Insinöörimatematiikka: Diskreetti matematiikka

Mika Hirvensalo
mikhirve@utu.fi

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2026

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

Diffie-Hellman Protokolla

- One-time Pad
- Diskreetti eksponenttifunktio
- Diskreetti Logaritmi
- Diffie-Hellman protokolla

Tekijärakenne

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.

Tekijärakenne

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.

Tekijärakenne

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 tekijärengas R/I on kunta tarkalleen silloin kuin I on maksimaalinen ihanne.

Tekijärakenne

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 $ab \equiv ba$.

Tekijärakenne

Polynomirenkaan ihanteet

- $\mathbb{R}[x]/\langle x^2+1\rangle$
- $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$