

ЛЕКЦИЯ 3

СМЕЖНЫЕ КЛАССЫ

ТЕОРЕМА ЛАГРАНЖА

ТЕОРЕМА КОШИ

НОРМАЛЬНЫЕ ПОДГРУППЫ

ЦЕНТР И ЦЕНТРАЛИЗАТОР

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 1. 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 2. 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 3. 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 1. 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).

ТЕОРЕМА ЛАГРАНЖА

Теорема 1 (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 $xH \cap yH \neq \emptyset$, 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) $|H| = |xH|$.

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 $h = h'$. \square

Теорема 2 (Лагранж, Joseph Louis 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 $n = kj$. □

СЛЕДСТВИЯ ИЗ ТЕОРЕМЫ ЛАГРАНЖА

Следствие 1. 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 $n = O(a) \cdot j$. \square

Следствие 2. Если $|G| = n$ и $a \in G$, то $a^n = e$.

Доказательство. В силу следствия 1 $n = O(a) \cdot j$. Тогда $a^n = (a^{O(a)})^j = e^j = e$. \square

Следствие 3 (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, $a^p \equiv a \pmod{p}$).

Доказательство.

1) Пусть $G = \mathbf{U}(\mathbb{Z}_m)$ — группа обратимых элементов кольца вычетов \mathbb{Z}_m , $|G| = |\mathbf{U}(\mathbb{Z}_m)| = \varphi(m)$ — функция Эйлера (т. е. $\varphi(m)$ — число тех $x \in \mathbb{N}$, что $0 < x < m$, $(x, m) = 1$). Так как

$$(a, m) = 1 \iff a + \mathbb{Z}m \in \mathbf{U}(\mathbb{Z}_m),$$

то

$$(a + \mathbb{Z}m)^{\varphi(m)} = a^{\varphi(m)} + \mathbb{Z}m = 1 + \mathbb{Z}m,$$

и поэтому

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

2) Если $m = p$, то $\varphi(p) = p - 1$. □

ЗАМЕЧАНИЕ 2. На применении малой теоремы Ферма основаны вероятностные алгоритмы нахождения больших простых чисел p : для достаточно большого числа случайных значений $a < p$ проверяется, что $a^{p-1} \equiv 1 \pmod{p}$.

Следствие 4 (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, $G \cong \mathbb{Z}_p$. \square

УПРАЖНЕНИЕ 1 (КЛАССИФИКАЦИЯ ГРУПП ПОРЯДКА $n \leq 5$).

Пусть G — группа и $|G| \leq 5$. Если $|G| = 1, 2, 3$ или 5 , то, по следствию 4 к теореме Лагранжа для $p = 2, 3$ или 5 , G — циклическая группа. Если $|G| = 4$ и в G есть элемент a порядка 4, то $G = \langle a \rangle$ — циклическая группа, $G \cong \mathbb{Z}_4$. В противном случае $G = \{e, a, b, c\}$, $a^2 = b^2 = c^2 = e$. Если $ab = e$, то $ab = e = a^2$, и поэтому $b = a$, что противоречит тому, что $a \neq b$; аналогично, $ab \neq a$, $ab \neq b$. Итак, $ab = c$. Так же проверяем, что $ba = c$, $ac = b = ca$, $bc = a = cb$. Таким образом, G — группа Клейна. \square

Следствие 5. *Группа S_3 является неабелевой группой наименьшего порядка.*

ТЕОРЕМА КОШИ

Одно из следствий теоремы Лагранжа утверждает, что если G — конечная группа, $n = |G| < \infty$, $g \in G$ — любой элемент группы G , то его порядок $m = O(g)$ является делителем порядка $n = |G|$ группы G . Оказывается, что обращение этого утверждения верно для простых делителей $m = p$ числа $n = |G|$. Это составляет содержание теоремы Коши, одного из первых тонких утверждений в началах теории групп, но имеющего многочисленные применения.

ЗАМЕЧАНИЕ 3. Для непростых делителей m порядка группы $n = |G|$ это утверждение уже не имеет места, как мы видели на прошлой лекции.

Теорема 3 (теорема Коши). *Пусть G — конечная группа, $n = |G| < \infty$. Если число $n = |G|$ делится на простое число p , то группа G содержит элемент порядка p .*

Доказательство. 1) Пусть

$$T = \left\{ (g_1, \dots, g_p) \in \underbrace{G \times \dots \times G}_p \mid g_1 \dots g_p = e \right\}.$$

Так как для любого набора $(g_1, g_2, \dots, g_{p-1})$, $g_i \in G$, $1 \leq i \leq p-1$, существует и единственный элемент $g_p = (g_1 \dots g_{p-1})^{-1} \in G$ такой, что

$$g_1 g_2 \dots g_{p-1} g_p = e,$$

то $|T| = |G|^{p-1}$. Так как в силу условия теоремы число $|G|$ делится на p , то и число $|T| = |G|^{p-1}$ делится на p .

2) Рассмотрим разбиение множества строк T :

$$T = S \cup T', \quad S \cap T' = \emptyset,$$

где

$$S = \{(g, \dots, g) \in T\} = \left\{ (g, \dots, g) \in \underbrace{G \times \dots \times G}_p \mid g^p = e \right\},$$

$$T' = \{(g_1, \dots, g_p) \in T \mid g_i \neq g_j \text{ для некоторых } i, j\}.$$

3) Если $(g_1, g_2, \dots, g_p) \in T'$, то все перестановки этой строчки по циклу также лежат в T' ,

$$(g_i, g_{i+1}, \dots, g_p, g_1, \dots, g_{i-1}) \in T'$$

для любого $1 \leq i \leq p$.

Действительно,

$$e = g_1 \dots g_p = (g_1 \dots g_{i-1})(g_i \dots g_p),$$

поэтому

$$g_i \dots g_p = (g_1 \dots g_{i-1})^{-1},$$

и следовательно,

$$g_i \dots g_p g_1 \dots g_{i-1} = (g_1 \dots g_{i-1})^{-1} g_1 \dots g_{i-1} = e.$$

4) Для любой строки $(g_1, \dots, g_p) \in T'$ все p ее перестановок по циклу

$$\{(g_i, g_{i+1}, \dots, g_p, g_1, \dots, g_{i-1}) \mid 1 \leq i \leq p\}$$

являются различными строчками в T' , и поэтому число $|T'|$ делится на p .

Действительно, допустим противное: пусть при $1 \leq i < j \leq p$ ($t = j - i > 0$, $j = i + t$) имеем

$$(g_i, g_{i+1}, \dots, g_p, g_1, \dots, g_{i-1}) = (g_j, g_{j+1}, \dots, g_p, g_1, \dots, g_{j-1}).$$

Приравнивая 1-ю компоненту, получаем:

$$g_i = g_j (\equiv g_{i+t}).$$

Сравнивая $(t + 1)$ -ю компоненту, получаем

$$g_j = g_{i+t} = g_r, \quad i + 2t = pq + r, \quad 0 \leq r < p.$$

Удобно рассматривать наши индексы как элементы группы $\mathbb{Z}_p = (\{0 = p, 1, 2, \dots, p - 1\}, +)$, тогда

$$g_i = g_{i+t} = g_{i+2t} = \dots = g_{i+(p-1)t}.$$

Так как группа $(\mathbb{Z}_p, +)$ — циклическая группа порядка p , то любой ее ненулевой элемент t является образующим порядка p , $\mathbb{Z}_p = \langle t \rangle$, $O(t) = p$, и поэтому

$$\{0, t, 2t, \dots, (p - 1)t\} = \{0, 1, 2, \dots, p - 1\}.$$

Итак,

$$g_1 = g_2 = \dots = g_p.$$

Но это противоречит тому, что

$$(g_1, g_2, \dots, g_p) \in T' = T \setminus S.$$

Итак, множество строк T' разбито на непересекающиеся подмножества из p элементов каждое, поэтому число $|T'|$ делится на p .

5) Так как $|S| = |T| - |T'|$, при этом числа $|T|$ и $|T'|$ делятся на p , то $|S|$ делится на p , и поэтому $|S| \geq p \geq 2$.

6) Рассмотрим $\hat{S} = \{g \in G \mid g^p = e\} \subseteq G$. Тогда $e \in \hat{S}$, $|\hat{S}| = |S| \geq 2$, поэтому найдется элемент $e \neq g \in G$ такой, что $g^p = e$. Итак, $O(g) \neq 1$ и $O(g)$ — делитель числа p , следовательно, $O(g) = p$. □

НОРМАЛЬНЫЕ ПОДГРУППЫ

Подгруппа H группы G называется *нормальной*, если $xH = Hx$ для всех $x \in G$ (т. е. если разбиения на левые и правые смежные классы совпадают). Будем использовать обозначение $H \triangleleft G$ в этом случае. Приведем ряд условий, эквивалентных условию нормальности.

Теорема 4. Пусть H — подгруппа группы G . Тогда эквивалентны следующие условия:

- 1) $gH = Hg$ для всех $g \in G$;
- 2) $g^{-1}Hg \subseteq H$ для всех $g \in G$ (т. е. $g^{-1}hg \in H$ для всех $g \in G$, $h \in H$);
- 3) $g^{-1}Hg = H$ для всех $g \in G$.

Доказательство.

1) \implies 2). Так как $Hg = gH$, то $hg = gh'$, $h' \in H$, и поэтому $g^{-1}hg = h' \in H$.

2) \implies 3). Так как $h = g^{-1}(ghg^{-1})g \in g^{-1}Hg$, поскольку $ghg^{-1} = (g^{-1})^{-1}h(g^{-1}) \in H$, то $H \subseteq g^{-1}Hg$, и поэтому $H = g^{-1}Hg$.

3) \implies 1). Если $g^{-1}Hg = H$ для всех $g \in G$, то, умножая слева на g , получаем, что $Hg = gH$. \square

Элемент $g^{-1}hg$ называется *сопряженным с h при помощи элемента g* .

ПРИМЕР 4. Ясно, что $\{e\} \triangleleft G$ и $G \triangleleft G$. Группы G , в которых нет других нормальных подгрупп, кроме $\{e\}$ и G , называются *простыми* (например, \mathbb{Z}_p , p — простое число, \mathbf{A}_5). Строение (конечных) простых групп весьма непросто!

ПРИМЕР 5. Если $|G| = 2|H|$, т. е. H — подгруппа индекса 2 в группе G , то H нормальна в G .

Доказательство. Разбиения на левые и правые классы совпадают, это $eH = H = He$ и $G \setminus H$. □

Следствие 6. $\mathbf{A}_n \triangleleft \mathbf{S}_n$ (т. е. подгруппа четных подстановок нормальна).

Это ясно и из непосредственного подсчета четности для $\pi \in \mathbf{A}_n$:

$$\varepsilon(\sigma^{-1}\pi\sigma) = \varepsilon(\sigma^{-1})\varepsilon(\pi)\varepsilon(\sigma) = \varepsilon(\sigma)^2 = 1$$

для всех $\sigma \in \mathbf{S}_n$.

УПРАЖНЕНИЕ 2. \mathbf{A}_n — единственная подгруппа индекса 2 в \mathbf{S}_n . Более того, при $n \geq 5$ \mathbf{A}_n — единственная собственная нормальная подгруппа группы \mathbf{S}_n .

УПРАЖНЕНИЕ 3. Пусть $|G| = n < \infty$ — конечная группа, p — наименьшее простое число, делящее n . Тогда любая подгруппа H индекса p в G нормальна в G .

ЦЕНТР ГРУППЫ

ОПРЕДЕЛЕНИЕ 1. Пусть G — группа, *центром группы G* называется подмножество элементов

$$\mathbf{Z}(G) = \{a \in G \mid ag = ga \ \forall g \in G\}.$$

Теорема 5. *Центр $\mathbf{Z}(G)$ является нормальной подгруппой группы G .*

Доказательство.

1) Если $a, b \in \mathbf{Z}(G)$ и $g \in G$, то:

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab),$$

и поэтому $ab \in \mathbf{Z}(G)$; $ag = ga$, следовательно, $ga^{-1} = a^{-1}g$, и поэтому $a^{-1} \in \mathbf{Z}(G)$. Таким образом, $\mathbf{Z}(G)$ — подгруппа группы G .

2) Если $g \in G$ и $a \in \mathbf{Z}(G)$, то $ag = ga$, поэтому

$$g^{-1}ag = g^{-1}ga = ea = a \in \mathbf{Z}(G).$$

Итак, $\mathbf{Z}(G) \triangleleft G$. □

УПРАЖНЕНИЕ 4. Вычислите $\mathbf{Z}(\mathrm{GL}_n(K))$, $\mathbf{Z}(\mathrm{SL}_n(K))$; покажите, в частности, что $\mathbf{Z}(\mathrm{SL}_2(\mathbb{Z}_p)) = \{\pm E\}$ при $p > 2$.

ЦЕНТРАЛИЗАТОР ЭЛЕМЕНТА ГРУППЫ

Пусть G — группа, $a \in G$, централизатором элемента $a \in G$ в группе G называется подмножество

$$C(a) = C_G(a) = \{g \in G \mid ga = ag\}$$

группы G .

Лемма 1. *Централизатор $C(a)$ любого элемента a группы G является подгруппой в G .*

Доказательство. Если $g, g_1, g_2 \in C(a)$, то $ga = ag$, $g_1a = ag_1$, $g_2a = ag_2$, и поэтому:

$$(g_1g_2)a = g_1(g_2a) = g_1(ag_2) = (g_1a)g_2 = (ag_1)g_2 = a(g_1g_2),$$

следовательно, $g_1g_2 \in C(a)$;

$$g^{-1}a = g^{-1}agg^{-1} = g^{-1}gag^{-1} = ag^{-1},$$

следовательно, $g^{-1} \in C(a)$.

Итак, $C(a)$ — подгруппа группы G . □

ЗАМЕЧАНИЕ 4. 1) $\mathbf{Z}(G) = \bigcap_{a \in G} C(a)$;

2) $a \in \mathbf{Z}(G)$ тогда и только тогда, когда $C(a) = G$.

Лемма 2. $C(g^{-1}ag) = g^{-1}C(a)g$ для любых элементов g и a группы G .

Доказательство. Пусть $x \in G$, тогда:

$$\begin{aligned}x \in C(g^{-1}ag) &\iff x(g^{-1}ag) = (g^{-1}ag)x \iff gxg^{-1}ag = agx \iff \\ &\iff (gxg^{-1})a = g(xg^{-1}ag)g^{-1} = g(g^{-1}agx)g^{-1} = a(gxg^{-1}) \iff \\ &\iff gxg^{-1} \in C(a) \iff x \in g^{-1}C(a)g. \quad \square\end{aligned}$$

УПРАЖНЕНИЕ 5. В группе \mathbf{S}_n найдите все подстановки σ , перестановочные с циклом $(i_1 \dots i_n)$.