Порядок элемента. Теорема Лагранжа

Определение. Если множество G состоит из конечного числа элементов, то группа G называется конечной. Число элементов конечной группы G будет обозначать $|G|$ и называть порядком этой группы. Если множество G бесконечно, то группу G называют бесконечной.

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 1. *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 $a^{-1}b^k a = (a^{-1}ba)^k$, то $b^k = e$ тогда и только тогда, когда $a^{-1}b^k a = e$, 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,

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

Отсюда следует совпадение порядков этих сопряженных между собой элементов. $\square$

Пример 1. 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*:

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

□

Лемма 2. *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. □

Замечание 1. 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 1. *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 $h_1h_2 \in H_i$ для каждого i, и поэтому $h_1h_2 \in \bigcap\limits_{i\in I} H_i = H$.

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 $X \subseteq H = \bigcap_{i \in I} H_i$ 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. $\square$

Пример 2. 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*.

Рассмотрим строение подгрупп, порожденных одним элементом.

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

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

(т. е. совокупность всех *целых* степеней элемента a).

Лемма 3. 1) $\langle a \rangle$ *является коммутативной подгруппой группы* G, *называемой* циклической подгруппой, порожденной элементом a;

2) $|\langle a \rangle| = O(a)$ (*т. е. число элементов в подгруппе* $\langle a \rangle$ *равно порядку элемента* 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

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

□

Пример 3 (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 2. 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 4 (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 $n < 3$. Действительно, $\mathbf{S}_1 = \langle e \rangle$, $\mathbf{S}_2 = \langle (1\,2) \rangle$, при $n \geq 3$ группа $\mathbf{S}_n$ некоммутативна, поэтому она не может быть циклической.

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 4. *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 3. 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 $1 \leq k \leq n - 1$ и k взаимно просто с n. Число таких чисел k обозначается через $\varphi(n)$ (*функция Эйлера* $\varphi(n)$ часто возникает в теории чисел и в комбинаторике.

Теорема 2 (о первообразных комплексных корнях из 1). *Пусть*

$$G = \{e = \varepsilon_0,\ \varepsilon_1 = \varepsilon,\ \varepsilon_2 = \varepsilon^2, \ldots,\ \varepsilon_{n-1} = \varepsilon^{n-1}\} -$$

группа комплексных корней n-й степени из 1,

$$\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}, \quad \varepsilon_k = \varepsilon^k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}.$$

Так как $G = \langle\varepsilon\rangle$ — циклическая группа с образующим ε, то $\varepsilon_k = \varepsilon^k$ является образующим группы G (такой корень называется первообразным*: все другие корни являются его степенями) тогда и только тогда, когда k взаимно просто с n. Число первообразных корней из* 1 *степени n равно $\varphi(n)$.*

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 $k \geq 0$).*

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, $H = \langle a^k \rangle$. $\square$

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 5. 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.

Теорема 4 (о разбиении группы на левые смежные классы). *Пусть G — группа и H — подгруппа группы G, тогда*:

1) $x \in xH$ *для всех* $x \in G$;

2) *если* $z \in xH$, *то* $zH = xH$;

3) *если* $xH \cap yH \neq \varnothing$, *то* $xH = yH$ (*т. е. два левых смежных класса либо не пересекаются, либо совпадают*);

4) *равносильны следующие условия*:

a) $xH = yH$;

b) $y^{-1}x \in H$;

c) $x^{-1}y \in H$;

5) *если* $|H| = k < \infty$, *то* $|xH| = k$.

Доказательство.

1) $x = xe \in xH$, так как $e \in H$.

2) Если $z \in xH$, то $z = xh_0$, где $h_0 \in H$. Тогда $x = zh_0^{-1}$, где $h_0^{-1} \in H$. Пусть $h \in H$. Тогда:

$$zh = (xh_0)h = x(h_0h) \in xH, \text{ так как } h_0h \in H;$$
$$xh = (zh_0^{-1})h = z(h_0^{-1}h) \in zH, \text{ так как } h_0^{-1}h \in H.$$

Итак, $zH \subseteq xH$ и $xH \subseteq zH$, т. е. $zH = xH$.

3) Пусть $z \in xH \cap yH$. В силу 2) $xH = zH = yH$.

4) Если $xH = yH$, то $x \in xH = yH$, и поэтому $x = yh$, $h \in H$, т. е. $y^{-1}x = h \in H$. Аналогично, $y \in yH = xH$, $y = xh'$, $h' \in H$, т. е. $x^{-1}y = h' \in H$. Если $y^{-1}x = h \in H$, то $x = yh \in yH$. В силу 2) $xH = yH$. Если $x^{-1}y = h' \in H$, то $y = xh' \in xH$. В силу 2) $yH = xH$.

5) Если $xh = xh'$, то, умножая на x^{-1}, видим, что $h = h'$. □

Теорема 5 (Лагранж, Joseph Lois Lagrange (1736—1813)). *Если H — подгруппа группы G, $|G| = n < \infty$, $|H| = k$, то k — делитель числа n, а именно, $n = kj$, где j — число левых (правых) смежных классов, называемое индексом подгруппы H в G (обозначение: $j = (G : H)$).*

Доказательство. Рассмотрим разбиение группы G на j различных левых смежных классов xH. Так как $|xH| = |H| = k$, то $n = kj$. □

Следствие 2. *Если $a \in G$, $|G| = n$, то порядок $O(a)$ элемента a является делителем числа n, порядка группы G.*

Доказательство. Рассмотрим циклическую подгруппу $H = \langle a \rangle$. Тогда $|H| = O(a)$. В силу теоремы Лагранжа $n = O(a) \cdot j$. □

Следствие 3. *Если $|G| = n$ и $a \in G$, то $a^n = e$.*

Доказательство. В силу следствия 2 $n = O(a) \cdot j$. Тогда $a^n = \left(a^{O(a)}\right)^j = e^j = e$. □

Следствие 4 (теорема Эйлера и малая теорема Ферма). *Если $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$, то*

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

где $\varphi(m) = |U(\mathbb{Z}_m)|$ — функция Эйлера. В частности, при $m = p$ получаем малую теорему Ферма: если a не делится на простое число p, то

$$a^{p-1} \equiv 1 \pmod{p}$$

(другими словами, $a^p \equiv a \pmod{p}$).

Следствие 5 (о цикличности группы простого порядка). *Порядок $|G|$ конечной группы G равен простому числу p тогда и только тогда, когда $G \cong \mathbb{Z}_p$ (т. е. группа G циклическая и изоморфна группе вычетов $\mathbb{Z}_p$ по модулю простого числа p). Итак, если $|G| = p$, то G — циклическая группа и в качестве циклического образующего группы G можно выбирать любой неединичный элемент группы G. В частности, в группе G нет подгрупп, отличных от $\{e\}$ и G.*

Доказательство.

1) Если $G \cong \mathbb{Z}_p$, то $|G| = |\mathbb{Z}_p| = p$.

2) Пусть $|G| = p$ и $e \neq a \in G$. Тогда число $O(a)$ является делителем числа $p = |G|$, поэтому $O(a) = p$ и $|\langle a \rangle| = O(a) = p = |G|$. Следовательно, $\langle a \rangle = G$, т. е. G — циклическая группа порядка p. Итак, $G \cong \mathbb{Z}_p$. □