

ALGEBRA

KEVÄT 2011

JOUNI PARKKONEN

SISÄLTÖ

1. Laskutoimitukset	1
2. Kompleksiluvut	8
3. Tekijälaskutoimitus, kokonaisluvut ja rationaaliluvut	15
4. Ryhmät	20
5. Aliryhmät	26
6. Äärelliset permutaatioryhmät	32
7. Normaali aliryhmä ja tekijäryhmä	39
8. Renkaat	47
9. Kokonaislukujen jaollisuus	55
10. Polynomit	61
11. Ideaalit ja tekijärenkaat	67
Lukemista	72

1. LASKUTOIMITUKSET

Algebra käsittelee laskemista. Osin tämä tarkoittaa “numeroilla laskemista” luvkualueissa $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ laskutoimituksilla $+$ ja $\cdot$ ja niiden käänteisoperaatioilla $-$ ja $/$ siinä määrin kuin käänteisoperaatiot ovat hyvin määriteltäviä. Tällä kurssilla yleistämme laskutoimituksen käsitteen ja tarkastelemme erilaisia laskutoimitusten määrittämiä niinsanottuja algebrallisia rakenteita. Keskeisessä osassa on “abstrakti laskeminen”, jossa ei tiedetä tai välitetä siitä, millä lasketaan, vaan tehdään päätelmiä, kun laskutoimitusten jotkin ominaisuudet tunnetaan. Lisäksi tarkastelemme kuvauksia, “jotka säilyttävät algebralliset rakenteet”.

Yksi algebran keskeinen ajatus on se, että erilaisissa matemaattisissa yhteyksissä tunnustetaan samankaltaisia rakenteita, esimerkiksi havaitaan, että laskutoimituksilla on sopivia lisäominaisuuksia. Jos osoittautuu, että nämä lisäominaisuudet määrittelevät jonkin algebrallisen rakenteen (ryhmä, rengas, ...), voidaan tarkasteltavaa tilannetta usein ymmärtää paremmin näille algebrallisille rakenteille todistettujen yleisten tulosten avulla. Näin voidaan nähdä yleisiä rakenteita teknisten ominaisuuksien takana.

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

Määritelmä 1.1. Epätyhjän joukon A *laskutoimitus* on kuvaus $*$: $A \times A \rightarrow A$. *Laskutoimituksella varustettu joukko* on pari $(A, *)$, missä $*$ on joukon A laskutoimitus.

Laskutoimituksen tulosta merkitään yleensä $a * a' = *(a, a')$. Laskutoimitus on siis sääntö, joka liittää kahteen joukon A alkioon a, a' joukon A alkion $a * a'$.

Luonnollisten lukujen joukko on tällä kurssilla

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

Joskus nollaa ei haluta lukea luonnolliseksi luvuksi eikä tästä valinnasta tule suu-
rempia ongelmia.

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

Samassa joukossa E voidaan määritellä erilaisia laskutoimituksia kuten Esimerkissä 1.2 havaittiin. Tarkastelemme tällä kurssilla myös *renkaiden* teoriaa, renkaat ovat kahdella laskutoimituksella varustettuja joukkoja, joiden laskutoimituksilta vaaditaan muutamia lisäominaisuuksia, jotka esimerkiksi kokonais-, rationaali- ja reaalilukujen yhteen- ja kertolaskulla on.

Jos $*_A$ on laskutoimitus joukossa A ja $*_B$ on laskutoimitus joukossa B , niiden avulla voidaan määritellä laskutoimitus joukossa $A \times B$:

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

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

Esimerkki 1.3. (a) Luonnollisten lukujen yhteenlaskun avulla saadaan *komponentteittainen yhteenlasku* joukkoon $\mathbb{N} \times \mathbb{N}$ määrittelemällä se komponenttien yhteenlaskun tulolaskutoimituksena $(m, n) + (p, q) = (m + p, n + q)$.

(b) Avaruudessa $\mathbb{R}^n$ määritellään *komponentteittainen yhteenlasku* vastaavalla tavalla

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

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

Esimerkki 1.4. (a) Joukon X osajoukot muodostavat *potenssijoukon* $\mathcal{P}(X) = \{A \subset X\}$. Esimerkiksi, kun $X = \{0, 1\}$, niin

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

Joukkojen leikkaus $(A, B) \mapsto A \cap B$ ja yhdiste $(A, B) \mapsto A \cup B$ ovat laskutoimituksia potenssijoukossa $\mathcal{P}(X)$.

(b) Olkoon $X \neq \emptyset$, ja olkoon $\mathcal{F}(X) = \{f: X \rightarrow X\}$. Kuvausten yhdistäminen on laskutoimitus joukossa $\mathcal{F}(X)$: $(f, g) \mapsto f \circ g$.

(c) Olkoon $M_n(\mathbb{R})$ reaalisten $n \times n$ -matriisien joukko. Kurssilla Lineaarialgebra 1 määriteltiin kaksi laskutoimitusta joukossa $M_n(\mathbb{R})$. Seuraavassa, jos C on matriisi, merkintä C_{lm} tarkoittaa sen lm -kerrointa. Matriisien yhteenlasku määritellään komponentteittain 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

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

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

Jos samassa lausekkeessa esiintyy useita laskutoimituksia, niiden suorittamisjärjestystä ohjataan suluilla: Sulkujen sisällä olevat laskutoimitukset tehdään aina ensin ja sisäkkäisiä sulkuja sisältävät lausekkeet käsitellään ”sisältä lähtien” vastaavaan tapaan kuin esimerkiksi lausekkeessa $a(b + ((cd)(e + f)))$ lasketaan ensin summa $(e + f)$ ja tulo (cd) , näiden laskujen tulokset kerrotaan keskenään, saatu tulos lisätään lukuun b ja lopulta tämän laskun tuloksella kerrotaan a . 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 $a, b \in A$.

Jos joukossa A on määritelty kaksi laskutoimitusta $*$ ja $\oplus$, niin 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*. Distributiivisuutta sanotaan myös *osittelulaiksi*.

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: $a \cdot b = ab$.

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, esimerkiksi Harjoitustehtävässä 6 käsiteltävä ristitulo ei ole assosiatiivinen.

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).
 (3) $m(n + l) = mn + ml$ kaikilla m, n, l , eli kertolasku on distributiivinen yhteenlaskun suhteen.

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

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

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

kaikilla $x \in X$ ja

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

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

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

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 $g \in A$.
- 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 1.8. Luku 0 on luonnollisten lukujen, kokonais-, rationaali ja reaalilukujen yhteenlaskun neutraalialkio, ja luku 1 on kertolaskun neutraalialkio. Useimmilla luonnollisilla luvuilla ei ole käänteisalkiota kummankaan laskutoimituksen suhteen, 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: $0x = x0 = 0 \neq 1$ kaikilla luvuilla x . Kaikilla nollasta poikkeavilla rationaali- ja reaaliluvuilla x taas on käänteisluku $x^{-1} = 1/x$, esimerkiksi rationaaliluvulle $a/b \neq 0$ pätee $(a/b)^{-1} = b/a$.

Esimerkki 1.9. (a) Identtinen kuvaus $\text{id} = \text{id}_X$ on joukon $\mathcal{F}(X)$ laskutoimituksen $\circ$ neutraalialkio:

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

kaikilla $f \in \mathcal{F}(X)$. Jos $f \in \mathcal{F}(X)$ on bijektio, sen käänteiskuvaus f^{-1} on kuvauksen f käänteisalkio laskutoimituksen $\circ$ suhteen: $f \circ f^{-1} = \text{id} = f^{-1} \circ f$. Muilla joukon $\mathcal{F}(X)$ alkioilla ei ole käänteisalkiota.

(b) Varustamme nyt joukon $X \neq \emptyset$ potenssijoukon laskutoimituksella $\setminus$, joka määritellään

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

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

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 merkin-
tää $-x$.

Lause 1.10. *Olkoon $(X, *)$ laskutoimituksella varustettu joukko.*

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

Todistus. (1) Käyttämällä oletettuja ominaisuuksia ylläolevassa järjestyksessä saadaan $e = e * e' = e'$. Koska e siis toteuttaa $e * g = g$ ja $g * e = g$ kaikilla $g \in X$, e on neutraalialkio.

(2) Todistamme kohdan (a): Olkoon g' alkion g vasen käänteisalkio, ja olkoon g'' sen oikea käänteisalkio. Tällöin

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

Tällöin siis g' on alkion g käänteisalkio. Toinen suunta seuraa suoraan määritelmästä. Kohdat (b) ja (c) todistetaan harjoituksissa. $\square$

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 sen indusoivalle laskutoimitukselle $*$: $*|_B = *$.

Esimerkki 1.11. Olkoon

$$P = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) : c = 0 \right\} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{R}) \right\}.$$

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 .

Määritelmä 1.12. Olkoot $(E, *)$ ja $(E', \otimes)$ laskutoimituksella varustettuja joukkoja. Kuvaus $h: (E, *) \rightarrow (E', \otimes)$ on *homomorfismi*, jos $h(a * b) = h(a) \otimes h(b)$ kaikille $a, b \in E$.

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

Laskutoimituksella varustetut joukot $(E, *)$ ja $(E', \otimes)$ ovat *isomorfsia (keskenään)*, jos on isomorfismi $h: (E, *) \rightarrow (E', \otimes)$.

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 1.13. (a) Reaalilukujen kertolasku indusoi laskutoimituksen positiivisten reaalilukujen joukossa $\mathbb{R}_+ =]0, \infty[$. Eksponenttikuvaus $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_+, \cdot)$, $\exp(x) = e^x$ 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, siis se on isomorfismi. Eksponenttifunktion käänteisfunktio $\log: (\mathbb{R}_+, \cdot) \rightarrow (\mathbb{R}, +)$ on myös homomorfismi (ja tietysti myös isomorfismi): Kaikille $x, y \in \mathbb{R}_+$ pätee

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

(b) Yhteenlaskulla varustetut joukot $(M_n(\mathbb{R}), +)$ ja $(\mathbb{R}^{n^2}, +)$ ovat selvästi isomorfisia.

(c) Kuvaus $h: \mathbb{Z} \rightarrow M_2(\mathbb{R})$,

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

on homomorfismi, kun kokonaisluvut varustetaan yhteenlaskulla ja $M_2(\mathbb{R})$ 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 1.13 avulla huomaamme.

Propositio 1.14. *Olkoon $h: (E, *) \rightarrow (E', \otimes)$ surjektiivinen homomorfismi.*

- (1) *Jos $*$ on kommutatiivinen, niin $\otimes$ on kommutatiivinen*
- (2) *Jos $*$ on assosiatiivinen, niin $\otimes$ 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

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

joten $\otimes$ on kommutatiivinen.

(2) Harjoitustehtävä.

(3) Olkoon $g' \in E'$. Tällöin $g' = h(g)$ jollain $g \in E$ ja pätee

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

ja

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

joten $h(e)$ on neutraalialkio. □

Neutraalialkio ei välttämättä kuvaudu neutraalialkiolle, jos homomorfismi ei ole surjektiivinen. Helppo esimerkki tästä ilmiöstä on homomorfismi $h: (\mathbb{N}, +) \rightarrow (\mathbb{N}, \cdot)$, $h(n) = 0$ kaikilla $n \in \mathbb{N}$. Kuvaus h on todellakin homomorfismi koska kaikille $m, n \in \mathbb{N}$ pätee

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

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

Harjoitustehtäviä.

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

Tehtävä 2. Onko laskutoimituksilla $\cap$ ja $\cup$ neutraali-alkiot? Onko jokaisella $A \in \mathcal{P}(X)$ käänteisalkiot laskutoimitusten $\cap$ ja $\cup$ suhteen?

Tehtävä 3. Onko joukon $\mathcal{P}(X)$ laskutoimitus $\setminus$ assosiatiivinen?

Tehtävä 4. Onko matriisien kertolasku assosiatiivinen joukossa $M_2(\mathbb{R})$? Onko se kommutatiivinen? Onko matriisien kertolaskulla neutraali-alkio joukossa $M_2(\mathbb{R})$?

Tehtävä 5. Olkoon

$$\Gamma = \{A \in M_2(\mathbb{R}) : \det A = 1\}.$$

Osoita, että matriisien kertolasku indusoi laskutoimituksen joukossa Γ . Miten matriisien yhteenlasku käyttäytyy?

Tehtävä 6. Avaruuden $\mathbb{R}^3$ vektoritulo eli *ristitulo* on laskutoimitus, joka määritellään asettamalla jokaiselle $a, b \in \mathbb{R}^3$

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

- (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.

Tehtävä 7. 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

Tehtävä 8. Olkoot $(A, *)$ ja $(C, \otimes)$ laskutoimituksella varustettuja joukkoja ja olkoon $f: (A, *) \rightarrow (C, \otimes)$ homomorfismi. Osoita:

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

Tehtävä 9. Olkoon $h: (E, *) \rightarrow (E', \otimes)$ surjektiivinen homomorfismi. Osoita: Jos $*$ on assosiatiivinen, niin $\otimes$ on assosiatiivinen.

⁶Vihje: Kannattaa kerrata lineaarialgebran tietoja. Assosiatiivisuuden puuttumisen voi nähdä esimerkiksi tarkastelemalla standardikantavektorien keskinäisiä tuloja.

2. KOMPLEKSILUVUT

Kompleksiluvut $\mathbb{C}$ saadaan varustamalla taso $\mathbb{R}^2$ komponenteittaisella yhteenlaskulla (joka on reaalilukujen yhteenlaskun tulo itsensä kanssa, katso Luku 1) 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 . Erityisesti otamme käyttöön merkinnät $(1, 0) = 1 \in \mathbb{C}$ ja $(0, 0) = 0 \in \mathbb{C}$.

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

$$(a, b) = (a, 0) + (0, b) = a(1, 0) + b(0, 1) = a + ib,$$

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

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

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

(b) $(1 + i)^2 = (1 \cdot 1 - 1 \cdot 1) + i(1 \cdot 1 + 1 \cdot 1) = 2i$.

(c) $\left(\frac{1+i}{\sqrt{2}}\right)^8 = i^4 = 1$.

Kompleksiluvun $z = a + ib$

- *reaaliosa* on $\operatorname{Re}(z) = a$,
- *imaginaariosa* on $\operatorname{Im}(z) = b$.
- *(kompleksi)konjugaatti* eli *liittoluku* on $\bar{z} = a - ib$
- *moduli* (eli itseisarvo) on

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

Propositio 2.2. (1) *Kompleksilukujen yhteen- ja kertolasku ovat assosiatiivisia ja kommutatiivisia laskutoimituksia.*

(2) *Yhteenlaskun neutraalialkio on 0 ja kertolaskun neutraalialkio on 1.*

(3) *Kompleksilukujen kertolasku on distributiivinen yhteenlaskun suhteen.*

(4) *Jokaisella kompleksiluvulla z on vastaluku $-z$ ja jokaisella nollasta poikkeavalla kompleksiluvulla z on käänteisluku*

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

(5) *Kuvaus $j: \mathbb{R} \rightarrow \mathbb{C}$, $j(x) = ix$ on injektiivinen homomorfismi yhteenlaskun ja kertolaskun suhteen.*

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

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

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

ja

$$j(x)j(y) = (x + 0i)(y + 0i) = (xy - 0) + i(x0 + 0y) = xy + 0i = j(xy).$$

□

Koska kompleksilukujen kertolasku on kommutatiivinen, niin kaikille $w \in \mathbb{C}$ pätee $wi = iw$. Erityisesti siis, jos $x \in \mathbb{R} \subset \mathbb{C}$, voidaan kompleksilukua xi merkitä haluttaessa myös ix . Jos x on “konkreettinen reaaliluku”, käytetään yleensä järjestystä xi kuten Esimerkissä 2.1.

Kannattaa huomata myös se, että kompleksilukujen kertolaskut voidaan laskea “tavallisilla laskusäännöillä” huomioimalla, että $i^2 = -1$

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

Lemma 2.3. *Kompleksikonjugoinnille ja modulille pätee kaikilla $z, w \in \mathbb{C}$*

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

Lisäksi moduli toteuttaa kolmioepäyhtälön:

$$|z + w| \leq |z| + |w|$$

kaikilla $z, w \in \mathbb{C}$, ja jos $x \in \mathbb{R} \subset \mathbb{C}$, niin sen moduli kompleksilukuna on sama kuin sen itseisarvo reaalilukuna.

Todistus. Kohdat (1)–(5) Harjoitustehtävässä 11.

Kolmioepäyhtälö on todistettu kurssilla Lineaarinen algebra ja geometria 1: Kompleksiluvun $z = x + iy$ moduli on vastaavan tason $\mathbb{R}^2$ pisteen (x, y) normi.

Viimeinen väite on selvä: Jos $x \in \mathbb{R} \subset \mathbb{C}$, niin $|x| = |x + 0i|$. □

Lemman 2.3 kohtien (1)–(3) avulla nähdään helposti

Propositio 2.4. *Kompleksikonjugointi on isomorfismi kompleksilukujen yhteenlaskun ja kertolaskun suhteen.*

Todistus. Ajatellaan ensin kompleksikonjugointia kuvauksena $k: (\mathbb{C}, +) \rightarrow (\mathbb{C}, +)$, $k(z) = \bar{z}$. Tällöin Lemman 2.3 kohdan (2) nojalla saadaan suoraan

$$k(z + w) = \overline{z + w} = \bar{z} + \bar{w} = k(z) + k(w),$$

joten k on homomorfismi. Lisäksi Lemman 2.3 kohdan (1) nojalla jokaiselle $z \in \mathbb{C}$ pätee $z = k(k(z))$, joten k on bijektio, ja ensimmäinen väite on todistettu.

Toinen väite todistetaan samalla tavalla Lemman 2.3 kohdan (3) avulla. □

Napakoordinaattikuvaus $N: \mathbb{R}_+ \times \mathbb{R} \rightarrow \mathbb{R}^2$,

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

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

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

Itse asiassa Lemman 2.3(5) nojalla

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

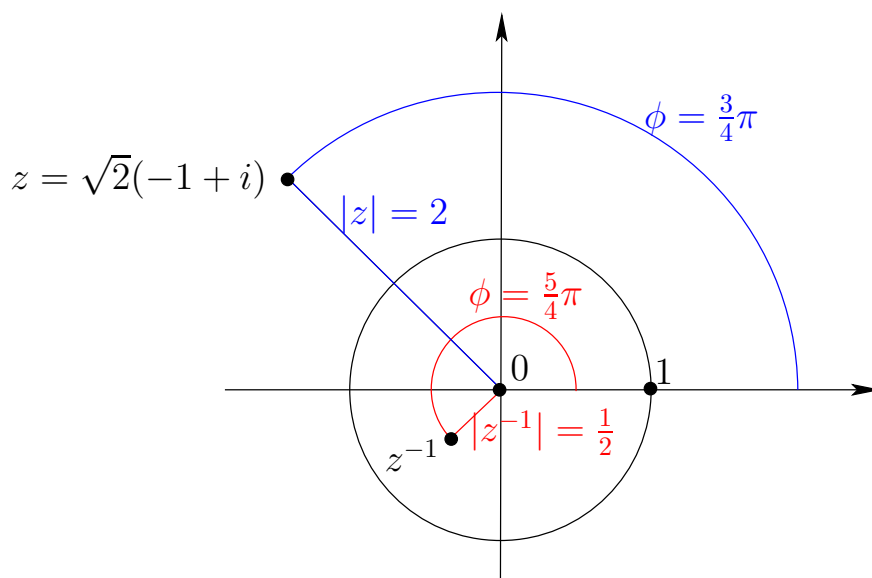
joten

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

missä $\phi \in \mathbb{R}$ on tason $\mathbb{R}^2$ vektorien $(1, 0)$ ja $(\operatorname{Re}(z), \operatorname{Im}(z))$ välinen kulma “positiiviseen kiertosuuntaan”. Kulma ϕ on kompleksiluvun z *argumentti*. Se on tarkalleen ottaen 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 saamme seuraavan tuloksen, jonka mukaan kompleksilukujen kertolasku sopii hyvin yhteen napakoordinaattiesityksen kanssa:

Propositio 2.5. (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 $z_k = r_k(\cos \phi_k + i \sin \phi_k)$, $k = 1, 2, \dots, n$. Tällöin

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

Todistus. Harjoitustehtävä 12. □

Sovellamme napakoordinaattiesitystä ja Propositiota 2.5 kompleksilukujen juurten tarkasteluun: Kompleksiluku z , jolle pätee $z^k = w$ on kompleksiluvun w k :s juuri. Erityisen tärkeitä ovat *ykkösen juuret*, jotka ovat ne kompleksiluvut $z \in \mathbb{C}$, joille pätee $z^k = 1$ jollain $k = 1, 2, 3, \dots$.

Lemma 2.6. Luvulla $1 \in \mathbb{C}$ on m kappaletta m . juuria. Jos

$$(1) \quad \zeta_m = \cos \frac{2\pi}{m} + i \sin \frac{2\pi}{m},$$

niin ykkösen m . juuret ovat $\zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}$ ja 1.

Todistus. Proposition 2.5 nojalla

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

Jos $n \in \{1, 2, \dots, m\}$, niin Proposition 2.5 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.

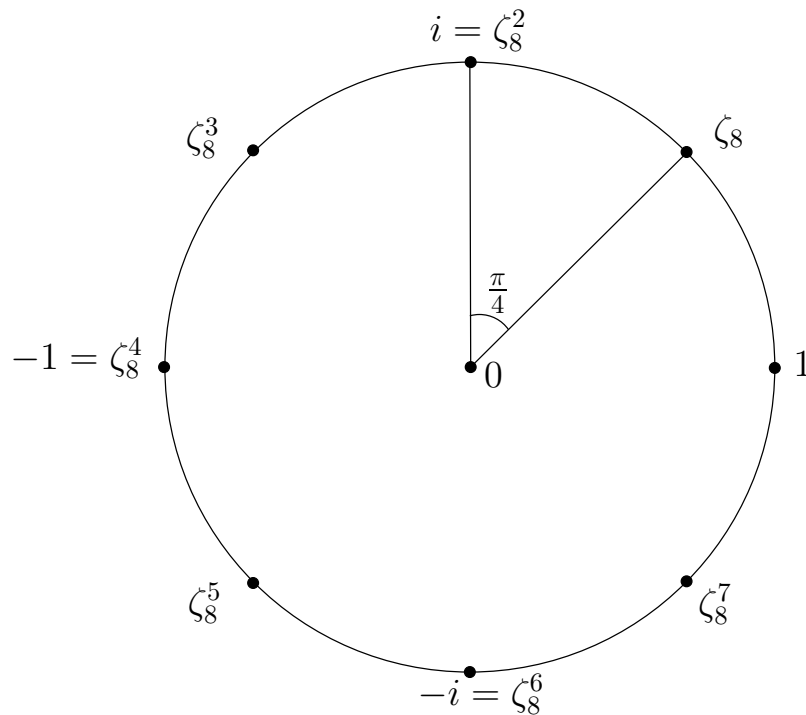
Toisaalta, jos $\zeta = r(\cos \phi + i \sin \phi)$ ja $\zeta^m = 1$, niin Proposition 2.5 nojalla $r^m = 1$ ja $m\phi = k2\pi$ jollakin $k \in \mathbb{Z}$. Siis $r = 1$ ja

$$\phi = \frac{k2\pi}{m} = D2\pi + \frac{R2\pi}{m}$$

joillekin $D, R \in \mathbb{Z}$, $0 \leq R \leq m-1$, sillä $k = Dm + R$ joillekin tällaisille kokonaisluvuille D ja R . Siis

$$\zeta = \cos \frac{R2\pi}{m} + i \sin \frac{R2\pi}{m} = \zeta_m^R,$$

joten kaikki ykkösen juuret sisältyvät joukkoon $\{1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}\}$. □



KUVA 2. Ykkösen kahdeksannet juuret.

Propositio 2.7. Jokaisella kompleksiluvulla $z \in \mathbb{C} \setminus \{0\}$ on m kappaletta m . juuria.
Jos

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

niin juuret ovat

$$w_1, w_1 \zeta_m, \dots, w_1 \zeta_m^{m-1},$$

missä

$$w_1 = \sqrt[m]{r} \left(\cos \frac{\phi}{m} + i \sin \frac{\phi}{m} \right)$$

ja

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

Todistus. Harjoitustehtävä 14. □

Esimerkki 2.8. Luvun $2 \in \mathbb{C}$ kolmannet juuret ovat $\sqrt[3]{2}$,

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

ja

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

Proposition 2.7 avulla voimme myös ratkaista toisen, kolmannen ja neljännen asteen polynomiyhtälöt.

Propositio 2.9. Olkoot $a_0, a_1 \in \mathbb{C}$. Olkoon $\sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}$ toinen kompleksiluvun $\left(\frac{a_1}{2}\right)^2 - a_0$ neliöjuurista. Luvut

$$z_1 = -\frac{a_1}{2} + \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0} \quad \text{ja} \quad z_2 = -\frac{a_1}{2} - \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}$$

ovat yhtälön

$$z^2 + a_1 z + a_0 = 0$$

ratkaisuja.

Todistus. Havaitsemme, että

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

mistä väite seuraa. □

Kaikki toisen asteen kompleksikertoimiset polynomiyhtälöt voidaan ratkaista Proposition 2.9 avulla. Kaikki kolmannen asteen kompleksikertoimiset yhtälöt saadaan muuttujanvaihdolla muotoon $z^3 + pz + q = 0$. Jos $u_0, v_0 \in \mathbb{C}$ siten, että

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

ja $\zeta_3 = -\frac{1}{2} + i \frac{\sqrt{3}}{2}$ on kaavan (1) antama ykkösen kolmas juuri, niin luvut $z_1 = u_0 + v_0$, $z_2 = \zeta_3 u_0 + \zeta_3^2 v_0$ ja $z_3 = \zeta_3^2 u_0 + \zeta_3 v_0$ ovat yhtälön $z^3 + pz + q = 0$ ratkaisuja. Alkupe-
räisen yhtälön juuret saadaan näistä tekemällä muuttujanvaihto toiseen suuntaan.

Neljännen asteen yhtälöiden ratkaisukaavat ovat samankaltaisia kuin kolmannen asteen tapauksessa. Kolmannen ja neljännen asteen yhtälöiden ratkaisemista käsitel-
lään enemmän kurssilla Lukualueet ja esimerkiksi kirjassa K. Väisälä: Lukuteorian ja korkeamman algebran alkeet. Kurssin lukualueet moniste on saatavissa tämän kurssin kotisivulta.

Abel osoitti vuonna 1826, että viidennen ja korkeamman asteen polynomeille ei ole samanlaista ratkaisualgoritmia kuin alemman asteen polynomeille. Tämän väitteen

todistuksessa käytetään yleensä ryhmäteoriaa, jota tarkastelemme luvusta 4 alkaen. Polynomeja tarkastellaan lähemmin tämän kurssin lopussa.

Jokaisella nollasta poikkeavalla kompleksiluvulla on käänteisalkio kertolaskun suhteen. Otamme käyttöön erityisen merkinnän

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

laskutoimituksella varustetulle joukolle $(\mathbb{C} \setminus \{0\}, \cdot)$. Vastaavasti

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

ja

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

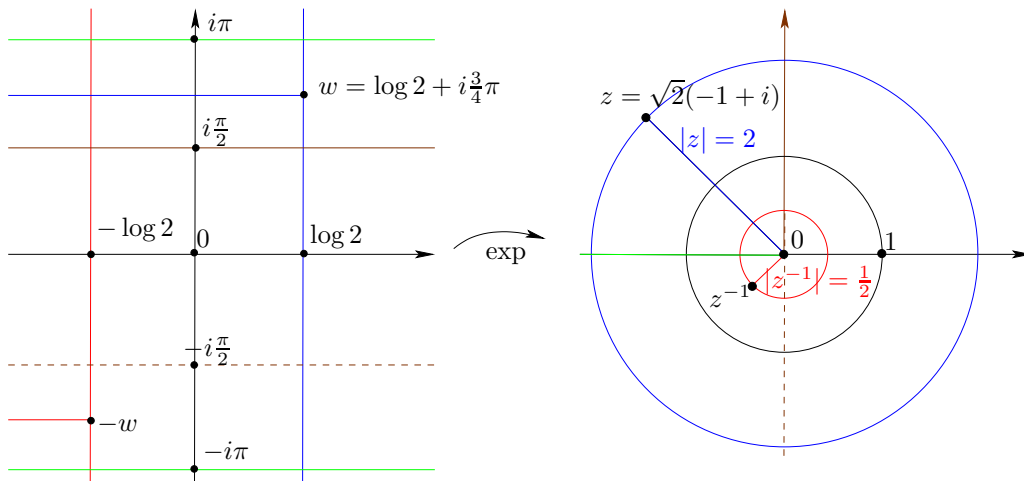
Näitä laskutoimituksella varustettuja joukkoja kutsutaan (kurssin aikana selvenevistä syistä) kompleksilukujen, reaalilukujen ja rationaalilukujen *multiplikatiivisiksi ryhmiksi*. Laskutoimituksella varustetut joukot $(\mathbb{C}, +)$, $(\mathbb{R}, +)$ ja $(\mathbb{Q}, +)$ taas ovat kompleksilukujen,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

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

Määritelmä 2.10. Kuvaus $\exp: \mathbb{C} \rightarrow \mathbb{C}$, joka määritellään asettamalla jokaiselle $z = x + iy \in \mathbb{C}$

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

on (kompleksinen) eksponenttifunktio.



KUVA 3. 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} .

Propositio 2.11. Eksponenttifunktio $\exp: (\mathbb{C}, +) \rightarrow \mathbb{C}^\times$ on surjektiivinen homomorfismi.

Todistus. Osoitamme ensin, että kompleksinen eksponenttifunktio on homomorfismi. Olkoot $z = x + iy, w = u + iv \in \mathbb{C}$. Tällöin reaalisen eksponenttifunktion laskusääntöjen ja Proposition 2.5 nojalla

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

Olkoon $g: \mathbb{R}^2 \rightarrow \mathbb{R}_+ \times \mathbb{R}$, $g(x, y) = (e^x, y)$. Tällöin $g(\mathbb{R}^2) = \mathbb{R}_+ \times \mathbb{R}$. Jos tulkitsemme kompleksisen eksponenttikuvauksen 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 surjektiivisiä. $\square$

Kompleksisen eksponenttifunktion avulla saadaan yksinkertainen lauseke ykkösen juurille: Yhtälön $z^m = 1$ ratkaisut ovat luvut

$$\zeta_m^R = e^{R \frac{2\pi}{m} i},$$

$$0 \leq R \leq m - 1.$$

Harjoitustehtäviä.

Tehtävä 10. Osoita, että kompleksilukujen kertolasku on assosiatiivinen ja kommutatiivinen laskutoimitus. Osoita, että kompleksilukujen kertolasku on distributiivinen yhteenlaskun suhteen. Onko kompleksilukujen yhteenlasku distributiivinen kertolaskun suhteen?

Tehtävä 11. Osoita, että kaikilla $z, w \in \mathbb{C}$ pätee

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

Tehtävä 12. Olkoot $z = r(\cos \phi + i \sin \phi)$, ja $w = s(\cos \theta + i \sin \theta)$. Osoita, että

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

Tehtävä 13. Olkoot $z_k = r_k(\cos \phi_k + i \sin \phi_k)$, $k = 1, 2, \dots, n$. Osoita induktiolla, että

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

Tehtävä 14. Osoita, että jokaisella kompleksiluvulla $z \in \mathbb{C} \setminus \{0\}$ on m kappaletta m . juuria.

Tehtävä 15. Määritä ykkösen kuudennet juuret. Kirjoita juuret muodossa, jossa ei käytetä trigonometrisiä funktioita eikä kompleksista eksponenttifunktiota. Piirrä kuva, jossa kaikki juuret esitetään tason pisteinä.

Tehtävä 16. Ratkaise yhtälöt $z^3 = i$ ja $z^5 = -\frac{1}{2}$ napakoordinaattien avulla. Havainnollista ratkaisuja kuvalla.

Tehtävä 17. Ratkaise yhtälöt $z^2 - z + 1 = 0$ ja $z^2 - iz + 1 = 0$.

Tehtävä 18. Olkoot $a_k \in \mathbb{R}$ kaikilla $k \in \{1, 2, \dots, n\}$ ja olkoon $z_0 \in \mathbb{C}$ yhtälön

$$(2) \quad \sum_{k=1}^n a_k z^k = 0$$

ratkaisu. Osoita, että $\bar{z}_0$ on yhtälön (2) ratkaisu.

¹⁰Vihje: Käytä reaali lukujen vastaavia ominaisuuksia, jotka oletamme tunnetuiksi

3. TEKIJÄLASKUTOIMITUS, KOKONAISLUVUT JA RATIONAALILUVUT

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 *relaatio* joukossa A .

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

Määritelmä 3.2. Joukon A relaatio R on

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

Jos relaatio on refleksiivinen, symmetrinen ja transitiivinen, se on *ekvivalenssirelaatio*. Jos R on ekvivalenssirelaatio joukossa A , sanotaan, että joukon A alkio a ja b ovat *ekvivalentteja*, jos $a R b$.

Ekvivalenssirelaation merkinä käytetään usein merkkiä $\sim$. Tällöin käytetään merkintää $a \sim b$, jos a ja b ovat ekvivalentteja.

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

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

on ekvivalenssirelaatiota $\sim$ vastaavaksi joukon A *tekijäjoukko*. Kuvaus $E \rightarrow E/\sim$, $a \mapsto [a]$, on ekvivalenssirelaatiota $\sim$ vastaava *tekijäkuvaus* eli *luonnollinen kuvaus*.

Ekvivalenssiluokat ovat erillisiä:

Lemma 3.4. 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 21. □

Jos

$$(3) \quad A = \bigcup_{i \in I} A_i$$

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 3.4 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 $x R y$, jos ja vain jos $x, y \in A_i$ jollain $i \in I$. Osoittautuu, että relaatio R on ekvivalenssirelaatio.

Propositio 3.5. *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 3.4.

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

- (1) Koska $A = \bigcup_{i \in I} A_i$, niin jokaiselle $a \in A$ pätee $a \in A_i$ jollakin $i \in I$. Siis $a R a$, joten R on refleksiivinen.
- (2) Symmetrisyys on selvä, koska relaatio R määritellään ehdolla $a, b \in A_i$.
- (3) 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 3.6. 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*.

Propositio 3.7. *Olkoon $\sim$ ekvivalenssirelaatio laskutoimituksella varustetussa joukossa $(E, *)$. Jos ekvivalenssirelaatio $\sim$ ja laskutoimitus $*$ ovat yhteensopivat, niin luonnollinen kuvaus on surjektiivinen homomorfismi. Jos $e \in E$ on laskutoimituksen $*$ neutraalialkio, niin $[e] \in E/\sim$ on tekijälaskutoimituksen neutraalialkio.*

Todistus. Tämä seuraa määritelmästä: 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 Propositionista 1.14. □

Propositio 3.8. *Jos laskutoimitus $*$ on assosiatiivinen, sen tekijälaskutoimitus on assosiatiivinen. Jos $*$ on kommutatiivinen, sen tekijälaskutoimitus on kommutatiivinen.*

Todistus. Koska luonnollinen kuvaus on Proposition 3.7 mukaan surjektiivinen homomorfismi, väite seuraa Propositionista 1.14. □

Esimerkki 3.9. 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) $a = a + 0q$ kaikilla $a \in \mathbb{Z}$,
- (2) jos $b = a + kq$ jollain $k \in \mathbb{Z}$, niin $a = b + (-kq)$,
- (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

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

Kongruenssia vastaavia ekvivalenssiluokkia sanotaan *kongruenssiluokiksi (modulo q)* ja vastaavalle tekijäjoukolle käytetään merkintää

$$\mathbb{Z}/q\mathbb{Z} = \{[0], [1], [2], \dots, [q-1]\}.$$

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

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

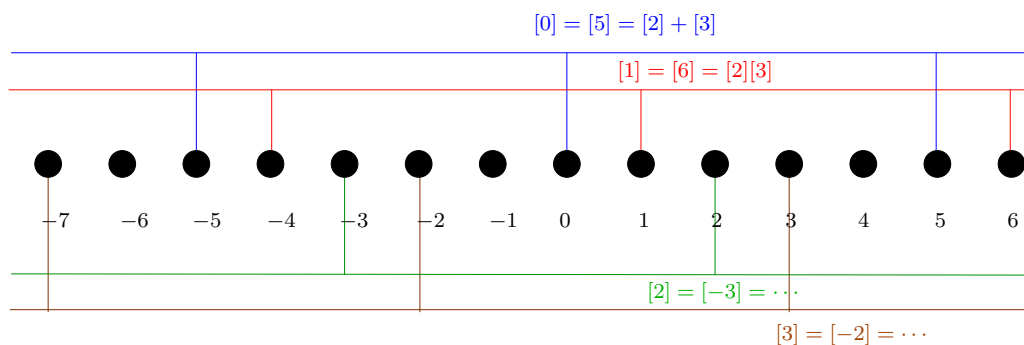
joten

$$a' + b' \equiv a + b \pmod{q}.$$

Kertolaskulle väite osoitetaan samaan tapaan harjoituksissa (Harjoitustehtävä 22). Kokonaislukujen yhteenlasku ja kertolasku määräävät siis laskutoimitukset q alkion joukolla $\mathbb{Z}/q\mathbb{Z}$. Lemman 3.8 nojalla molemmat laskutoimitukset ovat assosiatiivisia ja kommutatiivisia. Käytämme molemmille kongruenssiluokkien laskutoimituksille samaa merkintää kuin indusoiville laskutoimituksille:

$$[a] + [b] = [a + b] \quad \text{ja} \quad [a][b] = [ab]$$

kaikille $[a], [b] \in \mathbb{Z}/q\mathbb{Z}$. Proposition 3.7 mukaan $[0]$ on kongruenssiluokkien yhteenlaskun neutraalialkio ja $[1]$ on kongruenssiluokkien kertolaskun neutraalialkio.



KUVA 4. Kongruenssiluokat modulo 5.

Kurssilla Lukualueet tarkastellaan kokonaislukujen ja rationaalilukujen konstruktioita luonnollisista luvuista lähtien esimerkkinä tekijälaskutoimituksesta. Luonnollisten lukujen joukko ja sen laskutoimitukset yhteenlasku ja kertolasku oletetaan “intuitiivisesti tunnetuiksi”. Lukualueiden kurssin aikana konstruoidaan muut lukualueet

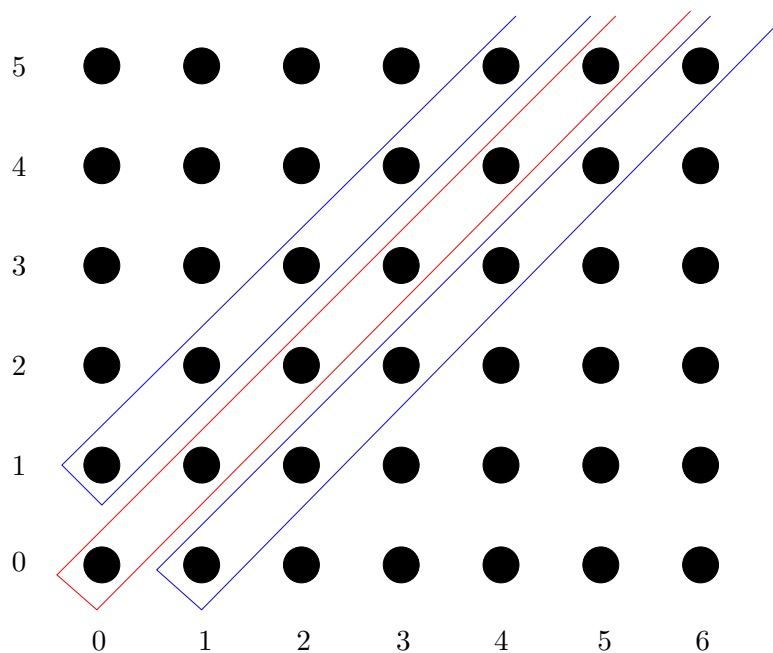
$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

laajentamalla asteittain luonnollisista luvuista lähtien. Samalla tarkastellaan, miten algebralliset ominaisuudet muuttuvat laajempaan lukualueeseen siirryttäessä. Tällä kurssilla tarkastelemme kokonaislukujen ja rationaalilukujen määrittelyä lyhyesti esimerkkinä tekijälaskutoimituksista.

Esimerkki 3.10. 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. Toisaalta sama luonnollinen luku voidaan esittää erotuksena äärettömän monella eri tavalla, sillä kaikilla $k \in \mathbb{N}$ pätee

$$(m + k) - (n + k) = m - n.$$

Näiden havaintojen opastamana määrittelemme joukkoon $\mathbb{N} \times \mathbb{N}$ relaation $\sim$ asettamalla $(m, n) \sim (p, q)$, jos ja vain jos $m + q = p + n$. Harjoitustehtävässä 23 osoitetaan, että relatio $\sim$ on ekvivalenssirelaatio.



KUVA 5. 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 tulon

$$(4) \quad (m, n) + (p, q) = (m + p, n + q),$$

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

$$(5) \quad (m, n) * (p, q) = (mp + nq, mq + np)$$

indusoima laskutoimitus.

Laskutoimitusten määritelmät ovat järkeviä: Paria (m, n) tulee ajatella erotuksena $m - n$, jolloin lausekkeet (4) ja (5) vastaavat lausekkeitä

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

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 24.

Esimerkki 3.11. Rationaaliluvut muodostetaan vastaavalla tavalla kuin kokonaisluvut edellä kokonaislukujen muodollisten osamäärien avulla: Määrittelemme ekvivalenssirelaation $\sim$ joukossa $\mathbb{Z} \times \mathbb{Z}^*$ (missä $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$) 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 tulon

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

indusoima laskutoimitus. Harjoitustehtävässä 25 osoitetaan, että laskutoimitukset $\oplus$ ja $\otimes$ ovat ekvivalenssirelaation $\sim$ kanssa yhteensopivia.

Harjoitustehtäviä.

Tehtävä 19. Olkoon R relaatio joukossa $\mathbb{R}^2$ siten, että $(x, y) R (z, w)$, jos ja vain jos $x^2 + y^2 = z^2 + w^2$. Osoita, että R on ekvivalenssirelaatio. Millaisia joukkoja relaation R ekvivalenssiluokat ovat?

Tehtävä 20. Mitkä seuraavista ovat joukon $\mathbb{C}$ ekvivalenssirelaatioita?

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

Tehtävä 21. 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 $[x] = [y]$.

Tehtävä 22. Osoita, että kokonaislukujen kertolasku on yhteensopiva kongruenssin kanssa.

Tehtävä 23. 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.

Tehtävä 24. Määritellään laskutoimitus $*$ joukossa $\mathbb{N} \times \mathbb{N}$ asettamalla

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

Osoita, että $*$ on yhteensopiva tehtävän 23 ekvivalenssirelaation kanssa.

Tehtävä 25. Osoita, että joukon $\mathbb{Z} \times \mathbb{Z}^*$ ekvivalenssirelaatio, joka määritellään asettamalla $(a, b) \sim (c, d)$, jos ja vain jos $ad = bc$, on yhteensopiva laskutoimitusten

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

ja

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

kanssa.

Tehtävä 26. 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.

²⁴Vihje: Todistuksessa voi käyttää vain luonnollisia lukuja!

²⁶Vihje: Euklidiset avaruudet.

4. RYHMÄT

Tässä luvussa tarkastelemme laskutoimituksella varustettuja joukkoja, joiden laskutoimitukselta oletamme muutamia yksinkertaisia ominaisuuksia:

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

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

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.

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 $\mathbb{C}^\times$,
- positiivisten reaalilukujen *multiplikatiivinen* ryhmä $(\mathbb{R}_+, \cdot)$ ja
- äärellinen syklinen ryhmä $(\mathbb{Z}/q\mathbb{Z}, +)$

Se, että yllä olevan luettelon kokonais-, rationaali- ja reaaliluvuista koostuvat laskutoimituksella varustetut joukot ovat ryhmiä, seuraa näiden lukualueiden tunnetuista ominaisuuksista. Kompleksiluvuille tämä seuraa Propositionista 2.2.

Osoitamme, että $(\mathbb{Z}/q\mathbb{Z}, +)$ on ryhmä: Kokonaislukujen yhteenlaskun indusoima laskutoimitus on assosiatiivinen Lemman 3.8 mukaan. Alkio $[0]$ on neutraalialkio Proposition 3.7 mukaan, koska luonnollinen kuvaus on surjektiivinen homomorfismi. Alkion $[k] \in \mathbb{Z}/q\mathbb{Z}$ käänteisalkio on $[-k]$:

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

(b) Olkoon $n \in \mathbb{N}$, $n \geq 2$ ja olkoot $M_n(\mathbb{R})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{C})$ ja $M_n(\mathbb{Z})$ sellaisten $n \times n$ -matriisien joukot joiden kertoimet ovat reaalilukuja, rationaalilukuja, kompleksilukuja ja kokonaislukuja. Jos nämä joukot varustetaan matriisien kertolaskulla, ne eivät muodosta ryhmiä: Jokainen näistä matriisien joukoista sisältää muunmuassa nollamatriisin, jolla ei ole käänteismatriisia.

Kurssin lineaarialgebra 1 nojalla tiedämme, että matriisien kertolaskulla varustettujen joukkojen $M_n(\mathbb{R})$, $M_n(\mathbb{Q})$ ja $M_n(\mathbb{C})$ osajoukot, jotka koostuvat matriiseista, joiden determinantti on nollasta poikkeava, muodostavat ryhmiä: Olkoon seuraavassa $\mathbb{K}$ jokin lukualueista $\mathbb{Q}$, $\mathbb{R}$ tai $\mathbb{C}$. Jos $A, B \in M_n(\mathbb{K})$ ja $\det A \neq 0 \neq \det B$, niin determinantin laskusäännöistä seuraa, että $\det AB \neq 0$. Siispä joukko $\{A \in M_n(\mathbb{K}) : \det A \neq 0\}$ on vakaa, ja matriisien kertolasku indusoi laskutoimituksen tähän joukkoon. Matriisien kertolasku on assosiatiivinen, identtisen matriisin $I_n = \text{diag}(1, \dots, 1)$ determinantti on 1 ja jokaisella matriisilla A , jolle pätee $\det A \neq 0$ on käänteismatriisi. Tarkastelemamme matriisit muodostavat *K-kertoimisen yleisen lineaarisen ryhmän*

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

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

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

jonka laskutoimitus on matriisien kertolasku.

On helppo nähdä, että matriisien kertolaskulla varustettu joukko $\{A \in M_n(\mathbb{Z}) : \det A \neq 0\}$ ei ole ryhmä: $\det \text{diag}(2, 2) = 4 \neq 0$, joten sillä on käänteismatriisi $\text{diag}(1/2, 1/2) \in GL_2(\mathbb{Q})$. Käänteismatriisi on yksikäsitteinen, joten matriisilla $\text{diag}(2, 2)$ ei ole käänteismatriisia. Cramerin säännön (Kofaktorimatriisin) avulla voidaan sen sijaan osoittaa (Harjoitustehtävä 28), että

$$SL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : \det A = 1\}$$

on ryhmä.

Jatkossa ryhmän laskutoimitus jätetään usein mainitsematta ja puhutaan vain "ryhmästä G ". Tällöin laskutoimitus on kuitenkin kiinnitetty ja usein konkreettisesti tilanteessa se on ennalta tiedossa. Esimerkiksi merkinnät $\mathbb{C}^\times$ ja $GL_n(\mathbb{R})$ 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. *Olkoon G ryhmä. Tällöin*

- (1) *Neutraalialkio e on yksikäsitteinen.*
- (2) *Jokaisen alkion käänteisalkio on yksikäsitteinen.*
- (3) *Jos $\bar{a}a = e$, niin $\bar{a}$ on alkion a käänteisalkio.*
- (4) *$(a^{-1})^{-1} = a$ kaikilla $a \in G$.*
- (5) *$(ab)^{-1} = b^{-1}a^{-1}$.*

Todistus. (1), (2), (3): Lause 1.10.

(4): Koska $aa^{-1} = e$, niin kohdan (3) nojalla $a = (a^{-1})^{-1}$.

(5): Koska pätee

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

niin väite seuraa kohdasta (3). □

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

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

Supistussäännöt ovat voimassa monissa laskutoimituksella varustetuissa joukoissa kuten esimerkiksi luonnollisissa luvuissa ja kaikissa ryhmissä.

Propositio 4.4. *Supistussäännöt pätevät ryhmässä.*

Todistus. Harjoitustehtävä 30. □

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 31. □

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

Propositio 4.6. *Olko G_1 ja G_2 ryhmiä. Niiden tulo $G_1 \times G_2$ on ryhmä (varustettuna laskutoimitusten tulolla).*

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

Esimerkki 4.7. Joukot $\mathbb{R}^n$ ja $\mathbb{Z}^n$ varustettuna vektorien komponenteittaisella yhteenlaskulla, eli yhteenlaskun n -kertaisella tulolla, ovat ryhmiä.

Olkoon X epätyhjä joukko ja olkoon

$$S(X) = \{f: X \rightarrow X : f \text{ on bijektio}\}.$$

Laskutoimituksella $\circ$ varustettu joukko $S(X)$ on joukon X *permutaatioryhmä*. Permutaatioryhmä on todellakin ryhmä Esimerkkien 1.6(c) ja 1.9(a) nojalla. Ryhmän $S(X)$ 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. Olkoon $X = \mathbb{R}^n$. Kuvaus $L: \mathbb{R}^n \rightarrow \mathbb{R}^n$ on *lineaarikuvaus*, jos kaikilla $x, y \in \mathbb{R}^n$ ja $a \in \mathbb{R}$ pätee

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

ja

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

Vektoriavaruuden $\mathbb{R}^n$ lineaariset bijektioiden joukko on permutaatioryhmän vakaa osajoukko, sillä lineaarialgebrassa osoitetaan, että kahden lineaarikuvauksen yhdistetty kuvaus on lineaarikuvaus. Nämä lineaariset bijektiot muodostavat ryhmän $GL(\mathbb{R}^n)$, jossa kuvausten yhdistäminen on laskutoimituksena: Laskutoimituksen assosiatiivisuutta ei tarvitse tarkastaa, koska se on ryhmän $S(\mathbb{R}^n)$ 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 $SL_n(\mathbb{R})$ ei ole kommutatiivinen, tämä osoitettiin harjoitustehtävässä 4 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 $q, r \in \mathbb{N}$.

(c) Kuvaukset $\text{id}, f, g, h: \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{0\}$, $f(x) = -x$, $g(x) = 1/x$, $h(x) = -1/x$, muodostavat äärellisen ryhmän $K \subset S(\mathbb{R} \setminus \{0\})$ laskutoimituksena kuvausten yhdistäminen. On helppo nähdä, että K on vakaa, joten laskutoimitus on hyvin määriteltä. Joukon K alkioille f, g, h pätee

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

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

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

joten K on kommutatiivinen.

Äärellisiä (pieniä) ryhmiä voi myös tarkastella *laskutaulujen* avulla: Muodostetaan ryhmän alkioilla indeksoitu taulukko, jossa paikalla (g, h) on alkio gh . Ryhmän laskutaulussa (tai kertotaulussa, kuten sitä usein kutsutaan) jokaisella rivillä ja jokaisessa sarakkeessa esiintyvät kaikki ryhmän alkio (Harjoitustehtävä 35).

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)	(0,1)	(1,0)	(1,1)		o	id	f	g	h
0	0	1	2	3		(0,0)	(0,0)	(0,1)	(1,0)	(1,1)		id	id	f	g	h
1	1	2	3	0	,	(0,1)	(0,1)	(0,0)	(1,1)	(1,0)	ja	f	f	id	h	g
2	2	3	0	1		(1,0)	(1,0)	(1,1)	(0,0)	(0,1)		g	g	h	id	f
3	3	0	1	2		(1,1)	(1,1)	(1,0)	(0,1)	(0,0)		h	h	g	f	id

Näissä laskutauluissa käytetään kongruenssiluokan $[k]$ 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 $\phi: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow K$,

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

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

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

Muille tapauksille pätee vastaavasti. Ryhmä K on siis "ryhmäteorian kannalta sama ryhmä kuin $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ ".

Jos G ja G' ovat ryhmiä, niin homomorfismia $\phi: G \rightarrow G'$ 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 $\phi: G \rightarrow G'$ kuvaa ryhmän G neutraali-alkion ryhmän G' neutraali-alkioksi, ja jokaiselle $g \in G$ pätee $\phi(g^{-1}) = \phi(g)^{-1}$.

Todistus. Neutraali-alkiota koskeva väite todistetaan harjoitustehtävässä 29.

Todistetaan käänteisalkiota koskeva väite: Olkoon e ryhmän G neutraali-alkio. Olkoon $g \in G$. Tällöin

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

Ensimmäisen väitteen mukaan tämä on ryhmän G neutraali-alkio. Väite seuraa Proposition 4.3 kohdasta (3). $\square$

Esimerkki 4.13. (a) Esimerkissä 1.13(a) osoitettiin, että $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_+, \cdot)$ on ryhmäisomorfismi.

(b) Vektoriavaruuden $\mathbb{R}^n$ lineaaristen bijektioiden ryhmä $\text{GL}(\mathbb{R}^n)$ (katso Esimerkki 4.8) on isomorfinen yleisen lineaarisen ryhmän $\text{GL}_n(\mathbb{R})$ kanssa: Olkoon $K = \{v_1, v_2, \dots, v_n\}$ 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 $\text{Mat}: \text{GL}(\mathbb{R}^n) \rightarrow \text{GL}_n(\mathbb{R})$,

$$\text{Mat}(L) = ((Lv_1)_K, (Lv_2)_K, \dots, (Lv_n)_K),$$

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

$$\text{Mat}(L_2 L_1) = \text{Mat}(L_2) \text{Mat}(L_1).$$

Harjoitustehtäviä.

Tehtävä 27. Osoita, että joukon X potenssijoukko $\mathcal{P}(X)$ varustettuna laskutoimituksella $\triangle$ (symmetrinen erotus), joka määritellään asettamalla kaikille $A, B \in \mathcal{P}(X)$

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

on ryhmä.

Tehtävä 28. Osoita, että $\mathrm{SL}_n(\mathbb{Z})$ varustettuina matriisien kertolaskulla on ryhmä.

Tehtävä 29. Olkoot G ja G' ryhmiä. Olkoon $h : G \rightarrow G'$ homomorfismi. Osoita, että h kuvaa ryhmän G neutraalialkion ryhmän G' neutraalialkioksi.

Tehtävä 30. 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 $a = c$.

Tehtävä 31. 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 $a, b \in A$.

Tehtävä 32. Olkoon $T : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z})$, $T(B) = {}^tB$, kuvaus, joka liittää matriisiin B sen transpoosin. Olkoon $\mathrm{inv} : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z})$ 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?

Tehtävä 33. Olkoon G ryhmä, ja olkoon $\mathrm{Aut} G$ sen automorfismien joukko. Osoita, että $\mathrm{Aut} G$ on ryhmä, kun laskutoimituksena on kuvausten yhdistäminen.

Tehtävä 34. Kuvaus $f : \mathbb{R} \rightarrow \mathbb{R}$ on *kasvava*, jos kaikille $x, y \in \mathbb{R}$ pätee $f(x) \geq f(y)$, kun $x \geq y$. Kuvaus $f : \mathbb{R} \rightarrow \mathbb{R}$ on *vähenevä*, jos kaikille $x, y \in \mathbb{R}$ pätee $f(x) \leq f(y)$, kun $x \geq y$. Kuvaus on *monotoninen*, jos se on kasvava tai vähenevä. Kasvavien, vähenevien ja monotonisten bijektioiden joukot ovat permutaatioryhmän $S(\mathbb{R})$ osajoukkoja. Indusoiko kuvausten yhdistäminen laskutoimituksen näihin joukkoihin? Muodostavatko kasvavat bijektiot ryhmän? Entä vähenevät bijektiot? Entä monotoniset bijektiot?

Tehtävä 35. Osoita, että kaikki ryhmän alkioit esiintyvät sen laskutaulun jokaisella rivillä ja sarakkeella.

Tehtävä 36. Olkoot X ja Y epätyhjiä joukkoja, ja olkoon $f : X \rightarrow Y$ bijektio. Osoita, että permutaatioryhmät $S(X)$ ja $S(Y)$ ovat isomorfisia.

Tehtävä 37. Olkoon

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

Osoita, että H_3 varustettuna matriisien kertolaskulla on ryhmä.

Tehtävä 38. Osoita, että tehtävässä 37 määritelty ryhmä H_3 ei ole isomorfinen ryhmän $(\mathbb{R}^3, +)$ kanssa.

²⁹Vihje: Supistussääntö.

³⁷Vihje: Propositio 1.14(1)

Tehtävä 39. Määritellään reaalilukujen joukossa $\mathbb{R}$ laskutoimitus $*$ asettamalla

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

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

Tehtävä 40. Olkoon G ryhmä. Olkoon R ryhmän G relaatio, joka määritellään säännöllä

$$aRb \iff a = gb g^{-1} \text{ jollakin } g \in G.$$

Onko R ekvivalenssirelaatio?

³⁹Vihje: Jos x on reaaliluku, sen kolmas juuri $\sqrt[3]{x}$ on reaaliluku, jolle pätee $(\sqrt[3]{x})^3 = x$. Jokaisella reaaliluvulla on yksikäsitteinen reaalinen kolmas juuri.

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. Seuraava tulos antaa keinon tarkastaa, onko jokin ryhmän osajoukko aliryhmä:

Propositio 5.2. Ryhmän G osajoukko $H \neq \emptyset$ on aliryhmä, jos

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

Todistus. Olkoon $e \in G$ neutraali alkio. 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 $xy = x(y^{-1})^{-1} \in H$.

Ehdosta (2) seuraa ehto (1), joten väite seuraa kohdasta (1). $\square$

Esimerkki 5.3. (a) Jokaisella ryhmällä on aliryhmiä: ryhmä itse, ja neutraali alkion 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 muunmuassa

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

kaikilla $n \geq 2$ ja

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

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 5.4. Reaalinen vektoriavaruus (eli $\mathbb{R}$ -vektoriavaruus) muodostuu laskutoimituksella varustetusta joukosta $(V, +)$, jossa on määritelty alkioiden kertominen reaaliluvulla. Reaaliluvulla kertominen tarkoittaa kuvausta $\mathbb{R} \times V \rightarrow V$, $(\lambda, v) \mapsto \lambda v$. Laskutoimitukselta ja reaaliluvulla kertomiselta oletetaan

- (1) $(V, +)$ on kommutatiivinen ryhmä,
- (2) $\lambda(v + w) = \lambda v + \lambda w$ kaikille $\lambda \in \mathbb{R}$ ja $v, w \in V$,
- (3) $(\lambda + \mu)v = \lambda v + \mu v$ kaikille $\lambda, \mu \in \mathbb{R}$ ja $v \in V$,
- (4) $\mu(\lambda v) = (\mu\lambda)v$ kaikille $\lambda, \mu \in \mathbb{R}$ ja $v \in V$ ja
- (5) $1 v = v$.

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 aliavaruuksia. Esimerkiksi $\mathbb{R}$ -vektoriavaruudella $\mathbb{R}$ on vain kaksi aliavaruutta $\{0\}$ ja $\mathbb{R}$ mutta reaalilukujen additiivisella ryhmällä on paljon enemmän aliryhmiä: Esimerkiksi joukot

$$\alpha\mathbb{Z} = \{\alpha k : k \in \mathbb{Z}\}$$

ja

$$\alpha\mathbb{Q} = \{\alpha q : q \in \mathbb{Q}\}$$

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 $\alpha \in \mathbb{R}$.

Jos W on toinen $\mathbb{R}$ -vektoriavaruus, niin kuvaus $L: V \rightarrow W$ 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.

Käyttämällä edellä olevassa määritelmässä reaalilukujen sijaan rationaalilukuja tai kompleksilukuja saadaan $\mathbb{Q}$ -vektoriavaruuden ja $\mathbb{C}$ -vektoriavaruuden ja vastavien $\mathbb{Q}$ - ja $\mathbb{R}$ -lineaarikuvausten käsitteet.

Propositio 5.5. *Aliryhmien leikkaus on aliryhmä.*

Todistus. Harjoitustehtävä 43. □

Propositio 5.6. *Olkoon $\phi: G \rightarrow G'$ ryhmähomomorfismi. Olkoot $H \leq G$, $H' \leq G'$ aliryhmiä. Tällöin $\phi(H) \leq G'$ ja $\phi^{-1}(H') \leq G$ ovat aliryhmiä.*

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

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

koska $gh^{-1} \in H$. Siis $\phi(H)$ on aliryhmä Proposition 5.2(1) nojalla.

Toinen väite todistetaan harjoitustehtävässä 44. □

Jokaiseen ryhmähomomorfismiin liittyy kaksi tärkeää aliavaruutta, yksi määrittelyjoukossa ja yksi maalijoukossa:

Määritelmä 5.7. Ryhmähomomorfismin $\phi: G \rightarrow G'$ ydin on $\ker \phi = \phi^{-1}(e')$ ja sen kuva on $\text{Im } \phi = \phi(G)$.

Propositio 5.6 mukaan ryhmähomomorfismin ydin ja kuva ovat aliryhmiä.

Esimerkki 5.8. (a) Olkoon $\phi_q: \mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ 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 $A, B \in M_n(\mathbb{R})$ pätee

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

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

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

Propositio 5.9. *Ryhmähomomorfismi on injektio, jos ja vain jos sen ydin on neutraalialkion muodostama ryhmä.*

Todistus. Olkoon $\phi: G \rightarrow G'$ ryhmähomomorfismi. Aiemmin osoitettiin (harjoitustehtävä 29), 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 $x = y$. □

Propositio 5.9 mukaan ryhmähomomorfismin injekttiivisyyden toteamiseksi riittää tarkastella neutraalialkion alkukuvaa.

Määritelmä 5.10. 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 alkioit ovat ryhmän $\langle B \rangle$ *virittäjiä*.

Joukon B virittämä aliryhmän aliryhmän määritelmässä voi todellakin puhua pienimmästä joukon B sisältävästä aliryhmästä sillä Proposition 5.5 nojalla

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

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

Propositio 5.11. *Olkoon G ryhmä, ja olkoon $B \subset G$, $B \neq \emptyset$. Joukon B virittämä aliryhmä on*

$$(6) \quad \{b_1^{\pm 1} b_2^{\pm 1} \cdots b_k^{\pm 1} : b_1, b_2, \dots, b_k \in B, k \in \mathbb{N} \setminus \{0\}\}.$$

Todistus. Lausekkeen (6) antama osajoukko $\tilde{B}$ on ryhmän G aliryhmä Propositionien 4.3(5) ja 5.2 nojalla. Erityisesti se on ryhmä, joka sisältää joukon B , joten $\langle B \rangle \leq \tilde{B}$.

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 $b_1^{\pm 1} b_2^{\pm 1} \cdots b_k^{\pm 1}$ olevat alkioit. Siis $\tilde{B} \leq \langle B \rangle$. □

Esimerkki 5.12. (a) $\langle \mathbb{Z}, + \rangle = \langle 1 \rangle = \langle -1 \rangle$ ja kaikilla $q \in \mathbb{Z} \setminus \{-1, 1\}$ 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 $\mathbb{Z}/5\mathbb{Z}$:

$$\mathbb{Z}/5\mathbb{Z} = \langle [1] \rangle = \langle [2] \rangle = \langle [3] \rangle = \langle [4] \rangle.$$

Toisaalta $\mathbb{Z}/4\mathbb{Z} = \langle [1] \rangle = \langle [3] \rangle$ mutta $\langle [2] \rangle < \mathbb{Z}/4\mathbb{Z}$.

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

Propositio 5.13. *Olkoon $G = \langle S \rangle$ ryhmä. Olkoot $\phi, \psi: G \rightarrow H$ ryhmähomomorfismeja, joille pätee $\phi|_S = \psi|_S$. Tällöin $\phi = \psi$.*

Todistus. Harjoitustehtävä 51. □

Kun ryhmän alkiot kirjoitetaan virittäjien avulla on kätevää käyttää monikertojen ja potenssien yleistyksiä ryhmille. Itse asiassa nämä käsitteet voidaan määritellä hieman yleisemmässä tapauksessa: 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 $a^{n+1} = aa^n$. 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 $1a = a$, ja $(n+1)a = na + a$ kaikille $n \in \mathbb{Z}$, $n \geq 1$. Jos laskutoimituksella varustetussa joukossa $(A, +)$ on neutraalialkio, niin asetetaan $0a = 0 \in A$, ja jos alkiolla $a \in A$ on käänteisalkio laskutoimituksen $+$ suhteen, asetetaan $(-1)a = -a$, ja negatiivisille $n \in \mathbb{Z}$ asetamme $na = (-n)(-a)$.

Tavanomaiset laskulait pätevät potensseille ja monikerroille:

Lemma 5.14. *Olkoon $(G, \cdot)$ ryhmä. Tällöin*

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

Olkoon $(H, +)$ ryhmä. Tällöin

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

Todistus. Harjoitustehtävä 45. □

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

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

ovat alkoiden $a \in G$ ja $b \in H$ virittämät sykliset aliryhmät.

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.*

Todistus. Huomataan ensin, että $\{0\} = 0\mathbb{Z}$ ja $\mathbb{Z} = 1\mathbb{Z}$. Olkoon $H < \mathbb{Z}$, $H \neq \{0\}$ jokin aliryhmä. Olkoon q pienin positiivinen kokonaisluku aliryhmässä H . Tällöin siis $q\mathbb{Z} < H$.

Osoitamme, että $H = q\mathbb{Z}$. Jos on $m \in H \setminus q\mathbb{Z}$, niin $m = aq + b$ 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 $H = q\mathbb{Z}$. □

Määritelmä 5.17. Ryhmä G on *syklinen ryhmä*, jos on $a \in G$ siten, että $G = \langle a \rangle$.

Edellä käsitellyistä esimerkeistä muunmuassa 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 aina numeroituva, rationaalilukujen tapaus käsitellään harjoitustehtävässä 49.

Lause 5.18. (1) *Syklinen ryhmä, jossa on vähintään kaksi alkioa, 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 $\phi: \mathbb{Z} \rightarrow C$, $\phi(n) = g^n$. Lemman 5.14 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 $\ker \phi = q\mathbb{Z}$ jollain $q \geq 2$. Olkoon $\psi: \mathbb{Z}/q\mathbb{Z} \rightarrow C$, $\psi([k]) = \phi(k) = g^k$. Kuvaus ψ on hyvin määritelty: jos $k \equiv k' \pmod{q}$, niin $k - k' \in q\mathbb{Z} = \ker \phi$, joten $g^k = g^{k'}$. Kuvaus ψ on homomorfismi:

$$\psi([n])\psi([m]) = g^n g^m = g^{n+m} = \psi([n+m]) = \psi([n] + [m]).$$

Homomorfismi ψ on surjektio koska ϕ on surjektio. Huomataan vielä, että $\ker \psi = [0]$: Jos $\psi([k]) = e \in G$, niin $\phi(k) = e$, joten $k \in q\mathbb{Z}$ ja $[k] = [0]$.

(2) Harjoitustehtävä 50.

(3) Väite todistettiin sykliselle ryhmälle $(\mathbb{Z}, +)$ Propositionissa 5.16. Olkoon $C = \langle g \rangle$ syklinen ryhmä, ja olkoon $H < C$. Olkoon $\phi: \mathbb{Z} \rightarrow C$ homomorfismi $\phi(n) = g^n$. Tällöin $\phi^{-1}(H) \leq \mathbb{Z}$, joten $\phi^{-1}(H) = N\mathbb{Z}$ jollain $N \in \mathbb{Z}$, erityisesti $\phi^{-1}(H)$ on syklinen ryhmä. Koska $H = \phi(\phi^{-1}(H))$, väite seuraa kohdasta (2). $\square$

Koska Lauseen 5.18 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_∞ .

Esimerkki 5.19. (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 kommutativiset ryhmät $\mathbb{Z}/4\mathbb{Z}$ ja $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ eivät ole isomorfisia. Edellä käyttöönotetun syklisen ryhmien merkinnän avulla edellinen on hieman lyhyempi ilmaista: ryhmät C_4 ja $C_2 \times C_2$ eivät ole isomorfisia.

Harjoitustehtäviä.

Tehtävä 41. Osoita, että

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

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

Tehtävä 42. Anna esimerkki surjektiivisesta homomorfismista $f: (\mathbb{R}, +) \rightarrow (\mathbb{S}^1, \cdot)$.

Tehtävä 43. Olkoon G ryhmä, olkoon $I \neq \emptyset$ jokin indeksijoukko ja olkoot $H_i \leq G$, $i \in I$. Osoita, että

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

Tehtävä 44. Olkoon $\phi: G \rightarrow G'$ ryhmähomomorfismi. Olkoon $H' \leq G'$. Osoita: $\phi^{-1}(H') \leq G$.

Tehtävä 45. Todista Lemman 5.14 kohtien (1) ja (2) potenssien laskusäännöt.

Tehtävä 46. Määritä kaikki ryhmien $\mathbb{Z}/6\mathbb{Z}$ ja $\mathbb{Z}/7\mathbb{Z}$ aliryhmät.

Tehtävä 47. Osoita, että ryhmät $\mathbb{Z}/6\mathbb{Z}$ ja $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ovat isomorfisia.

Tehtävä 48. Olkoon $q \in \mathbb{N} \setminus \{0\}$. Osoita, että joukko

$$G_q = \{w \in \mathbb{C} : w^q = 1\}$$

varustettuna kompleksilukujen kertolaskulla on ryhmän $\mathbb{C}^\times$ aliryhmä. Osoita, että ryhmä G_q on isomorfinen ryhmän $\mathbb{Z}/q\mathbb{Z}$ kanssa.

Tehtävä 49. Osoita, että rationaalilukujen additiivinen ryhmä ei ole syklinen.

Tehtävä 50. Olkoon C syklinen ryhmä ja olkoon $\phi: C \rightarrow G$ ryhmähomomorfismi. Osoita, että $\phi(C) \leq G$ on syklinen aliryhmä.

Tehtävä 51. Olkoon $G = \langle S \rangle$ ryhmä. Olkoot $\phi, \psi: G \rightarrow H$ ryhmähomomorfismeja, joille pätee $\phi|_S = \psi|_S$. Osoita, että $\phi = \psi$.

⁴⁷Vihje: Osoita, että $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ on syklinen ryhmä.

6. ÄÄRELLISET PERMUTAATIORYHMÄT

Luvussa 4 tutustuimme alustavasti permutaatioryhmiin. Äärellisen n alkiosta koostuvan joukon $\{1, 2, \dots, n\}$ symmetriaryhmälle käytetään yleisesti merkintää

$$S_n = S(\{1, 2, \dots, n\}).$$

Harjoitustehtävän 36 nojalla minkä tahansa n alkion joukon permutaatioryhmä on isomorfinen ryhmän S_n kanssa. Kaikkia näitä permutaatioryhmiä voidaan siksikin kutsua ryhmäksi S_n vastaavalla tavalla kuin voidaan puhua abstrakteista syklisistä ryhmistä C_n ja C_∞ . Äärelliset permutaatioryhmät, joita kutsutaan joskus myös symmetrisiksi ryhmiksi, ovat yllättävän tärkeitä ryhmiä matematiikan eri aloilla, esimerkiksi Galois'n teoriassa, joka käsittelee muunmuassa polynomien algebrallista ratkeavuutta, samoin ne tulevat vastaan geometriassa tarkasteltaessa esimerkiksi säännöllisten monitahokkaiden symmetriaryhmiä.

Luvun aluksi määrittelemme yleisiä käsitteitä, joita havainnollistamme ensin tuilla ryhmillä:

Määritelmä 6.1. Ryhmän G alkioden lukumäärä $\#G$ on ryhmän G *kertaluku*. Ryhmän G alkion g *kertaluku* $\text{ord } g$ on sen virittämän syklisen aliryhmän kertaluku, $\text{ord } g = \# \langle g \rangle$.

Lemma 6.2. Olkoon G ryhmä ja olkoon e ryhmän G neutraalialkio. Tällöin

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

Todistus. Harjoitustehtävä 53. □

Esimerkki 6.3. (a) Ryhmien K ja $C_2 \times C_2$ kertaluku on 4 ja niiden jokaisen neutraalialkiosta poikkeavan alkion kertaluku on 2.

(b) Ryhmän $C_4 \cong \mathbb{Z}/4\mathbb{Z}$ kertaluku on 4 ja sen alkioden $[1]$ ja $[3]$ kertaluku on 4.

Seuraavat perusominaisuudet on helppo tarkastaa.

Propositio 6.4. (1) Permutaatioryhmän S_n kertaluku on $n!$.

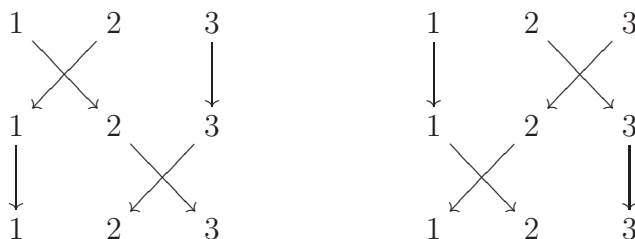
(2) Jos $n \geq 3$, niin S_n ei ole kommutatiivinen.

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 $\bar{\sigma}|_{\{1,2,3\}} = \sigma$, $\bar{\tau}|_{\{1,2,3\}} = \tau$, ja $\bar{\sigma}(k) = k = \bar{\tau}(k)$. Näille pätee $\bar{\sigma} \circ \bar{\tau} \neq \bar{\tau} \circ \bar{\sigma}$ kuten tapauksessa $n = 3$. □

Permutaatioilla operointia voi havainnollistaa monilla eri tavoilla. Proposition 6.4 todistuksessa käyttämämme tapa antaa permutaatio luettelemalla kaikkien alkioden kuvautuminen ei ole kovin kätevää. Esimerkiksi seuraavat kaaviot havainnollistavat Proposition 6.4 todistuksessa esiintyvien permutaatioiden σ ja τ yhdistettyjä kuvauksia $\tau \circ \sigma$ ja $\sigma \circ \tau$:



Yksinkertaistamista varten otamme joillekin permutaatioille käyttöön tiiviimmän merkinnän:

Määritelmä 6.5. Olkoon $\{a_1, a_2, \dots, a_m\} \subset \{1, 2, \dots, n\}$ m alkion osajoukko, $m \geq 2$. *Sykli* $(a_1 a_2 \dots a_m)$ on permutaatio, joka kuvaa alkion a_i alkioiksi a_{i+1} kaikilla $i \in \{1, 2, \dots, m-1\}$, alkion a_m alkioiksi a_1 ja on identtinen kuvaus osajoukon $\{a_1, a_2, \dots, a_m\}$ komplementissa. Syklin $(a_1 a_2 \dots a_m)$ *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*.

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

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

Sykliden yhdistettyä kuvausta sanotaan niiden *tuloksi*.

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

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

Propositiossa 6.4 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 6.6. *Erilliset syklit kommutoivat.*

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

Jos $f: X \rightarrow X$ on kuvaus ja $x \in X$, niin pisteen x rata (kuvauksella f) on

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

Lemma 6.7. *Jokaisen m -syklin kertaluku on m .*

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

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

koostuu m pisteestä ja sama pätee kaikille muillekin pisteille $a_2, \dots, a_m$. Väite seuraa tästä. $\square$

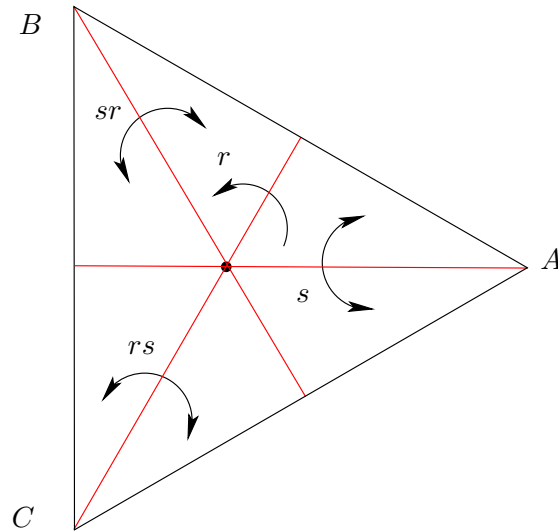
Esimerkki 6.8. (1) Kaikki Proposition 6.4 todistuksessa esiintyvät kuvaukset ovat syklejä: $\sigma = (12)$, $\tau = (23)$, $\sigma \circ \tau = (23)(12) = (132)$ ja $\tau \circ \sigma = (23)(12) = (123)$. Loput permutaatioryhmän S_3 alkiot ovat vaihto (13) ja identtinen kuvaus.

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

Esimerkki 6.9. Jos P_n on säännöllinen n -kulmio tasossa, sen symmetriaryhmä on *diedriryhmä* D_n , jonka virittävät kierto kulman $2\pi/n$ verran keskipisteen ympäri, ja heijastus valitun symmetria-akselin suhteen. Tarkastelemme kahta erikoistapausta, tasasivuista kolmiota ja neliötä.

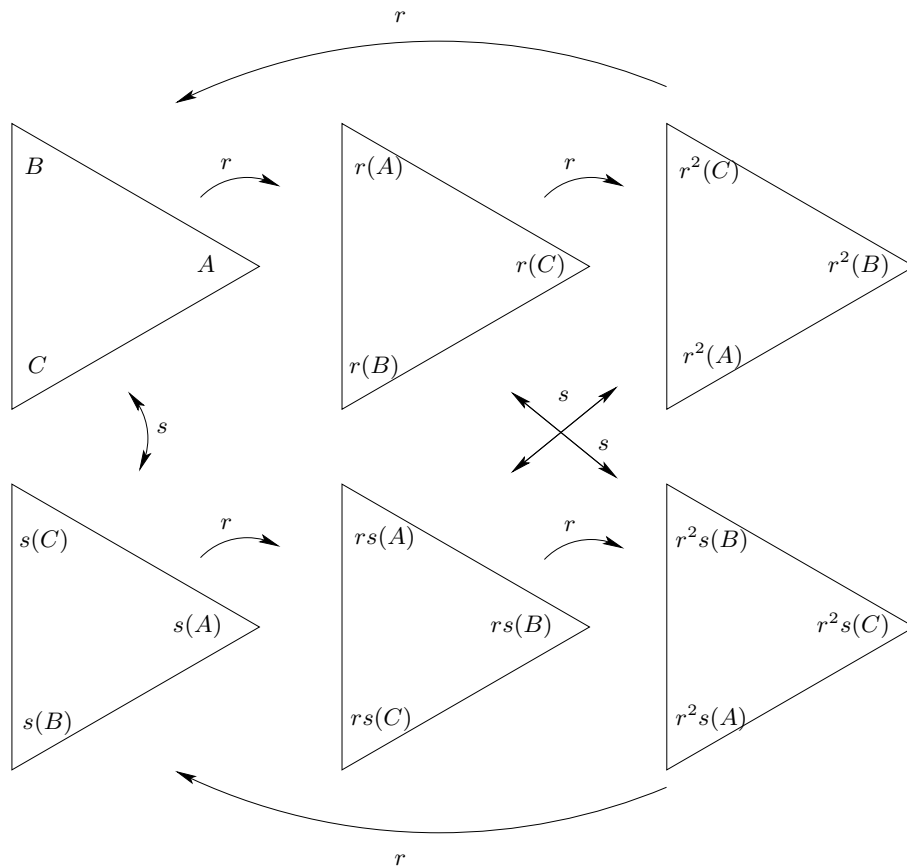
Olkoon P_3 tasasivuinen kolmio, jonka kärjet ovat A , B ja C . Kolmiolla P_3 on kuusi symmetriaa: identtinen kuvaus id , kierto r vastapäivään kulman $2\pi/3$ verran, r^2 , joka on kierto kulman $4\pi/3$ verran samaan suuntaan ja peilaukset kunkin kärjen kautta kulkevien kulmanpuolittajasuorien suhteen.

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

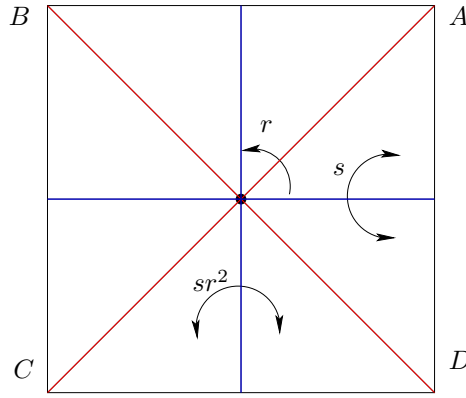


yläpuoleksi ja muut kuvaavat yläpuolen alapuoleksi. Jos s on peilaus kärjen A kautta kulkevan ja vastakkaista sivua vastaan kohtisuoran suoran suhteen, on melko helppo nähdä, että muut peilaukset ovat rs ja sr .

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) .



Säännöllisen n -kulmion symmetriaryhmä D_n on vastaavalla tavalla isomorfinen ryhmän S_n jonkin aliryhmän kanssa. Koska ryhmän D_n kertaluku on $2n$, tämä aliryhmä on permutaatioryhmän S_n aito aliryhmä. Esimerkiksi neliön symmetriaryhmä 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 -matriisien 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 $GL_2(\mathbb{R})$ aliryhmänä.

Yleistämme Esimerkissä 6.9 tehdyn havainnon ja osoitamme, että kaikki ryhmät voi halutessa ajatella permutaatioryhmien aliryhminä, äärettömät ryhmät tietenkin äärettömien joukkojen permutaatioryhmien.

Propositio 6.10. *Ryhmä G on isomorfinen ryhmän $S(G)$ jonkin aliryhmän kanssa.*

Todistus. Olkoon $g \in G$. Kuvaus $\ell_g: G \rightarrow G$ on surjektio koska $\ell_g(g^{-1}z) = z$ kaikilla $z \in G$ ja supistussäännön nojalla se on injektio. Siis voidaan määritellä kuvaus $\rho: G \rightarrow S(G)$, $\rho(g) = \ell_g$. 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 Φ on injektio, joten $\Phi: G \rightarrow \Phi(G) < S(G)$ on isomorfismi. $\square$

Propositio 6.11. *Olkoon G äärellinen ryhmä, jonka kertaluku on n . Permutaatioryhmällä S_n on aliryhmä, joka on isomorfinen ryhmän G kanssa.*

Todistus. Ryhmät S_n ja $S(G)$ ovat isomorfisia, joten voimme käsitellä ryhmää $S(G)$ ja väite seuraa Propositioista 6.10 $\square$

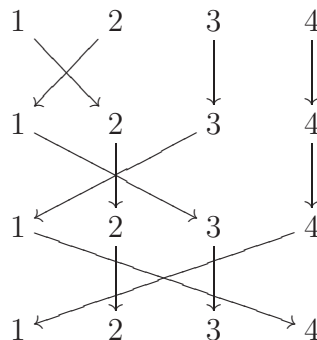
Tarkastelemme seuraavaksi äärellisten permutaatioryhmien rakennetta.

Propositio 6.12. *Jokainen sykli on vaihtojen tulo.*

Todistus. Induktiolla on helppo osoittaa, että

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

Todistuksen idea sisältyy seuraavaan kaavioon:



Yksityiskohdat harjoitustehtävässä 59. □

Propositio 6.13. *Jokainen vaihto on alkeisvaihtojen pariton tulo.*

Todistus. Koska harjoitustehtävässä 58 osoitetaan, että $(km) = (1k)(1m)(1k)$ kaikilla $k, m \in \{1, 2, \dots, n\}$, $k \neq m$, riittää osoittaa, että $(1k)$ on alkeisvaihtojen pariton tulo kaikilla $k \in \{2, 3, \dots, n\}$. Vaihto (12) on alkeellinen. Oletetaan, että $(1\ k-1)$ on alkeisvaihtojen tulo. Koska $(1k) = (1\ k-1)(k-1\ k)(1\ k-1)$, väite seuraa. □

Propositio 6.14. *Jokainen identtisestä kuvauksesta poikkeava permutaatio voidaan esittää erillisten syklien tulona.*

Todistus. Jos permutaatio τ kiinnittää pisteet $a_1, a_2, \dots, a_k \in \{1, 2, \dots, n\}$, riittää todistaa väite permutaation τ rajoittumalle joukkoon $\{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots, a_k\}$. 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

$$\mathcal{O}(1) = \{1, \tau(1), \tau^2(1), \dots, \tau^k(1), \dots\}.$$

Koska $\{1, \dots, n\}$ on äärellinen joukko täytyy olla $\tau^q(1) = \tau^r(1)$ joillain luonnollisilla luvuilla $q < r$. Valitaan luvut q ja r siten, että q on minimaalinen. Koska τ on bijektio, täytyy olla $q = 0$, $\tau^r(1) = 1$. Tästä nähdään, että

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

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

Propositioista 6.12, 6.13 ja 6.14 saadaan

Lause 6.15. *(Alkeis)vaihdot virittävät permutaatioryhmän.* □

Jokaiseen permutaatioon liittyvä tärkeä invariantti on permutaation merkki:

Määritelmä 6.16. 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

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

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

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

Propositio 6.17. *Olkoon $f: X^n \rightarrow V$ antisymmetrinen kuvaus. Tällöin*

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

jos σ on r alkeistransposition tulo.

Todistus. Väite pätee selvästi, kun $r = 1$. Oletetaan, että se pätee, kun σ on $r-1$ alkeispermutaation tulo. Olkoon $\sigma = \tau \circ \omega$ permutaatio, joka on r alkeistransposition tulo siten, että ω on $r-1$ alkeistransposition tulo ja τ on alkeistranspositio.

Nyt soveltamalla antisymmetrisyyden määritelmää alkeistranspositiolla τ ja pisteellä $(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$ saadaan

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

Proposition 6.13 avulla saadaan välittömästi

Seuraus 6.18. *Jos f on antisymmetrinen, niin kaikille transpositioille $\tau \in S_n$ pätee*

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

Propositio 6.19. *Permutaation merkki on hyvin määritelty.*

Todistus. Kuvaus $f: \mathbb{Z}^n \rightarrow \mathbb{Z}$,

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

on antisymmetrinen (Harjoitustehtävä 61). Lisäksi, kun muuttujan x komponentit ovat eri kokonaislukuja, $f(x) \neq 0$. Jos permutaatio σ voidaan esittää r ja s permutaation tulona, saadaan Proposition 6.17 nojalla $(-1)^r = (-1)^s$, joten $r \equiv s \pmod{2}$. $\square$

Lause 6.20. *Permutaation merkki $\epsilon: S_n \rightarrow \{-1, 1\}$ on ainoa homomorfismi permutaatioryhmästä S_n multiplikatiiviseen ryhmään $\{-1, 1\}$, joka saa transpositioilla arvon -1 .*

Todistus. Harjoitustehtävässä 62 osoitetaan, että ϵ on homomorfismi. Proposition 6.17 nojalla $\epsilon(\tau) = -1$ kaikille vaihdoille, joten merkki on halutunlainen homomorfismi. Toisaalta alkeisvaihdot virittävät koko permutaatioryhmän, joten, jos homomorfismin arvot tunnetaan kaikille alkeisvaihdoille, sen arvot kiinnittyvät kaikille permutaatioille. Siis ϵ on ainoa homomorfismi, jolla on haluttu ominaisuus. $\square$

Permutaatioiden merkkihomomorfismin $\epsilon: S_n \rightarrow \{-1, 1\}$ ydin on *alternoiava ryhmä* A_n , joka koostuu parillisista permutaatioista.

Esimerkki 6.21. (a) $A_3 = \langle (123) \rangle < S_3$, $A_3 \cong C_3$.

(b) $A_4 = \langle (123), (124), (134), (234), (12)(34), (13)(24), (14)(23) \rangle < S_4$.

(c) 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

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

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

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

Harjoitustehtäviä.

Tehtävä 52. Osoita, että permutaatioryhmän S_n kertaluku on $n!$.

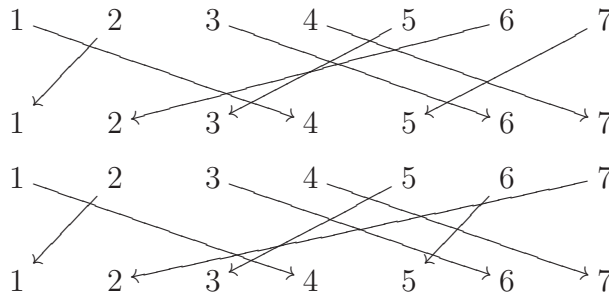
Tehtävä 53. Olkoon G ryhmä ja olkoon e ryhmän G neutraalialkio. Osoita, että
$$\text{ord } g = \min\{k \geq 1 : g^k = e\}.$$

Tehtävä 54. Määritä matriisien $A, B, C \in \text{SL}_2(\mathbb{Z})$ kertaluvut, kun

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

Tehtävä 55. Kirjoita permutaatio $(123)(24)$ syklinä.

Tehtävä 56. Kirjoita kaavioita



vastaavat permutaatiot erillisten syklien tuloina.

Tehtävä 57. Kirjoita permutaatio $(1234)(235)$ erillisten syklien tulona.

Tehtävä 58. Osoita, että $(km) = (1k)(1m)(1k)$.

Tehtävä 59. Täydennä Proposition 6.12 todistus induktiotodistukseksi.

Tehtävä 60. Osoita, että $S_3 = \langle (12), (23) \rangle$

Tehtävä 61. Osoita, että kuvaus $f: \mathbb{Z}^n \rightarrow \mathbb{Z}$,

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

on antisymmetrinen.

Tehtävä 62. Osoita, että permutaation merkki $\epsilon: S_n \rightarrow \{-1, 1\}$ on homomorfismi.

Olkoon seuraavissa tehtävissä

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

Tehtävä 63. Osoita, että joukko B varustettuna matriisien kertolaskulla on ryhmän $\text{GL}_2(\mathbb{Q})$ aliryhmä. Onko B ryhmän $\text{SL}_2(\mathbb{Z})$ aliryhmä?

Tehtävä 64. Onko ryhmä B kommutatiivinen? Onko se syklinen? Luettele kaikki ryhmän B aliryhmät.

Tehtävä 65. Osoita, että ryhmä B on isomorfinen permutaatioryhmän S_3 kanssa.

⁶⁵Vihje: Homomorfismi $\phi: S_3 \rightarrow B$ määräytyy arvoista $\phi((12))$ ja $\phi((23))$. Koska $(12)(12) = (23)(23) = \text{id}$, täytyy olla $\phi((12))^2 = \phi((23))^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

7. NORMAALI ALIRYHMÄ JA TEKIJÄRYHMÄ

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

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

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

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

Propositio 7.1. *Olkoon G ryhmä, ja olkoon H sen aito aliryhmä. Tällöin*

- (1) $gH = H$, jos ja vain jos $g \in H$.
- (2) $Hg = H$, jos ja vain jos $g \in H$.
- (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 66.

(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 inklusion toiseen suuntaan. Kohdan (4) todistus on samanlainen.

(5) Vasemman sivuluokan määritelmän nojalla kuvaus $\ell_x: H \rightarrow xH$, $\ell_x h = xh$, on surjektio. Supistussäännöstä (Propositio 4.4) seuraa, että ℓ_x on injektio. Vastaavasti kuvaus $r_x: H \rightarrow Hx$, $r_x h = hx$, antaa bijektion joukkojen H ja Hx välille. $\square$

Propositioden 7.1 ja 3.5 mukaan vasemmat sivuluokat määräävät ekvivalenssirelaation, jonka ekvivalenssiluokat ovat vasemmat sivuluokat ja vastaavasti oikeat sivuluokat määräävät ekvivalenssirelaation, jonka ekvivalenssiluokat ovat oikeat sivuluokat. Vasempien sivuluokkien kokoelmalle käytetään merkintää G/H ja oikeiden sivuluokkien kokoelmalle käytetään merkintää $H \backslash G$. Jälkimmäistä merkintää ei pidä sekoittaa joukkojen erotukseen.

Propositio 7.2. *Olkoon G ryhmä ja olkoon $H \leq G$. Joukot G/H ja $H \backslash G$ ovat yhtä mahtavia.*

Todistus. Harjoitustehtävä 67 $\square$

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

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

Sen oikeat sivuluokat ovat

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

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

Usein, jos ryhmä G ei ole kommutatiivinen, sillä on aliryhmiä, joiden vasemmat ja oikeat sivuluokat eroavat toisistaan. Harjoitustehtävissä 69–71 tarkastellaan esimerkkiä ryhmästä, joka ei ole kommutatiivinen vaikka sen kaikkien aliryhmien vasemmat ja oikeat sivuluokat ovat samoja joukkoja. Kommutatiivisten ryhmien tilanne on yksinkertaisempi:

Lemma 7.4. *Olko G kommutatiivinen ryhmä. Tällöin jokaiselle $x \in G$ ja jokaiselle $H \leq G$ pätee $xH = Hx$.* $\square$

Esimerkki 7.5. Kongruenssi modulo q on aliryhmän $q\mathbb{Z}$ määräämä ekvivalenssirelaatio. Koska $(\mathbb{Z}, +)$ on kommutatiivinen, aliryhmän $q\mathbb{Z}$ vasemmat ja oikeat sivuluokat ovat samoja ja kongruenssin modulo q ekvivalenssiluokat eli kongruenssiluokat ovat joukot

$$[n] = \{n + kq : k \in \mathbb{Z}\} = n + q\mathbb{Z} = \{kq + n : k \in \mathbb{Z}\} = q\mathbb{Z} + n,$$

koska laskutoimitukselle käytetään additiivista merkintää. Kongruenssiluokkien joukolle Esimerkissä 3.9 käyttöön otettu merkintä $\mathbb{Z}/q\mathbb{Z}$ on yllä käyttöön otetun yleisemmän merkintätavan mukainen. Kongruenssiluokkien laskutoimitukset voidaan siis kirjoittaa myös näin

$$(n + q\mathbb{Z}) + (m + q\mathbb{Z}) = (n + m) + q\mathbb{Z}$$

ja

$$(n + q\mathbb{Z})(m + q\mathbb{Z}) = nm + q\mathbb{Z}.$$

Ryhmän ja sen aliryhmän suhdetta kuvaava indeksi voidaan määritellä kumman tahansa aliryhmään H liittyvän ekvivalenssirelaation avulla Proposition 7.2 nojalla:

Määritelmä 7.6. Aliryhmän $H < G$ indeksi on

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

Esimerkki 7.7. (a) Aliryhmän $C_2 \times \{e\}$ indeksi ryhmässä $C_2 \times C_2$ on

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

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

Lause 7.8 (Lagrange'n lause). *Olko G äärellinen ryhmä, ja olko $H < G$. Tällöin*

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

Todistus. Proposition 7.1 nojalla kaikki sivuluokat ovat yhtä mahtavia ja sivuluokat osittavat ryhmän G . $\square$

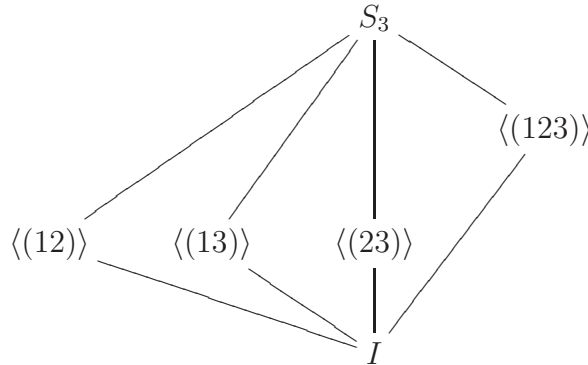
Propositio 7.9. *Olko G äärellinen ryhmä. Tällöin $g^{\#G} = e$ jokaiselle $g \in G$.*

Todistus. Olko $H = \langle g \rangle$. Tällöin $\#H = \text{ord } g$. Koska Lagrange'n lauseen mukaan $\#G = k\#H$ jollain $k \in \mathbb{N}$, pätee potenssisääntöjen ja Lemman 6.2 nojalla

$$g^{\#G} = g^{k \text{ord } g} = (g^{\text{ord } g})^k = e^k = e. \quad \square$$

Koska ryhmän kertaluku ja aliryhmän indeksi ovat luonnollisia lukuja, Lagrange'n lause antaa äärellisen ryhmän G aliryhmien mahdolliset indeksit ja kertaluvut.

Esimerkki 7.10. 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 päällekkäisille 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 $I = \{\text{id}\}$.

Esimerkissä 7.10 permutaatioryhmällä S_3 on jokaista Lagrangen lauseen sallimaa kokoa olevia aliryhmiä. Aina ei kuitenkaan ole näin, Esimerkissä 7.27 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 $H \triangleleft G$.

Koska ryhmän G normaalin aliryhmän H vasemmat ja oikeat sivuluokat määräävät saman osituksen ryhmälle G , ne määräävät saman ekvivalenssirelaation. ovat samat. Tämä on oleellisen tärkeää tarkasteltaessa ryhmän G laskutoimituksen yhteensopivuutta sivuluokkien määräämän ekvivalenssirelaation kanssa Lauseessa 7.20.

Esimerkki 7.12. (a) Ryhmä itse ja neutraali-alkion muodostama aliryhmä ovat normaaleja.

(b) Lemman 7.4 mukaan $n\mathbb{Z} \triangleleft \mathbb{Z}$ ja $\mathbb{R} \times \{0\} \triangleleft \mathbb{R}^2$, mutta Esimerkin 7.3 aliryhmä $\langle(12)\rangle < S_3$ ei ole normaali.

Joissain tilanteissa normaalius on helppo tarkastaa:

Lemma 7.13. Jos aliryhmän $H < G$ indeksi on kaksi, se on normaali.

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

Lemma 7.14. Olkoon $K \trianglelefteq G$ ja $K < H < G$. Tällöin $K \trianglelefteq H$. □

Esimerkki 7.15. $A_n \triangleleft S_n$, sillä $\#S_n = n! = 2 \#A_n$, joten $[S_n : A_n]$ 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 $g^{-1}H \subset Hg^{-1}$ kaikille $g \in G$. Koska jokainen ryhmän G alkio on jonkin alkion käänteisalkio, väite on todistettu. $\square$

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

Propositio 7.17. *Olkoon $\phi: G \rightarrow G'$ ryhmähomomorfismi.*

(1) *Olkoon $H \trianglelefteq G$. Tällöin $\phi(H) \trianglelefteq \text{Im } \phi$.*

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

Todistus. (1) Proposition 5.6 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 74. $\square$

Propositioista 7.17 saadaan tärkeänä erikoistapauksena

Seuraus 7.18. *Ryhmähomomorfismin ydin on normaali aliryhmä.* $\square$

Esimerkki 7.19. (a) $A_n = \ker \epsilon \triangleleft S_n$.

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

Lause 7.20. *Olkoon G ryhmä ja olkoon $H < G$ 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 $h_1y = yh_3$, joten

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

Siis $x'y'H$ ja xyH Proposition 7.1 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 3.8. Koska luonnollinen homomorfismi on surjektiivinen, se kuvaa ryhmän G neutraali-alkion tekijälaskutoimituksen neutraali-alkioksi Proposition 1.14 nojalla, pätee $gHH = gH' = HgH$ ja $(gH)(g^{-1}H) = H$ kaikilla $g \in G$.

Luonnollinen homomorfismi on siis ryhmähomomorfismi $G \rightarrow G/H$ ja sen ydin on H . Proposition 7.17 nojalla H on normaali. $\square$

Seuraus 7.21. *Jos $H \trianglelefteq G$, niin tekijäjoukko G/H varustettuna tekijälaskutoimituksella on ryhmä. Tekijäryhmän G/H neutraali-alkio on H .* $\square$

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 $a \equiv b \pmod{q}$ vastaava kokonaislukujen ryhmän tekijäryhmä. Additiivisen ryhmän alkion x sivuluokalle käytetään merkintää $x + H$ ja tekijäryhmän laskutoimitus on siis

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

Sykliset ryhmät käyttäytyvät hyvin tekijäryhmienkin suhteen

Propositio 7.22. *Jokainen syklisen ryhmän tekijäryhmä on syklinen.*

Todistus. Harjoitustehtävä 76. □

Todistamme seuraavaksi tärkeimmän tekijäryhmiä koskevan tuloksen. Todistus on Lauseen 5.18(1) todistuksen yleistys.

Lause 7.23 (Ryhmiä (ensimmäinen) isomorfismilause). *Olkoon $\phi: G \rightarrow G'$ ryhmähomomorfismi. Tällöin*

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

Todistus. Jos $x \ker \phi = y \ker \phi$, niin jollain $h \in \ker \phi$ pätee $y = xh$, joten

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

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

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

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 $\text{Im } \psi \subset \text{Im } \phi$ ja jokaiselle $x \in G$ pätee $\psi(x \ker \phi) = \phi(x)$, joten $\phi(x) \in \text{Im } \psi$ 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 7.1(1) nojalla seuraa $x \ker \phi = \ker \phi$. □

Seuraus 7.24. *Jos $\phi: G \rightarrow G'$ on surjektiivinen ryhmähomomorfismi ja $N = \ker \phi$, niin $[G : N] = \#G'$.* □

Lause 7.25. *Olkoon $\phi: G \rightarrow G'$ surjektiivinen ryhmähomomorfismi, ja olkoon $H' \trianglelefteq G'$. Tällöin $G / \phi^{-1}(H') \cong G' / H'$.*

Todistus. Proposition 7.17(2) mukaan $H = \phi^{-1}(H') \trianglelefteq G$. Olkoon $\pi: G' \rightarrow G' / H'$ luonnollinen homomorfismi. Tällöin $\tilde{\psi} = \pi \circ \phi: G \rightarrow G' / H'$ on surjektiivinen homomorfismi, jonka ydin on H . Lauseen 7.23 mukaan $G / H \cong G' / H'$. □

Esimerkki 7.26. (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 $(2\mathbb{Z})^2$.

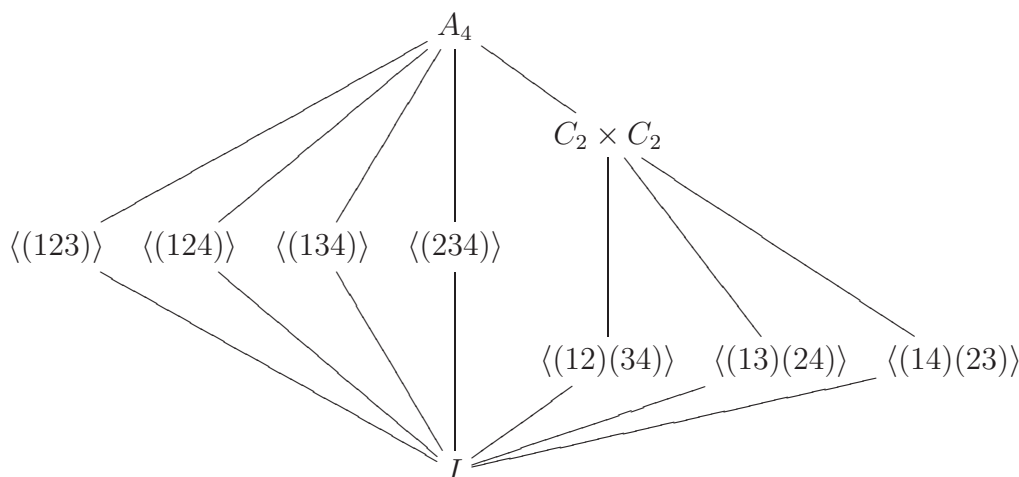
(b) $\text{GL}_n(\mathbb{R}) / \text{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times$ koska $\det \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$ on surjektiivinen homomorfismi.

Ryhmiä isomorfismilause antaa vastaavuuden surjektiivisten homomorfismien ja normaali aliryhmien välille: Jos $N \trianglelefteq G$, niin luonnollinen homomorfismi on surjektiivinen homomorfismi $G \rightarrow G/N$. Toisaalta jokaisen ryhmähomomorfismin ydin on määrittelyryhmänsä normaali aliryhmä. Tämä vastaavuus ei kuitenkaan ole bijektio sillä esimerkiksi homomorfismeilla $\exp: \mathbb{C} \rightarrow \mathbb{C}^\times$ ja $k \circ \exp$, missä k on kompleksikonjugointi, on sama ydin $\ker \exp = \{k 2\pi i : k \in \mathbb{Z}\}$.

Esimerkki 7.27. Osoitamme esimerkin avulla, että Lagrangen lauseen 7.8 käänteinen väite ei päde: Alternoivan ryhmän A_4 kertaluku on $\#A_4 = 4!/2 = 12$. Jos $H < A_4$ on aliryhmä, jonka kertaluku on 6, niin Lagrangen lauseen nojalla $[A_4 : H] = 2$. Lemman 7.13 nojalla $H \triangleleft A_4$, joten ensimmäisen isomorfismilauseen nojalla $A_4/H \cong C_2$. Siis kaikille $g \in G$ pätee $g^2H = gHgH = H$, joten Proposition 7.1(1) nojalla $g^2 \in H$ kaikille $g \in G$.

Kaikki 3-sykliä ovat parillisia permutaatioita, joten ne kuuluvat ryhmään A_4 . Jos $g \in A_4$ on 3-sykli, niin $g = g^4 = (g^2)^2 \in H$. Kuitenkin ryhmässä A_4 on 8 3-sykliä, joiden siis pitäisi sisältyä kuuden alkion ryhmään. Siis ryhmällä A_4 ei ole kuuden alkion aliryhmää vaikka $\#A_4 = 12 = 6 \times 2$.

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 esiintyvä Kleinin neliryhmän $C_2 \times C_2$.

Esimerkin 6.9 tarkastelun yleistys kolmeen ulottuvuuteen osoittaa, että ryhmä A_4 on isomorfinen säännöllisen tetraedrin symmetriaryhmän kanssa.

Esimerkki 7.28. (a) Harjoitustehtävässä 33 osoitettiin, että ryhmän G automorfismit muodostavat ryhmän $\text{Aut}(G)$. Olkoon $a \in G$. Kuvaus $\phi_a: G \rightarrow G$, $\phi_a(g) = aga^{-1}$ on ryhmän G automorfismi: Se on homomorfismi:

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

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

Ryhmän G sisäiset automorfismit muodostavat *sisäisten automorfismien ryhmän*

$$\text{Inn}(G) = \{\phi_a : a \in G\} < \text{Aut}(G).$$

Harjoitustehtävässä 77 osoitetaan, että sisäisten automorfismien ryhmä on automorfismiryhmän normaali aliryhmä. Tekijäryhmä

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

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 78 osoitetaan, että $Z(G)$ on ryhmän G normaali aliryhmä.

(c) Kuvaus $\rho: G \rightarrow \text{Aut}(G)$, $\rho(a) = \phi_a$, on homomorfismi. Tämä tarkastetaan kuten Proposition 6.10 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 $\text{Im}(\rho) = \rho(G) = \text{Inn}(G)$. Lisäksi $\rho(g)$ on identtinen automorfismi täsmälleen silloin, kun $g \in Z(G)$, joten ryhmien isomorfismlauseen nojalla pätee

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

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

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

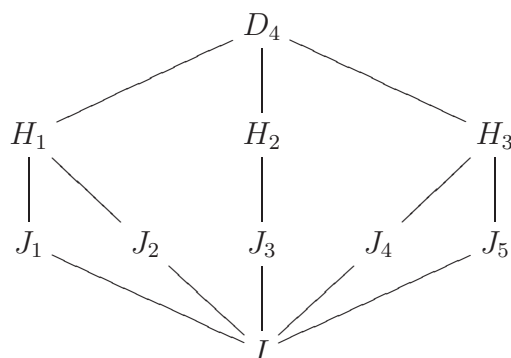
Harjoitustehtävässä 32 osoitettiin, että kuvaukset $B \mapsto B^{-1}$ ja $C \mapsto {}^tC$ eivät ole ryhmän $\mathrm{SL}_2(\mathbb{Z})$ automorfismeja. Kuitenkin niiden yhdistetty kuvaus on automorfismi!

Harjoitustehtäviä.

Tehtävä 66. Olkoon G ryhmä, ja olkoon H sen aito aliryhmä. Osoita, että $gH = H$, jos ja vain jos $g \in H$

Tehtävä 67. Olkoon G ryhmä, ja olkoon $H < G$. Osoita, että tekijäjoukkojen välinen kuvaus $b : G/H \rightarrow H \backslash G$, $b(aH) = Ha^{-1}$ on bijektio.

Tehtävä 68. 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.

Tehtävä 69. Osoita, että ryhmä H ei ole kommutatiivinen ja että $\#H = 8$.

Tehtävä 70. Osoita, että ryhmällä H on aliryhmien H ja $\{I\}$ lisäksi neljä aliryhmää, jotka ovat kaikki normaaleja.

Tehtävä 71. Piirrä ryhmän H aliryhmäkaavio.

⁶⁸Vihje: Kaikki ryhmät H_j , $1 \leq j \leq 3$ eivät ole isomorfisia.

⁶⁹Vihje: Tarkasta ensin, että $BA = -AB$ ja käytä tätä tietoa ja Propositiota 5.11

Tehtävä 72. Olkoon G äärellinen ryhmä. Olkoot $K < H < G$. Osoita Lagrangen lauseen avulla, että indekseille pätee:

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

Tehtävä 73. Olkoon G ryhmä. Olkoot $K < H < G$ siten, että $[G : H] < \infty$ ja $[H : K] < \infty$. Osoita, että indekseille pätee:

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

Tehtävä 74. Olkoon $\phi: G \rightarrow G'$ ryhmähomomorfismi. Olkoon $H' \trianglelefteq G'$. Osoita, että

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

Tehtävä 75. Olkoon tA neliömatriisin A transpoosi, ja olkoon I_n identtinen $n \times n$ -matriisi. Olkoon

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

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

Tehtävä 76. Olkoon C syklinen ryhmä. Osoita, että kaikki ryhmän C tekijäryhmät ovat syklisiä.

Tehtävä 77. Olkoon G ryhmä. Osoita, että ryhmän G sisäiset automorfismit muodostavat ryhmän $\text{Aut}(G)$ normaalin aliryhmän.

Tehtävä 78. Osoita, että ryhmän G keskus $Z(G)$ on kommutatiivinen normaali aliryhmä.

Tehtävä 79. Määritä ryhmien S_3 , D_3 ja $C_2 \times C_2$ keskukset.

Tehtävä 80. Määritä ryhmien S_3 , D_3 ja $C_2 \times C_2$ sisäiset automorfismiryhmät.

⁷³Vihje: Oletetaan, että $G = \bigsqcup_{i=1}^m a_i H$ ja $H = \bigsqcup_{j=1}^n b_j K$. Osoita, että $G = \bigsqcup_{i=1}^m \bigsqcup_{j=1}^n a_i b_j K$.

8. RENKAAT

Tarkastelemme seuraavaksi rakenteita, joissa on määritelty kaksi assosiatiivista laskutoimitusta, joista toinen on kommutatiivinen. Vaadimme näillä laskutoimituksilla varustetulta joukolta joitakin samoja ominaisuuksia joita kokonaisluvuilla on, mutta kertolasku ei välttämättä ole kommutatiivinen.

Määritelmä 8.1. Olkoon $R \neq \emptyset$ joukko, jolla on määritelty kaksi assosiatiivista laskutoimitusta, kommutatiivinen yhteenlasku $+$ ja toinen laskutoimitus, jota merkitsemme kertolaskulla. Kolmikko $(R, +, \cdot)$ on (*ykkösellinen*) *renkas*, jos

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

Laskutoimituksen $+$ neutraalialkioille käytetään merkintää $0 = 0_R$. Ryhmä $(R, +)$ on renkaan R *additiivinen ryhmä*. Renkas 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 $q \in \mathbb{N}$. Kongruenssiluokkien muodostama joukko $\mathbb{Z}/q\mathbb{Z}$ varustettuna kokonaislukujen yhteen- ja kertolaskujen tekijälaskutoimituksilla on kommutatiivinen renkas. (Harjoitustehtävä 81)

(c) Olkoon $X \neq \emptyset$, ja olkoon R renkas. Olkoon $\mathcal{F}(X, R)$ joukko, joka koostuu kaikista kuvauksista joukolta X renkaaseen R . Määritellään tässä joukossa yhteen- ja kertolasku pisteittäin: Olkoot $f, g \in \mathcal{F}(X, R)$. Asetamme

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

kaikilla $x \in X$. Joukko $\mathcal{F}(X, R)$ varustettuna näillä laskutoimituksilla on renkas, 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. Kertolaskun neutraalialkio on vakiofunktio $1: X \rightarrow R$, joka määritellään asettamalla $1(x) = 1 \in R$ kaikilla $x \in X$.

Tässä esimerkissä merkitsemme kuten on tapana renkaan $\mathcal{F}(X, R)$ 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.

Renkas $\mathcal{F}(X, R)$ on kommutatiivinen, jos R on kommutatiivinen. Esimerkiksi siis $\mathcal{F}(\mathbb{R}, \mathbb{R})$ on kommutatiivinen renkas.

Propositio 8.3. *Olkoon R renkas. Tällöin*

- (1) $0_R \cdot x = 0_R$ kaikilla $x \in R$,
- (2) $x(-y) = (-x)y = -(xy)$ kaikilla $x, y \in R$,
- (3) $x(y - z) = xy - xz$ ja $(y - z)x = yx - zx$ kaikilla $x, y, z \in R$,

Todistus. (1) Distributiivisuuden nojalla

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

kaikilla $x \in R$. Supistussäännöstä seuraa, että $0_R x = 0_R$.

Loput todistetaan harjoitustehtävässä 83. □

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

$$x = 1x = 0x = 0.$$

Toinen väite todistetaan harjoitustehtävänä 85. □

Renkaan yhteen- ja kertolaskuiksi kutsuttujen laskutoimitusten ei tarvitse olla tavanomaisia lukujen yhteen- ja kertolaskuja tai näistä lukujen 1 ja 3 konstruktiolla muodostettuja laskutoimituksia vaan ne voivat olla mitä tahansa laskutoimituksia, joilla on vaaditut ominaisuudet.

Esimerkki 8.5. (a) Olkoon $(A, +)$ kommutatiivinen ryhmä. Olkoon

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

Varustamme joukkoon $\text{Hom}(A, A)$ kahdella laskutoimituksella: Homomorfismien yhteenlasku määritellään asettamalla

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

ja kertolaskuna käytetään homomorfismien yhdistämistä. Yhteenlasku on laskutoimitus: Jos $\phi, \phi' \in \text{Hom}(A, A)$, 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 $\phi + \phi' \in \text{Hom}(A, A)$. Laskutoimituksella varustettu joukko $(\text{Hom}(A, A), +)$ on kommutatiivinen ryhmä. Laskutoimituksen assosiativisuus ja kommutatiivisuus osoitetaan harjoitustehtävässä 84. Homomorfismien yhteenlaskun neutraalialkio on nollahomomorfismi 0 , $0(a) = 0$ kaikille $a \in A$, ja homomorfismin ϕ käänteisalkio yhteenlaskun suhteen on homomorfismi $-\phi$, joka määritellään asettamalla $(-\phi)(a) = -\phi(a)$ kaikilla $a \in A$.

Identtinen homomorfismi on homomorfismien kertolaskun neutraalialkio, joten tarkastettavaksi jää kertolaskun distributiivisuus yhteenlaskun suhteen: Jos $\phi, \psi, \zeta \in \text{Hom}(A, A)$, 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 $\text{Hom}(A, A)$ kertolasku, homomorfismien yhdistetty kuvaus on yllä merkitty ilman yhdistetyn kuvauksen merkkiä $\circ$.

(b) Olkoon R rengas, $\#R \geq 2$. Kaikkien R -kertoimisten $n \times n$ -matriisien joukko $M_n(R)$ varustettuna matriisien yhteen- ja kertolaskulla on rengas. Kaikki muut ominaisuudet paitsi distributiivisuus osoitettiin tapauksessa $n = 2$ ja $R = \mathbb{R}$ Esimerkissä 1.13(b) ja harjoitustehtävässä 4. Kun $n \geq 2$, niin $M_n(R)$ ei ole kommutatiivinen rengas, koska matriisien kertolasku ei ole kommutatiivinen.

Määritelmä 8.6. Jos R on rengas ja alkiolla $u \in R$ on käänteisalkio kertolaskun suhteen, niin u on renkaan R yksikkö. Renkaan R yksiköiden ryhmä (tai multiplikaatiivinen ryhmä) on

$$R^\times = \{u \in R : u \text{ on yksikkö}\}$$

varustettuna renkaan R kertolaskun indusoimalla laskutoimituksella.

Propositio 8.7. 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 $(u^{-1})^{-1} = u$. $\square$

Jos renkaassa on ainakin kaksi alkioita, niin $0 \neq 1$ ja 0 ei ole yksikkö.

Määritelmä 8.8. Olkoon R rengas, jossa on ainakin kaksi alkioita. Jos kaikki renkaan R nollasta poikkeavat alkiot ovat yksiköitä, niin R on *jakorengas*. Kommutatiivinen jakorengas on *kunta*. Jakorengas, joka ei ole kunta on *vinokunta*.

Määritelmä 8.9. Olkoon R rengas, $\#R \geq 2$.

- (1) Jos $a, b, c \in R$ siten, että $ab = c$, niin a ja b ovat alkion c tekijöitä.
- (2) Jos $a, b \in R$, $a, b \neq 0$, ja $ab = 0$, niin a ja b ovat nollan jakajia.
- (3) Jos renkaassa R ei ole nollan jakajia, ja R on kommutatiivinen, niin R on kokonaisalue.

Jos $d, m \in R$ ja d on alkion m tekijä sanotaan joskus, että d jakaa alkion m ja merkitään $d \mid m$.

Esimerkki 8.10. (a) $\mathbb{Z}$ on kokonaisalue mutta se ei ole jakorengas eikä siis kunta. Renkaan $\mathbb{Z}$ ainoat yksiköt ovat ± 1 .

(b) $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat kuntia.

(c) Matriisirengas $M_n(R)$ ei ole kokonaisalue, kun $n \geq 2$, koska monella matriisilla ei ole käänteismatriisia. Esimerkiksi $M_n(\mathbb{R})^\times = \text{GL}_n(\mathbb{R})$.

(d) Hamiltonin kvaterniot on joukko

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in M_2(\mathbb{C}) \right\}.$$

varustettuna matriisien yhteenlaskulla ja matriisien kertolaskulla. Suoraviivainen lasku osoittaa, että $\mathbb{H}$ vakaa yhteenlaskun ja kertolaskun suhteen ja että se on rengas renkaasta $M_2(\mathbb{C})$ indusoiduilla laskutoimituksilla. Lisäksi

$$\det \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = |a|^2 + |b|^2,$$

joten jokainen $A \in \mathbb{H} \setminus \{0\}$ on kääntyvä matriisi. Lisäksi

$$\frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = I_2,$$

joten kaikki nollasta poikkeavat alkiot ovat yksiköitä. 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 $\phi: \mathbb{C} \rightarrow \mathbb{H}$, $\phi(z) = \text{diag}(z, \bar{z})$ on homomorfismi yhteenlaskun ja kertolaskun suhteen, joten voimme samastaa sen kuvajoukon

$$\phi(\mathbb{C}) = \left\{ \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix} \in M_2(\mathbb{C}) \right\}.$$

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

$$(7) \quad \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$

ja

$$(8) \quad \mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \quad \mathbf{ki} = \mathbf{j} = -\mathbf{ik}, \quad \mathbf{jk} = \mathbf{i} = -\mathbf{kj}.$$

Matriisit $1, \mathbf{i}, \mathbf{j}$ ja $\mathbf{k}$ virittävät avaruuden $\mathbb{H}$ neliulotteisena reaalisen vektoriavaruuksena, joten Hamiltonin kvaterniot voidaan esittää reaalina 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 (7) ja (8).

Esimerkki 8.11. Jos $A, B \in M_n(R)$, ja niiden ainoat nollasta poikkeavat kertoimet ovat A_{11} ja B_{nn} , niin $AB = 0$. Siis matriisit A ja B ovat nollan jakajia.

Propositio 8.12. *Jakorengaassa ei ole nollan jakajia. Erityisesti kunta on kokonaisalue.*

Todistus. Olkoon K jakorengas. Olkoot $a, b \in K$, $a, b \neq 0$. Tällöin a ja b ovat yksiköitä, joten niillä on käänteisalkiot kertolaskun suhteen. Oletetaan, että $ab = 0$. Silloin $b = a^{-1}0 = 0$, mikä on ristiriita. $\square$

Lause 8.13. *Äärellinen kokonaisalue on kunta.*

Todistus. Olkoon E äärellinen kokonaisalue. Olkoon $a \in E$, $a \neq 0$. Kuvaus $\ell_a: E \rightarrow E$, $\ell_a(x) = ax$ on injektio: Jos $\ell_a(x) = \ell_a(y)$, niin $a(x - y) = 0$. Koska kokonaisalueessa E ei ole nollan jakajia, $x = y$. Kuvaus ℓ_a on surjektio, koska E on äärellinen. Siis on $\bar{a} \in E$, jolle $a\bar{a} = 1$. Koska E on kommutatiivinen, $\bar{a} = a^{-1}$. $\square$

Määritelmä 8.14. Olkoot R ja R' renkaita. Kuvaus $\phi: R \rightarrow R'$ on rengashomomorfismi, jos

- ϕ on homomorfismi yhteenlaskulle ja kertolaskulle ja
- $\phi(1) = 1$.

Bijektiivinen rengashomomorfismi on *rengasisomorfismi*. Jos renkaat R ja R' ovat kuntia, sanotaan rengashomomorfismia $\phi: R \rightarrow R'$ *kuntahomomorfismiksi*.

Propositiossa 1.14 osoitettiin, että surjektiivinen homomorfismi kuvaa neutraali-alkion neutraali-alkioksi, mutta ilman surjektiivisuutta näin ei välttämättä ole. Ryhmähomomorfismille ei tarvita vastaavaa vaatimusta Proposition 4.12 nojalla. Erityisesti siis rengashomomorfismi kuvaa nollan nollaksi.

Esimerkki 8.15. (a) Luonnollinen kuvaus renkaasta $(\mathbb{Z}, +, \cdot)$ renkaaseen $(\mathbb{Z}/q\mathbb{Z}, +, \cdot)$ on surjektiivinen rengashomomorfismi.

(b) Kuvaus $h: \mathcal{F}(\mathbb{R}, \mathbb{R}) \rightarrow \mathbb{R}$, $h(f) = f(\frac{1}{2})$ on rengashomomorfismi:

$$\begin{aligned} h(f+g) &= (f+g)(1/2) = f(1/2) + g(1/2) = h(f) + h(g), \\ h(fg) &= (fg)(1/2) = f(1/2)g(1/2) = h(f)h(g) \end{aligned}$$

ja

$$h(1) = 1(1/2) = 1.$$

Propositio 8.16. (1) Jos $f: R \rightarrow S$ ja $g: S \rightarrow T$ ovat rengashomomorfismeja, niin $g \circ f$ on rengashomomorfismi.

(2) Rengashomomorfismi $f: R \rightarrow S$ on rengasisomorfismi, jos ja vain jos on rengashomomorfismi $\bar{f}: S \rightarrow R$, jolle $\bar{f} \circ f = \text{id}_R$ ja $f \circ \bar{f} = \text{id}_S$.

Todistus. Harjoitustehtävät 86 ja 87. □

Kokonaislukujen renkaan $\mathbb{Z}$ kaikki alkiot ovat alkion 1 monikertoja. Tästä seuraa erityisominaisuus renkaassa $\mathbb{Z}$ määritellyille rengashomomorfismeille:

Propositio 8.17. Olkoon R rengas. On täsmälleen yksi rengashomomorfismi $\phi: \mathbb{Z} \rightarrow R$.

Todistus. Koska 1 virittää additiivisen ryhmän $(\mathbb{Z}, +)$, Proposition 5.13 nojalla halutunlaisia homomorfismeja on korkeintaan yksi. Väite seuraa havainnosta, että kuvaus $\phi: \mathbb{Z} \rightarrow R$, $\phi(n) = n1_R = 1_R + 1_R + \cdots + 1_R$, on rengashomomorfismi:

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

ja

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

Monilla renkailla on yhteen- ja kertolaskun suhteen vakaita osajoukkoja, jotka ovat renkaita.

Määritelmä 8.18. 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. Jos R ja S ovat kuntia, niin S on kunnan R alikunta.

Määritelmän mukaan alirenkaan inkluusiokuvaus $i: S \rightarrow R$, $i(s) = s$ on rengashomomorfismi.

Esimerkki 8.19. (a) $\mathbb{Z}$ on renkaan $\mathbb{Q}$ alirengas.

(b) Joukko

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$$

on rengas renkaasta $M_2(\mathbb{R})$ indusoiduilla laskutoimituksilla. Sen kertolaskun neutraalialkio on $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, joten S ei ole renkaan $M_2(\mathbb{R})$ alirengas. Rengas S on rengasisomorfinen renkaan $\mathbb{R}$ kanssa: Kuvaus $a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ on rengasisomorfismi.

Alirenkaalle on samanlainen testi kuin aliryhmälle (Propositio 5.11).

Propositio 8.20. Olkoon R rengas, ja olkoon $S \subset R$, $S \neq \emptyset$. Tällöin S on renkaan R alirengas, jos ja vain jos

(1) Kaikille $x, y \in S$ $x + y \in S$ ja $xy \in S$, ja

(2) $-1 \in S$.

Todistus. Harjoitustehtävä 90. □

Esimerkki 8.21. (a) Samaan tapaan kuin permutaatioryhmille määriteltiin aliryhmiä rajoittumalla kuvauksiin, joilla on tiettyjä ominaisuuksia, voimme määritellä funktiorenkaiden $\mathcal{F}(X, R)$ alirenkaita. Kurssilla Analyysi 2 osoitetaan, että indusoiduilla laskutoimituksilla varustetut joukot

$$C(\mathbb{R}) = \{f: \mathbb{R} \rightarrow \mathbb{R} : f \text{ on jatkuva}\}, \text{ ja}$$

$$C^k(\mathbb{R}) = \{f: \mathbb{R} \rightarrow \mathbb{R} : f \text{ on } k \text{ kertaa jatkuvasti derivoituva}\}, \quad k \in \mathbb{N}.$$

ovat funktiorenkaiden $\mathcal{F}(\mathbb{R}, \mathbb{R})$ alirenkaita

(b) Vektoriavaruuden $\mathbb{R}^n$ lineaarikuvaukset muodostavat renkaan $\text{Hom}(\mathbb{R}^n, \mathbb{R}^n)$ alirenkaan

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

Lineaarikuvaukset ovat ryhmän $(\mathbb{R}^n, +)$ homomorfismeja itselleen, joten niiden summa on myös homomorfismi. Lisäksi aina, kun $L, L' \in \text{End}(\mathbb{R}^n)$, $x \in \mathbb{R}^n$ ja $a \in \mathbb{R}$, myös

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

joten lineaarikuvauksen toinenkin ehto toteutuu. Lineaarialgebran kurssilla on osoitettu, että lineaarikuvausten yhdistetty kuvaus on lineaarikuvaus. Siis molemmat laskutoimitukset toteuttavat Proposition 8.20 ehdon (1). Lisäksi identtinen kuvaus $\text{id}: \mathbb{R}^n \rightarrow \mathbb{R}^n$ on lineaarikuvaus, kuten myös $-\text{id}$, joten Proposition 8.20 mukaan $\text{End}(\mathbb{R}^n)$ on renkaan $\text{Hom}(\mathbb{R}^n, \mathbb{R}^n)$ alirengas.

(c) Esimerkissä 4.13 käsitelty kuvaus $\text{Mat}: \text{End}(\mathbb{R}^n) \rightarrow M_n(\mathbb{R})$, joka liittää lineaarikuvaukseen L sen matriisin kiinnitetyssä kannassa, on rengasisomorfismi. Jos $L, L' \in \text{End}(\mathbb{R}^n)$, niin $(L + L')(v) = Lv + L'v$, joten

$$\text{Mat}(L + L') = \text{Mat}(L) + \text{Mat}(L'),$$

eli Mat on ryhmähomomorfismi additiivisten ryhmien välillä. Lisäksi kaikille lineaarikuvauksille $L, L' \in \text{End}(\mathbb{R}^n)$ pätee

$$\text{Mat}(L'L) = \text{Mat}(L') \text{Mat}(L)$$

ja identtisen kuvauksen matriisi on I_n .

Alirenkaat ja rengashomomorfismit ovat yhteensopivia samaan tapaan kuin aliryhmät ja ryhmähomomorfismit:

Propositio 8.22. *Olkoon $\phi: R \rightarrow R'$ 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 5.6 mukaan $(\phi(S), +)$ on ryhmä, joten Propositiota 8.20 sovellettaessa riittää 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 $-1_R \in S$, pätee

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

Siis Proposition 8.20 oletukset ovat voimassa.

(2) Harjoitustehtävä 91. □

Harjoitustehtäviä.

Tehtävä 81. Osoita, että $\mathbb{Z}/q\mathbb{Z}$ varustettuna kokonaislukujen yhteen- ja kertolaskujen tekijälaskutoimituksilla on kommutatiivinen rengas.

Tehtävä 82. Olkoon X joukko. Määritellään joukkojen $A, B \in \mathcal{P}(X)$ *symmetrinen erotus* asettamalla

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

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

Tehtävä 83. 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 $x, y, z \in R$,

Tehtävä 84. Olkoon $(A, +)$ kommutatiivinen ryhmä. Osoita, että joukon $\text{Hom}(A, A)$ laskutoimitus $+$, joka määritellään asettamalla

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

on assosiatiiivinen ja kommutatiivinen.

Tehtävä 85. Olkoon $R \neq \{0\}$ rengas. Osoita, että yhteenlaskun neutraalialkiolla 0 ei ole käänteisalkiota kertolaskun suhteen.

Tehtävä 86. Olkoot $f: R \rightarrow S$ ja $g: S \rightarrow T$ rengashomomorfismeja. Osoita, että $g \circ f$ on rengashomomorfismi.

Tehtävä 87. Osoita, että rengashomomorfismi $f: R \rightarrow S$ on rengasisomorfismi, jos ja vain jos on rengashomomorfismi $f: S \rightarrow R$, jolle $f \circ f = \text{id}_R$ ja $f \circ f = \text{id}_S$.

Tehtävä 88. Määritellään joukossa $\mathbb{Z}^3$ yhteenlasku komponenteittain ja kertolasku asettamalla

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

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

Tehtävä 89. Ovatko funktiorenkoot $\mathcal{F}([0, 1], \mathbb{R})$ ja $\mathcal{F}([0, 2], \mathbb{R})$ isomorfisia?

Tehtävä 90. Olkoon R rengas, ja olkoon $S \subset R$, $S \neq \emptyset$. Osoita, että S on renkaan R alirengas, jos ja vain jos

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

Tehtävä 91. Olkoon $\phi: R \rightarrow R'$ rengashomomorfismi. Olkoon S' renkaan R' alirengas. Osoita, että $\phi^{-1}(S')$ on renkaan R alirengas.

Tehtävä 92. 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 .

Tehtävä 93. 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 $a, b \in K'$, $b \neq 0$.

⁸²Vihje: Harjoitustehtävä 27.

⁸⁸Vihje: $(1, 0, 1)$

Tehtävä 94. Olkoon

$$K = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M_2(\mathbb{R}) \right\}$$

Osoita, että K varustettuna matriisien yhteen- ja kertolaskulla on kunta. Osoita, että kunta K on isomorfinen kompleksilukujen kunnan kanssa.

Tehtävä 95. Olkoot *Gaussin kokonaisluvut*

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

ja *Gaussin rationaaliluvut*

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

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

Tehtävä 96. Määritä Gaussin kokonaislukujen yksiköiden ryhmä.

Tehtävä 97. Osoita, että

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Z}\},$$

on reaalilukujen renkaan alirengas.

Tehtävä 98. Osoita, että $\mathbb{Z}[\sqrt{2}]^\times$ on ääretön.

⁹⁶Vihje: Käytä kompleksilukujen normin ominaisuuksia.

⁹⁸Vihje: Etsi sopiva yksikkö ja käytä Propositiota 8.7

9. KOKONAISLUKUJEN JAOLLISUUS

Tarkastelemme tässä luvussa jaollisuutta kokonaislukujen renkaassa $\mathbb{Z}$ ja todistamme tuloksia, joita käytetään kongruenssiluokkien renkaan $\mathbb{Z}/q\mathbb{Z}$ ominaisuuksien tarkastelussa. Luvussa 10 tarkastelemme polynomien jaollisuutta. Seuraavat jaollisuuden perusominaisuudet on helppo tarkastaa yleisessä tapauksessa.

Propositio 9.1. *Olkoon K kokonaisalue. 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 100. □

Alkiot, joilla on vain vähän tekijöitä ovat tärkeässä osassa jaollisuutta tarkasteltaessa.

Määritelmä 9.2. Luonnollinen luku $p \neq 1$ on *alkuluku*, jos kaikilla $m, n \in \mathbb{N}$, joille $mn = p$ pätee $m = 1$ tai $n = 1$.

Esimerkki 9.3. Luvut $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots$ ovat alkulukuja.

Kokonaislukuja käsiteltäessä merkintää p käytetään yleensä vain alkuluvuille.

Propositio 9.4. *Jokainen nollasta poikkeava kokonaisluku $q \in \mathbb{Z} \setminus \{0\}$ 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 $a_p(q) \neq 0$ vai äärelliselle joukolle alkulukuja p .

Todistus. Riittää tarkastella positiivisia lukuja. Selvästi väite pätee pienille luvuille $1, 2, 3, \dots$ 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 $m, n \in \mathbb{N} \setminus \{1, p\}$, 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. □

Määritelmä 9.5. Jos luku $d \in \mathbb{Z}$ jakaa kokonaisluvut a ja b , niin d on lukujen a ja b yhteinen tekijä. Jos $m, n \in \mathbb{Z} \setminus \{0\}$ $d \in \mathbb{Z}$ 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 $d = \text{syt}(m, n)$.

Jos $\text{syt}(m, n) = 1$, sanotaan, että luvut m ja n ovat *suhteellisia alkulukuja*, ja että m ja n ovat keskenään *jaottomia*.

Jos $d = \text{syt}(m, n)$, niin myös $-d = \text{syt}(m, n)$, joten $\text{syt}(m, n)$ on merkintä, ei funktio. Proposition 9.1 nojalla kahden kokonaisluvun suurin yhteinen tekijä on määritelty merkkiä vaille, jos voidaan osoittaa, että kaikilla kokonaislukupareilla on suurin yhteinen tekijä. Tämä seuraa alla todistettavasta Propositioista 9.6.

Propositio 9.6. *Olkoot $m, n \in \mathbb{Z} \setminus \{0\}$. Jos $\langle m, n \rangle = \langle d \rangle$, niin $d = \text{syt}(m, n)$.*

Todistus. 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 9.1(4) nojalla $e \mid d$. □

Seuraus 9.7. *Nollasta poikkeavilla kokonaisluvuilla on suurin yhteinen tekijä, joka on merkkiä vaille yksikäsitteinen.*

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 Propositionista 9.6 ja siitä, että $\mathbb{Z}^\times = \{-1, 1\}$. $\square$

Seuraus 9.8. (1) $\mathbb{Z}/q\mathbb{Z} = \langle a + q\mathbb{Z} \rangle$, jos ja vain jos $1 = \text{syte}(a, q)$.

(2) $a + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ on yksikkö, jos ja vain jos $1 = \text{syte}(a, q)$.

Todistus. (1) Harjoitustehtävä 101.

(2) Kongruenssin määritelmän nojalla $ab \equiv 1 \pmod{q}$, jos ja vain jos on $c \in \mathbb{Z}$, jolle $ab = 1 + cq$. Tämä taas on Proposition 9.6 ja Seurauksen 9.7 nojalla yhtäpitävää sen kanssa, että $1 = \text{syte}(a, q)$. $\square$

Edellisten tulosten nojalla siis kokonaislukujen $m, n \in \mathbb{Z}$ suurin yhteinen tekijä d voidaan esittää sopivien kokonaislukujen $r, s \in \mathbb{Z}$ avulla muodossa

$$(9) \quad d = rm + sn.$$

Yhtälöä (9) kutsutaan *Bezout'n yhtälöksi*.

Suurin yhteinen tekijä voidaan määritellä vastaavasti myös useammalle kokonaisluvulle: Aliryhmän $\langle a_1, a_2, \dots, a_n \rangle$ virittäjä on lukujen $a_1, a_2, \dots, a_n \in \mathbb{Z}$ suurin yhteinen tekijä.

Esimerkki 9.9. (a) $\text{syte}(12, 30) = 6$: Luvun 12 positiiviset tekijät ovat 1, 2, 3, 4, 6 ja luvun positiiviset tekijät ovat 30 1, 2, 3, 5, 6, 10, 15, 30.

(b) $\text{syte}(6, 10, 15) = 1$.

(c) $\text{syte}(n, n+1) = 1$ kaikilla $n \in \mathbb{N}$: Olkoon $d \in \mathbb{N}$ lukujen n ja $(n+1)$ jakaja. Koska d jakaa luvun $n + (-1)(n+1) = -1$, niin on oltava $d = 1$. Luvuilla n ja $n+1$ ei siis ole muita positiivisia yhteisiä tekijöitä kuin 1.

Propositio 9.10. *Alkulukuja on äärettömän monta.*

Todistus. Harjoitustehtävä 104 $\square$

Seuraavat jaollisuustulokset pätevät keskenään jaottomille luvuille.

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 $\text{syte}(a, b) = 1$, 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 $cxa + ybc = c$. $\square$

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

Todistus. Jos $p \nmid a$, niin $\text{syty}(a, p) = 1$. Proposition 9.11(2) perusteella $p \mid b$. Yleinen tapaus todistetaan induktiolla. $\square$

Nyt voimme täydentää Proposition 9.4 tuloksen kokonaislukujen aritmetiikan keskeiseksi tulokseksi.

Lause 9.13 (Aritmetiikan peruslause). *Jokainen nollasta poikkeava kokonaisluku $q \in \mathbb{Z} \setminus \{0\}$ 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. Propositionissa 9.4 osoitettiin, että q voidaan esittää väitteen mukaisen tulona. Osoitetaan yksikäsitteisyys. Riittää käsitellä positiivisia lukuja. Oletetaan, että

$$(10) \quad q = p_1 \cdots p_k = q_1 \cdots q_s,$$

missä p_i ja q_j ovat alkulukuja kaikilla $1 \leq i \leq k$ ja $1 \leq j \leq s$.

Koska $p_1 \mid n$, niin Lemman 9.12 perusteella se jakaa luvun q_j jollain $j = 1, \dots, s$. Numeroimalla tekijät $q_1, \dots, q_s$ 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 (10)

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

Kuten edellä päättelimme, että $p_2 = q_2$. Toistamalla prosessia, joka loppuu $\min(k, s)$ askeleen jälkeen, saamme $p_1 = q_1, p_2 = q_2, \dots, p_k = q_k$, erityisesti, $k = s$. $\square$

Määritelmä 9.14. Aritmetiikan peruslauseen antamaa luvun $n \in \mathbb{N}, n \geq 2$, esitystä

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

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

Sovellamme jaollisuustuloksia renkaiden $\mathbb{Z}/q\mathbb{Z}$ teoriaan:

Lause 9.15. *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. Kohtien (1) ja (2) yhtäpitävyys seuraa Lauseesta 8.13. Osoitetaan, että kohdat (1) ja (3) ovat yhtäpitäviä: Olkoot $x, y \in \mathbb{Z} \setminus q\mathbb{Z}$. Jos $(x + q\mathbb{Z})(y + q\mathbb{Z}) = q\mathbb{Z}$, niin $q \mid xy$. Jos q on alkuluku, niin Eukleideen lemmän nojalla $q \mid x$ tai $q \mid y$, jolloin $(x + q\mathbb{Z}) = 0$ tai $(y + q\mathbb{Z}) = 0$. Jos $q = ab$, $a, b \notin \{\pm 1\}$, ei ole alkuluku, niin q ei jaa tekijöitä a ja b , joten $a + q\mathbb{Z}$ ja $b + q\mathbb{Z}$ ovat nollan jakajia. $\square$

Lauseen 9.15 todistusta tarkastelemalla saadaan kaikkia kongruenssiluokkien muodostamia renkaita koskeva tulos

Propositio 9.16. *Alkio $a + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$, $a \notin q\mathbb{Z}$, on nollan jakaja, jos ja vain jos $\text{syty}(a, q) > 1$.*

Todistus. Harjoitustehtävä 103. $\square$

Seuraus 9.17. *Renkaan $\mathbb{Z}/q\mathbb{Z}$ nollasta poikkeava alkio on joko nollan jakaja tai yksikkö.*

Esimerkki 9.18. Renkaan $\mathbb{Z}/8\mathbb{Z}$ yksiköiden ryhmä on isomorfinen Kleinin neliryhmän $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ kanssa: Yksiköt toteuttavat $1 = 1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod{8}$ ja $3 \cdot 5 \equiv 7 \pmod{8}$. Kuvaus $1 \mapsto (0, 0)$, $3 \mapsto (0, 1)$, $5 \mapsto (1, 0)$, $7 \mapsto (1, 1)$ on isomorfismi.

Rengasteoriassa käytetään usein hieman alkuluvun määritelmää kuin tässä luvussa käytetty Määritelmä 9.2: Sanotaan, että renkaan R alkio p , joka ei ole yksikkö, on *renkaan R alkuluku*, jos kaikille $a, b \in R$ pätee $p \mid a$ tai $p \mid b$, jos $p \mid ab$, toisin sanoen, jos Eukleideen lemmän väite pätee alkiolle p . Alkiota $p \in R$, jonka kaikki tekijät ovat yksiköitä tai muotoa up , missä u on renkaan R yksikkö, sanotaan *renkaan R jaottomiksi alkioiksi*. Kokonaislukujen renkaassa jaottomat alkiot ja (rengasteorian määritelmän mukaiset) alkuluvut ovat samoja. Näillä määritelmillä luvut $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29, \dots$ ovat alkulukuja ja jaottomia lukuja. Aritmetiikan peruslause (Lause 9.14) pätee tälläkin määritelmällä kunhan alkutekijäesityksessä rajoitutaan positiivisiin alkulukuihin.

Alkulukuesityksen yksikäsitteisyys ei ole itsestään selvä asia: Olkoon

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

Joukko $\mathbb{P}$ on yhteenlaskun ja kertolaskun suhteen vakaa joukko mutta se ei ole rengas koska kertolaskulla ei ole neutraalialkiota. Yhteen- ja kertolaskulla varustetussa joukossa $\mathbb{P}$ voidaan määritellä käsitteet tekijä, jaollisuus ja alkuluku samaan tapaan kuin kokonaislukujen joukossa, esim. luku $m \in \mathbb{P}$ jakaa luvun $n \in \mathbb{P}$, jos on $k \in \mathbb{P}$ siten, että $n = km$. Joukon $\mathbb{P}$ alkulukuja ovat esimerkiksi 2, 6, 10, 14, 18, 26 ja 30. Nyt

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

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

Kahden kokonaisluvun suurimman yhteisen tekijän etsiminen listaamalla ensin molempien lukujen kaikki tekijät ja etsimällä suurin yhteinen tekijä näiden joukosta on isoilla luvuilla työläs menetelmä. Seuraavaan lemmaan perustuva *Eukleideen algoritmi* antaa tehokkaamman keinon suurimman yhteisen tekijän löytämiseksi.

Lemma 9.19. Jos $a, b, q, r \in \mathbb{Z}$ ja $a = qb + r$, niin $\text{syt}(a, b) = \text{syt}(b, r)$.

Todistus. Proposition 9.1 nojalla jokainen lukujen b ja r yhteinen tekijä jakaa summan $qb + r = a$. Vastaavasti jokainen lukujen a ja b yhteinen tekijä jakaa luvun $a - qb = r$. Pareilla a, b ja b, r on siis samat yhteiset tekijät. Siten on myös $\text{syt}(a, b) = \text{syt}(b, r)$. $\square$

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

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

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

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

$$(11) \quad a = q_1 b + r_1 \quad \text{ja} \quad 0 \leq r_1 < b.$$

Jos $r_1 = 0$, niin $b \mid a$. Tällöin $d = b$; lopetetaan.

Jos $r_1 > 0$, jaetaan b luvulla r_1 . Jakoyhtälö antaa luvut $q_2, r_2 \in \mathbb{Z}$, joille

$$(12) \quad b = q_2 r_1 + r_2 \quad \text{ja} \quad 0 \leq r_2 < r_1.$$

Lemman 9.19 nojalla $\text{syt}(a, b) = \text{syt}(b, r_1)$. Siten, jos $r_2 = 0$, niin $d = r_1$; lopetetaan.

Jos $r_2 > 0$, jaetaan r_1 luvulla r_2 . Jakoyhtälö antaa luvut $q_3, r_3 \in \mathbb{Z}$, joille

$$(13) \quad r_1 = q_3 r_2 + r_3 \quad \text{ja} \quad 0 \leq r_3 < r_2.$$

Jatketaan kuten edellä. Koska jakoyhtälön antamat jakojäännökset r_i eivät ole negatiivisia ja ne muodostavat aidosti vähenevän jonon,

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

niin jollain n on oltava $r_n = 0$. Viimeiset kaksi vaihetta ovat

$$(14) \quad r_{n-3} = q_{n-1}r_{n-2} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2},$$

$$(15) \quad r_{n-2} = q_n r_{n-1} + r_n, \quad r_n = 0.$$

Propositio 9.20 (Eukleideen algoritmi). *Olkoot a, b ja jakojäännökset r_i kuten yllä. Tällöin r_{n-1} , viimeinen positiivinen jakojäännös, on $\text{syt}(a, b)$.*

Todistus. Lemma 9.19 sovellettuna lausekkeisiin (11)–(14) kertoo, että

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

Yhtälön (15) perusteella $r_{n-1} \mid r_{n-2}$, joten $\text{syt}(r_{n-2}, r_{n-1}) = r_{n-1}$. Siten $d = r_{n-1}$. $\square$

Esimerkki 9.21. Lasketaan $\text{syt}(22, 60)$ ja etsitään sellaiset luvut $x, y \in \mathbb{Z}$, että $\text{syt}(a, b) = xa + yb$. Eukleideen algoritmilla saadaan

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

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

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

Harjoitustehtäviä.

Tehtävä 99. Olkoon K kokonaisalue ja olkoot $a \in K \setminus \{0\}$ ja $u, v \in K$. Osoita, että $u = v$, jos $au = av$.

Tehtävä 100. Olkoon K kokonaisalue. Osoita, että

- (1) $a \mid a$ kaikille $a \in \mathbb{Z}$
- (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 $a \mid b + c$.

Tehtävä 101. Osoita, että $\mathbb{Z}/q\mathbb{Z} = \langle a + q\mathbb{Z} \rangle$, jos ja vain jos $1 = \text{syt}(a, q)$.

Tehtävä 102. Määritä $\langle 30, 42, 70, 105 \rangle \leq (\mathbb{Z}, +)$.

Tehtävä 103. Olkoon $q \in \mathbb{N}$ ja olkoon $a \in \mathbb{Z} \setminus q\mathbb{Z}$. Osoita, että $a + \mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ on nollan jakaja, jos ja vain jos $\text{syt}(a, q) > 1$.

Tehtävä 104. Osoita, että alkulukuja on äärettömän monta.

Tehtävä 105. Määritä renkaiden $\mathbb{Z}/6\mathbb{Z}$ ja $\mathbb{Z}/10\mathbb{Z}$ ja $\mathbb{Z}/101\mathbb{Z}$ yksiköt.

¹⁰⁴Vihje: Olkoot $p_1, p_2, \dots, p_n$ alkulukuja. Mitä voit päätellä luvusta $p_1 p_2 \cdots p_n + 1$?

Tehtävä 106. Määritä renkaan $\mathbb{Z}/9\mathbb{Z}$ yksiköt ja nollan jakajat. Onko renkaan $\mathbb{Z}/9\mathbb{Z}$ yksiköiden ryhmä syklinen?

Tehtävä 107. Määritä Eukleideen algoritmilla lukujen 1059 ja 675 suurin yhteinen tekijä.

10. POLYNOMIT

Tässä luvussa tarkastelemme polynomien muodostamia renkaita ja polynomien jaollisuutta käsitteleviä perustuloksia. Algebrassa on tapana pitää erillään polynomin ja polynomifunktion käsitteet. Ennen näiden käsitteiden määrittelyä teemme 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 merkinä.

Määritelmä 10.1. Olkoon R kommutatiivinen rengas, jossa on vähintään kaksi alkia. Olkoon $n \in \mathbb{N}$, ja olkoot $a_n, a_{n-1}, \dots, a_1, a_0 \in R$. Lauseke

$$P(X) = \sum_{k=0}^n a_k X^k = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

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

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

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

ja

$$(16) \quad P(X)Q(X) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) X^k.$$

Polynomien yhteen- ja kertolasku määritellään siis kuten tavallista ja on helppo nähdä, että ne ovat laskutoimituksia.

Propositio 10.2. *Olkoon R kommutatiivinen rengas, jossa on vähintään kaksi alkia. Joukko $R[X]$ varustettuna polynomien yhteen- ja vähennyslaskulla on kommutatiivinen rengas. Kuvaus $i: R \rightarrow R[X]$, joka kuvaa renkaan R alkion a polynomiksi $a \in R[X]$, on injektiivinen rengashomomorfismi.*

Todistus. Selvästi polynomit 0 ja 1 ovat yhteenlaskun ja kertolaskun neutraalialkiot. Muut ominaisuudet seuraavat suoraviivaisesti siitä, että R on rengas. $\square$

Polynomirenkaat ovat tärkeitä kommutatiivisia renkaita, havainnollistamme niiden merkitystä hieman kurssin viimeisessä luvussa, kun sovellamme niitä äärellisten kuntien konstruktiossa. Rengas R voidaan ajatella Proposition 10.2 kuvauksen i avulla polynomirenkaan $R[X]$ alirenkaaksi.

Vähemmän havainnollinen Määritelmän 10.1 kanssa ekvivalentti tapa määritellä polynomit on korvata polynomin lauseke $\sum_{k=0}^n a_k X^k$ kertoimien muodostamalla jonolla $(a_0, a_1, \dots, a_n, 0, 0, \dots)$ ja määritellä yhteenlasku kuten jonoille on tapana ja kertolasku kaavan (16) mukaisesti. Tällöin jono $(0, 1, 0, 0, 0, \dots)$ on symbolin X vastine.

Määritelmä 10.3. Olkoon R kommutatiivinen rengas. Polynomin

$$P(X) = \sum_{k=0}^n a_k X^k \in R[X]$$

määrittää *polynomifunktio* on $P: R \rightarrow R$, $x \mapsto \sum_{k=0}^n a_k x^k = P(x)$.

Propositio 10.4. *Kuvaus, joka liittää R -kertoimiseen polynomiin $P(X)$ polynomi-funktion $P: R \rightarrow R$, on rengashomomorfismi polynomirenkaasta $R[X]$ funktioren-kaaseen $\mathcal{F}(X, R)$.*

Todistus. Harjoitustehtävä 108.

Esimerkki 10.5. Joillakin renkailla R kaksi polynomirenkaan $R[X]$ eri polynomia voi määrätä saman polynomifunktion: 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.

Esimerkki 10.6. Olkoot $P(X), Q(X) \in \mathbb{Z}[X]$.

$$P(X) = 2X^2 + 2, \quad Q(X) = 1 + 2X.$$

Tällöin

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

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

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 aina kongruenssi-luokaksi $a_k + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$, niin

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

Edelleen pätee $\deg(P(X)) = 2$, $\deg(Q(X)) = 1$ mutta nyt

$$\deg(P(X)Q(X)) = 2 < 3 = 2 + 1.$$

Esimerkin 10.6 tulos yleistyy kaikille polynomirenkaille:

Lemma 10.7. *Olkoon R kommutatiivinen rengas, $R \neq \{0\}$. Tällöin*

$$\deg(P(X)Q(X)) \leq \deg P(X) + \deg Q(X)$$

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

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. $\square$

Propositio 10.8. Jos K on kokonaisalue, niin $K[X]$ on kokonaisalue. Tällöin

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

Todistus. Lemman 10.7 merkinnöillä tulopolynomin korkeimman asteen termin kerroin on $a_nb_m \neq 0$, sillä K on kokonaisalue. $\square$

Esimerkki 10.9. Polynomi $2X$ on nollan jakaja renkaassa $(\mathbb{Z}/4\mathbb{Z})[X]$:

$$(2X)(2X) = 4X^2 = 0.$$

Nyt siis

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

Polynomirengas ei ole koskaan kunta. Jos K on kokonaisalue, niin Proposition 10.8 mukaan ainoat polynomit, joilla on käänteisalkio kertolaskun suhteen ovat vakiopolynomit u , missä $u \in K^\times$. Sen sijaan, jos kerroinrenkas ei ole kokonaisalue, niin vakiopolynomeilla a , missä a on nollan jakaja renkaassa K , ei ole käänteisalkiota. Nyt kuitenkin joillakin korkeamman asteen polynomeilla on käänteisalkiot.

Esimerkki 10.10. Renkaassa $(\mathbb{Z}/4\mathbb{Z})[X]$ pätee

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

Samalla lausekkeella annettujen polynomien jaollisuus riippuu tarkasteltavasta polynomirenkaasta:

Esimerkki 10.11. (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) $(X + 1) \nmid (X^2 + 1)$ renkaassa $\mathbb{C}[X]$: Jos $(X + 1) \mid (X^2 + 1)$, niin on $A, B \in \mathbb{C}$, joille $(X + 1)(AX + B) = X^2 + 1$. Tällöin toisen ja nollannen asteen kertoimia tarkastelemalla havaitaan, että pitää olla $A = 1 = B$, mutta ensimmäisen asteen termit eivät täsmää.

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

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

Todistamme seuraavaksi vastaavan tuloksen polynomeille:

Lause 10.12 (Jakoyhtälö). *Olkoon R kommutatiivinen rengas, jossa on vähintään kaksi alkiota. Olkoot $A(X), B(X) \in R[X]$ siten, että $B(X) \neq 0$ ja polynomin $B(X)$ korkeimman asteen termin kerroin on yksikkö. Tällöin on yksikäsitteiset $Q(X), J(X) \in R[X]$, joille*

$$A(X) = Q(X)B(X) + J(X)$$

ja $\deg J(X) < \deg B(X)$.

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

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

Selvästi $S \neq \emptyset$. Koska $B(X) \nmid A(X)$, niin $0 \notin S$, joten

$$t = \min\{\deg P(X) : P(X) \in S\} \geq 0.$$

Olkoon $Q(X) \in R[X]$ polynomi, jolle pätee $\deg(A(X) - Q(X)B(X)) = t$. Olkoon

$$J(X) = A(X) - Q(X)B(X) = a_t X^t + \cdots + a_0.$$

Osoitamme, että $t < d = \deg B(X)$. Olkoon b_d polynomin $B[X]$ korkeimman asteen kerroin. Jos olisi $t \geq d$, niin

$$J(X) - a_t b_d^{-1} X^{t-d} B(X) = A(X) - (Q(X) + a_t b_d^{-1} X^{t-d}) B(X) \in S$$

ja $\deg(J(X) - a_t b_d^{-1} X^{t-d} B(X)) < t$, mutta tämä on mahdotonta, koska polynomin $J(X)$ aste on minimaalinen.

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

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

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

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

Siis $\tilde{Q}(X) = Q(X)$ ja $\tilde{J}(X) = J(X)$. $\square$

Seuraus 10.13 (Jakoyhtälö). *Olkoon K kunta. Olkoot $A(X), B(X) \in K[X]$ siten, että $B(X) \neq 0$. Tällöin on yksikäsitteiset $Q(X), J(X) \in R[X]$, joille*

$$A(X) = Q(X)B(X) + J(X)$$

ja $\deg J(X) < \deg B(X)$. $\square$

Esimerkki 10.14. Jakoyhtälö voidaan toteuttaa algoritmisesti jakokulman avulla kuten kokonaisluvuillekin. Tällöin esimerkiksi polynomeille $A(X) = 2X^3 + X^2 - X - 1$ ja $B(X) = X^2 - 2$ renkaassa $\mathbb{Z}[X]$ jakokulma antaa

$$\begin{array}{r} 2X \quad +1 \\ X^2 - 2 \overline{) \begin{array}{rrrr} 2X^3 & +X^2 & -X & -1 \\ \mp 2X^3 & & & \\ \hline & X^2 & +3X & -1 \\ & X^2 & & +2 \\ \hline & & 3X & +1 \end{array}} \end{array}.$$

Toisin sanoen

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

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

$$(17) \quad 2X^3 + X^2 - X - 1 = (2X + 1)(X^2 - 2) + 1 = (2X + 1)(X^2 + 1) + 1.$$

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

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

josta ei voi jatkaa. Sen sijaan renkaassa $(\mathbb{Z}/3\mathbb{Z})[X]$ voidaan jatkaa, koska $\mathbb{Z}/3\mathbb{Z}$ on kunta. Nyt

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

ja päädytään yhtälöön (17). Renkaassa $\mathbb{Q}[X]$ jakoa voi myös jatkaa, ja saadaan

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

Polynomien jaollisuutta tutkittaessa on usein hyödyllistä tarkastella polynomien juuria (tai niitä vastaavien polynomifunktioiden nollakohtia).

Määritelmä 10.15. Olkoon R kommutatiivinen rengas, ja olkoon $P(X) \in R[X]$. Alkio $c \in R$ on polynomin $P(X)$ *juuri*, jos $P(c) = 0$.

Jakoyhtälö antaa seuraavan perustuloksen:

Propositio 10.16. *Olkoon R kommutatiivinen rengas. Olkoon $P(X) \in R[X]$, ja $c \in R$. Tällöin $P(c) = 0$, jos ja vain jos $(X - c) \mid P(X)$.*

Todistus. Oletetaan, että $P(c) = 0$. Jakoyhtälön mukaan on R -kertoimiset polynomit $Q(X)$ ja $J(X)$, joille $\deg J(X) < 1$ ja $A(X) = Q(X)(X - c) + J(X)$. Koska $\deg J < 1$, $J(X)$ on vakiopolynomi, joten on $b \in R$, jolle $J(a) = b$ kaikilla $a \in R$. Erityisesti

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

joten $b = 0$.

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

$$P(c) = (c - c)Q(c) = 0. \quad \square$$

Propositio 10.17. *Olkoon K kokonaisalue. Olkoon $P(X) \in K[X]$ polynomi, ja olkoot $c_1, c_2, \dots, c_k \in K$ polynomin $P(X)$ k eri juurta. Tällöin on $Q(X) \in K[X]$, jolle*

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

Todistus. Harjoitustehtävä 111. $\square$

Lause 10.18. *Olkoon K kokonaisalue, ja olkoon $n \geq 1$. Jos $P(X) \in K[X]$ ja $\deg P(X) = n$, niin polynomilla $P(X)$ on korkeintaan n juurta.*

Todistus. Propositioiden 10.17 ja 10.8 mukaan, jos polynomilla $P(X)$ on k juurta, niin $\deg(P(X)) \geq k$. $\square$

Erityisesti siis Propositio 2.9 antaa kaikki toisen asteen kompleksikertoimisen polynomiyhtälön ratkaisut.

Seuraus 10.19. *Olkoot $a_0, a_1 \in \mathbb{C}$. Yhtälön*

$$z^2 + a_1 z + a_0 = 0$$

ratkaisut ovat

$$z_1 = -\frac{a_1}{2} + \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0} \quad \text{ja} \quad z_2 = -\frac{a_1}{2} - \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}.$$

Propositio 10.20. *Olkoon K ääretön kokonaisalue. Tällöin jokaista kokonaisalueen K polynomifunktiota vastaa yksikäsitteinen polynomi renkaassa $K[X]$.*

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

Seuraus 10.21. *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 $P: K \rightarrow K$, on injektio.*

Määritelmä 10.22. Kunta K on *algebrallisesti suljettu*, jos jokaisella vakioista poikkeavalla polynomilla $P(X) \in K[X]$ on juuri.

Seuraus 10.23. *Jos K algebrallisesti suljettu kunta, niin jokainen vakioista poikkeava polynomi $P(X) \in K[X]$ on ensimmäisen asteen polynomien tulo.* $\square$

Polynomin $P(X) \in R[X]$ sanotaan olevan *jaoton* jos ei ole polynomeja $S(X) \in R[X]$ ja $T(X) \in R[X]$, joille $P(X) = S(X)T(X)$ ja $\deg S(X), \deg T(X) < \deg P(X)$. Seurauksen 10.23 mukaan, jos K on algebrallisesti suljettu kunta, niin mikään vähintään toisen asteen polynomi ei ole jaoton. Toisaalta kaikki ensimmäisen asteen polynomit ovat jaottomia Proposition 10.8 nojalla.

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

Seuraus 10.24. *Jos K algebrallisesti suljettu kunta, niin jokaisella nollasta poikkeavalla polynomilla $P(X) \in K[X]$ on juurten kertaluku huomioiden $\deg P(X)$ juurta.* $\square$

Lukualueiden ja kompleksianalyysin kursseilla todistetaan seuraava tärkeä tulos:

Lause 10.25 (Algebran peruslause). *Kompleksilukujen kunta on algebrallisesti suljettu.* $\square$

Seuraus 10.26. *Jokainen vakioista 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.* $\square$

Esimerkki 10.27. (a) Usein polynomeilla on vähemmän juuria kuin niiden asteesta tuleva maksimimäärä. Esimerkiksi polynomilla $X^3 + X \in \mathbb{R}[X]$ on täsmälleen yksi juuri ja polynomilla $X^2 + 1 \in \mathbb{R}[X]$ ei ole juuria lainkaan.

(b) Polynomi $X^2 + 1$ on jaoton renkaissa $\mathbb{Z}[X]$ ja $\mathbb{R}[X]$ mutta kompleksikertoimisten polynomien renkaassa $\mathbb{C}[X]$ pätee $X^2 + 1 = (X + i)(X - i)$.

(c) Polynomi $X^2 + X + 1$ on jaoton $\mathbb{Z}/2\mathbb{Z}$ -kertoimisten polynomien renkaassa 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 on selvä tapaus, samoin $X^2 + X = X(X + 1)$. Lisäksi $X^2 + 1 = (X + 1)^2$.

Harjoitustehtäviä.

Tehtävä 108. Osoita, että kuvaus, joka liittää polynomiin $P(X) \in R[X]$ vastaavan polynomifunktion $P \in \mathcal{F}(X, X)$, on rengashomomorfismi.

Tehtävä 109. Osoita, että $F(X) = 1 - 2X$ on yksikkö renkaassa $(\mathbb{Z}/16\mathbb{Z})[X]$.

Tehtävä 110. Olkoon p alkuluku. Montako juurta polynomilla $X^p - X \in (\mathbb{Z}/p\mathbb{Z})[X]$ on?

Tehtävä 111. Olkoon K kokonaisalue. Olkoon $P(X) \in K[X]$ polynomi, ja olkoot $c_1, c_2, \dots, c_k \in K$ polynomin $P(X)$ juuria. Osoita, että on $Q(X) \in K[X]$, jolle

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

Tehtävä 112. Olkoot $P(X), Q(X) \in (\mathbb{Z}/8\mathbb{Z})[X]$,

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

ja

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

(1) Kerro $Q(X)$ polynomilla $P(X)$.

(2) Jaa $Q(X)$ polynomilla $P(X)$.

Tehtävä 113. Olkoon K kunta. Osoita, että toisen tai kolmannen asteen polynomi $P(X) \in K[X]$ on jaoton, jos ja vain jos sillä ei ole juurta kokonaisalueessa K . Anna esimerkki, joka osoittaa, että väite ei päde neljännen asteen polynomeille.

Tehtävä 114. (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?

Tehtävä 115. 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 $(\mathbb{Z}/7\mathbb{Z})[X]$.

¹⁰⁹Vihje: Kerroinrengas $\mathbb{Z}/16\mathbb{Z}$ ei ole kokonaisalue.

¹¹⁰Vihje: Käytä ryhmäteoriaa!

11. IDEAALIT JA TEKIJÄRENKAAT

Rengashomomorfismi $\phi: R \rightarrow R'$ on erityisesti ryhmähomomorfismi $\phi: (R, +) \rightarrow (R', +)$ additiivisten ryhmien välillä. Rengashomomorfismin ydin määritellään tämän ryhmähomomorfismin ϕ ytimen avulla:

Määritelmä 11.1. Rengashomomorfismin $\psi: R \rightarrow R'$ ydin on

$$\ker \psi = \psi^{-1}(0) = \{x \in R : \psi(x) = 0\}.$$

Proposition 5.6 nojalla ryhmähomomorfismin $\phi: G \rightarrow G'$ ydin on ryhmän G normaali aliryhmä, joten rengashomomorfismin ψ ydin on additiivisen ryhmän $(R, +)$ normaali aliryhmä. Kertolaskun suhteen homomorfinisuus antaa ytimelle lisää rakennetta, jota tarkastelemme seuraavaksi.

Määritelmä 11.2. Olkoon R rengas ja olkoon $\mathcal{I} \subset R$ siten, että $(\mathcal{I}, +)$ on ryhmän $(R, +)$ aliryhmä.

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

Jos R on kommutatiivinen rengas, niin Määritelmän 11.2 kohdissa (1)–(3) määritellyt käsitteet ovat kaikki samoja. Tällöin käytetään yleensä yksinkertaisempaa terminologiaa ja sanotaan, että $\mathcal{I}$ on *ideaali*.

Lemma 11.3. (1) $\mathcal{I}$ on vasen ideaali, jos ja vain jos $xa + x'a' \in \mathcal{I}$ kaikilla $x, x' \in R$ ja $a, a' \in \mathcal{I}$.

(2) $\mathcal{I}$ on oikea ideaali, jos ja vain jos $ay + a'y' \in \mathcal{I}$ kaikilla $y, y' \in R$ ja $a, a' \in \mathcal{I}$.

(3) $\mathcal{I}$ on kaksipuolinen ideaali, jos ja vain jos se on vasen ideaali ja oikea ideaali.

Todistus. Harjoitustehtävä 116. □

Esimerkki 11.4. (a) R ja $\{0\}$ ovat renkaan R kaksipuolisia ideaaleja.

(b) $q\mathbb{Z}$ on renkaan $\mathbb{Z}$ ideaali jokaisella $q \in \mathbb{Z}$.

(c) Olkoot $\Omega \neq \emptyset$, $\emptyset \neq A \subset \Omega$, ja R rengas. Olkoon

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

Tällöin $N(A)$ on funktio renkaan $\mathcal{F}(\Omega, R)$ kaksipuolinen ideaali. Jos nimittäin $g_1, g_2 \in \mathcal{F}(\Omega, R)$ ja $h_1, h_2 \in N(A)$ ja $a \in A$, niin

$$(g_1 h_1)(a) = g_1(a) h_1(a) = g_1(a) \cdot 0 = 0,$$

joten $gh \in N(A)$. Vastaavasti nähdään, että $g_2 h_2 \in N(A)$, joten

$$(g_1 h_1 + g_2 h_2)(a) = 0.$$

Siis $g_1 h_1 + g_2 h_2 \in N(A)$, joten $N(A)$ on vasen ideaali. Samalla tavalla tarkastetaan, että $N(A)$ on oikea ideaali, joten se on kaksipuolinen ideaali.

Sama konstruktio antaa kaksipuolisia ideaaleja monille renkaan $\mathcal{F}(\Omega, R)$ alirenkailla, esimerkiksi

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

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

Propositio 11.5. Olkoon $\phi: R \rightarrow S$ rengashomomorfismi. Tällöin

(1) Jos $\mathcal{I} \subset R$ on vasen (vastaavasti oikea tai kaksipuolinen) ideaali, niin $\phi(\mathcal{I})$ on renkaan $\phi(S)$ vasen (vastaavasti oikea tai kaksipuolinen) ideaali.

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

Todistus. (1) Harjoitustehtävä 117.

(2) Tarkastelemme vain tapausta, jossa $\mathcal{I}$ on vasen ideaali, oikean ideaalin tapaus todistetaan samalla tavalla ja kaksipuolista ideaalia koskeva väite seuraa yhdistämällä nämä kaksi tulosta. Proposition 5.6 nojalla $(\phi^{-1}(\mathcal{I}), +) \leq (R, +)$. Olkoot $a \in \phi^{-1}(\mathcal{I})$ ja $r \in R$. Tällöin $\phi(ra) = \phi(r)\phi(a) \in \mathcal{I}$, koska $\phi(a) \in \mathcal{I}$ ja $\mathcal{I}$ on vasen ideaali. Siis $ra \in \phi^{-1}(\mathcal{I})$. $\square$

Seuraus 11.6. *Rengashomomorfismin ydin on määrittelyrenkaansa kaksipuolinen ideaali.*

Todistus. Väite seuraa Propositioista 11.5(2) koska $\{0\}$ on kaksipuolinen ideaali. $\square$

Esimerkki 11.7. Luonnollinen kuvaus $\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ on surjektiivinen rengashomomorfismi, joten renkaan $\mathbb{Z}/q\mathbb{Z}$ ideaalit ovat täsmälleen renkaan $\mathbb{Z}$ ideaalien kuvat luonnollisissa homomorfismissa. Erityisesti jokainen renkaan $\mathbb{Z}/q\mathbb{Z}$ aliryhmä on jonkin ideaalin additiivinen ryhmä.

Propositio 11.8. *Jos renkaan R vasen, oikea tai kaksipuolinen ideaali $\mathcal{I}$ on alirenkas, niin $\mathcal{I} = R$.*

Todistus. Tarkastelemme ainoastaan vasempia ideaaleja. Oikeat ideaalit tarkastellaan samalla tavalla. Jos $\mathcal{I}$ on renkaan R vasen ideaali ja $1 = 1_R \in \mathcal{I}$, niin kaikilla $x \in R$ pätee $x = x1 \in \mathcal{I}$, joten $\mathcal{I} = R$. $\square$

Propositio 11.9. *Olko R jakorengas, ja olko $\mathcal{I}$ sen vasen, oikea tai kaksipuolinen ideaali. Silloin $\mathcal{I} = R$ tai $\mathcal{I} = \{0\}$. Erityisesti, jos R on kunta, niin sen ainoat ideaalit ovat $\{0\}$ ja R .*

Todistus. Jos $a \in R^\times$, niin sillä on käänteisalkio a^{-1} . Jos $\mathcal{I}$ on vasen ideaali, jolle $a \in \mathcal{I}$, niin $1 = a^{-1}a \in \mathcal{I}$. Väite seuraa Propositioista 11.8. $\square$

Kaksipuolinen ideaali vastaa Proposition 11.5 mukaan rengasteoriassa ryhmäteorian normaalia aliryhmää. Renkaan additiivinen ryhmä on kommutatiivinen, joten ideaali ajateltuna kommutatiivisena additiivisena ryhmänä on siis renkaan additiivisen ryhmän normaali aliryhmä. Käyttämällä samaa ekvivalenssirelaatiota kuin luvussa 4 muodostamme renkaan R ideaalia $\mathcal{I}$ vastaavan tekijäjoukon $R/\mathcal{I}$. Seuraavan tuloksen mukaan tämä tekijäjoukko voidaan varustaa kahdella laskutoimituksella.

Propositio 11.10. *Olko R rengas ja olko $I \subset R$ kaksipuolinen ideaali. Renkaan R yhteenlasku ja kertolasku ovat yhteensopivia ideaalin 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 $a - a' \in \mathcal{I}$ ja $b - b' \in \mathcal{I}$, joten

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

koska $\mathcal{I}$ on kaksipuolinen ideaali. $\square$

Propositio 11.10 mukaan renkaan R molemmat laskutoimitukset määrittelevät tekijälaskutoimituksen tekijäjoukossa $R/\mathcal{I}$. Ideaalia $\mathcal{I}$ vastaaville sivuluokille käytetään additiivista merkintää $x + I$, jolloin laskutoimitukset ovat siis

$$(x + I) + (y + I) = (x + y) + I$$

ja

$$(x + I)(y + I) = xy + I$$

kaikille $x, y \in R$.

Propositio 11.11. *Olkoon R rengas, ja olkoon $\mathcal{I}$ sen kaksipuolinen ideaali. Tällöin tekijäjoukko $R/\mathcal{I}$ on rengas.*

Todistus. Harjoitustehtävä 126. □

Esimerkki 11.12. Luvun $q \geq 2$ monikerrat muodostavat renkaan $\mathbb{Z}$ ideaalin $q\mathbb{Z}$. Tätä ideaalia vastaa tuttu tekijärengas $\mathbb{Z}/q\mathbb{Z}$.

Propositiot 3.7 ja 3.8 antavat seurauksena

Propositio 11.13. (1) *Tekijärengas on kommutatiivinen, jos alkuperäinen rengas on kommutatiivinen.*

(2) *Luonnollinen kuvaus $R \rightarrow R/\mathcal{I}$ on rengashomomorfismi.* □

Lause 11.14 (Renkaiden isomorfismilause). *Olkoon $\psi: R \rightarrow S$ rengashomomorfismi. Tällöin tekijärengas $R/\ker \psi$ on isomorfinen renkaan $\psi(R)$ kanssa.*

Todistus. Lause todistetaan kuten ryhmien isomorfismilause (Lause 7.23). Harjoitustehtävä 127. □

Esimerkki 11.15. (a) $R/R \cong \{0\}$, joten tekijärengas $R/\mathcal{I}$ voi olla kommutatiivinen vaikka R ei olisikaan. Toinen ääriesimerkki tekijärenkaasta on $R/\{0\} \cong R$.

(b) Olkoon R rengas, $\Omega \neq \emptyset$ ja $c \in \Omega$. Kuvaus $E_c: \mathcal{F}(\Omega, R) \rightarrow R$, $E_c(f) = f(c)$ on surjektiivinen rengashomomorfismi, jonka ydin on

$$N(a) = \{f \in \mathcal{F}(\Omega, R) : f(c) = 0\}.$$

Renkaiden isomorfismilauseen nojalla $\mathcal{F}(\Omega, R)/N(a)$ on rengasisomorfinen renkaan R kanssa.

(c) Reaaliluvut konstruoidaan kurssilla Lukualueet rationaalilukujen Cauchyn jonojen renkaan nollaan suppenevien jonojen ideaalia vastaavana tekijärenkaana.

Propositio 11.16. *Olkoot L ja M renkaan R vasempia (vastaavasti oikeita tai kaksipuolisia) ideaaleja. Tällöin niiden summa*

$$L + M = \{x_1 + x_2 : x_1 \in L, x_2 \in M\}$$

ja tulo

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

ovat renkaan R vasempia (vastaavasti oikeita tai kaksipuolisia) ideaaleja.

Todistus. Harjoitustehtävä 119. □

Propositio 11.17. *Olkoot $\mathcal{I}_i$, $i \in I$, renkaan R vasempia (vastaavasti oikeita tai kaksipuolisia) ideaaleja. Tällöin*

$$\bigcap_{i \in I} \mathcal{I}_i$$

on renkaan R vasen (vastaavasti oikea tai kaksipuolinen) ideaali.

Todistus. Harjoitustehtävä 124. □

Määritelmä 11.18. Jos $S \subset R$, $S \neq \emptyset$, niin joukon S virittämä vasen (vastaavasti oikea tai kaksipuolinen) ideaali on joukon S sisältävien (vastaavasti oikeiden tai kaksipuolisten) ideaalien leikkaus.

Lemma 11.19. *Olkoon R rengas. Äärellisen joukon $A = \{x_1, x_2, \dots, x_n\} \subset R$ virittämä vasen ideaali on*

$$RA = \left\{ \sum_{i=1}^n r_i x_i : r_1, r_2, \dots, r_n \in R \right\},$$

niiden virittämä oikea ideaali on

$$AR = \left\{ \sum_{i=1}^n x_i r_i : r_1, r_2, \dots, r_n \in R \right\}$$

ja niiden virittämä kaksipuolinen ideaali on

$$RAR = \left\{ \sum_{i=1}^n s_i x_i r_i : s_1, r_1, s_2 r_2, \dots, s_n, r_n \in R \right\}.$$

Todistus. Harjoitustehtävä 118. □

Erityisesti yhden alkion x virittämä vasen ideaali on $Rx = \{rx : r \in R\}$ ja sen virittämä oikea ideaali on xR . Jos rengas K on kommutatiivinen, niin $xK = Kx$ ja tätä ideaalia merkitään usein (x) ja sanotaan *pääideaaliksi*. Vastaavasti alkioiden $x_1, x_2, \dots, x_m$ virittämää ideaalia kommutatiivisessa renkaassa merkitään usein $(x_1, x_2, \dots, x_m)$. Kokonaisalue, jonka kaikki ideaalit ovat pääideaaleja on *pääideaalialue*.

Lause 11.20. Olkoon K kunta. Tällöin polynomirengas $K[X]$ on pääideaalialue.

Todistus. Olkoon $\mathcal{J}$ nollasta poikkeava ideaali renkaassa $K[X]$ ja olkoon $P_0(X) \in \mathcal{J} \setminus \{0\}$ polynomi, jolla on minimaalinen aste: $\deg P_0(X) \leq \deg P(X)$ kaikille $P(X) \in \mathcal{J} \setminus \{0\}$. Olkoon $A(X) \in \mathcal{J}$. Jakoyhtälön (Seuraus 10.13) mukaan on $Q(X), J(X) \in K[X]$, joille pätee

$$A(X) = Q(X)P_0(X) + J(X)$$

ja $\deg J(X) < \deg P_0(X)$. Erityisesti

$$J(X) = A(X) - Q(X)P_0(X) \in \mathcal{J}.$$

Koska $\deg P_0(X)$ on minimaalinen nollasta poikkeaville ideaalin $\mathcal{J}$ polynomeille, pätee $J(X) = 0$, joten $A(X) \in (P_0(X))$. □

Esimerkki 11.21. Olkoon $\psi: \mathbb{R}[X] \rightarrow \mathbb{C}$ kuvaus, joka määritellään asettamalla $\psi(Q(X)) = Q(i)$ kaikille $\mathbb{R}$ -kertoimisille polynomeille $Q(X)$. Tällöin ψ on surjektiivinen rengashomomorfismi, jonka ydin on jaottoman polynomin $X^2 + 1$ virittämä pääideaali $(X^2 + 1)$. Renkaiden isomorfismilauseen mukaan tekijärengas $\mathbb{R}[X]/(X^2 + 1)$ on rengasisomorfinen kompleksilukujen kunnan $\mathbb{C}$ kanssa.

Määritelmä 11.22. Olkoon K kunta. Jos polynomi $D(X) \in K[X]$ on polynomien $P(X), Q(X) \in K[X]$ yhteinen tekijä, joka on jaollinen jokaisella polynomien $P(X)$ ja $Q(X)$ yhteisellä tekijällä, niin $D(X)$ on polynomien $P(X)$ ja $Q(X)$ *suurin yhteinen tekijä*. Tällöin käytetään merkintää $D(X) = \text{syt}(P(X), Q(X))$.

Lause 11.23. Olkoon K kunta. Polynomeilla $P(X), Q(X) \in K[X]$ on *suurin yhteinen tekijä*. Jos $D(X) = \text{syt}(P(X), Q(X))$, niin on polynomit $R(X), S(X) \in K[X]$, joille pätee

$$(18) \quad D(X) = R(X)P(X) + S(X)Q(X).$$

Todistus. Harjoitustehtävä 129. □

Yhtälö (18) on polynomien *Bezout'n yhtälö*. Jos $u \in K$, $u \neq 0$, ja $D(X) = \text{syt}(P(X), Q(X))$, niin $uD(X) = \text{syt}(P(X), Q(X))$: Polynomi $uD(X)$ on polynomin $D(X)$ tekijä koska u on yksikkö. Siis $uD(X)$ on polynomien $P(X)$ ja $Q(X)$ yhteinen tekijä. Toisaalta $D(X) \mid uD(X)$, joten jokainen polynomien $P(X)$ ja $Q(X)$ yhteinen tekijä jakaa polynomin $uD(X)$. Jos polynomien $P(X)$ ja $Q(X)$ suurin yhteinen tekijä on nollannen asteen polynomi, pätee siis erityisesti $1 = \text{syt}(P(X), Q(X))$.

Lause 11.24. Olkoon K kunta ja olkoon $P(X) \in K[X]$ polynomi, jonka aste on d .

(1) Jos kunnassa K on q alkia, niin renkaassa $K[X]/(P(X))$ on q^d alkia.

(2) Jos $P[X]$ on jaoton, niin $K[X]/(P(X))$ on kunta.

Todistus. Käytämme todistuksessa merkintää $\mathcal{J} = (P(X))$.

(1) Kuntakertoimisten polynomien jakoyhtälön (Seuraus 10.13) nojalla jokaisella ekvivalenssiluokalla $Q(X) + (P(X)) \in K[X]/\mathcal{J}$ 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.

(2) Olkoon $\bar{Q}(X) \neq 0$ kuten kohdassa (1). Tällöin $P(X)$ ei ole polynomin $\bar{Q}(X)$ tekijä koska $\deg \bar{Q}(X) < \deg P(X)$. Toisaalta, jos $\bar{Q}(X) \mid P(X)$, niin $\bar{Q}(X)$ on vakio ja siis yksikkö koska oletimme, että $P(X)$ on jaoton. Siis $1 = \text{syt}(P(X), \bar{Q}(X))$ ja polynomien Bezout'n yhtälön mukaan on $R(X), S(X) \in K[X]$, joille pätee

$$1 = R(X)P(X) + S(X)\bar{Q}(X),$$

joten $S(X)\bar{Q}(X) \in 1 + \mathcal{J}$. Siis

$$(S(X) + \mathcal{J})(\bar{Q}(X) + \mathcal{J}) = 1 + \mathcal{J},$$

joten polynomin $\bar{Q}(X)$ luokka tekijärenkaassa $K[X]/\mathcal{J}$ on yksikkö. $\square$

Esimerkki 11.25. Polynomi $P(X) = X^2 + X + 1$ on jaoton toisen asteen polynomi polynomirenkaassa $(\mathbb{Z}/2\mathbb{Z})[X]$. Lauseen 11.24 nojalla $(\mathbb{Z}/2\mathbb{Z})[X]/(P[X])$ on neljän alkion kunta.

Ennen Esimerkkiä 11.25 olemme tavanneet äärellisistä kunnista ainoastaan kunnat $\mathbb{Z}/p\mathbb{Z}$, missä p on alkuluku, erityisesti siis näiden kuntien alkioiden lukumäärä on alkuluku. Esimerkin 11.25 tulos yleistyy kaikille alkulukupotensseille p^q . Emme kuitenkaan todista seuraavaa tulosta tällä kurssilla.

Lause 11.26. Jokaiselle luonnolliselle luvulle $q \geq 1$ ja alkuluvulle p on äärellinen kunta, jossa on p^q alkia. Toisaalta jokaisessa äärellisessä kunnassa on p^q alkia joillain tällaisilla p ja q . $\square$

Harjoitustehtäviä.

Tehtävä 116. Olkoon R rengas, ja olkoon $\mathcal{J} \subset R$. Osoita, että

(1) $\mathcal{J}$ on vasen ideaali, jos ja vain jos $xa + x'a' \in \mathcal{J}$ kaikilla $x, x' \in R$ ja $a, a' \in \mathcal{J}$.

(2) $\mathcal{J}$ on kaksipuolinen ideaali, jos ja vain jos se on vasen ideaali ja oikea ideaali.

Tehtävä 117. Olkoon $\psi : R \rightarrow S$ rengashomomorfismi. Olkoon $\mathcal{J}$ renkaan R vasen ideaali. Osoita, että $\psi(\mathcal{J})$ on renkaan $\psi(R)$ vasen ideaali.

Tehtävä 118. Olkoon R rengas. Olkoot $a_1, a_2, \dots, a_n \in R$. Osoita, että

$$\{x_1a_1 + x_2a_2 + \dots + x_na_n : x_1, x_2, \dots, x_n \in R\}$$

on renkaan R vasen ideaali.

Tehtävä 119. Olkoot L ja M renkaan R vasempia ideaaleja. Olkoot

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

ja

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

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

Tehtävä 120. Olkoon R rengas. Alkion $r \in R$ vasen annihilaattori on

$$\{a \in R : ar = 0\}.$$

Osoita, että vasen annihilaattori on vasen ideaali.

Tehtävä 121. Olkoon R kommutatiivinen rengas. Osoita, että renkaassa R pätee binomikaava

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

kaikille $a, b \in R$.

Tehtävä 122. Olkoon R kommutatiivinen rengas. Alkio $x \in R$ on *nilpotentti*, jos $x^n = 0$ jollain $n \in \mathbb{N}$. Osoita, että renkaan R nilpotentit alkioit muodostavat ideaalin.

Tehtävä 123. Sievennä lauseke $(a + b)^p$ kunnassa $\mathbb{Z}/p\mathbb{Z}$.

Tehtävä 124. Olkoot $\mathcal{I}_i$, $i \in I$ on renkaan R vasempia ideaaleja. Osoita, että $\bigcap_{i \in I} \mathcal{I}_i$ on renkaan R vasen ideaali.

Tehtävä 125. Olkoot L ja M renkaan R vasempia ideaaleja. Osoita, että $LM \subset L \cap M$, jos R on kommutatiivinen

Tehtävä 126. Olkoon R rengas, ja olkoon $\mathcal{I}$ sen kaksipuolinen ideaali. Osoita, että $R/\mathcal{I}$ on rengas.

Tehtävä 127. Todista renkaiden isomorfismilause.

Tehtävä 128. Olkoot K ja K' kuntia. Olkoon $\phi: K \rightarrow K'$ kuntahomomorfismi. Osoita, että ϕ on injektio.

Tehtävä 129. Olkoon K kunta. Osoita, että polynomeilla $P(X), Q(X) \in K[X]$ on suurin yhteinen tekijä. Jos $D(X) = \text{syt}(P(X), Q(X))$, osoita, että on polynomit $R(X), S(X) \in K[X]$, joille pätee

$$D(X) = R(X)P(X) + S(X)Q(X).$$

LUKEMISTA

Tämä kurssi antaa perustietoja algebrasta. Kiinnostunut lukija voi kurssin tietojen pohjalta tutustua algebraan laajemmin esimerkiksi seuraavan luettelon kirjojen avulla.

- (1) N. Bourbaki: Algebra I, Springer-Verlag, 1989
- (2) D. Dummit ja R. Foote: Abstract algebra, John Wiley & Sons, 2004.
- (3) R. Godement: Algebra, Hermann, 1968
- (4) A. Hillman ja G. Alexanderson : A first undergraduate course in abstract algebra, Wadsworth, 1983.

¹²²Vihje: Huomaa, että potenssi n voi riippua alkioista x . Käytä tehtävän 121 binomikaavaa.

¹²⁹Vihje: Tarkastele polynomien $P(X)$ ja $Q(X)$ virittämää ideaalia.

- (5) S. Lang: Undergraduate algebra, Springer-Verlag, 1987.
- (6) C. Pinter: A book of abstract algebra, Dover, 2010.