ЛЕКЦИЯ 2

СТЕПЕНЬ И ПОРЯДОК ЭЛЕМЕНТА ГРУППЫ.

ПОДГРУППЫ ГРУППЫ.

ЦИКЛИЧЕСКИЕ ГРУППЫ.

СМЕЖНЫЕ КЛАССЫ.

СТЕПЕНЬ ЭЛЕМЕНТА ГРУППЫ

Определение 1. 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 1. 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 1. 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 1. Если $0 \neq n \in (\mathbb{Z}, +)$, то $O(n) = \infty$.

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

Пример 3. $G = \mathbf{S}_3$,

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

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 1. *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 2. *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 1). Получили противоречие. □

Лемма 3. *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 4 (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 2. 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 5. *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 4. 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 6. *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 2. 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 5. 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 3. Группа, имеющая лишь конечное число подгрупп, конечна.

Упражнение 4.

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 7. 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 6 (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 $\langle i \rangle = G$, $\langle -1 \rangle = \{1, -1\}$, $\langle -i \rangle = G$.

ЦИКЛИЧЕСКИЕ ГРУППЫ

Группа G называется *циклической*, если найдется такой элемент $a \in G$, что $\langle a \rangle = G$, т. е. все элементы группы G являются (целыми) степенями этого элемента a, называемого в этом случае циклическим образующим группы G. Если $O(a) = n < \infty$, то $G = \langle a \rangle$ — *циклическая группа из n элементов*; если же $O(a) = \infty$, то $G = \langle a \rangle$ — *бесконечная* (счетная!) *циклическая группа.*

Замечание 3. Любая циклическая группа $G = \langle a \rangle$ является конечной или счетной коммутативной группой. Поэтому любая некоммутативная группа не является циклической и любая несчетная группа не является циклической группой.

Пример 7 (примеры циклических групп). 1) $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$ (это показывает, что циклических образующих может быть много!).

2) Группа подстановок $\mathbf{S}_n$ является циклической тогда и только тогда, когда $n < 3$.

3) Покажите, что счетная группа $(\mathbb{Q}, +)$ рациональных чисел не является циклической, однако является *локально циклической группой* (это означает, что каждое конечное подмножество порождает циклическую группу).

4) Группа $G = \sqrt[n]{1}$ комплексных корней из 1 является циклической группой из n элементов. Действительно,

$$G = \sqrt[n]{1} = \left\{ \varepsilon_k = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n} \;\middle|\; k = 0, 1, \ldots, n-1 \right\}$$

и $G = \langle a \rangle$ для $a = \varepsilon_1 = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, поскольку $\varepsilon_k = a^k$ для $k = 0, 1, \ldots, n-1$.

Лемма 8. *Если $G = \langle a \rangle$ — конечная циклическая группа порядка n (т. е. $O(a) = n$), $b = a^k \in G$, $k \in \mathbb{Z}$, то элемент b является циклическим образующим группы G (т. е. $G = \langle a \rangle = \langle b \rangle$) тогда и только тогда, когда числа k и n взаимно просты.*

Доказательство. Так как $|\langle b \rangle| = O(b)$, то $G = \langle a \rangle = \langle b \rangle$ тогда и только тогда, когда

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

Учитывая, что $O(b) = \frac{n}{d}$, где $d = \text{НОД}(k, n)$, мы видим, что $O(b) = O(a) = n$ тогда и только тогда, когда $d = 1$, т. е. числа k и n взаимно просты. □

Замечание 4. Пусть $G = \langle a \rangle$, $|G| = O(a) = n < \infty$. Если мы знаем какой-нибудь образующий a конечной циклической группы G из n элементов, то все циклические образующие группы G имеют вид $b = a^k$, где $1 \leqslant k \leqslant n - 1$ и k взаимно просто с n. Число таких чисел k обозначается через $\varphi(n)$ (*функция Эйлера*), оно часто возникает в теории чисел и в комбинаторике.

Упражнение 5. Покажите, что при $n > 30$ число $\varphi(n)$ строго больше числа делителей числа n.

Теорема 3 (о цикличности подгрупп циклической группы)**.** *Пусть* $G = \langle a \rangle$ *— циклическая группа,* a *— один из ее циклических образующих. Любая подгруппа* H *циклической группы* G *является циклической,* $H = \langle b \rangle$ *(при этом образующий в подгруппе* H *можно выбрать в виде* $b = a^k$*, где* $k \geqslant 0$*).*

Доказательство. Пусть $G = \langle a \rangle$ — циклическая группа, a — ее циклический образующий, $\varnothing \neq H \subseteq G$ — подгруппа.

Случай 1. $|H| = 1$, т. е. $H = \{e = a^0\} = \langle e \rangle$.

Случай 2. $|H| > 1$. Пусть $e \neq a^t \in H$, т. е. $0 \neq t \in \mathbb{Z}$. Тогда

$$a^{-t} = (a^t)^{-1} \in H.$$

Поэтому или $t > 0$, или $-t > 0$, т. е. в H содержится некоторая натуральная степень элемента a. Таким образом, среди положительных степеней $a^t \in H$, $t > 0$,

$$\{t \in \mathbb{N} \mid a^t \in H\} \subset \mathbb{N},$$

есть наименьшая степень $k > 0$. Так как $a^k \in H$, то $\langle a^k \rangle \subseteq H$.

Для любого элемента $h \in H$, поскольку $H \subseteq G = \langle a \rangle$, имеем $h = a^l$, $l \in \mathbb{Z}$. Пусть $l = kq + r$, $0 \leq r < k$. Тогда $h = a^l = (a^k)^q a^r$, т. е. $a^r = a^l (a^k)^{-q} \in H$, поскольку $a^l \in H$, $a^k \in H$ (а тогда и $(a^k)^{-q} \in H$). В силу выбора числа k остается лишь возможность $r = 0$, т. е. $l = kq$. Но тогда $h = a^l = (a^k)^q$, т. е. H является циклической группой с образующим a^k, $H = \langle a^k \rangle$. □

Упражнение 6. Приведите пример неабелевой группы, в которой каждая из собственных подгрупп — циклическая.

Упражнение 7. Пусть p — простое число, $\mathbb{Z}_{p^\infty}$ — группа всех комплексных корней из 1 степени p^n для всех натуральных n. Покажите, что любая собственная подгруппа группы $\mathbb{Z}_{p^\infty}$ — конечная циклическая группа, а также что любая нетривиальная фактор-группа группы $\mathbb{Z}_{p^\infty}$ изоморфна $\mathbb{Z}_{p^\infty}$. В группе $\mathbb{Z}_{p^\infty}$ любое конечное подмножество порождает циклическую группу.

СМЕЖНЫЕ КЛАССЫ

Пусть G — группа, H — подгруппа группы G, $x \in G$. *Левым смежным классом группы G по подгруппе H*, порожденным элементом x, называется множество

$$xH = \{xh \mid h \in H\}.$$

Аналогично, *правый смежный класс* определяется как

$$Hx = \{hx \mid h \in H\}.$$

Пример 8. Пусть $G = \mathbb{R}^2$ с операцией сложения, $H = \{(a, 0) \mid a \in \mathbb{R}\}$, $x = (1, 1)$. Тогда

$$x + H = \{(a, b) \in \mathbb{R}^2 \mid b = 1\}.$$

Все смежные классы группы $\mathbb{R}^2$ по H — это все прямые, параллельные прямой H.

Пример 9. Пусть $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ — группа всех комплексных чисел, отличных от нуля, с операцией умножения, $H \equiv T = \{z \in \mathbb{C} \mid |z| = 1\}$, $x = 1 + i$. Тогда

$$xH = \{w \in \mathbb{C} \mid |w| = \sqrt{2}\}.$$

Все смежные классы группы G по H в этом случае — это подмножества вида $\{w \in \mathbb{C} \mid |w| = r \neq 0\}$, т. е. концентрические окружности положительного радиуса с центром в нуле.

Пример 10. Пусть $G = \mathbf{S}_3$,

$$H = \langle (1\,2) \rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\},$$

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

Тогда:

$$xH = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3) \right\};$$

$$Hx = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2) \right\}.$$

Замечание 5. 1) Мы видим в этом примере, что $xH \neq Hx$ (т. е. правый и левый смежные классы по подгруппе, порожденные элементом x, могут не совпадать).

2) Если $x = e$ — нейтральный элемент группы G, то $eH = H = He$.

3) $xH = H$ тогда и только тогда, когда $x \in H$; $Hx = H$ тогда и только тогда, когда $x \in H$.

4) Пусть H и K — подгруппы группы G, $x \in G$.

а) $x(H \cap K) = xH \cap xK$; $(H \cap K)x = Hx \cap Kx$. Действительно: если $g \in H \cap K$, то $xg \in xH \cap xK$, поэтому

$$x(H \cap K) \subseteq xH \cap xK;$$

если $xh = xk \in xH \cap xK$, $h \in H$, $k \in K$, то $h = k \in H \cap K$, и поэтому $xh = xk \in x(H \cap K)$, поэтому

$$x(H \cap K) \supseteq xH \cap xK.$$

Второе равенство проверяется аналогично.

б) Постановка каждому левому смежному классу $x(H \cap K)$ в соответствие пары левых смежных классов (xH, xK) является корректным инъективным отображением. Действительно, если $x(H \cap K) = y(H \cap K)$, то $y = xd$, где $d \in H \cap K$, и поэтому

$$xH = xdH = yH, \quad xK = xdK = yK$$

(т. е. наше соответствие определено корректно). Если же $(xH, xK) = (x'H, x'K)$, $x, x' \in G$, то $xH = x'H$, $xK = x'K$, поэтому $x^{-1}x' \in H \cap K$, и следовательно,

$$x(H \cap K) = x'(H \cap K)$$

(т. е. наше отображение инъективно).