ЛЕКЦИИ ПО АЛГЕБРЕ

3 СЕМЕСТР

2012–2013 УЧЕБНЫЙ ГОД

БУНИНА ЕЛЕНА ИГОРЕВНА

helenbunina@gmail.com

(ПО ЛЕКЦИЯМ ПРОФЕССОРА
АЛЕКСАНДРА ВАСИЛЬЕВИЧА
МИХАЛЕВА)

Часть 1 — ОСНОВЫ ТЕОРИИ ГРУПП

ЛЕКЦИЯ 1

ГРУППЫ.

ИЗОМОРФИЗМЫ ГРУПП.

ПРИМЕРЫ ГРУПП.

СТЕПЕНЬ И ПОРЯДОК ЭЛЕМЕНТА ГРУППЫ.

НЕМНОГО ИСТОРИИ

- Начало развития теории групп относится к XVIII веку.
- Ж. Лагранж (J. Lagrange, 1771) в "Мемуаре об алгебраическом решении уравнений" рассматривал группы подстановок и их разложения на смежные классы по подгруппам.
- Н. Абель (N. Abel, 1824) и Э. Галуа (E. Galois, 1830) установили связь между свойствами алгебраического уравнения и свойствами группы подстановок на множестве корней уравнения.
- Л. Эйлер (L. Euler, 1761) рассматривал классы вычетов и сравнения, фактически используя разбиения на смежные классы по подгруппе.
- К. Гаусс (C. Gauss, 1801) в своих "Арифметических исследованиях", рассматривая уравнение деления круга, определил подгруппы его группы.
- А. Кэли (A. Cayley, 1854), классифицируя геометрии, доказал, что всякая конечная группа представима подстановками (т. е. вложима в соответствующую группу подстановок), и пришел к заданию группы образующими и определяющими соотношениями.
- В работах Ф. Клейна с С. Ли (S. Lie) было начато исследование бесконечных дискретных и топологических групп. Трехтомный трактат С. Ли и Ф. Энгеля (F. Engel), 1883—1893, зафиксировал рождение новой области в теории групп — теории групп Ли.
- к концу XIX века была полностью осознана важность теоретико–групповых идей и методов в математике и было выработано современное абстрактное определение группы (Кэли, Ли, Фробениус (F. G. L. Frobenius) и др.).
- Первую книгу по абстрактной теории групп опубликовал У. Бернсайд (W. Burnside, 1897), рассматривающий только конечные группы.

- Рассмотрение групп без предположения об их конечности стало общепринятым после выхода в 1916 году книги О. Ю. Шмидта “Абстрактная теория групп”.

- Теория групп за прошедший век расширила области своего применения: механика, физика (квантовая механика, ядерная физика, теория элементарных частиц); кристаллография; спектроскопия; криптография; информатика. В прикладных задачах возникли многие обобщения понятия группы.

ГРУППА — ОПРЕДЕЛЕНИЕ И ОСНОВНЫЕ СВОЙСТВА

Определение 1. Непустое множество G с бинарной операцией $*\colon G \times G \to G$, $(a, b) \to a * b \in G$ для $a, b \in G$, называется *группой*, если:

1) Операция ассоциативна (т. е. $(a*b)*c = a*(b*c)$ для всех $a, b, c \in G$);

2) Существует нейтральный элемент $e \in G$ (т. е. $g * e = g = e * g$ для всех $g \in G$);

3) Для каждого элемента $g \in G$ существует обратный элемент $g^{-1} \in G$ (т. е. $g * g^{-1} = e = g^{-1} * g$).

Замечание 1. Напомним, что нейтральный элемент (при мультипликативной записи называемый *единицей группы*) единственный. Действительно, если e и e' — два нейтральных элемента в группе G, то $eg = g = ge$, $e'g = g = ge'$ для всех $g \in G$. Но тогда

$$e' = ee' = e.$$

Замечание 2. Обратный элемент g^{-1} для элемента $g \in G$ определен однозначно. Действительно, если $f, h \in G$ — два обратных элемента для g, т. е. $fg = e = gf$, $hg = e = gh$, то $f = fe = f(gh) = (fg)h = eh = h$.

Лемма 1. *Если G — группа, $a, b, c \in G$, то*

1) *уравнение $ax = b$ имеет, и только одно, решение $x = a^{-1}b$;*

2) *уравнение $ya = b$ имеет, и только одно, решение $y = ba^{-1}$;*

3) *если $ab = ac$, то $b = c$; если $ba = ca$, то $b = c$;*

4) *уравнение $axb = c$ имеет единственное решение $x = a^{-1}cb^{-1}$;*

5) *если $x^2 = x$, то $x = e$;*

6) $(ab)^{-1} = b^{-1}a^{-1}$; $(a_1 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}$; $(a^{-1})^{-1} = a$.

Доказательство. 1) Ясно, что $a(a^{-1}b) = b$. Если же $ax = b$ для $x \in G$, то $x = a^{-1}ax = a^{-1}b$.

2) Ясно, что $(ba^{-1})a = b$. Если же $ya = b$ для $y \in G$, то $y = (ya)a^{-1} = ba^{-1}$.

3), 4) и 5) следуют из 1) и 2).

6) проверяется непосредственно. □

ИЗОМОРФИЗМ ГРУПП

Хотя изоморфизм групп (как частный случай гомоморфизмов групп) будет детально исследован позднее, в то же время на начальном этапе рассмотрения групп крайне необходимо понимать, какие группы надо считать “одинаковыми”.

Определение 2. Пусть G и G' — группы. Отображение

$$\alpha\colon G \to G'$$

называется *изоморфизмом*, если:

1) $\alpha\colon G \to G'$ — биекция;

2) $\alpha(xy) = \alpha(x)\alpha(y)$ для всех элементов $x, y \in G$ (здесь: в левой части $xy \in G$ с операцией произведения группы G; в правой части $\alpha(x)\alpha(y) \in G'$ с операцией произведения группы G').

При этом говорят, что условие 2) означает, что биекция $\alpha\colon G \to G'$ согласована с операциями групп G и G'.

Символ $G_1 \cong G_2$ будет означать, что существует хотя бы один изоморфизм $\alpha\colon G_1 \to G_2$ между группами G_1 и G_2, при этом будем говорить, что группы G_1 и G_2 *изоморфны*, обозначение $G_1 \cong G_2$.

Замечание 3. Отношение $G_1 \cong G_2$ на классе групп является отношением эквивалентности:

1) $G \cong G$, поскольку тождественное отображение $1_G\colon G \to G$ — изоморфизм;

2) если $G_1 \cong G_2$ и $\alpha\colon G_1 \to G_2$ — изоморфизм, то $\alpha^{-1}\colon G_2 \to G_1$ — изоморфизм (действительно, для любых $u = \alpha(x),\ v = \alpha(y) \in G_2$, $x, y \in G_1$:

$$\alpha^{-1}(uv) = \alpha^{-1}\big(\alpha(x)\alpha(y)\big) = \\ = \alpha^{-1}\big(\alpha(xy)\big) = xy = \alpha^{-1}(u)\alpha^{-1}(v)),$$

и поэтому $G_2 \cong G_1$;

3) если $G_1 \cong G_2$, $\alpha\colon G_1 \to G_2$ — изоморфизм, и $G_2 \cong G_3$, $\beta\colon G_2 \to G_3$ — изоморфизм, то $\beta\alpha\colon G_1 \to G_3$ — биекция, при этом для любых $x, y \in G_1$ имеем

$$(\beta\alpha)(xy) = \beta\big(\alpha(xy)\big) = \beta\big(\alpha(x)\alpha(y)\big) = \\ = \beta\big(\alpha(x)\big)\beta\big(\alpha(y)\big) = (\beta\alpha)(x)\beta\alpha(y),$$

и поэтому $\beta\alpha\colon G_1 \to G_3$ — изоморфизм групп, и следовательно, $G_1 \cong G_3$.

Из определения изоморфизма групп ясно, что любое свойство группы G, выраженное в ее мощности и ее групповой операции, также выполнено во всех группах G', изоморфных $G' \cong G$ группе G. Например, если $G \cong G'$, $\alpha\colon G \to G'$ — изоморфизм, то:

- если G — конечная группа, то G' — конечная группа;
- если G — p-группа, т. е. $|G| = p^k$, где p — простое число, то G' — p-группа;
- если G — коммутативная группа, то G' — коммутативная группа (если $u = \alpha(x),\ v = \alpha(y) \in G'$, $x, y \in G$, то $uv = \alpha(x)\alpha(y) = \alpha(xy) = \alpha(yx) = \alpha(y)\alpha(x) = vu$).

Пример 1. Следующие две группы G и G' изоморфны:

$$G = \{-1, 1\} = (\mathbf{U}(\mathbb{Z}), \cdot), \qquad \begin{array}{c|c|c} & -1 & 1 \\ \hline -1 & 1 & -1 \\ \hline 1 & -1 & 1 \end{array}$$

и

$$G' = \{0, 1\} = (\mathbb{Z}_2, +), \qquad \begin{array}{c|c|c} & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 1 & 1 & 0 \end{array}.$$

Действительно, пусть $f\colon G \to G'$ — биекция, где $f(1) = 0$, $f(-1) = 1$. Так как

$$\begin{aligned} &f(1 \cdot 1) = f(1) = 0 = 0 + 0 = f(1) + f(1), \\ &f\big((-1) \cdot 1\big) = f(-1) = 1 = 1 + 0 = f(-1) + f(1), \\ &f\big((-1) \cdot (-1)\big) = f(1) = 0 = 1 + 1 = f(-1) + f(-1), \\ &f\big(1 \cdot (-1)\big) = f(-1) = 1 = 0 + 1 = f(1) + f(-1), \end{aligned}$$

то

$$f(x \cdot y) = f(x) + f(y)$$

для всех $x, y \in G$, таким образом, f — изоморфизм групп G и G'. □

Заметим, что в этом примере выбор для биекции $f\colon G \to G'$ был не велик: так как изоморфизм переводит нейтральный элемент в нейтральный, то мы обязаны положить $f(1) = 0$; но тогда $f(-1)$ обязано быть равным 1.

ПРИМЕРЫ ГРУПП

1. Целые числа $\mathbb{Z}$, рациональные числа $\mathbb{Q}$, действительные числа $\mathbb{R}$, комплексные числа $\mathbb{C}$ с операцией сложения, при этом никакие две из групп $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ не являются изоморфными, однако $(\mathbb{R}, +) \cong (\mathbb{C}, +)$ (поскольку $\dim_{\mathbb{Q}} \mathbb{R} = \dim_{\mathbb{Q}} \mathbb{C}$).

Заметим, что: а) натуральные числа $\mathbb{N}$ с операцией сложения группой не являются (отсутствует нейтральный элемент); б) натуральные числа с нулем $\mathbb{N}_0$ также не являются группой (обратный элемент (в аддитивной

записи обычно называемый противоположным элементом) существует только для 0; таким образом, например, 1 уже не имеет обратного элемента).

2. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ ($K^* = K \setminus \{0\}$ для любого поля K) относительно умножения являются группами (называемыми *мультипликативными группами* соответствующих *полей*).

3. Линейная группа $\mathrm{GL}_n(K)$ обратимых $(n \times n)$-матриц над полем K ($\mathrm{GL}_n(K) = \mathbf{U}\big(\mathbf{M}_n(K)\big)$, где $\mathbf{M}_n(K)$ — кольцо $(n \times n)$-матриц над полем K). Специальная линейная группа $\mathrm{SL}_n(K)$ матриц $A \in \mathbf{M}_n(K)$ таких, что $|A| = 1$.

4. Группа комплексных чисел $z \in \mathbb{C}$ таких, что $|z| = 1$, с операцией умножения. Группа $\{z \in \mathbb{C} \mid z^n = 1\}$ комплексных корней n-й степени из 1, $n \in \mathbb{N}$.

5. Группа подстановок $\mathbf{S}_n$, $n \geq 1$; группа четных подстановок $\mathbf{A}_n$. Для произвольного непустого множества M группа $\mathbf{S}(M)$ всех *биекций* $f\colon M \to M$ с операцией умножения.

Замечание 4. Множество $\mathbf{T}(M)$ всех отображений $f\colon M \to M$ с операцией умножения (т. е. композицией) является *полугруппой* (т. е. множеством с ассоциативной бинарной операцией), но не является группой при $|M| > 1$ (существуют отображения $f\colon M \to M$, не являющиеся биекций и, следовательно, не имеющие обратного отображения).

Замечание 5. Полугруппа $\mathbf{T}(M)$ коммутативна тогда и только тогда, когда $|M| = 1$. Действительно, если $|M| \geq 2$, то для $a, b \in M$, $a \neq b$, имеем

$$f_a f_b = f_a \neq f_b = f_b f_a,$$

где $f_c(x) = c$ для всех $x \in M$, $c \in M$.

Замечание 6. Группа $\mathbf{S}_n$ коммутативна тогда и только тогда, когда $n \leq 2$ (в частности, группы $\mathbf{S}_n$ при $n \geq 3$ уже некоммутативны). Действительно, при $n \geq 3$ для циклов $(1\,2)$, $(1\,3)$:

$$(1\,3)(1\,2) \neq (1\,2)(1\,3).$$

Замечание 7. Линейная группа $\mathrm{GL}_n(R) = U\big(\mathbf{M}_n(K)\big)$ коммутативна тогда и только тогда, когда $n = 1$.

Действительно, если $\mathrm{GL}_n(K)$ — коммутативная группа, то $n = 1$ (при $n \geq 2$: $E + E_{12}, E + E_{21} \in \mathrm{GL}_n(R)$, но

$$(E + E_{12})(E + E_{21}) = E + E_{12} + E_{21} + E_{11} \neq \\ \neq E + E_{12} + E_{21} + E_{22} = (E + E_{21})(E + E_{12}))$$

и $\mathbf{U}(R) = \mathrm{GL}_1(R)$ — коммутативная группа.

6. Группа симметрий. Пусть V — евклидово аффинное пространство $\mathbb{R}^2$ или $\mathbb{R}^3$. Под *изометрией* пространства V понимается биекция $\alpha\colon V \to V$, сохраняющая расстояние (примеры: переносы; вращения; отражения). Если $\varnothing \neq X \subset V$, то будем говорить, что изометрия α является *симметрией* множества X, если $X = \alpha(X)$ $(= \{\alpha(x) \mid x \in X\})$, при этом возможно, что $x \neq \alpha(x)$. Совокупность $\mathrm{Sym}(X)$ всех симметрий α множества $\varnothing \neq X \subseteq V$ образует группу (*группа симметрий* $\mathrm{Sym}(X)$, подгруппа группы $\mathbf{S}(X)$).

а) Пусть T — правильный треугольник с вершинами A, B и C, с высотами-медианами L_A, L_B и L_C, с центром описанной окружности O.

Рассмотрим совокупность $\mathbf{D}_3$ симметрий правильного треугольника T (т. е. все сохраняющие расстояние отображения $f\colon P \to P$ плоскости $P = \mathbb{R}^2$ такие, что $f(T) = T$). С операцией композиции $\mathbf{D}_3$ — группа. Рассмотрим ее элементы:

- $e = 1_P$, $1_P(x) = x$ для всех $x \in P$;
- φ_1, φ_2 — два вращения плоскости P против часовой стрелки, соответственно на углы 120° и 240°;

- $\theta_1, \theta_2, \theta_3$ — три зеркальных отображения плоскости P, соответственно относительно прямых L_A, L_B, L_C.

Как результат, получаем таблицу умножения для группы $\mathbf{D}_3$:

	e	φ_1	φ_2	θ_1	θ_2	θ_3
e	e	φ_1	φ_2	θ_1	θ_2	θ_3
φ_1	φ_1	φ_2	e	θ_3	θ_1	θ_2
φ_2	φ_2	e	φ_1	θ_2	θ_3	θ_1
θ_1	θ_1	θ_2	θ_3	e	φ_1	φ_2
θ_2	θ_2	θ_3	θ_1	φ_2	e	φ_1
θ_3	θ_3	θ_1	θ_2	φ_1	φ_2	e

.

Если $S = \{1 = A,\ 2 = B,\ 3 = C\}$ — множество вершин правильного треугольника T, то каждому элементу группы $\mathbf{D}_3$ поставим в соответствие подстановку вершин треугольника T:

$$e \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \varphi_1 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \varphi_2 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\theta_1 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \theta_2 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \theta_3 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Можно проверить, что данная биекция осуществляет изоморфизм группы симметрий треугольника $\mathbf{D}_3$ и группы подстановок $\mathbf{S}_3$.

б) Пусть в данном примере T — квадрат в плоскости $P = \mathbb{R}^2$ с вершинами A, B, C, D, центром O, с серединами ребер E, F, G, K.

Рассмотрим группу симметрий $\mathbf{D}_4$ квадрата $ABCD$. Она состоит: из четырех вращений на 0°, 90°, 180°, 270°; из четырчх отражений относительно прямых L_{AC}, L_{BD}, L_{EG}, L_{KF}. Выпишите для группы $\mathbf{D}_4$, $|\mathbf{D}_4| = 8$, таблицу умножения.

Каждому элементу из $\mathbf{D}_4$ поставим в соответствие подстановку множества вершин $\{A = 1,\ B = 2,\ C = 3,\ D = 4\}$. Например, повороту на 90° соответствует подстановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Эта биекция осуществляет вложение ($\equiv$ инъективный гомоморфизм) группы $\mathbf{D}_4$ в группу подстановок $\mathbf{S}_4$. Отметим, что $|\mathbf{D}_4| = 8$, $|\mathbf{S}_4| = 24$, поэтому не все подстановки из $\mathbf{S}_4$ лежат в образе этой биекции. Например, подстановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

не является результатом никакой симметрии квадрата.

7. Группа симметрий правильного n-угольника (диэдральная группа $\mathbf{D}_n$ порядка $2n$) состоит: из n поворотов правильного n-угольника против часовой стрелки вокруг его центра (включая тождественное отображение); из n отражений относительно оси симметрии (если n нечетное, то ось отражения определяется вершиной и серединой противоположного ребра; если n четное, то имеется два типа отражений, определяемых парой противоположных вершин и определяемых серединами противоположных ребер, $(1/2)\,n + (1/2)\,n = n$).

8. Пусть X — непустое множество, $\mathcal{P}(X)$ — совокупность всех его подмножеств (включая пустое), $S \triangle T = (S \cup T) - (S \cap T)$ для $S, T \in \mathcal{P}(X)$. Тогда $(\mathcal{P}(X), \triangle)$ — коммутативная группа.

Упражнение 1. Найдите $|\,\mathrm{GL}_n(\mathbb{Z}_p)|$ и $|\,\mathrm{SL}_n(\mathbb{Z}_p)|$.

Упражнение 2. Докажите, что если в группе G $(xy)^2 = x^2y^2$ для всех $x, y \in G$, то группа G коммутативна.

Упражнение 3. Если для любых элементов x, y группы G найдется число n такое, что $(xy)^i = x^iy^i$ для $i = n, n+1, n+2$, то группа G коммутативна.

9. Группа Клейна. Пусть

$G = \{e,\ a = (1\,2)(3\,4),\ b = (1\,3)(2\,4),\ c = (1\,4)(2\,3)\} \subseteq \mathbf{S}_n,\ n \geq 4,$ —

группа Клейна $\mathbf{V}_4$ (*четверная группа*). Ее таблица умножения:

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

.

10. *Группа кватернионов* $\mathbf{Q}_8$ состоит из восьми матриц из $\mathbf{M}_4(\mathbb{R})$: $\pm E$, $\pm i$, $\pm j$, $\pm k$, где

$$E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$j = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

с операцией умножения матриц. Отметим, что:

$$i^2 = j^2 = k^2 = -E, \quad ij = k.$$

СТЕПЕНЬ ЭЛЕМЕНТА ГРУППЫ

Определение 3. Пусть G — группа, $a \in G$, $n \in \mathbb{Z}$ — целое число. Положим

$$a^n = \begin{cases} \underbrace{a \cdot a \cdot \ldots \cdot a}_{n}, & \text{если } n > 0, \\ e, & \text{если } n = 0, \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{m=-n}, & \text{если } n < 0, \text{ где } m = -n > 0, \end{cases}$$

(или рекурсивно для $n \geq 0$: $a^0 = e$; $a^{n+1} = a^n a$; $a^{-n} = (a^n)^{-1}$).

Замечание 8. Если $m > 0$, то $(a^{-1})^m = (a^m)^{-1}$. Действительно,

$$(\underbrace{a \dots a}_{m})(\underbrace{a^{-1} \dots a^{-1}}_{m}) = e = (\underbrace{a^{-1} \dots a^{-1}}_{m})(\underbrace{a \dots a}_{m}).$$

Теорема 1. *Пусть G — группа, $a \in G$, $m, n \in \mathbb{Z}$ — целые числа. Тогда*:
1) $a^m \cdot a^n = a^{m+n}$;
2) $(a^m)^n = a^{mn}$.

Доказательство. 1) Формально, мы должны рассмотреть $3 \times 3 = 9$ случаев.

Случай 1. $m > 0$, $n > 0$ (следовательно, $m + n > 0$). Тогда

$$a^m \cdot a^n = (\underbrace{a \dots a}_{m}) \cdot (\underbrace{a \dots a}_{n}) = \underbrace{a \dots a}_{m+n} = a^{m+n}.$$

Случай 2. $m > 0$, $n < 0$ (поэтому $n' = -n > 0$). Тогда

$$\begin{aligned} a^m \cdot a^n &= (\underbrace{a \dots a}_{m}) \cdot (\underbrace{a^{-1} \dots a^{-1}}_{n'=-n}) = \\ &= \begin{cases} \underbrace{a \cdot a \cdot \ldots \cdot a}_{m-n'=m+n}, & \text{если } m > n' = -n \text{ (т. е. } m+n > 0), \\ e, & \text{если } m = n' = -n \text{ (т. е. } m+n = 0), \\ \underbrace{a^{-1} \dots a^{-1}}_{n'-m=-n-m}, & \text{если } m < n' = -n \text{ (т. е. } m+n < 0) \end{cases} = \\ &= a^{m+n}. \end{aligned}$$

Аналогично разбираются остальные случаи: 3) $m < 0, n > 0$; 4) $m < 0$, $n < 0$; 5) $m = 0$, $n > 0$; 6) $m = 0$, $n = 0$; 7) $m = 0$, $n < 0$; 8) $m > 0$, $n = 0$; 9) $m < 0$, $n = 0$. □

Упражнение 4. Пусть G — группа, $a, b \in G$.
1) Если $a^2 = e$ и $a^{-1}b^2a = b^3$, то $b^5 = e$.
2) Если $a^{-1}b^2a = b^3$, $b^{-1}a^2b = a^3$, то $a = e = b$.

ПОРЯДОК ЭЛЕМЕНТА ГРУППЫ

Рассмотрим целые степени элемента a группы G

$$\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \ldots$$

Возможны два случая.

Случай 1. Все элементы в этом ряду различны (т. е. $a^k \neq a^l$ для всех целых чисел $k \neq l$). В этом случае будем говорить, что *порядок элемента бесконечный* (обозначение: $O(a) = \infty$).

Случай 2. В этом ряду $a^k = a^l$ для некоторых $k \neq l$. Пусть $k > l$. Тогда $a^{k-l} = e$, где $k-l > 0$, т. е. встретилась и натуральная степень элемента a, равная e. Рассмотрим множество $T = \{t \in \mathbb{Z} \mid t > 0,\ a^t = e\}$. Это непустое подмножество натуральных чисел. Следовательно, в T существует наименьший элемент n, который мы назовем *порядком элемента* a и обозначим через $O(a)$.

Таким образом:

1) $a^n = e$, $n > 0$;

2) если $a^k = e$, $k > 0$, то $k \geq n$.

Ясно, что если группа G конечна, то $O(g) < \infty$ для всех $g \in G$.

Пример 2. Если $0 \neq n \in (\mathbb{Z}, +)$, то $O(n) = \infty$.

Пример 3. $G = (\{1, -1\}, \cdot)$, $a = -1$. Тогда $a^1 = -1$, $a^2 = 1$, т. е. $O(a) = 2$.

Пример 4. $G = \mathbf{S}_3$,

$$a = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 1, & 3 \end{pmatrix} = (1\,2), \quad b = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 3, & 1 \end{pmatrix} = (1\,2\,3).$$

Тогда $a^1 = a$, $a^2 = e$, т. е. $O(a) = 2$; $b^1 = b \neq e$, $b^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq e$, $b^3 = e$, т. е. $O(b) = 3$.

Лемма 2. *Если* $O(a) = n < \infty$, *то*:

1) *все элементы* $e = a^0, a, a^2, \ldots, a^{n-1}$ *различны*;

2) *для любого* $k \in \mathbb{Z}$ *элемент* a^k *совпадает с одним из* $e, a, a^2, \ldots, a^{n-1}$, *а именно, если* $k = nq + r$, *где* $0 \leq r < n$, *то* $a^k = a^r$.

Доказательство.

1) Следует из определения порядка элемента $O(a)$.

2) Пусть $k \in \mathbb{Z}$. Тогда $k = nq + r$, где $0 \leq r < n$. Следовательно, $a^k = (a^n)^q a^r = ea^r = a^r$. □

Лемма 3. *Пусть* $O(a) = n < \infty$. *Тогда* $a^k = e$ *тогда и только тогда, когда* $k = nq$.

Доказательство.

1) Если $k = nq$, то $a^k = (a^n)^q = e^q = e$.

2) Допустим противное, т. е. что $k = nq + r$, где $0 < r < n$. Тогда $a^k = (a^n)^q a^r = a^r \neq e$ (по лемме 2). Получили противоречие. □

Лемма 4. *Пусть* G — *конечная группа. Тогда найдется число* $n \in \mathbb{N}$ *такое, что* $x^n = e$ *для всех* $x \in G$.

Доказательство. Пусть

$$n = \prod_{g \in G} O(g).$$

Тогда для любого $g \in G$ число n делится на $O(g)$, $n = O(g)q$, и поэтому $g^n = e$. □

Лемма 5 (порядок подстановки). *Пусть* $\pi \in \mathbf{S}_n$.

1) *Если* $\pi = (i_1, i_2, \ldots, i_r)$ — *цикл длины* r, *то* $O(\pi) = r$.

2) *Если* $\pi = \pi_1 \pi_2 \ldots \pi_k$, *где* π_i — *циклы с непересекающимися орбитами длины* l_i, *то* $O(\pi) = НОК\{l_1, l_2, \ldots, l_k\}$.

Доказательство.

1) Если $1 \leq k < r$, то $\pi^k = (i_1, i_{k+1}, \ldots)$ и

$$\pi^r = \begin{pmatrix} i_1 & i_2 & \ldots & i_r \\ i_1 & i_2 & \ldots & i_r \end{pmatrix} = e.$$

Итак, $O(\pi) = r$.

2) Так как $\pi_i \pi_j = \pi_j \pi_i$ для всех π_i, π_j, то $\pi^m = \pi_1^m \pi_2^m \ldots \pi_k^m$ для всех $m > 0$. Поэтому $\pi^m = e$ тогда и только тогда, когда $\pi_1^m = \pi_2^m = \ldots = \pi_k^m = e$. Итак, $O(\pi) = \text{НОК}\,\{l_1, \ldots, l_k\}$. □

Упражнение 5. Найдите наибольший из возможных порядков элементов в группе $\mathbf{S}_8$.

Теорема 2. *Пусть G — конечная абелева группа. Тогда*:

1) *произведение всех элементов группы G, порядки которых отличны от 2, равно единичному элементу*;

2) *если группа G содержит элемент порядка 2, то произведение всех элементов группы G равно произведению всех элементов порядка 2 группы G.*

Доказательство. Если $e \neq x \in G$, то $O(x) = 2$ тогда и только тогда, когда $x = x^{-1}$. Если $O(x) > 2$, то $O(x^{-1}) = O(x) > 2$, и $x \neq x^{-1}$. Так как G — абелева группа, то:

$$\prod_{\substack{g \in G \\ O(g) \neq 2}} g = \prod_{\substack{\{x, x^{-1}\} \\ O(x) \neq 2}} x \cdot x^{-1} = e;$$

$$\prod_{g \in G} g = \left(\prod_{\substack{x \in G \\ O(x) = 2}} x \right) \cdot \left(\prod_{\substack{y \in G \\ O(y) \neq 2}} y \right) = \prod_{\substack{x \in G \\ O(x) = 2}} x. \qquad \square$$

Теорема 3 (теорема Вилсона). *Если $p \in \mathbb{N}$, то p — простое число тогда и только тогда, когда*:

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказательство. 1) Пусть $G = (\mathbb{Z}_p \setminus \{0\}, \cdot) = \mathbb{Z}_p^*$ — мультипликативная группа поля вычетов $\mathbb{Z}_p$. Если $a \in \mathbb{Z}_p^*$ и $O(a) = 2$, то $a^2 \equiv 1 \pmod{p}$, следовательно, $a^2 - 1 = (a-1)(a+1)$ делится на p, поэтому или $a \equiv 1 \pmod{p}$, или $a \equiv -1 \pmod{p}$. В силу теоремы 2 в $\mathbb{Z}_p$

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot (-1) \equiv -1 \pmod{p}.$$

2) Если $p = k \cdot l$, $k, l \in \mathbb{N}$, $1 < k < p$, $1 < l < p$, то $(p-1)! \equiv 0 \pmod{k}$. Если $(p-1)! \equiv -1 \pmod{p}$, то $(p-1)! + 1 = p \cdot q = k \cdot l \cdot q$, что приводит к противоречию. □

Теорема 4. *Пусть G — группа, $|G| = 2k$. Тогда G содержит элемент g порядка $O(g) = 2$.*

Доказательство. Пусть для всех $e \neq g \in G$ имеем $O(g) > 2$. Тогда $g \neq g^{-1}$, $O(g^{-1}) = O(g)$, поэтому число неединичных элементов группы G четно, а $|G|$ — нечетное число. Получили противоречие. □