Ryhmät 23.3.2021

$\mathbb{R}^n$:n yleinen lineaarinen ryhmä

$GL(\mathbb{R}^n) = \{ L : \underbrace{\mathbb{R}^n \circlearrowleft}_{\mathbb{R}^n \to \mathbb{R}^n} \text{ lin. bijektio} \} < \mathrm{Perm}(\mathbb{R}^n) = (\{ f : \mathbb{R}^n \circlearrowleft \text{ bijektio} \}, \circ)$

$\mathbb{Q}, \mathbb{C}$

$GL_n(\mathbb{R}) = \{ A \in \underbrace{M_n(\mathbb{R})}_{\substack{n\times n\text{-matriisit} \\ \mathbb{R}\text{-kertoimiset}}} : \det A \neq 0 \}$ on vakaa laskut.var. joukossa $(M_n(\mathbb{R}), \cdot)$

matr. kertolasku

jos $\det A \neq 0 \neq \det B$,

niin $\det(AB) = \underbrace{\det(A)}_{\neq 0} \underbrace{\det(B)}_{\neq 0} \neq 0$.

($\det : (M_n(\mathbb{R}), \cdot) \to \mathbb{R}^\times$ on homomorfismi)

$I_n = \mathrm{diag}(1, 1, \ldots, 1) \in GL_n(\mathbb{R})$

Jos $A \in GL_n(\mathbb{R})$, niin A on kääntyvä (LAG): $\exists A^{-1} \in M_n(\mathbb{R})$,

$\det(A^{-1}) \neq 0$.

$\to$ $GL_n(\mathbb{R})$ on ryhmä, sillä matr. kertolasku on assosiatiivinen:

$(AB)C = A(BC) \quad \forall A, B, C \in M_n(\mathbb{R})$.

Prop. 9.9. $GL(\mathbb{R}^n) \cong GL_n(\mathbb{R})$

Tod. (LAG) Olk. $\mathrm{Mat}: GL(\mathbb{R}^n) \to GL_n(\mathbb{R})$ kuvaus, joka liittää lin. kuvaukseen L sen matriisin stand. kannassa.

$$\mathrm{Mat}(L)_{ij} = \underbrace{(e_i \mid Le_j)}_{\text{sisätulo}} = e_i \cdot (Le_j)$$

LAG: $\begin{cases} \mathrm{Mat}(L_1 \circ L_2) = \mathrm{Mat}(L_1)\,\mathrm{Mat}(L_2). \\ \mathrm{Mat} \text{ on bijektio.} \end{cases}$ $\square$

Määr. Olk. $\mathbb{K} \in \{\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}\}$. Erityinen lineaarinen ryhmä (special linear)

$$SL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) : \det A = 1\}.$$

$SL_n(\mathbb{R}) < GL_n(\mathbb{R})$ ($\mathbb{Q}$, $\mathbb{C}$; $\mathbb{Q}$, $\mathbb{C}$)

Os. tämä aliryhmätestillä:

$SL_n(\mathbb{R}) \ni I_n \Rightarrow SL_n(\mathbb{R}) \neq \emptyset$.

Jos $\det A = \det B = 1$, niin $\det(AB) = \underbrace{\det A}_{=1}\, \underbrace{\det B}_{=1} = 1$

$\Rightarrow AB \in SL_n(\mathbb{R})$, jos $A, B \in SL_n(\mathbb{R})$.

$A \in SL_n(\mathbb{R}) \subset GL_n(\mathbb{R}) \Rightarrow \exists A^{-1} \in GL_n(\mathbb{R})$.

LAG: $\det(A^{-1}) = \frac{1}{\det A} = \frac{1}{1} = 1$. $\Rightarrow A^{-1} \in SL_n(\mathbb{R})$.

Aliryhmätesti: $SL_n(\mathbb{R}) \underset{\uparrow}{<} GL_n(\mathbb{R})$

$\mathrm{diag}(2, \ldots, 2) \in GL_n(\mathbb{R}) - SL_n(\mathbb{R})$.

Jos $\mathbb{K} = \mathbb{Z}$, niin 2 ensimmäistä vaihetta samoin.

$A \in SL_n(\mathbb{Z}) \in GL_n(\mathbb{R}) \Rightarrow \exists A^{-1} \in GL_n(\mathbb{R})$

$\| \leftarrow$ LAG

$1 = \frac{1}{\det A}(\underbrace{\mathrm{cof} A}) \in SL_n(\mathbb{Z})$.

kertoimet A:n alimatriisien det $\in \mathbb{Z}$.

$\Rightarrow SL_n(\mathbb{Z}) < GL_n(\mathbb{R})$

Prop. 9.11 Olk $\varphi : G \to G'$ ryhmähomom.

1) Jos $H \leq G$, niin $\varphi(H) \leq G'$ $\Longrightarrow$ $\varphi(G) \leq G'$

2) Jos $H' \leq G'$, niin $\varphi^{-1}(H') \leq G$. $\Longrightarrow$ $\ker \varphi \leq G$

$\quad \overset{\shortparallel}{\{h \in G : \varphi(h) \in H'\}}$.

Tod. 1) Olk. $e \in G$ n.a. $e \in H \leq G$. Siis $\varphi(e) \in \varphi(H) \Rightarrow \varphi(H) \neq \emptyset$.

Olk. $\varphi(g), \varphi(h) \in \varphi(H)$. Tällöin

$$\varphi(g)\varphi(h)^{-1} \underset{\substack{\uparrow \\ \text{Prop. 8.17}}}{=} \varphi(g)\varphi(h^{-1}) \underset{\substack{\uparrow \\ \varphi \text{ homom}}}{=} \varphi(\underbrace{gh^{-1}}_{\in H}) \in \varphi(H).$$

Aliryhmätesti: $\varphi(H) \leq G'$.

2) Harj. $\square$

$e' \in G'$ on n.a.

φ:n ydin on $\ker \varphi = \varphi^{-1}(e')$, φ:n kuva on $\varphi(G)$.

$= \varphi^{-1}(\{e'\})$, $\{e'\} \leq G'$

Prop. 9.14. Olk. $\varphi: G \to G'$ ryhmähomomorfismi. φ on injektio $\Leftrightarrow \ker \varphi = \{e\}$.

Tod. Jos φ on injektio, niin $\varphi^{-1}(e') = \{e\}$, sillä $\varphi(e) = e'$ (Prop. 8.17)

Ol. että $\ker \varphi = \{e\}$. Olk. $g, h \in G$ s.e. $\varphi(g) = \varphi(h)$.

Tällöin $\varphi(gh^{-1}) = \varphi(g)\underbrace{\varphi(h)}_{=\varphi(g)}{}^{-1} = e' \Rightarrow gh^{-1} \in \ker \varphi = \{e\}$

$\Rightarrow gh^{-1} = e \Rightarrow \underline{g = h}$. Siis φ on injektio. $\square$

Esim. $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ on ryhmähomomorfismi.

$\ker \det = \det^{-1}(1) = \{A \in GL_n(\mathbb{R}) : \det A = 1\} = SL_n(\mathbb{R})$.

Jos $G_1, G_2 \leq G$, niin $G_1 \cap G_2 \leq G$ $(I = \{1,2\})$

Olk. G ryhmä.

Prop. 9.15. Olk. $I \neq \emptyset$, $H_i \leq G$ $\forall i \in I$.

Tällöin $\bigcap_{i \in I} H_i \leq G$.

$\left(\bigcap_{i \in I} H_i = \{ g \in G : g \in H_i \ \forall i \in I \} \right)$

Olk. G ryhmä, $B \subset G$, $B \neq \emptyset$.
Osajoukon B virittämä aliryhmä on

p. 9.15

$$\langle B \rangle = \bigcap_{\substack{H \leq G \\ B \subset H}} H \leq G \qquad \left(\text{Tässä } I = \{ H \leq G : B \subset H \} \right)$$

Olk. $B = \{b\}$. Tällöin $\langle b \rangle = \langle \{b\} \rangle$ on alkion b virittämä syklinen aliryhmä

Ryhmä Z on syklinen ryhmä, jos $Z = \langle a \rangle$ jollain $a \in Z$.

Huom. $b^2 = bb \in \langle b \rangle \leq G \rightsquigarrow b^3 = b\underbrace{b^2}_{\in \langle b \rangle} \in \langle b \rangle$

$b^{-1} \in \langle b \rangle \rightsquigarrow b^{-2} = \underbrace{b^{-1} b^{-1}}_{\in \langle b \rangle} \in \langle b \rangle$

$b^0 = e \in \langle b \rangle$

Aliryhmätesti: tämä on G:n aliryhmä.

$$\{ b^k : k \in \mathbb{Z} \} \ni b$$

$$\leq \langle b \rangle = \bigcap_{H \leq G,\ b \in H} H$$

tässä on $=$

⑥

Siis $\langle b \rangle = \{ b^k : k \in \mathbb{Z} \}$. (katso luku 1.9)

Esim. • $\mathbb{Z} = \langle 1 \rangle = \{ k \cdot 1 : k \in \mathbb{Z} \}$. (additiivinen merkintä → potenssien sijaan käytetään monikertoja)

• $\mathbb{Z}/q\mathbb{Z} = \langle 1 + q\mathbb{Z} \rangle = \{ k + q\mathbb{Z} : k \in \mathbb{Z} \}$

Yleisemmin:

Prop. 9.17 Olk. G ryhmä, $B \subset G$, $B \neq \emptyset$.

$B^{-1} = \{ b^{-1} : b \in B \}$.

Tällöin

$$\langle B \rangle = \{ a_1 a_2 \cdots a_k : a_1, \ldots, a_k \in B \cup B^{-1}, k \in \mathbb{N} - \{0\} \}$$

Esim $\mathbb{Z}^2 = \langle (1,0), (0,1) \rangle = \{ k(1,0) + l(0,1) : k, l \in \mathbb{Z} \}$.