Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo
mikhirve@utu.fi

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2026

Algebrallisista rakenteista

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 $\overline{2} \cdot \overline{3} = \overline{0}$.

Puolirengas

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

Polynomirengas

Jos R on jokin puolirengas, määritellään

$$R[x] = \{a_0 + a_1 x + a_2 x^2 + \dots a_n x^n \mid n \in \mathbb{N}, a_i \in R\}$$

Algebrallisista rakenteista

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

Algebrallisista rakenteista

Esimerkki

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

Määritelmä

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

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

Määritelmä

Kunnan $\mathbb{K}$ yli määritelty *algebra* A on vektoriavaruus, jossa muiden rakenteiden lisäksi vektoreille on määritelty kertolasku $\cdot$
$A \times A \to A$, joka on *bilineaarinen*, siis toteuttaa esim. ehdot

- $(a\boldsymbol{u} + b\boldsymbol{v}) \cdot \boldsymbol{w} = a \cdot \boldsymbol{u} \cdot \boldsymbol{w} + b \cdot \boldsymbol{u} \cdot \boldsymbol{w}$
- $\boldsymbol{u} \cdot (a\boldsymbol{w} + b\boldsymbol{w}) = a \cdot \boldsymbol{u} \cdot \boldsymbol{v} + b \cdot \boldsymbol{u} \cdot \boldsymbol{w}$
- $a\boldsymbol{u} \cdot b\boldsymbol{v} = ab \cdot \boldsymbol{u} \cdot \boldsymbol{v}$

(Karteesinen) tulo

Jos A ja B muodostavat algerallisen rakenteen, voidaan joillakin edellytyksillä muodostaa algebrallinen rakenne $A \times B$

Esimerkki

Tapauksessa $A = B = \mathbb{R}$, voidaan määritellä $(a, b) + (c, d) = (a + c, b + d)$ ja $\alpha(a, b) = (\alpha a, \alpha b)$ (Vektoriavaruus).

Algebrallisista rakenteista

Kongruenssi

- Olkoon $\equiv$ ekvivalessirelaatio joukossa A.
- Joukossa A määritelty algebrallinen operaatio $*$ on yhteensopiva relaation $\equiv$ kanssa, mikäli $a \equiv c \wedge b \equiv d \rightarrow a * b \equiv c * d$.
- Jos kaikki algebrallisen rakenteen operaatiot ovat yhteensopivia ekvivalenssirelaation $\equiv$ kanssa, sanotaan että relaatio $\equiv$ on *kongruenssi*.

Esimerkki

Lukuteoreettinen kongruenssi $a \equiv_n b$: $a \equiv_n b \wedge c \equiv_n d \rightarrow a + c \equiv_n b + d$, $ac \equiv_n bd$

Tekijärakenne

Määritelmä

Olkoon A jokin algebrallinen rakenne ja $\equiv$ sen kongruenssi. Tällöin tekijärakenne $A/\equiv$ tarkoittaa algebrallista rakennetta, jonka joukkona ovat ekvivalenssiluokat $[a] = \{x \mid x \equiv A\}$ ja operaatiot $*$ määritellään jokaista A:n operaatiota kohti ehdolla $[a] * [b] = [a * b]$.

Lause

Jos alkuperäisessä rakenteessa A toteutuu jokin operaatioita koskeva aksiooma, niin se toteutuu myös tekijärakenteessa $A/\equiv$.

Merkintä

Mikäli kongurenssin $\equiv$ indusoi jokin A:n alirakenne B, merkitään $A/\equiv$ sijasta A/B ja sanotaan, että A/B on saatu A:sta jakamalla alirakenne B.

Aliryhmä

- Ryhmä $H \subseteq G$ on G:n *aliryhmä*, jos $a, b \in H \rightarrow ab \in H, a^{-1} \in H$.
- Aliryhmä on siis ryhmän osajoukko, joka on suljettu ryhmäoperaatioiden suhteen (ryhmä ryhmän sisällä)
- Aliryhmä $H \subseteq G$ on *normaali*, jos $(\forall g \in G)$ $gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg$
- Aliryhmän normaalius merkitsee sitä, että $(\forall g \in G)(\forall h \in H)(\exists h_1 \in H)\ (gh = h_1 g)$.
- Kommutatiivisessa ryhmässä jokainen aliryhmä on normaali

Lause

Jos H on G:n normaali aliryhmä, niin ehdolla $a \equiv b \Leftrightarrow ab^{-1} \in H$ määritelty relaatio $\equiv$ on kongruenssi ryhmässä G.

Tekijärakenne

Määritelmä

Olkoon G ryhmä ja $H \subseteq G$ normaali aliryhmä.
Kongruenssin $a \equiv b \Leftrightarrow ab^{-1} \in H$ ekvivalenssiluokat muodostavat ryhmän, kun määritellään $[a] \cdot [b] = [a \cdot b]$ ja $[a]^{-1} = [a^{-1}]$. Tätä ryhmää sanotaan *tekijäryhmäksi* ja merkitään G/H.
Tässä tapauksessa merkitään usein myös $[a] = aH$. Tällä merkinnällä $aH \cdot bH = a \cdot bH$. Näitä ekvivalenssiluokkia kutsutaan myös *sivuluokiksi*.

Esimerkki

Lagrangen lause

Tekijärakenne

Määritelmä

Ryhmän G alkion a *kertaluku* $\mathrm{ord}(a)$ on pienin positiivinen luku n, jolle $a^n = 1$. Mikäli tällaista lukua ei ole, sanotaan että $\mathrm{ord}(a) = \infty$.

Lause

Äärellisessä ryhmässä jokaisella alkiolla on kertaluku.

Esimerkki

Syklisen ryhmän aliryhmät, Äärellinen kunta, Fermat'n lause