w4 p.1 | Порядок эл-та. Цикл гр-пы. Их подгр-пы.

G – мультипликативная группа

$S \subset G,\ S \neq \emptyset$

$\langle S \rangle = \bigcap\limits_{\substack{H \leq G \\ H \supset S}} H$ – наименьшая подгруппа, сод. систему S.

$\langle S \rangle$ – подгруппа, пород. S

Th $\langle S \rangle = \{ x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$, где $x_i \in S$, $\varepsilon_i \in \{\pm 1\} \} = H$

т.е. в правой части

всевозможные конечные пр-я эл-в S и обратных к ним

Д-во.

Проверим, что $H \leq G$

Будем расс. пр-е из пустого числа самих как e: $e \in H$.

$$(\underset{S}{\underset{\Uparrow}{x_1}}^{\varepsilon_1} \underset{S}{\underset{\Uparrow}{x_2}}^{\varepsilon_2} \dots \underset{S}{\underset{\Uparrow}{x_n}}^{\varepsilon_n}) \cdot (\underset{S}{\underset{\Uparrow}{x_{n+1}}}^{\varepsilon_n} \dots \underset{S}{\underset{\Uparrow}{x_{n+k}}}^{\varepsilon_{n+k}}) \in H$$

$$(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n})^{-1} = x_n^{-\varepsilon_n} \dots x_1^{-\varepsilon_1} \in H$$

Значит $H \leq G$

$H \subseteq \langle S \rangle$

$\langle S \rangle \leq H$, т.к. $\forall$ подгр, сод эл-ты S, обязана сод-ть их пр-я и обр к ним

$H = \langle S \rangle$ ■

Def. Мн-во S наз-ся порождающим мн-м $\langle S \rangle$.

Def. Подгруппа H в G наз-ся циклической подгруппой, пород. $a \in G$, если $H = \langle a \rangle$

Note. $H = \langle a \rangle = \{ \underbrace{\dots a^{-2}\, a^{-1}\, a \cdot a \cdot a^{1}\, a^{2} \dots}_{\text{степени } a} \}$ $\langle G, \cdot \rangle$

Note. Если $(G, +)$, то $\langle a \rangle = \{ \underbrace{\dots -2a, -a, 0, a, 2a \dots}_{\text{кр-е } a} \}$

Def. Пусть G – мульт группа.

Порядком элемента $g \in G$ наз-ся наим $n \in \mathbb{N}$: $g^n = e$

[$k \cdot g = 0$, если $(G, +)$]

Если $\forall n \in \mathbb{N}$ $g^n \neq e$, то эл-т g имеет беск пор-к.

Об-е $\operatorname{ord} g$.

Тв. Порядок эл-та $\forall$ группы равен пор-ку порожденной им цикл подгруппы
$ord\, a = |\langle a \rangle|$

Д-во.

1-й случай: Пусть все степени эл-та a попарно разл.
$\Rightarrow a^0 = e \quad a^n \neq e \; \forall n \Rightarrow ord\, a = \infty \quad |\langle a \rangle| = \infty$, т.к. все степени р-ны

2-й случай: пусть среди степеней a есть хотя бы две совп степени $a^k = a^l$, $l > k$
Тогда $a^{l-k} = a^l \cdot (a^k)^{-1} = a^l \cdot (a^l)^{-1} = e \Rightarrow ord\, a$ - конечен
Пусть $ord\, a = n$
Покажем, что $\langle a \rangle = \{e, a, a^2 \dots a^{n-1}\}$ (*)
$a^n = e$

а) Покажем, что в (*) все эл-ты попарно р-ны
$a^k = a^l \Rightarrow a^{l-k} = e$; $l - k < n$?! т.к. n - наименьшее ($ord\, a = n$)

б) Покажем, что $\forall$ степень эл. a содерж в (*)
$m = qn + r$; $r = 0 \dots n-1$
$a^m = a^{nq+r} = (a^n)^q \cdot a^r = e \cdot a^r = a^r \in \{e, a, \dots a^{n-1}\}$ ▨

Т2 (об изоморфизме цикл групп одного и того же пор-ка)
Все цикл группы одного пор-ка изоморфны между собой

Д-во.

а) Пусть G - цикл группа, $|G| = \infty$
Покажем, что гру. изоморфизм $\underset{(+)}{\mathbb{Z}} \cong \underset{(\cdot)}{G}$
$\exists a : G = \langle a \rangle \quad f : \mathbb{Z} \to G$

$$\left.\begin{array}{l} f(k) = a^k \in G \\ \quad \uparrow \\ \quad \mathbb{Z} \\ f(k+l) \overset{?}{=} f(k) \cdot f(l) \\ a^{k+l} = a^k \cdot a^l = a^k \cdot a^l \end{array}\right| \Rightarrow f \text{ - гомоморфизм}$$

Инъективность: $k \neq l \Rightarrow f(k) \neq f(l)$, т.к. $a^k \neq a^l$
(иначе гр-па конечна)

Сюръективность очевидно: $\forall a^k \in G \; \exists k \quad f(k) = a^k$

$\Rightarrow f$ - изоморфизм

$$\left.\begin{array}{l} G_1 \cong \mathbb{Z} \\ G_2 \cong \mathbb{Z} \end{array}\right| \Rightarrow G_1 \cong G_2$$

№4 р.2

б) пусть G – цикл. $G=\langle a\rangle$ $|G|=n$.

$\Rightarrow G=\{e, a, \dots a^{n-1}\}$

$\varphi: \mathbb{Z}_n \to G$ $\varphi(\bar{k})=a^k$

$\varphi(k)\cdot\varphi(l)=a^k\cdot a^l=a^{k+l}=\varphi(k+l)$ – гомоморфизм

Биективность очевидна

Проверим, что если $\bar{k}_1=\bar{k}_2$, то $\varphi(k_1)=\varphi(k_2)$

$$\Updownarrow$$

$$k_1\equiv k_2 (n)$$

$$\Updownarrow$$

$$\exists q\in\mathbb{Z}: k_1=qn+k_2.$$

$\varphi(k_1)=a^{k_1}=a^{qn+k_2}=a^{k_2}=\varphi(k_2)$ ⊠

Т2 (о подгруппах цикл группы)

а) Всякая подгруппа циклической группы – цикл группа

б) Порядок подгруппы цикл группы – делитель порядка группы. Если $|G|=n$ и q – делитель n, то в G существует единственная подгруппа порядка q

в) имеется вз. одн. соотв между $Div(n)$ – мн-во делителей n и $Sub(G)$ – мн-во подгрупп.

Д-во,

а) Д-во одновр для $|G|=\infty$ и $|G|<\infty$

Пусть $H\leq G$. Если $H=\{e\}$, то $H=\langle e\rangle$

Пусть $H\neq\{e\}$ $G=\langle a\rangle$

Если $a^k\in H$, то $a^{-k}\in H$

Тогда в H найдутся положительные степени a.

Пусть t – наим число: $t\in\mathbb{N}$, $a^t\in H$

$H\overset{?}{=}\langle a\rangle^t$

Пусть $h\in H\subseteq G \Rightarrow h=a^k$, $k\in\mathbb{Z}$

$k=qt+r$, $r\in\{0\dots t-1\}$.

$h=a^k=a^{qt+r}=a^{q\cdot t}\cdot a^r \Rightarrow a^r=a^k\cdot(a^{qt})^{-1}=\underset{\underset{H}{\Uparrow}}{a^k}\cdot\underset{\underset{H}{\Uparrow}}{(a^t)}^{-q}\in H$

Если $r>0$, то $r<t$, $r\in\mathbb{N}$, $a^r\in H$?!

$\Rightarrow r=0 \Rightarrow$

$\Rightarrow k=qt \Rightarrow h=(a^t)^q \Rightarrow H=\langle a^t\rangle$

б) G - цикл. $G = \langle a \rangle$ $|G| = n$

$G \cong \mathbb{Z}_n$, т.е будем считать, что $G = \mathbb{Z}_n$

Пусть $q \in \mathrm{Div}(n)$, $n = q \cdot t$.

Тогда $H_q = \{0, t, 2t \ldots (q-1)t\}$ - цикл. подгруппа

Покажем, что любая подгруппа H из q эл-тов равна H_q.

Пусть t - наим. $\mathbb{N}$: $\bar{t} \in H$

Пусть $n = q \cdot t + r \Rightarrow \underset{0}{\bar{n}} = q \underset{H}{\bar{t}} + \bar{r} = 0 \in H \Rightarrow \bar{r} \in H \Rightarrow \bar{r} = 0$

Значит, $H = \{\bar{0}, \bar{t}, \ldots (n-1)\bar{t}\}$ и H не сод. др-х эл-в.

т.к. $|H| = q \Rightarrow H = H_q$ ч.т.д.

в) сл-е а) и б) ■