Ryhmät 6.4.2021

G ryhmä, $B \subset G$, $B \neq \emptyset$.

$$\langle B \rangle = \bigcap_{\substack{H \le G \\ B \subset H}} H$$ osajoukon B vir. aliryhmä.

Prop. 9.17 Olk. G ryhmä, $B \subset G$, $B \neq \emptyset$. $B^{-1} = \{ b^{-1} : b \in B \}$.

$$\langle B \rangle = \underbrace{\{ a_1 a_2 \cdots a_k : a_1, \dots, a_k \in B \cup B^{-1},\ k \in \mathbb{N} \setminus \{0\} \}}_{\tilde{B}}$$

Tod. 1) $\tilde{B}$ on aliryhmä: $B \subset \tilde{B} \Rightarrow \tilde{B} \neq \emptyset$.

Jos $a_1 a_2 \cdots a_k$, $c_1 c_2 \cdots c_l \in \tilde{B}$, niin $a_1 \cdots a_k c_1 \cdots c_l \in \tilde{B}$

$$(a_1 a_2 \cdots a_{k-1} \cancel{a_k})(\underbrace{\cancel{a_k^{-1}} a_{k-1}^{-1} \cdots a_1^{-1}}_{\in \tilde{B}}) = e.$$

Aliryhmätesti $\Rightarrow \tilde{B} \le G$. Siis $\boxed{\langle B \rangle \le \tilde{B}}$.

$B \cup B^{-1} \subset \langle B \rangle$

2) Jos $\underbrace{a_1 \cdots a_k}_{\in \langle B \rangle} \in \tilde{B}$. Koska $B \subset \langle B \rangle$, niin $B^{-1} \subset \langle B \rangle \longrightarrow \boxed{\tilde{B} \le \langle B \rangle}$

$\square$

$g \in G \rightsquigarrow \langle g \rangle = \langle \{g\} \rangle$ on g:n virittämä syklinen aliryhmä.

Jos $G = \langle g \rangle$ jollain $g \in G$, niin G on syklinen ryhmä.

Esim. • $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ syklinen. ord $1 = \infty$.

• $\mathbb{Z}/q\mathbb{Z} = \langle 1 + q\mathbb{Z} \rangle$ syklinen. ord $(1+q\mathbb{Z}) = q$

$$K_4 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \{(0,0), (0,1), (1,0), (1,1)\}$$

$$\langle (0,0) \rangle = \{(0,0)\} < K_4$$

$$\langle (0,1) \rangle = \{(0,0), (0,1)\} < K_4$$

$$\langle (1,0) \rangle = \{(0,0), (1,0)\} < K_4$$

$$\langle (1,1) \rangle = \{(0,0), (1,1)\} < K_4$$

$\Rightarrow K_4$ ei ole syklinen.

$\# G$ on ryhmän G kertaluku, $\# \langle g \rangle = \text{ord } g$ (order) on alkion g kertaluku.

②

Lemma 9.22 $\operatorname{ord} g = \min\{k \geq 1 : g^k = e\}$, jos $\operatorname{ord} g \in \mathbb{N}$.

Tällöin $\langle g \rangle = \{e, g, g^2, \ldots, g^{k-1}\}$

Tod. Harj.

Prop. 9.24 Ryhmän $\mathbb{Z}$ kaikki aliryhmät ovat syklisiä.

Tod. Olk. $H \leq \mathbb{Z}$. Jos $H \neq \{0\} = \langle 0 \rangle$, niin $\exists\, b \in H - \{0\}$.

Tällöin $\{b, -b\} \cap (\mathbb{N} - \{0\}) \neq \emptyset \implies H \cap (\mathbb{N} - \{0\}) \neq \emptyset$.

$\implies \exists \min(H \cap (\mathbb{N} - \{0\})) = q \in \mathbb{N} - \{0\}$.

Os. että $H = \langle q \rangle = q\mathbb{Z} = \{kq : k \in \mathbb{Z}\}$.

Ol. $\exists\, m \in H - \langle q \rangle$. Jakoyhtälö $\implies \exists\, a \in \mathbb{Z}$, $0 < b < q$ s.e.

$$H \ni m = \overbrace{a\underbrace{q}_{\in H}}^{\in H} + b \implies b \in H$$

ristiriita. $\therefore H = \langle q \rangle$. $\square$

Lause 9.25. 1) Olkoon G syklinen ryhmä, $\# G \geq 2$, niin $G \cong \mathbb{Z}$ tai $G \cong \mathbb{Z}/q\mathbb{Z}$ jollain $q \geq 2$.

2) Jos G on syklinen ryhmä ja $\varphi : G \to G'$ on ryhmähomom., niin $\varphi(G)$ on syklinen.

Tod. Harj.

3) Syklisen ryhmän aliryhmät ovat syklisiä.

Tod. 1) Olk. $G = \langle g \rangle$, $g \in G$. Olk. $\varphi : \mathbb{Z} \to G$, $\varphi(k) = g^k \; \forall k \in \mathbb{Z}$.

Selvästi φ on surjektio.

$$\varphi(k+l) \underset{\substack{\uparrow \\ \varphi\text{:n määr}}}{=} g^{k+l} \underset{\substack{\uparrow \\ \text{assos}}}{=} g^k g^l \underset{\substack{\uparrow \\ \varphi\text{:n määr}}}{=} \varphi(k)\varphi(l)$$

, joten φ on homomorfismi.

Jos φ on injektio, niin se on isomorfismi. Tällöin $G \cong \mathbb{Z}$.

Ol. että φ ei ole injektio. Tällöin $\ker \varphi \neq \{0\} < \mathbb{Z}$.

Prop. 9.24 $\Rightarrow$ $\ker \varphi = q\mathbb{Z}$ jollain $q \in \mathbb{N} - \{0, 1\}$.

Os. että $G \cong \mathbb{Z}/q\mathbb{Z}$.

Olk. $\psi : \mathbb{Z}/q\mathbb{Z} \to G$, $\quad \psi(k+q\mathbb{Z}) = \varphi(k)$.

ψ on surjektio, koska φ on surjektio, kunhan ψ on hyvin määritelty.

ψ on hyvin määritelty: Jos $k+q\mathbb{Z} = k'+q\mathbb{Z}$, niin $k-k' \in \overset{\ker\varphi}{\overset{\parallel}{q\mathbb{Z}}}$

Siis $\quad g^k = \varphi(k) = \varphi(k'+(k-k')) \underset{\varphi \text{ homom.}}{=} \varphi(k')\underbrace{\varphi(k-k')}_{=e} = \varphi(k') = g^{k'}$.

ψ on homomorfismi:

$$\psi((m+q\mathbb{Z})+(n+q\mathbb{Z})) = \psi((m+n)+q\mathbb{Z}) \overset{\psi\text{:n määr.}}{=} \varphi(m+n) \overset{\varphi \text{ homom}}{=} \varphi(m)\varphi(n)$$

$$\underset{\psi\text{:n määr}}{=} \psi(m+q\mathbb{Z})\,\psi(n+q\mathbb{Z}).$$

Os. että ψ on injektio: Jos $\underset{\varphi(k)}{\underset{\parallel}{\psi(k+q\mathbb{Z})}} = e$, niin $k \in \ker\varphi = q\mathbb{Z}$.

Siis $k+q\mathbb{Z} = 0+q\mathbb{Z}$

$\Rightarrow \ker\psi = \{0+q\mathbb{Z}\} \Rightarrow \psi$ inj.

$\therefore$ ψ on isomorfismi.

3) Jos $G \cong \mathbb{Z}$, niin väite seuraa Prop. 9.24:stä:

Tällöin on isomorfismi $h : G \to \mathbb{Z}$. Jos $H \leq G$, niin $h(H) \leq \mathbb{Z}$ on syklinen. Tällöin $H = \underset{\substack{\uparrow \\ \text{käänteiskuvaus}}}{h^{-1}}(\underbrace{h(H)}_{\text{sykl.}})$ on syklinen 2):n nojalla.

Olk. $\varphi : \mathbb{Z} \to G = \langle g \rangle$, $\varphi(k) = g^k$.

Olk $H \leq G$. Tällöin $\underbrace{\varphi^{-1}(H)}_{\text{alkukuva.}} \leq \mathbb{Z}$ on syklinen P. 9.24 nojalla.

$H = \varphi(\underbrace{\varphi^{-1}(H)}_{\text{syklinen}})$ on syklinen kohdan 2) nojalla. □

Olk. G ryhmä, $S, T \leq G$.

$S \cup T \subset ST = \{st : s \in S, t \in T\} \subset \langle S \cup T \rangle$

6

Lemma 9.28 Jos G on komm, $S, T \leq G$, niin $ST = \langle S \cup T \rangle$.

Tod. Harj.

Esim. $U = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle < SL_2\mathbb{R}$, $L = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle < SL_2\mathbb{R}$. Tällöin UL ei ole aliryhmä.

$$\underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m}_{\in U} \underbrace{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^n}_{L} = \begin{pmatrix} 1+mn & m \\ n & 1 \end{pmatrix} \in UL$$

mutta sen käänt. alkio ei ole UL:ssä.

Määr. Olk. G ryhmä, $S, T \leq G$. Jos $ST = G$, $S \cap T = \{e\}$ ja $st = ts$ $\forall s \in S$ $\forall t \in T$, niin G on aliryhmien S ja T sisäinen suora tulo

Prop. 9.30 Jos G on aliryhmiensä H ja J sis. suora tulo, niin

$$G \cong H \times J$$
$$\parallel$$
$$(\{(h, j) : h \in H, j \in J\}, \cdot) \qquad (h_1, j_1)(h_2, j_2) = (h_1 h_2, j_1 j_2)$$

Tod. Harj.