

Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo
mikhirve@utu.fi

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2026

Määritelmä

Joukon A *permutaatio* on bijektio $f : A \rightarrow A$. Symmetrinen ryhmä $\text{Sym}(A)$ on kaikkien permutaatioiden $A \rightarrow A$ joukko, ryhmäoperaationa funktioiden yhdistäminen. Ryhmän $\text{Sym}(A)$ aliryhmiä kutsutaan permutaatioryhmiksi.

Määritelmä

Jos $A = \{1, 2, \dots, n\}$, merkitään $S_n = \text{Sym}(A)$.

Määritelmä (k -sykli)

$(i_1, i_2, \dots, i_k)$ tarkoittaa permutaatiota, jossa $i_1 \rightarrow i_2, \dots, i_{k-1} \rightarrow i_k, i_k \rightarrow i_1$ ja muut $i_j \rightarrow i_j$ muille alkiolle.

Esimerkki

Transpositiot, syklien yhdistäminen.

Cayleyn lause

Jos $a \in G$, on funktio $f_a(g) = ag$ ryhmän G alkioden permutaatio.

Seuraus

Ryhmien esitys, ryhmätaulu

Määritelmä

Alkiot $g_1, \dots, g_n$ generoivat ryhmän G , jos

$$G = \{g_{i_1}^{a_1} g_{i_2}^{a_2} \dots g_{i_k}^{a_k} \mid a_i \in \mathbb{Z}, k \in \mathbb{N} \cup \{0\}\}.$$

Tällöin merkitään

$$G = \langle g_1, \dots, g_n \rangle.$$

Määritelmä

Ryhmä G on syklinen, jos $G = \langle g \rangle$ jollekin $g \in G$. Tällöin

$$G = \{g^k \mid k \in \mathbb{Z}\}.$$

Äärellinen syklinen ryhmä

$$G = \{g^0, g^1, \dots, g^{n-1}\}.$$

Esimerkki

$$GL_n(\mathbb{R}) = \{A \in \mathbb{R}^{n \times n} \mid \det(A) \neq 0\}$$

Huomautus

- Epäkommutatiivisten ryhmien teorilla voidaan mallintaa symmetrioita.
- Ryhmäteorialla on lukuisa määrä sovelluksia erityisesti kvanttifysiikassa.
- Epäkommutatiivisten ryhmien operaatio $*$ jätetään yleensä merkitsemättä: $a * b$ merkitään ab .
- Kommutatiivisissa ryhmissä operaatiosta käytetään usein merkintää $+$, identiteettialkiosta merkintää 0 ja alkion a käänteisalkiosta merkintää $-a$.

Esimerkki

$\mathbb{Z}$ on kommutatiivinen ryhmä, kun ryhmäoperaatioksi valitaan tavallinen yhteenlasku $+$, neutraalialkioksi 0 ja a :n käänteisalkioksi vastaluku $-a$

- $(a + b) + c = a + (b + c)$
- $a + 0 = 0 + a = a$
- $a + (-a) = -a + a = 0$
- $a + b = b + a$ (kommutatiivisuus)

Esimerkki

$\mathbb{Q} \setminus \{0\}$ on kommutatiivinen ryhmä, kun ryhmäoperaatioksi valitaan tavallinen kertolasku $\cdot$, neutraalialkioksi 1, ja käänteisalkioksi käänteisluku a^{-1} :

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $a \cdot 1 = 1 \cdot a = a$
- $a \cdot a^{-1} = a^{-1} \cdot a = 1$

Määritelmä

Rengas (ring) $(R, +, \cdot, 0)$ on algebrallinen rakenne, jossa joukossa R on määritelty kaksi binääristä operaatiota $+$ ja $\cdot$ ja alkio 0 , jotka toteuttavat seuraavat ehdot:

- $(R, +, 0)$ on kommutatiivinen ryhmä.
- $(R, \cdot)$ on puoliryhmä.
- $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributiivisuus)
- Jos lisäksi $a \cdot b = b \cdot a$, sanotaan, että rengas R on kommutatiivinen.

Esimerkki

$(\mathbb{Z}, +, \cdot, 0)$ on kommutatiivinen rengas:

- $(\mathbb{Z}, +)$ on kommutatiivinen ryhmä.
- $(\mathbb{Z}, \cdot)$ on kommutatiivinen puoliryhmä (jopa monoidi),

Huomautus

On mahdollista näyttää toteen, että jokaisessa renkaassa $0 \cdot a = 0$.

Määritelmä

Renkaan R alkio a on *nollanjakaja*, jos on olemassa sellainen $b \in R \setminus \{0\}$, että $a \cdot b = 0$.

Rengas R on *kokonaisalue* (*integral domain*), jos renkaassa ei ole muita nollanjakajia kuin itse nolla-alkio 0 .

Esimerkki

Rengas $\mathbb{Z}$ on kokonaisalue, sillä yhtälöstä $ab = 0$ seuraa $a = 0$ tai $b = 0$, siis luku 0 on ainoa nollanjakaja joukossa $\mathbb{Z}$.

Esimerkki

Joukko $\mathbb{Z}_6$ on kommutatiivinen rengas, mutta ei kokonaisalue, sillä $\bar{2} \cdot \bar{3} = \bar{0}$.

Puolirengas

Muutoin kuin rengas, mutta ei vaadita vasta-alkiota yhteenlaskun suhteen

Polynomirengas

Jos R on jokin puolirengas, määritellään

$$R[x] = \{a_0 + a_1x + a_2x^2 + \dots a_nx^n \mid n \in \mathbb{N}, a_i \in R\}$$

Määritelmä

Kunta (Field) $(K, +, \cdot, 0, 1)$ on kommutatiivinen, rengas jossa jokaisella nollasta eroavalla alkiolla a on multiplikatiivinen käänteisalkio a^{-1} joka siis toteuttaa ehdon $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Huomautus

Määritelmän mukaan renkaassa on kaikilla alkioilla vasta-alkio yhteenlaskun suhteen, ja kunnassa lisäksi kaikilla nollasta poikkeavilla alkioilla on käänteisalkion kertolaskun suhteen

Esimerkki

Rationaaliluvut $(\mathbb{Q}, +, \cdot, 0, 1)$ muodostavat kunnan yhteen- ja kertolaskun suhteen, samoin reaalityluvut $(\mathbb{R}, +, \cdot, 0, 1)$.

Määritelmä

Vektoriavaruus on algebrallinen rakenne, jossa alkiojoukko koostuu kahdesta osasta: skalaarikunnasta $\mathbb{K}$ ja avaruudesta V , sekä operaatiosta $\mathbb{K} \times V \rightarrow V$ (skalaarikertolasku) jotka toteuttavat alla olevat aksioomat (merkitään skalaarikertolaskua ilman kertomerkkiä: $a\mathbf{v}$)

- $(V, +, \mathbf{0})$ on kommutatiivinen ryhmä
- $1\mathbf{v} = \mathbf{v}$
- $a(\mathbf{v} + \mathbf{w}) = a\mathbf{v} + a\mathbf{w}$
- $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$
- $a(b\mathbf{v}) = (ab)\mathbf{v}$