Renkaat ja kunnat 11.1.2021

Kirjalliset harjoitukset pal. ti klo 12 mennessä.
pal. sähköpostilla: 1 tiedostona pdf

Ratkaisut julk. ti iltapäivällä.
Ke klo 14 vast. otto Zoomissa.

Ratkomo to 14–18

Harjoituksista pisteitä 20% → 1
⋮
80% → 4

Tentti 24 p

Sisältö

- laskutoimitukset ...
- $(A, +, \cdot)$ $(\mathbb{R}, +, \cdot)$, (2x2-Matriisit, +, ·)
  joukko laskutoimituksia.
- Kongruenssiluokat mod q (vrt. lukuteoria 1)
  → $(\mathbb{Z}/q\mathbb{Z}, +, \cdot)$
- Polynomirenkaat
- Äärelliset kunnat

1

1 Laskutoimitukset

Esim. Kokonaislukujen $+$ ja $\cdot$ ovat laskutoimituksia.

$a, b \in \mathbb{Z}$ ($\mathbb{R}$) $\quad a+b \in \mathbb{Z}$ ($\mathbb{R}$)

$(a,b) \in \mathbb{Z} \times \mathbb{Z}$. $\quad a \cdot b \in \mathbb{Z}$ ($\mathbb{R}$).

Määr. Olk. $A \neq \emptyset$. Kuvaus $* : A \times A \to A$ on laskutoimitus.

$*(a,b) = a * b$.

Pari $(A, *)$ on $\begin{cases} \text{laskutoimituksella varustettu joukko.} \\ \text{magma.} \end{cases}$

Esim. 1) $x, y \in \mathbb{R}^n$ $\quad x = (x_1, \dots, x_n)$ $\quad$ Vektorien yhteenlasku: $x + y = (x_1+y_1, \dots, x_n+y_n) \in \mathbb{R}^n$

$y = (y_1, \dots, y_n)$

2) $M_n(\mathbb{R}) = \{ n \times n\text{-matriisit} \}$.

$A = (A_{ij})$, $B = (B_{ij})$ $\quad$ Kaksi laskutoimitusta: $A + B = (A_{ij} + B_{ij})$

$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}$ $\rightsquigarrow$ matriisien kertolasku.

Esim: A joukko. $\mathcal{P}(A) = \{ B \subset A \}$ A:n potenssijoukko.

Potenssijoukon laskutoimituksia: $\cup$ joukkojen yhdiste

$\cap$ —"— leikkaus.

$B_1, B_2 \in \mathcal{P}(A) \Rightarrow B_1, B_2 \subset A \Rightarrow B_1 \cup B_2 \subset A \Rightarrow B_1 \cup B_2 \in \mathcal{P}(A)$.

$\Rightarrow B_1 \cap B_2 \subset A \Rightarrow B_1 \cap B_2 \in \mathcal{P}(A)$.

Esim. 1) Vektorien pistetulo: $x, y \in \mathbb{R}^n \rightsquigarrow x \cdot y = \sum_{i=1}^{n} x_i y_i \in \mathbb{R}$

ei ole laskutoimitus.

2) Kokonaislukujen jakolasku ei ole laskutoimitus.

$1, 2 \in \mathbb{Z} \rightsquigarrow \frac{1}{2} \notin \mathbb{Z}$.

$1, 2 \in \mathbb{Q} \rightsquigarrow \frac{1}{2} \in \mathbb{Q}$ mutta esim $\frac{1}{0}$ ei ole määritelty, joten $\mathbb{Q}$:n jakolasku ei ole laskutoimitus

③

Laskutaulu. Jos A on äärellinen (pieni) joukko, void. muodostaa laskut. var. joukon $(A, *)$ laskutaulu

$*$	a_1	a_2	a_3
a_1	$a_1 * a_1$	$a_1 * a_2$	
a_2	$a_2 * a_1$	$a_2 * a_2$	
a_3			

$(\mathcal{P}(\{0,1\}), \cap)$

$\cap$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{0\}$	$\emptyset$	$\{0\}$	$\emptyset$	$\{0\}$
$\{1\}$	$\emptyset$	$\emptyset$	$\{1\}$	$\{1\}$
$\{0,1\}$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ Olk $+, \cdot$ $\mathbb{R}$:n yhteenlasku ja kertolasku.

$a, b \in \mathbb{N} \Rightarrow a+b \in \mathbb{N}$, $ab \in \mathbb{N}$ $\Rightarrow$ $\mathbb{R}$:n $+$ ja $\cdot$ määräävät 2 laskutoimitusta $\mathbb{N}$:ssä.

Määr. Olk. $(A, *)$ laskut. var. joukko. $B \subset A$ on <u>vakaa</u>, jos $b_1 * b_2 \in B$ $\forall\, b_1, b_2 \in B$.

$\rightsquigarrow$ $*$ <u>määrää</u> laskutoimituksen $*|_B$ B:ssä: $b_1 *|_B b_2 = b_1 * b_2$

Laskutoimitukselle $*|_B$ käyt. merkintää $*$. $*|_B$ on <u>indusoitu laskutoimitus</u>.

Esim. Jos $a, b \in \mathbb{R}$, $a, b \neq 0$, niin $ab \neq 0$. Merkintä $\mathbb{R}-\{0\} = \{x \in \mathbb{R} : x \neq 0\}$

$= \mathbb{R} \setminus \{0\}$

$\mathbb{R}-\{0\}$ on laskut. var. joukon $(\mathbb{R}, \cdot)$ vakaa osajoukko.

$\rightsquigarrow$ kertolasku määrää laskutoimituksen joukossa $\mathbb{R}-\{0\}$.

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

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

Esim exp on homomorfismi.

Analyysi: $\exp(x+y) = e^{x+y} = e^x e^y = \exp(x)\exp(y)$

Määr. Olk. $(A, *)$, $(B, \circledast)$ laskut. var. joukkoja. Kuvaus $\varphi : (A, *) \to (B, \circledast)$ on homomorfismi, jos $\varphi(a_1 * a_2) = \varphi(a_1) \circledast \varphi(a_2) \quad \forall a_1, a_2 \in A$.

Jos homomorfismi on bijektio, niin se on isomorfismi.

Jos $\varphi : (A, *) \to (B, \circledast)$ on isomorfismi, niin laskut. var. joukot $(A, *)$ ja $(B, \circledast)$ ovat isomorfisia.