

# Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo  
mikhirve@utu.fi

Matematiikan ja tilastotieteen laitos  
Turun yliopisto

2026

## Joukkojen mahtavuus

- Yhtä mahtavat joukot
- Hilbertin hotelli
- Joukkojen  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$  ja  $\mathbb{R}$  mahtavuudet
- Potenssijoukko

## 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  $\Sigma^+$  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  $\Sigma^+$  alkioita kutsutaan *sanoiksi* yli aakkoston  $\Sigma$ .

## 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  $\underline{aabbca} = \underline{abcbca} = \underline{bccbca} = \underline{bccaba}$ .

## Esimerkkejä

- $(abbca * ccab) * abcc = abbcaccab * abcc = abbcaccababcc$
- $abbca * (ccab * abcc) = abbcabcc = abbcaccababcc$
- 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  $\epsilon$  on *neutraalialkio* eli *identiteettialkio* eli *ykkösalkio*, jos  $\epsilon * w = w * \epsilon = w$  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

Olko  $A$  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*.

## Määritelmä

Monoidi on vasemmalta (oikealta) supistuva, jos  $xy = xz \Rightarrow y = z$  ( $yx = zx \Rightarrow y = z$ ). Monoidi on supistuva jos se on sekä oikealta että vasemmalta supistuva.

## Huomautus

Ryhmä on supistuva monoidi

## Lause

Supistuva monoidi voidaan laajentaa ryhmäksi