w 5 p. 1

Тк Лагранта о порядке подгруппы и следствия из нее

Def. $A \cdot B \overset{def}{=} \{a \cdot b \mid a \in A, b \in B\}$, где $A, B \subseteq G$ $(G, \cdot)$

частный сл-й

$A = \{a\}$

$\{a\} \cdot B = \{a \cdot b \mid b \in B\}$.

Причем $ab_1 = ab_2 \Leftrightarrow b_1 = b_2$

Note. $(AB) \cdot C = A(B \cdot C)$.

Пусть $H \leq G$, $x \in G$

Def. подмн-во $x \cdot H$ наз-ся левым смежным классом гр G, порожденным эл-м x по подгруппе H

Def. подм-во $H \cdot x$ —//— правым —//—

Note. В общем сл-е $xH \neq Hx$.

В абелевой $xH = Hx$

(1) $xH = H \Leftrightarrow x \in H$.

Д-во.

$\Rightarrow$

$xH = H$

$x \cdot e \in \cancel{x}H = H \Rightarrow x \in H$

$\Leftarrow$

$x \in H \Rightarrow xH \overset{?}{\subseteq} H$ и $H \overset{?}{\subseteq} xH$.

очев, т.к $x \in H$.

$x \in H \Rightarrow x^{-1} \in H$

$\forall h \in H$ $h = x \cdot \underbrace{x^{-1} \cdot h}_{\in H} \in xH$. ☐

Утв. Следующие св-ва лев. см. классов экв.

а) $xH \cap yH \neq \emptyset$

б) $x^{-1}y \in H$

в) $xH = yH$

г) $x \in yH$

Д-во.

а $\Rightarrow$ б. Пусть $xH \cap yH \neq \emptyset$

$\exists h_1 h_2 \in H$:

$xh_1 = yh_2$

x^{-1} h_2^{-1}

$h_1 h_2^{-1} = x^{-1}y \Rightarrow x^{-1}y \in H$.

=>в,

По ① $x^{-1}yH=H$

$yH=xH$

в=>г,

$xH=yH \quad x\in xH => x\in yH$

г=>а,

$\left.\begin{array}{l} x\in yH \\ x\in xH \end{array}\right| => x\in xH\cap yH.$ ☒

Note, ∀ два левых см. класса по подгруппе H либо не перес. либо совп.

Note,

$x^{-1}y\in H <=> xH=yH$

Т.о. $x\sim y <=> x^{-1}y\in H$ – отн. экв.

Note,

$G=\cup x_iH$, где x_iH – левые см. классы.

$G=\bigcup\limits_{x\in G} xH=\bigcup\limits_{i\in I} x_iH$ – оставим только п-е.

Df, $G=\bigcup\limits_{i\in I} x_iH$ – левост-е разбиение

Note, Все утв. верны и для пр-х.

$G=\bigcup\limits_{j\in J} Hy_j$

T2 (Лагранжа)

Порядок ∀ подгруппы конечной группы является делителем пор-ка группы.

Д-во

$|G|=n \quad H\leq G \quad |H|=k.$

$xH \overset{df}{=} \{\underbrace{xh_1 \dots xh_k}_{\text{попарно разл.}}\}$

$|xH|=|H|=k.$

Пусть $|I|=m.$

Из $G=\bigcup\limits_{i\in I} x_iH => n=m\cdot k$ ☒

w5
p.2

Сл-е 1.

Порядок $\forall$ эл-та конечной гр. – делитель пор. группы.

Д-во.

$x \in G$ Рассм $\langle x \rangle$

$\operatorname{ord} x = |\langle x \rangle|$

по Тh Лагранжа $\operatorname{ord}(x) \mid n$, где $|G| = n$. ■

Сл-е 2. Если порядок группы – простое число, то группа явл-ся циклической

Д-во.

Пусть $\operatorname{ord} G = p$, p – пр-е.

$\exists a \in G,\ a \neq e$

рассм $\langle a \rangle$ $p \,\vdots\, |\langle a \rangle| \Rightarrow |\langle a \rangle| = p$

$|\langle a \rangle| \neq 1$, т.к. $a \neq e$

$\Rightarrow G = \langle a \rangle$ ■

Сл-е 3. (Малая Тh Ферма)

Если p – пр-е, то $\forall\ a \not\equiv 0(p) \hookrightarrow a^{p-1} \equiv 1(p)$.

Д-во.

Рассм. группу $\mathbb{Z}_p^*$

$|\mathbb{Z}_p^*| = p-1$

$\bar{a} \in \mathbb{Z}_p^* \Rightarrow p-1 = \operatorname{ord}(\bar{a}) \cdot q$

$\bar{a}^{p-1} \equiv \bar{a}^{\operatorname{ord}(a) \cdot q} \equiv e = \bar{1} \Rightarrow a^{p-1} \equiv 1(p)$ ■

Сл-е 4. (Тh Эйлера)

$\varphi(n)$ – ф-я Эйлера. Если $(a, n) = 1$, то $a^{\varphi(n)} \equiv 1(n)$

Д-во.

Р-м группу $\mathbb{Z}_n^*$ – группа классов вычетов, взаимно простых с n.

$|\mathbb{Z}_n^*| = \varphi(n)$.

Пусть $a \in \mathbb{Z}_n^*$. Тогда $\varphi(n) = \operatorname{ord}(\bar{a}) \cdot q$

$\bar{a}^{\varphi(n)} = e = \bar{1} \Rightarrow a^{\varphi(n)} \equiv 1(n)$. ■