ALGEBRA 2014

JOUNI PARKKONEN

Tämä teksti on kevään 2014 kurssien Algebra 1A ja Algebra 1B oppimateriaali. Kurssit muodostavat johdatuksen abstraktiin algebraan, jota havainnollistetaan useilla "konkreettisilla" esimerkeillä matematiikan eri aloilta. Tapaamme yhteyksiä esimerkiksi naiiviin joukko-oppiin, lineaarialgebraan, geometriaan ja lukuteoriaan.

Kurssi Algebra 1A kattaa luvut 1–7. Kurssin aluksi luvuissa 1–3 tutustutaan laskutoimituksen käsitteeseen ja erilaisiin laskutoimituksiin sekä homomorfismeihin laskutoimituksella varustettujen joukkojen välillä. Luvuissa 4–7 tutustutaan ryhmäteorian perusasioihin normaaleihin aliryhmiin ja tekijäryhmiin saakka.

Kurssi Algebra 1B antaa perustiedot renkaiden ja kuntien teoriasta. Luvuissa 11 ja 12 tutustutaan polynomirenkaisiin. Viimeisessä luvussa tutustutaan ideaaleihin ja tekijärenkaisiin ja teoriaa sovelletaan äärellisten kuntien konstruktiossa.

Keskeisessä osassa molemmilla kursseilla on abstrakti algebra, jossa tehdään päätelmiä, kun laskutoimitusten jotkin ominaisuudet tunnetaan. Lisäksi tarkastelemme kuvauksia, jotka ovat yhteensopivia algebrallisten rakenteiden kanssa.

Yksi algebran keskeinen ajatus on se, että erilaisissa matemaattisissa yhteyksissä tunnistetaan samankaltaisia rakenteita. Jos tunnistetaan jokin tunnettu algebrallinen rakenne (ryhmä, rengas,...), voidaan tarkasteltavaa tilannetta usein ymmärtää paremmin näille algebrallisille rakenteille todistettujen yleisten tulosten avulla.

Kurssimateriaalissa käsitellään lyhykäisesti kompleksilukuja (luvut 2 ja 12), kokonaislukujen jaollisuutta ja alkulukuja ja jäännösluokkarenkaita (kongruenssiluokkia) (luvut 3 ja 9). Tarkastelussa keskitytään näiden kurssien kannalta oleellisimpaan ainekseen ja perusteellisempi käsittely jää muille kursseille.

Sisältö

Merkintöjä

Luonnollisten lukujen joukko on tällä kurssilla

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

Joukkojen $A, B \subset C$ joukko-opillista erotusta merkitään

$$A - B = \{a \in A : a \notin B\}.$$

Jos C on matriisi, merkintä C_{lm} tarkoittaa sen lm-kerrointa, joka on rivillä l ja sarakkeessa m. *Diagonaalimatriisi* on $n \times n$-matriisi, $D = \operatorname{diag}(a_1, a_2, \dots, a_n)$, jolle $D_{kk} = a_k$ kaikilla $k \in \{1, 2, \dots, n\}$ ja kaikki muut kertoimet ovat nollia. Erityistapaus $n \times n$-diagonaalimatriisista on $I_n = \operatorname{diag}(1, 1, \dots, 1)$.

Positiivisten reaalilukujen joukko on $\mathbb{R}_+ =]0, \infty[$. Funktio $\log\colon \mathbb{R}_+ \to \mathbb{R}$ on luonnollinen logaritmi.

Tarkasteltaessa kuvauksia joukosta X joukkoon Y, jos $y \in Y$, niin $\underline{y}\colon X \to Y$ on vakiokuvaus, jolle $\underline{y}(x) = y$ kaikille $x \in X$.

Jokaisen luvun lopussa on kokoelma harjoitustehtäviä. Osaan tehtävistä on alaviitteessä numeroitu vihje.

Kiitokset

Henna Koivusalo auttoi materiaalin työstämisessä kesällä 2007. Materiaalin viimeisimpiä versioita valmistettaessa Lassi Kuritun kommentit ovat olleet suurena apuna. Kiitokset kuuluvat myös muille, jotka ovat tuoneet tietooni tekstissä olleita painovirheitä ja muita ongelmia.

Tässä luvussa määrittelemme useita kurssin keskeisiä käsitteitä ja tutustumme niiden perusominaisuuksiin.

Määritelmä 1.1. Epätyhjän joukon A *laskutoimitus* on kuvaus $*\colon A \times A \to A$. *Laskutoimituksella varustettu joukko* eli *magma* on pari $(A, *)$, missä $*$ on joukon A laskutoimitus.

Laskutoimituksen tulosta merkitään yleensä $a * a' = *(a, a')$. Laskutoimitus on siis sääntö, joka liittää joukon A alkioiden a ja a' muodostamaan järjestettyyn pariin (a, a') joukon A alkion $a * a'$.

Esimerkki 1.2. Luonnollisten lukujen $\mathbb{N}$ ja kokonaislukujen $\mathbb{Z}$, rationaalilukujen $\mathbb{Q}$ ja reaalilukujen $\mathbb{R}$ yhteen- ja kertolasku ovat laskutoimituksia: $(m, n) \overset{+}{\mapsto} m + n$, $(m, n) \overset{\cdot}{\mapsto} m \cdot n = mn$. Tässä (kuten lähes aina) kertolaskun merkki $\cdot$ jätetään kirjoittamatta ja kertolaskun tulosta merkitään mn.

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 $*_B$ tulolaskutoimitukseksi* tai *tuloksi*. Laskutoimitusten $*_A$ ja $*_B$ tulolla varustettu varustettu joukko $(A \times B, *)$ on laskutoimituksella varustettujen joukkojen $(A, *_A)$ ja $(B, *_B)$ *tulo*. Vastaavalla tavalla voidaan määritellä laskutoimituksia useamman joukon karteesiseen tuloon.

Esimerkki 1.3. Avaruudessa $\mathbb{R}^n$ määritellään *komponenteittainen yhteenlasku* vastaavalla tavalla

$$x + y = (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

Edellä tarkastellut esimerkit liittyvät kaikki tavanomaiseen "luvuilla laskemiseen". Laskutoimituksen käsite on kuitenkin paljon laajempi, kuten seuraavista esimerkistä alkaa ilmetä:

Esimerkki 1.4. (a) Joukon X osajoukot muodostavat *potenssijoukon*

$$\mathscr{P}(X) = \{A : A \subset X\}.$$

Esimerkiksi, kun $X = \{0, 1\}$, niin

$$\mathscr{P}(X) = \big\{\emptyset, \{0\}, \{1\}, \{0, 1\}\big\}.$$

Joukkojen leikkaus $(A, B) \mapsto A \cap B$ ja yhdiste $(A, B) \mapsto A \cup B$ ovat laskutoimituksia potenssijoukossa $\mathscr{P}(X)$.
(b) Olkoon $X \neq \emptyset$ ja olkoon

$$\mathscr{F}(X) = \{f\colon X \to X\}.$$

Kuvausten yhdistäminen on laskutoimitus joukossa $\mathscr{F}(X)$: $(f, g) \mapsto f \circ g$.
(c) Olkoon $\mathrm{M}_n(\mathbb{R})$ reaalisten $n \times n$–matriisien joukko. Lineaarialgebran kursseilla määritellään kaksi laskutoimitusta joukossa $\mathrm{M}_n(\mathbb{R})$. Matriisien yhteenlasku määritellään komponenteittain asettamalla

$$(A + B)_{ij} = (A_{ij} + B_{ij})$$

kaikilla $1 \leq i, j \leq n$. Matriisien kertolasku määritellään asettamalla

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}$$

kaikilla $1 \leq i, j \leq n$.

Erityisesti dimensiossa 2 saadaan laskutoimitukset

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

ja

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

(d) Kahden alkion muodostamassa joukossa $X = \{0, 1\}$ on 16 eri laskutoimitusta: Joukossa

$$X \times X = \big\{(0,0), (0,1), (1,0), (1,1)\big\}$$

on neljä alkiota ja jokaisella alkiolla on kaksi mahdollista arvoa 0 tai 1.

(e) Kivi-paperi-sakset –pelissä kaksi pelaajaa näyttää samanaikaisesti kädellään yhden symboleista kivi, paperi tai sakset. Kivi voittaa sakset, sakset voittaa paperin ja paperi voittaa kiven. Jos molemmat pelaajat näyttävät saman symbolin, tämä symboli katsotaan voittajaksi. Pelin sääntö määrää laskutoimituksen kolmen alkion joukolla, jonka alkiot ovat kivi, paperi ja sakset.

Äärellisten (pienten) joukkojen laskutoimituksia voi myös tarkastella *laskutaulujen* avulla: Laskutoimituksella varustetun äärellisen joukon $(X, *)$ laskutaulu on joukon X alkioilla indeksoitu taulukko, jossa paikalla (g, h), siis rivillä g ja sarakkeessa h on alkio gh.

Esimerkiksi joukon $X = \{0, 1\}$ potenssijoukon laskutoimitusten $\cap$ ja $\cup$ laskutaulut ovat

$\cap$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{0\}$	$\emptyset$	$\{0\}$	$\emptyset$	$\{0\}$
$\{1\}$	$\emptyset$	$\emptyset$	$\{1\}$	$\{1\}$
$\{0,1\}$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$

ja

$\cup$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\emptyset$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\{0\}$	$\{0\}$	$\{0\}$	$\{0,1\}$	$\{0,1\}$
$\{1\}$	$\{1\}$	$\{0,1\}$	$\{1\}$	$\{0,1\}$
$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$

Laskutoimitusten suorittamisen järjestyksen kanssa on syytä olla huolellinen. Sulut kertovat, missä järjestyksessä operaatiot suoritetaan: Lausekkeessa $a*(b*c)$ muodostetaan ensin tulo $(b * c)$, joka kerrotaan vasemmalta alkiolla a kun taas lausekkeessa $(a * b) * c$ muodostetaan ensin tulo $(a * b)$, joka kerrotaan oikealta alkiolla c. Nämä eivät välttämättä anna samaa tulosta. Seuraava määritelmä antaa muutamia keskeisiä laskutoimitusten lisäominaisuuksia.

Määritelmä 1.5. 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 $a, b \in A$.

Sulkujen määrää lausekkeissa voi vähentää, jos laskutoimitus $*$ on assosiatiivinen: Koska sulkujen paikalla ei ole merkitystä lausekkeessa $a*(b*c) = (a*b)*c$, voimme käyttää merkintää

$$a * b * c = (a * b) * c = a * (b * c)$$

ilman vaaraa. Huomaa kuitenkin, että kaikki laskutoimitukset eivät ole assosiatiivisia.

Esimerkki 1.6. (a) Luonnollisten lukujen, kokonais-, rationaali- ja reaalilukujen yhteen- ja kertolaskulle pätee

(1) $m + n = n + m$ ja $mn = nm$ kaikilla m, n (kommutatiivisuus).
(2) $m + (n + l) = (m + n) + l$ ja $m(nl) = (mn)l$ kaikilla m, n, l (assosiatiivisuus).

(b) Kokonaislukujen vähennyslasku ei ole assosiatiivinen eikä kommutatiivinen:

$$1 - (1 - 1) = 1 \neq -1 = (1 - 1) - 1$$

ja

$$1 - 0 = 1 \neq -1 = 0 - 1.$$

(c) Joukon $\mathscr{P}(X)$ laskutoimitukset $\cap$ ja $\cup$ ovat

- assosiatiivisia: $A \cap (B \cap C) = (A \cap B) \cap C$ ja $A \cup (B \cup C) = (A \cup B) \cup C$ kaikilla $A, B, C \in \mathscr{P}(X)$ ja
- kommutatiivisia: $A \cap B = B \cap A$ ja $A \cup B = B \cup A$ kaikilla $A, B \in \mathscr{P}(X)$.

(d) Joukon $\mathscr{F}(X)$ laskutoimitus $\circ$ on assosiatiivinen: Olkoot $f, g, h \in \mathscr{F}(X)$. Yhdistetyn kuvauksen määritelmän mukaan

$$\big(f \circ (g \circ h)\big)(x) = f\big((g \circ h)(x)\big) = f\big(g(h(x))\big)$$

kaikilla $x \in X$ ja

$$\big((f \circ g) \circ h\big)(x) = (f \circ g)(h(x)) = f\big(g(h(x))\big)$$

kaikilla $x \in X$. Siis $f \circ (g \circ h) = (f \circ g) \circ h$ kaikilla $f, g, h \in \mathscr{F}(X)$.

Laskutoimitus $\circ$ ei kuitenkaan ole kommutatiivinen, jos joukossa X on ainakin kaksi alkiota: Olkoon $X = \{0, 1\}$ ja olkoot $\underline{0}, \underline{1} \in \mathscr{F}(X)$ vakiokuvaukset $\underline{0}(x) = 0$ ja $\underline{1}(x) = 1$ kaikilla $x \in X$. Tällöin $\underline{1} \circ \underline{0} = \underline{1} \neq \underline{0} = \underline{0} \circ \underline{1}$.

Määritelmä 1.7. 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 $g \in A$.

Propositio 1.8. *Olkoon $(X, *)$ laskutoimituksella varustettu joukko. Jos on alkiot $e \in X$ ja $e' \in X$ siten, että $e * g = g$ ja $g * e' = g$ kaikilla $g \in X$, niin $e = e'$. Erityisesti e on laskutoimituksen $*$ neutraalialkio.*

Todistus. Käyttämällä oletettuja ominaisuuksia ylläolevassa järjestyksessä saadaan $e = e * e' = e'$. Koska e siis toteuttaa ehdot $e * g = g$ ja $g * e = g$ kaikilla $g \in X$, niin e on neutraalialkio. □

Määritelmä 1.9. Olkoon $A \neq \emptyset$ ja olkoon $*$ joukon A laskutoimitus, jonka neutraalialkio on e.

- Alkio $\bar{x} \in A$ on alkion $x \in A$ *vasen käänteisalkio*, jos $\bar{x} * x = e$,
- Alkio $\bar{x} \in A$ on alkion $x \in A$ *oikea käänteisalkio*, jos $x * \bar{x} = e$.

Jos $\bar{x}$ on alkion x vasen ja oikea käänteisalkio, niin se on alkion x *käänteisalkio*.

Esimerkki 1.10. Luku 0 on luonnollisten lukujen, kokonais-, rationaali ja reaalilukujen yhteenlaskun neutraalialkio ja luku 1 on kertolaskun neutraalialkio. Useimmilla luonnollisilla luvuilla ei ole käänteisalkiota laskutoimituksella varustetuissa joukoissa $(\mathbb{N}, +)$ ja $(\mathbb{N}, \cdot)$. Sen sijaan jokaisella kokonais-, rationaali- ja reaaliluvulla x on vastaluku $-x$, joka on luvun x käänteisalkio yhteenlaskun suhteen.

Luvulla 0 ei ole käänteisalkiota kertolaskun suhteen edes rationaalilukujen joukossa: $0\,x = x\,0 = 0 \neq 1$ kaikilla luvuilla x. Kaikilla nollasta poikkeavilla rationaali- ja reaaliluvuilla x sen sijaan on käänteisluku $x^{-1} = 1/x$, esimerkiksi rationaaliluvulle $a/b \neq 0$ pätee $(a/b)^{-1} = b/a$.

Esimerkki 1.11. (a) 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.

(b) Olkoot $f, g \in \mathscr{F}(\mathbb{N})$ kuvaukset, jotka määritellään asettamalla

$$f(n) = \begin{cases} 0, \text{ kun } n = 0 \\ n - 1, \text{ kun } n \neq 0 \end{cases}$$

ja $g(n) = n + 1$. Kuvaukset f ja g eivät ole bijektioita, joten kummallakaan ei ole käänteisalkiota. Kuitenkin pätee $f \circ g = \mathrm{id}$, joten f on kuvauksen g vasen käänteisalkio ja vastaavasti g on kuvauksen f oikea käänteisalkio.

(c) Varustamme nyt joukon $X \neq \emptyset$ potenssijoukon laskutoimituksella $-$, joka määritellään

$$A - B = \{a \in A : a \notin B\}.$$

Tällöin jokaisella $A \in \mathscr{P}(X)$ pätee $A - \emptyset = A$, joten $\emptyset$ muistuttaa laskutoimituksen $-$ neutraalialkiota. Kuitenkin $\emptyset - A = \emptyset$ kaikilla $A \in \mathscr{P}(X)$, joten $\emptyset$ ei ole laskutoimituksen $-$ neutraalialkio. Neutraalialkiota ei itse asiassa ole, sillä kaikille $A \in \mathscr{P}(X)$ pätee $A - X = \emptyset \neq X$.

Merkintöjä $+$ ja $\cdot$ käytetään yleisesti eri laskutoimituksille. Merkintää $+$ käytetään kuitenkin ainoastaan kommutatiiviselle laskutoimitukselle. Usein laskutoimitukselle ei käytetä mitään erityistä merkkiä vaan laskutoimitusta merkitään kirjoittamalla laskutoimituksella varustetun joukon alkioista muodostettuja "sanoja" kuten tavanomaisessa kertolaskussa on tapana: $a \cdot b = ab$.

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

Lause 1.12. *Olkoon $(X, *)$ laskutoimituksella varustettu joukko. Jos $*$ on assosiatiivinen laskutoimitus, jolla on neutraalialkio e, niin*

(1) *alkiolla $g \in X$ on käänteisalkio, jos ja vain jos sillä on vasen ja oikea käänteisalkio.*
(2) *jos alkiolla $g \in X$ on käänteisalkio, se on yksikäsitteinen.*
(3) *jos alkiolla $g \in X$ on käänteisalkio, se on alkion g ainoa vasen/oikea käänteisalkio*

Todistus. Todistamme kohdan (1): 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 $g' = g''$ on alkion g käänteisalkio. Toinen suunta seuraa suoraan määritelmästä. Muut kohdat todistetaan harjoituksissa. □

Olkoon $(A, \cdot)$ assosiatiivisella laskutoimituksella varustettu joukko. Jokaiselle $a \in A$ määritellään positiiviset *potenssit*: Asetamme $a^1 = a$, ja kaikille $n \in \mathbb{N}$, $n \geq 1$

asetamme $a^{n+1} = a^n a$. Jos laskutoimituksella varustetussa joukossa $(A, \cdot)$ 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 $a^n = (a^{-1})^{-n}$.

Assosiatiivisella laskutoimituksella varustettu joukossa $(A, +)$ määrittelemme vastaavasti alkion a positiiviset *monikerrat* asettamalla $1\ a = a$ ja $(n+1)a = na + a$ kaikille $n \in \mathbb{Z}$, $n \geq 1$. Jos laskutoimituksella varustetussa joukossa $(A, +)$ on neutraalialkio 0, niin asetetaan $0\ a = 0 \in A$ ja jos alkiolla $a \in A$ on käänteisalkio $-a$ laskutoimituksen $+$ suhteen, asetetaan $(-1)\ a = -a$ ja negatiivisille $n \in \mathbb{Z}$ asetamme $na = (-n)(-a)$.

Tavanomaiset laskulait pätevät potensseille ja monikerroille:

Lemma 1.13. *Olkoon $(A, \cdot)$ assosiatiivisella laskutoimituksella varustettu joukko, jolla on neutraalialkio. Tällöin*

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

Jos alkiolla a on käänteisalkio, niin kohtien (1) ja (2) väitteet pätevät kaikille kokonaisluvuille $m, n \in \mathbb{Z}$.
Olkoon $(H, +)$ kommutatiivisella laskutoimituksella varustettu joukko, jolla on neutraalialkio. Tällöin

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

Jos alkiolla a on käänteisalkio, niin kohtien (3) ja (4) väitteet pätevät kaikille kokonaisluvuille $m, n \in \mathbb{Z}$.

Todistus. Harjoitustehtävä 1.12. □

Olkoon $(A, *)$ laskutoimituksella varustettu joukko. Jos $B \subset A$, $B \neq \emptyset$ ja kaikille $b, b' \in B$ pätee $b * b' \in B$, niin B on laskutoimituksella varustetun joukon $(A, *)$ *vakaa* osajoukko. Laskutoimitus $*$ määrittelee *indusoidun laskutoimituksen* $*|_B$ joukossa B, kun asetetaan $b *|_B b' = b * b'$. Yleensä indusoidulle laskutoimitukselle käytetään samaa merkintää kuin laskutoimitukselle, joka indusoi sen: $*|_B = *$.

Esimerkki 1.14. (a) Reaalilukujen ja rationaalilukujen kertolaskut indusoivat laskutoimitukset joukkoihin $\mathbb{R} - \{0\}$ ja $\mathbb{Q} - \{0\}$. Näitä laskutoimituksella varustettuja joukkoja

$$\mathbb{R}^\times = (\mathbb{R} - \{0\}, \cdot)$$

ja

$$\mathbb{Q}^\times = (\mathbb{Q} - \{0\}, \cdot)$$

kutsutaan (kurssin aikana selvenevistä syistä) reaalilukujen ja rationaalilukujen *multiplikatiivisiksi ryhmiksi*. Laskutoimituksella varustetut joukot $(\mathbb{R}, +)$ ja $(\mathbb{Q}, +)$ taas ovat reaalilukujen ja rationaalilukujen *additiiviset ryhmät*.

(b) Olkoon

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

Tällöin kaikille $A, B \in P$ pätee $A + B \in P$ ja $AB \in P$, joten matriisien yhteenlasku ja kertolasku indusoivat kaksi laskutoimitusta joukossa $P \subset \mathrm{M}_2(\mathbb{R})$.

Kahden laskutoimituksella varustetun joukon väliset kuvaukset, jotka sopivat laskutoimitusten kanssa hyvin yhteen, ovat algebrassa keskeisessä osassa:

Määritelmä 1.15. Olkoot $(E, *)$ ja $(E', \circledast)$ laskutoimituksella varustettuja joukkoja. Kuvaus $h\colon (E, *) \to (E', \circledast)$ on *homomorfismi*, jos $h(a * b) = h(a) \circledast h(b)$ kaikille $a, b \in E$.

- Bijektiivinen homomorfismi on *isomorfismi*.
- Isomorfismi laskutoimituksella varustetulta joukolta E itselleen on *automorfismi*.

Laskutoimituksella varustetut joukot $(E, *)$ ja $(E', \circledast)$ ovat *isomorfisia (keskenään)*, jos on isomorfismi $h\colon (E, *) \to (E', \circledast)$.

Edellä määriteltyjen lisäksi käytetään melko usein seuraavia nimityksiä:

- Injektiivinen homomorfismi on *monomorfismi*.
- Surjektiivinen homomorfismi on *epimorfismi*.

Tällä kurssilla käytämme näistä homomorfismityypeistä pääsääntöisesti nimityksiä injektiivinen ja surjektiivinen homomorfismi.

Esimerkki 1.16. (a) Reaalilukujen kertolasku indusoi laskutoimituksen positiivisten reaalilukujen joukossa $\mathbb{R}_+ =]0, \infty[$. Eksponenttikuvaus $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}_+, \cdot)$, $\exp(x) = e^x$, on homomorfismi: Kaikille $x, y \in \mathbb{R}$ pätee

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

Eksponenttifunktio on tunnetusti bijektio, joten se on isomorfismi. Eksponenttifunktion käänteisfunktio $\log\colon (\mathbb{R}_+, \cdot) \to (\mathbb{R}, +)$ on myös homomorfismi (ja tietysti myös isomorfismi): Kaikille $x, y \in \mathbb{R}_+$ pätee

$$\log(xy) = \log(x) + \log(y).$$

(b) Yhteenlaskulla varustetut joukot $(\mathrm{M}_n(\mathbb{R}), +)$ ja $(\mathbb{R}^{n^2}, +)$ ovat selvästi isomorfisia.
(c) 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:

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

Isomorfiset laskutoimituksella varustetut joukot ovat algebrallisilta ominaisuuksiltaan samanlaiset vaikka joukot ja laskutoimitukset voivat "ulkoisesti" olla hyvinkin erilaisia, kuten Esimerkin 1.16 avulla huomaamme.

Propositio 1.17. *Olkoon $h\colon (E, *) \to (E', \circledast)$ surjektiivinen homomorfismi.*

(1) *Jos $*$ on kommutatiivinen, niin $\circledast$ on kommutatiivinen*
(2) *Jos $*$ on assosiatiivinen, niin $\circledast$ on assosiatiivinen*
(3) *Jos laskutoimituksella varustetussa joukossa E on neutraalialkio e, niin $h(e)$ on laskutoimituksella varustetun joukon E' neutraalialkio.*

Todistus. (1) Olkoot $a', b' \in E'$. Tällöin on $a, b \in E$, joille $h(a) = a'$ ja $h(b) = b'$. Siis

$$a' \circledast b' = h(a) \circledast h(b) = h(a * b) = h(b * a) = h(b) \circledast h(a) = b' \circledast a',$$

joten $\circledast$ on kommutatiivinen.
(2) Harjoitustehtävä 1.15.
(3) Olkoon $g' \in E'$. Tällöin $g' = h(g)$ jollain $g \in E$ ja pätee

$$h(e) \circledast g' = h(e) \circledast h(g) = h(e * g) = h(g) = g'$$

ja

$$g' \circledast h(e) = h(g) \circledast h(e) = h(g * e) = h(g) = g',$$

joten $h(e)$ on neutraalialkio. □

Seuraavat esimerkit osoittavat, että mikään Proposition 1.17 väitteistä ei päde yleisesti ilman oletusta homomorfismin h surjektiivisuudesta.

Esimerkki 1.18. (a) Matriisien kertolasku joukossa $\mathrm{M}_n(R)$ ei ole kommutatiivinen, kun $n \geq 2$, koska esimerkiksi

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

Esimerkin 1.16 (c) homomorfismi antaa esimerkin homomorfismista kommutatiivisesta magmasta sellaiseen magmaan, joka ei ole kommutatiivinen.

(b) Esimerkissä 1.6 (b) osoitetiin, että laskutoimituksella varustettu joukko $(Z, -)$ ei ole assosiatiivinen. Kuvaus $k\colon \{0, +\} \to (\mathbb{Z}, -)$, $k(0) = 0$, on homomorfismi assosiatiivisesta magmasta magmaan, joka ei ole assosiatiivinen.

(c) Helppo esimerkki siitä, että neutraalialkio ei välttämättä kuvaudu neutraalialkiolle, jos homomorfismi ei ole surjektiivinen, on homomorfismi $h\colon (\mathbb{N}, +) \to (\mathbb{N}, \cdot)$, $h(n) = 0$ kaikilla $n \in \mathbb{N}$. Kuvaus h on todellakin homomorfismi, koska kaikille $m, n \in \mathbb{N}$ pätee

$$h(n + m) = 0 = 0\,0 = h(m)h(n).$$

Kuitenkaan neutraalialkio $0 \in (\mathbb{N}, +)$ ei kuvaudu neutraalialkioksi $1 \in (\mathbb{N}, \cdot)$.

Propositio 1.19. *(1) Isomorfismin käänteiskuvaus on isomorfismi.*
(2) Homomorfismien yhdistetty kuvaus on homomorfismi.

Todistus. (1) Olkoon $\phi\colon (A, *) \to (B, \circledast)$ isomorfismi. Olkoot $b_1, b_2 \in B$. Koska ϕ on bijektio, pätee

$$b_1 \circledast b_2 = \phi(\phi^{-1}(b_1)) \circledast \phi(\phi^{-1}(b_2)).$$

Koska ϕ on homomorfismi, saamme

$$\phi(\phi^{-1}(b_1)) \circledast \phi(\phi^{-1}(b_2)) = \phi(\phi^{-1}(b_1) * \phi^{-1}(b_2)).$$

Yhdistämällä nämä kaksi yhtälöä saamme

$$b_1 \circledast b_2 = \phi(\phi^{-1}(b_1) * \phi^{-1}(b_2)),$$

mistä seuraa

$$\phi^{-1}(b_1 \circledast b_2) = \phi^{-1}(b_1) * \phi^{-1}(b_2),$$

koska ϕ on bijektio. Siis ϕ^{-1} on homomorfismi.
(2) Harjoitustehtävä 1.16. □

Samassa joukossa E voidaan määritellä erilaisia laskutoimituksia kuten Esimerkissä 1.2 havaittiin. Tarkastelemme kurssilla Algebra 1B *renkaiden* teoriaa. Renkaat ovat kahdella laskutoimituksella varustettuja joukkoja, joiden laskutoimituksilta vaaditaan muutamia lisäominaisuuksia, jotka esimerkiksi kokonais-, rationaali- ja reaalilukujen yhteen- ja kertolaskulla on. Yksi näistä ominaisuuksista on distributiivisuus.

Määritelmä 1.20. Olkoon $(A, *, \oplus)$ kahdella laskutoimituksella varustettu joukko. Laskutoimitus $*$ on

- *vasemmalta distributiivinen laskutoimituksen $\oplus$ suhteen*, jos
$$a * (b \oplus c) = (a * b) \oplus (a * c)$$
kaikilla $a, b, c \in A$.
- *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.*

Distributiivisuuden määritteleviä yhtälöitä sanotaan *osittelulaeiksi.*

Esimerkki 1.21. Kokonais-, rationaali ja reaalilukujen kertolasku on distributiivinen yhteenlaskun suhteen: Kaikille m, n, l näissä lukualueissa pätee
$$m(n + l) = mn + ml = (n + l)m.$$

Harjoitustehtäviä.

1.1. Olkoon $*$ rationaalilukujen laskutoimitus, joka määritellään asettamalla
$$a * b = \frac{a + b}{2}.$$
Onko laskutoimitus $*$ assosiatiivinen? Onko laskutoimituksella $*$ neutraalialkio?

1.2. Olkoon $*$ positiivisten reaalilukujen joukon
$$\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\}$$
laskutoimitus, joka määritellään asettamalla
$$a * b = \sqrt{ab}.$$
Onko laskutoimitus $*$ assosiatiivinen? Onko laskutoimituksella $*$ neutraalialkio?

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

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

1.5. Onko joukon $\mathscr{P}(X)$ laskutoimitus $-$ assosiatiivinen?

1.6. Muodosta Esimerkissä 1.4 (e) kuvatun kivi-paperi-sakset –pelin laskutaulu. Onko pelin laskutoimitus assosiatiivinen?

1.7. Onko matriisien kertolasku assosiatiivinen joukossa $\mathrm{M}_2(\mathbb{R})$?

1.8. Olkoon
$$\Gamma = \{A \in \mathrm{M}_2(\mathbb{R}) : \det A = 1\}.$$
Osoita, että matriisien kertolasku indusoi laskutoimituksen joukossa Γ. Miten matriisien yhteenlasku käyttäytyy?

1.9. Varustetaan joukko $X = \{a, b\}$ laskutoimituksella $*$, jonka laskutaulu on

$*$	a	b
a	b	b
b	a	a

.

Onko laskutoimitus $*$ kommutatiivinen? Onko se assosiatiivinen?

1.10. Avaruuden $\mathbb{R}^3$ *vektoritulo* eli *ristitulo* on laskutoimitus, joka määritellään asettamalla kaikille $a = (a_1, a_2, a_3)$ ja $b = (b_1, b_2, b_3) \in \mathbb{R}^3$

$$a \times b = \left(\det \begin{pmatrix} a_2 & b_2 \\ a_3 & b_3 \end{pmatrix}, -\det \begin{pmatrix} a_1 & b_1 \\ a_3 & b_3 \end{pmatrix}, \det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \right).$$

(1) Osoita, että $\times$ on *antikommutatiivinen*: $b \times a = -a \times b$ kaikille $a, b \in \mathbb{R}^3$.
(2) Osoita, että $\times$ on distributiivinen vektorien komponenteittaisen yhteenlaskun suhteen.
(3) Osoita, että $\times$ ei ole assosiatiivinen.

1.11. Olkoon $X \neq \emptyset$ ja olkoon $*$ joukon X assosiatiivinen laskutoimitus. Osoita:

(1) Jos alkiolla $g \in X$ on käänteisalkio, se on yksikäsitteinen.
(2) Jos alkiolla $g \in X$ on käänteisalkio, se on alkion g ainoa vasen käänteisalkio

1.12. Todista Lemman 1.13 kohtien (1) ja (2) potenssien laskusäännöt.

1.13. Määritellään Harjoitustehtävässä 1.9 käsitellylle laskutoimitukselle $*$ joukon X alkioiden positiiviset potenssit kuten teimme ennen Lemmaa 1.13. Pätevätkö Lemman 1.13 laskusäännöt?

1.14. Olkoot $(A, *)$ ja $(C, \circledast)$ laskutoimituksella varustettuja joukkoja ja olkoon $f\colon (A, *) \to (C, \circledast)$ homomorfismi. Osoita:

(1) Jos $B \subset A$ on vakaa, niin $f(B) \subset C$ on vakaa.
(2) Jos $B \subset C$ on vakaa ja $f^{-1}(B)$ ei ole tyhjä joukko, niin $f^{-1}(B) \subset A$ on vakaa.

1.15. Olkoon $h\colon (E, *) \to (E', \circledast)$ surjektiivinen homomorfismi. Osoita: Jos $*$ on assosiatiivinen, niin $\circledast$ on assosiatiivinen.

1.16. Olkoot $f\colon (A, *) \to (B, \circledast)$ ja $g\colon (B, \circledast) \to (C, \cdot)$ laskutoimituksella varustettujen joukkojen homomorfismeja. Osoita, että $g \circ f$ on homomorfismi.

1.17. Olkoon $(A, *)$ laskutoimituksella varustettu joukko ja olkoon $\mathrm{Hom}(A, A)$ kaikkien homomorfismien $\phi\colon (A, *) \to (A, *)$ joukko. Osoita, että homomorfismien yhdistäminen on laskutoimitus joukossa $\mathrm{Hom}(A, A)$.

1.18. Osoita, että laskutoimituksella varustettu joukko $(\mathbb{R} - \{0\}, \cdot)$ on isomorfinen matriisien kertolaskulla varustetun joukon

$$\left\{ \operatorname{diag}(a, 1/a) : a \in \mathbb{R} - \{0\} \right\} = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} : a \in \mathbb{R} - \{0\} \right\}$$

kanssa.

1.19. Ovatko laskutoimituksella varustetut joukot $(\mathscr{P}(\{0, 1\}), \cap)$ ja $(\mathscr{P}(\{0, 1\}), \cup)$ isomorfisia?

1.20. Keksi esimerkki laskutoimituksella varustetusta joukosta $(A, *)$ ja alkiosta $a \in A$, jolla on useita vasempia käänteisalkioita.

---

[10]Vihje: Kannattaa kerrata lineaarialgebran tietoja. Assosiatiivisuuden puuttumisen voi nähdä esimerkiksi tarkastelemalla standardikantavektorien keskinäisiä tuloja.

[20]Vihje: Kannattaa miettiä tämän luvun esimerkkejä.

2. Kompleksiluvut

Tässä luvussa tutustumme lyhyesti kompleksilukuihin. Keskitymme lähes pelkästään algebran kannalta oleelliseen materiaaliin.

Kompleksiluvut $\mathbb{C} = (\mathbb{C}, +, \cdot)$ saadaan varustamalla taso $\mathbb{R}^2$ komponenteittaisella yhteenlaskulla (katso Esimerkki 1.3) ja kertolaskulla, joka määritellään asettamalla

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

Huomaa, että

$$(a, 0) + (c, 0) = (a + c, 0)$$

ja

$$(a, 0)(c, 0) = (ac, 0),$$

joten voimme ajatella kompleksilukuja $(a, 0)$ ja $(c, 0)$ reaalilukuina a ja c.

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

$$(a, b) = (a, 0) + (0, b) = a(1, 0) + b(0, 1) = a + i\, b,$$

jossa käytetään edellä tehtyä sopimusta, jonka mukaan kompleksiluku $(a, 0)$ samastetaan reaaliluvun a kanssa. Näillä merkinnöillä kompleksilukujen laskutoimitukset ovat

$$\begin{aligned}(a + i\, b) + (c + i\, d) &= (a + c) + i(b + d),\\ (a + i\, b)(c + i\, d) &= (ac - bd) + i(ad + bc).\end{aligned}$$

Esimerkki 2.1. (a) $i^2 = (0 \cdot 0 - 1 \cdot 1) + i(0 \cdot 1 + 1 \cdot 0) = -1$.
(b) $(1 + i)^2 = (1 \cdot 1 - 1 \cdot 1) + i(1 \cdot 1 + 1 \cdot 1) = 2\, i$.

Määritelmä 2.2. Olkoot a ja b reaalilukuja. Kompleksiluvun $z = a + i\, b$ *reaaliosa* on $\mathrm{Re}(z) = a$, *imaginaariosa* on $\mathrm{Im}(z) = b$ ja sen *(kompleksi)konjugaatti* eli *liittoluku* on $\bar{z} = a - i\, b$. Kompleksiluvun $z = a + i\, b$ *moduli* on

$$|z| = \sqrt{z\bar{z}} = \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2} = \sqrt{a^2 + b^2} = \|(a, b)\|.$$

Jos $x \in \mathbb{R} \subset \mathbb{C}$, niin sen moduli on sama kuin sen itseisarvo reaalilukuna:

$$|x + 0\, i| = \sqrt{x^2} = |x|.$$

Seuraava tulos antaa kompleksilukujen laskutoimitusten perusominaisuudet.

Propositio 2.3. *(1) Kompleksilukujen yhteen- ja kertolasku ovat assosiatiivisia ja kommutatiivisia laskutoimituksia.*

(2) Yhteenlaskun ja kertolaskun neutraalialkiot ovat $0 = 0 + 0\, i$ *ja* $1 = 1 + 0\, i$.

(3) Kompleksilukujen kertolasku on distributiivinen yhteenlaskun suhteen.

(4) Jokaisella kompleksiluvulla z *on vastaluku* $-z = -1\, z$. *Jokaisella nollasta poikkeavalla kompleksiluvulla* z *on käänteisluku*

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

(5) Upotuskuvaukset $j\colon (\mathbb{R}, +) \to (\mathbb{C}, +)$ *ja* $j\colon (\mathbb{R}, \cdot) \to (\mathbb{C}, \cdot)$, *jotka määritellään asettamalla* $j(x) = x$, *ovat injektiivisiä homomorfismeja.*

Todistus. Kohdat (1)–(4) jätetään harjoitustehtäviksi.

(5) Määritelmän mukaan kaikille reaaliluvuille x pätee $j(x) = x + 0\,i$. Siispä

$$j(x+y) = x + y + 0\,i = (x + 0\,i) + (y + 0\,i) = j(x) + j(y)$$

ja

$$j(x)j(y) = (x + 0\,i)(y + 0\,i) = (xy - 0) + i(x\,0 + 0\,y) = xy + 0\,i = j(xy). \quad \square$$

Proposition 2.3 nojalla kompleksilukujen kertolaskut voidaan laskea "tavallisilla laskusäännöillä" huomioimalla, että $i^2 = -1$:

$$\begin{aligned}(a + i\,b)(c + i\,d) &= a\,c + a\,i\,d + i\,b\,c + i\,b\,i\,d = ac + i\,ad + i\,bc + i^2\,bd \\ &= (ac - bd) + i(ad + bc).\end{aligned}$$

On helppo tarkastaa, että kompleksilukujen kertolasku indusoi laskutoimituksen joukkoon $\mathbb{C} - \{0\}$. Laskutoimituksella varustettu joukko

$$\mathbb{C}^\times = (\mathbb{C} - \{0\}, \cdot)$$

on *kompleksilukujen multiplikatiivinen ryhmä*. Laskutoimituksella varustettu joukko $(\mathbb{C}, +)$ on *kompleksilukujen additiivinen ryhmä*.

Esimerkki 2.4. Koska kompleksilukujen kertolasku on assosiatiivinen, voidaan määritellä kompleksilukujen potenssit. Esimerkiksi $\left(\dfrac{1+i}{\sqrt{2}}\right)^8 = i^4 = 1$.

Propositio 2.5. *Kuvaukset* $\bar{\cdot}\colon (\mathbb{C}, +) \to (\mathbb{C}, +)$ *ja* $\bar{\cdot}\colon (\mathbb{C}, \cdot) \to (\mathbb{C}, \cdot)$ *ovat automorfismeja. Kuvaukset* $|\cdot|\colon (\mathbb{C}, \cdot) \to ([0, \infty[, \cdot)$ *ja* $|\cdot|\colon \mathbb{C}^\times \to \mathbb{R}_+$ *ovat surjektiivisia homomorfismeja.*

Todistus. Kompleksikonjugoinnin homomorfisuutta koskevat väitteet todistetaan harjoitustehtävässä 2.4. Harjoitustehtävän 2.4 kohdan (1) nojalla jokaiselle $z \in \mathbb{C}$ pätee $z = \bar{\bar{z}}$, joten $\bar{\cdot}$ on bijektio ja siis automorfismi.

Osoitetaan, että moduli on homomorfismi: Olkoot $z, w \in \mathbb{C}$. Modulin määritelmän, kompleksikonjugoinnin homomorfisuuden ja kompleksilukujen kertolaskun kommutatiivisuuden ja assosiatiivisuuden nojalla saadaan

$$|zw|^2 = (zw)\overline{(zw)} = (zw)(\bar{z}\bar{w}) = (z\bar{z})(w\bar{w}) = |z|^2|w|^2\,,$$

mistä väite seuraa ottamalla neliöjuuri.

Modulin surjektiivisuus seuraa siitä, että reaaliluvun moduli kompleksilukuna on sama kuin sen itseisarvo. $\square$

Propositio 2.6 (Kolmioepäyhtälö)**.** *Kaikilla* $z, w \in \mathbb{C}$ *pätee*

$$|z + w| \leq |z| + |w|\,.$$

Todistus. Todistettu kurssilla Lineaarinen algebra ja geometria 1. $\square$

Napakoordinaattikuvaus $N\colon \mathbb{R}_+ \times \mathbb{R} \to \mathbb{R}^2$,

$$N(r, \phi) = (r\cos\phi, r\sin\phi),$$

kuvaa määrittelyjoukkonsa (oikean puolitason) joukoksi $\mathbb{R}^2 - \{0\}$. Napakoordinaattien avulla voimme siis esittää jokaisen kompleksiluvun $z \neq 0$ muodossa

$$z = N(r, \phi) = r(\cos\phi + i\sin\phi).$$

Itse asiassa normin homomorfisuuden nojalla saadaan

$$|z| = |r(\cos\phi + i\sin\phi)| = r|(\cos\phi + i\sin\phi)| = r\sqrt{\cos^2\phi + \sin^2\phi} = r,$$

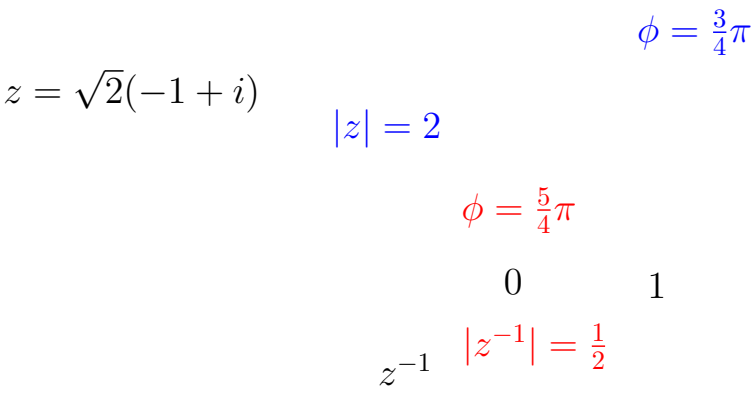
joten

$$z = |z|(\cos\phi + i\sin\phi),$$

missä $\phi \in \mathbb{R}$ on tason $\mathbb{R}^2$ vektorien $(1,0)$ ja $(\mathrm{Re}(z), \mathrm{Im}(z))$ välinen kulma positiiviseen kiertosuuntaan eli vastapäivään mitattuna. Kulma ϕ on kompleksiluvun z *argumentti*. Se on määritelty täyden kulman 2π monikertaa vaille trigonometristen funktioiden jaksollisuuden nojalla:

$$\cos(\phi + k\,2\pi) + i\sin(\phi + k\,2\pi) = \cos\phi + i\sin\phi$$

kaikilla $k \in \mathbb{Z}$.



KUVA 1. Kompleksiluvun $\sqrt{2}(-1+i)$ ja sen käänteisluvun esitykset napakoordinaattien avulla.

Trigonometristen funktioiden kulman yhteenlaskukaavojen avulla voimme osoittaa, että kompleksilukujen kertolasku sopii hyvin yhteen napakoordinaattien kanssa:

Propositio 2.7. *(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*

$$\prod_{k=1}^{n} z_k = z_1 z_2 \cdots z_n = (\prod_{k=1}^{n} r_k)(\cos(\sum_{k=1}^{n}\phi_k) + i\sin(\sum_{k=1}^{n}\phi_k)).$$

Todistus. Harjoitustehtävä 2.5. □

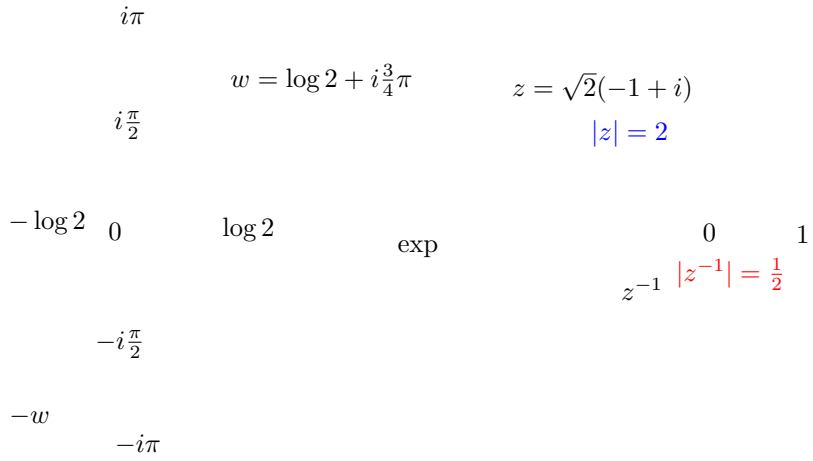
Napakoordinaattikuvauksen avulla voidaan määritellä algebran (ja myöhemmin kompleksianalyysin) kannalta merkittävä kuvaus:

Määritelmä 2.8. Kuvaus $\exp\colon \mathbb{C} \to \mathbb{C}$, joka määritellään asettamalla jokaiselle $z = x + i\,y \in \mathbb{C}$

$$\exp(z) = e^z = e^{x+iy} = e^x(\cos y + i\sin y),$$

on *(kompleksinen) eksponenttifunktio.*

Propositio 2.9. *Eksponenttifunktio* $\exp\colon (\mathbb{C}, +) \to \mathbb{C}^\times$ *on surjektiivinen homomorfismi.*



KUVA 2. Kompleksinen eksponenttifunktio. Eri suorien kuvautumista on havainnollistettu väreillä. Piste $w = \log 2 + i\frac{3}{4}\pi$ kuvautuu eksponenttifunktiolla pisteeksi $z = \sqrt{2}(-1+i)$ ja piste $-w$ pisteeksi z^{-1}.

Todistus. Osoitamme ensin, että kompleksinen eksponenttifunktio on homomorfismi. Olkoot $z = x + i\,y, w = u + i\,v \in \mathbb{C}$. Tällöin reaalisen eksponenttifunktion laskusääntöjen ja Proposition 2.7 nojalla

$$\begin{aligned}\exp(z+w) &= e^{x+u}\big(\cos(y+v) + i\sin(y+v)\big)\\ &= e^x e^u(\cos y + i\sin y)(\cos v + i\sin v)\\ &= \exp(z)\exp(w).\end{aligned}$$

Olkoon $g\colon \mathbb{R}^2 \to \mathbb{R}_+ \times \mathbb{R}$, $g(x,y) = (e^x, y)$. Tällöin $g(\mathbb{R}^2) = \mathbb{R}_+ \times \mathbb{R}$. Jos tulkitsemme kompleksisen eksponenttifunktion kuvauksena, joka on määritelty tasossa $\mathbb{R}^2$, pätee $\exp = N \circ g$. Siis exp on surjektiivinen, koska molemmat kuvaukset g ja napakoordinaattikuvaus N ovat surjektiivisia. □

Harjoitustehtäviä.

2.1. Osoita, että kompleksilukujen kertolasku on assosiatiivinen ja kommutatiivinen laskutoimitus. Osoita, että kompleksilukujen kertolasku on distributiivinen yhteenlaskun suhteen. Onko yhteenlasku distributiivinen kertolaskun suhteen?

2.2. Olkoot $z, w \in \mathbb{C}$ lukuja, joille pätee $zw = 0$. Osoita, että $z = 0$ tai $w = 0$ kahdella tavalla:

(1) käyttämättä napakoordinaatteja ja
(2) napakoordinaattien avulla.

2.3. Osoita, että kompleksilukujen kertolaskulle pätee seuraava laskusääntö: Jos $a, b, c \in \mathbb{C}$, $c \neq 0$ ja $ac = bc$, niin $a = b$.

2.4. Osoita, että kaikilla $z, w \in \mathbb{C}$ pätee

(1) $\bar{\bar{z}} = z$,
(2) $\overline{z+w} = \bar{z} + \bar{w}$,
(3) $\overline{zw} = \bar{z}\bar{w}$ ja
(4) $|\bar{z}| = |z|$.

[1]Vihje: Käytä reaalilukujen laskutoimitusten vastaavia ominaisuuksia, jotka oletamme tunnetuiksi

2.5. Olkoot $z = r(\cos\phi + i\sin\phi)$ ja $w = s(\cos\theta + i\sin\theta)$. Osoita, että

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

2.6. Olkoot $z_k = r_k(\cos\phi_k + i\sin\phi_k)$, $k = 1, 2, \ldots, n$. Osoita induktiolla, että

$$\prod_{k=1}^{n} z_k = z_1 z_2 \cdots z_n = (\prod_{k=1}^{n} r_k)(\cos(\sum_{k=1}^{n}\phi_k) + i\sin(\sum_{k=1}^{n}\phi_k)).$$

2.7. Olkoot $a_k \in \mathbb{R}$ kaikilla $k \in \{0, 1, 2, \ldots, n\}$ ja olkoon $z_0 \in \mathbb{C}$ yhtälön

$$\sum_{k=0}^{n} a_k z^k = 0 \tag{1}$$

ratkaisu. Osoita, että $\overline{z_0}$ on yhtälön (1) ratkaisu. Päteekö väite, jos oletetaan vain, että $a_k \in \mathbb{C}$ kaikilla $k \in \{0, 1, 2, \ldots, n\}$?

Tässä luvussa tutustumme kolmanteen tapaan muodostaa laskutoimitus joukkoon tunnettujen laskutoimitusten avulla. Tätä varten määrittelemme ensin tarvittavan ekvivalenssirelaation käsitteen.

Määritelmä 3.1. Olkoon A epätyhjä joukko. Joukon $A \times A$ osajoukko on *relaatio* joukossa A.

Jos $\mathrm{R} \subset A \times A$ on relaatio, usein merkitään $a \,\mathrm{R}\, b$, jos $(a, b) \in \mathrm{R}$.

Määritelmä 3.2. 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*. Jos R on ekvivalenssirelaatio joukossa A, sanotaan, että joukon A alkiot a ja b ovat *ekvivalentteja*, jos $a \,\mathrm{R}\, b$.

Ekvivalenssirelaation merkkinä käytetään usein merkkiä $\sim$.

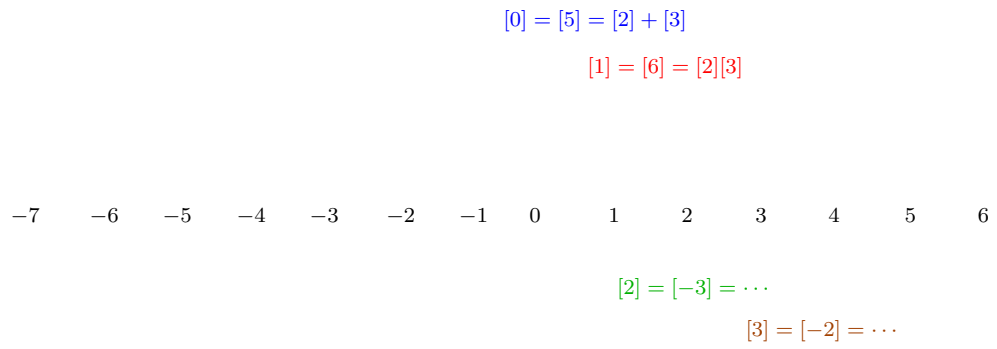
Määritelmä 3.3. Jos $\sim$ on ekvivalenssirelaatio joukossa A, niin jokainen joukon A alkio a määrää *ekvivalenssiluokan*

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

Ekvivalenssiluokkien joukko

$$A/\!\sim \;= \big\{[a] : a \in A\big\}$$

on ekvivalenssirelaatiota $\sim$ vastaava joukon A *tekijäjoukko*. Kuvaus $A \to A/\!\sim$, $a \mapsto [a]$, on ekvivalenssirelaatiota $\sim$ vastaava *tekijäkuvaus* eli *luonnollinen kuvaus*. Alkio $a \in A$ on ekvivalenssiluokkansa $[a]$ *edustaja*.



Kuva 3. Kongruenssiluokat modulo 5.

Esimerkki 3.4. Olkoon $q \in \mathbb{N}$, $q \geq 2$. Olkoon relaatio $\equiv$ kokonaislukujen joukossa $\mathbb{Z}$ määritelty säännöllä $a \equiv b$, jos on $k \in \mathbb{Z}$ siten, että $b = a + kq$. Tällöin $\equiv$ on ekvivalenssirelaatio:

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

Ekvivalenssirelaatiota $\equiv$ kutsutaan *kongruenssiksi (modulo q)*. Koska ekvivalenssirelaatio riippuu luonnollisesta luvusta q, tälle ekvivalenssirelaatiolle käytetään merkintää

$$a \equiv b \mod q \quad \text{tai} \quad a \equiv b \pmod{q}.$$

Kongruenssirelaation ekvivalenssiluokat ovat *kongruenssiluokkia (modulo q)*. Käytämme luvun $a \in \mathbb{Z}$ kongruenssiluokalle merkintää $a + q\mathbb{Z}$, erityisesti luvun 0 kongruenssiluokkaa merkitään $0 + q\mathbb{Z} = q\mathbb{Z}$. Kongruenssia modulo q vastaavalle tekijäjoukolle käytetään merkintää $\mathbb{Z}/q\mathbb{Z}$. Kokonaislukujen jakoyhtälön avulla (todistetaan lukuteorian alkeiskursseilla) nähdään, että

$$\mathbb{Z}/q\mathbb{Z} = \{q\mathbb{Z}, 1 + q\mathbb{Z}, 2 + q\mathbb{Z}, \ldots, q - 1 + q\mathbb{Z}\}.$$

Tämä merkintätapa on yhteensopiva luvussa 7 esiteltävän yleisen teorian kanssa.

Lemma 3.5. *Olkoon $\sim$ ekvivalenssirelaatio joukossa A. Pisteiden $x, y \in A$ ekvivalenssiluokille pätee:*

(1) *Jos $x \sim y$, niin $[x] = [y]$.*
(2) *Jos $[x] \cap [y] \neq \emptyset$, niin $[x] = [y]$.*

Todistus. Harjoitustehtävä 3.2. □

Olkoon I epätyhjä *indeksijoukko*. Olkoot A_i, $i \in I$, joukon A epätyhjiä osajoukkoja. Jos

$$A = \bigcup_{i \in I} A_i \tag{2}$$

ja kaikille $i \neq j$ pätee $A_i \cap A_j = \emptyset$, sanotaan, että A on *erillinen yhdiste* joukoista A_i, $i \in I$. Merkitsemme joukkojen A_i, $i \in I$, erillistä yhdistettä

$$A = \bigsqcup_{i \in I} A_i \,.$$

Tämä merkintä sisältää tiedon, että yhdistettävät joukot ovat erillisiä. Jos $A = \bigsqcup_{i \in I} A_i$, niin joukot A_i, $i \in I$ muodostavat joukon A *osituksen*.

Lemman 3.5 nojalla joukon X ekvivalenssirelaation $\sim$ ekvivalenssiluokat muodostavat joukon X osituksen. Itse asiassa myös käänteinen väite pätee: Jos joukot A_i, $i \in I$ muodostavat joukon A osituksen, määritellään relaatio R asettamalla $x \,\mathrm{R}\, y$, jos ja vain jos $x, y \in A_i$ jollain $i \in I$. Osoittautuu, että relaatio R on ekvivalenssirelaatio.

Propositio 3.6. *Olkoon $X \neq \emptyset$.*

(1) *Joukon X ekvivalenssirelaatio määrää joukon X osituksen.*
(2) *Joukon X ositus määrää joukon X ekvivalenssirelaation.*

Todistus. Kohta (1) seuraa Lemmasta 3.5.

Todistetaan kohta (2): Olkoon R osituksen $A = \bigsqcup_{i \in I} A_i$ määräämä relaatio. Tarkastamme ekvivalenssirelaation määrittelevät ominaisuudet:

- Koska $A = \bigcup_{i \in I} A_i$, niin jokaiselle $a \in A$ pätee $a \in A_i$ jollakin $i \in I$. Siis $a \,\mathrm{R}\, a$, joten R on refleksiivinen.
- Symmetrisyys on selvä, koska relaatio R määritellään ehdolla $a, b \in A_i$.
- Oletetaan, että $a, b \in A_i$ ja $b, c \in A_j$ joillain $i, j \in I$. Koska joukot A_k, $k \in I$ muodostavat joukon A osituksen, pätee joko $A_i = A_j$ tai $A_i \cap A_j = \emptyset$. Oletuksen mukaan $b \in A_i \cap A_j$, joten $A_i = A_j$ ja siis $a, c \in A_i$, joten relaatio R on transitiivinen. □

Määritelmä 3.7. Joukon A laskutoimitus $*$ ja ekvivalenssirelaatio $\sim$ ovat *yhteensopivat*, jos $a * b \sim a' * b'$ aina kun $a \sim a'$ ja $b \sim b'$. Jos joukon A ekvivalenssirelaatio $\sim$ ja laskutoimitus $*$ ovat yhteensopivat, niin joukon $A/\sim$ laskutoimitus $*$, joka määritellään asettamalla

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

on laskutoimituksen $*$ määräämä *tekijälaskutoimitus*.

On helppo nähdä, että yhteensopivuus takaa sen, että tekijälaskutoimitus on hyvin määritelty. Seuraavat havainnot seuraavat suoraviivaisesti määritelmistä:

Propositio 3.8. *Olkoon $\sim$ laskutoimituksella varustetun joukon $(E, *)$ laskutoimituksen $*$ kanssa yhteensopiva ekvivalenssirelaatio. Luonnollinen kuvaus $E \to E/\sim$ on surjektiivinen homomorfismi. Jos $e \in E$ on laskutoimituksen $*$ neutraalialkio, niin $[e] \in E/\sim$ on tekijälaskutoimituksen neutraalialkio.*

Todistus. Olkoon ϕ luonnollinen kuvaus. Kaikille $a, b \in E$ pätee

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

joten luonnollinen kuvaus on homomorfismi. Kuvauksen surjektiivisuus on selvää, koska jokaisella ekvivalenssiluokalla on edustaja joukossa E. Neutraalialkiota koskeva väite seuraa Propositiosta 1.17. □

Propositio 3.9. *Olkoon $\sim$ laskutoimituksella varustetun joukon $(E, *)$ laskutoimituksen $*$ kanssa yhteensopiva ekvivalenssirelaatio. Jos laskutoimitus $*$ on assosiatiivinen, sen tekijälaskutoimitus on assosiatiivinen. Jos $*$ on kommutatiivinen, sen tekijälaskutoimitus on kommutatiivinen.*

Todistus. Koska luonnollinen kuvaus on Proposition 3.8 mukaan surjektiivinen homomorfismi, väite seuraa Propositiosta 1.17. □

Esimerkki 3.10. (a) Kokonaislukujen yhteenlasku ja kertolasku ovat yhteensopivia kongruenssin kanssa. Osoitamme tämän yhteenlaskulle: Jos $a' = a+mq$ ja $b' = b+nq$, niin

$$a' + b' = a + b + (m + n)q,$$

joten

$$a' + b' \equiv a + b \mod q.$$

Kertolaskulle väite osoitetaan samaan tapaan harjoituksissa (Harjoitustehtävä 3.3). Kokonaislukujen yhteenlasku ja kertolasku määräävät siis laskutoimitukset q alkion joukossa $\mathbb{Z}/q\mathbb{Z}$. Proposition 3.9 nojalla molemmat laskutoimitukset ovat assosiatiivisia ja kommutatiivisia. Käytämme molemmille kongruenssiluokkien laskutoimituksille samaa merkintää kuin indusoiville laskutoimituksille:

$$(a + q\mathbb{Z}) + (b + q\mathbb{Z}) = (a + b) + q\mathbb{Z} \quad \text{ja} \quad (a + q\mathbb{Z})(b + q\mathbb{Z}) = ab + q\mathbb{Z}$$

kaikille $a + q\mathbb{Z}, b + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$. Proposition 3.8 mukaan $0 + q\mathbb{Z}$ on kongruenssiluokkien yhteenlaskun neutraalialkio ja $1 + q\mathbb{Z}$ on kongruenssiluokkien kertolaskun neutraalialkio.

(b) Määritellään ekvivalenssirelaatio $\sim$ reaalilukujen joukossa asettamalla $x \sim y$, jos ja vain jos $x - y \in \mathbb{Z}$. Reaalilukujen kertolasku ei ole yhteensopiva ekvivalenssirelaation $\sim$ kanssa, koska $1 \sim 2$ ja $1\,\frac{1}{2} = \frac{1}{2}$ ja $1 = 2\,\frac{1}{2}$ mutta luvut $\frac{1}{2}$ ja 1 eivät ole ekvivalentteja.

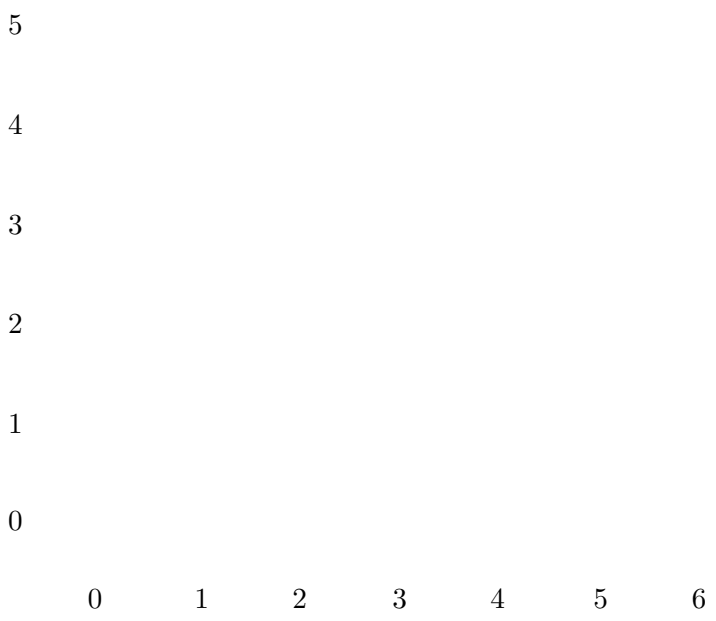
Reaalilukujen yhteenlasku on yhteensopiva ekvivalenssirelaation $\sim$ kanssa. Yhteenlasku siis määrittelee laskutoimituksen joukossa $\mathbb{R}/\sim$. Palaamme tähän esimerkkiin Harjoitustehtävässä 5.2.

Tarkastelemme seuraavaksi kokonaislukujen ja rationaalilukujen määrittelyä esimerkkinä tekijälaskutoimituksista.

Esimerkki 3.11. Määrittelemme kokonaisluvut "luonnollisten lukujen muodollisina erotuksina": Jos m ja n ovat luonnollisia lukuja ja $m \geq n$, niin niiden erotus $m - n$ on luonnollinen luku, se on yhtälön $n + x = m$ ratkaisu. 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 3.4 osoitetaan, että relaatio $\sim$ on ekvivalenssirelaatio.



KUVA 4. Kokonaislukujen määrittelyssä käytettävä ekvivalenssirelaatio joukossa $\mathbb{N} \times \mathbb{N}$.

Kokonaislukujen joukko on

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

Kokonaislukujen *yhteenlasku* on luonnollisten lukujen yhteenlaskun tulolaskutoimituksen

$$(m, n) + (p, q) = (m + p, n + q), \tag{3}$$

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

$$(m, n) * (p, q) = (mp + nq, mq + np) \tag{4}$$

indusoima laskutoimitus.

Laskutoimitusten määritelmät ovat järkeviä: Paria (m, n) tulee ajatella erotuksena $m - n$, jolloin lausekkeet (3) ja (4) vastaavat lausekkeita

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

ja

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

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 3.5.

Esimerkki 3.12. Rationaaliluvut muodostetaan vastaavalla tavalla kuin kokonaisluvut edellä kokonaislukujen muodollisten osamäärien avulla: Määrittelemme ekvivalenssirelaation $\sim$ joukossa $\mathbb{Z} \times \mathbb{Z}^*$ (missä $\mathbb{Z}^* = \mathbb{Z} - \{0\}$) asettamalla $(a,b) \sim (c,d)$, jos ja vain jos $ad = bc$.

Rationaalilukujen joukko on

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

Käytämme rationaaliluvuista tavanomaista merkintää $p/q = [(p,q)]$. Rationaalilukujen *yhteenlasku* on laskutoimituksen

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

indusoima tekijälaskutoimitus

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

ja rationaalilukujen *kertolasku* on kokonaislukujen kertolaskun tulolaskutoimituksen

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

indusoima laskutoimitus. Harjoitustehtävässä 3.6 osoitetaan, että laskutoimitukset $\oplus$ ja $\circledast$ ovat ekvivalenssirelaation $\sim$ kanssa yhteensopivia.

Kokonaislukujen ja rationaalilukujen konstruktiota luonnollisista luvuista lähtien tarkastellaan alkeellisemmin kurssin [LA] materiaalissa, jossa konstruoidaan myös reaali- ja kompleksiluvut laajentamalla asteittain luonnollisista luvuista lähtien. Samalla tarkastellaan, miten algebralliset ominaisuudet muuttuvat laajempaan lukualueeseen siirryttäessä.

Harjoitustehtäviä.

3.1. Mitkä seuraavista ovat joukon $\mathbb{C}$ ekvivalenssirelaatioita?

- $z \,\mathrm{R}\, w$, jos ja vain jos $\operatorname{Re} z = \operatorname{Re} w$.
- $z \,\mathrm{R}\, w$, jos ja vain jos $|z| \leq |w|$.
- $z \,\mathrm{R}\, w$, jos ja vain jos $\operatorname{Re} z = \operatorname{Im} w$.

3.2. Olkoon $\sim$ ekvivalenssirelaatio joukossa A. Olkoot $x, y \in A$. Osoita, että ekvivalenssiluokille pätee:

(1) Jos $x \sim y$, niin $[x] = [y]$.
(2) Jos $[x] \cap [y] \neq \emptyset$, niin $[x] = [y]$.

3.3. Osoita, että kokonaislukujen kertolasku on yhteensopiva kongruenssin kanssa.

3.4. Määritellään relaatio $\sim$ joukossa $\mathbb{N} \times \mathbb{N}$ asettamalla $(m,n) \sim (p,q)$, jos ja vain jos $m+q = n+p$. Osoita, että $\sim$ on ekvivalenssirelaatio.

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

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

Osoita, että $*$ on yhteensopiva tehtävän 3.4 ekvivalenssirelaation kanssa. Todistuksessa voi käyttää vain luonnollisia lukuja!

3.6. Määritellään relaatio $\sim$ joukossa $\mathbb{Z} \times \mathbb{Z}^*$ asettamalla $(a, b) \sim (c, d)$, jos ja vain jos $ad = bc$. Osoita, että $\sim$ on ekvivalenssirelaatio.

3.7. Määritellään laskutoimitukset $\oplus$ ja $\circledast$ joukossa $\mathbb{Z} \times \mathbb{Z}^*$ asettamalla

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

ja

$$(a, b) \circledast (c, d) = (ac, bd)\,.$$

Osoita, että nämä laskutoimitukset ovat yhteensopivia tehtävän 3.6 ekvivalenssirelaation kanssa.

3.8. Määritellään relaatio $\sim$ reaalilukujen joukossa $\mathbb{R}$ asettamalla $x \sim y$, jos ja vain jos $x = qy$ jollain $q \in \mathbb{Q}^\times$. Osoita, että $\sim$ on ekvivalenssirelaatio. Osoita, että tekijäjoukko $\mathbb{R}/\!\sim$ on ylinumeroituva.

3.9. Määritellään relaatio R joukossa $\mathbb{C}$ asettamalla $z\,\mathrm{R}\,w$, jos ja vain jos $|z| = |w|$. Osoita, että R on ekvivalenssirelaatio. Millaisia joukkoja relaation R ekvivalenssiluokat ovat?

3.10. Olkoon $f\colon X \to A$ jokin kuvaus. Määritellään relaatio $\sim_f$ joukossa X asettamalla $x \sim_f y$, jos ja vain jos $f(x) = f(y)$. Osoita, että $\sim_f$ on ekvivalenssirelaatio. Osoita, että f määrää bijektion $F\colon X/\!\sim_f \to f(X)$, kun asetetaan $F([x]) = f(x)$.

3.11. Olkoot $(X, *)$ ja $(A, \circledast)$ laskutoimituksella varustettuja joukkoja ja olkoon $\phi\colon (X, *) \to (A, \circledast)$ homomorfismi. Olkoon $\sim_\phi$ homomorfismin ϕ määräämä ekvivalenssirelaatio joukossa X kuten Harjoitustehtävässä 3.10. Osoita, että laskutoimitus $*$ ja ekvivalenssirelaatio $\sim_\phi$ ovat yhteensopivat. Osoita, että laskutoimitus $\circledast$ indusoi laskutoimituksen joukkoon $\phi(X)$ ja että homomorfismin ϕ määräämä kuvaus $\Phi\colon X/\!\sim_\phi \to \phi(X)$ on isomorfismi.

3.12. Määritellään ekvivalenssirelaatio $\sim$ laskutoimituksella varustetussa joukossa $\mathbb{C}^\times$ asettamalla $z \sim w$, jos ja vain jos $|z| = |w|$. Osoita, että $\sim$ on yhteensopiva kertolaskun kanssa. Osoita, että $\mathbb{C}^\times/\!\sim$ on isomorfinen laskutoimituksella varustetun joukon $(\mathbb{R}_+, \cdot)$ kanssa.

3.13. Määritellään ekvivalenssirelaatio $\sim$ laskutoimituksella varustetussa joukossa $(\mathbb{C}, +)$ asettamalla $z \sim w$, jos ja vain jos $z - w = k\ 2\pi i$ jollain $k \in \mathbb{Z}$. Osoita, että $\sim$ on yhteensopiva yhteenlaskun kanssa. Osoita, että $(\mathbb{C}, +)/\!\sim$ on isomorfinen kompleksilukujen multiplikatiivisen ryhmän $\mathbb{C}^\times$ kanssa.

Tässä luvussa tarkastelemme laskutoimituksella varustettuja joukkoja, joiden laskutoimitukselta oletamme muutamia yksinkertaisia ominaisuuksia. Näin määriteltävä ryhmän käsite on tärkeä esimerkiksi geometriassa ja lukuteoriassa.

Määritelmä 4.1. Laskutoimituksella varustettu joukko $(G, *)$ on *ryhmä*, jos

- laskutoimitus $*$ on assosiatiivinen,
- laskutoimituksella $*$ on neutraalialkio ja
- jokaisella $g \in (G, *)$ on käänteisalkio.

Ryhmän G alkioiden lukumäärä $\#G$ on ryhmän G *kertaluku*.

Ryhmä on keskeinen algebran rakenne, joka esiintyy monilla matematiikan aloilla esimerkiksi lineaarialgebrassa, geometriassa ja lukuteoriassa. Tällä kurssilla käsittelemme esimerkkejä eri aloilta yleisen teorian tarkastelun lisäksi.

Laskutoimituksella varustettuja joukkoja voidaan ryhmitellä ominaisuuksiensa mukaan erilaisiksi *algebrallisiksi rakenteiksi*, joista ryhmä on yksi esimerkki. Laskutoimituksella varustettu joukko on

- *puoliryhmä*, jos laskutoimitus on assosiatiivinen
- *monoidi*, jos se on puoliryhmä ja sillä on neutraalialkio

Ryhmä on siis monoidi, jonka jokaisella alkiolla on käänteisalkio.

Esimerkki 4.2. (a) Aikaisemmista esimerkeistämme ryhmiä ovat ainakin

- *kokonaislukujen (additiivinen) ryhmä* $(\mathbb{Z}, +)$,
- *rationaalilukujen (additiivinen) ryhmä* $(\mathbb{Q}, +)$,
- *reaalilukujen (additiivinen) ryhmä* $(\mathbb{R}, +)$,
- *kompleksilukujen (additiivinen) ryhmä* $(\mathbb{C}, +)$,
- *rationaalilukujen multiplikatiivinen ryhmä* $\mathbb{Q}^\times$,
- *reaalilukujen multiplikatiivinen ryhmä* $\mathbb{R}^\times$,
- *kompleksilukujen multiplikatiivinen ryhmä* $\mathbb{C}^\times$ ja
- *positiivisten reaalilukujen multiplikatiivinen ryhmä* $\mathbb{R}_+ = (\mathbb{R}_+, \cdot)$.

Se, että yllä olevan luettelon kokonais-, rationaali- ja reaaliluvuista koostuvat laskutoimituksella varustetut joukot ovat ryhmiä, seuraa näiden lukualueiden tunnetuista ominaisuuksista. Kompleksiluvuille tämä seuraa Propositiosta 2.3.

(b) Laskutoimituksella varustettu joukko $(\mathbb{Z}/q\mathbb{Z}, +)$ on ryhmä: Kokonaislukujen yhteenlaskun määräämä tekijälaskutoimitus on assosiatiivinen Proposition 3.9 mukaan. Alkio $0 = q\mathbb{Z}$ on neutraalialkio Proposition 3.8 mukaan. Alkion $k + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ käänteisalkio on $-k + q\mathbb{Z}$:

$$(k + q\mathbb{Z}) + (-k + q\mathbb{Z}) = (k - k) + q\mathbb{Z} = q\mathbb{Z} = (-k + q\mathbb{Z}) + (k + q\mathbb{Z}).$$

Ryhmä $(\mathbb{Z}/q\mathbb{Z}, +)$ on q alkion *äärellinen syklinen ryhmä*.

(c) Olkoon $n \in \mathbb{N}$, $n \geq 2$ ja olkoot $\mathrm{M}_n(\mathbb{C}) \supset \mathrm{M}_n(\mathbb{R}) \supset \mathrm{M}_n(\mathbb{Q}) \supset \mathrm{M}_n(\mathbb{Z})$ sellaisten $n \times n$-matriisien joukot joiden kertoimet ovat kompleksilukuja, reaalilukuja, rationaalilukuja ja kokonaislukuja. Matriisien kertolasku on assosiatiivinen laskutoimitus jokaisessa näistä joukoista. Sen neutraalialkio on matriisi $I_n = \mathrm{diag}(1, \ldots, 1)$, jonka determinantti on 1.

Olkoon $\mathbb{L}$ jokin lukualueista $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ tai $\mathbb{C}$. Jos $A, B \in \mathrm{M}_n(\mathbb{L})$ ja $\det A \neq 0 \neq \det B$, niin determinantin laskusäännöstä $\det AB = \det A \det B$ seuraa, että $\det AB \neq 0$. Siispä joukko $\{A \in \mathrm{M}_n(\mathbb{L}) : \det A \neq 0\}$ on laskutoimituksella varustetun joukon $(\mathrm{M}_n(\mathbb{L}), \cdot)$ vakaa osajoukko ja matriisien kertolasku indusoi laskutoimituksen tähän joukkoon. Joukko $\mathrm{M}_n(\mathbb{L})$ varustettuna matriisien kertolaskulla ei ole ryhmä, koska se sisältää muun muassa nollamatriisin, jolla ei ole käänteismatriisia.

Olkoon $\mathbb{K}$ nyt $\mathbb{Q}$, $\mathbb{R}$ tai $\mathbb{C}$. Jokaisella matriisilla $A \in \mathrm{M}_n(\mathbb{K})$, jonka determinantti ei ole 0, on käänteismatriisi A^{-1}, jonka determinantti on $1/\det A \neq 0$. Käänteismatriisi A^{-1} on siis alkion A käänteisalkio matriisien kertolaskulla varustetussa joukossa $\{A \in \mathrm{M}_n(\mathbb{K}) : \det A \neq 0\}$. Olemme löytäneet $\mathbb{K}$-*kertoimisen yleisen lineaarisen ryhmän*

$$\mathrm{GL}_n(\mathbb{K}) = \{A \in \mathrm{M}_n(\mathbb{K}) : \det A \neq 0\},$$

jonka laskutoimitus on matriisien kertolasku. Vastaavasti saadaan $\mathbb{K}$-*kertoiminen erityinen lineaarinen ryhmä*

$$\mathrm{SL}_n(\mathbb{K}) = \{A \in \mathrm{M}_n(\mathbb{K}) : \det A = 1\},$$

jonka laskutoimitus on matriisien kertolasku.

(d) Matriisien kertolaskulla varustettu joukko $\{A \in \mathrm{M}_n(\mathbb{Z}) : \det A \neq 0\} \subset \mathrm{GL}_n(\mathbb{Q})$ ei ole ryhmä. Matriisin $D = \mathrm{diag}(2, 2, \ldots, 2)$ determinantti on $2^n \neq 0$, joten matriisilla D on rationaalisessa yleisessä lineaarisessa ryhmässä käänteismatriisi

$$D^{-1} = \mathrm{diag}(1/2, 1/2, \ldots, 1/2) \in \mathrm{GL}_2(\mathbb{Q})\,.$$

Käänteismatriisi on yksikäsitteinen, joten matriisilla D ei ole käänteismatriisia magmassa $\{A \in \mathrm{M}_n(\mathbb{Z}) : \det A \neq 0\}$. Cramerin säännön (kofaktorimatriisin) avulla voidaan sen sijaan osoittaa, että

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

on ryhmä (Harjoitustehtävä 4.3).

Jatkossa ryhmän laskutoimitus jätetään usein mainitsematta ja puhutaan vain "ryhmästä G". Tällöin laskutoimitus on kuitenkin kiinnitetty ja usein konkreettisessa tilanteessa se on ennalta tiedossa. Esimerkiksi merkinnät $\mathbb{C}^\times$ ja $\mathrm{GL}_n(\mathbb{R})$ sisältävät tiedon käytettävästä laskutoimituksesta. Puhuttaessa abstraktisti vain ryhmästä G merkitään laskutoimitusta usein kuten kertolaskua ja neutraalialkiolle käytetään merkintää e tai joskus myös merkintää 1. Jos tarkastellaan useampia ryhmiä samalla kertaa voidaan niiden neutraalialkioille käyttää ryhmille käytettävien merkintöjen kanssa yhteensopivaa merkintää esimerkiksi niin, että ryhmän G' neutraalialkiota merkitään e'. Joskus tehdään toisenlaisiakin valintoja.

Propositio 4.3. *Ryhmällä G on seuraavat ominaisuudet:*

(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) $(ab)^{-1} = b^{-1}a^{-1}$ *kaikilla* $a, b \in G$.

Todistus. Väite (1) seuraa Propositiosta 1.8. Väitteet (2) ja (3) seuraavat Lauseesta 1.12.

Todistetaan väite (4): Koska pätee

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e,$$

niin väite seuraa kohdasta (3). □

Propositio 4.3(3) helpottaa siis käänteisalkion testaamista ryhmässä: riittää tarkastaa, että alkio on vasen tai oikea käänteisalkio.

Supistussäännöt ovat voimassa laskutoimituksella varustetussa joukossa $(A, *)$, jos kaikilla $a, b, c \in A$ pätee

(1) Jos $a * b = a * c$, niin $b = c$.
(2) Jos $a * b = c * b$, niin $a = c$.

Supistussäännöt ovat voimassa monissa laskutoimituksella varustetuissa joukoissa kuten esimerkiksi luonnollisten lukujen additiivisessa monoidissa $(\mathbb{N}, +)$, luonnollisten lukujen multiplikatiivisessa monoidissa $(\mathbb{N}-\{0\}, \cdot)$ ja kaikissa ryhmissä. Huomaa, että supistussääntö ei päde puoliryhmässä $(\mathbb{N}, \cdot)$, koska $0\,a = 0$ kaikille $a \in \mathbb{N}$.

Propositio 4.4. *Supistussäännöt pätevät ryhmässä.*

Todistus. Harjoitustehtävä 4.5. □

Propositio 4.5. *Olkoon A assosiatiivisella laskutoimituksella varustettu joukko, jossa on neutraalialkio. Tällöin A on ryhmä, jos ja vain jos yhtälöillä $ax = b$ ja $ya = b$ on ratkaisu joukossa A kaikilla $a, b \in A$.*

Todistus. Harjoitustehtävä 4.6. □

Seuraava tulos antaa keinon muodostaa uusia ryhmiä tunnetuista ryhmistä tulolaskutoimituksen avulla.

Propositio 4.6. *Olkoot G_1 ja G_2 ryhmiä. Niiden tulo $G_1 \times G_2$ on ryhmä.*

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 4.7. Laskutoimituksella varustetut joukot $(\mathbb{R}^n, +)$ ja $(\mathbb{Z}^n, +)$ ovat ryhmiä.

Olkoon X epätyhjä joukko ja olkoon

$$\mathrm{Perm}(X) = \{f \colon X \to X : f \text{ on bijektio}\}.$$

Laskutoimituksella $\circ$ varustettu joukko $\mathrm{Perm}(X)$ on joukon X *permutaatioryhmä*. Permutaatioryhmä on todellakin ryhmä Esimerkkien 1.6(d) ja 1.11(a) nojalla. Ryhmän $\mathrm{Perm}(X)$ alkioita voidaan kutsua joukon X *permutaatioiksi*. Näin on tapana tehdä erityisesti, jos joukko X on äärellinen.

Matematiikan eri aloilla joukkoihin voidaan liittää erilaisia lisärakenteita kuten vektoriavaruusrakenne, sisätulo, metriikka ja ryhmä. Tällaisten joukkojen permutaatioryhmien osajoukot, jotka säilyttävät valitun rakenteen tai ovat sen kanssa yhteensopivia, varustettuna indusoidulla laskutoimituksella (joka siis on kuvausten yhdistäminen) ovat usein ryhmiä.

Esimerkki 4.8. Lineaarialgebrasta muistamme, että kuvaus $L \colon \mathbb{R}^n \to \mathbb{R}^k$ on *lineaarikuvaus*, jos kaikilla $x, y \in \mathbb{R}^n$ ja $a \in \mathbb{R}$ pätee

$$L(x + y) = L(x) + L(y)$$

ja

$$L(ax) = aL(x).$$

Vektoriavaruuden $\mathbb{R}^n$ lineaaristen bijektioiden $L \colon \mathbb{R}^n \to \mathbb{R}^n$ joukko on permutaatioryhmän $\mathrm{Perm}(\mathbb{R}^n)$ vakaa osajoukko, sillä on helppo tarkastaa, että kahden lineaarikuvauksen yhdistetty kuvaus on lineaarikuvaus. Nämä lineaariset bijektiot muodostavat ryhmän $\mathrm{GL}(\mathbb{R}^n)$, jossa kuvausten yhdistäminen on laskutoimituksena: Laskutoimituksen assosiatiivisuutta ei tarvitse tarkastaa, koska se on permutaatioryhmän $\mathrm{Perm}(\mathbb{R}^n)$ laskutoimituksen indusoima. Identtinen kuvaus on lineaarikuvaus ja kurssilla Lineaarinen algebra ja geometria 1 osoitetaan, että lineaarisen bijektion käänteiskuvaus on lineaarinen bijektio.

Määritelmä 4.9. Ryhmä G on *kommutatiivinen* eli *Abelin ryhmä*, jos sen laskutoimitus on kommutatiivinen. Ryhmä G on *äärellinen*, jos joukko G on äärellinen.

Esimerkki 4.10. (a) Ryhmät $\mathbb{Z}$, $\mathbb{Z}/q\mathbb{Z}$, $\mathbb{Z}^n$ ovat kommutatiivisia. Erityinen lineaarinen ryhmä $\mathrm{SL}_n(\mathbb{R})$ ei ole kommutatiivinen, tämä osoitettiin harjoitustehtävässä 1.7 tapaukselle $n = 2$.

(b) Ryhmät $\mathbb{Z}/q\mathbb{Z}$ ja $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$, ovat äärellisiä ryhmiä kaikille $q, r \in \mathbb{N} - \{0, 1\}$.

(c) Olkoot $f, g, h \colon \mathbb{R} - \{0\} \to \mathbb{R} - \{0\}$ kuvaukset, joille $f(x) = -x$, $g(x) = 1/x$ ja $h(x) = -1/x$ kaikilla $x \in \mathbb{R} - \{0\}$. On helppo nähdä, että

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

on permutaatioryhmän $\mathrm{Perm}(\mathbb{R} - \{0\})$ vakaa osajoukko, joten kuvausten yhdistäminen indusoi laskutoimituksen joukkoon K. Joukon K alkioille f, g ja h pätee

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

joten kaikilla on käänteisalkio ja K on siis ryhmä, *Kleinin neliryhmä*. 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.

Esimerkki 4.11. Neljän alkion ryhmien $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ja K laskutaulut ovat

$+$	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

Näissä laskutauluissa käytetään kongruenssiluokkien $k + 2\mathbb{Z}$ ja $k + 4\mathbb{Z}$ merkintänä edustajaa $k \in \mathbb{Z}$.

Laskutauluja vertaamalla huomaamme, että ryhmät $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ja K ovat isomorfisia: Kuvaus $\phi \colon \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to K$,

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

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

$$\phi\big((1,0) + (0,1)\big) = \phi(1,1) = h = g \circ f = \phi(0,1) \circ \phi(1,0)$$

Ryhmä K on siis *isomorfismia vaille sama ryhmä* kuin $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ ja ryhmäteorian kannalta voidaan ajatella, että pohjimmiltaan on kyse samasta abstraktista ryhmästä.

Sen sijaan $\mathbb{Z}/4\mathbb{Z}$ ei ole isomorfinen ryhmien K ja $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ kanssa. Koska K ja $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ovat isomorfisia, riittää tarkastaa väite toiselle näistä ryhmistä. Kaikille $k \in K$ pätee $k \circ k = \mathrm{id}$. Jos $\phi \colon K \to \mathbb{Z}/4\mathbb{Z}$ olisi isomorfismi ja $\phi(k) = 1 + 4\mathbb{Z}$ jollain $k \in K$, niin

$$0 = \phi(\mathrm{id}) = \phi(k \circ k) = \phi(k) + \phi(k) = 2(1 + 4\mathbb{Z}) = 2 + 4\mathbb{Z},$$

mikä on mahdotonta.

Äärellisen ryhmän laskutaulussa (tai kertotaulussa, kuten sitä usein kutsutaan) jokaisella rivillä ja jokaisessa sarakkeessa esiintyvät kaikki ryhmän alkiot (Harjoitustehtävä 4.12).

Jos G ja G' ovat ryhmiä, niin homomorfismia $\phi \colon G \to G'$ kutsutaan joskus *ryhmähomomorfismiksi*. Huomaa, että isomorfismin, eli bijektiivisen homomorfismin, käänteiskuvaus on myös isomorfismi. Jos G ja G' ovat isomorfisia ryhmiä, voidaan käyttää merkintää $G \cong G'$.

Propositio 4.12. *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 4.7.

Todistetaan käänteisalkiota koskeva väite: 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 4.3 kohdasta (3). □

Proposition 1.17(3) mukaan surjektiivinen homomorfismi kuvaa neutraalialkion neutraalialkioksi. Proposition 4.12 mukaan ryhmähomomorfismin tapauksessa siis ei tarvita surjektiivisuutta.

Esimerkki 4.13. (a) Esimerkissä 1.16(a) osoitettiin, että $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}_+, \cdot)$ on ryhmäisomorfismi.

(b) Proposition 2.5 nojalla kompleksikonjugointi on ryhmäisomorfismi $\bar{\cdot}\colon (\mathbb{C}, +) \to (\mathbb{C}, +)$ ja $\bar{\cdot}\colon \mathbb{C}^\times \to \mathbb{C}^\times$. Kompleksilukujen moduli on surjektiivinen ryhmähomomorfismi $|\cdot|\colon \mathbb{C}^\times \to \mathbb{R}_+$.

(c) Vektoriavaruuden $\mathbb{R}^n$ lineaaristen bijektioiden ryhmä $\mathrm{GL}(\mathbb{R}^n)$ 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 sarakevektorina kannassa K. Lineaarialgebrassa on osoitettu, että kuvaus $\mathrm{Mat}\colon \mathrm{GL}(\mathbb{R}^n) \to \mathrm{GL}_n(\mathbb{R})$,

$$\mathrm{Mat}(L) = \big((Lv_1)_K, (Lv_2)_K, \ldots, (Lv_n)_K\big),$$

on isomorfismi: kaikille lineaarisille bijektioille $L_1, L_2\colon \mathbb{R}^n \to \mathbb{R}^n$ pätee

$$\mathrm{Mat}(L_2\, L_1) = \mathrm{Mat}(L_2)\,\mathrm{Mat}(L_1)\,.$$

Harjoitustehtäviä.

4.1. Osoita, että joukon X potenssijoukko $\mathscr{P}(X)$ varustettuna laskutoimituksella $\triangle$ (symmetrinen erotus), joka määritellään asettamalla kaikille $A, B \in \mathscr{P}(X)$

$$A \triangle B = (A - B) \cup (B - A),$$

on ryhmä.

4.2. Olkoon $X = \{1, 2, 3\}$. Muodosta ryhmän $(\mathscr{P}(X), \Delta)$ laskutaulu.

4.3. Osoita, että $\mathrm{SL}_n(\mathbb{Z})$ varustettuna matriisien kertolaskulla on ryhmä.

Jos $b_1 \equiv b_2 \mod 4$, niin $(-1)^{b_1} = (-1)^{b_2}$. Siis voimme määritellä kokonaisluvulle -1 ja kongruenssiluokalle $b = b_1 + 4\mathbb{Z}$

$$(-1)^b = (-1)^{b_1}\,.$$

Näin saadaan määriteltyä minkä tahansa ryhmän G alkion g monikerta $(-1)^b g$, kun $b \in \mathbb{Z}/4\mathbb{Z}$.

4.4. Määritellään joukossa $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ laskutoimitus $*$ asettamalla

$$(a, b) * (c, d) = (a + (-1)^b c, b + d)$$

kaikilla $(a, b), (c, d) \in (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$. Tässä $+$ on tavallinen kongruenssiluokkien yhteenlasku. Onko laskutoimituksella varustettu joukko $((\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}), *)$ ryhmä? Onko se kommutatiivinen?

4.5. Olkoon G ryhmä. Osoita, että kaikilla $a, b, c \in G$ pätee supistussääntö:

(1) Jos $ab = ac$, niin $b = c$.
(2) Jos $ab = cb$, niin $a = c$.

4.6. Olkoon A assosiatiivisella laskutoimituksella varustettu joukko, jossa on neutraalialkio. Osoita, että A on ryhmä, jos ja vain jos yhtälöillä $ax = b$ ja $ya = b$ on ratkaisu joukossa A kaikilla $a, b \in A$.

4.7. Olkoot G ja G' ryhmiä. Olkoon $h : G \to G'$ homomorfismi. Osoita, että h kuvaa ryhmän G neutraalialkion ryhmän G' neutraalialkioksi.

4.8. Anna esimerkki homomorfismista $\phi\colon (G, *) \to (E, \circledast)$ siten, että $(G, *)$ on ryhmä ja ryhmän G neutraalialkio ei kuvaudu neutraalialkioksi.

4.9. Olkoon $T\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z})$, $T(B) = {}^tB$, kuvaus, joka liittää matriisiin B sen transpoosin. Olkoon $\mathrm{inv}\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z})$ kuvaus $\mathrm{inv}(B) = B^{-1}$. Mitkä kuvauksista T, inv, $T \circ \mathrm{inv}$ ja $\mathrm{inv} \circ T$ ovat ryhmän $\mathrm{SL}_2(\mathbb{Z})$ automorfismeja?

4.10. Olkoon G ryhmä ja olkoon $\mathrm{Aut}\, G$ sen automorfismien joukko. Osoita, että $\mathrm{Aut}\, G$ on ryhmä, kun laskutoimituksena on homomorfismien yhdistäminen.

4.11. 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 $\mathrm{Perm}(\mathbb{R})$ osajoukkoja. Indusoiko kuvausten yhdistäminen laskutoimituksen näihin joukkoihin? Muodostavatko kasvavat bijektiot ryhmän? Entä vähenevät bijektiot? Entä monotoniset bijektiot?

4.12. Osoita, että kaikki äärellisen ryhmän alkiot esiintyvät sen laskutaulun jokaisella rivillä ja sarakkeella täsmälleen kerran.

4.13. Varustetaan joukko $A = \{a, b, c, d, e\}$ laskutoimituksella $*$, jonka laskutaulu on

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	c	e	d	b
b	b	d	c	a	e
c	c	e	d	b	a
d	d	b	a	e	c

Huomaa, että joukon A alkiot esiintyvät laskutaulun jokaisella rivillä ja sarakkeella täsmälleen kerran. Pätevätkö supistussäännöt laskutoimituksella varustetussa joukossa $(A, *)$? Onko $(A, *)$ ryhmä?

4.14. Monellako eri tavalla voit täydentää taulukon

$*$	e	a	b
e	e	a	b
a	a		
b	b		

niin, että tuloksena on ryhmän laskutaulu? Mitä voit päätellä tästä havainnosta?

[7] Vihje: Supistussääntö.

4.15. Olkoot X ja Y epätyhjiä joukkoja ja olkoon $f\colon X \to Y$ bijektio. Osoita, että permutaatioryhmät $\mathrm{Perm}(X)$ ja $\mathrm{Perm}(Y)$ ovat isomorfisia.

4.16. 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.

4.17. Osoita, että tehtävässä 4.16 määritelty ryhmä H_3 ei ole isomorfinen ryhmän $(\mathbb{R}^3, +)$ kanssa.

4.18. Määritellään reaalilukujen joukossa $\mathbb{R}$ laskutoimitus $*$ asettamalla

$$x * y = \sqrt[3]{x^3 + y^3}\,.$$

Osoita, että $(\mathbb{R}, *)$ on ryhmä, joka on isomorfinen ryhmän $(\mathbb{R}, +)$ kanssa.

4.19. Olkoon G ryhmä. Olkoon R ryhmän G relaatio, joka määritellään säännöllä

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

Onko R ekvivalenssirelaatio?

[17] Vihje: Propositio 1.17(1)

5. Aliryhmät

Luvun 4 esimerkeissä esiintyy usein ryhmä $(G, *)$ ja jokin vakaa osajoukko $B \subset G$ siten, että $(B, *|_B)$ on ryhmä. Määrittelemme seuraavassa käsitteitä, jotka auttavat tällaisten tilanteiden käsittelyssä. Osajoukko $A \subset B$ on joukon B aito osajoukko, jos $A \neq B$.

Määritelmä 5.1. Olkoon G ryhmä. Olkoon $B \subset G$, $B \neq \emptyset$, vakaa osajoukko. Jos indusoidulla laskutoimituksella varustettu joukko B on ryhmä, niin se on ryhmän G *aliryhmä*. Jos $H \subset G$ on ryhmän G aliryhmä, käytämme merkintää $H \leq G$. Jos aliryhmä H on ryhmän G aito osajoukko, se on *aito aliryhmä* ja voimme käyttää merkintää $H < G$.

Merkinnät $H \leq G$ ja $H' < G$ sisältävät tietojen $H, H' \subset G$ ja $H' \neq G$ lisäksi siis sen, että H ja H' ovat ryhmiä, joiden laskutoimitus on ryhmän G laskutoimituksen indusoima.

Lemma 5.2. *Olkoon G ryhmä. Jokaisen aliryhmän $H \leq G$ neutraalialkio on ryhmän G neutraalialkio.*

Todistus. Jos joillekin $a, b \in H \leq G$ pätee $ab = b$, niin ryhmän G supistussäännön nojalla a on ryhmän G neutraalialkio. □

Kaikki ryhmän vakaat osajoukot eivät ole ryhmiä, esimerkiksi ryhmän $\mathbb{Z}$ vakaa osajoukko $\mathbb{N}$ ei ole ryhmä. Seuraava tulos antaa keinon tarkastaa, onko jokin ryhmän osajoukko aliryhmä:

Propositio 5.3. *Ryhmän G osajoukko $H \neq \emptyset$ on aliryhmä, jos*

(1) *kaikilla $x, y \in H$ pätee $xy^{-1} \in H$, tai*
(2) *kaikilla $x, y \in H$ pätee $xy \in H$ 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 H on vakaa osajoukko. Edellisen nojalla kaikille $x, y \in H$ pätee $xy = x(y^{-1})^{-1} \in H$, joten H on vakaa.
Ehdosta (2) seuraa ehto (1), joten väite seuraa kohdasta (1). □

Esimerkki 5.4. (a) Jokaisella ryhmällä on aliryhmiä: ryhmä itse ja neutraalialkion muodostama yhden alkion ryhmä.
(b) $(\{0\}, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.
(c) $\{1\} < \{-1, 1\} < \mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$.
(d) Neliömatriiseista koostuville ryhmille pätee muun muassa

$$\{I_n\} < \{-I_n, I_n\} < \mathrm{GL}_n(\mathbb{Q}) < \mathrm{GL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{C})$$

kaikilla $n \geq 2$ ja

$$\{I_n\} < \{-I_n, I_n\} < \mathrm{SL}_n(\mathbb{Z}) < \mathrm{SL}_n(\mathbb{Q}) < \mathrm{SL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{C}),$$

kun n on parillinen.

Aliryhmillä on monia ominaisuuksia, jotka muistuttavat kursseilta Lineaarinen algebra 1 ja 2 tuttuja vektoriavaruuksien aliavaruuksien ominaisuuksia. Tämä ei ole yllättävää:

Esimerkki 5.5. Reaalinen vektoriavaruus (eli $\mathbb{R}$-vektoriavaruus) muodostuu kommutatiivisesta ryhmästä $(V, +)$, jossa on määritelty alkioiden kertominen reaaliluvulla. Reaaliluvulla kertominen tarkoittaa kuvausta $\mathbb{R} \times V \to V$, $(\lambda, v) \mapsto \lambda v$. Laskutoimitukselta ja reaaliluvulla kertomiselta oletetaan

(1) $\lambda(v+w) = \lambda v + \lambda w$ kaikille $\lambda \in \mathbb{R}$ ja $v, w \in V$,
(2) $(\lambda+\mu)v = \lambda v + \mu v$ kaikille $\lambda, \mu \in \mathbb{R}$ ja $v \in V$,
(3) $\mu(\lambda v) = (\mu\lambda)v$ kaikille $\lambda, \mu \in \mathbb{R}$ ja $v \in V$ ja
(4) $1\,v = v$ kaikille $v \in V$.

Määritelmän mukaan reaalisen vektoriavaruuden V aliavaruus on osajoukko $H \subset V$, joka on vakaa vektoriavaruuden V yhteenlaskun ja reaaliluvulla kertomisen suhteen ja on näillä operaatioilla varustettuna reaalinen vektoriavaruus. Erityisesti $(H, +)$ on additiivisen ryhmän $(V, +)$ aliryhmä.

Kaikki additiivisen ryhmän $(V, +)$ aliryhmät eivät ole $\mathbb{R}$-vektoriavaruuden V vektorialiavaruuksia. Esimerkiksi $\mathbb{R}$-vektoriavaruudella $\mathbb{R}$ on vain kaksi aliavaruutta $\{0\}$ ja $\mathbb{R}$ mutta reaalilukujen additiivisella ryhmällä on paljon enemmän aliryhmiä: Esimerkiksi joukot

$$\alpha\mathbb{Z} = \{\alpha\, k : k \in \mathbb{Z}\} \subset \mathbb{R}$$

ja

$$\alpha\mathbb{Q} = \{\alpha\, q : q \in \mathbb{Q}\} \subset \mathbb{R}$$

ovat ryhmän $(\mathbb{R}, +)$ vakaita osajoukkoja kaikilla $\alpha \in \mathbb{R}$ ja on helppo tarkastaa, että

$$(\alpha\mathbb{Z}, +) < (\alpha\mathbb{Q}, +) < (\mathbb{R}, +)$$

kaikilla $\alpha \in \mathbb{R} - \{0\}$.

Jos W on toinen $\mathbb{R}$-vektoriavaruus, niin kuvaus $L\colon V \to W$ on ($\mathbb{R}$-)lineaarikuvaus, jos se on homomorfismi kommutatiivisesta ryhmästä $(V, +)$ kommutatiiviseen ryhmään $(W, +)$, joka on lisäksi yhteensopiva reaaliluvulla kertomisen kanssa: Kaikille $\lambda \in \mathbb{R}$ ja $v \in V$ pätee $L(\lambda v) = \lambda L(v)$.

Sen todistaminen, että kaikki homomorfismit reaalilukujen additiiviselta ryhmältä itselleen eivät ole lineaarikuvauksia on hieman monimutkaisempaa. G. Hamel todisti tämän tuloksen valinta-aksiooman avulla vuonna 1905.

Propositio 5.6. *Aliryhmien leikkaus on aliryhmä.*

Todistus. Harjoitustehtävä 5.4. □

Määritelmä 5.7. Olkoot G ja G' ryhmiä ja olkoon e' ryhmän G' neutraalialkio. Ryhmähomomorfismin $\phi\colon G \to G'$ *ydin* on $\ker\phi = \phi^{-1}(e')$ ja sen *kuva* on $\operatorname{Im}\phi = \phi(G)$.

Propositio 5.8. *Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Olkoot $H \leq G$, $H' \leq G'$ aliryhmiä. Tällöin $\phi(H) \subset G'$ ja $\phi^{-1}(H') \subset G$ ovat aliryhmiä. Erityisesti* $\ker\phi \leq G$ *ja* $\operatorname{Im}\phi \leq G'$.

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 $gh^{-1} \in H$. Siis $\phi(H)$ on aliryhmä Proposition 5.3(1) nojalla.

Toinen väite todistetaan harjoitustehtävässä 5.5. □

Esimerkki 5.9. (a) Olkoon $\phi_q\colon (\mathbb{Z}, +) \to (\mathbb{Z}/q\mathbb{Z}, +)$ luonnollinen homomorfismi, $\phi_q(k) = [k] \in \mathbb{Z}/q\mathbb{Z}$. Homomorfismin ϕ_q ydin on $q\mathbb{Z}$.

(b) Lineaarialgebrassa osoitettiin, että kaikille neliömatriiseille $A, B \in \mathrm{M}_n(\mathbb{R})$ pätee

$$\det(AB) = \det A \det B.$$

Kun rajoitetaan determinantti nollajoukkonsa komplementtiin saadaan siis ryhmähomomorfismi $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$. Determinantin ydin on $\mathrm{SL}_n(\mathbb{R})$. Determinantti voidaan määritellä samalla lausekkeella myös kompleksikertoimisille neliömatriiseille, jolloin saadaan ryhmähomomorfismi $\det\colon \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$, jonka ydin on $\mathrm{SL}_n(\mathbb{C})$.

Tarkastelemme ydintä ja kuvaa lähemmin luvussa 7. Seuraava ytimen ominaisuus on hyvä todeta jo tässä vaiheessa:

Propositio 5.10. *Ryhmähomomorfismi on injektio, jos ja vain jos sen ydin on neutraalialkion muodostama ryhmä.*

Todistus. Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Aiemmin osoitettiin (harjoitustehtävä 4.7), että ryhmän G neutraalialkio e kuvautuu ryhmän G' neutraalialkioksi e', joten jos ϕ on injektio, sen ydin on $\{e\}$.

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 $x = y$. □

Proposition 5.10 mukaan ryhmähomomorfismin injektiivisyyden toteamiseksi riittää tarkastella neutraalialkion alkukuvaa.

Määritelmä 5.11. 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. Joukon B alkiot ovat ryhmän $\langle B\rangle$ *virittäjiä*.

Joukon B virittämä aliryhmän aliryhmän määritelmässä voi todellakin puhua pienimmästä joukon B sisältävästä aliryhmästä sillä Proposition 5.6 nojalla

$$\langle B\rangle = \bigcap\{H \leq G : B \subset H\} \leq G\,.$$

Ryhmä $\langle B\rangle$ voidaan esittää konkreettisesti virittäjiensä avulla:

Propositio 5.12. *Olkoon G ryhmä ja olkoon $e \in G$ neutraalialkio. Olkoon $B \subset G$, $B \neq \emptyset$. Joukon B virittämä aliryhmä on*

$$\left\{b_1^{\pm 1}b_2^{\pm 1}\cdot\cdots\cdot b_k^{\pm 1} : b_1, b_2, \ldots, b_k \in B, k \in \mathbb{N} - \{0\}\right\}. \tag{5}$$

Todistus. Lausekkeen (5) antama osajoukko $\widetilde{B}$ on ryhmän G aliryhmä Propositioiden 4.3(4) ja 5.3 nojalla. Erityisesti se on ryhmä, joka sisältää joukon B, joten $\langle B\rangle \leq \widetilde{B}$.

Toisaalta $\langle B\rangle$ on ryhmän G aliryhmä, joten erityisesti se on vakaa osajoukko. Koska $B \subset \langle B\rangle$, niin induktiolla on helppo nähdä, että vakaudesta seuraa, että $\langle B\rangle$ sisältää kaikki muotoa $b_1^{\pm 1}b_2^{\pm 1}\cdot\cdots\cdot b_k^{\pm 1}$ olevat alkiot. Siis $\widetilde{B} \leq \langle B\rangle$. □

Esimerkki 5.13. (a) $(\mathbb{Z}, +) = \langle 1\rangle = \langle -1\rangle$ ja kaikilla $q \in \mathbb{Z} - \{-1, 1\}$ pätee $\langle q\rangle < \mathbb{Z}$. Toisaalta $\mathbb{Z} = \langle 2, 3\rangle = \langle 6, 10, 15\rangle$, koska $1 = 3 - 2 = 6 + 10 - 15$, mutta aliryhmät $\langle 2\rangle, \langle 3\rangle, \langle 6, 10\rangle = \langle 2\rangle$, $\langle 6, 15\rangle = \langle 3\rangle$ ja $\langle 10, 15\rangle = \langle 5\rangle$ ovat ryhmän $(\mathbb{Z}, +)$ aitoja aliryhmiä.

(b) Kokeilemalla kaikki tapaukset on helppo nähdä, että jokainen nollasta poikkeava alkio virittää ryhmän $(\mathbb{Z}/5\mathbb{Z}, +)$:

$$(\mathbb{Z}/5\mathbb{Z}, +) = \langle 1 + 5\mathbb{Z}\rangle = \langle 2 + 5\mathbb{Z}\rangle = \langle 3 + 5\mathbb{Z}\rangle = \langle 4 + 5\mathbb{Z}\rangle\,.$$

Toisaalta $(\mathbb{Z}/4\mathbb{Z}, +) = \langle 1 + 4\mathbb{Z}\rangle = \langle 3 + 4\mathbb{Z}\rangle$ mutta $\langle 2 + 4\mathbb{Z}\rangle < (\mathbb{Z}/4\mathbb{Z}, +)$.

Seuraava tulos osoittaa, että ryhmässä G määritelty ryhmähomomorfismi määräytyy yksikäsitteisesti, jos sen arvot tunnetaan virittäjäjoukossa.

Propositio 5.14. *Olkoon $G = \langle S\rangle$ ryhmä. Olkoot $\phi, \psi\colon G \to H$ ryhmähomomorfismeja, joille pätee $\phi|_S = \psi|_S$. Tällöin $\phi = \psi$.*

Todistus. Harjoitustehtävä 5.12. □

Määritelmä 5.15. Olkoon G multiplikatiivinen ryhmä ja olkoon H additiivinen ryhmä. Aliryhmät

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

ja

$$\langle b\rangle = \{n\, b : n \in \mathbb{Z}\} \leq H$$

ovat alkioiden $a \in G$ ja $b \in H$ *virittämät sykliset aliryhmät*. Ryhmä Z on *syklinen ryhmä*, jos on $a \in Z$ siten, että $Z = \langle a\rangle$.

Kokonaislukujen additiivisella ryhmällä on sykliset aliryhmät

$$n\mathbb{Z} = \langle n\rangle = \{kn : k \in \mathbb{Z}\},$$

$n \in \mathbb{N}$. Itse asiassa ryhmällä $(\mathbb{Z}, +)$ ei ole mitään muita aliryhmiä:

Propositio 5.16. *Kokonaislukujen additiivisen ryhmän $(\mathbb{Z}, +)$ kaikki aliryhmät ovat syklisiä. Erityisesti $\mathbb{Z}$ on syklinen ryhmä.*

Todistus. Huomataan ensin, että $\{0\} = 0\,\mathbb{Z}$ ja $\mathbb{Z} = 1\,\mathbb{Z}$. Olkoon $H < \mathbb{Z}$, $H \neq \{0\}$ jokin aliryhmä. Tällöin $H \cap (\mathbb{N} - \{0\})$ ei ole tyhjä ja tässä joukossa on pienin positiivinen kokonaisluku $q \in H$. Erityisesti $q\mathbb{Z} < H$.

Osoitamme, että $H = q\mathbb{Z}$. Jos on $m \in H - q\mathbb{Z}$, niin kokonaislukujen jakoyhtälön nojalla $m = aq + b$ joillakin $a, b \in \mathbb{Z}$ siten, että $1 \leq b < q$. Nyt $b \in H$, joten q ei olekaan pienin positiivinen kokonaisluku ryhmässä H, mikä on ristiriita. Siis $H = q\mathbb{Z}$. □

Lause 5.17. *(1) Syklinen ryhmä, jossa on vähintään kaksi alkiota, on isomorfinen joko ryhmän $(\mathbb{Z}, +)$ tai jonkin ryhmän $(\mathbb{Z}/q\mathbb{Z}, +)$, $q \geq 2$ kanssa.*

(2) Syklisen ryhmän kuva ryhmähomomorfismissa on syklinen.

(3) Jokainen syklisen ryhmän aliryhmä on syklinen.

Todistus. (1) Olkoon $C = \langle g\rangle$ syklinen ryhmä ja olkoon $\phi\colon (\mathbb{Z}, +) \to C$, $\phi(n) = g^n$. Lemman 1.13 nojalla ϕ on homomorfismi ja ryhmän C määritelmän nojalla se on surjektio. Jos ϕ on injektio, se on isomorfismi.

Jos ϕ ei ole injektio, niin Propositioiden 5.8, 5.10 ja 5.16 nojalla $\ker\phi = q\mathbb{Z}$ jollain $q \geq 2$. Olkoon $\psi\colon (\mathbb{Z}/q\mathbb{Z}, +) \to C$,

$$\psi(k + q\mathbb{Z}) = \phi(k) = g^k\,.$$

Kuvaus ψ on hyvin määritelty: jos $k \equiv k' \mod q$, niin $k - k' \in q\mathbb{Z} = \ker\phi$, joten $g^k = g^{k'}g^{k-k'} = g^{k'}$. Kuvaus ψ on homomorfismi:

$$\begin{aligned}\psi(n + q\mathbb{Z})\psi(m + q\mathbb{Z}) &= g^n g^m = g^{n+m} = \psi((n + m) + q\mathbb{Z})\\ &= \psi((n + q\mathbb{Z}) + (m + q\mathbb{Z})).\end{aligned}$$

Homomorfismi ψ on surjektio, koska ϕ on surjektio. Proposition 5.10 nojalla injektiivisyyden todistamiseen riittää osoittaa, että $\ker\psi = \{0\}$. Oletetaan siis, että $\psi(k + q\mathbb{Z}) = e \in G$. Tällöin $\phi(k) = e$, joten $k \in q\mathbb{Z}$ ja $k + q\mathbb{Z} = q\mathbb{Z} = 0$.

(2) Harjoitustehtävä 5.11.

(3) Väite todistettiin sykliselle ryhmälle $(\mathbb{Z}, +)$ Propositiossa 5.16. Olkoon $C = \langle g\rangle$ syklinen ryhmä ja olkoon $H < C$. Olkoon $\phi\colon (\mathbb{Z}, +) \to C$ (surjektiivinen) homomorfismi $\phi(n) = g^n$. Tällöin Proposition 5.8 nojalla $\phi^{-1}(H) \leq (\mathbb{Z}, +)$, joten Proposition 5.16 nojalla $\phi^{-1}(H) = N\mathbb{Z}$ jollain $N \in \mathbb{Z}$. Erityisesti $\phi^{-1}(H)$ on syklinen ryhmä. Koska $H = \phi(\phi^{-1}(H))$, väite seuraa kohdasta (2). □

Koska Lauseen 5.17 mukaan kaikki keskenään yhtä mahtavat sykliset ryhmät ovat isomorfisia keskenään, voimme puhua abstraktista *n alkion syklisestä ryhmästä* C_n ja *äärettömästä syklisestä ryhmästä* C_∞. Toisinaan syklisille ryhmille käytetään merkintöjä Z_n ja Z_∞.

Edellä käsitellyistä esimerkeistä muun muassa ryhmät $\mathbb{Z} = \langle 1 \rangle$ ja $\mathbb{Z}/q\mathbb{Z} = \langle [1] \rangle$, $q \geq 2$, ovat syklisiä. Sen sijaan esimerkiksi $(\mathbb{Q}, +)$ ja $(\mathbb{R}, +)$ eivät ole syklisiä. Reaaliluvuille tämä on selvää, koska syklinen ryhmä on Lauseen 5.17 seurauksena aina numeroituva. Rationaalilukujen tapaus käsitellään harjoitustehtävässä 5.8.

Esimerkki 5.18. (a) 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 ryhmän $(\mathbb{Z}^2, +)$ aitoihin aliryhmiin $\mathbb{Z} \times \{0\}$ ja $\{0\} \times \mathbb{Z}$, joten myöskään tätä muotoa olevat alkiot eivät voi yksinään virittää ryhmää $(\mathbb{Z}^2, +)$.

(b) Esimerkissä 4.10 käsitelty *Kleinin neliryhmä* $K = \langle f, g \rangle$ ja sen kanssa isomorfinen ryhmä

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle (0,1), (1,0) \rangle$$

eivät ole syklisiä, koska jokaisen neutraalialkiosta poikkeavan alkion virittämä syklinen ryhmä on isomorfinen ryhmän $\mathbb{Z}/2\mathbb{Z}$ kanssa. Erityisesti siis neljän alkion kommutatiiviset ryhmät $\mathbb{Z}/4\mathbb{Z}$ ja $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ eivät ole isomorfisia. Edellä esitellyn syklisten ryhmien merkinnän avulla edellinen on hieman lyhyempi ilmaista: ryhmät C_4 ja $C_2 \times C_2$ eivät ole isomorfisia.

Määritelmä 5.19. Ryhmän G alkion g *kertaluku* $\operatorname{ord} g$ on sen virittämän syklisen aliryhmän kertaluku, $\operatorname{ord} g = \#\langle g \rangle$.

Lemma 5.20. *Olkoon G ryhmä ja olkoon e ryhmän G neutraalialkio. Jos jollain $k \in \mathbb{N} - \{0\}$ pätee $g^k = e$, niin*

$$\operatorname{ord} g = \min\{k \geq 1 : g^k = e\}.$$

Lisäksi

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{\operatorname{ord} g - 1}\}.$$

Todistus. Harjoitustehtävä 5.13. □

Esimerkki 5.21. (a) Ryhmien K ja $C_2 \times C_2$ kertaluku on 4 ja niiden jokaisen neutraalialkiosta poikkeavan alkion kertaluku on 2.

(b) Ryhmän $(\mathbb{Z}/4\mathbb{Z}, +)$ kertaluku on 4 ja sen alkioiden $1 + 4\mathbb{Z}$ ja $3 + 4\mathbb{Z}$ kertaluku on 4. Tämä on helppo tarkastaa vaikka alkiolle $3 + 4\mathbb{Z}$:

$$2(3 + 4\mathbb{Z}) = (3 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4\mathbb{Z},$$

$$3(3 + 4\mathbb{Z}) = (2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$$

ja

$$4(3 + 4\mathbb{Z}) = (1 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = (4 + 4\mathbb{Z}) = 0.$$

Harjoitustehtäviä.

5.1. Osoita, että

$$\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$$

on ryhmän $\mathbb{C}^\times$ aliryhmä.

5.2. Anna esimerkki surjektiivisesta homomorfismista $f \colon (\mathbb{R}, +) \to (\mathbb{S}^1, \cdot)$.

5.3. Olkoon ${}^tA$ neliömatriisin A transpoosi. Olkoon

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

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

5.4. Olkoon G ryhmä, olkoon $I \neq \emptyset$ jokin indeksijoukko ja olkoot $H_i \leq G$, $i \in I$. Osoita, että

$$\bigcap_{i \in I} H_i \leq G.$$

5.5. Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi ja olkoon $H' \leq G'$. Osoita, että $\phi^{-1}(H') \leq G$.

5.6. Määritä kaikki ryhmien $(\mathbb{Z}/6\mathbb{Z}, +)$ ja $(\mathbb{Z}/7\mathbb{Z}, +)$ aliryhmät.

5.7. Osoita, että ryhmät $\mathbb{Z}/6\mathbb{Z}$ ja $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ovat isomorfisia.

5.8. Osoita, että rationaalilukujen additiivinen ryhmä ei ole syklinen.

5.9. Olkoon $S \subset \mathbb{Q}$ äärellinen joukko. Osoita, että joukon S virittämä aliryhmä on syklinen ja että se on ryhmän $(\mathbb{Q}, +)$ aito aliryhmä.

5.10. Olkoon C syklinen ryhmä. Osoita, että ryhmällä $(\mathbb{S}^1, \cdot)$ on ryhmän C kanssa isomorfinen aliryhmä.

5.11. Olkoon C syklinen ryhmä ja olkoon $\phi\colon C \to G$ ryhmähomomorfismi. Osoita, että $\phi(C) \leq G$ on syklinen aliryhmä.

5.12. Olkoon $G = \langle S \rangle$ ryhmä. Olkoot $\phi, \psi\colon G \to H$ ryhmähomomorfismeja, joille pätee $\phi|_S = \psi|_S$. Osoita, että $\phi = \psi$.

5.13. Olkoon G ryhmä ja olkoon e ryhmän G neutraalialkio. Olkoon $g \in G$ alkio, jolle pätee $g^k = e$ jollain $k \in \mathbb{Z} - \{0\}$. Osoita, että

$$\operatorname{ord} g = \min\{k \geq 1 : g^k = e\}.$$

5.14. Määritä luvun $\omega = \frac{1+i\sqrt{3}}{2} \in \mathbb{C}$ kertaluku. Mitkä kompleksiluvut muodostavat aliryhmän $\langle \omega \rangle$?

5.15. Määritä matriisien $A, B, C \in \mathrm{SL}_2(\mathbb{Z})$ kertaluvut, kun

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

Kommutatiivisen ryhmän G *torsioaliryhmä* on

$$\operatorname{Tor} G = \{f \in G : \operatorname{ord} g < \infty\}.$$

5.16. Osoita, että $\operatorname{Tor} G$ on kommutatiivisen ryhmän G aliryhmä.

5.17. Määritä $\operatorname{Tor}(\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z}))$.

5.18. Anna esimerkki ryhmästä H, joka osoittaa, että joukko

$$\{f \in H : \operatorname{ord} g < \infty\}$$

ei välttämättä ole ryhmän H aliryhmä.

---

[7] Vihje: Osoita, että $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ on syklinen ryhmä.

[18] Vihje: Tehtävä 5.15

6. Symmetriset ryhmät

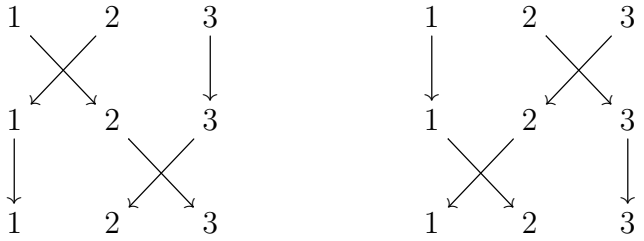
Äärellisen n alkiosta koostuvan joukon $\{1, 2, \ldots, n\}$ permutaatioryhmää kutsutaan *symmetriseksi ryhmäksi* S_n. Harjoitustehtävän 4.15 nojalla minkä tahansa n alkion joukon permutaatioryhmä on isomorfinen ryhmän S_n kanssa. Kaikkia näitä permutaatioryhmiä voidaankin siksi kutsua ryhmäksi S_n vastaavalla tavalla kuin voidaan puhua abstrakteista syklisistä ryhmistä C_n ja C_∞. Symmetriset ryhmät ovat yllättävän tärkeitä ryhmiä matematiikan eri aloilla, esimerkiksi Galois'n teoriassa, joka käsittelee muun muassa polynomien algebrallista ratkeavuutta, samoin ne tulevat vastaan geometriassa tarkasteltaessa esimerkiksi säännöllisten monikulmioiden ja monitahokkaiden symmetriaryhmiä. Tästä saamme hieman esimakua Esimerkissä 6.6.

Propositio 6.1. *(1) Symmetrisen ryhmän S_n kertaluku on $n!$.*
(2) Jos $n \geq 3$, niin S_n ei ole kommutatiivinen.

Todistus. (1) Harjoitustehtävä.
(2) Tarkastellaan ensin tapaus $n = 3$. Olkoon $\sigma \in S_3$, $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 3$ ja olkoon $\tau \in S_3$, $\tau(1) = 1$, $\tau(2) = 3$, $\tau(3) = 2$. Tällöin $\tau \circ \sigma(1) = \tau(2) = 3$ ja $\sigma \circ \tau(1) = \sigma(1) = 2$, joten $\sigma \circ \tau \neq \tau \circ \sigma$.

Edellä määritellyt permutaatiot on helppo laajentaa n alkion permutaatioiksi määrittelemällä kaikille $n \geq 4$ permutaatiot $\bar{\sigma}, \bar{\tau} \in S_n$, joille $\bar{\sigma}|_{\{1,2,3\}} = \sigma$, $\bar{\tau}|_{\{1,2,3\}} = \tau$, ja $\bar{\sigma}(k) = k = \bar{\tau}(k)$ kaikille $4 \leq k \leq n$. Näille permutaatioille pätee $\bar{\sigma} \circ \bar{\tau} \neq \bar{\tau} \circ \bar{\sigma}$ kuten tapauksessa $n = 3$. □

Permutaatioilla operointia voi havainnollistaa monilla eri tavoilla. Proposition 6.1 todistuksessa käyttämämme tapa antaa permutaatio luettelemalla kaikkien alkioiden kuvautuminen ei ole kovin kätevää. Esimerkiksi seuraavat kaaviot havainnollistavat Proposition 6.1 todistuksessa esiintyvien permutaatioiden σ ja τ yhdistettyjä kuvauksia $\tau \circ \sigma$ ja $\sigma \circ \tau$:



Yksinkertaistamista varten otamme joillekin permutaatioille käyttöön tiiviimmän merkinnän:

Määritelmä 6.2. Olkoon $\{a_1, a_2, \ldots, a_m\} \subset \{1, 2, \ldots, n\}$ m alkion osajoukko, $m \geq 2$. *Sykli* $(a_1 a_2 \cdots a_m)$ on permutaatio, joka kuvaa alkion a_i alkioksi a_{i+1} kaikilla $i \in \{1, 2, \ldots, m-1\}$, alkion a_m alkioksi a_1 ja on identtinen kuvaus osajoukon $\{a_1, a_2, \ldots, a_m\}$ komplementissa. Syklin $(a_1 a_2 \cdots a_m)$ *pituus* on m. Jos syklin pituus on m, se on *m-sykli*. Jos syklin pituus on 2, niin sitä kutsutaan *vaihdoksi* eli *transpositioksi*. Sanomme 2-sykliä $(i\ i+1)$ *alkeisvaihdoksi* eli *alkeistranspositioksi*.

Syklien yhdistettyä kuvausta merkitään ilman $\circ$-merkkiä: Jos $\sigma = (a_1 a_2 \cdots a_m)$ ja $\tau = (b_1 b_2 \cdots b_k)$, niin

$$\sigma \circ \tau = (a_1 a_2 \cdots a_m)(b_1 b_2 \cdots b_k).$$

Syklien yhdistettyä kuvausta sanotaan niiden *tuloksi*.

Syklit $(a_1 a_2 \cdots a_m)$ ja $(b_1 b_2 \cdots b_k)$ ovat *erilliset*, jos

$$\{a_1, a_2, \ldots, a_m\} \cap \{b_1, b_2, \ldots, b_k\} = \emptyset.$$

Propositiossa 6.1 osoitimme, että ryhmä S_n ei ole kommutatiivinen, kun $n \geq 3$. Vaikka ryhmä G ei olisikaan kommutatiivinen, niin joillekin alkioille $g, h \in G$ pätee $gh = hg$. Tällöin sanotaan, että g ja h *kommutoivat*.

Lemma 6.3. *Erilliset syklit kommutoivat.*

Todistus. Jos σ ja σ' ovat erillisiä, ne ovat kahden toisiaan leikkaamattoman osajoukon permutaatioita, joten väite pätee selvästi. □

Jos $f\colon X \to X$ on kuvaus ja $x \in X$, niin pisteen x *rata* (kuvauksella f) on

$$\mathscr{O}(x) = \bigcup_{n\in\mathbb{N}} \{f^n(x)\}.$$

Lemma 6.4. *Jokaisen m-syklin kertaluku on m.*

Todistus. Olkoon $\sigma = (a_1 a_2 \cdots a_m)$. Pisteen a_1 rata

$$\begin{aligned}\mathscr{O}(a_1) &= \{a_1, \sigma(a_1) = a_2, \sigma^2(a_1) = a_3, \ldots, \sigma^{m-1}(a_1) = a_m, \sigma(a_m) = a_1, \ldots\} \\ &= \{a_1, \sigma(a_1) = a_2, \sigma^2(a_1) = a_3, \ldots, \sigma^{m-1}(a_1) = a_m\}\end{aligned}$$

koostuu m pisteestä ja sama pätee kaikille muillekin pisteille $a_2, \ldots, a_m$. Siis kuvaukset σ^k, $k \in \{2, 3, \ldots, m-1\}$, eivät ole identtisiä kuvauksia ja $\sigma^m = \mathrm{id}$. Väite seuraa tästä. □

Esimerkki 6.5. (1) Kaikki Proposition 6.1 todistuksessa esintyvät kuvaukset ovat syklejä: $\sigma = (12)$, $\tau = (23)$, $\tau \circ \sigma = (23)(12) = (132)$ ja $\sigma \circ \tau = (12)(23) = (123)$. Loput permutaatioryhmän S_3 alkiot ovat vaihto (13) ja identtinen kuvaus.

(2) Kaikki syklin identtisestä kuvauksesta poikkeavat potenssit eivät välttämättä ole syklejä. Esimerkiksi $(1234)^2 = (1234)(1234) = (13)(24)$.

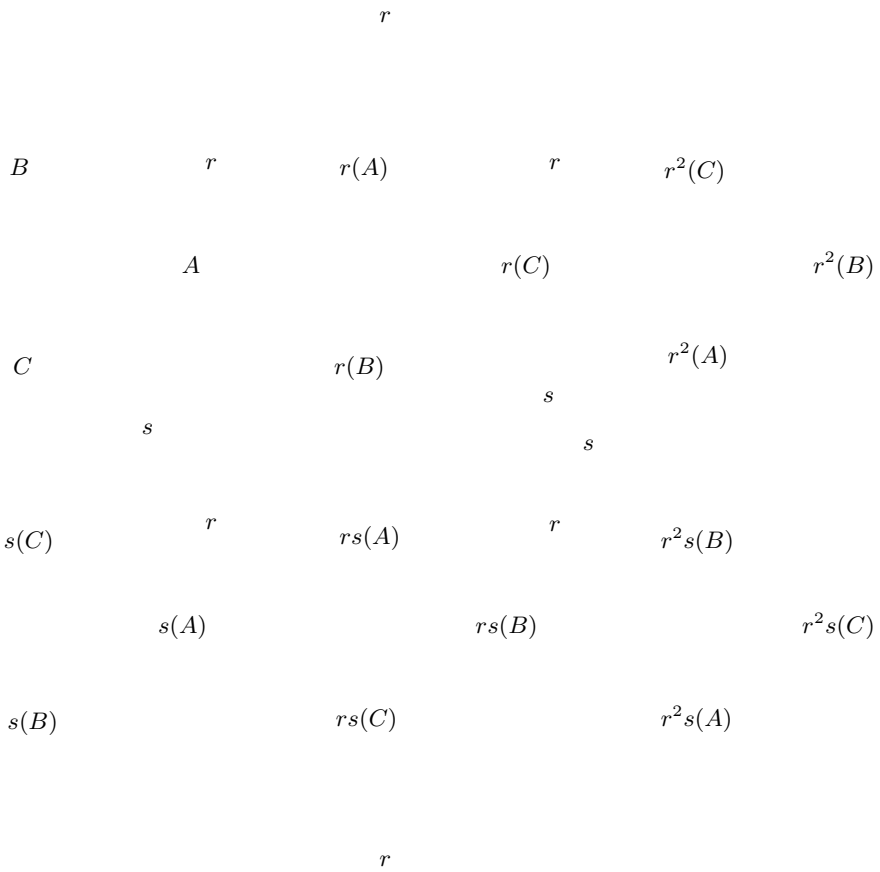
Esimerkki 6.6. Olkoon P_n on säännöllinen n-kulmio euklidisessa tasossa, jonka koordinaatit on valittu siten, että monikulmion P_n keskipiste on 0. Monikulmion P_n *symmetriaryhmä* koostuu ortogonaalikuvauksista $k \in \mathrm{O}(2)$, joille pätee $k(P_n) = P_n$. Tämä ryhmä on *diedriryhmä* D_n ja sen virittävät kierto kulman $2\pi/n$ verran keskipisteen ympäri ja heijastus valitun symmetria-akselin suhteen.

Kuvauksen $k \in D_n$ rajoittuma monikulmion P_n kärkien joukkoon V_n määrää symmetrisen ryhmän S_n alkion. Rajoittumakuvaus $k \mapsto k|_{V_n}$ on homomorfismi ryhmästä D_n ryhmään S_n. Se on itse asiassa injektiivinen, koska identtinen kuvaus on ainoa tason lineaarikuvaus, joka kiinnittää kaksi lineaarisesti riippumatonta vektoria. Siis

D_n on isomorfinen ryhmän S_n jonkin aliryhmän kanssa. Rajoittumakuvaus ei ole isomorfismi, kun $n \geq 4$, koska diedriryhmässä D_n on $2n$ alkiota ja symmetrisessä ryhmässä S_n on $n!$ alkiota.

Tarkastelemme kahta erikoistapausta, tasasivuista kolmiota ja neliötä. Olkoon P_3 tasasivuinen kolmio, jonka kärjet ovat A, B ja C. Kolmiolla P_3 on kuusi symmetriaa: identtinen kuvaus id, kierto r vastapäivään kulman $2\pi/3$ verran, r^2, joka on kierto kulman $4\pi/3$ verran samaan suuntaan ja peilaukset kunkin kärjen kautta kulkevien kulmanpuolittajasuorien suhteen.

Jos kolmio P_3 ajatellaan kolmiulotteisessa avaruudessa $\mathbb{R}^3$ kaksipuolisena levynä, joka sisältyy tasoon $\mathbb{R}^2 \times \{0\}$, niin kuvaukset id, r ja r^2 kuvaavat kolmion yläpuolen yläpuoleksi ja muut kuvaavat yläpuolen alapuoleksi. Jos s on peilaus kärjen A kautta kulkevan ja vastakkaista sivua vastaan kohtisuoran suoran suhteen, on melko helppo nähdä, että muut peilaukset ovat rs ja sr.



Ryhmä D_3 on isomorfinen permutaatioryhmän S_3 kanssa: Kun rajoitetaan symmetriakuvaukset kolmion P_3 kärkiin, r on 3-sykli (ABC), r^2 on 3-sykli $(ABC)^2 = (ACB)$, s on vaihto (BC), rs on vaihto (AB) ja sr on vaihto (AC).

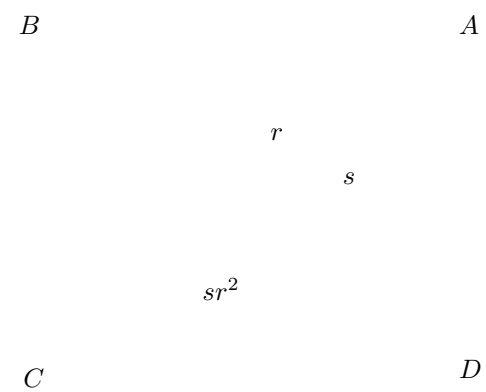
Diedriryhmä D_4 on isomorfinen ryhmän $\langle (1234), (14)(23) \rangle < S_4$ kanssa. Neliön

$$P_4 = \{x \in \mathbb{R}^2 : |x_1| \leq 1, |x_2| \leq 1\}$$

symmetriat ovat lineaarikuvauksia ja ne voidaan esittää reaalisten 2×2-ortogonaalimatriisien avulla:

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

Jokaisella diedriryhmällä on vastaavanlainen esitys ryhmän $\mathrm{O}(2) < \mathrm{GL}_2(\mathbb{R})$ aliryhmänä.



Yleistämme Esimerkissä 6.6 tehdyn havainnon ja osoitamme, että kaikki ryhmät voi halutessa ajatella permutaatioryhmien aliryhminä, äärettömät ryhmät tietenkin äärettömien joukkojen permutaatioryhmien. Tätä varten määritellään ryhmän G bijektio *vasen siirto* $\ell_g \colon G \to G$ alkiolla $g \in G$ asettamalla $\ell_g(x) = gx$ kaikilla $x \in G$.

Lemma 6.7. *Vasen siirto on bijektio.*

Todistus. Olkoon $g \in G$. Kuvaus $\ell_g \colon G \to G$ on surjektio, koska $\ell_g(g^{-1}z) = z$ kaikilla $z \in G$ ja supistussäännön nojalla se on injektio: Jos $\ell_g(x) = \ell_g(y)$, niin $gx = gy$, joten supistussäännön nojalla $x = y$. □

Propositio 6.8. *Ryhmä G on isomorfinen ryhmän* $\mathrm{Perm}(G)$ *jonkin aliryhmän kanssa.*

Todistus. Lemman 6.7 nojalla voidaan määritellä kuvaus $\rho \colon G \to \mathrm{Perm}(G)$, $\rho(g) = \ell_g$. Kuvaus ρ on homomorfismi sillä kaikille $x \in G$ pätee

$$\rho(gh)(x) = \ell_{gh}(x) = (gh)x = g(hx) = \ell_g \circ \ell_h(x) = \rho(g) \circ \rho(h)(x).$$

Supistussäännöstä seuraa myös, että ρ on injektio, joten $\rho \colon G \to \rho(G) < \mathrm{Perm}(G)$ on isomorfismi. □

Lause 6.9 (Cayleyn lause)**.** *Olkoon G äärellinen ryhmä, jonka kertaluku on n. Symmetrisellä ryhmällä S_n on aliryhmä, joka on isomorfinen ryhmän G kanssa.*

Todistus. Ryhmät S_n ja $\mathrm{Perm}(G)$ ovat isomorfisia, joten voimme käsitellä ryhmää $\mathrm{Perm}(G)$ ja väite seuraa Propositiosta 6.8 □

Abstraktin algebran kannalta isomorfiset ryhmät voidaan ajatella saman abstraktin ryhmän erilaisina "konkreettisina esityksinä". Jos ryhmät G ja H ovat isomorfisia, sanotaan, että ne kuuluvat samaan isomorfismiluokkaan. Selvästi isomorfismi määrää ekvivalenssirelaation kaikkien yhtä mahtavien ryhmien joukossa. Cayleyn lauseen avulla saadaan äärellisten ryhmien luokittelun perustulos:

Seuraus 6.10. *Kertalukua n olevien äärellisten ryhmien isomorfismiluokkien joukko on äärellinen jokaisella $n \in \mathbb{N} - \{0\}$.*

Todistus. Harjoitustehtävä 6.11. □

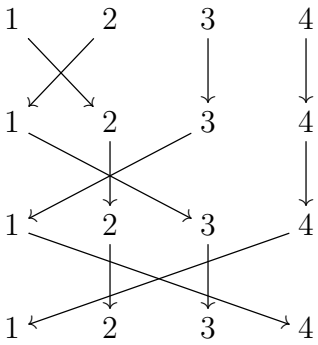
Tarkastelemme seuraavaksi symmetrisen ryhmän S_n rakennetta.

Propositio 6.11. *Jokainen sykli on vaihtojen tulo.*

Todistus. Induktiolla on helppo osoittaa, että

$$(a_1 a_2 \cdots a_m) = (a_1 a_m)(a_1 a_{m-1}) \ldots (a_1 a_2).$$

Todistuksen idea sisältyy seuraavaan kaavioon:



Yksityiskohdat harjoitustehtävässä 6.8. □

Propositio 6.12. *Jokainen vaihto on alkeisvaihtojen pariton tulo.*

Todistus. Koska harjoitustehtävässä 6.5 osoitetaan, että $(km) = (1k)(1m)(1k)$ kaikilla $k, m \in \{1, 2, \ldots, n\}$, $k \neq m$, riittää osoittaa, että $(1k)$ on alkeisvaihtojen pariton tulo kaikilla $k \in \{2, 3, \ldots, n\}$. Vaihto (12) on alkeellinen. Oletetaan, että $(1\ k-1)$ on alkeisvaihtojen pariton tulo. Koska $(1k) = (1\ k-1)(k-1\ k)(1\ k-1)$, väite seuraa. □

Propositio 6.13. *Jokainen identtisestä kuvauksesta poikkeava permutaatio voidaan esittää erillisten syklien tulona.*

Todistus. Jos permutaatio τ kiinnittää pisteet $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$, riittää todistaa väite permutaation τ rajoittumalle joukkoon $\{1, 2, \ldots, n\} - \{a_1, a_2, \ldots, a_k\}$. Riittää siis tarkastella permutaatioita, jotka eivät kiinnitä yhtään pistettä.

Selvästi väite pätee, kun $n = 2$. Oletetaan, että se pätee kaikilla S_k, kun $k \leq n-1$. Olkoon $\tau \in S_n$. Jos τ on sykli ei ole mitään todistettavaa, joten voimme olettaa, että τ ei ole sykli. Pisteen 1 rata on

$$\mathscr{O}(1) = \{1, \tau(1), \tau^2(1), \ldots, \tau^k(1), \ldots\}.$$

Koska $\{1, \ldots, n\}$ on äärellinen joukko, niin täytyy olla $\tau^q(1) = \tau^r(1)$ joillain luonnollisilla luvuilla $q < r$. Valitaan luvut q ja r niin, että ne ovat pienimmät mahdolliset. Koska τ on bijektio, täytyy olla $q = 0$, $\tau^r(1) = 1$. Tästä nähdään, että

$$\tau|_{\mathscr{O}(1)} = (1\, \tau(1)\, \tau^2(1) \cdots \tau^{r-1}(1)).$$

Induktio-oletuksesta seuraa, että permutaation τ rajoittuma pienempään joukkoon $\{1, 2, \ldots, n\} - \mathscr{O}(1)$ on syklien tulo, joten väite on todistettu. □

Propositioista 6.11, 6.12 ja 6.13 saadaan

Lause 6.14. *(Alkeis)vaihdot virittävät symmetrisen ryhmän S_n.* □

Jokaiseen permutaatioon liittyvä tärkeä invariantti on permutaation merkki:

Määritelmä 6.15. Permutaatio $\sigma \in S_n$ on *parillinen*, jos se on tulo parillisesta määrästä vaihtoja ja *pariton*, jos se on tulo parittomasta määrästä vaihtoja. Permutaation σ *merkki* on

$$\epsilon(\sigma) = \begin{cases} -1, & \text{jos } \sigma \text{ on pariton} \\ 1, & \text{jos } \sigma \text{ on parillinen.} \end{cases}$$

Proposition 6.12 nojalla permutaatio on tulo parillisesta määrästä vaihtoja, jos ja vain jos se on tulo parillisesta määrästä alkeisvaihtoja.

Osoitetaan, että permutaation merkki on hyvin määritelty kuvaus. Apuna käytetään antisymmetrisiä kuvauksia: Olkoon X epätyhjä joukko ja olkoon $(V, +)$ additiivinen ryhmä. Kuvaus $f\colon X^n \to V$ on *antisymmetrinen*, jos kaikille alkeisvaihdoille $\tau \in S_n$ pätee

$$f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) = -f(x).$$

Propositio 6.16. *Olkoon $f\colon X^n \to V$ antisymmetrinen kuvaus. Tällöin*

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = (-1)^r f(x),$$

jos σ on r alkeisvaihdon tulo.

Todistus. Väite pätee selvästi, kun $r = 1$. Oletetaan, että se pätee, kun σ on $r-1$ alkeisvaihdon tulo. Olkoon $\sigma = \tau \circ \omega$ permutaatio, joka on r alkeisvaihdon tulo siten, että ω on $r-1$ alkeisvaihdon tulo ja τ on alkeisvaihto. Nyt soveltamalla antisymmetrisyyden määritelmää alkeisvaihdolla τ ja pisteellä $(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$ saadaan

$$\begin{aligned} f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) &= f(x_{\tau(\omega(1)}, x_{\tau(\omega(2))}, \ldots, x_{\tau(\omega(n))}) \\ &= -f(x_{\omega(1)}, x_{\omega(2)}, \ldots, x_{\omega(n)}) = (-1)^r f(x)\,. \end{aligned}$$ □

Proposition 6.12 avulla saadaan välittömästi

Seuraus 6.17. *Jos f on antisymmetrinen, niin kaikille vaihdoille $\tau \in S_n$ pätee*

$$f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) = -f(x)\,.$$ □

Propositio 6.18. *Permutaation merkki on hyvin määritelty.*

Todistus. Kuvaus $f\colon \mathbb{Z}^n \to \mathbb{Z}$,

$$f(x) = \prod_{1 \le i < j \le n} (x_i - x_j)$$

on antisymmetrinen (Harjoitustehtävä 6.12). Lisäksi, kun muuttujan x komponentit ovat eri kokonaislukuja, $f(x) \neq 0$. Jos permutaatio σ voidaan esittää r vaihdon tulona ja toisaalta s vaihdon tulona, saadaan Proposition 6.16 nojalla $(-1)^r = (-1)^s$, joten $r \equiv s \mod 2$. □

Lause 6.19. *Merkki $\epsilon\colon S_n \to \{-1, 1\}$ on ainoa homomorfismi permutaatioryhmästä S_n multiplikatiiviseen ryhmään $\{-1, 1\}$, joka saa vaihdoilla arvon -1.*

Todistus. Harjoitustehtävässä 6.13 osoitetaan, että ϵ on homomorfismi. Määritelmän mukaan $\epsilon(\tau) = -1$ kaikille vaihdoille, joten merkki on halutunlainen homomorfismi. Toisaalta Lauseen 6.14 nojalla alkeisvaihdot virittävät koko permutaatioryhmän, joten Proposition 5.14 nojalla homomorfismin ϵ arvot kiinnittyvät kaikille permutaatioille. Siis ϵ on ainoa homomorfismi, jolla on haluttu ominaisuus. □

Olkoon $n \geq 3$. Permutaatioiden merkkihomomorfismin $\epsilon\colon S_n \to \{-1, 1\}$ ydin on *alternoiva ryhmä* A_n, joka koostuu parillisista permutaatioista. Alternoiva ryhmä on symmetrisen ryhmän aito aliryhmä, koska $(12) \in S_n - A_n$ kaikille $n \geq 2$. Luvun 7 menetelmillä on helppo osoittaa, että alternoivan ryhmän kertaluku on $n!/2$.

Esimerkki 6.20. (a) Permutaatio $(12\cdots n)$ kuuluu alternoivaan ryhmään A_n, jos ja vain jos n on parillinen: $(123) = (13)(12)$, $(1234) = (14)(123)$ ja niin edelleen.
(b) $A_3 = \langle (123) \rangle < S_3$, $A_3 \cong C_3$.

(c) $A_4 = \langle (12)(34), (123) \rangle < S_4$. Tämän voi osoittaa laskemalla esimerkiksi, että

$$\begin{aligned} (12)(34)(123) &= (243)\,, \\ (123)(12)(34) &= (134)\,, \\ (12)(34)(123)(12)(34) &= (142) \end{aligned}$$

ja

$$\begin{aligned} (123)(241) &= (13)(24)\,, \\ (13)(24)(12)(34) &= (14)(23)\,. \end{aligned}$$

Koska ryhmä $\langle (12)(34), (123) \rangle$ sisältää lisäksi identtisen kuvauksen ja edellä lueteltujen 3-syklien neliöt, saadaan kaikki ryhmän A_4 12 alkiota.

Propositio 6.21. *Alternoiva ryhmä A_n on 3-syklien virittämä.*

Todistus. Harjoitustehtävä 6.14. □

Permutaatiot esiintyvät lineaarialgebrassa determinanttien yhteydessä: Neliömatriisin $A = (a_{ij})_{i=1}^n$ determinantti on

$$\det A = \sum_{\sigma \in S_n} \epsilon(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n}\,.$$

Jos neliömatriisien vektoriavaruus M_n samastetaan avaruudeksi $(\mathbb{R}^n)^n$ esittämällä matriisi $A \in M_n$ sarakkeidensa tai riviensä avulla muodossa

$$A = \begin{pmatrix} v_1 \cdots v_n \end{pmatrix} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix},$$

niin determinantti on antisymmetrinen kuvaus $\det\colon (\mathbb{R}^n)^n \to \mathbb{R}$:

$$\det(v_{\sigma(1)}\ v_{\sigma(2)} \cdots v_{\sigma(n)}) = \det \begin{pmatrix} w_{\sigma(1)} \\ w_{\sigma(2)} \\ \vdots \\ w_{\sigma(n)} \end{pmatrix} = \epsilon(\sigma) \det A.$$

Alternoiva ryhmä A_4 on mielenkiintoinen muun muassa euklidisen geometrian kannalta: Olkoot

$$v_1 = (1,1,1), \quad v_2 = (1,-1,-1), \quad v_3 = (-1,1,-1), \quad v_4 = (-1,-1,1)$$

neljä avaruuden $\mathbb{R}^3$ pistettä. Tetraedri

$$T = \{a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4 : a_1, a_2, a_2, a_4 \in [0,1] \text{ ja } \sum_{i=1}^4 a_i = 1\}\,,$$

jonka kärkipisteet ovat v_1, v_2, v_3 ja v_4, on yksi kolmiulotteisen euklidisen avaruuden säännöllisistä monitahokkaista. Sillä on neljä kärkipistettä, sivua ja tahoa. Kaikki tetraedrin sivut ovat yhtä pitkiä keskenään ja kaikki tahot ovat tasasivuisia kolmioita. Tällä tavalla muodostetun tetraedrin painopiste on 0.

Euklidisen avaruuden $\mathbb{R}^n$ *ortogonaaliryhmä* on

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

ja sen tärkeä aliryhmä *erityinen ortogonaaliryhmä* on

$$\mathrm{SO}(n) = \{A \in \mathrm{O}(n) : \det A = 1\}.$$

Kolmiulotteisen avaruuden erityisen ortogonaaliryhmän SO(3) neutraalialkiosta poikkeavat alkiot vastaavat avaruuden $\mathbb{R}^3$ kiertoja jonkin (origon kautta kulkevan) suoran ympäri.

Olkoon T tetraedri, jonka painopiste on origossa. Esimerkin 6.6 tarkastelun yleistys kolmeen ulottuvuuteen osoittaa, että ryhmä A_4 on isomorfinen säännöllisen tetraedrin symmetriaryhmän

$$\{A \in \mathrm{SO}(3) : A(T) = T\}$$

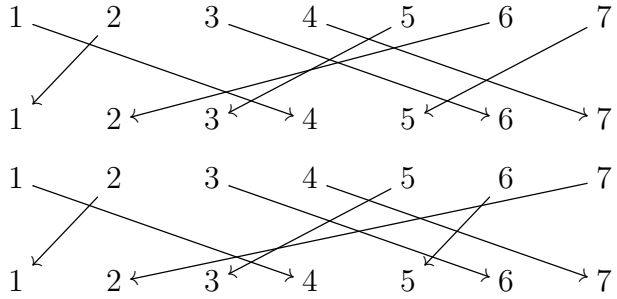
kanssa. Esimerkiksi jokainen 3-sykli vastaa tetraedrin kiertoa kulman $\frac{2\pi}{3}$ verran sellaisen suoran ympäri, joka kulkee tetraedrin kärjen ja sen vastakkaisen tahon keskipisteen kautta. Kurssilla Ryhmät ja geometria [RG] käsitellään tätä esimerkkiä ja sen yleistyksiä laajemmin.

Harjoitustehtäviä.

6.1. Osoita, että permutaatioryhmän S_n kertaluku on $n!$.

6.2. Kirjoita permutaatio (123)(24) syklinä.

6.3. Kirjoita kaavioita



vastaavat permutaatiot erillisten syklien tuloina.

6.4. Kirjoita permutaatio (1234)(235) erillisten syklien tulona.

6.5. Osoita, että $(km) = (1k)(1m)(1k)$.

6.6. Olkoot $\alpha_n = (123\cdots n)$ ja $\beta = (123)$. Määritä permutaatio

$$\beta^{-1}\alpha_n(12x)\alpha_n^{-1}\beta$$

jokaiselle $3 \leq x < n$.

6.7. Määritä permutaatiot

- $(12y)^{-1}(12x)(12y)$ kaikille $x, y \geq 3$, $x \neq y$ ja
- $(1xt)(1yz)(1tx)$ kaikille $x, y, t, z \geq 1$, kun $\#\{x, y, t, z\} = 4$.

6.8. Täydennä Proposition 6.11 todistus induktiotodistukseksi.

6.9. Osoita, että $S_3 = \langle (12), (23) \rangle$

6.10. Osoita, että isomorfismi määrittelee ekvivalenssirelaation kertalukua n olevien ryhmien joukossa.

6.11. Osoita, että kertalukua n olevien ryhmien isomorfismiluokkien joukko on äärellinen.

[11] Vihje: Cayleyn lause

6.12. Osoita, että kuvaus $f\colon \mathbb{Z}^n \to \mathbb{Z}$,

$$f(x) = \prod_{1 \le i < j \le n} (x_i - x_j)$$

on antisymmetrinen.

6.13. Osoita, että permutaation merkki $\epsilon\colon S_n \to \{-1, 1\}$ on homomorfismi.

6.14. Osoita, että kaikki ryhmän S_n parilliset permutaatiot voi esittää 3-syklien tulona, kun $n \geq 3$.

6.15. Osoita, että jokaiselle parittomalle $n \geq 5$ pätee $A_n = \langle (123), (123 \cdots n) \rangle$.

6.16. Määritä aliryhmä $\langle (123), (124) \rangle \leq A_4$.

Olkoon seuraavissa tehtävissä

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

6.17. Osoita, että joukko B varustettuna matriisien kertolaskulla on ryhmän $\mathrm{GL}_2(\mathbb{Q})$ aliryhmä. Onko B ryhmän $\mathrm{SL}_2(\mathbb{Z})$ aliryhmä?

6.18. Onko ryhmä B kommutatiivinen? Onko se syklinen? Luettele kaikki ryhmän B aliryhmät.

6.19. Osoita, että ryhmä B on isomorfinen permutaatioryhmän S_3 kanssa.

---

[14]Vihje: Kirjoita permutaatio vaihtojen tulona, tarkastele eri tapaukset ja tee induktio.

[15]Vihje: Käytä tehtävien 6.6 ja 6.7 tuloksia.

[19]Vihje: Homomorfismi $\phi\colon S_3 \to B$ määräytyy arvoista $\phi((12))$ ja $\phi((23))$. Koska $(12)(12) = (23)(23) = \mathrm{id}$, täytyy olla $\phi((12))^2 = \phi((23))^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Tarkastelemme luvun aluksi ryhmän ja sen aliryhmien suhdetta. Olkoon G ryhmä ja olkoon $H \leq G$. Alkion $g \in G$ *vasen sivuluokka* (aliryhmän H suhteen) on

$$gH = \{gh : h \in H\}$$

ja sen *oikea sivuluokka* (aliryhmän H suhteen) on

$$Hg = \{hg : h \in H\}.$$

Jos kommutatiivisen ryhmän G laskutoimitusta merkitään additiivisesti, niin aliryhmän $H \leq G$ sivuluokkia merkitään $x + H$ tai $H + x$.

Esimerkki 7.1. Aliryhmän $q\mathbb{Z} < (\mathbb{Z}, +)$ vasemmat ja oikeat sivuluokat toteuttavat

$$n + q\mathbb{Z} = \{n + kq : k \in \mathbb{Z}\} = \{kq + n : k \in \mathbb{Z}\} = q\mathbb{Z} + n.$$

Edellä tehty havainto yleistyy kaikille kommutatiivisille ryhmille:

Lemma 7.2. *Olkoon G kommutatiivinen ryhmä. Tällöin jokaiselle $x \in G$ ja jokaiselle $H \leq G$ pätee $xH = Hx$.* □

Yleisessä tapauksessa alkion x vasen ja oikea sivuluokka eroavat toisistaan.

Esimerkki 7.3. Olkoon $H = \langle (12) \rangle < S_3$. Aliryhmän H vasemmat sivuluokat ovat

$$\begin{aligned} H = (12)H &= \{\mathrm{id}, (12)\}, \\ (123)H = (13)H &= \{(123), (13)\} \quad \text{ja} \\ (132)H = (23)H &= \{(132), (23)\} \end{aligned}$$

Sen oikeat sivuluokat ovat

$$\begin{aligned} H = H(12) &= \{\mathrm{id}, (12)\}, \\ H(123) = H(23) &= \{(123), (23)\} \quad \text{ja} \\ H(132) = H(13) &= \{(132), (13)\}. \end{aligned}$$

Osoittautuu siis, että vasen sivuluokka $(123)H$ ei esiinny lainkaan oikeiden sivuluokkien kokoelmassa. Siis vasemmat ja oikeat sivuluokat määräävät kaksi erilaista ryhmän G ositusta.

Usein, jos ryhmä G ei ole kommutatiivinen, sillä on aliryhmiä, joiden vasemmat ja oikeat sivuluokat eroavat toisistaan. Harjoitustehtävissä 7.4–7.6 tarkastellaan esimerkkiä ryhmästä, joka ei ole kommutatiivinen, vaikka sen kaikkien aliryhmien vasemmat ja oikeat sivuluokat ovat samoja joukkoja.

Propositio 7.4. *Olkoon G ryhmä ja olkoon H sen aito aliryhmä. Tällöin*

(1) $xH = yH$, jos ja vain jos $y^{-1}x \in H$. Erityisesti $xH = H$, jos ja vain jos $x \in H$.

(2) $Hx = Hy$, jos ja vain jos $xy^{-1} \in H$. Erityisesti $Hx = H$, jos ja vain jos $x \in H$.

(3) Vasemmat sivuluokat muodostavat ryhmän G osituksen.

(4) Oikeat sivuluokat muodostavat ryhmän G osituksen.

(5) Joukot H, gH ja Hg ovat yhtä mahtavia.

Todistus. (1) ja (2) Harjoitustehtävä 7.1.

(3) Vasempien sivuluokkien yhdiste on koko G sillä $x \in xH$ kaikille $x \in G$. Osoitetaan, että vasemmat sivuluokat leikkaavat vain, jos ne ovat sama sivuluokka. Jos $xH \cap yH \neq \emptyset$, on $h, h' \in H$, joille $xh = yh'$. Mutta tällöin, jos $g \in xH$, niin

$g = xh'' = yh'h^{-1}h'' \in yH$. Vastaava päättely antaa inkluusion toiseen suuntaan. Kohdan (4) todistus on samanlainen.

(5) Lemman 6.7 nojalla vasen siirto $\ell_x \colon G \to G$ on bijektio. Vasemman sivuluokan määritelmän nojalla $\ell_x(H) = xH$. Vastaavasti oikea siirto $r_x \colon G \to G$, joka määritellään asettamalla $r_x(h) = hx$ kaikille $x \in G$, antaa bijektion joukkojen H ja Hx välille. □

Vasempien sivuluokkien kokoelmalle käytetään merkintää G/H ja oikeiden sivuluokkien kokoelmalle käytetään merkintää $H\backslash G$. Jälkimmäistä merkintää ei pidä sekoittaa joukkojen erotukseen.

Aliryhmän $q\mathbb{Z} < (\mathbb{Z}, +)$ sivuluokkien joukko on kongruenssiluokkien joukko (modulo q). Tämä on selitys sille, miksi kongruenssiluokkien joukolle käytetään merkintää $\mathbb{Z}/q\mathbb{Z}$.

Propositio 7.5. *Olkoon G ryhmä ja olkoon $H \leq G$. Joukot G/H ja $H\backslash G$ ovat yhtä mahtavia.*

Todistus. Harjoitustehtävä 7.2 □

Proposition 7.5 nojalla ryhmän ja sen aliryhmän suhdetta kuvaava indeksi voidaan määritellä kumman tahansa aliryhmään H liittyvän sivuluokkien joukon avulla.

Määritelmä 7.6. Aliryhmän $H < G$ *indeksi* on

$$[G : H] = \#(G/H) = \#(H\backslash G).$$

Esimerkki 7.7. (a) $[\mathbb{Z} : q\mathbb{Z}] = q$.

(b) Aliryhmän $C_2 \times \{e\}$ indeksi ryhmässä $C_2 \times C_2$ on

$$[C_2 \times C_2 : C_2 \times \{e\}] = 2.$$

(c) $[\mathbb{R}^2 : \mathbb{R} \times \{0\}] = \infty$, sillä sivuluokat ovat $\mathbb{R} \times \{0\} + (0, a) = \mathbb{R} \times \{a\}$, $a \in \mathbb{R}$.

Lause 7.8 (Lagrangen lause)**.** *Olkoon G äärellinen ryhmä ja olkoon $H < G$. Tällöin*

$$[G : H] = \frac{\#G}{\#H}.$$

Todistus. Proposition 7.4 nojalla kaikki sivuluokat ovat yhtä mahtavia ja sivuluokat osittavat ryhmän G. □

Propositio 7.9. *Olkoon G äärellinen ryhmä. Tällöin $g^{\#G} = e$ jokaiselle $g \in G$.*

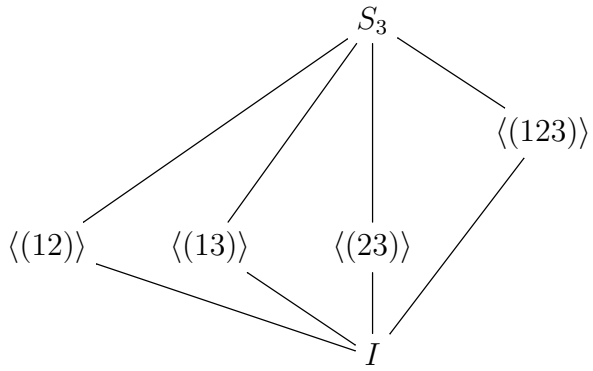
Todistus. Olkoon $H = \langle g \rangle$. Tällöin $\#H = \operatorname{ord} g$. Koska Lagrangen lauseen mukaan $\#G = k\#H$ jollain $k \in \mathbb{N}$, pätee potenssisääntöjen ja Lemman 5.20 nojalla

$$g^{\#G} = g^{k \operatorname{ord} g} = (g^{\operatorname{ord} g})^k = e^k = e.$$ □

Lagrangen lauseen mukaan äärellisen ryhmän G aliryhmien indeksit ja kertaluvut ovat ryhmän kertaluvun tekijöitä. Seuraavan esimerkin (b)-kohdassa näemme, että kaikki ryhmän kertaluvun tekijät eivät välttämättä esiinny sen aliryhmien kertalukujen joukossa.

Esimerkki 7.10. (a) Ryhmän S_3 kertaluku on 6, joten sen aliryhmien mahdolliset kertaluvut (ja indeksit) ovat 1, 2, 3 ja 6. Kolmen alkion permutaatioiden ryhmän

aliryhmärakenne on yksinkertainen ja sitä voi havainnollistaa *aliryhmäkaaviolla*:



Aliryhmäkaaviossa tarkasteltavan ryhmän aliryhmät asetellaan päällekäisille tasoille kertaluvun mukaan siten, että kertaluvultaan suuremmat ryhmät ovat ylemmillä tasoilla. Aliryhmä H yhdistetään janalla ylemmällä tasolla olevan aliryhmän K kanssa, jos $H < K$ eikä ole aliryhmää L, jolle pätee $H < L < K$. Ylläolevassa kaaviossa $I = \{\mathrm{id}\}$.

(b) Koska alternoivan ryhmän A_4 aidossa aliryhmässä voi Lagrangen lauseen mukaan olla korkeintaan 6 alkiota, Esimerkki 6.20 (c) olisi nyt helpompi tehdä: Koska aliryhmä $\langle(12)(34),(123)\rangle$ sisältää 3-syklit (123), (243) ja (134) ja niiden kaikki potenssit, niin siinä on ainakin 8 alkiota. Siis se on koko A_4.

Esimerkissä 7.10 (a) permutaatioryhmällä S_3 on jokaista Lagrangen lauseen sallimaa kokoa olevia aliryhmiä. Aina ei kuitenkaan ole näin, Esimerkissä 7.28 osoitetaan, että ryhmällä A_4 ei ole kuuden alkion aliryhmää vaikka $\#A_4 = 12 = 2 \times 6$.

Määritelmä 7.11. Ryhmän G aliryhmä H on *normaali*, jos $gH = Hg$ kaikille $g \in G$. Jos H on ryhmän G normaali aliryhmä, merkitään $H \trianglelefteq G$, aitoa normaalia aliryhmää merkitään $H \triangleleft G$.

Lemma 7.12. *Olkoon $K \trianglelefteq G$ ja $K < H < G$. Tällöin $K \trianglelefteq H$.* □

Propositioiden 7.4 ja 3.6 mukaan vasemmat sivuluokat määräävät ekvivalenssirelaation, jonka ekvivalenssiluokat ovat vasemmat sivuluokat ja vastaavasti oikeat sivuluokat määräävät ekvivalenssirelaation, jonka ekvivalenssiluokat ovat oikeat sivuluokat. Koska ryhmän G normaalin aliryhmän H vasemmat ja oikeat sivuluokat määräävät saman osituksen ryhmälle G, ne määräävät saman ekvivalenssirelaation. Tämä on oleellisen tärkeää tarkasteltaessa ryhmän G laskutoimituksen yhteensopivuutta sivuluokkien määräämän ekvivalenssirelaation kanssa Lauseessa 7.21.

Esimerkki 7.13. (a) Ryhmä itse ja neutraalialkion muodostama aliryhmä ovat normaaleja.

(b) Lemman 7.2 mukaan $q\mathbb{Z} \triangleleft (\mathbb{Z},+)$ ja $\mathbb{R} \times \{0\} \triangleleft (\mathbb{R}^2,+)$.

(c) Esimerkissä 7.3 osoitettiin, että aliryhmä $\langle(12)\rangle < S_3$ ei ole normaali.

Joissain tilanteissa normaalius on helppo tarkastaa:

Propositio 7.14. *Jos aliryhmän $H < G$ indeksi on kaksi, se on normaali.*

Todistus. Vasemmat sivuluokat ovat H ja $G - H$, samoin oikeat sivuluokat. □

Esimerkki 7.15. Olkoon $n \geq 3$. Olkoon $\tau \in S_n$ alkeisvaihto. Vasen siirto ℓ_τ on bijektio joukkojen A_n ja $S_n - A_n$ välillä. Siis $\#S_n = n! = 2\,\#A_n$. Lagrangen lauseen nojalla $[S_n : A_n] = 2$, joten Proposition 7.14 nojalla $A_n \triangleleft S_n$ kaikilla $n \geq 3$. Erityisesti $C_3 \cong \langle(123)\rangle = A_3 \triangleleft S_3$.

Usein on kätevä käyttää seuraavaa normaalin aliryhmän karakterisointia:

Propositio 7.16. *Ryhmän G aliryhmä H on normaali, jos ja vain jos $ghg^{-1} \in H$ kaikilla $h \in H$ ja kaikilla $g \in G$*

Todistus. Jos H on normaali, niin $gH = Hg$ kaikille $g \in G$. Siis jokaiselle $g \in G$ ja $h \in H$ pätee $gh = h'g$ jollain $h' \in H$, joten $ghg^{-1} = h' \in H$.

Jos taas kaikille $g \in G$ ja $h \in H$ pätee $ghg^{-1} \in H$, niin jokaiselle $g \in G$ ja $h \in H$ on $h' \in H$, jolle $ghg^{-1} = h'$. Siis $gh = h'g \in Hg$, joten $gH \subset Hg$ kaikille $g \in G$. Samoin saadaan $hg^{-1} \in g^{-1}H$, joten $Hg^{-1} \subset g^{-1}H$ kaikille $g \in G$. Koska jokainen ryhmän G alkio on jonkin alkion käänteisalkio, väite on todistettu. □

Esimerkki 7.17. Jos $\alpha \in A_n < S_n$ on parillinen permutaatio ja $\beta \in S_n$ on permutaatio, niin $\beta\alpha\beta^{-1}$ on parillinen permutaatio. Siis Propositio 7.16 antaa toisen todistuksen sille, että $A_n \lhd S_n$.

Sovellamme Propositiota 7.16, kun osoitamme, että normaalit aliryhmät sopivat hyvin yhteen homomorfismien kanssa.

Propositio 7.18. *Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Tällöin*

(1) Olkoon $H \trianglelefteq G$. Tällöin $\phi(H) \trianglelefteq \phi(G) = \operatorname{Im}\phi$.

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

Todistus. (1) Proposition 5.8 nojalla $\phi(H) \leq \phi(G)$. Olkoot $a' \in \phi(H)$ ja $g' \in \phi(G)$. Tällöin on $a \in H$ ja $g \in G$, joille $a' = \phi(a)$ ja $g' = \phi(g)$. Nyt

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

koska $gag^{-1} \in H$. Väite seuraa Proposition 7.16 nojalla.

(2) Harjoitustehtävä 7.9. □

Propositiosta 7.18 saadaan tärkeänä erikoistapauksena

Seuraus 7.19. *Ryhmähomomorfismin ydin on normaali aliryhmä.* □

Esimerkki 7.20. (a)$A_n = \ker\epsilon \lhd S_n$.

(b) $\mathrm{SL}_n(\mathbb{R}) = \ker\det \lhd \mathrm{GL}_n(\mathbb{R})$.

(c) $\mathrm{SO}(n) = \ker\det|_{\mathrm{O}(n)} \lhd \mathrm{O}(n)$.

Proposition 7.18 kohdassa (1) on syytä pitää mielessä, että $\phi(H)$ ei välttämättä ole ryhmän G' normaali aliryhmä: Jos $H < G$ on aliryhmä, joka ei ole normaali ja jos $\phi\colon H \to G$ on inkluusiokuvaus, ei tietenkään $\phi(H) = H$ ole ryhmän G normaali aliryhmä.

Lause 7.21. *Olkoon G ryhmä ja olkoon $H \leq G$ aliryhmä. Tällöin vasempien tai oikeiden sivuluokkien määräämä ekvivalenssirelaatio on yhteensopiva ryhmän G laskutoimituksen kanssa, jos ja vain jos H on ryhmän G normaali aliryhmä.*

Todistus. (1) Oletetaan, että H on normaali. Olkoot $x' \in xH$ ja $y' \in yH$. Tällöin on $h_1, h_2, h_3 \in H$, joille $x' = xh_1$, $y' = yh_2$ ja normaaliusoletuksen nojalla $h_1y = yh_3$, joten

$$x'y' = xh_1yh_2 = xyh_3h_2 \in xyH.$$

Siis $x'y'H = xyH$ Proposition 7.4 nojalla ja laskutoimitus on yhteensopiva sivuluokkien määräämän ekvivalenssirelaation kanssa.

(2) Jos laskutoimitus on yhteensopiva vasempien sivuluokkien määräämän relaation kanssa, niin G/H varustettuna tekijälaskutoimituksella on ryhmä: Tekijälaskutoimituksen assosiatiivisuus osoitettiin Propositiossa 3.9. Koska luonnollinen homomorfismi on surjektiivinen, niin Proposition 1.17 nojalla se kuvaa ryhmän G neutraalialkion tekijälaskutoimituksen neutraalialkioksi, joka siis on H. Tekijälaskutoimituksen määritelmän mukaan kaikille $gH \in G/H$ pätee $(gH)(g^{-1}H) = H$, joten laskutoimituksella varustetun joukon G/H jokaisella alkiolla on käänteisalkio.

Luonnollinen homomorfismi on siis ryhmähomomorfismi $G \to G/H$ ja sen ydin on H. Proposition 7.18 nojalla H on normaali. □

Lauseen 7.21 todistuksesta saadaan myös seuraava tulos:

Seuraus 7.22. *Jos $H \trianglelefteq G$, niin tekijäjoukko G/H varustettuna tekijälaskutoimituksella on ryhmä. Tekijäryhmän G/H neutraalialkio on H.* □

Ryhmää G/H kutsutaan normaalin aliryhmän H määräämäksi ryhmän G *tekijäryhmäksi*. Esimerkiksi ryhmä $\mathbb{Z}/q\mathbb{Z}$, jota tarkasteltiin esimerkin 4.2 kohdassa (a), on kongruenssia $a \equiv b \mod q$ vastaava kokonaislukujen ryhmän tekijäryhmä. Additiivisen ryhmän alkion x sivuluokalle käytetään merkintää $x + H$ ja tekijäryhmän laskutoimitus on siis tällä merkintätavalla

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

Sykliset ryhmät käyttäytyvät hyvin tekijäryhmienkin suhteen

Propositio 7.23. *Jokainen syklisen ryhmän tekijäryhmä on syklinen.*

Todistus. Harjoitustehtävä 7.11. □

Todistamme seuraavaksi tärkeimmän tekijäryhmiä koskevan tuloksen. Todistus on Lauseen 5.17(1) todistuksen yleistys.

Lause 7.24 (Ryhmien (ensimmäinen) isomorfismilause)**.** *Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Tällöin*

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

Todistus. Jos $x\ker\phi = y\ker\phi$, niin Proposition 7.4 nojalla jollain $h \in \ker\phi$ pätee $y = xh$. Siis

$$\phi(y) = \phi(xh) = \phi(x)\phi(h) = \phi(x)e' = \phi(x).$$

Tähän havaintoon perustuen määritellään kuvaus $\psi : G/\ker\phi \to \operatorname{Im}\phi$,

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

joka on homomorfismi: Olkoot $x, y \in G$. Tällöin

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

Määritelmän mukaan $\operatorname{Im}\psi \subset \operatorname{Im}\phi$ ja jokaiselle $x \in G$ pätee $\psi(x\ker\phi) = \phi(x)$, joten $\phi(x) \in \operatorname{Im}\psi$ ja ψ on siis surjektio. Injektiivisyyden toteamiseksi osoitamme, että kuvauksen ψ 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 Proposition 7.4(1) nojalla seuraa $x\ker\phi = \ker\phi$. □

Seuraus 7.25. *Surjektiiviselle ryhmähomomorfismille $\phi\colon G \to G'$ pätee*

$$[G : \ker\phi] = \#G'.$$ □

Lause 7.26. *Olkoon $\phi\colon G \to G'$ surjektiivinen ryhmähomomorfismi ja olkoon $H' \trianglelefteq G'$. Tällöin $G/\phi^{-1}(H') \cong G'/H'$.*

Todistus. Proposition 7.18(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 7.24 mukaan $G/H \cong G'/H'$. □

Esimerkki 7.27. (a) $[\mathbb{Z}^2 : (2\mathbb{Z})^2] = 4$ sillä luonnollinen homomorfismi

$$\mathbb{Z}^2 \ni (k_1, k_2) \mapsto (k_1 + 2\mathbb{Z}, k_2 + 2\mathbb{Z}) \in (\mathbb{Z}/2\mathbb{Z})^2$$

on surjektio, jonka ydin on $(2\mathbb{Z})^2$.
(b) Olkoon $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Tällöin $\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K}) \cong \mathbb{K}^\times$, koska $\det \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\times$ on surjektiivinen homomorfismi, jonka ydin on $\mathrm{SL}_n(\mathbb{K})$.

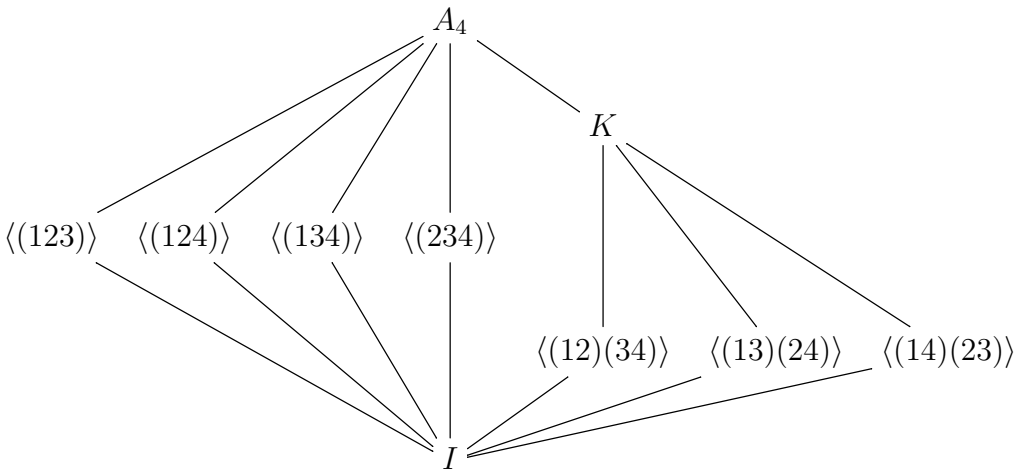
Ryhmien isomorfismilause antaa vastaavuuden surjektiivisten homomorfismien ja normaalien aliryhmien välille: Jos $N \trianglelefteq G$, niin luonnollinen homomorfismi on surjektiivinen homomorfismi $G \to G/N$, jonka ydin on N. Toisaalta jokaisen ryhmähomomorfismin ydin on määrittelyryhmänsä normaali aliryhmä. Tämä vastaavuus ei kuitenkaan ole bijektiivinen sillä esimerkiksi homomorfismeilla $\exp\colon \mathbb{C} \to \mathbb{C}^\times$ ja $k \circ \exp$, missä k on kompleksikonjugointi, on sama ydin

$$\ker(k \circ \exp) = \ker \exp = \{k\, 2\pi i : k \in \mathbb{Z}\}.$$

Esimerkki 7.28. Esimerkin 7.15 mukaan alternoivan ryhmän A_4 kertaluku on $\#A_4 = 4!/2 = 12$. Jos $H < A_4$ on aliryhmä, jonka kertaluku on 6, niin Lagrangen lauseen mukaan $[A_4 : H] = 2$. Proposition 7.14 nojalla $H \lhd A_4$, joten ensimmäisen isomorfismilauseen nojalla $A_4/H \cong C_2$. Siis kaikille $g \in G$ pätee $g^2 H = gHgH = H$, joten Proposition 7.4(1) nojalla $g^2 \in H$ kaikille $g \in G$.

Kaikki 3-syklit ovat parillisia permutaatioita, joten ne kuuluvat ryhmään A_4. Jos $g \in A_4$ on 3-sykli, niin $g = g^4 = (g^2)^2 \in H$. Kaikki 3-syklit siis sisältyvät aliryhmään H. Kuitenkin ryhmässä A_4 on 8 3-sykliä, joiden siis pitäisi sisältyä kuuden alkion aliryhmään. Siis ryhmällä A_4 ei ole kuuden alkion aliryhmää.

Ryhmän A_4 aliryhmärakenne on seuraavan kaavion mukainen:



Mitkä tahansa kaksi ryhmän A_4 kertaluvun 2 alkioista (12)(34), (13)(24) ja (14)(23) virittävät kaaviossa esiintyvän Kleinin neliryhmän K.

Esimerkki 7.29. (a) Harjoitustehtävässä 4.10 osoitettiin, että ryhmän G automorfismit muodostavat ryhmän $\mathrm{Aut}(G)$. Olkoon $a \in G$. Kuvaus $\phi_a\colon G \to G$, $\phi_a(g) = aga^{-1}$ on ryhmän G automorfismi: Se on homomorfismi:

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

Se on myös bijektio, koska sillä on käänteiskuvaus $\phi_a^{-1}\colon G \to G\colon \phi_a^{-1}(g) = a^{-1}ga$. Kuvaus ϕ_a on ryhmän G *sisäinen automorfismi.*

Ryhmän G sisäiset automorfismit muodostavat *sisäisten automorfismien ryhmän*

$$\mathrm{Inn}(G) = \{\phi_a : a \in G\} \leq \mathrm{Aut}(G).$$

Harjoitustehtävässä 7.12 osoitetaan, että sisäisten automorfismien ryhmä on automorfismiryhmän normaali aliryhmä. Tekijäryhmä

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$$

on ryhmän G *ulkoisten automorfismien ryhmä.*

(b) Automorfismi ϕ_a on identtinen kuvaus täsmälleen silloin, kun $aga^{-1} = g$ kaikilla $g \in G$. Tämän ehdon toteuttavat alkiot muodostavat ryhmän G *keskuksen*

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

Harjoitustehtävässä 7.13 osoitetaan, että $Z(G)$ on ryhmän G normaali aliryhmä. Jos G on kommutatiivinen, niin $Z(G) = G$, joten tekijäryhmä $G/Z(G)$ kuvaa ryhmän G epäkommutatiivisuutta.

(c) Kuvaus $\rho\colon G \to \mathrm{Inn}(G)$, $\rho(a) = \phi_a$, on homomorfismi. Tämä tarkastetaan kuten Proposition 6.8 todistuksessa: Jos $a, b \in G$, niin kaikille $x \in G$ pätee

$$\rho(ab)(x) = \phi_{ab}(x) = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = \phi_a(\phi_b(x)) = \rho(a) \circ \rho(b)(x).$$

Sisäisten automorfismien määritelmän nojalla $\mathrm{Im}(\rho) = \rho(G) = \mathrm{Inn}(G)$. Lisäksi $\rho(g)$ on identtinen automorfismi täsmälleen silloin, kun $g \in Z(G)$, joten ryhmien isomorfismilauseen nojalla pätee

$$\mathrm{Inn}(G) \cong G/Z(G)\,.$$

(d) Matriisi $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ määrää ryhmän $\mathrm{SL}_2(\mathbb{Z})$ sisäisen automorfismin ϕ_A,

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

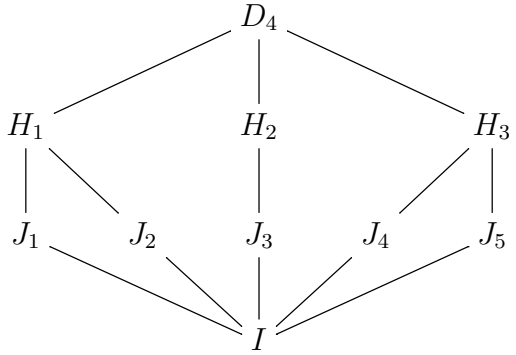
Harjoitustehtävässä 4.9 osoitettiin, että kuvaukset $B \mapsto B^{-1}$ ja $C \mapsto {}^tC$ eivät ole ryhmän $\mathrm{SL}_2(\mathbb{Z})$ automorfismeja. Kuitenkin niiden yhdistetty kuvaus on automorfismi!

Harjoitustehtäviä.

7.1. Olkoon G ryhmä ja olkoon H sen aliryhmä. Osoita, että $xH = yH$, jos ja vain jos $y^{-1}x \in H$

7.2. 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.

7.3. Täydennä diedriryhmän D_4 aliryhmäkaavio



Kaaviossa esiintyvien aliryhmien indeksit ovat $[D_4 : J_i] = 4$ ja $[D_4 : H_j] = 2$ kaikilla $1 \leq i \leq 5$ ja $1 \leq j \leq 3$.

Olkoot

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$$

ja

$$B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}).$$

Olkoon $H = \langle A, B \rangle < \mathrm{SL}_2(\mathbb{C})$ matriisien A ja B virittämä aliryhmä.

7.4. Osoita, että ryhmä H ei ole kommutatiivinen ja että $\#H = 8$.

7.5. Osoita, että ryhmällä H on aliryhmien H ja $\{I\}$ lisäksi neljä aliryhmää, jotka ovat kaikki normaaleja.

7.6. Piirrä ryhmän H aliryhmäkaavio.

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

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

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

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

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

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

7.10. Onko $\mathrm{O}(n) \lhd \mathrm{GL}_n(\mathbb{R})$?

7.11. Olkoon C syklinen ryhmä. Osoita, että kaikki ryhmän C tekijäryhmät ovat syklisiä.

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

7.13. Osoita, että ryhmän G keskus $Z(G)$ on kommutatiivinen normaali aliryhmä.

7.14. Määritä ryhmien S_3, D_3 ja $C_2 \times C_2$ keskukset.

7.15. Määritä ryhmien S_3, D_3 ja $C_2 \times C_2$ sisäiset automorfismiryhmät.

---

[3]Vihje: Kaikki ryhmät H_j, $1 \leq j \leq 3$ eivät ole isomorfisia.

[4]Vihje: Tarkasta ensin, että $A^{-1} = -A$, $B^{-1} = -B$ ja $BA = -AB$. Käytä näitä tietoja ja Propositiota 5.12

[8]Vihje: Oletetaan, että $G = \bigsqcup_{i=1}^{m} a_i H$ ja $H = \bigsqcup_{j=1}^{n} b_j K$.Osoita, että $G = \bigsqcup_{i=1}^{m} \bigsqcup_{j=1}^{n} a_i b_j K$.

7.16. Olkoon

$$H_3 = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

Heisenbergin ryhmä, jonka laskutoimitus on matriisien kertolasku. Osoita, että kuvaus $\psi\colon H_3 \to (\mathbb{R}^2, +)$, joka määritellään asettamalla

$$\psi(\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}) = (a, b),$$

on homomorfismi ja määritä sen ydin. Osoita, että tekijäryhmä $H_3/\ker\psi$ on isomorfinen ryhmän $(\mathbb{R}^2, +)$ kanssa.

Olkoon G ryhmä. Alkioiden $a, b \in G$ *kommutaattori* on $[a, b] = aba^{-1}b^{-1}$. Ryhmän G *kommutaattorialiryhmä* $[G, G]$ on kaikkien kommutaattorien $[a, b]$, $a, b \in G$ virittämä aliryhmä

$$[G, G] = \langle [a, b] : a, b \in G \rangle.$$

7.17. Osoita, että $[G, G] \trianglelefteq G$.

7.18. Osoita, että $G/[G, G]$ on kommutatiivinen ryhmä.

8. Renkaat

Renkaat ovat algebrallisia rakenteita, joissa on määritelty kaksi assosiatiivista laskutoimitusta, joista ainakin toinen on kommutatiivinen. Vaadimme näiltä kahdella laskutoimituksella varustetuilta joukoilta joitakin samoja ominaisuuksia joita kokonaisluvuilla on, mutta kertolasku ei välttämättä ole kommutatiivinen. Tässä luvussa aloitamme tutustumisen renkaiden perusominaisuuksiin ja eri tapoihin luokitella renkaita ominaisuuksiensa perusteella. Tutkimme myös useita esimerkkejä renkaista.

Määritelmä 8.1. Olkoon $R \neq \emptyset$ joukko, jolla on määritelty kaksi assosiatiivista laskutoimitusta $+$ ja $\cdot$. Kolmikko $(R, +, \cdot)$ on *(ykkösellinen) rengas*, jos

(1) $(R, +)$ on kommutatiivinen ryhmä,
(2) kertolasku on distributiivinen yhteenlaskun suhteen ja
(3) kertolaskulla on neutraalialkio $1 = 1_R \in R$.

Laskutoimituksen $+$ neutraalialkiolle käytetään merkintää $0 = 0_R$. Ryhmä $(R, +)$ on renkaan R *additiivinen ryhmä*. Rengas on *kommutatiivinen*, jos kertolasku on kommutatiivinen.

Kertolaskun distributiivisuus yhteenlaskun suhteen renkaassa R tarkoittaa, että kaikille $a, b, c \in R$ pätee $a(b + c) = ab + ac$ ja $(b + c)a = ba + ca$.

Esimerkki 8.2. (a) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ ja $(\mathbb{C}, +, \cdot)$ ovat kommutatiivisia renkaita.

(b) Olkoon $q \in \mathbb{N} - \{0, 1\}$. Kongruenssiluokkien muodostama joukko $\mathbb{Z}/q\mathbb{Z}$ varustettuna kokonaislukujen yhteen- ja kertolaskujen tekijälaskutoimituksilla on kommutatiivinen rengas, jota kutsutaan *jäännösluokkarenkaaksi*. (Harjoitustehtävä 8.1)

(c) 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

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

kaikilla $x \in X$. Joukko $\mathscr{F}(X, R)$ varustettuna näillä laskutoimituksilla on rengas, jota kutsutaan *funktiorenkaaksi*.

Laskutoimitusten assosiatiivisuus, yhteenlaskun kommutatiivisuus ja kertolaskun distributiivisuus yhteenlaskun suhteen seuraa siitä, että funktioiden arvot ovat renkaassa R ja funktioiden laskutoimitukset on määritelty pisteittäin. Yhteenlaskun (vastaavasti kertolaskun) neutraalialkio on vakiofunktio $\underline{0}\colon X \to R$ (vastaavasti $\underline{1}\colon X \to R$). Funktion $f \in \mathscr{F}(X, R)$ käänteisalkio yhteenlaskun suhteen on funktio $-f$, joka määritellään asettamalla $(-f)(x) = -f(x)$ kaikilla $x \in R$.

Merkitsemme renkaan $\mathscr{F}(X, R)$ yhteen- ja kertolaskuja samoilla merkinnöillä $+$ ja $\cdot$ kuin renkaan R laskutoimituksia. Samoin yhteen- ja kertolaskun neutraalialkioille on tapana käyttää merkintöjä 0 ja 1 useimmissa renkaissa.

Rengas $\mathscr{F}(X, R)$ on kommutatiivinen, jos R on kommutatiivinen. Esimerkiksi siis $\mathscr{F}(\mathbb{R}, \mathbb{R})$ on kommutatiivinen rengas.

Propositio 8.3. *Olkoon R rengas. Tällöin*

(1) $0_R \cdot x = 0_R$ *kaikilla* $x \in R$,
(2) $x(-y) = (-x)y = -(xy)$ *ja* $(-x)(-y) = xy$ *kaikilla* $x, y \in R$,
(3) $x(y - z) = xy - xz$ *ja* $(y - z)x = yx - zx$ *kaikilla* $x, y, z \in R$,
(4) *monikerroille pätee* $(nx)(mx) = (nm)x$ *kaikilla* $n, m \in \mathbb{N}$ *ja* $x \in R$.

Todistus. (1) Distributiivisuuden nojalla

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

kaikilla $x \in R$. Renkaan R additiivisen ryhmän supistussäännöstä seuraa, että $0_R\, x = 0_R$ kaikilla $x \in R$.
Loput väitteet todistetaan harjoitustehtävissä 8.4 ja 8.5. □

Edellä osoitettujen laskusääntöjen avulla on helppo osoittaa seuraavat perusominaisuudet

Propositio 8.4. *Olkoon R rengas. Jos $\#R \geq 2$, niin*
(1) $0 \neq 1$ *ja*
(2) *yhteenlaskun neutraalialkiolla* 0 *ei ole käänteisalkiota kertolaskun suhteen.*

Todistus. (1) Jos $1 = 0$, niin kaikille $x \in R$ pätee Proposition 8.3 nojalla

$$x = 1\, x = 0\, x = 0.$$

Toinen väite todistetaan harjoitustehtävänä 8.6. □

Esimerkki 8.5. Olkoon X joukko. Määritellään joukkojen $A, B \in \mathscr{P}(X)$ *symmetrinen erotus* asettamalla

$$A \triangle B = (A - B) \cup (B - A)\,.$$

Kahdella laskutoimituksella varustettu joukko $(\mathscr{P}(X), \triangle, \cap)$ on kommutatiivinen rengas. Sen yhteenlaskun $\triangle$ neutraalialkio on $\emptyset$ ja kertolaskun $\cap$ neutraalialkio on X. Lisäksi kaikille $A \in \mathscr{P}(X)$ pätee $A \cap A = A$ ja $A \triangle A = \emptyset$.

Esimerkin 8.5 kertolaskun ominaisuuden avulla voidaan luokitella renkaita ja niiden alkioita: Renkaan R alkio x on *idempotentti*, jos $x^2 = x$. Jos renkaan B kaikki alkiot ovat idempotentteja, niin B on *Boolen rengas*. Seuraava tulos osoittaa, että Boolen renkaalla on automaattisesti kaksi muutakin Esimerkin 8.5 renkaan ominaisuutta.

Propositio 8.6. *Olkoon B Boolen rengas. Tällöin*
(1) B on kommutatiivinen ja
(2) $2x = 0$ kaikille $x \in B$.

Todistus. Osoitamme kohdan (2), kohta (1) jätetään Harjoitustehtäväksi 8.8. Olkoon $x \in B$. Tällöin Proposition 8.3 (4) ja Lemman 1.13 nojalla

$$2x = (2x)^2 = 4x = 2x + 2x\,.$$

Koska $(B, +)$ on ryhmä, väite seuraa supistussäännön (Propositio 4.4) nojalla. □

Määritelmä 8.7. Jos R on rengas ja alkiolla $u \in R$ on käänteisalkio kertolaskun suhteen, niin u on renkaan R *yksikkö*. Renkaan R *yksiköiden ryhmä* (tai *multiplikatiivinen ryhmä*) on

$$R^\times = \{u \in R : u \text{ on yksikkö}\}$$

varustettuna renkaan R kertolaskun indusoimalla laskutoimituksella.

Propositio 8.8. *Renkaan yksiköiden joukko varustettuna kertolaskulla on ryhmä.*

Todistus. Renkaan R kertolasku on assosiatiivinen laskutoimitus, jonka neutraalialkio on 1. Yksiköiden joukko on vakaa kertolaskun suhteen: Jos u ja v ovat yksiköitä, niin uv on yksikkö, koska

$$(uv)(v^{-1}u^{-1}) = 1 = (v^{-1}u^{-1})(uv).$$

Kertolasku on siis assosiatiivinen laskutoimitus yksiköiden joukossa. Laskutoimituksella on neutraalialkio, koska 1 on yksikkö. Määritelmän mukaan jokaisella yksiköllä u on käänteisalkio u^{-1} renkaassa R. Myös u^{-1} on yksikkö, koska $(u^{-1})^{-1} = u$. □

Esimerkki 8.9. (a) Jos renkaassa on ainakin kaksi alkiota, niin Proposition 8.4 mukaan $0 \neq 1$ ja 0 ei ole yksikkö.

(b) Renkaissa $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ kaikki nollasta poikkeavat alkiot ovat yksiköitä, joten aiemmin esitellyt multiplikatiiviset ryhmät $\mathbb{Q}^\times$, $\mathbb{R}^\times$ ja $\mathbb{C}^\times$ sopivat yhteen Määritelmän 8.7 kanssa.

(c) Kokonaislukujen renkaan yksiköiden ryhmä on $\mathbb{Z}^\times = \{-1, 1\}$.

(d) Funktiorenkaan $\mathscr{F}(X, R)$ alkio f on yksikkö, jos ja vain jos $f(X) \subset R^\times$.

Renkaan R alkio x on *nilpotentti*, jos $x^n = 0$ jollain $n \in \mathbb{N}$. Pienin positiivinen luonnollinen luku n, jolle $x^n = 0$ on nilpotentin alkion x *aste*.

Esimerkki 8.10. (a) $2 + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$ on nilpotentti astetta 2, sillä

$$(2 + 4\mathbb{Z})^2 = 4 + 4\mathbb{Z} = 0\,.$$

(b) Olkoon R rengas, jossa on vähintään 2 alkiota. Kaikkien R-kertoimisten $n \times n$-matriisien joukko $\mathrm{M}_n(R)$ varustettuna matriisien yhteen- ja kertolaskulla on rengas. Kun $R = \mathbb{R}$, kaikki muut renkaan ominaisuudet paitsi distributiivisuus osoitettiin Esimerkissä 1.16 (b) ja harjoitustehtävässä 1.7 tapauksessa $n = 2$. Kun $n \geq 2$, niin $\mathrm{M}_n(R)$ ei ole kommutatiivinen rengas, koska matriisien kertolasku ei ole kommutatiivinen.

Matriisi $A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})$ on nilpotentti astetta 3 sillä $A^2 \neq 0$ ja $A^3 = 0$.

Propositio 8.11. *Olkoon R rengas, jossa on vähintään kaksi alkiota. Renkaan R yksikkö ei ole nilpotentti.*

Todistus. Jos $x \in R$ on nilpotentti, niin on $m \in \mathbb{N}$, jolle $x^m = 0$. Jos x on yksikkö, niin $x^{m-1} = x^m x^{-1} = 0\,x^{-1} = 0$. Toistamalla tätä saadaan $x = 0$, mikä on mahdotonta, koska 0 ei ole yksikkö. □

Esimerkki 8.12. Olkoon $(A, +)$ kommutatiivinen ryhmä. Olkoon

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

Varustamme joukon $\mathrm{Hom}(A, A)$ kahdella laskutoimituksella: Homomorfismien yhteenlasku määritellään asettamalla

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

kaikille $a \in A$ ja kertolaskuna käytetään homomorfismien yhdistämistä.

Yhteenlasku on laskutoimitus: Jos $\phi, \phi' \in \mathrm{Hom}(A, A)$, niin

$$\begin{aligned}(\phi + \phi')(a + b) &= \phi(a + b) + \phi'(a + b) = \phi(a) + \phi(b) + \phi'(a) + \phi'(b) \\ &= (\phi + \phi')(a) + (\phi + \phi')(b),\end{aligned}$$

joten $\phi + \phi' \in \mathrm{Hom}(A, A)$.

Laskutoimituksella varustettu joukko $(\mathrm{Hom}(A, A), +)$ on kommutatiivinen ryhmä: Laskutoimituksen assosiatiivisuus ja kommutatiivisuus osoitetaan harjoitustehtävässä 8.11. Homomorfismien yhteenlaskun neutraalialkio on nollahomomorfismi 0 ja homomorfismin ϕ käänteisalkio yhteenlaskun suhteen on homomorfismi $-\phi$, joka määritellään asettamalla $(-\phi)(a) = -\phi(a)$ kaikilla $a \in A$.

Kertolasku osoitettiin laskutoimitukseksi harjoitustehtävässä 1.17. Identtinen homomorfismi on homomorfismien kertolaskun neutraalialkio, joten tarkastettavaksi jää kertolaskun distributiivisuus yhteenlaskun suhteen: Jos $\phi, \psi, \zeta \in \mathrm{Hom}(A, A)$,niin

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

ja

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

Koska homomorfismien yhdistäminen on renkaan $\mathrm{Hom}(A,A)$ kertolasku, homomorfismien yhdistetty kuvaus on yllä merkitty ilman yhdistetyn kuvauksen merkkiä $\circ$.

Määritelmä 8.13. Olkoot R ja R' renkaita. Kuvaus $\phi : R \to R'$ on rengashomomorfismi, jos

- $\phi\colon (R,+) \to (R',+)$ on homomorfismi,
- $\phi\colon (R,\cdot) \to (R',\cdot)$ on homomorfismi ja
- $\phi(1) = 1$.

Bijektiivinen rengashomomorfismi on *rengasisomorfismi*.

Propositiossa 1.17 osoitettiin, että surjektiivinen homomorfismi kuvaa neutraalialkion neutraalialkioksi, mutta ilman surjektiivisuutta näin ei välttämättä ole. Ryhmähomomorfismille ei tarvita vastaavaa vaatimusta Proposition 4.12 nojalla. Erityisesti siis rengashomomorfismi kuvaa nollan nollaksi. Huomaa, että Proposition 8.4 nojalla rengashomomorfismille $\phi\colon R \to R'$ pätee $\phi(1) = 0$ vain, jos $R' = \{0\}$. Lisäksi yhden alkion renkaalta ei ole rengashomomorfismia renkaaseen, jossa on vähintään kaksi alkiota.

Esimerkki 8.14. (a) Luonnollinen kuvaus $k \mapsto k + q\mathbb{Z}$ renkaasta $(\mathbb{Z},+,\cdot)$ jäännösluokkarenkaaseen $(\mathbb{Z}/q\mathbb{Z},+,\cdot)$ on surjektiivinen rengashomomorfismi.
(b) Olkoon X epätyhjä joukko ja olkoon R rengas. Olkoon $a \in X$. *Evaluaatiokuvaus* $E_a\colon \mathscr{F}(X,R) \to R$, $E_a(f) = f(a)$, on rengashomomorfismi:

$$E_a(f+g) = (f+g)(a) = f(a)+g(a) = E_a(f)+E_a(g),$$
$$E_a(fg) = (fg)(a) = f(a)g(a) = E_a(f)E_a(g)$$

ja

$$E_a(\underline{1}) = \underline{1}(a) = 1.$$

Propositio 8.15. *(1) Jos $f\colon R \to S$ ja $g\colon S \to T$ ovat rengashomomorfismeja, niin $g \circ f$ on rengashomomorfismi.*
(2) 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. Harjoitustehtävät 8.13 ja 8.15. □

Kokonaislukujen renkaan $\mathbb{Z}$ rakenne on yksinkertainen: sen kaikki alkiot ovat alkion 1 monikertoja. Tästä seuraa erityisominaisuus renkaassa $\mathbb{Z}$ määritellyille rengashomomorfismeille.

Propositio 8.16. *Olkoon R rengas. On täsmälleen yksi rengashomomorfismi $\phi\colon \mathbb{Z} \to R$.*

Todistus. Koska 1 virittää additiivisen ryhmän $(\mathbb{Z},+)$, niin Proposition 5.14 nojalla halutunlaisia homomorfismeja on korkeintaan yksi. Väite seuraa havainnosta, että kuvaus $\phi\colon \mathbb{Z} \to R$,

$$\phi(n) = n1_R = 1_R + 1_R + \cdots + 1_R\,,$$

on rengashomomorfismi, sillä

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

ja

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

Lisäksi kuvauksen ϕ määritelmän mukaan $\phi(1) = 1_R$. □

Rengashomomorfismin $\psi\colon R \to S$ ydin määritellään renkaiden R ja S additiivisten ryhmien ryhmähomomorfismin $\phi\colon (R,+) \to (S,+)$ ytimen avulla:

Määritelmä 8.17. Rengashomomorfismin $\psi\colon R \to R'$ *ydin* on

$$\ker \psi = \psi^{-1}(0) = \{x \in R : \psi(x) = 0\}.$$

Ryhmien vastaava tulos Propositio 5.10 antaa välittömästi

Propositio 8.18. *Rengashomomorfismi on injektio, jos ja vain jos sen ydin on* $\{0\}$. □

Esimerkki 8.19. (a) Luonnollisen rengashomomorfismin $\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ ydin on $q\mathbb{Z}$ kaikilla $q \geq 2$.

(b) Inkluusiohomomorfismi $\mathbb{Z} \to \mathbb{Q}$, $k \mapsto k$, on injektio. Sen ydin on $\{0\}$.

Rengashomomorfismin ydin ei yleensä ole määrittelyrenkaansa alirengas, kuten tarkastelemamme esimerkitkin osoittavat. Homomorfismin $\mathbb{Z} \to R$, $k \mapsto k1$, ytimen virittäjä $\chi(R) \in \mathbb{N}$ on renkaan R *karakteristika*.

Renkaiden $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ karakteristika on 0, koska ne sisältävät kaikki isomorfisen kopion kokonaislukurenkaasta $\mathbb{Z}$. Jäännösluokkarenkaan $\mathbb{Z}/q\mathbb{Z}$ karakteristika on q.

Lemma 8.20. *Jos renkaan R karakteristika on q, niin $qx = 0$ kaikille $x \in R$.*

Todistus. Harjoitustehtävä 8.14 □

Määritelmä 8.21. Olkoon R rengas ja olkoon $S \subset R$ vakaa yhteenlaskun ja kertolaskun suhteen. Jos S varustettuna indusoiduilla laskutoimituksilla on rengas ja jos $1_S = 1_R$, niin S on renkaan R *alirengas*.

Määritelmän mukaan alirenkaan inkluusiokuvaus $i : S \to R$, $i(s) = s$, on rengashomomorfismi.

Esimerkki 8.22. (a) $\mathbb{Z}$ on renkaan $\mathbb{Q}$ alirengas.

(b) Homomorfismin $\psi\colon \mathbb{Z} \to R$ kuvajoukko $\{k1_R : k \in \mathbb{Z}\}$ on renkaan R alirengas.

(c) Joukko

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\} \subset \mathrm{M}_2(\mathbb{R})$$

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 renkaalta $\mathbb{R}$ renkaalle S.

Alirenkaalle on samanlainen testi kuin aliryhmälle (vertaa Propositioon 5.3).

Propositio 8.23. *Olkoon R rengas ja olkoon $S \subset R$. 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) $-1_R \in S$.

Todistus. Harjoitustehtävä 8.16. □

Esimerkki 8.24. (a) Samaan tapaan kuin permutaatioryhmille määriteltiin aliryhmiä rajoittumalla kuvauksiin, joilla on tiettyjä ominaisuuksia, voimme määritellä

funktiorenkaiden $\mathscr{F}(X,R)$ alirenkaita. Analyysin kursseilla osoitetaan, että indusoiduilla laskutoimituksilla varustetut joukot

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

ovat funktiorenkaan $\mathscr{F}(\mathbb{R},\mathbb{R})$ alirenkaita

(b) Vektoriavaruuden $\mathbb{R}^n$ *endomorfismirengas* on

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

varustettuna Esimerkissä 8.12 käsitellyn homomorfismirenkaan laskutoimituksilla. Osoitamme, että $\mathrm{End}(\mathbb{R}^n)$ on todellakin rengas näyttämällä Proposition 8.23 avulla, että se on homomorfismirenkaan $\mathrm{Hom}(\mathbb{R}^n,\mathbb{R}^n)$ alirengas.

Lineaarikuvaukset ovat additiivisen ryhmän $(\mathbb{R}^n,+)$ homomorfismeja itselleen, joten niiden summa on myös homomorfismi kuten Esimerkissä 8.12 todettiin. Lisäksi kaikille $L,L'\in\mathrm{End}(\mathbb{R}^n)$, $x\in\mathbb{R}^n$ ja $a\in\mathbb{R}$ pätee

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

joten lineaarikuvauksen toinenkin ehto toteutuu. Lineaarialgebran kurssilla on osoitettu, että lineaarikuvausten yhdistetty kuvaus on lineaarikuvaus: Jos $L_1,L_2\in\mathrm{End}(\mathbb{R}^n)$, $x,y\in\mathbb{R}^n$ ja $\alpha,\beta\in\mathbb{R}$, niin

$$\begin{aligned}L_2L_1(\alpha x+\beta y) &= L_2(L_1(\alpha x+\beta y)) = L_2(\alpha L_1(x)+\beta L_1(y))\\ &= \alpha L_2(L_1(x))+\beta L_2(L_1(y)) = \alpha L_2L_1(x)+\beta L_2L_1(y)\,.\end{aligned}$$

Siis molemmat laskutoimitukset toteuttavat Proposition 8.23 ehdon (1). Lisäksi identtinen kuvaus $\mathrm{id}\colon\mathbb{R}^n\to\mathbb{R}^n$ on lineaarikuvaus, kuten myös $-\mathrm{id}$, joten Proposition 8.23 mukaan $\mathrm{End}(\mathbb{R}^n)$ on renkaan $\mathrm{Hom}(\mathbb{R}^n,\mathbb{R}^n)$ alirengas.

(c) Valitaan jokin vektoriavaruuden $\mathbb{R}^n$ kanta. Esimerkissä 4.13 käsitelty kuvaus $\mathrm{Mat}\colon\mathrm{End}(\mathbb{R}^n)\to\mathrm{M}_n(\mathbb{R})$, joka liittää lineaarikuvaukseen L sen matriisin tässä kannassa, on rengasisomorfismi. Jos $L,L'\in\mathrm{End}(\mathbb{R}^n)$, niin $(L+L')(v)=Lv+L'v$, joten

$$\mathrm{Mat}(L+L') = \mathrm{Mat}(L)+\mathrm{Mat}(L'),$$

eli Mat on ryhmähomomorfismi additiivisten ryhmien välillä. Lisäksi kaikille lineaarikuvauksille $L,L'\in\mathrm{End}(\mathbb{R}^n)$ pätee

$$\mathrm{Mat}(L'L) = \mathrm{Mat}(L')\,\mathrm{Mat}(L)$$

ja identtisen kuvauksen matriisi on I_n.

Alirenkaat ja rengashomomorfismit ovat yhteensopivia samaan tapaan kuin aliryhmät ja ryhmähomomorfismit:

Propositio 8.25. *Olkoon $\phi\colon R\to R'$ rengashomomorfismi.*

(1) Jos S on renkaan R alirengas, niin $\phi(S)$ on renkaan R' alirengas.

(2) Jos S' on renkaan R' alirengas, niin $\phi^{-1}(S')$ on renkaan R alirengas.

Todistus. (1) Proposition 5.8 mukaan $(\phi(S),+)$ on kommutatiivinen ryhmä, joten Propositiota 8.23 sovellettaessa riittää kohdassa (1) tarkastella kertolaskua ja kertolaskun neutraalialkion kuvautumista. Olkoot $\phi(a),\phi(b)\in\phi(S)$. Tällöin

$$\phi(a)\phi(b) = \phi(ab)\in\phi(S)\,,$$

koska $\phi\colon (R,\cdot) \to (R',\cdot)$ on homomorfismi. Koska $-1_R \in S$, niin Propositio 4.12 sovellettuna ryhmähomomorfismiin $\phi\colon (R,\cdot) \to (R',\cdot)$ antaa

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

Siis Proposition 8.23 oletukset ovat voimassa.

(2) Harjoitustehtävä 8.17. □

Seuraus 8.26. *Olkoon $\phi\colon R \to R'$ rengashomomorfismi. Tällöin $\phi(R)$ on renkaan R' alirengas ja $\phi^{-1}(R')$ on renkaan R alirengas.* □

Harjoitustehtäviä.

8.1. Osoita, että $\mathbb{Z}/q\mathbb{Z}$ varustettuna kokonaislukujen yhteen- ja kertolaskujen tekijälaskutoimituksilla on kommutatiivinen rengas.

8.2. Osoita, että $\big(\mathscr{P}(X), \triangle, \cap\big)$ on Boolen rengas.

8.3. 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?

8.4. 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 $x, y, z \in R$.

8.5. Olkoon R rengas. Osoita, että monikerroille pätee $(nx)(mx) = (nm)x$ kaikilla $n, m \in \mathbb{N}$ ja $x \in R$. Jos x on yksikkö, osoita, että $(nx)(mx) = (nm)x$ kaikilla $n, m \in \mathbb{Z}$.

8.6. Olkoon $R \neq \{0\}$ rengas. Osoita, että yhteenlaskun neutraalialkiolla 0 ei ole käänteisalkiota kertolaskun suhteen.

8.7. Olkoon K kommutatiivinen rengas. Osoita, että renkaassa K pätee *binomikaava*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

kaikille $a, b \in K$.

8.8. Osoita, että Boolen rengas on kommutatiivinen.

8.9. Olkoon B Boolen rengas. Määritä $B^\times$.

8.10. Olkoon x renkaan R nilpotentti alkio. Osoita, että $1 - x$ on yksikkö.

8.11. Olkoon $(A,+)$ kommutatiivinen ryhmä. Osoita, että joukon $\mathrm{Hom}(A,A)$ laskutoimitus $+$, joka määritellään asettamalla

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

on assosiatiivinen ja kommutatiivinen.

8.12. Ovatko funktiorenkaat $\mathscr{F}\big([0,1],\mathbb{R}\big)$ ja $\mathscr{F}\big([0,2],\mathbb{R}\big)$ isomorfisia?

[2]Vihje: Harjoitustehtävä 4.1.
[3]Vihje: $(1,0,1)$
[10]Vihje: Jos x on astetta 2, niin $(1-x)(1+x) = 1$.

8.13. Olkoot $f\colon R \to S$ ja $g\colon S \to T$ rengashomomorfismeja. Osoita, että $g \circ f$ on rengashomomorfismi.

8.14. Olkoon R rengas, jonka karakteristika on q. Osoita, että $qx = 0$ kaikille $x \in R$.

8.15. Osoita, että 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 $f \circ \bar{f} = \mathrm{id}_S$.

8.16. Olkoon R rengas ja olkoon $S \subset R$. 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
- $-1_R \in S$.

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

8.18. Osoita, että renkaalla $\mathbb{Z}$ ei ole muita alirenkaita kuin $\mathbb{Z}$.

8.19. Olkoon $q \in \mathbb{N} - \{0, 1\}$. Osoita, että ei ole rengashomomorfismia jäännösluokkarenkaalta $\mathbb{Z}/q\mathbb{Z}$ renkaaseen $\mathbb{Z}$.

9. Renkaat $\mathbb{Z}$ ja $\mathbb{Z}/q\mathbb{Z}$

Tarkastelemme tässä luvussa jaollisuutta kokonaislukujen renkaassa $\mathbb{Z}$ ja todistamme tuloksia, joita käytetään jäännösluokkarenkaan $\mathbb{Z}/q\mathbb{Z}$ ominaisuuksien tarkastelussa.

Jos $a, b, c \in \mathbb{Z}$ ovat lukuja, joille pätee $ab = c$, niin luvut a ja b ovat luvun c *tekijöitä*. Tällöin luvut a ja b *jakavat* luvun c, mistä käytetään usein merkintää $a \mid c$ ja vastaavasti $b \mid c$. Luvut, joilla on vain vähän tekijöitä ovat tärkeässä osassa jaollisuutta tarkasteltaessa.

Määritelmä 9.1. Luonnollinen luku $p \neq 1$ on *alkuluku*, jos kaikilla $m, n \in \mathbb{N}$, joille $mn = p$ pätee $m = 1$ tai $n = 1$.

Esimerkki 9.2. Luvut $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$ ovat alkulukuja.

Kokonaislukuja käsiteltäessä merkintä p varataan usein alkuluvuille. Tämä johtuu siitä, että alkuluku on englanniksi prime, saksaksi Primzahl, ranskaksi nombre premier.

Propositio 9.3. *Jokainen nollasta poikkeava kokonaisluku $q \in \mathbb{Z} - \{0\}$ voidaan esittää alkulukujen tulona muodossa*

$$q = (-1)^{m(q)} \prod_p p^{a_p(q)},$$

missä $m(q) \in \{0, 1\}$ ja $a_p(q) \in \mathbb{N}$ kaikille alkuluvuille p ja $a_p(q) \neq 0$ vain äärelliselle joukolle alkulukuja p.

Todistus. Riittää tarkastella positiivisia lukuja. Selvästi väite pätee pienille luvuille $1, 2, 3, \ldots$ ja kaikille alkuluvuille. Oletetaan, että $N \in \mathbb{N}$ on pienin luku, jota ei voi esittää väitetyssä muodossa. Koska N ei erityisesti ole alkuluku, on $m, n \in \mathbb{N} - \{1, N\}$, joille $N = mn$. Mutta nyt $2 \leq m, n < N$, joten luvuilla m ja n on haluttu esitys. Kertomalla nämä esitykset keskenään saadaan luku N esitettyä halutussa muodossa. □

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 $e_1, \ldots e_k \in \mathbb{N} - \{0\}$, sanotaan luvun n *alkutekijäesitykseksi*. Luvut p_i ovat luvun n *alku(luku)tekijöitä*.

Määritelmä 9.4. Jos luku $d \in \mathbb{Z}$ jakaa kokonaisluvut a ja b, niin d on lukujen a ja b *yhteinen tekijä*. Jos $m, n \in \mathbb{Z}$ ja $d \in \mathbb{N}$ on lukujen m ja n yhteinen tekijä, jonka jokainen lukujen m ja n yhteinen tekijä jakaa, niin d on lukujen m ja n *suurin yhteinen tekijä*, merkitään $d = \mathrm{syt}(m, n)$.

Jos $\mathrm{syt}(m, n) = 1$, sanotaan, että luvut m ja n ovat *suhteellisia alkulukuja* ja että m ja n ovat *keskenään jaottomia*.

Seuraavat jaollisuuden perusominaisuudet on helppo tarkastaa.

Propositio 9.5. *Kaikilla $a, b, c \in \mathbb{Z}$ on seuraavat ominaisuudet:*

(1) $a \mid a$.

(2) Jos $a \mid b$ ja $b \mid a$, niin $a = \pm b$.

(3) Jos $a \mid b$ ja $b \mid c$, niin $a \mid c$.

(4) Jos $a \mid b$ ja $a \mid c$, niin $a \mid b + c$.

Todistus. Harjoitustehtävä 9.2. □

Esimerkki 9.6. (a) Luvun 12 tekijät ovat $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6$ ja luvun 30 tekijät ovat $\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30$. Lukujen 12 ja 30 yhteiset tekijät ovat siis $\pm 1, \pm 2, \pm 3, \pm 6$ ja $\mathrm{syt}(12, 30) = 6$.

(b) Peräkkäiset kokonaisluvut ovat keskenään jaottomia. Olkoon $n \in \mathbb{N} - \{0\}$ ja olkoon $d \in \mathbb{N}$ lukujen n ja $(n+1)$ jakaja. Koska Proposition 9.5(4) perusteella d jakaa luvun $(n+1) - n = 1$, niin on oltava $d = 1$. Luvuilla n ja $n+1$ ei siis ole muita positiivisia yhteisiä tekijöitä kuin 1, joten $\mathrm{syt}(n, n+1) = 1$.

Tähän mennessä tekemiemme havaintojen perusteella voidaan todistaa tärkeä huomio alkulukujen joukosta:

Lause 9.7. *Alkulukuja on äärettömän monta.*

Todistus. Harjoitustehtävä 9.3 □

Propositio 9.8. *Olkoot $m, n \in \mathbb{Z} - \{0\}$. Jos $\langle m, n\rangle = \langle d\rangle$, niin $d = \pm\,\mathrm{syt}(m, n)$.*

Todistus. Luku d on lukujen m ja n yhteinen tekijä, koska $m, n \in \langle d\rangle$. Olkoon $e \neq 0$ lukujen m ja n yhteinen tekijä. Koska $d \in \langle m, n\rangle$, on luvut $r, s \in \mathbb{Z}$ siten, että

$$rm + sn = d.$$

Siispä Proposition 9.5 (4) nojalla $e \mid d$. □

Seuraus 9.9. *Nollasta poikkeavilla kokonaisluvuilla on suurin yhteinen tekijä.*

Todistus. Proposition 5.16 mukaan kaikki kokonaislukujen additiivisen ryhmän aliryhmät ovat syklisiä, joten on $d \in \mathbb{N}$ siten, että $\langle d\rangle = \langle m, n\rangle$. Väite seuraa siis Propositiosta 9.8. □

Suurin yhteinen tekijä voidaan määritellä vastaavasti myös useammalle kokonaisluvulle. Käytämme hyödyksi tietoa, että lukujen $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, virittämä aliryhmä $\langle a_1, a_2, \ldots, a_n\rangle < (\mathbb{Z}, +)$ on Proposition 5.16 nojalla syklinen.

Määritelmä 9.10. Olkoot $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Aliryhmän $\langle a_1, a_2, \ldots, a_n\rangle < (\mathbb{Z}, +)$ virittäjä $d \in \mathbb{N}$ on lukujen $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ *suurin yhteinen tekijä*.

On helppo tarkastaa, että esimerkiksi $\mathrm{syt}(6, 10, 15) = 1$.

Proposition 9.8 todistuksessa huomattiin, että kokonaislukujen $m, n \in \mathbb{Z}$ suurin yhteinen tekijä d voidaan esittää sopivien kokonaislukujen $r, s \in \mathbb{Z}$ avulla muodossa

$$d = rm + sn. \tag{6}$$

Yhtälöä (6) kutsutaan *Bezout'n yhtälöksi*. Huomaa, että Proposition 9.8 nojalla $\mathrm{syt}(m, n) = 1$, jos on $r, s \in \mathbb{Z}$, joille pätee $rm + sn = 1$.

Osoitamme seuraavaksi, että Proposition 9.3 antama alkulukuesitys on yksikäsitteinen. Todistuksessa käytetään seuraavia jaollisuustuloksia, jotka pätevät keskenään jaottomille luvuille. Todistukset havainnollistavat Bezout'n yhtälön hyödyllisyyttä.

Propositio 9.11. *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 $\mathrm{syt}(a, b) = 1$, 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 $cxa + ybc = c$. □

Proposition 9.11 väitteet eivät päde ilman oletusta keskinäisestä jaottomuudesta. Tämä on helppo todeta esimerkiksi kohdan (1) tapauksessa huomaamalla, että 2 jakaa luvun 2 mutta $2 \cdot 2 = 4$ ei jaa lukua 2.

Lemma 9.12 (Eukleideen lemma)**.** *Olkoon p alkuluku ja olkoot $a, b \in \mathbb{Z}$. Jos $p \mid (ab)$, niin $p \mid a$ tai $p \mid b$. Jos $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ ja $p \mid a_1 \cdots a_n$, niin $p \mid a_i$ jollain $i \in \{1, 2, \ldots, n\}$.*

Todistus. Oletetaan, että alkuluku p jakaa tulon ab. Jos p ei jaa lukua a, niin $\text{syt}(a, p) = 1$. Proposition 9.11(2) perusteella $p \mid b$. Yleinen tapaus todistetaan induktiolla. □

Nyt voimme täydentää Proposition 9.3 tuloksen kokonaislukujen aritmetiikan keskeiseksi tulokseksi.

Lause 9.13 (Aritmetiikan peruslause)**.** *Jokainen nollasta poikkeava kokonaisluku $q \in \mathbb{Z} - \{0\}$ voidaan voidaan esittää alkulukujen äärellisenä tulona muodossa*

$$q = (-1)^{m(q)} \prod_p p^{a_p(q)},$$

missä $m(q) \in \{0, 1\}$ ja $a_p(q) \in \mathbb{N}$ kaikille alkuluvuille p. Tämä esitys on tekijöiden järjestystä vaille yksikäsitteinen.

Todistus. Propositiossa 9.3 osoitettiin, että q voidaan esittää väitteen mukaisen tulona. Osoitetaan yksikäsitteisyys. Riittää käsitellä positiivisia lukuja. Oletetaan, että

$$q = p_1 \cdots p_k = q_1 \cdots q_s, \tag{7}$$

missä p_i ja $q_j$ovat alkulukuja kaikilla $1 \leq i \leq k$ ja $1 \leq j \leq s$.

Koska $p_1 \mid q$, niin Lemman 9.12 perusteella se jakaa luvun q_j jollain $j = 1, \ldots, s$. Numeroimalla tekijät $q_1, \ldots, q_s$ tarvittaessa uudelleen voidaan olettaa, että $p_1 \mid q_1$. Koska p_1 ja q_1 ovat alkulukuja, niin on $p_1 = q_1$. Supistamalla tekijä p_1 saadaan yhtälöstä (7)

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

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

Sovellamme oppimaamme jäännösluokkarenkaan $\mathbb{Z}/q\mathbb{Z}$ additiivisen ryhmän ja yksiköiden ryhmän (eli multiplikatiivisen ryhmän) ominaisuuksien tarkasteluun. Samalla saamme todistettua kaksi lukuteorian klassista tulosta, Fermat'n pienen lauseen ja kiinalaisen jäännöslauseen.

Seuraus 9.14. *Olkoon $q \geq 2$. Tällöin $(\mathbb{Z}/q\mathbb{Z}, +) = \langle a + q\mathbb{Z} \rangle$, jos ja vain jos $syt(a, q) = 1$.*

Todistus. Harjoitustehtävä 9.7. □

Propositio 9.15. *Olkoon $q \geq 2$. Tällöin $a + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ on yksikkö, jos ja vain jos* $\text{syt}(a, q) = 1$. *Jos p on alkuluku ja $a \not\equiv 0 \mod p$, niin $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Erityisesti $\#(\mathbb{Z}/p\mathbb{Z})^\times = p - 1$.*

Todistus. Jäännösluokka $a + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ on yksikkö, jos ja vain jos on $b \in \mathbb{Z}$, jolle pätee

$$1 + q\mathbb{Z} = (a + q\mathbb{Z})(b + q\mathbb{Z}) = ab + q\mathbb{Z}\,.$$

Tämä on yhtäpitävää ehdon $ab \equiv 1 \mod q$ kanssa, joka taas pätee, jos ja vain jos on $c \in \mathbb{Z}$, jolle $ab = 1 + cq$. Tämä taas on Proposition 9.8 ja Seurauksen 9.9 nojalla yhtäpitävää sen kanssa, että $\mathrm{syt}(a, q) = 1$.

Jos p on alkuluku, niin $\mathrm{syt}(a, p) = 1$ kaikille $a \in \{1, 2, \ldots, p-1\}$, joten renkaan $\mathbb{Z}/p\mathbb{Z}$ kaikki nollasta poikkeavat alkiot ovat yksiköitä. □

Lause 9.16 (Fermat'n pieni lause)**.** *Olkoon p alkuluku. Kaikille $a \in \mathbb{Z}$ pätee $a^p \equiv a \mod p$.*

Todistus. Seuraa Propositioista 9.15 ja 7.9. □

Jos $a, b \in \mathbb{Z} - q\mathbb{Z}$ ja $ab \equiv 0 \mod q$, niin jäännösluokkarenkaassa $\mathbb{Z}/q\mathbb{Z}$ pätee $a + q\mathbb{Z} \neq 0$, $b + q\mathbb{Z} \neq 0$ ja

$$(a + q\mathbb{Z})(b + q\mathbb{Z}) = 0.$$

Tällöin sanotaan, että $a + q\mathbb{Z}$ ja $b + q\mathbb{Z}$ ovat *nollan jakajia* renkaassa $\mathbb{Z}/q\mathbb{Z}$.

Propositio 9.17. *Kongruenssirenkaan $\mathbb{Z}/q\mathbb{Z}$ yksiköt eivät ole nollan jakajia.*

Todistus. Jos $a + q\mathbb{Z}$ on yksikkö, niin Proposition 9.15 nojalla $\mathrm{syt}(a, q) = 1$. Jos $(a + q\mathbb{Z})(b + q\mathbb{Z}) = 0$, niin q jakaa tulon ab. Proposition 9.11 (2) nojalla $q \mid b$, joten $b + q\mathbb{Z} = 0$. □

Propositio 9.18. *Olkoon $q \geq 2$. Alkio $a + q\mathbb{Z} \in (\mathbb{Z}/q\mathbb{Z}) - \{0\}$ on nollan jakaja, jos ja vain jos* $\mathrm{syt}(a, q) > 1$. *Jos q ei ole alkuluku, niin renkaassa $\mathbb{Z}/q\mathbb{Z}$ on nollan jakajia.*

Todistus. Proposition 9.15 ja Lemman 9.17 nojalla riittää osoittaa, että $a + q\mathbb{Z}$ on nollan jakaja, jos $2 \leq \mathrm{syt}(a, q) < q$. Jos $2 \leq f = \mathrm{syt}(a, q) < q$, niin $a = fk$ ja $q = f\ell$ joillain keskenään jaottomilla $k, \ell \in \mathbb{Z}$. Tällöin

$$(a + q\mathbb{Z})(\ell + q\mathbb{Z}) = fk\ell + q\mathbb{Z} = q\mathbb{Z} = 0\,,$$

joten $a + q\mathbb{Z}$ on nollan jakaja.

Jos $q \geq 2$ ei ole alkuluku,niin $q = cd$ joillain $c, d \in \mathbb{Z} - \{\pm 1\}$. Erityisesti q ei jaa kumpaakaan tekijäänsä c ja d. Siis $c + q\mathbb{Z}$ ja $d + q\mathbb{Z}$ ovat nollan jakajia renkaassa $\mathbb{Z}/q\mathbb{Z}$. □

Seuraus 9.19. *Renkaan $\mathbb{Z}/q\mathbb{Z}$ nollasta poikkeava alkio on joko nollan jakaja tai yksikkö.*

Todistus. Seuraa Propositioista 9.18 ja 9.15. □

Esimerkki 9.20. Renkaan $\mathbb{Z}/8\mathbb{Z}$ yksiköiden ryhmä

$$(\mathbb{Z}/8\mathbb{Z})^\times = (\{1 + 8\mathbb{Z}, 3 + 8\mathbb{Z}, 5 + 8\mathbb{Z}, 7 + 8\mathbb{Z}\}, \cdot)$$

on isomorfinen Kleinin neliryhmän $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ kanssa: Kertolasku on kommutatiivinen ja pätee

$$1 = 1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \mod 8\,,$$
$$3 \cdot 5 \equiv 7 \mod 8\,,$$
$$3 \cdot 7 \equiv 5 \mod 8$$

ja

$$5 \cdot 7 \equiv 3 \mod 8\,.$$

Kuvaus $1 + 8\mathbb{Z} \mapsto (0, 0)$, $3 + 8\mathbb{Z} \mapsto (1, 0)$, $5 + 8\mathbb{Z} \mapsto (0, 1)$, $7 + 8\mathbb{Z} \mapsto (1, 1)$ on siis ryhmäisomorfismi ryhmien $(\mathbb{Z}/8\mathbb{Z})^\times$ ja $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ välillä.

Seurauksen 9.19 nojalla renkaan $\mathbb{Z}/8\mathbb{Z}$ nollan jakajat ovat $2+8\mathbb{Z}$, $4+8\mathbb{Z}$ ja $6+8\mathbb{Z}$. Tämä on myös helppo tarkastaa laskemalla

$$(2 + 8\mathbb{Z})(4 + 8\mathbb{Z}) = 0 = (6 + 8\mathbb{Z})(4 + 8\mathbb{Z})\,.$$

Propositio 9.21. *Olkoot* $q_1, q_2, \ldots, q_N \in \mathbb{N} - \{0,1\}$ *siten, että* $\operatorname{syt}(q_i, q_j) = 1$ *kaikilla* $i, j \in \{1, 2, \ldots, N\}$, $i \neq j$. *Tällöin ryhmät* $\prod_{i=1}^{N} \mathbb{Z}/q_i\mathbb{Z}$ *ja* $\mathbb{Z}/(\prod_{i=1}^{N} q_i)\mathbb{Z}$ *ovat isomorfiset.*

Todistus. Olkoon $\Phi\colon \mathbb{Z} \to \prod_{i=1}^{N} \mathbb{Z}/q_i\mathbb{Z}$ ryhmähomomorfismi

$$\Phi(k) = (k + q_1\mathbb{Z}, k + q_2\mathbb{Z}, \ldots, k + q_N\mathbb{Z})\,.$$

Jos $\Phi(k) = 0$, niin $q_i | k$ kaikilla $i \in \{1, 2, \ldots, N\}$. Koska $\operatorname{syt}(q_i, q_j) = 1$ kaikilla $i, j \in \{1, 2, \ldots, N\}$, $i \neq j$, niin Proposition 9.11 (1) yleistys N luvun tulolle antaa $\ker \Phi = (\prod_{i=1}^{N} q_i)\mathbb{Z}$. Siis Φ määrää injektiivisen homomorfismin

$$\Psi\colon \mathbb{Z}/(\prod_{i=1}^{N} q_i)\mathbb{Z} \to \prod_{i=1}^{N} \mathbb{Z}/q_i\mathbb{Z}\,.$$

Koska homomorfismin Ψ määrittely- ja maalijoukot ovat äärellisiä ryhmiä, joilla on sama kertaluku, Ψ on isomorfismi. □

Propositio 9.21 antaa seurauksena lukuteorian tuloksen, joka tunnettiin Kiinassa jo 400–luvulla.

Seuraus 9.22 (Kiinalainen jäännöslause, Sun Tzun lause)**.** *Olkoot* $q_1, q_2, \ldots, q_N \in \mathbb{N} - \{0,1\}$ *suhteellisia alkulukuja ja olkoot* $a_1, a_2, \ldots, a_N \in \mathbb{Z}$. *Tällöin kongruenssiyhtälöryhmällä*

$$x \equiv a_i \mod q_i \quad \textit{kaikilla} \quad i \in \{1, 2, \ldots, N\}$$

on ratkaisu, joka on yksikäsitteinen modulo $\prod_{i=1}^{N} q_i$. □

Kiinalainen jäännöslause takaa sen, että tarkasteltavalla kongruenssiyhtälöryhmällä on ratkaisu, ja se kertoo, missä mielessä ratkaisu on yksikäsitteinen. Se ei kuitenkaan anna keinoja yhtälöryhmän ratkaisemiseen. Ratkaisussa voidaan hyödyntää Eukleideen algoritmia, jota käsitellään lukuteorian alkeiskursseilla. Ratkaisun voi toki yksinkertaisissa tapauksissa löytää alkeellisemmallakin kokeilumenetelmällä.

Esimerkki 9.23. (1) Propositio 9.21 antaa uuden ratkaisun Harjoitustehtävälle 5.7 koska 2 ja 3 ovat alkulukuja.

(b) Kiinalaisen jäännöslauseen mukaan kongruenssiyhtälöryhmällä

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 1 \mod 3 \\ x \equiv 1 \mod 5 \\ x \equiv 0 \mod 7 \end{cases}$$

on yksikäsitteinen ratkaisu $x = 91$ modulo 210.

Kongruenssiyhtälöryhmällä

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 1 \mod 4 \\ x \equiv 1 \mod 5 \\ x \equiv 0 \mod 7 \end{cases}$$

on yksikäsitteinen ratkaisu $x = 301 = 91 + 210$ modulo 420.

Harjoitustehtäviä.

9.1. Olkoon G ryhmä, jonka kertaluku on alkuluku. Osoita, että G on syklinen.

9.2. Osoita, että kaikilla $a, b, c \in \mathbb{Z}$ on seuraavat ominaisuudet:
(1) $a \mid a$.
(2) Jos $a \mid b$ ja $b \mid a$, niin $a = \pm b$.
(3) Jos $a \mid b$ ja $b \mid c$, niin $a \mid c$.
(4) Jos $a \mid b$ ja $a \mid c$, niin $a \mid b + c$.

9.3. Osoita, että alkulukuja on äärettömän monta.

9.4. Määritä $\langle 30, 42, 70, 105\rangle \leq (\mathbb{Z}, +)$.

9.5. Olkoot $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Oletetaan, että $p \mid a_1 \cdots a_n$. Osoita, että $p \mid a_i$ jollain $i \in \{1, 2, \ldots, n\}$.

9.6. Osoita, että rationaalilukujen multiplikatiivinen ryhmä ei ole syklinen.

9.7. Osoita, että $(\mathbb{Z}/q\mathbb{Z}, +) = \langle a + q\mathbb{Z}\rangle$, jos ja vain jos $\text{syt}(a, q) = 1$.

9.8. Määritä renkaiden $\mathbb{Z}/6\mathbb{Z}$ ja $\mathbb{Z}/10\mathbb{Z}$ ja $\mathbb{Z}/101\mathbb{Z}$ yksiköt.

9.9. Osoita, että renkaiden $\mathbb{Z}/6\mathbb{Z}$ ja $\mathbb{Z}/10\mathbb{Z}$ yksiköiden ryhmät ovat syklisiä ryhmiä.

9.10. Määritä renkaan $\mathbb{Z}/9\mathbb{Z}$ yksiköt ja nollan jakajat. Onko renkaan $\mathbb{Z}/9\mathbb{Z}$ yksiköiden ryhmä syklinen?

9.11. Määritä renkaan $\mathbb{Z}/12\mathbb{Z}$ yksiköt ja nollan jakajat. Minkä kurssilla aiemmin käsitellyn ryhmän kanssa ryhmä $(\mathbb{Z}/12\mathbb{Z})^\times$ on isomorfinen?

9.12. Olkoon p alkuluku, $p \equiv 3 \mod 4$. Osoita, että $-1 + p\mathbb{Z}$ ei ole minkään alkion neliö yksiköiden ryhmässä $(\mathbb{Z}/p\mathbb{Z})^\times$.

[3]Vihje: Olkoot $p_1, p_2, \ldots, p_n$ alkulukuja. Mitä voit päätellä luvusta $p_1 p_2 \cdot \cdots \cdot p_n + 1$?
[6]Vihje: Aritmetiikan peruslause auttaa.
[12]Vihje: Jos $-1 + p\mathbb{Z} = \alpha^2$, mikä on alkion $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$ kertaluku?

Tässä luvussa tarkastelemme pääasiassa kahta tärkeää kommutatiivisten renkaiden luokkaa, kuntia ja kokonaisalueita. Todistamme joitakin näihin luokkiin kuuluvien renkaiden perusominaisuuksia. Käsittelemme myös jaollisuutta kokonaisalueessa. Tämä teoria yleistää Luvussa 9 tehtyjä kokonaislukujen jaollisuustuloksia yleisempään tilanteeseen.

Määritelmä 10.1. Olkoon K rengas, jossa on ainakin kaksi alkiota. Jos kaikki renkaan K nollasta poikkeavat alkiot ovat yksiköitä, niin K on *jakorengas*. Kommutatiivinen jakorengas on *kunta*. Jakorengas, joka ei ole kunta on *vino kunta*. Jos K ja K' ovat kuntia, rengashomomorfismia $\phi\colon K \to K'$ sanotaan *kuntahomomorfismiksi*.

Esimerkki 10.2. (a) Renkaassa $\mathbb{Z}$ on äärettömän monta alkiota mutta sen ainoat yksiköt ovat ± 1. Siis $\mathbb{Z}$ ei ole jakorengas eikä siis kunta.

(b) $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat kuntia.

(c) Olkoon R rengas, jossa on vähintään kaksi alkiota. Matriisirengas $\mathrm{M}_n(R)$ ei ole jakorengas, kun $n \geq 2$, koska monella matriisilla ei ole käänteismatriisia. Esimerkiksi $\mathrm{M}_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R})$ ja $\mathrm{M}_n(\mathbb{Z})^\times = \mathrm{SL}_n(\mathbb{Z})$.

Kuntaominaisuudet säilyvät homomorfismeissa:

Propositio 10.3. *Olkoon K kunta ja olkoon R rengas, jossa on ainakin kaksi alkiota. Olkoon $\phi\colon K \to R$ rengashomomorfismi. Tällöin ϕ on injektio ja $\phi(K)$ on kunta.*

Todistus. Seurauksen 8.26 mukaan $\phi(K)$ on rengas, joka on Proposition 1.17 mukaan kommutatiivinen. Koska ϕ on rengashomomorfismi ja renkaassa R on vähintään kaksi alkiota, pätee Proposition 8.4 mukaan

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

Siis renkaassa $\phi(K)$ on vähintään kaksi alkiota. Yksikön kuva on yksikkö Proposition 4.12 todistuksen nojalla: Jos $u \in K^\times = K - \{0\}$, niin

$$\phi(u)\phi(u^{-1}) = \phi(uu^{-1}) = \phi(1) = 1\,.$$

Siis renkaan $\phi(K)$ nollasta poikkeavat alkiot ovat yksiköitä, joten $\phi(K)$ on kunta.

Olkoon $a \in \ker\phi$. Jos $a \neq 0$, niin

$$1 = \phi(1) = \phi(aa^{-1}) = 0\,\phi(a^{-1}) = 0\,,$$

mikä on mahdotonta. Siis ϕ on injektio Proposition 8.18 nojalla. □

Jos K_1 ja K_2 ovat kuntia ja K_2 on kunnan K_1 alirengas, niin K_2 on kunnan K_1 *alikunta* ja K_1 on kunnan K_2 *laajennus*. Selvästi $\mathbb{Q}$ on reaalilukujen kunnan $\mathbb{R}$ ja kompleksilukujen kunnan $\mathbb{C}$ alikunta.

Esimerkki 10.4. Olkoon $d \in \mathbb{Z}$ kokonaisluku, joka ei ole jaollinen minkään alkuluvun neliöllä. Olkoot

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \subset \mathbb{R},$$

kun $d \in \mathbb{N}$ ja

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \subset \mathbb{C},$$

kun $d \notin \mathbb{N}$. On helppo osoittaa, että $\mathbb{Q}(\sqrt{d})$ on kompleksilukujen kunnan alikunta ja rationaalilukujen kunnan laajennus. Kunta $\mathbb{Q}(\sqrt{d})$ on kunnan $\mathbb{Q}$ *toisen asteen kuntalaajennus* eli *kvadraattinen lukukunta*. Kunta

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

on *Gaussin rationaalilukujen kunta*. Kokonaisalueen

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

alkioita kutsutaan *Gaussin kokonaisluvuiksi*.

Esimerkki 10.5. *Hamiltonin kvaterniot* on joukko

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a, b \in \mathbb{C} \right\} \subset \mathrm{M}_2(\mathbb{C})$$

varustettuna renkaasta $\mathrm{M}_2(\mathbb{C})$ indusoiduilla laskutoimituksilla, jotka siis ovat matriisien yhteenlasku ja matriisien kertolasku. Proposition 8.23 avulla on helppo osoittaa, että $\mathbb{H}$ on renkaan $\mathrm{M}_2(\mathbb{C})$ alirengas. Lisäksi

$$\det \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = |a|^2 + |b|^2,$$

joten jokainen $A \in \mathbb{H} - \{0\}$ on kääntyvä matriisi. Itse asiassa kaikki nollasta poikkeavat alkiot ovat yksiköitä, koska

$$\frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \in \mathbb{H}$$

ja pätee

$$\frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = I_2.$$

Siis $\mathbb{H}$ on jakorengas.

Jakorengas $\mathbb{H}$ ei ole kommutatiivinen sillä esimerkiksi

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

Siis Hamiltonin kvaterniot on vino kunta.

Injektiivinen kuvaus $\phi\colon \mathbb{C} \to \mathbb{H}$, $\phi(z) = \mathrm{diag}(z, \bar{z})$ on kuntahomomorfismi, joten voimme samastaa sen kuvajoukon

$$\phi(\mathbb{C}) = \left\{ \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix} : z \in \mathbb{C} \right\} \subset \mathrm{M}_2(\mathbb{C})$$

kompleksilukujen kunnan kanssa. Kvaternioita käsitellessä onkin tapana käyttää esimerkiksi merkintöjä

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Tällöin

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \tag{8}$$

ja

$$\mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \quad \mathbf{ki} = \mathbf{j} = -\mathbf{ik}, \quad \mathbf{jk} = \mathbf{i} = -\mathbf{kj}. \tag{9}$$

Matriisit 1, $\mathbf{i}$, $\mathbf{j}$ ja $\mathbf{k}$ virittävät avaruuden $\mathbb{H}$ neliulotteisena reaalisena vektoriavaruutena, joten Hamiltonin kvaterniot voidaan esittää reaalisina lineaarikombinaatioina

$$x = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k},$$

$x_0, x_1, x_2, x_3 \in \mathbb{R}$, joilla voi laskea kuten kompleksiluvuilla huomioiden laskusäännöt (8) ja (9).

Jaollisuus määritellään kommutatiivisessa renkaassa samalla tavalla kuin kokonaislukujen tapauksessa: Jos K on kommutatiivinen rengas ja $a, b, c \in K$ siten, että $ab = c$, niin a ja b ovat alkion c *tekijöitä*. Tällöin luvut a ja b *jakavat* luvun c, mistä käytetään merkintää $a \mid c$ ja vastaavasti $b \mid c$.

Seuraavat jaollisuuden perusominaisuudet on helppo tarkastaa kuten kokonaislukujen tapauksessa.

Propositio 10.6. *Olkoon K kommutatiivinen rengas. Tällöin*

(1) $a \mid a$ kaikille $a \in K$.

(2) Jos $a \mid b$ ja $b \mid a$, niin $a = ub$ jollain $u \in K^\times$.

(3) Jos $a \mid b$ ja $b \mid c$, niin $a \mid c$.

(4) Jos $a \mid b$ ja $a \mid c$, niin $a \mid b + c$.

Todistus. Harjoitustehtävä 10.2. □

Määritelmä 10.7. Olkoon R rengas, jossa on vähintään 2 alkiota. Jos $a, b \in R$, $a, b \neq 0$ ja $ab = 0$, niin a ja b ovat *nollan jakajia*. Kommutatiivinen rengas R, jossa ei ole nollan jakajia, on *kokonaisalue*.

Esimerkki 10.8. (a) Kokonaislukujen rengas on kokonaisalue.

(b) Proposition 9.15 todistuksessa huomasimme, että jäännösluokkarengas $\mathbb{Z}/q\mathbb{Z}$ ei ole kokonaisalue, kun $q \geq 4$ ei ole alkuluku: Jos $q = ab$ joillekin $a, b \in \mathbb{N} - \{0, 1\}$, niin $a + q\mathbb{Z}, b + q\mathbb{Z} = 0$ ja $(a + q\mathbb{Z})(b + q\mathbb{Z}) = 0$. Erityisesti siis kokonaisalueen kuva rengashomomorfismissa ei välttämättä ole kokonaisalue.

(c) Olkoon $n \geq 2$ ja olkoon R rengas. Jos $A, B \in \mathrm{M}_n(R)$ ovat neliömatriiseja, joiden ainoat nollasta poikkeavat kertoimet ovat A_{11} ja B_{nn}, niin $AB = 0$. Siis matriisit A ja B ovat nollan jakajia.

Seuraava tulos on yhteenveto tuloksista, jotka koskevat jäännösluokkarenkaan $\mathbb{Z}/q\mathbb{Z}$ ominaisuuksien riippuvuutta luvusta q.

Lause 10.9. *Seuraavat väitteet ovat yhtäpitäviä:*

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

Todistus. Seuraa Propositioista 9.15 ja 9.18. □

Sanomme, että renkaassa R pätee *kertolaskun supistussääntö*, jos $b = c$ aina, kun jollekin $a \in R - \{0\}$ pätee $ab = ac$ tai $ba = ca$. Renkaan kertolaskun supistussääntö poikkeaa hieman Luvussa 4 tarkastellusta laskutoimituksen supistussäännöstä, koska $0\,a = 0$ kaikille $a \in R$.

Propositio 10.10. *Kommutatiivinen rengas K on kokonaisalue, jos ja vain jos kertolaskun supistussääntö pätee renkaassa K.*

Todistus. Harjoitustehtävä 10.1 □

Propositio 10.11. *Kokonaisalueen karakteristika on 0 tai alkuluku.*

Todistus. Olkoon R rengas, jonka karakteristika on $\chi(R) = ab$, missä $a, b \neq 0$. Proposition 8.16 nojalla on täsmälleen yksi rengashomomorfismi $\phi\colon \mathbb{Z} \to R$. Karakteristikan määritelmän mukaan $\phi(ab) = 0$. Nyt $\phi(a), \phi(b) \neq 0$ ja $\phi(a)\phi(b) = \phi(ab) = 0$, joten R ei ole kokonaisalue. □

Propositio 10.12. *Yksikkö ei ole nollan jakaja.*

Todistus. Olkoon a yksikkö ja oletetaan, että $ab = 0$. Silloin $b = a^{-1}\,0 = 0$. Vastaavasti nähdään, että $b = 0$, jos $ba = 0$. □

Kongruenssiluokkien renkaassa $\mathbb{Z}/q\mathbb{Z}$ jokainen nollasta poikkeava alkio on joko yksikkö tai nollan jakaja. Vastaava tulos ei päde renkaille yleisesti, sillä kokonaislukujen renkaassa ei ole nollan jakajia ja siinä on ainoastaan kaksi yksikköä ± 1.

Seuraus 10.13. *Jakorenkaassa ei ole nollan jakajia. Erityisesti kunta on kokonaisalue.* □

Lause 10.14. *Äärellinen kokonaisalue on kunta.*

Todistus. Olkoon E kokonaisalue ja olkoon $a \in E - \{0\}$. Kuvaus $\ell_a : E \to E$, $\ell_a(x) = ax$ on injektio Proposition 10.10 nojalla. Kun oletamme lisäksi, että E on äärellinen, niin kuvaus ℓ_a on myös surjektio. Tällöin on $\bar{a} \in E$, jolle $a\bar{a} = 1$. Koska E on kommutatiivinen, $\bar{a} = a^{-1}$. □

Seuraava samanhenkinen tulos on vaikeampi todistaa:

Lause 10.15 (Wedderburnin lause)**.** *Äärellinen jakorengas on kunta.*

Todistus. Katso esimerkiksi [War, Theorem 39.9]. □

Yleistämme seuraavaksi Esimerkissä 3.12 käsitellyn rationaalilukujen konstruktion kokonaisalueille: Olkoon K kokonaisalue. Määrittelemme ekvivalenssirelaation $\sim$ joukossa $K \times (K - \{0\})$ asettamalla $(a, b) \sim (c, d)$, jos ja vain jos $ad = bc$. Merkitsemme alkion (a, b) ekvivalenssiluokkaa $\frac{a}{b}$. Varustamme tulojoukon $K \times (K - \{0\})$ yhteenlaskulla

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

ja tekijöidensä kertolaskujen tulolaskutoimituksella

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

Kokonaisalueen K laskutoimitusten assosiatiivisuudesta ja kommutatiivisuudesta seuraa, että nämä laskutoimitukset ovat assosiatiivisia ja kommutatiivisia. Samaan tapaan kuin rationaaliluvuille tehtiin Harjoitustehtävässä 3.6 voidaan osoittaa, että yllä määritellyt joukon $K \times (K - \{0\})$ laskutoimitukset ovat yhteensopivia ekvivalenssirelaation $\sim$ kanssa.

Kokonaisalueen K *murtokunta* on

$$\mathscr{Q}(K) = K \times (K - \{0\})/\!\sim$$

varustettuna tekijälaskutoimituksilla

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

ja

$$\frac{a}{b}\,\frac{c}{d} = \frac{ac}{bd}\,.$$

Tekijälaskutoimitukset ovat assosiatiivisia ja kommutatiivisia Proposition 3.9 nojalla. Kertolaskun distributiivisuus yhteenlaskun suhteen on helppo tarkastaa:

$$\frac{a}{b}\Big(\frac{c}{d} + \frac{e}{f}\Big) = \frac{a}{b}\Big(\frac{cf + de}{df}\Big) = \frac{acf + ade}{bdf} = \frac{acbf + aebd}{b^2df} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{d}{e}\,.$$

Yhteenlaskun neutraalialkio on $\frac{0}{1} = 0$ ja kertolaskun neutraalialkio on $\frac{1}{1} = 1$. Lisäksi jokaiselle $\frac{a}{b} \in \mathscr{Q}(K)$ pätee $\frac{a}{b} + \frac{-a}{b} = 0$ ja jokaiselle $\frac{a}{b} \in \mathscr{Q}(K) - \{0\}$ pätee $\frac{b}{a} \in \mathscr{Q}(K)$ ja $\frac{a}{b}\frac{b}{a} = \frac{ab}{ab} = 1$. Murtokunta on siis kunta.

Propositio 10.16. *Jos kunnalla k on alirengas, joka on isomorfinen kokonaisalueen K kanssa, niin kunnalla k on alikunta, joka on isomorfinen kokonaisalueen K murtokunnan kanssa.*

Todistus. Oletetaan, että $K \subset k$. Jokaisella $b \in K - \{0\} \subset k - \{0\}$ on käänteisalkio $b^{-1} \in k - \{0\}$. Kuvaus $\phi\colon \mathscr{Q}(K) \to k$, $\frac{a}{b} \mapsto ab^{-1}$ on kuntahomomorfismi, sillä

$$\phi\big(\frac{a}{b} + \frac{c}{d}\big) = \phi\big(\frac{ad+bc}{bd}\big) = (ad+bc)(bd)^{-1} = ab^{-1} + cd^{-1} = \phi\big(\frac{a}{b}\big) + \phi\big(\frac{c}{d}\big)\,,$$

$$\phi\big(\frac{a}{b}\frac{c}{d}\big) = \phi\big(\frac{ac}{bd}\big) = (ac)(bd)^{-1} = ab^{-1}cd^{-1} = \phi\big(\frac{a}{b}\big)\phi\big(\frac{c}{d}\big)$$

ja $\phi(\frac{1}{1}) = 1$. Siis Proposition 10.3 nojalla ϕ on injektio ja $\phi(\mathscr{Q}(K))$ on etsitty alikunta. □

Kokonaisalueen K murtokunta on siis pienin kunta, joka sisältää isomorfisen kopion kokonaisalueesta K. Erityisesti, jos k on kunta, niin kunnat k ja $\mathscr{Q}(k)$ ovat isomorfisia.

Seuraus 10.17. *Jos kunnan k karakteristika on 0, niin sillä on alikunta, joka on isomorfinen rationaalilukujen kunnan kanssa. Jos kunnan k karakteristika on alkuluku p, niin sillä on alikunta, joka on isomorfinen kunnan $\mathbb{Z}/p\mathbb{Z}$ kanssa.* □

Esimerkki 10.18. Murtokunta $\mathscr{Q}(\mathbb{Z}) = \mathbb{Q}$ on isomorfinen murtokunnan $\mathscr{Q}(\mathbb{Q})$ kanssa. Murtokunta $\mathscr{Q}(\mathbb{Z}/p\mathbb{Z})$ on isomorfinen kunnan $\mathbb{Z}/p\mathbb{Z}$ kanssa jokaisella alkuluvulla p.

Määritelmä 10.19. Olkoon K kunta. Jos $(V, +)$ on kommutatiivinen ryhmä, jossa on määritelty kuvaus $K \times V \to V$, $(\lambda, v) \mapsto \lambda v$, *vakiolla kertominen*, joka toteuttaa ehdot

(1) $\lambda(v + w) = \lambda v + \lambda w$ kaikille $\lambda \in K$ ja $v, w \in V$,
(2) $(\lambda + \mu)v = \lambda v + \mu v$ kaikille $\lambda, \mu \in K$ ja $v \in V$,
(3) $\mu(\lambda v) = (\mu\lambda)v$ kaikille $\lambda, \mu \in K$ ja $v \in V$ ja
(4) $1\, v = v$ kaikille $v \in V$.

niin V varustettuna tällä rakenteella on *K–vektoriavaruus.*

Jos K-vektoriavaruuden V osajoukko $H \subset V$, $H \neq \emptyset$, on vakaa vektoriavaruuden V yhteenlaskun ja vakiolla kertomisen suhteen ja jos se on näillä operaatioilla varustettuna reaalinen vektoriavaruus aliavaruus, niin H on vektoriavaruuden V *(vektori-)aliavaruus.*

Olkoot V ja W K-vektoriavaruuksia. Kuvaus $L\colon V \to W$ on *(K–)lineaarikuvaus*, jos se on homomorfismi kommutatiivisesta ryhmästä $(V, +)$ kommutatiiviseen ryhmään $(W, +)$, jolle pätee $L(\lambda v) = \lambda L(v)$ kaikilla $\lambda \in K$ ja $v \in V$.

Yleisen K-vektoriavaruuden vektoreiden lineaarinen riippumattomuus, kanta ja dimensio määritellään kuten reaalisessa tapauksessa. Erityisesti, jos K-vektoriavaruuden V dimensio on äärellinen, niin sillä on *kanta*, joka on lineaarisesti riippumaton joukko, jonka virittämä aliavaruus on koko V: Jos vektorit $v_1, v_2, \ldots, v_N \in V$ muodostavat K-vektoriavaruuden V kannan, niin jokaiselle $x \in V$ on yksikäsitteiset $x_1, x_2, \ldots, x_N \in K$, joille pätee

$$x = \sum_{i=1}^{N} x_i v_i\,.$$

Lineaarialgebran kursseilla käsitelty reaalisten vektoriavaruuksien ja lineaarikuvausten teoria yleistyy K-kertoimiseen tilanteeseen. Kuntakertoimiseen lineaarialgebraan voi perehtyä monien lineaarialgebran ja algebran kirjojen avulla, esimerkiksi [Gre], [DF], [War].

Propositio 10.20. *Äärellisessä kunnassa on p^q alkiota jollakin alkuluvulla p ja jollakin $q \in \mathbb{N} - \{0\}$.*

Todistus. Olkoon K äärellinen kunta. Tällöin kunnan K karakteristika on p jollain alkuluvulla p ja $\mathbb{Z}/p\mathbb{Z}$ on kunnan K alikunta. Koska Harjoitustehtävän 10.11 nojalla K on äärellinen $\mathbb{Z}/p\mathbb{Z}$-vektoriavaruus, niin sillä on äärellinen kanta. Olkoon kannassa q alkiota. Siis $\mathbb{Z}/p\mathbb{Z}$-vektoriavaruudessa K on yhtä monta alkiota kuin joukossa $(\mathbb{Z}/p\mathbb{Z})^q$. □

Harjoitustehtäviä.

10.1. Osoita, että kommutatiivinen rengas K on kokonaisalue, jos ja vain jos kertolaskun supistussääntö pätee renkaassa K.

10.2. Olkoon K kokonaisalue. Osoita, että
(1) $a \mid a$ kaikille $a \in K$.
(2) Jos $a \mid b$ ja $b \mid a$, niin $a = ub$ jollain $u \in K^\times$.
(3) Jos $a \mid b$ ja $b \mid c$, niin $a \mid c$.
(4) Jos $a \mid b$ ja $a \mid c$, niin $a \mid b + c$.

10.3. Olkoon K kunta ja olkoon $K' \subset K$ vakaa osajoukko, joka on kunta indusoiduilla laskutoimituksilla. Osoita, että kunnan K' yhteenlaskun ja kertolaskun neutraalialkiot ovat samat kuin kunnan K.

10.4. Osoita, että kunnan K osajoukko K' on alikunta, jos ja vain jos
- $\#K' \geq 2$,
- $a - b \in K'$ kaikilla $a, b \in K'$ ja
- $ab^{-1} \in K'$ kaikilla $a, b \in K'$, $b \neq 0$.

10.5. Olkoon
$$K = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{M}_2(\mathbb{R}) \right\}.$$
Osoita, että K varustettuna matriisien yhteen- ja kertolaskulla on kunta. Osoita, että kunta K on isomorfinen kompleksilukujen kunnan kanssa.

10.6. Osoita, että Hamiltonin kvaterniot muodostavat renkaan.

10.7. Osoita, että ei ole kuntahomomorfismia $\phi\colon \mathbb{R} \to \mathbb{Q}$.

10.8. Osoita, että ei ole kuntahomomorfismia $\phi\colon \mathbb{C} \to \mathbb{R}$.

10.9. Sievennä lauseke $(a + b)^p$ kunnassa, jonka karakteristika on p.

10.10. Olkoon K kommutatiivinen rengas, jonka karakteristika on alkuluku p. Olkoon $\phi\colon K \to K$ kuvaus $\phi(a) = a^p$. Osoita, että ϕ on rengashomomorfismi.

10.11. Olkoon L kunnan K alikunta. Osoita, että K on L-vektoriavaruus.

10.12. Osoita, että äärellisessä kunnassa on p^q alkiota jollakin alkuluvulla p ja jollakin $q \in \mathbb{N} - \{0\}$.

10.13. Osoita, että $\mathbb{Z}[i]$ on kokonaisalue ja että $\mathbb{Q}(i)$ on kunta (kompleksilukujen kunnasta indusoiduilla laskutoimituksilla).

10.14. Määritä Gaussin kokonaislukujen yksiköiden ryhmä.

10.15. Osoita, että Gaussin kokonaislukujen murtokunta on isomorfinen Gaussin rationaalilukujen kunnan kanssa.

10.16. Osoita, että

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Z}\},$$

on reaalilukujen renkaan alirengas.

10.17. Osoita, että $\mathbb{Z}[\sqrt{2}]^\times$ on ääretön.

[14]Vihje: Käytä kompleksilukujen modulin ominaisuuksia.

[15]Vihje: Valitse ekvivalenssiluokalle sopiva edustaja.

[17]Vihje: Etsi sopiva yksikkö ja käytä Propositiota 8.8

11. Polynomit

Tässä luvussa tarkastelemme polynomien muodostamia renkaita ja polynomien jaollisuutta käsitteleviä perustuloksia. Teemme luvun alkuun kaksi sopimusta:

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

Symbolille $-\infty$ ei ole määritelty muita operaatioita, käytämme sitä ainoastaan nollapolynomin asteen merkkinä.

Määritelmä 11.1. Olkoon K kommutatiivinen rengas, jossa on vähintään kaksi alkiota. Olkoon $n \in \mathbb{N}$ ja olkoot $a_n, a_{n-1}, \ldots, a_1, a_0 \in K$. Lauseke

$$P(X) = \sum_{k=0}^{n} a_k X^k = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

on *yhden muuttujan K-kertoiminen polynomi*. Luku a_0 on polynomin $P(X)$ *vakiotermi*. Jos ylläolevassa lausekkeessa $a_n \neq 0$, niin polynomin $P(X)$ *aste* on $\deg(P(X)) = n$ ja a_n on polynomin $P(X)$ *korkeimman asteen kerroin*. Nollapolynomin 0 aste on $-\infty$. Kaikkien K-kertoimisten polynomien joukkoa merkitään $K[X]$. Kommutatiivinen rengas K on polynomin $P(X) \in K[X]$ *kerroinrengas*.

Olkoot

$$P(X) = \sum_{k=1}^{n} a_k X^k \quad \text{ja} \quad Q(X) = \sum_{k=1}^{m} b_k X^k$$

K-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

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

Vähemmän havainnollinen mutta täsmällisempi ja Määritelmän 11.1 kanssa ekvivalentti tapa määritellä polynomit on korvata polynomin lauseke $\sum_{k=0}^{n} a_k X^k$ kertoimien muodostamalla jonolla $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ ja määritellä yhteenlasku komponenteittain kuten jonoille on tapana ja kertolasku kaavan (10) mukaisesti. Tällöin jono $(0, 1, 0, 0, 0, \ldots)$ on symbolin X vastine:

Määritelmä 11.1'. Olkoon K kommutatiivinen rengas, jossa on vähintään kaksi alkiota. Kuvaus $\omega\colon \mathbb{N} \to K$, jolle on $N_\omega \in \mathbb{N}$ siten, että $\omega(k) = 0$ kaikille $k \geq N_\omega$, on *K-kertoiminen polynomi*. Kaikkien K-kertoimisten polynomien joukko on $K[X]$.

Määritellään laskutoimitukset $+$ ja $\cdot$ joukossa $K[X]$ asettamalla

$$(\omega + \omega')(k) = \omega(k) + \omega'(k)$$

ja

$$(\omega\omega')(k) = \sum_{i,j \in \mathbb{N}: i+j=k} \omega(i)\omega'(j)$$

kaikille $k \in \mathbb{N}$. Polynomin $\omega \neq 0$ aste on

$$\deg \omega = \max\{k \in \mathbb{N} : \omega(k) \neq 0\}\,.$$

Nollapolynomin 0 aste on $-\infty$.

Huomaa, että polynomeille $P(X), Q(X) \in K[X]$ pätee $P(X) = Q(X)$ täsmälleen silloin, kun niiden kerroinjonot ovat samat.

Propositio 11.2. *Olkoon K kommutatiivinen rengas, jossa on vähintään kaksi alkiota. Joukko $K[X]$ varustettuna polynomien yhteen- ja kertolaskulla on kommutatiivinen rengas. Kuvaus $i\colon K \to K[X]$, joka kuvaa renkaan K alkion a polynomiksi $a = aX^0 \in K[X]$, on injektiivinen rengashomomorfismi. Polynomirenkaan karakteristika on sama kuin kerroinrenkaan karakteristika.*

Todistus. Selvästi polynomit 0 ja 1 ovat yhteenlaskun ja kertolaskun neutraalialkiot. Muut renkaan määrittelevät ominaisuudet seuraavat suoraviivaisesti siitä, että K on kommutatiivinen rengas. Kuvauksen i ominaisuudet on myös helppo tarkastaa. □

Polynomirenkaat ovat tärkeitä kommutatiivisia renkaita. Havainnollistamme niiden merkitystä hieman kurssin viimeisessä luvussa, kun sovellamme niitä äärellisten kuntien konstruktiossa. Rengas K voidaan ajatella Proposition 11.2 kuvauksen i avulla polynomirenkaan $K[X]$ alirenkaaksi.

Kun tarkastelemme polynomirengasta $(\mathbb{Z}/q\mathbb{Z})[X]$, merkitsemme kerrointa $a + q\mathbb{Z}$ yksinkertaisuuden vuoksi edustajalla a.

Esimerkki 11.3. (1) Olkoot $P(X), Q(X) \in \mathbb{Z}[X]$,

$$P(X) = 2X^2 + 2, \quad Q(X) = 1 + 2X\,.$$

Tällöin

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

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

(2) Jos polynomit $P(X), Q(X) \in (\mathbb{Z}/4\mathbb{Z})[X]$ määritellään samoilla lausekkeilla kuin edellä ja polynomin kertoimena oleva kokonaisluku a_k tulkitaan edellä tehdyn sopimuksen mukaan kongruenssiluokaksi $a_k + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$, niin

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

Nyt pätee $P(X)Q(X) = P(X) = P(X) \cdot 1$ mutta $Q(X) \neq 1$, joten kertolaskun supistussääntö ei päde polynomirenkaassa $(\mathbb{Z}/4\mathbb{Z})[X]$. Siis Proposition 10.10 nojalla $(\mathbb{Z}/4\mathbb{Z})[X]$ ei ole kokonaisalue. Itse asiassa polynomi $2X$ on nollan jakaja renkaassa $(\mathbb{Z}/4\mathbb{Z})[X]$:

$$(2X)(2X) = 4X^2 = 0.$$

Lisäksi pätee $\deg(P(X)) = 2$ ja $\deg(Q(X)) = 1$ mutta

$$\deg(P(X)Q(X)) = 2 < 3 = 2 + 1$$

ja

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

Lemma 11.4. *Olkoon K kommutatiivinen rengas, $K \neq \{0\}$. Tällöin*

$$\deg(P(X)Q(X)) \leq \deg P(X) + \deg Q(X)$$

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

Todistus. Olkoot $P(X) = \sum_{k=0}^{n} a_k X^k$ ja $Q(X) = \sum_{k=0}^{m} b_k X^k$ ja oletetaan, että $a_n \neq 0$, $b_m \neq 0$. 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 11.5. *Jos K on kokonaisalue, niin*

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

Lisäksi $K[X]$ on kokonaisalue.

Todistus. Lemman 11.4 merkinnöillä tulopolynomin korkeimman asteen termin kerroin on $a_n b_m \neq 0$, sillä K on kokonaisalue. Erityisesti kahden nollasta poikkeavan polynomin tulo ei ole nollapolynomi, koska tulon aste on luonnollinen luku. □

Polynomirengas ei ole koskaan kunta. Jos K on kokonaisalue, niin Proposition 11.5 mukaan ainoat polynomit, joilla on käänteisalkio kertolaskun suhteen, ovat vakiopolynomit u, missä $u \in K^\times$. Sen sijaan, jos kerroinrengas ei ole kokonaisalue, niin vakiopolynomeilla a, missä a on nollan jakaja renkaassa K, ei ole käänteisalkiota Propositioiden 10.12 ja 11.2 nojalla.

Esimerkki 11.6. Renkaassa $(\mathbb{Z}/4\mathbb{Z})[X]$ pätee

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

Koska merkitsemme polynomirenkaaseen $(\mathbb{Z}/q\mathbb{Z})[X]$ kuuluvan polynomin kertoimia käyttämällä renkaan $(\mathbb{Z}/q\mathbb{Z})$ alkioiden sijaan kokonaislukuedustajia, on syytä olla huolellinen jaollisuuden kanssa:

> *Samalla lausekkeella annettujen polynomien jaollisuus riippuu tarkasteltavasta polynomirenkaasta*

Seuraava esimerkki havainnollistaa tätä.

Esimerkki 11.7. (a) $(X-1) \mid (X^2-1)$ ja $(X+1) \mid (X^2-1)$ kaikissa polynomirenkaissa $R[X]$:

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

(b) $(X+1) \mid (X^2+1)$ renkaassa $(\mathbb{Z}/2\mathbb{Z})[X]$, sillä $1 = -1$ renkaassa $\mathbb{Z}/2\mathbb{Z}$.

(c) Polynomi $(X+1)$ ei jaa polynomia (X^2+1) renkaassa $\mathbb{C}[X]$: Jos $(X+1) \mid (X^2+1)$, niin on $A, B \in \mathbb{C}$, joille $(X+1)(AX+B) = X^2+1$. Tällöin toisen ja nollannen asteen kertoimia tarkastelemalla havaitaan, että pitää olla $A = 1 = B$, mutta ensimmäisen asteen termit eivät täsmää.

Lause 11.8 (Jakoyhtälö)**.** *Olkoon K kommutatiivinen rengas, jossa on vähintään kaksi alkiota. Olkoot $A(X)$, $B(X) \in K[X]$ siten, että $B(X) \neq 0$ ja polynomin $B(X)$ korkeimman asteen termin kerroin on yksikkö. Tällöin on yksikäsitteiset polynomit $Q(X), J(X) \in K[X]$, joille pätee*

$$A(X) = Q(X)B(X) + J(X)$$

ja $\deg J(X) < \deg B(X)$.

Todistus. Osoitetaan ensin, että on polynomit $Q(X)$ ja $J(X)$, jotka toteuttavat väitteen yhtälön. Jos $B(X)$ jakaa polynomin $A(X)$, ei ole mitään todistettavaa. Muuten olkoon

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

Koska $B(X)$ ei jaa polynomia $A(X)$, niin $0 \notin S$, joten joukko

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

on luonnollisten lukujen joukon epätyhjä osajoukko ja sillä on siis minimi $m \geq 0$.

Olkoon $Q(X) \in K[X]$ polynomi, jolle pätee $\deg(A(X)-Q(X)B(X)) = m$. Olkoon

$$J(X) = A(X) - Q(X)B(X) = a_m X^m + \cdots + a_0.$$

Nyt polynomit $Q(X)$ ja $J(X)$ siis toteuttavat väitteen yhtälön.

Osoitetaan sitten, että $m < d = \deg B(X)$. Olkoon b_d polynomin $B(X)$ korkeimman asteen kerroin, joka on oletuksen mukaan yksikkö. Jos olisi $m \geq d$, niin

$$J(X) - a_m b_d^{-1} X^{m-d} B(X) = A(X) - (Q(X) + a_m b_d^{-1} X^{m-d})B(X) \in S$$

ja $\deg\big(J(X) - a_m b_d^{-1} X^{m-d} B(X)\big) < m$, mutta tämä on mahdotonta, koska polynomin $J(X)$ aste on minimaalinen.

Osoitetaan lopuksi polynomien $Q(X)$ ja $J(X)$ yksikäsitteisyys. Jos $\widetilde{Q}(X)$ ja $\widetilde{J}(X)$ ovat polynomeja, joille pätee

$$A(X) = \widetilde{Q}(X)B(X) + \widetilde{J}(X)$$

ja $\deg \widetilde{J}(X) < d$, niin

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

Jos $\widetilde{Q}(X) \neq Q(X)$, niin yhtälön vasemman puolen polynomin aste on vähintään d. Kuitenkin, koska $\deg J(X) < d$ ja $\deg \widetilde{J}(X) < d$, niin

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

Siis $\widetilde{Q}(X) = Q(X)$ ja $\widetilde{J}(X) = J(X)$. □

Seuraus 11.9 (Jakoyhtälö)**.** *Olkoon K kunta. Olkoot $A(X)$, $B(X) \in K[X]$ siten, että $B(X) \neq 0$. Tällöin on yksikäsitteiset $Q(X), J(X) \in K[X]$, joille*

$$A(X) = Q(X)B(X) + J(X)$$

ja $\deg J(X) < \deg B(X)$. □

Esimerkki 11.10. (a) Jakoyhtälö voidaan toteuttaa algoritmisesti jakokulman avulla kuten kokonaisluvuillekin. Tällöin jakokulma antaa esimerkiksi polynomeille

$$A(X) = 2X^3 + X^2 - X - 1 \quad \text{ja} \quad B(X) = X^2 - 2$$

renkaassa $\mathbb{Z}[X]$

$$\begin{array}{r|llll} & 2X & +1 & & \\ \hline X^2-2 & 2X^3 & +X^2 & -X & -1 \\ & \mp 2X^3 & & \pm 4X & \\ \hline & & X^2 & +3X & -1 \\ & & X^2 & & \pm 2 \\ \hline & & & 3X & +1 \end{array}.$$

Toisin sanoen

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

joten Jakoyhtälön merkinnöillä $Q(X) = 2X + 1$ ja $J(X) = 3X + 1$.

(b) Olkoot $A(X), B(X) \in (\mathbb{Z}/3\mathbb{Z})[X]$ polynomit, joilla on sama lauseke kuin kohdassa (a). Tällöin pätee

$$2X^3 + X^2 - X - 1 = (2X+1)(X^2-2) + 1 = (2X+1)(X^2+1) + 1. \tag{11}$$

Jos $B(X) = 2X + 1$, niin jakoyhtälö ei toimi renkaassa $\mathbb{Z}[X]$, koska polynomin $B(X)$ korkeimman asteen kerroin ei ole yksikkö. Tällöin jakokulmassa päädytään ongelmalliseen tilanteeseen

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

josta ei voi jatkaa. Sen sijaan renkaassa $(\mathbb{Z}/3\mathbb{Z})[X]$ voidaan jatkaa, koska $\mathbb{Z}/3\mathbb{Z}$ on kunta. Nyt

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

ja päädytään yhtälöön (11). Renkaassa $\mathbb{Q}[X]$ jakoa voi myös jatkaa ja saadaan

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

Olkoon F kunta. Koska polynomirengas $F[X]$ on kokonaisalue Proposition 11.5 nojalla, sille voidaan muodostaa murtokunta

$$F(X) = \mathscr{Q}(F[X]) = \left\{ \frac{P(X)}{Q(X)} : P(X), Q(X) \in F[X],\ Q(X) \neq 0 \right\},$$

joka on *F-kertoimisten rationaalifunktioiden kunta.*

Harjoitustehtäviä.

11.1. Olkoon K kommutatiivinen rengas, jossa on ainakin kaksi alkiota. Osoita, että $K[X]$ on kommutatiivinen rengas.

11.2. Olkoot $P(X), Q(X) \in (\mathbb{Z}/5\mathbb{Z})[X]$,

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

ja

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

(1) Kerro $Q(X)$ polynomilla $P(X)$.

(2) Jaa $Q(X)$ polynomilla $P(X)$.

11.3. 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 $(\mathbb{Z}/7\mathbb{Z})[X]$.

11.4. Jaa polynomi

$$P(X) = X^3 + 2X^2 + X + 2 \in (\mathbb{Z}/3\mathbb{Z})[X]$$

polynomilla

$$Q(X) = X^2 + 2 \in (\mathbb{Z}/3\mathbb{Z})[X]\,.$$

11.5. Osoita, että $F(X) = 1 - 2X$ on yksikkö renkaassa $(\mathbb{Z}/16\mathbb{Z})[X]$.

11.6. 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 $u \in K^\times$, jolle $P(X) = uQ(X)$.

---

[5]Vihje: Kerroinrengas $\mathbb{Z}/16\mathbb{Z}$ ei ole kokonaisalue.

Varustetaan kommutatiivisen renkaan K *muodollisten potenssisarjojen joukko*

$$K[[X]] = \Big\{ \sum_{k=0}^{\infty} a_k X^k : a_k \in K \Big\}$$

ja kunnan F *muodollisten Laurentin sarjojen joukko*

$$F((X)) = \Big\{ \sum_{k=N}^{\infty} a_k X^k : a_k \in F,\ N \in \mathbb{Z} \Big\}$$

yhteen- ja kertolaskulla, jotka määritellään samoilla lausekkeilla kuin polynomeille Määritelmässä 11.1. Huomaa, että muodollisessa Laurentin sarjassa voi esiintyä myös muuttujan X negatiivisia potensseja.

11.7. Osoita, että $K[[X]]$ on kommutatiivinen rengas ja että polynomirengas $K[X]$ on muodollisten potenssisarjojen renkaan alirengas.

11.8. Osoita, että $1 - X \in K[[X]]^\times$.

11.9. Osoita, että $\sum_{k=0}^{\infty} a_k X^k \in K[[X]]^\times$ täsmälleen silloin, kun $a_0 \in K^\times$.

11.10. Osoita, että $F((X))$ on kunta.

11.11. Osoita, että kuvaus $i\colon F(X) \to F((X))$,

$$i\Big(\frac{P(X)}{Q(X)}\Big) = P(X)Q(X)^{-1},$$

on injektiivinen kuntahomomorfismi.

[10]Vihje: Tässä voi käyttää tehtävän 11.9 tulosta.

12. Polynomien juuret

Tässä luvussa käsittelemme polynomien juuria, jotka ovat vastaavien polynomiyhtälöiden ratkaisuja. Osoitamme muun muassa, että polynomi, jolla on juuri, on jaollinen ensimmäisen asteen polynomilla.

Määritelmä 12.1. Olkoon K kommutatiivinen rengas. Polynomin

$$P(X) = \sum_{k=0}^{n} a_k X^k \in K[X]$$

määräämä *polynomifunktio* on $P\colon K \to K$,

$$x \mapsto \sum_{k=0}^{n} a_k x^k = P(x)\,.$$

Algebrassa tulee pitää erillään polynomin ja polynomifunktion käsitteet ja siksi on hyvä käyttää määritelmän 12.1 merkintätapoja. Polynomirengas voi olla paljon suurempi joukko kuin vastaava polynomifunktioiden joukko: Jos K on kommutatiivinen rengas, jossa on ainakin kaksi alkiota, niin polynomirengas $K[X]$ on ääretön. Kuitenkin, jos K on äärellinen, niin funktioita joukolta K joukkoon K on ainoastaan äärellinen määrä.

Propositio 12.2. *Olkoon K kommutatiivinen rengas. Kuvaus, joka liittää polynomiin $P(X) \in K[X]$ polynomifunktion $P\colon K \to K$, on rengashomomorfismi polynomirenkaasta $K[X]$ funktiorenkaaseen $\mathscr{F}(K, K)$.*

Todistus. Harjoitustehtävä 12.1. □

Esimerkki 12.3. Olkoot $Q(X) = X^2, P(X) = X \in (\mathbb{Z}/2\mathbb{Z})[X]$. Tällöin $P(0) = 0 = 0^2 = Q(0)$ ja $P(1) = 1 = 1^2 = Q(1)$, joten polynomit $P(X)$ ja $Q(X)$ vastaavat samaa polynomifunktiota. Nollasta poikkeava polynomi $Q(X) - P(X) = X^2 - X$, määrää nollakuvauksen renkaalta $\mathbb{Z}/2\mathbb{Z}$ itselleen.

Määritelmä 12.4. Olkoon K kommutatiivinen rengas ja olkoon $P(X) \in K[X]$. Alkio $c \in K$ on polynomin $P(X)$ *juuri*, jos $P(c) = 0$.

Jakoyhtälö antaa seuraavan perustuloksen:

Propositio 12.5. *Olkoon K kommutatiivinen rengas, jossa on vähintään kaksi alkiota. Olkoon $P(X) \in K[X]$ ja $c \in K$. Tällöin $P(c) = 0$, jos ja vain jos $(X - c) \mid P(X)$.*

Todistus. Oletetaan, että $P(c) = 0$. Koska polynomin $X - c$ korkeimman asteen termin kerroin on $1 \in K^\times$, voimme soveltaa Propositiossa 11.8 todistettua jakoyhtälöä. Jakoyhtälön mukaan on K-kertoimiset polynomit $Q(X)$ ja $J(X)$, joille $\deg J(X) < 1$ ja

$$P(X) = Q(X)(X - c) + J(X)\,. \tag{12}$$

Koska $\deg J < 1$, $J(X)$ on vakiopolynomi $J(X) = b$ jollakin $b \in K$. Erityisesti

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

joten $b = 0$. Siis $J(X) = 0$ ja yhtälön (12) nojalla $(X - c) | P(X)$.

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

$$P(c) = (c - c)Q(c) = 0.$$ □

Kokonaisalueen E alkio $p \in E - E^\times$ on *jaoton*, jos a tai b on yksikkö aina, kun $p = ab$. Propositiosta 11.5 seuraa, että ensimmäisen asteen polynomit ovat jaottomia kuntakertoimisessa polynomirenkaassa, koska kaikki nollasta poikkeavat polynomit, joiden aste on pienempi kuin 1 ovat vakiopolynomeita, siis yksiköitä. Korkeamman asteen polynomin osoittaminen jaottomaksi ei ole välttämättä kovin helppoa. Tarkastelemme tätä kysymystä lähemmin tässä luvussa.

Jos K on kokonaisalue mutta ei kunta, niin kaikki vakiopolynomit renkaassa $K[X]$ eivät ole yksiköitä. Tällaisessa polynomirenkaassa polynomin $P(X) \in K[X]$, jonka aste on vähintään 1, sanotaan olevan *jaoton polynomi* jos ei ole polynomeja $S(X) \in K[X]$ ja $T(X) \in K[X]$, joille $P(X) = S(X)\,T(X)$ ja

$$1 \leq \deg S(X), \deg T(X) < \deg P(X)\,.$$

Erityisesti kaikki ensimmäisen asteen polynomit ovat jaottomia polynomeja Proposition 11.5 nojalla.

Seuraus 12.6. *Olkoon K kunta. Toisen tai kolmannen asteen polynomi $P(X) \in K[X]$ on jaoton, jos ja vain jos sillä ei ole juurta kunnassa K.*

Todistus. Harjoitustehtävä 12.2 □

Esimerkki 12.7. (a) Polynomi $P(X) = X^2+1 \in \mathbb{C}[X]$ ei ole jaoton koska $X^2+1 = (X+i)(X-i)$. Tämän polynomin juuret ovat $\pm i \in \mathbb{C}$. Sen sijaan Proposition 12.5 nojalla samalla lausekkeella määritellyt polynomit $P(X) \in \mathbb{Z}[X]$ ja $P(X) \in \mathbb{R}[X]$ ovat jaottomia, koska niillä ei ole juuria.

(b) Renkaassa $(\mathbb{Z}/2\mathbb{Z})[X]$ on neljä toisen asteen polynomia: X^2, X^2+1, X^2+X ja X^2+X+1. Proposition 12.6 mukaan polynomi $X^2+X+1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ on jaoton, koska sillä ei ole yhtään juurta kahden alkion kunnassa $\mathbb{Z}/2\mathbb{Z}$. Sen sijaan mikään muu toisen asteen polynomi ei ole jaoton tässä renkaassa: $X^2 = XX$, $X^2+X = X(X+1)$ ja $X^2+1 = (X+1)^2$.

(c) Polynomi $2X^2+2 \in \mathbb{Z}[X]$ on jaoton polynomi mutta se ei ole jaoton alkio kokonaisalueessa $\mathbb{Z}[X]$ koska $2X^2+2 = 2(X^2+1)$ ja alkiot $2, X^2+1 \in \mathbb{Z}[X]$ eivät ole yksiköitä.

Olkoon c polynomin $P(X) \in K[X]$ juuri. Jos $P(X) = (X-c)^k Q(X)$ jollain $Q(X) \in K[X]$ ja c ei ole polynomin $Q(X)$ juuri, niin c on polynomin $P(X)$ *k-kertainen juuri*. Kun lasketaan polynomin $P(X)$ juuria, k-kertainen juuri lasketaan k juureksi. Esimerkiksi 0 on polynomin $X^2(X-1) \in \mathbb{C}[X]$ kaksinkertainen juuri ja kertaluku huomioiden polynomilla $X^2(X-1) \in \mathbb{C}[X]$ on siis kolme juurta.

Lause 12.8. *Olkoon K kokonaisalue ja olkoon $n \geq 0$. Jos $P(X) \in K[X]$ ja $\deg P(X) = n$, niin polynomilla $P(X)$ on korkeintaan n juurta.*

Todistus. Jos polynomin aste on 0, niin se on nollasta poikkeava vakiopolynomi. Tällaisella polynomilla ei ole juuria, joten väite pätee, kun $n = 0$. Oletetaan, että kaikilla $n-1$ asteen polynomeilla on korkeintaan $n-1$ juurta. Olkoon $P(X)$ polynomi, jonka aste on n. Jos polynomilla $P(X)$ on juuri $c \in K$, niin Proposition 12.9 nojalla $P(X) = (X-c)Q(X)$ jollain $Q(X) \in K[X]$. Koska K on kokonaisalue, $P(a) = 0$, jos ja vain jos $a = c$ tai $Q(a) = 0$. Proposition 11.5 mukaan $\deg(Q(X)) = n-1$ ja sillä on siis induktio-oletuksen mukaan korkeintaan $n-1$ juurta. Siis polynomilla $P(X)$ on kertaluku huomioiden korkeintaan n juurta. □

Seuraus 12.9. *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 $m_1, m_2, \ldots, m_k \in \mathbb{N} - \{0\}$ ja $Q(X) \in K[X]$, joille pätee*

$$P(X) = (X-c_1)^{m_1}(X-c_2)^{m_2}\cdots(X-c_k)^{m_k}Q(X)$$

ja $\deg Q(X) = \deg P(X) - (m_1 + m_2 + \cdots + m_k)$. □

Esimerkki 12.10. Lauseen 12.8 väite ei päde kaikille kommutatiivisille renkaille. Esimerkiksi kongruenssirengas $\mathbb{Z}/16\mathbb{Z}$ ei ole kokonaisalue. Toisen asteen polynomilla $X^2 \in (\mathbb{Z}/16\mathbb{Z})[X]$ on neljä juurta: $0^2 = 4^2 = 8^2 = 12^2 = 0$.

Propositio 12.11. *Olkoon K ääretön kokonaisalue. Tällöin jokaista kokonaisalueen K polynomifunktiota vastaa yksikäsitteinen polynomi renkaassa $K[X]$.*

Todistus. Kuvaus, joka liittää polynomiin vastaavan polynomifunktion on on rengashomomorfismi, joten riittää osoittaa, että tämän homomorfismin ydin on $\{0\}$. Jos polynomia $P(X)$ vastaa nollafunktio, niin sillä on äärettömän monta juurta. Lauseen 12.8 nojalla ainoa tällainen polynomi on 0. □

Seuraus 12.12. *Olkoon K jokin kokonaisalueista $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ tai $\mathbb{C}$. Kuvaus, joka liittää jokaiseen polynomiin $P(X) \in K[X]$ vastaavan polynomifunktion $P\colon K \to K$, on injektio.* □

Määritelmä 12.13. Kunta K on *algebrallisesti suljettu*, jos jokaisella vakiosta poikkeavalla polynomilla $P(X) \in K[X]$ on juuri.

Lause 12.14. *Olkoon K algebrallisesti suljettu kunta. Jokainen vakiosta poikkeava polynomi $P(X) \in K[X]$ on ensimmäisen asteen polynomien tulo ja jokaisella nollasta poikkeavalla polynomilla $P(X) \in K[X]$ on juurten kertaluku huomioiden* $\deg P(X)$ *juurta. Polynomi $P(X) \in K[X]$ on jaoton, jos ja vain jos* $\deg P(X) = 1$.

Todistus. Todistetaan kuten Lause 12.8. □

Lause 12.15 (Algebran peruslause)**.** *Kompleksilukujen kunta on algebrallisesti suljettu.* □

Todistus. Todistetaan kompleksianalyysin kurssilla. Toinen todistus esitetään muun muassa kurssin Lukualueet materiaalissa. □

Seuraus 12.16. *Jokainen vakiosta poikkeava polynomi $P(X) \in \mathbb{C}[X]$ on ensimmäisen asteen polynomien tulo. Nollasta poikkeavalla polynomilla $P(X) \in \mathbb{C}[X]$ on juurten kertaluku huomioiden* $\deg P(X)$ *juurta.* □

Usein polynomeilla on vähemmän juuria kuin niiden asteesta tuleva maksimimäärä. Esimerkiksi polynomilla $X^3 + X \in \mathbb{R}[X]$ on täsmälleen yksi juuri ja polynomeilla $X^2 + 1 \in \mathbb{Q}[X]$, $X^2 + 1 \in \mathbb{R}[X]$ ja $X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ ei ole juuria lainkaan. Siis kunnat $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{Z}/2\mathbb{Z}$ eivät ole algebrallisesti suljettuja. Harjoitustehtävässä 12.8 osoitetaan, että $\mathbb{Z}/p\mathbb{Z}$ ei ole algebrallisesti suljettu millään alkuluvulla p.

Polynomin $X^k - w \in \mathbb{C}[X]$ juuri, siis kompleksiluku z, jolle pätee $z^k = w$, on kompleksiluvun w *k:s juuri*. Erityisen tärkeitä ovat *ykkösen juuret*.

Lemma 12.17. *Luvulla $1 \in \mathbb{C}$ on m kappaletta m. juuria. Jos*

$$\zeta_m = e^{\frac{2\pi}{m}i} = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}, \tag{13}$$

niin ykkösen m. juuret ovat $\zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}$ ja 1.

Todistus. Proposition 2.7 nojalla

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

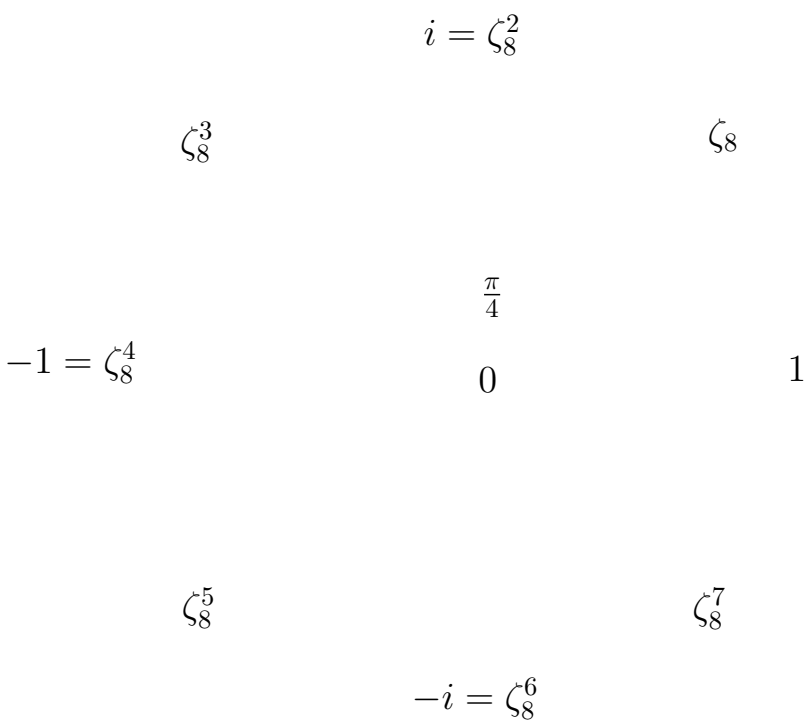
Jos $n \in \{1, 2 \ldots, m\}$, niin Proposition 2.7 nojalla

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

joten

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

Siis kaikki luvut ζ_m^n ovat ykkösen juuria. Lauseen 12.8 nojalla muita juuria ei ole. □



KUVA 5. Ykkösen kahdeksannet juuret.

Seuraus 12.18. *Jokaisella kompleksiluvulla $z \in \mathbb{C} - \{0\}$ on m kappaletta m. juuria. Luvun $z = r(\cos \phi + i \sin \phi)$ juuret ovat*

$$w_1, w_1\zeta_m, \ldots, w_1\zeta_m^{m-1},$$

missä

$$w_1 = \sqrt[m]{r}(\cos \frac{\phi}{m} + i \sin \frac{\phi}{m}). \quad \square$$

Esimerkki 12.19. (a) 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

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

(b) Ykkösen kahdeksannet juuret ovat 1, $\frac{1+i}{\sqrt{2}}$, i, $\frac{-1+i}{\sqrt{2}}$, -1, $\frac{-1-i}{\sqrt{2}}$, $-i$ ja $\frac{1-i}{\sqrt{2}}$. Katso kuva 5.

Proposition 12.18 avulla voimme myös ratkaista toisen asteen polynomiyhtälöt.

Propositio 12.20. *Olkoot $a_0, a_1, a_2 \in \mathbb{C}$, $a_2 \neq 0$. Polynomin*

$$a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$$

juuret ovat

$$z_\pm = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_2}\,.$$

Todistus. Havaitsemme, että

$$(X - z_+)(X - z_-) = X^2 + a_1X + a_0,$$

joten z_+ ja z_- ovat juuria. Lauseen 12.8 nojalla muita juuria ei ole. □

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

$$\begin{aligned} u_0^3 &= -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}, \\ v_0^3 &= -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}, \text{ ja} \\ u_0v_0 &= -\frac{p}{3}, \end{aligned}$$

ja $\zeta_3 = -\frac{1}{2} + i\,\frac{\sqrt{3}}{2}$ on kaavan (13) antama ykkösen kolmas juuri, niin luvut

$$\begin{aligned} z_1 &= u_0 + v_0\,, \\ z_2 &= \zeta_3u_0 + \zeta_3^2v_0 \text{ ja} \\ z_3 &= \zeta_3^2u_0 + \zeta_3v_0 \end{aligned}$$

ovat yhtälön $z^3 + pz + q = 0$ ratkaisuja. Alkuperäisen yhtälön juuret saadaan näistä *Cardanon kaavoista* tekemällä muuttujanvaihto toiseen suuntaan.

Neljännen asteen yhtälöiden ratkaisukaavat ovat samankaltaisia kuin kolmannen asteen tapauksessa. Kolmannen ja neljännen asteen yhtälöiden ratkaisemista käsitellään enemmän kurssilla [LA] ja esimerkiksi kirjassa K. Väisälä: Lukuteorian ja korkeamman algebran alkeet.

Abel osoitti 1820-luvulla, että viidennen ja korkeamman asteen polynomeille ei ole samanlaista ratkaisualgoritmia kuin alemman asteen polynomeille. Tämän väitteen todistuksessa käytetään yleensä ryhmäteoriaa. Aihepiiriin voi halutessaan tutustua esimerkiksi lähteiden [DF] ja [Väi] avulla ja kursseilla Algebra 2A ja 2B.

Harjoitustehtäviä.

12.1. Olkoon K kommutatiivinen rengas. Osoita, että kuvaus, joka liittää polynomiin $P(X) \in K[X]$ vastaavan polynomifunktion $P \in \mathscr{F}(K, K)$, on rengashomomorfismi.

12.2. 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 kunnassa K. Anna esimerkki, joka osoittaa, että väite ei päde neljännen asteen polynomeille.

12.3. Mitkä polynomit $aX^2 + bX + c \in \mathbb{R}[X]$ ovat jaottomia?

12.4. (a) Onko polynomi $X^2 - 2 \in (\mathbb{Z}/5\mathbb{Z})[X]$ jaoton?
(b) Onko polynomi $X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$ jaoton?

12.5. Osoita, että $1 + \mathbb{Z}/2\mathbb{Z}$ on polynomin $P(X) \in (\mathbb{Z}/2\mathbb{Z})[X]$ juuri, jos ja vain jos polynomilla $P(X)$ on parillinen määrä nollasta poikkeavia kertoimia.

12.6. Olkoon p alkuluku, $p \equiv 3 \mod 4$. Osoita, että $X^2+1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ on jaoton polynomi.

12.7. Olkoon p alkuluku. Montako juurta polynomilla $X^p - X \in (\mathbb{Z}/p\mathbb{Z})[X]$ on?

12.8. Osoita, että kunta $\mathbb{Z}/p\mathbb{Z}$ ei ole algebrallisesti suljettu millään alkuluvulla p.

12.9. Esitä polynomi $X^5 + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ jaottomien polynomien tulona.

12.10. Osoita, että yhtälöllä $x^2 = -1$ on äärettömän monta ratkaisua Hamiltonin kvaternioiden vinossa kunnassa.

12.11. Määritä ykkösen kuudennet juuret. Kirjoita juuret muodossa, jossa ei käytetä trigonometrisiä funktioita eikä kompleksista eksponenttifunktiota. Piirrä kuva, jossa kaikki juuret esitetään tason pisteinä.

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

12.13. Ratkaise yhtälöt $z^2 - z + 1 = 0$ ja $z^2 - iz + 1 = 0$.

12.14. Olkoon $q \in \mathbb{N} - \{0\}$. Osoita, että joukko

$$J_q = \{w \in \mathbb{C} : w^q = 1\}$$

varustettuna kompleksilukujen kertolaskulla on ryhmän $\mathbb{C}^\times$ aliryhmä. Osoita, että ryhmä J_q on isomorfinen ryhmän $(\mathbb{Z}/q\mathbb{Z}, +)$ kanssa.

12.15. Olkoon $p > 3$ alkuluku. Osoita, että $1 + p\mathbb{Z}$ ja $-1 + p\mathbb{Z}$ ovat ainoat kunnan $\mathbb{Z}/p\mathbb{Z}$ alkiot, jotka ovat omat käänteisalkionsa kertolaskun suhteen. Osoita, että

$$(2 + p\mathbb{Z})(3 + p\mathbb{Z}) \cdots (p - 2 + p\mathbb{Z}) = 1 + p\mathbb{Z}\,.$$

12.16. Osoita, että

$$(p-1)! \equiv -1 \mod p\,,$$

jos p on alkuluku.

12.17. Osoita, että

$$(q-1)! \equiv 0 \mod q$$

jos $q \geq 6$ ei ole alkuluku.

12.18. Olkoon p pariton alkuluku ja olkoon $k = \frac{p-1}{2}$. Osoita, että

$$(p-1)! = (-1)^k (k!)^2 \mod p\,.$$

Osoita, että polynomi $X^2 + 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ ei ole jaoton, jos $p \equiv 1 \mod 4$.

---

[6]Vihje: Tehtävä 9.12 ja sen vihje.

[7]Vihje: Käytä ryhmäteoriaa!

[8]Vihje: Tehtävä 12.7

[10]Vihje: Tarkastele kvaternioita, jotka ovat muotoa $a\mathbf{i} + b\mathbf{j} + c\mathbf{k}$, $a^2 + b^2 + c^2 = 1$.

13. Jako alkutekijöihin ja Eukleideen alueet

Kokonaisalueiden teoriassa käytetään usein hieman erilaista alkuluvun määritelmää kuin kokonaislukujen Määritelmä 9.1.

Määritelmä 13.1. Kokonaisalueen K alkio p, joka ei ole yksikkö, on *alkualkio* (tai *alkuluku*), jos kaikille $a, b \in K$ pätee $p \mid a$ tai $p \mid b$, jos $p \mid ab$.

Alkualkio siis toteuttaa Eukleideen lemman väitteen vastineen tarkasteltavassa renkaassa.

Propositio 13.2. *Kokonaisalueen alkualkiot ovat jaottomia.*

Todistus. Olkoon K kokonaisalue ja olkoon $p \in K$ alkualkio. Oletetaan, että $p = ab$. Riittää tarkastella tapaus $p \mid a$. Tällöin $a = pc$ jollakin $c \in K$, joten $p = pcb$. Proposition 10.10 nojalla kertolaskun supistussääntö on voimassa kokonaisalueessa K, joten b on yksikkö. Siis p on jaoton. □

Kokonaislukujen renkaassa jaottomat alkiot ja Määritelmän 13.1 mukaiset alkualkiot ovat samoja Eukleideen lemman nojalla. Näillä määritelmillä luvut ± 2, ± 3, ± 5, ± 7, ± 11, ± 13, ± 17, ± 19, ± 23, ± 29 ja niin edelleen ovat renkaan $\mathbb{Z}$ alkualkioita ja jaottomia alkioita.

Tarkastelemme tässä luvussa sellaisia kokonaisalueita, joissa pätee aritmetiikan peruslauseen yleistys.

Määritelmä 13.3. Olkoon K kokonaisalue. Funktio $D\colon K - \{0\} \to \mathbb{N}$ on *Eukleideen funktio*, jos

(1) $D(a) \leq D(ab)$ kaikille $a, b \in K - \{0\}$ ja
(2) kaikille $a, b \in K$, $b \neq 0$ on $q, r \in K$, joille pätee *jakoyhtälö*

$$a = qb + r$$

ja $r = 0$ tai $D(r) < D(b)$

Jos kokonaisalueella K on Eukleideen funktio, niin K on *Eukleideen alue*.

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

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

Tämä tulos on hyvin uskottava ja se todistetaan tarkasti lukuteorian alkeiskursseilla. Koska kokonaislukujen itseisarvo toteuttaa $|ab| = |a||b| \geq |a|$ kaikille $a, b \in \mathbb{Z} - \{0\}$, huomaamme, että itseisarvo on Eukleideen funktio kokonaislukujen renkaassa, joka on siis Eukleideen alue.

Lemma 13.4. *Olkoon K Eukleideen alue ja olkoon $D\colon K - \{0\} \to \mathbb{N}$ Eukleideen funktio. Tällöin $D(ab) = D(a)$, jos ja vain jos b on yksikkö.*

Todistus. Jos b on yksikkö, niin Eukleideen funktion ensimmäisen ominaisuuden nojalla pätee

$$D(a) \leq D(ab) \leq D(abb^{-1}) = D(a)\,.$$

Siis $D(a) = D(ab)$ kaikille $a \neq 0$. Jos taas b ei ole yksikkö, niin ab ei ole alkion a tekijä. Tällöin on $q \in K$ ja $r \in K - \{0\}$, joille $a = qab + r$ ja $D(r) < D(ab)$. Nyt $qa \neq 1$ ja Eukleideen funktion ensimmäisen ominaisuuden ja jakoyhtälön nojalla

$$D(a) \leq D(a(1 - qb)) = D(r) < D(ab)\,. \quad \square$$

Olkoon K kokonaisalue. Jos $a, b \in K$ siten, että $\{a, b\} \neq \{0\}$, ja jos $d \in K$ on alkioiden a ja b yhteinen tekijä, jonka jokainen alkioiden a ja b yhteinen tekijä jakaa, niin d on alkioiden a ja b *suurin yhteinen tekijä*, merkitään $d = \mathrm{syt}(a, b)$. Jos $u \in K^\times$ ja $d = \mathrm{syt}(a, b)$, niin $ud = \mathrm{syt}(a, b)$, joten suurin yhteinen tekijä on määritelty yksiköllä kertomista vaille yksikäsitteisesti, mikä on syytä muistaa merkintää $\mathrm{syt}(a, b)$ käytettäessä. Jos $1 = \mathrm{syt}(a, b)$, niin a ja b ovat *keskenään jaottomia*.

Propositio 13.5. *Eukleideen alueessa K millä tahansa kahdella alkiolla on suurin yhteinen tekijä. Olkoot $a, b \in K$ ja olkoon d niiden suurin yhteinen tekijä. Tällöin on $x, y \in K$, joille pätee $d = xa + yb$.*

Todistus. Olkoon K Eukleideen alue ja olkoon $D\colon K - \{0\} \to \mathbb{N}$ Eukleideen funktio. Voimme olettaa, että $b \neq 0$. Olkoon

$$\mathscr{I} = \{xa + yb : x, y \in K\}$$

ja olkoon $d \in \mathscr{I} - \{0\}$ alkio, jolle

$$D(d) = \min\left\{D(c) : c \in \mathscr{I} - \{0\}\right\}.$$

Koska E on Eukleideen alue, on $q, r \in E$, joille $a = qd + r$ ja $r = 0$ tai $D(r) < D(d)$. Nyt $d = sa + tb$ joillain $s, t \in K$, joten

$$r = a - qd = a - q(sa + tb) = (1 - qs)a + qtb \in \mathscr{I}\,.$$

Koska $D(d)$ on pienin Eukleideen funktion arvo nollasta poikkeaville alkioille joukossa $\mathscr{I}$, on siis $r = 0$ ja $d|a$. Vastaavalla tavalla osoitetaan, että $d|b$.

Jos c on lukujen a ja b yhteinen tekijä, niin $a = fc$ ja $b = gc$ joillakin $f, g \in K$. Siispä

$$d = sa + tb = sfc + tgc = (sf + tg)c\,,$$

joten $c|d$. Siis $d = \mathrm{syt}(a, b)$. □

Nyt voimme yleistää Eukleideen lemman Eukleideen alueiden tilanteeseen.

Lemma 13.6. *Olkoon K Eukleideen alue. Jos $a, b \in K$ ovat keskenään jaottomia ja $a|bc$, niin $a|c$.*

Todistus. Harjoitustehtävä 13.1 □

Lemma 13.7. *Eukleideen alueessa jaottomat alkiot ovat alkualkioita.*

Todistus. Harjoitustehtävä 13.2 □

Lause 13.8 (Yksikäsitteinen alkutekijöihin jako)**.** *Jokainen Eukleideen alueen nollasta poikkeava alkio, joka ei ole yksikkö, voidaan voidaan esittää jaottomien alkioiden äärellisenä tulona, joka on järjestystä ja yksiköillä kertomista vaille yksikäsitteinen.*

Todistus. Väite todistetaan kuten aritmetiikan peruslause. Todistuksessa ei voi rajoittua tarkastelemaan positiivisia lukuja vaan Proposition 9.3 vastineessa tarkastellaan alkiota, jolle haluttua tuloesitystä ei ole ja jolle Eukleideen funktion arvo on minimaalinen:

Olkoon K kokonaisalue ja olkoon $E \subset K - (\{0\} \cup K^\times)$ niiden alkioiden joukko, joita ei voi esittää jaottomien alkioiden äärellisenä tulona. Olkoon $N \in E$ siten, että $D(N) = \min\{D(a) : a \in E\}$. Tällöin N ei erityisesti ole jaoton. On siis $m, n \in K - K^\times$ siten, että $N = mn$. Koska K on Eukleideen alue, pätee Lemman 13.4 nojalla $D(m), D(n) < D(mn) = D(N)$. Siis alkiot m ja n voidaan esittää jaottomien alkioiden äärellisinä tuloina ja näiden esitysten tulona saadaan alkion N esitys jaottomien alkioiden äärellisenä tulona.

Alkutekijäesityksen yksikäsitteisyys osoitetaan kuten kokonaisluvuille Lemman 13.7 avulla. □

Esimerkki 13.9. Harjoitustehtävässä 10.13 osoitettiin, että *Gaussin kokonaislukujen rengas*

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

on kokonaisalue. Osoitetaan, että kompleksilukujen *normi*

$$D(z) = z\bar{z} = |z|^2$$

on Eukleideen funktio Gaussin kokonaislukujen renkaassa. On helppo nähdä, että normi toteuttaa Eukleideen funktion ensimmäisen ominaisuuden, koska kaikille $w \in \mathbb{Z}[i]$ pätee $|w|^2 \geq 1$. Tarkastellaan jakoyhtälöä. Olkoot $a, b \in \mathbb{Z}[i]$, $b \neq 0$. Tällöin $\frac{a}{b} \in \mathbb{Q}(i)$ ja on $q = m + in \in \mathbb{Z}[i]$ siten, että

$$\big|\operatorname{Re}\big(\frac{a}{b}\big) - m\big| \leq \frac{1}{2} \quad \text{ja} \quad \big|\operatorname{Im}\big(\frac{a}{b}\big) - n\big| \leq \frac{1}{2}\,. \tag{14}$$

Tällöin

$$\frac{a}{b} = q + \big(\operatorname{Re}\big(\frac{a}{b}\big) - m + i(\operatorname{Im}\big(\frac{a}{b}\big) - n)\big)\,,$$

joten

$$a = qb + b\big(\operatorname{Re}\big(\frac{a}{b}\big) - m + i(\operatorname{Im}\big(\frac{a}{b}\big) - n)\big)\,,$$

missä

$$r = b\big(\operatorname{Re}\big(\frac{a}{b}\big) - m + i(\operatorname{Im}\big(\frac{a}{b}\big) - n)\big) = a - qb \in \mathbb{Z}[i],$$

koska $a, b, q \in \mathbb{Z}[i]$ ja $\mathbb{Z}[i]$ on rengas. Tämä on jakoyhtälössä tarvittava muoto, kunhan osoitetaan, että $r = 0$ tai $D(r) < D(b)$. Ominaisuudesta (14) seuraa

$$\begin{aligned} D(r) &= D\big(b\big(\operatorname{Re}\big(\frac{a}{b}\big) - m + i(\operatorname{Im}\big(\frac{a}{b}\big) - n)\big)\big) \\ &= D(b)D\big(\operatorname{Re}\big(\frac{a}{b}\big) - m + i(\operatorname{Im}\big(\frac{a}{b}\big) - n)\big) \leq \frac{D(b)}{2} < D(b) \end{aligned}$$

kuten haluttiin. Siis $\mathbb{Z}[i]$ on Eukleideen alue. Lauseen 13.8 nojalla Gaussin kokonaisluvuille on siis yksikäsitteinen esitys alkulukujen tulona.

Normia tarkastelemalla on helppo osoittaa, että luvut $1 \pm i \in \mathbb{Z}[i]$ ovat jaottomia ja siis alkulukuja. Sen sijaan $2 = (1+i)(1-i)$ ei ole alkuluku Gaussin kokonaislukujen renkaassa.

Esimerkki 13.10. Rationaalilukujen toisen asteen kuntalaajennusten $\mathbb{Q}(\sqrt{d})$ avulla saadaan valitsemalla d sopivasti esimerkkejä kokonaisalueista, joissa kaikki jaottomat alkiot eivät ole alkualkioita. Esimerkiksi kunnan $\mathbb{Q}(\sqrt{10})$ alirenkaassa

$$\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} : a, b \in \mathbb{Z}\}$$

voidaan osoittaa, että alkiot 2, 3, $4 + \sqrt{10}$ ja $4 - \sqrt{10}$ ovat jaottomia mutta eivät alkualkioita, koska

$$2 \cdot 3 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$$

mutta 2 tai 3 ei ole lukujen $(4 \pm \sqrt{10})$ tekijä ja vastaavasti $(4 \pm \sqrt{10})$ ei ole lukujen 2 tai 3 .

Toinen esimerkki on kunnan $\mathbb{Q}(\sqrt{-5})$ alirengas

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\,i\sqrt{5} : a, b \in \mathbb{Z}\},$$

jossa luvut 3, $2 - i\sqrt{5}$ ja $2 + i\sqrt{5}$ ovat jaottomia mutta eivät alkulukuja, koska esimerkiksi

$$3^2 = 9 = (2 - i\sqrt{5})(2 + i\sqrt{5})$$

mutta 3 ei ole lukujen $2 - i\sqrt{5}$ ja $2 + i\sqrt{5}$ tekijä.

Lauseen 13.8 nojalla $\mathbb{Z}[\sqrt{10}]$ ja $\mathbb{Z}[\sqrt{-5}]$ eivät ole Eukleideen renkaita.

Seuraus 13.11. *Olkoon K kunta. Polynomirengas $K[X]$ on Eukleideen alue ja polynomin aste* $\deg\colon K[X] - \{0\} \to \mathbb{N}$ *on Eukleideen funktio.*

Todistus. Todistimme jakoyhtälön Seurauksena 11.9. Propositiossa 11.5 todistettiin $\deg P(X) \leq \deg(P(X)Q(X))$ kaikille $P(X), Q(X) \in K[X] - \{0\}$. Siis polynomin aste on Eukleideen funktio. □

Seuraus 13.12. *Olkoon K kunta. Jokainen polynomi $P(X) \in K[X]$ voidaan esittää jaottomien polynomien äärellisenä tulona, joka on järjestystä ja vakioilla $c \in K - \{0\}$ kertomista vaille yksikäsitteinen.* □

Jos K on kokonaisalue mutta ei kunta, niin kaikki vakiopolynomit renkaassa $K[X]$ eivät ole yksiköitä. Tällöin polynomin aste ei ole Eukleideen funktio kokonaisalueessa $K[X]$, koska jakoyhtälö ei toimi kuten näimme Esimerkissä 11.10.

Esimerkki 13.13. Vakiopolynomi $2 \in \mathbb{Z}[X]$ on kokonaisalueen $\mathbb{Z}[X]$ jaoton alkio mutta se ei ole jaoton polynomi, koska $\deg(2) = 0$. Toisaalta osoitamme Esimerkissä 12.7, että polynomi $2X^2 + 2 \in \mathbb{Z}[X]$ on jaoton polynomi mutta se ei ole renkaan $\mathbb{Z}[X]$ jaoton alkio, koska $2X^2 + 2 = 2(X^2 + 1)$.

Jos K on kunta, niin $P(X) \in K[X]^\times$, jos ja vain jos $\deg P(X) = 0$.

Harjoitustehtäviä.

13.1. Olkoon K Eukleideen alue ja olkoot $a, b \in K$ keskenään jaottomia. Oletetaan, että $a|bc$. Osoita, että $a|c$.

13.2. Olkoon K Eukleideen alue. Olkoon $p \in K$ jaoton ja olkoot $a, b \in K$ siten, että $p|ab$. Osoita, että $p|a$ tai $p|b$.

13.3. Osoita, että Eukleideen alueessa alkutekijöihin jako on tekijöiden järjestystä ja yksiköillä kertomista vaille yksikäsitteinen

13.4. Osoita, että $1 + i$ on jaoton Gaussin kokonaislukujen renkaassa.

Tässä luvussa tutustumme renkaiden ideaaleihin ja niiden avulla muodostettuihin tekijärenkaisiin. Sovellamme kehitettävää teoriaa äärellisten kuntien konstruktioon.

Rengashomomorfismin $\psi\colon R \to S$ ydin on additiivisen ryhmän $(R,+)$ (normaali) aliryhmä. Koska rengashomomorfismi on homomorfismi myös kertolaskun suhteen, ytimellä on toinenkin ominaisuus, jota tarkastelemme seuraavaksi.

Propositio 14.1. *Olkoon $\phi\colon R \to R'$ rengashomomorfismi. Kaikille $x \in R$ ja kaikille $a \in \ker\phi$ pätee $ax, xa \in \ker\phi$.*

Todistus. Väite seuraa helposti huomaamalla, että

$$\phi(xa) = \phi(x)\phi(a) = \phi(x)0 = 0$$

ja

$$\phi(ax) = \phi(a)\phi(x) = 0\,\phi(x) = 0\,. \quad \square$$

Määritelmä 14.2. Renkaan R epätyhjä osajoukko $\mathscr{I} \subset R$ on *ideaali*, jos

- $(\mathscr{I},+)$ on ryhmän $(R,+)$ aliryhmä ja
- $xa, ax \in \mathscr{I}$ kaikilla $x \in R$ ja $a \in \mathscr{I}$.

Seuraus 14.3. *Rengashomomorfismin ydin on määrittelyrenkaansa ideaali.* $\square$

Esimerkki 14.4. (a) Jokaisella renkaalla R on ainakin ideaalit R ja $\{0\}$.

(b) Propositiossa 5.16 osoitimme, että kaikki kokonaislukujen additiivisen ryhmän aliryhmät ovat muotoa $(a\mathbb{Z},+)$. On helppo tarkastaa, että joukko $a\mathbb{Z}$ on renkaan $\mathbb{Z}$ ideaali jokaisella $a \in \mathbb{Z}$. Muita ideaaleja ei ole, koska ideaali varustettuna yhteenlaskulla on aina ryhmä. Siis kokonaislukujen renkaan ideaalit ovat täsmälleen joukot $a\mathbb{Z}$, $a \in \mathbb{Z}$.

Lemma 14.5. *Jos renkaan R ideaali $\mathscr{I}$ sisältää yksikön, niin $\mathscr{I} = R$.*

Todistus. Olkoon $u \in \mathscr{I}$ yksikkö. Tällöin $1 = uu^{-1} \in \mathscr{I}$. Koska $\mathscr{I}$ on ideaali, niin kaikilla $x \in R$ pätee $x = x1 \in \mathscr{I}$, joten $\mathscr{I} = R$. $\square$

Propositio 14.6. *Jos renkaan R ideaali $\mathscr{I}$ on alirengas, niin $\mathscr{I} = R$.*

Todistus. Jos $\mathscr{I}$ on renkaan R alirengas, niin $1 = 1_R \in \mathscr{I}$. Väite seuraa Lemmasta 14.5. $\square$

Propositio 14.7. *Olkoon $\mathscr{I}$ jakorenkaan R ideaali. Silloin $\mathscr{I} = R$ tai $\mathscr{I} = \{0\}$. Erityisesti kunnan K ainoat ideaalit ovat $\{0\}$ ja K.*

Todistus. Väite seuraa Lemmasta 14.5. $\square$

Seuraus 14.8. *Kuntahomomorfismi on injektio.*

Todistus. Harjoitus 14.8. $\square$

Esimerkki 14.9. Olkoon $\Omega \neq \emptyset$ ja olkoon R rengas. Jos A on joukon Ω osajoukko, olkoon

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

On helppo tarkastaa, että $(N(A),+)$ on additiivisen ryhmän $(\mathscr{F}(\Omega,R),+)$ aliryhmä: Jos $h_1, h_2 \in N(A)$, niin

$$(h_1 - h_2)(a) = h_1(a) - h_2(a) = 0 - 0 = 0$$

kaikille $a \in A$. Lisäksi, jos $g \in \mathscr{F}(\Omega,R)$, $h \in N(A)$ ja $a \in A$, niin

$$(gh)(a) = g(a)h(a) = g(a) \cdot 0 = 0$$

ja

$$(hg)(a) = h(a)g(a) = 0 \cdot g(a) = 0$$

joten $gh, hg \in N(A)$. Siis $N(A)$ on ideaali.

Vastaava konstruktio antaa ideaaleja muissakin funktiorenkaissa, esimerkiksi

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

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

Propositio 14.10. *Olkoon $\phi\colon R \to S$ rengashomomorfismi. Tällöin*

(1) Jos $\mathscr{I} \subset R$ on ideaali, niin $\phi(\mathscr{I})$ on renkaan $\phi(S)$ ideaali.

(2) Jos $\mathscr{I} \subset S$ on ideaali, niin $\phi^{-1}(\mathscr{I})$ on renkaan R ideaali.

Todistus. (1) Harjoitustehtävä 14.3.

(2) Proposition 5.8 nojalla $(\phi^{-1}(\mathscr{I}), +) \leq (R, +)$. Olkoot $a \in \phi^{-1}(\mathscr{I})$ ja $r \in R$. Tällöin $\phi(ra) = \phi(r)\phi(a) \in \mathscr{I}$, koska $\phi(a) \in \mathscr{I}$ ja $\mathscr{I}$ on renkaan S ideaali. Siis $ra \in \phi^{-1}(\mathscr{I})$. Vastaavasti osoitetaan, että $ar \in \phi^{-1}(\mathscr{I})$. □

Esimerkki 14.11. Luonnollinen kuvaus $\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ on surjektiivinen rengashomomorfismi. Esimerkin 14.4 ja Proposition 14.10 mukaan joukot

$$a\mathbb{Z} + q\mathbb{Z} = \{ak + q\mathbb{Z} : k \in \mathbb{Z}\} \subset \mathbb{Z}/q\mathbb{Z} \tag{15}$$

ovat renkaan $\mathbb{Z}/q\mathbb{Z}$ ideaaleja. Toisaalta, jos $\mathscr{J}$ on renkaan $\mathbb{Z}/q\mathbb{Z}$ ideaali, niin sen alkukuva luonnollisessa kuvauksessa on renkaan $\mathbb{Z}$ ideaali. Siis renkaan $\mathbb{Z}/q\mathbb{Z}$ ideaalit ovat täsmälleen renkaan $\mathbb{Z}$ ideaalien kuvat luonnollisessa homomorfismissa. Toisin sanoen kaikki ideaalit ovat kuten lausekkeessa (15).

Jos H on renkaan $\mathbb{Z}/q\mathbb{Z}$ additiivisen ryhmän $(\mathbb{Z}/q\mathbb{Z}, +)$ aliryhmä, niin H on ryhmän $(\mathbb{Z}, +)$ jonkin aliryhmän kuva luonnollisessa kuvauksessa. Koska kaikki ryhmän $(\mathbb{Z}, +)$ aliryhmät ovat syklisiä, niin $H = a\mathbb{Z} + q\mathbb{Z}$ jollain $a \in \mathbb{Z}$. Siis jokainen renkaan $\mathbb{Z}/q\mathbb{Z}$ additiivisen ryhmän aliryhmä on renkaan $\mathbb{Z}/q\mathbb{Z}$ jonkin ideaalin additiivinen ryhmä.

Propositio 14.12. *Olkoon I epätyhjä indeksijoukko. Olkoot $\mathscr{I}_i$, $i \in I$, renkaan R ideaaleja. Tällöin $\bigcap_{i\in I} \mathscr{I}_i$ on renkaan R ideaali.*

Todistus. Harjoitustehtävä 14.5. □

Proposition 14.12 nojalla seuraava määritelmä on mielekäs.

Määritelmä 14.13. Jos $S \subset R$, $S \neq \emptyset$, niin *joukon S virittämä ideaali* on joukon S sisältävien ideaalien leikkaus.

Esimerkki 14.14. Olkoon R rengas ja olkoon $\Omega \neq \emptyset$. Esimerkissä 8.14 osoitimme, että evaluaatiokuvaus $E_c\colon \mathscr{F}(\Omega, R) \to R$, $E_c(f) = f(c)$ on rengashomomorfismi. Sen ydin on

$$N(c) = \ker E_c = \{f \in \mathscr{F}(\Omega, R) : f(c) = 0\}.$$

Erityisesti $N(c)$ on siis renkaan $\mathscr{F}(\Omega, R)$ ideaali ja Esimerkki 14.9 voidaan tehdä nopeasti uudelleen:

$$N(A) = \{f \in \mathscr{F}(\Omega, R) : f(a) = 0 \text{ kaikilla } a \in A\} = \bigcap_{a\in A} \ker E_a$$

on ideaali Proposition 14.12 nojalla.

Lemma 14.15. *Olkoon R rengas. Äärellisen joukon $A = \{x_1, x_2, \ldots, x_n\} \subset R$ virittämä ideaali on*

$$RAR = \left\{ \sum_{i=1}^{n} s_i x_i r_i : s_1, r_1, s_2, r_2, \ldots, s_n, r_n \in R \right\}.$$

Jos R on kommutatiivinen, niin

$$RAR = RA = \left\{ \sum_{i=1}^{n} s_i x_i : s_1, s_2, \ldots, s_n \in R \right\}.$$

Todistus. Harjoitustehtävä 14.7. □

Erityisesti yhden alkion x virittämä ideaali on $RxR = \{rxs : r, s \in R\}$. Jos rengas K on kommutatiivinen, niin alkion $x \in K$ virittämä ideaali on $xK = Kx$. Tätä ideaalia merkitään usein (x) ja sitä sanotaan *pääideaaliksi*. Vastaavasti alkioiden $x_1, x_2, \ldots, x_m$ virittämää ideaalia kommutatiivisessa renkaassa merkitään usein $(x_1, x_2, \ldots, x_m)$. Kokonaisalue, jonka kaikki ideaalit ovat pääideaaleja on *pääideaalialue*.

Lemma 14.16. *Jos R on rengas ja $u \in R^\times$, niin $(ua) = (a)$ kaikille $a \in R$.*

Todistus. Harjoitustehtävä 14.10. □

Esimerkki 14.17. (1) Esimerkin 14.4 (b) nojalla $\mathbb{Z}$ on pääideaalialue.
(2) Esimerkin 14.11 nojalla $\mathbb{Z}/q\mathbb{Z}$ on pääideaalialue kaikilla $q \geq 2$.
(3) Esimerkin 14.7 nojalla kaikki kunnat ovat pääideaalialueita.

Lause 14.18. *Eukleideen alue on pääideaalialue.*

Todistus. Olkoon $\mathscr{I}$ nollasta poikkeava ideaali Eukleideen alueessa K, jonka Eukleideen funktio on D. Olkoon $b \in \mathscr{I} - \{0\}$ alkio, jolle pätee $D(b) \leq D(b')$ kaikille $b' \in \mathscr{I} - \{0\}$. Olkoon $a \in \mathscr{I}$. Jakoyhtälön mukaan on $q, r \in K$, joille pätee $a = qb + r$ ja $D(r) < D(b)$ tai $r = 0$. Erityisesti $r = a - qb \in \mathscr{I}$. Koska $D(b)$ on minimaalinen nollasta poikkeaville ideaalin $\mathscr{I}$ alkioille, pätee siis $r = 0$, joten $a \in (b)$. □

Seuraus 14.19. *Olkoon K kunta. Tällöin polynomirengas $K[X]$ on pääideaalialue.*

Todistus. Seuraa Lauseesta 14.18 ja Seurauksesta 13.11. □

Seurauksen 14.19 oletus, että kerroinrengas on kunta on oleellinen. Esimerkiksi kokonaislukukertoimisten polynomien renkaan ideaalirakenne on monimutkaisempi:

Esimerkki 14.20. Polynomirenkaan $\mathbb{Z}[X]$ ideaali $\mathscr{I} = (2, X)$, joka koostuu niistä kokonaislukukertoimisista polynomeista, joiden vakiotermi on parillinen ei ole pääideaali: Jos $\mathscr{I} = (P(X))$ jollekin $P(X) \in \mathbb{Z}[X]$, niin $P(X)$ jakaa polynomin 2. Siis Proposition 11.5 nojalla $\deg P(X) \leq \deg 2 = 0$, koska kerroinrengas $\mathbb{Z}$ on kokonaisalue. Siis $P(X) \in \{\pm 1, \pm 2\} \subset \mathbb{Z}[X]$. Koska $X \in \mathscr{I}$, täytyy olla $P(X) = \pm 1$, joten $(P(X)) = \mathbb{Z}[X]$, mikä on ristiriita. Erityisesti siis polynomirengas $\mathbb{Z}[X]$ ei ole pääideaalirengas.

Muodostamme renkaan R ideaalia $\mathscr{I}$ vastaavan tekijäjoukon $R/\mathscr{I}$ additiivisen ryhmän $(R, +)$ sivuluokista kuten ryhmien tilanteessa tehtiin luvussa 7. Seurauksen 7.22 nojalla tekijäjoukko $R/\mathscr{I}$ varustettuna yhteenlaskun tekijälaskutoimituksella on kommutatiivinen ryhmä. Osoittautuu, että ideaaliominaisuuden vuoksi myös kertolasku on yhteensopiva ekvivalenssirelaation kanssa ja tekijälaskutoimitukset antavat tekijäjoukolle renkaan rakenteen. Seuraava tulos yleistää Harjoitustehtävän 3.3 tuloksen kokonaislukurenkaan tilanteesta yleiseen tapaukseen:

Propositio 14.21. *Olkoon R rengas ja olkoon $\mathscr{I} \subset R$ ideaali. Renkaan R yhteenlasku ja kertolasku ovat yhteensopivia ideaalin $\mathscr{I}$ määräämän ekvivalenssirelaation kanssa*

Todistus. Yhteenlaskun yhteensopivuus seuraa tekijäryhmien vastaavasta tuloksesta. Tarkastelemme siis vain kertolaskua: 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 ideaali. Siis $ab \sim a'b'$. □

Proposition 14.21 mukaan renkaan R molemmat laskutoimitukset määrittelevät tekijälaskutoimituksen tekijäjoukossa $R/\mathscr{I}$. Ideaalia $\mathscr{I}$ vastaaville sivuluokille käytetään additiivista merkintää $x + \mathscr{I}$, jolloin laskutoimitukset ovat siis

$$(x + \mathscr{I}) + (y + \mathscr{I}) = (x + y) + \mathscr{I}$$

ja

$$(x + \mathscr{I})(y + \mathscr{I}) = xy + \mathscr{I}$$

kaikille $x, y \in R$. Seuraava tulos yleistää Esimerkkien 8.2(b) ja 8.14(a) tulokset kokonaislukurenkaan tilanteesta yleiseen tapaukseen:

Propositio 14.22. *Olkoon R rengas ja olkoon $\mathscr{I}$ sen ideaali. Tällöin tekijäjoukko $R/\mathscr{I}$ on rengas ja luonnollinen kuvaus $R \to R/\mathscr{I}$ on rengashomomorfismi.*

Todistus. Harjoitustehtävä 14.11. □

Propositio 3.9 antaa seurauksena

Propositio 14.23. *Tekijärengas on kommutatiivinen, jos alkuperäinen rengas on kommutatiivinen.* □

Tekijärenkaille pätee ryhmien isomorfismilausetta vastaava tulos:

Lause 14.24 (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 (Lause 7.24). Harjoitustehtävä 14.12. □

Esimerkki 14.25. (a) Koska R on aina renkaan R ideaali ja $R/R \cong \{0\}$, niin tekijärengas $R/\mathscr{I}$ voi olla kommutatiivinen vaikka R ei olisikaan. Toinen ääriesimerkki tekijärenkaasta on $R/\{0\} \cong R$.

(b) Olkoon $\Omega \neq \emptyset$ ja olkoon R rengas. Esimerkeissä 8.14 ja 14.14 tarkasteltu evaluaatiohomomorfismi $E_c\colon \mathscr{F}(\Omega, R) \to R$ on surjektio kaikille $c \in \Omega$, koska $E_c(\underline{a}) = a$ kaikille $a \in R$. Renkaiden isomorfismilauseen nojalla $\mathscr{F}(\Omega, R)/\ker E_c$ on rengasisomorfinen renkaan R kanssa kaikille $c \in \Omega$.

(c) Reaaliluvut konstruoidaan kurssilla Lukualueet (katso [LA], luku 5) rationaalilukujen Cauchyn jonojen renkaan nollaan suppenevien jonojen ideaalia vastaavana tekijärenkaana.

Määritelmä 14.26. Olkoon R rengas. Renkaan R ideaali $\mathscr{I}$ on *aito*, jos $\mathscr{I} \neq R$. Renkaan R aito ideaali $\mathscr{M}$ on *maksimaalinen*, jos se ei ole minkään aidon ideaalin aito osajoukko.

Proposition 14.7 mukaan kunnan nollaideaali on maksimaalinen.

Propositio 14.27. *Kokonaislukurenkaan ideaali $q\mathbb{Z}$, $q \geq 2$, on maksimaalinen, jos ja vain jos q on alkuluku.*

Todistus. Jos q ei ole alkuluku, niin $q = ab$ joillakin $a, b \in \mathbb{N} - \{0, 1\}$. Tällöin $q \in a\mathbb{Z}$, joten ideaali $q\mathbb{Z}$ sisältyy aidosti aitoon ideaaliin $a\mathbb{Z}$ eikä $q\mathbb{Z}$ siis ole maksimaalinen.

Olkoon q alkuluku ja olkoon $r\mathbb{Z}$ ideaali, joka sisältää aidosti ideaalin $q\mathbb{Z}$. Siis $r \neq \pm q$. Erityisesti $q \in r\mathbb{Z}$ ja koska q on alkuluku, pitää olla $r = \pm 1$. Siis $r\mathbb{Z} = \mathbb{Z}$. □

Lauseen 10.9 mukaan tekijärengas $\mathbb{Z}/q\mathbb{Z}$ on kunta täsmälleen silloin, kun q on alkuluku. Proposition 14.27 mukaan tämä on yhtäpitävää sen kanssa, että $q\mathbb{Z}$ on kokonaislukurenkaan maksimaalinen ideaali. Seuraava havainto yleistää tämän havainnon.

Lause 14.28. *Olkoon $\mathscr{M}$ kommutatiivisen renkaan K maksimaalinen ideaali. Tällöin tekijärengas $K/\mathscr{M}$ on kunta.*

Todistus. Proposition 14.22 nojalla tekijärengas $K/\mathscr{M}$ on kommutatiivinen. Koska $\mathscr{M}$ on renkaan K aito osajoukko, niin tekijärenkaassa $K/\mathscr{M}$ on ainakin kaksi alkiota. Olkoon $a + \mathscr{M} \in K/\mathscr{M} - \{0\}$. Harjoitustehtävässä 14.14 osoitetaan, että

$$\mathscr{N} = \{ak + m : k \in K, m \in \mathscr{M}\}$$

on renkaan K ideaali. Ideaali $\mathscr{N}$ sisältää aidosti ideaalin $\mathscr{M}$, koska $a \in \mathscr{N} - \mathscr{M}$. Koska $\mathscr{M}$ on maksimaalinen, pätee $\mathscr{N} = K$. Erityisesti $1 \in \mathscr{N}$, joten on $k \in K$ ja $m \in \mathscr{M}$ siten, että $ak + m = 1$. Mutta tästä saadaan

$$(a + \mathscr{M})(k + \mathscr{M}) = ak + \mathscr{M} = 1 - m + \mathscr{M} = 1 \in K/\mathscr{M}\,,$$

joten $a + \mathscr{M}$ on yksikkö. □

Seuraavat tulokset antavat keinon maksimaalisten ideaalien tunnistamiseen joissain tapauksissa.

Lause 14.29. *Olkoon K pääideaalialue ja olkoon $a \in K - \{0\}$. Tällöin (a) on maksimaalinen ideaali, jos ja vain jos a on jaoton.*

Todistus. Olkoon a jaoton ja olkoon $\mathscr{N}$ ideaali, joka sisältää pääideaalin (a). Koska K on pääideaalialue, niin $\mathscr{N} = (b)$ jollain $b \in K$. Pätee siis $a = qb$ jollain $q \in K$. Koska a on jaoton, täytyy olla $q \in K^\times$ tai $b \in K^\times$. Jos q on yksikkö, niin Lemman 14.16 nojalla $\mathscr{N} = (b) = (qb) = (a)$. Jos taas b on yksikkö, niin Lemman 14.5 nojalla $\mathscr{N} = (b) = K$. Siis (a) on maksimaalinen.

Toinen suunta osoitetaan Harjoitustehtävässä 14.15. □

Seuraus 14.30. *Olkoon K Eukleideen alue ja olkoon $a \in K - \{0\}$. Tällöin (a) on maksimaalinen ideaali, jos ja vain jos a on jaoton.*

Todistus. Seuraa Lauseista 14.18 ja 14.29. □

Esimerkki 14.31. Esimerkissä 13.9 osoitettiin, että Gaussin kokonaislukujen rengas $\mathbb{Z}[i]$ on Eukleideen alue. Tarkastamalla kaikki Gaussin kokonaisluvut, joiden normi on pienempi kuin 9, huomaamme, että $3 \in \mathbb{Z}[i]$ on jaoton. Siis

$$3\,\mathbb{Z}[i] = \{3z : z \in \mathbb{Z}[i]\}$$

on renkaan $\mathbb{Z}[i]$ maksimaalinen ideaali Seurauksen 14.30 nojalla. Lauseen 14.28 nojalla tekijärengas $\mathbb{Z}[i]/3\,\mathbb{Z}[i]$ on kunta . Siinä on yhdeksän alkiota $0+3\mathbb{Z}[i]$, $1+3\mathbb{Z}[i]$, $2+3\mathbb{Z}[i]$, $i+3\mathbb{Z}[i]$, $1+i+3\mathbb{Z}[i]$, $2+i+3\mathbb{Z}[i]$, $2i+3\mathbb{Z}[i]$, $1+2i+3\mathbb{Z}[i]$ ja $2+2i+3\mathbb{Z}[i]$.

Seuraus 14.32. *Olkoon K kunta ja olkoon $P(X) \in K[X]$ jaoton. Tällöin $(P(X))$ on maksimaalinen ideaali.*

Todistus. Polynomirengas $K[X]$ on Eukleideen alue Seurauksen 13.11 nojalla. Väite seuraa siis soveltamalla Seurausta 14.30. □

Esimerkki 14.33. Polynomirengas $\mathbb{C}[X]$ on Euklidinen rengas koska $\mathbb{C}$ on kunta. Seurauksen 14.30 mukaan sen maksimaaliset ideaalit ovat ovat jaottomien polynomien virittämät pääideaalit. Algebran peruslauseen nojalla $\mathbb{C}$ on algebrallisesti suljettu, joten $P(X) \in \mathbb{C}[X]$ on jaoton, jos ja vain jos $\deg P(X) = 1$. Jos $\deg P(X) = 1$, niin $P(X) = aX + b$ joillakin $a \in \mathbb{C}^\times$ ja $b \in \mathbb{C}$. Siis $P(X) = a(X - \frac{b}{a})$. Lemman 14.16 mukaan $(P(X)) = (X - \frac{b}{a})$, joten polynomirenkaan $P(X) \in \mathbb{C}[X]$ maksimaaliset ideaalit ovat täsmälleen pääideaalit $(X - c)$, $c \in \mathbb{C}$.

Seuraava tulos osoittaa, että kuntakertoimisesta polynomirenkaasta $K[X]$ saadaan jaottoman polynomin avulla muodostettua tarkasteltavan kerroinkunnan kuntalaajennus k. Konstruktiossa käytetyllä polynomilla $P(X) \in K[X]$ ei ole juurta kunnassa K ei ole juuria Proposition 12.5 nojalla. Kun polynomin $P(X)$ kertoimet ajatellaan uuden kunnan alkioiksi samastamalla K vakiopolynomien antaman alikunnan kanssa, havaitaan, että polynomilla $P(X) \in k[X]$ on juuri.

Seuraus 14.34. *Olkoon K kunta ja olkoon $P(X) \in K[X]$ jaoton. Tällöin tekijärengas $K[X]/(P(X))$ on kunta. Kunnalla $k = K[X]/(P(X))$ on alikunta, joka on isomorfinen kunnan K kanssa. Polynomilla $P(X) \in k[X]$ on juuri.*

Todistus. Ensimmäinen väite seuraa Lauseesta 14.28 ja Seurauksesta 14.30.

Olkoon $i\colon K \to K[X]$ homomorfismi, joka kuvaa alkion $a \in K$ polynomiksi $a \in K[X]$ ja olkoon $\Phi\colon K[X] \to K[X]/(P(X))$ luonnollinen homomorfismi. Propositioiden 11.2 ja 14.22 mukaan kuvaus $\Phi \circ i$ on kuntahomomorfismi, joten se on injektio. Toinen väite seuraa tästä.

Osoitetaan vielä, että polynomilla $P(X) \in k[X]$ on juuri. Olkoon $\alpha = \Phi(X) \in k$ ja olkoon $P(X) = \sum_{k=0}^{n} b_k X^k$. Tällöin pätee

$$\begin{aligned} P(\alpha) = P(X + (P(X))) &= \sum_{k=0}^{n} (b_k + (P(X))(X + (P(X)))^k \\ &= \sum_{k=0}^{n} (b_k + (P(X))(X^k + (P(X))) = P(X) + (P(X)) = 0\,, \end{aligned}$$

joten α on polynomin $P(X) \in k[X]$ juuri. □

Esimerkki 14.35. Polynomi $X^2 + 1 \in \mathbb{R}[X]$ on jaoton, koska sillä ei ole juurta. Tekijärengas $k = \mathbb{R}[X]/(X^2 + 1)$ on Seurauksen 14.34 nojalla kunta ja polynomilla $X^2 + 1 \in k[X]$ on juuri.

Reaalikertoimisten polynomien rengas $\mathbb{R}[X]$ on kompleksikertoimisten polynomien renkaan $\mathbb{C}[X]$ alirengas ja Seurauksen 12.12 nojalla reaalikertoimiset polynomit voidaan samastaa kompleksitasossa määriteltyjen reaalikertoimisten polynomifunktioiden renkaan kanssa.

Olkoon $E_i\colon \mathbb{C}[X] \to \mathbb{C}$ Esimerkissä 8.14 määritelty evaluaatiokuvaus. Proposition 12.5 nojalla $\ker E_i = (X - i)$. Rajoittumakuvaus $E_i|_{\mathbb{R}[X]}\colon \mathbb{R}[X] \to \mathbb{C}$ on surjektiivinen rengashomomorfismi, koska $E_i(bX + a) = a + ib$ kaikilla $a, b \in \mathbb{R}$. Sen ydin on jaottoman polynomin $X^2 + 1 \in \mathbb{R}[X]$ virittämä pääideaali $(X^2 + 1)$: Harjoitustehtävän 2.7 mukaan $-i$ on jokaisen sellaisen polynomin $P(X) \in \mathbb{C}[X]$ juuri, jonka kertoimet ovat reaalisia ja jonka yksi juuri on i. Siis jokainen homomorfismin E_i ytimeen kuuluva polynomi on jaollinen polynomilla $X^2 + 1 = (X - i)(X + i)$, joten $\ker E_i|_{\mathbb{R}[X]} = (X^2 + 1)$. Renkaiden isomorfismilauseen mukaan kunta $\mathbb{R}[X]/(X^2 + 1)$ on isomorfinen kompleksilukujen kunnan $\mathbb{C}$ kanssa.

Seuraava havainto on hyödyllinen äärellisten kuntien konstruktiossa, todistamme hieman yleisemmän version, koska todistus on riippumaton siitä, onko tarkasteltava polynomi jaoton vai ei.

Lause 14.36. *Olkoon K kunta ja olkoon $P(X) \in K[X]$ polynomi, jonka aste on $d \geq 1$. Jos kunnassa K on q alkiota, niin renkaassa $K[X]/(P(X))$ on q^d alkiota.*

Todistus. Kuntakertoimisten polynomien jakoyhtälön (Seuraus 11.9) nojalla jokaisella ekvivalenssiluokalla $Q(X) + (P(X)) \in K[X]/(P(X))$ on edustaja $\bar{Q}(X)$, jolle pätee $\deg \bar{Q}(X) < \deg P(X) = d$:

$$Q(X) = T(X)P(X) + \bar{Q}(X)$$

yksikäsitteiselle $T(X) \in K[X]$. Tällaisia polynomeja on q^d kappaletta ja mitkään kaksi eivät ole ekvivalentteja. □

Esimerkki 14.37. Esimerkissä 12.7 osoitimme, että polynomi $P(X) = X^2 + X + 1$ on jaoton toisen asteen polynomi polynomirenkaassa $(\mathbb{Z}/2\mathbb{Z})[X]$. Seurauksen 14.30 ja Lauseen 14.36 nojalla $\mathbb{F}_4 = (\mathbb{Z}/2\mathbb{Z})[X]/(P(X))$ on neljän alkion kunta.

Lauseen 14.36 todistuksesta seuraa, että kunnan $\mathbb{F}_4$ alkiot ovat $0 = (P(X))$, $1 = 1 + (P(X))$, $\alpha = X + (P(X))$ ja $\alpha + 1 = X + 1 + (P(X))$. Neljän alkion kunnan yhteen- ja kertolaskun laskutaulut ovat

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
α+1	$\alpha+1$	α	1	0

ja

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
α+1	0	$\alpha+1$	1	α

.

Laskutaulusta huomaa, että kunnan $\mathbb{F}_4$ additiivinen ryhmä on isomorfinen Esimerkissä 4.11 tarkastellun Kleinin neliryhmän $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ kanssa.

Seurauksessa 14.34 totesimme, että kunnalla $\mathbb{F}_4$ on alikunta, joka on isomorfinen kunnan $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ kanssa, tämä alikunta koostuu tietenkin alkioista $0, 1 \in \mathbb{F}_4$. Harjoitustehtävässä 10.11 osoitettiin, että $\mathbb{F}_4$ on $\mathbb{F}_2$-vektoriavaruus. On helppo nähdä, että esimerkiksi alkiot 1 ja α muodostavat tämän $\mathbb{F}_2$-vektoriavaruuden kannan.

Ennen Esimerkkiä 14.37 olemme tavanneet äärellisistä kunnista ainoastaan kunnat $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, missä p on alkuluku. Erityisesti näiden kuntien alkioiden lukumäärä on alkuluku. Esimerkin 14.37 tulos yleistyy kaikille alkulukupotensseille p^q.

Lause 14.38. *Jokaiselle luonnolliselle luvulle $q \geq 1$ ja alkuluvulle p on äärellinen kunta, jossa on p^q alkiota. Toisaalta jokaisessa äärellisessä kunnassa on p^q alkiota joillain tällaisilla p ja q.*

Todistus. Proposition 10.20 mukaan äärellisessä kunnassa on p^q alkiota jollain alkuluvulla p ja jollain luonnollisella luvulla $q \geq 1$. Emme osoita tällä kurssilla äärellisen kunnan olemassaoloa yleisessä tapauksessa. Harjoitustehtävän 12.6 ja Lauseen 14.36 nojalla kaikilla alkuluvuilla $p \equiv 3 \mod 4$ on kunta, jossa on p^2 alkiota. Harjoitustehtävissä tehdään muutamia muita erikoistapauksia. Koko lauseen todistus on esimerkiksi lähteissä [DF, Luku 14.3] ja [War, Luku39] ja kursseilla Algebra 2 ja Äärelliset kunnat. □

Harjoitustehtäviä.

14.1. Olkoon K kommutatiivinen rengas. Alkion $k \in K$ *annihilaattori* on

$$\{a \in K : ak = 0\}.$$

Osoita, että annihilaattori on ideaali.

14.2. Olkoon R rengas ja olkoon $\mathscr{I}$ renkaan R epätyhjä osajoukko. Osoita, että $\mathscr{I}$ on ideaali, jos ja vain jos $xa + x'a', ax + a'x' \in \mathscr{I}$ kaikilla $x, x' \in R$ ja $a, a' \in \mathscr{I}$.

14.3. Olkoon $\psi\colon R \to S$ rengashomomorfismi. Olkoon $\mathscr{I}$ renkaan R ideaali. Osoita, että $\psi(\mathscr{I})$ on renkaan $\psi(R)$ ideaali.

14.4. Anna esimerkki, joka osoittaa, että tehtävän 14.3 tilanteessa $\psi(\mathscr{I})$ ei välttämättä ole renkaan S ideaali.

14.5. Olkoot $\mathscr{I}_i$, $i \in I$, renkaan R ideaaleja. Osoita, että $\bigcap_{i\in I} \mathscr{I}_i$ on renkaan R ideaali.

14.6. Olkoon K kommutatiivinen rengas. Osoita, että renkaan K nilpotentit alkiot muodostavat ideaalin.

14.7. Olkoon K kommutatiivinen rengas. Olkoot $a_1, a_2, \ldots a_n \in K$. Osoita, että

$$\{x_1a_1 + x_2a_2 + \cdots + x_na_n : x_1, x_2, \ldots, x_n \in K\}$$

on renkaan K ideaali.

14.8. Olkoon K kunta ja olkoon R rengas, jossa on vähintään kaksi alkiota. Olkoon $\phi\colon K \to R$ rengashomomorfismi. Osoita, että ϕ on injektio.

14.9. Oletetaan, että $\{0\}$ ja K ovat kommutatiivisen renkaan K ainoat ideaalit. Osoita, että K on kunta.

14.10. Olkoon R on rengas ja olkoon $u \in R^\times$. Osoita, että $(ua) = (a)$ kaikille $a \in R$.

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

14.12. Todista renkaiden isomorfismilause.

14.13. Osoita, että $\mathscr{I} = \{2, 4, 6\}$ on renkaan $\mathbb{Z}/6\mathbb{Z}$ ideaali. Osoita, että tekijäryhmä $(\mathbb{Z}/6\mathbb{Z})/\mathscr{I}$ on rengasisomorfinen renkaan $\mathbb{Z}/2\mathbb{Z}$ kanssa.

14.14. Olkoon $\mathscr{I}$ kommutatiivisen renkaan K ideaali ja olkoon $a \in K$. Osoita, että

$$\mathscr{N} = \{ak + m : k \in K, m \in \mathscr{I}\}$$

on renkaan K ideaali.

14.15. Olkoon K kokonaisalue ja olkoon $a \in K - \{0\}$ alkio, joka ei ole jaoton. Osoita, että (a) ei ole maksimaalinen ideaali.

14.16. Olkoon K kunta ja olkoon $P(X) \in K[X]$ jaoton polynomi. Osoita, että kunta $K[X]/(P(X))$ sisältää alikunnan, joka on isomorfinen kunnan K kanssa.

14.17. Osoita, että polynomi $X^3 + X^2 + X + 2 \in (\mathbb{Z}/3\mathbb{Z})[X]$ on jaoton. Osoita tämän avulla, että on kunta, jossa on 27 alkiota.

14.18. Anna esimerkki jaottomasta toisen asteen polynomista polynomirenkaassa $(\mathbb{Z}/3\mathbb{Z})[X]$. Osoita tämän avulla, että on kunta, jossa on 9 alkiota.

14.19. Määritä kaikki korkeintaan neljännen asteen polynomit renkaassa $(\mathbb{Z}/2\mathbb{Z})[X]$, jotka eivät ole jaollisia ensimmäisen asteen polynomeilla,

14.20. Osoita, että on sellainen kunta, jossa on täsmälleen 16 alkiota.

---

[6]Vihje: Katso määritelmä luvusta 8. Huomaa, että potenssi n voi riippua alkiosta x. Käytä tehtävän 8.7 binomikaavaa.

[20]Vihje: Muista Tehtävät 12.2 ja 12.9.

Kommutatiivisen renkaan K ideaali $\mathscr{P} \neq K$ on *alkuideaali*, jos sillä on seuraava ominaisuus: Jos $a, b \in K$ ja $ab \in \mathscr{P}$, niin $a \in \mathscr{P}$ tai $b \in \mathscr{P}$.

14.21. Mitkä kokonaislukujen renkaan ideaalit ovat alkuideaaleja?

14.22. Olkoon K kommutatiivinen rengas ja olkoon $\mathscr{I} \neq K$ sen ideaali. Osoita, että tekijärengas $K/\mathscr{I}$ on kokonaisalue, jos ja vain jos $\mathscr{I}$ on alkuideaali.

14.23. Osoita, että kommutatiivisen renkaan jokainen maksimaalinen ideaali on alkuideaali.

14.24. Osoita, esimerkillä, että että kommutatiivisen renkaan alkuideaali ei välttämättä ole maksimaalinen.

Lukemista

Kurssit Algebra 1A ja Algebra 1B antavat perustietoja algebrasta. Kiinnostunut lukija voi tutustua algebraan laajemmin esimerkiksi seuraavan luettelon kirjojen avulla. Hyviä kirjoja, jotka laajentavat kurssien Algebra 1A ja 1B materiaalia ovat esimerkiksi [Dur], [Gil], [God], [HA], [Lan], [Pin]. Bourbakin kirja [Bou] on hyvin perusteellinen. Lähteet [Art] ja [DF] ovat erinomaisia hieman haastavampia lähteitä. Armstrongin kirja [Arm] käsittelee ryhmäteoriaa geometrisesti ja sen geometrisia sovelluksia.

Viitteet

[Arm] M. A. Armstrong. *Groups and symmetry*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1988.

[Art] M. Artin. *Algebra*. Prentice Hall Inc., Englewood Cliffs, NJ, 1991.

[Bou] N. Bourbaki. *Algebra I. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998.

[DF] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[Dur] J. R. Durbin. *Modern algebra*. John Wiley & Sons Inc., New York, third edition, 1992.

[Gil] W. J. Gilbert. *Modern algebra with applications*. Wiley-Interscience, New York, 1976.

[God] R. Godement. *Algebra*. Hermann, Paris, 1968.

[Gre] W. Greub. *Linear algebra*. Springer-Verlag, New York, fourth edition, 1975. Graduate Texts in Mathematics, No. 23.

[HA] A. P. Hillman and Alexanderson. *A first undergraduate course in abstract algebra*. Wadsworth, 1987.

[Lan] S. Lang. *Undergraduate Algebra*. Springer, 1987.

[Pin] C. C. Pinter. *A book of abstract algebra*. Dover Publications Inc., Mineola, NY, 2010.

[Väi] K. Väisälä. *Lukuteorian ja korkeamman algebran alkeet*. Otava, 1950.

[War] S. Warner. *Modern algebra. Vols. I, II*. Prentice-Hall Inc., Englewood Cliffs, N.J., 1965.

Täydentävää materiaalia on myös kurssien Lukualueet, Ryhmät ja geometria ja Äärelliset kunnat monisteissa, jotka ovat saatavana kyseisten kurssien kotisivuilta:

[LA] Lukualueet: `http://users.jyu.fi/~parkkone/LA2012/`

[RG] Ryhmät ja geometria: `http://users.jyu.fi/~parkkone/RG2012/`

[ÄK] Äärelliset kunnat: `http://users.jyu.fi/~lehtonen/opetus/sl2013/`