ЛЕКЦИЯ 2

ПОДГРУППЫ ЦИКЛИЧЕСКОЙ ГРУППЫ

СМЕЖНЫЕ КЛАССЫ

ТЕОРЕМА ЛАГРАНЖА И СЛЕДСТВИЯ

ТЕОРЕМА КОШИ

НОРМАЛЬНЫЕ ПОДГРУППЫ

ЦЕНТР И ЦЕНТРАЛИЗАТОР

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 1. 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 1 (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 1. *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 2. 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 1. Покажите, что при $n > 30$ число $\varphi(n)$ строго больше числа делителей числа n.

Теорема 1 (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, $H = \langle a^k \rangle$. $\square$

Упражнение 2. Приведите пример неабелевой группы, в которой каждая из собственных подгрупп — циклическая.

Упражнение 3. 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 2. 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 3. 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 4. 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 3. 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 2 (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) $|H| = |xH|$.

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 3 (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 $n = kj$. □

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 $n = O(a) \cdot j$. □

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

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

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 4. 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, $G \cong \mathbb{Z}_p$. □

Упражнение 4 (классификация групп порядка $\boldsymbol{n \leqslant 5}$). Пусть G — группа и $|G| \leqslant 5$. 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. □

Следствие 5. *Группа* $\mathbf{S}_3$ *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 5. Для непростых делителей m порядка группы $n = |G|$ это утверждение уже не имеет места, как мы видели на прошлой лекции.

Теорема 4 (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

$$T = \left\{ (g_1, \ldots, g_p) \in \underbrace{G \times \ldots \times G}_{p} \;\middle|\; g_1 \ldots g_p = e \right\}.$$

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

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

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:

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

где

$$S = \{(g, \ldots, g) \in T\} = \Big\{(g, \ldots, g) \in \underbrace{G \times \ldots \times G}_{p} \;\Big|\; g^p = e\Big\},$$

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

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

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

для любого $1 \leq i \leq p$.

Действительно,

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

поэтому

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

и следовательно,

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

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

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

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

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

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 $\mathbb{Z}_p = (\{0 = p, 1, 2, \ldots, p-1\}, +)$, тогда

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

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

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

Итак,

$$g_1 = g_2 = \ldots = g_p.$$

Но это противоречит тому, что

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

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, $O(g) = p$. $\square$

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 $H \lhd G$ в этом случае. Приведем ряд условий, эквивалентных условию нормальности.

Теорема 5. *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) $\Longrightarrow$ 2). Так как $Hg = gH$, то $hg = gh'$, $h' \in H$, и поэтому $g^{-1}hg = h' \in H$.

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

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

Пример 5. Ясно, что $\{e\} \lhd G$ и $G \lhd G$. 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 6. 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. $\mathbf{A}_n \lhd \mathbf{S}_n$ (*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 5. $\mathbf{A}_n$ — единственная подгруппа индекса 2 в $\mathbf{S}_n$. Более того, при $n \geqslant 5$ $\mathbf{A}_n$ — единственная собственная нормальная подгруппа группы $\mathbf{S}_n$.

Упражнение 6. 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 6. *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, $\mathbf{Z}(G) \lhd G$. □

Упражнение 7. Вычислите $\mathbf{Z}\big(\mathrm{GL}_n(K)\big)$, $\mathbf{Z}\big(\mathrm{SL}_n(K)\big)$; покажите, в частности, что $\mathbf{Z}\big(\mathrm{SL}_2(\mathbb{Z}_p)\big) = \{\pm E\}$ 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 2. *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 6. 1) $\mathbf{Z}(G) = \bigcap\limits_{a \in G} C(a)$;

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

Лемма 3. *$C(g^{-1}ag) = g^{-1}C(a)g$ для любых элементов g и a группы G.*

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

$$x \in C(g^{-1}ag) \iff x(g^{-1}ag) = (g^{-1}ag)x \iff gxg^{-1}ag = agx \iff$$
$$\iff (gxg^{-1})a = g(xg^{-1}ag)g^{-1} = g(g^{-1}agx)g^{-1} = a(gxg^{-1}) \iff$$
$$\iff gxg^{-1} \in C(a) \iff x \in g^{-1}C(a)g. \qquad \square$$

Упражнение 8. В группе $\mathbf{S}_n$ найдите все подстановки σ, перестановочные с циклом $(i_1 \ \dots \ i_n)$.