Ryhmät 16.3.2021

Laskutoimituksella varustettu joukko[a] $(G, *)$ on *ryhmä*, jos

- laskutoimitus $*$ on assosiatiivinen, $(a*b)*c = a*(b*c)$
- laskutoimituksella $*$ on neutraalialkio,
- jokaisella $g \in (G, *)$ on käänteisalkio.

Ryhmän G alkioiden lukumäärä $\#G$ on ryhmän G *kertaluku*.

[a] Muista määritelmä luvusta 1.1.

$\mathbb{R}$

$\mathbb{Q}$

Esim. 1) $(\mathbb{Z}, +)$

2) $\mathbb{Q}^{\times} = (\mathbb{Q} - \{0\}, \cdot)$

Prop. 8.3. G ryhmä, $e \in G$ neutr. alkio.

1) Jos $e' \in G$ on n.a, niin $e' = e$.
2) Jos a^{-1} ja $\bar{a}$ ovat a:n käänt. alkioita, niin $\bar{a} = a^{-1}$
3) Jos $\bar{a}a = e$, niin $\bar{a} = a^{-1}$.
4) $(ab)^{-1} = b^{-1}a^{-1}$.

Tod. 1) $e' \underset{\substack{\uparrow \\ e \text{ on n.a}}}{=} ee' \underset{\substack{\uparrow \\ e' \text{ on n.a}}}{=} e$.

2) $\bar{a} = \bar{a}e = \bar{a}\underbrace{(aa^{-1})}_{=e} = \underbrace{(\bar{a}a)}_{=e}a^{-1} = a^{-1}$

3) $\bar{a} = \bar{a}e = \bar{a}\overbrace{(aa^{-1})}^{=e} = \overbrace{(\bar{a}a)}^{=e}a^{-1} = a^{-1}$

4) $(b^{-1}a^{-1})(ab) = b^{-1}\underbrace{(a^{-1}a)}_{=e}b = e$

3) $\Rightarrow b^{-1}a^{-1} = (ab)^{-1}$. $\square$

Prop. 8.4. Olk. G ryhmä. $a, b, c \in G$. Tällöin

$$\boxed{\begin{aligned} ab = ac &\Rightarrow b = c \\ ba = ca &\Rightarrow b = c \end{aligned}}$$

supistussäännöt

Tod. Ol. $ab = ac$. Tällöin $b = \underbrace{a^{-1}a}_{=e} b = a^{-1}(ab) = a^{-1}(ac) = c$. $\square$

Jos $G = \{g_1, \dots, g_n\}$ on äärellinen {laskut. var. joukko} ryhmä, laskut. voi havainnollistaa laskutaululla:

$*$	g_1	g_2	$\dots$	g_n
g_1		$g_1 * g_2$		
g_2				$g_2 * g_n$
$\vdots$				
g_n				

Lemma 8.6. Äärellisen ryhmän jokainen alkio on jokaisella rivillä ja jokaisella sarakkeella.

Neljän alkion ryhmän $\mathbb{Z}/4\mathbb{Z}$, laskutaulu on

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tod. kirjoitettu edustajien avulla $1 \rightsquigarrow 1 + 4\mathbb{Z}$

$(2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$

$5 - 1 = 4 \in 4\mathbb{Z}$.

Olk. G_1, G_2 ryhmiä. Määr. laskutoimitus joukossa $G_1 \times G_2$:

$$\underbrace{(g_1, g_2)}_{\in G_1 \times G_2}\underbrace{(h_1, h_2)}_{} = (g_1 h_1, g_2 h_2).$$ Assos OK koska G_1:in ja G_2:n laskut. on.

Jos $e_1 \in G_1$, $e_2 \in G_2$ ovat neutr. alkioita, niin

$$\left.\begin{array}{l}(e_1, e_2)(g_1, g_2) = (e_1 g_1, e_2 g_2) = (g_1, g_2) \\ (g_1, g_2)(e_1, e_2) = \dots = (g_1, g_2)\end{array}\right\} \Rightarrow (e_1, e_2) \in G_1 \times G_2 \text{ on n.a.}$$

$(g_1^{-1}, g_2^{-1})(g_1, g_2) = (e_1, e_2)$. Prop. 8,3 3) $\Rightarrow (g_1^{-1}, g_2^{-1}) = (g_1, g_2)^{-1}$.

Siis $G_1 \times G_2$ tällä laskut. on ryhmä: G_1:n ja G_2:n <u>suora</u> <u>tulo</u>.

Ryhmien G_α <u>suora</u> <u>tulo</u>:

<u>Määr.</u> $A \neq \emptyset$, G_α ryhmä $\forall \alpha \in A$.

$$\prod_{\alpha \in A} G_\alpha = \{(g_\alpha)_{\alpha \in A} : g_\alpha \in G_\alpha \ \forall \alpha \in A\}.$$

Jos $A = \{1,2\}$, niin $\prod_{\alpha \in \{1,2\}} G_\alpha = G_1 \times G_2$

3 laskutoimitus $(g_\alpha)_{\alpha \in A} (h_\alpha)_{\alpha \in A} = (g_\alpha h_\alpha)_{\alpha \in A}$.

<u>Prop. 8,10</u> $\prod G_\alpha$ on ryhmä.

Esim. 1) $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z})^2$

Kleinin 4-ryhmä K_4

laskut: $(a_1 + 2\mathbb{Z}, a_2 + 2\mathbb{Z}) + (b_1 + 2\mathbb{Z}, b_2 + 2\mathbb{Z}) = ((a_1 + b_1) + 2\mathbb{Z}, (a_2 + b_2) + 2\mathbb{Z})$

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

2) $\mathbb{R}^n$ $\quad (x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$.

on ryhmä.

Määr. G, G' ryhmiä, kuvaus $\varphi : G \to G'$ on (ryhmä)homomorfismi, jos $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \quad \forall g_1, g_2 \in G$.

Jos φ on lisäksi bijektio, niin φ on ryhmäisomorfismi.

Tällöin G ja G' ovat isomorfisia: $G \cong G'$.

Ryhmäisomorfismi $\varphi : G \to G$ on ryhmän G automorfismi.

Esim. $\exp : \mathbb{R} \to (\mathbb{R}_+, \cdot)$, $\exp(t) = e^t \quad \forall\, t \in \mathbb{R}$.

$\mathbb{R} = (\mathbb{R}, +)$, $\quad (\mathbb{R}_+, \cdot) = \underbrace{]0,\infty[}_{\text{ryhmä}}$

JMA: $\begin{cases} \exp \text{ on bijektio} \\ \exp(t+s) = e^{t+s} = e^t e^s = \exp(t)\exp(s) \quad \forall\, t, s \in \mathbb{R}. \end{cases}$

$\Rightarrow$ exp on homomorfismi.
isomorfismi.

$(\exp)^{-1} = \log : \mathbb{R}_+ \to \mathbb{R}$

JMA: $\log(xy) = \log x + \log y \quad \forall\, x, y > 0$. $\quad$ log on isomorfismi.

Prop. 8.16 $\quad$ 1) Jos $\varphi_1 : G_1 \to G_2$, $\varphi_2 : G_2 \to G_3$ ovat homom, niin $\varphi_2 \circ \varphi_1 : G_1 \to G_3$ on homomorfismi

2) Jos $\varphi : G \to G'$ on isomorfismi, niin $\varphi^{-1} : G' \to G$ on isomorfismi.

3) Jos $G_1 \cong G_2$ ja $G_2 \cong G_3$, niin $G_1 \cong G_3$

Tod. 1) Olk. $g, h \in G_1$. Tällöin $\varphi_2 \circ \varphi_1(gh) = \varphi_2(\overbrace{\varphi_1(gh)}^{\varphi_1(g)\varphi_1(h)}) = \varphi_2(\varphi_1(g))\varphi_2(\varphi_1(h))$
$= (\varphi_2 \circ \varphi_1(g))(\varphi_2 \circ \varphi_1(h))$.

2) $\varphi : G \to G'$ isomorfismi. Os. että $\varphi^{-1} : G' \to G$ on homomorfismi.

Olk. $g', h' \in G'$. Tällöin $\underline{\underline{g'h'}} = \varphi \circ \varphi^{-1}(g')\, \varphi \circ \varphi^{-1}(h')$

$\overset{\varphi \text{ homom}}{=} \underline{\underline{\varphi(\varphi^{-1}(g')\varphi^{-1}(h'))}}$

φ on $\underline{\underline{\text{bijektio}}}$ $\Rightarrow$ $\varphi^{-1}(g'h') = \varphi^{-1}(g')\varphi^{-1}(h')$.

3) Seuraa kohdasta 1). $\square$

Prop. 8.17 Olk. $\varphi : G \to G'$ ryhmähomom. $e \in G$, $e' \in G'$ neutr. alkiot.

Tällöin 1) $\varphi(e) = e'$

2) $\varphi(g)^{-1} = \varphi(g^{-1})$.

Tod. 1) $e'\,\underline{\underline{\varphi(e)}} = \varphi(e) = \varphi(e\,e) \overset{\varphi \text{ homom}}{=} \varphi(e)\,\underline{\underline{\varphi(e)}} \overset{\text{supista}}{\Longrightarrow} e' = \varphi(e)$.

2) $\varphi(g^{-1})\,\varphi(g) \underset{\varphi \text{ homom.}}{=} \varphi(g^{-1}g) = \varphi(e) \overset{1)}{=} e' \underset{P. 8.3\ 3)}{\Longrightarrow} \varphi(g)^{-1} = \varphi(g^{-1})$. $\square$

12.3 tai myöh.