2. Действие группы на мн-ве

Опр 1 Действием группы G на мн-ве Ω наз-ся произв. гом.зм $\varphi : G \to S(\Omega)$ из G в симметрическую группу подстановок мн-ва Ω.

Обозн: $G \curvearrowright \Omega$ и $\alpha \circ g := \alpha(g\varphi)$ — образ $\alpha \in \Omega$ под действием $g \in G$.

Предл 1 Если $G \curvearrowright \Omega$, то

1) $\alpha \circ (gh) = (\alpha \circ g) \circ h \quad \forall \alpha \in \Omega \quad \forall g, h \in G$,
2) $\alpha \circ e = \alpha \quad \forall \alpha \in \Omega$ и нейтр. эл-та $e \in G$.
3) $\alpha \circ g = \beta \Rightarrow \beta \circ g^{-1} = \alpha \quad \forall \alpha, \beta \in \Omega \quad \forall g \in G$.

Д-во: Опр-е гом-зма групп и его элем. св-ва

Упр 1 (см. упр 8.6.1 из [ВЛП])

Примеры ① Если $G \le S(\Omega)$, то тождеств. вложение $\varphi : G \to S(\Omega)$, $g \mapsto g$, определяет ест. действие $\alpha \circ g = \alpha g$ G на Ω.

② Если $G \le GL(V)$, то (тождеств.) вложение $\varphi : G \to GL(V) \le S(V)$, $g \mapsto g$, определяет ест. действие $v \circ g = vg$.

③ Если $\Omega = G$, то гом-зм $\varphi : G \to S(G)$, сопоставл. эл-ту g подстановку $\begin{pmatrix} \dots x \dots \\ \dots xg \dots \end{pmatrix}$, $x \in G$, задает

действие G на себе правыми сдвигами.

(4) Если $H \leq G$ и $\Omega = G/H$, то гом-зм $G \to S(G/H)$, отпр. $g \in G$ в подстановку $\begin{pmatrix} Hx \\ Hxg \end{pmatrix}$, $Hx \in G/H$, задает действие G на G/H правыми сдвигами

(5) Если $\Omega = G$, то гом-зм $G \to S(G)$, отпр. $g \in G$ в подстановку $\begin{pmatrix} x \\ x^g \end{pmatrix}$, $x \in G$, задает действие G на себе сопряжениями.

(6) Если $\Omega = H$ – группа, то гом-зм $\varphi: G \to \mathrm{Aut}(H)$ $\leq S(H)$, отпр. g в авт-зм $g\varphi$ группы H, т.е подстановку $\begin{pmatrix} h \\ h^{g\varphi} \end{pmatrix}$, $h \in H$, из $S(H)$, задает действие G на H автоморфизмами.

Зам. Ясно, что (3) и (5) — частные случаи (4) и (6) соответственно.

Опр 2 Пусть гом-зм $\varphi: G \to S(\Omega)$ задает действие G на Ω. Ядро $\operatorname{Ker}\varphi$ наз-ся ядром действия. Действие наз-ся точным, если $\operatorname{Ker}\varphi = 1$.

Упр 2 Найти ядра действие в примерах (1)–(6)

Опр 3 Пусть $G \circlearrowright \Omega$, $\alpha \in \Omega$.

$G_\alpha = \{g \in G \mid \alpha g = \alpha\}$ — стабилизатор α в G

$\alpha G = \{\alpha g \mid g \in G\}$ — орбита α под действием G.

G действует на Ω транзитивно, если $\alpha G = \Omega$ для $\alpha \in \Omega$.

Т. 1 Пусть $G \curvearrowright \Omega$. Тогда

1. мн-во орбит действия — разбиение мн-ва Ω.
2. G_α — подгруппа группы G
3. $\forall \alpha \in \Omega$ мн-ва G/G_α и αG равномощны.

Д-во: См. д-во Т. 9.6.1 из [ВАМ] $\boxed{\equiv}$

Следствие Если $|G| < \infty$, то $|G| = |G_\alpha| |\alpha G|$ $\forall \alpha \in \Omega$. В частности, если G транзитивно действует на Ω, то $|G| = |G_\alpha| \cdot |\Omega|$.

Примеры (в том числе, почему группа симметрий тетраэдра $\cong S_4$) см. в § 9.6.1 из [ВАМ].

Еще один пример того, как используется понятие действия дают док-ва теорем Силова. Мы знаём, что не для любого делителя k порядка и конечной группы обязательно найдется подгруппа порядка k. Скажем, в группе A_4 порядка 12, нет подгрупп порядка 6. Однако, оказывается, если k — это степень простого числа, то такая подгруппа всегда найдется. Среди таких подгрупп особую роль играют самые большие — их называют силовскими. Теорема (см. далее теоремы) о их существовании был доказан Людвигом Силов в 1872 году.

Т. 2 (Силов) Пусть $|G| = p^r \cdot l$, где p — простое число и $p \nmid l$.

① **Существование** Для $\forall \alpha \in \{1, \dots r\}$ в G существует подгруппа порядка p^α.

② **Вложение** Если $\alpha < r$, то каждая подгруппа порядка p^α из G вложена в некоторую подгруппу порядка $p^{\alpha+1}$.

③ **Сопряженность** Все подгруппы порядка p^r (они наз-ся силовскими) группы G сопряжены в G.

④ **Количество** Количество n_p силовских p-подгрупп в группе G делит $|G|$ и $n_p \equiv 1 \pmod p$.

Обозн. $P \in Syl_p(G)$ озн., что P — силовская p-подгруппа.

Д-во: ① Пусть $\mathfrak{M} = \{M \subseteq G \mid |M| = p^\alpha\}$. Имеем

$$|\mathfrak{M}| = C_{p^r \cdot l}^{p^\alpha} = p^{r-\alpha} \cdot l \prod_{j=1}^{p^\alpha - 1} \frac{p^r l - j}{j},$$

поэтому $p^{r-\alpha}$ — это наибольшая степень p, делящая $|\mathfrak{M}|$.

Группа G действует на $\mathfrak{M}$ правыми сдвигами, т.к. если $M \in \mathfrak{M}$, то $Mg = \{mg \mid m \in M\} \in \mathfrak{M}$.

Среди орбит этого действия есть хотя бы одна, порядок которой не делится на $p^{r-\alpha+1}$. Пусть $\Omega = \{M_1, \dots M_s\}$ — эта орбита. Положим $G_i = \{g \in G \mid M_1 g = M_i\}$, $i = 1..s$. Легко проверить, что $G_1 \leq G$ и G_i, $i = 1..s$, — правые смежные классы по подгруппе G_1.

Мы докажем, что G_1 — искомая подгр. порядка p^α. Пусть $|G_1| = t$. Тогда $p^r \cdot l = |G| = |\Omega||G_1| = st$ по т. о длине орбит (см. следствие из т. 9.6.1 из [ВАМ]).

Т.к наибольшая возм. степень p, делящая s, — это $p^{r-\alpha}$, то $p^\alpha \mid t$. В частности, $t \geq p^\alpha$. С др. стороны, если $x \in M_1$, то $xG_1 \subseteq M_1$, поэтому $|G_1| \leq |M_1| \leq p^\alpha$.

2 Пусть $P \leq G$: $|P| = p^\alpha$ и $\alpha < r$. Обозначим $\mathcal{P} = \{P^g \mid g \in G\}$ — класс подгрупп, сопряженных с P в G. Группа G действует на $\mathcal{P}$ сопряжениями, поэтому по той же лемме о длине орбит имеем

$$|\mathcal{P}| = |G : N_G(P)|, \text{ где } N_G(P) = \{g \in G \mid P^g = P\} —$$

нормализатор P в G.

Возможны два случая: 1) $p \nmid |\mathcal{P}|$. Тогда $p^{\alpha+1} \mid |N_G(P)|$ и, сл-но, в силу первой части т-мы в группе $\overline{N} = N_G(P)/P$ есть подгруппа $\overline{P^*}$ порядка p $\Rightarrow$ её прообраз P^* имеет порядок $p^{\alpha+1}$ и содержит P.

2) $p \mid |\mathcal{P}|$. Рассмотрим действие гр. P на $\mathcal{P}$ сопряжениями. Порядки орбит делят $|P|$, т.е имеют вид p^{α_i}, $\alpha_i \geq 0$. Имеется по крайней мере одна одноэлементная орбита $\{P\}$. Т.к. $p \mid |\mathcal{P}|$, то есть и ещё одна одноэлем. орбита $\{Q\}$, $Q \neq P$. Сл-но, $QP = PQ \Rightarrow PQ \leq G$, причём $|PQ| > |P|$ и $PQ/Q \simeq P/P \cap Q \Rightarrow PQ$ — p-подгруппа, порядка

большего, чем P, причём $Q \trianglelefteq PQ$. Т.к. Q и P лежат в одной орбите $\mathcal{P}$, то $\exists g \in G: Q^g = P$. Тогда $P = Q^g \trianglelefteq (PQ)^g = P_1$. Снова, применяя (1), находим в P_1/P подгруппу P^*/P порядка p, её прообраз P^* — искомая подгруппа порядка $p^{\alpha+1}$.

(3) Пусть теперь $P \in Syl_p(G)$, т.е $|P| = p^r$, а $\mathcal{P} = \{P^g \mid g \in G\}$. Пусть $Q \in Syl_p(G)$. Надо док-ть, что $Q \in \mathcal{P}$. Р-м действие Q на $\mathcal{P}$ сопряжениями. Порядки орбит этого действия сновадают $|Q|$, т.е равны p^{α_i}, $\alpha_i \geq 0$. Т.к $|\mathcal{P}| = |G : N_G(P)|$ теперь точно не делится на p, то имеется одноэлем. орбита $\{P'\}$. Тогда $P'Q = QP' \leq G$ и $P'Q$ — p-группа.

Но $Q \in Syl_p(G) \Rightarrow |P'Q| = |Q| = |P'| \Rightarrow Q = P'Q = P' \in \mathcal{P}$, что и требовалось.

(4) В обозн. из (3) $n_p = |\mathcal{P}| = |G : N_G(P)|$ делит $|G|$.

Чтобы док-ть, что $n_p \equiv 1 \pmod{p}$, достаточно показать, что $\{Q\}$ – единств. одноэлем. орбита. Если $\{Q'\}$ – другая такая орбита, то QQ' – p-подгр, отличная от Q, что невозможно. ∎

<u>Следствие</u> Пусть $P \in Syl_p(G)$. Тогда $P \trianglelefteq G \Leftrightarrow n_p = 1$.

<u>Упр 3</u> Найти силовские подгруппы в S_4

<u>Упр 4</u> (Аргумент Фраттини) Если $H \trianglelefteq G$ и $P \in Syl_p(H)$, то $G = N_G(P)\,H$.

Опр 4 Пусть гом-змы $\varphi: G \to S(\Omega)$ и $\varphi': G \to S(\Omega')$ задают действия G на мн-вах Ω и Ω' соотв-но.

Эти действия эквивалентны, если найдется биекция $\lambda: \Omega \to \Omega'$ такая, что $\forall \alpha \in \Omega$ $\forall g \in G$

$$(\alpha(g\varphi))\lambda = (\alpha\lambda)(g\varphi').$$

Из опр 5 сразу вытекает, что если $\varphi \sim \varphi'$, то $\forall \alpha \in \Omega$ $\quad |\alpha(G\varphi)| = |(\alpha\lambda)(G\varphi')|$ и даже

$$(G\varphi)_\alpha \simeq (G\varphi')_{(\alpha\lambda)}.$$

Пример $G = \langle a \rangle \times \langle b \rangle$, $|a| = |b| = 2$, $\Omega = \Omega' = \{1, 2, 3, 4\}$.

$a\varphi = (12)(34) = a\varphi'$ $\quad b\varphi = (13)(24)$ $\quad b\varphi' = (12)$

Тогда $\varphi \not\sim \varphi'$, т.к. $|1 \cdot G\varphi| = 4$, но $|1 \cdot G\varphi'| = 2$.

Т.3 Пусть гом-зм $\varphi : G \to S(\Omega)$ задаёт транзитивное действие G на Ω. Пусть $\alpha \in \Omega$ и $H = G_\alpha$. Тогда действие φ эквивалентно действию G на $\Omega' = G/H$ правыми сдвигами.

Д-во: Т.к. G действ. на Ω транзитивно, то $\forall \beta \in \Omega$ $\exists x \in G : \beta = \alpha(x\varphi)$. Определим от-е $\lambda : \Omega \to \Omega'$ правилом $\alpha(x\varphi) \mapsto Hx$. Поскольку $\alpha(x\varphi) = \alpha(y\varphi) \Leftrightarrow$ $\alpha(x\varphi)(y\varphi)^{-1} = \alpha \Leftrightarrow \alpha(xy^{-1})\varphi = \alpha \Leftrightarrow xy^{-1} \in H \Leftrightarrow$ $\Leftrightarrow Hx = Hy$, от-е λ определено корректно и биективно. Наконец, $\forall x, g \in G$

$$(\alpha(x\varphi) \cdot (g\varphi))\lambda = H(xg) = (Hx)g = (\alpha(x\varphi))\lambda \cdot g(\varphi)$$ ∎

Одним из основных понятий теории групп явл-ся понятие полупрямого произведения.

Опр 5 Группа G есть полупрямое произведение своих подгрупп H и K (обозн: $G = H \ltimes K$), если 1) $K \trianglelefteq G$, 2) $H \cap K = 1$, 3) $G = HK$.

Зам 1. В д-ве 2-ой т. о гом-змах мы видели, что если $K, H \le G$ и $K \trianglelefteq G$, то $HK = KH \le G$.

Зам. 2 Пп. 2, 3 опр 1 равносильны тому, что $\forall g \in G \ \exists!\, h \in H$ и $k \in K$: $g = hk$.

В частности, если $|G| < \infty$ и $G = H \ltimes K$, то $|G| = |H| \cdot |K|$.

Зам. 3 Прямое произведение двух подгрупп — частный случай полупрямого.

Примеры: 1) $S_3 = \langle (12) \rangle \rightthreetimes \langle (123) \rangle$ и вообще,

$S_n = \langle (12) \rangle \rightthreetimes A_n$.

2) $GL_n(K) = H \rightthreetimes SL_n(K)$, где $H = \{\mathrm{diag}(\lambda, 1, \dots 1) \mid \lambda \in K^*\}$.

3) $\mathrm{Isom}_2 = O_2 \rightthreetimes \mathrm{Tran}_2$ и $\mathrm{Isom}_3 = O_3 \rightthreetimes \mathrm{Tran}_3$.

Вообще $\mathrm{Isom}(\mathbb{R}^n) = GO(\mathbb{R}^n) \rightthreetimes \mathrm{Tran}(\mathbb{R}^n)$.

НАРЯДУ с „внутренним" определением $\S$, как и в случае с прямыми произведениями возможно и „внешнее" определение. Напомним (см. пример 6), что группа H действует на группе K автоморфизмами, если задан гомоморфизм $\varphi : H \to \mathrm{Aut}(K)$.

Теорема 4 Пусть H, K — группы и гомоморфизм $\varphi : H \to \mathrm{Aut}(K)$ задает действие H на K автоморфизмами.

Мн-во $G = H \times K$ с операцией, заданной правилом

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 h_2, k_1^{h_2\varphi} k_2), \qquad (*)$$

где $h_1, h_2 \in H$, $k_1, k_2 \in K$ и $k_1^{h_2\varphi}$ — образ k_1 под действием $h_2\varphi \in \mathrm{Aut}(K)$, образует группу. Причем

$$H' = \{(h,1) \mid h \in H\} \leq G, \quad K' = \{(1,k) \mid k \in K\} \trianglelefteq G,$$

$H' \cap K' = 1$ и $G = H'K'$, т.е. G есть полупрямое произведение своих подгрупп H' и K' (см. опр. 1).

Опр 6 Группа G из предл 1 наз-ся **полупрямое произведение** гр. H и K (относительно φ) и обозн. $G = H \ltimes_{\varphi} K$ или просто $H \ltimes K$.

Д-во: Очевидно, что $(1,1)$ — нейтр. элемент гр. G.

Т.к. $(1,1) = (h,k)\left(h^{-1}, (k^{-1})^{(h^{-1})\varphi}\right)$, то у каждого эл-та из G есть обратный. Проверка ассоциативности сводится к громоздкой прямой выкладке.

Чтв я $H', K' \le G$, $H' \cap K' = 1$ и $G = H'K'$.

Проверим, что $K' \trianglelefteq G$. Поскольку $G = H' \cdot K'$, это вытекает из след. цепочки рав-в:

$$(h^{-1},1)(1,k)(h,1) = (h^{-1},k)(h,1) = (1, k^{h\varphi}) \blacksquare$$

Зам. Иной путь д-ть эту т-му: см. Isaacs, Finite Groups, Theorem 3.2.

Обратно, если G есть полупрямое произведение своих подгрупп H и K, причем $K \trianglelefteq G$, то $G = H \underset{\psi}{\ltimes} K$, где $\psi: H \to \mathrm{Aut}(K)$ по правилу $h \mapsto \varphi_h$ и $k\varphi_h = h^{-1}kh$, т.е каждый эл-т из H отправляется в сопряжение эл-тов группы K (как подгруппы гр. G) этим эл-том.

<u>Упр 5</u> Покажите, что ни группу $\mathbb{Z}_4$, ни группу Q_8 нельзя представить в виде полупрямого произведения своих подгрупп, хотя собств. норм. подгруппы там имеются.

Т. 5 Пусть p и q — простые числа, $p < q$, G — группа, $|G| = pq$. Тогда $G = P \rtimes Q$ — полупрямое произведение силовских p-подгруппы P и q-подгруппы Q.

Кроме того, если $q \not\equiv 1 \pmod p$, то $G = P \times Q \simeq \mathbb{Z}_{pq}$ — циклическая группа, если $q \equiv 1 \pmod p$, то либо а) $G \simeq \mathbb{Z}_{pq}$, либо б) $n_p = q$, $b^{-1}ab = a^r$, где $P = \langle a \rangle$, $Q = \langle b \rangle$ и $r^p \equiv 1 \pmod q$, но $r \not\equiv 1 \, (q)$, причём группа, определяемая условиями п б) единственна.

Δ во: См. например, в п. 11.2 из [KM].