Algebra 1

Kevät 2007

Sisältö

Johdanto

Tämä on ensimmäinen valmiiksi kirjoittamani versio luentomuistiinpanoista, jotka ovat peräisin Jouni Parkkosen luennoimalta Algebra 1 –kurssilta (kevät 2007). Muistiinpanoissa voi olla virheitä, joten kannattaa lukea tekstiä silmät auki.

Toivottavasti monisteesta on apua.

Hauskoja lukuhetkiä,

Riku Ernesti Järvinen

Yleistä

Luennot ja harjoitukset

- Maanantai klo 12 MaD 202, paitsi 22.1 MaD 259
- Tiistai klo 14 MaD 259
- Ensimmäinen harjoitus *jo* 17.1
- Harjoitusten kirjallinen palauttaminen luennoijalle viimeistään tiistaina (MaD 363).

Hyvitykset

Välikokeilla (0-8p) seuraavalla kaavalla:

$$\frac{\text{9xtehdyt}}{\text{kaikki} + 1}$$

Tentillä (0-5p) vastaavalla kaavalla.

Arvostelu ja läpäisy

- Välikokeilla: $2 \cdot 4 \cdot 6p = 48p$
- Tentillä: $5 \cdot 6p = 30p$

Läpäisyyn vaaditaan

Välikokeilla: 24p

Tentillä: 15p

Luku 1

Sisällöstä ja laskutoimituksista

- Laskutoimitukset
- *Ryhmät:* $(G, *)$, missä G on joukko ja $*$ laskutoimitus.
- *Renkaat:* $(R, +, \cdot)$, joille on

$$a(b + c) = ab + ac$$

  $\rightarrow$ *Kunnat* (abstrakti tavara).
- *Lukualueet:* $\mathbb{N} \in \mathbb{Z} \in \mathbb{Q} \in \mathbb{R} \in \mathbb{C}$.

1.1 Laskutoimitukset: esittelyä

Algebra käsittelee laskemista. Osin tämä tarkoittaa ”numeroilla” laskemista lukualueissa $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ laskutoimituksilla $+, \cdot$ ja niiden käänteisillä operaatioilla $-, \div$. Tällä kurssilla tärkeässä osassa on *abstrakti laskeminen*; tällöin ei tiedetä tai välitetä millä lasketaan ja mitä laskutoimitukset ovat, vaan tehdään päätelmiä, kun tunnetaan laskutoimituksen jotain ominaisuuksia.

Jos $A \neq \emptyset$, on A:n laskutoimitus kuvaus $* : A \times A \rightarrow A$. Usein laskutoimituksen tulosta merkitään $a * a'$, siis $*(a, a') = a * a'$. Laskutoimitus on siis sääntö, joka liittää kahteen A:n alkioon (a, a') yhden A:n alkion $a * a'$

Jos $A, B \neq \emptyset$, joukon A *toiminta* joukolla B on kuvaus $t : A \times B \rightarrow B$.

Esimerkki 1.1.1 *1. Luonnollisten lukujen yhteen– ja kertolasku ovat laskutoimituksia:*

$$(n, m) \mapsto n + m$$

$$(n, m) \mapsto n \cdot m$$

2. *Olkoon X joukko. Muodostetaan X:n* potenssijoukko *s.e.*

$$\mathfrak{P}(X) = \{A \in X\}.$$

Potenssijoukko on X:n osajoukkojen joukko. Joukkojen leikkaus ja yhdiste ovat laskutoimituksia potenssijoukossa:

$$(A, B) \to A \cap B$$

$$(A, B) \to A \cup B$$

HUOMAUTUS. $A \in X \Leftrightarrow A \in \mathfrak{P}(X)$ *sekä* $A \cap B, A \cup B \in \mathfrak{P}(X)$.

3. *Olk.* $X \neq \emptyset$ *Olk.* $\mathfrak{F}(X) = \{f : X \to X\}$. *Kuvausten yhdistäminen on laskutoimitus* $\mathfrak{F}(X)$*:ssä:*

$$(f, g) \mapsto f \circ g \in \mathfrak{F}$$

4. *Joukko* $\mathbb{R}$ *toimii vektoriavaruudella* $\mathbb{R}^n$. *Toiminta on*

$$(\lambda, x) \mapsto \lambda x \in \mathbb{R}^n \quad \forall\, \lambda \in \mathbb{R}$$

$$(\lambda(x_1, \ldots, x_n)) \mapsto (\lambda x_1, \ldots, \lambda x_n).$$

Määritelmä 1.1.1 *Joukon A laskutoimitus* $*$ *on*

1. <u>Assosiatiivinen</u>*, jos* $a * (b * c) = (a * b) * c \quad \forall\, a, b, c, \in A$.
2. <u>Kommutatiivinen</u> *(vaihdannainen), jos* $a * b = b * a \quad \forall\, a, b \in A$.

Jos $*$ ja $\oplus$ ovat A:n laskutoimituksia, niin $*$ on distributiivinen $\oplus$:n suhteen jos

$$a * (b \oplus c) = (a * b) \oplus (a * c) \qquad \forall\, a, b, c \in A.$$

Merkintöjä $(+, \cdot)$ käytetään useille eri laskutoimituksille. Kertolaskua merkitään yleensä $(a, b) \mapsto ab$. Merkintää (+) käytetään ainoastaan *kommutatiiviselle* laskutoimitukselle.

Esimerkki 1.1.2 *Luonnollisten lukujen yhteen– ja kertolaskulle pätee*

1. *Assosiatiivisuus:*

$$\begin{cases} m + (n + l) = m + n + l \\ m(nl) = (mn)l \end{cases}$$

2. *kommutatiivisuus:*
$$\begin{cases} m+n = n+m \\ mn = nm \end{cases}$$

3. $m(n+l) = mn + ml$, *mutta* $m + (nl) \neq (m+n)(m+l)$ *(kertolasku ei ole distributiivinen yhteenlaskun suhteen).*

Esimerkki 1.1.3 *X:n potenssijoukossa* $\mathfrak{P}(X)$ *pätee*

$$\begin{cases} A \cap B = B \cap A \\ A \cup B = B \cup A \end{cases} \quad \forall A, B \in \mathfrak{P}(X).$$

Esimerkki 1.1.4 *Kuvausten yhdistäminen on* $\mathfrak{P}(X)$*:ssä assosiatiivinen:*

$$f \circ (g \circ h) = (f \circ g) \circ h \quad \forall\, f, g, h \in \mathfrak{P}(X)$$

Määritelmä 1.1.2 *Olkoon* $A \neq \emptyset$ *mielivaltainen joukko ja* $*$ *A:n laskutoimitus. Alkio* $e \in A$ *on laskutoimituksen* $*$ neutraalialkio, *jos*

$$e * g = g \quad ja \quad g * e = g \quad \forall\, g \in A.$$

Alkio $\overline{x}$ *on alkion* $x \in A$ *vasen käänteisalkio, jos* $\overline{x} * x = e$ *ja oikea käänteisalkio, jos*
$x * \overline{x} = e$*. Jos* $\overline{x}$ *on x:n vasen ja oikea käänteisalkio, se on x:n* käänteisalkio *(laskutoimitukselle* $*$*).*

Jos laskutoimitukselle käytetään tulomerkintää, niin x:n käänteisalkiota merkitään x^{-1}. Summamerkintää käytettäessä merkitään käänteisalkiota $-x$:llä.

Esimerkki 1.1.5 *1. 0 on luonnollisten lukujen yhteenlaskun neutraalialkio, 1 on luonnollisten lukujen kertolaskun neutraalialkio. Toisin sanoen,*

$$0 + n = n \quad \forall\, n \in \mathbb{N} \quad ja \quad 1 \cdot n = n \quad \forall\, n \in \mathbb{N}.$$

Useimmilla luonnollisilla luvuilla ei ole käänteisalkiota kummankaan laskutoimituksen suhteen.

2. *Identtinen kuvaus* $id(x) = id_X; id(x) \mapsto x \quad \forall\, x \in X$ *on joukon* $\mathfrak{F}(x)$ *laskutoimituksen* $\circ$ *neutraalialkio:* $id(x) \circ f = f = f \circ id(x)\ \forall x \in \mathfrak{F}(x)$*. Jos* $f \in \mathfrak{F}(x)$ *on bijektio, niin sillä on käänteiskuvaus* $f^{-1} \in \mathfrak{F}(x)$*. Käänteiskuvaukselle pätee* $f^{-1} \circ f = id$ *ja* $f \circ f^{-1} = id(x)$*, joten se on käänteisalkio laskutoimituksen* $\circ$ *suhteen. Muulla* $g \in \mathfrak{F}(x)$ *ei ole käänteisalkiota.*

3. *Varustamme epätyhjän joukon X potenssijoukon $\mathfrak{P}(x)$ laskutoimituksella $\setminus$ (joukkojen erotus). Tällöin jokaisella $A \in \mathfrak{P}(x)$ pätee $A\setminus\emptyset = A$, joten $\emptyset$ toteuttaa osan neutraalialkiolta vaadittavista ominaisuuksista. Kuitenkin (toisin päin) $\emptyset\setminus A = \emptyset$, joten $\emptyset$ ei ole neutraalialkio. Neutraalialkiota ei ole, koska $\forall\ A \in \mathfrak{P}(x)$ pätee $A\setminus X = \emptyset$.*

Lause 1.1.1 *Olkoon $A \neq \emptyset$ ja olk. $*$ X:n laskutoimitus.*

1. *Jos $e, e' \in X \quad$ s.e. $\quad e * g = g = g * e' \quad \forall\ g \in X$, niin $e = e'$*
2. *Jos $*$ on assosiatiivinen, niin*
   (a) *Alkiolla $g \in X$ on käänteisalkio täsmälleen silloin kun sillä on vasen ja oikea käänteisalkio.*
   (b) *Jos g:llä on käänteisalkio, se on yksikäsitteinen.*
   (c) *Jos g:llä on käänteisalkio, se on g:n ainoa vasen käänteisalkio ja ainoa oikea käänteisalkio.*

Tod.

1. *Harjoitus 2.*
2. (a) *Jätetään väliin.*
   (b) *Olk. g' g:n vasen käänteisalkio ja g'' oikea käänteisalkio (Piilotettu oletus on, että neutraalialkio on olemassa. Tämä seuraa oletuksesta, että on olemassa sekä vasen että oikea käänteisalkio).*
   Nyt $g'' = e * g'' = (g' * g) * g'' \overset{assosiatiivisuus}{=} g' * (g * g'') = g' * e = g'$. Siis $g' = g''$ on g:n käänteisalkio. Toinen suunta todistuksessa suoraan määritelmästä.
   (c) *Seuraa edellisestä.*

□

Tarkastellaan seuraavassa laskutoimitusten määrittelemistä toisten laskutoimitusten avulla: Jos $*$ on A:n laskutoimitus ja $B \subset A,\ B \neq \emptyset$, siten, että $b * b' \in B\ \forall b, b' \in B$, niin $*$ määrittelee *indusoidun* laskutoimituksen

$$(*|_B)$$

joukossa $B : b\ *|_B\ b' = b * b' \quad \forall\ b, b' \in B$. Yleensä indusoitua laskutoimitusta merkitään samalla tavalla kuin laskutoimitusta, joka indusoi sen: $*|_B = *$.

Esimerkki 1.1.6 *Olkoon* $\mathbb{M}_2\mathbb{R}$ *reaalisten* 2×2 *matriisien joukko. Kertolasku määritellään joukossa* $\mathbb{M}_2\mathbb{R}$ *asettamalla*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{21}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b12 + a_{22}b_{22} \end{pmatrix}.$$

Olkoon

$$P = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_2\mathbb{R} \quad | \quad c = 0 \right\} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \quad | \quad a, b, d \in \mathbb{R} \right\}.$$

Kaikille $A, B \in P$ pätee $AB \in P$, joten matriisien kertolasku indusoi laskutoimituksen joukossa P.

Jos $*|_A$ on laskutoimitus joukossa A ja $*|_B$ on laskutoimitus joukossa B, laskutoimitusten $*|_A$ ja $*|_B$ tulo on laskutoimitus joukossa

$$A \times B : \left\{(a, b), (a', b')\right\} \mapsto \left\{(a *|_A a'), (b *|_B b')\right\} \in A \times B.$$

Esimerkki 1.1.7 *Luonnollisten lukujen yhteenlaskun avulla saadaan yhteenlasku ks. joukossa:*

$$\mathbb{N} \times \mathbb{N} : (m, n) + (p, q) = (m + p, n + q)$$

Ennen seuraavaa konstruktiota puhutaan hieman ekvivalenssirelaatiosta.

1.2 Relaatioista

Määritelmä 1.2.1 Relaatio *joukossa A on joukon $A \times A$ osajoukko. Jos $R \subset A \times A$ on relaatio, usein merkitään $(a, b) \in R \Leftrightarrow aRb$. Joukon A relaatio R on*

1. Refleksiivinen, *jos* $aRa \quad \forall\, a \in A$
2. Symmetrinen, *jos* $aRb \Rightarrow bRa \quad \forall\, a, b \in A$
3. Transitiivinen, *jos* $\{aRb \,\&bRc\,\} \Rightarrow aRc \quad \forall\, a, b, c \in A$
4. Antisymmetrinen, *jos* $\{aRb \,\&\, bRa\} \Rightarrow a = b \quad \forall\, a, b \in A.$

Jos relaatio R on refleksiivinen, symmetrinen ja transitiivinen, niin R on ekvivalenssirelaatio. *Ekvivalenssirelaation merkkinä käytetään usein merkkiä $\sim$ eli $a \sim b$. Jos $\sim$ on ekvivalenssirelaatio, niin jokainen joukon A alkio a määrää* ekvivalenssiluokan

$$[a] = \{b \in A : a \sim b\}.$$

Ekvivalenssiluokkien joukkoa merkitään $A/\sim$ ja sitä kutsutaan ekvivalenssirelaatiota $\sim$ vastaavaksi tekijäjoukoksi. *Jos relaatio on refleksiivinen, antisymmetrinen ja transitiivinen, se on osittainen järjestys.*

Määritelmä 1.2.2 *Jos $*$ on laskutoimitus ja $\sim$ on ekvivalenssirelaatio joukossa A, ne ovat* yhteensopivat, *jos*

$$(a * b) \sim (a' * b')$$

aina kun

$$a \sim a', b \sim b'.$$

Laskutoimitus $*$ määrää tekijälaskutoimituksen $*$ *joukossa $A/\sim$ säännöllä*

$$[a] * [b] = [a * b].$$

Esimerkki 1.2.1 *Olkoon relaatio $\equiv$ kokonaislukujen joukossa $\mathbb{Z}$ määritelty säännöllä*

$$a \equiv b \Leftrightarrow \exists\, k \in \mathbb{Z} \;\; s.e. \;\; b = a + 3k.$$

Relaatio $\equiv$ on ekvivalenssirelaatio, jota sanotaan kongruenssirelaatioksi, *sillä se on yhteensopiva kokonaislukujen yhteenlaskun kanssa. Jos $a' = a + 3m$ ja $b' = b + 3n$ jollain $m, n \in \mathbb{Z}$, niin $a' + b' = a + 3m + b + 3n = a + b + 3(m + n)$, joten $a \equiv a'$ ja $b \equiv b' \Rightarrow a + b = a' + b'$. Siis kokonaislukujen yhteenlasku määrittelee laskutoimituksen kolmen alkion joukolla*

$$\mathbb{Z}/_{\equiv} : \{[0], \quad [1], \quad [2]\}.$$

Esimerkiksi käy vaikkapa

$$[2] + [2] = [4] = [1].$$

Lemma 1.2.1 *1. Jos $*$ on assosiatiivinen, niin sen tekijälaskutoimitus on assosiatiivinen.*

2. Jos $*$ on kommutatiivinen, niin sen tekijälaskutoimitus on kommutatiivinen.

Tod. Suoralla laskulla.

□

1.3 Perusmääritelmät kuvauksille, esimerkkejä

Määritelmä 1.3.1 *Olkoon E ja E' joukkoja, joiden laskutoimitusta merkitään kertolaskulla. Kuvaus $h : E \mapsto E'$ on homomorfismi, jos*

$$h(ab) = h(a)h(b) \quad \forall\, a, b \in E.$$

Bijektiivinen homomorfismi on isomorfismi. *Isomorfismi $h : E \mapsto E$ on* automorfismi.

Esimerkki 1.3.1 *1. Olkoon $*$ ja $\sim$ laskutoimitus ja ekvivalenssirelaatio joukossa E. Jos ne ovat yhteensopivia, niin luonnollinen kuvaus*

$$a \mapsto [a], \quad a \in E, \quad [a] \in E/_\sim$$

on surjektiivinen homomorfismi.

Tod.

Olk. $\phi : E \mapsto E/_\sim$ luonnollinen kuvaus. Surjektiivisuuden osaat todistaa. Homomorfisuus:

$$\phi(a) * \phi(b) = [a] * [b] = [a * b] = \phi(a * b) \quad \forall\, a, b, \in E.$$

□

2. Kuvaus

$$h : \mathbb{Z} \to \mathbb{M}_2\mathbb{R}, \quad h(k) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

on homomorfismi, kun $\mathbb{Z}$ varustetaan yhteenlaskulla ja $\mathbb{M}_2\mathbb{R}$ kertolaskulla:

$$h(m)h(n) = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m+n \\ 0 & 1 \end{pmatrix} = h(m+n).$$

Luku 2

Kokonaisluvut ja rationaaliluvut

2.1 Kokonaisluvut

Tarkastellaan kokonaislukujen ja rationaalilukujen konstruktiota luonnollisista luvuista lähtien. Oletamme, että luonnolliset luvut ja niiden laskutoimitukset (yhteen– ja kertolasku) ovat tunnettuja: Oikeasti hommat hoidetaan suurin piirtein seuraavalla tavalla:

$\mathbb{N} : \sigma : \mathbb{N} \to \mathbb{N}, \quad 0 \in \mathbb{N}, \quad \sigma(0) \neq 0, \quad \sigma : \mathbb{N} \to \mathbb{N} \backslash 0 \quad S \in \mathbb{N}, \quad 0 \in S, n \in S \Rightarrow \sigma(n) \in S \Rightarrow S = \mathbb{N}.$

Tällä kurssilla luonnollisten lukujen joukko on

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

Kurssin aikana konstruoimme muut lukualueet ketjussa

$$\mathbb{N} \in \mathbb{Z} \in \mathbb{Q} \in \mathbb{R} \in \mathbb{C}$$

asteittain laajentamalla siitä, mitä olemme konstruoineet aiemmin. Samalla tarkastelemme, miten lukualueiden algebralliset ominaisuudet eroavat toisistaan.

Luonnollisten lukujen yhteen– ja kertolaskun neutraalialkiot ovat 0 ja 1. Useimmilla luonnollisilla luvuilla ei ole käänteisalkiota kummankaan laskutoimituksen suhteen (ainoat poikkeukset ovat 0 ja 1, joille 0 on oma yhteenlaskun käänteisalkionsa ja 1 on oma kertolaskun käänteisalkionsa). Laajennamme luonnolliset luvut kokonaisluvuksi s.e. uudessa struktuurissa kaikilla alkioilla on käänteisalkio yhteenlaskun suhteen.

Määrittelemme kokonaisluvut ”luonnollisten lukujen muodollisena erotuksena:” Jos $m, n \in \mathbb{N}$ ja $m \geqslant n$, niin erotus $m - n$ on olemassa luonnolli-

sena lukuna, sillä se on yhtälön $n + p = m$ ratkaisu. Toisaalta, sama luonnollinen luku voidaan esittää erotuksina äärettömän monella eri tavalla:

$$(m + k) - (n + k) = m - n \quad \forall\, k \in \mathbb{N}.$$

Näiden havaintojen opastamana määritellään joukkoon $\mathbb{N} \times \mathbb{N}$ relaatio[1]

$$(m, n) \sim (p, q) \Leftrightarrow m + q = p + n.$$

Kokonaislukujen joukko on

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/_{\sim}.$$

Kokonaislukujen yhteenlasku on *luonnollisten lukujen yhteenlaskun tulon*

$$(m, n) + (p, q) = (m + p, n + q) \quad \forall\, m, n, p, q \in \mathbb{N} \tag{2.1}$$

indusoima laskutoimitus, ja kertolasku on laskutoimituksen

$$(m, n)(p, q) = (mp + nq, mq + np) \tag{2.2}$$

indusoima laskutoimitus.

HUOMAUTUS.

1. Määritelmät ovat järkeviä, sillä kun $m \geqslant n,\ p \geqslant q$, pareja (m, n) ja (p, q) voidaan ajatella luonnollisten lukujen erotuksina, jolloin pätee

   $$(m - n)(p - q) = mp + nq - mq - np.$$

2. Kokonaislukujen laskutoimitukset ovat hyvin määriteltyjä: joukkoon $\mathbb{N} \times \mathbb{N}$ määritellyt laskutoimitukset ovat yhteensopivia relaation (ekvivalenssi) $\sim$ kanssa:

   Tod. (yhteenlasku)

   Jos on
   $$(m, n) \sim (m', n'), \quad (p, q) \sim (p', q'),$$
   niin pätee
   $$m + n' = m' + n \quad \text{ja} \quad p + q' = p' + q.$$
   Siispä
   $$m + p + n' + q' = m' + p' + n + q$$

[1] $\sim$ on ekvivalenssirelaatio, ks. harjoitus 2.

eli

$$\underbrace{(m+p, n+q)}_{(m,n)+(p,q)} \sim \underbrace{(m'+p', n'+q')}_{(m',n')+(p',q')}.$$

Kertolaskun todistus harjoituksissa 2.

□

Propositio 2.1.1 *1. Kokonaislukujen yhteenlasku ja kertolasku ovat assosiatiivisia ja kommutatiivisia.*

2. *Kertolasku on distributiivinen yhteenlaskun suhteen.*

3. *Yhteenlaskun neutraalialkio on* $[(0,0)]$ *ja kertolaskun neutraalialkio on* $[(1,0)]$.

4. *Jokaisella alkiolla* $[(m,n)] \in \mathbb{Z}$ *on käänteisalkio yhteenlaskun suhteen:*

$$[(m,n)] + [(n,m)] = [(0,0)].$$

Tod.

1. *Seuraa yhtälöistä 2.1 ja 2.2 ja lemmasta 1.2.1.*

2. *Distributiivisuus: Koska laskutoimitukset ovat kommutatiivisia, riittää tarkastella distributiivisuutta vasemmalta. Olkoot*

$$a = [(m,n)],\ b = [(p,q)],\ c = [(r,s)];\ a,b,c \in \mathbb{Z}.$$

Teemme laskuja joukossa $\mathbb{N} \times \mathbb{N}$:

$$\begin{aligned} a(b+c) &= (m,n) * ((p,q) + (r,s)) \\ &= (m,n) * (p+r, q+s) \\ &= (m(p+r) + n(q+s), m(q+s) + n(p+r)) \end{aligned}$$

Toisaalta on

$$\begin{aligned} ab + ac &= (mp+nq, mq+np) + (mr+ns, ms+nr) \\ &= (m(p+r) + n(q+s), m(q+s) + n(p+r)). \end{aligned}$$

3. *Joukossa* $\mathbb{N} \times \mathbb{N}$ *on:*

$$(m,n) + (0,0) = (m,n) \text{ ja } (m,n)(1,0) = (m,n).$$

4. *Vastaavanlainen lasku kuin edellä.*

□

Proposition 2.1.1 perusteella voimme siis merkitä luvun $a = [(m,n)] \in \mathbb{Z}$ vastalukua $[(n,m)]$ $-a$:lla. Haluamme, että $\mathbb{Z}$ laajentaa $\mathbb{N}$:n; siis $\mathbb{N}$:n tulisi olla $\mathbb{Z}$:n osajoukko. Kuitenkin $\mathbb{Z}$ on määritelty joukon $\mathbb{N} \times \mathbb{N}$ abstraktina tekijäjoukkona. Siispä samastamme $\mathbb{N}$:n sopivan kokonaislukujoukon kanssa.

Propositio 2.1.2 *Kuvaus* $i : \mathbb{N} \mapsto \mathbb{Z}$, $i(n) = [(n,0)]$ *on* injektiivinen homomorfismi *yhteenlaskulle ja kertolaskulle:* $\forall\ m,n \in \mathbb{N}$ *pätee*

$$i(m+n) = i(m) + i(n) \ \ ja \ \ i(mn) = i(m)i(n).$$

Lisäksi jokainen kokonaisluku on muotoa $i(n)$ *tai* $-i(n)$ *jollekin* $n \in \mathbb{N}$.
Tod. Harjoitus 3.

□

Proposition 2.1.2 mukaan kuvaus i säilyttää yhteenlaskun, eli ei ole merkitystä, lasketaanko luvut m ja n yhteen vai kerrotaanko ne luonnollisina lukuina vai vastaavina kokonaislukuina.

Sopimus 1 *Tästä eteenpäin samastamme luonnolliset luvut vastaavan kokonaislukujen osajoukon kanssa.*

Nyt voimme määritellä uuden laskutoimituksen, *vähennyslaskun* kokonaislukujen joukossa asettamalla $m - n = m + (-n)$. Kertolaskun suhteen käänteisalkio on ainoastaan luvuilla 1 ja -1.

2.2 Rationaaliluvut

Rationaaliluvut muodostetaan vastaavalla tavalla kokonaislukujen muodollisten osamäärien avulla: määrittelemme ekvivalenssirelaation $\sim$ joukossa $\mathbb{Z} \times \mathbb{Z}^*$ (missä $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$) asettamalla

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

Rationaalilukujen joukko on

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* / \sim .$$

Merkitsemme parin (p, q) ekvivalenssiluokkaa p/q:lla. Rationaalilukujen *yhteenlasku* on laskutoimituksen

$$(a, b) \oplus (c, d) = (ad + bc, bd)$$

indusoima laskutoimitus, ja rationaalilukujen *kertolasku* on kokonaislukujen kertolaskun tulon

$$(a, b)(c, d) = (ac, bd)$$

indusoima laskutoimitus.

Konstruktio säilyttää kaikki kokonaislukujen ”hyvät” ominaisuudet ja lisäksi saadaan kertolaskulle käänteisalkioita:

Propositio 2.2.1 *1. Rationaalilukujen yhteenlasku ja kertolasku ovat assosiatiivisia ja kommutatiivisia.*

2. *Kertolasku on distributiivinen yhteenlaskun suhteen.*

3. *Yhteenlaskun neutraalialkio on* $0/1$ *ja kertolaskun neutraalialkio on* $1/1$.

4. *Jokaisella* $m/n \in \mathbb{Q}$ *on käänteisalkio yhteenlaskun suhteen:*

$$\frac{m}{n} + \left(-\frac{m}{n}\right) = \frac{0}{1}.$$

5. *Jokaisella* $m/n \in \mathbb{Q} \setminus \{0/1\}$ *on käänteisalkio kertolaskun suhteen:*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \frac{1}{1}$$

Tod. HT.

□

Propositio 2.2.2 *Kuvaus* $j : \mathbb{N} \mapsto \mathbb{Z}, \quad j(n) = n/1$ *on* injektiivinen homomorfismi *yhteenlaskulle ja kertolaskulle, eli pätee*

$$j(m + n) = j(m) + j(n) \;\; ja \;\; j(mn) = j(m)j(n).$$

Tod. kuten propositio 2.1.2.

□

Sopimus 2 *Tästä eteenpäin samastamme kokonaisluvut vastaavan rationaalilukujen osajoukon kanssa.*

Nyt voimme määritellä vähennyslaskun rationaaliluvuille asettamalla

$$\alpha - \beta = \alpha + (-\beta) \quad \forall\, \alpha, \beta \in \mathbb{Q},$$

missä $-\beta$ on rationaaliluvun β käänteisalkio yhteenlaskun suhteen. Edelleen voimme määritellä uuden laskutoimituksen, *jakolaskun,* joukossa

$$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$$

asettamalla

$$\frac{\alpha}{\beta} = \alpha\beta^{-1},$$

missä β^{-1} on rationaaliluvun $\beta \neq 0$ käänteisalkio kertolaskun suhteen.

Luku 3

Ryhmät

3.1 Määritelmä ja esimerkkejä

Tässä luvussa tarkastellaan pareja, jotka muodostuvat joukosta ja siinä määritellystä laskutoimituksesta. Laskutoimitukselta vaaditaan muutama yksinkertainen ominaisuus:

Määritelmä 3.1.1 *Olkoon G joukko, jossa on määritelty laskutoimitus. Joukko G varustettuna tällä laskutoimituksella on* ryhmä, *jos*

1. *Laskutoimitus on assosiatiivinen.*
2. *Laskutoimituksella on neutraalialkio.*
3. *Jokaisella joukon G alkiolla on käänteisalkio laskutoimituksen suhteen.*

Jos laskutoimituksena on $*$, käytetään merkintää $(G, *)$ ja sanotaan, että $(G, *)$ on ryhmä.

Esimerkki 3.1.1 *1. Aiemmista esimerkeistämme ryhmiä ovat (ainakin)*

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{Q}^*, \cdot), \quad (\mathbb{Z}_p, +).$$

Näistä $\mathbb{Z}_p$, $p \in \mathbb{Z}$ on kongruenssia $\equiv$, $a \equiv b \Leftrightarrow b = a + kp$ jollakin $k \in \mathbb{Z}$ vastaava $\mathbb{Z}$:n tekijäjoukko: $\mathbb{Z}_p = \mathbb{Z}/_{\equiv}$. Laskutoimitus on kokonaislukujen yhteenlaskua vastaava tekijälaskutoimitus: esimerkiksi

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\} : [1] + [3] = [1 + 3] = [4] = [0].$$

Tod.

(a) *Kokonaislukujen yhteenlasku on assosiatiivinen* $\Rightarrow$ $\mathbb{Z}_p$*:n yhteenlasku on assosiatiivinen.*

(b) $0 \in \mathbb{Z}$ *on yhteenlaskun neutraalialkio* $\Rightarrow [0]$ *on* $\mathbb{Z}_p$*:n neutraalialkio.*

(c) *Alkion* $[k] \in \mathbb{Z}_p$ *käänteisalkio on* $[-k]$*:*

$$[k] + [-k] = [k - k] = [0] = [-k] + [k].$$

□

2. *Olkoon* $\mathbb{M}_n\mathbb{Z}$ *vast.* $\mathbb{M}_n\mathbb{R}$ *sellaisten* $n \times n$*-matriisien joukkoja, joiden kaikki kertoimet ovat kokonaislukuja vast. reaalilukuja. Harjoituksissa 2 osoitettiin, että* $\mathbb{R}$*-kertoiminen erityinen lineaarinen ryhmä*

$$SL_2\mathbb{R} = \{A \in \mathbb{M}_2\mathbb{R} \mid det(A) = 1\}$$

on ryhmä, kun laskutoimituksena on matriisien kertolasku. Vastaavasti

$$SL_n\mathbb{R} = \{A \in \mathbb{M}_n\mathbb{R} \mid det(A) = 1\}$$

ovat ryhmiä, samoin $\mathbb{R}$*-kertoiminen yleinen lineaarinen ryhmä*

$$GL_n\mathbb{R} = \{A \in \mathbb{M}_n\mathbb{R} \mid det(A) \neq 0\},$$

samoin vastaavalla tavalla määritellyt $GL_n\mathbb{Q}$ *ja* $GL_n\mathbb{C}$*, mutta* EI $\mathbb{Z}$*-kertoimisten matriisien vastaava joukko.*

3.2 Ryhmän perusominaisuuksia

Propositio 3.2.1 *Olkoon G ryhmä. Olkoon* $e \in G$ *neutraalialkio. Tällöin*

1. *Neutraalialkio on yksikäsitteinen.*
2. *Jokaisen alkion käänteisalkio on yksikäsitteinen.*
3. *Jos* $\overline{a}a = e$*, niin* $\overline{a} = a^{-1} \quad \forall a \in G$*.*
4. $(a^{-1})^{-1} = a \quad \forall a \in G$*.*
5. *Supistussäännöt pätevät* $\forall\ a, b, c, \in G$*:*
   (a) $ab = ac \Rightarrow b = c$*.*

(b) $ab = cb \Rightarrow a = c$.

6. $(ab)^{-1} = b^{-1}a^{-1}$.

7. *Jokaisella yhtälöllä* $ax = b$ *ja* $ya = b$ *on ratkaisu G:ssä.*

Todistukset: Todistamme vain kohdan (6).

Tod. (6)

$(b^{-1}a^{-1})(ab) \overset{\text{assosiatiivisuus}}{=} b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$. *Toinen järjestys vastaavasti.*

□

HUOMAUTUS. Jos A on joukko, jossa on assosiatiivinen laskutoimitus ja tällä laskutoimituksella neutraalialkio, niin A on ryhmä, jos ja vain jos yhtälöillä

$$\begin{cases} ax &= b \\ ya &= b \end{cases}$$

on ratkaisut $\forall\, a, b \in A$ (Vrt. Propositio 3.2.1).

Supistussäännöt kohdassa 5 pätevät monessa muussakin rakenteessa kuin ryhmässä, esim. $\mathbb{N}$:ssä, $(\mathbb{N}, +)$:ssä, $(\mathbb{N}, \cdot)$:ssä, ...

Määritelmä 3.2.1 *(Potenssit) Olkoon A joukko, jossa on assosiatiivinen laskutoimitus (jota merkitään kertolaskulla). Nyt määritellään alkion $a \in A$ n:s potenssi, $n \in \mathbb{N}\setminus\{0\}$ asettamalla*

$$a^1 = a,\ a^{n+1} = a \cdot a^n\ \forall\, n \geqslant 1.$$

Jos A:ssa on neutraalialkio e, määritellään $a^0 = e$. Jos A:ssa on käänteisalkio, määritellään a:n -1:s potenssi a^{-1}, jolloin kyseinen alkio on a:n käänteisalkio. Jos $n \in \mathbb{Z},\ n \leqslant -2$, määritellään

$$a^n = (a^{-1})^{-n} \quad (-n \geqslant 2).$$

Jos laskutoimitusta merkitään yhteenlaskulla, määritellään alkion *a monikerrat* samaan tapaan:

$$\begin{aligned} 2a &= a + a,\ 3a = a + 2a \text{ jne.} \\ -a &= a\text{:n käänteisalkio} \\ -2a &= 2(-a) \text{ jne.} \end{aligned}$$

Potensseille ja monikerroille pätevät tavanomaiset laskusäännöt:

1. $(a^m)^n = a^{mn}$
2. $a^m a^n = a^{m+n}$
3. $mb + nb = (m+n)b$.

Luvussa 2 käsitellyt konstruktiot antavat mahdollisuuden tehdä uusia ryhmiä:

Propositio 3.2.2 *Olkoon G_1 ja G_2 ryhmiä. Tällöin niiden tulo on ryhmä: Jos $e_1 \in G_1$ ja $e_2 \in G_2$ ovat ryhmien G_1 ja G_2 neutraalialkiot, niin $(e_1, e_2) \in G_1 \times G_2$ on $G_1 \times G_2$:n neutraalialkio. Alkion $(g_1, g_2) \in G_1 \times G_2$ käänteisalkio on (g_1^{-1}, g_2^{-1}).*

□

Esimerkki 3.2.1 *Joukot $\mathbb{R}^n$ ja $\mathbb{Z}^n$ varustettuna yhteenlaskulla (komponenteittain yhteenlasku) ovat ryhmiä.*

Olkoon G ryhmä ja olkoon $\sim$ sen laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Luvun 2 määritelmän 1.2.2 avulla saamme tekijäjoukon $G/\sim$ laskutoimituksen, jota sanotaan *tekijälaskutoimitukseksi*.

Propositio 3.2.3 *Olkoon G ryhmä ja $\sim$ sen laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Tällöin $G/\sim$ varustettuna tekijälaskutoimituksella on ryhmä.*

Tod. (ryhmäominaisuudet)

1. *On aiemmin todistettu, että tekijälaskutoimitus on assosiatiivinen.*
2. *Olkoon nyt $e \in G$ neutraalialkio, $[a] \in G/\sim$.*

$$\begin{cases} [e][a] &= [ea] &= [a] \\ [a][e] &= [ae] &= [a]. \end{cases}$$

   Siispä $[e]$ on $G/\sim$:n neutraalialkio.

3. *Olkoon $[a] \in G/\sim$. Koska G on ryhmä, a:lla on käänteisalkio a^{-1}. Tällöin*

$$\begin{cases} [a][a^{-1}] &= [aa^{-1}] &= [e] \\ [a^{-1}][a] &= [a^{-1}a] &= [e], \end{cases}$$

   Nyt siis pätee $[a^{-1}] = [a]^{-1}$.

□

Ryhmää $G/\sim$ kutsutaan ekvivalenssirelaatiota $\sim$ vastaavaksi G:n *tekijäryhmäksi.*

HUOMAUTUS. Aiemmin käsitelty $\mathbb{Z}_p$ on kongruenssia $\equiv$,

$$a \equiv b \Leftrightarrow b = a + kp \quad \text{jollain } k \in \mathbb{Z}$$

vastaava kokonaislukujen ryhmän tekijäryhmä.

Osajoukolle indusoituva laskutoimitus antaa joskus (mutta ei aina!) ryhmiä. Tarkastellaan tätä lähemmin luvussa 5, seuraavassa esimakua.

3.3 Ryhmät ja kuvaukset

Esimerkki 3.3.1 *Olkoon $X \neq \emptyset$. Joukkoa $S(X)$, joka koostuu kaikista bijektioista joukolta X itselleen kutsutaan* permutaatioryhmäksi, *kun laskutoimituksena on kuvausten yhdistäminen. Monet permutaatioryhmän osajoukot, jotka määritellään*

$$\{f \in S(X) \mid \textit{funktiolla } f \textit{ on jokin ominaisuus}\}$$

ovat ryhmiä, kun ne varustetaan indusoidulla laskutoimituksella (laskutoimituksena on kuvausten yhdistäminen).

ESIMERKKI.

Olkoon

$$X = \mathbb{R}^n,\ n \in \mathbb{N},\ n \geqslant 1.$$

Kuvaus $L : \mathbb{R}^n \mapsto \mathbb{R}^n$ on lineaarikuvaus, jos

$$L(x+y) = L(x) + L(y) \quad ja \quad L(ax) = aL(x) \quad \forall\, x, y \in \mathbb{R}^n,\ a \in \mathbb{R}.$$

Lineaariset bijektiot vektoriavaruudelta $\mathbb{R}^n$ itselleen muodostavat ryhmän, kun laskutoimituksena käytetään kuvausten yhdistämistä.

Tod.

1. *Laskutoimituksen assosiatiivisuus seuraa siitä, että $S(\mathbb{R}^n)$:n laskutoimitus on assosiatiivinen ja tarkasteltava joukko on $S(\mathbb{R}^n)$:n osajoukko ja laskutoimitus on vastaava indusoitu laskutoimitus.*

2. *Identtinen kuvaus on lineaarinen, joten neutraalialkio on.*

3. *Lineaarisen bijektion käänteiskuvaus on lineaarinen bijektio, käänteiskuvaus on käänteisalkio.*

Lineaariset bijektiot $\mathbb{R}^n$:ltä itselleen muodostavat $S(\mathbb{R}^n)$:n aliryhmän.

Määritelmä 3.3.1 *Ryhmä on* kommutatiivinen*, jos sen laskutoimitus on sitä. Ryhmä G on* äärellinen*, jos joukko G on äärellinen. Jos G ei ole äärellinen, niin se on ääretön.*

Esimerkki 3.3.2 1. *Ryhmät $(\mathbb{Z},+)$, $(\mathbb{Z}_p,+)$, $(\mathbb{Z}^n,+)$ ovat kommutatiivisia.*

2. *Ryhmät $(\mathbb{Z}_p,+)$, $(\mathbb{Z}_p\times\mathbb{Z}_q,+)$ ovat äärellisiä. Samoin ryhmä K, joka muodostuu kuvauksista*

$$id, f, g, h : \mathbb{R}^* \to \mathbb{R}^*; \quad f(x) = -x, \quad g(x) = 1/x, \quad h(x) = -1/x,$$

ja jonka laskutoimitus on kuvausten yhdistäminen.

Nyt

$$f\circ f = id = g\circ g = id = h\circ h,$$
$$f\circ g = h = g\circ f,\ h\circ g = f\circ g\circ g = f = g\circ h,\ h\circ f = g = f\circ h.$$

Siispä

$$f = f^{-1},\ g = g^{-1},\ h = h^{-1}.$$

Laskuista seuraa, että indusoitu laskutoimitus on olemassa, koska kaikki laskutoimitukset, jotka tehdään permutaatioryhmässä $S(\mathbb{R}^*)$ antavat tuloksena joukon K alkion. Koska $id \in K$ ja kaikilla K:n alkioilla on käänteiskuvaus, K on ryhmä, Kleinin neliryhmä. Ryhmä K on isomorfinen *ryhmän $(\mathbb{Z}_2\times\mathbb{Z}_2,+)$ kanssa. Ryhmässä $(\mathbb{Z}_2\times\mathbb{Z}_2)$ on neljä alkiota:*

$$([0],[0]),\ ([0],[1]),\ ([1],[0]),\ ([1],[1]).$$

Kuvaus $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to K$,

$$\begin{aligned}([0],[0]) &\mapsto id\\ ([0],[1]) &\mapsto f\\ ([1],[0]) &\mapsto g\\ ([1],[1]) &\mapsto h\end{aligned}$$

on injektio. Onko ϕ *homomorfismi? Lasketaan:*

$$\phi : (([0],[1]) + ([0],[1])) = \phi([0],[0]) = id = f \circ f = \phi(([0],[1])) \circ \phi(([0],[1]))$$

Vastaavasti käy $([1],[0])$*:lle ja* $([1],[1])$*:lle:*

$$\phi(([0],[1]) + ([1],[0])) = \phi([1],[1]) = h = f \circ g = \phi([0],[1]) \circ \phi([1],[0]).$$

jne... OK. Siis ϕ *on* isomorfismi.

Jos G ja G' ovat ryhmiä, niin homomorfismia $\phi : G \to G'$ kutsutaan *ryhmähomomorfismiksi*.

Propositio 3.3.1 *Ryhmähomomorfismi* $\phi : G \to G'$ *kuvaa ryhmän* G *neutraalialkion ryhmän* G' *neutraalialkioksi, ja jokaiselle* $g \in G$ *pätee*

$$\phi(g)^{-1} = \phi(g^{-1}).$$

Tod.

Neutraalialkio todetaan harjoituksissa: Olk. $g \in G$*. Tällöin*

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e).$$

Ensimmäinen väite sanoo, että $\phi(e)$ *on* G'*:n neutraalialkio, joten*

$$\phi(g)^{-1} = \phi(g^{-1}).$$

Käänteisalkio tarvitsee tarkastaa vain toiselta puolelta (miksi?).

□

HUOMAUTUS. Isomorfismin *eli bijektiivisen homomorfismin käänteiskuvaus on myös isomorfismi. Jos* G *ja* G' *ovat ryhmiä ja on isomorfismi* $\phi : G \to G'$*, niin* G *ja* G' *ovat isomorfisia.*

Esimerkki 3.3.3 *1. Olkoon* $\mathbb{R}_+ =]0, \infty[$. *Varustetaan* $\mathbb{R}_+$ *kertolaskulla ja* $\mathbb{R}$ *yhteenlaskulla. Tällöin* $(\mathbb{R}_+, \cdot)$ *ja* $(\mathbb{R}, +)$ *ovat ryhmiä ja logaritmikuvaus* $\log : \mathbb{R}_+ \to \mathbb{R}$ *on isomorfismi:*

$$\log xy = \log x + \log y \quad \forall\, x, y \in \mathbb{R}_+.$$

Lisäksi log *on bijektio. Logaritmin käänteisfunktiolle, eksponenttifunktiolle pätee*

$$exp(x + y) = e^{x+y} = e^x e^y = exp(x)exp(y).$$

2. *Vektoriavaruuden* $\mathbb{R}^n$ *bijektiivisten lineaarikuvausten ryhmä (esim. 4.1.1 (2)) on isomorfinen ryhmän* $GL_n\mathbb{R}$ *kanssa: Olkoon*

$$K = \{v_1, v_2, \ldots, v_n\}$$

$\mathbb{R}^n$*:n kanta, ja olkoon* $(Lv_1)_K$ *vektorin* $Lv_1 \in \mathbb{R}^n$ *koordinaattivektori kannan K suhteen, kun* $L : \mathbb{R}^n \to \mathbb{R}^n$ *on lineaarinen bijektio. Lineaarialgebran kurssilla osoitetaan, että kuvaus*

$$L \mapsto ((Lv_1)_K, (Lv_2)_K, \ldots, (Lv_n)_K)$$

on isomorfismi (eli lineaarikuvausten yhdistäminen vastaa matriisien kertolaskua).

3. *Olkoon G ryhmä, ja olk.* $a \in G$. *Kuvaus*

$$\phi_a : G \to G, \quad \phi_a(g) = aga^{-1}$$

on ryhmän G automorfismi *eli isomorfismi ryhmältä G itselleen.*

Tod. (3)

ϕ_a *on homomorfismi:*

$$\phi_a(gg') = agg'a^{-1} = (aga^{-1})(ag'a^{-1}) = \phi_a(g)\phi_a(g').$$

Kuvaus on myös bijektio, sen käänteiskuvaus on $\phi_a^{-1}(g) = a^{-1}ga$. *Kuvaus* ϕ_a *on ryhmän sisäinen automorfismi.*

□

ESIMERKKI.

Ryhmässä $SL_2\mathbb{Z}$ *(ks. Esimerkki. 4.1.1 (2)):*

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2\mathbb{Z}.$$

Matriisia A vastaa $SL_2\mathbb{Z}$:n sisäinen automorfismi

$$\phi_A : \phi_A(B) = ABA^{-1}.$$

Nyt

$$A^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

jos

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

niin

$$\phi_A(B) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \ldots = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

Esimerkiksi

$$\phi_A \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}.$$

4. *Äärellisiä (pienehköjä) ryhmiä voi tarkastella myös laskutaulujen (usein kutsutaan kertotauluiksi) avulla: muodostetaan ryhmän alkioilla indeksoitu taulukko, jonka paikassa (g, h) on alkio gh.*

   ESIMERKKI. Neljän alkion ryhmien $(\mathbb{Z}_4, +)$, $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ ja K laskutaulut ovat kuten yllä (taulukoissa ekvivalenssiluokkaa $[k]$ merkitään k:lla).

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(K, \circ)$	id	f	g	h
id	id	f	g	h
f	f	id	h	g
g	g	h	id	f
h	h	g	f	id

$(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

   - *Ryhmän laskutauluissa jokaisella rivillä ja jokaisessa sarakkeessa esiintyy jokainen ryhmän alkio (miksi?).*

Luku 4

Aliryhmät

4.1 Määritelmä ja esimerkkejä

Määritelmä 4.1.1 *Olkoon G ryhmä. Olk. $\emptyset \neq B \subset G$. Jos B varustettuna indusoidulla laskutoimituksella on ryhmä, se on ryhmän G* aliryhmä. *Jos $H \subset G$ on G:n aliryhmä, merkitään $H \leqslant G$, ja jos $H \leqslant G$ ja $H \neq G$, merkitään $H < G$.*

HUOMAUTUS. Määritelmä 4.1.1 edellyttää, että $b * b' \in B \; \forall \; b, b' \in B$ (eli että indusoitu laskutoimitus on määritelty).

Propositio 4.1.1 *Ryhmän G osajoukko $H \neq \emptyset$ on aliryhmä, jos*

1. $\forall \; x, y \in H, \quad xy^{-1} \in H$, *tai*
2. $\forall \; x, y \in H, \quad xy \in H$ *ja* $y^{-1} \in H$.

Tod.

1. *Olk. $e \in G$ neutraalialkio. Olkoon $h \in H$. Oletuksen nojalla pätee $hh^{-1} = e \in H$ (valitaan x=y=h). Samoin $h^{-1} = eh^{-1} \in H$. Kaikki on siis kunnossa, kun indusoitu laskutoimitus on määritelty: edellisen nojalla $\forall \; x, y \in H$ pätee $x(y^{-1})^{-1} = xy \in H$.*
2. *Ehdosta 1 seuraa ehto 2.*

□

Esimerkki 4.1.1 *1. Jokaisella ryhmällä G on aliryhmänä G ja neutraalialkion muodostama ryhmä.*

2. *$SL_n\mathbb{Z} < SL_n\mathbb{R} < GL_n\mathbb{R}$ (ks. Esimerkki 4.1.1 (2)).*

3. *Olkoon G ryhmä, $a \in G$. Alkion a virittämä syklinen aliryhmä on*

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

4. *Sykliset aliryhmät*

$$\langle n \rangle = \{n \cdot k \mid k \in \mathbb{Z}\} = n\mathbb{Z}, \quad n = 0, 1, 2, 3, \ldots$$

ovat $\mathbb{Z}$:n aliryhmiä. Muita aliryhmiä ei ole. Huomaa:

$$0 \cdot \mathbb{Z} = \{0\}, \quad 1 \cdot \mathbb{Z} = \mathbb{Z}.$$

Tod.

Olkoon $\emptyset \neq H < \mathbb{Z}$, ja olkoon N pienin positiivinen kokonaisluku aliryhmässä H. Osoitetaan, että kaikki H:n alkiot ovat muotoa Nk, $k \in \mathbb{Z}$. Jos $m \in H \backslash N\mathbb{Z}$, niin on $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ s.e.

$$1 \leqslant b < N \text{ ja } m = aN + b,$$

siis $b \in H$. Mutta tämä on ristiriita, sillä N on pieni positiivinen kokonaisluku H:ssa. Siis $H = N\mathbb{Z}$.

□

4.2 Joukkojen virittämiä aliryhmiä

Propositio 4.2.1 *Aliryhmien leikkaus on aliryhmä.*

Tod.

Harjoituksissa: vinkkinä

$$\bigcap_{i \in I} H_i < G, \text{ jos } H_i < G \; \forall i \in I.$$

□

Määritelmä 4.2.1 *Olkoon G ryhmä, $\emptyset \neq B \in G$. Joukon B virittämä aliryhmä $\langle B \rangle$ on pienin ryhmän G aliryhmä, joka sisältää joukon B.*

Propositio 4.2.2 *Olkoon G ryhmä, $\emptyset \neq B \in G$. Tällöin*

$$\langle B \rangle = \{e\} \cup \left\{ b_1, b_2, \ldots, b_m \mid b_i \in B \text{ tai } b_i^{-1} \in B \quad \forall\, i = 1, 2, \ldots, m,\ m \in \{1, 2, \ldots, n\} \right\}.$$

Tod.

Olkoon $\tilde{B}$ väitteen joukko. $\tilde{B}$ on G:n aliryhmä: Olkoon $b_1, b_2, \ldots, b_m \in \tilde{B}$. Tällöin

$$b_m^{-1}, b_{m-1}^{-1}, \ldots, b_2^{-1}, b_1^{-1} \in \tilde{B}$$

ja

$$(**) \qquad (b_1 b_2 \cdots b_m) \cdot (b_m^{-1} b_{m-1}^{-1} \cdots b_2^{-1} b_1^{-1}) = e,$$

joten jokaisen $\tilde{B}$:n alkion käänteisalkio on $\tilde{B}$:ssä. Sama pätee $\tilde{B}$:n alkioiden tulolle. Selvästi $\tilde{B} \subset B$.

Joukon B virittämä aliryhmä sisältää kaikki B:n alkiot ja niiden käänteisalkiot. Samoin se sisältää kaikki B:n alkioista ja niiden käänteisalkioista muodostetut tulot, koska indusoitu laskutoimitus on laskutoimitus $\langle B \rangle$:ssä. Siis

$$\tilde{B} \subset \langle B \rangle,$$

joten $\tilde{B} = \langle B \rangle$.

□

HUOMAUTUS.

1. $(**)$:ssa sallitaan joskus $m = 0$, sitä vastaava ”tyhjä tulo” tulkitaan neutraalialkioksi. Mikäli näin on, $(**)$ saisi esimerkiksi muodon

$$\langle B \rangle = \left\{ b_1^{\pm 1}, b_2^{\pm 1}, \ldots, b_m^{\pm 1} \mid b_1, \ldots, b_m \in B,\ m \in \mathbb{N} \right\}.$$

2. Proposition 4.2.2 mukaan ryhmän yhden alkion virittämä aliryhmä on sama kuin sen virittämä *syklinen* aliryhmä:

$$\langle a \rangle = \langle \{a\} \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

   (Vrt. Kleinin neliryhmä).

3. Ryhmä G on *syklinen*, jos on $a \in G$ s.e. $G = \langle a \rangle$.

Esimerkki 4.2.1 *1. Ryhmät $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ ja $\mathbb{Z}_p = \langle [1] \rangle$ ovat syklisiä.*

2. *Ryhmän* $\mathbb{R}^2$ *alkiot* $(1,0)$ *ja* $(0,1)$ *virittävät aliryhmän*

$$\langle (1,0),(0,1)\rangle = \langle \{(1,0),(0,1)\}\rangle = \mathbb{Z}^2 < \mathbb{R}^2.$$

$\langle (a,b)\rangle$ ei ole ryhmä: jos $a,b \neq 0$, niin $(a,-b)$ ei kuulu joukkoon $\langle (a,b)\rangle$, ja selvästi $\langle (a,0)\rangle \leqslant \mathbb{Z}\times\{0\}$ ja $\langle (0,a)\rangle \leqslant \{0\}\times\mathbb{Z}$.

3. *Ryhmät $K = \langle f,g\rangle$ ja $\mathbb{Z}_2\times\mathbb{Z}_2 = \langle ([0],[1]),([1],[0])\rangle$ eivät ole syklisiä, koska jokaisen neutraalialkiosta poikkeavan alkion virittämä syklinen aliryhmä on isomorfinen kahden alkion ryhmän $\mathbb{Z}_2$ kanssa.*

Propositio 4.2.3 *Olkoon $\phi : G \to G'$* ryhmähomomorfismi *ja olkoon $H \leqslant G$ ja $H' \leqslant G'$. Tällöin*

$$\phi(H) \leqslant G' \quad ja \quad \phi^{-1}(H') \leqslant G$$

ovat aliryhmiä.

Tod.

Olkoon $x,y \in \phi(H)$. Tällöin on $g,h \in H$ s.e.

$$\phi(g) = x \quad ja \quad \phi(h) = y.$$

Nyt

$$xy^{-1} = \phi(g)(\phi(h))^{-1} = \phi(g)\phi(h^{-1}) = \phi(gh^{-1}) \in \phi(H),$$

sillä H on ryhmä.

Toinen väite todistetaan harjoituksissa 5.

□

Määritelmä 4.2.2 *Ryhmähomomorfismin $\phi : G \to G'$*

1. Ydin *on Ker $\phi = \phi^{-1}(e')$, missä $e' \in G'$ on neutraalialkio, ja*
2. Kuva *on $\phi(G)$.*

Proposition 4.2.3 mukaan ryhmähomomorfismin ydin ja kuva ovat aliryhmiä.

Propositio 4.2.4 *Ryhmähomomorfismi on injektio $\Leftrightarrow$ sen ydin on neutraalialkion muodostama ryhmä.*

Tod.

(⇒) Olkoon $\phi : G \to G'$ ryhmähomomorfismi. Harjoituksissa osoitettiin, että neutraalialkio kuvautuu neutraalialkioksi, joten jos ϕ on injektio, niin Ker $\phi = \{e\}$, missä e on G:n neutraalialkio.

(⇐) Olkoon Ker $\phi = \{e\}$. Olkoon $x, y \in G$ s.e. $\phi(x) = \phi(y)$. Tällöin

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)(\phi(y))^{-1} = e,$$

joten $xy^{-1} \in$ Ker ϕ, siis $xy^{-1} = e \Leftrightarrow x = y \Rightarrow \phi$ on injektio.

□

4.3 Ekvivalenssirelaatioita aliryhmissä, sivuluokista

Jokainen ryhmän G aliryhmä H määrää kaksi ekvivalenssirelaatiota (jotka voivat olla sama):

$$(\dagger) \quad x \underset{v}{\sim} y \Leftrightarrow x^{-1}y \in H \qquad \text{ja} \qquad (\dagger\dagger) \quad x \underset{o}{\sim} y \Leftrightarrow yx^{-1} \in H.$$

Alkion $x \in G$ ekvivalenssiluokka relaatiossa $(\dagger)$ koostuu alkioista $y \in G$, joille on $z \in H$ s.e. $x^{-1}y = z$ eli $y = xz$. Siksi yleensä (aina) x:n ekvivalenssiluokkaa relaation $(\dagger)$ suhteen merkitään xH:lla. Joukkoa xH kutsutaan *aliryhmän vasemmaksi sivuluokaksi.* Vastaavasti relaation $(\dagger\dagger)$ ekvivalenssiluokkia Hx kutsutaan *oikeiksi sivuluokiksi.* Ekvivalenssiluokkia vastaavia tekijäluokkia merkitään

$$G/\underset{v}{\sim} = G/H \qquad \text{ja} \qquad G/\underset{o}{\sim} = H\backslash G.$$

Merk. $\#X = X$:n alkioiden lukumäärä.

Lause 4.3.1 *(Lagrangen lause) Olkoon G äärellinen ryhmä. Tällöin*

$$\#G = \#(G/H)\#H = \#(H\backslash G)\#H.$$

Tod.

Kuvaukset ($h \in H$

$$\begin{cases} h \mapsto xh \\ H \to xH \end{cases} \quad ja \quad \begin{cases} h \mapsto hx \\ H \to Hx \end{cases}$$

ovat bijektioita: kuvaukset ovat surjektioita, koska sivuluokat ovat

$$xH = \{xh \mid h \in H\}$$

ja

$$Hx = \{hx \mid h \in H\}.$$

Olk. $h, h' \in H$ s.e. $xh = xh'$. Supistusssäännön mukaan $h = h'$, joten ensimmäinen kuvaus on injektio; toinenkin on injektio vastaavalla päättelyllä. Siis jokaisessa sivuluokassa on yhtä monta alkiota kuin aliryhmässä H. Koska sivuluokat ovat erillisiä ja saman kokoisia, niiden lukumäärä on $\#G/\#H$

□

Määritelmä 4.3.1 *$\#G$ on ryhmän G* kertaluku. *Ryhmän G alkion g* kertaluku *on $\#\langle g\rangle$. Aliryhmän $H < G$* indeksi *on $\#(G/H) = \#(H\backslash G)$. Indeksiä merkitään usein $[G : H]$:lla.*

HUOMAUTUS. Äärellisille ryhmille $[G : H] = \#G/\#H$ (Lagrangen lause).

Propositio 4.3.1 *Olkoon G äärellinen ryhmä. Tällöin $g^{\#G} = e \; \forall \; g \in G$.*

Tod.

Olkoon $H = \langle g\rangle$. Tällöin $\#G = n\#H$ jollain $n \in \mathbb{N}$. Potenssin laskusääntöjen nojalla ROE

$$g^{\#H} = e \qquad (g^{\#G} = g^{(\#H)n} = (g^{\#H})^n).$$

Mutta tämä on selvää, sillä muuten g virittäisi väärän kokoisen ryhmän:

$$\langle g\rangle = \left\{g, g^2, g^3, \cdots, g^{\#H}\right\}.$$

□

Esimerkki 4.3.1 *1. Jos G on kommutatiivinen $(ab = ba \ \forall \ a, b, \in G)$ ja $H < G$, niin $xH = Hx \ \forall \ x \in G$.*

2. $\mathbb{R} \times \{0\} \subset \mathbb{R}^2$, $[\mathbb{R}^2 : (\mathbb{R} \times \{0\})] = \infty$, koska sivuluokat ovat

$$\mathbb{R} \times \{a\}, \ a \in \mathbb{R}.$$

Olkoon $x \in \mathbb{R}^2$. Tällöin $x(\mathbb{R} \times \{0\})$ on ikävä merkintä, ja onkin parempi käyttää sivuluokista merkintää $H = \mathbb{R} \times \{0\}$:

$$\begin{aligned} x + H &= \{x + (a, 0) : a \in \mathbb{R}\} \\ &= \{(0, x_2) + (a, 0) : a \in \mathbb{R}\} \\ &= \{(0, x_2) + H\} = \mathbb{R} \times \{x_2\}. \end{aligned}$$

3. $\mathbb{Z}_n = \mathbb{Z}/_{\equiv} = \mathbb{Z}/n\mathbb{Z} = n\mathbb{Z}\backslash\mathbb{Z}$:

$$\begin{aligned} a \equiv b &\Leftrightarrow b - a = nk \quad \textit{jollekin } k \in \mathbb{Z} \\ &\Leftrightarrow b - a \in n\mathbb{Z}. \end{aligned}$$

HUOMAUTUS. *Laskutoimitusta merkitään $(+)$:lla. Nyt $n\mathbb{Z}$ on sivuluokkien määritelmässä esiintyvä aliryhmä H. Edelleen,*

$$[\mathbb{Z} : n\mathbb{Z}] = \#(\mathbb{Z}/n\mathbb{Z}) = n.$$

4. Euklidisen avaruuden $\mathbb{R}^n$ isometriat *muodostavat ryhmän*

$$Isom\mathbb{R}^n = \{\phi : \ \mathbb{R}^n \to \mathbb{R}^n \textit{ bijektio} : \|\phi(x) - \phi(y)\| = \|x - y\| \ \forall \ x, y \in \mathbb{R}^n\}.$$

(Edellisessä on $\|z\| = \sqrt{z_1^2 + z_2^2 + \ldots + z_n^2}$.) Ryhmä $Isom\mathbb{R}^n$ on $\mathbb{R}^n$:n permutaatioryhmän $S(\mathbb{R}^n)$ aliryhmä. $Isom\mathbb{R}^n$:llä on monia tärkeitä aliryhmiä: Olkoon $P_m, m \geqslant 3$ säännöllinen m-kulmio $\mathbb{R}^2$:ssa (kaikki sivut yhtä pitkiä).

Monikulmion P_m symmetriaryhmä koostuu niistä $\mathbb{R}^n$:n isometrioista, jotka kuvaavat P_m:n itselleen. Neliön symmetriaryhmä voidaan samastaa matriisiryhmän

$$D_4 = \left\langle r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle < GL_2\mathbb{R} \quad \textit{kanssa.}$$

Aliryhmä $\langle s \rangle = H$ on isomorfinen ryhmän $\mathbb{Z}$ kanssa, koska

$$s^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Aliryhmän H vasemmat sivuluokat[1] *ryhmässä D_4 (jossa on 8 alkiota) ovat*

$$\begin{aligned} H = sH = idH &= \{id, s\} \\ rH = rsH &= \{r, rs\} \\ r^2H = r^2sH &= \{r^2, r^2s\} \\ r^3H = r^3sH &= \{r^3, r^3s\}, \end{aligned}$$

ja oikeat sivuluokat ovat

$$\begin{aligned} H = Hs = Hid &= \{id, s\} \\ Hr = Hsr &= \{r, sr\} \\ Hr^2 = Hsr^2 &= \{r^2, sr^2\} \\ Hr^3 = Hsr^3 &= \{r^3, sr^3\}. \end{aligned}$$

Nyt $rH \neq Hr$, sillä

$$rs = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; sr = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

Määritelmä 4.3.2 *Ryhmän G aliryhmä H on* normaali, *jos*

$$ghg^{-1} \in H \quad \forall\, h \in H, \quad \forall\, g \in G.$$

Jos H on ryhmän G normaali aliryhmä, merkitään $H \trianglelefteq G$. Jos $H \trianglelefteq G$ ja $H < G$, merk. $H \triangleleft G$.

HUOMAUTUS.

1. Toinen tapa ilmaista aliryhmän H normaalius on sanoa, että kaikki ryhmän G sisäiset automorfismit kuvaavat H:n itselleen.

2. $gH = H = Hg \Leftrightarrow g \in H$.

Esimerkki 4.3.2 *1. G ja $\{e\}$ ovat G:n normaaleja aliryhmiä;*

$$G \trianglelefteq G, \; \{e\} \triangleleft G.$$

[1] Ks. sivu 31.

2. *Esimerkin 5.3.1 mukaan on*

$$n\mathbb{Z} \trianglelefteq \mathbb{Z} \; \forall n \in \mathbb{N},$$

mutta diedriryhmän D_4 aliryhmä H ei ole normaali:

$$rs \neq sr \Rightarrow s \neq r^{-1}sr.$$

Lisäksi $r^{-1}sr \neq id$, joten $r^{-1}sr \notin H$.

Propositio 4.3.2 *Olkoon $\phi : G \to G'$ ryhmähomomorfismi.*

1. *Olkoon $H \trianglelefteq G$. Tällöin $\phi(H) \trianglelefteq Im(\phi) = \phi(G)$.*
2. *Olk. $H' \trianglelefteq G'$. Tällöin $\phi^{-1}(H') \trianglelefteq G$. Erityisesti ϕ:n ydin $Ker(\phi)$ on G:n normaali aliryhmä.*

<u>Tod.</u>

1. *On todistettu aiemmin, että*

   $\phi(H)$ *on ryhmä*
   $\phi(H) \; < G'$.

   Olkoon $a' \in \phi(H)$ ja $g' \in \phi(G)$. Tällöin

   $$g'a'(g')^{-1} = \phi(g)\phi(a)\phi(g)^{-1} = \phi(g)\phi(a)\phi(g^{-1}) = \phi(\underbrace{gag^{-1}}_{\in H}) \in \phi(H),$$

   missä $a \in H$ s.e. $\phi(a) = a'$ ja $g \in G$ s.e. $\phi(g) = g'$.

2. *Harjoituksissa 6.*

□

Propositio 4.3.3 *Olkoon $H < G$. Tällöin $H \triangleleft G \Leftrightarrow xH = Hx \quad \forall x \in G$.*

<u>Tod.</u>

Harjoitus 6.

□

Propositio 4.3.4 *Aliryhmää $H < G$ vastaavat ekvivalenssirelaatiot $\underset{v}{\sim}$ ja $\underset{o}{\sim}$ ovat sama relaatio, jos ja vain jos $H \triangleleft G$.*

Tod.

Ekvivalenssiluokille tulos seuraa propositiosta 5.3.3 Ekvivalenssirelaatiot ovat samat $\Leftrightarrow$ niiden ekvivalenssiluokat ovat samat.

□

Jos $H \triangleleft G$, merkitsemme vastaavaa ekvivalenssirelaatiota $\sim$:llä. Tällöin voimme käyttää kumpaa tahansa ehdoista

$$x^{-1}y \in H \text{ tai } yx^{-1} \in H$$

x:n ja y:n ekvivalenssin toteamiseksi.

Yleisessä tilanteessa ryhmän G laskutoimitus ei ole yhteensopiva kummankaan ekvivalenssirelaation $\underset{v}{\sim}$ ja $\underset{o}{\sim}$ kanssa. Kun $H \triangleleft G$, on tilanne toinen:

Esimerkki 4.3.3
1. *Jos $H < G$, ja $[G : H] = 2$, niin $H \triangleleft G$. H:lla on kaksi sivuluokkaa: H ja H:n komplementti. Siis jokaiselle $x \in G$ pätee $xH = Hx$, joten $H \triangleleft G$ (sillä $xH = Hx \Leftrightarrow x \in H$).*
2. *Jos $K \trianglelefteq G$ ja $K < H < G$, niin $K \triangleleft H$.*

Lause 4.3.2 *Olkoon G ryhmä, $H < G$. Tällöin ekvivalenssirelaatio $\underset{\sim}{\sim}$ on yhteensopiva ryhmän G laskutoimituksen kanssa, jos ja vain jos $H \triangleleft G$. Jos $H \triangleleft G$, niin tekijäjoukko G/H on ryhmä.*

Tod.

1. *Ol. että H on normaali. Olk. $x, x', y, y' \in G$ s.e. $x \underset{v}{\sim} x'$, $y \underset{v}{\sim} y'$. Nyt $\underset{v}{\sim}$ ja $\underset{o}{\sim}$ ovat sama relaatio. Edelleen on $h_1, h_2 \in H$ s.e.*

   $$x' = h_1 x \text{ ja } y' = h_2 y \ (\underset{o}{\sim} \text{:n ehto}).$$

   Lisäksi on $h_3 \in H$ s.e. $h_3 x = x h_2$ ($xH = Hx$). Siis

   $$x'y' = h_1 x h_2 y = h_1 h_3 xy. \quad (h_1 \in H)$$

   Joten: $x'y' \sim xy$.

Toinen tapa:

On $\tilde{h_1}, \tilde{h_2} \in H$ s.e. $x' = x\tilde{h_1}$ ja $y' = y\tilde{h_2}$ ja on $\tilde{h_3}$ s.e. $\tilde{h_1}y = y\tilde{h_3}$. Tällöin $x'y' = x\tilde{h_1}y\tilde{h_2} = xy\tilde{h_3}\tilde{h_2}$, joten $x'y' \sim xy$.

2. *Jos laskutoimitus on yhteensopiva relaation $\underset{v}{\sim}$ kanssa, niin tekijäjoukko $G/\underset{v}{\sim}$ varustettuna tekijälaskutoimituksella on ryhmä proposition 4.3.2 nojalla. Luonnollisen homomorfismin*

$$G \to G/\underset{v}{\sim}$$

ydin on H. Proposition 4.3.2 nojalla $H \trianglelefteq G$.

□

HUOMAUTUS. Sama pätee relaatiolle $\underset{o}{\sim}$.

Tekijäryhmän G/H laskutoimitusta merkitään yleensä näin:

$$(xH(yH)) = xyH.$$

Jos G:n laskutoimitus on $+$, on tässäkin luontevaa käyttää seuraavanlaista merkintää: merkitään x:n sivuluokkaa $x + H$:lla (tai $H + x$:llä), jolloin laskutoimitus on

$$(x + H) + (y + H) = (x + y) + H.$$

Lause 4.3.3 *(Ryhmien isomorfismilause) Olkoon $\phi : G \to G'$ ryhmähomomorfismi. Tällöin $Im(\phi) = \phi(G)$ on isomorfinen tekijäryhmän $G/_{Ker(\phi)}$ kanssa:*

$$G/_{Ker(\phi)} \cong Im(\phi).$$

Tod.

Konstruoidaan haluttu kuvaus. Kuvaus $\psi : G/_{Ker(\phi)} \to Im(\phi)$,

$$\psi(xKer(\phi)) = \phi(x)$$

on isomorfismi (Käytetään merkintää $H = Ker(\phi)$). ψ on hyvin määritelty: Jos $xH = yH$, niin $xy^{-1} \in H$. Siis $\phi(xy^{-1}) = e'$,

$$\phi(x^{-1})\phi(y) = \phi(x)^{-1}\phi(y),$$

joten $\phi(x) = \phi(y)$.

ψ on homomorfismi:

$$\psi(xHyH) \overset{\text{tekijälaskutoimitus}}{=} \psi(xyH) \overset{\psi\text{:n määr.}}{=} \phi(xy) = \phi(x)\phi(y) \overset{\psi\text{:n määr.}}{=} \psi(xH)\psi(yH).$$

ψ on selvästi surjektio. Lisäksi ψ on injektio: osoitetaan, että kuvauksen ψ ydin koostuu ainoastaan ryhmän G/H neutraalialkiosta e'. Olkoon $xH \in G/H$. s.e.

$$\psi(xH) = e'.$$

Siis $\phi(x) = \psi(xH) = e'$, joten $x \in H = Ker(\phi)$. Siis $xH = H$.

□

Lause 4.3.4 *Olkoon $K \trianglelefteq H \trianglelefteq G$. Tällöin kuvaus*

$$\phi : G/K \to G/H,$$

$\phi(xK) = xH$ on surjektiivinen homomorfismi, jonka ydin on H/K. Erityisesti ryhmät

$$((G/K)/(H/K)) \text{ ja } G/H$$

ovat isomorfiset.

<u>Tod.</u>

Kuvaus ϕ on hyvin määritelty (mieti miksi, ei kuulemma ole vaikea). Kuvaus on selvästi surjektio (määritelmä).

Lisäksi

$$\phi((xK)(yK)) = \phi(xyK) = xyH = (xH)(yH).$$

Samalla tavalla meni kuin edellinen todistus, joten ϕ on homomorfismi.

Tarkastellaan kuvauksen ϕ ydintä: tekijäryhmän G/H neutraalialkio on H. Jos $h \in H$, niin

$$\phi(hK) = hH = H,$$

joten $H/K \subset Ker(\phi)$. Toisaalta, jos $g \notin H$,niin

$$\phi(gK) = gH = H$$

(jos olisi $gh = h' \Rightarrow g = h'h^{-1} \in H$, joka ei pidä paikkaansa.) Siispä $gH \notin H$. Siis $Ker(\phi) = H/_K$. Loppu seuraa lauseesta 5.3.3 ja surjektiivisuudesta.

□

Lause 4.3.5 *Olkoon $\phi : G \to G'$ surjektiivinen homomorfismi, ja olk. $H' \trianglelefteq G'$. Tällöin*

$$G/_{\phi(H')^{-1}} \cong G'/H'$$

Tod.

Proposition 5.3.2 nojalla $H = \phi(H')^{-1} \trianglelefteq G$. Olkoon

$$p : G' \to G'/H'$$

luonnollinen homomorfismi, eli $p(x) = xH'$. Kuvaus

$$\tilde{\phi} : G \to G'/H'$$

on surjektiivinen homomorfismi, jonka ydin on H. Lause 5.3.4 $\Rightarrow G/_H \cong G/H'$.

Syklisten ryhmien ominaisuuksia

Lause 4.3.6 *1. Syklinen ryhmä on isomorfinen ryhmän $\mathbb{Z}$ tai jonkin ryhmän $\mathbb{Z}_p$, $p \in \mathbb{N}$ kanssa.*

2. *Jokainen syklisen ryhmän aliryhmä on syklinen.*

3. *Jokainen syklisen ryhmän tekijäryhmä on syklinen.*

Tod.

1. *Harjoitus 6.*

2. *Äärettömälle sykiliselle ryhmälle tämä seuraa kohdasta (1) ja esimerkistä 5.1.1(?).*

   Olkoon C syklinen ryhmä, ja olk. $H < C$. Osoitetaan, että H on syklinen. Olk. $g \in C$ ryhmän C virittäjä ($g \in C$ s.e. $C = \{g^n \mid n \in \mathbb{Z}\}$). Olkoon

   $$\phi : \mathbb{Z} \to C,\ \phi(n) = g^n;$$

   ϕ on homomorfismi. Nyt $\phi^{-1}(H) \leqslant \mathbb{Z}$, joten on $N \in \mathbb{N}$ s.e. $\phi^{-1}(H) = N\mathbb{Z}$. Jos $h \in H$, niin $h = \phi(kN)$ jollain $k \in \mathbb{Z}$, joten $h = g^{kN} = (g^N)^k$. Siispä $H = \langle g^N \rangle$, eli H on syklinen.

3. *Harjoitus 7.*

□

Esimerkki 4.3.4 *Olkoon*

$$M = \left\{ f : \mathbb{R} \cup \{\infty\} : f(x) = \frac{ax+b}{cx+d} \quad | \quad a,b,c,d \in \mathbb{R},\ ad - bc \neq 0 \right\}.$$

Sopimus 3 ∞ *on* äärettömyyspiste, $\infty \notin \mathbb{R}$.

Jos

$$f(x) = \frac{ax+b}{cx+d},$$

niin $f(\infty) = a/c$ *ja* $f(-d/c) = \infty$. *Kuvaukset* $\phi \in M$ *ovat bijektioita, ja* M *on permutaatioryhmän* $S(\mathbb{R} \cup \{\infty\})$ *aliryhmä.*

Kuvaus

$$p : GL_2\mathbb{R} \to M,\ p(A) = p\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = f_A,\ f_A(x) = \frac{ax+b}{cx+d}$$

on surjektiivinen homomorfismi, jonka ydin on suuri; jos $\lambda \in \mathbb{R}^*$, *niin*

$$p\begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix} = p\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Koska kuvaus p *on homomorfismi,* M*:n kuvausten yhdistäminen voidaan tehdä kertomalla jotkin niitä vastaavat* $GL_2\mathbb{R}$*:n matriisit keskenään. Tulomatriisin kertoimet antavat yhdistetyn kuvauksen.* $GL_2\mathbb{R}$*:n sijaan voidaan käyttää* $SL_2\mathbb{R}$*:ää, sillä* $\forall\ A \in GL_2\mathbb{R}$ *on* $A' \in SL_2\mathbb{R}$ *s.e.* $p(A) = p(A')$. *Nyt*

$$ker(p) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mid \lambda \neq 0 \right\}$$
$$ker(p|_{SL_2\mathbb{R}}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Edelleen,

$$M \cong GL_2\mathbb{R}/_{Ker(p)} = SL_2\mathbb{R}/_{ker(p|_{SL_2\mathbb{R}})}.$$

Luku 5

Renkaat

5.1 Määritelmä ja perusominaisuuksia

Tarkastellaan algebrallisia rakenteita, joissa on määritelty kaksi (2) assosiatiivista laskutoimitusta:

$(+)$: kommutatiivinen laskutoimitus (yhteenlasku)
$(\cdot)$: (kertolasku).

Kolmikko $(R, +, \cdot)$ on *rengas*, jos

1. $(R, +)$ on kommutatiivinen ryhmä.
2. $a(b+c) = ab + ac$ ja $(b+c)a = ba + ca \quad \forall\, a, b, c \in R$.
3. kertolaskulla on neutraalialkio $1 = 1_R$.

Merkitään laskutoimituksen $(+)$ neutraalialkiota $0 = 0_R$:llä. Rengas on kommutatiivinen, jos kertolasku on sitä. Jos alkiolla $u \in R$ on käänteisalkio kertolaskun suhteen, niin u on renkaan R *yksikkö*. $(R, +)$ on renkaan *additiivinen* ryhmä.

Yleensä sanotaan, että R on rengas ja tarkoitetaan, että $(R, +, \cdot)$ on rengas.

HUOMAUTUS. Joskus renkaalta ei vaadita ominaisuutta (3). Tällaisissa lähteissä määrittelemäämme rakennetta sanotaan ykköselliseksi renkaaksi.

Propositio 5.1.1 *Olkoon R rengas. Tällöin*

1. $0_R x = 0_R \quad \forall x \in R$.

2. $x(-y) = (-x)y = -(xy) \quad \forall\, x, y \in R.$

3. $x(y-z) = xy - xz$ *ja* $(y-z)x = yx - zx \quad \forall\, x, y, z \in R.$

4. *Jos* $\#R \geqslant 2$, *niin* $0_R \neq 1_R$.

5. *Jos* $\#R \geqslant 2$, *niin* 0_R*:llä ei ole käänteisalkiota kertolaskun suhteen.*

Tod.

(1): Distributiivisuudesta seuraa, että

$$0_R x + x = (0_R + 1_R)x = 1_R x = x.$$

Koska neutraalialkio on yksikäsitteinen, pätee nyt $0_R x = 0_R$.

(5):

$$0_R x \neq 1_R \ \forall x \in R. \Leftarrow \begin{cases} (4) & \Rightarrow 1_R \neq 0_R \\ (1) & \Rightarrow 0_R x = 0_R \ \forall x \in R. \end{cases}$$

Loput harjoitustehtäviä.

□

Esimerkki 5.1.1 1. $\mathbb{Z}, \mathbb{Q}$ *ja* $\mathbb{R}$ *ovat renkaita.*

2. *Olkoon* $p \in \mathbb{N}$. *Kokonaislukujen kertolasku on yhteensopiva kongruenssin*

$$a \equiv a' \Leftrightarrow \exists\, k \in \mathbb{Z} \text{ s.e. } a' = a + kp$$

kanssa. Yleensä tätä kongruenssia merkitään

$$a \equiv a' mod(p),$$

luetaan a on kongruentti a'*:n kanssa modulo p. Joukko* $\mathbb{Z}_p$ *varustettuna* $\mathbb{Z}$*:n yhteen- ja kertolaskun tekijälaskutoimituksella on kommutatiivinen rengas (harj. 7).*

3. *Olkoon* $\emptyset \neq X$ *ja olk. R rengas. Olk.* $\mathfrak{F}(X, R)$ *joukko, joka koostuu kaikista kuvauksista joukosta X renkaaseen R. Määritellään joukon* $\mathfrak{F}(X, R)$ *yhteen- ja kertolasku pisteittäin: olk.* $f, g \in \mathfrak{F}(X, R)$, *ts.*

$$(f+g)(x) = f(x) + g(x) \quad \forall x \in X$$
$$(fg)(x) = f(x)g(x) \quad \forall x \in X.$$

Joukko $\mathfrak{F}(X,R)$ varustettuna näillä laskutoimituksilla on rengas, jota kutsutaan kuvausrenkaaksi. *$\mathfrak{F}(X,R)$ on kommutatiivinen, jos R on sitä.*

Yhteenlasku on assosiatiivinen: Olk. $f,g,h \in \mathfrak{F}(X,R)$. Tällöin

$$\begin{aligned}((f+g)+h)(x) &= ((f+g)(x))+h(x)\\ &= (f(x)+g(x))+h(x)\\ &= f(x)+(g(x)+h(x))\\ &= f(x)+(g+h)(x)\\ &= (f+(g+h))(x).\end{aligned}$$

Kertolasku samaan tapaan.

$(\mathfrak{F}(X,R),+)$ on ryhmä: $0 : X \to R,\ 0(x) = 0_R\ \forall x \in X$, on yhteenlaskun neutraalialkio: jos $f \in \mathfrak{F}(X,R)$, niin kuvaus $\overline{f} : X \to R,\ \overline{f}(x) = -f(x)\ \forall x \in X$ on f:n käänteisalkio yhteenlaskun suhteen:

$$(f+\overline{f})(x) = f(x) - f(x) = 0_R = 0(x) \quad \forall x \in X.$$

Kertolaskulla on neutraalialkio $1 : X \to R,\ 1(x) = 1 \quad \forall x \in X$. Distributiivisuus?? (Harj.) Kommutatiivisuus??

$$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x) \quad \forall x,$$

jos R on kommutatiivinen rengas (esimerkiksi $\mathfrak{F}(\mathbb{R},\mathbb{R})$).

4. *Olkoon $(A,*)$ kommutatiivinen ryhmä (kommutatiivista ryhmää kutsutaan usein* Abelin *ryhmäksi). Olk.*

$$Hom(A,A) = \{\phi : A \to A \text{ homomorfismi.}\}$$

Määritellään joukkoon $Hom(A,A)$ kaksi laskutoimitusta: pisteittäinen yhteenlasku $((\phi+\phi')(a) = \phi(a)+\phi'(a)\ \forall a \in A)$ ja kuvausten yhdistäminen.

Yhteenlasku on laskutoimitus, sillä $\phi+\phi'$ on homomorfismi:

$$\begin{aligned}(\phi+\phi')(a+b) &= \phi(a+b)+\phi'(a+b)\\ &= \phi(a)+\phi(b)+\phi'(a)+\phi'(b)\\ &= (\phi+\phi')(a)+(\phi+\phi')(b) \quad \forall a,b \in A.\end{aligned}$$

$(Hom(A,A),+,\circ)$ on rengas:

$(Hom(A,A),+)$ on kommutatiivinen ryhmä: assosiatiivisuus ja kommutatiivisuus on helppoa tarkistaa (harj.) Homomorfismin $\phi \in Hom(A,A)$ käänteisalkio yhteenlaskun suhteen on $\overline{\phi}$ kuten kohdassa (3) ja nollahomomorfismi

$$0 : A \to A,\ 0(a) = 0 \quad \forall a \in A,$$

on $(+)$:n neutraalialkio.

Identtinen homomorfismi $id : A \to A$ on kertolaskun eli kuvausten yhdistämisen neutraalialkio, joten vielä pitää tarkastaa distributiivisuus.

Olk. $\phi, \psi, \rho \in Hom(A,A)$. Tällöin

$$\begin{aligned}((\psi+\rho)\circ\phi)(a) = (\psi+\rho)(\phi(a)) &= \psi(\phi(a)) + \rho(\phi(a)) \\ &= (\psi\circ\phi)(a) + (\rho\circ\phi)(a),\end{aligned}$$

ja

$$\begin{aligned}(\psi\circ(\rho+\phi)(a) &= \psi(\rho(a)+\phi(a)) \\ &= \psi(\rho(a)) + \psi(\phi(a)) \\ &= (\psi\circ\rho)(a) + (\psi\circ\phi)(a) \quad \forall a \in A.\end{aligned}$$

5. *Olkoon R rengas, $\#R \geqslant 2$. R -kertoimiset $n \times n$ -matriisit, $n \geqslant 2$, muodostavat renkaan $M_n R$, joka ei ole kommutatiivinen. Harjoituksissa 1 osoitettiin muut ominaisuudet paitsi distributiivisuus, kun $n = 2$ ja $R = \mathbb{R}$.*

5.2 Kuvauksista ja renkaista

Määritelmä 5.2.1 *Olk. R, R' renkaita. Kuvaus*

$$\phi : R \to R'$$

on rengashomomorfismi, *jos se on homomorfismi yhteen- ja kertolaskulle ja $\phi(1_R) = 1_R$. Bijektiivinen rengashomomorfismi on* rengasisomorfismi.

HUOMAUTUS. *Harjoituksissa osoitettiin, että jos kuvaus ϕ on surjektiivinen, niin $\phi(1_R) = 1'_R$ kaikille ϕ jotka ovat homomorfismeja kertolaskulle:*

$$(\phi(x+y) = \phi(x) + \phi(y)\ \&\ \phi(xy) = \phi(x)\phi(y) \quad \forall x, y \in R.)$$

Ilman surjektiivisuutta näin ei välttämättä ole.

Propositio 5.2.1 *Jos $f : R \to S$ ja $g : S \to T$ ovat rengashomomorfismeja, niin*

$$g \circ f : R \to T$$

on rengashomomorfismi.

Rengashomomorfismi $f : R \to S$ on rengasisomorfismi, jos ja vain jos on rengashomomorfismi s.e.

$$\overline{f} : S \to R,\ \overline{f} \circ f = id_R \quad ja \quad f \circ \overline{f} = id_S.$$

Tod. Harjoitus ($R \xrightarrow{t} S \xrightarrow{g} T$; $S \xrightarrow{\overline{f}} R$.)

□

Määritelmä 5.2.2 *Olkoon R rengas. Jos $S \subset R$ varustettuna renkaasta R on rengas, ja jos $1_S = 1_R$, niin S on renkaan R* alirengas.

HUOMAUTUS. Halutaan siis, että identtinen kuvaus $id : S \to R$ on rengashomomorfismi.

Propositio 5.2.2 *Olkoon R rengas, $S \subset R$. Tällöin S on renkaan R* alirengas, *jos ja vain jos*

1. $\forall\ x, y \in S, \quad x + y \in S$ *ja* $xy \in S$.
2. $-1_R \in S$.

□

Esimerkki 5.2.1 *1. Joukko*

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

on renkaan

$$M_2\mathbb{R} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

osajoukko, joka on rengas indusoidulla laskutoimituksella. S ei ole $M_2\mathbb{R}$:n alirengas:

$$1_{M_2\mathbb{R}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 1_S.$$

Rengas S on rengasisomorfinen $\mathbb{R}$:n kanssa:

$$\begin{cases} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} & = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} & = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \end{cases} \Rightarrow \text{ kuvaus } a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \text{ on isomorfismi.}$$

2. *$\mathbb{Z}$ on $\mathbb{Q}$:n alirengas.*

3. *Olk.*
$$R = \{f : [0,1] \to \mathbb{R}\}.$$
Kuvaus $h : R \to \mathbb{R}$, $h(f) = f(1/2)$, on rengashomomorfismi:
$$h(f+g) = (f+g)(1/2) = f(1/2) + g(1/2) = h(f) + h(g).$$
Tulo lasketaan samaan tapaan. Renkaan R kertolaskun neutraalialkio on
$$1_R : [0,1] \to \mathbb{R},\ 1_R(x) = 1\ \forall x \in [0,1],$$
$$h(1_R) = 1_R(1/2) = 1 = 1_R.$$

4. *Samaan tapaan kuin teimme aliryhmiä permutaatioryhmille $S(x)$, saadaan alirenkaita kuvausrenkaisiin $\mathfrak{F}(X,R)$. Esimerkiksi*
$$C(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ jatkuva ja deriv.}\}$$
$$C^k(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ } k \text{ kertaa jatkuva ja deriv.}\}$$
ovat kuvausrenkaan $\mathfrak{F}(\mathbb{R},\mathbb{R})$ alirenkaita:

<u>Tod.</u>

Jos $f,g \in C^k(\mathbb{R})$, $k \in \mathbb{N}$, niin $f+g$, $fg \in C^k(\mathbb{R})$. Lisäksi kuvaus $-1_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$, $-1_R(x) = -1$ on k kertaa jatkuvasti derivoituva $\forall\ k \in \mathbb{N}$. Propositiosta 5.2.2 seuraa nyt väite.

□

5. *Olk.*
$$\mathfrak{L}(\mathbb{R}^n) = \{L : \mathbb{R}^n \to \mathbb{R}^n \mid L \text{ on lin. kuvaus}\}$$
$$= \{L \in Hom(\mathbb{R}^n,\mathbb{R}^n) \mid L(ax) = aL(x)\ \forall a \in \mathbb{R},\ \forall x \in \mathbb{R}^n\}.$$

$\mathfrak{L}(\mathbb{R}^n)$ on $Hom(\mathbb{R}^n, \mathbb{R}^n)$:n alirengas (laskutoimituksena kuvausten yhdistäminen): Olk. $L, L' \in \mathfrak{L}(\mathbb{R}^n)$. Tällöin

$$\begin{aligned}(L + L')(ax) = L(ax) + L'(ax) &= aL(x) + aL'(x) \\ &= a(L(x) + L'(x)) \\ &= a(L + L')(x).\end{aligned}$$

Edelleen,

$$(LL')(ax) = L(L'(ax)) = L(aL'(x)) = a(LL')(x)$$

Siis $L + L',\ LL' \in \mathfrak{L}(\mathbb{R}^n)$. Nyt

$$-1_{Hom(\mathbb{R}^n,\mathbb{R}^n)}(x) = -x \quad (1_{Hom(\mathbb{R}^n,\mathbb{R}^n)} = id_{\mathbb{R}^n}),$$

joka on lineaarikuvaus. Nyt Propositiosta 5.2.2 seuraa väite.

□

Propositio 5.2.3 *Olk. $\phi : R \to R'$ rengashomomorfismi.*

1. *Olkoon S renkaan R alirengas. Tällöin $\phi(S)$ on renkaan R' alirengas.*
2. *Olk. S' renkaan R' alirengas. Tällöin $\phi^{-1}(S')$ on renkaan R alirengas.*

Tod.

1. *Aiemmin on osoitettu, että $\phi(S)$ on kommutatiivinen ryhmä. Riittää tarkastella kertolaskua ja ykkösen kuvautumista.*

   Olk. $\phi(a), \phi(b) \in \phi(S)$. Tällöin

   $$\phi(a)\phi(b) = \phi(\underbrace{ab}_{\in S}) \in \phi(S).$$

   Koska $-1_S = -1_R \in S$, niin

   $$-1_{R'} = -\phi(1_R) = \phi(-1_R) \in \phi(S).$$

   Propositio 5.2.2 antaa jälleen väitteen

2. *Harjoituksissa 8.*

□

Määritelmä 5.2.3 *Olkoon R rengas, $\#R \geqslant 2$ (eli vähintään kaksi* eri *alkiota).*

1. *Jos $a, b, c \in R$ s.e. $ab = c$, niin a ja b ovat c:n* tekijöitä.
2. *Jos $a, b \in R,\ a \neq 0 \neq b$, ja $ab = 0$, niin a ja b ovat* nollan jakajia.
3. *Jos renkaassa R ei ole nollan jakajia ja R on kommutatiivinen, niin R on* kokonaisalue.
4. *Jos kaikki renkaan R nollasta poikkeavat alkiot ovat yksiköitä (yksiköllä on kertolaskun suhteen käänteisalkio), niin R on* jakorengas *eli* vino kunta.
5. *Kommutatiivinen jakorengas on* kunta.

Yleensä vinoksi kunnaksi sanotaan vain sellaisia jakorenkaita, jotka eivät ole kommutatiivisia.

Jos a on c:n tekijä, sanotaan usein että a jakaa c:n eli $a|c$.

Esimerkki 5.2.2
1. *$\mathbb{Z}$ on kokonaisalue, mutta se ei ole jakorengas, koska esim. $2 \in \mathbb{Z}$ ei ole yksikkö.*
2. *$\mathbb{R}, \mathbb{Q}$ ovat kuntia.*
3. *$M_n\mathbb{R}$ ei ole kokonaisalue, kun $n \geqslant 2$: Jos $A, B \in M_n\mathbb{R}$, ja ainoat nollasta poikkeavat kertoimet ovat a_{11} ja b_{nn}, niin $AB = 0 = 0_{n\times n}$.*
4. *Määritellään joukossa $\mathbb{R}^4$ yhteenlasku komponenteittain ja kertolasku asettamalla*

$$\begin{gathered} a \cdot b = (a_1, a_2, a_3, a_4) \cdot (b_1, b_2, b_3, b_4) \\ (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4, a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3, \\ a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2, a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1) \end{gathered}$$

Näillä laskutoimituksilla varustettuna $\mathbb{R}^4$ on vino kunta $\mathbb{H}$ (Hamiltonin kvaterniot). Kertolaskun neutraalialkio on $(1,0,0,0)$, distributiivisuus (harj.). $\mathbb{H}$ ei ole kommutatiivinen, sillä esim.

$$(0,1,0,0) \cdot (0,0,0,1) = (0,0,0,1) \neq (0,0,0,-1) = (0,0,0,1) \cdot (0,1,0,0).$$

Alkion $(a_1, a_2, a_3, a_4) \neq 0$ käänteisalkio kertolaskun suhteen on

$$\frac{a_1, -a_2, -a_3, -a_4}{a_1^2 + a_2^2 + a_3^2 + a_4^2};$$

Nimittäin,

$$(a_1, a_2, a_3, a_4) \cdot (a_1, -a_2, -a_3, -a_4) = (a_1^2 + a_2^2 + a_3^2 + a_4^2, 0, 0, 0).$$

Siis kaikki alkiot $a \in \mathbb{H}\backslash\{0\}$ ovat yksiköitä (eli niillä on kertolskun suhteen käänteisalkio).

Propositio 5.2.4 *1. Jakorenkaassa ei ole nollan jakajia. Erityisesti kunta on kokonaisalue.*

2. Äärellinen kokonaisalue on kunta.

Tod.

1. *Olk. R jakorengas. Olk. $a, b \in \mathbb{R},\ a, b, \neq 0$. Tällöin a:lla ja b:llä on käänteisalkiot kertolaskun suhteen: Jos $ab = 0$, niin $b = a^{-1}ab = a^{-1}0 = 0$, mikä on ristiriita. Kunta on kommutatiivinen ja siinä ei siis ole nollan jakajia, joten se on kokonaisalue.*

2. *Olk. E äärellinen kokonaisalue. Kuvaus*

$$V_a : E \to E,\ V_a(b) = ab$$

on injektio $\forall\ a \in E\backslash\{0\}$. Osoitetaan tämä:

Jos $V_a(x) = V_a(y)$, niin $0 = V_a(x) - V_a(y) = ax - ay = a(x - y) \Leftrightarrow a = 0$ tai $x - y = 0$. Oletuksen nojalla $a \neq 0 \Rightarrow x - y = 0 \Leftrightarrow x = y$.

Koska E on äärellinen joukko, niin kuvaus V_a on surjektio $\forall a \in E,\ a \neq 0$. Siis $\forall a \in E,\ a \neq 0$ on $\overline{a} \in E$ s.e.

$$a\overline{a} = V_a(\overline{a}) = 1 \quad \forall\ a \in E.$$

Koska E on kommutatiivinen, niin $a^{-1} = \overline{a}$. Siis E on kommutatiivinen rengas, $\#E \geqslant 2$, ja kaikki $E\backslash\{0\}$:n alkiot ovat yksiköitä (siis E on jakorengas määritelmän 5.2.3 nojalla).

Luku 6

Rengasformalismin soveltaminen kokonaislukuryhmiin

Tässä luvussa puhumme renkaista $\mathbb{Z}$ ja $\mathbb{Z}_p$.

6.1 Alkua

Määritelmä 6.1.1 *1. Jos luku $d \in \mathbb{Z}$ jakaa luvut $a, b, \in \mathbb{Z}$, niin d on a:n ja b:n* yhteinen tekijä.

2. *Jos $m, n \in \mathbb{Z}\backslash\{0\}$, niiden suurin yhteinen tekijä on positiivinen kokonaisluku d s.e.*

   - *d jakaa m:n ja n:n*
   - *Jos y on m:n ja n:n yhteinen tekijä, niin y jakaa d:n.*

   Merkitään suurinta yhteistä tekijää $syt(m, n)$:llä.

3. *Jos $syt(m, n) = 1$, niin m ja n ovat* keskenään jaottomia suhteellisia alkulukuja.

4. *Kokonaisluku $p \geqslant 2$ on* alkuluku, *jos $\forall\ m, n \in \mathbb{N}$ s.e. $mn = p$ pätee $m = 1$ tai $n = 1$.*

Lemma 6.1.1 *Luvuilla $a, b \in \mathbb{Z}$ on yksikäsitteinen suurin yhteinen tekijä,*

$$syt = MAX\{d \in \mathbb{N} \mid d|a \ \ ja \ \ d|b\}.$$

Tod.

Selvästi $syt(a,b)$ on kyseinen luku, jos se on olemassa. 1 on lukujen a ja b yhteinen tekijä. Olk.

$$A = \{d \in \mathbb{N} \mid d|a \ \ ja \ \ d|b\}\,.$$

Jos $k \in A$, niin $k \leqslant min\{a,b\}$ joten sillä on maksimi, joka on siis $syt(a,b)$.

□

Propositio 6.1.1 *Olkoon $m,n \in \mathbb{Z}\backslash\{0\}$. Tällöin $syt(m,n)$ virittää aliryhmän $\langle m,n\rangle$.*
Tod.

Muista:

$$\langle m,n\rangle = \{am+bn \mid a,b \in \mathbb{Z}\}\,.$$

HUOMAUTUS. Ryhmän $\mathbb{Z}$ alkioiden monikerrat am vastaavat renkaan $\mathbb{Z}$ alkioiden a ja m tuloja am. Aiemmin osoitettiin, että on $d \in \mathbb{N}$ s.e. $\langle d\rangle = \langle m,n\rangle$. Osoitetaan, että $d = syt(m,n)$.

Olk. c lukujen m ja nyhteinen tekijä[1]*. On siis $a,b \in \mathbb{Z}$ s.e. $m = ac$ ja $n = bc$. Koska $d \in \langle m,n\rangle$, niin on $r,s \in \mathbb{Z}$ s.e.*

$$(*) \qquad d = rm + sn.$$

Siis

$$d = rm + sn = rac + sbc = (ra+sb)c,$$

eli c on d:n tekijä (jakaa d:n) $\Rightarrow d = syt(m,n)$.

□

HUOMAUTUS.

1. Yhtälöä $(*)$ kutsutaan *Bezout'n* yhtälöksi.
2. Suurin yhteinen tekijä voidaan määritellä myös useammalle kokonaisluvulle $m_1, m_2, \ldots, m_n,\ m_i \in \mathbb{Z}\backslash\{0\}$.

Esimerkki 6.1.1 *1. (a) Luvun $12 \in \mathbb{Z}$ tekijät ovat $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12$.*

(b) Luvun $30 \in \mathbb{Z}$ tekijät ovat : $\pm1, \pm2 \pm 3, \pm5, \pm6, \pm10, \pm15, \pm30$. Suurin yhteinen tekijä on $syt(12,30) = 6$.

[1]Huomaa, että *c* on lukujen *m* ja *n mielivaltainen* yhteinen tekijä: *c* jakaa *d*:n kaikilla *c*, jotka ovat yhteisiä tekijöitä.

2. $syt(n, n+1) = 1\ \forall n \in \mathbb{N}$; *Olkoon d n:n ja n + 1:n jakaja. Tällöin d jakaa luvun* $(n+1) + (-1)n = 1$, *joten* $d = \pm 1$. *Siis* $D = syt(n, n+1) = 1$.

3. *Alkulukuja (esim. 2,3,5,7,...) on äärettömän monta (HT).*

Seuraavaan lemmaan perustuva *Eukleideen* algoritmi antaa kahden kokonaisluvun *syt*:n.

Lemma 6.1.2 *Jos* $a, b, q, r \in \mathbb{Z}\backslash\{0\}$, *ja* $a = qb + r$, *niin* $syt(a, b) = syt(b, r)$.

Tod.

Jos d on lukujen b ja r tekijä, niin d on a:n tekijä. Toisaalta, jos d' *on a:n ja b:n tekijä, niin se on luvun* $r = a - qb$ *tekijä. Siis pareilla* a, b *ja* b, r *on samat tekijät. Erityisesti siis syt on sama.*

□

6.2 Eukleideen algoritmi ja sen käyttöä

EUKLEIDEEN ALGORITMI

Olk. $a,\ b = r_0 \in \mathbb{Z}\backslash\{0\}$. Olk. $d = syt(a, b)$. Huomaa, että

$$syt(a, b) = syt(-a, b) = syt(a, -b) = syt(-a, -b),$$

joten VOE $a, b \in \mathbb{N}\backslash\{0\}$. Olkoon $a > b$. Tällöin on $q_1,\ r_1 \in \mathbb{N}$ s.e.

$$a = q_1 b + r_1$$

ja $0 \leqslant r_1 < b$.

Jos $r_1 = 0$, niin $b|a \Rightarrow syt(a, b) = b$ ja lopetetaan. Jos $r_1 > 0$, on $q_2,\ r_2 \in \mathbb{N}$ s.e.

$$b = q_2 r_1 + r_2,$$

$0 \leqslant r_2 < r_1$. Edellisen lemman nojalla $syt(a, b) = syt(b, r_1)$.

Jos $r_2 = 0$, niin $r_1 = syt(b, r_1) = syt(a, b)$ ja lopetetaan. Jos $r_2 > 0$, jatketaan.

Jakojäännökset $r_1, r_2, \ldots$ muodostavat aidosti vähenevän jonon luonnollisia lukuja, joten on $n \in \mathbb{N}$ s.e. $r_n = 0$. Lopussa vaiheet ovat

$$r_{n-3} = q_{n-1}r_{n-2} + r_{n-1}$$
$$r_{n-2} = q_n r_{n-1} + r_n = q_n r_{n-1}.$$

Propositio 6.2.1 *Olkoon a, b ja $r_1, \ldots, r_n$ kuten Eukleideen algoritmissa. Tällöin*

$$syt(a, b) = r_{n-1}.$$

Tod.

$syt(a, b) = syt(b, r_1) = syt(r_1, r_2) = \ldots = syt(r_{n-2}, r_{n-1})$
$\Rightarrow r_{n-1}|r_{n-2} \Rightarrow syt(r_{n-1}, r_{n-2}) = r_{n-1}$.

□

Esimerkki 6.2.1 *Määrätään $syt(22, 60)$ Eukleideen algoritmilla.*

$$60 = 2 \cdot 22 + 16$$
$$22 = 16 + 6$$
$$16 = 2 \cdot 6 + 4$$
$$6 = 4 + 2$$
$$4 = 2 \cdot 2$$

Siis $syt(22, 60) = 2$.

$$2 = 6 - 4 = 6 - (16 - 2 \cdot 6) = 3 \cdot 6 - 16 = 3(22 - 16) - 16 = 3 \cdot 22 - 4 \cdot 16$$
$$= 3 \cdot 22 - 4(60 - 2 \cdot 22) = 11 \cdot 22 - 4 \cdot 60.$$

Peruuttamalla Eukleideen algoritmissa vaiheesta $r_{n-3} = q_n r_{n-2} + r_{n-1}$ saadaan selville *Bezout'n* yhtälössä esiintyvät kertoimet.

Propositio 6.2.2 *Olkoon $a, b \in \mathbb{Z}\backslash\{0\}$ keskenään jaottomia. Tällöin*

1. *jos $a|c$ ja $b|c$, niin $ab|c$.*
2. *jos $a|bc$, niin $a|c$.*

Tod.

Nyt $syt(a, b) = 1$ (Huomaa: jos $a = b = c = 2$, niin $a|c$ & $b|c$, $ab = 4 \nmid 2 = c$. Jos $a = b = 2$ ja $c = 3$, niin $a|bc$ mutta $a \nmid c$.).

1. *Bezout:* $\exists\ x, y \in \mathbb{Z}$ *s.e.* $ax + by = 1$. *Oletetaan, että* $\exists\ k, l \in \mathbb{Z}$ *s.e.* $c = ka = lb$. *Nyt*

$$c = c(ax + by) = cxa + cyb = lbxa + kayb = ab(lx + ky).$$

2. *Kuten edellisessä,*

$$c = cxa + cyb = \ldots = a(xc + kyb).$$

Koska $a|a$ *ja* $a|bc$, *niin* $a|c$.

□

Lemma 6.2.1 *(Eukleideen lemma) Olkoon* p *alkuluku s.e.* $p|ab$. *Tällöin* $p|a$ *tai* $p|b$. *Jos* $p|a_1a_2\cdots a_n$, $a_i \in \mathbb{Z}$, *niin* $p|a$ *jollakin* $i \in \{1, 2, \ldots, n\}$.

<u>*Tod.*</u>

Todistetaan tapaus $p|ab$. *Yleinen tulos seuraa tästä induktiolla. Jos* $p|a$, *ok. Muuten* $syt(a, p) = 1$. *Propositiosta 6.2.2 seuraa, että* $p|b$.

□

Lause 6.2.1 *(Aritmetiikan peruslause) Jokainen luonnollinen luku joka on suurempi tai yhtäsuuri kuin 2 voidaan esittää alkulukujen tulona. Tämä esitys on tekijöiden järjestystä vaille yksikäsitteinen.*

HUOMAUTUS. *Jos jaollisuutta käsitellään esimerkiksi parillisten kokonaislukujen joukossa*

$$\{\ldots, -4, -2, 0, 2, 4, 6, \ldots\},$$

luvuilla on useampia esityksiä "alkulukujen" tulona: $180 = 6 \cdot 30 = 10 \cdot 18$.

<u>*Tod.*</u>

Olemassaolon todistaminen jätetään harjoitukseksi. Yksikäsitteisyys: Olk. $n \in \mathbb{N}$, $n \geqslant 2$. *Olk.* $p_1, \ldots, p_r$, $q_1, \ldots, q_s$ *alkulukuja s.e.* $p_1p_2\cdots p_r = q_1q_2\cdots q_s$. *Nyt* $p_1|q_1q_2\cdots q_s$. *Eukleideen lemman nojalla* $p_1 = q_i$ *jollekin* i; *voidaan olettaa, että* $q_i = q_1$. *Supistamalla* $p_2\cdots p_r = q_2\cdots q_s$ *ja jatkamalla kuten edellä saadaan* $p_2 = q_2$. *Jatketaan prosessia edelleen; koska siinä esiintyy vain luonnollisia lukuja ja* $p_k\cdots p_r > p_{k-1}\cdots p_r$, *niin prosessi päättyy ja saadaan* $p_i = q_i\ \forall i$. *Erityisesti siis* $r = s$.

□

Määritelmä 6.2.1 *Aritmetiikan peruslauseen antamaa luvun $n \in \mathbb{N}, n \geqslant 2$ esitystä*

$$n = p_1 \cdots p_k,$$

missä $p_1, \ldots, p_k$ ovat alkulukuja, sanotaan luvun n alkutekijäesitykseksi. *Luvut $p_1, \ldots, p_n$ ovat luvun n alkutekijöitä.*

Lemma 6.2.2 *Luku $n \in \mathbb{N}, n \geqslant 2$ ei ole alkuluku, joss on alkuluku p jolle $p^2 \leqslant 2$ ja joka jakaa luvun n.*

□

Esimerkki 6.2.2 $11^2 < 132 < 12^2$, *joten luvulla 132 on alkutekijä joka on korkeintaan 11 lemman 6.2.2 nojalla. Itse asiassa*

$$132 = 12 \cdot 11 = 3 \cdot 4 \cdot 11 = 2^2 \cdot 3 \cdot 11$$
$$132 = 2 \cdot 66 = 2 \cdot 6 \cdot 11 = 2^2 \cdot 3 \cdot 11.$$

Lause 6.2.2 *Seuraavat ovat yhtäpitäviä:*

1. *$\mathbb{Z}_p$ on kokonaisalue*
2. *$\mathbb{Z}_p$ on kunta*
3. *p on alkuluku.*

Tod.

On aiemmin todistettu, että kunta on kokonaisalue (propositio 5.2.4). Siispä ehdot 1 ja 2 ovat yhtäpitäviä. Osoitetaan nyt, että $1 \Leftrightarrow 3$.

Olkoon $x, y \in \mathbb{Z} \backslash p\mathbb{Z}$ ($p\mathbb{Z} = \{z \in \mathbb{Z} \mid z = pq,\ q \in \mathbb{Z}\}$). Nyt

$$[x][y] = [0] \Leftrightarrow xy \in p\mathbb{Z} \Leftrightarrow \exists\, q \in \mathbb{Z} \text{ s.e. } xy = pq \Leftrightarrow p|xy.$$

Siis $\mathbb{Z}_p$ on kokonaisalue joss $\forall\ x, y \in \mathbb{Z}$ pätee

$$p|xy \Rightarrow p|x \text{ tai } p|y. \qquad (*)$$

Proposition 6.2.2 ja Eukleideen lemman nojalla $(*)$ pätee jos p on alkuluku. Jos $p = ab$, niin $(*)$ ei päde kun $x = a$ ja $y = b$.

□

Edellistä todistusta tarkastelemalla saadaan:

Propositio 6.2.3 *$[a] \in \mathbb{Z}_p$ on nollan jakaja $\Leftrightarrow syt(a,p) > 1$.*

□

Propositio 6.2.4 *Olkoon R rengas. Tällöin $\exists$ täsmälleen 1 rengashomomorfismi renkaalta $\mathbb{Z}$ renkaalle R.*

Tod.

Kuvaus $\phi : \mathbb{Z} \to R$,

$$\phi(n) = n1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ kpl}}$$

on rengashomomorfismi:

$$\begin{aligned} \phi(n+m) &= (n+m)1_R = n1_R + m1_R = \phi(n) + \phi(m) \\ \phi(nm) &= nm1_R = n1_R m1_R = \phi(n)\phi(m). \end{aligned}$$

Jos $\psi : \mathbb{Z} \to R$ on rengashomomorfismi, niin

$$\begin{cases} \psi(1) &= 1_R \\ \psi(0) &= 0_R, \end{cases}$$

sillä neutraalilakio kuvautuu neutraalialkioksi. Nyt $\psi(n) = n1_R$ eli $\phi = \psi$.

□

HUOMAUTUS. Ryhmähomomorfismeja $\Phi : \mathbb{Z} \to G$ voi olla useita.

Luku 7

Ideaalit ja tekijärenkaat

7.1 Lähtökohdat

Ryhmähomomorfismin $\phi : G \to G'$ ydin[1] $Ker(\phi)$ on ryhmän G normaali aliryhmä[2]. Rengashomomorfismi $\psi : R \to R'$ on ryhmähomomorfismi additiiviselta ryhmältä $(R, +)$ additiiviselle ryhmälle $(R', +)$, joten sen ydin

$$Ker(\psi) = \{x \in R \mid \psi(x) = 0_{R'}\}$$

varustettuna yhteenlaskulla on ryhmän $(R, +)$ normaali aliryhmä. Rengashomomorfismin ytimellä on muitakin ominaisuuksia.

Määritelmä 7.1.1 *Olkoon R rengas ja olkoon $I \subset R$, $I \neq 0$ s.e. $(I, +)$ on $(R, +)$:n aliryhmä*[3].

1. *I on* vasen ideaali, *jos $xa \in I \; \forall x \in R$ ja $a \in I$.*
2. *I on* oikea ideaali, *jos $ay \in I \; \forall y \in R$ ja $a \in I$.*
3. *I on kaksipuolinen ideaali, jos $xay \in I \; \forall \; x, y \in R$ ja $a \in I$.*

HUOMAUTUS. Jos R on kommutatiivinen, niin kohdat 1-3 määräävät saman käsitteen. Tällöin sanotaan, että I on *ideaali*.

Lemma 7.1.1 1. *I on vasen ideaali $\Leftrightarrow xa + x'a' \in I \; \forall \; x, x' \in R, \; \forall \; a, a' \in I$.*

2. *I on oikea ideaali $\Leftrightarrow ay + a'y' \in I \; \forall \; y, y' \in R, \; \forall \; a, a' \in I$.*

[1] $Ker(\phi) = \{x \in G \mid \phi(x) = e'\}$.
[2] $\forall \; h \in \; Ker(\phi), \; \forall g \in G : \; ghg^{-1} \in \; Ker(\phi)$.
[3] Siis $(I, +)$ on ryhmä ja lisäksi $\forall \; i, j \in I, \; i + j \in I$.

3. *I on kaksipuolinen ideaali* $\Leftrightarrow$ *I on vasen ja oikea ideaali.*

□

Esimerkki 7.1.1 1. $n\mathbb{Z}$ *on* $\mathbb{Z}$*:n ideaali* $(\forall z \in \mathbb{Z},\ nz \in n\mathbb{Z}$ *ja* $zn \in n\mathbb{Z})$.

2. R, $\{0_R\}$ *ovat renkaan* R *kaksipuolisia ideaaleja.*

3. *Olkoon* $X \neq \emptyset$, $A \subset X$, R *rengas. Olk.*

$$N(A) = \{f \in \mathfrak{F}(X,R) \mid f(a) = 0\ \forall a \in A\}.$$

$N(A)$ on kuvausrenkaan $\mathfrak{F}(X,R)$[4] kaksipuolinen ideaali: jos $f, g \in N(A)$, niin $f(a) = 0 = g(a)\ \forall a \in A$; vast. $(-f)(a) = 0$, joten $-f \in N(A)$. Lisäksi

$$(f+g)(a) = f(a) + g(a) = 0 + 0 = 0,$$

joten $(N(A), +)$ on $\mathfrak{F}(X,R)$:n aliryhmä. Edelleen, jos $f \in N(A)$ ja $g \in \mathfrak{F}(X,R)$, niin

$$(fg)(a) = f(a)g(a) = 0 \cdot g(a) = 0\ \forall\ a \in A$$

joten $fg \in N(A)$. Siispä $N(A)$ on oikea ideaali. Vasen ideaali hoituu samalla tavalla. Edellisen lemman nojalla vasen- ja oikeanpuoleinen ideaali on kaksipuolinen.

Toinen tapa:

Jos $f \in N(A)$ ja $g, h \in \mathfrak{F}(X,R)$, niin $\forall a \in A$ on

$$(gfh)(a) = g(a)f(a)h(a) = g(a) \cdot 0 \cdot h(a) = 0.$$

□

Analogisesti saadaan ideaaleja monille $\mathfrak{F}(X,R)$:n alirenkaille; esimerkiksi

$$\{f \in C^\infty(\mathbb{R}) \mid f(0) = 0\}$$

on renkaan $C^\infty(\mathbb{R})$ ideaali.

[4]Joukko, joka koostuu kaikista kuvauksista joukolta X renkaaseen R, ks. esim. 5.1.1.

12.3.2007 $\downarrow$

Propositio 7.1.1 *Olkoon $\phi : R \to S$ rengashomomorfismi.*

1. *Jos $I \in R$ on vasen/oikea/kaksipuolinen ideaali, niin $\phi(I)$ on renkaan $\phi(R)$ vasen/oikea/kaksipuolinen ideaali.*

2. *Jos $I \in S$ on vasen/oikea/kaksipuolinen ideaali, niin $\phi^{-1}(I)$ on renkaan R vasen/oikea/kaksipuolinen ideaali.*

3. *Rengashomomorfismin ϕ ydin on renkaan R kaksipuolinen ideaali.*

Tod.

1. *Harjoitus.*

2. *Tarkastellaan tilannetta, jossa I on vasemmanpuoleinen ideaali; oikean ideaalin tilanne todistetaan analogisesti. Nyt $(\phi^{-1}(I), +)$ on propositio 5.2.3:n nojalla ryhmän $(R, +)$ aliryhmä. Olk. $r \in R, \quad a \in \phi^{-1}(I)$. Tällöin*

$$\phi(ra) = \underbrace{\phi(r)}_{\in S}\underbrace{\phi(a)}_{\in I} \in I,$$

   joten $ra \in \phi^{-1}(I)$.

3. *$Ker(\phi) = \phi^{-1}(\{0\})$ ja $\{0\}$ on S:n kaksipuolinen ideaali, joten väite seuraa kohdasta 2.*

□

Esimerkki 7.1.2 *Luonnollinen kuvaus*

$$\mathbb{Z} \to \mathbb{Z}_p \quad (r \mapsto [r])$$

on rengashomomorfismi. Proposition 7.1.1 mukaan jokaisen $\mathbb{Z}$:n ideaalin kuva luonnollisessa kuvauksessa on $\mathbb{Z}_p$:n ideaali ja jokaisen $\mathbb{Z}_p$:n ideaalin alkukuva on $\mathbb{Z}$:n ideaali.

$\mathbb{Z}$:n ideaalit ovat $N\mathbb{Z}$, $N \in \mathbb{N}$ joten $\mathbb{Z}_p$:n ideaalit ovat $N\mathbb{Z}$:n kuvat luonnollisessa kuvauksessa eli $[N\mathbb{Z}]$, siis jokainen $(\mathbb{Z}_p, +)$:n aliryhmä on $\mathbb{Z}_p$:n ideaali (ja muita ei ole, todistettu aiemmin).

Propositio 7.1.2 *1. Jos renkaan R vasen/oikea/kaksipuolinen ideaali I on alirengas, niin $I = R$.*

2. *Jos R on jakorengas*[5] *ja I on R:n vasen/oikea/kaksipuolinen ideaali, niin $I = R$ tai $I = \{0\}$.*

Tod.

1. *Tarkastellaan tilannetta, jossa I on vasen ideaali. Olk. $x \in R$. Nyt $x = x \cdot 1 \in I$, joten $I = R$.*

2. *$\{0\}$ ja R ovat aina ideaaleja. Jos $0 \neq r \in R$, niin $r^{-1} \in R$, $rr^{-1} = 1, r^{-1}r = 1$. Jos $r \in I$, niin $1 = r^{-1}r \in I$. Ensimmäisen väitteen todistuksen nojalla on $I = R$.*

□

HUOMAUTUS. Proposition 7.1.2 nojalla kunnan (kommutatiivisen jakorenkaan) K ainoat ideaalit ovat $\{0\}$ ja K.

Propositio 7.1.3 *Olkoon $I_1, I_2, I_j,\ j \in J$ renkaan R vasen/oikea/kaksipuoleisia ideaaleja. Tällöin*

$$I_1 + I_2 = \{a_1 + a_2 \mid a_1 \in I_1,\ a_2 \in I_2\} \text{ ja } \cap_{j \in J} I_j$$

ovat R:n vasen/oikea/kaksipuolisia ideaaleja.

Tod. Harjoituksissa.

□

Jos $\emptyset \neq S \subset R$, joukon S virittämä vas/oik/2-puol. ideaali on $\cap_{S \subset I} I$, eli leikkaus niistä R:n vasen/oikea/kaksipuolisista ideaaleista, jotka sisältävät joukon S.

Kaksipuoleinen ideaali vastaa rengasteoriassa normaalia aliryhmää. Koska renkaan R additiivinen ryhmä $(R, +)$ on kommutatiivinen ja R:n ideaalin kommutatiivinen ryhmä $(I, +)$ on $(R, +)$:n aliryhmä, niin se on *normaali* aliryhmä (kommutatiivisuuden nojalla, katso sivu 32). Käyttämällä samaa ekvivalenssirelaatiota kuin luvussa 4 (nyt $\underset{v}{\sim}$ ja $\underset{o}{\sim}$ ovat sama relaatio, ks. 29) muodostetaan renkaan R ideaalia I vastaava tekijäjoukko R/I eli *jäännösluokkarengas* ja varustetaan se tekijälaskutoimituksella[6].

[5] Elikkä jokaisella nollasta poikkeavalla alkiolla on käänteisalkio.

[6] Muistin virkistykseksi sivuluokista: jos $x \sim y,\ x \in R$, niin x:n ekvivalenssiluokka $[x]$ koostuu kaikista niistä alkioista $y \in R$, joille löytyy alkio $z \in I$ s.e. $x^{-1}y = z$ tai $yx^{-1} = z$. Edelleen, tekijäjoukko R/I sisältää kaikki tällaiset ekvivalenssiluokat. Kommutatiivisuus tarkoittaa, että $yx^{-1} = x^{-1}y$, joten voimme soveltaa kumpaa tahansa edellisistä ehdoista (pätee $R/I = I\backslash R$.). Tämä tarkoittaa myös sitä, että I on renkaan R *normaali aliryhmä,* sillä jos nyt $y \in I,\ x \in R$, saamme (kommutatiivisuuden nojalla) $xyx^{-1} = xx^{-1}y = 1 \cdot y = y \in I$.

MERKINTÖJÄ. Ideaalia I vastaavia sivuluokkia merkitään nyt $x + I$. Merkintä xR tarkoittaa x:n monikertoja $\{xr \mid r \in R\}$, ja vastaavasti $Rx = \{rx \mid r \in R\}$.

HUOMAUTUS Laskutoimituksena on nyt (+), joten käänteisalkiot tulee ymmärtää *yhteenlaskun* käänteisalkioina.

Propositio 7.1.4 *Olkoon R rengas ja olk. $I \subset R$ kaksipuolinen ideaali. Tällöin R/I on rengas.*

Tod.

Yhteenlasku on yhteensopiva ekvivalenssirelaation kanssa[7] *(ks. luku 5). Osoitetaan, että kertolasku on yhteensopiva.*

Olk. $a, a', b, b' \in R$ s.e. $a \sim a'$, $b \sim b'$ eli $a - a' \in I$, $b - b' \in I$. Tällöin

$$ab - a'b' = ab - ab' + ab' - a'b' = a\underbrace{(b - b')}_{\in I} + \underbrace{(a - a')}_{\in I} b' \in I,$$

sillä I on kaksipuolinen ideaali. Siispä $ab \sim a'b'$. Loput harjoituksena.

□

Propositio 7.1.5 *1. Tekijärengas $R/I = I\backslash R$ on kommutatiivinen $\Leftrightarrow$ R on kommutatiivinen.*

2. Luonnollinen kuvaus $R \to R/I$, $r \mapsto [r]$ on rengashomomorfismi.

□

Lause 7.1.1 *(Renkaiden isomorfismilause) Olkoon $\psi : R \to S$ rengashomomorfismi. Tällöin tekijärengas $R/Ker(\psi)$*[8] *on isomorfinen renkaan $\psi(R)$ kanssa.*

Tod.

Kuten ryhmien isomorfismilause (Harjoituksissa 9).

---

[7] Ks. sivu 8.

[8]
$$R/Ker(\psi) = \left\{ [x] \mid x,\ y \in R;\ x \sim y \Leftrightarrow \exists\, z \in Ker(\psi) \text{ s.e. } x^{-1}y = z \text{ tai } yx^{-1} = z. \right\}$$

.

Esimerkki 7.1.3 *1.*

$$R/\{0\} \cong R: \ \{0\} = Ker(id).$$

Selvästi

$$R/\{0\} = \left\{ [x] \mid x \sim y \Leftrightarrow x^{-1} + y = 0 \textit{ tai } y + x^{-1} = 0, \ x^{-1} = -x \right\}.$$

Siispä $[x] = x \ \forall x \in R$. *Näiltä lähtökohdilta voidaan todistaa joukkojen isomorfisuus. Vastaavasti*

$$R/R \cong \{0\}: \ R = Ker(0).$$

Tässä 0 on nollahomomorfismi $0 : R \to \{0\}$, $0(r) = 0 \ \forall r \in R$.

2. *Reaaliluvut konstruoidaan luvussa (8) rationaalilukujen Cauchy-jonojen renkaan nollaan suppenevien jonojen ideaalia vastaavana tekijärenkaana.*

HUOMAUTUS. Tekijärengas voi olla kommutatiivinen, vaikka alkuperäinen rengas ei ole kommutatiivinen: R/R on yhden alkion rengas.

Luku 8

Reaaliluvut

8.1 Johdantoa

Jatkamme lukualueiden määrittelyä ja tarkastelua kuten luvussa 2. Käytettävissä: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ja kurssilla tähän mennessä tarkasteltu teoria.

Rationaalilukujen kunta ei ole algebran kannalta riittävä lukualue:

Esimerkki 8.1.1 *Yhtälöllä $x^2 = 2$ ei ole ratkaisua rationaalilukujen kunnassa: jos $x = p|q \in \mathbb{Q}$ s.e. $x^2 = 2$, niin $p^2 = 2q^2$. Nyt yhtälön vasemman puolen mukaan luku 2 esiintyy luvun $p^2 = 2q^2$ alkutekijäesityksessä parillisen monta kertaa. Oikean puolen mukaan 2 esiintyy alkutekijäesityksessä parittoman monta kertaa. Aritmetiikan peruslauseen*[1] *mukaan tämä ei ole mahdollista.*

Määritellään lukualueisiin $\mathbb{Z}$ ja $\mathbb{Q}$ järjestys, joka vastaa "tavanomaista $\mathbb{Z}$:n ja $\mathbb{Q}$:n ajattelua lukusuoran osina". Olkoot

$$\mathbb{Z}_+ = \{[(n,0)] \in \mathbb{Z} \mid n \in \mathbb{N},\ n \geqslant 1\}$$
$$\mathbb{Q}_+ = \{p|q \in \mathbb{Q} \mid p,q \in \mathbb{Z}_+\}$$

Kutsutaan näitä joukkoja *positiivisten kokonaislukujen* ja *positiivisten rationaalilukujen* joukoiksi. Joukot sopivat hyvin yhteen $\mathbb{Z}$:n ja $\mathbb{Q}$:n laskutoimitusten kanssa:

Propositio 8.1.1 *Olkoon K s.e. $K = \mathbb{Z}$ tai $\mathbb{Q}$. Tällöin*

1. $\forall\, a,b \in K_+,\ a+b\ \in K_+$ *ja* $ab \in K_+$.
2. $K = K_+ \cup \{0\} \cup (-K_+)$.

[1] Sanoo, että jokainen luku voidaan esittää alkulukujen tulona.

3. $K_+ \cap (-K_+) = \emptyset$.

4. $\forall\ a \in \mathbb{Q}_+,\ a^{-1} \in \mathbb{Q}_+$.

Tod.

1. *Olkoon* $a = [(m,0)],\ b = [(n,0)] \in \mathbb{Z}_+$. *Tällöin*

$$a + b = [(m+n,0)] \in \mathbb{Z}_+.$$

Vastaavasti $ab = [(mn,0)] \in \mathbb{Z}_+$.

Olkoon $a = p|q,\ b = r|s \in \mathbb{Q}_+$. *Nyt*

$$a + b = \frac{ps + qr}{qs}.$$

Edellisen nojalla $ps,\ qr,\ ps + qr\ \in \mathbb{Z}_+$, *joten* $a + b \in \mathbb{Q}_+$. *Kertolasku vastaavasti.*

□

Nyt määritellään joukkoihin $\mathbb{Z}$ ja $\mathbb{Q}$ relaatio $<$ seuraavasti:

$$(\dagger\dagger) \qquad \begin{cases} a < b \Leftrightarrow b - a \in \mathbb{Z}_+ & \forall a, b \in \mathbb{Z} \\ a < b \Leftrightarrow b - a \in \mathbb{Q}_+ & \forall a, b \in \mathbb{Q}. \end{cases}$$

Vastaavasti $a > b \Leftrightarrow b < a$. Määritellään relaatio $\leqslant$:

$$a \leqslant b \Leftrightarrow a < b \text{ tai } a = b.$$

Joukon X relaatio on *osittainen järjestys*, jos se on refleksiivinen (aRa), antisymmetrinen (aRb & $bRa \Rightarrow a = b$) ja transitiivinen ($aRb,\ bRc \Rightarrow aRc$). Jos lisäksi kaikille $a, b \in X$ pätee aRb tai bRa, niin R on *täydellinen järjestys*. Jos $\leqslant$ on täydellinen järjestys joukossa X, niin $(X, \leqslant)$ on täydellisesti järjestetty. Tämä on erikoistapaus yleisemmästä:

Määritelmä 8.1.1 *Olkoon K kokonaisalue. Jos on olemassa $K_+ \subset K$ jolla on proposition 8.1.1 ominaisuudet (1), (2) ja (3), niin K on* järjestetty kokonaisalue. *Jos K on lisäksi kunta, niin se on* järjestetty kunta.

Lemma 8.1.1 *Jos K on järjestetty kunta, niin $x^{-1} \in K_+$ $\forall x \in K_+$.*

Tod.

Selvä tapaus, sillä jos $a \in K_+$, niin $a > 0$ ja siis K_+ ei sisällä yhteenlaskun neutraalialkiota. Koska kunta on kommutatiivinen jakorengas, jokaisella nollasta poikkeavalla alkiolla $x \in K_+$ on käänteisalkio.

□

Propositio 8.1.2 *Lausekkeen (††) avulla määriteltynä relaatio $\leqslant$ on täydellinen järjestys järjestetyssä kokonaisalueessa.*

□

Määritelmä 8.1.2 *Olkoon $(X, \leqslant)$ täydellinen järjestetty joukko. Olkoon $A \subset X$. Alkio $x \in X$ on joukon A* yläraja, *jos $a \leqslant x$ $\forall a \in A$. Alkio x_0 on joukon A pienin yläraja, jos $x_0 \leqslant x$ kaikilla joukon A ylärajoilla x. Vastaavasti määritellään joukon A alaraja ja suurin alaraja.*

Usein pieneintä ylärajaa sanotaan joukon A *supremumiksi* ja suurinta alarajaa joukon A *infimumiksi.*

Esimerkki 8.1.2 *Joukolla*

$$A = \left\{ x \in \mathbb{Q} \mid x^2 < 2 \right\}$$

ei ole pienintä ylärajaa joukossa $\mathbb{Q}$: ($0 \in A$, joten $A \neq \emptyset$, $x \in A \Rightarrow x \leqslant 2$.) Millekään $x \in \mathbb{Q}$ ei päde $x^2 = 2$ (ks. esim. 8.1.1). Jos $a = \frac{p}{q}$, niin $\frac{p^2}{q^2} < 2$.

Suurilla $n \in \mathbb{N}$ pätee

$$1 < \left(1 + \frac{1}{n}\right)^2 < \frac{2q^2}{p^2},$$

joten luvulle $b = (1 + \frac{1}{n})\frac{p}{q}$ pätee $b^2 = (1 + \frac{1}{n})^2 \frac{p^2}{q^2}$, ja $2 > b > a$. Siis a ei ole joukon A yläraja. Samaan tapaan osoitetaan, että mikään joukon

$$B = \left\{ x \in \mathbb{Q} \mid x^2 > 2 \right\}$$

alkio ei ole joukon A pienin yläraja.

Edellinen esimerkki osoittaa, että järjestetyssä kunnassa $\mathbb{Q}$ on "reikiä." Laajennetaan $\mathbb{Q}$ kunnaksi $\mathbb{R}$ (reaaliluvut) "arvioimalla" lukua $\sqrt{2}$ rationaalilukujen jonolla, joka "suppenee kohti lukua $\sqrt{2}$." Haluamme, että $\mathbb{R}$ on järjestetty kunta, joka laajentaa $\mathbb{Q}$:n järjestettynä kuntana: $\mathbb{Q}$ tulkitaan $\mathbb{R}$:n osaksi siten, että alkioiden järjestys säilyy ja laskutoimitukset säilyvät.

Tarkastellaan ensin rationaalilukujen jonoja. Olkoon

$$I(\mathbb{Q}) = \{(a_k)_{k=1}^{\infty} \mid a_k \in \mathbb{Q}\}.$$

Määritellään yhteenlasku ja kertolasku joukossa $I(\mathbb{Q})$ termeittäin: jos

$$\alpha = (a_k)_{k=1}^{\infty},\ \beta = (b_k)_{k=1}^{\infty} \in I(\mathbb{Q}),$$

niin

$$\alpha + \beta = (a_k + b_k)_{k=1}^{\infty}$$
$$\alpha\beta = (a_k b_k)_{k=1}^{\infty}.$$

Jonot ovat kuvauksia $\alpha : \mathbb{N} \to \mathbb{Q}$, $\alpha(n) = a_n$, joten $I(\mathbb{Q})$ on rengas edellä määritellyin laskutoimituksin varustettuna. Yhteenlaskun neutraalialkio on $0 = 0, 0, 0, 0, \ldots$ ja kertolaskun $1 = 1, 1, 1, 1, \ldots$

HUOMAUTUS. Rengas $I(\mathbb{Q})$ ei ole kunta; Olk.

$$a_k = \begin{cases} 1, & \text{kun } k = 1 \\ 0, & \text{kun } k \neq 1. \end{cases} \qquad b_k = \begin{cases} 1, & \text{kun } k = 2 \\ 0, & \text{kun } k \neq 2. \end{cases}$$

Tällöin jonoilla $(a_k)_{k=1}^{\infty}$ ja $(b_k)_{k=1}^{\infty}$ei ole käänteisalkoita kertolaskun suhteen: niissä esiintyy nollia. $I(\mathbb{Q})$ ei ole kokonaisalue:

$$(a_k)_{k=1}^{\infty} \cdot (b_k)_{k=1}^{\infty} = (a_k b_k)_{k=1}^{\infty} = (o)_{k=1}^{\infty}.$$

Määritelmä 8.1.3 *Olkoon K järjestetty kokonaisalue. Olkoon K_+ K:n positiivisten alkioiden joukko. Alkion $x \in K$ itseisarvo on*

$$|x| = \begin{cases} x, \text{ jos } x \in K_+ \\ 0, \text{ jos } x = 0 \\ -x, \text{ jos } x \in K \backslash (K_+ \cup \{0\}) \end{cases}$$

Propositio 8.1.3 *Olkoon K järjestetty kokonaisalue. Tällöin*

1. $|x| = 0 \Leftrightarrow x = 0.$
2. $|x - y| \leqslant |x - z| + |z - y| \qquad \forall\, x, y, z \in K.$
3. $|xy| = |x||y| \qquad \forall\, x, y, \in K.$

8.2 Reaalilukujen konstruktio ja Cauchyn jonot

Määritelmä 8.2.1 1. *Jono* $(a_k)_{k=1}^{\infty} \in I(\mathbb{Q})$ *on* rajoitettu, *jos on* $M \in \mathbb{Q}_+$ *s.e.*

$$|a_k| \leqslant M \quad \forall\, k \in \mathbb{N}.$$

2. *Jono* $(a_k)_{k=1}^{\infty} \in I(\mathbb{Q})$ *on* Cauchyn jono, *jos kaikilla* $\varepsilon \in \mathbb{Q}_+$ *on* $N \in \mathbb{N}$ *s.e.*

$$|a_n - a_m| < \varepsilon,$$

kun $n, m \geqslant N$.

3. *Jono* $(a_k)_{k=1}^{\infty} \in I(\mathbb{Q})$ suppenee *kohti lukua* $a \in \mathbb{Q}$, *jos* $\forall \varepsilon \in \mathbb{Q}_+$ *on* $N \in \mathbb{N}$ *s.e.*

$$|a_n - a| < \varepsilon,$$

kun $n \geqslant N$. *Luku* a *on jonon* $(a)_{k=1}^{\infty}$ raja-arvo, *merkitään*

$$a_k \underset{k\to\infty}{\to} a, \quad \lim_{k\to\infty} a_k = a, \quad a_k \to a, \text{ kun } k \to \infty.$$

Määritelmä yleistyy järjestetyille kokonaisalueille K (korvaa $\mathbb{Q}$ $(\mathbb{Q}_+)$ edellä K (K_+):lla). Tätä yleistä määritelmää käytetään reaalilukujonojen yhteydessä. Edellä määritellyt käsitteet liittyvät toisiinsa:

Propositio 8.2.1 1. *Suppeneva jono on Cauchyn jono.*

2. *Cauchyn jono on rajoitettu.*

Tod. (1)

Olkoon $(a_k)_{k=1}^{\infty}$ *suppeneva jono. Olkoon* $\varepsilon \in \mathbb{Q}_+$. *Tällöin on* $a \in \mathbb{Q}$ *ja* $N \in \mathbb{N}$ *s.e.*

$$|a_k - a| < \frac{\varepsilon}{2}, \text{ kun } k \geqslant N.$$

Olkoon $m, n \geqslant N$. *Tällöin*

$$|a_m - a_n| \leqslant |a_m - a| + |a_n - a| < \varepsilon.$$

Siis $(a_k)_{k=1}^{\infty}$ *on Cauchyn jono.*

□

HUOMAUTUS. Monet rationaalilukujen Cauchyn jonot eivät suppene kunnassa $\mathbb{Q}$. Esimerkiksi jono

$$1 = \frac{1}{1},\ 2 = \frac{2}{1},\ \frac{3}{2},\ \frac{5}{3},\ \frac{8}{5},\ \frac{13}{8},\ldots$$

joka jatkuu säännöllä

$$\frac{p_{n+2}}{q_{n+2}} = \frac{p_n + p_{n+1}}{q_n + q_{n+1}},$$

on rationaalilukujen Cauchy-jono, joka ei suppene kohti mitään rationaalilukua (Todistus: sivuutetaan...). Jono liittyy ketjumurtolukuihin ja geometriaan (kultainen leikkaus).

Olkoon

$$C(\mathbb{Q}) = \{(a_i)_{i=1}^{\infty} \in I(\mathbb{Q}) \mid (a_i)_{i=1}^{\infty} \text{ on Cauchyn jono}\}.$$

Propositio 8.2.2 *Cauchyn jonojen joukko $C(\mathbb{Q})$ on renkaan $I(\mathbb{Q})$ alirengas.*

□

Monet Cauchyn jonot suppenevat samaan pisteeseen:

$$\frac{1}{n} \to 0,\ \frac{1}{2^n} \to 0,\ n \to \infty.$$

Emme halua määritellä reaalilukuja suoraan rationaalilukujen Cauchyn jonojen avulla. Sitä paitsi jonoilla, joissa esiintyy nollia, ei ole käänteisalkiota kertolaskun suhteen.

Määritelmä 8.2.2 *Rationaalilukujen Cauchyn jono $(a_i)_{i=1}^{\infty}$ on* nollajono, *jos $a_i \to 0$, kun $i \to \infty$. Merkitään nollajonojen joukkoa $\mathfrak{N}(\mathbb{Q})$:lla.*

Lemma 8.2.1 *$\mathfrak{N}(\mathbb{Q})$ on renkaan $C(\mathbb{Q})$ ideaali.*

Tod.

Cauchyn jono on rajoitettu $\to \exists\ M \in \mathbb{N}$ *s.e.* $M \geqslant b_j\ \forall\ j \in \mathbb{N}$. *Olkoon* $(a_i)_{i=1}^{\infty} \in \mathfrak{N}(\mathbb{Q})$. *Nyt* $a_i b_i \leqslant a_i M \underset{i\to\infty}{\longrightarrow} 0$, *joten* $(a_i)_{i=1}^{\infty}(b_j)_{j=1}^{\infty} \in \mathfrak{N}(\mathbb{Q})$.

□

Määritelmä 8.2.3 Reaaliluvut *ovat tekijärengas*[2]

$$\mathbb{R} = C(\mathbb{Q})/\mathfrak{N}(\mathbb{Q}).$$

Reaaliluku on siis rationaalilukujen Cauchyn jonojen ekvivalenssiluokka; jonot $(a_k)_{k=1}^{\infty}$ ja $(b_k)_{k=1}^{\infty}$ ovat ekvivalentteja täsmälleen silloin kun niiden erotus (laskutoimituksena +) on nollajono:

$$(a_k)_{k=1}^{\infty} \sim (b_k)_{k=1}^{\infty} \Leftrightarrow a_k - b_k \underset{k\to\infty}{\longrightarrow} 0.$$

Reaalilukujen yhteenlaskun neutraalialkio on $0 = [(0)_{k=1}^{\infty}]$, ja kertolaskun neutraalialkio on $1 = [(1)_{k=1}^{\infty}]$. Myös jonot $\left(\frac{1}{k}\right)_{k=1}^{\infty}$ ja $\left(\frac{1}{2^k}\right)_{k=1}^{\infty}$ esittävät reaalilukua 0.

Lause 8.2.1 *Reaalilukujen rengas on kunta.*

Tod.

Lemma 1.2.1 $\Rightarrow \mathbb{R}$ *on kommutatiivinen, joten sen tekijälaskutoimitus on myös kommutatiivinen. Osoitetaan, että jokaisella* $x \in \mathbb{R}\backslash\{0\}$ *on käänteisalkio kertolaskun suhteen: Olk.* $x \in \mathbb{R}\backslash\{0\}$. *Tällöin on luvut* $a_k \in \mathbb{Q}^*$, $k = 1, 2, \ldots$ *s.e.* $x = [(a_k)_{k=1}^{\infty}]$. *Jono* $\left(\frac{1}{a_k}\right)_{k=1}^{\infty}$ *on Cauchyn jono: Olkoon* $\varepsilon > 0$. *Tällöin on* $N \in \mathbb{N}$, $q \in \mathbb{Q}_+$ *s.e.*

$$a_m,\ a_n > q\ \forall\ m, n \geqslant N.$$

Siis

$$\left|\ \frac{1}{a_m} - \frac{1}{a_n}\right| = \left|\frac{a_n - a_m}{a_m a_n}\right| < \frac{|a_n - a_m|}{q^2},$$

joka saadaan pieneksi valitsemalla m, n *riittävän suuriksi. Nyt*

$$[(a_k)_{k=1}^{\infty}] \cdot \left[\left(\frac{1}{a_k}\right)_{k=1}^{\infty}\right] = 1.$$

Siis täytyy olla

$$\left[\left(\frac{1}{a_k}\right)_{k=1}^{\infty}\right] = x^{-1}.$$

□

[2] $C(\mathbb{Q})/\mathfrak{N}(\mathbb{Q}) = \left\{[x] \mid x \sim y \Leftrightarrow \exists z \in \mathfrak{N}(\mathbb{Q}) \text{ s.e. } x^{-1}y = z\right\}$.

Olkoon

$$\mathbb{R}_+ = \{[(a_k)_{k=1}^{\infty}] \in \mathbb{R} \mid \text{on } n \in \mathbb{N},\ q \in \mathbb{Q}_+ \text{ s.e. } a_k > q \quad \forall k \geqslant n.\}$$

Positiivisten reaalilukujen joukko $\mathbb{R}_+$ on hyvin määritelty, sillä kaikille jonon $(a_k)_{k=1}^{\infty}$ ekvivalenteille jonoille $(b_k)_{k=1}^{\infty}$ on $n' \in \mathbb{N}$ s.e.

$$|a_k - b_k| < \frac{q}{2}$$

kun $k \geqslant n'$. Joten riittävän suurille k pätee $b_k > \frac{q}{2}$ kolmioepäyhtälön nojalla (laske läpi jos ei ole selvä).

Lause 8.2.2 *$\mathbb{R}$ on järjestetty kunta; sen järjestys on täydellinen. Jos K ja K' ovat kuntia ja $\phi : K \to K'$ on rengashomomorfismi, niin ϕ on* kuntahomomorfismi. *Kuvaus*

$$i : \mathbb{Q} \to \mathbb{R}, \quad i(q) = [(q)_{k=1}^{\infty}]$$

on järjestyksen säilyttävä injektiivinen kuntahomomorfismi.

Tod.

Osoitetaan, että joukolla $\mathbb{R}_+$ on propositiossa (8.1.1) luetellut ominaisuudet 1-3:

1. *(Tulon todistus) eli jos $a, b \in \mathbb{R}_+$, niin $ab \in \mathbb{R}_+$. Olkoon*

   $$\alpha = [(a_k)_{k=1}^{\infty}], \quad \beta = [(b_k)_{k=1}^{\infty}]$$

   Siis on $q \in \mathbb{Q}_+$ ja $N \in \mathbb{N}$ s.e. $a_k > q$ ja $b_k > q$, kun $k > N$. Nyt $q^2 \in \mathbb{Q}_+$ ja $a_k b_k > q^2$, kun $k > N$. Siis

   $$\alpha\beta = [(a_k b_k)_{k=1}^{\infty}] \in \mathbb{R}_+.$$

   Summa samaan tapaan.

2. *Olkoon $x \in \mathbb{R} \setminus (\{0\} \cup \mathbb{R}_+)$. Tällöin $a_k \in -\mathbb{Q}_+$ s.e. $x = [(a_k)_{k=1}^{\infty}]$. Nyt $-x = -[(a_k)_{k=1}^{\infty}] \in \mathbb{R}_+$. Edelleen, $a_k < q \in -\mathbb{Q}_+$ suurilla k, joten $-a_k > -q \in \mathbb{Q}_+$ suurilla k.*

3. *Olkoon $x \in \mathbb{R}_+ \cap \mathbb{R}_-$, $x = [(a_k)_{k=1}^{\infty}]$. Silloin (suurilla k) pätee $a_k \in \mathbb{Q}_+$ ja $a_k \in \mathbb{Q}_-$, eli $a_k \in \mathbb{Q}_+ \cap \mathbb{Q}_- = \emptyset$. Tämä on selvä ristiriita, joten $\mathbb{R}$ on järjestetty kunta.*

   Kuvauksen i injektiivisyys on selvä; homomorfisuus harjoituksissa 10.

Osoitetaan, että kuvaus i säilyttää järjestyksen. Olkoon $r, s \in \mathbb{Q}$ s.e. $r < s \Rightarrow s - r \in \mathbb{Q}_+$. Tällöin

$$i(s) - i(r) = [(s)_{k=1}^{\infty}] - [(r)_{k=1}^{\infty}] = [(s-r)_{k=1}^{\infty}].$$

Kaikilla $k \in \mathbb{N}$ pätee

$$s - r > \frac{s-r}{2} \in \mathbb{Q}_+,$$

joten[3] $i(s) - i(r) \in \mathbb{R}_+ \Leftrightarrow i(s) > i(r)$.

□

Sopimus 4 *Samastamme rationaaliluvut vastaavan reaalilukujen osan kanssa.*

Osoitetaan, että luvun alussa käsitellyt analyysin ongelmat korjataan siirtymällä reaalilukuihin.

Lemma 8.2.2 *Olkoon $(c_k)_{k=1}^{\infty} \in C(\mathbb{Q})$ ja olk. $c \in \mathbb{Q}_+$. Jos on $N \in \mathbb{N}$ s.e. $|c_k| < c$ kaikilla $k \geqslant N$, niin*

$$|[(c_k)_{k=1}^{\infty}]| \leqslant c.$$

Huomaa: tässä käytetään vasta tehtyä sopimusta. Nyt voimme verrata reaalilukuja ja rationaalilukuja.

Tod.

Antiteesi; oletetaan, että

$$\gamma = [(c_k)_{k=1}^{\infty}] \in \mathbb{R}_+ \quad ja \quad \gamma > c.$$

Nyt $\gamma - i(c) \in \mathbb{R}_+$. Siispä on $\delta \in \mathbb{Q}_+$, jolle $c_k - c > \delta$ suurilla k. Siis $c_k > c + \delta$ suurilla k. Muut tapaukset vastaavasti.

□

Lemma 8.2.3 *1. Olkoon $\varepsilon > 0$. Tällöin on $\varepsilon' \in \mathbb{Q}_+$ s.e. $0 < \varepsilon' < \varepsilon$.*

2. Olkoon $\varepsilon' \in \mathbb{Q}_+$. Tällöin on $\varepsilon \in \mathbb{R}_+$ s.e. $0 < \varepsilon < \varepsilon'$.

[3] Jos tämä valinta vaikuttaa epämääräiseltä, tarkista positiivisten reaalilukujen määritelmä.

3. *Olkoon* $M \in \mathbb{R}_+$, $\varepsilon \in \mathbb{R}_+$. *Tällöin on* $N \in \mathbb{N}$ *s.e.*

$$0 < \frac{M}{N} < \varepsilon.$$

□

Propositio 8.2.3 *Olkoon* $(a_k)_{k=1}^{\infty} \in C(\mathbb{Q})$. *Jono* $(a_k)_{k=1}^{\infty}$ *suppenee reaalilukujen järjestetyssä kunnassa. Sen raja-arvo tiedetään; se on* $[(a_k)_{k=1}^{\infty}]$.

Tod.

Tulkitaan rationaaliluku a_k *vakiojonon* $(a_k)_{j=1}^{\infty}$ *luokaksi (*$= i(a_k)$*) (huomaa uusi indeksi). Olkoon* $\varepsilon' \in \mathbb{Q}_+$. *Koska* $(a_k)_{k=1}^{\infty}$ *on Cauchyn jono, on* $N \in \mathbb{N}$ *s.e.* $|a_n - a_m| < \varepsilon'$ *kun* $n, m \geqslant N$. *Olk.* $m \geqslant N$. *Jos*

$$\alpha = [(a_k)_{k=1}^{\infty}],$$

huomaamme:

$$a_m - \alpha = [(a_m)_{j=1}^{\infty}] - [(a_j)_{j=1}^{\infty}] = [(a_m - a_j)_{j=1}^{\infty}]$$

Kun $j \geqslant N$, *Cauchyn ehdon nojalla pätee*

$$|a_m - a_j| < \varepsilon'.$$

Lemmasta 8.2.2 saadaan

$$|a_m - a_j| = |[(a_m - a_j)_{j=1}^{\infty}]| \leqslant \varepsilon'.$$

Väite seuraa tästä ja määritelmästä 8.2.1.

□

Lause 8.2.3 *Jokainen reaalilukujen Cauchy-jono suppenee.*

Tod.

Olkoon $(\alpha_n)_{n=1}^{\infty}$ $\mathbb{R}$*:n Cauchy-jono (* $\alpha_n \in \mathbb{R}_+$*). Nyt* $\alpha_n = [(a_{n,k_n})_{k=1}^{\infty}]$. *Proposition 8.2.3 nojalla* $\exists\, K_n \in \mathbb{N}$ *s.e.*

$$|\alpha_n - i(a_{n,K_n})| < \frac{1}{n} = i\left(\frac{1}{n}\right).$$

Olkoon $q_n = a_{n,K_n}$. *Olkoon* $\varepsilon \in \mathbb{R}_+$. *Koska* $(\alpha_n)_{n=1}^{\infty}$ *on Cauchyn jono, on* $N \in \mathbb{N}$ *s.e.*

$$|\alpha_n - \alpha_m| < \frac{\varepsilon}{3}.$$

Tällöin $\forall\, n, m \geqslant N$,

$$\begin{aligned} |i(q_n) - i(q_m)| &= |i(q_n) - \alpha_n + \alpha_n - \alpha_m + \alpha_m - i(q_m)| \\ &\leqslant |i(q_n) - \alpha_n| + |\alpha_n - \alpha_m| + |\alpha_m - i(q_m)| < \varepsilon. \end{aligned}$$

Siis $(q_n)_{n=1}^{\infty}$ *on* $\mathbb{Q}$*:n Cauchyn jono, joka määrää reaaliluvun*

$$\alpha = [(q_n)_{n=1}^{\infty}] = [(a_{n,K_n})_{n=1}^{\infty}].$$

Olkoon $N_2 \geqslant N$ *s.e.*

$$|\alpha_n - i(q_n)| < \frac{\varepsilon}{2} \qquad \forall n \geqslant N_2.$$

Tällöin

$$|\alpha_n - \alpha| \leqslant |\alpha_n - i(q_n)| + |i(q_n) - \alpha| < \varepsilon$$

isolla n, *joten* $\alpha_n \to \alpha$.

□

Koska $\mathbb{R}$:n kaikki Cauchyn jonot suppenevat, sanotaan, että $\mathbb{R}$ on *täydellinen.*

Lause 8.2.4 *Olkoon* $\emptyset \neq A \subset \mathbb{R}$ *ylhäältä rajoitettu. Tällöin* A*:lla on pienin yläraja.*

Tod.

Olkoon $n \in \mathbb{N},\ n > 1$. *Olk.* $y_n \in \mathbb{Z}$ *pienin kokonaisluku s.e.* $\frac{y_n}{n}$ *on* A*:n yläraja. Tällainen* y_n *on, sillä jokaisella alhaalta rajoitetulla epätyhjällä* $\mathbb{Z}$*:n osajoukolla on suurin alaraja, joka sisältyy ko. joukkoon (yhtäpitävää induktioperiaatteen kanssa). On siis* $x_n \in A$, *jolle*

$$\frac{y_n}{n} - \frac{1}{n} < x_n \leqslant \frac{y_n}{n}.$$

Jono $\left(\frac{y_n}{n}\right)_{n=1}^{\infty}$ *on Cauchyn jono; propositio 8.2.3 sanoo, että*

$$\lim_{n\to\infty} \frac{y_n}{n} = w \in \mathbb{R}.$$

Osoitetaan, että w *on* A*:n pienin yläraja:*

1. *w on yläraja: Jos olisi $x \in A$ s.e. $x > w$, niin $x - w \in \mathbb{R}_+$. (Raja-arvon määritelmän nojalla) on $n \in \mathbb{N}$ (kiinteä) s.e.*

$$\left| w - \frac{y_n}{n} \right| < \frac{x - w}{2}.$$

Tällöin

$$x - \frac{y_n}{n} = x - w + w - \frac{y_n}{n} \geqslant x - w - \left| w - \frac{y_n}{n} \right| \geqslant \frac{x - w}{2}.$$

Erityisesti $x - y_n/n \in \mathbb{R}_+$ eli $x > y_n/n$, joten y_n/n ei ole joukon A yläraja. Tämä on ristiriita.

2. *w on pienin yläraja: Olk. $u < w$. Tällöin on $n \in \mathbb{N}$ s.e*

$$\left| \frac{y_n}{n} - w \right| < \frac{w - u}{4}$$

ja on $a_n \in A$ s.e.

$$\left| \frac{y_n}{n} - a_n \right| < \frac{w - u}{4}.$$

Kuten 1:ssä, saamme

$$\begin{aligned} a_n - u &= w - u + a_n - \frac{y_n}{n} + \frac{y_n}{n} - w \\ &\geqslant w - u - \left| a_n - \frac{y_n}{n} \right| - \left| \frac{y_n}{n} - w \right| \\ &\geqslant \frac{w - u}{2} > 0, \end{aligned}$$

joten $a_n > u$ ja u ei ole joukon A yläraja.

□

HUOMAUTUS. Analyysin kursseilla on tapana ottaa lähtökohdaksi joko

- Suljettujen sisäkkäisten välien periaate: jos $\ldots I_3 \subset I_2 \subset I_1$ ovat suljettuja ja rajoitettuja välejä, joille $\mathfrak{L}(I) \to 0$, niin

$$\cap_{i=1}^{\infty} I_i = \{x\}.$$

- Täydellisyysaksioooma: Jokaisella epätyhjällä ylhäältä rajoitetulla osajoukolla on pienin yläraja.

Nyt nämä ovat lauseita!!!

Esimerkki 8.2.1 *Yhtälöllä $x^2 = 2$ on ratkaisu reaaliluvuissa: olkoo*

$$A = \left\{ x \in \mathbb{R} \mid x^2 < 2 \right\}.$$

Kuten esimerkissä 8.1.2 huomataan, että mikään joukon A alkioista ei ole joukon A yläraja ja ettei mikään joukon

$$B = \left\{ x \in \mathbb{R} \mid x^2 > 2 \right\}$$

alkio ole joukon A pienin yläraja. Tälle luvulle $a \in \mathbb{R}$ pätee siis $a^2 = 2$. Samalla päättelyllä joukon A suurin alaraja on myös yhtälön $x^2 = 2$ ratkaisu.

Lause 8.2.5 *Olkoon $x \in \mathbb{R}_+$, ja olkoon $n \in \mathbb{N}$. Tällöin on olemassa $\sqrt[n]{x} \in \mathbb{R}_+$, jolle pätee $\left(\sqrt[n]{x}\right)^n = x$. Lisäksi, jos $x < y$ niin $\sqrt[n]{x} < \sqrt[n]{y}$ $\forall\, x, y \in \mathbb{R}_+$.*

□

Luku 9

Kompleksiluvuista

9.1 Määrittelyä

Lauseen 8.2.5 mukaan jokaisella positiivisella reaaliluvulla on positiivinen n:s juuri. Sen sijaan esimerkiksi yhtälöllä $x^2 = -1$ ei ole ratkaisua $\mathbb{R}$:ssä, sillä $-1 \notin \mathbb{R}_+$. Toisaalta, jos $a \in \mathbb{R}^*$, $a^2 \in \mathbb{R}_+$. Laajennetaan lukualuetta tämän puutteen korjaamiseksi.

Määritelmä 9.1.1 *Kompleksilukujen joukko $\mathbb{C}$ on $\mathbb{R}^2$ varustettuna laskutoimituksilla*

$$(a,b) + (c,d) = (a+c, b+d)$$
$$(a,b)(c,d) = (ac - bd, ad + bc)$$

Propositio 9.1.1 *$\mathbb{C}$ on kunta: yhteenlaskun neutraalialkio on $(0,0)$ ja kertolaskun $(1,0)$. Kuvaus*

$$j : \mathbb{R} \to \mathbb{C}, \quad j(x) = (x,0)$$

on injektiivinen kuntahomomorfismi.

□

Sopimus 5 *Samaistetaan $\mathbb{R}$ vastaavan $\mathbb{C}$:n osajoukon kanssa.*

Kompleksilukua $i = (0,1)$ kutsutaan *imaginääriyksiköksi.* Jokainen kompleksiluku voidaan kirjoittaa muodossa

$$(a,b) = (a,0) + (0,b) = a + ib,$$

missä käytetään edellistä sopimusta. Kompleksiluvun $z = a + ib$

$$\text{reaaliosa } Re(z) = Re(a+ib) = a \in \mathbb{R}$$
$$\text{imaginääriosa } Im(z) = Im(a+ib) = b \in \mathbb{R}$$
$$\text{kompleksikonjugaatti } \overline{z} = \overline{a+ib} = a - ib.$$

Näillä merkinnöillä kompleksilukujen laskutoimitukset ovat

$$(a+ib)+(c+id) = (a+c)+ib+d)$$
$$(a+ib)(c+id) = (ac-bd)+i(ad+bc).$$

HUOMAUTUS. $i^2 = (0,1)(0,1) = -1$, joten yhtälöllä $x^2 = -1$ on ratkaisu $\mathbb{C}$:ssä.

Määritelmä 9.1.2 *Kompleksiluvun* $z = x + iy$ moduli *(itseisarvo) on*

$$|z| = \sqrt{x^2+y^2} = \sqrt{z\bar{z}}$$

ja se toteuttaa kolmioepäyhtälön.

HUOMAUTUS.

1. Jos $x \in \mathbb{R}$, niin $|x| = |j(x)|$.
2. $z^{-1} = \frac{1}{z} = \frac{\bar{z}}{|z|^2}$.

Määritelmä 9.1.3 *(Napakoordinaattiesitys)*

Kompleksiluku $z = x + iy$ *voidaan esittää muodossa*

$$z = |z|\left(\cos(\theta) + i\sin(\theta)\right),$$

missä θ *on origosta kompleksilukuun* z *vedetyn suoran viivan ja positiivisen x-akselin väliin jäävä kulma vastapäivään mitattuna (piirrä kuva!). Kulmaa* θ *kutsutaan kompleksiluvun* z argumentiksi *ja merkitään usein* $\theta = \arg(z)$.

Propositio 9.1.2 *Olkoon*

$$z = |z|\left(\cos(\phi) + i\sin(\phi)\right), \quad w = |w|\left(\cos(\theta) + i\sin(\theta)\right).$$

Tällöin kompleksilukujen z *ja* w *tulo on*

$$zw = |z||w|\left(\cos(\phi+\theta) + i\sin(\phi+\theta)\right).$$

Tulos yleistyy mielivaltaiselle numeroituvalle määrälle kompleksilukuja: jos $z_k = |z_k|\left(\cos(\theta_k) + i\sin(\theta_k)\right)$, $k = 1, \ldots, N$, *niin*

$$\prod_{k=1}^{N} z_k = \prod_{k=1}^{N} |z_k| \left(\cos(\sum_{k=1}^{N}\theta_k) + i\sin(\sum_{k=1}^{N}\theta_k)\right).$$

□

9.2 Kompleksilukujen juuret ja yhtälöiden ratkaisu

Määritelmä 9.2.1 *Jos $z^k = w$, $k \in \mathbb{N}\backslash\{0\}$, niin z on kompleksiluvun w k. juuri.*

Lemma 9.2.1 *Luvulla $1 \in \mathbb{C}$ on m kappaletta m. juuria.*

Tod.

Olkoon

$$\rho_m = \cos\left(\frac{2\pi}{m}\right) + i\sin\left(\frac{2\pi}{m}\right).$$

Propositiosta 9.1.2 seuraa, että

$$\rho_m^m = \cos(2\pi) + i\sin(2\pi) = 1.$$

Jos $n \in \{1, 2, \ldots, m\}$ niin

$$\rho_m^n = \cos\left(\frac{2\pi n}{m}\right) + i\sin\left(\frac{2\pi n}{m}\right).$$

Edelleen,

$$(\rho_m^n)^m = \cos\left(\frac{2\pi nm}{m}\right) + i\sin\left(\frac{2\pi nm}{m}\right) = 1.$$

□

Propositio 9.2.1 *Jokaisella kompleksiluvulla $z \neq 0$ on m kappaletta m. juuria*

□

Lemma 9.2.2 *Olkoon K järjestetty kokonaisalue. Olkoon $a \in K\backslash\{0\}$. Tällöin $a^2 \in K_+$. Erityisesti $1 \in K_+$.*

Tod.

Nyt $a \in K$, tai $-a \in K$. Siis $a^2 \in K_+$ tai $(-a)^2 \in K_+$. Koska $a^2 = (-a)^2$, niin $a^2 \in K_+$.

□

Propositio 9.2.2 *Kompleksilukujen kunnalla ei ole järjestettyä rakennetta.*

Tod.

Jos $z \neq 0$, niin $z = w^2$ jollekin $w \in \mathbb{C}\backslash\{0\}$ (sillä kuvaus $z \mapsto z^2$ on surjektio). Järjestetyssä kunnassa kaikki neliöt ovat positiivisia (tai nolla jos $z = 0$). Jos $\mathbb{C}$ olisi järjestetty kunta, niin kaikki kompleksiluvut $z \neq 0$ olisivat positiivisia, mikä ei pidä paikkaansa sillä esimerkiksi $i^2 = -1$.

□

Proposition 9.2.1 avulla voidaan ratkaista kaikki ($\mathbb{C}$-kertoimiset) 2.,3. ja 4. asteen polynomiyhtälöt.

Propositio 9.2.3 *Olkoon $a_0,\ a_1 \in \mathbb{C}$. Luvut*

$$z_1 = -\frac{a_1}{2} + \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0} \quad ja \quad z_2 = -\frac{a_1}{2} - \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}$$

ovat yhtälön

$$z^2 + a_1 z + a_0 = 0$$

ratkaisuja (ks. toisen asteen yhtälön ratkaisukaava).

Tod.

Selvästi nähdään, että $(z - z_1)(z - z_2) = z^2 + a_1 z + a_0$, mistä väite seuraa.

□

Emme tarkastele lähemmin 3. ja 4. asteen yhtälöiden ratkaisemista. Kaikki 3. asteen yhtälöt voidaan muuntaa muotoon $z^3 + pz + q = 0$. Jos $u_0,\ v_0 \in \mathbb{C}$ s.e.

$$u_0^3 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} \quad , \quad v_0^3 = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

ja $u_0 v_0 = -p/3$, niin luvut

$$z_1 = u_0 + v_0,\ z_2 = \rho_3 u_0 + \rho_2^3 v_0,\ z_3 = \rho_2^3 u_0 + \rho_3 v_0$$

ovat yhtälön $z^3 + pz + q = 0$ ratkaisuja (ks. lemma 9.2.1).

Neljännen asteen algoritmi on samantapainen. Viidennen ja sitä korkeamman asteen yhtälöille ei ole olemassa ratkaisualgoritmia.

Luku 10

Polynomit

10.1 Polynomeista ja polynomifunktioista

Algebrassa on tapana erottaa toisistaan *polynomin* ja *polynomifunktion* käsitteet.

Sopimus 6

- *X on muodollinen symboli, muuttuja.*
- *Symboli* $-\infty$ *tarkoittaa ääretöntä negatiivista lukua, jolle pätee*

  $-\infty < a \quad \forall a \in \mathbb{Z}.$

  $-\infty + (-\infty) = -\infty.$

  $-\infty + a = -\infty \quad \forall a \in \mathbb{Z}.$

  Mitään muita operaatioita ei ole määritelty symbolille $-\infty$.

Määritelmä 10.1.1 *Olkoon R kommutatiivinen rengas*[1], $n \in \mathbb{N}$, $a_n, a_{n-1}, \ldots, a_0 \in R$.

$$P(X) = \sum_{k=1}^{n} a_k X^k$$

on R-kertoiminen yhden muuttujan polynomi. *Jos* $a_n \neq 0$, *niin* $P(X)$*:n* aste *on* $deg P(X) = n$. *Sovitaan, että* $deg 0 = -\infty$. *R-kertoimisten polynomien joukkoa merkitään* $R[X]$.

[1]Kommutatiivinen rengas $(R, +, \cdot)$ on rengas, jolle myös tulo on kommutatiivinen ja siis $a(b+c) = ab + ac$, $(b+c)a = ba + ca \; \forall \; a, b, c \in R$ ja kertolaskulla on neutraalialkio.

Olkoon

$$P(X) = \sum_{k=0}^{n} a_k X^k \quad , \quad Q(X) = \sum_{k=0}^{m} b_k X^k \ \in R[X],$$

$n \geqslant m$, $b_{m+1}, \ldots, b_n = 0$. *Tällöin polynomien* $P(X)$ *ja* $Q(X)$ *summa ja tulo ovat*

$$(*) \begin{cases} P(X) + Q(X) & = \sum_{k=0}^{n} (a_k + b_k) X^k \\ P(X)Q(X) & = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) X^k. \end{cases}$$

Polynomi $P(X) \in R[X]$ *määrää* polynomifunktion

$$P : R \to R, \ \ P(x) = \sum_{k=0}^{n} a_k x^k.$$

Propositio 10.1.1 *Olkoon* R *kommutatiivinen rengas. Tällöin* $R[X]$ *on kommutatiivinen rengas.*

Tod.

Selvästi polynomit 0 ja 1 ovat $R[X]$*:n yhteen- ja kertolaskun neutraalialkiot. Muut ominaisuudet seuraavat* R*:n kommutatiivisuudesta ja laskutoimitusten määrittelystä.*

□

HUOMAUTUS.

1. Toinen (vähemmän havainnollinen) tapa määritellä polynomit on korvata lauseke $P(X) = \sum_{k=0}^{n} a_k X^k$ jonolla $a_1, a_2, \ldots, a_n, 0, 0, \ldots$ ja määritellä jonojen laskutoimitukset kaavojen $(*)$ mukaan. Tällöin jono $(0, 1, 0, 0, 0, \ldots)$ vastaa symbolia X
(esim. $(0, 1, 0, 0, \ldots)(0, 1, 0, 0, \ldots) = (0, 0, 1, 0, 0, 0, \ldots)$)

2. $(*)$ Määrittelee polynomien tavanomaiset laskutoimitukset.

3. Koska $R[X]$ on kommutatiivinen, polynomien termit voidaan kirjoittaa halutussa järjestyksessä:

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 = \sum_{k=0}^{n} a_k X^k = a_0 + \cdots + a_n X^n.$$

4. Kuvaus, joka liittää polynomiin $P(X) \in R[X]$ polynomifunktion $P \in \mathfrak{F}(R, R)$ on rengashomomorfismi (ks. esim. 5.1.1).

Esimerkki 10.1.1 *Olkoon* $P(X),\ Q(X) \in \mathbb{Z}[X]$,

$$P(X) = 2X^2 + 2, \quad Q(X) = 1 + 2X.$$

Nyt voidaan laskea tulo: saadaan

$$P(X)Q(X) = 4X^3 + 2X^2 + 4X + 2.$$

Edelleen, $deg\,(P(X)Q(X)) = 3 = 2 + 1 = degP(X) + degQ(X)$.

Lemma 10.1.1 *Olkoon* R *kommutatiivinen rengas, Olk.* $P(X), Q(X) \in R[X]$. *Tällöin*

$$deg\,(P(X)Q(X)) \leqslant degP(X) + degQ(X).$$

Tod.

Olk.

$$P(X) = \sum_{k=0}^{n} a_k X^k \quad , \quad Q(X) = \sum_{k=0}^{m} b_k X^k.$$

Tulon $P(X)Q(X)$ *korkeimman asteen termi on* $a_n b_m X^{n+m}$, *jos* $a_n b_m \neq 0$. *Siis* $deg\,(P(X)Q(X)) \leqslant n + m$.

□

Propositio 10.1.2 *Jos* K *on kokonaisalue, niin* $K[X]$ *on kokonaisalue. Tällöin*

$$deg\,(P(X)Q(X)) = degP(X) + degQ(X).$$

Tod.

Olk. $P(X), Q(X) \in K[X]\backslash\{0\}$ *eli* $a_n \neq 0,\ b_m \neq 0$. *Lemman 10.1.1 merkinnöillä tulopolynomin* $P(X)Q(X)$ *korkeimman asteen kerroin on* $a_n b_m \neq 0$. *Olkoon*

$$P(X) = \sum_{k=0}^{n} a_k X^k \quad , \quad Q(X) = \sum_{k=0}^{m} b_k X^k$$

ja $a_n \neq 0 \neq b_m$. *Nyt* $P(X)Q(X) \neq 0$, *koska sillä on kerroin, joka ei ole nolla. Erityisesti*

$$deg\,(P(X)Q(X)) = n + m = deg(P(X)) + deg(Q(X)).$$

□

Esimerkki 10.1.2 *1. Tarkastellaan polynomirengasta $\mathbb{Z}_p[X]$, jätetään polynomien kertoimista (ja muustakin $\mathbb{Z}_p$:n alkoista) ekvivalenssiluokan hakasulut merkitsemättä. Tällä tulkinnalla esimerkin 10.1.1 polynomit antavat esimerkkejä $\mathbb{Z}_p[X]$:n polynomeista kaikilla p.*

2. *Jos kerroinrengas R ei ole kokonaisalue, lemman 10.1.1 kaavassa voi olla erisuuruus. Polynomi $2X$ on nollan jakaja renkaassa $\mathbb{Z}_4[X]$:*

$$2X \cdot 2X = 4X^2 = 0,$$

koska $[4] = [0]$ joukossa $\mathbb{Z}_4$. Tällöin

$$-\infty = deg(2X \cdot 2X) < deg(2X) + deg(2X) = 1 + 1 = 2.$$

3. *Kaksi eri polynomia voi määrätä saman polynomifunktion, jos valitaan sopiva kerroinrengas: Olk. $P(X), Q(X) \in \mathbb{Z}_2[X]$,*

$$P(X) = X,\ Q(X) = X^2.$$

Nyt

$$P(0) = 0 = 0 \cdot 0 = 0^2 = Q(0)$$
$$P(1) = 1 = 1^2 = Q(1).$$

HUOMAUTUS. Polynomirengas ei ole koskaan kunta: Jos kerroinrengas R on kokonaisalue, niin proposition 10.1.2 mukaan vain vakiopolynomit $P(X) = u$, missä $u \in R$ on yksikkö, ovat yksiköitä $R[X]$:ssä. Toisaalta, jos R ei ole kokonaisalue, on $a, b \in R\backslash\{0\}$ s.e. $ab = 0$. Nyt esimerkiksi polynomit $P_a(X) = a$ ja $P_b(X) = b$ ovat nollan jakajia renkaassa $R[X]$: $P(X)Q(X) = ab = 0$.

Jos R ei ole kokonaisalue, niin joillain vakiosta poikkeavilla polynomeilla voi olla käänteisalkio kertolaskun suhteen, esimerkiksi renkaassa $\mathbb{Z}_4[X]$ pätee

$$(2X + 1)(2X + 1) = 4X^2 + 4X + 1 = 1,$$

koska $[4] = [0]$ renkaassa $\mathbb{Z}_4[X]$.

Esimerkki 10.1.3 *Samalla lausekkeella annettujen polynomien jaollisuus riippuu kerroinrenkaasta:*

1. *$(X - 1) \mid (X^2 - 1)$ ja $(X + 1) \mid (X^2 - 1)$ (ensimmäinen jakaa jälkimmäisen) eli löytyy $Q(X) \in R[X]$ s.e. esimerkiksi*

$$(X - 1)Q(X) = X^2 - 1$$

kaikissa polynomirenkaissa $R[X]$:

$$(X - 1)(X + 1) = X^2 - 1.$$

2. $(X+1) \mid (X^2+1)$ *renkaassa* $\mathbb{Z}_2[X]$, *koska* $[-1] = [1]$ $\mathbb{Z}_2$*:ssa.*

3. $(X+1) \nmid (X^2+1)$ *renkaassa* $\mathbb{C}[X]$: *Jos* $(X+1) \mid (X^2+1)$, *niin on* $a, b \in \mathbb{C}$ *s.e.*

$$(X+1)(aX+b) = X^2+1.$$

Nyt toisen ja 0. asteen termejä tarkastellessa huomataan, että $a = 1$ *ja* $b = 1$, *mutta nyt ensimmäisen asteen termit eivät täsmää.*

Jos $a, b \in \mathbb{Z}$ *ja* $a|b$ & $b|a$, *niin* $a = \pm b$. *Polynomeille vastaava tulos on*

Lemma 10.1.2 *Olkoon* $P(X), Q(X) \in R[X]$, *joille*

$$P(X)|Q(X) \text{ ja } Q(X)|P(X).$$

Tällöin on $u \in R^*$, *jolle* $P(X) = uQ(X)$.

□

Olemme käyttäneet kokonaislukujen jakoyhtälöä: Olk. $a, b \in \mathbb{Z}$, $b \neq 0$. Tällöin on yksikäsitteiset $q, j \in \mathbb{Z}$, joille

$$a = qb + j \quad \text{ja} \quad 0 \leqslant j < |b|.$$

Todistetaan vastaava tulos polynomien kolmena versiona.

10.2 Polynomien jakoyhtälö ja sen käyttöä

Propositio 10.2.1 *(JAKOYHTÄLÖ)*

Olk. R kommutatiivinen rengas. Olk. $A(X),\ B(X) \in R[X],\ B(X) \neq 0$ *ja ainakin yksi seuraavista 1-3 voimassa:*

1. $B(X)$*:n korkeimman asteen termin kerroin on 1.*

2. $B(X)$*:n korkeimman asteen termin kerroin on yksikkö.*

3. *R on kunta (kommutatiivinen jakorengas).*

Tällöin on yksikäsitteiset $Q(X),\ J(X) \in R[X]$ *s.e.*

$$A(X) = Q(X)B(X) + J(X), \quad degJ(X) < degB(X).$$

Tod.

(1) Jos $B(X)|A(X)$, niin ei ole mitään todistettavaa. Muuten, olkoon

$$S = \{A(X) - D(X)B(X) \mid D(X) \in R[X]\}.$$

Selvästi $S \neq \emptyset$. Lisäksi $0 \notin S$. [2] *Olkoon*

$$T = degS = \{degP(X) \mid P(X) \in S\}.$$

Olk. $t = minT$. Huomaa: $t \in \mathbb{N}\backslash\{0\}$, sillä $0 \notin S$. Olk. $Q(X) \in R[X]$ s.e.

$$deg(\underbrace{A(X) - Q(X)B(X)}_{J(X)}) = t$$

Olkoon $J(X) = a_tX^t + a_{t-1}X^{t-1} + \ldots + a_0$. Osoitetaan, että $degJ(X) < degB(X)$. Jos olisi $t \geqslant degB(X) = d$, niin

$$J(X) - a_tX^{t-d}B(X) = A(X) - \left(Q(X) + a_tX^{t-d}\right)B(X) \in S$$

ja

$$deg\left(J(X) - a_tX^{t-d}B(X)\right) < degJ(X),$$

koska asteen t termi kumoutuu ($B(X) = X^d + \ldots$). Siis löytyy polynomi $P(X) \in S$ s.e. $deg(P(X)) < deg(J(X))$. Tämä on mahdotonta, sillä $J(X)$:n aste on minimaalinen. Siis on $Q(X)$, $J(X)$ s.e.

$$A(X) = Q(X)B(X) + J(X) \quad \& \quad degJ(X) < degB(X).$$

Osoitetaan yksikäsitteisyys: Jos $\tilde{Q}(X), \tilde{J}(X) \in R[X]$, ovat polynomeja s.e.

$$A(X) = \tilde{Q}(X)B(X) + \tilde{J}(X),$$

niin

$$\left(Q(X) - \tilde{Q}(X)\right)B(X) = \tilde{J}(X) - J(X).$$

Jos $\tilde{Q}(X) \neq Q(X)$, niin $deg\left(Q(X) - \tilde{Q}(X)B(X)\right) \geqslant d$ ja $deg\left(\tilde{J}(X) - J(X)\right) \leqslant t < d$, ristiriita. Siis $\tilde{Q}(X) = Q(X)$ ja $\tilde{J}(X) = J(X)$.

□

Kohdan 2 todistus seuraa edellisestä. Vastaavasti (koska kaikki kunnan nollasta poikkeavat alkiot ovat yksiköitä) saadaan kohdan 2 avulla suoraan kohta 3.

[2] Jos näin olisi, niin olisi myös $B(X)|A(X)$.

Esimerkki 10.2.1 *Jakoyhtälö voidaan toteuttaa algoritmisesti jakokulmassa kuten kokonaisluvuillekin. Renkaassa $\mathbb{Z}[X]$: jos*

$$A(X) = 2X^3 + X^2 - X - 1$$
$$B(X) = X^2 - 2$$

niin

$$\underbrace{2X^3 + X^2 - X - 1}_{A(X)} = (\underbrace{2X + 1}_{Q(X)})(\underbrace{X^2 - 2}_{B(X)}) + \underbrace{3X + 1}_{J(X)}$$

Nyt voidaan laskea jakokulmalasku tavalliseen tapaan ja saadaan tulos.

Samoilla lausekkeilla annetuille polynomeille $A(X),\ B(X) \in \mathbb{Z}_3[X]$ pätee

$$2X^3 + X^2 - X - 1 = (2X + 1)(X^2 - 2) + 1.$$

Jos taas polynomille $B(X) \in \mathbb{Z}[X]$ on $B(X) = 2X + 1$, niin jakoyhtälön oletukset eivät ole voimassa eikä jakoyhtälö toimi: Jakokulmassa päädytään ongelmalliseen tilanteeseen (kokeile niin huomaat):

$$2X^3 + X^2 - X - 1 = X^2(2X + 1) - (X + 1),$$

josta ei voi jakaa. Sen sijaan, jos $A(X),\ B(X) \in \mathbb{Z}_3[X]$, niin oletukset ovat voimassa, sillä $\mathbb{Z}_3[X]$ on kunta. Nyt

$$-X - 1 = 2X - 1 = (2X + 1) - 2,$$

ja päädytään samaan yhtälöön kuin edellä[3] (luonnollisesti, sillä $[-2] = [1]$).

Renkaassa $\mathbb{Q}[X]$ jakoa voi myös jatkaa, ja saadaan

$$2X^3 + X^2 - X - 1 = (X^2 - \frac{1}{2})(2X + 1) - \frac{1}{2}.$$

Määritelmä 10.2.1 *Olkoon R kommutatiivinen rengas, ja olk. $P(X) \in R[X]$. $a \in R$ on polynomin $P(X)$* juuri *eli nollakohta, jos $P(a) = 0$ vastaavalle polynomikuvaukselle.*

Propositio 10.2.2 *Olkoon R kommutatiivinen rengas. Olk. $P(X) \in R[X]$, $c \in R$. Tällöin*

$$P(c) = 0 \Leftrightarrow (X - c)|P(X).$$

[3]Kunnassa $\mathbb{Z}_3$ on $-1 = 2 = 1 + 1 = 1 - 2$.

Tod.

($\Rightarrow$) Jos $P(c) = 0$, niin jakoyhtälön antama polynomi $J(X)$ on vakio[4]*:*

$$P(X) = Q(X)(X - c) + J(X), \quad degJ(X) < 1.$$

Nyt

$$0 = P(c) = Q(c)(c - c) + J(c) = J(c).$$

Koska $J(X) = b$ jollain $b \in R$, niin $b = 0 \Rightarrow J(X) = 0 \Rightarrow P(X) = Q(X)(X - c)$.

($\Leftarrow$) Jos $(X - c)|P(X)$, niin

$$P(X) = Q(X)(X - c),$$

joten $P(c) = Q(c)(c - c) = 0$.

□

Propositio 10.2.3 *Olkoon K kokonaisalue. Olk. $P(X) \in K[X]$ ja olk. $c_1, c_2, \ldots, c_k$ $P(X)$:n juuria. Tällöin on $Q(X) \in K[X]$ s.e.*

$$P(X) = (X - c_1)(X - c_2) \cdots (X - c_k)Q(X).$$

□

Lause 10.2.1 *Olkoon K kokonaisalue. Olk. $n \in \mathbb{N}$. Jos $P(X) \in K[X]$ ja $degP(X) = n$, niin $P(X)$:llä on korkeintaan n juurta.*

Tod.

Propositioiden 10.2.3 ja 10.1.2 mukaan; jos $P(X)$:llä on k juurta, niin $degP(X) \geqslant k$.

□

Propositio 10.2.4 *Olkoon K ääretön kokonaisalue. Tällöin jokaista K:n polynomifunktiota vastaa yksikäsitteinen polynomi renkaassa $K[X]$.*

Tod.

(Siis halutaan osoittaa, että kuvaus $P(X) \mapsto (P : K \to K)$ on injektio) Olk. $P(X)$, $Q(X) \in K[X]$ s.e. $P(c) = Q(c)\ \forall\ c \in K$. Tällöin polynomilla $P(X) - Q(X)$ on äärettömän monta juurta. Edellisen lauseen 10.2.1 mukaan $P(X) - Q(X) = 0 \Rightarrow P(X) = Q(X)$.

[4]Sillä $deg(X - c) = 1$.

□

HUOMAUTUS. Monilla polynomeilla ei ole maksimaalista määrää nollakohtia: esim. polynomilla $X^3 + X \in \mathbb{Z}[X]$ on täsmälleen 1 nollakohta, ja polynomilla $X^2 + 1 \in \mathbb{R}[X]$ ei ole nollakohtia. Sen sijaan polynomilla $X^2 + 1 \in \mathbb{C}[X]$ on kaksi nollakohtaa:

$$X^2 + 1 = (X + i)(X - i).$$

Jos $(X - c)^k | P(X)$, niin c on k-kertainen nollakohta. Polynomien juurten lukumäärä lasketaan yleensä s.e. k-kertaiset nollakohdat lasketaan k kertaa: esimerkiksi 0 on polynomin $X^2 \in \mathbb{Z}[X]$ kaksinkertainen nollakohta.

Renkaassa $\mathbb{C}[X]$ pätee:

Lause 10.2.2 *(ALGEBRAN PERUSLAUSE)*

Jokaisella kompleksikertoisella polynomilla on nollakohta, ja n-asteisella polynomilla on n nollakohtaa.

□