Алгебра на ФКН ПИ

Общий конспект всех лекций за 3 модуль

15 февраля 2021 г.

Утв Пусть G - группа и $g \in G$.
Тогда $|\langle g \rangle| = ord(g)$, где $|\langle g \rangle|$ - число элементов в циклической группе, порожденной элементом g.

□ Заметим, что если $g^k = g^s \Rightarrow g^{k-s} = e$ (так как $\exists g^{-1}$) $\Rightarrow$ порядок $g \leq k - s \Rightarrow$ если g имеет бесконечный порядок, то все элементы g^n ($n \in \mathbb{Z}$) различны и $\Rightarrow \langle g \rangle$ содержит бесконечно много элементов. В бесконечном случае доказано.

Если же $ord(g) = m$, то из минимальности $m \in \mathbb{N} \Rightarrow e = g^0, g = g^1, g^2, \ldots, g^{m-1}$ попарно различны.
Покажем, что $\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$:
$\forall n \in \mathbb{Z} : n = m \cdot q + r$, где $0 \leq r \leq m \Rightarrow g^n = g^{mq+r} = (g^m)^q \cdot g^r = e^q \cdot g^r = g^r$, где $0 \leq r \leq m \Rightarrow$ $\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$ и $|\langle g \rangle| = m = ord(g)$. ■

Утв Пусть $f : G \to F$ - гомоморфизм. Тогда f - инъективен (т.е. является мономорфизмом) $\Leftrightarrow \ker f = e_G$, где e_G - нейтральный элемент в группе в G, а $\ker f$ в данном случае является тривиальным **ядром** гомоморфизма.

Опр Ядром гомоморфизма $f : G \to F$ называется множество элементов группы G, которые переходят в e_F - нейтральный элемент во второй группе.

$$\ker f = \{g \in G | f(g) = e_F\}$$

Зам $\ker f$ никогда не является пустым множеством, так как по свойству гомоморфизма $f(e_G) = e_F$.

□
$\boxed{\Rightarrow}$ Необходимость:
Дано: $\forall x_1 \neq x_2 : f(x_1) \neq f(x_2) \Rightarrow f(e_G) = e_F$ (и для $x \in G$ $(x \neq e_G)$ $f(x) \neq f(e_G) = e_F$).
$\boxed{\Leftarrow}$ Достаточность:
Дано: $\ker f = e_G$. Допустим, что $\exists x_1 \neq x_2 : f(x_1) = f(x_2)$. Тогда $f(x_1 \cdot x_2^{-1}) = f(x_1) \cdot f(x_2^{-1}) = f(x_1) \cdot (f(x_2))^{-1} = e_F \Rightarrow x_1 \cdot x_2^{-1} = e_G \Leftrightarrow x_1 = x_2$ - противоречие, значит, f инъективно. ■

Опр Таблица Кэли - это матрица из попарных произведений элментов из группы.

Примеры групп:
1). D_n - группа диэдра - группа симметрий правильного n-угольника.

$$D_n = \{r, s | r^n = 1, s^2 = 1, s^{-1}rs = r^{-1}\}$$

Утв $D_3 \cong S_3$ (S_3 - группа подстановок).

2). $A_n \subset S_n$ (A_n - все четные подстановки длины n).
$|A_n| = \frac{n!}{2}$

3). Группа кватернионов:

$$Q_8 = \{\pm 1, \pm i, \pm, j, \pm k | (-1)^2 = 1, i^2 = j^2 = k^2 = -1 = ijk\}$$

Пример ядра:

$$f : GL_n(\mathbb{R}) \to R^*$$

$f(A) = \det A$. Тогда $\ker f = \{A | \det A = 1\} = SL_n(\mathbb{R})$ - специальная линейная группа.

Утв Любая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$ (числа, кратные k) для некоторого $k \in \mathbb{N} \cup \{0\}$.

□ $k\mathbb{Z}$, очевидно, является подгруппой в $\mathbb{Z}$. Докажем, что других подгрупп не существует.
Если подгруппа $H = \{0\}$, то положим $k = 0$. Иначе: $k = min(H \cap \mathbb{N})$. Тогда $k\mathbb{Z} \subseteq H$.
Если $a \in H$ и $a = qk + r$ $(0 \leq r \leq k) \Rightarrow r = a - kq$, где $a \in H$ и $kq \in H$, а значит, $r = 0$ и $H = k\mathbb{Z}$ ■

Опр Пусть G - группа и H - ее подгруппа. Путь фиксирован $g \in G$. Тогда левым смежным классом элемента g по подгруппе H называется множество:

$$gH = \{g \cdot h | h \in H\}$$

Аналогично правым смежным классом является такое множество:

$$Hg = \{h \cdot g | h \in H\}$$

Лемма 1 $\forall g_1, g_2 \in G$ либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \varnothing$.

□ Если $g_1H \cap g_2H \neq \varnothing$, то $\exists h_1, h_2 \in H : g_1h_1 = g_2h_2 \Rightarrow g_1 = g_2 \cdot h_2 \cdot h_1^{-1} \Rightarrow g_1H = g_2 \cdot h_2 \cdot h_1^{-1}H \subseteq H$.
А так как $h_2 \cdot h_1^{-1} \in H$, то $g_1H \subseteq g_2H$. Аналогично существует и обратное включение, а значит $g_1H = g_2H$. ■

Лемма 2 $|gH| = |H|$ $\forall g \in G$ и для любой конечной подгруппы H.

□ $|gH| \leq |H|$. Если $gh_1 = gh_2 \Rightarrow g^{-1}gh_1 = g^{-1}gh_2 \Rightarrow h_1 = h_2$, то есть совпадений нет. ■

Опр Индексом подгруппы H в группе G называется количество левых смежных классов G по подгруппе H.
Обозначение: $[G : H]$

Теорема (Лагранжа)
Пусть G - конечная группа, H - ее подгруппа, тогда $|G| = |H| \cdot [G : H]$.

□ Любой элемент группы лежит в своем левом смежном классе по H, и смежные классы не пересекаются (по лемме 1) и любой из этих смежных классов содержит по $|H|$ элементов (по лемме 2). ■

Следствие 1 Пусть G - конечная группа и взят элемент $g \in G$. Тогда $ord(g)$ делит $|G|$.

□ Возьмем $H = \langle g \rangle$. Мы знаем, что $|\langle g \rangle| = ord(g)$ и $|G| = |\langle g \rangle| \cdot [G : H]$, то есть $|G| \vdots ord(g)$. ■

Следствие 2 Пусть G - конечная группа, тогда $g^{|G|} = e$.

□ Применим следствие 1: $|G| = ord(g) \cdot s \Rightarrow g^{|G|} = g^{ord(g) \cdot s} = (g^{ord(g)})^s = e^s = e$. ■

Следствие 3 aka Малая Теорема Ферма:
Пусть $\overline{a}$ - ненулевой вычет попростому подулю p, тогда $\overline{a}^{p-1} = \overline{1}$, то есть $a^{p-1} \equiv 1 \pmod{p}$.

$\overline{0}, \overline{1}, \ldots, \overline{p-1}$ - *вычеты по модулю p, то есть остатки от деления* $m \in \mathbb{Z}$ *на p.*

□ На самом деле это следствие 2 ($g^{|G|} = e$), примененное к группе $\mathbb{Z}_p^* = \{\mathbb{Z}_p \backslash \{0\}, \cdot\}$, где Z_p - множество всех вычетов по модулю p. $|Z_p^*| = p - 1 \Rightarrow \overline{a}^{|Z_p^*|} = e$. ■

Зам Точно так же можно было рассмотреть и правые смежные классы. Но число левых смежных классов равно числу правых и равно $\frac{|G|}{|H|}$ (по теореме Лагранжа).