Московский государственный технический университет
имени Н. Э. Баумана

Факультет «Фундаментальные науки»
Кафедра «Прикладная математика»

К. Ю. Федоровский

АЛГЕБРА
Введение в теорию групп

Электронное учебное издание

Курс лекций по дисциплине «Алгебра»

Москва

УДК 512.54

Рецензенты:
Канатников Анатолий Николаевич, к.ф.-м.н., доц.,
Яворская Татьяна Леонидовна, к.ф.-м.н., доц.

Федоровский Константин Юрьевич

Алгебра. Введение в теорию групп. Курс лекций по дисциплине «Алгебра»

Издание представляет собой конспект лекций по курсу «Алгебра», который читается студентам факультета ФН на втором и третьем семестрах обучения, и охватывает весь материал этого курса для третьего семестра по теории групп.

Пособие предназначено для студентов 2-го курса, обучающихся по специальностям «Прикладная математика» и «Теоретическая физика».

Рекомендовано Учебно-методической комиссией НУК «Фундаментальные науки» МГТУ им. Н. Э. Баумана.

Федоровский Константин Юрьевич

АЛГЕБРА

Введение в теорию групп

Оглавление

Раздел 1. Алгебраические структуры. Полугруппы и группы 4
1.1. Ассоциативные и коммутативные операции, понятие полугруппы 5
1.2. Обобщенная ассоциативность, степени и кратные 8
1.3. Обратимость элементов в полугруппах с единицей 10
1.4. Понятие группы 11
1.5. Примеры групп. Основные матричные группы 12
1.6. Симметрическая и знакопеременная группы 13

Раздел 2. Введение в теорию групп 17
2.1. Изоморфизмы групп, теорема Кэли 17
2.2. Гомоморфизмы, автоморфизмы и внутренние автоморфизмы групп 18
2.3. Циклические группы, порядок элементов 21
2.4. Нормальные подгруппы 23
2.5. Системы образующих и определяющие соотношения в группах 24
2.6. Произведение групп 27

Раздел 3. Основные теоретико-групповые конструкции 29
3.1. Смежные классы по подгруппе 29
3.2. Факторгруппы 31
3.3. Описание групп малых порядков 32
3.4. Теоремы о гомоморфизмах групп 33
3.5. Коммутант 35
3.6. Разрешимые группы 37
3.7. Простые группы 38
3.8. Действие групп на множествах 39
3.9. Примеры действий групп 41

Раздел 4. Строение групп 43
4.1. Силовские подгруппы. Теоремы Силова 43
4.2. Строение групп порядка 12 и 15 46
4.3. Конечно порожденные абелевы группы 48
4.4. Строение конечно порожденных абелевых групп 51

РАЗДЕЛ 1

Алгебраические структуры. Полугруппы и группы

В курсе «Алгебра» вводятся и изучаются основные алгебраические структуры (полугруппы, группы, кольца, поля, модули) и изучаются их свойства. Отдельный раздел курса посвящен введению в теорию многочленов. Основная трудность при изучении этого курса заключается в необходимости овладения разумным "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 раздел (модуль) курса посвящен изучению основ теории групп.

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;
- множества $\mathbb{Z}$ всех целых чисел, множества $\mathbb{Z}_+ = \{0, 1, 2, \dots \}$ всех целых неотрицательных чисел и множества $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$;
- 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 $\mathfrak{S}(\Omega)$ всех подмножеств некоторого множества Ω;
- множества $\mathfrak{T}(\Omega)$ всех отображений некоторого множества Ω в себя или множества $\mathfrak{T}^*(\Omega)$ всех биективных отображений Ω в себя;
- множества $\mathrm{M}_n(E)$ 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

$$(\mathrm{M}_n(\mathbb{R}), +), \qquad \text{и} \quad (\mathrm{M}_n(\mathbb{R}), \times),$$

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 $y_1, y_2 \in Y$.*

1.1. Ассоциативные и коммутативные операции, понятие полугруппы

Данное выше 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 $\mathrm{M}_n(\mathbb{R})$ 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

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

Определение. *Алгебраическая структура $(X, *)$, где X – некоторое множество, а $*$ – ассоциативная операция на X, называется полугруппой.*

Если $(X, *)$ – полугруппа и если операция $*$ коммутативна, что полугруппа X называется коммутативной полугруппой.

Говорят также, что множество X *образует полугруппу (является полугруппой) относительно операции* $*$. Часто используют более короткую терминологию и говорят, что X – полугруппа. При этом имеется в виду, что соответствующая операция $*$ однозначно восстанавливается из контекста.

Если в полугруппе $(X, *)$ операция $*$ – это операция *умножения*, то такая полугруппа называется *мультипликативной*. А если $*$ – это операция *сложения*, то полугруппа X называется *аддитивной*. Безусловно, использование терминов "мультипликативная полугруппа" и "аддитивная полугруппа" носит довольно условный характер. Дело в том, что термин "умножение" часто используется для обозначения общей ассоциативной бинарной операции, а термин "сложение" – для обозначения общей ассоциативной и коммутативной бинарной операции.

Хорошим примером, демонстрирующим естественность такой терминологии являются операции сложения и умножения матриц из $\mathrm{M}_n(\mathbb{R})$, так как матричное сложение – это ассоциативная и коммутативная операция, а матричное умножение – это ассоциативная, но не коммутативная операция.

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.

Определение. *Элемент $e_L \in X$ называется левым единичным (или левым нейтральным) элементом алгебраической структуры $(X, *)$, 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 алгебраической структуре $(X, *)$ существуют левый единичный элемент e_L и правый единичный элемент e_R. 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 алгебраической структуры, 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*).

Обнаруженные свойства левых и правых единичных элементов оправдывают введение следующего определения:

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

Предложение. *Если в алгебраической структуре $(X, *)$ существует единичный элемент, то он является единственным.*

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

Определение. *Если X – полугруппа относительно операции $*$ и если в алгебраической структуре $(X, *)$ существует единичный элемент e, то X называется* **полугруппой с единицей**, *или* **моноидом**.

Пример 1.3. Пусть Ω – некоторое множество. Алгебраическая структура $(\mathfrak{T}(\Omega), \circ)$, где $\circ$ – операция композиции отображений, будет (некоммутативной) полугруппой с единицей. Единицей в этой полугруппе будет тождественное отображение id.

Кроме того, полугруппами с единицей будут алгебраические структуры $(\mathfrak{S}(\Omega), \cup)$ и $(\mathfrak{S}(\Omega), \cap)$, причем единицей в первой из этих полугрупп будет $\varnothing$, а во второй Ω.

Пример 1.4. Пусть $n > 1$ – натуральное число. Тогда $\mathrm{M}_n(\mathbb{R})$ будет коммутативной полугруппой с единицей относительно операции матричного сложения, причем единицей в этой полугруппе будет нулевая матрица 0. Относительно же операции матричного умножения $\mathrm{M}_n(\mathbb{R})$ будет некоммутативной полугруппой с единицей (которая в этом случае равно единичной матрице E).

Пример 1.5. При натуральном $n > 1$ положим

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

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

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

Определение. *Y называется* **подполугруппой** *полугруппы X.*

Пусть теперь X является полугруппой с единицей (моноидом) относительно операции $*$, а Y – замкнутым относительно операции $*$ подмножеством X таким, что $e \in Y$ (где e – единица полугруппы X). В этом случае оправдано следующее определение:

Определение. *Y называется* **подмоноидом** *моноида X.*

Так, при натуральном $n > 1$, структура $(n\mathbb{Z}, \cdot)$ – это подполугруппа полугруппы $(\mathbb{Z}, \cdot)$, а структура $(n\mathbb{Z}, +)$ – это подмоноид моноида $(\mathbb{Z}, +)$.

Замечание. Если есть желание или необходимость подчеркнуть, что алгебраическая структура $(X, *)$ является полугруппой с единицей e, то пишут, что $(X, *, e)$ – полугруппа с единицей.

1.2. Обобщенная ассоциативность, степени и кратные

Предположим, что на множестве X задана некоторая (произвольная) бинарная операция $*$. Пусть $n \geqslant 1$ – натуральное число и пусть $x_1, \ldots, x_n$ – некоторая упорядоченная последовательность элементов множества 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 $x_1 * (x_2 * x_3)$. 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 рассматриваемая операция $*$ ассоциативна, то нет необходимости указывать, как расставлены скобки в произведении. В самом деле, имеет место следующее важное свойство ассоциативных операций.

Предложение 1.6. *Пусть $*$ – ассоциативная бинарная операция на множестве X. 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. Для краткости будем называть операцию $*$ умножением, а элементы a и b в выражении $a * b$ – сомножителями. Предположим теперь, что $n > 3$ и, что для числа сомножителей, меньшего n, доказываемое условие справедливо. Нам необходимо показать, что из этого следует справедливость доказываемого утверждения для произведения 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. □

Пусть теперь на множестве X задана операция умножения и пусть $x_1, \ldots, x_n \in X$. По определению положим

$$\prod_{k=1}^{n} x_k = x_1 \cdot \cdots \cdot x_n = ((\cdots(x_1x_2)\cdots)x_{n-1})x_n.$$

Таким образом, выражение $\prod_{k=1}^{n} x_k$ означает, что произведение элементов $x_1, \ldots, x_n$ вычисляется в естественном порядке справа налево. Другими словами, выражение $\prod_{k=1}^{n} x_k$ – это каноническое произведение элементов $x_1, \ldots, x_n$, определенное при доказательстве Предложения 1.6. В случае, когда на X задана операция сложения, аналогично вводится обозначение $\sum_{k=1}^{n} x_k$.

Заметим, что если X – мультипликативная полугруппа, $x_1, \ldots, x_n \in X$, а $1 \leqslant m \leqslant n$, то справедливо равенство

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

которое непосредственно вытекает из Предложения 1.6.

Пусть на множестве X задана операция умножения, $x \in X$, а $n \in \mathbb{N}$. Выражение $x^n := \prod_{k=1}^{n} x$ называется *(n-ой) степенью* элемента x. При этом x называют основанием степени, а n – показателем. Аналогично, если на X задана операция сложения, то выражение $nx := \sum_{k=1}^{n} x$ называется *кратным* элемента x.

Если X – мультипликативная полугруппа с единицей e, то по определению полагают, что $x^0 = e$. Таким образом, в полугруппах с единицей понятие степени обобщается на показатели $n \in \mathbb{Z}_+$.

Отметим несколько простых свойств степени, которые непосредственно вытекают из формулы (1.1) и из Предложения 1.6. Пусть X – мультипликативная полугруппа с единицей e. Для любого $x \in X$ и для любых $n, m \in \mathbb{Z}_+$ имеют место равенства

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

Для дальнейшего изучения свойств степени в полугруппах нам потребуется следующее понятие

Определение. *Элементы $x \in X$ и $y \in X$ произвольной (не обязательно коммутативной) полугруппы $(X, *)$ называются коммутирующими (говорят также, что элементы x и y коммутируют), 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*

$$(x * y)^n = x^n * y^n. \tag{1.2}$$

Доказательство. Равенство (1.2) 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

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

1.3. Обратимость элементов в полугруппах с единицей

Пусть $(X, *, e)$ – полугруппа с единицей.

Определение. *Элемент $a \in X$ называется* ***обратимым****, если существует элемент $b \in X$ такой, что $a * b = b * a = e$. Этот элемент b называется* ***обратным*** *для элемента a.*

Если элемент $a \in X$ обратим, а $b \in X$ – соответствующий обратный элемент, то ясно, что b также является обратимым элементом.

Предложение. *Если элемент $a \in X$ обратим, то обратный для него элемент $b \in X$ является единственным.*

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

Определение. *Обратный элемент для a обозначают a^{-1}.*

Предложение. $(a^{-1})^{-1} = a$.

Проверка. В самом деле, $(a^{-1})^{-1} * a^{-1} = e$ и, аналогично, $a^{-1}(a^{-1})^{-1} = e$. □

Пример 1.8. Обратная матрица A^{-1} (если она существует) является обратным элементом для матрицы $A \in (\mathrm{M}_n(\mathbb{R}), \cdot, E)$. Число $1/x$ (если $x \neq 0$) является обратным элементов для числа $x \in (\mathbb{Q}, \times, 1)$.

Заметим, что в общем случае элемент x полугруппы с единицей X может не иметь обратного элемента (в полугруппе $\mathrm{M}_n(\mathbb{R})$, например, это так для любой вырожденной матрицы).

В случае аддитивной полугруппы обратный элемент называется ***противоположным***. Так, число $-x$ является противоположным элементом для числа $x \in (\mathbb{Z}, +, 0)$. Такая двойная терминология сложилась исторически и это приходится учитывать.

Замечание. Выше было сделано замечание о том, что в некоторых полугруппах могут существовать односторонние (правые или левые) единичные элементы и не существовать обычных (двусторонних) единичных элементов. Аналогично можно ввести понятие левого и правого обратных элементов для элемента x моноида X: элемент $x_L^{-1} \in X$ называется ***левым обратным*** для элемента x, если $x_L^{-1} * x = e$, а элемент $x_R^{-1} \in X$ называется ***правым обратным*** для элемента x, если $x * x_R^{-1} = e$. Как и в случае с односторонними единичными элементами односторонние обратные элементы могут быть не единственными. Кроме того, если в полугруппе X нет единичного элемента, но есть односторонний единичный элемент, то понятие обратного элемента можно ввести относительно такого одностороннего единичного элемента. В качестве ***упражнения*** предлагается привести примеры указанных ситуаций.

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

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

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

Задача 1.2. Пусть S – полугруппа с единицей относительно операции умножения и пусть $a \in S$ – некоторый произвольный элемент. Определим операцию $*$ на S по правилу $x*y = xay$ для произвольных $x, y \in S$. Проверить, что $(S, *)$ – полугруппа. Доказать, что элемент a обратим в S если и только если $(S, *)$ является полугруппой с единицей (которая в этом случае равна a^{-1}).

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

Для формулировки следующей задачи нам потребуется ввести еще одно важное для дальнейшего изложения понятие.

Определение. *Элемент $x \in X$ полугруппы $(X, *)$ называется* идемпотентным *элементом (или* идемпотентом*), если $x^2 = x$.*

Задача 1.4. Доказать, что любая конечная полугруппа всегда содержит идемпотент.

1.4. 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 (относительно операции $*$), то ее подмножество G_1 называется* подгруппой*, если $e \in G_1$ и для любых элементов $x, y \in G_1$ выполнены условия $x * y \in G_1$ и $x^{-1} \in G_1$.*

Другими словами, G_1 – подгруппа группы G, если G_1 – подмоноид G и множество G_1 замкнуто относительно операции взятия обратного элемента.

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

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 $g, h \in G$ справедливо равенство $g * h = h * g$.*

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 $x, y, z \in G$.

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

Замечание. В дальнейшем, если разумеется это не приведет к разночтениям и неоднозначности, выражение $x * y$ будем записывать в виде xy.

Далее, единицу мультипликативной группы G будем обозначать символом 1. Аналогично, единичный (нейтральный) элемент аддитивной группы будем обозначать символом 0. При необходимости будет также использоваться и введенное выше обозначение нейтрального элемента группы G через e.

И наконец, обратный элемент для элемента x в аддитивной группе мы будем обозначать символом $-x$ и называть ***противоположным*** элементом.

1.5. Примеры групп. Основные матричные группы

Пример 1.9. Пусть $n \in \mathbb{N}$. Рассмотрим множество матриц

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) : \ \det A \neq 0\}$$

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 $\mathrm{GL}_n(\mathbb{R})$ образует группу относительно операции матричного умножения. Эта группа часто называется ***общей линейной группой ранга*** n.

Группа $\mathrm{GL}_n(\mathbb{R})$ содержит важную подгруппу

$$\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) : \ \det A = 1\},$$

которую часто называют ***специальной линейной группой ранга*** n. Проверка того факта, что $\mathrm{SL}_n(\mathbb{R})$ 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 $\mathrm{GL}_n(\mathbb{Q})$ и $\mathrm{GL}_n(\mathbb{C})$ и их подгруппы $\mathrm{SL}_n(\mathbb{Q})$ и $\mathrm{SL}_n(\mathbb{C})$ соответственно.

Заметим однако, что множество матриц $\mathrm{GL}_n(\mathbb{Z})$ 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 $\mathrm{SL}_n(\mathbb{Z})$ уже будет группой относительно операции матричного умножения.

Кроме специальной линейной группы в группе $\mathrm{GL}_n(\mathbb{R})$ выделяют так называемую *унимодулярную группу*, которая состоит из всех матриц с определителем ± 1. В группе $\mathrm{GL}_n(\mathbb{C})$, 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 $A \in \mathrm{GL}_n(\mathbb{R})$ естественным образом связывается некоторое линейное невырожденное преобразование пространства $\mathbb{R}^n$, то можно считать, что $\mathrm{GL}_n(\mathbb{R}) \subset \mathfrak{T}^*(\mathbb{R}^n)$ – подгруппа группы $\mathfrak{T}^*(\mathbb{R}^n)$ всех биективных отображений пространства $\mathbb{R}^n$ в себя. Заметим также, что $\mathrm{GL}_1(\mathbb{R}) = (\mathbb{R}^*, \times)$, $\mathrm{GL}_1(\mathbb{Q}) = (\mathbb{Q}^*, \times)$, а $\mathrm{SL}_1(\mathbb{R}) = \mathrm{SL}_1(\mathbb{Q}) = \mathrm{SL}_1(\mathbb{Z}) = \{1\}$.

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

и другие группы. Напомним также, что

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

а также, что

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

причем соответствующий изоморфизм задается следующим образом

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

1.6. Симметрическая и знакопеременная группы

Как отмечалось выше, множество $\mathfrak{T}^*(\Omega)$ всех биективных отображений некоторого множества Ω на себя образует группу относительно операции композиции отображений.

Определение. *Множество* $\mathrm{S}_n = \mathfrak{T}^*(\{1, 2, \ldots, n\})$, *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 $|\mathrm{S}_n| = n!$.

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 $\sigma \in \mathrm{S}_n$ и $\tau \in \mathrm{S}_n$ 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 $\pi \in \mathrm{S}_n$, 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 $\Omega(n) := \{1, 2, \ldots, n\}$ при $n \in \mathbb{N}$ и пусть $\pi \in \mathrm{S}_n$ – 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 $\Omega(n) = \Omega_1 \sqcup \cdots \sqcup \Omega_q$ 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, $r = 1, \ldots, q$ и, если, $j \in \Omega_k$, то все множество Ω_k состоит из образов точки j при действии на нее степеней перестановки π:

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

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

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

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 $k = 1, 2, \ldots, q$ *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

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

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

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

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:

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

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 1.10. *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 1.10 вытекает следующее утверждение

Предложение 1.11. *Каждая перестановка $\pi \in \mathrm{S}_n$ может быть представлена в виде произведения транспозиций.*

Для **доказательства** достаточно заметить, что

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

(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 $\pi \in \mathrm{S}_n$ 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 $\pi \in \mathrm{S}_n$ и пусть f – произвольная функция от n переменных. Определим

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

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 $\tau \in \mathrm{S}_n$.*

Предложение 1.12. *Пусть π – перестановка из 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. **По определению**, число ε_π называется четностью подстановки π. Если $\varepsilon_\pi = 1$, то π называется четной, а если $\varepsilon_\pi = -1$, то π называется нечетной. Далее, $\varepsilon_{\alpha\beta} = \varepsilon_\alpha\varepsilon_\beta$ для любых перестановок $\alpha, \beta \in S_n$.*

Доказательство. 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

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

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 $\pi \in \mathrm{S}_n$ 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.

РАЗДЕЛ 2

Введение в теорию групп

2.1. Изоморфизмы групп, теорема Кэли

Рассмотрим следующий 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 $\mathrm{S}_3 = \{\mathrm{id}, (12), (23), (13), (123), (132)\}$. 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 $\varphi_1 \circ \varphi_2$ 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.

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 $f(a *_1 b) = f(a) *_2 f(b)$, где $*_{1,2}$ – групповая операция в $G_{1,2}$ соответственно. 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.*

Замечание. В дальнейшем, для сокращения и упрощения записи мы будем писать равенство $f(a *_1 b) = f(a) *_2 f(b)$ в виде $f(ab) = f(a)f(b)$, считая, что и в группе G_1 и в группе G_2 операция записывается одинаково.

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, $\mathrm{S}_3 \cong \mathrm{D}_3$ и $\mathrm{C}_n \cong \langle (12\cdots n)\rangle$.

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 $\ln(ab) = \ln a + \ln b$).

Теорема 2.2 (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 $\mathcal{T}^*(G)$ 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 $\mathcal{T}^*(G) \cong S_n$. В силу сказанного выше, отображение $a \mapsto f_a$ обладает всеми свойствами изоморфизма $G \cong H$. □

Замечание. Из теоремы Кэли вытекает, что совокупность $\{\mathrm{S}_n : n \in \mathbb{N}\}$ является "хранилищем" всех конечных групп (рассматриваемых с точностью до изоморфизма).

2.2. Гомоморфизмы, 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* $\mathrm{Aut}\, G$.

Предложение. *Для произвольной группы G множество* $\mathrm{Aut}\, G$ *образует группу относительно операции композиции отображений. При этом группа* $\mathrm{Aut}\, G$ *является подгруппой группы $\mathcal{T}^*(G)$ 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 $\varphi \circ \psi$ будет биективным. Далее, пусть a и b – произвольные элементы группы G. Тогда

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

следовательно, отображение $\varphi \circ \psi$ сохраняет операцию. Итак, множество $\mathrm{Aut}\, G$ замкнуто относительно операции композиции. Ясно, что $\mathrm{id} \in \mathrm{Aut}\, G$ и для любого отображения $\varphi \in \mathrm{Aut}\, G$ обратное отображение $\varphi^{-1} \in \mathrm{Aut}\, G$. Следовательно, $\mathrm{Aut}\, G$ – 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 $f_a \circ f_b = f_{ab}$. □

Рассмотрим теперь отображение $F : G \to \operatorname{Inn} G$, определенное по правилу $F(a) = f_a$. Оно обладает тем свойством, что для любых элементов $a, b \in G$ имеет место равенство

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

Таким образом отображение F обладает тем свойством изоморфизма групп, что оно "сохраняет операцию". 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. $\operatorname{Inn} G = \{\mathrm{id}\}$.

Однако отображения, сохраняющие групповую операцию, но не являющиеся изоморфизмами групп приходится рассматривать довольно-таки часто. Для таких отображений вводится специальный термин.

Определение. *Отображение $f : G_1 \to G_2$ группы G_1 в группу G_2 называется* гомоморфизмом, *если $f(a *_1 b) = f(a) *_2 f(b)$ для любых элементов $a, b \in G_1$. Здесь символом $*_{1,2}$ обозначена групповая операция в $G_{1,2}$. Гомоморфизм $f : G \to G$ некоторой группы G в себя называется* эндоморфизмом.

Кроме того, сюръективный гомоморфизм называется эпиморфизмом, *а инъективный гомоморфизм –* мономорфизмом.

Определение. *Пусть $f : G_1 \to G_2$ – гомоморфизм групп G_1 и G_2. Множество* $\operatorname{Ker} f = \{x \in G_1 : \ f(x) = e_2\}$ *называется* ядром *гомоморфизма f, а множество* $\operatorname{Im} f = \{f(x) : \ x \in G_1\}$ – образом.

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

Пример 2.3. Рассмотрим несколько примеров вычисления групп $\operatorname{Aut} G$. Пусть $G = \mathbb{Q}$ – аддитивная группа рациональных чисел. Первым делом определим, какие отображения будут гомоморфизмами группы $\mathbb{Q}$. Для этого нам необходимо найти отображения $f : \mathbb{Q} \to \mathbb{Q}$ такие, что для любых $r_1, r_2 \in \mathbb{Q}$ имеет место равенство $f(r_1 + r_2) = f(r_1) + f(r_2)$.

Первым делом заметим, что из выполнения равенства $f(r_1 + r_2) = f(r_1) + f(r_2)$ для любых $r_1, r_2 \in \mathbb{Q}$ 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

$$f(1) = f\left(\tfrac{1}{n} + \cdots + \tfrac{1}{n}\right) = nf\left(\tfrac{1}{n}\right)$$

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

Остается, наконец, заметить, что $f(m/n) = \frac{m}{n} f(1)$ 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 любой гомоморфизм $f : \mathbb{Q} \to \mathbb{Q}$ имеет вид $f = f_a : r \mapsto ar$ для некоторого $a \in \mathbb{Q}$.

Легко видеть, что при $a = 0$ гомоморфизм f_a тривиален ($\operatorname{Im} f_0 = \{0\}$). Для любого $a \in \mathbb{Q}^*$ гомоморфизм f_a, очевидно, является изоморфизмом (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 $q = f_a(q/a)$, $q/a \in \mathbb{Q}$).

Итак, любой автоморфизм группы $\mathbb{Q}$ может быть представлен в виде f_a при некотором $a \in \mathbb{Q}^*$. Следовательно, $\operatorname{Aut} \mathbb{Q} \cong \mathbb{Q}^*$.

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 $f = f_a : n \mapsto an$, где $a = f(1) \in \mathbb{Z}$. Но, так как $\operatorname{Im} f_a = a\mathbb{Z}$, то f_a будет биективным отображением только если $a = \pm 1$ (проверка необходимых деталей оставляется в качестве *упражнения*). Следовательно, $\operatorname{Aut} \mathbb{Z} \cong \{-1, 1\}$, или $\operatorname{Aut} \mathbb{Z} \cong \mathrm{Z}_2$ (где, напомним, через Z_2 обозначена циклическая группа порядка 2).

Пример 2.4. Приведем еще несколько полезных примеров гомоморфизмов групп. Пусть f – отображение аддитивной группы $\mathbb{R}$ вещественных чисел в группу $\mathrm{SO}(2)$ 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 $\operatorname{Ker} f = \{2\pi n : \ n \in \mathbb{Z}\}$. 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 $A \in \mathrm{GL}_n(\mathbb{R})$ ее (ненулевой) определитель является гомоморфизмом $\mathrm{GL}_n(\mathbb{R})$ на $\mathbb{R}^*$. Напомним, что $\mathbb{R}^*$ – это мультипликативная группа ненулевых вещественных чисел.

Пример 2.5. Пусть G – произвольная группа (без ограничения общности будем считать, что операцией в G является умножение). 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*.

Пример 2.6. По определению, группа *кватернионов* Q_8, – это мультипликативная группа, состоящая из элементов $\{\pm 1, \pm i, \pm j, \pm k\}$ со следующей таблицей умножения: $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

Определим матрицы $I, J, K \in \mathrm{M}_2(\mathbb{C})$

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

Тогда (проверка оставляется в качестве *упражнения*) множество $\{\pm E, \pm J, \pm I, \pm K\}$ образует группу относительно операции матричного умножения и эта группа будет изоморфна группе Q_8.

2.3. Циклические группы, порядок элементов

Пусть G – группа с операцией умножения и пусть $a \in G$. 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.

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

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

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

Определение. *Группа G называется* ***циклической****, если существует элемент $a \in G$ такой, что для любого элемента $g \in G$ найдется число $n \in \mathbb{Z}$ такое, что $g = a^n$. В этом случае используется обозначение $G = \langle a \rangle$.*

Замечание. Обозначение $\langle a \rangle := \{a^n : \ n \in \mathbb{Z}\}$ используется и в случае, когда a – некоторый элемент произвольной группы G, не обязательно циклической. В этом случае возникает циклическая подгруппа $\langle a \rangle$ группы G, порожденная элементом a. Если групповая операция в группе G – сложение, то $\langle a \rangle = \{na : \ a \in \mathbb{Z}\}$.

Пример 2.7. Группа $(\mathbb{Z}, +, 0)$ – циклическая группа, причем $\mathbb{Z} = \langle 1 \rangle$.

Далее, циклическая группа

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$

является (циклической) подгруппой группы $\mathrm{SL}_2(\mathbb{Z})$.

Заметим еще, что группа $(\{1, -1\}, \times)$ является циклической.

Пример 2.8. 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.

Циклические группы обладают рядом важных свойств, которые будут часто использоваться нами в дальнейшем. Во-первых, имеет место следующее утверждение:

Предложение 2.9. *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 группу $(\mathbb{Z}, +)$ 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 $f : G_1 \to G_2$ 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 $G_1 \cong G_2$. □

Опираясь на только что доказанное утверждение об изоморфности циклических групп одинакового порядка для обозначения циклической группы порядка n будем использовать символ Z_n.

Пример 2.10. Рассмотрим множество $\{0, 1, \ldots, n-1\}$ и введем на нем операцию $\oplus$ следующим образом: $k \oplus m = (k+m) \pmod n$. Нетрудно проверить (это оставляется в качестве *упражнения*), что $\{0, 1, \ldots, n-1\}$ является группой относительно операции $\oplus$ и что эта группа является циклической группой порядка n.

Циклические группы обладают также следующим свойством:

Предложение 2.11. *Всякая подгруппа циклической группы является циклической группой.*

Доказательство. Пусть H – произвольная подгруппа 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 – наименьшее положительное число, для которого $g^m \in H$. Запишем теперь любое целое число k в виде $k = am + b$, $0 \leqslant b < m$. Если теперь $g^k \in H$, то $g^b = g^{k-am} \in H$ из минимальности m вытекает, что $b = 0$. Следовательно, $H = \langle g^m \rangle$ – циклическая группа. □

Перейдем теперь к понятию порядка элемента группы. Пусть G – произвольная (не обязательно циклическая) группа, а $a \in G$.

Определение. *Если $a^m \neq a^n$ при любых целых $m \neq n$, 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 для некоторого элемента $a \in G$ найдутся некоторые целые числа m и n такие, что $a^m = a^n$ и $m > n$. Из этого вытекает, что существует натуральное число p (равное, например, $m - n$), такое что $a^p = 1$. Введем следующее определение.

Определение. *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 $\operatorname{ord}_G a = \operatorname{ord} a = \min\{p \in \mathbb{N} : \ a^p = 1\}$.*

Из определения порядка элемента вытекает, что если $|G| < \infty$, то $\operatorname{ord}_G a < \infty$ для любого элемента a группы G.

Предложение 2.12. *Для любого элемента a произвольной группы G верно равенство $\operatorname{ord} a = |\langle a \rangle|$. Если $\operatorname{ord} a = q < \infty$, то $\langle a \rangle = \{1, a, \ldots, a^{q-1}\}$ и, кроме того $a^n = 1$ если и только если $n = mq$, $m \in \mathbb{Z}$.*

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

Пусть теперь $\operatorname{ord} a = q < \infty$. Тогда все элементы $1, a, a^2, \ldots, a^{q_1}$ различны, а $a^q = 1$. Далее, для произвольного $n \in \mathbb{Z}$ из равенства $n = mq + r$, где $m \in \mathbb{Z}$, а $r \in \{0, 1, \ldots, q-1\}$, вытекает, что $a^n = a^{mq+r} = (a^q)^m a^r = a^r$. Из этого равенства непосредственно вытекают оставшиеся утверждения. □

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 2.1. 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 если и только если $d(G) = |G|$. Выяснить, сохранятся ли два последних утверждения в случае, если группа G не будет коммутативной.

Рассмотрим структуру циклических групп более подробно. Для удобства будем считать, что рассматриваемые группы являются аддитивными (групповая операция – сложение). Пусть $A = \langle a \rangle$ – аддитивная циклическая группа конечного порядка q, порожденная элементом a. При этом $A = \{0, a, \ldots, (q-1)a\}$ и, как было установлено при доказательстве Предложения 2.11, любая нетривиальная подгруппа A' группы A имеет вид $A' = \{0, ma, 2ma, \ldots\}$ при некотором (минимальном) $m \in \mathbb{N}$, причем если $ka \in A'$ при $k \in \mathbb{N}$, то $k = m\ell$, $\ell \in \mathbb{N}$. Пусть $q = dm + r$, $0 \leqslant r < m$. Тогда $0 = qa = d(ma) + ra$ и, следовательно, $ra = -d(ma) \in A'$. Из минимальности m вытекает, что $r = 0$. Таким образом $q = dm$ и $A' = \{0, ma, 2ma, \ldots, (d-1)ma\} = mA$ – подгруппа в A порядка d. Если при этом m пробегает последовательно всю совокупность делителей числа q, то тоже самое происходит и с d, а выражение mA доставляет нам ровно по одной подгруппе каждого порядка, делящего d. Итак

Подгруппы бесконечной аддитивной циклической группы $\mathbb{Z}$ – это в точности группы $n\mathbb{Z}$, $n \in \mathbb{N}$. Подгруппы циклической группы порядка q находятся во взаимно однозначном соответствии с положительными делителями числа q.

Замечание. В циклической группе $A = \langle a \rangle$ порядка q подгруппа порядка d, где d – положительный делитель числа q, совпадает с множеством $\{b \in A : \ db = 0\}$.

В самом деле, если $q = dm$, то соответствующая подгруппа имеет вид mA и, следовательно, $db = 0$ для $b \in mA$. Если, обратно, $b = \ell a \in A$ и $db = 0$, то $d\ell a = 0$ и, следовательно, $d\ell = qk = dmk$, откуда $\ell = mk$ и $b = k(ma) \in mA$.

В связи с рассмотренным выше понятием гомоморфизма групп полезно иметь в виду следующий пример: отображение $f : \mathbb{Z} \to \mathrm{Z}_q$ аддитивной группы целых чисел в циклическую группу $\mathrm{Z}_q = \langle g \rangle$ порядка q, определенное по формуле $f(n) = g^n$ является гомоморфизмом рассматриваемых групп. Его ядро равно $\operatorname{Ker} f = \{kq : \ k \in \mathbb{Z}\}$.

2.4. Нормальные подгруппы

Определение. *Пусть G – некоторая группа. Подгруппа $H \subset G$ называется нормальной в G, если $yHy^{-1} = H$ для любого $y \in G$, где $yHy^{-1} = \{yhy^{-1} : \ h \in H\}$.*

Тот факт, что H – это нормальная подгруппа группы G, традиционно обозначают символом $H \lhd G$.

Пример 2.13. Подгруппа $\langle (123) \rangle$ является нормальной подгруппой S_3, а подгруппа $\langle (12) \rangle$ – нет. Проверка оставляется в качестве *упражнения*.

Предложение 2.14. *Пусть $f : G \to G'$ – некоторый гомоморфизм групп G и G'. Тогда $\operatorname{Ker} f$ является нормальной подгруппой в G.*

Проверка. Для любых элементов $h \in \operatorname{Ker} f$, $g \in G$ имеют место равенства

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)1_{G'}f(g)^{-1} = 1_{G'},$$

где $1_{G'}$ – это единица группы G'. Т.е., если $h \in \operatorname{Ker} f$, то $ghg^{-1} \in \operatorname{Ker} f$ и, следовательно, $g(\operatorname{Ker} f)g^{-1} \subset \operatorname{Ker} f$ для любого $g \in G$. Аналогично проверяется, что если $h \in \operatorname{Ker} f$ и $g \in G$ – произвольны, то $h' := g^{-1}hg \in \operatorname{Ker} f$. Так как $h = gh'g^{-1}$, то $\operatorname{Ker} f \subset g(\operatorname{Ker} f)g^{-1}$ для любого $g \in G$. Окончательно получаем, что $\operatorname{Ker} f = g(\operatorname{Ker} f)g^{-1}$ для любого $g \in G$, что и требовалось. □

2.5. 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. Найдем подгруппу G_A группы G, обладающую таким свойство, что $A \subset G_A$ и для любой подгруппы $G_1 \subset G$ такой, что $A \subset G_1$ имеет место $G_A \subset G_1$. Другими словами, G_A – это минимальная подгруппа группы G, содержащая A. Из определения минимальной подгруппы непосредственно вытекает, что такая подгруппа (если она существует) будет единственной. В самом деле, если существуют две минимальные подгруппы G_A^1 и G_A^2 группы G, содержащая множество A, то в силу данного выше определения, имеют место включения $G_A^1 \subset G_A^2$ и $G_A^2 \subset G_A^1$ и, следовательно, $G_A^1 = G_A^2$.

Предложение. *Пусть G_j, $j \in J$ – некоторое семейство подгрупп группы G (здесь через J обозначено некоторое множество индексов). Тогда $G_J = \bigcap_{j\in J} G_j$ является подгруппой в G.*

Проверка. Так как единица 1 группы G принадлежит все подгруппам G_j, $j \in J$, то $1 \in G_J$, откуда вытекает, что G_J – полугруппа с единицей. Проверим, что G_J является подполугруппой G. Для этого проверим, что если $a, b \in G_J$, то $ab \in G_J$. В самом деле, если $a, b \in G_J$, то $a, b \in G_j$ для любого $j \in J$, следовательно, $ab \in G_j$ для любого $j \in J$ и, наконец, из этого вытекает, что $ab \in G_J$. Аналогично проверяется, что для любого элемента $a \in G_J$ элемент $a^{-1} \in G_J$. Таким образом, множество G_J в самом деле является подгруппой группы G. □

Определение. *Обозначим через $\langle A\rangle = \langle A\rangle_G$, где A – некоторое подмножество элементов группы G, пересечение всех таких подгрупп G_1 группы G, что $A \subset G_1$.*

Следствие. *Для любого множества $A \subset G$ группа G_A существует, при этом $G_A = \langle A\rangle_G$.*

Предложение 2.15. $\langle A\rangle = \{x_1 \cdots x_n : \ n \in \mathbb{N},\ x_j \in A \text{ или } x_j^{-1} \in A\}$.

Доказательство. Заметим, что $X_A := \{x_1 \cdots x_n : \ n \in \mathbb{N},\ x_j \in A \text{ или } x_j^{-1} \in A\}$ 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, $X_A \subset G$ – подгруппа и $A \subset X_A$. Следовательно, $\langle A\rangle \subset X_A$ (так как $\langle A\rangle$ – минимальная подгруппа, содержащая A).

Пусть теперь G_1 – произвольная подгруппа группы G, содержащая множество A. Следовательно $a \in G_1$ и $a^{-1} \in G_1$ для любого $a \in A$. Следовательно, любое произведение вида $x_1 \cdots x_n$, где $x_j \in A$ или $x_j^{-1} \in A$ принадлежит G_1 и, следовательно, $X_A \subset G_1$ для любой подгруппы G_1, содержащей A. Из этого окончательно вытекает, что $X_A \subset \langle A\rangle$, так как $\langle A\rangle$ – это пересечение всех таких G_1. □

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 группы G.*

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

Если $|A| = n < \infty$ и $A = \{a_1, \dots, a_n\}$, то пишут $\langle A\rangle = \langle a_1, \dots, a_n\rangle$. Если $G = \langle A\rangle$ и $|A| < \infty$, то G называют *конечно-порожденной* группой. Например, циклические группы являются конечно-порожденными.

Задача 2.2. 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 2.3. Доказать, что полугруппа с единицей X такая, что для любых $a, b \in X$ уравнения $ax = b$ и $xa = b$ разрешимы в X, является группой.

Задача 2.4. Проверить, что множество $\mathrm{Aff}_1(\mathbb{R}) := \{\varphi_{a,b} : x \mapsto ax+b :\ a \in \mathbb{R}^*, b \in \mathbb{R}\}$ аффинных преобразований вещественной прямой $\mathbb{R}$ образуют группу относительно операции умножения, определенной следующим образом $\varphi_{a,b}\varphi_{c,d} = \varphi_{ac,ad+b}$. В группе $\mathrm{Aff}_1(\mathbb{R})$ содержатся следующие интересные подгруппы: подгруппа $\mathrm{GL}_1(\mathbb{R})$ преобразований, оставляющих на месте начало координат, и подгруппа сдвигов $\{x \mapsto x+b :\ b \in \mathbb{R}\}$.

Задача 2.5. 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 $\mathrm{SL}_2(\mathbb{Z})$. Показать, что $\langle AB\rangle$ – бесконечная циклическая подгруппа в $\mathrm{SL}_2(\mathbb{Z})$.

Задача 2.6. Доказать, что если $|G| = 2n < \infty$, $n \in \mathbb{N}$, то в G обязательно существует элемент g порядка 2.

Задача 2.7. Предложить какую-либо систему образующих для мультипликативной группы $\mathbb{Q}_+$ положительных рациональных чисел.

Свободные группы. Пусть $F = \langle a_1, \dots, a_n\rangle$ – это группа, порожденная n образующими $a_1, a_2, \dots, a_n$. Тогда каждый элемент $g \in F$ можно записать (возможно многими различными способами) в виде

$$g = a_{j_1}^{k_1} a_{j_2}^{k_2} \cdots a_{j_m}^{k_m}, \tag{2.1}$$

где $k_1, \dots, k_m \in \mathbb{Z}$, $j_1, \dots, j_m \in \{1, \dots, n\}$ причем $j_s \neq j_{s+1}$ при $s = 1, 2, \dots, k-1$.

Легко проверяется (это оставляется в качестве *упражнения*), что единственность представления (2.1) для любого элемента $g \in F$ эквивалентна единственности такого представления для единицы группы F.

Определение. *Пусть F – группа, порожденная n образующими $a_1, \dots, a_n$ и пусть $g = a_{j_1}^{k_1} a_{j_2}^{k_2} \cdots a_{j_m}^{k_m}$. Если $g = 1$ тогда и только тогда, когда $k_1 = \cdots = k_m = 0$, то говорят, что F – свободная группа ранга n, порожденная n свободными образующими*

Пусть $F = \langle a_1, \dots, a_n\rangle$ и $G = \langle b_1, \dots, b_n\rangle$ – свободные группы ранга n. Определим отображение $\varphi : F \to G$ следующим образом: $\varphi(a_j) = b_j$ при $j = 1, \dots, n$, а для произвольного элемента $f = a_{j_1}^{k_1} \cdots a_{j_m}^{k_m} \in F$ положим $\varphi(f) = b_{j_1}^{k_1} \cdots b_{j_m}^{k_m}$. Это отображение будет изоморфизмом групп F и G (проверка оставляется в качестве *упражнения*). Таким образом, любые две свободные группы одного ранга n изоморфны.

В учетом этого замечания для каждого значения $n \in N$ интересно найти примеры реализаций свободных групп соответствующего ранга n.

Пример 2.16. Группа $F_1 \cong (\mathbb{Z}, +)$ – это свободная группа ранга 1. Другими словами, F_1 – это бесконечная циклическая группа.

Пример 2.17. Приведем пример свободной группы F_2 ранга 2. Рассмотрим матричную группу $\mathrm{SL}_2(\mathbb{Z}[t])$, где $\mathbb{Z}[t]$ – совокупность всех многочленов от переменного t с целочисленными коэффициентами (проверка того факта, что $\mathrm{SL}_2(\mathbb{Z}[t])$ – группа, оставляется в качестве *упражнения*). Пусть $F \subset \mathrm{SL}_2(\mathbb{Z}[t])$ – 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 F свободно, оставляется к качестве простого *упражнения* на операции с матрицами.

Определяющие соотношения. 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 $g^n = 1$.

Пусть теперь F_n – свободная группа со свободными образующими $a_1, \ldots, a_n$ и пусть $W \subset F_n$ – некоторое фиксированное подмножество F_n. Запишем каждый элемент $w_j \in W$, $j = 1, \ldots, J$ в виде некоторого соотношения вида (2.1) так, что $w_j = w_j(a_1, \ldots, a_n)$. Рассмотрим также минимальную нормальную подгруппу K в F_n такую, что $W \subset K$[1].

Определение. *Скажем, что группа G задана образующими $b_1, \ldots, b_n$ и определяющими соотношениями $w_j(b_1, \ldots, b_n) = 1$, если существует эпиморфизм $\pi : F_n \to G$ такой, что $\pi(a_j) = b_j$ при $j = 1, \ldots, n$ и $\operatorname{Ker}\pi = K$. В этом случае используется обозначение*

$$G = \langle b_1, \ldots, b_n \mid w_j(b_1, \ldots, b_n) = 1, j = 1, \ldots, J \rangle,$$

а если $|J| < \infty$, то говорят, что группа G конечно определена.

Пример 2.18. Пусть $G = \langle a, b \mid a^3 = b^2 = abab = 1 \rangle$. Легко заметить, что $|G| \leqslant 6$. Далее, так как $ba = a^{-1}b^{-1} = (a^3)^{-1}a^2b(b^2)^{-1} = a^2b$, то $G = \{1, a, a^2, b, ab, a^2b\}$. Заметим теперь, что в группе S_3 имеют место соотношения $(123)^3 = \mathrm{id}$, $(12)^2 = \mathrm{id}$ и $(123)(12)(123)(12) = \mathrm{id}$.

Таким образом, отображение $\varphi : G \to \mathrm{S}_3$ заданное следующим образом: $a \mapsto (123)$ и $b \mapsto (12)$ является изоморфизмом групп $G \cong \mathrm{S}_3$. Таким образом, группа S_3 задается двумя образующими и тремя определяющими соотношениями.

Аналогично можно заметить, что группа D_3 симметрий правильного треугольника также изоморфна G (соответствующий изоморфизм должен поставить элементу a в соответствие поворот на $120°$ относительно центра треугольника, а элементу b – симметрию треугольника относительно прямой, проходящей через центр и одну из вершин).

Упражнение. Пусть $n \geqslant 3$. Проверить, что $\mathrm{D}_n \cong \langle a, b \mid a^n = b^2 = (ab)^2 = 1 \rangle$.

Пример 2.19. Определим группу $X := \langle a, b \mid a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1} \rangle$. Так как $ba = a^{-1}b = a^3b$ и так как $a^2 = b^2$, то всякий элемент вида (2.1), 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, $|X| \leqslant 8$. Приведем пример группы порядка 8, образующие которых связаны между собой такими же соотношениями, как элементы a и b из определения группы X. Это будет группа кватернионов Q_8. В качестве *упражнения* предлагается проверить, что $\mathrm{Q}_8 = \langle i, j \rangle$ и, что требуемые определяющие соотношения выполняются при $a = i$ и $b = j$. Таким образом $X \cong \mathrm{Q}_8$ и часто группа X также называется группой кватернионов и обозначается символом Q_8. Выше было показано, что группа Q_8 может быть реализована и как матричная группа $\langle I, J \rangle$, порожденная матрицами

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

[1] В дальнейшем будем доказано (см. Теорему 3.5), что для любой нормальной подгруппы H группы G найдется такие группа G' и гомоморфизм $f : G \to G'$, что $\operatorname{Ker} f = H$

2.6. Произведение групп

Пусть G и H – две произвольные группы.

Определение. *Прямым произведением $G \times H$ групп G и H называется множество $\{(g,h) : \ g \in G, h \in H\}$ с операцией умножения $(g_1,h_1)\cdot(g_2,h_2) = (g_1g_2, h_1h_2)$. Часто используется также термин* внешнее прямое произведение.

Заметим, что в данном только что определении мы использовали одинаковые символы для записи операций умножения в G, H и $G \times H$. Это допустимо, так как из контекста всегда ясно, о каком именно умножении идет речь.

Упражнение. Проверить, что множество $G \times H$ относительно введенной операции умножения пар является группой.

Заметим также, что в $G \times H$ содержатся подгруппы $G \times 1 = \{(g,1) : \ g \in G, 1 \in H\}$ и $1 \times H = \{(1,h) : \ h \in H, 1 \in G\}$, 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*).

Аналогично можно убедится (проверка необходимых деталей оставляется в качестве *упражнения*), что для трех данных групп G_1, G_2 и G_3 можно определить прямые произведения $G_1 \times (G_2 \times G_3)$ и $(G_1 \times G_2) \times G_3$, причем $G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3$.

И, наконец, свойства коммутативности и ассоциативности (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.

В дальнейшем нам понадобится следующее понятие. Если $A \subset G$ и $B \subset G$ – два подмножества группы G, то подмножество AB (произведение подмножеств A и B) определяется следующим естественным образом $AB = \{ab : \ a \in A, b \in B\}$.

Упражнение. Показать, что для любых трех подмножеств A, B и C группы G верно равенство $(AB)C = A(BC)$.

Предложение 2.20. *Проверить, что подмножество $H \subset G$ является подгруппой если и только если $H^2 = H$ и $H^{-1} \subset H$, где $H^2 = HH$, а $H^{-1} = \{h^{-1} : \ h \in H\}$.*

Упражнение. Доказать Предложение 2.20.

Понятия прямого произведения групп и произведения подмножеств групп связаны следующим образом.

Теорема 2.21. *Пусть G – группа, а A и B – такие ее нормальные подгруппы, что $A \cap B = \{1\}$ и $AB = G$. Тогда $A \times B \cong G$.*

Доказательство. Так как $G = AB$, то для любого элемента $g \in G$ существуют такие элементы $a \in A$ и $b \in B$, что $g = ab$. Проверим, что в условиях теоремы такое представление единственно для любого $g \in G$. Пусть $g = a_1b_1 = a_2b_2$, где $a_1, a_2 \in A$, а $b_1, b_2 \in B$. Из равенства $a_1b_1 = a_2b_2$ вытекает, что $a_2^{-1}a_1 = b_2b_1^{-1}$ и, следовательно, $a_2^{-1}a_1 \in B$, а $b_2b_1^{-1} \in A$. А так как $A \cap B = \{1\}$, то $a_2^{-1}a_1 = 1$ и $b_2b_1^{-1} = 1$. Таким образом, $a_1 = a_2$ и $b_1 = b_2$.

Пусть g – произвольный элемент группы G. По доказанному выше существуют единственные элементы $a \in A$ и $b \in B$ такие, что $g = ab$. Вычислим теперь коммутатор $[a,b]$. Так как A – нормальная подгруппа группы G, то

$$[a,b] = aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = aa' \in A,$$

а так как B – нормальная подгруппа группы G, то

$$[a,b] = aba^{-1}b^{-1} = (aba^{-1})b^{-1} = b'b^{-1} \in B.$$

Так как $A \cap B = \{1\}$, то $[a, b] = 1$ и, окончательно, мы получаем, что $ab = ba$.

Рассмотрим теперь отображение $f : G \to A \times B$, определенное следующим образом: $f(g) = (a, b)$ для любого $g \in G$, $g = ab$, $a \in A$, $b \in B$. Так как $f(g_1g_2) = f(a_1b_1a_2b_2) = f(a_1a_2b_1b_2) = (a_1a_2, b_1b_2) = (a_1, b_1)(a_2, b_2) = f(a_1b_1)f(a_2b_2) = f(g_1)f(g_2)$, то f – гомоморфизм. Далее, $f(ab) = (1, 1)$ (ясно, что единицей в $A \times B$ является именно элемент $(1, 1)$) если и только если $a = b = 1$. Следовательно, $\operatorname{Ker} f = \{1\}$ и, следовательно, f – мономорфизм. Очевидно, что f является эпиморфизмом. Таким образом, f – изоморфизм G на $A \times B$. □

Замечание. Если группа G представима в виде $G = AB$, где A и B – ее нормальные подгруппы, то говорят, что G является *внутренним прямым произведением* A и B. Разница между внутренним и внешним прямыми произведениями состоит в том, что в случае внутреннего произведения перемножаются сами подгруппы A и B, а не изоморфные им подгруппы $A \times 1$ и $1 \times B$. При этом внешнее прямое произведение является внутренним произведением $A \times 1$ и $1 \times B$. Заметим, что разница между этими прямыми произведениями довольно условна и можно в обоих случаях использовать термин “прямое произведение”.

Отметим также, что подгруппы $A \times 1$ и $1 \times B$ прямого произведения групп $A \times B$ нормальны. В самом деле, если $x, a \in A$, а $y, b \in B$, то $(a, b)(x, 1)(a^{-1}, b^{-1}) = (axa^{-1}, 1) \in A \times 1$, а $(a, b)(1, y)(a^{-1}, b^{-1}) = (1, byb^{-1}) \in 1 \times B$. Таким образом, группы A и B изоморфны нормальным подгруппам $A \times 1$ и $1 \times B$ своего прямого произведения. Таким образом можно утверждать, 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 $H_2 \lhd G$. Аналогичное свойство верно и для прямого произведения большего числа сомножителей.

РАЗДЕЛ 3

Основные теоретико-групповые конструкции

3.1. Смежные классы по подгруппе

Заметим, что если $f : G \to G'$ – некоторый гомоморфизм групп и если $a \in G$ – произвольный элемент, то все элементы множества $a \operatorname{Ker} f = \{ax : \ x \in \operatorname{Ker} f\}$ отображаются при помощи f в один элемент $f(a) \in G'$. В самом деле, при $x \in \operatorname{Ker} f$ имеет место равенство $f(ax) = f(a)f(x) = f(a)1_{G'} = f(a)$. Обратно, если для некоторого элемента $g \in G$ верно равенство $f(g) = f(a)$, то $f(a^{-1}g) = f(a)^{-1}f(g) = 1_{G'}$, т.е. $x = a^{-1}g \in \operatorname{Ker} f$ и, окончательно, $g = ax \in a \operatorname{Ker} f$.

Это наблюдение оправдывает введение следующего понятия.

Определение. *Пусть $H \subset G$ – подгруппа группы G и пусть $g \in G$ – некоторый фиксированный элемент. Множество $gH = \{gh : \ h \in H\}$ называется* левым смежным классом *группы G по подгруппе H, а элемент g называется* представителем *смежного класса gH. Аналогично определяется* правый смежный класс *Hg.*

Заметим, что если $H = \operatorname{Ker} f$ – ядро некоторого гомоморфизма $f : G \to G'$, то (выше было показано, что $\operatorname{Ker} f$ является нормальной подгруппой), $gH = Hg$ для любого $g \in G$.

Заметим также, что сама подгруппа $H \subset G$ является и левым и правым смежным классом, так как $H = 1_G H = H 1_G$.

Однако в общем случае смежный класс gH не является подгруппой в G. В самом деле, если gH является подгруппой, то $1_G \in gH$ 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 3.1. *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 3.2. Рассмотрим, в качестве примера, разложение группы S_3 в объединение смежных классов по подгруппе S_2. Заметим, что $\mathrm{S}_2 = \langle(12)\rangle$. Непосредственным вычислением проверяем, что

$$\mathrm{S}_3 = \mathrm{S}_2 \sqcup (13)\mathrm{S}_2 \sqcup (23)\mathrm{S}_2 = \{\mathrm{id}, (12)\} \sqcup \{(13), (123)\} \sqcup \{(23), (132)\}$$

и, что

$$\mathrm{S}_3 = \mathrm{S}_2 \sqcup \mathrm{S}_2(13) \sqcup \mathrm{S}_2(23) = \{\mathrm{id}, (12)\} \sqcup \{(13), (132)\} \sqcup \{(23), (123)\}.$$

Заметим, что разложения на левые и правые смежные классы не совпадают. Можно также заметить, что при любом натуральном $n > 2$ имеет место разложение

$$\mathrm{S}_n = \bigsqcup_{k=0}^{n-1} \sigma_{n,k}\mathrm{S}_{n-1},$$

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 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 левых смежных классов группы G (по некоторой подгруппе $H \subset G$), то $\{1, g_1^{-1}, g_2^{-1}, \ldots\}$ – множество представителей всех соответствующих правых смежных классов. Мощности этих множеств совпадают.

Определение. *Множество всех левых смежных классов группы G по подгруппе H обозначается G/H. Если необходимо одновременно рассматривать множества левых и правых смежных классов, то для них используются обозначения $(G/H)_\ell$ и $(G/H)_r$. Величина $|G/H|$ называется* индексом подгруппы *H в G и обозначается специальным символом $(G : H)$.*

Замечание. В связи с только что введенным обозначением $(G : H)$ индекса подгруппы заметим, что $|G| = (G : \{1_G\})$, т.е. порядок группы совпадает с индексом ее единичной подгруппы. Соответственно, для порядка группы используется также символ $(G : 1)$ или $(G : e)$.

Справедлива следующая важная теорема

Теорема 3.3 (теорема Лагранжа)**.** *Порядок конечной группы делится на порядок любой подгруппы этой группы.*

Доказательство. Пусть g – произвольный элемент группы G. В ходе доказательства теоремы Кэли было, по существу, установлено, что естественное отображение $H \to gH$ такое, что $h \mapsto gh$, $h \in H$, является биективным. Следовательно, $|gH| = (H : 1)$. Из этого и из того факта, что каждая группа разлагается в объединение непересекающихся смежных классов, вытекает, что

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

Следствие. *Порядок любого элемента группы делит порядок группы. Группа простого порядка p всегда циклическая и, с точностью до изоморфизма, единственная.*

Проверка. По определению, порядок элемента $g \in G$ группы G – это порядок порожденной элементом g циклической группы $\langle g\rangle$ и для проверки первого утверждения осталось непосредственно сослаться на теорему Лагранжа. Пусть теперь G такова, что $|G| = p \in \mathbb{P}$. Если H – не тривиальная подгруппа G, то $|H|$ делит $|G|$ и, следовательно, $|H| = p$. Таким образом, $G = H$. Отсюда вытекает, что G совпадает с циклической

группой, порожденной любым элементом $g \in G$, $g \neq 1$. Единственность вытекает из того, что все циклические подгруппы одного порядка изоморфны. □

Замечание. Интересно, что не для любого делителя m порядка $|G|$ группы G можно найти подгруппу $H \subset G$ такую, что $|H| = m$. Например, в группе A_4 (для которой $|A_4| = 12$) нет подгрупп порядка 6 (проверка оставляется в качестве *упражнения*).

В завершении этого раздела сформулируем еще одно понятие, которое будет применяться в дальнейшем.

Определение. *Две подгруппы H_1 и H_2 группы G называются* сопряженными, *если найдется такой элемент $g \in G$, что $H_2 = gH_1g^{-1} = \{ghg^{-1} : \ h \in H_1\}$.*

3.2. Факторгруппы

Пусть G – некоторая группа, а $H \subset G$ – ее подгруппа. Напомним два понятия, связанных с этими объектами и введенных ранее. Это, во-первых, множество G/H смежных классов группы G по подгруппе H и, во-вторых, понятие нормальной подгруппы. Напомним, что подгруппа $H \subset G$ называется *нормальной* (ранее было введено обозначение $H \lhd G$), если $gHg^{-1} = H$ для любого $g \in G$, или, другими словами, если $gH = Hg$ для любого $g \in G$. Как отмечалось ранее, характерными примерами нормальных подгрупп являются ядра $\operatorname{Ker}\varphi$ гомоморфизмов $\varphi : G \to G_1$ группы G в некоторую группу G_1 (см. Предложение 2.14).

Итак, рассмотрим некоторую группу G, ее нормальную подгруппу H и множество G/H 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 $a^{-1}b \in H$.

Пусть теперь элементы $a, b, c, d \in G$ таковы, что $a \sim_H c$, а $b \sim_H d$. Так как $H \lhd G$, то

$$(ab)^{-1}cd = b^{-1}a^{-1}cd = b^{-1}(a^{-1}c)d = b^{-1}h_1d = b^{-1}h_1bb^{-1}d = b^{-1}h_1bh_2 = h_3h_2 \in H,$$

где $h_1 = a^{-1}c \in H$, $h_2 = b^{-1}d \in H$ и $h_3 = b^{-1}h_1b \in H$. Таким образом, из эквивалентности элементов $a \sim_H c$ и $b \sim_H d$ вытекает, что $ab \sim_h cd$. Следовательно, если $H \lhd G$, то операция умножения в группе G индуцирует операцию умножения смежных классов по подгруппе H.

Используя введенную выше операцию произведения подмножеств групп, можно сказать, что любой смежный класс gH по подгруппе H представляет собой произведение $\{g\}H$. Заметим теперь, что произведение смежных классов g_1H и g_2H – это множество $g_1H \cdot g_2H$, которое, в общем случае, не является смежным классом. В самом деле, имеет место, например, следующая ситуация.

Упражнение. Проверить, что если $H = \{\mathrm{id}, (12)\}$ – подгруппа в S_3, то $H \cdot (13)H = (13)H \cup (23)H$.

Однако, если $H \lhd G$, то описанная в предыдущем примере ситуация не возможна, а имеют место следующие равенства

$$aH \cdot bH = a(Hb)H = a(bH)H = abHH = abH,$$

т.е. произведение смежных классов по нормальной подгруппе будет смежным классом по этой подгруппе. Более того, в этом случае будут выполнены следующие свойства операции умножения смежных классов: $H \cdot aH = aH \cdot H = aH$ и $a^{-1}H \cdot aH = aH \cdot a^{-1}H = H$. Из всего сказанного вытекает следующий результат.

Теорема 3.4. *Если H – нормальная подгруппа некоторой группы G, то операция умножения смежных классов $aH \cdot bH = abH$ 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 $a^{-1}H$.*

В случае, когда G – конечная группа, из теоремы Лагранжа вытекает, что

$$|G/H| = |G|/|H| = (G : H).$$

3.3. Описание групп малых порядков

Первым делом установим два следующих простых факта.

Предложение. *Если в некоторой группе G все элементы $g \neq 1$ имеют порядок 2, то 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 $g, h \in G$. □

Предложение. *Пусть G – группа, а $H \subset G$ – подгруппа. Если $(G : H) = 2$, то H – нормальная подгруппа.*

Проверка. 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, $H = gHg^{-1}$ (т.е., H – нормальная подгруппа). □

Ясно, что любая группа порядка 2 изоморфна группе Z_2 (проверка этого тривиального факта оставляется в качестве *упражнения*).

Рассмотрим теперь группу G порядка 4. Такие группы могут быть устроены одним из двух следующих способов (с точностью до изоморфизма). Если группа G содержит элемент порядка 4, то она изоморфна группе Z_4. В противном случае все элементы группы G имеют порядок 2, эта группа коммутативна и изоморфна группе $\mathrm{Z}_2 \times \mathrm{Z}_2$.

Устройство группы порядка 6. Рассмотрим группу G порядка 6. Имеют место следующие возможности. Во-первых, в G может существовать элемент порядка 6. В этом случае ясно, что $G \cong \mathrm{Z}_6$. Во-вторых, может случиться так, что все элементы группы G, не равные 1, имеют порядок 2. В этом случае группа G коммутативна.

Пусть теперь G – некоммутативная группа порядка 6. Из вышеизложенного вытекает, что в G существует 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 – 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 $ab = ba$, а из этого вытекает, 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 $b^2 = e$.

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 $\mathrm{S}_3 \cong \mathrm{D}_3$.

Задача 3.1. Пусть p – простое число, а G – некоммутативная группа такая, что $|G| = 2p$. Доказать, что если в G содержится элемент порядка 2, то $G \cong \mathrm{D}_p$.

Задача 3.2. Если группа G некоммутативна и $|G| = 8$, то $G \cong \mathrm{D}_4$ или $G \cong \mathrm{Q}_8$. Если $|G| = 10$, то $G \cong \mathrm{Z}_{10}$ или $G \cong \mathrm{D}_5$.

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).

3.4. Теоремы о гомоморфизмах групп

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

Теорема 3.5 (основная теорема о гомоморфизме групп)**.** *Если G и H – группы, а $\varphi : G \to H$ – гомоморфизм, то $\operatorname{Ker}\varphi \lhd G$ и $G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$. Кроме того, если $K \lhd G$ – нормальная подгруппа, то существуют такие группа H и эпиморфизм $\pi : G \to H$, что $\operatorname{Ker}\pi = K$.*

Доказательство. Тот факт, что $K := \operatorname{Ker}\varphi \lhd G$ был проверен раньше (см. Предложение 2.14). Следовательно, G/K – группа. Определим отображение $\Phi : G/K \to H$ по правилу $\Phi(gK) = \varphi(g)$.

Проверим, что такое определение отображения Φ корректно в том смысле, что $\Phi(gK)$ 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 Φ является гомоморфизмом. Это вытекает из следующей цепочки равенств (в которой учтено, что $K = \operatorname{Ker}\varphi$ – нормальная подгруппа):

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

для любых $g_1, g_2 \in G$. Пусть теперь $g_1 \in G$ и $g_2 \in G$ таковы, что $\Phi(g_1K) = \Phi(g_2K)$. 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 Φ – мономорфизм. Остается заметить, что $\operatorname{Im}\Phi = \operatorname{Im}\varphi$.

Обратно, если $K \lhd G$ – некоторая нормальная подгруппа, то отображение $\pi : g \mapsto gK$, $g \in G$, 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 3.6. *Пусть G – группа, $H \subset G$ – ее подгруппа, а $K \lhd G$ – нормальная подгруппа. 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 $f : hK \mapsto h(H \cap K)$ 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 $\pi : G \to G/K$ и его сужение π_0 на H, т.е. $\pi_0 = \pi_{|H}$. Так как $K \lhd HK$, то определена факторгруппа HK/K. По определению π_0 получаем, что $\operatorname{Im}\pi_0 = \{hK : \ h \in H\} = HK/K$. Итак, $\pi_0 : H \to HK/K$ – эпиморфизм. Найдем

его ядро: $\operatorname{Ker}\pi_0 = \{h \in H:\ \pi_0(h) = hK = K\}$ так как K – единица в HK/K. Заметим, что $hK = K$ при $h \in H$ если и только если $h \in K$, т.е. $\operatorname{Ker}\pi_0 = H \cap K$. 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 $\overline{\pi}_0 : H/(H \cap K) \to HK/K$, определенное следующим образом $\overline{\pi}_0 : h(H \cap K) \mapsto \pi_0(h) = hK$ – изоморфизм $H/(H \cap K) \cong HK/K$. Для завершения доказательства теоремы остается заметить, что $f = \overline{\pi}_0^{-1}$. □

Установим еще один результат, который будет весьма полезен при анализе конкретных примеров. Для произвольной группы G обозначим через $\mathcal{S}(G)$ совокупность всех ее подгрупп, а через $\mathcal{S}(G, K)$, где K – некоторая подгруппа в G, совокупность всех подгрупп $H \subset G$ таких, что $K \subset H$.

Теорема 3.7 (теорема о соответствии)**.** *Пусть G – группа, $K \lhd G$ – ее нормальная подгруппа и пусть $\overline{G} = G/K$. Тогда*

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

(2) Если $H \in \mathcal{S}(G, K)$, 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 $H \in \mathcal{S}(G, K)$, т.е. $K \subset H \subset G$. Из определения G/K вытекает, что $\overline{H} = H/K$ – подгруппа в $\overline{G} = G/K$. Рассмотрим отображение $\pi^* : H \mapsto \overline{H}$. Проверим инъективность отображения π^*. Пусть $H_1 \in \mathcal{S}(G, K)$ и $H_2 \in \mathcal{S}(G, K)$ 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 $\overline{H} \in \mathcal{S}(\overline{G})$. 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 $K \subset H$.

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 $H \in \mathcal{S}(G, K)$ 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 $\pi : G \to G/K$ и $\overline{\pi} : \overline{G} \mapsto \overline{H}$, определенные соотношениями $\pi : g \to gK$ и $\overline{\pi} : \overline{g} \mapsto \overline{g}\overline{H}$, 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 $\operatorname{Ker}\psi$:

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

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 3.8. 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 $\chi : x \mapsto dx + n\mathbb{Z}$. 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, $\operatorname{Ker}\chi = m\mathbb{Z}$. Применяя теорему 3.5 (основную теорему о гомоморфизмах) получаем, что $\mathrm{Z}_m = \mathbb{Z}/m\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z}$. Далее, из теоремы 3.7 (о соответствии) вытекает, что $\mathrm{Z}_d = \mathbb{Z}/d\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})/(\mathbb{Z}/m\mathbb{Z}) = \mathrm{Z}_n/\mathrm{Z}_m$, т.е. $\mathrm{Z}_d \cong \mathrm{Z}_n/\mathrm{Z}_m$.

Заметим, что все подгруппы и факторгруппы циклической группы сами являются циклическими группами.

Пример 3.9. Рассмотрим группу S_4 и две ее подгруппы S_3 и *группу Клейна* V_4, которая равна

$$\mathrm{V}_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}.$$

В качестве *упражнения* проверить, что $\mathrm{V}_4 \lhd \mathrm{S}_4$. Так как $\mathrm{S}_3 \cap \mathrm{V}_4 = \{\mathrm{id}\}$, то, применяя теорему 3.6, получаем, что для подгруппы $H = \mathrm{S}_3\mathrm{V}_4 \subset \mathrm{S}_4$ справедливы следующие соотношения

$$H/\mathrm{V}_4 \cong \mathrm{S}_3/(\mathrm{S}_3 \cap \mathrm{V}_4) \cong \mathrm{S}_3.$$

По теореме Лагранжа, $|H| = |\mathrm{V}_4||\mathrm{S}_3| = 24$. Следовательно, $H = \mathrm{S}_4$. Таким образом, группа S_4 обладает подгруппой, изоморфной группе S_3 и факторгруппой, также изоморфной группе S_3.

Вычислим теперь множество $\mathcal{S}(\mathrm{S}_4, \mathrm{V}_4)$. Так как

$$\mathrm{S}_3 = \{\mathrm{id}, (12), (23), (13), (123), (132)\},$$

то, применяя Теорему 3.7, получаем, что

$$\mathcal{S}(\mathrm{S}_4, \mathrm{V}_4) = \{\mathrm{V}_4, \langle(12)\rangle\mathrm{V}_4, \langle(23)\rangle\mathrm{V}_4, \langle(13)\rangle\mathrm{V}_4, \langle(123)\rangle\mathrm{V}_4, \mathrm{S}_4\}$$

причем $\langle(123)\rangle\mathrm{V}_4 = \mathrm{A}_4$.

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.

3.5. Коммутант

Пусть G – некоторая группа. Напомним, что величина $[x, y] = xyx^{-1}y^{-1}$ называется коммутатором элементов x и y.

Заметим, что $[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$, т.е. величина, обратная к коммутатору двух произвольных элементов группы G, сама является коммутатором. Однако произведение коммутаторов $[x, y]$ и $[z, w]$ не обязано, в общем случае, быть коммутатором каких либо элементов группы G.

Определение. *Подгруппа G' группы G, порожденная множеством всех коммутаторов элементов из G, называется* коммутантом *группы G. Наряду с обозначением G' для коммутанта используется также обозначение $G^{(1)}$.*

Из определения коммутанта следует, что

$$G' = \{[x_1, y_1][x_2, y_2]\cdots[x_k, y_k] : \quad k \in \mathbb{Z}_+, \ x_1, \ldots, y_k \in G\}.$$

Пример 3.10. Вычислим коммутант группы S_n.

Для любых перестановок $\alpha \in \mathrm{S}_n$ и $\beta \in \mathrm{S}_n$ выражение $\alpha\beta\alpha^{-1}\beta^{-1}$ (равное коммутатору $[\alpha, \beta]$ перестановок α и β) является *четной перестановкой* (проверка этого простого факта оставляется в качестве *упражнения*). Следовательно, $\mathrm{S}'_n \subset \mathrm{A}_n$.

Пусть теперь $a, b, c \in \{1, \ldots, n\}$. Вычислим коммутатор двух транспозиций $\alpha = (ab)$ и $\beta = (ac)$:

$$[\alpha, \beta] = (ab)(ac)(ab)^{-1}(ac)^{-1} = (ab)(ac)(ab)(ac) = (abc).$$

Так как a, b и c – произвольные числа из $\{1, \ldots, n\}$, то всякий тройной цикл (abc) может быть записан в виде коммутатора пары транспозиций. Остается вспомнить, что тройные циклы порождают всю знакопеременную группу A_n. Итак, $\mathrm{S}'_n = \mathrm{A}_n$.

Упражнение. Проверить, что $\mathrm{A}'_4 = \mathrm{V}_4$ (группа Клейна).

Упражнение. Найти Q'_8.

Пусть теперь G и H – произвольные группы, а $f : G \to H$ – некоторый гомоморфизм. Так как

$$f([x, y]) = f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} = [f(x), f(y)]$$

для любых $x, y \in G$, то $f(G') \subset H'$. Более того, если f – эпиморфизм, то $f(G') = H'$.

Рассмотрим $K \lhd G$ – нормальную подгруппу в G. Пусть $\varphi \in \operatorname{Inn} G$ – произвольный внутренний автоморфизм группы G. Напомним, что $\operatorname{Inn} G = \{x \mapsto gxg^{-1} : \ g \in G\}$. При этом, так как K – нормальная подгруппа в G, то $\varphi_{|K}$ – эндоморфизм. Так как $\varphi(K') \subset K'$, то $K' \lhd G'$. Итак, нами установлен следующий важный факт:

Предложение 3.11. *Если K – нормальная подгруппа некоторой группы G, то коммутант K' является нормальной подгруппой соответствующего коммутанта G'.*

Теорема 3.12. *Если K – такая подгруппа группы G, что $G' \subset K$, то K – нормальная подгруппа в G. Факторгруппа G/G' – абелева. Для любой нормальной подгруппы K в G такой, что G/K – абелева группа, верно включение $G' \subset K$.*

Доказательство. Если $x \in K$, $g \in G$ и $G' \subset K$, то $gxg^{-1} = gxg^{-1}x^{-1}x = [g, x]x \in G'K = K$, так что $K \lhd G$. Вычислим теперь коммутатор произвольных двух смежных классов aK и bK в G/K:

$$[aK, bK] = aK \cdot bK \cdot (aK)^{-1} \cdot (bK)^{-1} = aba^{-1}b^{-1}K = [a, b]K \tag{3.1}$$

(так как K – нормальная подгруппа, то умножение смежных классов сводится к умножению представителей). Так как $G' \subset K$, то $[a, b]K = K$ и, следовательно, $[aK, bK] = K$. Так как K – единичный элемент в G/K, то G/K – абелева. Взяв теперь $K = G'$, получим второе утверждение нашей теоремы.

Пусть теперь $K \lhd G$ и пусть факторгруппа G/K – абелева. Тогда, прочитав цепочку равенств (3.1) от конца к началу, получим, что $[a, b]K = [aK, bK] = K$ для любых смежных классов aK и bK из G/K. А это в точности означает, что $[a, b] \in K$. Так как G' порождена всеми коммутаторами, то $G' \subset K$. □

Замечание. Интересно рассмотреть две, на первый взгляд совершенно независимые нормальные подгруппы, имеющиеся в любой группе G – ее центр $Z(G)$ (см. определение выше) и коммутант G'. Можно отметить следующую закономерность: чем “больше” центр группы, тем меньше ее коммутант и наоборот.

Задача 3.3. Доказать, что факторгруппа $G/Z(G)$ неабелевой группы G по ее центру $Z(G)$ не может быть циклической.

3.6. Разрешимые группы

Отталкиваясь от понятия коммутанта, рассмотрим следующую ситуацию. Пусть G – некоторая группа, G' – ее коммутант. Определим теперь второй коммутант $G^{(2)}$ группы G как коммутант $(G')'$ ее первого коммутанта G'. Действуя аналогичным образом, мы определим понятие коммутанта $G^{(k)}$ уровня k, $k \in N$, группы G следующим (индуктивным) образом: $G^{(k)} = (G^{(k-1)})'$. В результате возникает цепочка включений

$$G \rhd G' \rhd G^{(2)} \rhd \cdots \rhd G^{(m)} \rhd \cdots ,$$

которая может оборваться на каком-то конечном шаге m, $m \in \mathbb{N}$, или быть бесконечной (здесь, как и всегда, под включением понимается нестрогое включение, так что стабилизация цепочки вполне возможна). Под обрывом рассматриваемой цепочки включений понимается, естественно, ситуация, когда $G^{(m)} = \{1\}$. Наименьший индекс m, обладающей таким свойством, называется *уровнем разрешимости* группы G.

Пример 3.13. Любая абелева группа G такова, что $G' = \{1\}$. Следовательно, абелевы группы разрешимые уровня 1. В любой разрешимой группе уровня m существует абелева нормальная подгруппа – это подгруппа $G^{(m-1)}$. Как было вычислено выше, $\mathrm{S}_4' = \mathrm{A}_4$, $\mathrm{A}_4' = \mathrm{V}_4$, а $\mathrm{V}_4' = \{1\}$. Таким образом, группа S_4 разрешимая уровня 3, а группа A_4 – разрешимая уровня 2.

Упражнение. Доказать, что группа $\mathrm{T}_n(\mathbb{R})$ всех верхнетреугольных матриц из $\mathrm{GL}_n(\mathbb{R})$ является разрешимой.

Теорема 3.14. *Пусть G – некоторая группа, а $K \lhd G$ – ее нормальная подгруппа. Тогда G разрешима если и только если группы K и G/K разрешимы.*

Доказательство. Первым делом заметим, что если $H \subset G$, то $H' \subset G'$ и, следовательно, для любого $k \in \mathbb{N}$ справедливо включение $H^{(k)} \subset G^{(k)}$. Следовательно, любая подгруппа разрешимой группы разрешима.

Пусть теперь $K \lhd G$, а G – разрешимая группа. Пусть, как обычно, π – естественный гомоморфизм $G \to G/K$. Его ограничение на G' приводит к эпиморфизму $G' \to (G/K)'$ и, далее, к эпиморфизму $G^{(k)} \to (G/K)^{(k)}$. Из этого и из разрешимости G вытекает, что для некоторого $m \in \mathbb{N}$ (уровня разрешимости G, например) прообраз множества $(G/K)^{(m)}$ при соответствующем эпиморфизме – это множество $\{1\}$. Таким образом, G/K – разрешимая группа.

Проверим теперь обратное утверждение. Заметим, что

$$[g_1K, g_2K] = [g_1g_2]K$$

для любых $g_1, g_2 \in G$. Из этого равенства вытекает, что $(G/K)^{(\ell)} = G^{(\ell)}/K$. Пусть m – уровень разрешимости G/K, а n – уровень разрешимости K. Тогда

$$G^{(m)}/K = (G/K)^{(m)} = K$$

и, следовательно, $G^{(m)} \subset K$. А из этого уже вытекает, что $G^{(m+n)} \subset K^{(n)} = \{1\}$ и, следовательно, G – разрешимая группа. □

***Следствие* 3.15.** *Если $K_1 \lhd G$ и $K_2 \lhd G$ и если K_1 и K_2 разрешимые группы, то их произведение K_1K_2 также будем разрешимой группой.*

Этот факт непосредственно вытекает из только что доказанной теоремы и из соотношения

$$K_1K_2/K_1 \cong K_1/(K_1 \cap K_2).$$

Замечание. Произведение всех разрешимых нормальных подгрупп группы G будет максимальной разрешимой нормальной подгруппой $F(G)$ в G. При этом факторгруппа $G/F(G)$ не содержит разрешимых нормальных подгрупп.

3.7. Простые группы

Существуют нетривиальные группы, совпадающие со своим коммутантом. Такие группы не являются разрешимыми. На самом деле существуют (неабелевы) группы, в которых вообще нет собственных нетривиальных нормальных подгрупп (т.е. нормальных подгрупп, отличных от $\{1\}$ и от G).

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

В частности, коммутативная группа будет простой тогда и только тогда, когда она является циклической группой простого порядка (проверка этого простого факта оставляется в качестве ***упражнения***).

Существуют неабелевы простые группы, как конечные, так и бесконечные. Например, имеет место следующее утверждение:

Теорема 3.16. *Пусть $n \geqslant 5$ – натуральное число. Группа A_n – простая.*

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 $n \geqslant 5$. Заметим, что любая нормальная подгруппа H группы A_n, содержащая хотя бы один цикл длины 3, совпадает с 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 $H \lhd \mathrm{A}_n$, то $(pqr) \in H$. Таким образом, вместе с любым циклом длины 3 подгруппа $H \lhd \mathrm{A}_n$ содержит ***все*** циклы длины 3 и, следовательно, совпадает с A_n.

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.

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

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

где $\tau \in \mathrm{S}_n$ – некоторая перестановка. Рассмотрим цикл $\alpha = (abc)$ длины 3. Так как $\alpha \in \mathrm{A}_n$, а $H \lhd \mathrm{A}_n$, то $\widetilde{\sigma} := \alpha\sigma\alpha^{-1} \in H$. Прямое вычисление показывает, что $\widetilde{\sigma} = (bcad \ldots z)\tau$. Наконец, $\widetilde{\sigma}\sigma^{-1} \in H$, а

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

Таким образом, H содержит цикл (abd) длины 3 и, по ранее доказанному, $H = \mathrm{A}_n$.

Пусть теперь все циклы, входящие в разложение элемента $\sigma \in H$ имеют длину 2 или 3. 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 $H = \mathrm{A}_n$.

Предположим теперь, что в разложении рассматриваемой перестановки σ содержаться 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.

Таким образом, любая перестановка $\sigma \in H$ 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, как было показано выше, группа Клейна V_4). Таким образом, условие $n \geqslant 5$ в Теореме 3.16 является существенным.

Теорема 3.16 показывает, что существует бесконечно много простых неабелевых конечных групп. Такие группы, впрочем, далеко не исчерпываются знакопеременными. Заметим также, что в приведенном доказательстве Теоремы 3.16 нигде не использовалась конечность группы A_n. Можно определить и счетную знакопеременную группу и, более того, знакопеременные группы любой бесконечной мощности и рассуждая аналогично установить, что все они будут простыми.

Задача 3.4. Доказать, что группа $\mathrm{SO}(3)$ – простая.

3.8. Действие групп на множествах

Определение действия групп на множествах. Напомним, что если Ω – множество произвольной природы, то через $\mathfrak{T}^*(\Omega)$ мы обозначали совокупность всех биективных отображений множества Ω в себя. Применительно к некоторой группе G нас интересует вполне естественный вопрос – а нельзя ли интерпретировать G как некоторую подгруппу группы $\mathfrak{T}^*(\Omega)$ в случае разумно выбранного множества Ω. При этом под возможностью соответствующей интерпретации мы будем понимать существование гомоморфизма $\Phi : G \to \mathfrak{T}^*(\Omega)$. Так как Φ – гомоморфизм, то $\Phi_1 = \mathrm{id}_\Omega$, где $1 = 1_G$ – единица группы G и $\Phi_{fg} = \Phi_f \circ \Phi_g$ для любых $f, g \in G$. Часто образ $\Phi_g(x) \in \Omega$ точки $x \in \Omega$ при отображении Φ_g, соответствующем элементу $g \in G$ обозначается просто gx. Другими словами, в рассматриваемой ситуации определено отображение $(g, x) \mapsto gx$ множества $G \times \Omega \to \Omega$, для которого выполнены следующие свойства:

(1) $1x = x$ для любого $x \in \Omega$;

(2) $(fg)x = f(gx)$ для любого $x \in \Omega$ и для любых $f, g \in G$.

Исходя из этого естественно сформулировать следующее определение.

Определение. *Если задано отображение $(g, x) \mapsto gx$ из $G \times \Omega$ в Ω, удовлетворяющее свойствам (1) и (2), то говорят, что группа G действует (слева) на множестве Ω. Само множество Ω в таком случае называют G-множеством.*

Если Ω – некоторое G-множество, а $g \in G$, то мы можем определить отображение $\Phi_g : \Omega \to \Omega$ по правилу $\Phi_g(x) = gx$. В этом случае условия (1) и (2) означают, что отображение $g \mapsto \Phi_g$ будет гомоморфизмом из G в $\mathfrak{T}^*(\Omega)$. Ядро $\operatorname{Ker}\Phi$ этого гомоморфизма Φ называют *ядром действия группы* G. Если Φ – мономорфизм (т.е., если из того, что $gx = x$ для любого $x \in \Omega$, вытекает, что $g = 1$), то говорят, что группа G действует на Ω *эффективно*.

Если G действует на Ω, то для любого натурального m можно определить действие группы G на множестве $\Omega \times \cdots \times \Omega$ (всего m сомножителей) по правилу $g(x_1, \ldots, x_m) = (gx_1, \ldots, gx_m)$.

Интересный пример получается, если рассмотреть действие группы G на множестве $\mathfrak{S}(\Omega)$ всех подмножеств Ω. Чтобы определить это действие, положим $g\varnothing = \varnothing$ для любого $g \in G$ и $g\Omega_1 = \{gx : \ x \in \Omega_1\}$ для любого $\Omega_1 \subset \Omega$.

Орбиты и стационарные подгруппы точек. Пусть группа G действует на множестве Ω.

Определение. *Скажем, что две точки $x, y \in \Omega$ G-эквивалентны, если существует такой элемент $g \in G$, что $y = gx$. Факт G-эквивалентности точек x и y будем записывать $x \sim_G y$.*

Упражнение. Проверить, что отношение $\sim_G$ на Ω является отношением эквивалентности, т.е. рефлексивным, симметричным и транзитивным бинарным отношением.

В соответствии с общей идеей факторизации, множество Ω распадается на непересекающиеся классы эквивалентности по отношению $\sim_G$.

Определение. *Классы эквивалентности, на которые распадается Ω то отношению $\sim_G$, называются G-орбитами. G-орбита, содержащая заданную точку $x \in \Omega$ обозначается $G(x)$.*

По определению, $G(x) = \{gx : \ g \in G\}$. Если из контекста ясно, о какой группе идет речь, то вместо термина "G-орбита" будем использовать более короткий термин "орбита".

Выберем точку $x \in \Omega$ и рассмотрим множество

$$\mathrm{St}(x) = \mathrm{St}_G(x) = \{g \in G : \ gx = x\}.$$

Заметим, что $1x = x$ и, следовательно, $1 \in \mathrm{St}(x)$. Далее, если $g_1 \in \mathrm{St}(x)$ и $g_2 \in \mathrm{St}(x)$, то $(g_1g_2)x = g_1(g_2x) = g_1x = x$, т.е. $g_1g_2 \in \mathrm{St}(x)$. Итак, $\mathrm{St}(x)$ – подгруппа в G.

Определение. *Подгруппа $\mathrm{St}(x)$ группы G называется стабилизатором в G точки $x \in \Omega$. Также $\mathrm{St}(x)$ называется стационарной подгруппой точки $x \in \Omega$.*

Пример 3.17. Пусть $G = \mathrm{SO}(2)$, а $\Omega = \mathbb{R}^2$. Напомним, что любой поворот в плоскости $\mathbb{R}^2$ относительно начала координат задается матрицей $A \in \mathrm{SO}(2)$. При этом орбитой любой точки $\boldsymbol{x} \in \mathbb{R}^2 \setminus \{0\}$ будет окружность с центром в начале координат, проходящая через точку $\boldsymbol{x}$. Орбитой 0 будет $\{0\}$. При таком определении действия группы $\mathrm{SO}(2)$ на $\mathbb{R}^2$ стационарные подгруппы любых точек $x \in \mathbb{R}^2 \setminus \{0\}$ равны $\{1\}$, а стационарная подгруппа нуля совпадает со всей группой $\mathrm{SO}(2)$.

Заметим теперь, что если $x \in \Omega$, а $g_1, g_2 \in G$, то $g_1x = g_2x$ если и только если $g_1^{-1}g_2 \in \mathrm{St}(x)$. А это эквивалентно тому, что $g_2 \in g_1 \mathrm{St}(x)$. Таким образом, левые смежные классы группы G по стационарной подгруппе $\mathrm{St}(x)$ находятся в биективном соответствии с точками орбиты $G(x)$. В частности,

$$|G(x)| = |G/\mathrm{St}(x)| = (G : \mathrm{St}(x)), \tag{3.2}$$

где, как обычно, $G/\mathrm{St}(x)$ – фактормножество G по $\mathrm{St}(x)$, а $(G : \mathrm{St}(x)$ – индекс подгруппы $\mathrm{St}(x)$ в G. Величину $|G(x)|$ естественно называть *длиной G-орбиты* точки x.

Замечание. Из теоремы Лагранжа вытекает, что если G – конечная группа, то длина G-орбиты любой точки $x \in \Omega$ делит порядок группы G.

Нетрудно проверить, что для любой точки $x_1 \in G(x)$ верны следующие равенства

$$|G(x)| = |G(x_1)| = (G : \mathrm{St}(x_1)).$$

Пусть теперь $y = gx$ при $g \in G$ и $x \in \Omega$. В этом случае для любого $h \in \mathrm{St}(y)$ верны равенства $hgx = hy = y = gx$, т.е. $g^{-1}hgx = x$. Из этого вытекает, что $g^{-1}\mathrm{St}(y)g \subset \mathrm{St}(x)$. Аналогично $gfg^{-1}y = y$ для любого $f \in \mathrm{St}(x)$ и, следовательно, $g\,\mathrm{St}(x)g^{-1} \subset \mathrm{St}(y)$. Из этого вытекает, что

$$\mathrm{St}(y) = g\,\mathrm{St}(x)g^{-1},$$

т.е. стационарные подгруппы точек одной орбиты *сопряжены*. Итак, доказано

Предложение 3.18. *Если группа G действует на множестве Ω и если две точки $x, y \in \Omega$ принадлежат одной G-орбите, то их стационарные подгруппы сопряжены.*

Если, дополнительно, группа G – конечна и $\Omega = \Omega_1 \cup \cdots \cup \Omega_m$ – разбиение Ω на конечное число орбит с представителями $x_1, \ldots, x_m$, то

$$|\Omega| = \sum_{k=1}^{m} (G : \mathrm{St}(x_k)). \tag{3.3}$$

3.9. Примеры действий групп

Рассмотрим два примера действий групп, которые будут активно применяться в дальнейшем.

Действие группы сопряжениями. Пусть G – группа и пусть $\Omega = G$. Тогда действие группы G на себе можно определить соотношением $h \mapsto I_g(h) = ghg^{-1}$. В этом случае говорят, что G действует на себе *сопряжениями*. Множество

$$Z(G) = \{z \in G : \ I_g(z) = z \text{ для любого } g \in G\} = \{z \in G : \ zg = gz \text{ для любого } g \in G\}$$

– ядро действия сопряжениями, называется *центром* группы G.

Орбита элемента $x \in G$ относительно такого действия группы G на себе называется *сопряженным классом*, содержащим x и обозначается x^G.

Имеет место следующее полезное свойство нормальных подгрупп:

Предложение 3.19. *Любая нормальная подгруппа K группы G является объединением некоторого числа сопряженных классов группы G.*

Доказательство. Если $x \in K \lhd G$, то для любого $g \in G$ имеет место включение $gxg^{-1} \in K$. Таким образом, вместе с любым элементом $x \in K$ в K содержится вся орбита x^G элемента x. Следовательно $K = \bigcup_x x^G = \bigcup_{j \in J} x_j^G$ для некоторого множества индексов J. □

И, наконец, стационарная подгруппа $\mathrm{St}_G(x)$ элемента $x \in G$ при действии группы G на себе сопряжениями называется *централизатором* элемента x и обозначается $C(x)$ или $C_G(x)$.

Введем еще одно важное понятие, связанное с действием группы на себе сопряжениями. Пусть $H \subset G$ – некоторая подгруппа группы G. Тогда

$$N(H) = N_G(H) = \mathrm{St}(H) = \{g \in G : \ gHg^{-1} = H\}$$

называется *нормализатором* H в G. Если H – нормальная подгруппа, то $N(H) = G$.

Рассмотрев действие группы G на множестве $\mathfrak{S}(G)$ сопряжениями (при таком действии множеству $Y \in \mathfrak{S}(G)$ ставится в соответствие множество $gYg^{-1} = \{gyg^{-1} : \ y \in Y\}$) и применив равенство (3.3) получим, что число $|H^G|$ подгрупп группы G, сопряженных с подгруппой $H \subset G$ равно индексу $(G : N(H))$ нормализатора $N(H)$ в G.

Рассмотрим конечную группу G. Пусть $x_1^G, \ldots, x_m^G$, $m \in \mathbb{N}$, – все сопряженные классы группы G. Предположим, что первые k, $k \leqslant m$, классов среди них тривиальные, т.е. $x_j^G = \{x_j\}$, $j = 1, \ldots, k$. Тогда $Z(G) = \{x_1, \ldots, x_k\}$, а соотношения (3.2) и (3.3) имеют вид

$$|x_j^G| = (G : C(x_j)), \quad j = 1, \ldots, k, k+1, \ldots, m$$

и, соответственно,

$$|G| = |Z(G)| + \sum_{j=k+1}^{m} (G : C(x_j)). \tag{3.4}$$

Рассмотрим пример группы $G = \mathrm{S}_3$. В этом случае $m = 3$, $k = 1$ (откуда, в частности, вытекает, что $Z(\mathrm{S}_3) = \{1\}$) и

$$\mathrm{S}_3 = \{\mathrm{id}\} \cup \{(12), (23), (13)\} \cup \{(123), (132)\}$$

– разбиение S_3 на сопряженные классы.

Определение. *Если p – простое число, то любая конечная группа G порядка $|G| = p^n$, $n \in \mathbb{N}$, называется p-группой. В этом случае используется также термин примарная группа.*

Из формулы (3.4) непосредственно вытекает следующее утверждение.

Предложение 3.20. *Всякая p-группа G имеет нетривиальный центр $Z(G)$.*

Доказательство. В самом деле, если G – абелева группа, то $Z(G) = G$ и наше утверждение верно. Если G не является абелевой, то в соотношении (3.4) обязательно $m > k$. Далее, $(G : C(x_j)) = p^{n_j}$ при $j = k+1, \dots, m$, где $n_j \geqslant 1$ – целые числа. Из формулы (3.4) вытекает, что

$$p^n = |Z(G)| + \sum_{j=k+1}^{m} p^{n_j},$$

откуда вытекает, что $|Z(g)|$ делится на p. □

Пример 3.21. Группа

$$P = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : \ a, b, c \in \mathrm{Z}_p \right\},$$

где p – простое число, Z_p – поле из p элементов, является p-группой. Проверка оставляется в качестве *упражнения*.

Действие группы левыми сдвигами. Пусть G – группа, а $a \in G$ – некоторый ее элемент. Отображение $L_a : G \to G$, определенное соотношением $L_a(g) = ag$ уже использовалось нами раньше, например, при доказательстве теоремы Кэли. Это отображение называется *левым сдвигом* на a.

Заметим, что $L_e(g) = g$ и $L_{ab}(g) = (ab)g = a(bg) = L_a(L_b(g))$. Таким образом, левые сдвиги задают действие группы G на себе. Это действие естественным образом индуцирует действие группы G на подмножествах G.

Пусть $H \subset G$ – подгруппа группы G, а G/H – соответствующее множество смежных классов $\{gH : \ g \in G\}$. Легко проверить (это необходимо сделать в качестве *упражнения*), что отображение

$$x \circ gH := x(gH) = (xg)H$$

задает действие L^H группы G на множестве G/H. Найдем ядро этого действия:

$$\operatorname{Ker} L^H = \{x \in G : \ L^H_x(gH) = gH, \ \forall g \in G\} = \{x \in G : \ xgH = gh, \ \forall g \in G\},$$

т.е. $x \in \operatorname{Ker} L^H$ если и только если $g^{-1}xg \in H$ или, эквивалентно, $x \in gHg^{-1}$ для всех $g \in G$. Отсюда

$$\operatorname{Ker} L^H = \bigcap_{g \in G} gHg^{-1}$$

– максимальная нормальная подгруппа группы G, содержащаяся в H. При этом эффективность действия G на G/H равносильна отсутствию нетривиальной подгруппы $K \subset H$, нормальной в G.

РАЗДЕЛ 4

Строение групп

В разделе 3.3 выше были получены результаты о строении групп малых порядков. Так, было показано, что существуют ровно две (с точностью до изоморфизма) группы порядка 6 – это группы Z_6 и S_3. Установленное в разделе 3.1 следствие теоремы Лагранжа утверждает, что группа простого порядка всегда циклическая и, с точностью до изоморфизма, единственная. В этом разделе мы установим ряд общих результатов о строении групп.

4.1. Силовские подгруппы. Теоремы Силова

Пусть G – конечная группа и пусть число d – один из делителей порядка $|G|$ этой группы. Естественным образом возникает следующий вопрос: существует ли подгруппа группы G порядка d? Как отмечалось выше, ответ на этот вопрос в общем случае отрицательный: группа A_4 порядка 12 не содержит подгруппы порядка 6. Приведем еще один пример. Как было показано выше, любая подгруппа $H \subset G$ такая, что $(G : H) = 2$ нормальна. Следовательно, в неабелевой простой группе не может быть подгрупп индекса 2. Так, например, в группе A_5 порядка 60 нет подгрупп порядка 30.

Упражнение. Проверить, что в группе A_5 нет подгрупп порядка 15 и 20.

Следующий пример показывает, в каких случаях возможны положительные ответы на поставленный выше вопрос. Группа S_4 имеет порядок 24. Среди делителей числа 24 выделим числа 8 и 3 (смысл такого выделения будет понятен несколько позднее) и заметим, что в S_4 есть подгруппы порядка 8, например, $\langle (12) \rangle \mathrm{V}_4$ или $\langle (1234), (13) \rangle \cong \mathrm{D}_4$ и подгруппы порядка 3, например, $\langle (123) \rangle$.

Определение. *Пусть G – конечная группа порядка $|G| = p^n q$, где p – простое число, $n \in \mathbb{N}$, а $q \in \mathbb{N}$ такое, что* $\mathrm{НОД}(p, q) = 1$.

Подгруппа $P \subset G$ группы G порядка $|P| = p^n$ (если такая существует), называется силовской p-подгруппой *группы G.*

Таким образом, в группе S_4 существуют силовские 2-подгруппы и 3-подгруппы.

Определение. *Обозначим через $\nu_p(G)$ число силовских p-подгрупп группы G.*

Теорема 4.1. *Пусть G – конечная группа порядка $|G| = p^n q$, где p – простое число, $n \in \mathbb{N}$, а $q \in \mathbb{N}$ такое, что* $\mathrm{НОД}(p, q) = 1$.

1 (первая теорема Силова). *Силовские p-подгруппы существуют.*

2 (вторая теорема Силова). *Пусть P_1 и P_2 – две силовские p-подгруппы группы G. Тогда существует $g \in G$ такой, что $P_2 = gP_1g^{-1}$. Другими словами, все силовские p-подгруппы группы G сопряжены.*

3 (третья теорема Силова). *$\nu_p(G) = (G : N(P))$, где P – силовская p-подгруппа группы G, а $N(P)$ – ее нормализатор. Кроме того, $\nu_p(G) \equiv 1 \pmod{p}$.*

Доказательство. Доказательство первой теоремы Силова мы начнем с проверки следующего факта:

***Лемма* 4.2.** *Пусть G – абелева группа, $|G| < \infty$, а p – такое простое число p, что $p \mid |G|$. Тогда в G существует подгруппа порядка p.*

Доказательство. Пусть n – показатель группы G (напомним, что число $n > 0$ называется *показателем* группы G, если $g^n = 1$ для любого $g \in G$). Проверим, что существует такое целое число k, что $|G| \mid n^k$. Для этого воспользуемся индукцией по величине порядка группы. Рассмотрим произвольный элемент $g \in G$, $g \neq 1$ и соответствующую циклическую подгруппу $H = \langle g \rangle$ группы G. Так как $g^n = 1$, то $|H| \mid n$ и, следовательно, $n = |H|x$, где $x \in \mathbb{Z}$. Так как n является показателем и для факторгруппы G/H, то, согласно предположению индукции, существует такое цело число k_1, что $|G/H| \mid n^{k_1}$. Другими словами, $n^{k_1} = |G/H|y$, при $y \in \mathbb{Z}$, откуда

$$|G|xy = y|G/H|x|H| = n^{k_1}n = n^{k_1+1}.$$

Пусть теперь порядок группы G делится на . В силу только что доказанного в G существует элемент g, период которого делится на . Пусть этот период равен ps, где s – некоторое целое число. Тогда $g^s \neq 1$ и, очевидно, элемент g^s имеет период p и порождает подгруппу порядка , что и требовалось доказать. □

Перейдем непосредственно к доказательство первой теоремы Силова. Как и при доказательстве Леммы 4.2 будем рассуждать по индукции по порядку группы G.

Если порядок группы G простой, то требуемое утверждение очевидно. Предположим теперь, что первая теорема Силова доказана для всех групп, порядок которых меньше порядка группы G. Если в G имеется собственная подгруппа , индекс которой взаимно прост с p, то силовская p-подгруппа группы H (она существует по предположению индукции) будет также силовской p-подгруппой в группе G.

Предположим теперь, что у всякой собственной подгруппы группы G индекс делится на p. Пусть теперь группа G действует на себе сопряжениями. Из формулы (3.4) получаем, что $|G| = |Z(G)| + \sum(G : C(x_j))$, где последняя сумма берется по всем нетривиальным сопряженным классам группы G. В силу сделанного предположения, каждое слагаемое в этой сумме делится на p. Так как $p \mid |G|$, то $p \mid |Z(G)|$ и, следовательно, группа G имеет нетривиальный центр $Z(G)$.

Из Леммы 4.2 вытекает, что в группе $Z(G)$ найдется циклическая подгруппа H, порожденная элементов порядка p. При этом H – нормальная подгруппа в $Z(G)$ и, следовательно, в G. Рассмотрим естественное отображение $\pi : G \to G/H$. Если p^m – наибольшая степень p, делящая $|G|$, то $p^{m-1} \mid |G/H|$. По предположению индукции в группе G/H существует силовская p-подгруппа K. Заметим, что $\pi^{-1}(K)/H \cong K$ и группа $\pi^{-1}(K)$ имеет порядок $p^{m-1}p = p^m$. Таким образом, $\pi^{-1}(K)$ – силовская p-подгруппа в G.

Докажем вторую теоремы Силова. Пусть P – силовская p-подгруппа группы G и пусть P_1 – произвольная p-подгруппа группы G, т.е. подгруппа порядка p^k, где $k \leqslant n$ – натуральное число (т.е. P_1 не обязательно силовская подгруппа). Рассмотрим действие группы G левыми сдвигами на множестве G/P смежных классов группы G по P и его ограничение на подгруппу P_1. Так как длина любой орбиты относительно этого действия делит порядок группы P_1, равный p^k (где $k \leqslant n$), то верны следующие равенства

$$q = p^n q/p^n = |G|/|P| = |G/P| = p^{k_1} + p^{k_2} + \cdots,$$

где последняя сумма берется по всем орбитам относительно описанного действия группы P_1. Так так

$$q = p^{k_1} + p^{k_2} + \cdots$$

и, так как $\text{НОД}(p, q) = 1$, то одно из слагаемых p^{k_j} равно 1. Соответствующая орбита имеет вид $P_1 \cdot gP = gP$ при $g \in G$, откуда получаем, что $P_1 \cdot gPg^{-1} = gPg^{-1}$. Следовательно, $P_1 \subset gPg^{-1}$. Если теперь P_1 – силовская p-подгруппа группы G, то $|P_1| = |P|$ и, окончательно, $P_1 = gPg^{-1}$.

Перейдем к доказательству третьей теоремы Силова. Рассмотрим действие группы G сопряжениями на множестве $\Sigma_p(G)$ всех силовских p-подгрупп группы G. Так как все силовские p-подгруппы группы G сопряжены, то на основании формулы (3.3) получаем

$\nu_p(G) = |\Sigma_p(G)| = (G : \mathrm{St}(P))$, где P – произвольная силовская p-подгруппа группы G. Остается заметить, что $\mathrm{St}(P) = N(P)$.

Установим теперь, что $\nu_p(G) \equiv 1 \pmod p$. Представим порядок группы G в виде $|G| = p^m t$, где $m \leqslant n$, а натуральное число t может делиться на p. Пусть $\nu_p^m(G)$ – число всех подгрупп порядка p^m в G. Мы докажем, что $\nu_p^m(G) \equiv 1 \pmod p$. Из этого будет, в частности, следовать существование подгрупп любого порядка p^m в G при $m = 1, \ldots, n$ и, при $m = n$, требуемое соотношение $\nu_p(G) \equiv 1 \pmod p$. Пусть $\ell = p^m$.

Действие группы G на себе левыми сдвигами индуцирует соответствующее действие группы G на множестве Ω всех ℓ-элементных подмножеств $M = \{g_1, \ldots, g_\ell\}$ группы G. Напомним, что $g \cdot M = g \cdot \{g_1, \ldots, g_\ell\} = \{gg_1, \ldots, gg_\ell\}$. При этом множество Ω распадается на орбиты относительно рассматриваемого действия, т.е. $\Omega = \bigcup_{j\in J} \Omega_j$ и $|\Omega| = \sum_{j\in J} |\Omega_j|$, где $|\Omega_j| = (G : G_j)$, а $G_j = \{g \in G : \ gM_j = M_j\}$ стационарная группа некоторого представителя $M_j \in \Omega_j$, $j \in J$.

Так как $G_jM_j = M_j$, то множество $M_j = \bigcup_{s=1}^{k_j} G_j g_{js}$ является объединением некоторого числа правых смежных классов группы G по подгруппе G_j. Из этого следует, что $p^m = |M_j| = k_j|G_j|$ и, соответственно, что $|G_j| = p^{m_j} \leqslant p^m$. Если $|G_j| < p^m$, то $|\Omega_j| = p^{m-m_j}t$, откуда видно, что $|\Omega_j| \equiv 0 \pmod{pt}$. Заметим также, что равенства $|G_j| = p^m$ и $|\Omega_j| = t$ эквивалентны. Таким образом

$$|\Omega| \equiv \sum_{j:\ |\Omega_j|=t} |\Omega_j| \pmod{pt}.$$

Так как $|\Omega| = C^\ell_{|G|}$, то

$$C^\ell_{|G|} \equiv \sum_{j:\ |\Omega_j|=t} |\Omega_j| \pmod{pt}. \tag{4.1}$$

Пусть теперь индекс j таков, что $|\Omega_j| = t$. Тогда $|G_j| = p^m$ и, следовательно, $M_j = G_j a_j$, где a_j – некоторый элемент группы G. Таким образом, $a_j^{-1}M_j = a_j^{-1}G_j a_j$ – подгруппы порядка p^m. Обозначим эту подгруппу символом P_j. Орбита Ω_j состоит из некоторого числа левых смежных классов gP_j группы G по P_j.

Пусть теперь $H \subset G$ – подгруппа порядка p^m. Возникает орбита $\Omega_H = \{gH : \ g \in G\}$ длины t. Проверим, что если H_1 и H_2 – две различные подгруппы группы G порядка $|H_1| = |H_2| = p^m$, то орбиты Ω_{H_1} и Ω_{H_2} также различны. В самом деле, из равенства $H_1 = gH_2$ вытекает, что $1 = gh_2$, где $g \in G$ и $h_2 \in H_2$, откуда $g = h_2^{-1} \in H_2$ и, следовательно, $H_1 = H_2$.

Таким образом между подгруппами порядка p^m и орбитами Ω_j длины t имеется взаимно-однозначное соответствие. Другими словами число $\nu_p^m(G)$ равно числу орбит длины t при рассматриваемом действии группы G на множестве Ω. Следовательно, сравнение (4.1) можно переписать в виде

$$C^\ell_{|G|} \equiv t\nu_p^m(G) \pmod{pt}. \tag{4.2}$$

В специальном частном случае, когда G – циклическая группа порядка $|G| = p^m t$ из Предложения 2.11 и из замечания после него вытекает, что $\nu_p^m(G) = 1$. В этом случае сравнение (4.1) имеем вид

$$C^\ell_{|G|} \equiv t \pmod{pt}. \tag{4.3}$$

Так как левые части сравнений (4.2) и (4.3) одинаковы и не зависят от природы группы G, то $t \equiv t\nu_p^m(G) \pmod{pt}$ и, окончательно, $\nu_p^m(G) \equiv 1 \pmod{pt}$. □

Упражнение. Пусть p – простое число. Проверить, что $|\mathrm{SL}_2(\mathrm{Z}_p)| = p(p^2 - 1)$ и установить, что множества

$$P := \left\{ \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} : \ z \in \mathrm{Z}_p \right\} \qquad \text{и} \quad \widetilde{P} := \left\{ \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} : \ z \in \mathrm{Z}_p \right\}$$

являются силовскими p-подгруппами группы $\mathrm{SL}_2(\mathrm{Z}_p)$.

Замечание. *Силовская p-подгруппа P конечной группы G нормальна в G в том и только том случае, когда $\nu_p(G) = 1$.*

В самом деле, согласно второй теореме Силова, все силовские p-подгруппы, отвечающие одному и тому же простому делителю p порядка $|G|$ группы G взаимно сопряжены. Пусть P – такая подгруппа. Тогда $\nu_p(G) = 1$ если и только если $xPx^{-1} = P$ для любого $x \in G$. А это в точности условие нормальности $P \lhd G$.

Следующее утверждение представляет собой полезное уточнение теорем Силова.

Теорема 4.3. *Пусть G – конечная группа. Если $|G| = p_1^{k_1} \cdots p_m^{k_m}$, где $p_1, \ldots, p_m$ – простые, а $k_1, \ldots, k_m$ – натуральные числа, то G является прямым произведением своих силовских p_j-подгрупп P_j, $j = 1, \ldots, m$ если и только если $P_j \lhd G$ для любого $j = 1, \ldots, m$.*

Доказательство. Если $P_1 \times \cdots \times P_m = G$ – прямое произведение, то всякая подгруппа P_j нормальна в G как прямой сомножитель (см. замечание в конце раздела 2.6).

Предположим теперь, что $P_j \lhd G$ при $j = 1, \ldots, m$. При этом $\nu_{p_j}(G) = 1$. Заметим, что при $j \neq \ell$, $j, \ell = 1, \ldots, m$ подгруппы P_j и P_ℓ имеют тривиальное пересечение. В самом деле, если $x \in P_j \cap P_\ell$, то найдутся такие числа σ и τ, что $x^{p_j^\sigma} = x^{p_\ell^\tau} = 1$, а из взаимной простоты p_j и p_ℓ вытекает, что $x = 1$. Далее, аналогично тому, как это было проделано при доказательстве Теоремы 2.21, устанавливается, что элементы $x_j \in P_j$ и $x_\ell \in P_\ell$ коммутируют.

Предположим, что $1 = y_1 y_2 \cdots y_m$, где $y_j \in P_j$ – элемент порядка $a_j = p_j^{\alpha_j}$. Пусть $a = \prod_{\ell \neq j} a_\ell$. Так как элементы $y_1, \ldots, y_m$ коммутируют, то $1 = (y_1 y_2 \cdots y_m)^a = y_j^a$. Из взаимной простоты a и a_j и из того, что $y_j^a = y_j^{a_j} = 1$ вытекает, что $y_j = 1$. Таким образом $y_1 \cdots y_m = 1$ если и только если $y_1 = \cdots = y_m = 1$.

Пусть $x \in G$ – элемент порядка $r = r_1 \cdots r_m$, где $r_j = p_j^{\alpha_j}$. Найдем представление x в виде $x = x_1 x_2 \cdots x_m$, где $|\langle x_j \rangle| = r_j$. Положим $r'_j = r/r_j$, определим числа $t_1, \ldots, t_m$ из соотношения

$$1 = r'_1 t_1 + r'_2 t_2 + \cdots + r'_m t_m$$

и, наконец, определим $x_j = x^{t_j r'_j}$. Если $x = x'_1 x'_2 \cdots x'_m$ – другая запись x рассматриваемого вида, то из равенства $1 = xx^{-1}$ и перестановочности элементов $x_1, \ldots, x_m$ вытекает, что $(x'_1 x_1^{-1}) \cdots (x'_m x_m^{-1}) = 1$ и, следовательно, $x'_j x_j^{-1} = 1$, т.е. $x'_j = x_j$. Так как любой элемент G единственным образом разложен в произведение элементов из попарно непересекающихся нормальных подгрупп $P_1, \ldots, P_m$, то $G = P_1 \times \cdots \times P_m$. □

В завершении заметим, что нормальные силовские p-подгруппы группы G инвариантны относительно любого автоморфизма $\varphi \in \operatorname{Aut} G$. В самом деле, $|\varphi(P)| = |P|$, откуда $\varphi(P)$ – силовская p-подгруппа, а так как P – нормальна, то $\nu_p(G) = 1$.

4.2. Строение групп порядка 12 и 15

Применяя теоремы Силова, выясним, как устроены группы порядка 12 и 15.

Предложение 4.4. *Если $|G| = 15$, то $G \cong \mathrm{Z}_3 \times \mathrm{Z}_5$.*

Доказательство. В силу первой теоремы Силова в группе G есть силовская 3-подгруппа H_3 и силовская 5-подгруппа H_5. Так как $|H_3| = 3$, то $H_3 \cong \mathrm{Z}_3$, а так как $|H_5| = 5$, то $H_5 \cong \mathrm{Z}_5$. Далее, так как число $\nu_3(G)$ делит 15 и $\nu_3(G) \equiv 1 \pmod 3$, то $\nu_3(G) = 1$. Аналогично $\nu_5(G) = 1$. Следовательно, $H_3 \lhd G$ и $H_5 \lhd G$. Далее, так как $\mathrm{НОД}(|H_3|, |H_5|) = 1$, то $H_3 \cap H_5 = \{1\}$.

Проверим, что каждый элемент произведения $H_3 H_5$ представляется в виде xy, где $x \in H_3$, а $y \in H_5$ единственным образом. В самом деле, если $x_1 y_1 = x_2 y_2$ при $x_1, x_2 \in H_3$ и $y_1, y_2 \in H_5$, то $x_2^{-1} x_1 = y_2 y_1^{-1}$. Левое выражение в этом равенстве – это элемент H_3, а правое – элемент H_5. Следовательно, $x_2^{-1} x_1 = 1$ и $y_2 y_1^{-1} = 1$. Таким образом, $G = H_3 H_5$. Применяя Теорему 2.21 получаем, что $G \cong H_3 \times H_5$. □

Предложение 4.5. *Если G – некоммутативная группа порядка 12, то G изоморфна одной из трех следующих групп A_4, D_6 или $\widehat{\mathrm{S}}_3$ (которая будет описана ниже).*

Доказательство. В группе G существуют силовские 2-подгруппы (они имеют порядок 4 и являются коммутативными) и силовские 3-подгруппы (они имеют порядок 3 и также являются коммутативными).

Итак, пусть H – некоторая силовская 3-подгруппа группы G, а K – ее силовская 2-подгруппа. Аналогично тому, как это было сделано в доказательстве Предложения 4.4, проверяется, что $G = HK$.

Выясним, чему могут равняться числа $\nu_2(G)$ и $\nu_3(G)$ силовских 2- и 3-подгрупп соответственно. Если $\nu_2(G) = \nu_3(G) = 1$, то подгруппы H и K будут нормальны. Применяя Теорему 2.21 (аналогично доказательству Предложения 4.4) получаем, что $G \cong H \times K$. Так как элементы подгрупп H и K взаимно коммутируют (этот факт был доказан при доказательстве Теоремы 2.21), то группа G будет коммутативной.

Итак, хотя бы одно из чисел $\nu_2(G)$ и $\nu_3(G)$ будет больше единицы. Пусть $\nu_3(G) > 1$. Тогда из третьей теоремы Силова вытекает, что $\nu_3(G) = 4$. Проверим, что в этом случае $\nu_2(G) = 1$. В самом деле, различные подгруппы порядка 3 могут иметь только тривиальное пересечение (проверка этого простого факта оставляется в качестве *упражнения*). Таким образом, в объединении $\widehat{H}$ четырех силовских 3-подгрупп будет 9 элементов. Рассмотрим оставшиеся не единичные элементы k_1, k_2 и k_3 группы G. Ясно, что элементы $\{1, k_1, k_2, k_3\}$ образуют подгруппу K. В силу второй теоремы Силова множестве $\widehat{H}$ инвариантно относительно сопряжения. Следовательно, подгруппа K также инвариантна относительно сопряжения и, соответственно, $K \lhd G$. Из этого уже вытекает, что $\nu_2(G) = 1$.

Пусть теперь $\nu_2(G) > 1$. Тогда (по третьей теореме Силова) $\nu_2(G) = 3$ и, следовательно, $\nu_3(G) = 1$ (так как числа $\nu_2(G)$ и $\nu_3(G)$ не могут одновременно быть равными 1 и не могут одновременно быть большими 1).

Возникли два случая: $\nu_3(G) = 4$, $\nu_2(G) = 1$ и $\nu_3(G) = 1$, $\nu_2(G) = 3$. Разберем их по отдельности.

Пусть $\nu_3(G) = 4$, а $\nu_2(G) = 1$. Покажем, что в этом случае $G \cong \mathrm{A}_4$. Пусть группа H (силовская 3-подгруппа группы G) действует на группе K (силовской 2-подгруппе группы G) сопряжениями. У этого действия есть орбита длины 3, состоящая из элементов k_1, k_2, k_3. В самом деле, если все орбиты относительно рассматриваемого действия имеют длину 1, то все элементы H коммутируют со всеми элементами K и, следовательно, группа G (равная HK) коммутативна. Так как сопряжение – это автоморфизм, то все элементы k_1, k_2, k_3 имеют одинаковый порядок. Из этого вытекает, что группа K (ее порядок равен 4) – это группа Клейна V_4 (напомним, что существует ровно две неизоморфные группы порядка 4 – это группы Z_4 и $\mathrm{V}_4 \cong \mathrm{Z}_2 \times \mathrm{Z}_2$).

Пусть теперь $H = \{1, h, h^{-1}\}$. Можно так выбрать индексы у элементов k_1, k_2, k_3, чтобы

$$hk_1h^{-1} = k_2, \quad hk_2h^{-1} = k_3, \quad hk_3h^{-1} = k_1.$$

Таким образом, $G = \{h^\ell, h^\ell k_j : \ \ell = 0, 1, 2, j = 1, 2, 3\}$ и таблица умножения в группе G определяется однозначно. Итак, группа G порядка 12 с тем свойством, что $\nu_3(G) = 4$, а $\nu_2(G) = 1$, единственна, с точностью до изоморфизма. Заметим, что группа A_4 обладает требуемой структурой, причем K – это группа Клейна, а 4 группы порядка 3 порождаются циклами длины 3.

Рассмотрим теперь второй случай, в котором $\nu_3(G) = 1$, а $\nu_2(G) = 3$. Первое наблюдение в этом случае состоит в том, что группа G содержит циклическую нормальную подгруппу порядка 6. В самом деле, рассмотрим действие группы K на H (а она нормальна, так как $\nu_3(G) = 1$) сопряжениями. H распадается на орбиты относительно этого действия. Все эти орбиты не могут содержать по одному элементу, так как в этом случае группа G будет коммутативной (см. выше). Следовательно, элементы группы H, отличные от единицы, должны составлять орбиту относительно рассматриваемого

действия (и длина этой орбиты равна двум). Следовательно, в K существует элемент k_0, отличный от единицы и коммутирующий с каждым элементом группы H (проверка оставляется в качестве *упражнения*). Этот элемент k_0 не может быть образующим в K и, следовательно, $\operatorname{ord}_K k_0 = 2$ (иначе группа G окажется коммутативной). Таким образом, группа $A = H \sqcup k_0 H$ является коммутативной подгруппой порядка 6, циклической и нормальной в G.

Пусть теперь a – образующий группы A, т.е. $A = \langle a \rangle$. Выберем элемент $b \in K \setminus \{1, k_0\}$. Заметим, что $G = A \sqcup bA$, т.е. $G = \langle a, b \rangle$ (другими словами, a и b – образующие для G).

Так как элемент bab^{-1} является образующим в группе $bAb^{-1} = A$, то возможны только две возможности: $bab^{-1} = a$ и $bab^{-1} = a^{-1}$. Но в первом случае из равенства $bab^{-1} = a$ вытекает, что $ba = ab$ а это, в свою очередь, приводит к коммутативности G. Следовательно, имеет место соотношение $bab^{-1} = a^{-1}$.

Далее, из представления $G = A \sqcup bA$ вытекает, что $b^2 \in A$. В этом случае имеют место следующие две возможности:

а) $b^2 = 1$. В этом случае группа G задается двумя образующими (a и b), связанными соотношениями $a^6 = 1$, $b^2 = 1$ и $bab^{-1} = a^{-1}$. Последнее из этих трех соотношений можно заменить на эквивалентное ему соотношение $abab = 1$. Как известно, группа $\langle a, b : \ a^6 = 1, b^2 = 1, abab = 1 \rangle$ – это группа D_6.

б) $b^2 \neq 1$. В этом случае $\operatorname{ord} b^2 = 2$ и, так как $b^2 \in A$, то $b^2 = a^3$ (других элементов порядка 2 в A нет). В этом случае группа G задается двумя образующими (a и b), связанными соотношениями $a^6 = 1$, $b^2 = a^3$ и $bab^{-1} = a^{-1}$. Нетрудно проверить, что матрицы

$$\alpha = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{и} \qquad \beta = \begin{pmatrix} i & 0 \\ i & -i \end{pmatrix}$$

удовлетворяют соотношениями $\alpha^6 = E$, $\alpha^3 = \beta^2$ и $\beta\alpha\beta^{-1} = \alpha^{-1}$ и образуют в группе $\mathrm{SL}_2(\mathbb{C})$ подгруппу из 12 элементов. □

Задача 4.1. Для группы $\widehat{\mathrm{S}}_3 := \langle a, b : \ a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1} \rangle$ вычислить ее центр $Z(\widehat{\mathrm{S}}_3)$ и доказать, что $\widehat{\mathrm{S}}_3 / Z(\widehat{\mathrm{S}}_3) \cong \mathrm{S}_3$.

Задача 4.2. Реализовать группу $\widehat{\mathrm{S}}_3$ как подгруппу группы S_n при минимальном возможном n (возможность такой реализации вытекает из теоремы Кэли).

Задача 4.3. Пусть G – группа порядка $|G| = pq$, где p и q – простые числа, причем $p < q$. Доказать, что G является либо циклической группой, либо неабелевой группой, имеющей нормальную силовскую q-подгруппу, причем последнее возможно если и только если число $q - 1$ делится на p.

4.3. Конечно порожденные абелевы группы

Напомним, что термин *абелева группа* используется как синоним термина *коммутативная группа*. В этом разделе мы изучим строение конечно порожденных абелевых групп. Как отмечалось ранее, при изучении абелевых групп бывает удобно считать, что групповой операцией является сложение и, соответственно, использовать *аддитивную* нотацию. Чтобы сделать и такую нотацию привычной и понятной мы воспользуемся ей в этом разделе.

Итак, пусть $A = (A, +)$ – аддитивная абелева группа (т.е. такая группа, что $a_1 + a_2 = a_2 + a_1$ для любых $a_1, a_2 \in A$). В качестве первого простого примера можно привести группу $\mathbb{Z}$ целых чисел с операцией сложения. Напомним некоторую специфику аддитивных обозначений. Во-первых, единичный элемент в аддитивной группе всегда обозначается символом 0. Во-вторых, степень элемента $a \in A$ записывается в виде $na := a + a + \cdots \{n \text{ раз}\} \cdots + a$, где $n \in \mathbb{Z}$, $n > 0$. Кроме того, $0a = 0$, где в левой части этого равенства 0 – это целое число, а в правой части 0 – это нейтральный элемент

группы A. Далее, $(-n)a = (-a) + \cdots \{n \text{ раз}\} \cdots + (-a)$ при $n \in \mathbb{Z}$, $n > 0$, и для любых целых n и m выполняются следующие равенства

$$m(na) = (mn)a, \qquad (m+n)a = ma + na, \qquad m(a+b) = ma + mb,$$

верные для любых элементов a и b группы A. Таким образом, в аддитивной абелевой группе допустимо рассматривать *целочисленные линейные комбинации*, т.е. выражения вида

$$n_1 a_1 + \cdots + n_k a_k,$$

где $a_1, \ldots, a_k$ – элементы группы A, а коэффициенты $n_1, \ldots, n_k$ – целые числа.

Напомним, что система элементов $\{a_1, \ldots, a_k\}$ аддитивной абелевой группы A называется *системой образующих* (или *системой порождающих элементов*) для этой группы, если любой элемент $a \in A$ может быть представлен в виде целочисленной линейной комбинации элементов $a_1, \ldots, a_k$, т.е., если существуют такие целые коэффициенты $n_1, \ldots, n_k$, что $a = n_1 a_1 + \cdots + n_k a_k$. В таком случае пишут $A = \langle a_1, \ldots, a_k \rangle$. Отметим, что в определении системы образующих *не требуется* единственности представления элемента a в виде линейной комбинации образующих.

Пример 4.6. В группе $\mathbb{Z}$ можно предложить две образующих: числа ± 1. При этом в качестве *упражнения* предлагается проверить, что никакое число $m \neq \pm 1$ не может быть принято в качестве образующей для группы $\mathbb{Z}$, а также найти все возможные образующие в группе $n\mathbb{Z}$, $n \in \mathbb{N}$.

Пример 4.7. При $n \in \mathbb{N}$ рассмотрим аддитивную группу $\mathbb{Z}^n$ состоящую из всех векторов пространства $\mathbb{R}^n$ с целочисленными координатами. Ясно, что совокупность векторов

$$e_1 = (1, 0, \cdots, 0), \quad e_2 = (0, 1, \cdots, 0), \quad \cdots \quad e_n = (0, 0, \cdots, 1)$$

будет системой образующих в $\mathbb{Z}^n$.

В группе $\mathbb{Z}^3$ кроме системы образующих $\{e_1, e_2, e_3\}$ можно построить и другие системы образующих. Например, система элементов

$$a_1 = (1, 1, 0), \quad a_2 = (1, -1, 0), \quad a_3 = (4, 1, 0), \quad a_4 = (-1, -1, 1)$$

будет системой образующих, так как

$$e_1 = 3a_1 + 2a_2 - a_3, \quad e_2 = -2a_1 - 2a_2 + a_3, \quad e_3 = a_1 + a_4.$$

В качестве *упражнения* предлагается проверить, можно ли из системы образующих $\{a_1, a_2, a_3, a_4\}$ убрать хотя бы один элемент так, чтобы оставшаяся система по-прежнему являлась системой образующих в $\mathbb{Z}^3$.

Разумеется, существуют абелевы группы, в которых нельзя выделить никакой конечной системы образующих. Это, например, аддитивная группа $\mathbb{R}$ всех вещественных чисел, мультипликативная группа всех комплексных чисел с модулем 1, аддитивная группа $\mathbb{Q}$ всех рациональных чисел, или мультипликативная группа $\mathbb{Q}^*$ всех ненулевых рациональных чисел.

Заметим также, что в случае аддитивных групп вместо термина *прямое произведение* используется термин *прямая сумма* групп и применяется обозначение $A \oplus B$.

Ранее символ Z_n использовался для обозначения мультипликативной циклической группы порядка n. В дальнейшем мы будем применять его и для обозначения аддитивной циклической группы порядка n, причем из контекста всегда будет ясно, о какой группе (аддитивной или мультипликативной) идет речь. Имеют место следующие простые свойства циклических групп.

Предложение. *Прямая сумма конечного числа циклических групп является конечно порожденной группой. Прямая сумма двух конечных циклических групп, имеющих взаимно простые порядки n и m является циклической группой (порядка nm).*

Проверка. Проверим первое утверждение. Пусть $A_1 = \langle a_1 \rangle, \dots, A_k = \langle a_k \rangle$ – циклические группы. Тогда ясно, что система элементов $\{(a_1, 0, \cdots, 0), \cdots, (0, 0, \cdots, a_k)\}$ будет системой образующих группы $A_1 \oplus \cdots \oplus A_k$.

Рассмотрим теперь группу $\mathrm{Z}_n \oplus \mathrm{Z}_m$. Пусть a – образующая для Z_n, а b – образующая для Z_m. Тогда (a, b) – образующая для $\mathrm{Z}_n \oplus \mathrm{Z}_m$. Пусть $k(a, b) = (ka, kb) = (0, 0)$ при $k \in \mathbb{N}$. Тогда $ka = 0$ и, следовательно, $k = tn$. Аналогично, $kb = 0$ и, следовательно $k = sm$. Так как $tn = sm$, $t, s \in \mathbb{N}$ и так как НОД$(n, m) = 1$, то t кратно m, а s кратно n. Отсюда $k = nm$ и, следовательно $\mathrm{Z}_n \oplus \mathrm{Z}_m \cong \mathrm{Z}_{nm}$. □

Приведем еще один, весьма общий, пример конечно порожденных абелевых групп. Рассмотрим произвольную конечно порожденную группу G и рассмотрим факторгруппу G/G' (где, напомним, G' – это коммутант группы G). Коммутативность (очевидно конечно порожденной) факторгруппы G/G' вытекает из Теоремы 3.12.

Абелевы группы без кручения. Скажем, что аддитивная абелева группа A – это *группа без кручения*, если из равенства $na = 0$ при $n \neq 0$ вытекает, что $a = 0$. Группы без кручения по многим своим свойствам очень похожи на линейные пространства и соответствующая аналогия будет прослеживаться и активно использоваться в дальнейшем. В частности, многие термины в теории групп без кручения позаимствованы из теории линейных пространств.

Так скажем, что система элементов $\{a_1, \dots, a_k\}$ группы A является *независимой*, если из равенства $n_1 a_1 + \cdots + n_k a_k = 0$ при $n_1, \dots, n_k \in \mathbb{Z}$ вытекает, что $n_1 = \cdots = n_k = 0$. Далее, система элементов $\{a_1, \dots, a_k\}$ группы A называется *базисом*, если она независима и является системой образующих группы A.

Теорема 4.8. *Всякая конечно порожденная абелева группа A без кручения обладает базисом. Все базисы группы A равномощны, т.е. состоят из одинакового числа элементов.*

Доказательство. Пусть $\{a_1, \dots, a_n\}$ – некоторая система образующих группы A. Рассмотрим выражение $m_1 a_1 + \cdots + m_n a_n = 0$. Всякое такое выражение назовем *соотношением* в A. Число $\min\{|m_1|, \dots, |m_n|\}$ назовем *высотой* соответствующего соотношения. Соотношение в A называется минимальным, если оно имеет минимально возможную высоту. В любой группе всегда существует минимальное соотношение (так как высота соотношения – это натуральное число). Однако, минимальное соотношение не обязательно единственно (в качестве *упражнения* предлагается привести соответствующий пример).

Пусть $m_1 a_1 + \cdots + m_n a_n = 0$ – минимальное соотношение в группе A. Если $d :=$ НОД$(m_1, \dots, m_n) > 1$, то, разделив все коэффициенты $m_1, \dots, m_n$ на d, мы придем к соотношению в A с меньшей высотой. Это противоречит минимальности соотношения $m_1 a_1 + \cdots + m_n a_n = 0$. Следовательно, для минимального соотношения $m_1 a_1 + \cdots + m_n a_n = 0$ всегда верно равенство НОД$(m_1, \dots, m_n) = 1$.

Пусть соотношение $m_1 a_1 + \cdots + m_n a_n = 0$ имеет высоту 1. Тогда найдется такое j, что $|m_j| = 1$. В этом случае ясно, что a_j выражается через остальные образующие и система $\{a_1, \dots, a_n\} \setminus \{a_j\}$ будет системой образующих в A.

Предположим теперь, что минимальное соотношение $m_1 a_1 + \cdots + m_n a_n = 0$ в группе A имеет высоту $h > 1$. Переставив элементы $\{a_1, \dots, a_n\}$ местами и домножив их, если надо, на -1, можно считать, что $m_1 = h$. Так как НОД$(m_1, \dots, m_n) = 1$ (рассматриваемое соотношение минимально), то найдется такое j, что m_j не делится на h. Без ограничения общности считаем, что $j = 2$. Тогда $m_2 = sh + r$, где $s \in \mathbb{Z}$, а $r \in \mathbb{Z}$ и $0 < r < h$. Перепишем соотношение $m_1 a_1 + \cdots + m_n a_n = 0$ в виде

$$0 = ha_1 + m_2 a_2 + m_3 a_3 + \cdots + m_n a_n = h(a_1 + sa_2) + ra_2 + m_3 a_3 + \cdots + m_n a_n.$$

Система $\{a_1' := a_1 + sa_2, a_2, a_3, \ldots, a_n\}$ снова будет системой образующих в A. Но для этой системы имеется соотношение $ha_1' + ra_2 + m_3a_3 + \cdots + m_na_n = 0$ которое имеет высоту не превосходящую числа $r < h$.

Выберем теперь в A минимальную систему образующих $\{a_1, \ldots, a_n\}$. Среди всех систем, состоящих из n элементов, найдем минимальную высоту минимального соотношения h и предположим, что выбранная система $\{a_1, \ldots, a_n\}$ удовлетворяет минимальному соотношению высоты h. Если $h = 1$, то из системы $\{a_1, \ldots, a_n\}$ можно удалить элемент. Но система $\{a_1, \ldots, a_n\}$ выбрана минимальной. Следовательно, $h > 1$. В этом случае мы перейдем к системе $\{a_1', a_2, a_3, \ldots, a_n\}$ как показано выше. Высота минимального соотношения для этой системы меньше. Полученное противоречие показывает, что минимальная система образующих в аддитивной абелевой группе без кручения не может удовлетворять никакому нетривиальному соотношению вида $m_1a_1 + \cdots + m_na_n = 0$. Следовательно, такая система независима и, по определению, образует базис в A.

Равномощность двух любых базисов группы A вытекает из следующего результата.

Предложение. *Если $A = \langle a_1, \ldots, a_n\rangle$, а элементы $b_1, \ldots, b_k \in A$ таковы, что система $\{b_1, \ldots, b_k\}$ независима, то $k \leqslant n$.*

Проверка. В самом деле, так как $\{a_1, \ldots, a_n\}$ – система образующих, то $b_j = \sum_{\ell=1}^{n} m_{j\ell}a_\ell$ при $j = 1, \ldots, k$. Рассмотрим систему векторов $\boldsymbol{m}_j = (m_{j1}, \ldots, m_{jn})$ в линейном пространстве $\mathbb{Q}^n$. Если $k > n$, то система векторов $\{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_k\}$ будет линейно зависимой. Таким образом, найдутся рациональные числа $q_1, \ldots, q_k$ такие, что $\sum_{j=1}^{k} |q_j| > 0$, но $q_1\boldsymbol{m}_1 + \cdots + q_k\boldsymbol{m}_k = \boldsymbol{0}$. Умножая, если необходимо, числа $q_1, \ldots, q_k$ на их общий знаменатель, можно считать, что все числа $q_1, \ldots, q_k$ – целые. Таким образом, существует нетривиальная целочисленная линейная комбинация $q_1\boldsymbol{m}_1 + \cdots + q_k\boldsymbol{m}_k$, равная $\boldsymbol{0}$. Из этого вытекает, что

$$\sum_{j=1}^{k} q_jb_j = \sum_{j=1}^{k}\sum_{\ell=1}^{n} q_jm_{j\ell}a_\ell = \sum_{\ell=1}^{n}\left(\sum_{j=1}^{k} q_jm_{j\ell}\right)a_\ell = 0,$$

а это противоречит независимости системы $\{b_1, \ldots, b_k\}$. Следовательно $k \leqslant n$ и наше предложение справедливо.

Пусть теперь $\{a_1, \ldots, a_n\}$ и $\{b_1, \ldots, b_k\}$ – два базиса группы A. Тогда, в силу только что установленного предложения, $n \leqslant k$ и $k \leqslant n$. Откуда $k = n$. □

Определение. *Пусть $n \in \mathbb{N}$. Конечно порожденная абелева группа A называется свободной ранга n, если $A \cong \mathbb{Z}^n = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. Для свободной абелевой группы ранга n применяется обозначение F_n^{ab}.*

Ранг группы, состоящей из одного элемента (нуля), считается равным 0. Любой базис свободной абелевой группы A называется также ее *свободной системой образующих*. В качестве *упражнения* предлагается рассмотреть Пример 4.7 и понять, какая из приведенных там систем образующих для группы $\mathbb{Z}^3$ будет свободной.

Замечание. Если A – конечно порожденная абелева группа без кручения, то она, как доказано выше, обладает базисом. Ясно, что отображение, переводящее элементы базиса $\{a_1, \ldots, a_n\}$ группы A в элементы $\{e_1, \ldots, e_n\}$ стандартного базиса в $\mathbb{Z}^n$ будет (в силу того, что группа A – это группа без кручения) изоморфизмом $A \mapsto \mathbb{Z}^n$ (проверка необходимых деталей оставляется в качестве *упражнения*). Таким образом, A – свободная группа некоторого ранга n.

4.4. Строение конечно порожденных абелевых групп

Изучение вопроса о строении конечно порожденных абелевых групп мы начнем с доказательства следующего несложного результата.

Теорема 4.9. *Пусть A – абелева группа, а $B \subset A$ такая ее подгруппа, что факторгруппа A/B – свободная. Тогда A является прямой суммой B и некоторой свободной абелевой группы, т.е. $A = B \oplus F^{ab}$.*

Доказательство. Докажем вначале следующее простое утверждение. Пусть факторгруппа A/B является прямой суммой вида

$$A/B = \bigoplus_{k=1}^{n} (A_k/B),$$

в которой каждая подгруппа A_k имеет вид $A_k = B \oplus G_k$. Тогда A имеет вид

$$A = B \oplus \left(\bigoplus_{k=1}^{n} G_k \right).$$

Ясно, что B и все подгруппы G_k порождают A. Предположим теперь, что $b + g_1 + \cdots + g_n = 0$, где $b \in B$, а $g_k \in G_k$ при $k = 1, \ldots, n$. Из этого соотношения следует соотношение $\overline{g}_1 + \cdots + \overline{g}_n = 0$ для смежных классов по подгруппе B. Так как A_k/B – прямое слагаемое в факторгруппе A/B, то $\overline{g}_k = 0$. Таким образом, $g_k \in B$ при всех $k = 1, \ldots, n$. Далее, $g_k \in B \cap G_k = \{0\}$ и, следовательно, $g_k = 0$ при всех $k = 1, \ldots, n$. Остается заметить, что $b = 0$. Итак, любой элемент $a \in A$ представляется в виде суммы $a = b + g_1 + \cdots + g_n$, где $b \in B$, а $g_k \in G_k$ при $k = 1, \ldots, n$, единственным образом.

Переходим непосредственно к доказательству теоремы. Так как группа A/B есть прямая сумма бесконечных циклических групп, то (в силу только что доказанного утверждения), нам достаточно рассмотреть случай, когда $A/B \cong \mathbb{Z}$. Итак, пусть $A/B = \langle \alpha \rangle$, где α – некоторый смежный класс по подгруппе B. Выберем представитель $a \in \alpha$ так, чтобы $a \neq 0$ и $a \notin B$. В этом случае элементы ma при $m \in \mathbb{Z}$ будут представителями смежных классов $m\alpha$. Следовательно, $A = B \oplus \langle a \rangle$. □

Определение. *Периодической частью абелевой группы A называется совокупность всех элементов конечного порядка этой группы. Периодическая часть группы A обозначается символом $T(A)$ и называется подгруппой кручения группы A.*

Символ T в обозначении подгруппы кручения $T(A)$ группы A происходит от английского слова *torsion*. Легко проверяется, что $T(A)$ является подгруппой группы A. В самом деле, пусть $a_1, a_2 \in T(A)$ и пусть числа $m_1, m_2 \in \mathbb{Z}$ таковы, что $m_1 a_1 = 0$ и $m_2 a_2 = 0$. Тогда

$$m_1 m_2 (n_1 a_1 + n_2 a_2) = (m_2 n_1)(m_1 a_1) + (m_1 n_2)(m_2 a_2) = 0$$

для любых $n_1, n_2 \in \mathbb{Z}$. Ясно также, что имеет место следующий факт

Предложение. *Для любой абелевой группы A факторгруппа $A/T(A)$ – это группа без кручения.*

Проверка. В самом деле, пусть $\overline{a} = a + T(A)$ – элемент конечного порядка в $A/T(A)$. Тогда найдется $m \in \mathbb{Z}$ такое, что $m\overline{a} = ma + T(A)$ – это нулевой смежный класс, т.е. $ma \in T(A)$. Следовательно, найдется такое $n \in \mathbb{Z}$, что $n(ma) = 0$. Но в этом случае $(nm)a = 0$ и, следовательно, $a \in T(A)$. □

Рассмотрим теперь конечно порожденную абелеву группу с n образующими. Так как $A/T(A)$ – группа без кручения, то эта факторгруппа изоморфна некоторой свободной абелевой группе ранга $r \leqslant n$. В силу Теоремы 4.9 имеет место равенство

$$A = T(A) \oplus F_r^{ab}.$$

Из этого равенства, в частности, вытекает, что $T(A) \cong A/F_r^{ab}$ и, следовательно, число образующих группы $T(A)$ также не превосходит n. Если $\{a_1, \ldots, a_k\}$ – образующие группы $T(A)$, то существуют такие числа $m_1, \ldots, m_k \in \mathbb{N}$, что $m_1 a_1 = \cdots = m_k a_k = 0$. Таким образом, $T(A)$ – конечная группа, причем $|T(A)| \leqslant m_1 \cdots m_k$.

Итак, нами доказано следующее важное утверждение

Теорема 4.10. *Всякая конечно порожденная абелева группа A является прямой суммой конечной абелевой группы $T(A)$ и свободной абелевой группы F_r^{ab}.*

Мы уже знаем, как устроена свободная абелева группа. Рассмотрим теперь строение группы $T(A)$.

Пусть A – некоторая периодическая абелева группа. Рассмотрим совокупность $A(p)$ всех элементов из A, порядки которых являются степенями простого числа p. Ясно, что для некоторых p будем получать $A(p) = \{0\}$. Проверим, что $A(p)$ будет подгруппой группы A. Пусть $a, b \in A(p)$. Тогда $p^s a = 0$ и $p^t b = 0$ при некоторых целых s, t. Пусть $m = st$. Тогда $p^m(a - b) = 0$ и, следовательно, $a - b \in A(p)$ (здесь символом $a - b$ для краткости обозначено выражение $a + (-b)$).

Пусть теперь $p_1, \dots, p_k$ – различные простые числа. Каждый элемент из $A(p_1) + \dots + A(p_k)$ имеет порядок, который не может делиться на простое число p, отличное от $p_1, \dots, p_k$. Следовательно, $A(p) \cap \big(A(p_1) + \dots + A(p_k)\big) = \{0\}$, а из этого следует, что подгруппы $A(p)$ порождают прямую сумму $\bigoplus_p A(p)$, где сумма берется по всем простым числам p.

Покажем, что группа A порождается своими p-компонентами $A(p)$. Возьмем произвольный элемент $a \in A$ и пусть $\operatorname{ord}_A a = n = p_1^{m_1} \cdots p_k^{m_k}$ – разложение порядка элемента a на (различные) простые множители $p_1, \dots, p_k$, причем $m_1 > 0, \cdots, m_k > 0$. Определим целые числа $n_1, \dots, n_k$ равенствами $n = n_j p_j^{m_j}$. Эти числа взаимно просты и, следовательно, найдутся целые числа $t_1, \dots, t_k$ такие, что $t_1 n_1 + \dots + t_k n_k = 1$. Из этого равенства следует, что элемент a можно записать в виде

$$a = (t_1 n_1 + \dots + t_k n_k)a = \sum_{j=1}^{k} t_j(n_j a),$$

где $n_j a \in A(p_j)$ (так как $p_j^{m_j}(n_j a) = na = 0$). Таким образом, произвольный элемент группы a записан в виде суммы элементов, принадлежащих подгруппам $A(p_j)$, $j = 1, \dots, k$.

Проверим теперь, что подгруппы $A(p)$ однозначно определяются по группе A. В самом деле, если $A = \bigoplus_p A(p)$ и $A = \bigoplus_p B(p)$ то, по определению подгрупп $A(p)$ получаем, что $A(p) \subset B(p)$ и $B(p) \subset A(p)$. Нами доказано

Предложение 4.11. *Всякая периодическая абелева группа A представима в виде прямой суммы p-групп $A(p)$, отвечающих различным простым p. Каждое прямое слагаемое $A(p)$ в такой сумме определяется по группе A однозначно.*

Докажем теперь классический результат о структуре конечных абелевых групп. Имеет место следующая теорема:

Теорема 4.12 (теорема Фробениуса)**.** *Каждая конечная абелева группа является прямой суммой конечного числа примарных циклических групп.*

Доказательство. С учетом Предложения 4.11 теорему достаточно доказать для конечных p-групп.

Пусть A – конечная абелева p-группа, а $a \in A$ – элемент максимального порядка p^k. Установим, что $\langle a \rangle$ – *прямое слагаемое* в A. Для этого рассмотрим максимальную подгруппу $B \subset A$ такую, что $B \cap \langle a \rangle = \{0\}$. Тогда $H := \langle B, a \rangle = B \oplus \langle a \rangle$. Наша цель состоит в том, чтобы доказать, что $H = A$. Будем рассуждать от противного и допустим, что $H \subset A$ – собственная подгруппа в A. В этом случае найдется элемент $x \in A$ такой, что $x \notin H$, но $px \in H$. В самом деле, возьмем произвольный элемент $y \in A \setminus H$ и рассмотрим последовательность элементов $y, py, p^2y, \dots,$. Либо в этой цепочке возникнет ненулевой элемент $p^\ell y \in H$, либо, так как A – конечная p-группа, найдется ℓ такое, что $p^\ell y = 0$. В любом случае в качестве x можно взять $p^{\ell-1}y$. Итак, для элемента x имеет место равенство

$$px = b + ma,$$

где $b \in B$, а $m \in \mathbb{Z}$. Так как p^k – это максимальный из порядков элементов в A, то

$$p^k x = p^{k-1}(b + ma) = p^{k-1}b + p^{k-1}ma = 0.$$

Так как H – прямая сумма B и $\langle a \rangle$, то из последнего равенства вытекает, что $p^{k-1}ma = 0$. Следовательно, $p^{k-1}m$ делится на p^k, откуда $m = pt$ для некоторого $t \in \mathbb{Z}$. Рассмотрим теперь элемент $z = x - ta$ и заметим, что $pz = b \in B$. Однако $z \notin H$ и, следовательно, группа $\langle B, z \rangle$ содержит (так как B – максимальна) ненулевой элемент $ra \in \langle a \rangle$. Таким образом, $ra = b' + sz$ при $b' \in B$ и $s \in \mathbb{Z}$. Следовательно, $sz \in B + \langle a \rangle = H$. Если s делится на p, то $sz \in B$ и тогда $b' + sz = b'' \in B$ и $0 \neq ra = b''$. Таким образом $B \cap \langle a \rangle \neq \{0\}$, что противоречит выбору B. Следовательно, $\text{НОД}(s, p) = 1$. Из этого и из того, что $sz \in H$ и $pz \in H$, то вытекает, что $z \in H$. Но $z \notin H$ и снова возникает противоречие. Таким образом $A = B \oplus \langle a \rangle$.

Из доказанного утверждения доказательство теоремы Фробениуса получается следующим образом: надо взять в группе A элемент a максимального порядка, представить A в виде $A = \langle a \rangle \oplus B$ и повторить процедуру для B. Так как $|B| < |A|$, то этот процесс сходится за конечное число шагов. □

Кроме того, полученное представление конечной абелевой группы A в виде прямой суммы примарных циклических групп обладает следующим свойством единственности:

Теорема 4.13. *Пусть конечная абелева p-группа A разложена в прямую сумму примарных циклических групп двумя способами:*

$$A_1 \oplus \cdots \oplus A_r = A = B_1 \oplus \cdots \oplus B_s,$$

то $r = s$ и порядки групп A_j и B_k совпадают при определенном упорядочении групп в наборах $\{A_j\}$ и $\{B_k\}$.

Доказательство. Если $|A| = p$, то теорема, очевидно, верна. Будем рассуждать по индукции по величине $|A|$. Занумеруем слагаемые A_j и B_k так, чтобы их порядки не возрастали:

$$A_j = \langle a_j \rangle, \quad \operatorname{ord} a_j = p^{m_j}, \quad m_1 \geqslant m_2 \geqslant \cdots \geqslant m_q > m_{q+1} = \cdots = m_r = 1,$$
$$B_k = \langle b_k \rangle, \quad \operatorname{ord} b_k = p^{n_k}, \quad n_1 \geqslant n_2 \geqslant \cdots \geqslant n_t > n_{t+1} = \cdots = n_s = 1.$$

Множество $pA = \{pa : a \in A\}$ – это подгруппа в A, не зависящая, разумеется, от разложения A в прямую сумму примарных компонент. Возьмем произвольный элемент $x \in A$. Тогда $x = u_1a_1 + \cdots + u_ra_r$ и $x = v_1b_1 + \cdots + v_sb_s$. Учитывая принятое упорядочение прямых слагаемых в обоих разложениях получаем

$$u_1(pa_1) + \cdots + u_q(pa_q) = px = v_1(pb_1) + \cdots + v_t(pb_t).$$

Из этого равенства вытекает, что при $a'_j = pa_j$, $j = 1, \ldots, q$, $b'_k = pb_k$, $k = 1, \ldots, t$ имеют место разложения

$$\langle a'_1 \rangle + \cdots + \langle a'_q \rangle = pA = \langle b'_1 \rangle + \cdots + \langle b'_t \rangle.$$

Заметим, что порядки элементов a'_j и b'_k (при $j = 1, \ldots, q$ и $k = 1, \ldots, t$ соответственно) равны $p^{m_j - 1}$ и $p^{n_k - 1}$ соответственно. Так как $|pA| < |A|$, то к группе pA применимо предположение индукции, согласно которому $q = t$ и $m_1 - 1 = n_1 - 1, \ldots, m_q - 1 = n_q - 1$. Таким образом, $m_i = n_i$ при $i = 1, \ldots, q = t$.

Заметим еще, что $|A_{q+1} + \cdots + A_r| = p^{r-q}$ и $|B_{t+1} + \cdots + B_s| = p^{s-t}$. Следовательно,

$$p^{m_1 + \cdots + m_q} p^{r-q} = |A| = p^{n_1 + \cdots + n_t} p^{s-t}$$

и, так как $q = t$, то $r = s$ и теорема доказана полностью. □

Суммируя все доказанные выше утверждения о строении конечных абелевых групп, мы приходим к следующему результату.

Теорема 4.14. *Всякая конечная абелева группа A является прямым произведением примарных циклических подгрупп. Любые два таких разложения имеют по одинаковому числу прямых сомножителей одинакового порядка.*

Пусть элементы $\{a_1, \dots, a_r\}$ – это базис в абелевой группе A и пусть $n_1, \dots, n_r$ – порядки элементов $a_1, \dots, a_r$ соответственно. Тогда всякий элемент $a \in A$ единственным образом записывается в виде $a = k_1a_1 + \dots + k_ra_r$, где $0 \leqslant k_j < n_j$ при $j = 1, \dots, r$. В этом случае ясно, что $|A| = n_1 \cdots n_r$ и $A = \langle a_1 \rangle \oplus \dots \oplus \langle a_r \rangle$.

Теорема 4.14 утверждает, что в A существует такой базис, что все элементы a_j примарны (т.е. их порядки являются степенями простых делителей числа $|A|$), а система $\{n_1, \dots, n_k\}$ не зависит от выбора базиса.

В силу этого обстоятельства числа $n_1, \dots, n_k$ называют *инвариантными делителями* для A. Используется также терминология, согласно которой набор $\{n_1, \dots, n_k\}$ называется *типом конечной абелевой группы* A.

Пусть дана конечная абелева группа A и пусть $|A| = p_1^{m_1} \cdots p_k^{m_k}$, где $p_1, \dots, p_k$ – все различные простые делители числа $|A|$, а $m_1, \dots, m_k \in \mathbb{Z}_+$. Рассмотрим всевозможные представления числа $|A|$ в виде произведения

$$|A| = n_1 \cdots n_k,$$

где $n_j = p_1^{t_1} \cdots p_k^{t_k}$ при $t_\ell \in \{0, 1, \dots, m_\ell\}$, $\ell = 1, \dots, k$, причем $n_{j-1} \mid n_j$ при $j = 2, \dots, k$. Числа $\{n_1, \dots, n_k\}$ называются *инвариантными факторами* для группы A. Группа A может быть записана в виде прямой суммы циклических групп порядков $n_1, \dots, n_k$ соответственно.

Пример 4.15. Пусть $|A| = 36 = 2^2 3^3$. В этом случае $k = 2$, $p_1 = 2$, $p_2 = 3$, а $m_1 = m_2 = 2$ и возникают следующие наборы инвариантных факторов: $\{1, 36\}$, $\{2, 18\}$, $\{3, 12\}$ и $\{6, 6\}$.

В первом случае $A \cong \mathrm{Z}_{36}$, что соответствует разложению группы A в прямую сумму примарных циклических групп вида $A \cong \mathrm{Z}_4 \oplus \mathrm{Z}_9$.

Во втором случае возникает разложение $A \cong \mathrm{Z}_2 \oplus \mathrm{Z}_{18} \cong \mathrm{Z}_2 \oplus \mathrm{Z}_2 \oplus \mathrm{Z}_9$.

В третьем случае получаем $A \cong \mathrm{Z}_3 \oplus \mathrm{Z}_{12} \cong \mathrm{Z}_4 \oplus \mathrm{Z}_3 \oplus \mathrm{Z}_3$.

И, наконец, в четвертом случае возникает разложение $A \cong \mathrm{Z}_6 \oplus \mathrm{Z}_6 \cong \mathrm{Z}_2 \oplus \mathrm{Z}_2 \oplus \mathrm{Z}_3 \oplus \mathrm{Z}_3$.