

Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo
`mikhirve@utu.fi`

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2023

Määritelmä

Algebrallinen rakenne on joukko A , jossa on määritelty äärellinen määrä operaatioita. Operaatiot voivat olla unaarisia, binäärisiä, ternäärisiä, jne. Operaatioiden lisäksi voi olla äärellinen määrä aksioomia.

Esimerkki

$(\mathbb{R}, +, \cdot, 0, 1)$ (kts. Differentiaali- ja integraalilaskenta). Aksioomia: $(\forall a)(\forall b)(a + b = b + a)$, $(\forall a)(\forall b)(\forall c)(a \cdot (b + c) = a \cdot b + a \cdot c)$, jne.

Esimerkki

(Grupoidi eli Magma) Joukko $A = \{\alpha, \beta, \gamma, \delta\}$ ja binäärinen operaatio $*$:

$*$	α	β	γ	δ
α	β	γ	β	δ
β	δ	δ	α	α
γ	α	γ	α	β
δ	β	δ	γ	δ

- $\alpha * \beta = \gamma, \beta * \alpha = \delta,$
- $(\alpha * \beta) * \gamma = \gamma * \gamma = \alpha, \alpha * (\beta * \gamma) = \alpha * \alpha = \beta.$
- Säännöt $x * y = y * x$ ja $x * (y * z) = (x * y) * z$ eivät siis välttämättä päde.
- Ei juurikaan merkitystä teorialle tai sovelluksille.

Puoliryhmä

Puoliryhmä (semigroup) on magma jonka operaatio $*$ toteuttaa aksiooman

$$(\forall x, y, z)((x * y) * z = x * (y * z)).$$

Tämän aksiooman toteuttavaa operaatiota $*$ kutsutaan *assosiatiiviseksi*. Voidaan siis myös sanoa, että puoliryhmä on assosiatiivinen magma.

Esimerkki (Vapaa puoliryhmä)

Olkoon $\Sigma = \{a, b, c\}$, $\Sigma^2 = \{aa, ab, ac, ba, bb, bc, ca, cb, cc\}$,
 $\Sigma^3 = \{aaa, aab, aac, aba, abb, \dots, ccc\}$, jne. ja
 $\Sigma^+ = \Sigma \cup \Sigma^2 \cup \Sigma^3 \cup \dots$

Määritellään operaatio $*$ joukossa Σ^+ seuraavasti: Jos $w_1, w_2 \in \Sigma^+$ ovat n_1 - ja n_2 -pituisia merkkijonoja, niin $w_1 * w_2$ on $n_1 + n_2$ -pituisen merkkijono, joka saadaan kirjoittamalla w_1 ja w_2 peräkkäin. Vapaan puoliryhmän Σ^+ alkioita kutsutaan *sanoiksi* yli aakkoston Σ .

Huomautus

On mahdollista määritellä esimerkiksi $A = \langle \Sigma^+ \mid ab = bc \rangle$, jolloin saadaan puoliryhmä joka ei ole vapaa, vaan toteuttaa ehdon $ab = bc$. Puoliryhmässä A on esimerkiksi
 $\underline{a}ab\underline{b}ca = \underline{a}bc\underline{b}ca = bcc\underline{b}ca = bcc\underline{a}ba$.

Esimerkkejä

- $(abbca * ccab) * abcc = abbcaccab * abcc = abbcaccababcc$
- $abbca * (ccab * abcc) = abbca * ccababcc = abbcaccababcc$
- Puoliryhmiä käytetään mm. merkkijonojen mallintamiseen
- Erittäin suuri merkitys teoreettisessa tietojenkäsittelyopissa.

Huomautus

Puoliryhmien teoriassa jätetään usein operaatiosymboli $*$ merkitsemättä ja kirjoitetaan $w_1 * w_2 = w_1 w_2$. (vrt. kertolaskumerkintä $5 \cdot x = 5x$)

Määritelmä

Puoliryhmän A alkio ϵ on *neutraalialkio* eli *identiteettialkio* eli *ykkösalkio*, jos $\epsilon * w = w * \epsilon$ kaikille $w \in A$.

Huomautus

Puoliryhmän neutraalialkiosta käytetään myös merkintää 1 , ja vapaan puoliryhmän neutraalialkiota kutsutaan *tyhjäksi sanaksi*.

Määritelmä

Monoidi on puoliryhmä, jossa on neutraalialkio 1 .

Määritelmä

Olkoon A monoidi ja $x \in A$. Alkio y on x :n käänteisalkio, jos $xy = yx = 1$. Tällöin merkitään $y = x^{-1}$.

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} :

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