ЛЕКЦИИ ПО АЛГЕБРЕ

3 СЕМЕСТР

2020/2021 УЧЕБНЫЙ ГОД

БУНИНА ЕЛЕНА ИГОРЕВНА

helenbunina@gmail.com

Часть 1 — ОСНОВЫ ТЕОРИИ ГРУПП

ЛЕКЦИЯ 1

ГРУППЫ.

ИЗОМОРФИЗМЫ ГРУПП.

ПРИМЕРЫ ГРУПП.

СТЕПЕНЬ ЭЛЕМЕНТА ГРУППЫ.

ПОДГРУППЫ.

ЦИКЛИЧЕСКИЕ ПОДГРУППЫ.

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*) единственен.

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.

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

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

и

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

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'. □

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 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 $\mathbf{S}_n$, $n\geqslant 1$; 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 биекцией и, следовательно, не имеющие обратного отображения).

Замечание 5. Полугруппа $\mathbf{T}(M)$ коммутативна тогда и только тогда, когда $|M| = 1$. Действительно, если $|M| \geqslant 2$, 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 $n \leqslant 2$ (в частности, группы $\mathbf{S}_n$ при $n \geqslant 3$ уже некоммутативны). Действительно, при $n \geqslant 3$ для циклов $(1\,2)$, $(1\,3)$:

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

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

Действительно, при $n \geqslant 2$: $E + E_{12}, E + E_{21} \in \mathrm{GL}_n(R)$, но

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

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 расстояния (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°;
- θ_1, θ_2, θ_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 четырех 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

$G = \{e,\ a = (1\,2)(3\,4),\ b = (1\,3)(2\,4),\ c = (1\,4)(2\,3)\} \subseteq \mathbf{S}_n,\ n \geqslant 4,$ — *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 $n \geqslant 0$: $a^0 = e$; $a^{n+1} = a^n a$; $a^{-n} = (a^n)^{-1}$).

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

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

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

$$a^m \cdot a^n = (\underbrace{a \dots a}_{m}) \cdot (\underbrace{a^{-1} \dots a^{-1}}_{n'=-n}) =$$

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

$$= a^{m+n}.$$

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 $k \geqslant n$.

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 $0 \leqslant r < n$, 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 $0 \leqslant r < n$. 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 $1 \leqslant k < r$, 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 $\mathbf{S}_8$.

ПОРЯДОК ПРОИЗВЕДЕНИЯ ДВУХ ЭЛЕМЕНТОВ ГРУППЫ

Пусть G — группа, $a, b, c \in G$ и $a = bc$. В общем случае (без дополнительных предположений) мало что можно сказать о порядке $O(a)$ элемента a, зная порядки $O(b)$ и $O(c)$. Приведем несколько утверждений и примеров.

Лемма 6. *Пусть G — группа, $a, b, c, a_1, a_2, \ldots, a_k \in G$. Тогда*:

1) $O(a^{-1}) = O(a)$,

2) $O(b) = O(a^{-1}ba)$,

3) $O(ab) = O(ba)$, $O(abc) = O(bca) = O(cab)$ *и, более того,*

$$O(a_1a_2 \ldots a_k) = O(a_2a_3 \ldots a_ka_1) = \ldots = O(a_ka_1 \ldots a_{k-1}).$$

Доказательство.

1) Для любого $k \in \mathbb{Z}$ $a^k = e$ тогда и только тогда, когда $(a^{-1})^k = a^{-k} = e$, поэтому $O(a^{-1}) = O(a)$.

2) Так как $a^{-1}b^ka = (a^{-1}ba)^k$, то $b^k = e$ тогда и только тогда, когда $a^{-1}b^ka = e$, поэтому $O(a^{-1}ba) = O(b)$.

3) Так как $a^{-1}(ab)a = ba$, то в силу 2) $O(ab) = ba$. Аналогично $a^{-1}(abc)a = bca$, $b^{-1}(bca)b = cab$, и поэтому $O(abc) = O(bca) = O(cab)$. И более того,

$$\begin{aligned} a_1^{-1}(a_1a_2 \ldots a_k)a_1 &= a_2 \ldots a_ka_1, \\ a_2^{-1}(a_2a_3 \ldots a_ka_1)a_2 &= a_3 \ldots a_ka_1a_2, \\ &\ldots \\ a_{k-1}^{-1}(a_{k-1}a_ka_1 \ldots a_{k-2})a_{k-1} &= a_ka_1 \ldots a_{k-1}. \end{aligned}$$

Отсюда следует совпадение порядков этих сопряженных между собой элементов. □

Пример 5. 1) В группе $G = \mathrm{GL}_2(\mathbb{Q})$ произведение двух элементов конечного порядка может не быть элементом конечного порядка (таким образом, совокупность $\mathcal{T}(G)$ всех элементов конечного порядка неабелевой группы G не является подгруппой).

Действительно, пусть

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad O(a) = 4, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad O(b) = 3,$$

поскольку

$$a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad a^3 = -a, \quad a^4 = E; \quad b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad b^3 = E.$$

В то же время

$$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (ab)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \quad \text{для} \quad k \in \mathbb{Z},$$

поэтому $O(ab) = \infty$. □

2) В группе $G = \mathbb{Z}_2 \oplus \mathbb{Z}$ существуют два элемента a, b бесконечного порядка, сумма $a + b$ которых имеет конечный порядок.

Действительно:

$$a = (0, 1), \quad O(a) = \infty; \quad b = (1, -1), \quad O(b) = \infty;$$
$$a + b = (1, 0), \quad O(a + b) = 2.$$ □

ПОДГРУППЫ ГРУППЫ

Лемма 7. *Для непустого подмножества H группы G следующие условия эквивалентны:*

1) *H является группой относительно исходной операции в группе G;*

2) *подмножество H удовлетворяет следующим двум условиям*:

2.1) *если $h_1, h_2 \in H$, то $h_1 h_2 \in H$;*

2.2) *если $h \in H$, то $h^{-1} \in H$.*

Непустое подмножество H группы G удовлетворяющее эквивалентным условиям 1) и 2), называется *подгруппой группы G*.

Доказательство.

1) $\Longrightarrow$ 2). Если $h_1, h_2 \in H$, то, поскольку операция определена на H (т. е. не выводит из H), имеем $h_1 h_2 \in H$, т. е. 2.1).

Если e' — нейтральный элемент группы H, то $e' \cdot e' = e'$. Умножая в группе обе стороны этого равенства на $(e')^{-1}$, получаем $e' = e$ (здесь e — нейтральный элемент группы G).

Если h_1^{-1} — обратный элемент для элемента $h \in H$ в группе H, то $h_1^{-1} \cdot h = e' = e = h \cdot h_1^{-1}$, т. е. $h^{-1} = h_1^{-1} \in H$ (условие 2.2)).

2) $\Longrightarrow$ 1). Условие 2.1) показывает, что операция определена на множестве H. Конечно, она ассоциативна. Далее, для $h \in H$ в силу 2.2) $h^{-1} \in H$, и поэтому в силу 2.1) $e = h \cdot h^{-1} \in H$. Ясно, что e — нейтральный элемент в H, а h^{-1} — обратный элемент для h в H. Итак, H — группа относительно операции, индуцированной операцией группы G. $\square$

Замечание 9. Пусть G — группа и $\varnothing \neq H \subseteq G$.

H — подгруппа тогда и только тогда, когда $h_1 h_2^{-1} \in H$ для всех $h_1, h_2 \in H$.

Действительно, если H — подгруппа и $h_1, h_2 \in H$, то $h_2^{-1} \in H$ и поэтому $h_1 h_2^{-1} \in H$. Если же $h_1 h_2^{-1} \in H$ для всех $h_1, h_2 \in H$, то $e = h_1 (h_1)^{-1} \in H$, $h_2^{-1} = e h_2^{-1} \in H$, $h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$. Итак, H — подгруппа. □

Теорема 2. *Пусть G — группа, $\{H_i \mid i \in I\}$ — любое семейство подгрупп группы G. Тогда их пересечение $H = \bigcap\limits_{i \in I} H_i$ также является подгруппой.*

Доказательство. 1) Если $h_1, h_2 \in H = \bigcap\limits_{i \in I} H_i$, то $h_1, h_2 \in H_i$ для каждого i. Так как H_i — подгруппа, то $h_1 h_2 \in H_i$ для каждого i, и поэтому $h_1 h_2 \in \bigcap\limits_{i \in I} H_i = H$.

2) Если $h \in H = \bigcap\limits_{i \in I} H_i$, то $h \in H_i$ для каждого i. Так как H_i — подгруппа, то $h^{-1} \in H_i$ для каждого i, и поэтому $h^{-1} \in \bigcap\limits_{i \in I} H_i = H$.

Итак, $H = \bigcap\limits_{i \in I} H_i$ — подгруппа группы G. □

Следствие 1. *Пусть X — непустое подмножество группы G. Тогда*:

1) *существует подгруппа H, являющаяся наименьшей среди подгрупп, содержащих подмножество X (эта подгруппа называется подгруппой, порожденной подмножеством X, она обозначается через $\langle X \rangle$)*;

2) *подгруппа $\langle X \rangle$ состоит из всех элементов группы G, имеющих вид $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$, где $x_i \in X$, $k_i = \pm 1$, $n \geq 0$.*

Доказательство. 1) Множество всех подгрупп H_i, $i \in I$, содержащих подмножество X, не пусто, ему принадлежит сама группа G. Ясно, что $X \subseteq H = \bigcap\limits_{i \in I} H_i$ и H — наименьшая подгруппа среди всех H_i, $i \in I$.

2) Указанные элементы лежат в $\langle X \rangle$, в то же время они сами образуют подгруппу, содержащую подмножество X. □

Пример 6. 1) Четные числа $2\mathbb{Z}$ — подгруппа в группе целых чисел $(\mathbb{Z}, +)$.

2) $\mathbb{Z} \subset (\mathbb{Q}, +)$, $\mathbb{Q} \subset (\mathbb{R}, +)$, $\mathbb{R} \subset (\mathbb{C}, +)$ — подгруппы.

3) $\mathbf{A}_n \subset \mathbf{S}_n$ (четные подстановки являются подгруппой в группе всех подстановок).

4) $\mathrm{SL}_n(K) \subset \mathrm{GL}_n(K)$— подгруппа линейной группы $\mathrm{GL}_n(K)$.

5) В любой группе G имеем наименьшую подгруппу $H = \{e\}$ (и наибольшую подгруппу $H = G$). Если $H < G$, то подгруппа H называется *собственной*.

Упражнение 6. Группа, имеющая лишь конечное число подгрупп, конечна.

Упражнение 7.

1) Пусть H и K — подгруппы группы G. Тогда $H \cup K$ — подгруппа в том и только в том случае, если либо $H \subseteq K$, либо $K \subseteq H$.

2) Никакая группа G не является объединением $H \cup K$ двух собственных подгрупп $H \subset G$, $K \subset G$.

3) Приведите пример группы G, являющейся объединением трех собственных подгрупп.

ЦИКЛИЧЕСКИЕ ПОДГРУППЫ

Рассмотрим строение подгрупп, порожденных одним элементом.

Пусть a — элемент группы G. Рассмотрим в G следующее подмножество:

$$\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

Лемма 8. 1) $\langle a\rangle$ *является коммутативной подгруппой группы* G*, называемой циклической подгруппой, порожденной элементом* a;

2) $|\langle a\rangle| = O(a)$.

Доказательство. 1) Для $m, n \in \mathbb{Z}$

$$a^m a^n = a^{m+n} \in \langle a\rangle; \quad (a^n)^{-1} = a^{-n} \in \langle a\rangle.$$

Таким образом, для $\langle a\rangle$ выполнены условия предыдущей леммы, т. е. $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$ — подгруппа группы G. Так как

$$a^m a^n = a^{m+n} = a^n a^m,$$

то $\langle a\rangle$ — коммутативная группа.

2) Если $O(a) = \infty$, то

$$\langle a\rangle = \{\ldots, a^{-1}, e, a, \ldots\},$$

при этом в ряду целых степеней элемента a все элементы различны, т. е. $|\langle a\rangle| = \infty$. Если же $O(a) = n < \infty$, то, как мы отметили ранее, $\langle a\rangle = \{e, a, \ldots, a^{n-1}\}$ и

$$|\langle a\rangle| = n = O(a). \qquad \square$$

Пример 7 (примеры циклических групп). 1) Если $G = \mathbb{Z}$ и $a = 2$, то

$$\langle a \rangle = \{2n \mid n \in \mathbb{Z}\} = 2\mathbb{Z}$$

(все четные числа).

2) Если $G = \mathrm{GL}_2(\mathbb{R})$ и

$$a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

то

$$\langle a \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

3) Если $G = \{1, i, -1, -i\}$ — группа комплексных корней четвертой степени из 1, то $\langle i \rangle = G$, $\langle -1 \rangle = \{1, -1\}$, $\langle -i \rangle = G$.