Лекция 17, 24.01.24

Утв.: $\forall$ подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\cdot\mathbb{Z} = \{k\cdot m \mid m \in \mathbb{Z}\}$ для некоторого $k \in \mathbb{N}\cup\{0\}$.

Пример: $2\cdot\mathbb{Z}$ – мн-во чётных чисел.

□ Если $H = \{0\}$, то возьмём $k = 0$. Иначе, пусть H – подгруппа в $\mathbb{Z}$ и $k = \min(H \cap \mathbb{N})$ – наименьшее натур. число в H.

Тогда $k\mathbb{Z} \subseteq H$, т.к. $k\mathbb{Z} = \{k\cdot m \mid m \in \mathbb{Z}\}$ – мн-во степеней k в аддитивной записи. То есть это цикл. подгруппа $\langle k\rangle$ в H.

Пусть $a \in H$, разделим a с остатком на k:

$a = q\cdot k + r$, где $0 \le r < k$, $\Rightarrow$

$\Rightarrow r = a - qk = \underbrace{a}_{\in H} + \underbrace{(-q\cdot k)}_{\in H} \Rightarrow r \in H$, но т.к. k – миним. натур. ч. в H

$\Rightarrow r = 0 \Rightarrow a$ имеет вид $a = k\cdot q \in k\cdot\mathbb{Z} \Rightarrow H \subseteq k\mathbb{Z} \Rightarrow$

$\Rightarrow H = k\mathbb{Z}$ ■

Теорема Лагранжа

Пусть G – группа и H – подгруппа ($H \subseteq G$)

Опр: <u>Левым смежным классом</u> эл-та $g \in G$ по подгруппе H наз. множество: $gH = \{g\cdot h \mid h \in H\}$.

Пример: $\mathbb{C}^* = (\mathbb{C}\setminus\{0\}, \cdot)$

$g = 5 + i$, H – подгруппа компл. корней 6й степени из 1.

$gH = \{(5+i)\varepsilon_k \mid k = \overline{0,5}\}$, где ε_k – k-й корень 6й степени из 1.

Пример: $(\mathbb{Z}, +)$, $H = 3\mathbb{Z} \sim \bar{0}$ – вычет по mod 3.

Пусть $g=1 \Rightarrow gH = \{1+k \mid k \in 3\mathbb{Z}\} \sim \bar{1}$

$g=2 \Rightarrow gH = \{2+k \mid k \in 3\mathbb{Z}\} = 2+3\mathbb{Z} \sim \bar{2}$

$g=3 \Rightarrow gH = 3+3\mathbb{Z} = 3\mathbb{Z} \sim \bar{0}$

$g=4 \Rightarrow gH = 4+3\mathbb{Z} = 1+3\mathbb{Z} \sim \bar{1}$

и т.д.

$\mathbb{Z} = \bar{0} \sqcup \bar{1} \sqcup \bar{2}$ (разбиение)

Лемма 1. $\forall g_1, g_2 \in G$ левые смежные классы по подгр. H либо совпадают ($g_1H = g_2H$), либо не пересекаются ($g_1H \cap g_2H = \emptyset$).

□ Если $g_1H \cap g_2H \neq \emptyset$, то $\exists h_1$ и $h_2 \in H$ $g_1h_1 = g_2h_2$

$\Rightarrow g_2 = g_1 \underbrace{h_1 \cdot h_2^{-1}}_{\in H} \Rightarrow g_2H = g_1h_1h_2^{-1}H \subseteq g_1H$

(т.е. если эл-т $a \in g_2H$, то $\exists h^{-1} \in H$: что $a = g_1h' \Rightarrow a \in g_1H$)

Аналогично $g_1H \subseteq g_2H \Rightarrow g_1H = g_2H$ ■

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

(т.е. во всех смежных классах одинак. число эл-тов)

Опр: Индексом подгруппы H в группе G наз. число левых смежных классов G по H.

Обозн: $[G : H]$

□ $|gH| \leq |H|$, т.к. по опр. $gH = \{gh \mid h \in H\}$. И они не склеиваются, т.к. если $gh_1 = gh_2 \Leftrightarrow g^{-1}gh_1 = g^{-1}gh_2 \Leftrightarrow h_1 = h_2$ ■

Теорема (Лагранжа): Пусть G – конечная группа, и $H \leq G$ – подгруппа в G. Тогда $|G| = |H| \cdot [G:H]$

□ $\forall$ элемент группы G лежит в своём левом смежном классе по H и смежные классы не пересек. (по Лемме 1). И $\forall$ из них содержит по $|H|$ элементов (по Лемме 2) $\Rightarrow |G| = |H| \cdot [G:H]$ ■

Следствие 1: Пусть G – конечная группа и $g \in G$. Тогда $ord(g)$ делит порядок группы.

□ Рассмотрим $H = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ – цикл. подгруппа в G, порожд. эл-т g, по доказанному ранее $ord(g) = |\langle g \rangle|$
$\Rightarrow$ по т. Лагранжа $|G| = \underbrace{|\langle g \rangle|}_{=ord(g)} \cdot [G:H] \Rightarrow ord(g) \mid |G|$ ■

Следствие 2: Пусть G – конечн. группа, $g \in G$. Тогда $g^{|G|} = e$ ← (нейтр. эл-т в G)

□ По след-вию 1 $|G| = ord(g) \cdot s$ ← нек. целое число $\Rightarrow$
$\Rightarrow g^{|G|} = g^{ord(g) \cdot s} = (g^{ord(g)})^s = e^s = e$ ■

Следствие 3 (Малая т. Ферма)
Рассм. $\mathbb{Z}_p^* = (\mathbb{Z}_p \setminus \{\bar{0}\}, \cdot)$, где p – простое число
(умножение; вычет по простому mod p)
Пусть $\bar{a}$ – ненулевой вычет по простому модулю p.
Тогда $\bar{a}^{p-1} = \bar{1} \Leftrightarrow a^{p-1} \equiv 1 \mod p$.

□ Z_p^* - группа

$|Z_p^*| = p-1 \Rightarrow$ по следствию 2

$\bar{a}^{|Z_p^*|} = e \Leftrightarrow \bar{a}^{p-1} = \bar{1}$ ■

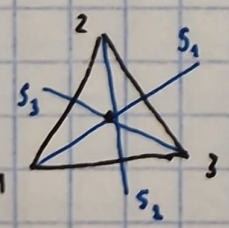
Замеч: Точно так же можно было рассмотреть правые смежные классы гр. G по подгр. H: $Hg = \{h \cdot g \mid h \in H\}$. Из теор. Лагр. следует, что число левых и число правых совп. и равно $\frac{|G|}{|H|}$. При этом сами смежные классы могут не совпадать.

Опр: Подгруппа H группы G наз. нормальной, если $\forall g \in G$ $gH = Hg$ (т.е. левые и правые смежные классы по ней совп.)

Замеч: В абелевой группе все подгруппы нормальные.

Пример: Группа диэдра - группа симметрий (движений) правильного n-угольника.

Обознач: D_n



D_3

3 поворота: P_0, $P_{\frac{2\pi}{3}}$, $P_{-\frac{2\pi}{3}}$

3 отражения (осевых): S_1, S_2, S_3

$|D_n| = 2n$

$P_0 \sim Id$ $\quad S_1 \sim (2\,3)$

$P_{\frac{2\pi}{3}} \sim (1\,2\,3)$ $\quad S_2 \sim (1\,3)$ $\quad D_3 \cong S_3$

$P_{-\frac{2\pi}{3}} \sim (1\,3\,2)$ $\quad S_3 \sim (1\,2)$

Теорема Кэли (Cayley): $\forall$ конечная группа порядка $n \in \mathbb{N}$ изоморфна некоторой подгруппе в S_n.

(гр. подстановок или симметрич. группе)