

Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo
`mikhirve@utu.fi`

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2023

Määritelmä 1

Ryhmä (group) on monoidi, jossa jokaisella alkiolla on käänteisalkio.

Määritelmä 2

Ryhmä on algebrallinen rakenne, johon kuuluu joukko G ja yksi binäärinen joukossa G määritelty operaatio $*$ joka toteuttaa seuraavat aksioomat:

- $(\forall x, y, z \in G) ((x * y) * z = x * (y * z))$ (assosiatiivisuus)
- $(\exists 1 \in G)(\forall x \in G) (x * 1 = 1 * x)$ (neutraalialkion olemassaolo)
- $(\forall x \in G)(\exists y \in G) (x * y = y * x = 1)$ (käänteisalkion olemassaolo).

Jos edellämainittujen ehtojen lisäksi pätee $x * y = y * x$ kaikille $x, y \in G$, sanotaan että G on *kommutatiivinen ryhmä* eli *Abelin ryhmä*.

Huomautus

- Epäkommutatiivisten ryhmien teorialla 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 algebrallinen rakenne, jossa $(K, \cdot, +, 0, 1)$ on kommutatiivinen rengas jossa jokaisella nollasta eroavalla alkiolla a on multiplikatiivinen käänteisalkio a^{-1} joka toteuttaa ehdon $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Huomautus

Määritelmän mukaan renkaassa on kaikilla alkiolla vasta-alkio yhteenlaskun suhteen, ja kunnassa lisäksi kaikilla nollasta poikkeavilla alkiolla 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
- $1\mathbf{v} = \mathbf{v}$
- $a(\mathbf{v} + \mathbf{w}) = a\mathbf{v} + a\mathbf{w}$
- $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$
- $a(b\mathbf{v}) = (ab)\mathbf{v}$

Määritelmä

Kunnan $\mathbb{K}$ yli määritelty *algebra* A on vektoriavaruus, jossa muiden rakenteiden lisäksi vektoreille on määritelty kertolasku $\cdot$

$A \times A \rightarrow A$, joka on *bilineaarinen*, siis toteuttaa esim. ehdot

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

(Karteesinen) tulo

Jos A ja B muodostavat algebrallisen 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).

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

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 $(\forall g \in G)(\forall h \in H)(\exists h_1 \in H) (gh = h_1g)$.
- 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 .

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*.

Määritelmä

- $S \subseteq R$ on renkaan R alirengas, jos $a, b \in S \rightarrow a + b, ab, -a \in S$.
- Alirengas $I \subseteq R$ on renkaan R ihanne (ideal), jos $ri, ir \in I$ aina, kun $r \in R$ ja $i \in I$.
- Renkaan ihanne on siis alirengas joka "vetää" kertolaskulla kaikki renkaan alkiot ihanteeseen.
- Kaikissa renkaissa on ainakin ihanteet $\{0\}$ ja R .

Lause

Jos I on renkaan R ihanne, on ehdolla $a \equiv b \Leftrightarrow a - b \in I$ määrittyvä relaatio on kongruenssi.

Määritelmä

Olkoon $I \subseteq S$ renkaan S ihanne. Kongruenssin $a \equiv b \Leftrightarrow a - b \in I$ ekvivalenssiluokat muodostavat renkaan, kun määritellään $[a] + [b] = [a + b]$, $[a] \cdot [b] = [a \cdot b]$ ja $-[a] = [-a]$. Tätä rengasta sanotaan *tekijärenkaaksi* ja merkitään R/I .

Tällöin merkitään usein myös $[a] = a + I$. Näillä merkinnöillä $(a + I) + (b + I) = (a + b) + I$ sekä $(a + I)(b + I) = ab + I$.

Esimerkki

Olkoon $n \in \mathbb{N}$. Tällöin $n\mathbb{Z} = \{n \cdot m \mid m \in \mathbb{Z}\}$ on renkaan $\mathbb{Z}$ ihanne. Se muodostuu kokonaisluvuista, jotka ovat jaollisia luvulla n . Ihanne $I = n\mathbb{Z}$ määrittää edellämainitun mukaan ekvivalenssirelaation $a \equiv b \Leftrightarrow a - b \in I$, mikä tarkoittaa sitä, että $a - b = nk$ jollekin $k \in \mathbb{Z}$. $a - b = nk$ puolestaan tarkoittaa sitä, että $n \mid a - b$, mistä seuraa edelleen, että $n \mid b - a$. Kyseessä on siis lukuteoreettinen kongruenssi.

Määritelmä

Renkaan R ihanne $I \subsetneq R$ on *maksimaalinen*, jos ei ole suurempaa ihannetta $J \subsetneq R$ johon I sisältyy aidosti, siis $I \subsetneq J$.

Lause

Jokaisessa renkaassa on ainakin yksi maksimaalinen ihanne

Lause

Jos R on multiplikatiivisen ykkösalkion sisältävä kommutatiivinen rengas, on tekijärenkas R/I on kunta tarkalleen silloin kuin I on maksimaalinen ihanne.

Esimerkki

Renkaan $\mathbb{Z}$ ihanne $6\mathbb{Z}$ ei ole maksimaalinen, koska se sisältyy suurempiin ihanteisiin $2\mathbb{Z}$ ja $3\mathbb{Z}$. Nämä molemmat ovat maksimaalisia, samoin kuin $5\mathbb{Z}$.

Esimerkki

- Olkoon $(R, +, \cdot, 0, 1)$ kommutatiivinen kokonaisalue ja määritellään joukossa $R \times R \setminus \{0\}$ kertolasku ja yhteenlasku seuraavasti: $(a, b) \cdot (c, d) = (ac, bd)$ ja $(a, b) + (c, d) = (ad + bc, bd)$
- Määritellään ekvivalenssi joukossa $R \times R \setminus \{0\}$ ehdolla $(a, b) \equiv (c, d) \leftrightarrow ad = bc$. Näin määritelty ekvivalenssi on kongruenssi joukossa $R \times R \setminus \{0\}$ ja ekvivalenssiluokat määrittävät ns. *osamääräkunnan*.

Jos on olemassa myös ykkösalkio 1, on osamääräkunnassa on voimassa $[(a, b)] \cdot [(b, a)] = [(ab, ba)] = [(1, 1)]$, siis jokaisella alkiolla on myös multiplikatiivinen käänteisalkio, koska $ab \equiv ba$.