Ryhmät 22.3.2021

G_1, G_2 ryhmiä $\rightsquigarrow$ $G_1 \times G_2$: n laskutoimitus $(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2)$.

ryhmien G_1 ja G_2 suora tulo.

Prop 8.19 Jos $G_1 \cong H_1$, $G_2 \cong H_2$, niin $G_1 \times G_2 \cong H_1 \times H_2$.

Tod. Olk. $\varphi_1 : G_1 \to H_1$ isomorfismeja
$\varphi_2 : G_2 \to H_2$ bijektiivisiä homomorfismeja.

Olk. $\Phi : G_1 \times G_2 \to H_1 \times H_2$,

$$\Phi(g_1, g_2) = (\varphi_1(g_1), \varphi_2(g_2)).$$

Os. että Φ on isomorfismi:

Olk. $g_1, g_1' \in G_1$, $g_2, g_2' \in G_2$. Tällöin

$$\Phi((g_1, g_2)(g_1', g_2')) = \Phi(g_1 g_1', g_2 g_2') = (\varphi_1(g_1 g_1'), \varphi_2(g_2 g_2'))$$

$$= (\varphi_1(g_1)\varphi_1(g_1'), \varphi_2(g_2)\varphi_2(g_2')) = (\varphi_1(g_1), \varphi_2(g_2))(\varphi_1(g_1'), \varphi_2(g_2'))$$

($\Phi(g_1, g_2)$ ja $\Phi(g_1', g_2')$)

Siis Φ on homomorfismi.

Selvästi $\Phi^{-1}(h_1, h_2) = (\varphi_1^{-1}(h_1), \varphi_2^{-1}(h_2))$. Siis Φ on bijektio. □

Jäännösluokkien multiplikatiiviset ryhmät

$(\mathbb{Z}/8\mathbb{Z}, \cdot)$: Huomataan, että

$(3+8\mathbb{Z})(5+8\mathbb{Z}) = 7+8\mathbb{Z}$
$(3+8\mathbb{Z})(7+8\mathbb{Z}) = 5+8\mathbb{Z}$
$(5+8\mathbb{Z})(7+8\mathbb{Z}) = 3+8\mathbb{Z}$

$(1+8\mathbb{Z})(1+8\mathbb{Z}) = 1+8\mathbb{Z}$
$(3+8\mathbb{Z})(3+8\mathbb{Z}) = 1+8\mathbb{Z}$
$9+8\mathbb{Z}$
$(5+8\mathbb{Z})(5+8\mathbb{Z}) = 1+8\mathbb{Z}$
$(7+8\mathbb{Z})(7+8\mathbb{Z}) = 1+8\mathbb{Z}$.
$-1+8\mathbb{Z}$

$\rightsquigarrow Y = \{1+8\mathbb{Z}, 3+8\mathbb{Z}, 5+8\mathbb{Z}, 7+8\mathbb{Z}\}$ on vakaa $(\mathbb{Z}/8\mathbb{Z}, \cdot)$:ssa ja jokaisella alkiolla on käänteisalkio ja n.o on $1+8\mathbb{Z}$.

$\rightsquigarrow (Y, \cdot)$ on ryhmä. (Renkaan $\mathbb{Z}/8\mathbb{Z}$ Y:ksikköiden ryhmä $(\mathbb{Z}/8\mathbb{Z})^*$)

$(\mathbb{Z}/8\mathbb{Z}, \cdot)$:n alkioilla $0+8\mathbb{Z}$, $2+8\mathbb{Z}$, $4+8\mathbb{Z}$ ja $6+8\mathbb{Z}$ ei ole käänteisalkiota.

Prop. 8.20 Olk. $q \geq 2$. Alkiolla $a + q\mathbb{Z} \in (\mathbb{Z}/q\mathbb{Z}, \cdot)$ on käänteisalkio

$\Leftrightarrow$ $\mathrm{syt}(a, q) = 1$.

Tod. $b + q\mathbb{Z}$ on $a + q\mathbb{Z}$:n käänt. alkio $\Leftrightarrow$ $(a+q\mathbb{Z})(b+q\mathbb{Z}) = 1+q\mathbb{Z}$

$= ab + q\mathbb{Z}$.

$\Leftrightarrow$ $ab \equiv 1 \bmod q$ $\Leftrightarrow$ $\exists\, k \in \mathbb{Z}$: $ab + qk = 1$ $\Leftrightarrow$ $\mathrm{syt}(a, b) = 1$. $\square$

↑ Bézout / ks. Lukuteoria 1.

Seuraus. Jos p on alkuluku, niin jokaisella $a + p\mathbb{Z}$, $1 \leq a \leq p-1$, on käänteisalkio.

Prop. 8.21. $\{ a + q\mathbb{Z} : \mathrm{syt}(a, q) = 1 \}$ on vaikea $(\mathbb{Z}/q\mathbb{Z}, \cdot)$:ssa.

Tod. $\big((a+q\mathbb{Z})(b+q\mathbb{Z})\big)\big((\bar{a}+q\mathbb{Z})(\bar{b}+q\mathbb{Z})\big)$

$= 1 + q\mathbb{Z}$.

$(a+q\mathbb{Z})(\bar{a}+q\mathbb{Z}) = 1+q\mathbb{Z}$

$(b+q\mathbb{Z})(\bar{b}+q\mathbb{Z}) = 1+q\mathbb{Z}$.

$\rightsquigarrow \left(\{a+q\mathbb{Z} : sgn(a,q)=1\}, \cdot\right) = \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ on rythmé.

$\left(\mathbb{Z}/8\mathbb{Z}\right)^\times$ $\qquad$ $3+8\mathbb{Z}$ =

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$K_4 = \left(\mathbb{Z}/2\mathbb{Z}\right)^2$ $\qquad$ $f(7)$ =

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

$f(5) = f(3)$

Kuvaus $\quad 1+8\mathbb{Z} \xrightarrow{f} (0,0)$

$3+8\mathbb{Z} \mapsto (0,1)$

$5+8\mathbb{Z} \mapsto (1,0)$

$7+8\mathbb{Z} \mapsto (1,1)$

on isomorfismi.

$\rightsquigarrow \left(\mathbb{Z}/8\mathbb{Z}\right)^\times \cong K_4$

9 Aliryhmät.

$B \neq \emptyset$ $\quad b_1 b_2 \in B \;\forall\; b_1, b_2 \in B.$ (=)

Määr. Olk. G ryhmä, $B < G$ vakaa. Jos B on ryhmä (indusoidulla laskutoimituksella, G:n laskutoimitus, määrää B:n laskutoimituksen)
niin B on G:n aliryhmä, $B \leq G$.

Jos $B \leq G$ ja $B \neq G$, merk. $B < G$, B on G:n aito aliryhmä.

Esim. 1) $G \leq G$, $\{e\} \leq G$ $\forall\, G$.

2) $\mathbb{Z} \leq \mathbb{R} \leq \mathbb{C}$ $\quad \mathbb{Z} < \mathbb{R} < \mathbb{C}$.

3) $\mathbb{R}^\times = (\mathbb{R} - \{0\}, \cdot)$, $\quad \mathbb{R}_+ = (]0, \infty[, \cdot) \rightsquigarrow \mathbb{R}_+ < \mathbb{R}^\times$

Lemma 9.2. Jos $H \leq G$ ja $e \in G$ on n.a., niin $e \in H$. (ja on siis H:n n.a)

Tod. Jos $a, b \in H$ ja $ab = b = eb \Rightarrow a = e$. (Gin supistussääntö) $\square$

(5) H on ryhmä, joten sillä on n.a.

Prop. 9.3 (Aliryhmätesti) Olk. G ryhmä, $H \subset G$, $H \neq \emptyset$.

1) Jos $xy^{-1} \in H$ $\forall$ $x, y \in H$, niin $H \leq G$.

2) Jos $xy \in H$ $\forall$ $x, y \in H$ ja $y^{-1} \in H$ $\forall$ $y \in H$, niin $H \leq G$.

Tod. $e \in G$ n. a.

Ol. että 1):n oletus on voimassa.

Jos $h \in H$, niin 1) $\Rightarrow e = h h^{-1} \in H$ $\Rightarrow$ H:ssa on n.a.

$\Rightarrow$ $h^{-1} = e h^{-1} \in H$.

Os. vieä, että H on vakaa: Olk. $a, b \in H$. Tällöin $b^{-1} \in H$, joten

$a b = a (b^{-1})^{-1} \in H$. ☒

2) seuraa testistä 1. ☐

(Esim. Os. testissä 2), että $\mathbb{Z} \leq \mathbb{R}$: $k, l \in \mathbb{Z} \Rightarrow k + l \in \mathbb{Z}$ OK.
$k \in \mathbb{Z}$ $(-1 \cdot k) + k = 0 \Rightarrow -k \in \mathbb{Z}$.
$\in \mathbb{Z}$)

Esim. Olk. $X \neq \emptyset$. X:n permutaatioryhmä on

$$\mathrm{Perm}(X) = (\{ f : X \to X \text{ bijektio} \}, \circ)$$

kuvausten yhdistäminen.
(assos. laskutoimitus)

$id : X \to X$ on $\mathrm{Perm}(X)$:n n.a

f:in käänteisalkio on f:in käänteiskuvaus.

$X = \mathbb{R}^n$

$$GL(\mathbb{R}^n) = \{ L : \mathbb{R}^n \to \mathbb{R}^n \text{ bijektiivinen lineaarikuvaus} \} \leq \mathrm{Perm}(\mathbb{R}^n) :$$

$GL(\mathbb{R}^n) \ni id \Rightarrow GL(\mathbb{R}^n) \neq \emptyset$.

Jos $L_1, L_2 \in GL(\mathbb{R}^n)$, niin L_1, L_2 lin. kuvauksia $\mathbb{R}^n \to \mathbb{R}^n$.

LAG1 : $L_1 \circ L_2$ on lin. kuvaus. $\rightsquigarrow L_1 \circ L_2 \in GL(\mathbb{R}^n)$.

LAG1 : Jos $L \in GL(\mathbb{R}^n)$, niin L^{-1} on lin. bijektio $\rightsquigarrow L^{-1} \in GL(\mathbb{R}^n)$.

Alkuehtotesti : $GL(\mathbb{R}^n) \leq \mathrm{Perm}(\mathbb{R}^n)$

$\mathbb{R}^n$:n yleinen lineaarinen ryhmä (general linear group)