Оглавление

Глава 1

Теория групп

1.1 Теорема Кэли

Теорема 1 (Кэли). G – конечная группа, $|G| = n$. Тогда $\exists\, H < S_n : G \simeq H$

Пример. $G = Z_3$
$G = \{\, g_1, g_2, g_3 \,\}, \qquad g_1 = \overline{0}, \quad g_2 = \overline{1}, \quad g_3 = \overline{2}$

$$\begin{cases} g_1 g_1 = \overline{0} + \overline{0} = \overline{0} = g_1 \\ g_1 g_2 = \overline{0} + \overline{1} = g_2 \\ g_1 g_3 = \overline{0} + \overline{2} = g_3 \end{cases}$$

g_1 будет соотетствовать тождественной перестановке

$$\begin{cases} g_2 g_1 = g_2 \\ g_2 g_2 = g_3 \\ g_2 g_3 = g_1 \end{cases}$$

Получили, что g_2 соответствует перестановка $\begin{cases} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{cases}$, то есть $g_2 \to \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Аналогично, $g_3 \to \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

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

Доказательство. Пронумеруем элементы группы $g_1, \ldots, g_n$
Докажем, что $\forall a \in G$ элементы $ag_1, \ldots, ag_n$ – это элементы $g_1, \ldots, g_n$ в некотором порядке
Достаточно проверить, что $ag_1, \ldots, ag_n$ различны:

$$ag_i = ag_j \xRightarrow[\text{свойство сокращения}]{} g_i = g_j \qquad \lightning$$

Пусть $\sigma \in S_n$:

$$ag_1 = g_{\sigma(1)}, \ldots\ldots\ldots, ag_n = g_{\sigma(n)}$$

Определим $\varphi : G \to S_n : \varphi(a) = \sigma : \forall i \quad ag_i = g_{\sigma(i)}$
Проверим, что φ – гомоморфизм:
Пусть $\varphi(a) = \sigma, \quad \varphi(b) = \tau$

$$(ab)g_i = a(bg_i) \underset{(\varphi(b)=\tau)}{=} ag_{\tau(i)} \underset{(\varphi(a)=\sigma)}{=} g_{\sigma(\tau(i))} = g_{(\sigma\circ\tau)(i)} \quad \forall i \implies \varphi(ab) = \sigma \circ \tau$$

Положим $H = \operatorname{Im}\varphi \implies H < S_n$
Проверим, что $\varphi : G \to H$ – изоморфизм:

- φ сюръективна по определению Im
- Проверим инъективность:
Пусть $\varphi(a) = e_{S_n} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$

$$ag_1 = g_1, \dots\dots, ag_n = g_n$$

$$ag_1 = eg_1 \implies a = e \implies \ker\varphi = \{ e \}$$

□

1.2 Действие группы на множество

Определение 1. Пусть G – группа, M – множество
Говорят, что группа G действует (слева) на множество M, если каждой паре $g \in G, m \in M$ сопоставлен элемент $g(m) \in M$, и при этом выполнены свойства:

1. $(gh)(m) = g\big(h(m)\big) \quad \forall g, h \in G, m \in M$
2. $e(m) = m \quad \forall m \in M$

Замечание. Для $g, h \in G, m \in M$ запись ghm означает $(gh)(m) = g\big(h(m)\big)$

Примеры.

1. M – множество, G – множество биекций в себя
2. D_n – группа самосовмещений правильного n-угольника
3. M – множество вершин n-угольника, раскрашенных в несколько цветов, G – группа самосовмещений
4. $M = G$, $(m, g) \to gm$
5. $M = G$, действие – сопряжение: $(m, g) \to g^{-1}mg$

Определение 2. Введём на множестве M отношение эквивалентности $\sim$:
$m \sim l$, если $\exists\, g \in G : gm = l$

Определение 3. Классы эквивалентности по отношению $\sim$ называются орбитами

Обозначение. $\mathrm{Orb}(m), \quad Gm$

Корректность. Проверим, что $\sim$ является отношением эквивалентности:

- $em = m \implies m \sim m$
- $m \sim e \implies l = gm \implies g^{-1}l = g^{-1}gm = m \implies l \sim m$
- $\left.\begin{matrix} m \sim l \implies l = gm \\ l \sim k \implies k = hl \end{matrix}\right\} \implies k = h(gm) = (hg)(m) \implies m \sim k$

Замечание. Если говорят про орбиты в группе без множества, имеются в виду орбиты по сопряжению (см. пример 5)

Определение 4. Действие группы называется транзитивным, если есть ровно одна орбита

Определение 5. Стабилизатором элемента $m \in M$ называется множество $\{ g \in G \mid gm = m \}$

Обозначение. $\mathrm{Fix}(m), \quad G_m$

Определение 6. Фиксатором элемента $g \in G$ называется множество $\{\, m \in M \mid gm = m \,\}$

Обозначение. $\mathrm{Fix}(g)$

Свойства.

1. $\mathrm{St}(m) < G \quad \forall m \in M$

   Доказательство.

$$\left.\begin{aligned} gm = m \\ hm = m \end{aligned}\right\} \implies (gh)m = g(hm) = gm = m$$

$$gm = m \implies g^{-1}m = g^{-1}gm = em = e$$

□

2. Пусть G – конечная группа. Тогда

$$|G| = |\operatorname{Orb}(m)| \cdot |\operatorname{St}(m)| \quad \forall m \in M$$

Доказательство. Пусть $k := |\operatorname{Orb}(m)|$

$$\operatorname{Orb}(m) = \{\, m_1, ..., m_k \,\}$$

$g_1, ..., g_k \in G$ – такие, что $g_i m = m$
Докажем, что $g_1, ..., g_k$ принадлежат разным смежным классам по подгруппе $\mathrm{St}(m)$ и являются представителями всех классов:

- Различность:
  Пусть g_i и g_j в одном классе

$$g_i^{-1} g_j \in \mathrm{St}(m) \implies g_i^{-1} g_j m = m \implies g_i g_i^{-1} g_j m = g_i m$$

□