# Algebra

Jouni Parkkonen

## Lukijalle

Tämä moniste perustuu kevään 2007 Algebran kurssiin. Koko materiaali on mahdollista käydä 12 viikon kurssilla, mahdollisesti algebran peruslauseen todistusta lukuunottamatta.

Kurssilla käsitellään algebran peruskäsitteitä ja -rakenteita kuten laskutoimituksia, ryhmiä ja renkaita. Lukualueiden $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ konstruktio esitetään lähtien luonnollisista luvuista.

Kurssin keskeinen tavoite on algebrallisten rakenteiden tarkastelu. En ole käsitellyt joukko-opin operaatioita kuin esimerkkeinä laskutoimituksista. Luonnollisten lukujen aksiomaattinen tarkastelu ei myöskään sisälly tähän kurssiin.

Monisteen lopussa olevan lähdeluettelon kirjat ovat olleet apuna kurssin suunnittelussa. Niiden avulla kiinnostunut lukija voi tutustua algebraan paljon laajemmin kuin tällä kurssilla on voitu tehdä.

Henna Koivusalo auttoi monisteen viimeistelyssä, kiitokset!

## Sisältö

# 1. Laskutoimitukset

Algebra käsittelee laskemista. Osin tämä tarkoittaa "numeroilla laskemista" lukualueissa $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ laskutoimituksilla $+, \cdot$ ja niiden käänteisoperaatioilla $-, /$. Tällä kurssilla keskeisessä osassa on "abstrakti laskeminen", jossa ei tiedetä/välitetä siitä, millä lasketaan, vaan tehdään päätelmiä, kun laskutoimitusten jotkin ominaisuudet tunnetaan.

Epätyhjän joukon $A$ *laskutoimitus* on kuvaus $* : A \times A \to A$. Laskutoimituksen tulosta merkitään yleensä $a * a' = *(a, a')$. Laskutoimitus on siis sääntö, joka liittää kahteen joukon $A$ alkioon $a, a'$ joukon $A$ alkion $a * a'$. Toinen algebrassa usein tarkasteltava operaatio on toiminta: joukon $A$ *toiminta* joukolla $B$ on kuvaus joukolta $A \times B$ joukolle $B$. Tällä kurssilla emme juurikaan käsittele toimintoja, sen sijaan esimerkiksi lineaarialgebrassa ne ovat keskeisellä sijalla, katso esimerkki 1.1.

Esimerkki 1.1. (a) Luonnollisten lukujen yhteen- ja kertolasku ovat laskutoimituksia: $(m, n) \mapsto m + n$, $(m, n) \mapsto mn$.
(b) Joukon $X$ osajoukot muodostavat *potenssijoukon* $\mathscr{P}(X) = \{A \subset X\}$. Joukkojen leikkaus ja yhdiste ovat laskutoimituksia potenssijoukossa $\mathscr{P}(X)$: $(A, B) \mapsto A \cap B$, $(A, B) \mapsto A \cup B$.
(c) Olkoon $X \neq \emptyset$, ja olkoon $\mathscr{F}(X) = \{f \colon X \to X\}$. Kuvausten yhdistäminen on laskutoimitus joukossa $\mathscr{F}(X)$: $(f, g) \mapsto f \circ g$.
(d) Joukko $\mathbb{R}$ toimii vektoriavaruudella $\mathbb{R}^n$: Olkoot $\lambda \in \mathbb{R}$ ja

$$x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n.$$

Toiminta määritellään kuvauksella

$$(\lambda, x) \mapsto \lambda x = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n).$$

Määritelmä 1.2. Joukon $A$ laskutoimitus $*$ on

(1) *assosiatiivinen eli liitännäinen*, jos $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in A$.
(2) *kommutatiivinen eli vaihdannainen*, jos $a * b = b * a$ kaikilla $a, b \in A$.

Joukon $A$ laskutoimitus $*$ on *vasemmalta distributiivinen laskutoimituksen* $\oplus$ *suhteen*, jos $a * (b \oplus c) = (a * b) \oplus (a * c)$ kaikilla $a, b, c \in A$. Se on *oikealta distributiivinen laskutoimituksen* $\oplus$ *suhteen*, jos $(b \oplus c) * a = (b * a) \oplus (c * a)$ kaikilla $a, b, c \in A$. Jos $*$ on oikealta ja vasemmalta distributiivinen laskutoimituksen $\oplus$ suhteen, se on *distributiivinen laskutoimituksen* $\oplus$ *suhteen*. Näitä kutsutaan osittelulaeiksi.

Merkintöjä $+$ ja $\cdot$ käytetään yleisesti eri laskutoimituksille. Merkintää $+$ käytetään kuitenkin ainoastaan kommutatiiviselle laskutoimitukselle. Usein kertolasku merkitään ilman pistettä $a \cdot b = ab$.

Esimerkki 1.3. (a) Luonnollisten lukujen yhteen- ja kertolaskulle pätee

(1) $m + n = n + m$ ja $mn = nm$ kaikilla $m, n \in \mathbb{N}$ (kommutatiivisuus).
(2) $m + (n + l) = (m + n) + l$ ja $m(nl) = (mn)l$ kaikilla $m, n, l \in \mathbb{N}$ (assosiatiivisuus).
(3) $m(n + l) = mn + ml$ kaikilla $m, n, l \in \mathbb{N}$, eli kertolasku on distributiivinen yhteenlaskun suhteen.

(b) Joukon $\mathscr{P}(X)$ laskutoimitukset $\cap$ ja $\cup$ ovat kommutatiivisia: $A \cap B = B \cap A$ ja $A \cup B = B \cup A$ kaikilla $A, B \in \mathscr{P}(X)$.
(c) Joukon $\mathscr{F}(X)$ laskutoimitus $\circ$ on assosiatiivinen: $f \circ (g \circ h) = (f \circ g) \circ h$ kaikilla $f, g, h \in \mathscr{F}(X)$.

MÄÄRITELMÄ 1.4. Olkoon $A \neq \emptyset$, ja olkoon $*$ joukon $A$ laskutoimitus. Alkio $e \in A$ on laskutoimituksen $*$ *neutraalialkio*, jos $e * g = g$ ja $g * e = g$ kaikilla $g \in A$. Alkio $\bar{x} \in A$ on alkion $x \in A$ *vasen käänteisalkio*, jos $\bar{x} * x = e$, ja *oikea käänteisalkio*, jos $x * \bar{x} = e$. Jos $\bar{x}$ on alkion $x$ vasen ja oikea käänteisalkio, niin se on alkion $x$ *käänteisalkio*.

Jos laskutoimituksesta käytetään tulomerkintää, neutraalialkiota merkitään usein 1:llä, ja summamerkintää kaytettäessä 0:lla. Alkion $x$ käänteisalkiota merkitään yleensä $x^{-1}$:llä, summamerkintää käytettäessä kuitenkin käytetään merkintää $-x$.

ESIMERKKI 1.5. (a) 0 on luonnollisten lukujen yhteenlaskun neutraalialkio. 1 on luonnollisten lukujen kertolaskun neutraalialkio. Useimmilla luonnollisilla luvuilla ei ole käänteisalkiota kummankaan laskutoimituksen suhteen.
(b) Identtinen kuvaus $\mathrm{id} = \mathrm{id}_X$ on joukon $\mathscr{F}(X)$ laskutoimituksen $\circ$ neutraalialkio:

$$\mathrm{id} \circ f = f = f \circ \mathrm{id}$$

kaikilla $f \in \mathscr{F}(X)$. Jos $f \in \mathscr{F}(X)$ on bijektio, sen käänteiskuvaus $f^{-1}$ on kuvauksen $f$ käänteisalkio laskutoimituksen $\circ$ suhteen: $f \circ f^{-1} = \mathrm{id} = f^{-1} \circ f$. Muilla joukon $\mathscr{F}(X)$ alkioilla ei ole käänteisalkiota.
(c) Varustamme nyt joukon $X \neq \emptyset$ potenssijoukon laskutoimituksella $\setminus$. Tällöin jokaisella $A \in \mathscr{P}(X)$ pätee $A \setminus \emptyset = A$, joten $\emptyset$ muistuttaa laskutoimituksen $\setminus$ neutraalialkiota. Kuitenkin $\emptyset \setminus A = \emptyset$ kaikilla $A \in \mathscr{P}(X)$, joten $\emptyset$ ei ole laskutoimituksen $\setminus$ neutraalialkio. Neutraalialkiota ei itse asiassa ole, sillä kaikille $A \in \mathscr{P}(X)$ pätee $A \setminus X = \emptyset$.

LAUSE 1.6. *Olkoon $X \neq \emptyset$, ja olkoon $*$ joukon $X$ laskutoimitus.*

(1) *Jos on alkiot $e \in X$ ja $e' \in X$ siten, että $e * g = g$ ja $g * e' = g$ kaikilla $g \in X$, niin $e = e'$.*
(2) *Jos $*$ on assosiatiivinen laskutoimitus, jolla on neutraalialkio $e$, niin*
   (a) *Alkiolla $g \in X$ on käänteisalkio, jos ja vain jos sillä on vasen ja oikea käänteisalkio.*
   (b) *Jos alkiolla $g$ on käänteisalkio, se on yksikäsitteinen.*
   (c) *Jos alkiolla $g$ on käänteisalkio, se on alkion $g$ ainoa vasen/oikea käänteisalkio*

*Todistus.* (1) Harjoitustehtävä 9.
(2) Todistamme kohdan (a): Olkoon $g'$ alkion $g$ vasen käänteisalkio, ja olkoon $g''$ sen oikea käänteisalkio. Tällöin

$$g'' = e * g'' = (g' * g) * g'' = g' * (g * g'') = g' * e = g'.$$

Tällöin siis $g'$ on alkion $g$ käänteisalkio. Toinen suunta seuraa suoraan määritelmästä. Kohdat (b) ja (c) seuraavat kohdasta (a). □

Tarkastelemme seuraavaksi uusien laskutoimitusten muodostamista tunnettujen laskutoimitusten avulla.

Jos $*$ on joukon $A$ laskutoimitus, ja jos $B \subset A$, $B \neq \emptyset$ siten, että $b * b' \in B$ kaikilla $b, b' \in B$, niin $*$ määrittelee *indusoidun laskutoimituksen* $*|_B$ joukossa $B$: $b *|_B b' = b * b'$. Yleensä indusoidulle laskutoimitukselle käytetään samaa merkintää kuin sen indusoivalle laskutoimitukselle $*$: $*|_B = *$.

Esimerkki 1.7. Olkoon $\mathrm{M}_2\mathbb{R}$ reaalisten $2 \times 2$–matriisien joukko. Kertolasku määritellään joukossa $\mathrm{M}_2\mathbb{R}$ asettamalla

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

Olkoon

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

Tällöin 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 $B$, niiden avulla voidaan määritellä laskutoimitus joukossa $A \times B$:

$$((a, b), (a', b')) \mapsto (a *_A a', a *_B b').$$

Tätä laskutoimitusta kutsutaan *laskutoimitusten $*_A$ ja $*_B$ tuloksi*. Vastaavalla tavalla voidaan määritellä laskutoimituksia useamman joukon karteesiseen tuloon.

Esimerkki 1.8. Luonnollisten lukujen yhteenlaskun avulla saadaan yhteenlasku joukkoon $\mathbb{N} \times \mathbb{N}$: $(m, n) + (p, q) = (m + p, n + q)$.

Ennen kolmatta laskutoimituksen konstruktiota palautamme mieliin ekvivalenssirelaation käsitteen:

Määritelmä 1.9. *Relaatio* joukossa $A$ on joukon $A \times A$ osajoukko. Jos $\mathrm{R} \subset A \times A$ on relaatio, usein merkitään $a \,\mathrm{R}\, b \iff (a, b) \in \mathrm{R}$. Joukon $A$ relaatio R on

(1) *refleksiivinen*, jos $a \,\mathrm{R}\, a$ kaikilla $a \in A$,
(2) *symmetrinen*, jos $b \,\mathrm{R}\, a$ kaikilla $a, b \in A$, joille $a \,\mathrm{R}\, b$,
(3) *transitiivinen*, jos $a \,\mathrm{R}\, c$ aina kun $a \,\mathrm{R}\, b$ ja $b \,\mathrm{R}\, c$,
(4) *antisymmetrinen*, jos $b = a$ kaikilla $a, b \in A$, joille $a \,\mathrm{R}\, b$ ja $b \,\mathrm{R}\, a$.

Jos relaatio on refleksiivinen, symmetrinen ja transitiivinen, se on *ekvivalenssirelaatio*. Ekvivalenssirelaation merkkinä käytetään usein merkkiä $\sim$; tällöin merkitään $a \sim b$. 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 $A$:n *tekijäjoukoksi*.

Jos relaatio on refleksiivinen, antisymmetrinen ja transitiivinen, se on *osittainen järjestys*.

Määritelmä 1.10. Jos $*$ on laskutoimitus ja $\sim$ on ekvivalenssirelaatio joukossa $A$, ne ovat *yhteensopivat*, jos $a * b \sim a' * b'$ aina kun $a \sim a'$ ja $b \sim b'$. Laskutoimitus $*$ määrää *tekijälaskutoimituksen* $*$ joukossa $A/\!\sim$ säännöllä $[a] * [b] = [a * b]$.

Esimerkki 1.11. Olkoon relaatio $\equiv$ kokonaislukujen joukossa $\mathbb{Z}$ määritelty säännöllä $a \equiv b$, jos on $k \in \mathbb{Z}$ siten, että $b = a + 3k$. Tällöin $\equiv$ on ekvivalenssirelaatio:

(1) $a = a + 3 \cdot 0$ kaikilla $a \in \mathbb{Z}$,
(2) jos $b = a + 3k$ jollain $k \in \mathbb{Z}$, niin $a = b + 3 \cdot (-k)$,
(3) jos $b = a + 3k$ ja $c = b + 3n$ joillain $k, n \in \mathbb{Z}$, niin $c = a + 3(k + n)$.

Ekvivalenssirelaatiota $\equiv$ kutsutaan *kongruenssiksi*. Yhteenlasku on yhteensopiva ekvivalenssirelaation $\equiv$ kanssa: Jos $a' = a + 3m$ ja $b' = b + 3n$, niin

$$a' + b' = a + b + 3(m + n).$$

Siis kokonaislukujen yhteenlasku määrää laskutoimituksen kolmen alkion joukolla

$$\mathbb{Z}/\equiv = \{[0], [1], [2]\}.$$

LEMMA 1.12. *Jos $*$ on assosiatiivinen, sen tekijälaskutoimitus on assosiatiivinen. Jos $*$ on kommutatiivinen, sen tekijälaskutoimitus on kommutatiivinen.*

*Todistus.* Jos $*$ on kommutatiivinen, niin

$$[a] * [b] = [a * b] = [b * a] = [b] * [a],$$

joten tekijälaskutoimitus on kommutatiivinen. Assosiatiivisuus todistetaan harjoitustehtävässä 12. □

MÄÄRITELMÄ 1.13. Olkoot $E$ ja $E'$ joukkoja, joiden laskutoimitusta merkitään kertolaskulla. Kuvaus $h\colon E \to E'$ on *homomorfismi*, jos $h(ab) = h(a)h(b)$ kaikille $a, b \in E$. Bijektiivinen homomorfismi on *isomorfismi*, ja isomorfismi joukolta $E$ itselleen on *automorfismi*.

ESIMERKKI 1.14. (1) Olkoot $*$ ja $\sim$ laskutoimitus ja ekvivalenssirelaatio joukossa $E$. Jos ne ovat yhteensopivat, niin *luonnollinen kuvaus* $E \to E/\sim$, $a \mapsto [a]$, on surjektiivinen homomorfismi. Tämä seuraa määritelmästä: Olkoon $\phi$ luonnollinen kuvaus. Kuvauksen surjektiivisuus on selvää. Lisäksi kaikille $a, b \in E$ pätee

$$\phi(a) * \phi(b) = [a] * [b] = [a * b] = \phi(a * b).$$

(2) Kuvaus $h\colon \mathbb{Z} \to \mathrm{M}_2\mathbb{R}$,

$$h(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

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

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

**Harjoitustehtäviä.**

TEHTÄVÄ 1. Onko joukon $\mathscr{P}(X)$ laskutoimitus $\cap$ distributiivinen laskutoimituksen $\cup$ suhteen? Onko laskutoimitus $\cup$ distributiivinen laskutoimituksen $\cap$ suhteen?

TEHTÄVÄ 2. Onko laskutoimituksilla $\cap$ ja $\cup$ neutraalialkiot?

TEHTÄVÄ 3. Onko jokaisella $A \in \mathscr{P}(X)$ käänteisalkiot laskutoimitusten $\cap$ ja $\cup$ suhteen?

TEHTÄVÄ 4. Onko joukon $\mathscr{P}(X)$ laskutoimitus $\setminus$ assosiatiivinen?

TEHTÄVÄ 5. Onko matriisien yhteenlasku assosiatiivinen joukossa $\mathrm{M}_2\mathbb{R}$? Onko se kommutatiivinen?

TEHTÄVÄ 6. Onko matriisien kertolasku assosiatiivinen joukossa $\mathrm{M}_2\mathbb{R}$? Onko se kommutatiivinen?

TEHTÄVÄ 7. Onko matriisien yhteenlaskulla neutraalialkio joukossa $\mathrm{M}_2\mathbb{R}$? Onko matriisien kertolaskulla neutraalialkio joukossa $\mathrm{M}_2\mathbb{R}$?

TEHTÄVÄ 8. Olkoon

$$\Gamma = \{A \in \mathrm{M}_2\mathbb{R} : \det A = 1\}.$$

Osoita, että matriisien kertolasku indusoi laskutoimituksen joukossa $\Gamma$. Miten yhteenlasku käyttäytyy?

TEHTÄVÄ 9. Olkoon $X \neq \emptyset$, ja olkoon $*$ joukon $X$ laskutoimitus. Osoita: Jos on alkiot $e \in X$ ja $e' \in X$ siten, että $e * g = g$ ja $g * e' = g$ kaikilla $g \in X$, niin $e = e'$.

TEHTÄVÄ 10. Olkoon R relaatio joukossa $\mathbb{R}^2$ siten, että

$$(x, y)\,\mathrm{R}(z, w) \iff x^2 + y^2 = z^2 + w^2.$$

Osoita, että R on ekvivalenssirelaatio.

TEHTÄVÄ 11. Olkoon $\sim$ ekvivalenssirelaatio joukolla $A$. Olkoot $x, y \in A$. Osoita, että ekvivalenssiluokille pätee: Jos $[x] \cap [y] \neq \emptyset$, niin $[x] = [y]$.

TEHTÄVÄ 12. Osoita, että tekijälaskutoimitus on assosiatiivinen, jos alkuperäinen laskutoimitus on assosiatiivinen.

## 2. Kokonaisluvut ja rationaaliluvut

Tarkastelemme kokonaislukujen ja rationaalilukujen konstruktiota luonnollisista luvuista lähtien esimerkkinä tekijälaskutoimituksesta. Luonnollisten lukujen joukko on tällä kurssilla

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

Luonnollisten lukujen joukko ja sen laskutoimitukset yhteenlasku ja kertolasku oletetaan "intuitiivisesti tunnetuiksi". Kurssin aikana konstruoimme muut lukualueet

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

laajentamalla asteittain luonnollisista luvuista lähtien. Tarkastelemme samalla, miten lukualueiden algebralliset ominaisuudet muuttuvat.

Luonnollisten lukujen yhteen- ja kertolaskulla on neutraalialkiot 0 ja 1. Useimmilla luonnollisilla luvuilla ei kuitenkaan ole käänteisalkiota kummankaan laskutoimituksen suhteen. Laajennamme seuraavaksi luonnollisten lukujen lukualuetta siten, että jokaisella alkiolla on uudessa struktuurissa käänteisalkio yhteenlaskun suhteen.

Määrittelemme kokonaisluvut "luonnollisten lukujen muodollisina erotuksina": Jos $m$ ja $n$ ovat luonnollisia lukuja ja $m \geq n$, niin erotus $m - n$ on olemassa luonnollisena lukuna: se on yhtälön $n + x = m$ ratkaisu. Toisaalta sama luonnollinen luku voidaan esittää erotuksena äärettömän monella eri tavalla, sillä kaikilla $k \in \mathbb{N}$ pätee $(m + k) - (n + k) = m - n$. Näiden havaintojen opastamana määrittelemme joukkoon $\mathbb{N} \times \mathbb{N}$ relaation $\sim$ asettamalla $(m, n) \sim (p, q)$, jos ja vain jos $m + q = p + n$. Harjoitustehtävässä 13 osoitetaan, että relaatio $\sim$ on ekvivalenssirelaatio.

*Kokonaislukujen joukko* on

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

Kokonaislukujen *yhteenlasku* on luonnollisten lukujen yhteenlaskun tulon

$$(m,n)+(p,q)=(m+p,n+q), \tag{1}$$

indusoima laskutoimitus, ja *kertolasku* on joukon $\mathbb{N}\times\mathbb{N}$ laskutoimituksen

$$(m,n)*(p,q)=(mp+nq,mq+np) \tag{2}$$

indusoima laskutoimitus.

HUOMAUTUKSIA: (1) Laskutoimitusten määritelmät ovat järkeviä: Paria $(m,n)$ tulee ajatella erotuksena $m-n$, jolloin lausekkeet (1) ja (2) vastaavat lausekkeita

$$(m-n)+(p-q)=(m+p)-(n+q)$$

ja

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

(2) Kokonaislukujen laskutoimitukset ovat hyvin määriteltyjä, koska vastaavat joukkoon $\mathbb{N}\times\mathbb{N}$ määritellyt laskutoimitukset ovat yhteensopivia ekvivalenssirelaation $\sim$ kanssa. Todistamme tämän yhteenlaskulle: Jos $(m,n)\sim(m',n')$ ja $(p,q)\sim(p',q')$, niin määritelmän mukaan pätee $m+n'=m'+n$ ja $p+q'=p'+q$. Siis

$$(m+p)+(n'+q')=(m'+p')+(n+q),$$

joten $(m+p,n+q)\sim(m'+p',n'+q')$. Kertolasku käsitellään harjoitustehtävässä 14. Huomaa: Todistuksessa voi käyttää vain luonnollisia lukuja!

PROPOSITIO 2.1. (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:*

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

*Todistus.* (1) Indusoivien laskutoimitusten assosiatiivisuus ja kommutatiivisuus on helppo todeta lausekkeista (1) ja (2). Väite seuraa Lemmasta 1.12.
(2) Distributiivisuus: Koska laskutoimitukset ovat kommutatiivisia, riittää tarkastaa distributiivisuus vasemmalta. Olkoot $a=[(m,n)]$, $b=[(p,q)]$ ja $c=[(r,s)]$ kokonaislukuja. Teemme laskun joukossa $\mathbb{N}\times\mathbb{N}$:

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

Toisaalta

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

(3) Joukossa $\mathbb{N}\times\mathbb{N}$: $(m,n)+(0,0)=(m,n)$ ja $(m,n)(1,0)=(m+0,0+n)=(m,n)$. Kohta (4) on vastaavanlainen lasku. □

Proposition 2.1 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 pitäisi olla joukon $\mathbb{Z}$ osajoukko. Kuitenkin $\mathbb{Z}$ on määritelty joukon $\mathbb{N}\times\mathbb{N}$ abstraktina tekijäjoukkona. Siispä samastamme $\mathbb{N}$:n sopivan kokonaislukujoukon kanssa.

PROPOSITIO 2.2. *Kuvaus* $i\colon \mathbb{N} \to \mathbb{Z}$, $i(n) = [(n,0)]$ *on injektiivinen homomorfismi yhteenlaskulle ja kertolaskulle: kaikilla* $m, n \in \mathbb{N}$ *pätee*

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

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

*Todistus.* Harjoitustehtävät 15 ja 16. □

Proposition 2.2 mukaan kuvaus $i$ säilyttää yhteenlaskun, eli ei ole merkitystä, lasketaanko luvut $m$ ja $n$ yhteen tai kerrotaanko ne luonnollisina lukuina vai vastaavina kokonaislukuina.

---

SOPIMUS: Tästedes 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 $-1$.

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

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

*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 tekijälaskutoimitus, ja rationaalilukujen *kertolasku* on kokonaislukujen kertolaskun tulon

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

indusoima laskutoimitus. Laskutoimitukset ovat hyvin määriteltyjä, sillä vastaavat laskutoimitukset joukossa $\mathbb{Z} \times \mathbb{Z}^*$ ovat ekvivalenssirelaation $\sim$ kanssa yhteensopivia. Tämä osoitetaan harjoitustehtävänä 17.

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

PROPOSITIO 2.3. (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:*

$$m/n + (-m/n) = 0/1.$$

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

$$(m/n)(n/m) = 1/1.$$

*Todistus.* Harjoitustehtävä ((2) harjoitustehtävässä 18). □

PROPOSITIO 2.4. *Kuvaus* $j\colon \mathbb{Z} \to \mathbb{Q}$, $j(n) = n/1$ *on injektiivinen homomorfismi yhteenlaskulle ja kertolaskulle: pätee*

$$j(m+n) = j(m) + j(n) \quad ja \quad j(mn) = j(m)j(n)$$

*kaikilla* $m, n \in \mathbb{Z}$.

*Todistus.* Kuten Propositio 2.2. □

---

SOPIMUS: Tästedes samastamme kokonaisluvut vastaavan rationaalilukujen osajoukon kanssa.

---

Nyt voimme määritellä vähennyslaskun kaikille rationaaliluvuille $\alpha, \beta \in \mathbb{Q}$ asettamalla $\alpha - \beta = \alpha + (-\beta)$, missä $-\beta$ on rationaaliluvun $\beta$ käänteisalkio yhteenlaskun suhteen, ja uuden laskutoimituksen, *jakolaskun*, joukossa $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ asettamalla $\alpha/\beta = \alpha\beta^{-1}$, missä $\beta^{-1}$ on rationaaliluvun $\beta \neq 0$ käänteisalkio kertolaskun suhteen.

**Harjoitustehtäviä.**

TEHTÄVÄ 13. Olkoon $\sim$ relaatio joukossa $\mathbb{N} \times \mathbb{N}$ siten, että

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

Osoita, että $\sim$ on ekvivalenssirelaatio.

TEHTÄVÄ 14. Määritellään laskutoimitus $*$ joukossa $\mathbb{N} \times \mathbb{N}$ asettamalla

$$(m, n) * (p, q) = (mp + nq, mq + np)$$

Osoita, että $*$ on yhteensopiva tehtävän 13 ekvivalenssirelaation kanssa.

TEHTÄVÄ 15. Olkoon $i\colon \mathbb{N} \to \mathbb{Z}$, $i(n) = [(n, 0)]$. Osoita, että $i$ on injektio, jolle pätee

$$i(m+n) = i(m) + i(n) \quad \text{ja} \quad i(mn) = i(m)i(n)$$

kaikilla $m, n \in \mathbb{N}$.

TEHTÄVÄ 16. Olkoon $i$ kuten tehtävässä 15. Osoita, että jokainen kokonaisluku on muotoa $i(n)$ tai $-i(n)$ jollain luonnollisella luvulla $n$.

TEHTÄVÄ 17. Osoita, että joukon $\mathbb{Z} \times \mathbb{Z}^*$ ekvivalenssirelaatio

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

on yhteensopiva laskutoimitusten

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

ja

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

kanssa.

TEHTÄVÄ 18. Osoita, että rationaalilukujen kertolasku on distributiivinen yhteenlaskun suhteen.

# 3. Ryhmät

Tässä luvussa tarkastelemme pareja, jotka koostuvat joukosta ja siinä määritellystä laskutoimituksesta. Oletamme laskutoimitukselta muutamia yksinkertaisia ominaisuuksia:

Määritelmä 3.1. Olkoon $*$ joukon $G \neq \emptyset$ laskutoimitus. Joukko $G$ varustettuna tällä laskutoimituksella on *ryhmä*, jos

- laskutoimitus on assosiatiivinen,
- joukossa $G$ on neutraalialkio, ja
- jokaisella $g \in G$ on käänteisalkio.

Esimerkki 3.2. (a) Aikaisemmista esimerkeistämme ryhmiä ovat (ainakin) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^*, \cdot)$ ja $(\mathbb{Z}_p, +)$. Näistä viimeisessä esimerkissä $\mathbb{Z}_p$ on kongruenssia

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

vastaava tekijäjoukko, ja $+$ on yhteenlaskua vastaava tekijälaskutoimitus. Osoitamme $(\mathbb{Z}_p, +)$:n ryhmäksi: Laskutoimitus on assosiatiivinen Proposition 2.1 ja Lemman 1.12 mukaan. Alkio $[0]$ on neutraalialkio, koska luonnollinen kuvaus on surjektiivinen homomorfismi, katso Esimerkki 1.14(1). Alkion $[k] \in \mathbb{Z}_p$ käänteisalkio on $[-k]$: $[k] + [-k] = [k - k] = [0] = [-k] + [k]$.
(b) Olkoot $\mathrm{M}_n\mathbb{R}$ ja $\mathrm{M}_n\mathbb{Z}$ sellaisten $n \times n$-matriisien joukot, $n \in \mathbb{N}$, $n \geq 2$, joiden kertoimet ovat reaalilukuja ja kokonaislukuja. Harjoitustehtävässä 19 osoitetaan dimensiossa $n = 2$, että $\mathbb{R}$-kertoiminen *erityinen lineaarinen ryhmä*

$$\mathrm{SL}_2\mathbb{R} = \{A \in \mathrm{M}_2\mathbb{R} : \det A = 1\}$$

on ryhmä, kun laskutoimituksena on matriisien kertolasku. Vastaavasti myös $\mathbb{Z}$-kertoiminen *erityinen lineaarinen ryhmä*

$$\mathrm{SL}_n\mathbb{Z} = \{A \in \mathrm{M}_n\mathbb{Z} : \det A = 1\}$$

ja *yleinen lineaarinen ryhmä*

$$\mathrm{GL}_n\mathbb{R} = \{A \in \mathrm{M}_n\mathbb{R} : \det A \neq 0\}$$

ovat ryhmiä, kuten myös molempien tapausten $\mathbb{Q}$– ja $\mathbb{C}$–kertoimiset versiot.

Propositio 3.3. *Olkoon $G$ ryhmä. Tällöin*

(1) *Neutraalialkio $e$ on yksikäsitteinen.*
(2) *Jokaisen alkion käänteisalkio on yksikäsitteinen.*
(3) *Jos $\bar{a}a = e$, niin $\bar{a}$ on alkion $a$ käänteisalkio.*
(4) *$(a^{-1})^{-1} = a$ kaikilla $a \in G$.*
(5) *Supistussäännöt pätevät kaikilla $a, b, c \in G$:*
    (a) *Jos $ab = ac$, niin $b = c$.*
    (b) *Jos $ab = cb$, niin $a = c$.*
(6) *$(ab)^{-1} = b^{-1}a^{-1}$.*
(7) *Olkoot $a, b \in G$. Yhtälöillä $ax = b$ ja $ya = b$ on ratkaisu ryhmässä $G$.*

*Todistus.* (1), (2), (3): Lause 1.6.
(4): Koska $aa^{-1} = e$, niin kohdan (3) nojalla $a = (a^{-1})^{-1}$.
(6): $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e$.
Loput harjoitustehtävissä 24 ja 25. □

HUOMAA: Jos $A$ on joukko, jossa on assosiatiivinen laskutoimitus, jolla on neutraalialkio, niin Proposition 3.3 kohdan (7) ominaisuudesta seuraa, että $A$ on ryhmä. Supistussäännöt (5) ovat voimassa monissa muissakin rakenteissa, esimerkiksi luonnollisissa luvuissa.

Jos $A$ on joukko, jossa on assosiatiivinen laskutoimitus, jota merkitään kuin kertolaskua, voidaan jokaiselle $a \in A$ määritellä positiiviset *potenssit*: Asetamme $a^1 = a$, ja kaikille $n \in \mathbb{N}$, $n \geq 1$ asetamme $a^{n+1} = aa^n$. Jos joukossa $A$ on neutraalialkio $e$, asetamme $a^0 = e$, ja jos alkiolla $a \in A$ on käänteisalkio, määrittelemme sen $-1$. potenssiksi käänteisalkion $a^{-1}$, ja kaikille $n \in \mathbb{Z}$, $n \leq -2$ asetamme $a^n = (a^{-1})^{-n}$.

Jos $A$:n laskutoimitusta merkitään kuten yhteenlaskua, määrittelemme vastaavasti $a$:n positiiviset *monikerrat* asettamalla $1a = a$, ja $(n+1)a = na + a$ kaikille $n \in \mathbb{Z}$, $n \geq 1$. Lisäksi $0a = 0 \in A$, $-1a = -a$, ja negatiivisille $n \in \mathbb{Z}$ asetamme $na = (-n)(-a)$.

Tavanomaiset laskulait pätevät potensseille ja monikerroille:

LEMMA 3.4. *Olkoon $G$ ryhmä. Jos laskutoimitusta merkitään kertolaskulla, niin*

(1) $(a^n)^m = a^{nm}$ *kaikilla* $a \in G$, $n, m \in \mathbb{Z}$.
(2) $a^n a^m = a^{n+m}$ *kaikilla* $a \in G$, $n, m \in \mathbb{Z}$.

*Jos laskutoimitusta merkitään yhteenlaskulla, niin*

(3) $na + ma = (n+m)a$ *kaikilla* $a \in G$, $n, m \in \mathbb{Z}$.
(4) $n(ma) = (nm)a$ *kaikilla* $a \in G$, $n, m \in \mathbb{Z}$.

*Todistus.* Harjoitustehtävä 26. □

Luvussa 1 määriteltyjen konstruktioiden avulla voimme muodostaa uusia ryhmiä tunnetuista ryhmistä lähtien.

PROPOSITIO 3.5. *Olkoot $G_1$ ja $G_2$ ryhmiä. Niiden tulo $G_1 \times G_2$ on ryhmä (varustettuna laskutoimitusten tulolla).*

*Todistus.* Laskutoimituksen assosiatiivisuus on selvää. Jos $e_1$ ja $e_2$ ovat ryhmien $G_1$ ja $G_2$ neutraalialkiot, niin $(e_1, e_2)$ on neutraalialkio joukossa $G_1 \times G_2$. Alkion $(g_1, g_2) \in G_1 \times G_2$ käänteisalkio on $(g_1^{-1}, g_2^{-1})$. □

ESIMERKKI 3.6. Joukot $\mathbb{R}^n$ ja $\mathbb{Z}^n$ varustettuna vektorien komponenteittaisella yhteenlaskulla, eli yhteenlaskun $n$-kertaisella tulolla, ovat ryhmiä.

PROPOSITIO 3.7. *Olkoon $G$ ryhmä, ja olkoon $\sim$ sen laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Tällöin $G/\sim$ varustettuna tekijälaskutoimituksella on ryhmä.*

*Todistus.* Laskutoimituksen assosiatiivisuus osoitettiin Lemmassa 1.12. Olkoon $e$ ryhmän $G$ neutraalialkio. Koska kaikille $[a] \in G/\sim$ pätee

$$[e][a] = [ea] = [a] = [ae] = [a][e],$$

niin $[e]$ on neutraalialkio. Samoin luokan $[a]$ käänteisalkio on $[a^{-1}]$:

$$[a^{-1}][a] = [a^{-1}a] = [e] = [aa^{-1}] = [a][a^{-1}].$$

□

Ryhmää $G/\sim$ kutsutaan ekvivalenssirelaatiota $\sim$ vastaavaksi ryhmän $G$ *tekijäryhmäksi*. Esimerkiksi ryhmä $\mathbb{Z}_p$, jota tarkasteltiin esimerkin 3.2 kohdassa (a), on kongruenssia $a \equiv b \iff b = a + kp$ jollain $k \in \mathbb{Z}$, vastaava kokonaislukujen ryhmän tekijäryhmä.

Osajoukolle indusoituva laskutoimitus antaa myös ryhmiä, jos osajoukko on laskutoimituksen kanssa yhteensopiva. Tarkastelemme tätä lähemmin luvussa 4, seuraava esimerkki antaa kuitenkin esimakua.

Esimerkki 3.8. Olkoon $X$ epätyhjä joukko. Joukkoa $S(X)$, joka koostuu kaikista bijektioista joukolta $X$ itselleen kutsutaan joukon $X$ *permutaatioryhmäksi*, kun laskutoimituksena käytetään kuvausten yhdistämistä. Monet joukon $S(X)$ osajoukot varustettuna indusoidulla laskutoimituksella (joka siis on kuvausten yhdistäminen) ovat ryhmiä. Olkoon $X = \mathbb{R}^n$. Kuvaus $L\colon \mathbb{R}^n \to \mathbb{R}^n$ on *lineaarikuvaus*, jos kaikilla $x, y \in \mathbb{R}^n$ ja $a \in \mathbb{R}$ pätee $L(x + y) = L(x) + L(y)$ ja $L(ax) = aL(x)$. Lineaariset bijektiot muodostavat ryhmän, jossa kuvausten yhdistäminen on laskutoimituksena: Identtinen kuvaus on lineaarikuvaus, ja lineaarisen bijektion käänteiskuvaus on lineaarinen bijektio. Laskutoimituksen assosiatiivisuutta ei tarvitse tarkastaa, koska se on ryhmän $S(\mathbb{R}^n)$ laskutoimituksen indusoima.

Määritelmä 3.9. Ryhmä $G$ on *kommutatiivinen*, jos sen laskutoimitus on kommutatiivinen. Ryhmä $G$ on *äärellinen*, jos joukko $G$ on äärellinen.

Esimerkki 3.10. (1) Ryhmät $\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{Z}^n$ ovat kommutatiivisia. Erityinen lineaarinen ryhmä $\mathrm{SL}_n\mathbb{R}$ ei ole kommutatiivinen, tämä osoitettiin harjoitustehtävässä 6.
(2) Ryhmät $\mathbb{Z}_p$ ja $\mathbb{Z}_p \times \mathbb{Z}_q$, $p, q \in \mathbb{N}$, ovat äärellisiä ryhmiä.
(3) Funktiot $\mathrm{id}, f, g, h\colon \mathbb{R}^* \to \mathbb{R}^*$, $f(x) = -x, g(x) = 1/x$, $h(x) = -1/x$, muodostavat äärellisen ryhmän $K \subset S(\mathbb{R}^*)$ laskutoimituksena kuvausten yhdistäminen. On helppo nähdä, että laskutoimitus on hyvin määritelty. Joukon $K$ alkioille $f, g, h$ pätee

$$f \circ f = g \circ g = h \circ h = \mathrm{id},$$

joten kaikilla on käänteisalkio, ja $K$ on siis ryhmä. Lisäksi pätee:

$$f \circ g = g \circ f = h, \quad g \circ h = h \circ g = f \quad \text{ja} \quad h \circ f = f \circ h = g,$$

joten $K$ on kommutatiivinen. Itse asiassa $K$ "on ryhmäteorian kannalta sama ryhmä kuin $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$". Täsmällisemmin ilmaistuna: kuvaus $\phi\colon\ : \mathbb{Z}_2 \times \mathbb{Z}_2 \to K$,

$$\phi([0],[0]) = \mathrm{id}, \quad \phi([0],[1]]) = f, \quad \phi([1],[0]) = g, \quad \phi([1],[1]) = h,$$

on isomorfismi. Kuvaus on selvästi bijektio, ja homomorfisuuden voi tarkastaa tutkimalla kaikki tapaukset, esimerkiksi

$$([1],[0]) + ([0],[1]) = ([0],[1]) + ([1],[0]) = ([1],[1]),$$

joka vastaa yhtälöitä $f \circ g = g \circ f = h$. Muille tapauksille pätee vastaavasti (katso Esimerkki 3.12 (4)).

Jos $G$ ja $G'$ ovat ryhmiä, niin homomorfismia $\phi\colon G \to G'$ kutsutaan *ryhmähomomorfismiksi*. Huomaa, että isomorfismin, eli bijektiivisen homomorfismin, käänteiskuvaus on myös isomorfismi (mieti!). Ryhmiä, joiden välillä on isomorfismi sanotaan *isomorfisiksi*. Jos $G$ ja $G'$ ovat isomorfisia ryhmiä, merkitään $G \cong G'$.

Propositio 3.11. *Ryhmähomomorfismi $\phi\colon G \to G'$ kuvaa ryhmän $G$ neutraalialkion ryhmän $G'$ neutraalialkioksi, ja jokaiselle $g \in G$ pätee $\phi(g^{-1}) = \phi(g)^{-1}$.*

*Todistus.* Neutraalialkiota koskeva väite todistetaan harjoitustehtävässä 22. Olkoon $e$ ryhmän $G$ neutraalialkio. Olkoon $g \in G$. Tällöin

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

Ensimmäisen väitteen mukaan tämä on ryhmän $G$ neutraalialkio. Väite seuraa Proposition 3.3 kohdasta (3). □

Esimerkki 3.12. (1) Olkoon $\mathbb{R}_+$ positiivisten reaalilukujen joukko. Varustetaan $\mathbb{R}_+$ kertolaskulla ja $\mathbb{R}$ yhteenlaskulla. Tällöin $(\mathbb{R}_+, \cdot)$ ja $(\mathbb{R}, +)$ ovat ryhmiä. Logaritmifunktio $\log : \mathbb{R}_+ \to \mathbb{R}$ on isomorfismi: Tunnetusti $\log(xy) = \log(x) + \log(y)$ kaikilla $x, y > 0$. Logaritmin käänteiskuvaus on eksponenttifunktio $\exp\colon \mathbb{R} \to \mathbb{R}_+$, jolle pätee

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

(2) Vektoriavaruuden $\mathbb{R}^n$ lineaaristen bijektioiden ryhmä (katso Esimerkki 3.8) on isomorfinen yleisen lineaarisen ryhmän $\mathrm{GL}_n\mathbb{R}$ kanssa: Olkoon $K = \{v_1, v_2, \ldots, v_n\}$ vektoriavaruuden $\mathbb{R}^n$ kanta, ja olkoon $(Lv_i)_K \in \mathbb{R}^n$ vektorin $Lv_i$ koordinaattivektori kannassa $K$. Lineaarialgebrassa on osoitettu, että kuvaus

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

on isomorfismi.
(3) Olkoon $G$ ryhmä, ja olkoon $a \in G$. Kuvaus $\phi\colon G \to G$, $\phi(g) = aga^{-1}$ on ryhmän $G$ automorfismi: Se on homomorfismi:

$$\begin{aligned}\phi(g)\phi(g') &= (aga^{-1})(ag'a^{-1}) = (ag)(a^{-1}a)(g'a^{-1}) = (ag)e(g'a^{-1}) \\ &= (ag)(g'a^{-1}) = a(gg')a^{-1} = \phi(gg').\end{aligned}$$

Se on myös bijektio, koska sillä on käänteiskuvaus $\phi^{-1}\colon G \to G$: $\phi^{-1}(g) = a^{-1}ga$. Kuvaus $\phi$ on ryhmän $G$ *sisäinen automorfismi*. Esimerkiksi matriisia $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ vastaa sisäinen automorfismi $\phi_A : B \mapsto ABA^{-1}$. Jos $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, kuvaus on siis

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

(4) Äärellisiä (pieniä) ryhmiä voi myös tarkastella *laskutaulujen* avulla: Muodostetaan ryhmän alkioilla indeksoitu taulukko, jossa paikalla $(g, h)$ on alkio $gh$. Esimerkiksi neljän alkion ryhmien $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ ja $K$ laskutaulut ovat (kun käytetään ekvivalenssiluokan $[k]$ merkintänä $k$:ta)

| $+$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 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) |

ja

| $\circ$ | id | $f$ | $g$ | $h$ |
|---|---|---|---|---|
| id | id | $f$ | $g$ | $h$ |
| $f$ | $f$ | id | $h$ | $g$ |
| $g$ | $g$ | $h$ | id | $f$ |
| $h$ | $h$ | $g$ | $f$ | id |

Ryhmän laskutaulussa (tai kertotaulussa, kuten sitä usein kutsutaan) jokaisella rivillä ja jokaisessa sarakkeessa esiintyvät kaikki ryhmän alkiot (Harjoitustehtävä 33). Ryhmien $\mathbb{Z}_2 \times \mathbb{Z}_2$ ja $K$ isomorfisuus on helppo todeta vertaamalla laskutauluja.

**Harjoitustehtäviä.**

TEHTÄVÄ 19. Osoita, että $\mathrm{SL}_2\mathbb{R}$ varustettuna matriisien kertolaskulla on ryhmä.

TEHTÄVÄ 20. Osoita: Jos $h\colon E \to E'$ on surjektiivinen homomorfismi ja $E$:llä on neutraalialkio $e$, niin $h(e)$ on $E'$:n neutraalialkio.

TEHTÄVÄ 21. Osoita, että tehtävän 20 väite ei päde ilman surjektiivisuutta.

TEHTÄVÄ 22. Olkoot $G$ ja $G'$ ryhmiä. Olkoon $h : G \to G'$ homomorfismi. Osoita, että $h$ kuvaa $G$:n neutraalialkion $G'$:n neutraalialkioksi.

TEHTÄVÄ 23. Keksi esimerkki, joka osoittaa, että tehtävän 22 väite ei päde, jos $G$ on ryhmä mutta $G'$ ei ole ryhmä.

TEHTÄVÄ 24. Olkoon $G$ ryhmä. Osoita, että kaikilla $a, b, c \in G$ pätee

$$ab = ac \implies b = c \quad \text{ja} \quad ba = ca \implies b = c.$$

TEHTÄVÄ 25. Olkoon $A$ joukko, jossa on assosiatiivinen laskutoimitus, jolla on neutraalialkio. Osoita: Kaikilla $a, b \in A$, yhtälöillä $ax = b$ ja $ya = b$ on ratkaisut $A$:ssa, jos ja vain jos $A$ on ryhmä.

TEHTÄVÄ 26. Todista Lemman 3.4 laskusäännöt.

TEHTÄVÄ 27. Olkoon $G$ ryhmä, ja olkoon $\operatorname{Aut} G$ sen automorfismien joukko. Osoita, että $\operatorname{Aut} G$ on ryhmä, kun laskutoimituksena on kuvausten yhdistäminen.

TEHTÄVÄ 28. Kuvaus $f\colon \mathbb{R} \to \mathbb{R}$ on kasvava, jos kaikille $x, y \in \mathbb{R}$ pätee $f(x) \geq f(y)$, kun $x \geq y$. Kuvaus $f\colon \mathbb{R} \to \mathbb{R}$ on vähenevä, jos kaikille $x, y \in \mathbb{R}$ pätee $f(x) \leq f(y)$, kun $x \geq y$. Kuvaus on monotoninen, jos se on kasvava tai vähenevä. Kasvavien, vähenevien ja monotonisten bijektioiden joukot ovat permutaatioryhmän $S(\mathbb{R})$ osajoukkoja. Indusoiko kuvausten yhdistäminen laskutoimituksen näihin joukkoihin? Muodostavatko kasvavat bijektiot ryhmän? Entä vähenevät bijektiot? Entä monotoniset bijektiot?

TEHTÄVÄ 29. Olkoot $X$ ja $Y$ epätyhjiä joukkoja, ja olkoon $f\colon X \to Y$ bijektio. Osoita, että permutaatioryhmät $S(X)$ ja $S(Y)$ ovat isomorfisia.

TEHTÄVÄ 30. Olkoon $G$ kommutatiivinen ryhmä, ja olkoon $G'$ ryhmä. Olkoon $\phi\colon G \to G'$ isomorfismi. Osoita, että ryhmä $G'$ on kommutatiivinen.

TEHTÄVÄ 31. Olkoon

$$H_3 = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{R} \right\}.$$

Osoita, että $H_3$ varustettuna matriisien kertolaskulla on ryhmä.

TEHTÄVÄ 32. Osoita, että tehtävässä 31 määritelty ryhmä $H_3$ ei ole isomorfinen ryhmän $(\mathbb{R}^3, +)$ kanssa.

[21]Vihje: Anna esimerkki tilanteesta, jossa homomorfismi ei kuvaa neutraalialkiota neutraalialkioksi.

[23]Vihje: Anna esimerkki homomorfismista joltakin ryhmältä $G$ sopivaan laskutoimituksella varustettuun joukkoon $G'$ siten, että $G$:n neutraalialkio ei kuvaudu neutraalialkioksi.

TEHTÄVÄ 33. Osoita, että kaikki ryhmän alkiot esiintyvät sen laskutaulun jokaisella rivillä ja sarakkeella.

TEHTÄVÄ 34. Olkoon $G$ ryhmä. Olkoon R ryhmän $G$ relaatio

$$a\mathrm{R}b \iff a = gbg^{-1} \text{ jollakin } g \in G.$$

Onko R ekvivalenssirelaatio?

TEHTÄVÄ 35. Määritellään reaalilukujen laskutoimitus $*$ asettamalla $x*y = \sqrt[3]{x^3 + y^3}$.

(a) Osoita, että $(\mathbb{R}, *)$ on ryhmä.

(b) Osoita, että ryhmät $(\mathbb{R}, *)$ ja $(\mathbb{R}, +)$ ovat isomorfiset.

(Muista: Jos $x$ on reaaliluku, sen kolmas juuri $\sqrt[3]{x}$ on reaaliluku, jolle pätee $(\sqrt[3]{x})^3 = x$. Jokaisella reaaliluvulla on yksikäsitteinen reaalinen kolmas juuri.)

## 4. ALIRYHMÄT

MÄÄRITELMÄ 4.1. Olkoon $G$ ryhmä. Olkoon $B \subset G$, $B \neq \emptyset$. Jos joukko $B$ varustettuna indusoidulla laskutoimituksella on ryhmä, se on ryhmän $G$ *aliryhmä*. Jos $H \subset G$ on ryhmän $G$ aliryhmä, merkitään usein $H \leq G$, ja jos $H \leq G$ ja $H \neq G$, merkitään $H < G$.

Ylläoleva määritelmä vaatii tietysti, että $bb' \in B$ kaikilla $b, b' \in B$ eli, että indusoitu laskutoimitus on määritelty. Seuraava tulos antaa keinon tarkastaa, onko jokin ryhmän osajoukko aliryhmä:

PROPOSITIO 4.2. *Ryhmän $G$ osajoukko $H \neq \emptyset$ on aliryhmä, jos*

(1) *kaikilla $x, y \in H$ pätee $xy^{-1} \in H$, tai*
(2) *kaikilla $x, y \in H$ $xy \in H$ ja $y^{-1} \in H$.*

*Todistus.* Olkoon $e \in G$ neutraalialkio. Tarkastellaan ehtoa (1): Olkoon $h \in H$. Oletuksen mukaan $hh^{-1} \in H$, joten $e \in H$. Samoin $y^{-1} = ey^{-1} \in H$ kaikilla $y \in H$. Kaikki on siis kunnossa, jos indusoitu laskutoimitus on määritelty joukossa $H$: edellisen nojalla kaikille $x, y \in H$ pätee $xy = x(y^{-1})^{-1} \in H$.
Ehdosta (2) seuraa ehto (1), joten sitä ei tarvitse tarkastella erikseen. □

ESIMERKKI 4.3. (1) Jokaisella ryhmällä on ainakin kaksi aliryhmää: ryhmä itse, ja sen neutraalialkion muodostama yhden alkion ryhmä.
(2) $\mathrm{SL}_n\mathbb{Z} < \mathrm{SL}_n\mathbb{R} < \mathrm{GL}_n\mathbb{R}$.
(3) Olkoon $G$ ryhmä, ja olkoon $a \in G$. Joukko

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

on ryhmän $G$ aliryhmä, se on alkion $a$ *virittämä syklinen aliryhmä*.
(4) Kokonaislukujen ryhmällä on sykliset aliryhmät $\langle n \rangle = \{nk : k \in \mathbb{Z}\} = n\mathbb{Z}$, $n \in \mathbb{N}$. Muita ei ole: Huomataan ensin, että $\{0\} = 0\mathbb{Z}$ ja $\mathbb{Z} = 1\mathbb{Z}$. Olkoon $H < \mathbb{Z}$, $H \neq \{0\}$ jokin aliryhmä. Olkoon $N$ pienin positiivinen kokonaisluku aliryhmässä $H$. Osoitamme, että $H = N\mathbb{Z}$. Jos on $m \in H \setminus N\mathbb{Z}$, niin $m = aN + b$ joillakin $a, b \in \mathbb{Z}$ siten, että $1 \leq b < N$. Nyt $b \in H$, joten $N$ ei olekaan pienin positiivinen kokonaisluku ryhmässä $H$, ristiriita. Siis $H = N\mathbb{Z}$.

Aliryhmillä on monia ominaisuuksia, jotka muistuttavat vektoriavaruuksien aliavaruuksien ominaisuuksia.

PROPOSITIO 4.4. *Aliryhmien leikkaus on aliryhmä.*

*Todistus.* Harjoitustehtävä 39. □

MÄÄRITELMÄ 4.5. Olkoon $G$ ryhmä, ja olkoon $B \subset G$, $B \neq \emptyset$. Joukon $B$ *virittämä aliryhmä* $\langle B \rangle$ on pienin aliryhmä, joka sisältää joukon $B$.

PROPOSITIO 4.6. *Olkoon $G$ ryhmä, ja olkoon $B \subset G$, $B \neq \emptyset$. Joukon $B$ virittämä aliryhmä on*

$$\{e\} \cup \{b_1^{\pm 1} b_2^{\pm 1} \cdot \cdots \cdot b_k^{\pm 1} : b_1, b_2, \ldots, b_k \in B, k \in \mathbb{N} \setminus \{0\}\}, \tag{3}$$

*missä $e$ on ryhmän $G$ neutraalialkio.*

*Todistus.* Olkoon $\widetilde{B}$ lausekkeen (3) antama osajoukko. Joukko $\widetilde{B}$ varustettuna indusoidulla laskutoimituksella on ryhmän $G$ aliryhmä, sillä alkion $b_1^{\pm 1} b_2^{\pm 1} \cdot \cdots \cdot b_k^{\pm 1}$ käänteisalkio $b_k^{\mp 1} b_{k-1}^{\mp 1} \cdot \cdots \cdot b_1^{\mp 1}$ on joukossa $\widetilde{B}$, samoin kaikkien alkioiden tulot ovat oikeaa muotoa. Joukon $B$ virittämä aliryhmä sisältää kaikki muotoa $b_1^{\pm 1} b_2^{\pm 1} \cdot \cdots \cdot b_k^{\pm 1}$ olevat alkiot, sillä muuten $\langle B \rangle$ ei ole laskutoimituksen suhteen suljettu. □

Jos tulkitsemme tyhjän tulon neutraalialkioksi, lauseke (3) voidaan korvata seuraavalla:

$$\{b_1^{\pm 1} b_2^{\pm 1} \cdot \cdots \cdot b_k^{\pm 1} : b_1, b_2, \ldots, b_k \in B, k \in \mathbb{N}\},$$

Proposition 4.6 mukaan ryhmän alkion virittämä aliryhmä on sama kuin sen virittämä syklinen aliryhmä kuten esimerkissä 4.3. Ryhmä $G$ on *syklinen ryhmä*, jos on $a \in G$ siten, että $G = \langle a \rangle$. Ryhmät $\mathbb{Z} = \langle 1 \rangle$ ja $\mathbb{Z}_p = \langle [1] \rangle$, $p \in \mathbb{N} \setminus \{0\}$ ovat syklisiä.

ESIMERKKI 4.7. (1) Ryhmän $\mathbb{R}^2$ alkiot $(0,1)$ ja $(1,0)$ virittävät aliryhmän

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

$\mathbb{Z}^2$ ei ole syklinen ryhmä: Jos $a, b \neq 0$, niin $(-a, b)$ ei ole alkion $(a, b) \in \mathbb{Z}^2$ virittämässä aliryhmässä. Lisäksi alkioiden $(a, 0)$ ja $(0, a)$ virittämät sykliset ryhmät sisältyvät $\mathbb{Z}^2$:n aitoihin aliryhmiin $\mathbb{Z} \times \{0\}$ ja $\{0\} \times \mathbb{Z}$.
(2) 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 ryhmä on isomorfinen ryhmän $\mathbb{Z}_2$ kanssa.

PROPOSITIO 4.8. *Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Olkoot $H \leq G$, $H' \leq G'$ aliryhmiä. Tällöin $\phi(H) \leq G'$ ja $\phi^{-1}(H') \leq G$ ovat aliryhmiä.*

*Todistus.* Olkoot $\phi(g), \phi(h) \in \phi(H)$. Tällöin

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

koska $gh^{-1} \in H$. Toinen väite todistetaan harjoitustehtävänä 40. □

MÄÄRITELMÄ 4.9. Ryhmähomomorfismin $\phi\colon G \to G'$ *ydin* on $\ker \phi = \phi^{-1}(e')$ ja sen *kuva* on $\operatorname{Im} \phi = \phi(G)$.

Proposition 4.8 mukaan ydin ja kuva ovat aliryhmiä. Tarkastelemme ydintä ja kuvaa lähemmin hieman myöhemmin. Seuraava ytimen ominaisuus on hyvä todeta jo tässä vaiheessa:

PROPOSITIO 4.10. *Ryhmähomomorfismi on injektio, jos ja vain jos sen ydin on neutraalialkion muodostama ryhmä.*

*Todistus.* Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Aiemmin osoitettiin (harjoitustehtävä 22), että neutraalialkio kuvautuu neutraalialkioksi, joten jos $\phi$ on injektio, sen ydin on väitetyn lainen. Oletetaan, että $\ker\phi = \{e\}$. Olkoot $x, y \in G$ siten, että $\phi(x) = \phi(y)$. Tällöin $\phi(xy^{-1}) = \phi(x)(\phi(y))^{-1} = e'$, joten $xy^{-1} = e$ eli $x = y$. □

Jokainen ryhmän $G$ aliryhmä määrittelee kaksi ekvivalenssirelaatiota $G$:ssä (joskus relaatiot ovat samat):

$$x \underset{v}{\sim} y \iff x^{-1}y \in H \quad \text{ja} \quad x \underset{o}{\sim} y \iff yx^{-1} \in H.$$

Alkion $x \in G$ ekvivalenssiluokka relaatiossa $\underset{v}{\sim}$ koostuu niistä alkioista $y$, joille on $z \in H$ siten, että $x^{-1}y = z$ eli $y = xz$. Siksi $x$:n ekvivalenssiluokkaa relaatiossa $\underset{v}{\sim}$ merkitään yleensä (aina) $xH$:lla. Joukkoa $xH$ kutsutaan aliryhmän $H$ *vasemmaksi sivuluokaksi*. Vastaavasti relaation $\underset{o}{\sim}$ ekvivalenssiluokat $Hx$ ovat *oikeita sivuluokkia*. Vastaavia tekijäjoukkoja merkitään $G/\underset{v}{\sim} = G/H$ ja $G/\underset{o}{\sim} = H\backslash G$. (Tätä ei saisi luulla joukkojen erotukseksi...)

Seuraavassa $\#X$ merkitsee joukon $X$ alkioiden lukumäärää.

LAUSE 4.11 (Lagrangen lause). *Olkoon $G$ äärellinen ryhmä, ja olkoon $H < G$. Tällöin*

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

*Todistus.* Kuvaukset $h \mapsto xh$ ja $h \mapsto hx$ ovat bijektioita $H \to xH$ ja $H \to Hx$. Sivuluokkien määritelmän mukaan kuvaukset ovat surjektioita. Olkoot $h, h' \in H$ siten, että $xh = xh'$. Supistussäännöstä seuraa, että $h = h'$, joten ensimmäinen kuvaus on injektio. Sama pätee toiselle. Väite seuraa nyt siitä, että sivuluokat osittavat ryhmän $G$. □

MÄÄRITELMÄ 4.12. $\#G$ on ryhmän $G$ *kertaluku*. $\#(G/H) = \#(H\backslash G)$ on aliryhmän $H$ *indeksi*, josta usein käytetään merkintää $[G : H]$. Ryhmän $G$ alkion $g$ *kertaluku* on sen virittämän syklisen aliryhmän kertaluku.

Lagrangen lauseen kaava voidaan siis muotoilla myös $[G : H] = \frac{\#G}{\#H}$.

PROPOSITIO 4.13. *Olkoon $G$ äärellinen ryhmä. Tällöin $g^{\#G} = e$ jokaiselle $g \in G$.*

*Todistus.* Olkoon $H = \langle g \rangle$. Koska Lagrangen lauseen mukaan $\#G = k\#H$ jollain $k \in \mathbb{N}$, riittää osoittaa, että $g^{\#H} = e$. Mutta tämä on selvää, sillä muuten $g$ virittäisi väärän kokoisen ryhmän (mieti!). □

ESIMERKKI 4.14. (1) Jos $G$ on kommutatiivinen ja $H < G$, niin $xH = Hx$ kaikilla $x \in G$.
(2) $[\mathbb{R}^2 : \mathbb{R} \times \{0\}] = \infty$, sillä sivuluokat ovat $\mathbb{R} \times \{a\}$, $a \in \mathbb{R}$.

(3) $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = n\mathbb{Z}\backslash\mathbb{Z}$. $[\mathbb{Z} : n\mathbb{Z}] = n$.
(4) Olkoon

$$D_4 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle = \langle r, s \rangle.$$

Ryhmässä $D_4$ on 8 alkiota (mieti!). Aliryhmä $H = \langle s \rangle$ on selvästi isomorfinen ryhmän $\mathbb{Z}_2$ kanssa. Sen vasemmat sivuluokat ovat

$$H = sH = \{\mathrm{id}, s\}, \quad rH = rsH = \{r, rs\},$$
$$r^2H = r^2sH = \{r^2, r^2s\}, \text{ ja } \quad r^3H = r^3sH = \{r^3, r^3s\},$$

ja oikeat sivuluokat ovat

$$H = Hs = \{\mathrm{id}, s\}, \quad Hr = Hsr = \{r, sr\},$$
$$Hr^2 = Hsr^2 = \{r^2, sr^2\}, \text{ ja } \quad Hr^3 = Hsr^3 = \{r^3, sr^3\}.$$

Sivuluokat $rH$ ja $Hr$ ovat eri joukot, sillä

$$rs = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{ja} \quad sr = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

Ryhmä $D_4$ on neliön symmetriaryhmä, *diedriryhmä*. Jos $P$ on säännöllinen $n$-kulmio tasossa, sen symmetriaryhmä on diedriryhmä $D_n$, jonka virittävät kierto kulman $2\pi/n$ verran keskipisteen ympäri, ja heijastus "symmetria-akselin" suhteen.

Määritelmä 4.15. Ryhmän $G$ aliryhmä $H$ on *normaali*, jos

$$ghg^{-1} \in H \text{ kaikille } g \in G, h \in H.$$

Jos $H$ on ryhmän $G$ normaali aliryhmä, merkitään $H \trianglelefteq G$, aitoa normaalia aliryhmää merkitään $H \triangleleft G$.

Huomautuksia: (1) Toinen tapa ilmaista aliryhmän normaalius on sanoa, että kaikki ryhmän $G$ sisäiset automorfismit pitävät $H$:n paikallaan.
(2) $xH = H$, jos ja vain jos $x \in H$.

Esimerkki 4.16. (1) Ryhmä itse ja neutraalialkion muodostama aliryhmä ovat normaaleja.
(2) Esimerkin 4.14 mukaan $n\mathbb{Z} \triangleleft \mathbb{Z}$ ja $\mathbb{R} \times \{0\} \triangleleft \mathbb{R}^2$, mutta kohdan (4) diedriryhmän aliryhmä $H$ ei ole normaali.

Propositio 4.17. *Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi.*
*(1) Olkoon $H \trianglelefteq G$. Tällöin $\phi(H) \trianglelefteq \operatorname{Im}\phi$.*
*(2) Olkoon $H' \trianglelefteq G'$. Tällöin $\phi^{-1}(H') \trianglelefteq G$. Erityisesti siis ryhmähomomorfismin ydin on normaali aliryhmä.*

*Todistus.* (1) Olkoot $a' \in \phi(H)$, $g' \in \phi(G)$. Tällöin on $a \in H$ ja $g \in G$, joille $a' = \phi(a)$ ja $g' = \phi(g)$. Nyt

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

koska $gag^{-1} \in H$.
(2) Harjoitustehtävä 47. □

Propositio 4.18. *Olkoon $G$ ryhmä, ja olkoon $H < G$. Tällöin $H \triangleleft G$, jos ja vain jos kaikille $g \in G$ pätee $gH = Hg$.*

*Todistus.* Harjoitustehtävä 48. □

Esimerkki 4.19. (1) Jos aliryhmän $H < G$ indeksi on kaksi, se on normaali: Vasemmat sivuluokat ovat $H$ ja $H$:n komplementti, samoin oikeat sivuluokat. Väite seuraa Propositiosta 4.18.
(2) Olkoon $K \trianglelefteq G$ ja $K < H < G$. Tällöin $K \trianglelefteq H$.

Propositio 4.20. *Normaalin aliryhmän määräämät relaatiot* $\underset{v}{\sim}$ *ja* $\underset{o}{\sim}$ *ovat samat.*

*Todistus.* Niiden ekvivalenssiluokat ovat samat. □

Jos $H \trianglelefteq G$, merkitsemme vastaavaa ekvivalenssirelaatiota merkillä $\sim$. Tällöin voimme käyttää kumpaa tahansa ehdoista $xy^{-1} \in H$ tai $y^{-1}x \in H$ ekvivalenssin toteamiseksi. Yleisessä tilanteessa ryhmän $G$ laskutoimitus ei ole yhteensopiva ekvivalenssirelaatioiden $\underset{v}{\sim}$ ja $\underset{o}{\sim}$ kanssa. Jos aliryhmä on normaali, tilanne on toinen:

Lause 4.21. *Olkoon $G$ ryhmä ja olkoon $H < G$ aliryhmä. Tällöin ekvivalenssirelaatio $x \underset{v}{\sim} y \iff x^{-1}y \in H$ on yhteensopiva ryhmän $G$ laskutoimituksen kanssa, jos ja vain jos $H$ on ryhmän $G$ normaali aliryhmä. Jos $H \trianglelefteq G$, niin tekijäjoukko $G/H$ varustettuna tekijälaskutoimituksella on ryhmä. Tekijäryhmän $G/H$ neutraalialkio on $H$.*

*Todistus.* (1) Oletetaan, että $H$ on normaali. Olkoot $x, x', y, y' \in X$, $x \sim x'$ ja $y \sim y'$. Tällöin on $h_1, h_2 \in H$ siten, että $x' = h_1 x$ ja $y' = h_2 y$. Koska $H$ on normaali aliryhmä, pätee $xH = Hx$, erityisesti on siis $h_3 \in H$, jolle $h_3 x = x h_2$. Siispä

$$x'y' = h_1 x h_2 y = h_1 h_3 xy,$$

joten $xy \sim x'y'$. Loppu seuraa Propositiosta 3.7.

(2) Jos laskutoimitus on yhteensopiva relaation $\underset{v}{\sim}$ kanssa, niin $G/H$ varustettuna tekijälaskutoimituksella on ryhmä Proposition 3.7 nojalla. Luonnollisen homomorfismin $G \to G/H$ ydin on $H$. Proposition 4.17 nojalla $H$ on normaali. □

Huomautuksia: (1) Lauseen 4.21 väite pätee myös relaatiolle $\underset{o}{\sim}$. Molemmissa tapauksissa $H$ on normaali aliryhmä, joten vasen ja oikea ekvivalenssirelaatio ovat sama relaatio.
(2) Tekijäryhmän $G/H$ laskutoimitusta merkitään $xHyH = xyH$. Jos laskutoimitus on yhteenlasku, on nytkin luontevinta merkitä sivuluokkia $x+H$:lla ja $y+H$:lla, jolloin tekijäryhmän laskutoimitus on $(x + H) + (y + H) = (x + y) + H$.

Lause 4.22 (Ryhmien isomorfismilause). *Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Tällöin*

$$\operatorname{Im}\phi \cong G/\ker\phi.$$

*Todistus.* Kuvaus $\psi : G/\ker\phi \to \operatorname{Im}\phi$,

$$\psi(x \ker\phi) = \phi(x),$$

on hyvin määritelty: Jos $x \sim y$, niin $x^{-1}y \in \ker\phi$, joten $\phi(x) = \phi(y)$. Osoitamme, että se on homomorfismi: Olkoot $x, y \in G$. Tällöin

$$\psi(x\ker\phi)\psi(y\ker\phi) = \phi(x)\phi(y) = \phi(xy) = \psi(xy\ker\phi) = \psi(x\ker\phi\ y\ker\phi).$$

Selvästi kuvaus $\psi$ on surjektio. Injektiivisyyden toteamiseksi osoitamme, että kuvauksen $\psi$ ydin koostuu ainoastaan tekijäryhmän $G/\ker\phi$ neutraalialkiosta $\ker\phi$. Jos $\psi(x\ker\phi) = e'$, niin $\phi(x) = e'$, joten $x \in \ker\phi$, mistä seuraa $x\ker\phi = \ker\phi$. □

LAUSE 4.23. *Olkoot $K \leq H \leq G$, $K \trianglelefteq G$, $H \trianglelefteq G$. Tällöin kuvaus $\phi\colon G/K \to G/H$, $\phi(xK) = xH$ on surjektiivinen homomorfismi,* $\ker\phi = H/K$. *Erityisesti ryhmät $G/H$ ja $(G/K)/(H/K)$ ovat isomorfisia.*

*Todistus.* Mieti, miksi kuvaus on hyvin määritelty! Surjektiivisuus on selvää. Lisäksi

$$\phi(xKyK) = \phi(xyK) = xyH = xHyH = \phi(xK)\phi(yK),$$

joten kuvaus on homomorfismi. Lisäksi $\phi(yK) = yH = H$, kun $y \in H$, joten $H/K \subset \ker\phi$. Toisaalta, jos $y \notin H$, niin $yH \neq H$, joten $H/K = \ker\phi$. Viimeinen väite seuraa isomorfismilauseesta 4.22. □

Samaan tapaan todistetaan

LAUSE 4.24. *Olkoon kuvaus $\phi\colon G \to G'$ surjektiivinen ryhmähomomorfismi, ja olkoon $H' \trianglelefteq G'$. Tällöin $G/\phi^{-1}(H') \cong G'/H'$.*

*Todistus.* Proposition 4.17(2) mukaan $H = \phi^{-1}(H') \trianglelefteq G$. Olkoon $\pi\colon G' \to G'/H'$ luonnollinen homomorfismi. Tällöin $\widetilde{\psi} = \pi \circ \phi\colon G \to G'/H'$ on surjektiivinen homomorfismi, jonka ydin on $H$. Lauseen 4.22 mukaan $G/H \cong G'/H'$. □

Tarkastellaan vielä hieman syklisiä ryhmiä:

LAUSE 4.25. *(1) Syklinen ryhmä on isomorfinen joko ryhmän $\mathbb{Z}$ tai jonkin ryhmän $\mathbb{Z}_n$, $n \in \mathbb{N}$ kanssa.*
*(2) Jokainen syklisen ryhmän aliryhmä on syklinen.*
*(3) Jokainen syklisen ryhmän tekijäryhmä on syklinen.*

*Todistus.* (1) Harjoitustehtävä 50.
(2) Äärettömälle sykliselle ryhmälle tämä seuraa Esimerkistä 4.3(4). Tämä todistus toimii kaikille: Olkoon $C$ syklinen ryhmä, ja olkoon $H < C$. Olkoon $g$ ryhmän $C$ virittäjä, ja olkoon $\phi\colon \mathbb{Z} \to C$ homomorfismi $\phi(n) = g^n$. Tällöin $\phi^{-1}(H) < \mathbb{Z}$, joten $\phi^{-1}(H) = N\mathbb{Z}$ jollain $N \in \mathbb{Z}$. Jos $h \in H$, niin $h = \phi(kN) = \phi(N)^k$ jollakin $k \in \mathbb{Z}$. Siis

$$H = \langle\phi(N)\rangle = \langle g^N\rangle.$$

(3) Harjoitustehtävä 54. □

**Harjoitustehtäviä.**

TEHTÄVÄ 36. Määritä kaikki ryhmien $\mathbb{Z}_6$ ja $\mathbb{Z}_7$ aliryhmät.

TEHTÄVÄ 37. Osoita, että ryhmät $\mathbb{Z}_4$ ja $\mathbb{Z}_2 \times \mathbb{Z}_2$ eivät ole isomorfisia.

TEHTÄVÄ 38. Osoita, että ryhmät $\mathbb{Z}_6$ ja $\mathbb{Z}_2 \times \mathbb{Z}_3$ ovat isomorfisia.

[37]Vihje: Osoita, että $\mathbb{Z}_2 \times \mathbb{Z}_2$ ei ole syklinen ryhmä.
[38]Vihje: Osoita, että $\mathbb{Z}_2 \times \mathbb{Z}_3$ on syklinen ryhmä.

TEHTÄVÄ 39. Osoita, että aliryhmien leikkaus on aliryhmä. Siis: Olkoon $G$ ryhmä, ja olkoot $H_i \leq G$, $i \in I$. Osoita, että $\bigcap_{i\in I} H_i \leq G$.

TEHTÄVÄ 40. Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Olkoon $H' \leq G'$. Osoita: $\phi^{-1}(H') \leq G$.

TEHTÄVÄ 41. Määritä matriisien $A, B, C \in \mathrm{SL}_2\mathbb{Z}$ kertaluvut, kun

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ ja } C = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

TEHTÄVÄ 42. Osoita, että relaatiot

$$x \underset{v}{\sim} y \iff x^{-1}y \in H \quad \text{ja} \quad x \underset{o}{\sim} y \iff yx^{-1} \in H.$$

ovat ekvivalenssirelaatioita.

TEHTÄVÄ 43. Olkoon $G$ ryhmä, ja olkoon $H < G$. Osoita, että tekijäjoukkojen välinen kuvaus $b : G/H \to H\backslash G$, $b(aH) = Ha^{-1}$ on bijektio.

---

Olkoon $S_n = S\big(\{1, 2, \ldots, n\}\big)$. Kuvaus $f \in S_n$ voidaan esittää matriisin tapaan luettelemalla kaikkien alkioiden kuvat näin:

$$\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ f(1) & f(2) & \ldots & f(n-1) & f(n) \end{pmatrix}$$

Kun $n = 3$, kahden kuvauksen yhdistetty kuvaus saadaan näin:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

---

TEHTÄVÄ 44. Määritä ryhmän $S_3$ kaikki aliryhmät.

TEHTÄVÄ 45. Onko alkion $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ virittämä syklinen aliryhmä ryhmän $S_3$ normaali aliryhmä?

TEHTÄVÄ 46. Ryhmän $G$ *keskus* on

$$Z = \{z \in G : zg = gz \text{ kaikilla } g \in G\}.$$

Osoita, että $Z$ on kommutatiivinen normaali aliryhmä. Määritä ryhmän $S_3$ keskus.

TEHTÄVÄ 47. Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Olkoon $H' \trianglelefteq G'$. Osoita, että

$$\phi^{-1}(H') \trianglelefteq G.$$

TEHTÄVÄ 48. Olkoon $G$ ryhmä, ja olkoon $H < G$. Osoita, että $H \lhd G$, jos ja vain jos kaikille $g \in G$ pätee $gH = Hg$.

TEHTÄVÄ 49. Olkoon $A^t$ neliömatriisin $A$ transpoosi, ja olkoon $I_n$ identtinen $n \times n$-matriisi. Olkoon

$$O(n) = \{A \in \mathrm{GL}_n\mathbb{R} : AA^t = I_n\}.$$

Osoita, että $O(n) < \mathrm{GL}_n\mathbb{R}$. Onko $O(n) \lhd \mathrm{GL}_n\mathbb{R}$?

TEHTÄVÄ 50. Olkoon $C$ syklinen ryhmä. Osoita, että $C$ on isomorfinen joko ryhmän $\mathbb{Z}$ tai jonkin ryhmän $\mathbb{Z}_n$, $n \in \mathbb{N}$ kanssa.

TEHTÄVÄ 51. Olkoon $G$ äärellinen ryhmä. Olkoot $K < H < G$. Osoita Lagrangen lauseen avulla, että indekseille pätee:

$$[G : K] = [G : H][H : K].$$

TEHTÄVÄ 52. Olkoon $G$ ryhmä. Olkoot $K < H < G$ siten, että $[G : H] < \infty$ ja $[H : K] < \infty$. Osoita, että indekseille pätee:

$$[G : K] = [G : H][H : K].$$

TEHTÄVÄ 53. Olkoon $G$ ryhmä. Osoita, että ryhmän $G$ sisäiset automorfismit muodostavat ryhmän $\mathrm{Aut}(G)$ normaalin aliryhmän.

TEHTÄVÄ 54. Olkoon $C$ syklinen ryhmä. Osoita, että kaikki ryhmän $C$ tekijäryhmät ovat syklisiä.

TEHTÄVÄ 55. Olkoon $G$ ryhmä, ja olkoon $\sim$ ekvivalenssirelaatio, joka on yhteensopiva ryhmän $G$ laskutoimituksen kanssa. Osoita, että neutraalialkion $e \in G$ ekvivalenssiluokka on ryhmän $G$ normaali aliryhmä.

TEHTÄVÄ 56. Olkoon

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \right\}.$$

Joukko $G$ varustettuna matriisien kertolaskulla on ryhmä.

(1) Onko ryhmä $G$ kommutatiivinen?
(2) Onko ryhmä $G$ isomorfinen ryhmän $\mathbb{Z}_p \times \mathbb{Z}_q$ kanssa joillakin $p, q \in \mathbb{N}$?
(3) Luettele kaikki ryhmän $G$ aliryhmät, jotka ovat isomorfisia ryhmän $\mathbb{Z}_2$ kanssa.

TEHTÄVÄ 57. Olkoon

$$K = \{([0], [0]), ([1], [1]), ([2], [2])\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3.$$

Osoita, että ryhmä $\mathbb{Z}_3$ on isomorfinen tekijäryhmän $(\mathbb{Z}_3 \times \mathbb{Z}_3)/K$ kanssa.

## 5. RENKAAT

Tarkastelemme seuraavaksi rakenteita, joissa on määritelty kaksi laskutoimitusta, joista toinen on kommutatiivinen. Vaadimme muuten samat ominaisuudet kuin kokonaisluvuilta, mutta kertolasku ei välttämättä ole kommutatiivinen.

MÄÄRITELMÄ 5.1. Olkoon $R \neq \emptyset$ joukko, jolla on määritelty kaksi assosiatiivista laskutoimitusta, kommutatiivinen laskutoimitus $+$ ja toinen laskutoimitus, jota merkitsemme kertolaskulla. Kolmikko $(R, +, \cdot)$ on *(ykkösellinen) rengas*, jos

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

[52]Vihje: Oletetaan, että $G = \bigcup_{i=1}^{m} a_i H$ ja $H = \bigcup_{j=1}^{n} b_j K$, ja että yhdisteiden joukot ovat erillisiä. Osoita, että $G = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} a_i b_j K$, ja että yhdisteen joukot ovat erillisiä.

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

HUOMAA: Joskus renkaalta ei vaadita ominaisuutta (3). Tällöin yllä määrittelemäämme rakennetta kutsutaan ykköselliseksi renkaaksi.

PROPOSITIO 5.2. *Olkoon $R$ rengas. Tällöin*

(1) $0_R \cdot x = 0_R$ *kaikilla* $x \in R$,
(2) $x(-y) = (-x)y = -(xy)$ *kaikilla* $x, y \in R$,
(3) $x(y - z) = xy - xz$ *ja* $(y - z)x = yx - zx$ *kaikilla* $x, y, z \in R$,
(4) *jos* $\#R \geq 2$, *niin* $0 \neq 1$,
(5) *jos* $\#R \geq 2$, *niin* $0$*:lla ei ole käänteisalkiota kertolaskun suhteen.*

*Todistus.* (1) Distributiivisuuden nojalla

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

kaikilla $x \in R$. Supistussäännöstä seuraa, että $0_R x = 0_R$.
(5) Seuraa kohdista (4) ja (1).
Loput harjoitustehtävässä 60. □

ESIMERKKI 5.3. (1) $\mathbb{Z}$, $\mathbb{R}$ ja $\mathbb{Q}$ ovat kommutatiivisia renkaita.
(2) Olkoon $p \in \mathbb{N}$. Kokonaislukujen kertolasku on yhteensopiva kongruenssin $\equiv$,

$$a \equiv a' \iff a' = a + kp \text{ jollain } k \in \mathbb{Z}$$

kanssa. Tätä kongruenssia merkitään usein $a \equiv a' \mod p$, ja sanotaan, että $a$ on kongruentti luvun $a'$ kanssa modulo $p$. Joukko $\mathbb{Z}_p$ varustettuna kokonaislukujen yhteen- ja kertolaskujen tekijälaskutoimituksilla on kommutatiivinen rengas. (Harjoitustehtävä 58)
(3) Olkoon $X \neq \emptyset$, ja olkoon $R$ rengas. Olkoon $\mathscr{F}(X, R)$ joukko, joka koostuu kaikista kuvauksista joukolta $X$ renkaaseen $R$. Määritellään tässä joukossa yhteen- ja kertolasku pisteittäin: Olkoot $f, g \in \mathscr{F}(X, R)$. Asetamme

$$(f + g)(x) = f(x) + g(x) \text{ ja } (fg)(x) = f(x)g(x)$$

kaikilla $x \in X$. Joukko $\mathscr{F}(X, R)$ varustettuna näillä laskutoimituksilla on rengas, jota kutsutaan *kuvausrenkaaksi*. Se on kommutatiivinen, jos $R$ on kommutatiivinen. Esimerkiksi siis $\mathscr{F}(\mathbb{R}, \mathbb{R})$ on kommutatiivinen rengas.
(4) Olkoon $(A, +)$ kommutatiivinen ryhmä. Olkoon

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

Määrittelemme joukkoon $\mathrm{Hom}(A, A)$ kaksi laskutoimitusta: Homomorfismien yhteenlasku: $(\phi + \phi')(a) = \phi(a) + \phi'(a)$, ja homomorfismien yhdistäminen. Yhteenlasku on laskutoimitus: Jos $\phi, \phi' \in \mathrm{Hom}(A, A)$, niin

$$(\phi+\phi')(a+b) = \phi(a+b)+\phi'(a+b) = \phi(a)+\phi(b)+\phi'(a)+\phi'(b) = (\phi+\phi')(a)+(\phi+\phi')(b),$$

joten $\phi + \phi' \in \mathrm{Hom}(A, A)$. $(\mathrm{Hom}(A, A), +)$ on kommutatiivinen ryhmä: Laskutoimituksen assosiatiivisuus ja kommutatiivisuus on helppo tarkastaa (Harjoitustehtävä 61). Homomorfismin $\phi$ käänteisalkio yhteenlaskun suhteen on $\bar{\phi}$, $\bar{\phi}(a) = -a$ kaikilla $a \in A$, ja nollahomomorfismi $n$, $n(a) = 0$ kaikille $a \in A$, on neutraalialkio.

Identtinen homomorfismi on kertolaskun neutraalialkio, joten tarkastettavaksi jää distributiivisuus: Olkoot $\phi, \psi, \zeta \in \mathrm{Hom}(A, A)$. Tällöin

$$(\psi + \zeta)\phi(a) = \psi\phi(a) + \zeta\phi(a) = (\psi\phi + \zeta\phi)(a),$$

ja

$$\phi(\psi + \zeta)(a) = \phi(\psi(a) + \zeta(a)) = \phi\psi(a) + \phi\zeta(a) = (\phi\psi + \phi\zeta)(a).$$

(5) Olkoon $R$ rengas, $\#R \geq 2$. $R$-kertoimisten $n \times n$-matriisien joukko $\mathrm{M}_n R$ varustettuna matriisien yhteen- ja kertolaskulla on rengas. Kaikki muut ominaisuudet paitsi distributiivisuus osoitettiin tapauksessa $n = 2$ ja $R = \mathbb{R}$ harjoitustehtävissä 5, 6 ja 7. Kun $n \geq 2$, niin $\mathrm{M}_n R$ ei ole kommutatiivinen rengas, koska matriisien kertolasku ei ole kommutatiivinen.

MÄÄRITELMÄ 5.4. Olkoot $R$ ja $R'$ renkaita. Kuvaus $\phi : R \to R'$ on rengashomomorfismi, jos se on homomorfismi yhteenlaskulle ja kertolaskulle, ja jos lisäksi $\phi(1) = 1$. Bijektiivinen rengashomomorfismi on *rengasisomorfismi*.

Muista: Harjoitustehtävissä 20 ja 21 osoitettiin, että surjektiivinen homomorfismi kuvaa neutraalialkion neutraalialkioksi, mutta ilman surjektiivisuutta näin ei välttämättä ole.

PROPOSITIO 5.5. *Jos $f\colon R \to S$ ja $g\colon S \to T$ ovat rengashomomorfismeja, niin $g \circ f$ on rengashomomorfismi. Rengashomomorfismi $f\colon R \to S$ on rengasisomorfismi, jos ja vain jos on rengashomomorfismi $\bar{f}\colon S \to R$, jolle $\bar{f} \circ f = \mathrm{id}_R$ ja $f \circ \bar{f} = \mathrm{id}_S$.*

*Todistus.* Harjoitustehtävä 62. □

MÄÄRITELMÄ 5.6. Olkoon $R$ rengas. Jos $S \subset R$ varustettuna indusoiduilla laskutoimituksilla on rengas, ja jos $1_S = 1_R$, niin $S$ on renkaan $R$ *alirengas*.

Halutaan siis, että inkluusiokuvaus $i : S \to R$, $i(s) = s$ on rengashomomorfismi. Alirenkaalle on samanlainen testi kuin aliryhmälle (Propositio 4.6).

PROPOSITIO 5.7. *Olkoon $R$ rengas, ja olkoon $S \subset R$, $S \neq \emptyset$. Tällöin $S$ on renkaan $R$ alirengas, jos ja vain jos*

(1) *Kaikille $x, y \in S$ $x + y \in S$ ja $xy \in S$, ja*
(2) *$-1 \in S$.*

*Todistus.* Harjoitustehtävä 66. □

ESIMERKKI 5.8. (1) $\mathbb{Z}$ on $\mathbb{Q}$:n alirengas.
(2) Joukko

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

on rengas renkaasta $\mathrm{M}_2\mathbb{R}$ indusoiduilla laskutoimituksilla. Sen kertolaskun neutraalialkio on $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, joten $S$ ei ole renkaan $\mathrm{M}_2\mathbb{R}$ alirengas. Rengas $S$ on rengasisomorfinen renkaan $\mathbb{R}$ kanssa: Kuvaus $a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ on rengasisomorfismi.
(3) Olkoon

$$R = \{ f\colon [0, 1] \to \mathbb{R} \}.$$

Kuvaus $h\colon R \to \mathbb{R}$, $h(f) = f(\frac{1}{2})$ on rengashomomorfismi:

$$h(f+g) = (f+g)(1/2) = f(1/2) + g(1/2) = h(f) + h(g),$$

ja niin edelleen.
(4) Samaan tapaan kuin permutaatioryhmille määriteltiin aliryhmiä rajoittumalla kuvauksiin, joilla on tiettyjä ominaisuuksia, voimme määritellä kuvausrenkaiden $\mathscr{F}(X, R)$ alirenkaita. Tällaisia ovat esimerkiksi kuvausrenkaan $\mathscr{F}(\mathbb{R}, \mathbb{R})$ alirenkaat (vertaa Analyysi 2)

$$C(\mathbb{R}) = \{f\colon \mathbb{R} \to \mathbb{R} : f \text{ on jatkuva}\}, \text{ ja}$$
$$C^k(\mathbb{R}) = \{f\colon \mathbb{R} \to \mathbb{R} : f \text{ on } k \text{ kertaa jatkuvasti derivoituva}\}, \ k \in \mathbb{N}.$$

(5) Olkoon

$$\mathscr{L}(\mathbb{R}^n) = \{L : \mathbb{R}^n \to \mathbb{R}^n : L \text{ on lineaarikuvaus}\}.$$

Osoita, että $\mathscr{L}(\mathbb{R}^n)$ on renkaan $\mathrm{Hom}(\mathbb{R}^n, \mathbb{R}^n)$ alirengas: Lineaarikuvaukset ovat ryhmän $(\mathbb{R}^n, +)$ homomorfismeja itselleen, joten niiden summa on myös homomorfismi. Lisäksi aina, kun $L, L' \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^n)$, $x \in \mathbb{R}^n$ ja $a \in \mathbb{R}$, myös

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

joten lineaarikuvauksen toinenkin ehto toteutuu. Lineaarialgebran kurssilla on osoitettu, että lineaarikuvausten yhdistetty kuvaus on lineaarikuvaus. Siis molemmat laskutoimitukset toteuttavat Proposition 5.7 ehdon (1). Lisäksi identtinen kuvaus $\mathrm{id}\colon \mathbb{R}^n \to \mathbb{R}^n$ on lineaarikuvaus, kuten myös $-\mathrm{id}$, joten Proposition 5.7 mukaan $\mathscr{L}(\mathbb{R}^n, \mathbb{R}^n)$ on alirengas.

Alirenkaat ja rengashomomorfismit ovat yhteensopivia samaan tapaan kuin ryhmähomomorfismit:

PROPOSITIO 5.9. *Olkoon $\phi\colon R \to R'$ rengashomomorfismi.*
*(1) Olkoon $S$ renkaan $R$ alirengas. Tällöin $\phi(S)$ on renkaan $R'$ alirengas.*
*(2) Olkoon $S'$ renkaan $R'$ alirengas. Tällöin $\phi^{-1}(S')$ on renkaan $R$ alirengas.*

*Todistus.* (1) Proposition 4.8 mukaan riittää tarkastella kertolaskua ja ykkösen kuvautumista. Olkoot $\phi(a), \phi(b) \in \phi(S)$. Tällöin $\phi(a)\phi(b) = \phi(ab) \in \phi(S)$. Koska $-1_R \in S$, pätee $\phi(-1_R) = -\phi(1_R) = -1_{R'} \in \phi(S)$.
(2) Harjoitustehtävä 67.

□

MÄÄRITELMÄ 5.10. Olkoon $R$ rengas, $\#R \geq 2$.

(1) Jos $a, b, c \in R$ siten, että $ab = c$, niin $a$ ja $b$ ovat $c$:n *tekijöitä*.
(2) Jos $a, b \in R$, $a, b \neq 0$, 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, niin $R$ on *vino kunta* eli *jakorengas*.
(5) Kommutatiivinen jakorengas on *kunta*.

Yleensä nimitystä vino kunta käytetään vain sellaisista jakorenkaista, jotka eivät ole kuntia. Jos $d, m \in R$ ja $d$ on $m$:n tekijä sanotaan joskus, että $d$ jakaa $m$:n ja merkitään $d \mid m$.

Esimerkki 5.11. (1) $\mathbb{Z}$ on kokonaisalue mutta se ei ole jakorengas eikä siis kunta.
(2) $\mathbb{Q}$ ja $\mathbb{R}$ ovat kuntia.
(3) $\mathrm{M}_n R$ ei ole kokonaisalue, kun $n \geq 2$ ja $R$ on kunta. Jos $A, B \in \mathrm{M}_n R$, ja niiden ainoat nollasta poikkeavat kertoimet ovat $A_{11}$ ja $B_{nn}$, niin $AB = 0$.
(4) Määritellään joukossa $\mathbb{R}^4$ yhteenlasku komponenteittain, ja kertolasku asettamalla

$$\begin{aligned} ab &= (a_1, a_2, a_3, a_4)(b_1, b_2, b_3, b_4) \\ &= \big(a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4,\ a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3, \\ &\qquad a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2,\ a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1\big). \end{aligned}$$

Näillä laskutoimituksilla varustettuna $\mathbb{R}^4$ on vino kunta $\mathbb{H}$, *(Hamiltonin) kvaterniot*. Kertolaskun neutraalialkio on $(1, 0, 0, 0)$, tarkasta distributiivisuus! Se ei ole kommutatiivinen, koska

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

Alkion $(a, b, c, d) \in \mathbb{H} \setminus \{0\}$ käänteisalkio kertolaskun suhteen on $\dfrac{(a, -b, -c, -d)}{a^2 + b^2 + c^2 + d^2}$.

Propositio 5.12. *(1) Jakorenkaassa ei ole nollan jakajia. Erityisesti kunta on kokonaisalue.*
*(2) Äärellinen kokonaisalue on kunta.*

*Todistus.* (1) Olkoon $K$ jakorengas. Olkoot $a, b \in K$, $a, b \neq 0$. Tällöin $a$ ja $b$ ovat yksiköitä, joten niillä on käänteisalkiot kertolaskun suhteen. Oletetaan, että $ab = 0$. Silloin $b = a^{-1}0 = 0$, mikä on ristiriita.
(2) Olkoon $E$ äärellinen kokonaisalue. Olkoon $a \in E$, $a \neq 0$. Kuvaus $V_a : E \to E$, $V_a(x) = ax$ on injektio: Jos $V_a(x) = V_a(y)$, niin $a(x-y) = 0$. Koska kokonaisalueessa $E$ ei ole nollan jakajia, $x = y$. Kuvaus $V_a$ on surjektio, koska $E$ on äärellinen. Siis on $\bar{a} \in E$, jolle $a\bar{a} = 1$. Koska $E$ on kommutatiivinen, $\bar{a} = a^{-1}$. □

Määritelmä 5.13. Jos $K$ on kunta ja $K' \subset K$ varustettuna indusoiduilla laskutoimituksilla on kunta, niin $K'$ on kunnan $K$ *alikunta*.

**Harjoitustehtäviä.**

Tehtävä 58. Osoita, että kokonaislukujen kertolasku on yhteensopiva kongruenssin kanssa. Osoita, että $\mathbb{Z}_p$ varustettuna kokonaislukujen yhteen- ja kertolaskujen tekijälaskutoimituksilla on kommutatiivinen rengas.

Tehtävä 59. Olkoon $X$ joukko. Määritellään joukkojen $A, B \in \mathscr{P}(X)$ *symmetrinen erotus* asettamalla

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

Osoita, että $\big(\mathscr{P}(X), \triangle, \cap\big)$ on rengas. Onko se kommutatiivinen?

Tehtävä 60. Olkoon $R$ rengas. Osoita, että

(1) $x(-y) = (-x)y = -(xy)$ kaikilla $x, y \in R$,
(2) $x(y - z) = xy - xz$ ja $(y - z)x = yx - zx$ kaikilla $x, y, z \in R$,
(3) jos $\#R \geq 2$, niin $0_R \neq 1_R$.

Tehtävä 61. Olkoon $(A, +)$ kommutatiivinen ryhmä, ja olkoon

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

Näytä, että joukon $\mathrm{Hom}(A, A)$ laskutoimitus $+$, joka määritellään asettamalla

$$(\phi + \phi')(a) = \phi(a) + \phi'(a),$$

on assosiatiivinen ja kommutatiivinen.

Tehtävä 62. Todista Propositio 5.5.

Tehtävä 63. Olkoon $R^*$ renkaan $R$ yksiköiden joukko. Osoita, että $R^*$ varustettuna kertolaskun indusoimalla laskutoimituksella on ryhmä.

Tehtävä 64. Määritellään joukossa $\mathbb{Z}^3$ yhteenlasku komponenteittain ja kertolasku asettamalla

$$(a, b, c)(x, y, z) = (ax, bx + cy, cz)$$

kaikilla $(a, b, c), (x, y, z) \in \mathbb{Z}^3$. Onko $\mathbb{Z}^3$ varustettuna näillä laskutoimituksilla rengas? Onko se kommutatiivinen?

Tehtävä 65. Olkoot

$$R = \{f\colon [0, 1] \to \mathbb{R}\}$$

ja

$$S = \{f\colon [0, 2] \to \mathbb{R}\}$$

varustettu kuvausrenkaiden laskutoimituksilla. Ovatko renkaat $R$ ja $S$ isomorfisia?

Tehtävä 66. Olkoon $R$ rengas, ja olkoon $S \subset R$, $S \neq \emptyset$. Osoita, että $S$ on renkaan $R$ alirengas, jos ja vain jos

- $x + y \in S$ ja $xy \in S$ kaikilla $x, y \in S$, ja
- $-1 \in S$.

Tehtävä 67. Olkoon $\phi\colon R \to R'$ rengashomomorfismi. Olkoon $S'$ renkaan $R'$ alirengas. Osoita, että $\phi^{-1}(S')$ on renkaan $R$ alirengas.

Tehtävä 68. Olkoon $K$ kunta, ja olkoon $K'$ sen alikunta. Osoita, että alikunnan $K'$ yhteenlaskun ja kertolaskun neutraalialkiot ovat samat kuin kunnan $K$.

Tehtävä 69. Osoita, että kunnan $K$ osajoukko $K'$ on $K$:n alikunta, jos ja vain jos

- $\#K' \geq 2$,
- $a - b \in K'$ kaikilla $a, b \in K'$, ja
- $ab^{-1} \in K'$ kaikilla $a, b \in K'$, $b \neq 0$.

## 6. Renkaat $\mathbb{Z}$ ja $\mathbb{Z}_p$

Tarkastelemme lyhyesti lähinnä jaollisuutta renkaassa $\mathbb{Z}$ ja luvun $p$ ominaisuuksien vaikutusta renkaan $\mathbb{Z}_p$ ominaisuuksiin.

[64] Vihje: $(1, 0, 1)$

MÄÄRITELMÄ 6.1. (1) Jos luku $d \in \mathbb{Z}$ jakaa kokonaisluvut $a$ ja $b$, niin $d$ on lukujen $a$ ja $b$ *yhteinen tekijä*.
(2) Jos $m, n \in \mathbb{Z} \setminus \{0\}$, niiden *suurin yhteinen tekijä* $\text{syt}(m, n)$ on luku $d > 0$, joka on lukujen $m$ ja $n$ yhteinen tekijä, jonka jokainen lukujen $m$ ja $n$ yhteinen tekijä jakaa.
(3) Jos $\text{syt}(m, n) = 1$, sanotaan, että luvut $m$ ja $n$ ovat *suhteellisia alkulukuja*, ja että $m$ ja $n$ ovat *keskenään jaottomia*.
(4) Kokonaisluku $p \geq 2$ on *alkuluku*, jos kaikilla $m, n \in \mathbb{N}$, joille $mn = p$ pätee $m = 1$ tai $n = 1$.

LEMMA 6.2. *Luvuilla $a, b \in \mathbb{Z}$ on yksikäsitteinen suurin yhteinen tekijä,*

$$\text{syt}(a, b) = \max\{d \in \mathbb{N} : d \mid a \text{ ja } d \mid b\}.$$

*Todistus.* Selvästi $\text{syt}(a, b)$ on väitetty luku, jos se on olemassa. Merkitään

$$A = \{d \in \mathbb{N} : d \mid a \text{ ja } d \mid b\}.$$

Luku 1 on jokaisen kokonaislukuparin yhteinen tekijä, erityisesti $1 \in A$.

Toisaalta, jos $d \in A$, niin $d \leq |a|$. Vastaavasti, jos $b \neq 0$, niin $d \leq |b|$. Siten jokaisella $d \in A$ pätee

$$d \leq \max\{|a|, |b|\}.$$

Luonnollisten lukujen joukko A on epätyhjä ja ylhäältä rajoitettu, joten siinä on suurin alkio, joka siis on $\text{syt}(a, b)$. □

PROPOSITIO 6.3. *Olkoot $m, n \in \mathbb{Z}\setminus\{0\}$. Tällöin $\text{syt}(m, n)$ virittää aliryhmän $\langle m, n\rangle$.*

*Todistus.* Esimerkissä 4.3(4) osoitettiin, että on $d \in \mathbb{N}$ siten, että $\langle d\rangle = \langle m, n\rangle$. Osoitamme, että $d = \text{syt}(m, n)$. Olkoon $e \neq 0$ lukujen $m$ ja $n$ yhteinen tekijä. On siis $a, b \in \mathbb{Z}$, joille $m = ae$ ja $n = be$. Koska $d \in \langle m, n\rangle$, on luvut $r, s \in \mathbb{Z}$ siten, että

$$rm + sn = d. \tag{4}$$

Siispä $d = rae + sbe = (ra + sb)e$, joten $e \mid d$. □

Yhtälöä (4) kutsutaan *Bezout'n yhtälöksi*. Suurin yhteinen tekijä voidaan määritellä vastaavasti myös useammalle kokonaisluvulle.

ESIMERKKI 6.4.

(a) $\text{syt}(12, 30) = 6$: Luvun 12 positiiviset tekijät ovat $1, 2, 3, 4, 6$ ja luvun 30 $1, 2, 3, 5, 6, 10, 15, 30$.
(b) $\text{syt}(n, n + 1) = 1$ kaikilla $n \in \mathbb{N}$: Olkoon $d \in \mathbb{N}$ lukujen $n$ ja $(n + 1)$ jakaja. Koska $d$ jakaa luvun $n + (-1)(n + 1) = -1$, niin on oltava $d = 1$. Luvuilla $n$ ja $n + 1$ ei siis ole muita positiivisia yhteisiä tekijöitä kuin 1.
(c) 10 ensimmäistä alkulukua ovat $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$. Alkulukuja on äärettömän monta. (Harjoitustehtävä 70)

Miten kahden kokonaisluvun suurin yhteinen tekijä löydetään? Ensimmäisenä mieleentuleva tapa on molempien lukujen tekijöiden listaaminen ja suurimman yhteisen tekijän etsiminen yhteisten tekijöiden joukosta. Tämä tapa on isoilla luvuilla työläs. Seuraavaan lemmaan perustuva *Eukleideen algoritmi* antaa tehokkaamman keinon suurimman yhteisen tekijän löytämiseksi.

LEMMA 6.5. *Jos $a, b, q, r \in \mathbb{Z}$ ja $a = qb + r$, niin $\text{syt}(a, b) = \text{syt}(b, r)$.*

*Todistus.* Jokainen lukujen $b$ ja $r$ yhteinen tekijä jakaa summan $qb + r = a$. Vastaavasti jokainen $a$:n ja $b$:n yhteinen tekijä jakaa luvun $a - qb = r$. Pareilla $a, b$ ja $b, r$ on siis samat yhteiset tekijät. Siten on myös $\text{syt}(a, b) = \text{syt}(b, r)$. □

EUKLEIDEEN ALGORITMI: Olkoot $a, b \in \mathbb{Z} \setminus \{0\}$. Merkitään $d = \text{syt}(a, b)$. Koska

$$\text{syt}(a, b) = \text{syt}(-a, b) = \text{syt}(a, -b) = \text{syt}(-a, -b),$$

niin voidaan olettaa, että $a, b \in \mathbb{N}$ ja että $a > b$.

Jakamalla $a$ luvulla $b$ saadaan luvut $q_1, r_1 \in \mathbb{Z}$, joille

$$a = q_1 b + r_1 \quad \text{ja } 0 \leq r_1 < b.$$

Jos $r_1 = 0$, niin $b \mid a$. Tällöin $d = b$; lopetetaan.
Jos $r_1 > 0$, jaetaan $b$ luvulla $r_1$. Jakoyhtälö antaa luvut $q_2, r_2 \in \mathbb{Z}$, joille

$$b = q_2 r_1 + r_2 \quad \text{ja } 0 \leq r_2 < r_1.$$

Lemman 6.5 nojalla $\text{syt}(a, b) = \text{syt}(b, r_1)$. Siten, jos $r_2 = 0$, niin $d = r_1$; lopetetaan. Jos $r_2 > 0$, jaetaan $r_1$ luvulla $r_2$. Jakoyhtälö antaa luvut $q_3, r_3 \in \mathbb{Z}$, joille

$$r_1 = q_3 r_2 + r_3 \quad \text{ja } 0 \leq r_3 < r_2.$$

Jatketaan kuten edellä. Koska jakoyhtälön antamat jakojäännökset $r_i$ ovat ei-negatiivisia ja muodostavat aidosti vähenevän jonon,

$$b > r_1 > r_2 > \cdots \geq 0,$$

niin jollain $n$ on oltava $r_n = 0$ (korkeintaan $b$ askelta). Viimeiset kaksi vaihetta ovat

$$\begin{aligned} r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, && 0 < r_{n-1} < r_{n-2}, \\ r_{n-2} &= q_n r_{n-1} + r_n, && r_n = 0. \end{aligned} \tag{5}$$

PROPOSITIO 6.6 (Eukleideen algoritmi). *Olkoot $a, b$ ja jakojäännökset $r_i$ kuten yllä. Tällöin $r_{n-1}$, viimeinen positiivinen jakojäännös, on* $\text{syt}(a, b)$.

*Todistus.* Lemma 6.5 sovellettuna ylläoleviin $a$:n, $b$:n, $r_1$:n, ... ja $r_{n-3}$:n yhtälöihin kertoo, että

$$d = \text{syt}(a, b) = \text{syt}(b, r_1) = \text{syt}(r_1, r_2) = \cdots = \text{syt}(r_{n-2}, r_{n-1}).$$

Yhtälön (5) perusteella $r_{n-1} \mid r_{n-2}$, joten $\text{syt}(r_{n-2}, r_{n-1}) = r_{n-1}$. Siten $d = r_{n-1}$. □

ESIMERKKI 6.7. Lasketaan $\text{syt}(22, 60)$ ja etsitään sellaiset luvut $x, y \in \mathbb{Z}$, että $\text{syt}(a, b) = xa + yb$. Eukleideen algoritmilla saadaan

$$\begin{aligned} 60 &= 2 \cdot \underline{22} + \boxed{16} && 16 = 60 - 2 \cdot 22 \\ \underline{22} &= 1 \cdot \boxed{16} + \underline{\underline{6}} && 6 = 22 - 16 \\ \boxed{16} &= 2 \cdot \underline{\underline{6}} + \boxed{4} && 4 = 16 - 2 \cdot 6 \\ \underline{\underline{6}} &= 1 \cdot \boxed{4} + \underline{2} && 2 = 6 - 4 \\ \boxed{4} &= 2 \cdot \underline{2}. \end{aligned}$$

Siten $\text{syt}(22, 60) = 2$. "Peruuttamalla" algoritmissa saadaan

$$\begin{aligned} 2 &= 6 - 4 = 6 - (16 - 2 \cdot 6) = 3 \cdot 6 - 16 = 3(22 - 16) - 16 \\ &= 3 \cdot 22 - 4 \cdot 16 = 3 \cdot 22 - 4(60 - 2 \cdot 22) \\ &= 11 \cdot 22 - 4 \cdot 60. \end{aligned}$$

Huomaa, että luvut $a, b \in \mathbb{Z}$ ovat keskenään jaottomia jos ja vain jos $xa + yb = 1$ jollain $x, y \in \mathbb{Z}$. Huomaa myös, että jos $\text{syt}(a, b) = 1$, niin kaikki kokonaisluvut $c \in \mathbb{Z}$ voidaan esittää summana $c = ka + lb$, $k, l \in \mathbb{Z}$.

Seuraavat jaollisuustulokset pätevät keskenään jaottomille luvuille. Yleisessä tapauksessa Propositio 6.8 ei ole totta.

PROPOSITIO 6.8. *Olkoot $a, b \in \mathbb{Z}$ keskenään jaottomia ja $c \in \mathbb{Z}$. Tällöin*

(1) *Jos $a \mid c$ ja $b \mid c$, niin $ab \mid c$.*
(2) *Jos $a \mid bc$, niin $a \mid c$.*

*Todistus.* (1): Koska $\text{syt}(a, b) = 1$, niin $xa + yb = 1$ jollain $x, y \in \mathbb{Z}$. Oletuksen nojalla on $k, l \in \mathbb{Z}$ siten, että $ka = c = lb$. Nyt on

$$c = c(xa + yb) = cxa + cyb = (lb)xa + (ka)yb = ab(lx + ky)$$

ja $lx + ky \in \mathbb{Z}$, joten $ab \mid c$.

(2): Kuten kohdassa (1), saadaan $c = cxa + cyb$ jollain $x, y \in \mathbb{Z}$. Koska $a \mid bc$ ja $a \mid a$, niin $a$ jakaa summan $cxa + ybc = c$. □

LEMMA 6.9 (Eukleideen lemma). *Olkoot $p$ alkuluku ja $a, b \in \mathbb{Z}$. Jos $p \mid (ab)$, niin $p \mid a$ tai $p \mid b$. Yleisemmin, jos $p \mid (a_1 \cdots a_n)$, missä $a_i \in \mathbb{Z}$ kaikilla $i = 1, \ldots, n$, niin $p \mid a_i$ jollain $i$.*

*Todistus.* Jos $p \mid a$, niin OK. Jos $p \nmid a$, niin $\text{syt}(a, p) = 1$. Proposition 6.8 (2) perusteella $p \mid b$. Yleinen tapaus todistetaan induktiolla. □

Tavoitteena on todistaa seuraava lause:

LAUSE 6.10 (Aritmetiikan peruslause). *Jokainen luonnollinen luku $n \geq 2$ voidaan esittää alkulukujen tulona. Tämä esitys on tekijöiden järjestystä vaille yksikäsitteinen.*

HUOMAA: Alkulukuesityksen yksikäsitteisyys ei ole itsestään selvä asia: Olkoon

$$\mathbb{P} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} = \{n \in \mathbb{Z} : n \text{ on parillinen}\}.$$

Yhteen-, vähennys- ja kertolasku ovat joukon $\mathbb{P}$ sisäisiä laskutoimituksia. Joukossa $\mathbb{P}$ voidaan määritellään käsitteet tekijä, jaollisuus ja alkuluku samaan tapaan kuin kokonaislukujen joukossa, esim. luku $m \in \mathbb{P}$ jakaa luvun $n \in \mathbb{P}$, jos on $k \in \mathbb{P}$ siten, että $n = km$. Joukon $\mathbb{P}$ alkulukuja ovat esimerkiksi $2, 6, 10, 14, 18, 26$ ja $30$. Nyt

$$180 = 6 \cdot 30 = 10 \cdot 18,$$

missä kaikki tekijät ovat joukon $\mathbb{P}$ alkulukuja.

LAUSEEN 6.10 TODISTUS. Olemassaolo harjoitustehtävänä 71.

Oletetaan, että

$$n = p_1 \cdots p_k = q_1 \cdots q_s, \tag{6}$$

missä $p_i, q_j$:t ovat alkulukuja.

Koska $p_1 \mid n$, niin Lemman 6.9 perusteella se jakaa $q_j$:n jollain $j = 1, \ldots, s$. Numeroimalla $q_j$:t tarvittaessa uudelleen voidaan olettaa, että $p_1 \mid q_1$. Koska $p_1$ ja $q_1$ ovat alkulukuja, niin on $p_1 = q_1$. Jakamalla (6) $p_1$:llä saadaan

$$p_2 \cdots p_k = q_2 \cdots q_s.$$

Kuten edellä päättelemme, että $p_2 = q_2$. Toistamalla prosessia, joka loppuu $k$ askeleen jälkeen, saamme $p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k$, erityisesti, $k = s$. □

MÄÄRITELMÄ 6.11. Aritmetiikan peruslauseen antamaa luvun $n \in \mathbb{N}$, $n \geq 2$, esitystä

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

missä $p_1 < \cdots < p_k$ ovat alkulukuja ja $e_1, \ldots e_k \in \mathbb{N}$, sanotaan $n$:n *alkutekijäesitykseksi*. Luvut $p_i$ ovat $n$:n *alku(luku)tekijöitä*.

Alkutekijäesityksen löytäminen isoille luvuille voi olla hankalaa. Seuraava lemma helpottaa tekijöiden löytämistä.

LEMMA 6.12. *Luku $n \in \mathbb{N}$, $n \geq 2$ ei ole alkuluku, jos ja vain jos on alkuluku $p$, jolle $p^2 \leq n$, ja joka jakaa $n$:n.*

*Todistus.* Harjoitustehtävä 72. □

ESIMERKKI 6.13. Etsitään luvun $n = 132$ alkutekijäesitys. Koska $n$ on parillinen, niin se ei ole alkuluku. Koska

$$11^2 = 121 < 132 < 144 = 12^2,$$

niin on $11 < \sqrt{n} < 12$. Siten luvulla 132 on lukua 12 pienempi alkutekijä (mahdolliset tekijät ovat 2, 3, 5, 7, 11). Nyt

$$132 = \begin{cases} 12 \cdot 11 = 2^2 \cdot 3 \cdot 11 \\ 2 \cdot 66 = 2^2 \cdot 33 = 2^2 \cdot 3 \cdot 11. \end{cases}$$

LAUSE 6.14. *Seuraavat väitteet ovat yhtäpitäviä:*

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

*Todistus.* Kohtien (1) ja (2) yhtäpitävyys seuraa Propositiosta 5.12. Osoitetaan, että kohdat (1) ja (3) ovat yhtäpitäviä: Olkoot $x, y \in \mathbb{Z} \setminus p\mathbb{Z}$. Nyt $[x][y] = [0]$, jos ja vain jos $xy = pq$ jollain $q \in \mathbb{Z}$, jos ja vain jos $p \mid xy$. Siis $\mathbb{Z}_p$ on kokonaisalue, jos ja vain jos

$$p \mid xy \implies p \mid x \text{ tai } p \mid y \text{ kaikilla } x, y \in \mathbb{Z} \setminus p\mathbb{Z}. \tag{7}$$

Proposition 6.8 mukaan (7) pätee, jos $p$ on alkuluku. Jos $p = ab$ ei ole alkuluku, niin (7) ei päde, kun $x = a$ ja $y = b$. □

Lauseen 6.14 todistusta tarkastelemalla saadaan

PROPOSITIO 6.15. *Alkio $[a] \in \mathbb{Z}_n$ on nollan jakaja, jos ja vain jos* $\operatorname{syt}(a, n) > 1$.

*Todistus.* Harjoitustehtävä 73. □

Tarkastellaan vielä yhtä renkaan $\mathbb{Z}$ erityisominaisuutta:

PROPOSITIO 6.16. *Olkoon $R$ rengas. On täsmälleen yksi rengashomomorfismi renkaalta $\mathbb{Z}$ renkaalle $R$.*

*Todistus.* Kuvaus $\phi\colon \mathbb{Z} \to R$, $\phi(n) = n1_R$ on rengashomomorfismi:

$$\phi(m+n) = (m+n)1_R = m1_R + n1_R = \phi(m) + \phi(n)$$

ja

$$\phi(mn) = mn1_R = m1_R n1_R = \phi(m)\phi(n).$$

Jos $\psi\colon \mathbb{Z} \to R$ on rengashomomorfismi, niin $\psi(1) = 1_R$. Siis $\psi(m) = m\psi(1_R)$, joten $\psi = \phi$. □

**Harjoitustehtäviä.**

TEHTÄVÄ 70. Osoita, että alkulukuja on äärettömän monta.

TEHTÄVÄ 71. Osoita, että jokainen luonnollinen luku $n \geq 2$ voidaan esittää alkulukujen tulona.

TEHTÄVÄ 72. Osoita: Luku $n \in \mathbb{N}$, $n \geq 2$ ei ole alkuluku, jos ja vain jos on alkuluku $p$ siten, että $p \mid n$ ja $p^2 \leq n$.

TEHTÄVÄ 73. Olkoot $a \in \mathbb{Z}$, $n \in \mathbb{N}$. Osoita, että $[a] \in \mathbb{Z}_n$ on nollan jakaja, jos ja vain jos $\operatorname{syt}(a, n) > 1$.

TEHTÄVÄ 74. Määritä renkaiden $\mathbb{Z}_6$ ja $\mathbb{Z}_8$ ja $\mathbb{Z}_{101}$ yksiköt.

TEHTÄVÄ 75. Olkoon $p \in \mathbb{N}$. Olkoon $a \in \mathbb{Z}$. Millä ehdolla $[a]$ on ryhmän $\mathbb{Z}_p$ virittäjä?

TEHTÄVÄ 76. (1) Mitkä alkiot ovat nollan jakajia renkaassa $\mathbb{Z}_9$?
(2) Mitkä alkiot ovat yksiköitä renkaassa $\mathbb{Z}_9$?
(3) Onko renkaan $\mathbb{Z}_9$ yksiköiden ryhmä syklinen?

## 7. Ideaalit ja tekijärenkaat

Ryhmähomomorfismin $\phi\colon G \to G'$ ydin on ryhmän $G$ normaali aliryhmä. Rengashomomorfismi $\psi\colon R \to R'$ on ryhmähomomorfismi additiivisten ryhmien $(R, +)$ ja $(R', +)$ välillä, joten rengashomomorfismin $\psi$ *ydin*

$$\ker \psi = \{x \in R : \psi(x) = 0\}$$

on additiivisen ryhmän $(R, +)$ normaali aliryhmä. Kertolaskun suhteen homomorfisuus antaa ytimelle lisää rakennetta.

MÄÄRITELMÄ 7.1. Olkoon $R$ rengas, ja olkoon $\mathscr{I} \subset R$ siten, että $(\mathscr{I}, +)$ on ryhmän $(R, +)$ aliryhmä.

(1) $\mathscr{I}$ on *vasen ideaali*, jos $xa \in \mathscr{I}$ kaikilla $x \in R$ ja $a \in \mathscr{I}$.
(2) $\mathscr{I}$ on *oikea ideaali*, jos $ay \in \mathscr{I}$ kaikilla $y \in R$ ja $a \in \mathscr{I}$.
(3) $\mathscr{I}$ on *kaksipuolinen ideaali*, jos $xay \in \mathscr{I}$ kaikilla $x, y \in R$ ja $a \in \mathscr{I}$.

HUOMAA: Jos $R$ on kommutatiivinen rengas, niin Määritelmän 7.1 kohdissa (1)–(3) määritellyt käsitteet ovat kaikki samoja. Tällöin $\mathscr{I}$:tä sanotaan *ideaaliksi*.

[70] Vihje: Olkoot $p_1, p_2, \ldots, p_n$ alkulukuja. Mitä voit päätellä luvusta $p_1 p_2 \cdot \cdots \cdot p_n + 1$?

LEMMA 7.2. *(1) $\mathscr{I}$ on vasen ideaali, jos ja vain jos $xa + x'a' \in \mathscr{I}$ kaikilla $x, x' \in R$ ja $a, a' \in \mathscr{I}$.*
*(2) $\mathscr{I}$ on oikea ideaali, jos ja vain jos $ay + a'y' \in \mathscr{I}$ kaikilla $y, y' \in R$ ja $a, a' \in \mathscr{I}$.*
*(3) $\mathscr{I}$ on kaksipuolinen ideaali, jos ja vain jos se on vasen ideaali ja oikea ideaali.*

*Todistus.* (1) ja (3) harjoitustehtävässä 77. □

ESIMERKKI 7.3. (1) $R$ ja $\{0\}$ ovat renkaan $R$ kaksipuolisia ideaaleja.
(2) $n\mathbb{Z}$ on renkaan $\mathbb{Z}$ ideaali.
(3) Olkoot $X \neq \emptyset$, $\emptyset \neq A \subset X$, ja $R$ rengas. Olkoon

$$N(A) = \{f \in \mathscr{F}(X, R) : f(a) = 0 \text{ kaikilla } a \in A\}.$$

Tällöin $N(A)$ on kuvausrenkaan $\mathscr{F}(X, R)$ kaksipuolinen ideaali. Samalla tavalla saadaan kaksipuolisia ideaaleja monille renkaan $\mathscr{F}(X, R)$ alirenkaille, esimerkiksi

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

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

PROPOSITIO 7.4. *Olkoon $\phi\colon R \to S$ rengashomomorfismi.*
*(1) Jos $\mathscr{I} \subset R$ on vasen/oikea/kaksipuolinen ideaali, niin $\phi(\mathscr{I})$ on renkaan $\phi(S)$ vasen/oikea/kaksipuolinen ideaali.*
*(2) Jos $\mathscr{I} \subset S$ on vasen/oikea/kaksipuolinen ideaali, niin $\phi^{-1}(\mathscr{I})$ on renkaan $R$ vasen/oikea/kaksipuolinen ideaali.*
*(3) Rengashomomorfismin ydin on määrittelyrenkaansa kaksipuolinen ideaali.*

*Todistus.* (1) Harjoitustehtävä 78.
(2) Tarkastelemme vain tapausta, jossa $\mathscr{I}$ on vasen ideaali. Muut tapaukset todistetaan vastaavasti. Proposition 4.8 nojalla $(\phi^{-1}(\mathscr{I}), +) < (R, +)$. Olkoot $a \in \phi^{-1}(\mathscr{I})$ ja $r \in R$. Tällöin $\phi(ra) = \phi(r)\phi(a) \in \mathscr{I}$, koska $\mathscr{I}$ on vasen ideaali. Siis $ra \in \phi^{-1}(\mathscr{I})$.
(3) Seuraa kohdasta (2). □

ESIMERKKI 7.5. Luonnollinen kuvaus $\mathbb{Z} \to \mathbb{Z}_p$ on surjektiivinen rengashomomorfismi, joten renkaan $\mathbb{Z}_p$ ideaalit ovat täsmälleen renkaan $\mathbb{Z}$ ideaalien kuvat. Siis kaikki renkaan $\mathbb{Z}_p$ aliryhmät ovat ideaaleja.

PROPOSITIO 7.6. *(1) Jos renkaan $R$ vasen/oikea/kaksipuolinen ideaali $\mathscr{I}$ on alirengas, niin $\mathscr{I} = R$.*
*(2) Olkoon $R$ jakorengas, ja olkoon $\mathscr{I}$ sen vasen/oikea/kaksipuolinen ideaali. Silloin $\mathscr{I} = R$ tai $\mathscr{I} = \{0\}$. Erityisesti, jos $R$ on kunta, niin sen ainoat ideaalit ovat $\{0\}$ ja $R$.*

*Todistus.* Tarkastelemme ainoastaan vasempia ideaaleja. Oikeat ideaalit tarkastellaan samalla tavalla.
(1) Jos $\mathscr{I}$ on renkaan $R$ vasen ideaali ja $1 = 1_R \in \mathscr{I}$, niin kaikilla $x \in R$ pätee $x = x1 \in \mathscr{I}$, joten $\mathscr{I} = R$.
(2) Jos $a \in R^*$, niin sillä on käänteisalkio $a^{-1}$. Jos $\mathscr{I}$ on vasen ideaali, jolle $a \in \mathscr{I}$, niin $1 = a^{-1}a \in \mathscr{I}$. Väite seuraa kohdasta (1). □

PROPOSITIO 7.7. *Olkoot $\mathscr{I}_i$, $i \in I$, $\mathscr{I}_1$ ja $\mathscr{I}_2$ renkaan $R$ vasempia/oikeita/ kaksipuolisia ideaaleja. Tällöin*

$$\bigcap_{i\in I} \mathscr{I}_i \quad ja \quad \mathscr{I}_1 + \mathscr{I}_2 = \{x_1 + x_2 : x_j \in \mathscr{I}_j\}$$

*ovat renkaan $R$ vasempia/oikeita/kaksipuolisia ideaaleja.*

*Todistus.* Harjoitustehtävät 80 ja 81. □

Jos $S \subset R$, $S \neq \emptyset$, joukon $S$ virittämä vasen/oikea/kaksipuolinen ideaali on joukon $S$ sisältävien ideaalien leikkaus.

Kaksipuolinen ideaali vastaa Proposition 7.4 mukaan rengasteoriassa ryhmäteorian normaalia aliryhmää. Huomaa, että renkaan additiivinen ryhmä on kommutatiivinen, joten ideaali (ajateltuna kommutatiivisena additiivisena ryhmänä) on siis sen normaali aliryhmä. Käyttämällä samaa ekvivalenssirelaatiota kuin luvussa 3 muodostamme renkaan $R$ ideaalia $\mathscr{I}$ vastaavan tekijäjoukon $R/\mathscr{I}$, ja varustamme sen tekijälaskutoimituksilla. Näin saamme *tekijärenkaan* eli *jäännösluokkarenkaan.*

Ideaalia $\mathscr{I}$ vastaavia sivuluokkia merkitään additiivisesti $x+I$:llä. Olkoon $x \in R$. Alkion $x$ *virittämää vasenta ideaalia*, joka koostuu $x$:n monikerroista $xr$, $r \in R$ merkitään usein $xR$:llä, vastaavaa oikeaa ideaalia merkitään $Rx$.

PROPOSITIO 7.8. *Olkoon $R$ rengas, ja olkoon $\mathscr{I}$ sen kaksipuolinen ideaali. Tällöin tekijäjoukko $R/\mathscr{I}$ on rengas.*

*Todistus.* Osoitamme, että kertolasku on yhteensopiva ekvivalenssirelaation kanssa: Olkoot $a, a', b, b' \in R$, $a \sim a'$ ja $b \sim b'$. Nyt $a - a' \in \mathscr{I}$ ja $b - b' \in \mathscr{I}$, joten

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

koska $\mathscr{I}$ on kaksipuolinen ideaali. Loput harjoitustehtävässä 82. □

Propositio 1.12 antaa seurauksena

PROPOSITIO 7.9. *(1) Tekijärengas on kommutatiivinen, jos alkuperäinen rengas on kommutatiivinen.*
*(2) Luonnollinen kuvaus $R \to R/\mathscr{I}$ on rengashomomorfismi.*

*Todistus.* Lemma 1.12 ja Esimerkki 1.14. □

HUOMAA: Tekijärengas $R/\mathscr{I}$ voi olla kommutatiivinen vaikka $R$ ei olisikaan: $R/R$ on yhden alkion rengas!

LAUSE 7.10 (Renkaiden isomorfismilause). *Olkoon $\psi\colon R \to S$ rengashomomorfismi. Tällöin tekijärengas $R/\ker\psi$ on isomorfinen renkaan $\psi(R)$ kanssa.*

*Todistus.* Lause todistetaan kuten ryhmien isomorfismilause 4.22. Harjoitustehtävä 84. □

ESIMERKKI 7.11. (1) $R/R \cong \{0\}$, $R/\{0\} \cong R$.
(2) Reaaliluvut konstruoidaan luvussa 8 rationaalilukujen Cauchyn jonojen renkaan nollaan suppenevien jonojen ideaalia vastaavana tekijärenkaana.

**Harjoitustehtäviä.**

TEHTÄVÄ 77. Olkoon $R$ rengas, ja olkoon $\mathscr{I} \subset R$. Osoita, että

(1) $\mathscr{I}$ on vasen ideaali, jos ja vain jos $xa + x'a' \in \mathscr{I}$ kaikilla $x, x' \in R$ ja $a, a' \in \mathscr{I}$.
(2) $\mathscr{I}$ on kaksipuolinen ideaali, jos ja vain jos se on vasen ideaali ja oikea ideaali.

TEHTÄVÄ 78. Olkoon $\psi : R \to S$ rengashomomorfismi. Olkoon $\mathscr{I}$ renkaan $R$ vasen ideaali. Osoita, että $\psi(\mathscr{I})$ on renkaan $\psi(R)$ vasen ideaali.

TEHTÄVÄ 79. Olkoon $R$ rengas. Olkoot $a_1, a_2, \ldots a_n \in R$. Osoita, että

$$(a_1, a_2, \ldots, a_n) = \{x_1a_1 + x_2a_2 + \cdots + x_na_n : x_1, x_2, \ldots, x_n \in R\}$$

on renkaan $R$ vasen ideaali.

TEHTÄVÄ 80. Olkoot $L$ ja $M$ renkaan $R$ vasempia ideaaleja. Olkoot

$$LM = \{x_1y_1 + x_2y_2 + \cdots + x_ny_n : x_i \in L, y_i \in M, n \in \mathbb{N}\},$$

ja

$$L + M = \{x + y : x \in L, y \in M\},$$

Osoita, että $LM$ ja $L + M$ ovat renkaan $R$ vasempia ideaaleja.

TEHTÄVÄ 81. Olkoot $L$ ja $M$ renkaan $R$ vasempia ideaaleja.

(1) Osoita, että $L \cap M$ on renkaan $R$ vasen ideaali.
(2) Osoita, että jos $\mathscr{I}_i$, $i \in I$ on renkaan $R$ vasen ideaali, niin $\bigcap_{i\in I} \mathscr{I}_i$ on renkaan $R$ vasen ideaali.
(3) Osoita, että $LM \subset L \cap M$, jos $R$ on kommutatiivinen.
(4) Voiko $LM$ olla ideaalin $L + M$ aito osajoukko, jos $R$ on kommutatiivinen?

TEHTÄVÄ 82. Olkoon $R$ rengas, ja olkoon $\mathscr{I}$ sen kaksipuolinen ideaali. Osoita, että $R/\mathscr{I}$ on rengas.

TEHTÄVÄ 83. Olkoon $p$ alkuluku. Olkoon

$$R = \left\{\frac{m}{n} \in \mathbb{Q} : \text{syt}(m, n) = 1 \text{ ja } n \text{ ei ole jaollinen luvulla } p\right\} \cup \{0\}.$$

Olkoon

$$\mathscr{I} = \left\{\frac{m}{n} \in R : m \text{ on jaollinen luvulla } p\right\}.$$

Osoita, että $R$ on kommutatiivinen rengas, ja että $\mathscr{I}$ on renkaan $R$ ideaali.
(Rationaaliluku $m/n$ on *supistetussa muodossa*, jos $\text{syt}(m, n) = 1$.)

TEHTÄVÄ 84. Todista renkaiden isomorfismilause.

TEHTÄVÄ 85. Olkoot $K$ ja $K'$ kuntia. Olkoon $\phi\colon K \to K'$ kuntahomomorfismi. Osoita, että $\phi$ on injektio.

## 8. REAALILUVUT

Tässä luvussa jatkamme lukualueiden määrittelyä luvun 2 pohjalta. Käytettävissä on siis lukualueet $\mathbb{N}, \mathbb{Z}$ ja $\mathbb{Q}$ sekä kurssilla tähän mennessä kehitetty teoria.

Tunnetusti rationaaliluvut eivät ole algebran ja analyysin kannalta riittävän hyvä lukualue:

ESIMERKKI 8.1. Yhtälöllä $x^2 = 2$ ei ole ratkaisua rationaalilukujen joukossa: Jos $x^2 = 2$ ja $x = p/q \in \mathbb{Q}$, saadaan $p^2 = 2q^2$. Tällöin luku 2 esiintyy luvun $p^2$ alkutekijäesityksessä parillisen monta kertaa, ja luvun $2q^2$ esityksessä parittoman monta kertaa. Aritmetiikan peruslauseen 6.10 mukaan tämä ei ole mahdollista.

Tähän mennessä tarkasteltuihin lukualueisiin $\mathbb{Z}$ ja $\mathbb{Q}$ voi määritellä järjestyksen, joka vastaa niiden tavanomaista ajattelemista "lukusuoran osajoukkoina". Olkoot

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

ja

$$\mathbb{Q}_+ = \{p/q \in \mathbb{Q} : p, q \in \mathbb{Z}_+\}$$

*positiivisten kokonaislukujen* ja *positiivisten rationaalilukujen* joukot. Nämä joukot sopivat laskutoimitusten kanssa hyvin yhteen:

PROPOSITIO 8.2. *Olkoon $K$ joko $\mathbb{Z}$ tai $\mathbb{Q}$. Tällöin*

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

*Lisäksi*

(4) *kaikilla $a \in \mathbb{Q}_+$, $a^{-1} \in \mathbb{Q}_+$.*

*Todistus.* (1) Olkoot $a = [(m, 0)], b = [(n, 0)]$, $m, n \in \mathbb{N}$. Tällöin $a+b = [(m+n, 0)]$, ja koska $m + n \in \mathbb{N}$, $a + b \in \mathbb{N}_+$. Samoin $ab = [(mn, 0)] \in \mathbb{N}_+$.

Olkoot $a = p/q, b = r/s$, $p, q, r, s \in \mathbb{N}, q, s \neq 0$. Tällöin $a + b = (ps + qr)/qs$. Edellisen nojalla $ps, qr, ps + qr, qs \in \mathbb{Z}_+$, joten $a + b \in \mathbb{Q}_+$. Kertolasku vastaavasti.

Loput harjoitustehtäviä (osa harjoitustehtävissä 86 ja 90). □

Nyt määrittelemme järjestyksen kokonaisluvuille ja rationaaliluvuille: $<$ on relaatio joukoissa $\mathbb{Z}$ ja $\mathbb{Q}$, joka määritellään:

$$\begin{aligned} a < b &\iff b - a \in \mathbb{Z}_+ \quad \text{kaikilla } a, b \in \mathbb{Z} \\ a < b &\iff b - a \in \mathbb{Q}_+ \quad \text{kaikilla } a, b \in \mathbb{Q}. \end{aligned} \tag{8}$$

Vastaavasti $a > b$, jos ja vain jos $b < a$. Jos $a < b$, niin $a$ on *pienempi* kuin $b$. Jos $a > b$, niin $a$ on *suurempi* kuin $b$. Määrittelemme vielä toisen relaation $\leq$ joukoissa $\mathbb{Z}$ ja $\mathbb{Q}$: Jos $a < b$ tai $a = b$, niin $a \leq b$.

Muista, että joukon $X$ relaatio $R$ on osittainen järjestys, jos se on refleksiivinen, antisymmetrinen ja transitiivinen. Jos lisäksi kaikille $a, b \in R$ pätee $aRb$ tai $bRa$, $R$ on *täydellinen järjestys*. Jos $\leq$ on täydellinen järjestys joukossa $X$, niin $(X, \leq)$ on *täysin järjestetty*.

Edellä esitetty on erikoistapaus yleisemmästä käsitteestä:

MÄÄRITELMÄ 8.3. Olkoon $K$ kokonaisalue. Jos on $K_+ \subset K$, jolla on Proposition 8.2 ominaisuudet (1),(2) ja (3), niin $K$ on *järjestetty kokonaisalue*. Jos $K$ on lisäksi kunta, se on *järjestetty kunta*.

PROPOSITIO 8.4. *Lausekkeen* (8) *avulla määritelty järjestys $\leq$ on täydellinen järjestys.*

*Todistus.* Harjoitustehtävä 87. □

Siis erityisesti $\mathbb{Z}$ ja $\mathbb{Q}$ ovat täydellisesti järjestettyjä. $\mathbb{Z}$ on järjestetty kokonaisalue ja $\mathbb{Q}$ on järjestetty kunta.

MÄÄRITELMÄ 8.5. Olkoon $(X, \leq)$ täysin järjestetty joukko. Olkoon $A \subset X$. Alkio $x \in X$ on joukon $A$ *yläraja*, jos $a \leq x$ kaikilla $a \in A$. Joukon $A$ yläraja $x_A$ on joukon $A$ *pienin yläraja*, jos $x_A \leq x$ kaikilla joukon $A$ ylärajoilla $x$. Vastaavasti määritellään joukon $A$ *alaraja* ja *suurin alaraja*.

Usein pienintä ylärajaa kutsutaan supremumiksi, ja siitä käytetään tällöin merkintää $\sup A$. Suurinta alarajaa kutsutaan infimumiksi, ja tällöin merkitään $\inf A$.

ESIMERKKI 8.6. Joukolla

$$A = \{x \in \mathbb{Q} : x^2 \leq 2\}$$

ei ole pienintä ylärajaa rationaalilukujen joukossa $\mathbb{Q}$: Millekään luvulle $x \in \mathbb{Q}$ ei päde $x^2 = 2$. Jos $a = p/q \in A$, niin $p^2/q^2 < 2$. Tarpeeksi suurilla $n \in \mathbb{N}$, $(1 + 1/n)^2 < 2q^2/p^2$, joten $b = (1 + 1/n)^2 p^2/q^2 \in A$ ja $a < b$, joten $a$ ei ole joukon $A$ yläraja. Vastaavasti osoitetaan, että mikään joukon

$$B = \{x \in \mathbb{Q} : x^2 > 2\}$$

alkio ei ole joukon $A$ pienin yläraja. (Harjoitustehtävä 88)

Edellinen esimerkki osoittaa, että rationaalilukujen joukossa on reikiä. Laajennamme rationaalilukujen joukon $\mathbb{Q}$ reaalilukujen joukoksi arvioimalla esimerkiksi lukua "$\sqrt{2}$" rationaalilukujen jonolla, joka "suppenee kohti lukua $\sqrt{2}$". Haluamme, että näin konstruoitava lukualue on kunta, joka on kunnan $\mathbb{Q}$ laajennus järjestettynä kuntana, eli $\mathbb{Q}$ voidaan tulkita reaalilukujen osaksi siten, että laskutoimitukset ja järjestys säilyvät.

Tarkastelemme ensin rationaalilukujen jonoja. Olkoon

$$\mathscr{J} = \{(a_n)_{n=1}^{\infty} : a_n \in \mathbb{Q}\}.$$

Määrittelemme yhteenlaskun ja kertolaskun joukossa $\mathscr{J}$ komponenteittain. Siis, jos $\alpha = (a_n)_{n=1}^{\infty}$ ja $\beta = (b_n)_{n=1}^{\infty}$, niin

$$\alpha + \beta = (a_n + b_n)_{n=1}^{\infty} \quad \text{ja} \quad \alpha\beta = (a_n b_n)_{n=1}^{\infty}.$$

Jonot ovat kuvauksia $\alpha : \mathbb{N} \to \mathbb{Q}$, $\alpha(n) = a_n$, joten $\mathscr{J}$ on rengas edellä määritellyillä laskutoimituksilla varustettuna, katso Esimerkki 5.8. Kertolaskun neutraalialkio on vakiojono $1 = (1)_{k=1}^{\infty} = 1, 1, 1, \ldots$ ja yhteenlaskun $0 = (0)_{k=1}^{\infty} = 0, 0, 0, \ldots$.

HUOMAA: Rengas $\mathscr{J}$ ei ole kunta: Olkoot $\alpha = (a_n)_{n=1}^{\infty}$ ja $\beta = (b_n)_{n=1}^{\infty}$,

$$a_n = \begin{cases} 1, \text{ kun } n = 1 \\ 0, \text{ kun } n \neq 1 \end{cases}$$

ja

$$b_n = \begin{cases} 1, \text{ kun } n = 2 \\ 0, \text{ kun } n \neq 2 \end{cases}.$$

Tällöin jonolla $\alpha$ ei ole käänteisalkiota, koska jonon $\alpha\gamma$ kaikki indeksiä $k \geq 2$ vastaavat kertoimet ovat nollia, olipa $\gamma$ mikä jono tahansa. Sitä paitsi $(a_k)_{k=1}^{\infty}(b_k)_{k=1}^{\infty} = 0$, joten rengas $\mathscr{J}$ ei ole myöskään kokonaisalue.

MÄÄRITELMÄ 8.7. Olkoon $K$ järjestetty kokonaisalue. Olkoon $K_+$ sen positiivisten alkioiden joukko. Alkion $x \in K$ *itseisarvo* on

$$|x| = \begin{cases} x, \text{ jos } x \in K_+, \\ -x, \text{ jos } x \in -K_+, \\ 0, \text{ jos } x = 0. \end{cases}$$

PROPOSITIO 8.8. *Olkoon $K$ järjestetty kokonaisalue. Tällöin*

(1) $|x| = 0 \iff x = 0$.
(2) $|x - y| \leq |x - z| + |z - y|$ *kaikilla* $x, y, z \in K$.
(3) $|xy| = |x||y|$ *kaikilla* $x, y \in K$.

*Todistus.* Kuten kurssilla Analyysi 1. □

Tarkastelemme nyt reaalilukujen konstruktiota rationaalilukujonojen avulla.

MÄÄRITELMÄ 8.9. (1) Jono $(a_k)_{k=1}^{\infty}$, $a_k \in \mathbb{Q}$ on *rajoitettu*, jos on $M \in \mathbb{Q}$ siten, että $|a_k| \leq M$ kaikilla $k \in \mathbb{N}$.
(2) Jono $(a_k)_{k=1}^{\infty}$, $a_k \in \mathbb{Q}$ on *Cauchyn jono*, jos kaikilla $\epsilon \in \mathbb{Q}_+$ on $N \in \mathbb{N}$ siten, että

$$|a_n - a_m| < \epsilon, \quad \text{kun} \quad n, m \geq N.$$

(3) Jono $(a_k)_{k=1}^{\infty}$, $a_k \in \mathbb{Q}$, *suppenee kohti alkiota* $a \in \mathbb{Q}$, jos kaikilla $\epsilon \in \mathbb{Q}_+$ on $N \in \mathbb{N}$ siten, että

$$|a_n - a| < \epsilon, \quad \text{kun} \quad n \geq N.$$

Jos jono $(a_k)_{k=1}^{\infty}$ suppenee kohti lukua $a \in \mathbb{Q}$, $a$ on jonon *raja-arvo*, merkintöjä:

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

Määritelmä 8.9 yleistyy kaikille järjestetyille kokonaisalueille, ja käytämmekin sitä reaalilukujen yhteydessä. Edellä määritellyt käsitteet liittyvät toisiinsa:

PROPOSITIO 8.10. *(1) Suppeneva jono on Cauchyn jono.*
*(2) Cauchyn jono on rajoitettu.*

*Todistus.* (1) Olkoon $(a_k)_{k=1}^{\infty}$ suppeneva jono. Olkoon $\epsilon \in \mathbb{Q}_+$. Tällöin on $a \in \mathbb{Q}$ ja $N \in \mathbb{N}$ siten, että $|a_k - a| < \epsilon/2$, kun $k \geq N$. Olkoot $m, n \geq N$. Tällöin

$$|a_m - a_n| \leq |a_m - a| + |a - a_n| \leq \epsilon.$$

(2) Harjoitustehtävä 91. □

HUOMAA: Monet rationaalilukujen Cauchyn jonot eivät suppene joukossa $\mathbb{Q}$. Esimerkiksi jono

$$1 = \frac{1}{1}, \ 2 = \frac{2}{1}, \ \frac{3}{2}, \ \frac{5}{3}, \ \frac{8}{5}, \ \frac{13}{8}, \ \frac{21}{13}, \ldots$$

joka jatkuu säännöllä

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

on rationaalilukujen Cauchyn jono, joka ei suppene rationaalilukujen joukossa. Sivuutamme tämän seikan todistuksen. Jono liittyy ketjumurtolukuihin ja kultaiseen leikkaukseen.

PROPOSITIO 8.11. *Cauchyn jonojen joukko*

$$\mathscr{C}(\mathbb{Q}) = \{(a_i)_{i\in\mathbb{N}} \in \mathscr{J}(\mathbb{Q}) : (a_i)_{i\in\mathbb{N}} \text{ on Cauchyn jono}\},$$

*on renkaan* $\mathscr{J}(\mathbb{Q})$ *alirengas.*

*Todistus.* Harjoitustehtävä 92. □

Monet Cauchyn jonot suppenevat samaan pisteeseen, esimerkiksi $1/n \to 0$ ja $\pm 1/2^n \to 0$, kun $n \to \infty$. Emme siis halua määritellä reaalilukuja suoraan rationaalilukujen Cauchyn jonojen avulla. Monilla Cauchyn jonoilla ei sitä paitsi ole käänteisalkiota kertolaskun suhteen. Nämä ongelmat korjataan siirtymällä sopivaan tekijärenkaaseen.

MÄÄRITELMÄ 8.12. Rationaalilukujen Cauchyn jono $(a_k)_{k=1}^{\infty}$ on *nollajono*, jos se suppenee kohti lukua $0 \in \mathbb{Q}$. Merkitsemme nollajonojen joukkoa $\mathscr{N}(\mathbb{Q})$.

LEMMA 8.13. $\mathscr{N}(\mathbb{Q})$ *on renkaan* $\mathscr{C}(\mathbb{Q})$ *ideaali.*

*Todistus.* Harjoitustehtävä 93. □

MÄÄRITELMÄ 8.14. *Reaaliluvut* ovat tekijärengas $\mathbb{R} = \mathscr{C}(\mathbb{Q})/\mathscr{N}(\mathbb{Q})$.

Reaalilukujen yhteenlaskun ja kertolaskun neutraalialkiot ovat $0 = [0, 0, \dots]$ ja $1 = [1, 1, \dots]$.

LAUSE 8.15. *Reaalilukujen rengas on kunta.*

*Todistus.* Lemman 1.12 nojalla $\mathbb{R}$ on kommutatiivinen rengas. Osoitetaan, että jokaisella $x \in \mathbb{R} \setminus \{0\}$ on käänteisalkio kertolaskun suhteen. Jos $x \in \mathbb{R} \setminus \{0\}$, niin on luvut $a_k \in \mathbb{Q}^*$, $k \in \mathbb{N}$, joille $x = [(a_k)_{k=1}^{\infty}]$. Jono $(1/a_k)_{k=1}^{\infty}$ on Cauchyn jono: Olkoon $\epsilon \in \mathbb{Q}_+$. Tällöin on $N \in \mathbb{N}$ ja $q \in \mathbb{Q}_+$, joille $|a_m|, |a_n| \geq q$, kun $m, n \geq N$. Siis

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

joka on pieni, kun $m$ ja $n$ ovat riittävän suuria. Nyt $[(a_k)_{k=1}^{\infty}][(1/a_k)_{k=1}^{\infty}] = 1$.

□

Olkoon

$$\mathbb{R}_+ = \big\{[(a_k)_{k=1}^{\infty}] : \text{on } N \in \mathbb{N}, q \in \mathbb{Q}_+ \text{ siten, että } a_n > q \text{ kaikilla } n \geq N\big\}.$$

*Positiivisten reaalilukujen joukko* $\mathbb{R}_+$ on hyvin määritelty, sillä kaikille jonon $(a_k)_{k=1}^{\infty}$ kanssa ekvivalenteille jonoille $(b_k)_{k=1}^{\infty}$ on $N' \in \mathbb{N}$, siten, että $|b_k - a_k| < \frac{q}{2}$, kun $k \geq N'$. Siis kolmioepäyhtälön nojalla saadaan $b_k > q/2$ suurilla $k$.

Jos $K$ ja $K'$ ovat kuntia, ja $\phi\colon K \to K'$ on rengashomomorfismi, sanotaan, että $\phi$ on *kuntahomomorfismi.*

LAUSE 8.16. $\mathbb{R}$ *on järjestetty kunta. Sen järjestys on täydellinen. Kuvaus* $i\colon \mathbb{Q} \to \mathbb{R}$, $i(q) = [(q)_{k=1}^{\infty}]$ *on järjestyksen säilyttävä injektiivinen kuntahomomorfismi.*

*Todistus.* Osoitetaan, että positiivisten reaalilukujen joukolla $\mathbb{R}_+$ on Proposition 8.2 ominaisuudet (1), (2) ja (3):
(1) Tarkastellaan tuloa: Olkoot $\alpha = [(a_k)_{k=1}^{\infty}], \beta = [(b_k)_{k=1}^{\infty}] \in \mathbb{R}_+$. Tällöin on $N \in \mathbb{N}$ ja $q \in \mathbb{Q}_+$ siten, että $a_k, b_k \geq q$, kun $k \geq N$. Nyt $q^2 \in \mathbb{Q}_+$ ja $a_k b_k \geq q^2$ kaikilla $k \geq N$, joten $\alpha\beta \in \mathbb{R}_+$. Yhteenlasku samaan tapaan.
(2) Olkoon $x \in \mathbb{R} \setminus (\mathbb{R}_+ \cup \{0\})$. Tällöin on $a_k \in -\mathbb{Q}_+$, joille $x = [(a_k)_{k=1}^{\infty}]$. Nyt

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

(3) Olkoon $[(a_k)_{k=1}^{\infty}] \in \mathbb{R}_+ \cap -\mathbb{R}_+$ Tällöin suurille $k$ pätee $a_k > q$ ja $-a_k > q$ jollain $q \in \mathbb{Q}_+$. Tällöin erityisesti $a_k, -a_k \in \mathbb{Q}_+ \cap -\mathbb{Q}_+ = \emptyset$ !
Järjestyksen täydellisyys: Harjoitustehtävä 87.
Kuvauksen $i$ homomorfisuus todistetaan kuten Propositioissa 2.2 ja 2.4 (Harjoitustehtävä 94). Osoitetaan, että kuvaus $i$ säilyttää järjestyksen. Olkoot $q, r \in \mathbb{Q}$ siten, että $q > r$ eli $q - r \in \mathbb{Q}_+$. Nyt

$$i(q) - i(r) = [(q)_{k=1}^{\infty}] - [(r)_{k=1}^{\infty}] = [(q-r)_{k=1}^{\infty}]\,. \tag{9}$$

Oletuksen mukaan $q - r \in \mathbb{Q}_+$ kaikilla $k$, joten yhtälön (9) mukaan $i(q) > i(r)$. □

---

Sopimus: Tästedes samastamme rationaaliluvut vastaavan reaalilukujen osajoukon kanssa.

---

Osoitamme seuraavaksi, että luvun alussa havaitut rationaaliluvuilla esiintyvät analyysin ongelmat on korjattu siirtymällä reaalilukuihin. Kirjaamme aluksi kaksi pientä käyttökelpoista tulosta:

Lemma 8.17. *Olkoon $\gamma = (c_k)_{k=1}^{\infty}$ rationaalilukujen Cauchyn jono, ja olkoon $c \in \mathbb{Q}_+$. Jos on $N \in \mathbb{N}$ siten, että $|c_k| < c$, kun $k \geq N$, niin $|[\gamma]| \leq c$.*

*Todistus.* Jos $[\gamma] \in \mathbb{R}_+$ ja $[\gamma] > c$, niin $[\gamma] - i(c) \in \mathbb{R}_+$, eli on $\delta \in \mathbb{Q}_+$, jolle $c_k - c > \delta$ kaikilla suurilla $k$. Siis $c_k > c + \delta$ kaikilla suurilla $k$. Muut tapaukset tarkastetaan samaan tapaan. □

Lemma 8.18. *(1) Olkoon $\epsilon \in \mathbb{Q}_+$. On $\epsilon' \in \mathbb{R}_+$ siten, että $0 < \epsilon' < \epsilon$.*
*(2) Olkoon $\epsilon' \in \mathbb{R}_+$. On $\epsilon \in \mathbb{Q}_+$ siten, että $0 < \epsilon < \epsilon'$. Erityisesti jokaisella $M \in \mathbb{R}_+$ on $n \in \mathbb{N}$, jolle $\frac{M}{n} < \epsilon'$.*

*Todistus.* Harjoitustehtävä 95. □

Huomaa: Samastamme näissä tuloksissa rationaaliluvut vastaavia vakiojonoja vastaavien reaalilukujen kanssa, joten reaaliluvun ja rationaaliluvun vertaaminen on sallittua!

Propositio 8.19. *Olkoon $(a_k)_{k=1}^{\infty}$ rationaalilukujen Cauchyn jono. Jono $(a_k)_{k=1}^{\infty}$ suppenee reaalilukujen joukossa, ja sen raja-arvo on $\alpha = [(a_k)_{k=1}^{\infty}]$.*

*Todistus.* Tulkitsemme nyt rationaaliluvun $a_k$ vakiojonon $(a_k)_{j=1}^{\infty}$ luokaksi $\mathbb{R}$:ssa, huomaa indeksit! Olkoon $\epsilon' \in \mathbb{Q}_+$. Koska $(a_k)_{k=1}^{\infty}$ on Cauchyn jono, on $N \in \mathbb{N}$, siten, että kun $k, m \geq N$, niin $|a_k - a_m| < \epsilon'$. Olkoon $m \geq N$. Silloin

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

joten Lemman 8.17 mukaan $|[(a_m)_{k=1}^{\infty}] - \alpha| \leq \epsilon'$. Väite seuraa tästä ja Lemmasta 8.18. □

Siis jokainen rationaalilukujen Cauchyn jono suppenee reaalilukujen kunnassa. Tällaisen jonon raja-arvo on se reaaliluku, jonka se määrää!

Lause 8.20. *Jokainen reaalilukujen Cauchyn jono suppenee.*

*Todistus.* Idea: Arvioimme reaalilukujen Cauchyn jonoa rationaalilukujen Cauchyn jonolla, ja osoitamme, että alkuperäinen jono suppenee kohti tämän jonon määräämää reaalilukua.

Olkoon $(\alpha_n)_{n=1}^{\infty}$ $\mathbb{R}$:n Cauchyn jono. Nyt $\alpha_n = [(a_{n,k})_{k=1}^{\infty}]$. Proposition 8.19 nojalla on indeksi $K_n \in \mathbb{N}$ siten, että

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

Olkoon $q_n = a_{n,K_n}$.

Olkoon $\epsilon \in \mathbb{R}_+$. Koska $(\alpha_n)_{n=1}^{\infty}$ on Cauchyn jono, niin on $N \in \mathbb{N}$ siten, että $|\alpha_n - \alpha_m| < \epsilon/3$, kun $n, m \geq N$. Olkoon $N_1 \geq N$ siten, että $1/N_1 < \epsilon/3$. Tällöin kaikilla $n, m \geq N_1$ pätee

$$\begin{aligned} |q_n - q_m| &= |i(q_n) - i(q_m)| = |i(q_n) - \alpha_n + \alpha_n - \alpha_m + \alpha_m - i(q_m)| \\ &\leq |i(q_n) - \alpha_n| + |\alpha_n - \alpha_m| + |\alpha_m - i(q_m)| < \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon. \end{aligned}$$

Siis $(q_n)_{n=1}^{\infty}$ on rationaalilukujen Cauchyn jono, joka määrää reaaliluvun $\alpha = [(q_n)_{n=1}^{\infty}]$.

Olkoon $N_2 \geq N_1$ siten, että $|\alpha - i(q_n)| < \epsilon/2$, kun $n \geq N_2$ (Propositio 8.19). Tällöin

$$|\alpha_n - \alpha| \leq |\alpha_n - i(q_n)| + |i(q_n) - \alpha| < \epsilon,$$

joten $\alpha_n \to \alpha$, kun $n \to \infty$. □

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

Lause 8.21. *Olkoon $A \subset \mathbb{R}$ ylhäältä rajoitettu, $A \neq \emptyset$. Tällöin joukolla $A$ on pienin yläraja.*

*Todistus.* Olkoon $M$ joukon $A$ yläraja. Olkoon $n \in \mathbb{N}$. Olkoon $y_n \in \mathbb{Z}$ pienin luku siten, että $y_n/n$ on joukon $A$ yläraja. Tällainen on, sillä jokaisella alhaalta rajoitetulla kokonaislukujen epätyhjällä osajoukolla on minimi (induktioperiaatteen kanssa ekvivalentti ominaisuus!). On siis $x_n \in A$, jolle

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

Olkoot $m, n \in \mathbb{N}$ siten, että $\frac{y_n}{n} \leq \frac{y_m}{m}$. Tällöin

$$\frac{y_m}{m} - \frac{1}{m} < \frac{y_n}{n} \leq \frac{y_m}{m},$$

sillä muuten $y_m$ ei olisi minimaalinen (Mieti!). Siispä

$$\left|\frac{y_m}{m} - \frac{y_n}{n}\right| < \frac{1}{m}\,.$$

Valitsemalla $m, n > 1/\epsilon$ saamme

$$\left|\frac{y_m}{m} - \frac{y_n}{n}\right| < \epsilon\,,$$

joten jono $(y_n/n)_{n=1}^{\infty}$ on Cauchyn jono. Proposition 8.19 mukaan se suppenee kohti raja-arvoa $w \in \mathbb{R}$.

Osoitamme, että $w$ on joukon $A$ yläraja: Jos olisi $x \in A$, jolle $w < x$, niin $x - w \in \mathbb{R}_+$, ja raja-arvon määritelmän nojalla on $n \in \mathbb{N}$, jolle

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

Tällöin (mieti, miksi!)

$$x - \frac{y_n}{n} \geq \frac{x-w}{2}.$$

Erityisesti siis $x > y_n/n$, joten $y_n/n$ ei ole joukon $A$ yläraja.

Osoitetaan vielä, että $w$ on joukon $A$ pienin yläraja: Olkoon $u < w$. Tällöin on $n \in \mathbb{N}$, siten, että

$$\left|\frac{y_n}{n} - w\right| \leq \frac{w-u}{4}$$

ja jollain $a_n$ pätee

$$\left|\frac{y_n}{n} - a_n\right| \leq \frac{w-u}{4}.$$

Nyt

$$\begin{aligned} a_n - u &= w - u + a_n - \frac{y_n}{n} + \frac{y_n}{n} - w \\ &\geq w - u + \left|a_n - \frac{y_n}{n}\right| + \left|\frac{y_n}{n} - w\right| \geq \frac{w-u}{2}, \end{aligned}$$

joten $u$ ei ole joukon $A$ yläraja. □

Analyysin kursseilla on tapana ottaa lähtökohdaksi joko

- (suljettujen) *sisäkkäisten välien periaate*: Jos $I_1 \supset I_2 \supset \ldots$ ovat sisäkkäisiä suljettuja ja rajoitettuja reaalilukuvälejä, niin niiden leikkaus $\cap I_i$ ei ole tyhjä joukko, tai
- täydellisyysaksiooma: Jokaisella ylhäältä rajoitetulla epätyhjällä joukolla $A \subset \mathbb{R}$ on pienin yläraja.

Nämä periaatteet ovat nyt lauseita!

Esimerkki 8.22. Yhtälöllä $x^2 = 2$ on ratkaisu reaalilukujen joukossa. Olkoon

$$A = \{x \in \mathbb{R} : x^2 < 2\}.$$

Kuten Esimerkissä 8.6 huomaamme, että mikään joukon $A$ luvuista ei ole joukon $A$ yläraja, ja että mikään joukon

$$B = \{x \in \mathbb{R} : x^2 > 2\}$$

luvuista ei ole joukon $A$ pienin yläraja. Kuitenkin Lauseen 8.21 mukaan joukolla $A$ on pienin yläraja. Tälle luvulle $a \in \mathbb{R}$ pätee siis $a^2 = 2$. Samalla päättelyllä saadaan, että joukon $A$ suurin alaraja on saman yhtälön ratkaisu.

LAUSE 8.23. *Olkoon $x \in \mathbb{R}_+$, ja olkoon $n \in \mathbb{N}$. Tällöin on $\sqrt[n]{x} \in \mathbb{R}_+$, jolle pätee $(\sqrt[n]{x})^n = x$. Lisäksi, jos $x, y \in \mathbb{R}_+$ ja $x < y$, niin $\sqrt[n]{x} < \sqrt[n]{y}$.*

*Todistus.* Luvun $\sqrt[n]{x}$ olemassaolo todistetaan kuten esimerkissä 8.22. Järjestyksen säilyminen seuraa harjoitustehtävästä 89. □

**Harjoitustehtäviä.**

TEHTÄVÄ 86. Osoita:

(1) Kaikilla $a, b \in \mathbb{Q}_+$ pätee $a + b \in \mathbb{Q}_+$ ja $ab \in \mathbb{Q}_+$.
(2) Jos $\alpha \in \mathbb{Q}^*$, niin $\alpha \in \mathbb{Q}_+$ tai $-\alpha \in \mathbb{Q}_+$.

TEHTÄVÄ 87. Määritellään järjestetyssä kokonaisalueessa $K$ relaatio $\leq$ asettamalla

$$a \leq b \iff \big(b - a \in K_+ \ \text{ tai } \ a = b\big).$$

Osoita, että relaatio $\leq$ on täydellinen järjestys.

TEHTÄVÄ 88. Osoita, ettei mikään joukon $B = \{x \in \mathbb{Q} : x^2 > 2\}$ alkio ole joukon $A = \{x \in \mathbb{Q} : x^2 \leq 2\}$ pienin yläraja.

TEHTÄVÄ 89. Olkoon $K$ järjestetty kokonaisalue. Osoita, että

- Jos $a < b$ ja $c > 0$, niin $ac < bc$.
- Jos $a < b$ ja $c < d$, niin $a + c < b + d$.

TEHTÄVÄ 90. Olkoon $K$ järjestetty kokonaisalue. Olkoot $a, b \in K$. Osoita, että

- Jos $a > 0$ ja $b < 0$, niin $ab < 0$.
- Jos $a \neq 0$, niin $a^2 > 0$.
- Jos $a$ on yksikkö ja $a > 0$, niin $a^{-1} > 0$.

TEHTÄVÄ 91. Olkoon $K$ järjestetty kokonaisalue. Osoita, että $K$:n Cauchyn jonot ovat rajoitettuja.

TEHTÄVÄ 92. Osoita, että $\mathscr{C}(\mathbb{Q})$ on renkaan $\mathscr{J}(\mathbb{Q})$ alirengas.

TEHTÄVÄ 93. Osoita, että $\mathscr{N}(\mathbb{Q})$ on renkaan $\mathscr{C}(\mathbb{Q})$ ideaali. Onko $\mathscr{N}(\mathbb{Q})$ renkaan $\mathscr{J}(\mathbb{Q})$ ideaali?

TEHTÄVÄ 94. Osoita, että kuvaus $i\colon \mathbb{Q} \to \mathbb{R}$, $i(q) = [(q)_{k=1}^{\infty}]$ on injektiivinen kuntahomomorfismi.

TEHTÄVÄ 95. (a) Olkoon $\epsilon \in \mathbb{Q}_+$. Osoita, että on $\epsilon' \in \mathbb{R}_+$ siten, että $0 < \epsilon' < \epsilon$.
(b) Olkoon $\epsilon' \in \mathbb{R}_+$. Osoita, että on $\epsilon \in \mathbb{Q}_+$ siten, että $0 < \epsilon < \epsilon'$.

## 9. KOMPLEKSILUVUT

Lauseen 8.23 mukaan jokaisella positiivisella reaaliluvulla on positiivinen $n$:s juuri kaikilla $n \in \mathbb{N}$. Sen sijaan esimerkiksi yhtälöllä $x^2 = -1$ ei ole ratkaisua reaalilukujen kunnassa: $-1 \notin \mathbb{R}_+$ ja toisaalta järjestetyssä kunnassa kaikkien lukujen neliöt ovat positiivisia. Laajennamme nyt lukualuetta tämän ongelman poistamiseksi.

MÄÄRITELMÄ 9.1. *Kompleksilukujen joukko* on $\mathbb{R}^2$ varustettuna komponenteittaisella yhteenlaskulla ja kertolaskulla, joka määritellään asettamalla

$$(a, b)(c, d) = (ac - bd, ad + bc).$$

PROPOSITIO 9.2. $\mathbb{C}$ *on kunta. Yhteenlaskun neutraalialkio on* $(0, 0)$ *ja kertolaskun neutraalialkio on* $(1, 0)$. *Kuvaus* $j\colon \mathbb{R} \to \mathbb{C}$, $j(x) = (x, 0)$ *on injektiivinen kuntahomomorfismi.*

*Todistus.* Harjoitus. (Kompleksilukujoukon kuntaominaisuus harjoitustehtävässä 97) □

---

SOPIMUS: Tästedes samastamme reaaliluvut vastaavan kompleksilukujen osajoukon kanssa.

---

Kompleksilukua $i = (0, 1)$ kutsutaan *imaginaariyksiköksi*. Jokainen kompleksiluku voidaan esittää summana

$$(a, b) = (a, 0) + (0, b) = a + ib,$$

missä viimeisessä vaiheessa käytetään edellä tehtyä sopimusta, jonka mukaan kompleksiluku $(a, 0)$ samastetaan reaaliluvun $a$ kanssa. Kompleksiluvun $z = a + ib$ *reaaliosa* on $\mathrm{Re}(z) = a$ ja *imaginaariosa* on $\mathrm{Im}(z) = b$. Luku $\bar{z} = a - ib$ on kompleksiluvun $z = a + ib$ *(kompleksi)konjugaatti* eli *liittoluku*.

Näillä merkinnöillä kompleksilukujen laskutoimitukset ovat

$$(a + ib) + (c + id) = (a + c) + i(b + d),$$
$$(a + ib)(c + id) = (ac - bd) + i(ad + bc).$$

Yhteenlaskun neutraalialkio on 0 ja kertolaskun neutraalialkio on 1.
HUOMAA: $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$, joten yhtälöllä $x^2 = -1$ on ratkaisu kompleksilukujen kunnassa.

Kompleksiluvun $z = x + iy$ *moduli* (eli itseisarvo) on

$$|z| = \sqrt{z\bar{z}} = \sqrt{x^2 + y^2} = \|(x, y)\|.$$

Jos $x \in \mathbb{R}$, niin $|x| = |j(x)| = |x|$. Moduli toteuttaa kolmioepäyhtälön:

$$|z + z'| \leq |z| + |z'|$$

kaikilla $z, z' \in \mathbb{C}$, vertaa Euklidiset avaruudet. Modulin avulla havaitaan helposti

$$z^{-1} = \frac{\bar{z}}{|z|^2}.$$

Napakoordinaattien avulla voimme esittää jokaisen kompleksiluvun $z \neq 0$ muodossa $z = |z|(\cos\phi + i\sin\phi)$, missä $\phi$ on tason $\mathbb{R}^2$ vektorien $(1, 0)$ ja $(\mathrm{Re}(z), \mathrm{Im}(z))$ välinen kulma "positiiviseen kiertosuuntaan". Trigonometristen funktioiden kulman yhteenlaskukaavojen avulla saamme:

PROPOSITIO 9.3. *(1) Olkoot* $z = r(\cos\phi + i\sin\phi)$, *ja* $w = s(\cos\theta + i\sin\theta)$. *Tällöin*

$$zw = rs(\cos(\phi+\theta) + i\sin(\phi+\theta)).$$

*(2) Olkoot* $z_k = r_k(\cos\phi_k + i\sin\phi_k)$, $k = 1, 2, \ldots, n$. *Tällöin*

$$\prod_{k=1}^{n} z_k = (\prod_{k=1}^{n} r_k)(\cos(\sum_{k=1}^{n}\phi_k) + i\sin(\sum_{k=1}^{n}\phi_k)).$$

*Todistus.* Analyysi 1. □

Jos $z^k = w$, niin $z$ on luvun $w$ *k. juuri.*

LEMMA 9.4. *Luvulla* $1 \in \mathbb{C}$ *on* $m$ *kappaletta* $m$*. juuria.*

*Todistus.* Olkoon

$$\zeta_m = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}.$$

Tällöin Proposition 9.3 nojalla

$$\zeta_m^m = \cos 2\pi + i\sin 2\pi = 1.$$

Jos $n \in \{1, 2\ldots, m\}$, niin Proposition 9.3 nojalla

$$\zeta_m^n = \cos\frac{2\pi n}{m} + i\sin\frac{2\pi n}{m},$$

joten

$$(\zeta_m^n)^m = \cos\frac{2\pi nm}{m} + i\sin\frac{2\pi nm}{m} = 1.$$

Siis kaikki luvut $\zeta_m^n$ ovat ykkösen juuria. □

PROPOSITIO 9.5. *Jokaisella kompleksiluvulla* $z \in \mathbb{C}^*$ *on* $m$ *kappaletta* $m$*. juuria.*

*Todistus.* Harjoitustehtävä 98. □

Seuraavan havainnon avulla osoitamme helposti, että kompleksilukujen kuntaa ei voi järjestää kuten reaalikukuja:

LEMMA 9.6. *Olkoon* $K$ *järjestetty kokonaisalue, ja olkoon* $a \in K \setminus \{0\}$. *Tällöin* $a^2 \in K_+$. *Erityisesti* $1 \in K_+$.

*Todistus.* Nyt $a \in K_+$ tai $-a \in K_+$. Siispä $a^2 \in K_+$ tai $(-a)^2 \in K_+$, ja koska $a^2 = (-a)^2$, väite seuraa. □

PROPOSITIO 9.7. *Kompleksilukujen kunnalla ei ole järjestetyn kunnan rakennetta.*

*Todistus.* Järjestetyssä kunnassa jokaisen luvun neliö on positiivinen. Jokainen kompleksiluku $z \neq 0$ on Proposition 9.5 mukaan neliö. Siis kaikki nollasta poikkeavat luvut olisivat positiivisia, mikä on mahdotonta. □

ESIMERKKI 9.8. Luvun $2 \in \mathbb{C}$ kolmannet juuret ovat $\sqrt[3]{2}$,

$$\sqrt[3]{2}\big(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\big) = \sqrt[3]{2}\big(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\big)$$

ja

$$\sqrt[3]{2}\big(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\big) = -\sqrt[3]{2}\big(\frac{1}{2} + i\frac{\sqrt{3}}{2}\big).$$

Proposition 9.5 avulla voimme myös ratkaista toisen, kolmannen ja neljännen asteen polynomiyhtälöt.

PROPOSITIO 9.9. *Olkoot $a_0, a_1 \in \mathbb{C}$. 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.*

*Todistus.* Havaitsemme, että

$$(z - z_1)(z - z_2) = z^2 + a_1 z + a_0 = 0,$$

mistä väite seuraa. □

Kaikki kolmannen asteen kompleksikertoimiset yhtälöt saadaan muuttujanvaihdolla muotoon $z^3 + pz + q = 0$. Jos $u_0, v_0 \in \mathbb{C}$ siten, että

$$\begin{aligned} u_0^3 &= -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}, \\ v_0^3 &= -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}, \text{ ja} \\ u_0 v_0 &= -\frac{p}{3}, \end{aligned}$$

niin luvut $z_1 = u_0 + v_0$, $z_2 = \zeta_3 u_0 + \zeta_3^2 v_0$ ja $z_2 = \zeta_3^2 u_0 + \zeta_3 v_0$ ovat yhtälön $z^3 + pz + q = 0$ ratkaisuja.

Emme tarkastele korkeamman asteen kaavoja tarkemmin tällä kurssilla. Neljännen asteen kaavat ovat saman tapaisia kuin kolmannen asteen tapauksessa. Abel osoitti vuonna 1826, että viidennen ja korkeamman asteen polynomeille ei ole tällaista ratkaisualgoritmia. Tämän väitteen todistuksessa käytetään yleensä ryhmäteoriaa. Aiheesta enemmän esimerkiksi kirjassa K. Väisälä: Lukuteorian ja korkeamman algebran alkeet.

Polynomiyhtälöitä ja niiden ratkaisujen lukumäärää tarkastellaan lähemmin luvussa 10.

**Harjoitustehtäviä.**

TEHTÄVÄ 96. Osoita, että kompleksilukujen kertolasku on assosiatiivinen ja kommutatiivinen.

TEHTÄVÄ 97. Osoita, että $\mathbb{C}$ on kunta.

TEHTÄVÄ 98. Osoita, että jokaisella kompleksiluvulla $z \in \mathbb{C}^*$ on $m$ kappaletta $m$. juuria.

TEHTÄVÄ 99. Ratkaise yhtälöt $z^3 = i$ ja $z^5 = -\frac{1}{2}$. Havainnollista ratkaisuja kuvalla.

TEHTÄVÄ 100. Olkoot *Gaussin kokonaisluvut*

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\},$$

ja *Gaussin rationaaliluvut*

$$\mathbb{Q}(i) = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Q}\}.$$

Osoita, että $\mathbb{Z}[i]$ on rengas, ja että $\mathbb{Q}(i)$ on kunta.

## 10. POLYNOMIT

Tarkastelemme lyhyessä viimeisessä luvussa polynomirenkaiden teoriaa ja polynomiyhtälöiden ratkaisemista. Algebrassa on tapana pitää erillään polynomin ja polynomifunktion käsitteet.

Sopimuksia:

- Tässä luvussa $X$ on muodollinen symboli, jota usein kutsutaan muuttujaksi.
- Symbolin $-\infty$:n sovitaan tarkoittavan "ääretöntä negatiivista lukua", jolle pätee
  - $-\infty < a$ kaikilla kokonaisluvuilla $a$,
  - $-\infty + -\infty = -\infty$, ja
  - $-\infty + a = -\infty$ kaikilla kokonaisluvuilla $a$.

  Mitään muita operaatioita sille ei ole määritelty!

MÄÄRITELMÄ 10.1. Olkoon $R$ kommutatiivinen rengas, $\#R \geq 2$. Olkoon $n \in \mathbb{N}$, ja olkoot $a_n, a_{n-1}, \ldots, a_1, a_0 \in R$. Lauseke

$$P(X) = \sum_{k=1}^{n} a_k X^k = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

on *yhden muuttujan $R$-kertoiminen polynomi*. Jos $a_n \neq 0$, niin polynomin $P(X)$ *aste* on $\deg(P(X)) = n$. Nollapolynomin 0 aste on $-\infty$. Kaikkien $R$-kertoimisten polynomien joukkoa merkitään $R[X]$:llä.

Olkoot $P(X) = \sum_{k=1}^{n} a_k X^k$ ja $Q(X) = \sum_{k=1}^{m} b_k X^k$ $R$-kertoimisia polynomeja, $n \geq m$. Olkoot $b_{m+1} = b_{m+2} = \cdots = b_n = 0$, jos $n > m$. Polynomien summa ja tulo määritellään asettamalla

$$P(X) + Q(X) = \sum_{k=0}^{n} (a_k + b_k) X^k$$

ja

$$P(X)Q(X) = \sum_{k=0}^{n+m} \Big( \sum_{i+j=k} a_i b_j \Big) X^k \tag{10}$$

Polynomi $P(X) = \sum_{k=1}^{n} a_k X^k \in R[X]$ määrittelee *polynomifunktion* $P\colon R \to R$, $x \mapsto \sum_{k=1}^{n} a_k x^k$.

PROPOSITIO 10.2. *$R[X]$ on kommutatiivinen rengas.*

*Todistus.* Selvästi polynomit 0 ja 1 ovat yhteenlaskun ja kertolaskun neutraalialkiot. Muut ominaisuudet seuraavat siitä, että $R$ on rengas suoraviivaisella tarkastuksella. □

HUOMAUTUKSIA: (1) Toinen, vähemmän havainnollinen tapa määritellä polynomit on korvata edellä lauseke $\sum_{k=1}^{n} a_k X^k$ jonolla $(a_0, a_1, \dots, a_n, 0, 0, \dots)$, ja määritellä yhteenlasku kuten jonoille on tapana ja kertolasku kaavan (10) mukaisesti. Tällöin jono $(0, 1, 0, 0, 0, \dots)$ on symbolin $X$ vastine.
(2) Polynomien laskutoimitukset ovat siis tavanomaiset.
(3) Polynomit voi halutessaan kirjoittaa kasvavien $X$:n potenssien mukaan sillä $R[X]$ on kommutatiivinen.
(4) Kuvaus $P(X) \mapsto (P : R \to R)$ on rengashomomorfismi polynomirenkaasta $R[X]$ kuvausrenkaaseen $\mathscr{F}(X, X)$.

ESIMERKKI 10.3. Olkoot $P(X), Q(X) \in \mathbb{Z}[X]$, $P(X) = 2X^2 + 2$, $Q(X) = 1 + 2X$. Tällöin

$$P(X)Q(X) = 4X^3 + 2X^2 + 4X + 2.$$

Nyt $\deg(P(X)) = 2$, $\deg(Q(X)) = 1$ ja $\deg(P(X)Q(X)) = 3$.

LEMMA 10.4. *Olkoon $R$ kommutatiivinen rengas. Tällöin*

$$\deg(P(X)Q(X)) \leq \deg P(X) + \deg Q(X) \tag{11}$$

*kaikille $P(X), Q(X) \in R[X]$.*

*Todistus.* Olkoot $P(X) = \sum_{k=1}^{n} a_k X^k$ ja $Q(X) = \sum_{k=1}^{m} b_k X^k$, $a_n \neq 0$, $b_m \neq 0$. Tulopolynomin $P(X)Q(X)$ korkeimman asteen termi on $a_n b_m X^{n+m}$, jos $a_n b_m \neq 0$, muuten aste on alempi. □

PROPOSITIO 10.5. *Jos $K$ on kokonaisalue, niin $K[X]$ on kokonaisalue. Tällöin*

$$\deg(P(X)Q(X)) = \deg(P(X)) + \deg(Q(X)).$$

*Todistus.* Käytämme Lemman 10.4 merkintöjä. Tulopolynomin korkeimman asteen termin kerroin on $a_n b_m \neq 0$, sillä $K$ on kokonaisalue. □

ESIMERKKI 10.6. (1) Kun tarkastellaan polynomirengasta $\mathbb{Z}_p[X]$, polynomien kertoimista jätetään yleensä ekvivalenssiluokan sulut pois. Tällöin esimerkin 10.3 kokonaislukukertoimisten polynomien lausekkeet voidaan tulkita polynomirenkaan $\mathbb{Z}_p[X]$ polynomeiksi.
(2) Jos kerroinrengas ei ole kokonaisalue, kaavassa (11) voi olla erisuuruus: Polynomi $2X$ on nollan jakaja renkaassa $\mathbb{Z}_4[X]$: $(2X)(2X) = 4X^2 = 0$. Nyt siis

$$-\infty = \deg 0 = \deg((2X)(2X)) < 2 \deg(2X) = 2.$$

(3) Joillakin renkailla $R$ kaksi eri polynomia polynomirenkaassa $R[X]$ voi määrätä saman polynomifunktion (katso Propositio 10.15): Olkoot $Q(X), P(X) \in \mathbb{Z}_2[X]$, $Q(X) = X^2, P(X) = X$. Tällöin $P(0) = 0 = 0^2 = Q(0)$, ja $P(1) = 1 = 1^2 = Q(1)$.

HUOMAA: Polynomirengas ei ole koskaan kunta. Jos $K$ on kokonaisalue, niin Proposition 10.5 mukaan ainoat polynomit, joilla on käänteisalkio kertolaskun suhteen ovat nollasta poikkeavat vakiopolynomit. Sen sijaan, jos kerroinrengas ei ole kokonaisalue, muillakin polynomeilla voi olla käänteisalkioita: Esimerkiksi renkaassa $\mathbb{Z}_4[X]$ pätee

$$(2X + 1)(2X + 1) = 4X^2 + 4X + 1 = 1.$$

Nyt kuitenkaan kaikilla nollasta poikkeavilla vakiopolynomeilla ei ole käänteisalkiota.

Esimerkki 10.7. Samalla lausekkeella annettujen polynomien jaollisuus riippuu tarkasteltavasta polynomirenkaasta:
(1) $(X-1) \mid (X^2-1)$ ja $(X+1) \mid (X^2-1)$ kaikissa renkaissa $R[X]$, missä $R$ on kommutatiivinen rengas:

$$(X-1)(X+1) = X^2 + (1-1)X - 1 = X^2 - 1.$$

(2) $(X+1) \mid (X^2+1)$ renkaassa $\mathbb{Z}_2[X]$, sillä $1 = -1$ renkaassa $\mathbb{Z}^2$.
(3) $(X+1) \nmid (X^2+1)$ renkaassa $\mathbb{C}[X]$: Jos $(X+1) \mid (X^2+1)$, niin on $A, B \in \mathbb{C}$, joille $(X+1)(AX+B) = X^2+1$ (miksi?). Tällöin toisen ja nollannen asteen kertoimia tarkastelemalla havaitaan, että $A = 1 = B$, mutta ensimmäisen asteen termit eivät täsmää.

Jos kokonaisluvut $a, b$ jakavat toisensa, $a \mid b$ ja $b \mid a$, niin $a = \pm b$. Polynomeille ei voi päätellä näin, vaan oikea päätelmä on seuraava:

Lemma 10.8. *Olkoon $K$ kokonaisalue, ja olkoot $P(X), Q(X) \in K[X]$ siten, että $P(X) \mid Q(X)$ ja $Q(X) \mid P(X)$. Silloin on $u \in K^*$, jolle $P(X) = uQ(X)$.*

*Todistus.* Harjoitustehtävä 103. □

Olemme käyttäneet kurssilla muutamia kertoja kokonaislukujen jakoyhtälöä: Olkoot $a, b \in \mathbb{Z}$ ja $b \neq 0$. Tällöin on yksikäsitteiset $q, j \in \mathbb{Z}$, joille

$$a = qb + j \quad \text{ja} \quad 0 \leq j < |b|.$$

Todistamme vastaavan tuloksen polynomeille kolmena hieman erilaisena versiona:

Propositio 10.9 (Jakoyhtälö). *Olkoon $R$ kommutatiivinen rengas. Olkoot $A(X)$, $B(X) \in R[X]$ siten, että $B(X) \neq 0$ ja*

(1) *$B(X)$:n korkeimman asteen termin kerroin on 1, tai*
(2) *$B(X)$:n korkeimman asteen termin kerroin on yksikkö, tai*
(3) *$R$ on kunta.*

*Tällöin on yksikäsitteiset $Q(X), J(X) \in R[X]$, joille*

$$A(X) = Q(X)B(X) + J(X) \quad ja \quad \deg J(X) < \deg B(X).$$

*Todistus.* (1) Jos $B(X)$ jakaa polynomin $A(X)$, ei ole mitään todistettavaa. Muuten, olkoon

$$S = \{A(X) - D(X)B(X) : D(X) \in R[X]\}.$$

Selvästi $S \neq \emptyset$. Olkoon

$$T = \deg S = \{\deg P(X) : P(X) \in S\}.$$

Koska $B(X) \nmid A(X)$, niin $0 \notin S$, joten $t = \min T > 0$.

Olkoon $Q(X) \in R[X]$ sellainen, että $\deg(A(X) - Q(X)B(X)) = \deg J(X) = t$. Olkoon $J(X) = a_t X^t + \cdots + a_0$. Osoitamme, että $t < d = \deg B(X)$. Jos olisi $t \geq d$, niin

$$J(X) - a_t X^{t-d} B(X) = A(X) - (Q(X) + a_t X^{t-d})B(X) \in S$$

ja $\deg\big(J(X) - a_t X^{t-d} B(X)\big) < t$, mutta tämä on mahdotonta, koska polynomin $J(X)$ aste on minimaalinen.

Jos $\widetilde{Q}(X)$ ja $\widetilde{J}(X)$ ovat polynomeja, joilla on samat ominaisuudet kuin polynomeilla $Q(X)$ ja $J(X)$, niin

$$(Q(X) - \widetilde{Q}(X))B(X) = \widetilde{J}(X) - J(X).$$

Jos $\widetilde{Q}(X) \neq Q(X)$, niin vasemman puolen aste on vähintään $d$, kuitenkin

$$\deg(\widetilde{J}(X) - J(X)) \leq t < d.$$

Siis $\widetilde{Q}(X) = Q(X)$ ja $\widetilde{J}(X) = J(X)$.
(2) Harjoitustehtävä 104.
(3) Seuraa kohdasta (2), koska kaikki nollasta poikkeavat kunnan alkiot ovat yksiköitä. □

Esimerkki 10.10. Jakoyhtälö voidaan toteuttaa algoritmisesti jakokulman avulla kuten kokonaisluvuillekin. Tällöin esimerkiksi polynomeille $A(X) = 2X^3+X^2-X-1$ ja $B(X) = X^2 - 2$ renkaassa $\mathbb{Z}[X]$ pätee

$$2X^3 + X^2 - X - 1 = (2X + 1)(X^2 - 2) + 3X + 1,$$

joten $Q(X) = 2X + 1$ ja $J(X) = 3X + 1$. Renkaassa $\mathbb{Z}_3[X]$ samoilla polynomeilla $A(X)$ ja $B(X)$

$$2X^3 + X^2 - X - 1 = (2X + 1)(X^2 - 2) + 1 = (2X + 1)(X^2 + 1) + 1. \tag{12}$$

Toisaalta, jos $B(X) = 2X+1$, niin jakoyhtälö ei toimi renkaassa $\mathbb{Z}[X]$: jakokulmassa päädytään ongelmalliseen tilanteeseen

$$2X^3 + X^2 - X - 1 = X^2(2X + 1) - X - 1,$$

josta ei voi jatkaa. Sen sijaan renkaassa $\mathbb{Z}_3[X]$ voidaan jatkaa, koska $\mathbb{Z}_3$ on kunta. Nyt

$$-X - 1 = 2X + 2 = (2X + 1) + 1$$

ja päädytään yhtälöön (12). Renkaassa $\mathbb{Q}[X]$ jakoa voi myös jatkaa, ja saadaan

$$2X^3 + X^2 - X - 1 = (X^2 - \frac{1}{2})(2X + 1) - \frac{1}{2}.$$

Tarkastelemme nyt yhden muuttujan polynomiyhtälöitä. Tämän kanssa on yhtäpitävää tarkastella polynomien (tai niitä vastaavien polynomifunktioiden) nollakohtia.

Määritelmä 10.11. Olkoon $R$ kommutatiivinen rengas, ja olkoon $P(X) \in R[X]$. Alkio $c \in R$ on polynomin $P(X)$ *juuri* eli *nollakohta*, jos $P(c) = 0$.

Jakoyhtälö antaa seuraavan perustuloksen:

Propositio 10.12. *Olkoon $R$ kommutatiivinen rengas. Olkoon $P(X) \in R[X]$, ja $c \in R$. Tällöin*

$$P(c) = 0 \iff (X - c) \mid P(X).$$

*Todistus.* Jos $P(c) = 0$, niin jakoyhtälön mukaan on $Q(X), J(X)$, joille $\deg J(X) < 1$ ja $A(X) = Q(X)(X-c)+J(X)$. Siis $J(X)$ on vakiopolynomi, on $b \in R$, jolle $J(a) = b$ kaikilla $a \in R$. Erityisesti

$$0 = P(c) = Q(c)(c - c) + J(c) = b,$$

joten $b = 0$.

Toisaalta, jos $P(X) = (X - c)Q(X)$ jollain polynomilla $Q(X) \in R[X]$, niin

$$P(c) = (c - c)Q(c) = 0.$$

□

PROPOSITIO 10.13. *Olkoon $K$ kokonaisalue. Olkoon $P(X) \in K[X]$ polynomi, ja olkoot $c_1, c_2, \ldots, c_k \in K$ polynomin $P(X)$ juuria. Tällöin on $Q(X) \in K[X]$, jolle*

$$P(X) = (X - c_1)(X - c_2) \cdots (X - c_k)Q(X).$$

*Todistus.* Harjoitustehtävä 105. □

LAUSE 10.14. *Olkoon $K$ kokonaisalue, ja olkoon $n \in \mathbb{N}$. Jos $P(X) \in K[X]$ ja $\deg P(X) = n$, niin polynomilla $P(X)$ on korkeintaan $n$ juurta.*

*Todistus.* Propositioiden 10.13 ja 10.5 mukaan, jos polynomilla $P(X)$ on $k$ juurta, niin $\deg(P(X)) \geq k$. □

Erityisesti siis Propositio 9.9 antaa kaikki (kaksi) toisen asteen kompleksikertoimisen polynomiyhtälön ratkaisut.

PROPOSITIO 10.15. *Olkoon $K$ ääretön kokonaisalue. Tällöin jokaista kokonaisalueen $K$ polynomifunktiota vastaa yksikäsitteinen polynomi renkaassa $K[X]$.*

*Todistus.* Olkoot $P(X), Q(X) \in K[X]$ siten, että $P(c) = Q(c)$ kaikilla $c \in K$. Tällöin polynomilla $P(X) - Q(X)$ on äärettömän monta juurta. Ainoa tällainen polynomi on 0. □

Usein polynomeilla on vähemmän nollakohtia kuin niiden asteesta tuleva maksimimäärä. Esimerkiksi polynomilla $X^3 + X \in \mathbb{R}[X]$ on täsmälleen yksi nollakohta, ja polynomilla $X^2 + 1 \in \mathbb{R}[X]$ ei ole nollakohtia lainkaan. Sen sijaan polynomilla $X^2 + 1 \in \mathbb{C}[X]$ on kaksi nollakohtaa: $(X + i)(X - i) = (X^2 + 1)$.

Jos $(X - c)^k$ jakaa polynomin $P(X)$ renkaassa $R[X]$, $c$ on *$k$-kertainen juuri*. Yleensä, kun lasketaan polynomin juuria, $k$-kertaiset juuret huomioidaan laskussa $k$ kertaa. Esimerkiksi 0 on polynomin $X^2$ kaksinkertainen nollakohta, ja kertaluku huomioiden polynomilla $X^2$ on siis kaksi nollakohtaa.

Kunta $K$ on *algebrallisesti suljettu*, jos jokaisella $P(X) \in K[X]$, joka ei ole vakiopolynomi, on juuri. Edellä esitettyjen tulosten mukaan algebrallisesti suljetussa kunnassa $n$. asteen polynomilla on (kertaluvun huomioiden) $n$ juurta.

LAUSE 10.16. *[Algebran peruslause] Kompleksilukujen kunta on algebrallisesti suljettu.*

*Todistus.* Tässä todistuksessa tarvitsemme Euklidisten avaruuksien kurssin tietoja jatkuvuudesta ja kompakteista joukoista.

Jos $P : \mathbb{C} \to \mathbb{C}$ on polynomifunktio, niin kuvaus $\widetilde{P} : \mathbb{R}^2 \to \mathbb{R}^2$,

$$\widetilde{P}(x, y) = (\mathrm{Re}(P(x + iy)), \mathrm{Im}(P(x + iy)))$$

on muotoa $\widetilde{P}(x, y) = (Q(x, y), R(x, y))$, missä $Q$ ja $R$ ovat kahden muuttujan polynomifunktioita. Siis $\widetilde{P}$ on jatkuva. Myös kuvaus $|\cdot| : \mathbb{C} \to \mathbb{R}$ on jatkuva, koska normikuvaus $\|\cdot\| : \mathbb{R}^2 \to \mathbb{R}$ on jatkuva. Näin ollen kuvaus $g : \mathbb{C} \to \mathbb{R}$, $g(t) = |P(t)|$ on jatkuva.

Olkoon nyt

$$P(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0,$$

missä $a_0, a_1, \ldots, a_n, t \in \mathbb{C}$, ja $a_n \neq 0$. Jos $t \neq 0$, pätee

$$g(t) = |P(t)| = |a_n t^n| \left| 1 + \frac{a_{n-1}}{a_n t} + \cdots + \frac{a_0}{a_n t^n} \right|.$$

Kolmioepäyhtälön avulla nähdään (Harjoitustehtävä 110), että on $R_0 > 0$ siten, että

$$\left| 1 + \frac{a_{n-1}}{a_n t} + \cdots + \frac{a_o}{a_n t^n} \right| > \frac{1}{2}.$$

kun $|t| > R_0$. Olkoon nyt $M > 0$. Silloin

$$g(t) > \left| \frac{a_n}{2} \right| |t^n| > M, \text{ kun } |t| > \max\{ \sqrt[n]{2M/|a_n|}, R_0 \}.$$

Merkitään $g(0) = |P(0)| = K$. Valitaan $R$ siten, että $g(t) = |P(t)| > K$ kaikilla $t \in \mathbb{C} \backslash \overline{B(0,R)}$. Kuvaus $g$ saavuttaa jokaisessa suljetussa pallossa $\overline{B(0,R)}$ pienimmän arvonsa. Siis on $z_0 \in \overline{B(0,R)}$ siten, että

$$g(t) = |P(t)| \geq |P(z_0)| = g(z_0) \text{ kaikille } t \in \overline{B(0,R)}.$$

Samalle $z_0$ myös $g(t) \geq g(z_0)$ kaikilla $t \in \mathbb{C}$, sillä $g(t) > K = g(0) \geq g(z_0)$, jos $t \notin \overline{B(0,R)}$.

Osoitetaan nyt, että $g(z_0) = 0$, mikä on yhtäpitävää sen kanssa, että $P(z_0) = 0$. Oletetaan, että $P(z_0) = c_0 \neq 0$. Yksinkertaistamme laskua vaihtamalla muuttujan $t$ tilalle muuttujan $z$, jolle

$$t = z + z_0 \iff z = t - z_0.$$

Tällöin (Harjoitustehtävä 111)

$$\begin{aligned} P(t) = P(z + z_0) = P_1(z) &= c_0 + c_1 z + \cdots + c_n z^n \\ &= c_0 + c_m z^m + z^{m+1} F(z), \end{aligned} \tag{13}$$

missä $m$ on pienin potenssi siten, että $c_m \neq 0$, ja $F(z)$ on sopiva polynomi. Tarkastelemme ensin erikoistapausta $P_1(z) = c_0 + c_1 z + c_2 z^2$. Jos $c_1 = 0$, niin $P_1(\sqrt{-(c_0/c_2)}) = 0$. Voimme siis olettaa, että $c_1 \neq 0$. Olkoon $\lambda \in [0,1]$. Tutkimme pisteitä $-\lambda(c_0/c_1)$. Koska

$$P_1\left( -\frac{\lambda c_0}{c_1} \right) = c_0 - c_1 \frac{\lambda c_0}{c_1} + \frac{\lambda^2 c_0^2}{c_1^2} c_2,$$

niin

$$\begin{aligned} \left| P_1\left( -\frac{\lambda c_0}{c_1} \right) \right| &\leq |c_0| ((1 - \lambda) + \left| \frac{c_0 c_2}{c_1^2} \right| \lambda^2) \\ &= |c_0| (1 - \lambda (1 - \left| \frac{c_2 c_0}{c_1^2} \right| \lambda)) \\ &< |c_0|, \end{aligned}$$

sillä $\left| \frac{c_2 c_0}{c_1^2} \right| \lambda < 1$, kun $\lambda$ on pieni. Tämä on ristiriita, koska

$$g(z_0) = |P(z_0)| = |P_1(0)| = |c_0|$$

on globaali minimi.

Yleistämme edellisen tarkastelun lausekkeelle (13). Olkoon $z_1 \in \mathbb{C}$ siten, että $z_1^m = -\dfrac{c_0}{c_m}$. Tällainen löydetään Proposition 9.5 perusteella. Olkoon taas $\lambda \in [0,1]$. Funktio $F$ on polynomina jatkuva ja $c_0 \neq 0$, ja joukko $\{\lambda z_1 : \lambda \in [0,1]\}$ on kompakti. Siksi on $C > 0$, jolle

$$\left| z_1^{m+1} \frac{F(\lambda z_1)}{c_0} \right| < C \text{ kaikille } \lambda \in [0,1].$$

Siten

$$\begin{aligned} |P_1(\lambda z_1)| \leq & (1 - \lambda^m + C\lambda^{m+1})|c_0| \\ = & (1 - \lambda^m(1 - C\lambda))|c_0|. \end{aligned}$$

Tässä $1 - C\lambda > 0$, kun $\lambda$ on pieni. Koska silloin $1 - \lambda^m(1 - C\lambda) < 1$, niin $|P_1(\lambda z_1)| < |c_0|$, mikä on ristiriita. Siis $g(z_0) = 0$, eli $P(z_0) = 0$. □

**Harjoitustehtäviä.**

TEHTÄVÄ 101. Osoita, että polynomi $F(X) = 1 - 2X$ on yksikkö renkaassa $\mathbb{Z}_{16}[X]$.

TEHTÄVÄ 102. Olkoon $p$ alkuluku. Montako juurta polynomilla $X^p - X \in \mathbb{Z}_p[X]$ on?

TEHTÄVÄ 103. Olkoon $K$ kokonaisalue. Olkoot $P(X), Q(X) \in K[X]$. Osoita: Jos $P(X) \mid Q(X)$ ja $Q(X) \mid P(X)$, niin on $u \in K^*$, jolle $P(X) = uQ(X)$.

TEHTÄVÄ 104. Olkoon $R$ kommutatiivinen rengas. Olkoot $A(X), B(X) \in R[X]$ siten, että $B(X) \neq 0$ ja $B(X)$:n korkeimman asteen termin kerroin on yksikkö. Osoita, että tällöin on $P(X), J(X) \in R[X]$, joille

$$A(X) = Q(X)B(X) + J(X) \quad \text{ja} \quad \deg J(X) < \deg B(X).$$

TEHTÄVÄ 105. Olkoon $K$ kokonaisalue. Olkoon $P(X) \in K[X]$ polynomi, ja olkoot $c_1, c_2, \ldots, c_k \in K$ polynomin $P(X)$ juuria. Osoita, että on $Q(X) \in K[X]$, jolle

$$P(X) = (X - c_1)(X - c_2) \cdots (X - c_k)Q(X).$$

TEHTÄVÄ 106. Olkoot $P(X), Q(X) \in \mathbb{Z}_8[X]$,

$$P(X) = 3 + 2X + 4X^2 + 2X^3$$

ja

$$Q(X) = 4 + 4X + 4X^2 + 4X^3 + 4X^4.$$

(1) Kerro $Q(X)$ polynomilla $P(X)$.
(2) Jaa $Q(X)$ polynomilla $P(X)$.

---

Olkoon $K$ kokonaisalue. Polynomi $P(X) \in K[X]$ on *jaoton*, jos ei ole olemassa polynomeja $A(X), B(X) \in K[X]$, joille $\deg A(X), \deg B(X) \geq 1$ siten, että

$$P(X) = A(X)B(X).$$

[101] Vihje: Kerroinrengas $\mathbb{Z}_{16}$ ei ole kokonaisalue.
[102] Vihje: Käytä ryhmäteoriaa!

---

TEHTÄVÄ 107. Olkoon $K$ kunta. Osoita, että toisen tai kolmannen asteen polynomi $P(X) \in K[X]$ on jaoton, jos ja vain jos sillä ei ole juurta kokonaisalueessa $K$. Anna esimerkki, joka osoittaa, että väite ei päde neljännen asteen polynomeille.

TEHTÄVÄ 108. (a) Onko polynomi $X^2 - 2 \in \mathbb{Z}_5[X]$ jaoton?
(b) Onko polynomi $X^2 + 1 \in \mathbb{Z}_5[X]$ jaoton?

TEHTÄVÄ 109. Jaa polynomi

$$P(X) = X^3 + 2X^2 + 3X + 2$$

polynomilla

$$Q(X) = 2X^2 + 3X + 1$$

(1) polynomirenkaassa $\mathbb{Q}[X]$ ja
(2) polynomirenkaassa $\mathbb{Z}_7[X]$.

TEHTÄVÄ 110. Olkoon $P : \mathbb{C} \to \mathbb{C}$, $P(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$, missä $a_0, \ldots, a_n \in \mathbb{C}$, $n$. asteen polynomifunktio. Osoita, että on $R_0 > 0$ siten, että

$$\left| 1 + \frac{a_{n-1}}{a_n t} + \cdots + \frac{a_0}{a_n t^n} \right| > \frac{1}{2},$$

kun $|t| > R_0$.

TEHTÄVÄ 111. Olkoon $P : \mathbb{C} \to \mathbb{C}$ $n$. asteen polynomifunktio. Olkoon $z = t - z_0$, missä $z_0 \in \mathbb{C}$ on vakio. Osoita, että $P_1 : \mathbb{C} \to \mathbb{C}$, $P_1(z) = P(t)$ on $n$. asteen polynomifunktio (muuttujana $z$).

# Kirjallisuutta

[1] N. Bourbaki: Algebra I, Springer-Verlag, 1989
[2] R. Godement: Algebra, Hermann, 1968
[3] A. Hillman: A first undergraduate course in abstract algebra, Wadsworth, 1983
[4] S. Lang: Undergraduate algebra, Springer-Verlag, 1987
[5] T. Metsänkylä & M. Näätänen: Algebra, Jyväskylän yliopistopaino, 1999