классы не совпадают.

Можно также заметить, что при любом натуральном $n > 2$ имеет место разложение

$$S_n = \bigsqcup_{k=0}^{n-1} \sigma_{n,k} S_{n-1},$$

где $\sigma_{n,0} = \mathrm{id}$ и $\sigma_{n,k} = (kn)$ (транспозиция, переводящая k в n) при $k = 1, \ldots, n-1$.

Итак, множества левых и правых смежных классов в общем случае не совпадают. Рассмотрим, однако, следующую конструкцию. Пусть x — элемент некоторого левого смежного класса gH, т.е. $x = gh$ для некоторого $h \in H$. Тогда $x^{-1} = (gh)^{-1} = h^{-1}g^{-1}$. При этом $h^{-1} \in H$ и, следовательно, $x^{-1} \in Hg^{-1}$. Проверим, что соответствие $x \mapsto x^{-1}$ устанавливает биективное соответствие между множествами $\{gH\}$ и $\{Hg\}$ левых и правых смежных классов. Пусть $h_1g_1^{-1} = h_2g_2^{-1}$, тогда $g_1 = g_2h_2^{-1}h_1$ и, следовательно, $g_1H = g_2H$.

Из сделанного наблюдения вытекает, что если $\{1, g_1, g_2, \ldots\}$ — множество представителей всех (различных) левых смежных классов группы G (по некоторой подгруппе $H \leq G$), то $\{1, g_1^{-1}, g_2^{-1}, \ldots\}$ — множество представителей всех соответствующих правых смежных классов. Мощности этих множеств совпадают.

Множества всех левых и правых смежных классов группы G по подгруппе H обозначается символами G/H (или $(G/H)_\ell$) и $(G/H)_r$ соответственно. Заметим, что $|G/H| = |(G/H)_r|$ так как между множествами левых и правых смежных классов имеется взаимнооднозначное соответственно.

Определение. *Величина $|G/H|$ называется индексом подгруппы H в G и обозначается специальным символом $(G : H)$.*

Заметим, что $|G| = (G : 1)$, т.е. порядок группы совпадает с индексом ее единичной подгруппы. Соответственно, порядок группы часто обозначают символами $(G : 1)$ или $(G : e)$.

В случае конечных групп справедлива следующая важная теорема

Теорема 2.10 (теорема Лагранжа)**.** *Пусть G — группа, $|G| < \infty$, и пусть $H \leq G$ — подгруппа в G. Тогда $|G| = (G : H)|H|$, т.е. порядок конечной группы делится на порядок любой подгруппы этой группы.*

Доказательство. Пусть g — произвольный элемент группы G. Проверим, что отображение $H \to gH$, определенное по правилу $h \mapsto gh$, $h \in H$ является биективным. В самом деле, умножив равенство $gh_1 = gh_2$ на g^{-1} слева получаем, что $h_1 = h_2$,

а тот факт, что любой элемент множества gH имеет вид gh для некоторого $h \in H$ очевиден. Следовательно, $|gH| = (H : 1)$. Из этого и из того факта, что каждая группа разлагается в объединение непересекающихся смежных классов, вытекает, что

$$(G : 1) = (G : H)(H : 1). \quad \square$$

Пусть $g \in G$ — произвольный элемент группы G. Так как $\operatorname{ord}_G g = |\langle g \rangle|$, а $\langle g \rangle \leq G$, то из теоремы Лагранжа вытекает, что $ord_G g$ делит порядок $|G|$ группы G.

Предложение 2.11. *Группа простого порядка p всегда циклическая и, с точностью до изоморфизма, единственная.*

Доказательство. Пусть $|G| = p$ — простое числе. Если H — некоторая нетривиальная подгруппа группы G, то $|H|$ делит $|G|$ и, следовательно, $|H| = p$. Таким образом, $G = H$. Отсюда вытекает, что G совпадает с циклической группой, порожденной любым отличным от единицы элементом $g \in G$. Единственность вытекает из того, что все циклические подгруппы одного порядка изоморфны. $\square$

Замечание. Интересно, что не для любого делителя m порядка $|G|$ группы G можно найти подгруппу $H \subset G$ такую, что $|H| = m$.

Упражнение. Показать, что в группе A_4 (для которой $|A_4| = 12$) нет подгрупп порядка 6.

2.3. Нормальные подгруппы, факторгруппы

Пусть G — некоторая произвольная группа. Среди всех подгрупп группы G естественно выделяется класс, состоящий из всех таких подгрупп $H \leq G$, что для любого элемента $g \in G$ смежные классы gH и Hg совпадают. Соответствующее определение удобно сформулировать в несколько других обозначениях. По аналогии со смежными классами для подгруппы $H \leq G$ и для элемента $g \in G$ определим множество $gHg^{-1} := \{ghg^{-1} \colon h \in H\}$.

Определение. *Подгруппа $H \leq G$ называется нормальной, если $gHg^{-1} = H$ для любого $g \in G$. Этот факт обозначается символом $H \lhd G$.*

В качестве простого *упражнения* предлагается проверить, что подгруппа $\langle (123) \rangle$ является нормальной подгруппой группы S_3, а подгруппа $\langle (12) \rangle$ — нет. Установим два простых достаточных условия, при выполнении которых подгруппа $H \leq G$ группы G является нормальной.

Предложение 2.12. *Пусть $H \leq G$ — такая подгруппа группы G, что $(G : H) = 2$. Тогда $H \lhd G$.*

Доказательство. Так как $(G : H) = 2$, то для любого элемента $g \in G \setminus H$ имеют место разложения $G = H \sqcup gH = H \sqcup Hg$. Следовательно, $gH = G \setminus H = Hg$ и, окончательно, $H = gHg^{-1}$. $\square$

Полученное условие нормальности допускает следующее простое обобщение:

Задача 2.2. Пусть p — минимальный простой делитель порядка $|G|$ конечной группы G. Тогда подгруппа H такая, что $(G : H) = p$ является нормальной.

Очень просто доказывается и следующее утверждение:

Предложение 2.13. *Пусть $f : G \to H$ — некоторый гомоморфизм групп G и H. Тогда* $\ker f$ *является нормальной подгруппой в G.*

Проверка. Для любых элементов $h \in \ker f$, $g \in G$ имеют место равенства

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)1_H f(g)^{-1} = 1_H,$$

где 1_H — это единица группы H. Т.е., если $x \in \ker f$, то $gxg^{-1} \in \ker f$ и, следовательно, $g(\ker f)g^{-1} \subset \ker f$ для любого $g \in G$. Аналогично проверяется, что если $x \in \ker f$ и $g \in G$ — произвольны, то $x' := g^{-1}hg \in \ker f$. Так как $x = gx'g^{-1}$, то $\ker f \subset g(\ker f)g^{-1}$ для любого $g \in G$. Окончательно получаем, что $\ker f = g(\ker f)g^{-1}$ для любого $g \in G$, что и требовалось. □

Упражнение. Проверить, что

$$V_4 \cong \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$$

и что $V_4 \lhd A_4$ (т.е. группа Клейна является нормальной подгруппы знакопеременной группы четвертого порядка).

Факторгруппы. Пусть G — некоторая группа, а $H \leq G$ — ее подгруппа. Рассмотрим некоторую множество G/H (левых) смежных классов G по H. Напомним, что G/H — это фактормножество множества G по отношению эквивалентности $\sim_H$, которое определяется на элементах $a, b \in G$ следующим образом: $a \sim_H b$ если $a^{-1}b \in H$.

Предположим теперь, что H — *нормальная* подгруппа G. Пусть элементы $a, b, c, d \in G$ таковы, что $a \sim_H c$, а $b \sim_H d$. Тогда

$$(ab)^{-1}cd = b^{-1}a^{-1}cd = b^{-1}(a^{-1}c)d = b^{-1}h_1 d = b^{-1}h_1 bb^{-1}d = b^{-1}h_1 bh_2 = h_3h_2 \in H,$$

где $h_1 = a^{-1}c \in H$, $h_2 = b^{-1}d \in H$ и $h_3 = b^{-1}h_1 b \in H$. Таким образом, при условии $H \lhd G$, из эквивалентности элементов $a \sim_H c$ и $b \sim_H d$ вытекает, что $ab \sim_H cd$. Следовательно, если H — нормальная подгруппа группы G, то операция умножения в G индуцирует операцию умножения смежных классов группы G по подгруппе H.

Для того, чтобы определить эту операция более аккуратно, нам потребуется понятие *произведения* подмножеств групп.

Определение. *Пусть G — группа, а $A \subset G$ и $B \subset G$ — некоторые подмножества G (не обязательно являющиеся подгруппами). Множество $AB = \{ab\colon a \in A,\ b \in B\}$ называется произведением множеств A и B.*

Используются также обозначения $A^2 := AA$ и $A^{-1} = \{a^{-1}\colon a \in A\}$.

Предложение 2.14. *Для любых трех подмножеств A, B и C группы G верно равенство $(AB)C = A(BC)$. Подмножество $H \subset G$ является подгруппой если и только если $H^2 = H$ и $H^{-1} \subset H$.*

Доказательство этих несложных утверждений оставляется в качестве задачи:

Задача 2.3. Доказать Предложение 2.14.

В качестве простого примера произведения подмножеств групп можно рассмотреть любой смежный класс gH, который равен $\{g\}H$.

Важно отметить, что *произведение смежных классов не обязано являться смежным классом*. В самом деле, произведение $(g_1H)(g_2H)$ состоит из элементов вида $g_1h_1g_2h_2$ при $h_1, h_2 \in H$ и почему множитель g_2 можно переставить с множителем h_1 (так, чтобы соответствующее произведение было равно g_3h_3 для некоторых $g_3 \in G$ и $h_3 \in H$) в общем случае неясно. В самом деле, имеет место, например, следующая ситуация.

Упражнение. Проверить, что если $H = \langle(12)\rangle \leq S_3$, то $(H)(\sigma H) = (\sigma H) \cup (\tau H)$ при $\sigma = (13)$, а $\tau = (23)$.

Однако, если H является нормальной подгруппой, то произведение h_1g_2 можно записать в виде g_2h_2' с некоторым $h_2' \in H$. Но в этом случае произведение смежных классов g_1H и g_2H в самом деле будет смежным классом g_1g_2H, как и утверждалось выше:

$$(g_1H)(g_2H) = g_1(Hg_2)H = g_1(g_2H)H = g_1g_2HH = g_1g_2H.$$

Более того, в этом случае будут выполнены следующие свойства операции умножения смежных классов: $H(aH) = (aH)H = aH$ и $(a^{-1})H(aH) = (aH)(a^{-1}H) = H$. Из всего сказанного вытекает следующий результат.

Теорема 2.15. *Если H – нормальная подгруппа некоторой группы G, то операция умножения смежных классов $(aH)(bH) = abH$ задает на множестве G/H структуру группы. Эта группа называется факторгруппой группы G по подгруппе H. Единицей в G/H служит смежный класс H, а элементом, обратным к смежному классу aH — смежный класс $a^{-1}H$.*

Для конечных групп G индекс $(G : H)$ в случае нормальной подгруппы H совпадает с порядком соответствующей факторгруппы G/H. При этом из теоремы Лагранжа вытекает, что $|G/H| = |G|/|H|$.

Пусть теперь $H \leq G$ — произвольная подгруппа. Заметим, что из выполнения условия $(g_1H)(g_2H) = g_1g_2H$ для всех элементов $g_1, g_2 \in G$ вытекает нормальность H в G. В самом деле, если для любых $g_1, g_2 \in H$ и для любых $h_1, h_2 \in H$ существует элемент $h_3 \in H$ такой, что $g_1h_1g_2h_2 = g_1g_2h_3$, то $g_2^{-1}h_1g_2 = h_3h_2^{-1} \in H$. Таким образом, множество G/H является группой относительно операции умножения смежных классов в том и только том случае, когда подгруппа $H \leq G$ является нормальной (т.е. $H \lhd G$).

Упражнение. Доказать, что любая факторгруппа циклической группы является циклической.

2.4. Простые группы

Последнее наблюдение, сделанное в предыдущем разделе оправдывает следующий вопрос о структуре данной группы G: как много в ней содержится нетривиальных (т.е. отличных от $\{1\}$ и самой G) нормальных подгрупп. Оказывается, что существуют группы, вообще не имеющие нетривиальных нормальных подгрупп.

Определение. *Группа называется простой, если она не имеет нетривиальных нормальных подгрупп.*

Коммутативная группа будет простой тогда и только тогда, когда она является циклической группой простого порядка (проверка этого простого факта оставляется в качестве *упражнения*). Более того, существуют неабелевы простые группы, как конечные, так и бесконечные. Например, имеет место следующее утверждение:

Теорема 2.16. *Для любого натурального $n \geqslant 5$ знакопеременная группа A_n является простой.*

Доказательство. В этом доказательстве строчные латинские буквы $a, b, c, \ldots, z$ обозначают числа из множества $\{1, \ldots, n\}$.

Проверим первым делом, что при любом натуральном $n \geqslant 3$ группа A_n совпадает с группой, порожденной всеми циклами длины 3. В самом деле, всякая четная перестановка является произведением четного числа транспозиций, а

$$(ab)(ac) = (acb) \qquad \text{и} \qquad (ab)(cd) = (adc)(abc).$$

Пусть теперь $n \geqslant 5$. Дальнейшее рассуждение разобьем на несколько шагов.

Шаг 1. Пусть H — произвольная нормальная подгруппа группы A_n. Если H содержит хотя бы один цикл длины 3, то $H = A_n$.

В самом деле, пусть $(abc) \in H$ — данный цикл длины 3, а (pqr) — некоторый другой цикл длины 3. Найдется такая *четная* перестановка α, что $(pqr) = \alpha(abc)\alpha^{-1}$ (проверка этого факта оставляется в качестве простого *упражнения*). Так как $H \lhd A_n$, то $(pqr) \in H$. Таким образом, вместе с любым циклом длины 3 подгруппа $H \lhd A_n$ содержит *все* циклы длины 3 и, следовательно, совпадает с A_n.

Шаг 2. Предположим теперь, что группа A_n не является простой. Тогда существует нетривиальная нормальная подгруппа H группы A_n. Рассмотрим возможные разложения элементов группы H в произведение независимых циклов.

Шаг 2, первый случай. Допустим, что существует такой элемент $\sigma \in H$, в разложении которого присутствует цикл длины большей или равной 4, т.е.

$$\sigma = (abcd\dots z)\tau,$$

где $\tau \in S_n$ — некоторая перестановка. Рассмотрим цикл $\alpha = (abc)$ длины 3. Так как $\alpha \in A_n$, а $H \lhd A_n$, то $\widetilde{\sigma} := \alpha\sigma\alpha^{-1} \in H$. Прямое вычисление показывает, что $\widetilde{\sigma} = (bcad\dots z)\tau$. Наконец, $\widetilde{\sigma}\sigma^{-1} \in H$, а

$$\widetilde{\sigma}\sigma^{-1} = (bcad\dots z)\tau\tau^{-1}(z\dots dcba) = (abd).$$

Таким образом, H содержит цикл (abd) длины 3 и, в силу результата, полученного на первом шаге доказательства, $H = A_n$.

Шаг 2, второй случай. Пусть теперь все циклы, входящие в разложение элемента $\sigma \in H$ имеют длину 2 или 3 и пусть в разложение элемента σ входит только один цикл длины 3 и некоторое количество циклов длины 2. В этом случае σ^2 будет просто циклом длины 3 и, так как $\sigma^2 \in H$, то $H = A_n$.

Шаг 2, третий случай. Предположим теперь, что все циклы, входящие в разложение элемента $\sigma \in H$ имеют длину 2 или 3, причем среди них имеется два цикла длины 3, т.е. пусть

$$\sigma = (abc)(pqr)\tau.$$

Рассмотрим цикл $\alpha = (cpq)$ длины 3 и перестановку $\widetilde{\sigma} := \alpha\sigma\alpha^{-1} = (abp)(crq)\tau \in H$. Тогда $\sigma\widetilde{\sigma} \in H$, но

$$\sigma\widetilde{\sigma} = (acpbq)\tau^2,$$

т.е. перестановка $\sigma\widetilde{\sigma}$ содержит цикл длины 5 и этот случай сводится к рассмотренному ранее.

Шаг 3. Из доказанного ранее вытекает, что любая перестановка $\sigma \in H$ (напомним, что H — это нормальная подгруппа группы A_n, отличная от $\{1\}$) может содержать только (четное число) циклов длины 2. Пусть $\sigma = (ab)(cd) \in H$. Тогда

$$(bx)(cd) = (abx)\sigma(abx)^{-1} \in H \qquad \text{и} \qquad \sigma(bx)(cd) = (abx) \in H.$$

Таким образом, и в этом случае H содержит цикл длины 3. И, наконец, если $\sigma = (ab)(cd)(pq)(rs) \in H$ и $\alpha = (dp)(bc)$, то $\widetilde{\sigma} := \alpha\sigma\alpha^{-1} = (ac)(bp)(dq)(rs) \in H$, откуда $\sigma\widetilde{\sigma} = (adp)(bqc)$ и мы снова пришли к ранее рассмотренному случаю. □

Заметим, что группа A_3 является циклической группой порядка 3 и, следовательно, простой. Однако, группа A_4 содержит нетривиальную нормальную собственную подгруппу (это группа Клейна V_4, см. выше). Таким образом, условие $n \geqslant 5$ в Теореме 2.16 является существенным.

Теорема 2.16 показывает, что существует бесконечно много простых неабелевых конечных групп. Такие группы, впрочем, далеко не исчерпываются знакопеременными, однако рассмотрение других примеров выходит за рамки данного курса.

Задача 2.4. Доказать, что группа $SO(3)$ — простая.

2.5. Произведение групп

Нам потребуется понятие произведения групп, которое является очень полезным и важным при изучении строения различных групп. Итак, пусть G и H — две произвольные группы. Рассмотрим множество $G \times H$ состоящее из всех упорядоченных пар (g, h), где $g \in G$, а $h \in H$. Определим операцию умножения пар из $G \times H$ следующим образом:

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2), \tag{2.2}$$

где g_1g_2 — произведение в G, а h_1h_2 — произведение в H. Легко видеть, что введенная операция произведения пар является *ассоциативной*, что элемента $(1_G, 1_H)$ является единичным элементом относительно введенной произведения и, что элемент (g^{-1}, h^{-1})

является обратным элементом к паре (g, h). Таким образом, множество $G \times H$ оказывается наделенным структурой группы.

Определение. *Прямым произведением $G \times H$ групп G и H называется множество $G \times H = \{(g, h) \colon g \in G,\ h \in H\}$ с операцией (2.2).*

Заметим, что группа $G \times H$ имеет подгруппы $G \times 1 = \{(g, 1_H) \colon g \in G\}$ и $1 \times H = \{(1_G, h) \colon h \in H\}$, которые изоморфны группам G и H соответственно.

Далее, отображение $\psi : G \times H \to H \times G$, определенное по правилу $\psi((g, h)) = (h, g)$, при $g \in G$ и $h \in H$, является *изоморфизмом* групп $G \times H$ и $H \times G$ (проверка необходимых свойств отображения ψ оставляется в качестве *упражнения*). Таким образом, операция взятия внешнего прямого произведения групп коммутативна (разумеется, с точностью до изоморфизма).

Аналогично можно убедится (проверка необходимых деталей оставляется в качестве *упражнения*), что для трех данных групп G, H и K можно определить прямые произведения $G \times (H \times K)$ и $(G \times H) \times K$, причем $G \times (H \times K) \cong (G \times H) \times K$.

И, наконец, свойства коммутативности и ассоциативности операции внешнего прямого произведения (рассматриваемые, естественно, с точностью до изоморфизма) позволяют определить прямое произведение любого конечного числа групп $\prod_{k=1}^{n} G_k$ не определяя явно, в каком порядке должны браться попарные прямые произведения.

Имеет место следующее важное свойство:

Теорема 2.17. *Пусть G — группа, а $H \lhd G$ и $K \lhd G$ — ее нормальные подгруппы. Если $H \cap K = \{1\}$ и $HK = G$, то $G \cong H \times K$.*

Доказательство. Так как $G = HK$, то для любого элемента $g \in G$ существуют такие элементы $h \in H$ и $k \in K$, что $g = hk$. Проверим, что в условиях теоремы такое представление единственно для любого $g \in G$. Пусть $g = h_k b_1 = h_2 k_2$, где $h_1, h_2 \in A$, а $k_1, k_2 \in B$. Из равенства $h_1 k_1 = h_2 k_2$ вытекает, что $h_2^{-1} h_1 = k_2 k_1^{-1}$ и, следовательно, $h_2^{-1} h_1 \in K$, а $k_2 k_1^{-1} \in H$. А так как $H \cap K = \{1\}$, то $h_2^{-1} h_1 = 1$ и $k_2 k_1^{-1} = 1$. Таким образом, $h_1 = h_2$ и $k_1 = k_2$.

Пусть теперь g — произвольный элемент группы G. По доказанному выше существуют единственные элементы $h \in H$ и $k \in K$ такие, что $g = hk$. Вычислим теперь коммутатор $[h, k]$. Так как $H \lhd G$ — нормальная подгруппа группы G, то

$$[h, k] = hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) = hh' \in H,$$

а так как $K \lhd G$ тоже нормальная подгруппа группы G, то

$$[h, k] = hkh{-}1k^{-1} = (hkh^{-1})k^{-1} = k'k^{-1} \in K.$$

Так как $H \cap K = \{1\}$, то $[h, k] = 1$ и, окончательно, мы получаем, что $hk = kh$.

Рассмотрим теперь отображение $f : G \to H \times K$, определенное следующим образом: $f(g) = (h, k)$ для любого $g \in G$, $g = hk$, $h \in H$, $k \in K$. Так как $f(g_1 g_2) = f(h_1 k_1 h_2 k_2) = f(h_1 h_2 k_1 k_2) = (h_1 h_2, k_1 k_2) = (h_1, k_1)(h_2, k_2) = f(h_1 k_1) f(h_2 k_2) = f(g_1) f(g_2)$, то f является гомоморфизмом.

Ясно, что единицей в группе $H \times K$ является элемент $(1, 1)$. Пусть $g \in G$, $g = hk$ при $h \in H$ и $k \in K$, и пусть $f(g) = (1, 1)$. Тогда $h = 1$ и $k = 1$ и, следовательно, $g = 1$. Таким образом, $\ker f = \{1\}$, т.е. f — это мономорфизм. То, что f является эпиморфизмом очевидно. Таким образом, f — изоморфизм G на $H \times K$. □

Проверим еще один интересный и важный факт, связанный с только что доказанным утверждением.

Предложение 2.18. *Пусть G и H — произвольные группы. Тогда $G \times 1_H \lhd G \times H$ и $1_G \times H \lhd G \times H$ (т.е. подгруппы $G \times 1_H$ и $1_G \times H$ являются нормальными подгруппами в $G \times H$).*

Доказательство. В самом деле, если $g, x \in G$, а $h, y \in H$, то $(g,h)(x,1_H)(g^{-1},h^{-1}) = (gxg^{-1}, hh^{-1}) = (gxg^{-1}, 1_H) \in G \times 1_H$, а $(g,h)(1_G,y)(g^{-1},h^{-1}) = (1_G, hyh^{-1}) \in 1_G \times H$. □

Если группа G представима в виде $G = HK$, где H и K — ее нормальные подгруппы (как в Теореме 2.17), то говорят, что G является *внутренним прямым произведением* H и K. Разница между прямым произведением (его иногда называют еще *внешним прямым произведением* и внутренним прямым произведением состоит в том, что в случае внутреннего произведения перемножаются сами подгруппы H и K, а не изоморфные им подгруппы $H \times 1$ и $1 \times K$.

Из Предложения 2.18 вытекает, что если некоторая группа G является прямым произведением своих подгрупп H_1 и H_2, т.е., если $G = H_1 \times H_2$, то $H_1 \lhd G$ и $H_2 \lhd G$ (это следует из того, что группы H_1 и H_2 изоморфны *нормальным* подгруппам своего прямого произведения). Аналогичное свойство верно и для прямого произведения большего числа сомножителей.

Заметим, что разница между обычным и внутренним прямыми произведениями довольно условна и, не опасаясь неоднозначности, можно в обоих случаях использовать термин *прямое произведение*.

2.6. Описание групп малых порядков

В завершении этого раздела мы изучим структуру групп малых порядков (до порядка 8 включительно) и приведем из полное описание. Первым делом установим два следующих простых факта.

Предложение. *Пусть G — такая группа, что $\operatorname{ord}_G g = 2$ для любого элемента $g \in G \setminus \{1\}$. Тогда группа G является коммутативной.*

Проверка. В самом деле, так как для любого элемента $g \in G$, $g \neq 1$, верно равенство $g^2 = 1$, то $gh = (gh)^{-1} = h^{-1}g^{-1} = h^2h^{-1}g^{-1}g^2 = hg$ для любых $g, h \in G$. □

Числа $2, 3, 5, 7$ являются простыми, поэтому группы порядка $2, 3, 5, 7$ изоморфны циклическим группам Z_2, Z_3, Z_5 и Z_7 соответственно (см. Предложение 2.11).

Структура групп порядка 4. Пусть G — группа порядка 4. Возможны два случая. Во-первых, в группе G может быть элемент порядка 4. В этом случае, очевидно, группа G изоморфна циклической группе Z_4 соответствующего порядка.

Пусть теперь в группе G четвертого порядка нет элементов четвертого порядка. Это означает, что все отличные от единицы элементы группы G имеют порядок 2. Как было показано выше, это означает, что группа G является коммутативной.

Пусть $G = \{1, a, b, c\}$ — коммутативная группа и $a^2 = b^2 = c^2 = 1$. Найдем, чему равно ab. Если $ab = 1$, то $a = b^{-1} = b$ так как $b^2 = 1$, что невозможно так как элементы a и b различны. Далее, если $ab = a$, то $b = 1$, а если $ab = b$, то $a = 1$, что также невозможно. Остается только одна возможность $ab = c$. Циклические подгруппы $\langle a \rangle$ и $\langle b \rangle$ нормальны в G (так как G коммутативна, то все подгруппы в ней нормальные). Заметим также, что $\langle a \rangle \cap \langle b \rangle = \{1\}$ и $\langle a \rangle \langle b \rangle = \{1, a, b, ab\} = G$. В силу Теоремы 2.17 $G \cong \langle a \rangle \times \langle b \rangle \cong Z_2 \times Z_2$.

Итак, существуют только две (с точностью до изоморфизма) группы порядка 4: циклическая группа Z_4 и группа $Z_2 \times Z_2$. Заметим также, что группа Клейна V_4, введенная выше, изоморфна группе $Z_2 \times Z_2$, что видно, например, из рассмотрения таблиц Кэли для этих групп.

Устройство группы порядка 6. В случае группы G порядка 6 целесообразно отдельно рассмотреть коммутативный и некоммутативный случаи. Если группа G порядка 6 является коммутативной, то она изоморфна циклической группе Z_6 порядка 6, которую можно эквивалентно реализовать как прямое произведение $Z_2 \times Z_3$. Проверка этого факта может быть сделана непосредственно (это оставляется в качестве *задачи*

для самостоятельного решения). Мы же сошлемся на теорему о строении конечных абелевых групп, которая будет изучена позже.

Пусть теперь G — некоммутативная группа порядка 6. Тогда все отличные от единицы элементы группы G могут иметь порядки 2, 3 и 6. Если все отличные от единицы элементы группы G имеют порядок 2, то такая группа будет коммутативна, что невозможно в силу сделанного предположения. Таким образом, в группе G есть элемент a порядка 3.

Пусть $H := \langle a \rangle$. Тогда $(G : H) = 2$ и $G = H \sqcup bH$, где $b \in G \setminus H$. Так как $H \lhd G$ — нормальная подгруппа (ее индекс равен двум), то $b^{-1}ab \in H$. Легко проверить, что $b^{-1}ab \neq 1$. Следовательно, остаются ровно две возможности: $b^{-1}ab = a$ и $b^{-1}ab = a^2$. Первое из этих равенств означает, что $ab = ba$, т.е., что группа G является коммутативной.

Итак, $b^{-1}ab = a^2 = a^{-1}$, откуда $ab = ba^{-1}$ и умножение в группе G работает следующим образом:

$$a^k a^m = a^{k+m} \in H, \quad ba^k a^m = ba^{k+m} \in bH, \quad a^k ba^m = ba^{m-k} \in bH, \quad ba^k ba^m = b^2 a^{m-k}.$$

Снова вспоминая, что $(G : H) = 2$ заключаем, что $b^2 \in H$. Таким образом возникают три возможности: $b^2 = 1$, $b^2 = a$ и $b^2 = a^2$. Пусть $b^2 = a$. Тогда $ab = b^3 = ba$ и, следовательно, группа G является коммутативной. Аналогично, из равенства $b^2 = a^2$ вытекает, что $b^4 = a^4 = a$, откуда $ab = b^5 = ba$. Итак, в случае некоммутативной группы G реализуется единственная возможность $b^2 = 1$.

Окончательно делаем вывод, что в некоммутативной группе порядка 6 можно задать единственную таблицу умножения. Из этого факта вытекает, что существует ровно одна (с точностью до изоморфизма) некоммутативная группа порядка 6. Легко привести пример такой группы — это группа S_3 (или изоморфная ей группа D_3).

Задача 2.5.

(1) Пусть p — простое число, а G — некоммутативная группа порядка $|G| = 2p$. Доказать, что если в G содержится элемент порядка 2, то $G \cong D_p$.
(2) Если группа G некоммутативна и $|G| = 8$, то $G \cong D_4$ или $G \cong Q_8$.
(3) Если $|G| = 10$, то $G \cong Z_{10}$ или $G \cong D_5$.

В дальнейшем мы разберем два более сложных примера — мы изучим строение групп порядка 12 и 15. Однако для этого нам потребуются теоремы Силова (см. ниже).

РАЗДЕЛ 3

Основные понятия теории групп — теоретико-групповые конструкции

3.1. Теоремы о гомоморфизмах групп

В этом разделе мы установим ряд общих фактов о подгруппах, гомоморфизмах и факторгруппах, широко применяющихся в различных разделах математики.

Теорема 3.1 (основная теорема о гомоморфизме групп)**.** *Пусть G и H — группы, а $\varphi\colon G \to H$ — гомоморфизм. Тогда $\ker\varphi \lhd G$ и $G/\ker\varphi \cong \operatorname{Ran}\varphi$. Кроме того, если $K \lhd G$ — нормальная подгруппа, то существуют такие группа H и эпиморфизм $\pi\colon G \to H$, что $\ker\pi = K$.*

Доказательство. Тот факт, что $K := \ker\varphi \lhd G$ был проверен раньше (см. Предложение 2.13). Следовательно, G/K — группа. Определим отображение $f\colon G/K \to H$ по правилу $f(gK) = \varphi(g)$.

Проверим, что такое определение отображения f корректно в том смысле, что $f(gK)$ не зависит от выбора конкретного представителя смежного класса gK. В самом деле, если $g_1K = g_2K$, $g_1, g_2 \in G$, то $g_1^{-1}g_2 \in K$ и, следовательно, $\varphi(g_1^{-1}g_2) = 1$, т.е. $\varphi(g_1) = \varphi(g_2)$.

Проверим теперь, что f является гомоморфизмом. Это вытекает из следующей цепочки равенств (в которой учтено, что $K = \ker\varphi$ – нормальная подгруппа):

$$f((g_1K)(g_2K)) = f(g_1g_2K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = f(g_1K)f(g_2K),$$

для любых $g_1, g_2 \in G$. Пусть теперь $g_1 \in G$ и $g_2 \in G$ таковы, что $f(g_1K) = f(g_2K)$. Тогда $\varphi(g_1) = \varphi(g_2)$ и, следовательно, $\varphi(g_1^{-1}g_2) = 1$ и $g_1^{-1}g_2 \in K$, откуда $g_1K = g_2K$. Таким образом установлено, что f — мономорфизм. Остается заметить, что $\operatorname{Ran} f = \operatorname{Ran}\varphi$.

Обратно, если $K \lhd G$ — некоторая нормальная подгруппа, то отображение $\pi\colon g \mapsto gK$, $g \in G$, удовлетворяет всем требуемым условиям. Проверка необходимых деталей оставляется в качестве *упражнения.* □

Замечание. В связи с только что установленной теоремой целесообразно отметить, что заданием ядра гомоморфизм определяется неоднозначно. Так, если G — абелева группа простого порядка $p > 2$, то автоморфизмы $g \mapsto g$ и $g \mapsto g^{-1}$ этой группы различны, но оба имеют тривиальные (т.е. равные $\{1\}$) ядра.

Теорема 3.2. *Пусть G — группа, $H \leq G$ — ее произвольная, а $K \lhd G$ — нормальная подгруппы. Тогда*

(1) $HK = KH$ — подгруппа в G (содержащая K);

(2) $H \cap K$ — нормальная подгруппа в G;

(3) Факторгруппы HK/K и $H/(H\cap K)$ изоморфны, а отображение $f\colon hK \mapsto h(H\cap K)$ является изоморфизмом этих групп.

Доказательство. Так как $K \lhd G$, то $gK = Kg$ для любого $g \in G$ и, следовательно, $hK = Kh$ для любого $h \in H \subset G$. Далее

$$HK = \{hk:\ h \in H, k \in K\} = \bigcup_{h\in H} hK = \bigcup_{h\in H} Kh = \{kh:\ h \in H, k \in K\} = KH.$$

Так как $1 \in K$ и $1 \in H$, то $1 \in KH$. Записав элемент $x \in HK$ в виде $x = hk$, $h \in H$, $k \in K$, получим, что $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1})$ и, так как $hk^{-1}h^{-1} \in K$

(так как K – нормальная подгруппа), то $x^{-1} = h^{-1}k_1$, где $h^{-1} \in H$ и $k_1 \in K$, т.е. $x^{-1} \in HK$. Остается заметить, что

$$(HK)(HK) = HKHK = H(KH)K = H(HK)K = H^2K^2 = HK.$$

Итак, $HK = KH$ подгруппа в G и первое утверждение теоремы доказано.

Так как $K \lhd G$ – нормальная подгруппа, то определена факторгруппа G/K. Рассмотрим естественный эпиморфизм $\pi\colon G \to G/K$ и его сужение π_H на H. Так как $K \lhd HK$, то определена факторгруппа HK/K. По определению π_H получаем, что $\operatorname{Ran}\pi_H = \{hK\colon h \in H\} = HK/K$. Итак, отображение $\pi_H\colon H \to HK/K$ является эпиморфизмом. Найдем его ядро: $\ker\pi_H = \{h \in H\colon \pi_H(h) = hK = K\}$ так как K — единица в HK/K. Заметим, что $hK = K$ при $h \in H$ если и только если $h \in K$, т.е. $\ker\pi_H = H \cap K$. Из этого вытекает, что $H \cap K$ — нормальная подгруппа (как ядро гомоморфизма).

Рассмотрим теперь факторгруппу $H/(H \cap K)$ В силу основной теоремы о гомоморфизмах групп, отображение $\overline{\pi}_H\colon H/(H \cap K) \to HK/K$, определенное следующим образом $\overline{\pi}_H\colon h(H \cap K) \mapsto \pi_H(h) = hK$ является изоморфизмом $H/(H \cap K) \cong HK/K$. Для завершения доказательства теоремы остается заметить, что $f = \overline{\pi}_H^{-1}$. □

Установим еще один результат, который будет весьма полезен при анализе конкретных примеров. Для произвольной группы G обозначим через $\Sigma^*(G)$ совокупность всех ее подгрупп, а через $\Sigma^*(G, K)$, где K — некоторая подгруппа в G, совокупность всех подгрупп $H \leq G$ таких, что $K \leq H$.

Теорема 3.3 (теорема о соответствии)**.** *Пусть G — группа, $K \lhd G$ — ее нормальная подгруппа и пусть $\overline{G} = G/K$. Тогда*

(1) Отображение $\pi^*\colon H \mapsto \overline{H}$, где $\overline{H} = H/K$ является биективным отображением множества $\Sigma^*(G, K)$ на множество $\Sigma^*(\overline{G})$.

(2) Если $H \in \Sigma^*(G, K)$, то $H \lhd G$ если и только если $\overline{H} \lhd \overline{G}$. В этом случае

$$G/H \cong \overline{G}/\overline{H} = (G/K)/(H/K).$$

Доказательство. Пусть $H \in \Sigma^*(G, K)$, т.е. $K \leq H \leq G$. Из определения G/K вытекает, что $\overline{H} = H/K$ — это подгруппа в $\overline{G} = G/K$. Рассмотрим отображение $\pi^*\colon H \mapsto \overline{H}$. Проверим инъективность отображения π^*. Пусть $H_1 \in \Sigma^*(G, K)$ и $H_2 \in \Sigma^*(G, K)$ таковы, что $H_1/K = H_2/K$. Из этого равенства вытекает, что для любого $h_1 \in H_1$ смежный класс $h_1K \in H_2/K$, т.е. найдется такой элемент $h_2 \in H_2$, что $h_1K = h_2K$. А это, в свою очередь, означает, что $h_1 = h_2k$ при некотором $k \in H_2$. А так как $K \subset H_2$, то $h_1 = h_2k \in H_2$. То есть $H_1 \subset H_2$. Аналогично проверяется, что $H_2 \subset H_1$. Таким образом из равенства $H_1/K = H_2/K$ вытекает, что $H_1 = H_2$ и, следовательно, π^* инъективно.

Следующий шаг доказательства – проверка сюръективности отображения π^*. Пусть $\overline{H} \in \Sigma^*(\overline{G})$. Рассмотрим множество H, состоящее из тех элементов группы G, которые принадлежат хотя бы одному смежному классу xK, принадлежащему $\overline{H}$. Нам необходимо проверить, что H — подгруппа в G и $K \leq H$.

Из определения множества H непосредственно вытекает, что $K \subset H$. Пусть теперь $a \in H$ и $b \in H$. Тогда $aK \in \overline{H}$ и $bK \in \overline{H}$. Так как K – нормальная подгруппа, то $abK = aK \cdot bK \in \overline{H}$ и, следовательно, $ab \in H$. Аналогично, $a^{-1}K = (aK)^{-1} \in \overline{H}$, откуда $a^{-1} \in H$. Таким образом, H – подгруппа в G. Кроме того, $\overline{H} = H/K$ (это прямо вытекает из определения H). Следовательно, отображение π^* сюръективно (H является прообразом $\overline{H}$ при отображении π^*).

Пусть теперь $H \in \Sigma^*(G, K)$ такова, что $H \lhd G$. Тогда для любых $g \in G$ и $h \in H$ получаем

$$(gK) \cdot (hK) \cdot (gK)^{-1} = ghg^{-1}K = h_1K \in \overline{H},$$

откуда следует, что $\overline{H} \lhd \overline{G}$. Обратное утверждение проверяется аналогично: если $\overline{H} \lhd \overline{G}$, то для любых $g \in G$ и $h \in H$ имеют место равенства

$$ghg^{-1}K = (gK) \cdot (hK) \cdot (gK)^{-1} \in \overline{H},$$

т.е. $ghg^{-1} \in H$ и, окончательно, $H \lhd G$.

Установим теперь последнее утверждение теоремы. Пусть $H \lhd G$ и, соответственно, $\overline{H} \lhd \overline{G}$. Рассмотрим естественные гомоморфизмы $\pi\colon G \to G/K$ и $\overline{\pi}\colon \overline{G} \mapsto \overline{H}$, определенные соотношениями $\pi\colon g \to gK$ и $\overline{\pi}\colon \overline{g} \mapsto \overline{g}\overline{H}$, где $\overline{g} = gK$ при $g \in G$. Определим отображение $\psi = \overline{\pi} \circ \pi$, т.е. $\psi(g) = \overline{g}\overline{H}$ при $g \in G$. Заметим, что ψ — эпиморфизм G на $\overline{G}/\overline{H}$. Вычислим $\ker\psi$:

$$\ker\psi = \{g \in G :\ \psi(g) = \overline{H}\} = \{g \in G :\ \overline{g} \in \overline{H}\} = \{g \in G :\ \exists\, h \in H :\ gK = hK\} = H.$$

Остается применить основную теорему о гомоморфизмах групп и убедится, что отображение $gH \mapsto \overline{g}\overline{H}$, $g \in G$, задает изоморфизм $G/H \cong \overline{G}/\overline{H}$. □

Рассмотрим теперь несколько примеров применения только что доказанных утверждений.

Пример 3.4. Пусть $n, m, d \in \mathbb{N}$ таковы, что $n = dm$, а $d > 1$. При этом $n\mathbb{Z} \subset d\mathbb{Z}$. Рассмотрим отображение $\chi\colon x \mapsto dx + n\mathbb{Z}$. В качестве несложного *упражнения* предлагается проверить, что χ является эпиморфизмом аддитивных групп $\mathbb{Z} \to (d\mathbb{Z})/(n\mathbb{Z})$, причем $(d\mathbb{Z})/(n\mathbb{Z}) = \{dk + n\mathbb{Z} :\ \ k = 0, 1, \ldots, m-1\}$. Как нетрудно проверить, $\ker\chi = m\mathbb{Z}$. Применяя теорему 3.1 (основную теорему о гомоморфизмах) получаем, что $Z_m = \mathbb{Z}/m\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z}$. Далее, из теоремы 3.3 (о соответствии) вытекает, что $Z_d = \mathbb{Z}/d\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z}) = Z_n/Z_m$, т.е. $Z_d \cong Z_n/Z_m$.

Пример 3.5. Рассмотрим группу S_4 и две ее подгруппы S_3 и V_4 (группа Клейна, см. выше). В качестве *упражнения* проверить, что $V_4 \lhd S_4$. Так как $S_3 \cap V_4 = \{\mathrm{id}\}$, то, применяя теорему 3.2, получаем, что для подгруппы $H = S_3V_4 \subset S_4$ справедливы следующие соотношения

$$H/V_4 \cong S_3/(S_3 \cap V_4) \cong S_3.$$

По теореме Лагранжа, $|H| = |V_4||S_3| = 24$. Следовательно, $H = S_4$. Таким образом, группа S_4 обладает подгруппой, изоморфной группе S_3 и факторгруппой, также изоморфной группе S_3.

Вычислим теперь множество $\Sigma^*(S_4, V_4)$. Так как

$$S_3 = \{\mathrm{id}, (12), (23), (13), (123), (132)\},$$

то, применяя Теорему 3.3, получаем, что

$$\Sigma^*(S_4, V_4) = \{V_4, \langle(12)\rangle V_4, \langle(23)\rangle V_4, \langle(13)\rangle V_4, \langle(123)\rangle V_4, S_4\}$$

причем $\langle(123)\rangle V_4 = A_4$.

Упражнение. Проверить, что группа S_4 содержит ровно две собственные (т.е. не равные $\{1\}$ и S_4) нормальные подгруппы: A_4 и V_4.

Литература

[1] Кострикин А. И. Введение в алгебру. Часть I. Основы алгебры. М.: Физматлит, 2004. 272 с.

[2] Кострикин А. И. Введение в алгебру. Часть 3. Основные структуры. М.: Физматлит, 2004. 272 с.

[3] Сборник задач по алгебре/Под ред. А. И. Кострикина. М.: Физматлит, 2001. 464 с.

[4] ван дер Варден Б. Л. Алгебра. М.: Наука, 1979. 624 с.

[5] Курош А. Г. Лекции по общей алгебре. М.: Наука, 1973. 400с.

[6] Курош А. Г. Теория групп. М.: Наука, 1967. 648с.

[7] Ленг С. Алгебра. М.: Наука, 1965. 431с.

[8] Артамонов В. А., Словохотов Ю. Л. Группы и их приложения в физике, химии , кристаллографии. М.: Издательский центр «Академия», 2005. 512 с.

[9] Овсянников Л. В. Групповой анализ дифференциальных уравнений. М.: Наука, 1978. 400 с.