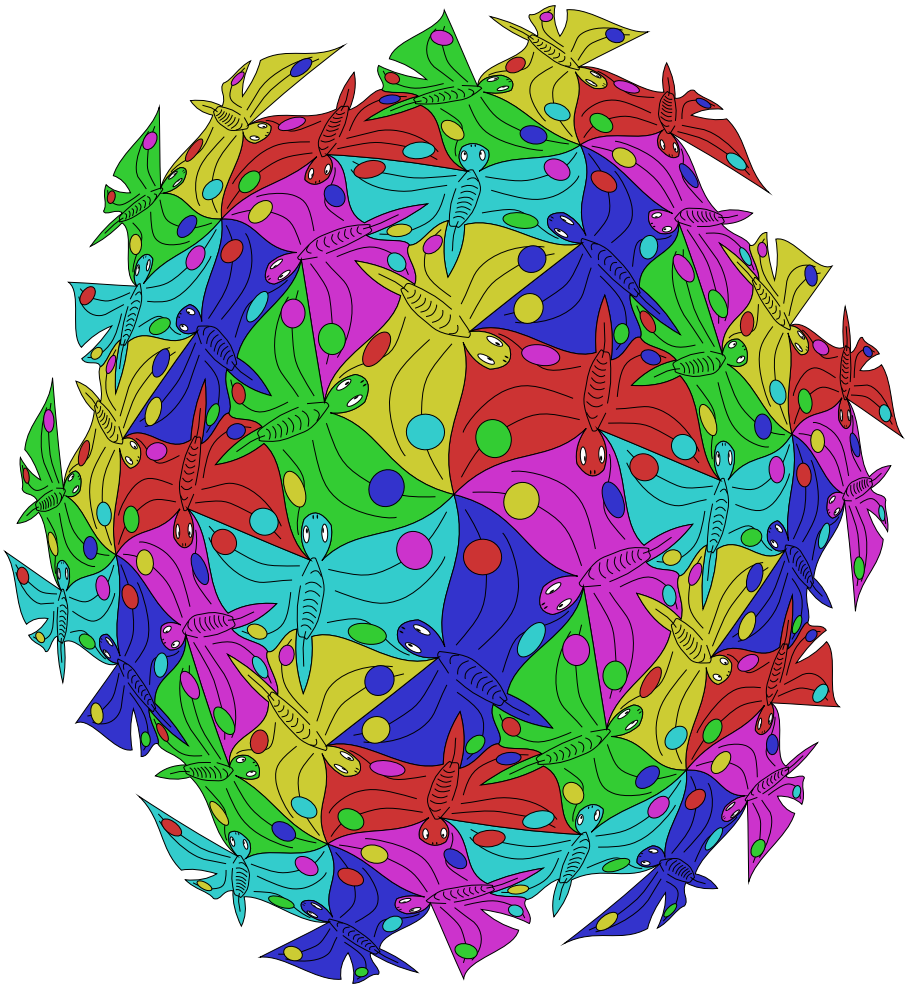
ALGEBRA

Tauno Metsänkylä — Marjatta Näätänen



2010

ALGEBRA

Tauno Metsänkylä – Marjatta Näätänen

Esipuhe

Tämä kirja on syntynyt toisen tekijän (T.M.) Turun yliopistossa pitämän kurssin pohjalta. Nykyisen muotonsa teksti on saanut monien parannusten ja lisäysten, osittain laajojenkin, jälkeen. Ansio niistä kuuluu suurelta osin toiselle tekijöistä (M.N.), mutta lisäksi niitä ovat tehneet lukuisat työtoverit, joille lausumme tässä kiitoksemme. Erityisesti haluamme kiittää Kari Astalaa, Iiro Honkalaa, Heikki Junnilaa, Juhani Karhumäkeä, Simo K. Kivelää ja Martti Nikusta.

Kirjan esityksen vaikeustaso vaihtelee. Kirjan alussa, ennen varsinaisen algebran alkua, on pitkähkö osa hyödyllisiä (osittain vähimmäistarpeet ylittäviäkin) pohjatietoja. Ensimmäisen algebrallisen struktuurin, ryhmän, määritelmää edeltää tavanmukaista laajempi valmistelu, jonka tarkoitus on helpottaa käsitteen omaksumista. Kirjan loppua kohti esitys voi tuntua vaikeammalta myös siksi, että sen ymmärtäminen vaatii siihen asti käsitellyn asian hallintaa. Vaikeuksien ilmetessä lukijan onkin syytä kerrata jo luettuja kohtia ja miettiä, onko jotain niissä jäänyt omaksumatta.

Kirjassa on runsaasti esimerkkejä ja harjoitustehtäviä. Kirjan lopussa oleviin tehtäviin on annettu myös ratkaisut. Lukijan olisi silti viisasta ratkaista nämäkin tehtävät itse ja vasta sen jälkeen katsoa annettua ratkaisua.

Matematiikkaan ei ole oikotietä, vaan osaaminen on rakennettava oman harjoittelun kautta. Usein opettavaisimpia ovat tehtävät, joiden ratkaisu ei heti onnistu. Ratkaisun pohtiminen, vaikka se ei johtaisikaan tulokseen, auttaa asian ymmärtämistä paljon paremmin kuin valmiin ratkaisun katsominen. Myös lauseiden todistuksia voi monissa tapauksissa ajatella ratkaistuina harjoitustehtävinä: niitäkin on siis hyvä miettiä itse ennen kirjassa esitetyn todistuksen lukemista.

Kirjan tähän laitokseen on pienten korjausten lisäksi tehty se muutos, että reaalilukujen aksiomaattinen määrittely, jota ei yleensä katsota algebran alaan kuuluvaksi, on siirretty varsinaisesta tekstiosasta liitteeksi. Mukaan on myös otettu uutena liitteenä lyhyt esittely p-adisista luvuista.

Turussa ja Helsingissä, maaliskuussa 2010

Tauno Metsänkylä Marjatta Näätänen

Sisältö

0. LOGIIKKAA

Tarkastelemalla puhekielen käyttöä väittelyssä ja päättelyssä voidaan todeta, että kieli on usein epämääräistä ja sitä voidaan tulkita eri tavoin. Puheen lisäinformaatio on äänenpainossa, eleissä yms., jotka voivat muuttaa sanotun merkitystä. Tätä lisäinformaatiota ei saa kirjoitetusta tekstistä. Pyrkimys luoda eksakti kieli liittyy logiikan kehittämiseen; kyseessä on formaalien päättelysääntöjen tekeminen. Myös puhekielessä käytetyt päättelysäännöt ovat intuitiivisia ja usein tiedostamattomia.

0.1 Propositiot ja kvanttorit

Propositiot

Formaalin logiikan peruselementti on *propositio* eli *lause*. Lauseita merkitään $A, B, C, ...$ Tällöin kiinnitetään huomio vain *totuusarvoon*; lause on joko *tosi* tai *epätosi* (mutta ei molempia yhtäaikaa eli kyseessä on ns. kaksiarvoinen logiikka). Ellei voida päättää onko lause tosi vai epätosi, ei se kelpaa lauseeksi. Merkitään lyhyesti $+$ (tosi) ja $-$ (epätosi).

Esimerkki 1. "2 on parillinen luku" on tosi.

Kuten kielessä, muodostetaan annetuista lauseista uusia.

1) *Negaatio* "ei", merkitään $\neg A$, lauseen A "vastakohta". Ei-sanan käytön perusteella on luonnollista vaatia, että jos lause A on tosi, on sen negaatio $\neg A$ epätosi ja kääntäen. Totuusarvo esiteltynä taulukon avulla:

A	$\neg A$
$+$	$-$
$-$	$+$

2) *Konjunktio* "ja", merkitään $A \wedge B$, on tosi vain kun sekä A että B ovat tosia:

A	B	$A \wedge B$
$+$	$+$	$+$
$+$	$-$	$-$
$-$	$+$	$-$
$-$	$-$	$-$

Esimerkki 2. $A =$ "3 on pariton luku" ja $B =$ "$2 + 2 = 5$". Tällöin $A \wedge B$ on epätosi.

3) *Disjunktio* "tai" merkitään $A \vee B$. Kielessä on kaksi tai-sanaa, poissulkeva "joko-tai" ja molemmat salliva "joko-tai- tai molemmat". Disjunktiolla on jälkimmäinen merkitys:

A	B	$A \vee B$
+	+	+
+	−	+
−	+	+
−	−	−

4) *Implikaatio* "jos A niin B" eli "A:sta seuraa B" merkitään $A \Rightarrow B$. Totuusarvon määrittelyssä aiheuttaa vaikeutta tapaus A epätosi. Sovitaan, että tällöin implikaatio on tosi. Jos A on tosi, on implikaatio tosi täsmälleen, kun B on tosi:

A	B	$A \Rightarrow B$
+	+	+
+	−	−
−	+	+
−	−	+

On huomattava, että tässä ei tarvitse olla syy-seuraus-suhdetta; $A \Rightarrow B$ saattaa olla tosi, vaikka lauseilla A ja B ei olisi minkäänlaista yhteyttä toisiinsa.

Esimerkki 3. $A =$ "Lauralla on punainen pusero" ja $B =$ "Kello on nyt 12".

5) *Ekvivalenssi* "A ja B yhtäpitävät" eli "A jos ja vain jos B", merkitään $A \Leftrightarrow B$. Tässä tapauksessa $A \Leftrightarrow B$ on tosi, jos A:lla ja B:llä on samat totuusarvot, ja epätosi, jos A:lla ja B:llä on eri totuusarvot:

A	B	$A \Leftrightarrow B$
+	+	+
+	−	−
−	+	−
−	−	+

Edellisiä taulukoita voidaan käyttää totuusarvojen määrittämiseen: jos tiedetään lauseiden A ja B totuusarvot, voidaan uusien lauseiden totuusarvot määrittää taulukkojen avulla.

Esimerkki 4. Tarkoittakoon V lausetta $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$. Tehdään totuusarvotaulu V:lle:

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$	V
+	+	−	−	+	+	+
+	−	−	+	−	−	+
−	+	+	−	+	+	+
−	−	+	+	+	+	+

Tulokseksi saadaan, että V on tosi riippumatta A:n ja B:n totuusarvoista. Tällaista lausetta sanotaan *tautologiaksi* tai *identtisesti todeksi*.

Eräät tautologiat muodostavat päättelysääntöjä, joita käytetään matemaattisissa todistuksissa. Seuraavan lauseen eri kohdat voidaan todistaa muodostamalla totuusarvotaulut.

Lause 1. *Olkoot p, q ja r lauseita. Seuraavat lauseet ovat identtisesti tosia:*

(1) $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$ (de Morganin laki),
(2) $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$ (de Morganin laki),
(3) $[p \wedge (q \vee r)] \Leftrightarrow [(p \wedge q) \vee (p \wedge r)]$ (osittelulaki),
(4) $[p \vee (q \wedge r)] \Leftrightarrow [(p \vee q) \wedge (p \vee r)]$ (osittelulaki),
(5) $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$ (implikaatio),
(6) $(p \Leftrightarrow q) \Leftrightarrow [(p \Rightarrow q) \wedge (q \Rightarrow p)]$ (ekvivalenssi),
(7) $[(p \Rightarrow q) \wedge (p \Rightarrow \neg q)] \Leftrightarrow \neg p$,
(8) $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$ (kontrapositio),
(9) $[p \wedge (p \Rightarrow q)] \Rightarrow q$,
(10) $[(p \Rightarrow q) \wedge \neg q] \Rightarrow \neg p$,
(11) $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$,
(12) $[(p \Leftrightarrow q) \wedge (q \Leftrightarrow r)] \Rightarrow (p \Leftrightarrow r)$.

Käytetään seuraavia nimityksiä:

Lauseessa $L \Rightarrow M$ on L *oletus* ja M *johtopäätös*. Jos $L \Rightarrow M$ on tosi, on "L tosi" *riittävä ehto* sille, että M on tosi, ja "M tosi" *välttämätön ehto* sille, että L on tosi.

Kvanttorit

Esimerkki 5. Jokainen rationaaliluku on reaaliluku. Luku 3 on rationaaliluku, joten 3 on reaaliluku.

Tähänastisella logiikalla ei voida muodollisesti päätellä, että lopputulos on oikea. Otetaan lisäksi käyttöön
– *universaalikvanttori*: "jokaisella x", "kaikilla x", merkitään $\forall x$;
– *olemassaolokvanttori*: "on olemassa x, jolla...", "jollakin alkiolla x", "ainakin yhdellä alkiolla x", merkitään $\exists x$.
Merkintä $A(x)$ tarkoittaa x:ää koskevaa väitettä, joka on tosi tai epätosi sen mukaan, mikä x on. Tätä sanotaan *yksipaikkaiseksi predikaatiksi* tai *yksipaikkaiseksi lausefunktioksi*.

Esimerkki 6. Olkoon $A(x)$ väite "$x > 2$". Jos muuttujalle x sijoitetaan arvo 1, saadaan epätosi lause, arvolla 3 saadaan tosi lause.

Olemassaolokvanttorista käytetään myös muotoa $\exists!x$: "on olemassa täsmälleen yksi x, jolla..."

Seuraavissa esimerkeissä x ja y ovat reaalilukuja:

ESIMERKKI 7.A. $\forall x\ (x^2 > x)$, "kaikilla reaaliluvuilla x pätee $x^2 > x$". Väite on epätosi. Epäyhtälö ei päde esimerkiksi arvolla $x = \frac{1}{2}$.

ESIMERKKI 7.B. $\exists x\ (x^2 > x)$, "on olemassa x, jolla $x^2 > x$". Tämä on tosi.

ESIMERKKI 7.C. $\exists!x\ (|x| \leq 0)$ "on olemassa täsmälleen yksi x, jolla $|x| \leq 0$". Tämäkin on tosi, sillä $x = 0$ on ainoa luku, jolla epäyhtälö on tosi.

ESIMERKKI 7.D. $\forall x\ \exists y\ (x^2 - y = y^2 - x)$ "jokaisella x on olemassa y, jolla $x^2 - y = y^2 - x$". Tosi, esim. $y = x$ kelpaa.

ESIMERKKI 7.E. $\exists y\ \forall x\ (x^2 - y = y^2 - x)$ "on olemassa sellainen luku y, että kaikilla luvuilla x on $x^2 - y = y^2 - x$". Sijoittamalla $x = 0$ nähdään, että välttämättä $y = 0$ tai $y = -1$. Mutta arvolla $x = 1$ ei kumpikaan näistä kelpaa. Väite on siis epätosi.

ESIMERKKI 7.F. 1. $\forall x\ A(x)$: "Jokaisella alkiolla x on $A(x)$ tosi".

2. $\exists x\ A(x)$: "On olemassa x, jolla $A(x)$ on tosi".

3. $\forall x\ \neg A(x)$: "Millään alkiolla x ei $A(x)$ ole tosi" eli "kaikilla alkioilla x on $A(x)$ epätosi".

4. $\exists x\ \neg A(x)$: "On olemassa x, jolla $A(x)$ on epätosi".

Totea, että 1 ja 4 ovat toistensa negaatioita, samoin 2 ja 3.

Jos negaatio ja kvanttori (tai kaksi kvanttoria, ks. esim. 7.D., 7.E.) ovat samassa väitteessä, on järjestys tärkeä. Seuraavissa esimerkeissä x tarkoittaa ihmistä ja $P(x)$ predikaattia "x on kuolevainen".

1. $\neg(\forall x\ P(x))$ voidaan lukea seuraavasti: "ei ole totta, että jokainen ihminen on kuolevainen" eli "on olemassa joku kuolematon ihminen"; tämä voidaan siis myös kirjoittaa $\exists x\ \neg P(x)$.
2. $\forall x\ \neg P(x)$ tarkoittaa "jokainen ihminen on kuolematon".

Merkitys siis muuttui, kun negaation ja kvanttorin järjestys vaihtui!

ESIMERKKI 8. $L(x, y)$ on kaksipaikkainen lausefunktio. Merkintä $\forall(x, y)\ L(x, y)$ luetaan "kaikilla alkioilla x ja y on voimassa $L(x, y)$". Merkintä $\forall x\ \exists y\ L(x, y)$ luetaan "kaikilla alkioilla x on olemassa ainakin yksi sellainen y, että $L(x, y)$ (on voimassa)". Merkintä $\exists y\ \forall x\ L(x, y)$ luetaan "on olemassa ainakin yksi sellainen y, että $L(x, y)$ (on voimassa) kaikilla alkioilla x".

HUOMAUTUS. Tavallisessa matematiikan kielenkäytössä jätetään merkintä $\forall x$ usein kirjoittamatta näkyviin. Esim. kirjoitettaessa $(x + 1)^2 = x^2 + 2x + 1$ (missä x ajatellaan reaaliluvuksi) tarkoitetaan itse asiassa, että $\forall x\ [(x + 1)^2 = x^2 + 2x + 1]$.

ESIMERKKI 9. Väitteen "funktiolla f on jokaisessa pisteessä ominaisuus A" negaatio: "on olemassa piste, jossa f:llä ei ole ominaisuutta A". Varo virhettä: "f:llä ei ole missään pisteessä ominaisuutta A".

Lause 2. *Seuraavat propositiot ovat tosia kaikilla predikaateilla $p(x)$ ja $q(x)$:*

$$\begin{aligned}
&\forall x\ [p(x) \wedge q(x)] \Leftrightarrow [\forall x\ p(x) \wedge \forall x\ q(x)],\\
&\exists x\ [p(x) \wedge q(x)] \Rightarrow [\exists x\ p(x) \wedge \exists x\ q(x)],\\
&\exists x\ [p(x) \vee q(x)] \Leftrightarrow [\exists x\ p(x) \vee \exists x\ q(x)],\\
&[\forall x\ p(x) \vee \forall x\ q(x)] \Rightarrow \forall x\ [p(x) \vee q(x)].
\end{aligned}$$

Jälkimmäiset kaksi propositiota saadaan edellisten avulla:

$$\begin{aligned}
&\exists x\ [p(x) \vee q(x)] \Leftrightarrow \neg\neg\exists x\ [p(x) \vee q(x)]\\
\Leftrightarrow&\neg\forall x\ \neg[p(x) \vee q(x)] \Leftrightarrow \neg\forall x\ [\neg p(x) \wedge \neg q(x)]\\
\Leftrightarrow&\neg[\forall x\ \neg p(x) \wedge \forall x\ \neg q(x)] \Leftrightarrow [\neg\forall x\ \neg p(x)] \vee [\neg\forall x\ \neg q(x)]\\
\Leftrightarrow&[\exists x\ \neg\neg p(x)] \vee [\exists x\neg\neg q(x)] \Leftrightarrow [\exists x\ p(x) \vee \exists x\ q(x)];
\end{aligned}$$

$$\begin{aligned}
&[\forall x\ p(x) \vee \forall x\ q(x)] \Leftrightarrow [\forall x\ \neg\neg p(x)] \vee [\forall x\ \neg\neg q(x)]\\
\Leftrightarrow&[\neg\exists x\ \neg p(x)] \vee [\neg\exists x\ \neg q(x)] \Leftrightarrow \neg[\exists x\ \neg p(x) \wedge \exists x\ \neg q(x)]\\
\Rightarrow&\neg\exists x[\neg p(x) \wedge \neg q(x)] \Leftrightarrow \neg\exists x\ \neg[p(x) \vee q(x)]\\
\Leftrightarrow&\neg\neg\forall x\ [p(x) \vee q(x)] \Leftrightarrow \forall x\ [p(x) \vee q(x)].
\end{aligned}$$

0.2 Matemaattisesta todistamisesta

Matematiikassa tarkastellaan abstrakteja *struktuureja*. Lähtökohdaksi otetaan aluksi määriteltävät käsitteet. Näillä *oletetaan* olevan joitakin perusominaisuuksia, jotka luetellaan *aksioomissa*. Aksiooma on siis lause, josta sovitaan, että se on tosi. Määritelmät ja aksioomat kiinnittävät tarkasteltavan struktuurin.

Aksioomien tulee olla *ristiriidattomia*: Ne eivät saa sisältää vastakkaisia vaatimuksia, mutta niiden tulee myös olla sellaisia, että niistä ei loogisilla päättelyillä voida johtaa ristiriitaisia lausumia. Aksioomien lukumäärä pyritään supistamaan mahdollisimman vähiin: niiden tulee olla *riippumattomia*, ts. mikään aksiooma ei saa olla osoitettavissa todeksi muiden perusteella. Aksiomaattisen lähestymistavan ideana on, että kaikki tarkasteltavan struktuurin ominaisuudet johdetaan aksioomista.

Myöhemmin tarkastellaan esimerkkinä luonnollisten lukujen aksiomaattista määrittelyä. Tämän jälkeen kehitetään ao. struktuuria koskevaa matemaattista teoriaa todistamalla sitä koskevia *lauseita* tosiksi aksioomista lähtien. Lause muodostuu *oletuksesta* p ja *väitöksestä* q; lauseen todistamisessa päätellään, että jos p on tosi, niin myös q on tosi.

Lauseen *suora todistaminen* vastaa tautologiaa

$$[p \wedge (p \Rightarrow q)] \Rightarrow q,$$

jolloin ajatuksena on, että jos p on tosi ja implikaatio $p \Rightarrow q$ voidaan päätellä todeksi, niin myös väitös q on tosi. Todistuksen olennainen sisältö muodostuu siis implikaation $p \Rightarrow q$ todistamisesta.

Koska $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$ on identtisesti tosi, on myös

$$[p \wedge (\neg q \Rightarrow \neg p)] \Rightarrow q$$

tautologia. Tämä sisältää *epäsuoran todistuksen* periaatteen: Jos oletus p on tosi ja voidaan osoittaa, että väitöksen negaatiosta $\neg q$ seuraa oletuksen negaatio $\neg p$, syntyy ristiriita, jos $\neg q$ on tosi. Sekä p että $\neg p$ eivät nimittäin voi molemmat olla tosia. Ainoa mahdollisuus on, että $\neg q$ ei ole tosi, ts. q on tosi.

Epäsuoran todistuksen olennainen sisältö muodostuu siis implikaation $\neg q \Rightarrow \neg p$ todistamisesta. Tällöin lähdetään tarkastelemaan väitöksen negaatiota $\neg q$, ns. *antiteesia* eli *vastaoletusta* ja tutkitaan, mitä tästä seuraa. Jos ajaudutaan ristiriitaan oletuksen (tai jonkin siitä johdetun lauseen) kanssa, ei antiteesi voi olla tosi, jolloin sen negaatio eli väitös on tosi.

Esimerkki 1. Luonnollista lukua sanotaan *täydelliseksi*, jos se on tekijöidensä summa. Tekijöihin ei lueta lukua itse. Täydellisiä lukuja ovat esimerkiksi $6 = 1 + 2 + 3$ ja $28 = 1 + 2 + 4 + 7 + 14$.

Epäsuorasti voidaan todistaa seuraava lause: Täydellinen luku ei ole alkuluku. Oletus p on tällöin "n on täydellinen luku" ja väitös q "n ei ole alkuluku". Antiteesi on "n on alkuluku".

Jos n on alkuluku, sillä on vain kaksi tekijää, 1 ja n. Tekijöiden summaan ei luvun täydellisyyttä tutkittaessa oteta lukua itse, joten summa $= 1$. Koska $n > 1$, ei n ole täydellinen luku.

Antiteesista on siis jouduttu ristiriitaan oletuksen kanssa; antiteesi on epätosi ja siis väitös on tosi.

Erityisesti on huomattava, että lausetta ei voida todistaa johtamalla väitöksestä oletus tai jokin muu tosi lause. Tämä on nähtävissä siitä, että propositiot $p \Rightarrow q$ ja $q \Rightarrow p$ eivät ole yhtäpitäviä, ts. $(p \Rightarrow q) \Leftrightarrow (q \Rightarrow p)$ ei ole tautologia. Esimerkiksi (sinänsä väärää) lausetta "n-kulmion kulmien summa on $n\frac{\pi}{3}$" ei voida perustella toteamalla, että arvolla $n = 3$ se antaa aivan oikean tuloksen.

Sen sijaan väitöksestä q lähteminen ja oletukseen tai muuhun toteen lauseeseen p päätyminen kelpaa todistukseksi, jos voidaan muodostaa ekvivalenssiketju

$$q \Leftrightarrow \ldots \Leftrightarrow p,$$

mutta tällöin onkin olennaista, että tämä ketju sisältää implikaatioketjun oikealta vasemmalle, so. päättelyn oletuksesta väitökseen.

Muotoa $\forall x\ p(x)$ olevan proposition toteaminen vääräksi on yleensä helpompaa kuin sen toteaminen oikeaksi. Vääräksi osoittamiseen riittää löytää yksi alkio x, jolla $p(x)$ on epätosi; tätä sanotaan *vastaesimerkiksi*. Jos sen sijaan propositio on todistettava oikeaksi, on periaatteessa tarkasteltava kaikkia mahdollisia alkioita.

Esimerkiksi edellä käsitelty lause "kaikkien n-kulmioiden kulmien summa saadaan kaavasta $n\pi/3$", voidaan osoittaa vääräksi toteamalla, että se ei päde neliöllä. Vastaavan oikean lauseen "kaikkien n-kulmioiden kulmien summa saadaan kaavasta $(n-2)\pi$" todistaminen oikeaksi on vaikeampaa.

Todettakoon lopuksi, että matemaattisten lauseiden todistamisessa ei yleensä noudateta formaalin logiikan menettelytapoja, vaan sovelletaan pikemminkin luonnollista intuitiivista logiikkaa. Loogiset symbolit on ymmärrettävä lähinnä lyhennysmerkintöinä. Joskus kuitenkin todistuksen looginen rakenne saattaa olla niin hankala, että sen hahmottaminen edellyttää formaalin logiikan käyttöä.

0.3 Joukko-opin merkintöjä

Matematiikan kielessä tärkeimpiä perusobjekteja ovat *joukot*, esimerkiksi lukujoukot, funktiojoukot, vektorijoukot. Olet varmasti jo koulussa tottunut seuraaviin lukujoukkojen merkintöihin:

$\mathbb{N} = \{0, 1, 2, ...\}$, *luonnolliset luvut*,

$\mathbb{Z}$ *kokonaisluvut*,

$\mathbb{Q}$ *rationaaliluvut*,

$\mathbb{R}$ *reaaliluvut*,

$\mathbb{C}$ *kompleksiluvut*.

Seuraavat käsitteet ja merkinnät ovat matemaatikon jokapäiväisiä työkaluja.

$x \in A$: x on joukon A alkio eli x kuuluu joukkoon A; vastakohta merkitään $x \notin A$;

$B \subset A$ (tai $B \subseteq A$): B on joukon A *osajoukko* eli B sisältyy joukkoon A;

$B \subsetneq A$: B on joukon A *aito osajoukko* (siis $B \subset A$, $B \neq A$);
$\{x, y, z, ...\}$: joukko jonka alkiot ovat $x, y, z, ...$;

$\{x \in A \mid P_1(x), ..., P_n(x)\}$ tai $\{x \mid P_1(x), ..., P_n(x)\}$: niiden (joukon A) alkioiden x joukko, jotka täyttävät ehdot $P_1(x), ..., P_n(x)$.

Esimerkki 1. (i) Jos A=$\{2, 4, 6, 8, 10\}$, niin esimerkiksi $6 \in A$, $7 \notin A$, $\{4, 8\} \subset A$ ja $\{4, 8\} \subsetneq A$.

(ii) Huomaa, että esimerkiksi $\{1,2\} = \{2,1\} = \{1,1,2\}$.

(iii) $\{x \in \mathbb{Z} \mid 0 < x < 5, \;\; x \text{ parillinen } \} = \{2,4\}$.

(iv) $\{x \in \mathbb{R} | a < x < b\}$ = avoin väli pisteestä a pisteeseen b, merkintä (a,b). (Joskus käytetään myös merkintää $]a,b[$.)

Jos A ja B ovat jonkin joukon M ("perusjoukon") osajoukkoja, niiden avulla määritellään lisää M:n osajoukkoja seuraavasti:

$$\textit{yhdiste (unioni)} \; A \cup B = \{x \in M \mid x \in A \text{ tai } x \in B\},$$

$$\textit{leikkaus} \; A \cap B = \{x \in M \mid x \in A \text{ ja } x \in B\},$$

$$\textit{erotus} \; A \setminus B = \{x \in M \mid x \in A \text{ ja } x \notin B\},$$

$$\textit{komplementti} \; A^c = M \setminus A.$$

Leikkaus ja unioni määritellään samalla tavalla myös useammalla kuin kahdella (jopa äärettömän monella) joukolla.

Joukkoa, jossa ei ole yhtään alkiota, sanotaan *tyhjäksi joukoksi.* Siitä käytetään merkintää $\emptyset$. Huomaa, että $\emptyset \subset A$, olipa A mikä hyvänsä joukko.

Esimerkki 2. (i) $A \setminus B = A \cap B^c$,

(ii) $\mathbb{Z} \setminus \;\mathbb{Q} = \emptyset$,

(iii) $\{(x,y) \in \mathbb{R}^2 | \; x = y\} \cap \{(x,y) \in \mathbb{R}^2 \mid x = -y\} = \{(0,0)\}$,

(iv) kaikkien suljettujen reaalilukuvälien $[n, n+1]$ unioni, missä $n = 0, \pm 1, \pm 2, ...$, on $= \mathbb{R}$.

Edelleen merkitään
– joukon A *potenssijoukko* $\mathcal{P}(A) = \{B \mid B \subset A\}$,
– joukkojen A ja B *karteesinen tulo*

$$A \times B = \{(x,y) \mid x \in A, \; y \in B\}.$$

Joukkoa $A \times A$ merkitään myös A^2.

Harjoitustehtäviä

1. Olkoon $\mathbb{N}$ luonnollisten lukujen $0, 1, 2, \ldots$ joukko. Ilmaisu $\forall x \in \mathbb{N}$ tarkoittaa "kaikilla luonnollisilla luvuilla x" ja $\exists x \in \mathbb{N}$ tarkoittaa "on olemassa luonnollinen luku x, jolla". Merkinnät $x + y$, $=$, $\leq$ ja $<$ ovat kuten koulukurssissa. Mitkä seuraavista väitteistä ovat tosia?
   a) $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\forall z \in \mathbb{N})(x + y = z \Rightarrow y + x = z)$,
   b) $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(x + y = 0)$,
   c) $(\exists y \in \mathbb{N})(\forall x \in \mathbb{N})(x + y = x)$.

2. a) $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(x \leq y)$,
   b) $(\exists y \in \mathbb{N})(\forall x \in \mathbb{N})(x \leq y)$,
   c) $(\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(x \leq y)$.

   Olkoot p, q ja r lauseita. Todista, että seuraavat lauseet ovat identtisesti tosia:

3. $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$ (de Morganin laki).

4. $[p \vee (q \wedge r)] \Leftrightarrow [(p \vee q) \wedge (p \vee r)]$ (osittelulaki).

5. $[(p \Leftrightarrow q) \wedge (q \Leftrightarrow r)] \Rightarrow (p \Leftrightarrow r)$.

6. Tarkoittakoon x miestä ja y naista sekä merkintä $f(x, y)$, että x ja y ovat avioliitossa keskenään. Esitä sanoilla seuraavat merkinnät:

$$\begin{aligned} &(\forall x)(\exists y) \quad f(x, y), \\ &(\exists y)(\forall x) \quad f(x, y). \end{aligned}$$

7. Osoita, että $\bigcup_{n=1}^{\infty} \{x \in \mathbb{R} \mid 0 < x < \frac{1}{n}\} = \{x \in \mathbb{R} \mid 0 < x < 1\}$.

8. Määritä ne parit $(a, b) \in \mathbb{R}^2$, joilla $\{x \in \mathbb{R} \mid x^2 - a^2 < 1 \ \wedge \ x^2 - b^2 > 4\} = \emptyset$.

9. Merkitään $a = \{\emptyset\}$, $b = \{\emptyset, a\}$ ja $A = \{a, b\}$. Mitkä seuraavista väitteistä ovat tosia?
   i) $a \in A$, ii) $a \subset A$, iii) $\{a\} \in A$,
   iv) $\{a\} \subset A$, v) $a \in b$, vi) $a \subset b$.

10. Näytä, että
$$\Big(\big\{\{a\}, \{a, b\}\big\} = \big\{\{c\}, \{c, d\}\big\}\Big) \Leftrightarrow (a = c \ \wedge \ b = d)$$
    kaikilla alkioilla a, b, c, d.

11. Osoita, että $\bigcap_{n=1}^{\infty} \{x \in \mathbb{R} \mid 0 < x < \frac{1}{n}\} = \emptyset$.

12. Muodostetaan joukkoperheestä $(A_i)_{i \in \mathbb{N}}$ joukkoperhe $(B_i)_{i \in \mathbb{N}}$ asettamalla $B_0 = A_0$, $B_{n+1} = A_{n+1} \setminus \bigcup_{i=0}^{n} A_i$. Osoita:

a) $B_i \cap B_j = \emptyset$, kun $i \neq j$.
b) $\bigcup_{i=0}^{\infty} A_i = \bigcup_{i=0}^{\infty} B_i$.

Seuraavassa A, B ja C ovat mielivaltaisia joukkoja. Todista:

13. $A \subset B \Leftrightarrow A \setminus B = \emptyset \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A$.

14. $A \subset B \subset A \Leftrightarrow A = B$.

15. $A \cup (A \cap B) = A = A \cap (A \cup B)$.

16. $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B) \Leftrightarrow (A \subset B \ \vee \ B \subset A)$.

17. $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

18. a) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap B \cap C) = (A \setminus B) \cup (A \cap C)$,
b) $(A \setminus B) \setminus C = A \setminus (B \cup C)$.

19. Merkitään $A_k = [\frac{-1}{k+1}, \frac{1}{k+1}] \times \mathbb{R}$ ja $B_k = \mathbb{R} \times [\frac{-1}{k+1}, \frac{1}{k+1}]$ kaikilla $k \in \mathbb{N}$. Näytä, että

$$\bigcap_{k \in \mathbb{N}} (A_k \cup B_k) = \{(x, y) \in \mathbb{R}^2 \mid xy = 0\}.$$

20. Todista de Morganin kaavat

$$(A \cup B)^c = A^c \cap B^c, \ (A \cap B)^c = A^c \cup B^c \ \text{ (ks. 0.1 Lause 1).}$$

I. LUKUTEORIAA

I.1 Kokonaislukujen tekijöihinjako

Seuraavassa tutkitaan kokonaislukujen joukkoa $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$.

Jos kokonaisluku a on jaollinen kokonaisluvulla b, ts. jos on olemassa $c \in \mathbb{Z}$, jolla $a = bc$, merkitään $b \mid a$. Käytetään myös sanontoja: *b jakaa a*:n, b on a:n *tekijä*, a on b:n *monikerta.* Vastakohta merkitään $b \nmid a$.

Siis esim. $2 \mid 8$, $3 \mid 15$, mutta $6 \nmid 21$.

Jaollisuudella on mm. seuraavat yksinkertaiset ominaisuudet (perustele ne!):

(i) $a \mid a \quad \forall\ a \in \mathbb{Z}$,

(ii) jos $a \mid b$ ja $b \mid a$, niin $a = \pm b$,

(iii) jos $a \mid b$ ja $b \mid c$, niin $a \mid c$,

(iv) jos $a \mid b$ ja $a \mid c$, niin $a \mid (b + c)$.

Kokonaislukua $p > 1$, jonka ainoat tekijät ovat ± 1 ja $\pm p$, sanotaan *alkuluvuksi* tai *jaottomaksi* luvuksi (engl. prime). Muita kokonaislukuja $n > 1$ sanotaan *yhdistetyiksi* (composite) luvuiksi. Tällaiset luvut voidaan siis aina hajottaa muotoon ("hajottaa tekijöihin")

$$n = n_1 n_2, \qquad 1 < n_1 < n, \quad 1 < n_2 < n.$$

Jatkamalla tässä tekijöiden n_1 ja n_2 hajottamista (jos mahdollista) saadaan lopuksi luvun n *alkutekijähajotelma*

$$n = p_1 p_2 \cdots p_s \qquad (p_1, \dots, p_s \text{ alkulukuja}). \tag{1}$$

Se voidaan kirjoittaa myös muodossa

$$n = q_1^{h_1} q_2^{h_2} \cdots q_r^{h_r} \qquad (q_1, \dots, q_r \text{ erisuuria alkulukuja},\ h_i \geq 1 \quad \forall\ i). \tag{2}$$

Myöhemmin todistetaan ns. aritmetiikan peruslause, jonka mukaan luvun n alkutekijähajotelma (1) on yksikäsitteinen, samoin siis (2). Jälkimmäistä sanotaan luvun n *kanoniseksi (alkutekijä)hajotelmaksi.*

Esimerkki 1. $700 = 2 \cdot 2 \cdot 5 \cdot 5 \cdot 7 = 2^2 \cdot 5^2 \cdot 7$.

Alkulukujen joukkoa merkitään $\mathbb{P}$:llä; siis

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \dots\}.$$

Lause 1 (Eukleides). *Alkulukuja on äärettömän monta.*

Todistus. Tehdään vastaoletus: $p_1, \ldots, p_r$ ovat kaikki alkuluvut. Muodostetaan luku $n = p_1 \cdots p_r + 1$. Koska $n > 1$, se voidaan hajottaa alkutekijöihin. Olkoon q jokin alkutekijöistä; silloin q on vastaoletuksen mukaan jokin p_i. Nyt q siis jakaa luvun $n - p_1 \cdots p_r$, ts. $q \mid 1$. Ristiriita! $\square$

Miten selvitetään, onko annettu (suuri) luku N alkuluku? Jos N ei ole alkuluku, miten löydetään sen tekijät? Nämä ovat klassisia kysymyksiä, jotka ovat nousseet uudestaan vilkkaan tutkimuksen kohteiksi. Lisäksi alkulukuihin liittyy paljon muita ratkaisemattomia probleemoja, joiden tutkimus on jatkuvasti käynnissä.

Alkeellinen menetelmä sen ratkaisemiseksi, onko annettu kokonaisluku a jaollinen toisella kokonaisluvulla b, on jaon suorittaminen jakokulmassa eli jakoalgoritmi:

Lause 2 (Jakoyhtälö). *Jos $a, b \in \mathbb{Z}$ ja $b \neq 0$, niin on olemassa sellaiset yksikäsitteiset luvut $q, r \in \mathbb{Z}$, että*

$$a = qb + r, \qquad 0 \leq r < |b|.$$

Todistus. Jos $b > 0$, valitaan joukosta $\{\, a - nb \mid n \in \mathbb{Z} \}$ *pienin* ei-negatiivinen luku $r = a - qb$ (mieti, miksi se on mahdollista). Silloin $r < b$, sillä muuten $a - (q+1)b$ olisi vielä pienempi tällainen luku.

Tapaus $b < 0$ palautetaan edelliseen korvaamalla b luvulla $-b$:

$$a = q(-b) + r = (-q)b + r, \qquad 0 \leq r < -b = |b|.$$

Yksikäsitteisyys: Jos myös q' ja r' täyttävät lauseen ehdot, niin

$$r - r' = (q' - q)b, \qquad 0 \leq |r - r'| < |b|.$$

Epäyhtälöstä $q \neq q'$ seuraisi nyt $|r - r'| \geq |b|$, siis ristiriita. Täten $q = q'$ ja siis myös $r = r'$. $\square$

Esimerkki 2. $50 = 4 \cdot 11 + 6, \qquad 19 = (-2)(-7) + 5, \qquad -8 = (-1) \cdot 10 + 2.$

Kahdella kokonaisluvulla a ja b, joista ainakin toinen on $\neq 0$, on aina vähintään yksi yhteinen positiivinen tekijä, nimittäin 1. *Suurimmasta yhteisestä tekijästä* (joka siis on ≥ 1) käytetään merkintää $\mathrm{syt}(a, b)$ tai (a, b). Jos $\mathrm{syt}(a, b) = 1$, sanotaan, että a ja b ovat *keskenään jaottomia* (tai suhteellisia alkulukuja, *relatively prime*). Tutki kuvaa pykälässä II.6.

Lemma. $\mathrm{Syt}(a, b)$ *on joukon* $\{\, xa + yb \mid x, y \in \mathbb{Z} \}$ *pienin positiivinen luku.*

Todistus. Olkoon kyseinen pienin luku $d = ua + vb$.

Näytetään ensin, että $d \mid a$. Jakoalgoritmia käyttäen saadaan $a = qd + r$, missä $0 \leq r < d$. Tämä antaa

$$r = a - qd = (1 - qu)a + (-qv)b.$$

Näin ollen r kuuluu lemmassa mainittuun joukkoon. Jos $r > 0$, tämä on ristiriidassa d:n minimaalisuuden kanssa. Täten $r = 0$ ja siis $d \mid a$.

Symmetrian perusteella myös $d \mid b$; siis d on a:n ja b:n yhteinen tekijä. Jos myös c on näiden yhteinen tekijä, niin $c \mid (ua + vb)$ eli $c \mid d$. Koska $d > 0$, tästä seuraa, että $c \leq d$. Näin ollen $d = \text{syt}(a, b)$. □

Lause 3. *Luku $d = \text{syt}(a, b)$ täyttää seuraavat ehdot:*

(i) *d on jaollinen jokaisella lukujen a ja b yhteisellä tekijällä;*

(ii) *on olemassa sellaiset kokonaisluvut u ja v, että*

$$d = ua + vb \qquad \textit{(Bezout'n identtisyys).}$$

Todistus. Väitteet seuraavat suoraan lemmasta ja sen todistuksesta. □

Huomaa, etteivät edellä mainitut luvut u ja v ole yksikäsitteisiä: esim. $\text{syt}(4, 6) = 2 = 2 \cdot 4 - 1 \cdot 6 = (-1) \cdot 4 + 1 \cdot 6$.

$\text{Syt}(a, b)$ saadaan lasketuksi *Eukleideen algoritmilla.* Siinä sovelletaan jakoalgoritmia toistuvasti (oletetaan, että $b \neq 0$):

$$\begin{aligned}
a &= q_1 b + r_1, && 0 < r_1 < |b|,\\
b &= q_2 r_1 + r_2, && 0 < r_2 < r_1,\\
r_1 &= q_3 r_2 + r_3, && 0 < r_3 < r_2,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
r_{n-2} &= q_n r_{n-1} + r_n, && 0 < r_n < r_{n-1},\\
r_{n-1} &= q_{n+1} r_n \ (+0).
\end{aligned}$$

Menettely päättyy, koska jakojäännökset r_i muodostavat aidosti vähenevän jonon positiivisia kokonaislukuja. Viimeinen positiivinen jakojäännös r_n on haettu syt :

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

Tämä osoitetaan seuraavasti: Koska $r_n \mid r_{n-1}$, niin viimeistä edellisen yhtälön mukaan myös $r_n \mid r_{n-2}$. Jatkamalla samoin yhtälöketjussa ylöspäin saadaan tulokset $r_n \mid a$ ja $r_n \mid b$. Näin ollen r_n on lukujen a ja b yhteinen tekijä. Jos toisaalta $c \mid a$ ja $c \mid b$, niin ensimmäinen yhtälö antaa $c \mid r_1$, toinen sen jälkeen $c \mid r_2$ jne. Lopuksi nähdään, että $c \mid r_n$. Luku r_n on siis yhteisistä tekijöistä suurin.

Eukleideen algoritmi antaa myös eräät sellaiset kokonaisluvut u, v, että $r_n = ua + vb$. Tätä varten yhtälöketjusta on vain eliminoitava $r_{n-1}, r_{n-2}, \ldots, r_2, r_1$ (esim. sijoitusmenettelyllä alhaalta lähtien).

Esimerkki 3. Lasketaan syt$(306, 657)$ ja lausutaan se muodossa $306u + 657v$, missä $u, v \in \mathbb{Z}$.

Seuraava lauseeseen 4 perustuva tulos ilmaisee alkulukujen tärkeän ominaisuuden. (Mieti, onko millään yhdistetyllä luvulla samaa ominaisuutta.) Siitä saadaan ensimmäisenä sovelluksena *aritmetiikan peruslause.*

Lause 4. *Olkoon p alkuluku. Jos $p \mid ab \quad (a, b \in \mathbb{Z})$, niin $p \mid a$ tai $p \mid b$. Yleisemmin, jos $p \mid a_1 \cdots a_k \quad (a_i \in \mathbb{Z})$, niin p jakaa jonkin luvuista $a_i \quad (i = 1, \ldots, k)$.*

Todistus. Riittää todistaa lauseen alkuosa; loppuosa seuraa induktiolla.

Koska $p \in \mathbb{P}$, niin syt$(p, a) = p$ tai 1. Edellisessä tapauksessa $p \mid a$. Jälkimmäisessä tapauksessa Bezout'n identtisyys kuuluu $1 = up + va$. Siis

$$b = (up + va)b = (ub)p + v(ab).$$

Koska $p \mid ab$, nähdään että $p \mid b$. $\square$

Lause 5 (Aritmetiikan peruslause). *Jokainen kokonaisluku $n > 1$ voidaan esittää alkulukujen tulona eli muodossa*

$$n = p_1 p_2 \cdots p_s \qquad (p_i \in \mathbb{P} \quad \forall \ i)$$

tekijöiden p_i järjestystä vaille yksikäsitteisesti.

Todistus. Alkutekijähajotelman olemassaolo perusteltiin tämän pykälän alussa. Yksikäsitteisyyden todistamiseksi oletetaan, että n:llä on myös esitys $n = q_1 q_2 \cdots q_r$, missä q_j:t ovat alkulukuja. Silloin $p_1 \mid q_1 q_2 \cdots q_r$, siis lauseen 4 nojalla p_1 jakaa jonkin q_j:n. Voidaan olettaa, että $p_1 \mid q_1$. Koska kyseessä ovat alkuluvut, $p_1 = q_1$. Tämän jälkeen tarkasteltavana on yhtälö

$$p_2 \cdots p_s = q_2 \cdots q_r.$$

Jatkamalla samoin saadaan $p_2 = q_2, \ldots, p_s = q_s$ (ja $r = s$). $\square$

On luonnollista sopia, että luvulla 1 on esitys "tyhjänä" alkulukutulona (siis $s = 0$). Negatiivisilla kokonaisluvuilla on yksikäsitteinen esitys muodossa $-p_1 p_2 \cdots p_s$.

Lause 5 oikeuttaa aikaisemmin mainitun nimityksen *kanoninen hajotelma.*

Kahden luvun a ja b syt voidaan laskea tietysti myös määrittämällä ensin lukujen kanoniset hajotelmat. Jos a ja b ovat suuria, Eukleideen algoritmi on kuitenkin nopeampi menetelmä.

Esimerkki 4. $72 = 2^3 \cdot 3^2$, $60 = 2^2 \cdot 3 \cdot 5$, siis syt$(72, 60) = 2^2 \cdot 3 = 12$.

HUOMAUTUS. Jaollisuuskäsite voidaan yleistää tietyt ehdot täyttäviin *renkaisiin*, joista $\mathbb{Z}$ on erikoistapaus; esimerkkinä mainittakoon muotoa $a + b\sqrt{n}$ olevien lukujen joukko, missä $a, b \in \mathbb{Z}$ ja n on sopivasti valittu kiinteä kokonaisluku. Näiden lukujen *jaottomuus* määritellään vastaavasti kuin $\mathbb{Z}$:ssa. Mutta lukujen esitys jaottomien lukujen tulona ei yleensä ole yksikäsitteinen!

Lukujen suurimman yhteisen tekijän käsittely on välittömästi yleistettävissä useamman kuin kahden luvun tapaukseen: $\text{syt}(a_1, \ldots, a_n)$ (missä ainakin yksi luvuista a_i on $\neq 0$) on pienin positiiviluku joukossa

$$\left\{ x_1 a_1 + \cdots + x_n a_n \;\middle|\; x_1, \ldots, x_n \in \mathbb{Z} \right\}$$

ja se mm. voidaan siis aina esittää muodossa $d = u_1 a_1 + \cdots + u_n a_n$, missä $u_1, \ldots, u_n \in \mathbb{Z}$.

Suurimman yhteisen tekijän käsitteen kanssa analoginen on lukujen a ja b *pienin yhteinen monikerta* (eli *pienin yhteinen jaettava*) $\text{pyj}(a, b)$. Jos a ja b ovat positiivisia, nämä käsitteet sitoo toisiinsa kaava (mieti!)

$$\text{syt}(a, b) \cdot \text{pyj}(a, b) = ab.$$

Harjoitustehtäviä

1. Olkoot m, n ja p kokonaislukuja. Osoita, että
   a) $m|n$ ja $n|p \Rightarrow m|p$,
   b) $p|m$ ja $p|n \Rightarrow p \mid m + n$,
   c) $p|m$ ja $p \not| n \Rightarrow p \not| m + n$.

2. Määritä lukujen 2279 ja 989 suurin yhteinen tekijä Eukleideen algoritmilla.

3. Määritä sellaiset kokonaisluvut x ja y, että

$$127x - 87y = 1.$$

4. Määritä kaikki kokonaislukuparit (x, y), joilla

$$26x + 35y = 2.$$

5. Osoita, että jokainen alkuluku $p > 3$ on muotoa $6n \pm 1$, missä $n \in \mathbb{N}$.

6. Olkoon $p \in \mathbb{Z}$ alkuluku. Näytä, että $x^5 \neq p$ kaikilla $x \in \mathbb{Q}$. (Ohje: x:n osoittajan ja nimittäjän alkutekijäesitys. Kerro yhtälöstä $x^5 = p$ pois nimittäjä.)

7. Etsi lukujen 42, 258 ja 336 alkutekijäesitykset, suurin yhteinen tekijä ja pienin yhteinen monikerta.

8. Näytä, että luku $p = 257$ on alkuluku. Etsi Eukleideen algoritmilla sellainen $a \in \mathbb{N}$, $0 < a < p$, että $p|(1 - 25a)$. (Ohje: Jos p ei ole jaoton, sillä on sellainen alkutekijä $q > 1$, että $q^2 \leq p$.)

9. Oletetaan, että $a, b, c \in \mathbb{Z}$ ja ainakin toinen luvuista a, b on $\neq 0$. Näytä, että yhtälöllä

$$ax + by = c \tag{1}$$

on ratkaisuja $(x, y) \in \mathbb{Z}^2$ aina ja vain, kun $\text{syt}(a, b)$ on c:n tekijä.

10. Olkoon edellä $ab \neq 0$, $d = \text{syt}(a, b) \in \mathbb{N}$ ja olkoon $(x_0, y_0) \in \mathbb{Z}^2$ yhtälön (1) ratkaisu. Näytä, että kaikki ratkaisut $(x, y) \in \mathbb{Z}^2$ saadaan kaavasta $x = x_0 + t\frac{b}{d}$, $y = y_0 - t\frac{a}{d}$, $t \in \mathbb{Z}$.

I.2 Kongruenssi

Seuraavassa esitettävä *kongruenssin* käsite mahdollistaa jaollisuuteen liittyvien asioiden käsittelyn tavalla, joka muistuttaa yhtälöiden käsittelyä.

MÄÄRITELMÄ. Olkoon m positiivinen kokonaisluku. Jos $a, b \in \mathbb{Z}$ ja $a - b$ on jaollinen luvulla m, sanotaan, että a on *kongruentti* b:n kanssa *modulo* m, ja merkitään

$$a \equiv b \pmod{m}.$$

Tätä nimitetään joukon $\mathbb{Z}$ *kongruenssiksi*; luku m on sen *moduli*.

Edellisen vastakohta: a on *epäkongruentti* (eli *inkongruentti*) b:n kanssa modulo m, merkintä $a \not\equiv b \pmod{m}$.

ESIMERKKI 1. $38 \equiv 2 \pmod{6}$, $\quad 12 \equiv -13 \pmod{5}$, $\quad 100 \not\equiv 1 \pmod{10}$.

Lemma. *Olkoon m positiivinen kokonaisluku. Kaikilla $a, b, c \in \mathbb{Z}$ on*

$$a \equiv a \pmod{m},$$
$$a \equiv b \pmod{m} \implies b \equiv a \pmod{m},$$
$$a \equiv b \pmod{m} \text{ ja } b \equiv c \pmod{m} \implies a \equiv c \pmod{m}.$$

Määritelmän mukaan $a \equiv b \pmod m$ jos ja vain jos a on m:n monikertaa vaille yhtäkuin b; siis lyhyesti

$$a \equiv b \pmod m \qquad \Longleftrightarrow \qquad a = b + mq, \quad q \in \mathbb{Z}.$$

Tästä nähdään, että kongruenssi $\bmod m$ hajottaa $\mathbb{Z}$:n seuraavaa muotoa oleviin pistevieraisiin joukkoihin:

$$[a] = \left\{ a + mk \;\middle|\; k \in \mathbb{Z} \right\}.$$

Joukkoa $[a]$ sanotaan luvun a *jäännösluokaksi modulo* m; siitä käytetään yleensä merkintää $\overline{a}$, $[a]_m$, a_m tai $a + m\mathbb{Z}$. Samaan jäännösluokkaan kuuluvat luvut antavat m:llä jaettaessa saman jakojäännöksen. Käymällä läpi kaikki mahdolliset jakojäännökset eli luvut $0, 1, \ldots, m-1$ saadaan eräs jäännösluokkien edustajisto, kokonaislukujen *pienimmät ei-negatiiviset jäännökset* $\bmod m$. Niiden avulla kaikkien jäännösluokkien $\bmod m$ joukko, jota merkitään $\mathbb{Z}_m$:llä, voidaan kirjoittaa seuraavasti:

$$\mathbb{Z}_m = \left\{ \overline{0}, \overline{1}, \ldots, \overline{m-1} \right\}.$$

Esimerkki 2. $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, missä

$$\begin{aligned}
0_3 = \overline{0} = \quad 3\mathbb{Z} &= \{\, 3k \mid k \in \mathbb{Z}\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}, \\
1_3 = \overline{1} = 1 + 3\mathbb{Z} &= \{\, 1 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}, \\
2_3 = \overline{2} = 2 + 3\mathbb{Z} &= \{\, 2 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}.
\end{aligned}$$

Joukko $\mathbb{Z}_3$ voidaan esittää myös esim. muodossa $\{\, \overline{-1}, \overline{0}, \overline{1}\,\}$ tai $\{\, \overline{7}, \overline{33}, \overline{2}\,\}$.

Esimerkki 3. Rajatapauksessa $m = 1$ kongruenssi $\bmod m$ on triviaali: $a \equiv b \pmod 1 \quad \forall\ a, b \in \mathbb{Z}$. Erityisesti siis $\mathbb{Z}_1 = \{\overline{0}\}$, missä $\overline{0} = \mathbb{Z}$.

Lause 6. (i) *Jos* $a \equiv b \pmod m$ *ja* $c \equiv d \pmod m$, *niin*

$$a + c \equiv b + d \pmod m \qquad \textit{ja} \qquad ac \equiv bd \pmod m.$$

(ii) *Jos* $ca \equiv cb \pmod m$ *ja* $\operatorname{syt}(c, m) = 1$, *niin* $a \equiv b \pmod m$.

(iii) *Jos* $a \equiv b \pmod{km}$, *missä* k *on kokonaisluku* > 0, *niin* $a \equiv b \pmod m$.

Todistus. (i) Luku $(a+c)-(b+d) = (a-b)+(c-d)$ on jaollinen m:llä, koska $m \mid a-b$ ja $m \mid c-d$; samoin luku $ac - bd = (a-b)c + b(c-d)$.

(ii) Ehdoista $m \mid c(a-b)$ ja $\operatorname{syt}(c, m) = 1$ yhdessä seuraa, että $m \mid a-b$ (ajattele lukujen kanonisia hajotelmia).

(iii) Koska $a - b$ on luvun km monikerta, se on myös m:n monikerta. $\square$

Lauseen (i)-kohdan mukaan kongruensseja $\bmod m$ voidaan laskea yhteen ja kertoa puolittain, samoin siis vähentää puolittain ja korottaa potenssiin puolittain. Erityisesti, jos $P(x)$ on kokonaiskertoiminen polynomi, siis

$$P(x) = c_0 + c_1 x + \cdots + c_t x^t \qquad (c_i \in \mathbb{Z} \quad \forall\ i),$$

niin kongruenssista $a \equiv b \pmod m$ seuraa, että $P(a) \equiv P(b) \pmod m$.

Esimerkki 4. Lasketaan, mikä on jakojäännös, kun luku $18^2 + 2^{100}$ jaetaan luvulla 11.

Esimerkki 5. Jos kongruenssi $3 \equiv 15 \pmod{12}$ jaetaan puolittain 3:lla, saadaan $1 \equiv 5 \pmod{12}$, mikä ei pidä paikkaansa. Huomaa, että $\operatorname{syt}(3, 12) \neq 1$. Lauseen 6 (ii)-kohdan oletus $\operatorname{syt}(c, m) = 1$ on siis välttämätön.

Huomaa kuitenkin, että $1 \equiv 5 \pmod 4$. Keksi tästä yleinen tulos ja perustele se!

Jäännösluokkien joukko $\mathbb{Z}_m$ muodostaa tärkeän *algebrallisen systeemin*, kun siinä määritellään yhteen- ja kertolasku sopivasti. Sitä käsitellään jäljempänä ryhmien, renkaiden ja kuntien teoriassa. Asian valmistelemiseksi määritellään kyseiset laskutoimitukset tässä:

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{ab}. \tag{1}$$

Probleemana kuitenkin on, että jäännösluokat $\overline{a}$ ilmaistaan edustajan a avulla eikä edustajan valinta ole yksikäsitteinen. On siis näytettävä, että näin määritellyt summa ja tulo ovat silti yksikäsitteisiä, ts. riippumattomia edustajien valinnasta.

Tällainen tilanne, jossa määritelmä sisältää näennäisen riippuvuuden (ekvivalenssi)luokan edustajan valinnasta, on matematiikassa tavallinen. Kun on osoitettu, ettei riippuvuus ole todellinen, on tapana sanoa, että ko. käsite on *hyvinmääritelty* (well defined).

Lause 7. *Yhtälöiden* (1) *mukaiset jäännösluokkien summa ja tulo ovat hyvinmääriteltyjä.*

Todistus. Oletetaan, että $\overline{a} = \overline{a'}$ ja $\overline{b} = \overline{b'}$. Silloin $a \equiv a'$ ja $b \equiv b' \pmod m$. Lauseen 6(i) mukaan siis

$$a + b \equiv a' + b', \qquad ab \equiv a'b' \qquad (\bmod m).$$

Tästä seuraa, että $\overline{a+b} = \overline{a'+b'}$ ja $\overline{ab} = \overline{a'b'}$, mikä todistaa väitteen. □

Esimerkki 6. Jäännösluokkien $\bmod 7$ joukossa $\overline{4} + \overline{5} = \overline{2}$. Toisaalta $\overline{4} = \overline{60}$ ja $\overline{5} = \overline{75}$, siis $\overline{4} + \overline{5} = \overline{60} + \overline{75} = \overline{135}$. Varmistu laskemalla, että $\overline{135} = \overline{2}$.

Kongruensseja sovelletaan mm. tutkittaessa *Diofantoksen yhtälöitä.* Nämä ovat yhtälöitä, joille etsitään kokonaislukuratkaisuja.

Esimerkki 7. Tarkastellaan Diofantoksen yhtälöä $x^2 - 2y^2 = 5$. Osoitetaan, ettei kongruenssilla $x^2 - 2y^2 \equiv 5 \pmod 8$ ole yhtään ratkaisua x, y. Tästä seuraa, ettei myöskään ko. yhtälöllä ole (kokonaisluku)ratkaisuja.

Esimerkki 8. A osti isoja kakkuja hintaan 15 €/kpl ja pieniä hintaan 11 €/kpl. Lasku oli 137 €. Montako kappaletta kumpaakin lajia oli?

Ratkaistavana on Diofantoksen yhtälö $15x + 11y = 137$. Ratkaistaan se siirtymällä kongruenssiin $15x \equiv 137 \pmod{11}$.

Kuten välittömästi nähdään, lineaarisen kahden tuntemattoman Diofantoksen yhtälön $ax + my = c$ ratkaiseminen on yleisestikin ekvivalentti tehtävä kongruenssin

$$ax \equiv c \pmod{m} \tag{2}$$

ratkaisemisen kanssa. Seuraava tätä kongruenssia koskeva tulos on myöhemmin useassa yhteydessä tarpeellinen.

Lause 8. *Jos* $\mathrm{syt}(a, m) = 1$, *kongruenssilla* (2) *on yksikäsitteinen ratkaisu* $x \in \mathbb{Z}$ *välillä* $0 \leq x \leq m - 1$.

Todistus. Oletuksen nojalla on olemassa sellaiset luvut $u, v \in \mathbb{Z}$, että $au + mv = 1$ ja siis

$$a(uc) + m(vc) = c.$$

Kongruenssilla on täten ratkaisu $x = uc$. Lisäksi kongruenssin kaikki ratkaisut x ovat keskenään kongruentteja mod m, sillä lauseen 6(ii) mukaan

$$ax_1 \equiv ax_2 \pmod{m} \qquad \Longrightarrow \qquad x_1 \equiv x_2 \pmod{m}.$$

Ratkaisuista on siis tarkalleen yksi välillä $0 \leq x \leq m - 1$. □

Pienillä m:n arvoilla ko. ratkaisu löydetään usein helpoimmin kokeilemalla.

Harjoitustehtäviä

1. Onko $73 \equiv 2 \pmod{7}$, $15 \equiv -1 \pmod{4}$?
2. Ratkaise kongruenssit

$$4x \equiv 3 \pmod{7}, \qquad 3x \equiv 6 \pmod{12}, \qquad 5x \equiv 7 \pmod{10}.$$

II. JOUKOT JA RELAATIOT

II.1 Kuvauksista

Matematiikan termit *funktio* (engl. function) ja *kuvaus* (mapping) ovat synonyymejä. Algebrassa käytetään tavallisimmin kuvaus-termiä. Seuraavassa on yhteenveto kuvauksiin liittyvistä perusasioista, lähinnä peruskäsitteistä.

Kuvaus f *joukolta* A *joukkoon* B, lyhyesti merkittynä $f : A \to B$, liittää *jokaiseen* A:n alkioon x *yksikäsitteisen* B:n alkion $y = f(x)$. Tässä

- A on kuvauksen f *määrittelyjoukko* (domain),
- B on kuvauksen f *maalijoukko* (range),
- y on alkion x *kuva*.

Sanotaan myös, että f *kuvaa* alkion x alkioksi y, ja merkitään

$$f : A \longrightarrow B, \qquad x \mapsto y,$$

tai

$$f : A \longrightarrow B, \qquad f(x) = y.$$

Esimerkki 1. Merkitään $\mathbb{R}_+^* = \{x \mid x > 0\}$. Reaalianalyysista ovat tuttuja kuvauksia

$$f : \mathbb{R} \longrightarrow \mathbb{R}, \qquad f(x) = \sin x,$$
$$g : \mathbb{R}_+^* \longrightarrow \mathbb{R}, \qquad g(x) = \ln x.$$

(Näistä voitaisiin myös käyttää merkintöjä $f = \sin$ ja $g = \ln$, mutta esim. kuvaukselle $h(x) = x^2$ ei vastaavanlaista merkintää ole.)

Esimerkki 2. Seuraavassa esimerkkejä lineaarialgebrasta.

(i) Determinanttikuvaus

$$d : \mathcal{M}_2(\mathbb{R}) \longrightarrow \mathbb{R}, \qquad d(A) = \det(A).$$

Determinanttikuvaus voidaan määritellä myös yleisesti $\mathcal{M}_n(\mathbb{R}) \longrightarrow \mathbb{R}$.

(ii) Merkitään S_n:llä lukujen $1, 2, \ldots, n$ kaikkien permutaatioiden joukkoa. Permutaation $\alpha \in S_n$ merkki $\operatorname{sign}(\alpha)$ määrittelee kuvauksen

$$s : S_n \longrightarrow \mathbb{Z}, \qquad s(\alpha) = \operatorname{sign}(\alpha).$$

(iii) Jos V on vektoriavaruus, voidaan määritellä kuvaus

$$n : V \longrightarrow V, \qquad n(X) = -X.$$

(iv) Vektoriavaruudessa $\mathbb{R}$ on määritelty itseisarvokuvaus

$$N : \mathbb{R} \longrightarrow \mathbb{R}, \qquad N(X) = |X|.$$

Tämä voidaan yleistää sisätuloavaruuden V normikuvaukseksi

$$N : V \longrightarrow \mathbb{R}, \qquad N(X) = \|X\|.$$

Lisää kuvaukseen $f : A \to B$ liittyvää terminologiaa:

• Joukko $f(A) = \{ f(x) \mid x \in A \}$ on kuvauksen f *arvojoukko* eli *kuvajoukko*, lyhyesti *kuva* (image). Siitä käytetään myös merkintää $\mathrm{Im}(f)$.

• Yleisemmin, jos $A_0 \subset A$, joukko $f(A_0) = \{ f(x) \mid x \in A_0 \}$ on joukon A_0 *kuva(joukko)*.

• Jos $B_0 \subset B$, joukko $f^{-1}(B_0) = \{ x \in A \mid f(x) \in B_0 \}$ on joukon B_0 *alkukuva*.

• Kuvaus f on *surjektio* (eli *surjektiivinen*), jos $\mathrm{Im}(f) = B$. Tällöin sanotaan, että f on kuvaus joukolta A jouko*lle* B.

• Kuvaus f on *injektio* (eli *injektiivinen*), jos eri alkioilla on eri kuvat, ts.

$$x_1, x_2 \in A, \quad x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

Tämä voidaan kirjoittaa myös seuraavassa muodossa, joka on usein mukavampi käyttää:

$$x_1, x_2 \in A, \quad f(x_1) = f(x_2) \implies x_1 = x_2.$$

• Kuvaus f on *bijektio* (eli *bijektiivinen*) eli *kääntäen yksikäsitteinen*, jos se on injektio ja surjektio. Silloin siis jokaisella B:n alkiolla y on yksikäsitteinen alkukuva x joukossa A.

Esimerkki 3. Tutkitaan, ovatko esimerkkien 1 ja 2 kuvaukset surjektiivisia tai injektiivisiä.

Kuvaukset $f_1 : A \to B$ ja $f_2 : A \to B$ määritellään samoiksi, jos

$$f_1(x) = f_2(x) \quad \forall \ x \in A.$$

Tällöin merkitään $f_1 = f_2$. Erityisesti kuvauksilla on siis tällöin sama määrittelyjoukko ja sama maalijoukko.

Kuvausta

$$f : A \longrightarrow A, \qquad f(x) = x,$$

sanotaan joukon A *identiteettikuvaukseksi* ja merkitään $f = \mathrm{id}_A$.

Kuvausten $f : A \to B$ ja $g : B \to C$ *yhdistetty kuvaus* eli *tulo* on

$$g \circ f : A \longrightarrow C, \qquad (g \circ f)(x) = g(f(x)).$$

Tästä seuraa välittömästi, että kuvaustulo on assosiatiivinen, ts. jos edellisten kuvausten f ja g lisäksi h on kuvaus $C \to D$, niin

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

Kuvauksen yhdistäminen identiteettikuvauksen kanssa on yksinkertaista:

$$\mathrm{id}_B \circ f = f, \qquad f \circ \mathrm{id}_A = f. \tag{1}$$

Yhdistetty kuvaus $g \circ f$ merkitään myös gf.

Jos kuvaus $f : A \to B$ on bijektio, sillä on *käänteiskuvaus*

$$f^{-1} : B \longrightarrow A, \qquad f(x) \mapsto x.$$

Silloin (mieti!)

$$f^{-1} \circ f = \mathrm{id}_A, \qquad f \circ f^{-1} = \mathrm{id}_B\,.$$

Yleisemmin jokainen injektiivinen kuvaus $f : A \to B$ määrittelee bijektion $A \to \mathrm{Im}(f), \quad x \mapsto f(x)$. Myös tällöin kuvausta $\mathrm{Im}(f) \to A, \quad f(x) \mapsto x$, sanotaan yleensä (hiukan epätäsmällisesti) f:n käänteiskuvaukseksi ja merkitään f^{-1}:llä.

Jos kuvauksella $f : A \to B$ on käänteiskuvaus, merkintä $f^{-1}(B_0)$, missä $B_0 \subset B$, voidaan tulkita kahdella tavalla. Molemmat tarkoittavat kuitenkin samaa joukkoa.

Esimerkki 4. Tutkitaan, millä esimerkkien 1 ja 2 kuvauksista on käänteiskuvaus.

Lause 1. *Olkoon f kuvaus $A \to B$. Jos on olemassa sellainen kuvaus $g : B \to A$, että*

$$g \circ f = \mathrm{id}_A, \qquad f \circ g = \mathrm{id}_B,$$

niin f on bijektio ja $f^{-1} = g$.

Todistus. Jos $y \in B$, niin ehdon $f \circ g = \mathrm{id}_B$ nojalla $f(g(y)) = y$. Siis y:llä on alkukuva $g(y)$, joten f on surjektio.

Jos $x_1, x_2 \in A$ ja $f(x_1) = f(x_2)$, niin myös $g(f(x_1)) = g(f(x_2))$. Koska $g \circ f = \mathrm{id}_A$, tämä yhtälö sievenee muotoon $x_1 = x_2$. Kuvaus f on siis injektio.

Edellisen nojalla f on bijektio ja sen käänteiskuvaus f^{-1} siis on olemassa. Yhtälöstä $f \circ g = \mathrm{id}_B$ seuraa, että

$$f^{-1} \circ (f \circ g) = f^{-1} \circ \mathrm{id}_B\,.$$

Soveltamalla tähän kuvaustulon assosiatiivisuutta, ehtoa $f^{-1} \circ f = \mathrm{id}_A$ ja yhtälöitä (1) saadaan tulos $g = f^{-1}$. $\square$

Jos f on kuvaus $A \to B$ ja $A_0 \subset A$, kuvausta

$$g : A_0 \longrightarrow B, \qquad g(x) = f(x),$$

sanotaan f:n *rajoittumaksi* (eli *restriktioksi*) *joukkoon* A_0 ja merkitään $g = f|_{A_0}$. Sanotaan myös, että f on kuvauksen g *laajennus* (eli *ekstensio*) joukolle A.

Esimerkki 5. Merkitään $\mathbb{R}_+ = \{\, x \in \mathbb{R} \mid x \geq 0 \}$. Kuvaus

$$f : \mathbb{R}_+ \longrightarrow \mathbb{R}_+, \qquad f(x) = \sqrt{x},$$

on bijektio; sen käänteiskuvaus on kuvauksen

$$h : \mathbb{R} \longrightarrow \mathbb{R}_+, \qquad h(x) = x^2,$$

rajoittuma joukolle $\mathbb{R}_+$.

Esimerkki 6. Kompleksiluvun $z = x + iy$ itseisarvo $|z| = \sqrt{x^2 + y^2}$ määrittelee kuvauksen $\mathbb{C} \to \mathbb{R}_+, \quad z \mapsto |z|$, joka on kuvauksen $\mathbb{R} \to \mathbb{R}_+, \quad x \mapsto |x|$, laajennus.

Lemma. *Jos f on kuvaus $X \to Y$ sekä $A \subset X$ ja $B \subset Y$, niin*

$$a) \quad f^{-1}\big(f(A)\big) \supset A,$$
$$b) \quad f\big(f^{-1}(B)\big) \subset B.$$

Kummassakin tapauksessa voi olla kyseessä aito sisältyminen.

Todistus. a) Olkoon $x \in A$. Tällöin $f(x) \in f(A)$, joten $x \in f^{-1}\big(f(A)\big)$.

b) Olkoon $y \in f\big(f^{-1}(B)\big)$. Silloin on olemassa $x \in f^{-1}(B)$, jolla $y = f(x)$. Koska $x \in f^{-1}(B)$, niin $f(x) \in B$. Siis $y \in B$.

Esimerkki, joka osoittaa, että sisältyminen voi olla aito: $X = Y = \{1, 2, 3\} \quad f : X \to Y$, $f(x) = 1$. Olkoon $A = \{3\}$, $B = Y$. Tällöin $f^{-1}\big(f(A)\big) = f^{-1}(\{1\}) = X \neq A$, $f\big(f^{-1}(B)\big) = f(X) = \{1\} \neq B$. $\square$

Harjoitustehtäviä

1. Olkoon $f : B \to A$ injektio ja $g, h : C \to B$ kuvauksia. Todista: $f \circ g = f \circ h \Rightarrow g = h$.

2. Olkoon $f : X \to Y$ surjektio ja $g, h : Y \to \mathbb{Z}$ kuvauksia. Todista: $g \circ f = h \circ f \Rightarrow g = h$.

3. Osoita, että $f : x \mapsto (3x-2)/(x-2)$ on kuvaus joukolta $A = \mathbb{R}\backslash\{2\}$ joukkoon $B = \mathbb{R}\backslash\{3\}$ ja että $f(A) = B$.

4. Määritä kuvauksessa $f : \mathbb{R} \to \mathbb{R},\ f(x) = 2x$, joukon $\{x \in \mathbb{R} \mid -1 < x < 1\}$ kuva ja joukon $\{y \in \mathbb{R} \mid y \leq 0\}$ alkukuva.

5. Olkoot f ja g kuvauksia $\mathbb{R} \to \mathbb{R},\ f(x) = 2x+1,\ g(x) = x^2 - 2$. Muodosta $f \circ g$ ja $g \circ f$.

6. Olkoon f kuvaus $A \to B$ ja g kuvaus $B \to C$ sekä $X \subset A$ ja $Y \subset C$. Todista:

$$(g \circ f)(X) = g\big(f(X)\big),$$
$$(g \circ f)^{-1}(Y) = f^{-1}\big(g^{-1}(Y)\big).$$

7. Olkoon f kuvaus $X \to Y$. Osoita, että f on surjektio jos ja vain jos $f(f^{-1}B) = B$ jokaisella $B \subset Y$.

8. Olkoot A ja B epätyhjiä joukkoja. Muodosta jokin bijektio $A \times B \to B \times A$.

9. Mitkä seuraavista ehdoista määrittelevät yksikäsitteisesti kuvauksen $f : \mathbb{R} \to \mathbb{R}$?

   i) $x + f(x) = 1$,
   ii) $xf(x) = 1$,
   iii) $x^2 + |f(x)| = 1$,
   iv) $(f(x) \in \mathbb{Z}) \ \wedge\ (0 < x - f(x) \leq 1)$.

   Perustelu!

10. Määritä $f\big(f^{-1}(A)\big)$ ja $f^{-1}\big(f(A)\big)$, kun $f : \mathbb{R} \to \mathbb{R}$ saadaan kaavasta $f(x) = 1 + x^2$ ja $A = [-1, 2)$.

11. Olkoon $D \in \mathcal{P}(A)$ mielivaltainen ja $Y \in \mathcal{P}(A)$ sellainen, että $D \subset Y$. Olkoon $f : \mathcal{P}(A) \to \mathcal{P}(A), \quad f(X) = X \cup D$. Näytä:

    i) $f(\mathcal{P}(A)) = \{U \in \mathcal{P}(A) \mid D \subset U\}$.
    ii) $f^{-1}(Y) = \{X \in \mathcal{P}(A) \mid X \setminus D = Y \setminus D\}$.

12. Näytä edellisen tehtävän merkinnöillä, että kuvaus $g : \mathcal{P}(A) \to \mathcal{P}(A \setminus D),\ X \mapsto X \setminus D$ on surjektio. Milloin g on bijektio?

13. Näytä, että yhtälö $f(X, Y) = X \times Y$ määrittelee injektion

$$f : \big(\mathcal{P}(A) \setminus \{\emptyset\}\big) \times \big(\mathcal{P}(B) \setminus \{\emptyset\}\big) \to \mathcal{P}(A \times B) \setminus \{\emptyset\}.$$

    Näytä, ettei f ole yleensä surjektio, tarkastelemalla tapausta $A = B = \{1, 2\}$.

14. Olkoot A ja B joukkoja ja olkoon $f : A \to B$ injektio, $g : B \to A$ surjektio sekä $f \circ g = id_B$. Näytä, että f on bijektio ja $g = f^{-1}$.

II.2 Luonnolliset luvut; induktio

Luonnollisten lukujen joukko $\mathbb{N} = \{0, 1, 2, ...\}$ on tärkeä, koska se on lähtökohta, jonka avulla konstruoidaan monimutkaisempia joukkoja (kokonaisluvut, rationaaliluvut, reaaliluvut, jäännösluokat $\mathbb{Z}_n$ jne). Lisäksi esimerkiksi algebrallisia struktuureja tutkittaessa tarvitaan tiettyjä kuvauksia luonnollisilta luvuilta ko. struktuuriin.

Luonnolliset luvut voidaan muodostaa puhtaasti joukko-opillisella konstruktiolla. Toinen mahdollisuus on määritellä $\mathbb{N}$ aksiomaattisesti. Tässä käytetään $\mathbb{N}$:n määrittelyyn Peanon aksioomia. Intuitiivisesti $\mathbb{N}$:ssä on ensimmäinen luku $0 \in \mathbb{N}$ ja voidaan määritellä seuraajakuvaus $s : \mathbb{N} \to \mathbb{N},\ 0 \mapsto 1 \mapsto 2 \mapsto ... \mapsto n \mapsto n + 1 \mapsto ...$

MÄÄRITELMÄ (Peanon aksioomat). Olkoon $\mathbb{N}$ joukko, s kuvaus $\mathbb{N} \to N$ ja $0 \in \mathbb{N}$. Kolmikko $(\mathbb{N}, s, 0)$, on luonnollisten lukujen joukko, jos seuraavat ehdot ovat voimassa:

(P1) s on injektio;
(P2) $0 \notin s(\mathbb{N})$;
(P3) jos $A \subset \mathbb{N}$ ja
(i) $0 \in A$,
(ii) $n \in A \Rightarrow s(n) \in A$,

niin $A = \mathbb{N}$ (induktioaksiooma).

Näiden aksioomien pohjalta voidaan määritellä yhteen- ja kertolasku; erityisesti $s(n) = n + 1$.

Aksioomasta (P3) seuraa *induktiotodistuksen* periaate:

Oletetaan, että jokaiseen luonnolliseen lukuun liitetään väite $E(n)$, ja merkitään $A = \{n \in \mathbb{N} \mid E(n) \text{ tosi}\}$. Jos $E(0)$ on tosi ja jos $E(r) \Rightarrow E\big(s(r)\big)$, niin $E(n)$ on tosi kaikilla $n \in \mathbb{N}$. (Vaihetta $E(r) \Rightarrow E\big(s(r)\big)$ sanotaan induktioaskeleeksi.)

Induktiotodistusta voidaan soveltaa myös muotoa $E(n) \quad \forall n \geq n_0$ oleviin väitteisiin, ts. "aloituskohta" voi olla 0:n asemesta jokin $n_0 \geq 0$.

Induktion aloittamisen luvusta 1 oikeuttaa

Lause 2. *Olkoon $A \subset \mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Jos*

(i) $1 \in A$ ja
(ii) $k \in A \Rightarrow k + 1 \in A$,

niin $A = \mathbb{N}_+$.

Todistus. Merkitään $B = A \cup \{0\}$. Silloin $0 \in B$. Olkoon nyt $n \in B$. Jos $n = 0$, niin $1 \in A \subset B$, joten $0 + 1 \in B$. Jos $n \neq 0$, niin $n \in A$, joten $n + 1 \in A$. Silloin $n + 1 \in B$. Nyt $B = \mathbb{N}$, joten $A = B \setminus \{0\} = \mathbb{N} \setminus \{0\}$. □

Havainnollisesti ajatellen on induktioperiaatteen sisältö seuraava: Aluksi todetaan väitteen $E(n_0)$ pätevyys. Kun induktioaskel on todistettu, saadaan väitteen $E(n_0 + 1)$ oikeus. Vastaavasti askeleittain saadaan todistetuksi $E(n_0 + 2)$ ja edelleen $E(n)$ kaikilla luvuilla $n \geq n_0$.

Esimerkki 1. Todistetaan induktiolla, että

$$1^2 + 2^2 + \cdots + n^2 = \frac{n}{6}(n+1)(2n+1),\ n \in \mathbb{N} \setminus \{0\}.$$

Nyt $E(n)$ on yhtälö $1^2 + 2^2 + \cdots + n^2 = \frac{n}{6}(n+1)(2n+1)$ ja aloituskohta on $n_0 = 1$.

Todistus.
1) Arvolla $n = 1$ on vasen puoli $1^2 = 1$, oikea puoli $\frac{1}{6} \cdot 2 \cdot 3 = 1$, joten $E(1)$ on tosi.
2) Induktioaskelta todistettaessa *oletetaan* $E(n)$ ja *todistetaan tämän avulla* $E(n+1)$:

$$1^2 + 2^2 + \cdots + n^2 + (n+1)^2 = [1^2 + 2^2 + \cdots + n^2] + (n+1)^2$$

$$\overset{(*)}{=} \frac{n}{6}(n+1)(2n+1) + (n+1)^2 = \frac{n+1}{6}[(n+1)+1][2(n+1)+1],$$

missä perusteluna kohdassa (*) on induktio-oletus $E(n)$.

□

Esimerkki 2. Todistetaan induktiolla kaava

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

Todistus.
1) Arvolla $n = 0$ on vasen puoli 0, oikea puoli $\dfrac{0(0+1)}{6} = 0$, joten $E(0)$ on tosi.
2) Induktioaskel:

$$1 + 2 + \cdots + n + (n+1) = [1 + 2 + \cdots + n] + (n+1)$$

$$= \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)[(n+1)+1]}{2}.$$

□

Peanon aksioomat eivät määritä luonnollisten lukujen joukkoa yksikäsitteisesti, vaan useat eri joukot toteuttavat aksioomat (P1) – (P3). Nämä ovat yhtä hyviä malleja luonnollisten lukujen joukolle, sillä ne ovat "rakenteeltaan samanlaiset". Tämä voidaan ilmaista täsmällisesti seuraavalla lauseella, jonka todistus tässä sivuutetaan:

Jos $(\mathbb{N}, s, 0)$ ja $(\mathbb{N}', s', 0')$ ovat luonnollisten lukujen joukon malleja, niin on olemassa yksikäsitteinen bijektio $f : \mathbb{N} \to \mathbb{N}'$, jolla $f \circ s = s' \circ f$ ja $f(0) = 0'$.

Harjoitustehtäviä

1. Todista induktiolla luvun n suhteen: jos $k_1, ..., k_n$ ovat luonnollisia lukuja, niin

$$\sum_{i=1}^{n} k_i \leq n \cdot \max(k_1, ..., k_n).$$

2. Osoita induktiolla, että

$$2^n > n^2$$

kaikilla luonnollisilla luvuilla $n \geq 5$.

II.3 Lukumäärän laskemisesta

Seuraavissa pykälissä määritellään täsmällisesti joukon äärellisyys, äärettömyys ja alkioiden lukumäärä. Tässä pykälässä johdetaan eräitä yksinkertaisia kaavoja heuristisesti.

Olkoon S äärellinen joukko, ts. joukko jossa on äärellisen monta alkiota; näiden lukumäärä olkoon $\#S = n$. (Lukumäärälle käytetään myös merkintää $|S|$.)

Tarkastellaan joukon S *osajoukkojen muodostamaa joukkoa* $\mathcal{P}(S)$. Jos $A \subset S$ on jokin osajoukko, voidaan sen koostumus ilmaista jonolla, jossa on n kappaletta lukuja 0 tai 1; kukin luku vastaa tiettyä joukon S alkiota ja on $= 0$, jos kyseinen alkio ei kuulu joukkoon A, ja $= 1$, jos alkio on joukossa A. Kutakin osajoukkoa vastaa jokin tällainen jono ja kääntäen. Erilaisia jonoja voidaan muodostaa 2^n kappaletta, koska jokainen jonon alkio voidaan muista riippumattomasti valita kahdella tavalla. Pelkkien ykkösten muodostama jono vastaa osajoukkoa S, ts. koko joukkoa, nollien muodostama jono taas tyhjää joukkoa, joka on minkä tahansa joukon osajoukko. Saadaan siis lause:

Lause 3. *Jos* $\#S = n$, *niin* $\#\big(\mathcal{P}(S)\big) = 2^n$.

Bijektiota $p : S \to S$ sanotaan *permutaatioksi*. Koska bijektio on sekä surjektio että injektio, kuvauksen arvona on jokainen joukon S alkio täsmälleen kerran. Tämä merkitsee, että permutaatio voidaan tulkita joukon S alkioiden järjestämisenä permutaation antamaan järjestykseen.

Esimerkki 1. Jos $S = \{1, 2, 3, 4, 5\}$, määrittelevät yhtälöt

$$p(1) = 2,\ p(2) = 4,\ p(3) = 1,\ p(4) = 3,\ p(5) = 5$$

erään permutaation, ts. lukujen 1, 2, 3, 4, 5 uuden järjestyksen 2, 4, 1, 3, 5.

Kaikkien permutaatioiden lukumäärä voidaan laskea tarkastelemalla joukon S alkioiden eri järjestysten lukumäärää. Jos alkiot kirjoitetaan jonoksi, voidaan ensimmäiselle paikalle valita alkio vapaasti, ts. n tavalla, toiselle paikalle $n-1$ tavalla (koska ensimmäiselle paikalle valittu alkio ei ole enää käytettävissä), kolmannelle paikalle $n-2$ tavalla jne. Viimeiselle eli n:nnelle paikalle tuleva alkio on yksikäsitteisesti määrätty. Mahdollisia järjestyksiä on siten $n \cdot (n-1) \cdots 2 \cdot 1 = n!$ kappaletta. (Luetaan *n-kertoma*.)

Lause 4. *Jos $\#S = n$, voidaan joukon S alkiot kirjoittaa $n!$ erilaiseen järjestykseen, ts. joukon S permutaatioita on $n!$ kappaletta.*

Jos joukosta S poimitaan p alkiota, voidaan ensimmäinen alkio valita n eri tavalla, toinen alkio tämän jälkeen $n-1$ eri tavalla jne. Viimeinen eli p:s alkio voidaan valita $n-(p-1)$ eri tavalla. Kaikkiaan voidaan siis saada $n \cdot (n-1) \cdots (n-p+1)$ erilaista p:n alkion pituista jonoa. Tähän määrään sisältyy kuitenkin jokainen samat p alkiota sisältävä jono kaikissa mahdollisissa järjestyksissä; jokaista p:n alkion valintaa kohden on siis $p!$ jonoa, jotka poikkeavat toisistaan vain alkioiden järjestyksen suhteen. Erilaisia p:n alkion muodostamia osajoukkoja on siten

$$\frac{n \cdot (n-1) \cdots (n-p+1)}{p!} = \frac{n!}{p!(n-p)!}$$

kappaletta. Luku

$$\binom{n}{p} = \frac{n!}{p!(n-p)!}$$

on *binomikerroin*; merkintä luetaan "*n yli p:n*".

Lause 5. *Jos $\#S = n$, voidaan joukon S alkioista muodostaa $\binom{n}{p}$ erilaista p:n alkion muodostamaa osajoukkoa.*

Luvut $\binom{n}{p}$ saadaan *Pascalin kolmiosta*. Seuraavassa annetaan kolmion seitsemän ensimmäistä riviä:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}$$

Pascalin (1623-62) kolmio julkaistiin Kiinassa v. 1303 ja oli tunnettu jo sitäkin aikaisemmin.

Laskemalla joukon S osajoukkojen lukumäärät sen mukaisesti, montako alkiota niissä on, saadaan tärkeä kaava

$$\sum_{p=0}^{n} \binom{n}{p} = 2^n.$$

Olkoon joukko S muodostettu yhdisteenä joukoista $S_1, ..., S_n : S = \bigcup_{k=1}^{n} S_k$. Jos $n = 2$ tai $n = 3$, saadaan joukon S alkioiden lukumäärä ilmeisesti kaavoista

$$\#S = \#S_1 + \#S_2 - \#(S_1 \cap S_2),$$

$$\#S = \#S_1 + \#S_2 + \#S_3 - \#(S_1 \cap S_2) - \#(S_2 \cap S_3) - \#(S_1 \cap S_3) + \#(S_1 \cap S_2 \cap S_3).$$

Tämä tulos yleistyy seuraavasti:

Lause 6. *Olkoon $S = \bigcup_{k=1}^{n} S_k$. Joukon S alkioiden lukumäärä on*

$$\#S = \sum_{1 \le k \le n} \#S_k - \sum_{1 \le j < k \le n} \#(S_j \cap S_k) + \sum_{1 \le i < j < k \le n} \#(S_i \cap S_j \cap S_k) - \cdots + (-1)^{n-1} \#(S_1 \cap \cdots \cap S_n).$$

Todistus perustuu induktioon.

Lause 7 (Binomikaava). *Olkoot x ja y reaalilukuja ja olkoon n luonnollinen luku. Tällöin*

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k},$$

missä

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

on binomikerroin. (Tässä $n! = 1 \cdot 2 \cdots n$ on n-kertoma; erityisesti asetetaan $0! = 1$.)

Todistus. Harj. □

Harjoitustehtäviä

1. Todista *binomikaava* eli Lause 7.
2. Laske termin x^6 kerroin polynomissa $(1 + x)^8$.
3. Todista, että

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1},$$

kun n ja k ovat positiivisia kokonaislukuja, $k \le n$.

4. Osoita, että
$$\binom{s-1}{0} + \binom{s}{1} + \cdots + \binom{s+n-2}{n-1} + \binom{s+n-1}{n} = \binom{s+n}{n},$$
kun s ja n ovat positiivisia kokonaislukuja.

5. Osoita, että
$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1},$$
kun n ja k ovat positiivisia kokonaislukuja, $n \geq k$.

6. Osoita, että
$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}, \quad \text{kun } n \geq r \geq k.$$

7. Laske termin $x^3y^4z^2$ kerroin polynomissa $(x+y+z)^9$.

II.4 Äärelliset joukot; lokeroperiaate

Tässä pykälässä käsitellään formaalisella tavalla äärellisiä joukkoja. Väitteet ovat intuitiivisesti ajatellen hyvin luonnollisia; todistuksia ei olekaan tarkoitettu opeteltaviksi.

Merkitään
$$J_n = \{1, ..., n\} = \{k \in \mathbb{N}_+ \mid k \leq n\} \qquad (n = 0, 1, 2, \dots),$$
jolloin $J_0 = \emptyset$.

MÄÄRITELMÄ. Joukko X on *äärellinen*, mikäli jollain luvulla $n \in \mathbb{N}$ on olemassa bijektio $J_n \to X$. Jos X ei ole äärellinen, niin sanotaan, että X on *ääretön*.

Koska bijektion käänteiskuvaus on bijektio, niin nähdään, että joukko X on äärellinen jos ja vain jos jollain luvulla $n \in \mathbb{N}$ on olemassa bijektio $X \to J_n$.

Annetun määritelmän nojalla tyhjä joukko on äärellinen.

Joukon äärellisyyttä voidaan havainnollisesti luonnehtia jonojen avulla.

Seuraavassa jonoa $(x_1, \dots, x_n)$ sanotaan *yksinkertaiseksi*, mikäli alkiot x_i ovat parittain erisuuret.

Asetetaan n:n alkion jonot vastaamaan kuvauksia joukolta J_n seuraavasti: jonoa $(x_1, \dots, x_n)$ vastaa kuvaus $J_n \to \{x_1, \dots, x_n\}$, $\quad i \mapsto x_i$, ja kääntäen kuvausta f joukolta J_n vastaa jono $(f(1), \dots, f(n))$. Tässä vastaavuudessa yksinkertaiset jonot ja bijektiiviset kuvaukset vastaavat toisiaan. Täten joukko X on äärellinen jos ja vain jos on olemassa yksinkertainen jono $(x_1, \dots, x_n)$, jolla $\{x_1, \dots, x_n\} = X$.

Todistetaan nyt induktioperiaatteen sovelluksena äärellisiä joukkoja koskevia alkeistuloksia.

Lemma 1. *Olkoon n luonnollinen luku. Millään sitä pienemmällä luonnollisella luvulla k ei ole olemassa surjektiota $J_k \to J_n$.*

Todistus. Merkitään $P(n)$:llä luonnollisen luvun n ominaisuutta: "Millään luonnollisella luvulla $k < n$ ei ole olemassa surjektiota $J_k \to J_n$."

1^o $P(0)$ pätee triviaalisti (ei ole olemassa luonnollista lukua < 0).

2^o Oletetaan, että $P(n)$ pätee. Todistetaan, että $P(n+1)$ on voimassa. Tehdään vastaoletus: on olemassa $k < n+1$ ja surjektio $f : J_k \to J_{n+1}$.

Koska $J_0 = \emptyset$, niin $k > 0$. Osoitetaan, että on olemassa surjektio $g : J_{k-1} \to J_n$. Jos $f(k) = n+1$, niin kuvaus

$$g : J_{k-1} \to J_n, \qquad g(i) = \min(f(i), n)$$

on surjektio. Oletetaan, että $f(k) \neq n+1$. Määritellään nyt $g : J_{k-1} \to J_n$ asettamalla $g(i) = f(i)$ jos $f(i) \neq n+1$ ja $g(i) = f(k)$ jos $f(i) = n+1$. Silloin g on surjektio. Vastaoletus johti siis ristiriitaan induktio-oletuksen kanssa. Täten $P(n+1)$ pätee. □

Lause 7. *Olkoon A äärellinen joukko. On vain yksi luonnollinen luku n, jolla bijektio $J_n \to A$ on olemassa.*

Todistus. Olkoot n ja k luonnollisia lukuja, joilla on olemassa bijektiot $f : J_n \to A$ ja $g : J_k \to A$. Osoitetaan, että $n = k$. Bijektioiden yhdistettyinä kuvauksina kuvaukset $g^{-1} \circ f : J_n \to J_k$ ja $f^{-1} \circ g : J_k \to J_n$ ovat bijektioita ja täten surjektioita. Lemman 1 tuloksesta seuraa, että $n \geq k$ ja $k \geq n$. Täten $n = k$. □

Olkoon A äärellinen joukko. Lauseen 7 antamasta yksikäsitteisestä luvusta n käytetään merkintää $\#A$ ("A:n *alkioiden lukumäärä*" tai "A:n *koko*"). Kun $\#A = n > 0$, niin A voidaan esittää muodossa $A = \{a_1, \ldots, a_n\}$: asetetaan $a_i = \varphi(i)$ $\forall i \in J_n$, missä φ on bijektio $J_n \to A$.

Kun A on äärellinen joukko ja $\#A = n$, käytetään myös sanontaa, että A on *n-joukko*. Sekä merkintää "$\#B = n$" että sanontaa "B on n-joukko" käytetään seuraavassa lyhennyksenä sanonnalle "B on äärellinen joukko ja n on luonnollinen luku, jolla on voimassa $\#B = n$".

Ainoa 0-joukko on tyhjä joukko. Koska joukon identtinen kuvaus on aina bijektio joukolta itselleen, niin aina $\#J_n = n$.

Seuraavaksi osoitetaan, että äärellisten joukkojen osajoukot ovat äärellisiä. Todistetaan tämä ensin joukkojen J_n, $n \in \mathbb{N}$, osajoukoille.

Lemma 2. *Olkoon n luonnollinen luku ja olkoon A joukon J_n aito osajoukko. Tällöin jollain luonnollisella luvulla $k < n$ on olemassa bijektio $A \to J_k$.*

Todistus. Suoritetaan todistus induktiolla luvun n suhteen.

Väite on tosi arvolla $n = 0$, koska joukolla J_0 ei ole aitoja osajoukkoja.

Oletetaan, että väite pätee luvulla $n \in \mathbb{N}$ ja todistetaan se luvulla $n+1$. Olkoon A joukon J_{n+1} aito osajoukko. Merkitään $B = A \cap J_n$. Jos $B = J_n$, niin välttämättä $A = B$ ja väite pätee A:lla ja $(n+1)$:llä, kun valitaan $k = n$. Oletetaan, että B on J_n:n aito osajoukko. Induktio–oletuksen nojalla on olemassa $k < n$ ja bijektio $f : B \to J_k$. Jos $A = B$, niin väite on todistettu joukolle A. Oletetaan, että $B \neq A$. Tällöin $A = B \cup \{n+1\}$.

Nähdään helposti, että kuvaus $g : A \to J_{k+1}$, missä $g(i) = f(i)$ jokaisella $i \neq n+1$ ja $g(n+1) = k+1$, on bijektio. Ehdosta $k < n$ seuraa $k+1 < n+1$. On siis osoitettu, että väite pätee luvulla $n+1$. □

Lause 8. *Olkoon A äärellinen joukko ja olkoon B A:n aito osajoukko. Tällöin B on äärellinen ja $\#B < \#A$.*

Todistus. Koska A on äärellinen, niin on olemassa $n = \#A$ ja bijektio $f : A \to J_n$. Merkitään $C = f(B) = \{f(b) | b \in B\}$. Koska f on bijektio ja $B \subsetneq A$, niin $C \subsetneq J_n$. Lemman 2 nojalla on olemassa $k < n$ ja bijektio $g : C \to J_k$. Kuvaus $\varphi : B \to J_k, \quad \varphi(b) = g(f(b))$ on bijektio. Täten B on äärellinen ja $\#B = k < n = \#A$. □

Edellisten tulosten avulla voidaan luonnehtia $\mathbb{N}$:n osajoukkojen äärellisyyttä.

Lemma 3. *Olkoon $A \subset \mathbb{N}$ epätyhjä äärellinen joukko, $\#A = m$. Tällöin joukolla A on sellainen esitys $A = \{a_i : i \in J_m\}$, että $a_i < a_{i+1}$ aina kun $i \in J_{m-1}$.*

Todistus. Todistetaan lemman väite induktiolla luvun m suhteen. Merkitään a_1:llä joukon A pienintä alkiota min A. Jos $m = 1$, niin $A = \{a_1\}$ on haluttu esitys joukolle A. Oletetaan nyt, että $m > 1$ ja väite on todistettu kaikilla joukoilla $B \subset \mathbb{N}$, missä $\#B < m$. Merkitään $B = A \setminus \{a_1\}$. Tällöin B on A:n aito osajoukko, joten lauseen 8 nojalla joukko B on äärellinen ja $\#B < \#A = m$. Induktio-oletuksen nojalla on olemassa sellainen joukon B esitys $B = \{b_i | i \in J_k\}$, että $k = \#B$ ja $b_i < b_{i+1}$ aina kun $i \in J_{k-1}$. Merkitään $a_i = b_{i-1}$, kun $i = 2, \ldots, k+1$. Tällöin $B = \{a_2, \ldots, a_{k+1}\}$, joten $A = \{a_1\} \cup B = \{a_1, \ldots, a_{k+1}\}$. Lisäksi $a_i < a_{i+1}$ aina kun $i \in J_k$, joten $A = \{a_i : i \in J_{k+1}\}$ on haluttua muotoa oleva joukon A esitys. Kuvaus $i \mapsto a_i$ on bijektio $J_{k+1} \to A$, joten $k+1 = \#A = m$. □

Lause 9. *Joukon $\mathbb{N}$ osajoukko on äärellinen jos ja vain jos osajoukko on rajoitettu.*

Todistus. Välttämättömyys. Olkoon $A \subset \mathbb{N}$ äärellinen joukko. Jos $A = \emptyset$, niin A on rajoitettu. Oletetaan, että $A \neq \emptyset$. Lemman 3 nojalla A voidaan esittää muodossa $A = \{a_1, \ldots, a_m\}$ siten, että $a_i < a_{i+1}$ aina kun $i \in J_{m-1}$. Nyt a_m on A:n suurin luku, joten A on rajoitettu.

Riittävyys. Kuvaus $k \mapsto k+1$ on bijektio joukolta $\{0, \ldots, n\}$ joukolle J_{n+1}, joten joukko $\{0, \ldots, n\}$ on äärellinen ($n = 0, 1, 2, \ldots$). Lauseen 8 nojalla myös jokainen joukon $\{0, \ldots, n\}$ osajoukko on äärellinen. Rajoitettujen joukkojen äärellisyys seuraa edellisestä, sillä joukko $E \subset \mathbb{N}$ on rajoitettu jos ja vain jos on olemassa sellainen $n \in \mathbb{N}$, että $E \subset \{0, \ldots, n\}$. □

Äärellisiä joukkoja koskevia väitteitä todistetaan usein *induktiolla joukkojen koon suhteen.* Tällaiset induktiotodistukset ovat seuraavaa muotoa: Olkoon $\mathcal{B}$ jokin joukko, jonka alkiot ovat äärellisiä joukkoja, ja olkoon P joukon $\mathcal{B}$ alkioiden ominaisuus. Määritellään seuraava luonnollisten lukujen ominaisuus Q:

$$Q(n) \Leftrightarrow (\forall A \in \mathcal{B})\,(\#A = n \;\Rightarrow P(A))\,.$$

Jos voidaan todistaa induktiolla, että jokaisella luonnollisella luvulla on ominaisuus Q, niin tällöin päätellään, että jokaisella joukkoon $\mathcal{B}$ kuuluvalla joukolla on ominaisuus P.

Esimerkkinä induktiosta joukon koon suhteen osoitetaan, että äärellisen monen äärellisen joukon yhdiste on äärellinen. (Joukon $\mathbb{N}$ äärellisille osajoukoille tämä tulos seuraa helposti edellisen lauseen tuloksesta.)

Lause 10. *Äärellisen monen äärellisen joukon yhdiste on äärellinen.*

Todistus. Todistetaan lauseen tulos kahden äärellisen joukon tapauksessa; tästä voidaan helposti johtaa yleinen tulos induktiolla joukkojen lukumäärän suhteen.

Olkoot siis X ja Y äärellisiä joukkoja. Merkitään $\mathcal{P}(X) = \{A \mid A \subset X\}$. Lauseen 8 nojalla jokainen tämän parven joukko on äärellinen. Merkitään Q:lla seuraavaa luonnollisten lukujen ominaisuutta:

$$Q(n) \Leftrightarrow (\forall A \in \mathcal{P}(X))\,(\#A = n \;\Rightarrow\; \text{joukko } A \cup Y \text{ on äärellinen.})\,.$$

Osoitetaan induktiolla, että jokaisella luonnollisella luvulla on ominaisuus Q. Luvulla 0 on ominaisuus Q, sillä jos $\#A = 0$, niin $A = \emptyset$ ja $A \cup Y = Y$, joten joukko $A \cup Y$ on äärellinen. Olkoon nyt n sellainen luonnollinen luku, että jokaisella luonnollisella luvulla $k \leq n$ on ominaisuus Q. Osoitetaan, että myös luvulla $n+1$ on ominaisuus Q. Olkoon $A \in \mathcal{P}(X)$ sellainen joukko, että $\#A = n+1$. Osoitetaan, että joukko $A \cup Y$ on äärellinen. Koska $\#A = n+1 > 0$, niin $A \neq \emptyset$ ja täten on olemassa alkio $a \in A$. Joukko $B = A \setminus \{a\}$ kuuluu parveen $\mathcal{P}(X)$ ja lauseen 8 nojalla $\#B < \#A$. Induktio-oletuksen nojalla joukko $B \cup Y$ on äärellinen. Täten on olemassa $m \in \mathbb{N}$ ja bijektio $\varphi : J_m \to B \cup Y$. Määritellään kuvaus $\psi : J_{m+1} \to A \cup Y$ asettamalla $\psi(k) = \varphi(k)$, jos $k \leq m$, ja $\psi(m+1) = a$. Nähdään helposti, että kuvaus ψ on bijektio. Täten joukko $A \cup Y$ on äärellinen. On siis osoitettu, että luvulla $n+1$ on ominaisuus Q. Induktioperiaatteen nojalla seuraa, että jokaisella luonnollisella luvulla on ominaisuus Q. Erityisesti luvulla $\#X$ on tämä ominaisuus, joten joukko $X \cup Y$ on äärellinen. □

Lokeroperiaate

Tarkastellaan kahden äärellisen joukon välisten kuvausten vaikutusta joukkojen kokoihin.

Lause 11. *Olkoot A ja B joukkoja, joiden välillä on bijektio $A \to B$. Jos joko A tai B on äärellinen, niin tällöin sekä A että B ovat äärellisiä ja $\#A = \#B$.*

Todistus. Olkoon f bijektio $A \to B$.

Oletetaan, että joukko A on äärellinen. Tällöin on olemassa $n \in \mathbb{N}$ ja bijektio $\varphi : J_n \to A$. Yhdistetty kuvaus $f \circ \varphi$ on bijektio $J_n \to B$. Täten B on äärellinen ja $\#B = n = \#A$.

Koska kuvaus f^{-1} on bijektio $B \to A$, niin edellä esitetystä seuraa, että jos B on äärellinen, myös A on äärellinen ja $\#A = \#B$. □

Jos f on injektio joukolta A joukkoon B, niin tällöin f on bijektio joukolta A joukon B osajoukolle $f(A)$. Osoitetaan nyt, että joukkojen A ja B ollessa äärellisiä jokaisella surjektiolla $f : A \to B$ on rajoittuma, joka on bijektio joukolle B.

Lemma 4. *Olkoon A äärellinen joukko ja olkoon f surjektio joukolta A joukolle B. Tällöin on olemassa sellainen A:n osajoukko C, että kuvaus $f|_C$ on bijektio $C \to B$.*

Todistus. Merkitään $n = \#A$ ja esitetään joukko A muodossa $A = \{a_i \mid i \in J_n\}$. Kullakin joukon B alkiolla b merkitään $k(b)$:llä epätyhjän joukon $\{i \in J_n | f(a_i) = b\} \subset \mathbb{N}$ pienintä lukua. Merkitään edelleen $C = \{a_{k(b)} | b \in B\}$ ja $g = f|_C$. Kuvaus g on surjektio $C \to B$, koska $a_{k(b)} \in C$ ja $g(a_{k(b)}) = f(a_{k(b)}) = b$ aina kun $b \in B$. Kuvaus g on myös injektio. Jos nimittäin a ja a' ovat joukon C kaksi eri alkiota, niin on olemassa sellaiset joukon B alkiot b ja b', että $a = a_{k(b)}$ ja $a' = a_{k(b')}$. Silloin $g(a) = f(a) = b$ ja $g(a') = f(a') = b'$ ja lisäksi $b \neq b'$. □

Lause 12. *Olkoot A ja B joukkoja ja olkoon f kuvaus $A \to B$.*
(a) Jos A on äärellinen ja f on surjektio, niin B on äärellinen ja $\#A \geq \#B$.
(b) Jos B on äärellinen ja f on injektio, niin A on äärellinen ja $\#A \leq \#B$.

Todistus. (a) Oletetaan, että A on äärellinen ja f on surjektio. Lemman 4 nojalla on olemassa sellainen joukko $C \subset A$, että kuvaus $f|_C$ on bijektio $C \to B$. Lauseen 8 nojalla joukko C on äärellinen ja $\#C \leq \#A$. Lauseen 11 tuloksesta seuraa nyt, että joukko B on äärellinen ja $\#B = \#C \leq \#A$.

(b) Oletetaan, että B on äärellinen ja f on injektio. Lauseen 8 nojalla joukon B osajoukko $f(A)$ on äärellinen ja $\#f(A) \leq \#B$. Koska f on bijektio $A \to f(A)$, niin Lauseen 10 tuloksesta seuraa, että joukko A on äärellinen ja $\#A = \#f(A) \leq \#B$. □

Osoitetaan, että edellisen lauseen epäyhtälöissä pätee yhtäsuuruus ainoastaan siinä tapauksessa, että kuvaus f on bijektio.

Lause 13. *Olkoot A ja B äärellisiä joukkoja ja olkoon f kuvaus $A \to B$. Oletetaan, että $\#A = \#B$. Tällöin seuraavat ehdot ovat keskenään yhtäpitävät:*
A. f on surjektio;
B. f on injektio;
C. f on bijektio.

Todistus. Koska f on bijektio jos ja vain jos f on sekä surjektio että injektio, niin lauseen todistamiseksi riittää näyttää, että A⇒C ja B⇒C.

A⇒C: Oletetaan, että f on surjektio. Osoitetaan, että tällöin f on injektio. Lemman 4 nojalla on olemassa sellainen joukko $C \subset A$, että kuvaus $f|_C$ on bijektio $C \to B$. Lauseen 11 nojalla joukko C on äärellinen ja $\#C = \#B$. Koska $C \subset A$ ja $\#C = \#B = \#A$, niin Lauseen 8 tuloksesta seuraa, että $C = A$. Edellä esitetyn nojalla kuvaus $f|_A$, eli kuvaus f, on bijektio.

B⇒C: Oletetaan, että f on injektio. Tällöin f on bijektio $A \to f(A)$ ja lauseiden 11 ja 8 tuloksista seuraa kuten todistuksen edellisessä osassa, että tässä tapauksessa on voimassa $f(A) = B$. Täten f on bijektio. □

Seuraava tulos osoittaa, että kahden äärellisen joukon kokoja voidaan vertailla kuvausten avulla.

Lause 14. *Olkoot X ja Y äärellisiä joukkoja, $Y \neq \emptyset$.*
(a) $\#X \leq \#Y$ jos ja vain jos on olemassa injektio $X \to Y$.
(b) $\#X \geq \#Y$ jos ja vain jos on olemassa surjektio $X \to Y$.
(c) $\#X = \#Y$ jos ja vain jos on olemassa bijektio $X \to Y$.

Todistus. Merkitään $n = \#X$ ja $m = \#Y$. Olkoot kuvaukset $f : X \to J_n$ ja $g : Y \to J_m$ bijektioita.

(a) Jos $n \leq m$, niin $g^{-1} \circ f$ on injektio $X \to Y$.

Jos on olemassa injektio $X \to Y$, niin lauseen 12 nojalla $n \leq m$.

(b) Jos $n \geq m$, niin seuraava kuvaus $h : X \to Y$ on surjektio: $h(x) = g^{-1}(f(x))$, jos $f(x) \in J_m$, ja $h(x) = g^{-1}(m)$, jos $f(x) \notin J_m$.

Jos on olemassa surjektio $X \to Y$, niin lauseen 12 nojalla $n \geq m$.

(c) Jos $n = m$, niin kuvaus $g^{-1} \circ f$ on bijektio $X \to Y$.

Jos on olemassa bijektio $X \to Y$, niin lauseen 11 nojalla $n = m$. □

Seuraus (Lokeroperiaate). *Jos X ja Y ovat äärellisiä joukkoja ja $\#X > \#Y$ sekä jos f on kuvaus $X \to Y$, niin joukossa X on sellaiset alkiot x, z, että $x \neq z$ ja $f(x) = f(z)$.*

Todistus. Muutoin f olisi injektio ja siis $\#X \leq \#Y$. □

Lokeroperiaatteen tulkinta: Jos "esineitä" on enemmän kuin "lokeroita", niin jossain lokerossa on välttämättä ainakin kaksi esinettä (siis X = esineiden joukko, Y = lokeroiden joukko, f = esineiden sijoittaminen lokeroihin).

Esimerkki 1. Näytetään, että jokaisessa ihmisjoukossa X ($\#X \geq 2$) on ainakin kahdella henkilöllä sama määrä tuttavia joukossa X (tuttavuus ymmärretään molemminpuoliseksi).

Merkitään $\#X = n$. Määritellään

$$f : X \to \{0, 1, \ldots, n-1\}, \quad f(x) = \#\{y \in X \mid y \text{ on } x\text{:n tuttava}\}.$$

Nyt joko $0 \notin f(X)$ tai $n-1 \notin f(X)$ ("jos joku on kaikkien tuttava, niin jokaisella on joku tuttava"). Täten $\#f(X) \leq n-1 < \#X$. Lokeroperiaatteen nojalla on sellaiset $x \neq y$, että $f(x) = f(y)$.

Esimerkki 2. Olkoon $A \subset \mathbb{N}$ äärellinen joukko ja olkoon $n \in \mathbb{N}^*$, $\quad n < \#A$. Todistetaan, että on sellaiset $a, b \in A$, että $a \neq b$ ja $a - b$ on jaollinen n:llä.

Olkoon $a \in A$. Kokonaislukujen jakoyhtälön nojalla on sellaiset $q_a, r_a \in \mathbb{N}$, että

$$a = q_a \cdot n + r_a, \qquad 0 \leq r_a < n.$$

Koska $\#\{0, 1, \ldots, n-1\} = n < \#A$, niin lokeroperiaatteen nojalla on olemassa sellaiset A:n alkiot a ja b, että $a \neq b$ ja $r_a = r_b$. Nyt

$$a - b = q_a \cdot n + r_a - q_b \cdot n - r_b = (q_a - q_b) \cdot n,$$

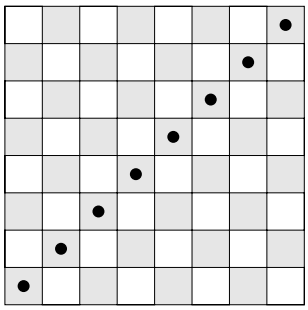
joten $a - b$ on jaollinen n:llä.

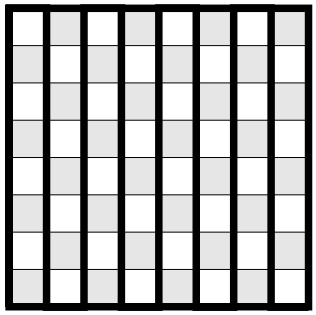
Esimerkki 3. Mikä on suurin määrä torneja, jotka voidaan sijoittaa yhtaikaa shakkilaudan eri ruuduille ilman, että mitkään kaksi tornia uhkaavat toisiaan?

Ratkaisu: Jos kaksi eri ruudussa olevaa tornia uhkaavat toisiaan, niin ne ovat joko samalla ruutujen muodostamalla "vaakarivillä" tai samalla "pystyrivillä". Sijoittamalla torni jommankumman "lävistäjän" jokaiseen ruutuun, kuten alla vasemmanpuoleisessa kuvassa, saadaan vaaditulla tavalla sijoitetuksi *kahdeksan* tornia.

Osoitetaan, että kahdeksan onkin suurin mahdollinen määrä. Jaetaan laudan ruudukko oikeanpuoleisen kuvan mukaisesti kahdeksaan "lokeroon". Jos yhteen lokeroon tulee

useampi kuin yksi torni, niin lokerossa on kaksi tornia, joiden ”välissä” ei ole kolmatta, ja tällöin nämä kaksi uhkaavat toisiaan. Täten jokaiseen lokeroon voidaan sijoittaa enintään yksi torni ja siis torneja voidaan sijoittaa yhteensä enintään kahdeksan.





Harjoitustehtäviä

1. Olkoon A mielivaltainen 101 kokonaislukua sisältävä joukko. Osoita, että A:sta löytyy kaksi (eri) lukua, joiden erotus on jaollinen 100:lla.
2. Olkoot A ja B äärellisiä ja pistevieraita. Osoita, että $\#(A \cup B) = \#A + \#B$. (Ohje: induktio $\#B$:n suhteen.)
3. Olkoot A ja B äärellisiä. Osoita, että $\#(A \times B) = \#A \cdot \#B$.

II.5 Joukkojen mahtavuus

Jos on olemassa bijektio $p : A \to B$ ja joukossa A on äärellisen monta alkiota, on joukossa B yhtä monta alkiota. Seuraavassa tämä yleistetään koskemaan myös äärettömän monen alkion joukkoja.

MÄÄRITELMÄ. Olkoot A ja B joukkoja. Jos on olemassa bijektio $p : A \to B$, ovat joukot A ja B *yhtä mahtavat*. Tällöin merkitään $A \approx B$. Lauseen 12 mukaisesti merkitään $A \leq B$, jos on olemassa injektio $A \to B$.

Äärellisen monen alkion joukoista yhtä mahtavia ovat ne, joissa on sama määrä alkioita. Joukkoa, joka on yhtä mahtava kuin luonnollisten lukujen joukko $\mathbb{N}$, sanotaan *numeroituvaksi*. Jokaista numeroituvan joukon alkiota vastaa em. bijektiossa jokin luonnollinen luku ja alkiot voidaan siis järjestää jonoon luonnollisten lukujen suuruusjärjestyksen mukaisesti. Kääntäen joukko voidaan osoittaa numeroituvaksi "järjestämällä sen alkiot jonoon".

ESIMERKKI 1. Osoitetaan, että parillisten luonnollisten lukujen joukko, kaikkien kokonaislukujen joukko ja rationaalilukujen joukko ovat numeroituvia.

Parillisten luonnollisten lukujen tapauksessa tarvittava bijektio voidaan määritellä asettamalla $n \mapsto 2n,\ n \in \mathbb{N}$. Jono on siten $0,\ 2,\ 4,\ 6,\ 8, \ldots$ Mahtavuuskäsitteen mielessä siis luonnollisia lukuja ja parillisia luonnollisia lukuja on yhtä paljon.

Kaikkien kokonaislukujen joukko voidaan järjestää jonoon seuraavasti:

$$0,\ -1,\ 1,\ -2,\ 2,\ -3,\ 3, \ldots$$

Bijektio luonnollisten lukujen joukkoon saadaan asettamalla kokonaisluvun kuvaksi sen paikkaa tässä jonossa osoittava järjestysluku.

Positiiviset rationaaliluvut voidaan kirjoittaa muotoon $\frac{p}{q},\ p, q \in \mathbb{N} \setminus \{0\}$. Nämä voidaan järjestää jonoksi keräämällä ensin ne luvut, joissa $p + q = 2$, sitten luvut, joissa $p + q = 3$, jne. Tällöin saadaan jono, joka alkaa seuraavasti:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \frac{1}{5}, \frac{2}{4}, \cdots$$

Jonosta on tämän jälkeen poistettava saman luvun eri esitykset; jokainen rationaaliluku esiintyy nimittäin jonossa myös kaikissa lavennetuissa muodoissaan. Tuloksena saadaan jono, jossa jokainen positiivinen rationaaliluku esiintyy täsmälleen kerran. Kaikki rationaaliluvut voidaan tämän jälkeen järjestää jonoon lomittamalla positiiviset ja negatiiviset rationaaliluvut samalla tavalla kuin kokonaislukuja koskevassa esimerkissä.

ESIMERKKI 2. Näytetään, että reaalilukujoukko ei ole numeroituva.

Rajoitutaan tarkastelemaan puoliavoimen välin $(0,1]$ reaalilukuja. Pidetään tunnettuna, että jokaisella reaaliluvulla on päättymätön desimaaliesitys; jos desimaaliesitys muodostuu äärellisen monesta desimaalista, siitä saadaan päättymätön lisäämällä loppuun nollia. Toisaalta jokainen muotoa $0, xxxx\ldots$ oleva desimaaliesitys vastaa jotakin välin $(0,1]$ reaalilukua.

Desimaaliesitys ei ole yksikäsitteinen, koska esim. $0,1 = 0,099\ldots$. Siitä saadaan tarvittaessa yksikäsitteinen sulkemalla pois ne desimaaliesitykset, jotka ovat jostain kohdasta alkaen muotoa $99\ldots$. Tehdään näin seuraavassa tarkastelussa.

Jos välin $(0,1]$ reaaliluvut muodostavat numeroituvan joukon, ne voidaan järjestää jonoon. Muodostetaan tämän jonon avulla uusi desimaaliesitys, jossa

$$k\text{:s desimaali } = \begin{cases} 2, \text{ jos jonon } k\text{:nnen luvun } k\text{:s desimaali} = 1, \\ 1, \text{ jos jonon } k\text{:nnen luvun } k\text{:s desimaali} \neq 1. \end{cases}$$

Uusi desimaaliesitys esittää välin $(0,1]$ reaalilukua, mutta se ei ole mikään jonon luku. Tämä on ristiriita; siis välin $(0,1]$ reaalilukuja ei voida järjestää jonoon.

Koko reaalilukujoukko ja välin $(0,1]$ reaaliluvut muodostavat yhtä mahtavat joukot. Tarvittava bijektio on helposti löydettävissä.

Harjoitustehtäviä

1. Olkoon X äärellinen joukko, $A \subset X$ ja olkoon $\mathcal{P}_A(X) = \{B \in \mathcal{P}(X) \mid A \subset B\}$. Mikä on joukon $\mathcal{P}_A(X)$ mahtavuus?
2. Olkoot $A,\ B,\ C$ joukkoja. Todista:
$$A \leq B \ \wedge \ B \leq C \ \Rightarrow \ A \leq C.$$
3. Todista: Jos $B \neq \emptyset$, niin $A \leq A \times B$.
4. Konstruoi esimerkki joukoista $A,\ B,\ C,\ D$, joilla $A \approx B$ ja $C \approx D$ mutta $A \cap C \not\approx B \cap D$ ja $A \cup C \not\approx B \cup D$.
5. Olkoot A ja B numeroituvia. Osoita, että $A \cup B$ on numeroituva.
6. Joukot $E_n,\ n = 1, 2, \ldots$ ovat numeroituvia. Osoita, että $\bigcup_{n=1}^{\infty} E_n$ on numeroituva.
7. Osoita, että numeroituvan joukon ääretön osajoukko on numeroituva.
8. Indeksoi eli "aseta jonoon" kokonaiskertoimisten 1. asteen polynomien joukko.

9. Osoita, että joukko $\{x \in \mathbb{R} \mid 0 < x < \epsilon\}$ on yhtä mahtava kuin $\mathbb{R}$, olipa $\epsilon > 0$ mikä tahansa.

10. Olkoon $A \subset B$. Osoita, että jos A on yhtä mahtava aidon osajoukkonsa kanssa, niin myös B on yhtä mahtava aidon osajoukkonsa kanssa.

11. Olkoot A ja B epätyhjiä joukkoja. Näytä, että $A \times B = B \times A \Leftrightarrow A = B$.

12. Olkoot $a, b, c, d \in \mathbb{R}$ sellaisia, että $a < b$ ja $c < d$. Näytä, että $[a, b] \approx (c, d]$.

Tehtävissä 13-16 A ja B ovat mielivaltaisia joukkoja. Todista:

13. $B \leq A$, jos on olemassa surjektio $A \to B$.

14. $A \times B \approx B \times A$.

15. $A \times B$ on ääretön, jos $B \neq \emptyset$ ja A on ääretön.

16. Näytä, että $\mathcal{P}(A) \approx \{0, 1\}^A$ kaikilla joukoilla A.
(Ohje: Tarkastele kuvausta $\psi : \{0, 1\}^A \to \mathcal{P}(A),\ f \mapsto f^{-1}\{1\}$.)

II.6 Ekvivalenssirelaatio ja ositus

Palautetaan mieleen, että kahden joukon A_1 ja A_2 *karteesinen tulo* $A_1 \times A_2$ tarkoittaa joukkoa, jonka muodostavat kaikki järjestetyt parit (a_1, a_2), missä $a_1 \in A_1$ ja $a_2 \in A_2$. Karteesisesta tulosta $A \times A$ käytetään myös merkintää A^2.

Jokainen karteesisen tulon $A \times A$ osajoukko R määrittelee *relaation joukossa* A: Jos $(a, b) \in R$, sanotaan, että alkio a on relaatiossa R alkion b kanssa, ja merkitään lyhyesti $a\ R\ b$. Matemaattisesti mielenkiintoiset relaatiot ovat yleensä sellaisia, joissa voidaan ilmoittaa jollain "säännöllä", milloin $a\ R\ b$. Relaatioksi R sanotaan usein myös (hiukan epätäsmällisesti) tätä sääntöä.

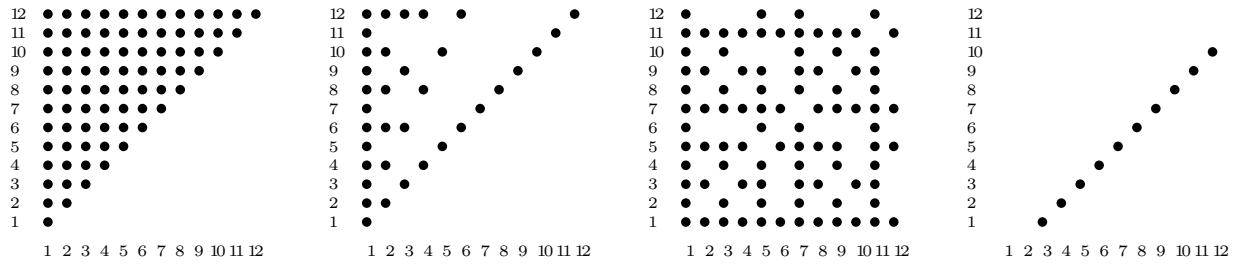
Esimerkki 1. Esimerkkejä erilaisista relaatioista.

(i) Joukossa $\mathbb{R}^2$: pisteen (x_1, y_1) etäisyys pisteestä (x_2, y_2) on kokonaisluku.

(ii) Joukossa $\mathbb{R}$: $x < y$.

(iii) Joukossa $\mathcal{M}_2(\mathbb{R})$ $(= 2 \times 2$ -matriisit $)$: $\det(AB) = 0$.

(iv) Kokonaisluvut x ja y voivat olla keskenään mm. seuraavissa relaatioissa: $x \leq y$, $x|y$, syt $(x, y) = 1$, $x = 2 + y$. Tapauksessa $A = \{1, ..., 12\}$ nämä vastaavat seuraavia joukon $A \times A$ osajoukkoja:



$x \leq y$ $x|y$ $\text{syt}(x, y) = 1$ $x = 2 + y$

Määritelmä. Relaatiota R joukossa A sanotaan A:n *ekvivalenssi(relaatio)ksi*, jos se täyttää seuraavat ehdot:

E1. $\forall\ a \in A:\quad a\ R\ a$ (*refleksiivisyys*),

E2. jos $a, b \in A$ ja $a\ R\ b$, niin $b\ R\ a$ (*symmetrisyys*),

E3. jos $a, b, c \in A$ ja $a\ R\ b$ ja $b\ R\ c$, niin $a\ R\ c$ (*transitiivisuus*).

Nämä ehdot voidaan esittää myös seuraavasti: kaikilla $a, b, c \in A$

$$(a,a) \in R,$$
$$(a,b) \in R \Rightarrow (b,a) \in R,$$
$$(a,b) \in R \quad \text{ja} \quad (b,c) \in R \quad \Rightarrow \quad (a,c) \in R.$$

Ekvivalenssirelaatiosta käytetään merkintää $\sim$. Jos $a \sim b$, sanotaan, että a on *ekvivalentti* b:n kanssa. Symmetrian nojalla voidaan myös sanoa: a ja b ovat ekvivalentit.

Esimerkki 2. Tutkitaan, onko esimerkin 1 relaatioilla ominaisuuksia E1, E2, E3.

Esimerkki 3. Jokaisen joukon triviaali ekvivalenssirelaatio: $a = b$.

Esimerkki 4. Tason kaikkien suorien joukossa relaatio $L_1 \parallel L_2$ on ekvivalenssi.

Esimerkki 5. Luvussa I.2 määritelty kongruenssi $\pmod m$ on joukon $\mathbb{Z}$ ekvivalenssirelaatio.

Määritelmä. Olkoon $\sim$ joukon A ekvivalenssirelaatio. Kunkin alkion $a \in A$ kanssa ekvivalentit alkiot muodostavat A:n osajoukon, jota sanotaan alkion a *ekvivalenssiluokaksi* ja merkitään $[a]$:lla; siis

$$[a] = \left\{ b \in A \;\middle|\; b \sim a \right\}.$$

Alkiota a sanotaan ekvivalenssiluokan $[a]$ *edustajaksi*.

Jokainen ekvivalenssiluokka muodostuu keskenään ekvivalenteista alkioista, ts.

$$a \text{ ja } b \text{ kuuluvat samaan ekvivalenssiluokkaan} \qquad \Longleftrightarrow \qquad a \sim b.$$

Jos nimittäin ensiksikin $a \sim b$, niin $b \in [a]$ ja (E1:n nojalla) $a \in [a]$. Jos kääntäen a ja b kuuluvat luokkaan $[c]$, niin $a \sim c$ ja $b \sim c$, siis E2:n ja E3:n nojalla $a \sim b$.

Lause 15. *Jos $\sim$ on joukon A ekvivalenssirelaatio, niin A voidaan esittää erillisten ekvivalenssiluokkien unionina:*

$$A = \bigcup_{a \in D} [a] \qquad ([a] \cap [a'] = \emptyset \quad \forall \; a, a' \in D, \; a \neq a'),$$

missä D on A:n osajoukko, joka sisältää tarkalleen yhden edustajan jokaisesta ekvivalenssiluokasta, ns. ekvivalenssiluokkien edustajisto.

Todistus. On näytettävä, että kun $a, b \in A$, niin joko $[a] = [b]$ tai $[a] \cap [b] = \emptyset$.

Oletetaan, että $[a] \cap [b] \neq \emptyset$. Silloin jokin joukon A alkio c kuuluu luokkiin $[a]$ ja $[b]$, siis $c \sim a$ ja $c \sim b$. Kuten yllä tästä seuraa

$$a \sim b.$$

Olkoon nyt x mielivaltainen luokan $[a]$ alkio. Tällöin $x \sim a$. Yhdessä juuri saadun tuloksen kanssa tämä antaa E3:n nojalla $x \sim b$, siis $x \in [b]$. Näin on todistettu, että $[a] \subset [b]$. Symmetrian nojalla myös $[b] \subset [a]$. Näistä seuraa yhtäsuuruus $[a] = [b]$. □

Jos joukko A on erillisten epätyhjien osajoukkojensa unioni, sanotaan, että nämä osajoukot muodostavat A:n *osituksen* eli *partition*. Tätä termiä käyttäen lause 1 voidaan siis muotoilla näin: *Jos joukossa A on määritelty ekvivalenssirelaatio, niin ekvivalenssiluokat muodostavat A:n osituksen.*

Kaikkien ekvivalenssiluokkien joukkoa (eli "parvea"; parvi = perhe = joukkojen joukko) sanotaan A:n *osamäärä-* tai *tekijäjoukoksi*. Sitä merkitään symbolilla $A/\!\sim$; siis

$$A/\!\sim = \big\{\ [a]\ \big|\ a \in A\big\} = \big\{\ [a]\ \big|\ a \in D\big\}\,.$$

Esimerkki 6. Katsotaan, millaisia ovat ekvivalenssirelaatioiden antamat ositukset esimerkeissä 3, 4 ja 5.

Esimerkkejä joukon $A(\neq \emptyset)$ osituksista:

(a) $\mathcal{B} = \{A\}$,
(b) $\mathcal{B} = \big\{\{a\}\ \big|\ a \in A\big\}$,
(c) $\mathcal{B} = \{B, A \setminus B\}$, kun $\emptyset \neq B \subsetneq A$.

Lause 16. *Jos $f : A \to E$ on kuvaus, niin joukko*

$$\mathcal{O}_f = \big\{\ f^{-1}\{e\}\ \big|\ e \in f(A)\big\}$$

on A:n ositus.

Kääntäen jokainen A:n ositus voidaan muodostaa tällä tavalla.

Todistus. Triviaalisti $f^{-1}\{e\} \neq \emptyset$ jokaisella alkiolla $e \in f(A)$. Jokainen $a \in A$ kuuluu täsmälleen yhteen perheen $\mathcal{O}_f$ joukkoon, nimittäin joukkoon $f^{-1}\{f(a)\}$. Täten $\mathcal{O}_f$ on A:n ositus.

Kääntäen olkoon $\mathcal{O}$ A:n ositus. Tällöin voidaan määritellä kuvaus $g : A \to \mathcal{O}$ asettamalla $g(a) = O$, kun $a \in O \in \mathcal{O}$. Kuvaus g on surjektio, ja jokainen $O \in \mathcal{O}$ täyttää ehdon $O = g^{-1}\{O\}$. Näin ollen $\mathcal{O} = \mathcal{O}_g$. □

Todistuksessa määriteltyä kuvausta g sanotaan *kanoniseksi surjektioksi* $A \to \mathcal{O}$.

Lause 17. *Jos $\mathcal{O}$ on joukon X ositus, niin relaatio*

$$E_{\mathcal{O}} = \{(x, y) \in X \times X \mid \exists O \in \mathcal{O} : \quad x \in O \text{ ja } y \in O\}$$

on ekvivalenssirelaatio.

Todistus. Olkoon $f : X \to \mathcal{O}$ kanoninen surjektio, siis $f(x) = O \Leftrightarrow x \in O$, missä $O \in \mathcal{O}$ on mielivaltainen. Ehto $(x, y) \in E_{\mathcal{O}}$ on siis yhtäpitävä ehdon $f(x) = f(y)$ kanssa. Täten kaikilla joukon X alkioilla x, y, z

$$\begin{aligned} &f(x) = f(x); \\ &f(x) = f(y) \quad \Rightarrow \quad f(y) = f(x); \\ &f(x) = f(y) \quad \text{ja} \quad f(y) = f(z) \quad \Rightarrow \quad f(x) = f(z). \end{aligned}$$

□

Harjoitustehtäviä

1. Luettele joukon $\{a, b, c, d\}$ kaikki ositukset.
2. Osoita, että n-joukolla, missä $n \neq 0$, on täsmälleen $2^{n-1} - 1$ kaksiosaista ositusta.
3. Tarkoittakoon merkintä xRy, että
   a) x on y:n isä,
   b) x on y:n ystävä,
   c) x on y:n jälkeläinen.
   Onko relaatio R refleksiivinen, symmetrinen, transitiivinen?
4. Mitkä seuraavista joukon $\mathbb{N}_+$ alkioiden x ja y välisistä relaatioista ovat refleksiivisiä, symmetrisiä tai transitiivisia:
   a) "$x + y$ on parillinen".
   b) $x - y < 10$.
   c) "xy on pariton".
5. Määritellään joukossa $\mathbb{R} \times \mathbb{R}$ relaatio S:
   $$(x, y)S(x', y') \Leftrightarrow x^2 + y^2 = x'^2 + y'^2.$$
   Näytä, että tämä on ekvivalenssirelaatio, ja tulkitse geometrisesti sen ekvivalenssiluokat.
6. Kokonaislukujen joukossa määritellään relaatio $m \sim n$, jos on olemassa sellaiset kokonaisluvut $p \neq 0$ ja $q \neq 0$, että $p^2 m = q^2 n$. Osoita, että relaatio on ekvivalenssi.
7. Mitkä ehtojen i), ii), iii) määrittelemistä kolmesta joukon $\mathbb{R}^2$ relaatiosta R ovat ekvivalensseja?

$(a,b)R(c,d) \Leftrightarrow$

i) $|a-c|+|b-d| \leq 1$,
ii) $(a=c)$ ja $(\sin b = \sin d)$,
iii) $(a=b)$ ja $(\sin c = \sin d)$

$(a,b,c,d \in \mathbb{R})$. Perustelu! Määritä alkioiden $(x,y) \in \mathbb{R}^2$ ekvivalenssiluokat, kun R on ekvivalenssi.

8. Laske joukon $\{1,2,3\}$ ekvivalenssien lukumäärä. (Ohje: Ositukset.)

9. Osoita, että relaatio
$$(a,b) \sim (c,d) \Leftrightarrow a+d = b+c$$
on joukon $\mathbb{N} \times \mathbb{N}$ ekvivalenssirelaatio.

Parin (m,n) ekvivalenssiluokkaa $[m,n]$ sanotaan *kokonaisluvuksi*. Näin saadaan $\mathbb{Z}$ muodossa $\mathbb{N} \times \mathbb{N}/\sim$.

10. Kokonaislukujen joukossa $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$ (ks. edellinen esim.) määritellään yhteenlasku
$$[m,n]+[p,q] = [m+p, n+q].$$
Osoita, ettei yhteenlaskun määrittely riipu käytetystä edustajasta, eli että $(m',n') \sim (m,n)$ ja $(p',q') \sim (p,q) \quad \Rightarrow \quad (m'+p', n'+q') \sim (m+p, n+q) \quad \Rightarrow \quad [m'+p', n'+q'] = [m+p, n+q]$.

11. Kokonaislukujen joukossa $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$ määritellään kertolasku kaavalla
$$[m,n] \cdot [p,q] = [mp+nq, mq+np].$$
Todista, ettei määritelmä riipu käytetyistä ekvivalenssiluokkien edustajista.

12. Todista, että $\sqrt{2}$ ei ole rationaaliluku.

13. Todista, että $\sqrt{5}$ ei ole rationaaliluku.

II.7 Järjestysrelaatio

Olkoon A joukko.

MÄÄRITELMÄ. Relaatiota $\leq$ joukossa A sanotaan A:n *osittaiseksi järjestykseksi* (partial ordering), jos se täyttää seuraavat ehdot:

J1. $\forall\ a \in A: \quad a \leq a \qquad$ *(refleksiivisyys)*,

J2. jos $a,b \in A$ ja $a \leq b$ ja $b \leq a$, niin $a = b \qquad$ *(antisymmetrisyys)*,

J3. jos $a, b, c \in A$ ja $a \leq b$ ja $b \leq c$, niin $a \leq c$ *(transitiivisuus).*

Jos lisäksi pätee

J4. $\forall\ a, b \in A:\quad a \leq b$ tai $b \leq a$ *(vertailtavuus)*,

relaatiota $\leq$ sanotaan *totaaliseksi (täydelliseksi, lineaariseksi) järjestykseksi* tai lyhyesti *järjestykseksi.*

Joukkoa A varustettuna tällaisella relaatiolla $\leq$ sanotaan vastaavasti *osittain järjestetyksi* tai *(totaalisesti, täydellisesti, lineaarisesti) järjestetyksi joukoksi.* Totaalisesti järjestettyä joukkoa sanotaan myös *ketjuksi.* (Englanninkielisessä kirjallisuudessa "order" voi tarkoittaa joko osittaista tai täydellistä järjestystä.)

Ehto $a \leq b$ voidaan lukea "a edeltää b:tä" tai "b seuraa a:ta". Huomaa, että postulaatin J1 mukaan jokainen alkio a edeltää (ja seuraa) itseään.

Esimerkki 1. Tavallinen suuruusrelaatio $x \leq y$ on totaalinen järjestys $\mathbb{R}$:ssä.

Esimerkki 2. Jaollisuusrelaatio $a \mid b$ on osittainen järjestys positiivisten kokonaislukujen joukossa $\mathbb{Z}_+$. (Miksei järjestys ole totaalinen? Miksei jaollisuusrelaatio ole osittainen järjestys $\mathbb{Z}$:ssa?)

Esimerkki 3. Sisältymisrelaatio $A \subset B$ on osittainen järjestys annetun joukon X kaikkien osajoukkojen parvessa $\mathcal{P}(X)$.

Huomaa, että jos $(A, \leq)$ on osittain (tai totaalisesti) järjestetty joukko, samoin on jokainen A:n osajoukko (relaation $\leq$ suhteen).

Harjoitustehtäviä

1. Olkoon $(X, \leq)$ osittain järjestetty joukko. Osoita, että $(X \times X, \leq)$ on osittain järjestetty joukko, kun siinä asetetaan

$$(x, y) \leq (x', y') \Leftrightarrow x \leq x' \text{ ja } y \leq y'.$$

   Onko $X \times X$ totaalisesti järjestetty, jos X on totaalisesti järjestetty joukko, jossa on vähintään kaksi alkiota?

2. Onko jaollisuusrelaatio $a|b$ osittainen järjestys luonnollisten lukujen joukossa $\mathbb{N}$?

3. Olkoot $(X_\nu, J_\nu)\quad (\nu = 1,\ 2;\ X_1 \neq \emptyset \neq X_2)$ järjestettyjä joukkoja, olkoon $X = X_1 \times X_2$ ja olkoon J X:n vastaava tulojärjestys:

$$(x_1, x_2) J (y_1, y_2) \Leftrightarrow (x_1 J_1 y_1) \text{ ja } (x_2 J_2 y_2)\ (x_\nu, y_\nu \in X_\nu;\ \nu = 1,\ 2).$$

   Näytä, että J voi olla totaalinen vain, kun X_1 tai X_2 on yhden alkion joukko (eli *yksiö*).

4. Olkoot ed. tehtävässä J_1 ja J_2 täydellisiä. Määritellään tulojoukolla X relaatio J:

$$(x_1, x_2)J(y_1, y_2) \Leftrightarrow (x_1 \neq y_1 \text{ ja } x_1 J_1 y_1) \text{ tai } (x_1 = y_1 \text{ ja } x_2 J_2 y_2),$$

missä $x_\nu, y_\nu \in X_\nu$ $(\nu = 1,\ 2)$. Osoita, että J on joukon X totaalinen järjestys ("sanakirjajärjestys").

III. RYHMÄ

III.1 Ryhmän käsite

Ryhmä on algebran peruskäsitteitä. Ryhmän käsitettä käytti jo Galois, mutta nykyinen määritelmä on pitkällisen kehityksen tulos. Johdantona ryhmän käsitteelle tarkastellaan ensin kahden lukujoukon ominaisuuksia ja kiteytetään näistä esille ryhmän määritelmä. Sen jälkeen esitetään esimerkkejä ryhmistä eri matematiikan aloilta. Ryhmäteoriaa käsitellään myös seuraavassa luvussa.

Tarkastellaan kokonaislukujen joukkoa $\mathbb{Z}$ ja reaalilukujen osajoukkoa $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Yhteisten ominaisuuksien korostamiseksi käytetään rinnakkaista taulukointia:

$\mathbb{Z}$, **laskutoimituksena** $+$	$\mathbb{R}^*$, **laskutoimituksena** $\cdot$
1. Vakaus laskutoimituksen suhteen:	
$b, c \in \mathbb{Z} \Rightarrow b + c \in \mathbb{Z}$.	$b, c \in \mathbb{R}^* \Rightarrow b \cdot c \in \mathbb{R}^*$.
2. Assosiatiivisuus eli liitännäisyys:	
Kaikilla $a, b, c \in \mathbb{Z}$ on $(a + b) + c = a + (b + c)$.	Kaikilla $a, b, c \in \mathbb{R}^*$ on $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Neutraalialkion olemassaolo:	
On olemassa $0 \in \mathbb{Z}$, jolla $0 + a = a + 0 = a \quad \forall a \in \mathbb{Z}$.	On olemassa $1 \in \mathbb{R}^*$, jolla $1 \cdot a = a \cdot 1 = a \quad \forall a \in \mathbb{R}^*$.
4. Käänteis/vasta-alkion olemassaolo:	
Jokaista lukua $a \in \mathbb{Z}$ vastaa $-a \in \mathbb{Z}$, jolla $a + (-a) = (-a) + a = 0$.	Jokaista lukua $a \in \mathbb{R}^*$ vastaa $a^{-1} \in \mathbb{R}^*$, jolla $a \cdot a^{-1} = a^{-1} \cdot a = 1$. (Merkitään myös $a^{-1} = 1/a$.)

Nämä eivät tietenkään ole ainoita ominaisuuksia, jotka ovat yhteisiä kokonaislukujen yhteenlaskulle ja nollasta poikkeavien reaalilukujen kertolaskulle. Nämä valitaan, koska ne tulevat esiin myös monissa muissa yhteyksissä.

Huomautus. Myös rationaalilukujen joukolla $\mathbb{Q}$ on kaikki ominaisuudet 1-4 yhteenlaskun suhteen, samoin reaalilukujen joukolla $\mathbb{R}$ ja kompleksilukujen joukolla $\mathbb{C}$. Samoin nämä ominaisuudet ovat voimassa, jos $\mathbb{Z}$ korvataan niiden x:n polynomien joukolla, joiden kertoimet ovat kokonaislukuja, tai yhtä hyvin rationaali-, reaali- tai kompleksilukuja (näitä joukkoja merkitään $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$).

Ominaisuus 4 ei päde kokonaislukujen kertolaskussa, koska ei ole olemassa kokonaislukua x, jolla esimerkiksi $3 \cdot x = 1$. Toisaalta esim. joukoilla $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ ja $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ on ominaisuudet 1-4 kertolaskun suhteen.

Tarkastellaan edellisiä ehtoja tarkemmin.

Kyseessä on joukko, $\mathbb{Z}$ tai $\mathbb{R}^*$, ja laskutoimitus eli tapa liittää joukon alkioparin kolmas alkio. Jos laskutoimitusta joukossa S merkitään $\circ$, voidaan kirjoittaa $s \circ s' = s''$, missä $s, s', s'' \in S$. Edellisessä esimerkissä laskutoimitus $\circ$ on $\mathbb{Z}$:n tapauksessa $+$, $\mathbb{R}^*$:n tapauksessa $\cdot$. Ominaisuus 2 kertoo, että laskutoimitus on liitännäinen.

Luetteloon ei ole otettu kommutatiivisuusehtoja $a + b = b + a$, $a \cdot b = b \cdot a$. Tämä on tehty tarkoituksella, koska ei haluta rajoittua ns. kommutatiivisiin ryhmiin.

Koska laskutoimituksen tulos saa riippua alkioparin keskinäisestä järjestyksestä, on alkioparin sijasta tarkasteltava *järjestettyä paria*, ts. paria, jossa alkioiden järjestys otetaan huomioon. Näin päädytään laskutoimituksen määritelmään:

MÄÄRITELMÄ. Joukon S laskutoimitus $\circ$ liittää jokaiseen järjestettyyn pariin S:n alkioita s, s' yksikäsitteisen S:n alkion s''.

Tämä voidaan kirjoittaa esim. seuraavilla tavoilla:

$$s \circ s' = s'' \qquad \text{tai} \qquad (s, s') \quad \overset{\circ}{\mapsto} \quad s''.$$

Tämä määritelmä voidaan sanoa lyhyesti myös näin: *Joukon S laskutoimitus on kuvaus $S \times S \to S$.*

Esitetään nyt ryhmän määritelmä:

MÄÄRITELMÄ. Olkoon G epätyhjä joukko. Paria $(G, \circ)$ sanotaan *ryhmäksi* (group), jos se täyttää seuraavat ehdot:

G0. $\circ$ on jokin joukon G laskutoimitus, ts. $a \circ b \in G \quad \forall\ a, b \in G$;

G1. $(a \circ b) \circ c = a \circ (b \circ c) \quad \forall\ a, b, c \in G \qquad$ (*liitäntälaki*);

G2. on olemassa sellainen G:n alkio e (ns. *neutraalialkio*), että

$$e \circ a = a \circ e = a \quad \forall\ a \in G;$$

G3. jokaista G:n alkiota a kohti on olemassa sellainen G:n alkio a^{-1} (ns. a:n *käänteisalkio*), että

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Jos laskutoimitus lisäksi on kommutatiivinen eli vaihdannainen, sanotaan että $(G, \circ)$ on *kommutatiivinen ryhmä* eli *Abelin ryhmä*; se täyttää siis ehdon

G4. $a \circ b = b \circ a \quad \forall\ a, b \in G \qquad$ (*vaihdantalaki*).

Jos $(G, \circ)$ on ryhmä, sanotaan myös lyhyesti, että G on ryhmä (laskutoimituksen $\circ$ suhteen).

Abelin ryhmän nimi johtuu norjalaisesta matemaatikosta Niels Henrik Abelista.

Esimerkki 1 (Lukuryhmät). Esim. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ovat Abelin ryhmiä yhteenlaskun suhteen. Neutraalialkiona on luku 0, luvun a käänteisalkiona vastaluku $-a$.

Merkitään

$$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \qquad \mathbb{R}^* = \mathbb{R} \setminus \{0\}, \qquad \mathbb{C}^* = \mathbb{C} \setminus \{0\}.$$

Nämä lukujoukot ovat Abelin ryhmiä kertolaskun suhteen. Neutraalialkiona on 1, luvun a käänteisalkiona käänteisluku $1/a$. (Mieti, mikseivät $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ole ryhmiä kertolaskun suhteen. Entä $\mathbb{Z}$ tai $\mathbb{Z} \setminus \{0\}$?)

Tarkastellaan seuraavaa viiden kohdan luetteloa, jossa on ryhmien $(\mathbb{Z}, +)$ ja $(\mathbb{R}^*, \cdot)$ yhteisiä ominaisuuksia:

1. Ryhmän neutraalialkio on yksikäsitteinen.

2. Ryhmässä on kullakin alkiolla täsmälleen yksi käänteis/vasta-alkio $\bar{a}$.

3. Jos a ja b ovat ryhmän alkioita, niin on olemassa yksikäsitteiset ryhmän alkiot x ja y, joilla $a \circ x = b$ ja $y \circ a = b$.

4. *Supistussäännöt* ovat voimassa:
   Jos $a \circ b = a \circ c$, niin $b = c$;
   jos $b \circ a = c \circ a$, niin $b = c$.

5. Alkion $a \circ b$ käänteisalkio/vasta-alkio on $\bar{b} \circ \bar{a}$.

Ryhmän $(\mathbb{Z}, +)$ tapauksessa ominaisuus 1 kertoo siis, että 0 on ainoa kokonaisluku z, jolla $z + a = a + z = a$ aina kun $a \in \mathbb{Z}$. Ominaisuuden 2 mukaan kullakin kokonaisluvulla z on täsmälleen yksi vastaluku $-z$. Ominaisuus 3 lausuu, että yhtälöt $a + x = b$ ja $y + a = b$ voidaan aina ratkaista $\mathbb{Z}$:ssa, olivatpa a ja b mitä kokonaislukuja tahansa.

Ominaisuus 4 sanoo, että yhtälöistä $a + b = a + c$ tai $b + a = c + a$ seuraa $b = c$. Ominaisuuden 5 mukaan luvun $a + b$ vastaluku on $(-b) + (-a)$.

Käy läpi vastaavasti tapaus $(\mathbb{R}, \cdot)$.

Kaikki mainitut viisi ominaisuutta voidaan johtaa ryhmän määritelmän ehdoista. Tämä merkitsee, että aina kun jokin joukko on todettu ryhmäksi (tietyllä laskutoimituksella varustettuna), niin myös ehdot 1-5 ovat voimassa. Seuraavassa näytetään, miten kohdat 1 ja 2 seuraavat ryhmän määritelmästä.

Lause 1. *Ryhmän G neutraalialkio on yksikäsitteinen, samoin kunkin alkion a käänteisalkio a^{-1}.*

Todistus. Jos myös e' on G:n neutraalialkio, niin G2 antaa $e' = e' \circ e = e$.

Jos alkiolla a on myös käänteisalkio a', niin operoimalla yhtälöön $a \circ a' = e$ vasemmalta a^{-1}:llä saadaan $(a^{-1} \circ a) \circ a' = a^{-1} \circ e$, siis $a' = a^{-1}$. (Tässä tarvittiin jokaista postulaateista G1, G2, G3 – mieti miten!) $\square$

Ryhmäteoriassa merkitään ryhmän G laskutoimitus $\circ$ yleensä kertolaskuna:

$$a \circ b = a \cdot b = ab.$$

Tällöin neutraalialkiota sanotaan myös *ykkösalkioksi* ja merkitään $e = 1 = 1_G$.

Joskus käytetään yhteenlaskumerkintää: $a \circ b = a + b$. Näin tehdään usein, jos G on Abelin ryhmä (ja tietenkin silloin, jos käsiteltävä ryhmätoimitus on "todellinen" yhteenlasku). Tässä tapauksessa neutraalialkiota sanotaan myös *nolla-alkioksi* ja merkitään $e = 0 = 0_G$. Alkion a käänteisalkiota a^{-1} sanotaan *vasta-alkioksi* ja merkitään $(-a)$:lla.

Käytetään myös sanontoja: $(G, \cdot)$ on *multiplikatiivinen ryhmä* ja $(G, +)$ on *additiivinen ryhmä*. Katso uudestaan esimerkkiä 1.

Ryhmän G alkioiden lukumäärää $\#G$ sanotaan G:n *kertaluvuksi* (order). (Kuten edellisessä luvussa, joukon S alkioiden lukumäärälle käytetään merkintää $\#S$; muita mahdollisia merkintöjä olisivat esim. $|S|$, $\mathrm{card}(S)$.)

Esimerkki 2 (Vektoriryhmät). Mielivaltaisen vektoriavaruuden V vektorit muodostavat additiivisen Abelin ryhmän, nolla-alkiona nollavektori 0 ja vektorin X vasta-alkio vastavektori $-X$.

Tällaisia ryhmiä ovat siis esimerkiksi $\mathbb{R}^n$ ja $\mathbb{C}^n$ $(n = 1, 2, \dots)$, $F(\mathbb{R})$ (= funktiot $\mathbb{R} \to \mathbb{R}$) sekä reaalikertoimisten polynomien joukko $\mathbb{R}[x]$.

Seuraavissa esimerkeissä tarvitaan matriisien laskutoimituksia. Ne on esitetty 2×2 -matriisien tapauksessa Liitteen 11 kohdassa III.1.

Esimerkki 3 (Matriisiryhmät). Matriisijoukko $\mathcal{M}_{m\times n}(\mathbb{R})$ on additiivinen Abelin ryhmä, nolla-alkiona nollamatriisi ja matriisin A vasta-alkiona $-A$. (Tämä ryhmä kuuluu myös esimerkin 2 kategoriaan.)

Esimerkki 4 Säännöllisten 2×2-matriisien joukko

$$GL_2(\mathbb{R}) = \left\{ A \in \mathcal{M}_2(\mathbb{R}) \;\middle|\; \det(A) \neq 0 \right\}$$

on multiplikatiivinen ryhmä, ykkösalkiona identiteettimatriisi I_2 ja matriisin A käänteisalkiona käänteismatriisi A^{-1}. Tämä ryhmä ei ole Abelin ryhmä.

Samoin määritellään yleisesti $GL_n(\mathbb{R})$. Sitä sanotaan *yleiseksi lineaariseksi ryhmäksi* (general linear group).

Esimerkki 5 (Jäännösluokkaryhmät). Jäännösluokat mod m muodostavat additiivisen Abelin ryhmän $(\mathbb{Z}_m, +)$, kun yhteenlasku määritellään pykälässä I.2 esitetyllä tavalla: $\overline{a} + \overline{b} = \overline{a + b}$. Nolla-alkiona on $\overline{0}$ ja alkion $\overline{a}$ vasta-alkiona $\overline{-a}$.

Tämä on esimerkki *äärellisestä* ryhmästä: $\#Z_m = m$.

Jos $\mathrm{syt}(a, m) = 1$, jäännösluokkaa $\overline{a}$ sanotaan *alkuluokaksi*. Huomaa, että tämä käsite on hyvinmääritelty, ts.

$$\mathrm{syt}(a, m) = 1, \quad \overline{a} = \overline{a'} \qquad \Longrightarrow \qquad \mathrm{syt}(a', m) = 1$$

(mieti perustelu). Kaikkien alkuluokkien mod m joukko

$$\mathbb{Z}_m^* = \big\{\, \overline{a} \in \mathbb{Z}_m \;\big|\; \mathrm{syt}(a,m) = 1 \big\}$$

on ryhmä jäännösluokkien kertolaskun $\overline{a}\cdot\overline{b} = \overline{ab}$ suhteen. Ykkösalkiona on jäännösluokka $\overline{1}$ ja alkion $\overline{a}$ käänteisalkiona se jäännösluokka $\overline{x}$, jossa x toteuttaa kongruenssin

$$ax \equiv 1 \pmod{m}$$

(ks. lause I.8); silloinhan nimittäin $\overline{a}\cdot\overline{x} = \overline{ax} = \overline{1}$.

Ryhmää $(\mathbb{Z}_m^*, \cdot)$ sanotaan *multiplikatiiviseksi jäännösluokkaryhmäksi* mod m. Merkitään

$$\#\mathbb{Z}_m^* = \varphi(m);$$

tätä m:n funktiota sanotaan *Eulerin φ-funktioksi* (engl. kirjallisuudessa usein $\varphi = \phi$).

Jos $p \in \mathbb{P}$, niin $\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$; siis $\varphi(p) = p - 1$.

Esim. $\mathbb{Z}_9^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$.

Esimerkki 6 (Permutaatioryhmät). Joukon $J_n = \{1, 2, \ldots, n\}$ *permutaatioksi* sanotaan bijektiivistä kuvausta $\alpha : J_n \to J_n$. Kun $\alpha(j) = k_j \quad \forall\ j \in J_n$, permutaatio α voidaan merkitä muodossa

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix},$$

missä siis $k_1, k_2, \ldots, k_n$ ovat luvut $1, 2, \ldots, n$ jossain järjestyksessä.

Kaikki joukon $\{1, 2, \ldots, n\}$ permutaatiot muodostavat ryhmän kuvaustulon suhteen, ns. n:n alkion *symmetrisen ryhmän*

$$S_n = \big\{\, \alpha : J_n \longrightarrow J_n \;\big|\; \alpha \text{ on bijektio } \big\}.$$

Ykkösalkiona on joukon J_n identiteettikuvaus ja permutaation α käänteisalkiona käänteiskuvaus α^{-1} (mieti myös G0 ja G1). Jos $n > 2$, S_n ei ole Abelin ryhmä.

Muista, että $\#S_n = n!$.

Tässä käyttöönotettu merkintätapa sopii hyvin permutaatioiden tulon laskemiseen. Esim. (huomaa järjestys)

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

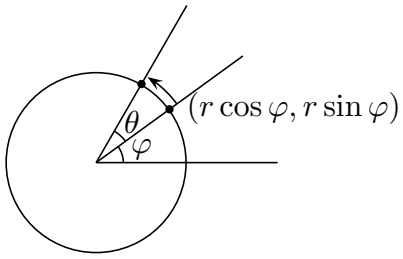
Esimerkki 7 (Kiertoryhmät). Tarkastellaan lineaarisia kuvauksia $\varrho_\theta : \mathbb{R}^2 \to \mathbb{R}^2$, joiden matriisit ovat muotoa

$$L_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Kirjoittamalla piste $(x_1, x_2) \in \mathbb{R}^2$ napakoordinaateilla muotoon $(r\cos\varphi, r\sin\varphi)$ nähdään, että

$$\varrho_\theta(x_1, x_2) = \big(r\cos(\varphi+\theta), r\sin(\varphi+\theta)\big);$$

täten ϱ_θ on kierto origon ympäri positiiviseen suuntaan kulman θ verran ($\theta > 0$).



Kuvausten ϱ_θ joukossa voidaan määritellä laskutoimitus yhdistämällä kuvaukset, jolloin tulokseksi saadaan $\varrho_{\theta_1} \circ \varrho_{\theta_2}$. Kertomalla näiden matriisit todetaan, että tämä on jälleen kierto, kulmana $\theta_1 + \theta_2$:

$$\varrho_{\theta_1} \circ \varrho_{\theta_2} = \varrho_{\theta_1+\theta_2}.$$

Identtisen kuvauksen matriisi on

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix},$$

joten $id = \varrho_0$. Kaava

$$\varrho_\theta \circ \varrho_{-\theta} = id = \varrho_{-\theta} \circ \varrho_\theta$$

kertoo, että kulman θ suuruinen kierto negatiiviseen suuntaan on kuvauksen ϱ_θ käänteisalkio (kierrot "kumoavat" toisensa).

Esimerkki 8 (Symmetriaryhmät). Ajatellaan xy-tasossa säännöllistä n-kulmiota "tasolevynä", jonka keskipiste on origossa. Tarkastellaan niitä tason kuvauksia (peilauksia suoran suhteen sekä kiertoja), jotka kuvaavat tämän n-kulmion itselleen. Ne muodostavat ryhmän kuvaustulon suhteen; sitä sanotaan ko. n-kulmion *symmetriaryhmäksi*) ja merkitään D_n:llä. Käytetään myös nimitystä *diedriryhmä.*

Esim. D_4 muodostuu neljästä kierrosta, kulmina 0, $\pi/2$, π ja $3\pi/2$, ja neljästä peilauksesta, akseleina neliön lävistäjät ja sivujen keskinormaalit, ks. IV.6.

Jos n-kulmion kärkiä merkitään numeroilla $1, 2, \ldots, n$, kukin D_n:n alkio voidaan esittää permutaationa $\alpha \in S_n$.

Symmetriaryhmän käsite voidaan yleistää myös useampiulotteisiin kappaleisiin. Nämä ryhmät ovat tärkeitä geometriassa (ja fysiikassa), jossa niillä luonnehditaan kappaleen symmetrisyyttä.

Huomautus. Paria $(G, \circ)$, joka täyttää ryhmän määritelmän postulaatit G0 ja G1 (siis "puolet" postulaateista), sanotaan *puoliryhmäksi.* Jos puoliryhmässä G lisäksi on neutraalialkio, ts. myös G2 on voimassa, niin G:tä sanotaan *monoidiksi.*

Esim. joukot $\mathbb{Z}$ ja $2\mathbb{Z}$ (= parilliset kokonaisluvut) ovat kertolaskun suhteen puoliryhmiä. Edellinen on lisäksi monoidi.

Puoliryhmien ja monoidien teoriaa ei käsitellä tässä kurssissa.

Harjoitustehtäviä

1. Mitkä seuraavista $\mathbb{Z}_{11}$:n osajoukoista ovat ryhmiä kertolaskun suhteen?
   a) $\{1_{11}, 3_{11}, 4_{11}, 5_{11}, 9_{11}\}$,
   b) $\{1_{11}, 3_{11}, 4_{11}, 5_{11}, 8_{11}\}$,
   c) $\{1_{11}, 10_{11}\}$.

2. Reaalilukujen joukossa määritellään laskutoimitus asettamalla

$$x * y = \text{ suurempi luvuista } x \text{ ja } y.$$

   Osoita, että laskutoimitus on liitännäinen.

3. Osoita, että kokonaislukujen vähennyslasku ei ole liitännäinen.

4. Osoita, että $(m, n) \mapsto m+n+1$ on $\mathbb{N}$:n laskutoimitus. Liittyykö siihen neutraalialkio?

5. Joukon E laskutoimitukseen liittyy *vasen neutraalialkio* e, joka täyttää ehdon $e * x = x \ \forall x \in E$, ja *oikea neutraalialkio* e', siis vastaavasti $x * e' = x \ \forall x \in E$. Osoita, että $e = e'$.

6. Joukon $E = \{0, 1\}$ laskutoimitus määritellään taululla

	0	1
0	0	1
1	1	0

   Osoita, että E on ryhmä tällä laskutoimituksella varustettuna.

7. Joukossa $\mathbb{R} \times \mathbb{R}$ määritellään laskutoimitus asettamalla

$$(x, y) * (x', y') = (xx', yx' + y').$$

   Osoita, että laskutoimitus on liitännäinen mutta ei vaihdannainen.

8. Millä monoidien $(\mathbb{N}, +)$ ja $(\mathbb{N}_+, \cdot)$ alkioilla on käänteisalkio?

9. Olkoon $(E, *)$ monoidi. Osoita, että jos E:n alkiolla x on vasen käänteisalkio x' ja oikea käänteisalkio x'', so. $x' * x = e$ ja $x * x'' = e$, niin $x' = x''$ (joten x:llä on käänteisalkio).

10. Kokonaislukujen joukossa määritellään laskutoimitus $x * y$ seuraavasti:

$$x * y = x + y + 1.$$

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

11. Joukossa $G = \{(x, y) \in \mathbb{R}^2 \mid x \neq 0\}$ määritellään laskutoimitus asettamalla

$$(x, y) * (x', y') = (xx', yx' + y').$$

Osoita, että $(G, *)$ on ryhmä.

12. Määritellään kuvausten $f : \mathbb{R} \to \mathbb{R}$ joukossa $\mathbb{R}^{\mathbb{R}}$ yhteenlasku asettamalla

$$(f + g)(x) = f(x) + g(x) \quad \forall x \in \mathbb{R}.$$

Osoita, että $(\mathbb{R}^{\mathbb{R}}, +)$ on ryhmä.

13. Olkoon $(A, \leq)$ täydellisesti järjestetty joukko. Merkitään $\forall a, b \in A$

$$a * b = \begin{cases} a, \text{ kun } a \leq b, \\ b, \text{ kun } b \leq a. \end{cases}$$

Näytä, että $*$ on vaihdannainen ja liitännäinen. Milloin $(A, *)$ on monoidi?

14. Määritä ed. tehtävässä A:n vakaat osajoukot ja mahdolliset alimonoidit.

15. Tutki, onko $(\mathbb{Z}, \cdot)$ ryhmä.

16. Tutki, onko joukko $\{1, -1, i, -i\}$ ryhmä, kun laskutoimituksena on kompleksilukujen kertolasku.

17. Onko positiivisten irrationaalilukujen joukko ryhmä, kun laskutoimituksena on reaalilukujen kertolasku?

18. Onko matriisilla $\begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$ käänteisalkiota, kun neutraalialkiona on identiteettimatriisi? Entä vasta-alkiota (neutraalialkiona nollamatriisi)?

III.2 Perusominaisuuksia

Seuraavassa ryhmää G merkitään multiplikatiivisesti, ellei toisin mainita.

Koska $a(bc) = (ab)c$, kolmen ja useamman alkion tulo ryhmässä voidaan merkitä ilman sulkeita, esim. abc.

Ryhmän G alkion *potenssi* määritellään tavalliseen tapaan:

$$a^0 = 1, \qquad a^n = a\cdot a\cdots a \quad (n \text{ tekijää}) , \qquad a^{-n} = (a^n)^{-1} \qquad (\forall\ n \geq 1).$$

On hyvä huomata, että $(a^n)^{-1} = (a^{-1})^n$. Tämä seuraa siitä, että

$$a^n(a^{-1})^n = a\cdots aa^{-1}\cdots a^{-1} = 1, \qquad (a^{-1})^n a^n = a^{-1}\cdots a^{-1}a\cdots a = 1.$$

Potenssin määritelmästä saadaan helposti laskusäännöt

$$(a^m)^n = a^{mn}, \qquad a^m a^n = a^{m+n}, \tag{1}$$

kun eksponentit m ja n ovat ei-negatiivisia. Lisäksi nähdään pienellä työllä, että nämä säännöt ovat voimassa kaikilla eksponenteilla. Esimerkiksi (kun $m > 0,\ n > 0$)

$$\begin{aligned}(a^m)^{-n} &= ((a^m)^n)^{-1} = (a^{mn})^{-1} = a^{-mn}\\ a^m a^{-n} &= a^m(a^{-1})^n = \underbrace{a\cdots a}_{m}\underbrace{a^{-1}\cdots a^{-1}}_{n} = a^{m-n} \qquad (m > n).\end{aligned}$$

Muut tapaukset voidaan käsitellä samoin.

Sen sijaan alkeisaritmetiikasta tuttu sääntö $(ab)^n = a^n b^n$ ei tietenkään yleensä päde, jos G ei ole kommutatiivinen!

Huomaa myös sääntö (vrt. matriisilaskenta)

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

Huomautus. Additiivista merkintää käytettäessä potenssia a^n vastaa *monikerta* na. Muotoile kaavat (1) tässä tapauksessa; huomaa ettei luku n tietenkään tässä tarkoita ryhmän alkiota.

Yhteenveto merkinnöistä, jotka riippuvat siitä, käytetäänkö ryhmän laskutoimitukselle kerto- vai yhteenlaskumerkintää.

$(G,\cdot)$		$(G,+)$	
$a\cdot b$ tai ab	tulo	$a+b$	summa
e tai 1	neutraali- tai ykkösalkio	0	neutraali- tai nolla alkio
a^{-1}	käänteisalkio	$-a$	a:n vasta-alkio
a^n	a:n potenssi	na	a:n monikerta
ab^{-1}	osamäärä	$a-b$	erotus

Lause 2. *Oletetaan, että $a, b \in G$. Yhtälöillä*

$$ax = b, \qquad ya = b$$

on ryhmässä G yksikäsitteiset ratkaisut, nimittäin $x = a^{-1}b,\ y = ba^{-1}$.

Todistus. Kertomalla yhtälö $ax = b$ puolittain vasemmalta a^{-1}:llä saadaan $x = a^{-1}b$. Kääntäen, $x = a^{-1}b$ toteuttaa ko. yhtälön, koska $a(a^{-1}b) = b$.

Toinen yhtälö käsitellään samoin. □

Voidaan päätellä (joko lauseesta 2 tai suoraan), että ryhmässä pätevät *supistamissäännöt*

$$ac = bc \implies a = b; \qquad ca = cb \implies a = b.$$

Äärellinen ryhmä voidaan esittää kirjoittamalla sen *kertotaulu*: nimetään taulukon vaaka- ja pystyrivit ryhmän alkioiden mukaan ja kirjoitetaan tulo ab vaakarivin a ja pystyrivin b leikkauskohtaan. Lauseesta 2 seuraa, että taulukon jokainen vaakarivi ja jokainen pystyrivi sisältää ryhmän kunkin alkion kerran.

Esimerkki 1. Kolmen alkion 1, a, b tapauksessa saadaan vain yksi mahdollinen kertotaulu, kun otetaan huomioon edellä mainittu vaatimus. Onko näin määritelty $G = \{1, a, b\}$ ryhmä? Postulaattien G0, G2 ja G3 täyttyminen nähdään välittömästi. G1:n tarkistaminen vaatii enemmän työtä; tältä voidaan välttyä etsimällä jokin tunnettu ryhmä, jolla on tämä taulu. Tällainen ryhmä (siis ryhmän $G = \{1, a, b\}$ "realisointi") on esim. additiivinen ryhmä $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

$\cdot$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tulos: Kolmen alkion ryhmiä on (olennaisesti) yksi. Tämä ryhmä voidaan myös esittää muodossa $G = \{1, a, a^2\}$, missä $a^3 = 1$. Tällaista ryhmää sanotaan *sykliseksi* (määritelmä myöhemmin).

Esimerkki 2. Näytetään, että 4 alkion ryhmiä on (olennaisesti) kaksi. Niiden kertotaulut ovat seuraavat:

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

syklinen ryhmä

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Kleinin neliryhmä

Määritelmä. Olkoon G ryhmä. Jos $H \subset G$ ja H on ryhmä (G:n laskutoimituksen suhteen), sanotaan että H on G:n *aliryhmä*. Merkintä: $H \leqslant G$.

Huomaa, että $1_H = 1_G$. Tämä nähdään kertomalla yhtälö $1_H 1_H = 1_H$ (ajateltuna ryhmässä G) puolittain 1_H^{-1}:llä.

Edellisestä seuraa, että aliryhmän H jokaisen alkion a käänteisalkio H:ssa = a:n käänteisalkio G:ssä.

Esimerkki 3. Ryhmän G triviaalit aliryhmät: $\{1\}$ ja G.

Jos $H \leqslant G$ ja $H \neq G$, sanotaan että H on G:n *aito* aliryhmä. Merkintä: $H < G$.

Esimerkki 4. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ (additiiviset ryhmät);

$\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$ (multiplikatiiviset ryhmät).

Seuraava lause antaa lyhyen tavan testata, onko ryhmän G osajoukko H tämän ryhmän aliryhmä. (Huomaa, että ab^{-1} tulee additiivisella merkinnällä muotoon $a - b$.)

Lause 3 (Aliryhmäkriteeri). *Olkoon G ryhmä ja $H \subset G$. Silloin H on G:n aliryhmä, jos ja vain jos $H \neq \emptyset$ ja*

$$ab^{-1} \in H \quad \forall\ a, b \in H.$$

Todistus. Oletetaan, että $a \in H$. Silloin $1 = aa^{-1} \in H$ ja edelleen $a^{-1} = 1 \cdot a^{-1} \in H$. Näistä nähdään, että H toteuttaa postulaatit G2 ja G3. Myös G1 toteutuu: koska assosiatiivisuus on voimassa G:ssä, se on voimassa H:ssa.

G0 todetaan seuraavasti. Jos $a, b \in H$, niin edellisen mukaan $b^{-1} \in H$ ja siis oletuksen nojalla $ab = a(b^{-1})^{-1} \in H$.

Täten H on ryhmä, siis $H \leqslant G$.

Käänteinen väite jätetään harjoitustehtäväksi. □

Osajoukko H on tavallisesti annettu kaikkien G:n alkioiden joukkona, joilla on jokin ominaisuus P. Edellisen lauseen käyttöön liittyy kaksi vaihetta (vertaa myös induktiotodistuksen rakenteeseen):

1. Näytetään, että jollain G:n alkiolla on ominaisuus P. Sopiva alkio on usein G:n neutraalialkio. (Näin siis todetaan, että $H \neq \emptyset$.)
2. *Oletetaan*, että alkioilla a ja b on ominaisuus P, ja *tämän avulla* näytetään, että alkiolla ab^{-1} on ominaisuus P.

Esimerkki 5. Olkoon G Abelin ryhmä, neutraalialkiona e. Näytetään, että osajoukko $H = \{x \in G \mid x^2 = e\}$ on G:n aliryhmä.

Nyt osajoukon H määrittelevänä ominaisuutena P on ehto $x^2 = e$. Ensin todetaan, että $e^2 = e$, joten $H \neq \emptyset$. Sitten oletetaan, että $a, b \in H$. Tämä tarkoittaa, että $a^2 = e$ ja $b^2 = e$. On näytettävä, että $(ab^{-1})^2 = e$. Koska G on Abelin ryhmä, on $(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2(b^{-1})^2 = a^2(b^2)^{-1} = ee^{-1} = e$. Siis $ab^{-1} \in H$ ja lauseen 3 perusteella H on G:n aliryhmä.

Lauseesta 3 saadaan helposti myös seuraava, hiukan pidempi aliryhmätesti:

Aliryhmätesti. *Olkoon G ryhmä ja H jokin G:n epätyhjä osajoukko. Silloin H on G:n aliryhmä, jos*

$$ab \in H \quad \forall a, b \in H \quad \text{ja}$$
$$a^{-1} \in H \quad \forall a \in H.$$

Todistus. Lauseen 3 perusteella riittää näyttää, että jos $a, b \in H$, niin $ab^{-1} \in H$. Olkoot $a, b \in H$. Silloin $b^{-1} \in H$ jälkimmäisen ehdon perusteella ja $ab^{-1} \in H$ ensimmäisen ehdon perusteella. □

Jos tutkittavana on ryhmän G *äärellinen* osajoukko, sen käsittely on hieman edellistä helpompaa:

Lause 4. *Olkoon G ryhmä ja H sen äärellinen osajoukko. Silloin H on G:n aliryhmä, jos $H \neq \emptyset$ ja*

$$ab \in H \quad \forall \ a, b \in H.$$

Todistus. Oletetaan, että $a, b \in H$. Osoitetaan, että $ab^{-1} \in H$, jolloin väite seuraa lauseesta 3.

Lauseen oletuksen mukaan $b^k \in H$ aina, kun $k \geq 1$, ja siis $ab^k \in H$ aina, kun $k \geq 0$. Koska H on äärellinen, $ab^k = ab^j$ joillakin eksponenteilla $k, j \geq 0,\ k \neq j$. Voidaan olettaa $k < j$. Silloin $j - k - 1 \geq 0$, ja nähdään että

$$ab^{-1} = ab^{j-k-1} \in H. \quad \square$$

Lauseen 3 seuraus. *Jos $H \leqslant G$ ja $K \leqslant G$, niin $H \cap K \leqslant G$.*

Todistus. Koska $1 \in H \cap K$, leikkaus ei ole tyhjä. Jos $a, b \in H \cap K$, niin $a, b \in H$ ja $a, b \in K$, joten H (ryhmänä) sisältää alkion ab^{-1}, samoin K. Siis $ab^{-1} \in H \cap K$. □

Tämä tulos voidaan yleistää mielivaltaisen monen aliryhmän leikkaukselle.

Esimerkki 6. Näytetään, että seuraavat ryhmien osajoukot ovat aliryhmiä:

a) $G = GL_n(\mathbb{R}),\ H = \left\{ A \in GL_n(\mathbb{R}) \ \middle|\ \det(A) = 1 \right\}$;

b) $G = D_n$ (diedriryhmä), $H = \left\{ r \in D_n \ \middle|\ r \text{ on kierto} \right\}$;

c) $G = \mathbb{Z}$ (addit.), $\quad H = m\mathbb{Z} = \left\{ mk \ \middle|\ k \in \mathbb{Z} \right\}$.

Lause 5. *Jos G_1 ja G_2 ovat ryhmiä, niiden karteesinen tulo $G_1 \times G_2$ on ryhmä seuraavan laskutoimituksen suhteen:*

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2) \qquad (a_i, b_i \in G_i). \tag{2}$$

Tätä ryhmää sanotaan ryhmien G_1 ja G_2 suoraksi tuloksi (tai suoraksi summaksi, jos käytetään additiivista merkintää).

Todistus. Postulaattien G0, . . . ,G3 voimassaolo saadaan tarkistetuksi helposti. Huomaa, että ykkösalkio on $(1, 1)$ ja $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$. □

Esimerkki 7. Jos $G_1 = G_2 = \mathbb{R}$ (additiivinen ryhmä), niin lause 4 antaa tutun ryhmän $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, jossa $(u_1, u_2) + (v_1, v_2) = (u_1 + v_1, u_2 + v_2)$ (ks. esimerkki III.1.2).

Huomaa, että kaavan (2) tulomerkinnässä $a_1 b_1$ on kyse ryhmän G_1 operaatiosta ja tulossa $a_2 b_2$ ryhmän G_2 operaatiosta.

Suoran tulon (ja summan) määritelmä yleistyy vastaavalla tavalla ryhmille $G_1, \ldots, G_n$, $n > 2$.

Harjoitustehtäviä

1. Onko $(\mathbb{Z}_n, +)$ ryhmän $(\mathbb{Z}, +)$ aliryhmä?
2. Ratkaise $\mathbb{Z}_8$:ssa yhtälöpari
$$\begin{cases} 1_8 x^2 + 4_8 y^2 &= 0_8 \\ 1_8 x \ + 2_8 y &= 4_8. \end{cases}$$
3. Tarkastellaan joukkoa $\mathbb{R}$ varustettuna yhteenlaskulla. Osoita, että rationaalilukujen osajoukko on vakaa. Onko irrationaalilukujen joukko vakaa?
4. Osoita, että ryhmässä $(G, \circ)$ yhtälöllä
$$a \circ x \circ b \circ c \circ x = a \circ b \circ x$$
on yksikäsitteinen ratkaisu, ja määritä se.
5. Ratkaise kolmen alkion symmetrisessä ryhmässä S_3 yhtälö
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ S = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$
6. Osoita, että $(x^m)^n = x^{mn}$ kaikilla $m, n \in \mathbb{Z}$, kun x on ryhmän G alkio.

7. Ryhmässä $(G, +)$ on voimassa laki $2(x + y) = 2x + 2y$. Osoita, että G on Abelin ryhmä.

8. Olkoon $(G, +)$ Abelin ryhmä ja H niiden G:n alkioiden joukko, joilla $4x = x$. Osoita, että $(H, +)$ on $(G, +)$:n aliryhmä.

9. Oletetaan, että ryhmällä $G = \{0, 1, 2, 3\}$, jonka laskutoimitus merkitään yhteenlaskuna, on taulu

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

   Määritä ryhmän $(G, +)$ kaikki aliryhmät.

10. Olkoon $(G, \circ)$ ryhmä ja

$$H = \{x \in G \mid x \circ a = a \circ x \text{ kaikilla } a \in G\}.$$

    Osoita, että $(H, \circ)$ on $(G, \circ)$:n kommutatiivinen aliryhmä.

11. Olkoot H ja K ryhmän G aliryhmiä. Osoita, että $H \cup K$ on G:n aliryhmä, jos ja vain jos $H \subset K$ tai $K \subset H$.

12. Olkoot a ja b ryhmän $(G, \cdot)$ alkioita, joilla

$$b^6 = e \text{ ja } ab = b^4a.$$

    Osoita, että $b^3 = e$ ja $ab = ba$.

13. Olkoon $(A, +)$ Abelin ryhmä ja B sen aliryhmä. Näytä, että joukko

$$H = \{\, a \in A \mid na \in B \text{ jollakin } n \in \mathbb{N} \setminus \{0\}\}$$

    on A:n aliryhmä, joka sisältää B:n.

14. Olkoon $(E, \circ)$ monoidi ja olkoon sen alkiolla a käänteisalkio E:ssä. Näytä, että kuvaukset

$$f : E \to E,\ x \mapsto a \circ x;$$
$$g : E \to E,\ x \mapsto x \circ a,$$

    ovat bijektioita.

15. Joukon $\mathbb{Z}^* \times \mathbb{Z}$ laskutoimitus $\circ$,

$$(i, a) \circ (j, b) = (ij, a + ib)$$

    $(i, j \in \mathbb{Z}^* = \{1, -1\};\ a, b \in \mathbb{Z})$ tiedetään liitännäiseksi. Näytä, että $(\mathbb{Z}^* \times \mathbb{Z}, \circ)$ on epäkommutatiivinen ryhmä, ja laske siinä alkion $(-1, 5)$ käänteisalkio.

16. Olkoon $(A, \circ)$ äärellinen monoidi ja olkoot $a, b \in A$ sellaisia, että $a \circ b = e_A$. Näytä, että a ja b ovat toistensa käänteisalkioita. (Ohje: Näytä, että kuvaus $f : A \to A$, $f(x) = b \circ x$, on injektio.)

17. Ratkaise symmetrisessä ryhmässä S_6 yhtälö

$$f \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 5 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 4 & 1 & 5 \end{pmatrix}.$$

18. Todista, että $(\mathbb{Z}, +)$ on Abelin ryhmä, lähtemällä määritelmästä $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$ (teht. II.7.9) ja käyttämällä vastaavia $(\mathbb{N}, +)$:n ominaisuuksia.

19. Todista, että $\{5, 15, 25, 35\}$ on ryhmä, kun laskutoimituksena on kertolasku mod 40. Mikä on neutraalialkio?

III.3 Ryhmän virittäminen eli generointi; syklinen ryhmä

Olkoon G ryhmä ja S jokin G:n osajoukko. Tarkastellaan kaikkien niiden G:n aliryhmien H parvea, jotka sisältävät joukon S. Tämä parvi on epätyhjä, koska ainakin G itse kuuluu siihen. Aliryhmien H leikkaus on G:n aliryhmä (todistus kuten lauseen 3 seurauslauseen), jota sanotaan *joukon S virittämäksi eli generoimaksi G:n aliryhmäksi* ja merkitään symbolilla $\langle S \rangle$; siis

$$\langle S \rangle = \bigcap_{S \subset H \leqslant G} H.$$

Joukon S alkioita sanotaan ryhmän $\langle S \rangle$ *virittäjiksi* eli *generaattoreiksi.*

Jos generaattoreita on äärellisen monta, ts. $S = \{a_1, \ldots, a_k\}$, sanotaan, että ryhmä $\langle S \rangle$ on *äärellisesti viritetty eli äärellisesti generoitu(va)*, ja käytetään merkintää

$$\langle S \rangle = \langle a_1, \ldots, a_k \rangle.$$

Edellisen määritelmänsä mukaan ryhmä $\langle S \rangle$ on "suppein" G:n aliryhmä, joka sisältää joukon S. ("Suppeus" on ymmärrettävä sisältymisrelaation mielessä: parven joukko on suppein, jos se sisältyy kaikkiin muihin joukkoihin.)

Esimerkki 1. $\langle \emptyset \rangle = \{1\}$, $\langle 1 \rangle = \{1\}$. Jos $H \leqslant G$, niin $\langle H \rangle = H$.

Lause 6. *Ryhmän G osajoukon S generoima aliryhmä muodostuu kaikista tuloista, joiden tekijät ovat S:n alkioita ja S:n alkioiden käänteisalkioita (mukaanluettuna "tyhjä tulo" $= 1$), ts.*

$$\langle S \rangle = \left\{ a_1 a_2 \cdots a_m \;\middle|\; a_i \text{ tai } a_i^{-1} \in S \quad \forall\ i;\ m \geq 0 \right\}.$$

Todistus. Merkitään H:lla yhtälön oikealla puolella olevaa joukkoa. Aliryhmäkriteeristä nähdään, että $H \leqslant G$. Lisäksi $S \subset H$; ajattele esim. yhden alkion "tuloja". Näin ollen $\langle S\rangle \subset H$, koska $\langle S\rangle$ on määritelmänsä mukaan pienin aliryhmä, joka sisältää S:n.

Toisaalta jokainen G:n aliryhmä, joka sisältää joukon S, sisältää myös kaikki edellä mainitut tulot, siis ryhmän H. Täten H sisältyy kaikkien tällaisten aliryhmien leikkaukseen eli ryhmään $\langle S\rangle$.

Nämä tulokset yhdessä antavat yhtälön $\langle S\rangle = H$. $\square$

Huomautus. Jos ryhmä G on äärellinen, lauseen kaava saa yksinkertaisemman muodon

$$\langle S\rangle = \left\{ a_1 a_2 \cdots a_m \;\middle|\; a_i \in S \quad \forall\ i;\ m \geq 0 \right\}.$$

Nyt voidaan nimittäin käyttää lausetta 4.

Esimerkki 2. Ryhmän $\mathbb{R}^*$ osajoukko $\mathbb{P}$ (alkuluvut) virittää aliryhmän $\mathbb{Q}_+$, joka koostuu kaikista positiivisista rationaaliluvuista (laskutoimituksena kertolasku).

Esimerkki 3. Jos V on vektoriavaruus, jonka dimensio $= n$, niin V:n kanta $\{B_1, \ldots, B_n\}$ generoi ryhmälle $(V, +)$ aliryhmän $\left\{ k_1 B_1 + \cdots + k_n B_n \;\middle|\; k_i \in \mathbb{Z} \quad \forall\ i \right\}$. (Miksei tämä ole V:n aliavaruus?)

Esimerkki 4. Diedriryhmä $D_4 = \langle r, s\rangle$, missä $r = (\pi/2)$:n kierto ja $s =$ sopiva peilaus.

Esimerkki 5. Ääretön ryhmä $\mathbb{Z}$ on äärellisesti generoitu: $\mathbb{Z} = \{\, n\cdot 1 \;\mid\; n \in \mathbb{Z}\} = \langle 1\rangle = \langle -1\rangle$.

Määritelmä. Ryhmää G sanotaan *sykliseksi*, jos G on yhden alkion generoima, ts. jos on olemassa sellainen $a \in G$, että $G = \langle a\rangle$.

Lause 7. *Olkoon G syklinen ryhmä, $G = \langle a\rangle$. Jos $\#G = n \in N$, G on muotoa*

$$G = \left\{1, a, a^2, \ldots, a^{n-1}\right\}$$

ja n on pienin positiivinen kokonaisluku, jolla $a^n = 1$. Jos $\#G = \infty$, niin

$$G = \left\{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\right\}$$

ja kaikki potenssit a^m $(m \in \mathbb{Z})$ ovat erisuuria, erityisesti $a^m \neq 1 \quad \forall\ m \neq 0$.

Todistus. Lauseen 6 nojalla

$$G = \left\{ a^m \;\middle|\; m \in \mathbb{Z} \right\}. \tag{1}$$

Oletetaan ensin, että $\#G = n$. Silloin potenssien a^m joukossa on vain n erisuurta, joten on olemassa jotkin sellaiset eksponentit m ja k, että $m > k$ mutta $a^m = a^k$. Nyt siis $a^{m-k} = 1$ ja $m - k > 0$. Valitaan *pienin* positiivinen eksponentti, jolla $a^s = 1$ (siis $s \leq m - k$).

Jakoalgoritmin mukaan jokainen eksponentti $m \geq 0$ voidaan kirjoittaa muotoon $m = qs + r$, missä $0 \leq r \leq s - 1$. Koska

$$a^m = a^{qs+r} = (a^s)^q a^r = 1^q a^r = a^r,$$

G:n kaikki alkiot ovat muotoa $a^r,\ r = 0, \ldots, s-1$. Nämä alkiot ovat lisäksi erisuuria; muussa tapauksessahan samanlainen päättely kuin edellä johtaisi tulokseen $a^t = 1$, missä $0 < t < s$, ja tämä olisi vastoin s:n minimaalisuutta. Erityisesti siis $\#G = s$, joten $s = n$. Lisäksi nähdään, että G on juuri väitettyä muotoa.

Jos G on ääretön, niin kaavassa (1) kaikki potenssit a^m ovat erisuuria, sillä muuten päädyttäisiin äärelliseen ryhmään samoin kuin edellä. □

Esimerkki 6. $\mathbb{Z}_m$ on kertalukua m oleva (additiivinen) syklinen ryhmä $\forall\ m \geq 1$:

$$\mathbb{Z}_m = \langle\, \overline{1} \,\rangle = \left\{ \overline{0}, \overline{1}, 2{\cdot}\overline{1}, \ldots, (m-1){\cdot}\overline{1} \right\}.$$

$\mathbb{Z}$ on ääretön syklinen ryhmä (ks. esimerkki 5). Mitkä ovat virittäjät?

Esimerkki 7. Näytetään, että $\mathbb{Z}_5^* = \langle\, \overline{2} \,\rangle$.

Mistä johtuu syklisen ryhmän nimitys? Jos $G = \langle a \rangle$ on kertalukua n, niin päättymättömän jonon $\ldots, a^{m-1}, a^m, a^{m+1}, \ldots$ mitkä tahansa n peräkkäistä alkiota muodostavat "syklin", joka toistuu samanlaisena siirryttäessä jonossa eteenpäin. Tämä voidaan ilmaista myös seuraavasti:

$$a^k = a^h \qquad \Longleftrightarrow \qquad k \equiv h \pmod{n}.$$

Ääretön syklinen ryhmä on (edellisessä mielessä) rajatapaus, jossa on vain yksi äärettömän pitkä sykli.

Määritelmä. Olkoon G ryhmä ja $a \in G$. Ryhmän G aliryhmän $\langle a \rangle$ kertalukua sanotaan *alkion a kertaluvuksi* ja merkitään $\mathrm{ord}(a)$:lla; siis

$$\mathrm{ord}(a) = \#\langle a \rangle.$$

Lauseesta 7 seuraa välittömästi: *a on (äärellistä) kertalukua n jos ja vain jos n on pienin positiivinen eksponentti, jolla $a^n = 1$.* Lisäksi tällöin a:n kaikki erisuuret potenssit ovat $1, a, a^2, \ldots, a^{n-1}$.

Huomaa, että $\mathrm{ord}(a) = 1$ silloin ja vain silloin, kun $a = 1$.

ESIMERKKI 8. (i) Ryhmässä $\mathbb{R}^*$ on $\text{ord}(1) = 1$, $\text{ord}(-1) = 2$ ja kaikkien muiden alkioiden kertaluku $= \infty$.

(ii) Lasketaan ryhmän $\mathbb{Z}_{21}^*$ alkioiden $\overline{2}$ ja $\overline{20}$ kertaluvut.

Myöhemmin esitetään, miten määritelmään perustuvaa kertaluvun määritystä voidaan yksinkertaistaa.

Harjoitustehtäviä

1. Tarkastellaan ryhmää $(\mathbb{Z}_{10}, +)$. Mikä on $\langle\overline{10}\rangle$?
2. Onko $\langle\overline{-1}\rangle = \mathbb{Z}_m$?
3. Mikä on ryhmän $\mathbb{Z}_{12}$ kertaluku? Laske sen jokaisen alkion kertaluku.
4. Etsi ryhmälle $(\mathbb{Z}_8, +)$ kaikki mahdolliset virittäjät.
5. Määritä osajoukon $\{6, 15, 21\}$ virittämä $\mathbb{R}$:n aliryhmä.
6. Olkoon $G = \langle a,\ b\rangle$, missä $\text{ord}(a) = \text{ord}(b) = 2$ ja $ab = ba$. Osoita, että G on Kleinin neliryhmä.
7. Todista, että $\langle a\rangle = \langle a^{-1}\rangle$, olipa a mikä hyvänsä ryhmän alkio.
8. Mikä on matriisin $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ kertaluku $GL_2(\mathbb{R})$:ssä?
9. Olkoon x ryhmän $(G, \cdot)$ alkio. Oletetaan, että $x^2 \neq 1$ ja $x^6 = 1$. Todista, että $x^4 \neq 1$ ja $x^5 \neq 1$. Mitä voidaan sanoa alkion x kertaluvusta?

III.4 Ryhmien homomorfia ja isomorfia

Pykälässä III.2 mainittiin, että ryhmät ovat olennaisesti samat, jos niillä on alkioiden nimitystä vaille sama kertotaulu. Tässä pykälässä käsitellään tätä ryhmien "yhtäsuuruutta" täsmällisemmin. Lähtökohtana on ryhmien välinen vertailu, joka perustuu seuraavaan määritelmään.

MÄÄRITELMÄ. Olkoot $(G,\cdot)$ ja $(G',*)$ ryhmiä. Kuvausta $f : G \to G'$ sanotaan *(ryhmä)homomorfismiksi*, jos se toteuttaa *homomorfiaehdon*

$$f(ab) = f(a) * f(b) \quad \forall\ a,b \in G. \tag{1}$$

Jos kummankin ryhmän laskutoimitukselle käytetään kertolaskumerkintää, homomorfiaehto saa muodon $f(ab) = f(a)f(b) \quad \forall\ a,b \in G$.

ESIMERKKI 1. Jokainen vektoriavaruuksien U ja V välinen lineaarikuvaus $t : U \to V$ on additiivisten ryhmien U ja V välinen homomorfismi, koska

$$t(X_1 + X_2) = tX_1 + tX_2 \quad \forall\ X_1, X_2 \in U.$$

ESIMERKKI 2. (i) Kuvaus $f : \mathbb{R}^* \to \mathbb{R}^*, \quad f(x) = x^2$, on homomorfismi, koska

$$f(xy) = (xy)^2 = x^2y^2 = f(x)f(y) \quad \forall\ x,y \in \mathbb{R}^*.$$

(ii) Merkitään $\mathbb{R}_+$:lla positiivisten reaalilukujen muodostamaa multiplikatiivista ryhmää. Kuvaus $f : \mathbb{R}_+ \to \mathbb{R}, \quad f(x) = \ln x$, on homomorfismi, koska $f(xy) = \ln(xy) = \ln x + \ln y = f(x) + f(y)$.

(iii) Kuvaus $f : \mathbb{Z} \to \mathbb{Z}_m, \quad f(a) = \overline{a}$, on homomorfismi, koska $\overline{a+b} = \overline{a} + \overline{b}$.

(iv) *Triviaali homomorfismi* $f : G \to G', \quad f(a) = 1_{G'} \quad \forall\ a \in G$.

Ryhmähomomorfismi $G \to G'$ "säilyttää ykkösalkion ja käänteisalkiot", ts.

$$f(1_G) = 1_{G'}, \qquad f\left(a^{-1}\right) = f(a)^{-1} \quad \forall\ a \in G.$$

Näistä ensimmäinen yhtälö nähdään oikeaksi kertomalla yhtälö $f(1)f(1) = f(1\cdot 1)$ puolittain $f(1)^{-1}$:llä (tässä merkittiin $1_G = 1$; usein merkitään *molempien* ryhmien ykkösalkiota 1:llä). Jälkimmäinen seuraa puolestaan siitä, että $f(a)f(a^{-1}) = f(aa^{-1}) = f(1) = 1$ ja samoin $f(a^{-1})f(a) = 1$.

Lineaarikuvaukseen t sovellettuna edellinen tulos ilmaisee sen tutun asian, että t "säilyttää nolla-alkion ja vasta-alkiot". (Lineaarikuvausten teoriassa tämä seuraa suoraan t:n määritelmästä).

MÄÄRITELMÄ. Olkoot $(M,\cdot)$ ja $(M',*)$ monoideja. Kuvausta $f : M \to M'$ sanotaan *(monoidi)homomorfismiksi*, jos se toteuttaa homomorfiaehdon (1) ja ehdon $f(1_M) = 1_{M'}$.

Seuraavalla lauseella on analogia lineaarikuvausten teoriassa.

Lause 8. *Olkoon $f : G \to G'$ ryhmähomomorfismi.*

(i) *Jos $H \leqslant G$, niin $f(H) \leqslant G'$.*

(ii) *Jos $H' \leqslant G'$, niin $f^{-1}(H') \leqslant G$.*

Todistus. (i) Joukko $f(H)$ on epätyhjä, koska $H \neq \emptyset$. Jos $a', b' \in f(H)$, siis $a' = f(a),\ b' = f(b)$ (missä $a, b \in H$), niin

$$a'b'^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in f(H).$$

Väite seuraa nyt aliryhmäkriteeristä ($ab^{-1} \in H$ koska H on aliryhmä).

(ii) Koska H' sisältää G':n ykkösalkion, jonka alkukuva on G:n ykkösalkio 1, niin $1 \in f^{-1}(H')$. Täten $f^{-1}(H') \neq \emptyset$. Implikaatio $a, b \in f^{-1}(H') \implies ab^{-1} \in f^{-1}(H')$ todistetaan jälleen homomorfiaehdon avulla (tee se!). □

Kuten lineaarikuvauksilla, poimitaan lauseen tärkeät erikoistapaukset $H' = \{1\}$ ja $H = G$: homomorfismin $f : G \to G'$ *ydin*

$$\mathrm{Ker}(f) = f^{-1}(\{1\}) = \big\{\, a \in G \;\big|\; f(a) = 1 \big\}$$

ja *kuva*

$$\mathrm{Im}(f) = f(G) = \big\{\, f(a) \;\big|\; a \in G \big\}\,.$$

Esimerkki 3. Määritetään esimerkin 2 homomorfismien ydin ja kuva.

Ryhmää $\mathrm{Im}(f)$ sanotaan ryhmän G *homomorfiseksi kuvaksi*. Tämä ryhmä säilyttää G:n piirteitä; toisaalta se hävittää G:n ominaisuuksia sitä enemmän (karkeasti sanottuna), mitä useampia alkioita f kuvaa samaksi G':n alkioksi. Asian täsmällinen käsittely lykätään tuonnemmaksi; nyt otetaan esiin vain se tärkeä rajatapaus, jossa f on tässä suhteessa paras mahdollinen.

Määritelmä. Ryhmähomomorfismia $f : G \to G'$ sanotaan *(ryhmä)isomorfismiksi*, jos f on bijektiivinen. Ryhmää G sanotaan ryhmän G' kanssa *isomorfiseksi*, jos on olemassa jokin isomorfismi $f : G \to G'$. Merkintä: $G \simeq G'$.

Esimerkki 4. Esimerkin 2 (ii) kuvaus $f : \mathbb{R}_+ \to \mathbb{R}, \quad f(x) = \ln x$, on isomorfismi, joten $\mathbb{R}_+ \simeq \mathbb{R}$ (tarkemmin: $(\mathbb{R}_+, \cdot) \simeq (\mathbb{R}, +)$).

Jos homomorfismi $f : G \to G'$ on injektio, niin kuvaus $f : G \to \mathrm{Im}(f)$ on bijektiivinen homomorfismi, siis isomorfismi. *Ryhmän G homomorfinen kuva* $\mathrm{Im}(f)$ *injektiivisessä kuvauksessa f on siis G:n kanssa isomorfinen.*

Homomorfismin injektiivisyyttä tutkittaessa on seuraava lause usein mukava.

Lause 9. *Ryhmähomomorfismi $f : G \to G'$ on injektio jos ja vain jos* $\mathrm{Ker}(f) = \{1_G\}$.

Todistus. a) Olkoon f injektio. Koska $f(1_G) = 1_{G'}$, on tällöin $\mathrm{Ker}(f) = \{1_G\}$.

b) Olkoot $x, y \in G$ ja $f(x) = f(y)$. Silloin $1_{G'} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$, joten $xy^{-1} \in \mathrm{Ker}(f)$. Oletuksesta $\mathrm{Ker}(f) = \{1_G\}$ seuraa nyt $x = y$. Täten f on injektio. □

Esimerkki 5. Olkoon G ryhmä ja $u \in G$. Osoitetaan, että kuvaus

$$f_u : G \longrightarrow G, \qquad f_u(a) = uau^{-1},$$

on isomorfismi. (Isomorfismia G:ltä itselleen sanotaan G:n *automorfismiksi*.)

Lause 10. *Olkoot $f : G \to G'$ ja $g : G' \to G''$ ryhmähomomorfismeja. Silloin*

(i) *kuvaus $g \circ f : G \to G''$ on homomorfismi;*

(ii) *jos f ja g ovat isomorfismeja, samoin on $g \circ f$.*

Todistus. (i) $g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b))$.

(ii) Kuvauksen $g \circ f$ bijektiivisyys todetaan suoraviivaisesti. Sen jälkeen väite seuraa (i)-kohdasta. □

Lause 11. *Olkoon $f : G \to G'$ ryhmäisomorfismi. Silloin $f^{-1} : G' \to G$ on isomorfismi.*

Todistus. Kuvaus f^{-1} on triviaalisti bijektiivinen; on siis todistettava vain sen homomorfisuus. Olkoot $a', b' \in G'$, siis $a' = f(a)$, $b' = f(b)$, missä $a, b \in G$. Silloin $a'b' = f(a)f(b) = f(ab)$, joten

$$f^{-1}(a'b') = ab = f^{-1}(a')f^{-1}(b'). \quad \square$$

Huomautus. Lauseen todistuksesta seuraa erityisesti, että homomorfismin käänteiskuvaus, jos se on olemassa, on homomorfismi.

Ryhmien isomorfia on ekvivalenssirelaatio (missä tahansa ryhmien parvessa). Relaation symmetrisyys seuraa näet lauseesta 11 ja transitiivisuus lauseen 10 (ii)-kohdasta; refleksiivisyyttä varten riittää huomata, että id_G on isomorfismi $G \to G$ (tai vaihtoehtoisesti käyttää esimerkkiä 5).

Isomorfiset ryhmät G ja G' ovat ryhmäteorian kannalta katsottuna samanlaiset: niiden alkiot vastaavat bijektiivisesti toisiaan ja G:n alkioiden tuloa vastaa G':ssa näiden vastinalkioiden (= kuvien) tulo. Jos erityisesti G ja G' ovat äärellisiä, G:n kertotaulusta saadaan G':n taulu korvaamalla jokainen alkio vastinalkiollaan.

Esimerkki 6. Pykälän III.2 esimerkit 1 ja 2 osoittavat, että on olemassa isomorfiaa vaille tarkalleen yksi kertalukua 3 oleva ryhmä ja tarkalleen kaksi kertalukua 4 olevaa ryhmää. (Entä kertalukuja 1 ja 2?)

ESIMERKKI 7. Näytetään, etteivät ryhmät $(\mathbb{R}, +)$ ja $(\mathbb{R}^*, \cdot)$ ole isomorfiset.

Ryhmäteorian perusprobleemoja on kaikkien epäisomorfisten ryhmien luokittelu, ks. IV.5.

Harjoitustehtäviä

1. Tutki, ovatko $(\mathbb{Z}, +)$ ja $(2\mathbb{Z}, +)$ isomorfiset.

2. Onko kuvaus $f : (\mathbb{R}_+, \cdot) \to (\mathbb{R} \setminus \{-1\}, \circ)$, $f(x) = x - 1$, homomorfismi, kun $\cdot$ on tavallinen kertolasku ja $\circ$ määritellään kaavalla $x \circ y = xy + x + y$?

3. Olkoon E joukko ja F sen (kiinteä) osajoukko. Määritellään potenssijoukossa $\mathcal{P}(E)$ laskutoimitus $(A, B) \mapsto A \cap B$. Osoita, että kuvaus $f : \mathcal{P}(E) \to \mathcal{P}(E)$, $f(A) = A \cup F$, täyttää homomorfiaehdon ja kuvaa neutraalialkion neutraalialkioksi (eli on *monoidihomomorfismi*).

4. Olkoot X, Y joukkoja ja $f : X \to Y$ kuvaus. Näytä, että kuvaus

$$\theta : \mathcal{P}(Y) \to \mathcal{P}(X);\ \theta(B) = f^{-1}(B);$$

on monoidihomomorfismi $\big(\mathcal{P}(Y), \cup\big) \to \big(\mathcal{P}(X), \cup\big)$.

5. Olkoon $f : G \to H$ ryhmähomomorfismi. Näytä, että $f(x^n) = f(x)^n$ $\forall x \in G$, $n \in \mathbb{Z}$.

6. Määritä tehtävän III.2.15 ryhmän $(\mathbb{Z}^* \times \mathbb{Z}, *)$ sykliset aliryhmät ja näytä näin ko. ryhmä epäsykliseksi.

7. Olkoot G ja H ryhmiä, A joukon $S \subset G$ virittämä aliryhmä ja $f : G \to H$ homomorfismi. Näytä, että aliryhmä $f(A)$ on joukon $f(S)$ virittämä.

8. Olkoon $G = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ ja $H = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \,|\, a, b \in \mathbb{Q} \right\}$. Ovatko G ja H isomorfisia ryhmiä, kun laskutoimituksena on yhteenlasku?

III.5 Lagrangen lause; sovelluksia

MÄÄRITELMÄ. Olkoon $H \leqslant G$. Ryhmän G kuhunkin alkioon a liittyvää osajoukkoa

$$aH = \{\, ah \mid h \in H \}$$

sanotaan aliryhmän H *vasemmaksi sivuluokaksi* (coset) G:ssä. Vastaavasti määritellään oikeat sivuluokat Ha.

Additiivista merkintää käytettäessä sivuluokat kirjoitetaan $a + H,\ H + a$.

Seuraavassa käsitellään lähinnä vasempia sivuluokkia; oikeat sivuluokat käyttäytyvät samalla tavalla. Jos G on Abelin ryhmä, niin $aH = Ha \quad \forall\ a \in G$ ja määreet "vasen" ja "oikea" voidaan siis jättää pois.

Ehto

$$b \sim a \qquad \Longleftrightarrow \qquad b \in aH$$

määrittelee G:ssä ekvivalenssirelaation (tarkista!). Sen ekvivalenssiluokat ovat muotoa

$$[a] = \{\, b \in G \mid b \in aH \} = aH;$$

ne ovat siis juuri H:n vasemmat sivuluokat. Tästä nähdään, että aliryhmän H vasemmat sivuluokat G:ssä muodostavat G:n osituksen

$$G = \bigcup_{a \in D} aH,$$

missä a käy läpi jonkin vasempien sivuluokkien edustajiston D.

Aliryhmä H itse on yksi sivuluokka: esim. $H = 1 \cdot H = H \cdot 1$.

Ehto $b \in aH$ on yhtäpitävä ehdon $a^{-1}b \in H$ kanssa. Sivuluokkia käsiteltäessä kannattaa pitää mielessä sääntö

$$aH = bH \qquad \Longleftrightarrow \qquad a \in bH,$$

joka seuraa osituksen perusominaisuuksista.

ESIMERKKI 1. Ryhmän $\mathbb{Z}$ aliryhmän $\langle m \rangle = m\mathbb{Z}$ sivuluokat ovat $m\mathbb{Z},\ 1 + m\mathbb{Z},\ 2 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}$; ne ovat siis jäännösluokat $\bmod m\ (m \geq 1)$.

Additiivisen Abelin ryhmän tapauksessa aliryhmän sivuluokista käytetään usein yleisestikin nimitystä jäännösluokka.

ESIMERKKI 2. Diedriryhmän $D_4 = \langle r, s \rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ aliryhmän $H = \langle s \rangle$ vasemmat sivuluokat (huomaa että $rs = sr^3$):

$$H = \{1, s\}, \qquad rH = \{r, sr^3\}, \qquad r^2H = \{r^2, sr^2\}, \qquad r^3H = \{r^3, sr\}.$$

Määritä myös oikeat sivuluokat.

Ryhmän G aliryhmän H vasempien sivuluokkien lukumäärää sanotaan H:n *indeksiksi* G:ssä ja merkitään $[G : H]$. Indeksi voi tietysti olla myös ääretön. Seuraavaa lausetta sanotaan indeksilauseeksi:

Lause 12 (Lagrange). *Jos G on äärellinen ryhmä ja $H \leqslant G$, niin*

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

Erityisesti siis äärellisen ryhmän G aliryhmän kertaluku jakaa G:n kertaluvun.

Todistus. Jokaisessa sivuluokassa aH on yhtä monta alkiota kuin H:ssa, sillä yhtälöstä $ah_1 = ah_2$ seuraa $h_1 = h_2$ $(h_1, h_2 \in H)$. Saadaan siis

$$\#G = \sum_{a \in D} \#(aH) = \sum_{a \in D} \#H = [G : H] \cdot (\#H). \quad \square$$

Huomautus. (i) Myös siinä tapauksessa, että H on ääretön (ja samoin siis G), jokainen sivuluokka aH on yhtä mahtava kuin H. Kuvaus $H \to aH$, $h \mapsto ah$, on nimittäin bijektio.

(ii) Indeksi $[G : H]$ ilmoittaa myös H:n oikeiden sivuluokkien lukumäärän. Tämä seuraa, kun osoitetaan (tee se!), että kuvaus $aH \mapsto Ha^{-1}$ on bijektio vasempien sivuluokkien joukolta oikeiden sivuluokkien joukolle. Jos G on äärellinen, tulos saadaan helpommin katsomalla lauseen 12 todistusta.

Esimerkki 3. Esimerkit 1 ja 2 antavat tulokset $[\mathbb{Z} : m\mathbb{Z}] = m$, $[D_4 : \langle s \rangle] = 4$. Jälkimmäinen näistä seuraa (helpommin) myös Lagrangen lauseesta.
$[\mathbb{C} : \mathbb{R}] = \infty$, koska eri reaaliluvut y määrittävät eri sivuluokat $iy + \mathbb{R}$.

Esimerkki 4. Oletetaan, että ryhmällä G on äärelliset aliryhmät H ja K, joiden kertalukujen syt $= 1$. Mikä on $H \cap K$?
Vastauksen antaa Lagrangen lause: Koska $(H \cap K)$:n kertaluku jakaa sekä $\#H$:n että $\#K$:n, se on $= 1$. Täten $H \cap K = \{1\}$.

Lagrangen lause on tehokas apu tutkittaessa, mitkä annetun äärellisen ryhmän G osajoukoista ovat aliryhmiä. Lauseesta seuraa mm., ettei G:n aito osajoukko S, jossa on enemmän kuin $(\#G)/2$ alkiota, voi olla G:n aliryhmä.

Seuraus 1. *Äärellisen ryhmän G alkioiden kertaluvut jakavat G:n kertaluvun.*

Todistus. Myös tämä seuraa suoraan Lagrangen lauseesta, koska $\mathrm{ord}(a) = \#\langle a \rangle$. $\square$

Esimerkki 5. Lasketaan ryhmän $\mathbb{Z}_{13}^*$ alkioiden kertaluvut.

Seuraus 2. *Jos G on äärellinen ryhmä, $\#G = g$, ja $a \in G$, niin $a^g = 1$.*

Todistus. Merkitään alkion a kertalukua h:lla; silloin $a^h = 1$. Seurauslauseen 1 mukaan $h \mid g$, siis $g = th$, missä $t \in \mathbb{Z}$. Nyt $a^g = a^{th} = (a^h)^t = 1$. □

Esimerkki 6. Ryhmään $\mathbb{Z}_m^*$ sovellettuna edellinen tulos merkitsee, että $\overline{a}^{\varphi(m)} = \overline{1} \quad \forall\ \overline{a} \in \mathbb{Z}_m^*$. Kirjoittamalla tämä kongruenssin muotoon saadaan *Eulerin lause*:

$$a^{\varphi(m)} \equiv 1 \pmod{m} \qquad \text{aina kun } \operatorname{syt}(a, m) = 1.$$

Erityisesti tapauksessa $m = p \in \mathbb{P}$ tästä seuraa *Fermat'n (pikku) lause*:

$$a^{p-1} \equiv 1 \pmod{p} \qquad \text{aina kun } p \nmid a.$$

Siis esim. $3^4 \equiv 1 \pmod 5$, $22^{102} \equiv 1 \pmod{103}$ jne. Fermat kykeni todistamaan tämän pelkästään lukuteorian menetelmin (koeta itse samaa!).

Fermat'n lause voidaan kirjoittaa myös muotoon

$$a^p \equiv a \pmod{p} \quad \forall\ a \in \mathbb{Z}.$$

Huomaa, että Eulerin lause, joka lukuteoriassa on hyvin tärkeä, saatiin yllä vain vaatimattomana erikoistapauksena yleisestä ryhmäteorian tuloksesta.

Seuraus 3. *Jos ryhmän G kertaluku on alkuluku p, niin G on syklinen.*

Todistus. Valitaan $a \in G,\ a \neq 1$. Koska $\operatorname{ord}(a)$ jakaa p:n ja on > 1, sen on oltava $= p$. Täten a generoi koko ryhmän G: $G = \langle a \rangle$. □

Koska samaa kertalukua olevat sykliset ryhmät ovat isomorfiset (mieti), edellisestä seuraa, että on olemassa isomorfiaa vaille tarkalleen yksi ryhmä, jonka kertaluku on annettu alkuluku (vrt. pykälän III.4 esimerkki 6).

Harjoitustehtäviä

1. Olkoon $H = 7\mathbb{Z}$. Muodosta kaikki H:n sivuluokat $\mathbb{Z}$:ssa.
2. Etsi kaikki ryhmän $(\mathbb{Z}_{30}, +)$ aliryhmät.
3. Etsi kaikki virittäjät ryhmille $(\mathbb{Z}_6, +)$, $(\mathbb{Z}_8, +)$ ja $(\mathbb{Z}_{20}, +)$.
4. Olkoon a ryhmän alkio, $\operatorname{ord}(a) = 15$. Laske alkioiden a^n, $0 \leq n \leq 15$, kertaluvut.

5. Miksi kertalukua p^2 (p alkuluku) olevan ryhmän G kaikki epätriviaalit aliryhmät ovat syklisiä? Mikä on suurin mahdollinen määrä tällaisia G:n aliryhmiä?

6. Olkoon $H = 3\mathbb{Z}$; tarkastellaan H:n sivuluokkia $\mathbb{Z}$:ssa. Tutki ovatko seuraavat sivuluokat samoja:

   a) $11 + H$ ja $17 + H$,

   b) $-1 + H$ ja $5 + H$.

7. Olkoot H ja K ryhmän G aliryhmiä. Osoita: jos ryhmässä G on sellaiset alkiot a, b, että $aH = bK$, niin $H = K$.

IV. RYHMIEN RAKENTEESTA

IV.1 Tekijäryhmä

Annettua ryhmää G tutkittaessa on usein hyödyllistä käyttää apuna ryhmiä, jotka ovat yksinkertaisempia, esim. kertaluvultaan pienempiä. Tätä varten tarvitaan *normaalin aliryhmän* ja *tekijäryhmän* käsitteet.

Jos G on ryhmä ja H sen aliryhmä, eivät sivuluokat aH ja Ha välttämättä yhdy kaikilla alkioilla $a \in G$. Jos ne yhtyvät, saadaan tärkeä erikoistapaus, jonka merkityksen jo Galois huomasi noin 150 vuotta sitten.

MÄÄRITELMÄ. Ryhmän G aliryhmää N sanotaan *normaaliksi*, jos sen vasemmat ja oikeat sivuluokat yhtyvät, ts.

$$aN = Na \quad \forall\ a \in G.$$

Merkintä: $N \trianglelefteq G, \quad N \triangleleft G$ (aito).

Jos G on Abelin ryhmä, sen jokainen aliryhmä on siis normaali.

Huomaa, että määritelmän yhtälöstä $aN = Na$ ei seuraa, että $an = na \quad \forall\, a \in G,\ n \in N$; sensijaan siitä seuraa, että

$$\forall\ n \in N \quad \exists\ n_1 \in N\ : \qquad an = n_1 a. \tag{1}$$

Seuraava kriteeri soveltuu usein aliryhmän normaalisuuden testaamiseen.

Lause 1 (Aliryhmän normaalisuuskriteeri). *Olkoon $N \leqslant G$. Silloin*

$$N \trianglelefteq G \qquad \Longleftrightarrow \qquad ana^{-1} \in N \quad \forall\ a \in G,\, n \in N \qquad \text{eli} \qquad aNa^{-1} \subset N \quad \forall\ a \in G.$$

Todistus. ($\Longrightarrow$) Jos $N \trianglelefteq G$, niin soveltamalla ehtoa (1) saadaan $ana^{-1} = n_1 \in N$.

($\Longleftarrow$) Olkoon $a \in G$. On osoitettava, että $aN = Na$.

Olkoon $n \in N$; merkitään $ana^{-1} = n_1$. Oletuksen mukaan $n_1 \in N$. Saadaan siis, että $an = n_1 a \in Na$. Täten $aN \subset Na$.

Sovelletaan nyt oletusta alkioihin a^{-1} ja n. Silloin saadaan, että $a^{-1}na = n_2 \in N$, siis $na = an_2 \in aN$. Tämä osoittaa, että $Na \subset aN$.

Nämä tulokset yhdessä todistavat väitteen. □

HUOMAUTUS. Jos $N \trianglelefteq G$, niin määritelmästä seuraa, että

$$aNa^{-1} = N \quad \forall a \in G.$$

Normaalisuuskriteeri siis lausuu, että normaalisuuden varmistamiseksi *riittää* todistaa tässä yhtäsuuruuden asemesta sisältymisrelaatio ” $\subset$ ”.

Esimerkki 1. G:n triviaalit aliryhmät G ja $\{1\}$ ovat normaaleja.

Myös indeksiä 2 oleva aliryhmä H on aina normaali: $aH = H = Ha\ \forall a \in H$ ja $aH = G \setminus H\ \forall a \notin H$, joten H:n vasemmat sivuluokat ovat H ja $G \setminus H$; samoin oikeat sivuluokat. Näin ollen vasemmat ja oikeat sivuluokat yhtyvät.

Esimerkki 2. Näytetään, että matriisiryhmän $GL_n(\mathbb{R})$ aliryhmistä

$$SL_n(\mathbb{R}) = \left\{ A \in GL_n(\mathbb{R}) \;\middle|\; \det(A) = 1 \right\},$$

$$H = \left\{ A \in GL_n(\mathbb{R}) \;\middle|\; A \text{ on lävistäjämatriisi} \right\}$$

edellinen on normaali mutta jälkimmäinen (kun $n > 1$) ei ole.

Huomautus. Oletetaan, että $a, x \in G$. Ryhmän alkiota $y = axa^{-1}$ sanotaan alkion x *konjugaattialkioksi.* Sanotaan myös, että axa^{-1} saadaan alkiosta x *konjugoimalla* a:lla.

Relaatio

$$x \sim y \qquad \Longleftrightarrow \qquad \exists\ a \in G: \quad y = axa^{-1}$$

on G:n ekvivalenssirelaatio (vrt. matriisien similaarisuus). Sen ekvivalenssiluokkia

$$[x] = \left\{ axa^{-1} \;\middle|\; a \in G \right\}$$

sanotaan ryhmän G *konjugaattiluokiksi.*

Aliryhmän normaalisuuskriteeri (lause 1) voidaan ilmaista myös seuraavasti: Ryhmän G aliryhmä N on normaali jos ja vain jos N *on suljettu eli vakaa kaikilla G:n alkioilla konjugoinnin suhteen* (eli jos ja vain jos N *koostuu G:n kokonaisista konjugaattiluokista*).

Jos $N \trianglelefteq G$, niin N:n sivuluokkien joukkoa G:ssä merkitään (G/N):llä; siis

$$G/N = \left\{ aN \;\middle|\; a \in G \right\} = \left\{ aN \;\middle|\; a \in D \right\},$$

missä D on jokin sivuluokkien edustajisto.

Lause 2. *Oletetaan, että $N \trianglelefteq G$. Joukko G/N on ryhmä seuraavasti määritellyn laskutoimituksen suhteen:*

$$aN \cdot bN = abN.$$

Todistus. Postulaatti G0 seuraa, kun osoitetaan, että laskutoimitus on hyvinmääritelty.

Oletetaan, että $aN = a'N$ ja $bN = b'N$. Silloin $a \in a'N$ ja $b \in b'N$, joten

$$a = a'n_1, \qquad b = b'n_2 \qquad (n_1, n_2 \in N).$$

Nyt $ab = a'n_1b'n_2$. Koska aliryhmä N on normaali, niin $Nb' = b'N$ ja alkio n_1b' siis voidaan kirjoittaa muotoon $b'n_3$, missä $n_3 \in N$. Tuloksena on

$$ab = a'b'n_3n_2 \in a'b'N.$$

Tämä osoittaa, että $abN = a'b'N$, toisin sanoen $aN \cdot bN = a'N \cdot b'N$.

Assosiatiivisuus G1 seuraa G:n laskutoimituksen assosiatiivisuudesta:

$$(aN \cdot bN) \cdot cN = abN \cdot cN = (ab)cN = a(bc)N = aN \cdot bcN = aN \cdot (bN \cdot cN).$$

Neutraalialkiona on N ja alkion aN käänteisalkiona $a^{-1}N$ (tarkista!). $\square$

MÄÄRITELMÄ. Ryhmää $(G/N, \cdot)$ sanotaan G:n *tekijäryhmäksi* N:n suhteen.

Huomaa, että $\#(G/N) = [G : N]$.

Jos G on Abelin ryhmä ja $H \leqslant G$, niin $H \trianglelefteq G$ ja tekijäryhmä G/H on Abelin ryhmä, sillä $aH \cdot bH = abH = baH = bH \cdot aH \quad \forall\ a, b \in G$.

ESIMERKKI 3. Muodostetaan tekijäryhmä $\mathbb{Z}_{21}^* / H$ (kertotaulu), missä $H = \langle \overline{4} \rangle$.

ESIMERKKI 4. Ryhmän $\mathbb{R}^*$ tekijäryhmä aliryhmän $H = \langle -1 \rangle = \{+1, -1\}$ suhteen on

$$\mathbb{R}^* / H = \left\{ aH \;\middle|\; a \in \mathbb{R}^* \right\} = \left\{ aH \;\middle|\; a \in \mathbb{R}_+ \right\}; \qquad aH \cdot bH = abH.$$

Tässä $aH = \{+a, -a\}$.

ESIMERKKI 5. Ryhmän $\mathbb{Z}$ tekijäryhmä aliryhmän $\langle m \rangle = m\mathbb{Z}$ suhteen ($m \geq 1$) on

$$\mathbb{Z}/m\mathbb{Z} = \left\{ k + m\mathbb{Z} \;\middle|\; k \in \mathbb{Z} \right\} = \left\{ k + m\mathbb{Z} \;\middle|\; k = 0, 1, \ldots, m-1 \right\},$$

laskutoimituksena $(k + m\mathbb{Z}) + (h + m\mathbb{Z}) = (k + h) + m\mathbb{Z}$. Toisin merkittynä:

$$\mathbb{Z}/m\mathbb{Z} = \left\{ \overline{0}, \overline{1}, \ldots, \overline{m-1} \right\}; \qquad \overline{k} + \overline{h} = \overline{k+h}.$$

Kyseessä on siis vanha tuttu, nimittäin jäännösluokkaryhmä mod m : $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

(Voitkin ajatella yleisen tekijäryhmän käsitettä jäännösluokkaryhmän mod m käsitteen yleistyksenä.)

MÄÄRITELMÄ. Joukossa A määritelty laskutoimitus ja ekvivalenssi $\sim$ ovat *yhteensopivia*, jos $a \sim a'$, $b \sim b' \quad \Rightarrow \quad ab \sim a'b'$.

Harjoitustehtäviä

1. Olkoon $H = \langle 6_{18} \rangle$. Muodosta kaikki H:n sivuluokat $\mathbb{Z}_{18}$:ssa ja tee yhteenlaskutaulu ryhmälle $(\mathbb{Z}_{18}/H, +)$.
2. Olkoot $(G_1, \cdot)$ ja $(G_2, \cdot)$ ryhmiä. Osoita, että $G_1 \times \{1_{G_2}\}$ on ryhmän $G = G_1 \times G_2$ aliryhmä. Onko se normaali aliryhmä?

3. Olkoot H ja K ryhmän G normaaleja aliryhmiä. Osoita, että myös $H \cap K$ on G:n normaali aliryhmä.
4. Määritä ryhmän $(\mathbb{Z}_4, +)$ aliryhmät ja vastaavat tekijäryhmät.
5. Koska $\mathbb{R}$ on Abelin ryhmä, sen aliryhmä $\mathbb{Z}$ on normaali ja tekijäryhmä $\mathbb{R}/\mathbb{Z}$ on siis määritelty. Perustele, miksi tekijäryhmän alkiot voidaan lausua muodossa $q+\mathbb{Z}$, missä $q \in \mathbb{R}, \quad 0 \leq q < 1$. Lausu tässä muodossa alkiot $(\frac{1}{2}+\mathbb{Z})+(\frac{2}{3}+\mathbb{Z})$ ja $-(\frac{3}{4}+\mathbb{Z})$. Mikä on alkion $\frac{35}{99}+\mathbb{Z}$ kertaluku?
6. Olkoon G ryhmä ja E G:n laskutoimituksen kanssa yhteensopiva G:n ekvivalenssirelaatio. Näytä, että G:n ykkösalkion ekvivalenssiluokka on G:n normaali aliryhmä ja G:n ositus tämän aliryhmän sivuluokkiin vastaa ekvivalenssia E.
7. Määritä tehtävän III.2.15 ryhmän sykliset aliryhmät, jotka ovat normaaleja.
8. Todista, että $\langle 3\rangle/\langle 12\rangle$ on isomorfinen $\mathbb{Z}_4$:n kanssa, missä $\langle 3\rangle \leq \mathbb{Z}$ ja $\langle 12\rangle \leq \mathbb{Z}$.
9. Olkoon H ryhmän G normaali aliryhmä, jonka indeksi on k. Todista, että $a^k \in H \ \forall a \in G$. (Ohje: Ajattele tekijäryhmää.)
10. Mikä on ryhmän $\mathbb{Z}_{60}/\langle\overline{15}\rangle$ kertaluku?

IV.2 Ryhmien homomorfialause

Lause 3. *Olkoon $f : G \to G'$ ryhmähomomorfismi.*

(i) *Jos $N \trianglelefteq G$, niin $f(N) \trianglelefteq f(G)$.*

(ii) *Jos $N' \trianglelefteq G'$, niin $f^{-1}(N') \trianglelefteq G$.*

(Vertaa tätä lauseeseen III.8, jossa $\trianglelefteq$:n tilalla on $\leqslant$. Huomaa toinenkin ero!)

Todistus. (i) Lauseen III.8 nojalla $f(N)$ on ryhmä, siis $f(N) \leqslant f(G)$. On siis vain näytettävä, että $byb^{-1} \in f(N) \quad \forall\ b \in f(G),\ y \in f(N)$.

Voidaan kirjoittaa $b = f(a),\ y = f(x)$, missä $a \in G$ ja $x \in N$. Silloin

$$byb^{-1} = f(a)f(x)f(a^{-1}) = f(axa^{-1}).$$

Koska G:n aliryhmä N on normaali, niin $axa^{-1} \in N$. Täten $f(axa^{-1}) \in f(N)$.

(ii) Tämän todistus on samanlainen (mieti). $\square$

Kun valitaan erityisesti $N' = \{1\}$, saadaan tulos: *Ryhmähomomorfismin $f : G \to G'$ ydin* $\mathrm{Ker}(f)$ *on G:n normaali aliryhmä.*

Seuraavan lauseen mukaan jokainen homomorfismi antaa tietyn isomorfian, siksi tätä lausetta sanotaan myös ryhmien isomorfialauseeksi. Tämä on ryhmäteorian peruslauseita!

Lause 4 (Homomorfialause). *Jos $f : G \to G'$ on ryhmähomomorfismi, niin*

$$G/\operatorname{Ker}(f) \simeq \operatorname{Im}(f).$$

Tarkemmin: homomorfismi f indusoi isomorfismin

$$F : G/\operatorname{Ker}(f) \longrightarrow \operatorname{Im}(f), \qquad F(a\cdot\operatorname{Ker}(f)) = f(a).$$

Todistus. Merkitään $K = \operatorname{Ker}(f)$ ja tarkastellaan kuvausta F. Osoitetaan ensiksi, että F on hyvinmääritelty. Jos $aK = bK$, niin $a \in bK$, siis $a = bk$, missä $k \in K$. Nyt

$$F(aK) = f(a) = f(bk) = f(b)f(k) = f(b)\cdot 1 = f(b) = F(bK),$$

mikä todistaa väitteen.

On näytettävä, että F on isomorfismi.

Homomorfisuus: Kun $aK, bK \in G/K$, niin

$$F(aK\cdot bK) = F(abK) = f(ab) = f(a)f(b) = F(aK)F(bK).$$

Injektiivisyys: Jos $F(aK) = 1$, niin $f(a) = 1$ ja siis $a \in K$. Silloin $aK = K =$ ryhmän G/K ykkösalkio. Tämä todistaa F:n injektioksi (lause III.9).

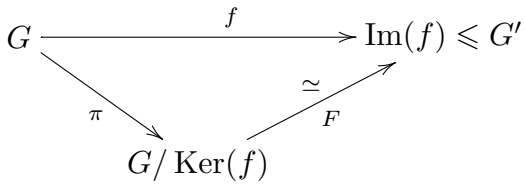
Surjektiivisuus seuraa suoraan kuvauksen F määritelmästä. □

Huomautus 1. Jos $N \trianglelefteq G$, kuvausta

$$\pi : G \longrightarrow G/N, \qquad \pi(a) = aN,$$

sanotaan *(kanoniseksi) projektioksi tai surjektioksi* ryhmältä G tekijäryhmälle G/N. Se on triviaalisti surjektiivinen ja lisäksi homomorfismi (tarkista).

Jos kyseessä on homomorfialauseen tilanne ja N:ksi valitaan ryhmä $K = \operatorname{Ker}(f)$,



nähdään että $f(a) = F(aK) = F(\pi(a)) \quad \forall\ a \in G$. Näin ollen

$$f = F \circ \pi.$$

Tämä ilmaistaan myös sanomalla, että viereinen kaavio *kommutoi* (alkioiden kuvautuminen ei riipu "reitistä"). Merkintä $\simeq$ tarkoittaa, että F on isomorfismi.

Huomautus 2. Lauseen 4 nojalla ryhmän G jokainen homomorfinen kuva $f(G) = \operatorname{Im}(f)$ on isomorfinen G:n jonkin tekijäryhmän $G/\operatorname{Ker}(f)$ kanssa. Kääntäen jokainen G:n tekijäryhmä G/N on isomorfinen (vieläpä identtinen) G:n jonkin homomorfisen kuvan kanssa; edellisen huomautuksen mukaan näet $G/N = \operatorname{Im}(\pi)$, missä π on projektio $G \to G/N$.

Edellisestä seuraa, että kaikki G:n homomorfiset kuvat voidaan löytää pelkän G:n avulla, etsimällä kaikki G:n tekijäryhmät. Voidaan siis lähteä G:n homomorfismeista f, jolloin aina $\operatorname{Ker}(f)$ on G:n normaali aliryhmä ja tekijäryhmä $G/\operatorname{Ker}(f)$ on isomorfinen kuvan $\operatorname{Im}(f)$ kanssa; tai voidaan lähteä G:n normaaleista aliryhmistä N ja käyttää kanonista projektiota $\pi : G \to G/N$.

ESIMERKKI 1. Tutkitaan homomorfismin $f : \mathbb{Z} \to \mathbb{Z}_m, \quad f(a) = \overline{a}$, indusoimaa isomorfismia ($m \geq 1$). Saadaanko tästä tulos $\mathbb{Z}/\langle m \rangle \simeq \mathbb{Z}_m$?

ESIMERKKI 2. Homomorfismin $f : \mathbb{R}^* \to \mathbb{R}_+, \quad f(x) = |x|$, indusoima isomorfismi on

$$F : \mathbb{R}^*/\{\pm 1\} \longrightarrow \mathbb{R}_+, \qquad F\left(x\{\pm 1\}\right) = x \quad \forall \ x > 0.$$

Huomaa, että $x\{\pm 1\} = \{\pm x\}$. (Vrt. pykälän IV.1 esimerkki 4.)

ESIMERKKI 3. Homomorfismi $f : GL_n(\mathbb{R}) \to \mathbb{R}^*, \quad f(A) = \det(A)$, antaa isomorfian

$$GL_n(\mathbb{R})/\, SL_n(\mathbb{R}) \simeq \mathbb{R}^* \qquad \text{(ks. pykälän IV.1 esimerkki 2).}$$

ESIMERKKI 4. Triviaali homomorfismi $f : G \to G, \quad f(a) = 1$, sekä identtinen kuvaus (homomorfismi) id_G antavat vastaavasti isomorfiat

$$G/G \simeq \{1\}, \qquad G/\{1\} \simeq G.$$

Mieti mitkä ovat kyseiset isomorfismit.

Soveltamalla homomorfialausetta erilaisiin homomorfismeihin saadaan joukko yleisiä *isomorfialauseita*. Seuraavassa näistä esimerkkinä yksi.

Jos $H \leqslant G$ ja $K \trianglelefteq G$, niin joukko

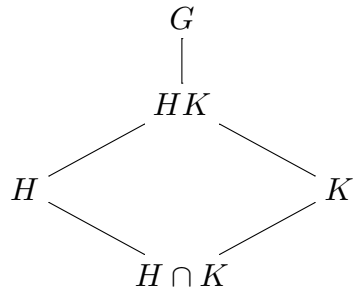
$$HK = \left\{ hk \;\middle|\; h \in H,\, k \in K \right\}$$

on G:n aliryhmä (tarkista aliryhmäkriteerillä; huomaa myös, että tämä on joukon $H \cup K$ generoima G:n aliryhmä). Oletuksesta seuraa, että K on myös HK:n normaali aliryhmä. Kuvaus

$$f : H \longrightarrow HK/K, \qquad f(a) = aK,$$

on homomorfismi, ja $\mathrm{Ker}(f) = H \cap K$, $\mathrm{Im}(f) = HK/K$ (varmistu näistä itse). Täten

$$H/(H \cap K) \simeq HK/K.$$



Viereisen kaavion avulla on helppo ymmärtää, miksi tätä isomorfialausetta sanotaan *suunnikassäännöksi.*

Harjoitustehtäviä

1. Määritä kokonaislukujen ryhmän kaikki
   a) homomorfismit itseensä,
   b) automorfismit.
2. Osoita, että tekijäryhmä $(5\mathbb{Z}/20\mathbb{Z}, +)$ on isomorfinen ryhmän $(\mathbb{Z}_4, +)$ kanssa.
3. Näytä, että joukko $H := \{f \in S_4 \mid f(4) = 4\}$ on S_3:n kanssa isomorfinen S_4:n aliryhmä, jonka sivuluokat $g \circ H$ ovat
$$X_k := \{f \in S_4 \mid f(4) = k\} \ (k = 1,\ 2,\ 3,\ 4).$$
4. Näytä, ettei ryhmä $\mathbb{Z}_6$ ole isomorfinen symmetrisen ryhmän S_3 kanssa.
5. Näytä, että ryhmän $(\mathbb{C}^*, \cdot)$ eli $(\mathbb{C} \setminus \{0\}, \cdot)$ aliryhmä $T := \{z \in \mathbb{C} \mid |z| = 1\}$ on isomorfinen ryhmän $(\mathbb{R}, +)$ tekijäryhmän $\mathbb{R}/\mathbb{Z}$ kanssa. (Ohje: $|z|^2 = \bar{z}z$. Käytä homomorfialausetta ja Eulerin kaavaa $e^{2\pi it} = \cos t + i(\sin t),\ t \in \mathbb{R}$.)
6. Olkoon $\overline{G} = \mathbb{R}^{\mathbb{R}} = \{f | f : \mathbb{R} \to \mathbb{R}\}$ ja $G = \{f \in \overline{G} |\ f$ integroituva$\}$. Osoita, että $\overline{G}$ ja G ovat ryhmiä yhteenlaskun suhteen ja että kuvaus $f \mapsto \int f$ on homomorfismi $G \to \overline{G}$, kun oletetaan, että integroimisvakio on 0. Mikä on tämän kuvauksen ydin? Onko kuvaus homomorfismi, jos oletetaan, että integroimisvakio on 1?
7. Montako homomorfismia on ryhmältä $(\mathbb{Z}_{20}, +)$ ryhmään $(\mathbb{Z}_8, +)$? Montako näistä on surjektioita?

IV.3 Sykliset ryhmät

Muista, että ryhmää G sanotaan sykliseksi, jos se on yhden alkionsa generoima:

$$G = \langle a \rangle$$

Sykliset ryhmät muodostavat yksinkertaisimman luokan kaikkien ryhmien joukossa. Tässä pykälässä määritetään mm. syklisten ryhmien kaikki aliryhmät.

Kertalukua n olevasta syklisestä ryhmästä käytetään merkintää C_n :

$$C_n = \langle c \rangle = \left\{1, c, c^2, \ldots, c^{n-1}\right\}; \quad c^n = 1$$

$(n = 1, 2, \dots)$. Vastaavasti ääretön syklinen ryhmä on

$$C_\infty = \langle c \rangle = \{\dots, c^{-2}, c^{-1}, 1, c, c^2, \dots\}.$$

Näitä ryhmiä käsiteltäessä on usein hyödyllistä muistaa, että

$$C_n \simeq \mathbb{Z}/n\mathbb{Z}, \qquad C_\infty \simeq \mathbb{Z},$$

isomorfismeina vastaavasti esim. $c \mapsto \overline{1}$ ja $c \mapsto 1$ (tässä siis oikeanpuoliset ryhmät ovat additiivisia).

Esimerkki 1. Yhtälön $x^n = 1$ kompleksilukuratkaisut ovat luvut

$$e^{2\pi ik/n} = \cos(2\pi k/n) + i{\cdot}\sin(2\pi k/n) \qquad (k = 0, 1, \dots, n-1),$$

ns. *n:nnet ykkösenjuuret*. Kun merkitään $\zeta_n = e^{2\pi i/n}$, nämä luvut voidaan kirjoittaa muodossa ${\zeta_n}^k$, missä $k = 0, 1, \dots, n-1$. Ne muodostavat ryhmän $\mathbb{C}^*$ aliryhmän, joka on syklinen ja kertalukua n, generaattorina esim. ζ_n :

$$\langle \zeta_n \rangle \simeq C_n.$$

Tässä on siis yksi ryhmän C_n multiplikatiivinen realisointi. (Esitä luvut ${\zeta_n}^k$ kompleksitasossa.)

Lause 5. *Äärettömän syklisen ryhmän $C_\infty = \langle c \rangle$ aliryhmät ovat ryhmät*

$$\langle c^n \rangle, \qquad n = 0, 1, 2, \dots$$

Ne ovat keskenään erisuuria.

Todistus. Ryhmällä C_∞ on joka tapauksessa mainitut ryhmät $\langle c^n \rangle$ aliryhminä.

Oletetaan, että H on C_∞:n aliryhmä. Jos $H = \{1\}$, niin $H = \langle c^0 \rangle$. Jos $H \neq \{1\}$, niin H sisältää jonkin alkion c^n, missä $n > 0$. Valitaan *pienin* tällainen n. Osoitetaan, että $H = \langle c^n \rangle$.

Jos $a \in H$, niin koska $a \in \langle c \rangle$, a on muotoa c^m, missä $m \in \mathbb{Z}$. Kirjoittamalla $m = kn + r$, missä $0 \leq r < n$, saadaan

$$c^r = c^{m-kn} = c^m (c^n)^{-k} \in H.$$

Luvun n minimaalisuuden nojalla $r = 0$. Täten $m = kn$ ja siis $a = c^m = (c^n)^k \in \langle c^n \rangle$. Näin on saatu tulos $H \subset \langle c^n \rangle$. Käänteinen relaatio $\langle c^n \rangle \subset H$ seuraa välittömästi siitä, että $c^n \in H$. Yhdessä nämä todistavat väitteen.

Koska c^n on ryhmään $\langle c^n \rangle$ kuuluva alin positiivinen c:n potenssi, nähdään että

$$\langle c^n \rangle = \langle c^{n'} \rangle, \quad n, n' > 0 \qquad \Longrightarrow \qquad n = n'.$$

Tästä seuraa lauseen jälkimmäinen väite. □

Äärettömän syklisen ryhmän C_∞ kaikki aliryhmät $\neq \{1\}$ ovat siis $\simeq C_\infty$.

Ryhmään $\mathbb{Z}$ sovellettuna edellinen lause ilmaisee, että $\mathbb{Z}$:n kaikki aliryhmät ovat ryhmät $n\mathbb{Z}$ $(n = 0, 1, \dots)$. Entä $\mathbb{Z}$:n kaikki tekijäryhmät? Koska $\mathbb{Z}$ on Abelin ryhmä, sen kaikki aliryhmät ovat normaaleja; $\mathbb{Z}$:n tekijäryhmät ovat siis ryhmät $\mathbb{Z}/n\mathbb{Z}$. Pykälän IV.1 esimerkin 5 nojalla tästä saadaan tulos: *Ryhmän $\mathbb{Z}$ kaikki tekijäryhmät ovat jäännösluokkaryhmät $\mathbb{Z}_n$ $(n = 1, 2, \dots)$ sekä $\mathbb{Z}$ itse $(n = 0)$.*

Vastaava tulos pätee tietysti myös yleisen syklisen ryhmän C_∞ tapauksessa.

Lause 6. *Kertalukua n olevalla syklisellä ryhmällä $C_n = \langle c \rangle$ on jokaista n:n tekijää m kohti tarkalleen yksi aliryhmä, jonka kertaluku on m. Tämä on*

$$\langle c^k \rangle = \left\{1, c^k, c^{2k}, \dots, c^{(m-1)k}\right\} \qquad (k = n/m).$$

Ryhmällä C_n ei ole muita aliryhmiä.

Todistus. Koska $(c^k)^m = c^n = 1$, lauseessa mainittu ryhmä on C_n:n kertalukua m oleva aliryhmä. On siis vain näytettävä, että se on ainoa tällainen aliryhmä.

Olkoon $H \leqslant C_n$, $\#H = m$. Jos $m = 1$, niin $H = \{1\} = \langle 1 \rangle$, kuten pitääkin. Oletetaan, että $m > 1$. Kuten lauseen 5 todistuksessa valitaan *pienin* positiivinen eksponentti k, jolla $c^k \in H$. Samanlainen päättely antaa nytkin tuloksen $H = \langle c^k \rangle$. Tässä alkion c^k kertaluku $= \#H = m$, joten $km = n$ ja siis $k = n/m$.

Lauseen viimeinen väite seuraa Lagrangen lauseesta. □

Lauseista 5 ja 6 seuraa: *Syklisen ryhmän kaikki aliryhmät ovat syklisiä.*

Lauseesta 6 saadaan myös seuraus: Jos p on alkuluku, ryhmällä C_p ei ole muita aliryhmiä kuin triviaalit.

Esimerkki 2. Määritetään ryhmän C_{12} aliryhmät ja esitetään ne diagrammana (ns. *Hassen kaavio*).

Seuraava lause antaa yksinkertaisen kaavan äärellisen syklisen ryhmän alkioiden kertaluvun laskemiseksi.

Lause 7. *Jos* $\operatorname{ord}(a) = n$, *niin* $\operatorname{ord}(a^m) = \dfrac{n}{\operatorname{syt}(n, m)}$.

Todistus. Merkitään $d = \operatorname{syt}(n, m)$ ja $n = n_1 d$, $m = m_1 d$. On todistettava, että $\operatorname{ord}(a^m) = n_1$, toisin sanoen että

$$(a^m)^r = 1 \qquad \Longleftrightarrow \qquad n_1 \mid r.$$

Koska $\operatorname{ord}(a) = n$, niin $a^{mr} = 1$ jos ja vain jos $n \mid mr$. Tämä on ekvivalentti ehdon $n_1 \mid m_1 r$ kanssa. Koska $\operatorname{syt}(n_1, m_1) = 1$, väite seuraa. □

Tästä seuraa, että syklisen ryhmän $C_n = \langle c \rangle$ generaattoreita ovat tarkalleen ne ryhmän alkiot c^m, missä $\text{syt}(n, m) = 1$. Näiden lukumäärä on $\varphi(n)$.

Esimerkki 3. Lasketaan ryhmän $\mathbb{Z}_9^*$ alkioiden kertaluvut.

Esimerkki 4. Jokainen alkulukukertalukua oleva ryhmä on syklinen (ks. III.5 seuraus 3).

Harjoitustehtäviä

1. Luettele $(\mathbb{Z}_{18}, +)$:n aliryhmään $\langle \overline{3} \rangle$ kuuluvat alkiot.
2. Mitkä ovat ryhmän $(\mathbb{Z}_{30}, +)$ aliryhmät? Laske myös niiden kertaluvut ja anna virittäjät.
3. Etsi syklisten ryhmien $C_6 = \langle a \rangle,\ C_8 = \langle b \rangle,\ C_{20} = \langle c \rangle$ kaikki virittäjät.
4. Mistä alkioista muodostuu ryhmän $\mathbb{C}^*$ aliryhmä $H = \langle a,\ b \rangle$, kun $a = e^{2\pi i/5}$ ja $b = e^{2\pi i/7}$? Tutki, onko H syklinen.
5. Laadi syklisen ryhmän C_{30} kaikista aliryhmistä Hassen kaavio. Valitse sellainen C_{30}:n aliryhmä H, että tekijäryhmä C_{30}/H on kertalukua 3, ja laadi tämän tekijäryhmän kertotaulu.
6. Olkoot G ja H äärellisiä ryhmiä, joiden kertaluvut ovat erisuuria alkulukuja. Määritä kaikki homomorfismit $f : G \to H$. (Ohje: Ajattele ryhmiä $\text{Ker}(f)$ ja $\text{Im}(f)$.)
7. Määritä kaikki ryhmähomomorfismit $f : \mathbb{Z}_9 \to \mathbb{Z}_{15}$. (Ohje: Ryhmän $(\mathbb{Z}, +)$ aliryhmät tiedetään syklisiksi. Määritä ensin kaikki homomorfismit $g : \mathbb{Z} \to \mathbb{Z}_{15}$ ja ratkaise sitten yhtälöt $f \circ j = g$, missä j on projektio $\mathbb{Z} \to \mathbb{Z}_9$.)

IV.4 Permutaatioryhmät

Pykälässä III.1 tarkasteltiin esimerkkinä n:n alkion symmetristä ryhmää

$$S_n = \left\{ \alpha : J_n \longrightarrow J_n \;\middle|\; \alpha \text{ bijektio} \right\},$$

missä $J_n = \{1, 2, \ldots, n\}$ ja bijektiota eli *permutaatiota* α merkittiin

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}.$$

Tässä siis $\alpha(i) = k_i \ \ (i = 1, \ldots, n)$.

Ryhmän S_n aliryhmiä sanotaan *permutaatioryhmiksi.*

Nyt permutaatioille otetaan käyttöön mukavampi merkintätapa. Alkioiden $a_1, \ldots, a_r$ (jotka ovat kaikki erisuuria) permutaatiota, jossa

$$a_1 \mapsto a_2, \quad a_2 \mapsto a_3, \ \ \ldots, \ \ a_{r-1} \mapsto a_r, \quad a_r \mapsto a_1,$$

sanotaan *r-pituiseksi sykliksi* tai lyhyesti *r-sykliksi* ja merkitään

$$(a_1 a_2 \ldots a_r).$$

Jokainen permutaatio $\alpha \in S_n$ voidaan kirjoittaa sellaisten syklien tulona, joilla ei ole yhteisiä alkioita. Todistuksen idea on, että kirjoitetaan ensin esim. alkiosta 1 lähtien sykli, sitten jostain jäljellä olevasta alkiosta lähtien uusi sykli jne. Esim.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123), \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix} = (142)(36)(5).$$

Voidaan osoittaa, että tällainen permutaation *sykliesitys* eli *syklimuoto* on yksikäsitteinen, paitsi että syklit voidaan kirjoittaa mihin järjestykseen tahansa ja kukin sykli voidaan aloittaa millä tahansa alkiollaan (mieti), esim.

$$(142)(36)(5) = (36)(214)(5).$$

Lisäksi 1-syklit jätetään tulossa yleensä (identiteettikuvauksina) kirjoittamatta, siis esim. $(142)(36)(5) = (142)(36)$. Pane erityisesti merkille, että alkiovieraat syklit kommutoivat keskenään.

2-sykliä sanotaan *transpositioksi.*

Huomaa permutaatioiden tulon (= yhdistetyn kuvauksen) muodostamisjärjestys: esim.

$$(23)(12) = (132), \qquad (12)(23) = (123).$$

Esimerkki 1. Kirjoitetaan S_4:n alkiot syklimuodossa. Etsitään S_4:n aliryhmä, joka on Kleinin neliryhmä (ks. pykälän III.2 esimerkki 2).

Permutaation $\alpha \in S_n$ sanotaan olevan *tyyppiä* $(r_1, \ldots, r_m)$, jos sen syklien pituudet ovat $r_1, \ldots, r_m$. Siis esim. edellinen kuuden alkion permutaatio on tyyppiä $(1, 2, 3)$. Luvut $r_1, \ldots, r_m$ (joiden järjestyksellä ei ole tässä väliä) muodostavat luvun n *osituksen*, toisin sanoen

$$r_1 + \cdots + r_m = n.$$

Lause 8. *Jos permutaatio $\alpha \in S_n$ on tyyppiä $(r_1, \ldots, r_m)$, niin*

$$\operatorname{ord}(\alpha) = \operatorname{pyj}(r_1, \ldots, r_m).$$

Todistus. Kun $k = 1, \ldots, r-1$, permutaatio $(a_1 a_2 \ldots a_r)^k$ kuvaa alkion a_1 alkioksi a_{k+1}. Täten $(a_1 a_2 \ldots a_r)^k \neq \mathrm{id}_{J_n}$ näillä k:n arvoilla. Koska $(a_1 a_2 \ldots a_r)^r = (1)$, nähdään että r-syklin kertaluku on $= r$.

Oletuksen mukaan $\alpha = \alpha_1 \cdots \alpha_m$, missä α_j:t ovat alkiovieraita r_j-syklejä. Koska alkiovieraat syklit kommutoivat, niin $\alpha^t = {\alpha_1}^t \cdots {\alpha_m}^t$. Saadaan siis

$$\alpha^t = (1) \quad \Longleftrightarrow \quad {\alpha_j}^t = (1) \ \ (j = 1, \ldots, m) \quad \Longleftrightarrow \quad r_j \mid t \ \ (j = 1, \ldots, m).$$

Tästä seuraa väite. □

Huomautus 1. Ryhmän S_n kukin konjugaattiluokka (ks. pykälän IV.1 huomautus) muodostuu kaikista samaa tyyppiä olevista permutaatioista. Tämä nähdään kirjoittamalla

$$\alpha = (a_1 a_2 \ldots a_p)(a_{p+1} \ldots a_q) \cdots (\ldots a_n),$$

$$\tau = \begin{pmatrix} a_1 & a_2 & \ldots & a_p & a_{p+1} & \ldots & a_q & \ldots & a_n \\ b_1 & b_2 & \ldots & b_p & b_{p+1} & \ldots & b_q & \ldots & b_n \end{pmatrix}$$

ja laskemalla näistä, että

$$\tau\alpha\tau^{-1} = (b_1 b_2 \ldots b_p)(b_{p+1} \ldots b_q) \cdots (\ldots b_n).$$

Esimerkki 2. Näytetään, että $H_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ on S_4:n normaali aliryhmä.

Tarkastellaan n:n muuttujan $x_1, \ldots, x_n$ polynomia

$$\begin{aligned} \Delta = \prod_{i<j} (x_i - x_j) = (x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n) \cdot \\ (x_2 - x_3) \cdots (x_2 - x_n) \cdot \\ \cdots\cdots\cdots\cdots \\ (x_{n-1} - x_n). \end{aligned}$$

Oletetaan, että $\alpha \in S_n$. Merkitään $\alpha(\Delta)$:lla polynomia, joka saadaan suorittamalla edellisessä polynomissa Δ indeksien permutaatio α.

Siis esim. jos $n = 3$ ja $\alpha = (13)$, niin

$$\alpha(\Delta) = (x_3 - x_2)(x_3 - x_1)(x_2 - x_1) = -\Delta.$$

Nähdään, että joka tapauksessa $\alpha(\Delta) = \pm\Delta$. Tässä esiintyvää etumerkkiä sanotaan permutaation α *merkiksi* ja merkitään $\operatorname{sign}(\alpha)$:lla; tällöin

$$\alpha(\Delta) = \operatorname{sign}(\alpha)\Delta = \begin{cases} +\Delta, & \text{jos } \alpha \text{ on parillinen,} \\ -\Delta, & \text{jos } \alpha \text{ on pariton.} \end{cases}$$

Jos $\alpha \in S_n$ ja $\beta \in S_n$, niin

$$\operatorname{sign}(\alpha\beta) = \operatorname{sign}(\alpha)\operatorname{sign}(\beta), \tag{1}$$

sillä

$$\operatorname{sign}(\alpha\beta)\Delta = (\alpha\beta)(\Delta) = \alpha(\beta(\Delta)) = \operatorname{sign}(\alpha)\operatorname{sign}(\beta)\Delta.$$

Kuvaus $\operatorname{sign} : S_n \to \{\pm 1\}$ on siis homomorfismi.

Esimerkki 3. *a)* $\operatorname{sign}(\alpha^{-1}) = \operatorname{sign}(\alpha)$, koska

$$\operatorname{sign}(\alpha^{-1})\operatorname{sign}(\alpha) = \operatorname{sign}(\alpha^{-1}\alpha) = \operatorname{sign}(\mathrm{id}) = 1.$$

b) $\operatorname{sign}(*\alpha*^{-1}) = \operatorname{sign}(*)\operatorname{sign}(\alpha)\operatorname{sign}(*^{-1}) = \operatorname{sign}(*)^2\operatorname{sign}(\alpha) = \operatorname{sign}(\alpha)$.

Lause 10. (i) *Samaa tyyppiä olevilla permutaatioilla on sama merkki.*

(ii) *Transpositiot ovat parittomia. Yleisemmin: r-syklin merkki on* $(-1)^{r-1}$.

Todistus. (i) Huomautuksen 1 nojalla permutaatiot $\in S_n$ ovat samaa tyyppiä jos ja vain jos ne ovat S_n:n konjugaattialkioita. Väite seuraa nyt esimerkin 3 *b*-kohdasta.

(ii) Transpositio $\alpha = (12)$ on pariton, koska $\alpha(\Delta) = -\Delta$. Kaikki transpositiot ovat nyt parittomia (i)-kohdan perusteella. Yleisempi väite saadaan kaavan (1) nojalla siitä, että r-sykli on aina $(r-1)$:n transposition tulo:

$$(a_1 a_2 \dots a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2). \quad \square$$

Koska

$$(ab) = (1a)(1b)(1a),$$

edellisen todistuksen viimeinen kaava osoittaa, että jokainen sykli – ja siis jokainen permutaatio – voidaan kirjoittaa transpositioiden $(12), (13), \dots, (1n)$ tulona. Tuloksena on siis, että *transpositiot* $(12), (13), \dots, (1n)$ *generoivat ryhmän* S_n.

Vertaa ko. transpositioiden lukumäärää ryhmän S_n kertalukuun!

Kaikkien n:n alkion parillisten permutaatioiden joukko

$$A_n = \{\, \alpha \in S_n \;\mid\; \operatorname{sign}(\alpha) = +1 \}$$

muodostaa S_n:n aliryhmän (koska parillisten permutaatioiden tulo on parillinen; ajattele aliryhmäkriteeriä). Sitä sanotaan n:n alkion *alternoivaksi* (alternating) *ryhmäksi.*

Voidaan osoittaa, että $A_1 = S_1$ ja $[S_n : A_n] = 2 \quad \forall\ n \geq 2$. Erityisesti siis $A_n \trianglelefteq S_n$.

Esimerkki 4. Määritetään ryhmän A_4 alkiot.

Permutaatioryhmien merkitystä ryhmäteoriassa valaisee *Cayleyn lause: Jokainen äärellinen ryhmä on isomorfinen jonkin permutaatioryhmän kanssa.*

Todistuksen periaate on yksinkertainen: Olkoot ryhmän G alkiot $x_1, \ldots, x_n$. Kun $x \in G$, kuvaus $t_x : t_x(x_i) = xx_i$ on G:n permutaatio. Merkitään $xx_i = x_j$; todetaan, että indeksin i käydessä läpi joukon $\{1, 2, \ldots, n\}$ myös j käy sen läpi. Tällä tavoin t_x määrittelee permutaation $\alpha_x \in S_n$. Kuvaus

$$p : G \longrightarrow S_n, \qquad p(x) = \alpha_x,$$

on injektiivinen homomorfismi; siis $G \simeq \operatorname{Im}(p) \leqslant S_n$. (Mieti yksityiskohdat.)

Esimerkki 5. Määritetään permutaatioryhmä, jonka kanssa C_3 on isomorfinen.

Harjoitustehtäviä

1. Mitkä ovat seuraavien permutaatioiden kertaluvut?
   a) (14), b) (147), c) (14762), d) (147)(62).
2. Olkoon $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{pmatrix}$ ja $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{pmatrix}$. Laske
   a) α^{-1}, b) $\alpha\beta$, c) $\beta\alpha$.
3. Olkoon $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 3 & 5 & 4 & 7 & 6 & 8 \end{pmatrix}$. Esitä α erillisten syklien tulona.
4. Todista kaava $[S_n : A_n] = 2$. (Käytä esim. homomorfialausetta).

IV.5 Mitä ryhmäteoriassa seuraavaksi?

Tässä pykälässä esitellään lyhyesti muutamia ideoita, joiden avulla edellä käsitelty ryhmien alkeisteoria johtaa useiden laajakantoisten probleemojen ratkaisuun.

Jos $H \lhd G$, ryhmän G ominaisuudet voidaan palauttaa ryhmiin H ja G/H (muista että G/H on ryhmän G homomorfinen kuva). Tämä antaa aiheen määritelmään: Ryhmää G sanotaan *yksinkertaiseksi* (simple), jos sen ainoat normaalit aliryhmät ovat $\{1\}$ ja G.

Esimerkki 1. Syklinen ryhmä C_p on yksinkertainen, kun p on alkuluku.
Voidaan osoittaa, että alternoiva ryhmä A_n on yksinkertainen, kun $n \geq 5$.

Jokainen äärellinen ryhmä G voidaan "rakentaa" yksinkertaisista ryhmistä seuraavassa mielessä: on olemassa sellainen jono normaaleja aliryhmiä,

$$\{1\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_t \trianglelefteq G,$$

että ryhmät G/H_t, $H_t/H_{t-1}, \ldots, H_2/H_1$, H_1 ($\simeq H_1/\{1\}$) ovat yksinkertaisia. Näitä (tekijä)ryhmiä sanotaan ryhmän G *kompositiotekijöiksi*; ne ovat isomorfiaa vaille yksikäsitteiset.

Kaikkien (äärellisten) ryhmien luokittelemiseksi on siis välttämätöntä tuntea kaikki (äärelliset) yksinkertaiset ryhmät. Näiden etsiminen on tarjonnut ryhmäteoreetikoille monivaiheisen "tutkimusmatkan", joka saatiin päätökseen vasta vuonna 1981.

Määritelmä. Äärellistä ryhmää G sanotaan *ratkeavaksi* (solvable), jos sen kompositiotekijät ovat syklisiä ryhmiä, joiden kertaluku on alkuluku.

Helposti todetaan, että ratkeavan ryhmän kaikki aliryhmät ovat ratkeavia.

Esimerkki 2. Symmetrisen ryhmän S_n ratkeavuus:

- $n = 1$, $n = 2$: $S_1 \simeq C_1$, $S_2 \simeq C_2$; siis S_1 ja S_2 ovat ratkeavia.
- $n = 3$: $\{(1)\} \lhd A_3 \lhd S_3$, missä $S_3/A_3 \simeq C_2$ ja $A_3 \simeq C_3$; siis S_3 on ratkeava.
- $n = 4$: $\{(1)\} \lhd \{(1), (12)(34)\} \lhd H_4 \lhd A_4 \lhd S_4$ (ks. IV.4, esimerkki 2), joten S_4:n kompositiotekijät ovat C_2, C_3, C_2, C_2; täten S_4 on ratkeava.
- $n \geq 5$: $\{(1)\} \lhd A_n \lhd S_n$, missä S_n/A_n on yksinkertainen ($\simeq C_2$), samoin A_n (esimerkki 1). Kyseessä siis ovat S_n:n kompositiotekijät. Koska $\#A_n$ ei ole alkuluku, ryhmä S_n ei ole ratkeava ($n \geq 5$).

Jokaiseen yhtälöön

$$p(x) = 0,$$

missä $p(x)$ on n:nnen asteen polynomi, voidaan liittää tietty (yhtälön juurien määräämä) permutaatioryhmä $G_p \leqslant S_n$, joka täyttää seuraavan ehdon: yhtälö $p(x) = 0$ on ratkeava jos ja vain jos ryhmä G_p on ratkeava. Yhtälön ratkeavuus tarkoittaa tässä, että sen juuret

saadaan polynomin kertoimista rationaalisilla laskutoimituksilla ja juurenotoilla (ajattele toisen asteen yhtälön ratkaisukaavaa).

Kutakin n:n arvoa kohti voidaan muodostaa sellainen polynomi $p(x)$, johon liittyvä ryhmä G_p on koko S_n. Nähdään siis, että on olemassa n:nnen asteen yhtälön *yleinen ratkaisukaava* jos ja vain jos ryhmä S_n on ratkeava. Edellinen esimerkki osoittaa, että näin on silloin ja vain silloin, kun $n < 5$.

Tämän tuloksen saavuttivat Abel ja Galois 1800-luvun alkupuolella. Se ratkaisi matemaatikkoja satoja vuosia askarruttaneen kysymyksen ja merkitsi samalla ryhmäteorian alkua.

Cayleyn lauseen todistuksessa (edellinen pykälä) liitettiin ryhmän $G = \{x_1, x_2, \ldots, x_n\}$ kuhunkin alkioon x joukon $\{1, 2, \ldots, n\}$ permutaatio α_x. Olkoon V n-ulotteinen (kompleksikertoiminen) vektoriavaruus ja olkoon $\{B_1, \ldots, B_n\}$ sen kiinnitetty kanta. Kun sovelletaan permutaatiota α_x kantavektoreihin, saadaan säännöllinen lineaarikuvaus $V \to V$. Tätä puolestaan vastaa säännöllinen $n \times n$-matriisi A_x. Näin muodostuu kuvaus

$$G \longrightarrow GL_n(\mathbb{C}), \qquad x \mapsto A_x,$$

joka on ryhmähomomorfismi. Tätä kuvausta – tai G:n homomorfisena kuvana näin saatua matriisiryhmää – sanotaan ryhmän G *säännölliseksi esitykseksi*. Matriisiryhmän $GL_n(C)$ asemesta voidaan yhtä hyvin tarkastella sen kanssa isomorfista kuvausryhmää

$$GL(V) = \left\{ t : V \longrightarrow V \;\middle|\; t \text{ on säännöllinen lineaarikuvaus} \right\}.$$

Yleisesti mitä tahansa ryhmähomomorfismia

$$G \longrightarrow GL_n(\mathbb{C}) \qquad \text{tai} \qquad G \longrightarrow GL(V)$$

sanotaan ryhmän G *esitykseksi* (representation). Esitysten avulla ryhmiä voidaan tutkia matriisien tai lineaarikuvausten teoriaa käyttäen. Tämä ns. ryhmien esitysteoria on osoittautunut hyvin hyödylliseksi sekä itse ryhmäteoriassa että sen sovelluksissa.

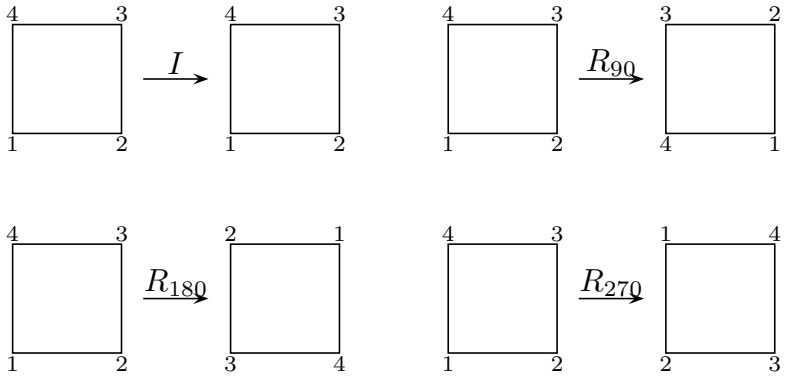
Esimerkki 3. Määritetään syklisen ryhmän C_3 säännöllinen (matriisi)esitys.

IV.6 Neliön symmetriaryhmä eli diedriryhmä D_4

Tässä pykälässä havainnollistetaan luvuissa III ja IV esitettyä teoriaa tutkimalla tarkemmin diedriryhmää D_4. Tarkastellaan siis neliötä ${}^{d}_{a}\square^{c}_{b}$ tason pistejoukkona sekä niitä tason kiertoja ja peilauksia, jotka kuvaavat neliön itselleen. (Katso myös liitteet Symmetriaryhmät ja Matematiikan monet kasvot.)

1. Kierrot

Neliö (tason pistejoukkona) kuvautuu itselleen seuraavissa kierroissa: kulman α kierto neliön keskipisteen ympäri, missä $\alpha = 0,\ \frac{\pi}{2},\ \pi,\ \frac{3\pi}{2}$. Merkitään näitä kiertoja $I = R_0$ (identtinen kuvaus), $R_{90},\ R_{180},\ R_{270}$. Merkitsemällä kärkiä 1, 2, 3, 4 saadaan yhteys neljän alkion permutaatioihin: esim. $R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4$. Tässä käytetään kuitenkin havaintoon perustuvaa geometrista tarkastelua:



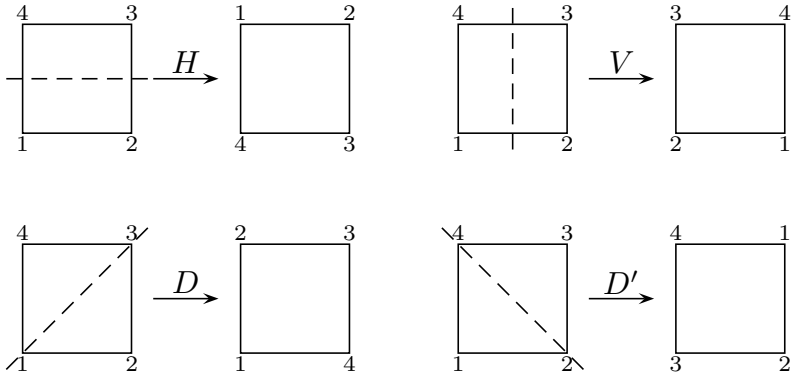
Laskutoimituksena on kuvausten yhdistäminen, esim. $(R_{180}, R_{90}) \mapsto R_{180} \circ R_{90} = R_{270}$. Tällöin on muistettava, että $A \circ B$ tarkoittaa yhdistettyä kuvausta, jossa ensin tehdään B, sitten A. Tämä on tunnetusti assosiatiivinen, neutraalialkio on identtinen kuvaus I, kuvauksilla $I,\ R_{90},\ R_{180},\ R_{270}$ on käänteisalkiot (esim. $R_{270}^{-1} = R_{90}$, koska $R_{270} \circ R_{90} = R_{90} \circ R_{270} = I$). Siis $(\{I, R_{90}, R_{180}, R_{270}\}, \circ)$ on ryhmä. Tarkista oheinen kertotaulu ja totea, että siitä näkyy myös ryhmän kommutatiivisuus (taulukko on symmetrinen lävistäjän suhteen). Kertotaulumerkintä on pykälässä III.2 esitetyn mukainen.

	h	g
h		$h \circ g$
g	$g \circ h$	

$\circ$	I	R_{90}	R_{180}	R_{270}
I	I	R_{90}	R_{180}	R_{270}
R_{90}	R_{90}	R_{180}	R_{270}	I
R_{180}	R_{180}	R_{270}	I	R_{90}
R_{270}	R_{270}	I	R_{90}	R_{180}

2. Peilaukset

Neliöllä on täsmälleen neljä symmetria-akselia (ks. kuva) ja se kuvautuu itselleen peilauksissa niiden suhteen: H on peilaus vaaka-akselin suhteen, V peilaus pystyakselin suhteen, D peilaus kärkien 1 ja 3 kautta kulkevan lävistäjän suhteen ja D' peilaus kärkien 2 ja 4 kautta kulkevan lävistäjän suhteen.



Esimerkiksi $(\{I, H\}, \circ)$ muodostaa ryhmän, jonka kertotaulu on

$\circ$	I	H
I	I	H
H	H	I

Vertaa tätä ryhmään $(\mathbb{Z}_2, +)$. Muodostaako $(\{I, H, D\}, \circ)$ ryhmän?

Yhdistämällä em. peilauksia saadaan esim. $H \circ V = R_{180}$ (tarkista seuraamalla, miten kärkipisteet kuvautuvat – montako kärkipistettä riittää?). Peilaukset eivät siis muodosta ryhmää, mutta $(\{I, R_{90}, R_{180}, R_{270}, H, V, D, D'\}, \circ)$ on ryhmä, *neliön symmetriaryhmä* eli *diedriryhmä* D_4 ja sille saadaan kertotaulu:

$\circ$	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
I	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	I	D	D'	V	H
R_{180}	R_{180}	R_{270}	I	R_{90}	V	H	D'	D
R_{270}	R_{270}	I	R_{90}	R_{180}	D'	D	H	V
H	H	D'	V	D	I	R_{180}	R_{270}	R_{90}
V	V	D	H	D'	R_{180}	I	R_{90}	R_{270}
D	D	H	D'	V	R_{90}	R_{270}	I	R_{180}
D'	D'	V	D	H	R_{270}	R_{90}	R_{180}	I

Tämä ryhmä ei ole kommutatiivinen (esim. $H \circ R_{270} = D$, $R_{270} \circ H = D'$). Kuvauksia I, R_{90}, R_{180}, R_{270}, H, V, D_1, D' sanotaan neliön *symmetrioiksi*.

Neliön kiertojen ryhmä $G = (\{I, R_{90}, R_{180}, R_{270}\}, \circ)$ on D_4:n aliryhmä, esim. siksi että G todettiin edellä ryhmäksi ja $G \subset D_4$.

3. D_4:n aliryhmät

a) Tutkitaan ensin neliön kiertojen muodostamaa aliryhmää G. Vertaamalla allaolevia taulukoita todetaan, että $(\mathbb{Z}_4, +)$ on isomorfinen ryhmän $(G, \circ)$ kanssa:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

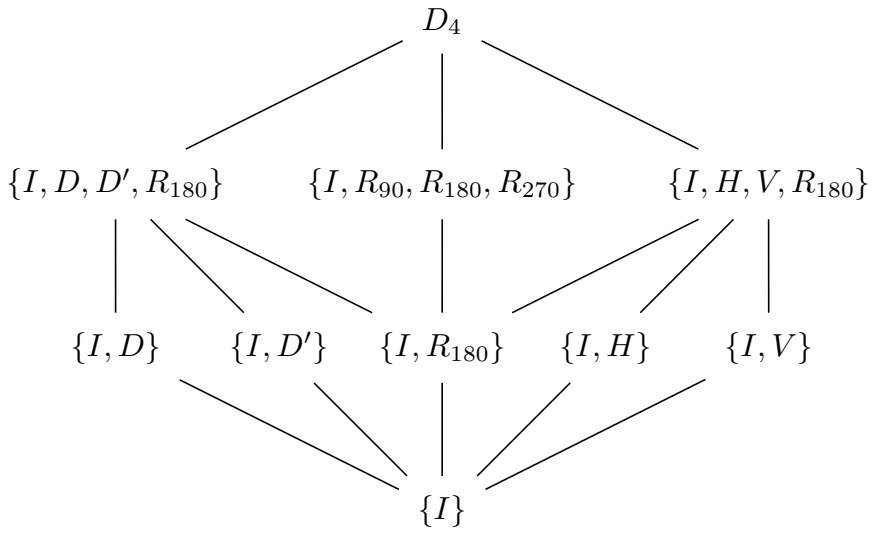
$\circ$	I	R_{90}	R_{180}	R_{270}
I	I	R_{90}	R_{180}	R_{270}
R_{90}	R_{90}	R_{180}	R_{270}	I
R_{180}	R_{180}	R_{270}	I	R_{90}
R_{270}	R_{270}	I	R_{90}	R_{180}

Kuvaus $f : 0 \mapsto I,\ 1 \mapsto R_{90},\ 2 \mapsto R_{180},\ 3 \mapsto R_{270}$ on bijektio $\mathbb{Z}_4 \to G$ ja ryhmähomomorfismi, koska kaikilla $a,\ b \in \mathbb{Z}_4$ on $f(a+b) = f(a) \circ f(b)$. Huomaa myös kaavan $f(x^{-1}) = f(x)^{-1}$ tulkinta (tässä $f(-x) = f(x)^{-1}$), esim. $-3 = 1$ (koska $3 + 1 = 0$) ja $f(-3) = f(1) = R_{90} = R_{270}^{-1} = f(3)^{-1}$.

b) G on esimerkki syklisestä ryhmästä, esim. R_{270} virittää sen: käyttämällä tavallista merkintää $R_{270}^2 = R_{270} \circ R_{270}$ saadaan $R_{270}^2 = R_{180}$; $R_{270}^3 = R_{90}$, $R_{270}^4 = I$. Myös R_{90} virittää ryhmän G : $(R_{90})^2 = R_{180}$, $(R_{90})^3 = R_{270}, (R_{90})^4 = I$. Huomaa myös geometria: R_{270} on kulman $-\frac{\pi}{4}$ kierto ja R_{90} on kulman $\frac{\pi}{4}$ kierto, siis R_{270} on kierto negatiiviseen suuntaan ("myötäpäivään"), R_{90} positiiviseen suuntaan ("vastapäivään").

c) D_4:n aliryhmät. Etsitään kaikki D_4:n aliryhmät käyttämättä apuna geometriaa. Helpointa on aloittaa tutkimalla, mitkä ovat D_4:n sykliset aliryhmät, ts. tyyppiä $\{a^n \mid n \in \mathbb{Z}\}$ olevat aliryhmät. Joka tapauksessa ryhmällä on yhden alkion syklinen aliryhmä $\{I\}$. Kahden alkion sykliset D_4:n aliryhmät saadaan ottamalla identtisen kuvauksen lisäksi jokin peilaus tai kierto π:llä (tapaukset, joissa kuvauksen kertaluku on 2 eli kuvaus on oma käänteiskuvauksensa): $\{I, D\}$, $\{I, D'\}$, $\{I, R_{180}\}$, $\{I, H\}$, $\{I, V\}$. (Totea tämä kertotaulusta ja vertaa sitä luvun III.1 harjoitustehtävään 6.) Kolmen alkion syklisiä aliryhmiä ei tässä tapauksessa ole, mutta G on neljän alkion syklinen aliryhmä. Muita syklisiä aliryhmiä ei ole. (Käyttämällä hyväksi tietoa $\#D_4 = 8 = 2 \cdot 2 \cdot 2$ saataisiin suoraan tulos, että D_4:llä voi olla vain aliryhmiä, joissa on 1, 2, 4 tai 8 alkiota.)

Kokeilemalla tutkitaan, mitkä ovat D_4:n aliryhmät, jotka eivät ole syklisiä mutta jotka saadaan kahden alkion virittäminä. Olkoon S alkioiden a ja b virittämä. Silloin on oltava $a^n,\ b^n \in S$ ja $a^i b^j \in S$ aina kun $n, i, j \in \mathbb{Z}$, ja toisaalta näistä alkioista saadaan tässä tapauksessa aliryhmä. Aliryhmän $\{I, D, D', R_{180}\}$ virittäjät ovat $D,\ D'$ tai $D,\ R_{180}$ tai $D',\ R_{180}$. Aliryhmän $\{I, H, V, R_{180}\}$ virittäjät ovat $R_{180},\ H$ tai $H,\ V$ tai $R_{180},\ V$. Ryhmän D_4 virittäjät ovat $R_{270},\ H$ tai $D,\ H$ tai $D',\ H$.



D_4:n aliryhmät järjestettyinä sisältymisrelaation suhteen, eli ryhmän D_4 Hassen kaavio.

Tarkastellaan vielä lähemmin väitettä, että D_4:n virittävät R_{270} ja H:

$$R_{270}^0 = I,\ R_{270} = R_{270},\ R_{270}^2 = R_{180},\ R_{270}^3 = R_{90},\ H = H,$$
$$R_{270} \circ H = D',\ R_{270}^2 \circ H = V,\ R_{270}^3 \circ H = D,$$
$$R_{270}^4 = I,\ H^2 = I.$$

Kaikki ryhmän D_4 alkiot voidaan esittää yksikäsitteisesti muodossa

$$R_{270}^j H^i, \qquad j = 0, 1, 2, 3, \quad i = 0, 1.$$

Tämän varmistamiseksi on huomattava, että

$$H \circ R_{270} = R_{270}^3 \circ H, \quad R_{270}^4 = I, \quad H^2 = I$$

(ns. *relaatiot*). Esim.

$$V \circ D' = (R_{270}^2 \circ H) \circ (R_{270} \circ H) = R_{270}^2 \circ (H \circ R_{270}) \circ H$$
$$= R_{270}^2 \circ R_{270}^3 \circ H \circ H = R_{270} \circ H^2 = R_{270} \circ I = R_{270}$$

.

4. Sivuluokat

Määritetään suoraan laskemalla, nojautumatta yleiseen teoriaan, mitkä ovat aliryhmän $S = \{I, H\}$ vasemmanpuoleiset sivuluokat. Nämä ovat siis tyyppiä $x \circ S,\ x \in D_4$:

$$
\begin{aligned}
I \circ \{I, H\} &= \{I, H\},\\
R_{180} \circ \{I, H\} &= \{R_{180} \circ I, R_{180} \circ H\} = \{R_{180}, V\},\\
R_{270} \circ \{I, H\} &= \{R_{270}, R_{270} \circ H\} = \{R_{270}, D'\},\\
R_{90} \circ \{I, H\} &= \{R_{90}, R_{90} \circ H\} = \{R_{90}, D\},\\
H \circ \{I, H\} &= \{H, I\},\ V \circ \{I, H\} = \{V, R_{180}\},\\
D \circ \{I, H\} &= \{D, R_{90}\},\ D' \circ \{I, H\} = \{D', R_{270}\}.
\end{aligned}
$$

Siis S:n vasemmanpuoleiset sivuluokat ovat $\{I, H\}$, $\{R_{180}, V\}$, $\{R_{270}, D'\}$ ja $\{R_{90}, D\}$. S ei ole normaali, koska esim. $R_{270} \circ \{I, H\} = \{R_{270}, D'\}$ ja $\{I, H\} \circ R_{270} = \{R_{270}, H \circ R_{270}\} = \{R_{270}, D\}$.

Lopuksi todetaan, että on saatu ryhmän D_4 ositus neljään sivuluokkaan, joissa kussakin on kaksi alkiota. Koska $2 \cdot 4 = 8$, näin pitääkin olla. (Minkä lauseen perusteella?)

5. D_4:n keskus

Määritetään joukko $N = \{x \in D_4 \mid x \circ y = y \circ x \quad \forall y \in D_4\}$. Kertotaulusta nähdään, että $N = \{I, R_{180}\}$. N on normaali aliryhmä, koska $y \circ N = N \circ y$, $\forall y \in D_4$. Nyt sivuluokat ovat

$$
\begin{aligned}
I \circ N = R_{180} \circ N &= \{I, R_{180}\},\\
R_{270} \circ N = R_{90} \circ N &= \{R_{270}, R_{90}\},\\
H \circ N = V \circ N &= \{H, V\},\\
D \circ N = D' \circ N &= \{D, D'\}
\end{aligned}
$$

ja esim. $R_{270} \circ \{I, R_{180}\} = \{R_{270}, R_{90}\} = \{I, R_{180}\} \circ R_{270}$. Koska $\{I, R_{180}\}$ on normaali aliryhmä, voidaan muodostaa tekijäryhmä

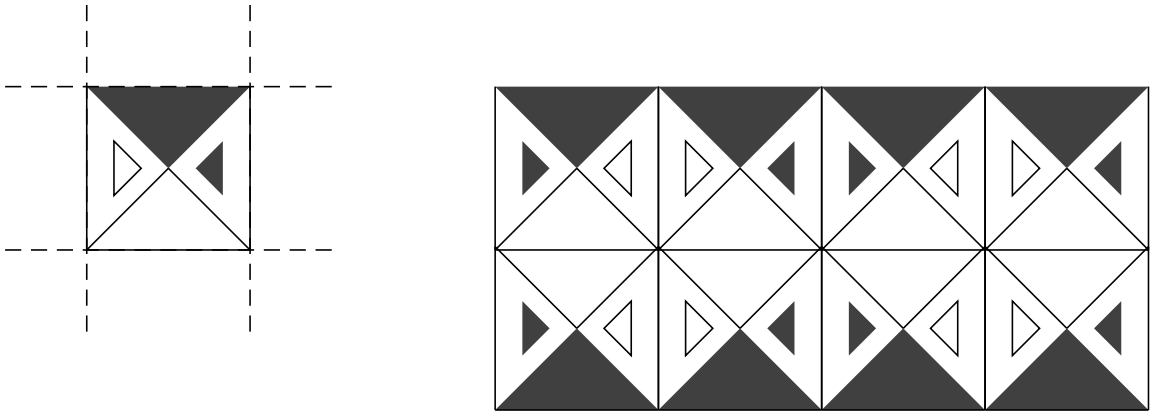
$$D_4/N = \big\{\{R_{270}, R_{90}\}, \{H, V\}, \{D, D'\}, \{I, R_{180}\}\big\}.$$

Laskutoimitus on $(x \circ N) \circ (y \circ N) = (x \circ y) \circ N$.

(Esim. $\{R_{270}, R_{90}\} \circ \{H, V\} = (R_{270} \circ N) \circ (H \circ N) = (R_{270} \circ H) \circ N = D' \circ N = \{D, D'\}$.)
Projektio $\pi : D_4 \to D_4/N$ on homomorfismi, $\pi(x) = x \circ N$, $\quad \mathrm{Ker}(\pi) = N$.

6. Ornamentit

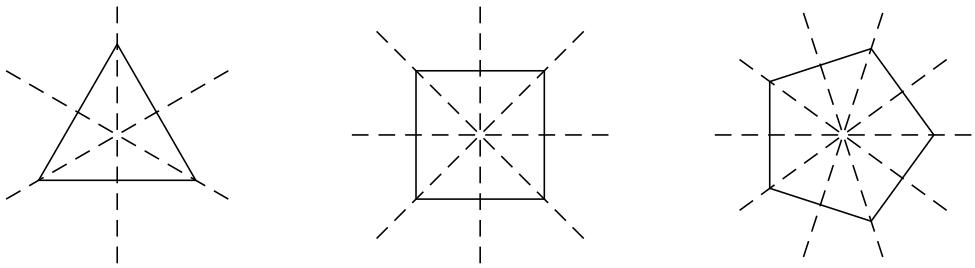
Säännöllisten geometristen kuvioiden symmetriaryhmiä käytetään mm. ornamenttikoristelussa.



Peilaamalla neliön sivujen suhteen (peilausakselit merkitty pilkkuviivoilla), saadaan taso peitetyksi ylläolevalla tavalla neliönkuvilla. Huomaa, että yhdistämällä peilaukset vaaka- ja pystyakselin suhteen saadaan kulman π suuruinen kierto neliön kärjen ympäri (edellä $H \circ V = V \circ H = R_{180}$).

7. D_n ja C_n

D_n on säännöllisen n-kulmion symmetriaryhmä, kun $n \geq 3$. Ryhmällä D_n on syklinen aliryhmä C_n, jonka virittää kierto R kulman $2\pi/n$ verran n-kulmion keskipisteen ympäri; siis $R^n = I$. Lisäksi ryhmään D_n kuuluvat peilaukset n-kulmion symmetria-akselien suhteen.



$n = 3$ $n = 4$ $n = 5$

Jos merkitään peilausta jonkin symmetria-akselin suhteen H:lla, niin ryhmässä D_n ovat voimassa relaatiot $H^2 = I,\ R^n = I$ ja kuvaukset H ja R virittävät ryhmän D_n.

Harjoitustehtäviä

1. Olkoon G ympyrän symmetriaryhmä. Osoita, että jokaista positiivista kokonaislukua n kohti on G:n alkio, jonka kertaluku on n. Etsi jokin G:n alkio, jonka kertaluku on ääretön.
2. Mitä kuvauksia kuuluu ryhmään D_6? Millä n:n arvoilla $C_n \leq D_6$?

V. RENGAS JA KOKONAISALUE

V.1 Rengas

Ryhmä kuuluu algebrallisiin systeemeihin, joissa on määritelty yksi laskutoimitus. Seuraavassa määritellään kahden laskutoimituksen systeemi, *rengas*, josta tyypillinen esimerkki on kokonaislukujen joukko $\mathbb{Z}$ varustettuna yhteen- ja kertolaskulla. Myös yleisessä määritelmässä on tapana käyttää ko. laskutoimituksille yhteen- ja kertolaskumerkintää.

MÄÄRITELMÄ. Kolmikkoa $(R, +, \cdot)$ sanotaan *renkaaksi*, jos se täyttää ehdot

R1. $(R, +)$ on Abelin ryhmä (ns. *renkaan additiivinen ryhmä)*;

R2. kertolasku $\cdot$ on joukossa R määritelty laskutoimitus;

R3. $a(bc) = (ab)c \quad \forall\ a, b, c \in R$ (tulon *assosiatiivisuus*);

R4. joukossa R on sellainen alkio 1 (renkaan *ykkösalkio*), että $a{\cdot}1 = 1{\cdot}a = a\ \forall\ a \in R$;

R5. $a(b + c) = ab + ac, \quad (a + b)c = ac + bc \quad \forall\ a, b, c \in R$ (*distributiivisuus*).

Rengas R on siis joukko, jossa on annettu kaksi laskutoimitusta, jotka toteuttavat yllämainitut ehdot.

Jos kertolasku lisäksi on kommutatiivinen, ts. $ab = ba \quad \forall\ a, b \in R$, sanotaan että R on *kommutatiivinen rengas.*

Postulaatit R2, R3 ja R4 yhdessä ilmaisevat, että $(R, \cdot)$ on monoidi (ks. huomautus III.1:n lopussa). Joskus renkaan määritelmästä jätetään postulaatti R4 pois, ts. $(R, \cdot)$:sta vaaditaan vain, että se on puoliryhmä. Tällöin yllä määriteltyä rengasta sanotaan *ykkösalkiolla varustetuksi.*

Renkaan ykkösalkio 1 on välttämättä yksikäsitteinen. Tämä seuraa postulaatista R4 samalla tavoin kuin ryhmillä.

Postulaatti R1 tuottaa renkaaseen *nolla-alkion* 0 ja alkioiden a *vasta-alkiot* $-a$. Lisäksi R1:stä seuraa, että renkaan yhteenlasku on assosiatiivinen ja kommutatiivinen.

ESIMERKKI 1 (LUKURENKAAT). Esim. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ovat renkaita tavallisen yhteen- ja kertolaskun suhteen, ykkösalkiona luku 1. Sensijaan esimerkiksi $2\mathbb{Z}$ ei ole rengas.

Myös esim. joukko $\mathbb{Z}[i] = \left\{ a + bi \;\middle|\; a, b \in \mathbb{Z} \right\}$ on rengas lukujen yhteen- ja kertolaskun suhteen (ns. *Gaussin kokonaisluvut*).

Lukurenkaat ovat kommutatiivisia.

ESIMERKKI 2 (MATRIISIRENKAAT). Tyyppiä $n \times n$ olevien reaalialkioisten matriisien joukko $\mathcal{M}_n(\mathbb{R})$ muodostaa renkaan matriisien yhteen- ja kertolaskun suhteen, ykkösalkiona identiteettimatriisi I_n. Muita matriisirenkaita ovat esim. $\mathcal{M}_n(\mathbb{Z})$, $\mathcal{M}_n(\mathbb{Q})$, $\mathcal{M}_n(\mathbb{C})$ (tarkista, että nämä joukot ovat suljettuja kyseisten laskutoimitusten suhteen).

Mainitut matriisirenkaat ovat epäkommutatiivisia, kun $n > 1$.

Esimerkki 3 (Funktiorenkaat). Funktiojoukko

$$C[a,b] = \{\, f : [a,b] \longrightarrow \mathbb{R} \;\mid\; f \;\text{ jatkuva} \,\}$$

on rengas funktioiden "pisteittäisen" yhteen- ja kertolaskun suhteen:

$$(f+g)(x) = f(x) + g(x), \qquad (fg)(x) = f(x)g(x) \quad \forall\ x \in [a,b].$$

Ykkösalkiona on funktio $f(x) = 1 \quad \forall\ x \in [a,b]$. (Muista, että $C[a,b]$ on myös vektoriavaruus. Siitä seuraa, että $(C[a,b], +)$ on Abelin ryhmä; vrt. III.1:n esimerkki 2.)

Rengas $C[a,b]$ on kommutatiivinen. Määritelmä voidaan yleistää korvaamalla $\mathbb{R}$ mielivaltaisella renkaalla R, jolloin kommutatiivisuus riippuu renkaan R kommutatiivisuudesta.

Esimerkki 4 (Jäännösluokkarenkaat). Jäännösluokkien $\bmod m$ joukko $\mathbb{Z}_m$ muodostaa renkaan jäännösluokkien yhteen- ja kertolaskun suhteen, ykkösalkiona $\overline{1}$.

$\mathbb{Z}_m$ on äärellinen kommutatiivinen rengas. Siitä käytetään nimitystä *jäännösluokkarengas modulo m*. (Jäännösluokkarengas-termi otetaan myöhemmin käyttöön yleisemmässä merkityksessä.)

Esimerkki 5 (Boolen renkaat). Annetun joukon S kaikkien osajoukkojen parvi $\mathcal{P}(S)$ muodostaa renkaan, jossa yhteenlaskuna on joukkojen *symmetrinen erotus*

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

ja kertolaskuna joukkojen leikkaus $A \cap B$. Nolla-alkiona on $\emptyset$, ykkösalkiona S. (Käy läpi postulaatit.)

Esimerkki 6 (Endomorfismirenkaat). Olkoon $(G, +)$ jokin Abelin ryhmä. Joukko

$$\mathrm{End}(G) = \{\, f : G \longrightarrow G \;\mid\; f \;\text{ on ryhmähomomorfismi} \,\}$$

muodostaa renkaan kuvausten (pisteittäisen) summan ja kuvaustulon suhteen:

$$(f+g)(a) = f(a) + g(a), \qquad (f \circ g)(a) = f(g(a)) \quad \forall\ a \in G.$$

Ykkösalkiona on identiteettikuvaus id_G. Postulaattien tarkistaminen on hyvä harjoitustehtävä!

Ryhmähomomorfismia $G \to G$ sanotaan ryhmän G *endomorfismiksi.* Tästä johtuu renkaan $\mathrm{End}(G)$ merkintä ja nimitys *endomorfismirengas.* Tämä rengas ei yleensä ole kommutatiivinen.

Yhden alkion joukko $R = \{a\}$ muodostaa triviaalisti renkaan, kun määritellään $a+a = a$ ja $a \cdot a = a$. Koska a on silloin R:n nolla-alkio, tätä rengasta sanotaan myös *nollarenkaaksi.*

Vastedes oletetaan (ellei toisin mainita), ettei rengas R ole nollarengas.

MÄÄRITELMÄ. Renkaan R alkiota u sanotaan renkaan *yksiköksi* (unit), jos u:lla on käänteisalkio u^{-1} renkaassa R, ts. jos $\exists\ u^{-1} \in R :\ uu^{-1} = u^{-1}u = 1$.

Renkaan kaikkien yksiköiden joukosta käytetään merkintää R^*.

Lause 1. *$(R^*, \cdot)$ on ryhmä (renkaan R yksikköryhmä).*

Todistus. $R^* \neq \emptyset$, koska 1 on yksikkö (käänteisalkiona 1). Joukko R^* on suljettu kertolaskun suhteen, koska kahden yksikön u ja v tulolla uv on käänteisalkio $v^{-1}u^{-1}$.

Tulo on assosiatiivinen koko R:ssä, siis myös R^*:ssä. Jos $u \in R^*$, myös sen käänteisalkio $u^{-1} \in R^*$, sillä $(u^{-1})^{-1} = u$. $\square$

ESIMERKKI 7. Lukurenkaiden $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ yksikköryhmät ovat $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Nämä ovat ryhmäteoriasta tuttuja ryhmiä, samoin kuin jäännösluokkarenkaan $\mathbb{Z}_m$ $(m \geq 2)$ yksikköryhmä $\mathbb{Z}_m^* = \left\{ \overline{a} \in \mathbb{Z}_m \;\middle|\; \text{syt}(a, m) = 1 \right\}$.

Esimerkkejä muista yksikköryhmistä:

$$\mathbb{Z}^* = \{-1, +1\}, \qquad \mathcal{M}_n(R)^* = GL_n(\mathbb{R}) = \left\{ A \in \mathcal{M}_n(\mathbb{R}) \;\middle|\; \det(A) \neq 0 \right\}.$$

Harjoitustehtäviä

1. Joukolla $\{0_6, 2_6, 4_6\}$ on ykkösalkio kertolaskun suhteen. Mikä se on?
2. Määritellään $\mathbb{Z}$:ssa laskutoimitukset
$$x \oplus y = x + y - 1,\ x \odot y = x + y - xy.$$
Osoita, että $(\mathbb{Z}, \oplus, \odot)$ on rengas.
3. Osoita, että joukko $\{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ on lukujen yhteen- ja kertolaskun suhteen kommutatiivinen rengas.
4. Näytä, että kertolasku
$$(a, b, c)(x, y, z) = (ax, bx + cy, cz)$$
tekee tuloryhmästä $(\mathbb{Z}^3, +)$ ei-kommutatiivisen renkaan, jolla on ykkösalkio $(1, 0, 1)$.
5. Olkoot $(R_1, +, \cdot)$ ja $(R_2, +, \cdot)$ renkaita. Osoita, että $(R_1 \times R_2, +, \cdot)$ on rengas (ns. tulorengas), kun määritellään
$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2),$$
$$(x_1, x_2)\,(y_1, y_2) = (x_1 y_1, x_2 y_2).$$
6. Määritä lukurenkaan $\mathbb{Z}[i]$ yksiköt. Onko tämä yksikköryhmä syklinen?

V.2 Renkaan aritmetiikkaa

Koska $(R,+)$ on ryhmä (vieläpä Abelin), yhteenlasku renkaassa noudattaa ryhmäteoriasta tuttuja sääntöjä. Kuten aina additiivisessa ryhmässä, alkioiden a ja b *erotus* $a-b=a+(-b)$.

Myös kertolaskusäännöt voidaan päätellä ryhmäteoriasta. Huomaa, että alkion a negatiiviset potenssit on määritelty vain, kun a:lla on käänteisalkio a^{-1}.

Nyt esitetään tarvittavat säännöt siitä, miten renkaan kertolasku kytkeytyy yhteenlaskuun. Pohjana on tietysti distributiivisuus R5. Ensiksikin niistä saadaan induktiolla kaavat

$$a(b_1+\cdots+b_n)=ab_1+\cdots+ab_n,$$
$$(a_1+\cdots+a_m)b=a_1b+\cdots+a_mb$$

ja yleisemmin kaava

$$(a_1+\cdots+a_m)(b_1+\cdots+b_n)=a_1b_1+a_1b_2+\cdots+a_mb_n.$$

Lause 2. *Jos R on rengas ja $a,b,c\in R$, niin*

(i) $0\cdot a=a\cdot 0=0$,

(ii) $a(-b)=(-a)b=-(ab)$, $(-a)(-b)=ab$,

(iii) $a(b-c)=ab-ac$, $(a-b)c=ac-bc$.

Todistus. (i) Kirjoittamalla $0\cdot a=(0+0)a=0\cdot a+0\cdot a$ ja vähentämällä saadun yhtälön molemmilta puolilta $0\cdot a$ päädytään yhtälöön $0=0\cdot a$. Väite $a\cdot 0=0$ todistetaan samoin.

(ii) Koska $ab+a(-b)=a(b+(-b))=a\cdot 0=0$, tulo $a(-b)$ on (ab):n vasta-alkio. Samoin nähdään, että myös $(-a)b$ on (ab):n vasta-alkio.

Edellisten yhtälöiden avulla saadaan $(-a)(-b)=-((-a)b)=-(-(ab))=ab$.

(iii) $a(b-c)=ab+a(-c)=ab+(-(ac))=ab-ac$; jälkimmäinen samoin. □

Huomautus 1. Lause 2 voidaan todistaa myös tarkastelemalla kuvauksia

$$\rho: R\to R, \qquad \rho(a)=ab,$$
$$\tau: R\to R, \qquad \tau(a)=ba,$$

missä $b\in R$ on kiinteä. Kuvaukset ρ ja τ ovat ryhmän $(R,+)$ homomorfismeja (endomorfismeja) ja väitteet (i)–(iii) seuraavat homomorfismien perusominaisuuksista.

HUOMAUTUS 2. (i)-kohdasta seuraa: *Renkaassa on aina* $1 \neq 0$. Jos näet $1 = 0$, niin $a = a\cdot 1 = a\cdot 0 = 0 \quad \forall\ a \in R$. (Muista, että tapaus $R = \{0\}$ suljettiin pois.)

(ii)-kohdan nojalla voidaan ilman sekaannuksen vaaraa käyttää merkintää $-ab$ (miinusmerkki voidaan ajatella kuuluvaksi joko tuloon ab tai alkioon a).

Kuten ryhmäteoriassa todettiin, alkioiden monikerrat toteuttavat laskulait

$$(m+n)a = ma + na, \quad (mn)a = m(na), \quad n(a+b) = na + nb \quad \forall\ m, n \in \mathbb{Z},\ a, b \in R.$$

Huomaa myös, että merkinnät $0a$ ja $1a$ voidaan ymmärtää kahdella tavalla, mutta joka tapauksessa $0a = 0$ ja $1a = a$. Selvyyden vuoksi voidaan renkaan nolla- ja ykkösalkiolle käyttää myös merkintöjä 0_R ja 1_R.

Lause 3. *Jos R on rengas ja $a, b \in R$, niin*

(iv) $na = (n\cdot 1)a = a(n\cdot 1) \quad \forall\ n \in \mathbb{Z} \quad$ (tässä $1 = 1_R$),

(v) $n(ab) = (na)b = a(nb) \quad \forall\ n \in \mathbb{Z}$,

(vi) $(ma)(nb) = (mn)(ab) \quad \forall\ m, n \in \mathbb{Z}$.

Todistus. (iv) Jos $n = 0$, kaikki kolme tuloa ovat $= 0$. Olkoon sitten $n > 0$. Tällöin on ensinnä

$$(n\cdot 1)a = (1 + \cdots + 1)a = a + \cdots + a = na.$$

Edelleen $(-n)\cdot 1 = n(-1)$ ja $(-n)a = n(-a)$ negatiivisen monikerran määritelmän nojalla; siis

$$((-n)\cdot 1)a = ((-1) + \cdots + (-1))a = (-a) + \cdots + (-a) = n(-a) = (-n)a.$$

Tulot $a(n\cdot 1)$ ja $a((-n)\cdot 1)$ käsitellään samoin.

(v) palautuu helposti (iv)-kohtaan; (vi) palautuu (v):een. □

Myös tämä voidaan todistaa toisella tavalla käyttäen huomautuksessa 1 mainittuja homomorfismeja ρ ja τ.

ESIMERKKI 1. $(a+b)^2 = a^2 + ab + ba + b^2$.
Jos R on kommutatiivinen, niin $(a+b)^2 = a^2 + 2ab + b^2$ ja yleisesti

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + b^n.$$

ESIMERKKI 2. Renkaassa $\mathbb{Z}_m$ on (iv)-kohdan perusteella $k\overline{a} = \overline{k}\cdot\overline{a} \quad \forall\ k, a \in \mathbb{Z}$.
Renkaassa $\mathbb{Z}_2$ on $(\overline{a} + \overline{b})^2 = (\overline{a})^2 + (\overline{b})^2$, koska $2\overline{ab} = \overline{2}\cdot\overline{ab} = \overline{0}\cdot\overline{ab} = \overline{0}$.

Harjoitustehtäviä

1. Todista kommutatiivisessa renkaassa oikeaksi kaava $x^2 - y^2 = (x + y)(x - y)$.
2. Osoita, että rengas R on kommutatiivinen, jos ja vain jos $(x + y)^2 = x^2 + y^2 + 2xy \ \forall x, y \in R$.
3. Oletetaan, että renkaassa $(R, +, \cdot)$ on $x^2 = x \ \forall x \in R$. Osoita, että $2x = 0 \ \ \forall x \in R$ ja että R on kommutatiivinen.
4. Mitkä seuraavista yhtälöistä pätevät (mielivaltaisessa) renkaassa R?
   a) $a^2 - ba = (a - b)a$,
   b) $(a + b + 1)(a - b - 1) = a^2 - b^2 - 2b - 1$,
   c) $2a \cdot 4b - ab = 7ab$.

V.3 Alirengas ja ideaali

MÄÄRITELMÄ. Renkaan $(R, +, \cdot)$ osajoukkoa S sanotaan R:n *alirenkaaksi*, jos

AR1. S on rengas operaatioiden $+$ ja $\cdot$ suhteen ja

AR2. S:n ykkösalkio = R:n ykkösalkio.

Jos S on renkaan R alirengas, niin $(S, +)$ on ryhmän $(R, +)$ aliryhmä. Tästä seuraa mm., että R:n nolla-alkio 0 kuuluu S:ään ja on S:n nolla-alkio.

ESIMERKKI 1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$; tässä jokainen rengas on sitä seuraavien renkaiden (aito) alirengas.

ESIMERKKI 2. Kaikki matriisit $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, missä $a \in \mathbb{R}$, muodostavat renkaan, joka sisältyy matriisirenkaaseen $\mathcal{M}_2(\mathbb{R})$. Se ei kuitenkaan ole $\mathcal{M}_2(\mathbb{R})$:n alirengas, koska sen ykkösalkiona on matriisi $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Lause 4 (Alirengaskriteeri). *Olkoon R rengas ja $S \subset R$. Silloin S on R:n alirengas jos ja vain jos seuraavat ehdot toteutuvat:*

(a) $1_R \in S$,

(b) $a - b \in S \quad \forall\ a, b \in S$,

(c) $ab \in S \quad \forall\ a, b \in S$.

Todistus. Jos S on R:n alirengas, se täyttää triviaalisti ko. ehdot. Kääntäen ehdon (a) nojalla $S \neq \emptyset$ ja täten ehdosta (b) seuraa, että $(S, +)$ on ryhmän $(R, +)$ aliryhmä. Ehdot (a) ja (c) takaavat, että S toteuttaa rengaspostulaatit R4 ja R2. Postulaateissa R3 ja R5 vaaditut laskulait periytyvät S:ään renkaalta R. Täten AR1 toteutuu, ja AR2 seuraa suoraan ehdosta (a). □

Annettu joukko voidaan usein todeta renkaaksi helpommin alirengaskriteeriä käyttäen kuin käymällä läpi rengaspostulaatit.

Esimerkki 3. Lukujoukot

$$\mathbb{Z}\left[\sqrt{n}\,\right] = \left\{\, a + b\sqrt{n} \;\middle|\; a, b \in \mathbb{Z} \right\} \qquad (n = -1, \pm 2, \pm 3, \dots)$$

ovat $\mathbb{C}$:n alirenkaita (ja myös $\mathbb{R}$:n alirenkaita, kun $n > 0$). Erikoistapauksessa $n = -1$ kyseessä ovat Gaussin kokonaisluvut (V.1:n esimerkki 1).

Renkaita $\mathbb{Z}\left[\sqrt{n}\,\right]$ tarkasteltaessa oletetaan tavallisesti, että n on *neliövapaa*, ts. ei ole jaollinen minkään kokonaisluvun > 1 neliöllä. Silloin $\mathbb{Z}\left[\sqrt{n_1}\,\right] \neq \mathbb{Z}\left[\sqrt{n_2}\,\right]$ aina kun $n_1 \neq n_2$.

Esimerkki 4 (Polynomirenkaat). Kaikkien reaalikertoimisten polynomien joukko

$$\mathbb{R}[x] = \left\{\, a_0 + a_1 x + \cdots + a_n x^n \;\middle|\; n \geq 0, \quad a_k \in \mathbb{R}\ \ (k = 0, \dots, n) \right\}$$

on rengas polynomien yhteen- ja kertolaskun suhteen, nimittäin funktiorenkaan

$$C(\mathbb{R}) = \left\{\, f : \mathbb{R} \longrightarrow \mathbb{R} \;\middle|\; f \ \text{ jatkuva } \right\}$$

alirengas (vrt. V.1:n esimerkki 3).

Muita polynomirenkaita ovat esim. $\mathbb{R}[x]$:n alirenkaat $\mathbb{Z}[x]$ ja $\mathbb{Q}[x]$ (siis kertoimet vastaavasti kokonais- tai rationaalilukuja). Myöhemmin käsitellään yleistä polynomirengasta $R[x]$, missä R on mikä tahansa kommutatiivinen rengas.

Esimerkki 5. Olkoon V (reaalinen) vektoriavaruus. Lineaarikuvausten joukko

$$\mathrm{End}_{\mathbb{R}}(V) = \left\{\, t : V \longrightarrow V \;\middle|\; t \ \text{ lineaarinen } \right\}$$

on $\mathrm{End}(V)$:n alirengas. Tässä $\mathrm{End}(V)$ tarkoittaa V.1:n esimerkin 6 mukaan ryhmän $(V, +)$ endomorfismeja; kuvausten summa määritellään pisteittäin ja kuvausten tulo yhdistettynä kuvauksena.

Ryhmäteoriassa todettiin, että ryhmän kaikkien aliryhmien joukossa *normaaleilla* aliryhmillä on erityisasema. Rengasteoriassa normaaleja aliryhmiä vastaavat *ideaalit.*

MÄÄRITELMÄ. Renkaan R osajoukkoa I sanotaan R:n *ihanteeksi* eli *ideaaliksi*, jos

I1. $(I,+)$ on ryhmän $(R,+)$ aliryhmä ja

I2. $ra \in I$ ja $ar \in I \quad \forall\ r \in R$ ja $a \in I$.

(Jos I2:ssa jätetään pois ehto $ar \in I$, saadaan yleisempi ns. *vasemman ideaalin* käsite; vastaavasti *oikea ideaali*.)

Jokaisella renkaalla R on triviaaleina ideaaleina R itse ja nollaideaali $\{0\}$.

Onko renkaan ideaali I myös alirengas? Jos se on, niin $1 \in I$ ja siis ehdon I2 nojalla $r \in I \quad \forall\ r \in R$, toisin sanoen $I = R$. Näin ollen R itse on ainoa R:n ideaali, joka on (ali)rengas.

Edellinen päättely antaa myös tuloksen: *Jos I on renkaan R aito ideaali (siis $I \subset R$), niin $I \cap R^* = \emptyset$.* Yksikön u mukana I näet sisältäisi tulon $uu^{-1} = 1$ ja silloin I olisi $= R$.

ESIMERKKI 6. Pykälässä IV.3 osoitettiin, että ryhmän $(\mathbb{Z},+)$ kaikki aliryhmät ovat ryhmät $m\mathbb{Z}$, $m = 0, 1, \ldots$ Koska joukot $m\mathbb{Z}$ täyttävät myös ehdon I2, ne ovat renkaan $\mathbb{Z}$ ideaaleja. Nämä ovat siis renkaan $\mathbb{Z}$ *kaikki* ideaalit.

Lause 5 (Ideaalikriteeri). *Olkoon R rengas ja $I \subset R$. Silloin I on R:n ideaali jos ja vain jos seuraavat ehdot toteutuvat:*

(a) $I \neq \emptyset$,

(b) $a - b \in I \quad \forall\ a, b \in I$,

(c) $ra \in I$ *ja* $ar \in I \quad \forall\ r \in R$, $a \in I$.

Todistus. Ehdot (a) ja (b) yhdessä ovat yhtäpitävät I1:n kanssa ja ehto (c) on sama kuin I2. □

ESIMERKKI 7. Näytetään, että reaalikertoimiset polynomit, joiden vakiotermi $= 0$, muodostavat polynomirenkaan $\mathbb{R}[x]$ ideaalin.

Lause 6. *Jos I ja J ovat renkaan R ideaaleja, samoin ovat niiden leikkaus $I \cap J$ ja summa*

$$I + J = \left\{ a + b \;\middle|\; a \in I,\, b \in J \right\}.$$

Sama on yleisemmin voimassa useammankin kuin kahden ideaalin tapauksessa (leikkauksen suhteen jopa äärettömän monen ideaalin).

Todistus. Tämä seuraa välittömästi ideaalikriteeristä. □

Vastaavasti kuin ryhmän G osajoukko virittää G:n aliryhmän, renkaan R osajoukko S virittää R:n ideaalin

$$\langle S\rangle = \bigcap_{\substack{S\subset I \\ I \text{ on } R\text{:n ideaali}}} I;$$

tässä käytetään lausetta 6. Ideaali $\langle S\rangle$ on "suppein" R:n ideaali, joka $\supset S$.

Jos S on äärellinen joukko, $S = \{a_1, \ldots, a_k\}$, niin ideaalin $\langle S\rangle$ sanotaan olevan *äärellisesti viritetty.* Merkintä: $\langle S\rangle = \langle a_1, \ldots, a_k\rangle$.

Yhden alkion a virittämää ideaalia $\langle a\rangle$ sanotaan *pääideaaliksi.*

Huomaa, että

$$\langle a_1, \ldots, a_k\rangle = \langle b_1, \ldots, b_h\rangle,$$

jos kumpikin ideaali sisältää toisen virittäjät. Esim. ehdosta $a_i \in \langle b_1, \ldots, b_h\rangle$ $(i = 1, \ldots, k)$ seuraa nimittäin yllä todetun nojalla, että $\langle a_1, \ldots, a_k\rangle \subset \langle b_1, \ldots, b_h\rangle$

Esimerkki 8. Triviaalit ideaalit R ja $\{0\}$ ovat pääideaaleja: $R = \langle 1\rangle$ ja $\{0\} = \langle 0\rangle$.

Lause 7. *Jos rengas R on kommutatiivinen, niin*

$$\langle a_1, \ldots, a_k\rangle = \left\{ r_1a_1 + \cdots + r_ka_k \;\middle|\; r_i \in R \quad \forall\ i \right\}.$$

Todistus. Samanlainen kuin lauseen III.5 todistus. Olennaista on, että oikeanpuoleinen joukko ensiksikin on ideaalikriteerin mukaan ideaali ja toiseksi sisältyy jokaiseen ideaaliin, jossa alkiot $a_1, \ldots, a_k$ ovat. □

Käytettäessä samanlaista merkintätapaa kuin esim. aliryhmän sivuluokille voidaan kirjoittaa (kun R on kommutatiivinen)

$$\langle a_1, \ldots, a_k\rangle = Ra_1 + \cdots + Ra_k, \qquad \text{erityisesti } \langle a\rangle = Ra.$$

Merkintä $Ra_1 + \cdots + Ra_k$ voidaan ymmärtää myös pääideaalien Ra_i summana.

Esimerkki 9. Polynomirenkaassa $\mathbb{R}[x]$ alkion x virittämä pääideaali on

$$\langle x\rangle = x\mathbb{R}[x] = \left\{ a_0x + a_1x^2 + \cdots + a_nx^{n+1} \;\middle|\; n \geq 0,\ a_i \in \mathbb{R} \quad \forall\ i \right\},$$

siis sama ideaali, joka esiintyi esimerkissä 7.

Esimerkki 10. Esimerkin 6 mukaan renkaan $\mathbb{Z}$ kaikki ideaalit ovat pääideaalit

$$\langle m\rangle = m\mathbb{Z} \qquad (m = 0, 1, \ldots).$$

Määritelmä. Rengasta, jonka kaikki ideaalit ovat pääideaaleja, sanotaan *pääideaalirenkaaksi* (principal ideal ring), lyhennettynä PIR.

Esimerkki 11. Esimerkki 10 osoittaa, että $\mathbb{Z}$ on PIR. Jos siis $a_1, \ldots, a_k \in \mathbb{Z}$, niin on olemassa sellainen $d \in \mathbb{Z}$, että

$$\langle a_1, \ldots, a_k \rangle = \langle d \rangle.$$

Miten d saadaan määritetyksi? Osoitetaan, että vastaus on yksinkertainen: $d = \text{syt}(a_1, \ldots, a_k)$.

Siis esim. $\langle 3, 4 \rangle = \langle 1 \rangle = \mathbb{Z}$, $\quad \langle 4, 6 \rangle = \langle 2 \rangle = 2\mathbb{Z}$.

Esimerkki 12. Olkoon $R = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ ja $S = \{f \in R \mid f \text{ on derivoituva}\}$. Silloin S on R:n alirengas, mutta ei ideaali.

Harjoitustehtäviä

1. Osoita, että $\{0_6, 2_6, 4_6\}$ on rengas, mutta ei ole renkaan $\mathbb{Z}_6$ alirengas.
2. Olkoon R rengas ja $C(R) = \{x \in R \mid xy = yx \ \forall y \in R\}$. Osoita, että $C(R)$ on R:n alirengas.
3. Osoita, että $\mathbb{R}^{\mathbb{R}}$ on rengas ja derivoituvat funktiot $\mathbb{R} \to \mathbb{R}$ muodostavat sen alirenkaan. (Kuten aikaisemmin, $\mathbb{R}^{\mathbb{R}} = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$, laskutoimitukset kuten luvun V.1 esimerkissä 3.)
4. Osoita, että
$$I = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(1) = 0\}$$
on renkaan $\mathbb{R}^{\mathbb{R}}$ ideaali.
5. Olkoot A ja B renkaan R ideaaleja. Osoita, että myös $A + B$ on R:n ideaali.
6. Olkoot A ja B renkaan R ideaaleja. Osoita, että myös $A \cap B$ on R:n ideaali.
7. Määritä renkaan $\mathbb{Z}_{12}$ ideaalit.
8. Näytä, että joukko $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}$ on renkaan $\mathbb{R}$ alirengas.
9. Näytä, että M ja $\{0_M\}$ ovat matriisirenkaan $M = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}\}$ ainoat ideaalit. (Ohje: Jos $I \neq \{0_M\}$ on M:n ideaali, näytä, että $1_M \in I$.)
10. Osoita, että Gaussin luvut $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ muodostavat kompleksilukujen renkaan $\mathbb{C}$ alirenkaan.
11. Osoita, että joukko $\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Z}\}$ on renkaan $\mathcal{M}_2(\mathbb{Z})$ alirengas.

V.4 Jäännösluokkarengas

Ryhmän G normaalin aliryhmän N avulla määriteltiin G:n tekijäryhmä G/N. Analoginen käsite renkaalla R on *jäännösluokkarengas* eli tekijärengas R/I, missä I on R:n ideaali.

Oletetaan, että I on renkaan R ideaali. Silloin $(I,+)$ on $(R,+)$:n normaali aliryhmä (normaalisuus seuraa ryhmän $(R,+)$ kommutatiivisuudesta), joten voidaan muodostaa tekijäryhmä

$$R/I = \{\, a+I \mid a \in R\} = \{\, a+I \mid a \in D\},$$
$$(a+I)+(b+I) = (a+b)+I,$$

missä D on jokin *jäännösluokkien* (= sivuluokkien, ks. III.5:n esimerkki 1) $a+I$ edustajisto.

Lause 8. *Jos I on renkaan R ideaali, niin R/I on rengas seuraavasti määriteltyjen yhteen- ja kertolaskun suhteen:*

$$(a+I)+(b+I) = (a+b)+I, \qquad (a+I)(b+I) = ab+I.$$

Todistus. Kuten edellä todettiin, $(R/I,+)$ on ryhmä. Se on vieläpä Abelin ryhmä, koska $(R,+)$ on Abelin ryhmä.

Toiseksi osoitetaan, että lauseessa annettu jäännösluokkien kertolasku on hyvinmääritelty. Olkoon $a+I = a'+I$ ja $b+I = b'+I$, siis $a = a'+i_1$ ja $b = b'+i_2$, missä $i_1, i_2 \in I$. Silloin

$$ab = (a'+i_1)(b'+i_2) = a'b' + a'i_2 + i_1b' + i_1i_2.$$

Koska I on R:n ideaali, se sisältää tulot $a'i_2$, i_1b' ja i_1i_2 ja siis myös niiden summan. Näin ollen $ab = a'b' + i$, missä $i \in I$. Tämä voidaan lausua myös muodossa $ab \in a'b' + I$ ja merkitsee siis, että $ab + I = a'b' + I$.

Rengaspostulaatit R3-R5 palautuvat jäännösluokkien yhteen- ja kertolaskun määritelmien perusteella suoraan vastaaviin postulaatteihin R:ssä. Renkaan R/I ykkösalkioksi tulee $1+I$. □

MÄÄRITELMÄ. Rengasta R/I sanotaan R:n *jäännösluokkarenkaaksi* ideaalin I suhteen. (Käytetään myös nimitystä *tekijärengas*; engl. residue class ring, factor ring.)

Muista, että $\forall a, b \in R$

$$a+I = b+I \iff a \in b+I \iff a-b \in I.$$

Varmistu myös, että ymmärrät seuraavat tosiasiat R/I:stä: nolla-alkio on I $(= 0+I)$, ykkösalkio $1+I$, alkion $a+I$ vasta-alkio $-a+I$ ja (siinä tapauksessa, että a on yksikkö) käänteisalkio $a^{-1}+I$. Jos rengas R on kommutatiivinen, samoin on R/I.

ESIMERKKI 1. Renkaan $\mathbb{Z}$ jäännösluokkarengas ideaalin $m\mathbb{Z}$ suhteen on

$$\mathbb{Z}/m\mathbb{Z} = \{\, a + m\mathbb{Z} \mid a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\},$$
$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a}\cdot\overline{b} = \overline{ab}.$$

Kyseessä on siis ennestään tuttu rengas $\mathbb{Z}_m$, jäännösluokkarengas mod m.

Tapauksessa $m = 1$ saadaan nollarengas $\mathbb{Z}/\mathbb{Z} = \{\overline{0}\}$. (Samoin tietenkin yleisesti $R/R = \{0\}$.)

Harjoitustehtäviä

1. Muodosta ideaalin $I = \langle\, \sqrt{2}\, \rangle$ jäännösluokat renkaassa $\mathbb{Z}[\sqrt{2}]$.
2. Olkoon $\langle 2_4 \rangle$ alkion 2_4 virittämä jäännösluokkarenkaan $\mathbb{Z}_4$ ideaali. Muodosta tekijärengas $\mathbb{Z}_4/\langle 2_4 \rangle$.
3. Muodosta jäännösluokkarengas $\mathbb{Z}\left[\sqrt{10}\right]/I$, missä $\mathbb{Z}\left[\sqrt{10}\right] = \{\, a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ ja $I = \langle 5, \sqrt{10}\,\rangle$.

V.5 Renkaiden homomorfia ja isomorfia

MÄÄRITELMÄ. Olkoot R ja R' renkaita. Kuvausta $f : R \to R'$ sanotaan *(rengas)homomorfismiksi*, jos se täyttää ehdot

RH1. $f(a+b) = f(a) + f(b) \quad \forall\ a, b \in R$,

RH2. $f(ab) = f(a)f(b) \quad \forall\ a, b \in R$,

RH3. $f(1_R) = 1_{R'}$.

Määritelmän mukaan kuvaus $f : R \to R'$ on rengashomomorfismi jos ja vain jos f on ryhmähomomorfismi $(R, +) \to (R', +)$ ja sillä on ominaisuudet RH2 ja RH3. Tästä seuraa ryhmähomomorfismien ominaisuuksien perusteella, että rengashomomorfismi $f : R \to R'$ täyttää ehdot

$$f(0_R) = 0_{R'}\,, \qquad f(-a) = -f(a) \quad \forall\ a \in R.$$

Lisäksi RH2:n ja RH3:n nojalla

$$f(a^{-1}) = f(a)^{-1} \quad \forall\ a \in R^*,$$

sillä $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_R) = 1_{R'}$, ja samoin $f(a^{-1})f(a) = 1_{R'}$.

Esimerkki 1. Identiteettikuvaus id_R on homomorfismi $R \to R$. Nollakuvaus $f(a) = 0 \quad \forall\ a \in R$ ei ole homomorfismi, koska se ei täytä ehtoa RH3.

Esimerkki 2. Kuvaus $f : \mathbb{R}[x] \to \mathbb{R}, \quad f(a_0 + a_1x + \cdots + a_nx^n) = a_0$, on (rengas)homomorfismi. Onko kuvaus $g(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1 + \ldots + a_n$ rengashomomorfismi?

Seuraava lause antaa analogiset tulokset ryhmäteorian lauseille III.8 ja IV.3.

Lause 9. *Olkoon $f : R \to R'$ rengashomomorfismi.*

(i) *Jos S on R:n alirengas, niin $f(S)$ on R':n alirengas.*

(ii) *Jos S' on R':n alirengas, niin $f^{-1}(S')$ on R:n alirengas.*

(iii) *Jos I on R:n ideaali, niin $f(I)$ on renkaan $f(R)$ ideaali.*

(iv) *Jos I' on R':n ideaali, niin $f^{-1}(I')$ on R:n ideaali.*

Todistus. Nämä todistetaan suoraviivaisesti alirengas- ja ideaalikriteereihin sekä homomorfiaehtoihin RH1-RH3 nojautuen. Kohtien (iii) ja (iv) todistuksessa voidaan ideaalikriteerin sijasta käyttää myös ideaalin määritelmää ja lausetta III.8. □

Kohdan (iv) nojalla erityisesti rengashomomorfismin *ydin*

$$\mathrm{Ker}(f) = f^{-1}(\{0\}) = \big\{\, a \in R \;\big|\; f(a) = 0 \big\}$$

on renkaan R ideaali.

Samoin (i):n nojalla renkaan R *homomorfinen kuva*

$$\mathrm{Im}(f) = f(R) = \big\{\, f(a) \;\big|\; a \in R \big\}$$

on rengas, nimittäin renkaan R' alirengas.

Jos kuvausta f ajatellaan vain ryhmähomomorfismina $(R, +) \to (R', +)$, sen ydin ja kuva ovat samat joukot kuin yllämainitut $\mathrm{Ker}(f)$ ja $\mathrm{Im}(f)$. (Pane erityisesti merkille, että ytimen määritelmässä esiintyy 0 eikä siis 1!) Erityisesti siis lauseesta III.9 seuraa: *Rengashomomorfismi $f : R \to R'$ on injektio jos ja vain jos* $\mathrm{Ker}(f) = \{0\}$.

Esimerkki 3. Määritetään esimerkin 2 homomorfismin f ydin ja kuva.

Määritelmä. Rengashomomorfismia $f : R \to R'$ sanotaan *(rengas)isomorfismiksi*, jos f on bijektiivinen. Rengasta R sanotaan renkaan R' kanssa *isomorfiseksi*, merkitään $R \simeq R'$, jos on olemassa jokin isomorfismi $R \to R'$.

HUOMAUTUS. Lisää homomorfismeihin liittyvää terminologiaa (eräät termeistä on mainittu myös aikaisemmin):

monomorfismi = injektiivinen homomorfismi,
epimorfismi = surjektiivinen homomorfismi,
endomorfismi = homomorfismi systeemiltä itseensä,
automorfismi = isomorfismi systeemiltä itselleen.

ESIMERKKI 4. Näytetään, että kuvaus $f : \mathbb{C} \to \mathbb{C}, \quad f(x+iy) = x - iy$, on renkaan $\mathbb{C}$ automorfismi.

Ryhmä- ja rengashomomorfismien analogia koskee myös lauseita III.10 ja III.11, jotka voidaan helposti ulottaa myös rengashomomorfismeihin. Seurauksena on, että myös renkaiden isomorfia on ekvivalenssirelaatio. Isomorfiset renkaat voidaan rengasteorian kannalta katsottuna samaistaa.

Ryhmien homomorfialauseen (IV.4) vastine rengasteoriassa:

Lause 10 (Renkaiden homomorfialause). *Jos $f : R \to R'$ on rengashomomorfismi, niin*

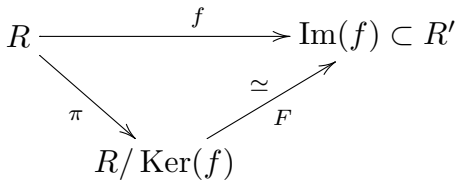
$$R/K \simeq \mathrm{Im}(f) \qquad (K = \mathrm{Ker}(f)).$$

Tarkemmin: f indusoi rengasisomorfismin $F : R/K \to \mathrm{Im}(f), \quad F(a+K) = f(a)$.

Todistus. Ryhmien homomorfialauseen nojalla kuvaus F on ryhmäisomorfismi $(R/K, +) \to (\mathrm{Im}(f), +)$. On siis enää todistettava, että F täyttää homomorfiaehdot RH2 ja RH3.

RH2: $F((a+K)(b+K)) = F(ab+K) = f(ab) = f(a)f(b) = F(a+K)F(b+K)$.

RH3: $F(1+K) = f(1) = 1$. $\square$



Kuten ryhmillä, homomorfialause antaa viereisen kommutoivan diagramman, jossa π on *(kanoninen) projektio*

$$\pi : R \longrightarrow R/I, \qquad \pi(a) = a + I,$$

tapauksessa $I = \mathrm{Ker}(f)$. Tarkista, että π todella on rengashomomorfismi. Koska π lisäksi on surjektiivinen, nähdään (lauseen 10 avulla), että renkaan R homomorfiset kuvat vastaavat bijektiivisesti R:n jäännösluokkarenkaita.

ESIMERKKI 5. Tutkitaan, minkä isomorfian esimerkin 2 homomorfismi antaa.

ESIMERKKI 6. Todetaan, että kuvaus $f : \mathbb{Z} \to \mathbb{Z}_m, \quad f(a) = \overline{a}$, on rengashomomorfismi ($m \geq 2$), ja tutkitaan sen indusoimaa isomorfismia.

Harjoitustehtäviä

1. Näytä, että ehto $x_4 \mapsto (5x)_{10}$, $x \in \mathbb{Z}$, antaa hyvinmääritellyn kuvauksen $\mathbb{Z}_4 \to \mathbb{Z}_{10}$. Onko se rengashomomorfismi?
2. Oletetaan, että on olemassa surjektiivinen homomorfismi kommutatiiviselta renkaalta R renkaalle R'. Osoita, että myös R' on kommutatiivinen.
3. $(\mathbb{Z}, \oplus, \odot)$ on rengas, kun $x \oplus y = x + y - 1$ ja $x \odot y = x + y - xy$. Osoita, että $(\mathbb{Z}, \oplus, \odot)$ on isomorfinen renkaan $(\mathbb{Z}, +, \cdot)$ kanssa.
4. Olkoon X joukko ja $Y \subset X$. Osoita, että Boolen renkaiden välinen kuvaus $f : \mathcal{P}(X) \to \mathcal{P}(Y)$, $f(A) = A \cap Y$, on rengashomomorfismi. Määritä $\mathrm{Ker}(f)$.
5. Määritä kaikki rengashomomorfismit $f : \mathbb{Z} \to \mathbb{Z}$ ja $g : \mathbb{Q} \to \mathbb{Q}$.
6. Joukko $A = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R} \right\}$ on rengas. Näytä, että joukko $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{R} \right\}$ on A:n ideaali ja tekijärengas A/I on isomorfinen tulorenkaan $\mathbb{R} \times \mathbb{R}$ kanssa. (Ohje: Renkaiden homomorfialause.)
7. Olkoon $f : R \to R$ rengashomomorfismi. Todista: Jos I on R:n ideaali, niin $f(I)$ on renkaan $f(R)$ ideaali.
8. Onko olemassa kuvausta $f : 2\mathbb{Z} \to 3\mathbb{Z}$, joka toteuttaa ehdot $RH1$ ja $RH2$? Onko tällaista bijektiota?
9. Tutki, onko kuvaus $f : \mathbb{Z}_4 \to \mathbb{Z}_{12}$, $x_4 \mapsto (3x)_4$ $(\forall x \in \mathbb{Z})$ hyvinmääritelty. Toteuttaako se ehdot $RH1$ ja $RH2$?
10. Osoita, että $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ ja $H = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$ ovat isomorfiset renkaina.

V.6 Kokonaisalue; karakteristika

Lukurenkailla on se tärkeä ominaisuus, että kahden luvun tulo $= 0$ vain, kun ainakin toinen tekijä $= 0$. Tätä käytetään mm. ratkaistaessa yhtälöitä, esim.

$$x^4 = 1 \qquad \Longleftrightarrow \qquad (x-1)(x+1)(x-i)(x+i) = 0 \qquad \Longleftrightarrow \qquad x = \pm 1, \pm i.$$

Samaa ominaisuutta ei ole kaikilla renkailla: esim. renkaassa $\mathbb{Z}_{12}$ on $\overline{3} \cdot \overline{4} = \overline{0}$.

ESIMERKKI 1. Ratkaistaan renkaassa $\mathbb{Z}_{10}$ yhtälö $x^3 + x = 0$.

MÄÄRITELMÄ. Renkaan R alkiota a sanotaan *nollanjakajaksi* (zero divisor), jos $a \neq 0$ ja on olemassa sellainen $b \in R$, $b \neq 0$, että

$$ab = 0 \qquad \text{tai} \qquad ba = 0.$$

ESIMERKKI 2. Matriisi $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ on renkaan $\mathcal{M}_2(\mathbb{R})$ nollanjakaja, koska

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 6 & 2 \\ -3 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

ESIMERKKI 3. Osoitetaan, että $\overline{a}$ on renkaan $\mathbb{Z}_m$ nollanjakaja jos ja vain jos $\overline{a} \neq \overline{0}$ ja $\text{syt}(a, m) > 1$.

MÄÄRITELMÄ. Rengasta R sanotaan *kokonaisalueeksi* (integral domain), jos

D1. R on kommutatiivinen ja

D2. R:ssä ei ole nollanjakajia.

ESIMERKKI 4. Kaikki lukurenkaat ($\mathbb{Z}$, $\mathbb{Q}$ jne.) ovat kokonaisalueita.

ESIMERKKI 5. Esimerkistä 3 seuraa: *Jäännösluokkarengas $\mathbb{Z}_m$ on kokonaisalue jos ja vain jos m on alkuluku.*

Kokonaisalueessa D on voimassa *supistamislaki*: Jos $a \in D,\ a \neq 0$, niin

$$ab = ac \qquad \Longrightarrow \qquad b = c \qquad \forall\ b, c \in D.$$

Vasemmanpuolinen yhtälö voidaan nimittäin kirjoittaa muotoon $a(b-c) = 0$; väite seuraa tästä, koska a ei ole nollanjakaja. (Huom. Tässä a:lla ei tarvitse olla käänteisalkiota.)

ESIMERKKI 6. Ratkaistaan renkaissa $\mathbb{Z}_5$ ja $\mathbb{Z}_7$ yhtälö $x^3 + 10x = 0$.

Huomataan, että laskutoimitukset kokonaisalueessa D riippuvat siitä, mitkä ykkösalkion $1 = 1_D$ monikerrat $n1 = 1+\cdots+1$ ovat $= 0$. Tämä johtaa seuraavaan määritelmään.

MÄÄRITELMÄ. Kokonaisalueen D *karakteristika* (characteristic)

$$\text{char}(D) = \begin{cases} \text{pienin positiivinen kokonaisluku } n, \text{ jolla } n1_D = 0, \\ 0, \text{ jos tällaista lukua } n \text{ ei ole olemassa.} \end{cases}$$

Toisin sanoen $\text{char}(D)$ on D:n ykkösalkion kertaluku ryhmässä $(D, +)$, paitsi jos tämä kertaluku $= \infty$, jolloin $\text{char}(D) = 0$.

ESIMERKKI 7. Jokaisen lukurenkaan karakteristika $= 0$. Jäännösluokkarenkaan $\mathbb{Z}_p$ (p alkuluku) karakteristika $= p$.

HUOMAUTUS. Kokonaisalueen D *kaikilla* nollasta eroavilla alkioilla a on sama kertaluku ryhmässä $(D,+)$ (karakteristikan määritelmässä esiintyy ykkösalkio vain yksinkertaisuuden vuoksi). Yhtälö $na = 0$ voidaan nimittäin lauseen 3 nojalla kirjoittaa muodossa $(n1_D)a = 0$, ja koska D:ssä ei ole nollanjakajia, tämä on yhtäpitävä yhtälön $n1_D = 0$ kanssa.

Lause 11. *Kokonaisalueen D karakteristika* $\operatorname{char}(D)$ *on joko* 0 *tai alkuluku.*

Todistus. Oletetaan, että $\operatorname{char}(D) = n \neq 0$. Kirjoitetaan $n = n_1 n_2$, missä n_1 ja n_2 ovat kokonaislukuja > 0. Silloin $n1 = (n_1 1)(n_2 1)$, joten oletuksen mukaan $(n_1 1)(n_2 1) = 0$. Koska D:ssä ei ole nollanjakajia, niin ainakin toinen tulon tekijä $= 0$, sanokaamme $n_1 1 = 0$. Mutta tällöin n:n minimaalisuuden perusteella $n_1 = n$. Luvun n ainoa jako tekijöihin on siis $n = n \cdot 1$, joten n on alkuluku. □

ESIMERKKI 8. Näytetään, että binomikertoimet $\binom{p}{k}$ ovat p:llä jaollisia, kun p on alkuluku ja $1 \leq k \leq p-1$. Päätellään tästä: Jos $\operatorname{char}(D) = p$, niin

$$(a+b)^p = a^p + b^p \quad \forall\ a, b \in D.$$

Ratkaistaan sovelluksena yhtälö $x^3 + y^3 = 0$ kokonaisalueessa D, jonka karakteristika $= 3$.

Harjoitustehtäviä

1. Osoita, että $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ on kokonaisalue.
2. Osoita, ettei $\mathcal{M}_2(\mathbb{Z})$ ole kokonaisalue.
3. Ratkaise kokonaisalueessa yhtälö $x^2 = x$.
4. Montako ratkaisua yhtälöllä $x^2 - 5x + 6 = 0$ on $\mathbb{Z}_7$:ssä? Entä $\mathbb{Z}_8$:ssa?
5. Oletetaan, että D ja E ovat kokonaisalueita ja $f : D \to E$ on rengashomomorfismi. Olkoon D:n karakteristika $\neq 0$. Todista, että D:llä ja E:llä on sama karakteristika.

VI. KUNTA JA POLYNOMIT

VI.1 Kunta

Tässä luvussa käsiteltävän algebrallisen systeemin, *kunnan*, mallina ovat rationaaliluvut, ts. lukujoukko, jossa on määritelty neljä "peruslaskutoimitusta". Tällainen systeemi on siis aritmeettisesti kehittyneempi kuin ryhmä ja rengas ja sisältää siksi monia toivottuja ominaisuuksia. Seuraavassa on tavoitteena mm. esittää kuntien perusluokittelu ja tutkia, miten kuntia voidaan konstruoida.

MÄÄRITELMÄ. Kolmikkoa $(K, +, \cdot)$ sanotaan *kunnaksi* (field), jos

K1. $(K, +, \cdot)$ on kommutatiivinen rengas ($\neq$ nollarengas) ja

K2. jokaisella K:n alkiolla $\neq 0$ on käänteisalkio K:ssa, ts. K:n yksikköryhmä $K^* = K \setminus \{0\}$.

Tämän mukaan $(K, +, \cdot)$ on kunta silloin ja vain silloin, kun se täyttää ehdot

K1'. $(K, +)$ on Abelin ryhmä (kunnan *additiivinen ryhmä*),

K2'. $(K \setminus \{0\}, \cdot)$ on Abelin ryhmä (kunnan *multiplikatiivinen ryhmä*),

K3'. $a(b + c) = ab + ac$ ja $(a + b)c = ac + bc \quad \forall\ a, b, c \in K$.

Jos luovutaan kertolaskun kommutointivaatimuksesta, saadaan ns. *vinokunta* (skew field) eli *jakorengas* (division ring). Se sivuutetaan tässä kurssissa.

ESIMERKKI 1. $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat (luku)kuntia. $\mathbb{Z}$ ei ole kunta.

ESIMERKKI 2. Kaikkien rationaalifunktioiden joukko määritellään seuraavasti:

$$\mathbb{R}(x) = \left\{ \frac{p(x)}{q(x)} \;\middle|\; p(x),\, q(x) \in \mathbb{R}[x],\ q(x) \neq \text{ nollapolynomi} \right\}.$$

$\mathbb{R}(x)$ on kunta funktioiden pisteittäisen yhteen- ja kertolaskun suhteen.

Lause 1. (i) *Jokainen kunta on kokonaisalue.* (ii) *Jokainen äärellinen kokonaisalue on kunta.* (Vrt. esimerkki 1: $\mathbb{Z}$ on ääretön kokonaisalue.)

Todistus. (i) Vertaa kunnan määritelmän ehtoa K1 kokonaisalueen määritelmään. On siis vain osoitettava, ettei kunnassa K ole nollanjakajia. Oletetaan, että $ab = 0$, missä $a, b \in K,\ a \neq 0$. Silloin a:lla on käänteisalkio $a^{-1} \in K$ ja tämä yhtälö antaa $b = a^{-1}\cdot 0 = 0$. Se todistaa väitteen.

(ii) Olkoon D äärellinen kokonaisalue. Nyt on todistettava, että jokaisella alkiolla $a \in D \setminus \{0\}$ on käänteisalkio D:ssä.

Muodostetaan D:n osajoukko $D_0 = \{\, ax \mid x \in D \,\}$. Soveltamalla supistamislakia kokonaisalueessa D nähdään, että $ax_1 \neq ax_2$ aina kun $x_1 \neq x_2$. Koska D on äärellinen, tästä seuraa, että D_0:ssa on yhtä monta alkiota kuin D:ssä ja siis $D_0 = D$. Silloin erityisesti myös D:n ykkösalkio on mukana D_0:ssa, ts.

$$\exists\ x' \in D: \qquad ax' = 1.$$

Tämä merkitsee (huomaa D:n kommutatiivisuus), että $x' = a^{-1}$. $\square$

Esimerkki 3. Tästä lauseesta ja pykälän V.6 esimerkistä 5 seuraa: *Jäännösluokkarengas $\mathbb{Z}_m$ on kunta jos ja vain jos m on alkuluku, $m = p \in \mathbb{P}$.*

Jäännösluokkakunta $\mathbb{Z}_p = \{\, \overline{0}, \overline{1}, \ldots, \overline{p-1} \,\}$ on esimerkki *äärellisestä* kunnasta.

Laaditaan kunnan $\mathbb{Z}_5$ yhteenlasku- ja kertotaulut.

Huomautus. Äärellistä kuntaa, jonka kertaluku on alkulukupotenssi p^k, merkitään $GF(p^k)$:lla. Tässä GF tulee saksankielisestä termistä Galois-Feld (engl. Galois field), joka on jäänyt pois käytöstä. Voidaan osoittaa, että jokaista alkulukupotenssia p^k kohti on olemassa isomorfiaa vaille yksikäsitteinen kunta $GF(p^k)$ ja ettei muita äärellisiä kuntia ole.

Tässä kurssissa näytetään, miten kuntia $GF(p^k)$ voidaan konstruoida.

Koska kunta on rengas, siinä on määritelty yhteen-, vähennys- ja kertolasku (muista, että $a - b = a + (-b)$). *Jakolasku* määritellään nyt tavalliseen tapaan asettamalla

$$\frac{a}{b} = ab^{-1}, \qquad \text{siis erityisesti} \qquad \frac{1}{b} = b^{-1} \qquad (b \neq 0).$$

Soveltamalla tavallisia kommutatiivisen renkaan laskulakeja todetaan, että

$$\frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd}, \qquad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad (b \neq 0,\ d \neq 0).$$

Osamäärillä $\dfrac{a}{b}$ lasketaan siis samoin kuin murtoluvuilla. Huomaa myös, että $\dfrac{a}{1} = a$.

Esimerkki 4. Lasketaan kunnassa $\mathbb{Z}_5$ summat $\dfrac{\overline{1}}{\overline{2}} + \dfrac{\overline{1}}{\overline{4}}$ ja $\dfrac{\overline{1}}{\overline{2}} + \dfrac{\overline{3}}{\overline{4}}$.

Jos ei ole sekaannuksen vaaraa, kunnassa K merkitään usein

$$1 + 1 = 2,\ \ 1 + 1 + 1 = 3, \ldots, \quad \text{yleisesti} \quad n\cdot 1 = n \quad \forall\ n \in \mathbb{Z}.$$

Koska kunta on kokonaisalue, sille on määritelty karakteristika $\mathrm{char}(K)$ ja tämä on joko 0 tai alkuluku (lause V.11). Huomaa erityisesti:

Jos $\mathrm{char}(K) = 0$*, niin* K *on ääretön. Äärellisen kunnan karakteristika on siis alkuluku.*

Jos $\mathrm{char}(K) = p$ *(alkuluku), niin*

$$n = 0 \qquad \Longleftrightarrow \qquad p \mid n.$$

Esimerkki 5. Määritetään esimerkeissä 1-3 esiintyneiden kuntien karakteristika.

Esimerkki 6. Ratkaistaan kunnassa K toisen asteen yhtälö $x^2 + ax + b = 0$ olettaen, että $\mathrm{char}(K) \neq 2$. Vertaa tulosta toisen asteen yhtälön ratkaisuun lukukunnissa.

Esimerkki 7. Osoitetaan, että jokainen *lukukunta* (kunta, jonka alkiot ovat kompleksilukuja) sisältää rationaalilukujen kunnan $\mathbb{Q}$, ts. $\mathbb{Q}$ on suppein lukukunta.

Koska kunta on rengas, voidaan puhua sen ideaaleista. Seuraava lause käsittelee ne tyhjentävästi.

Lause 2. *Kunnan* K *ainoat ideaalit ovat* K *ja* $\{0\}$.

Todistus. Jos I on K:n aito ideaali, niin $I \cap K^* = \emptyset$ erään pykälässä V.3 esitetyn ideaalien perusominaisuuden mukaan. Mutta $K^* = K \setminus \{0\}$; täten $I = \{0\}$. □

Jos K ja K' ovat kuntia, niin rengashomomorfismia $K \to K'$ sanotaan myös *kuntahomomorfismiksi* ja rengasisomorfismia $K \to K'$ *kuntaisomorfismiksi.*

Lause 3. *Jokainen kuntahomomorfismi* $f : K \to K'$ *on injektio.*

Todistus. Koska ydin $\mathrm{Ker}(f)$ on K:n ideaali, se on lauseen 2 mukaan joko K tai $\{0\}$. Edellisessä tapauksessa $f(a) = 0 \ \ \forall \ a \in K$. Tämä on kuitenkin mahdotonta, koska $f(1) = 1$ (postulaatti RH3). Näin ollen $\mathrm{Ker}(f) = \{0\}$ ja siis f on injektio. □

Tämän mukaan kunnan K kaikki homomorfiset kuvat ovat $\simeq K$.

Esimerkki 8. Osoitetaan pykälän V.6 esimerkkiin 8 nojautuen, että kuvaus

$$f_p : K \longrightarrow K, \qquad f_p(x) = x^p,$$

on kuntahomomorfismi, kun $\mathrm{char}(K) = p$. Lauseesta 3 seuraa silloin, että $K \simeq \mathrm{Im}(f_p)$. Jos erityisesti K lisäksi on äärellinen kunta, $\mathrm{Im}(f_p)$ siis sisältää yhtä monta alkiota kuin K ja on täten $= K$. Tässä tapauksessa f_p siis on kunnan K automorfismi.

Yksinkertaisin tapaus ko. ehdot täyttävästä kunnasta on $K = \mathbb{Z}_p$. Tällöin edellinen tulos kuitenkin on triviaali: f_p on kunnan identiteettikuvaus (ks. Eulerin lause; pykälän III.5 esimerkki 6).

Harjoitustehtäviä

1. Olkoon $R = \{0_{10}, 2_{10}, 4_{10}, 6_{10}, 8_{10}\} \subset \mathbb{Z}_{10}$. Todista, että R on kunta.
2. Anna esimerkki äärellisestä kunnasta, jonka jotkin alkiot $a, b \neq 0$ toteuttavat yhtälön $a^2 + b^2 = 0$.
3. Ratkaise $\mathbb{Z}_7$:ssä yhtälöpari
$$\begin{cases} -3x + 2y = \quad 1 \\ \quad\; x + 3y = -2. \end{cases}$$
4. Olkoon R kommutatiivinen rengas. Osoita, että R on kunta täsmälleen silloin, kun R:llä on vain triviaalit ideaalit $\{0\}$ ja R.
5. Laske alkion 31_{173} käänteisalkio kunnassa $\mathbb{Z}_{173}$ ja määritä kongruenssin $31x \equiv 5 \pmod{173}$ kaikki ratkaisut.
6. Todista, että kaikki matriisit $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ muodostavat kunnan, joka on isomorfinen kompleksilukujen kunnan $\mathbb{C}$ kanssa. Mikä matriisi vastaa imaginaariyksikköä i?
7. Näytä, että kertolasku
$$(a, b)(c, d) = (ac + bd, ad + bc + bd)$$
tekee tuloryhmästä $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ neljän alkion kunnan.
8. Olkoon K kunta, R rengas ja $f : K \to R$ rengashomomorfismi. Osoita, että f on injektio.
9. Näytä, että $\mathbb{Z}[\sqrt{3}]$ ei ole kunta.
10. Osoita, että jos f on funktiorenkaan $R = \mathbb{R}^{\mathbb{R}}$ alkio, $f \neq 0_R$, niin f on nollanjakaja tai yksikkö.

VI.2 Alikunta; alkukunta

MÄÄRITELMÄ. Kunnan $(K, +, \cdot)$ osajoukkoa F sanotaan K:n *alikunnaksi*, jos F on kunta operaatioiden $+$ ja $\cdot$ suhteen.

Jos F on kunnan K alikunta, niin $(F,+)$ on $(K,+)$:n aliryhmä ja $(F \setminus \{0\},\cdot)$ on $(K \setminus \{0\},\cdot)$:n aliryhmä. Tästä seuraa erityisesti, että K:n ja F:n nolla-alkiot yhtyvät, samoin ykkösalkiot.

Lause 4 (Alikuntakriteeri). *Kunnan K osajoukko F on K:n alikunta jos ja vain jos se täyttää seuraavat ehdot:*

AK1. *F:ssä on vähintään 2 alkiota,*

AK2. $a - b \in F \quad \forall\ a, b \in F$,

AK3. $\dfrac{a}{b} \in F \quad \forall\ a, b \in F,\ b \neq 0$.

Todistus. Jos F on K:n alikunta, se toteuttaa triviaalisti ehdot AK1-AK3. Jos kääntäen nämä ehdot ovat voimassa, niin AK1:n ja AK2:n nojalla $(F,+)$ on ryhmä, nimittäin $(K,+)$:n aliryhmä, ja samoin AK1:n ja AK3:n nojalla $(F \setminus \{0\},\cdot)$ on ryhmä (AK1 takaa sen, etteivät F ja $F \setminus \{0\}$ ole tyhjiä). Koska lisäksi F:ään periytyy distributiivisuus kunnalta K, niin F on kunta. □

Esimerkki 1. Joukko

$$\mathbb{Q}(\sqrt{n}\,) = \left\{\, a + b\sqrt{n} \;\middle|\; a, b \in \mathbb{Q} \right\} \qquad (n \text{ neliövapaa kokonaisluku} \neq 0, 1)$$

on $\mathbb{C}$:n alikunta (ja $\mathbb{R}$:n alikunta, jos $n > 0$), joka sisältää renkaan $\mathbb{Z}\,[\sqrt{n}\,]$.

Esimerkki 2. Jos $\operatorname{char}(K) = 2$, niin kunnalla K on alikuntana $\{0, 1\}$. Huomaa, että ehdon $1 + 1 = 0$ nojalla $0 - 1 = -1 = 1$.

Lause 5. *Kunnan K alikuntien leikkaus on K:n alikunta.*

Todistus. Suoraan alikuntakriteeristä. □

Lemma 1. *Jokainen kuntahomomorfismi $f : K \to K'$ indusoi kuntaisomorfismin $K \to \operatorname{Im}(f)$.*

Tämä seuraa lauseesta 3.

Millaisia alikuntia kunnalla K voi olla? Koska jokainen alikunta sisältää K:n ykkösalkion 1, se sisältää myös 1:n monikerrat $n1$. Tämä johtaa ensin seuraavaan havaintoon.

Lemma 2. *Jokainen kunta K sisältää kokonaisalueen*

$$D = \{\, n1 \mid n \in \mathbb{Z} \,\} \simeq \begin{cases} \mathbb{Z}_p, & \text{jos } \operatorname{char}(K) = p, \\ \mathbb{Z}, & \text{jos } \operatorname{char}(K) = 0. \end{cases}$$

Todistus. Muodostetaan kuvaus

$$f : \mathbb{Z} \longrightarrow K, \qquad f(n) = n1.$$

Tämä on rengashomomorfismi (tarkista), joten homomorfialauseen nojalla $\mathbb{Z}/\operatorname{Ker}(f) \simeq \operatorname{Im}(f) \subset K$. Tässä $\operatorname{Im}(f) = \{\, n1 \mid n \in \mathbb{Z} \}$ ja

$$\operatorname{Ker}(f) = \{\, n \in \mathbb{Z} \mid n1 = 0 \} = \begin{cases} p\mathbb{Z}, & \text{jos } \operatorname{char}(K) = p, \\ \{0\}, & \text{jos } \operatorname{char}(K) = 0. \end{cases}$$

Lemmassa mainitut isomorfiat saadaan nyt huomaamalla, että $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ ja $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$. Koska lisäksi $\mathbb{Z}_p$ ja $\mathbb{Z}$ ovat kokonaisalueita, väite seuraa. □

Palataan nyt alkuperäiseen kysymykseen, kunnan alikuntiin. Seuraavista lauseista ensimmäinen liittyy (yksinkertaisuudestaan huolimatta!) tärkeään kuntateorian peruskäsitteeseen, *osamääräkuntaan*, joka tulee esille myöhemmin. Toinen lause (lause 7) nojautuu tähän lauseeseen sekä lemmaan 2.

Lause 6. *Jos kunta K sisältää kokonaisalueen D, niin K:lla on alikunta*

$$K_D = \left\{ \frac{a}{b} \mid a, b \in D,\ b \neq 0 \right\}.$$

Lisäksi K_D sisältyy jokaiseen K:n alikuntaan F, joka täyttää ehdon $D \subset F$.

Todistus. Käytetään alikuntakriteeriä. Ensiksikin nähdään, että $D \subset K_D$, joten joukossa K_D on ainakin alkiot 0 ja 1. Jos $\dfrac{a}{b} \in K_D$ ja $\dfrac{c}{d} \in K_D$, niin niiden erotus $\dfrac{ad - bc}{bd} \in K_D$, samoin osamäärä $\dfrac{ad}{bc} \in K_D$ edellyttäen että $\dfrac{c}{d} \neq 0$ (huomaa, että tällöin $c \neq 0$).

Lauseen jälkimmäinen väite on ilmeinen, koska jokainen kunta F sisältää D:n alkioiden a, b mukana osamäärän $\dfrac{a}{b}$, kun $b \neq 0$. □

Esimerkki 3. Jos K on lukukunta, se sisältää kokonaisalueen $\mathbb{Z}$ (käytä lemmaa 2 tai – helpommin – ajattele suoraan luvun 1 monikertoja). Tällöin lauseessa 6 esiintyvä kunta $K_{\mathbb{Z}} = \mathbb{Q}$.

Lause 7. *Jokainen kunta K sisältää alikuntana kunnan*

$$P \simeq \begin{cases} \mathbb{Z}_p, & \text{jos } \operatorname{char}(K) = p, \\ \mathbb{Q}, & \text{jos } \operatorname{char}(K) = 0. \end{cases}$$

Todistus. Todistetaan, että P:ksi voidaan ottaa lauseen 6 mukainen kunta K_D, missä D on lemman 2 antama kokonaisalue.

Jos $\mathrm{char}(K) = p$, niin $D \simeq \mathbb{Z}_p$. Silloin D itse on kunta, joten se sisältää myös alkioidensa osamäärät. Täten $K_D = D$ ja K:lla siis on alikunta $K_D \simeq \mathbb{Z}_p$.

Oletetaan, että $\mathrm{char}(K) = 0$, jolloin

$$D = \{\, n1 \mid n \in \mathbb{Z} \,\} \simeq \mathbb{Z}.$$

Nyt siis $K_D = \left\{ \dfrac{n1}{m1} \mid n, m \in \mathbb{Z},\ m \neq 0 \right\}$. Tästä nähdään, että $K_D \simeq \mathbb{Q}$. □

MÄÄRITELMÄ. Kuntaa sanotaan *alkukunnaksi* (prime field), jos sillä ei ole aitoja alikuntia.

Lause 8. (i) *Kaikki alkukunnat (isomorfiaa vaille) ovat kunnat* $\mathbb{Z}_p$ *ja* $\mathbb{Q}$ *(*p *alkuluku).*

(ii) *Jokainen kunta* K *sisältää alikuntanaan yksikäsitteisen alkukunnan* P*; tämä on isomorfinen kunnan* $\mathbb{Z}_p$ *tai* $\mathbb{Q}$ *kanssa sen mukaan, onko* $\mathrm{char}(K) = p$ vai 0.

Todistus. (i) Rationaalilukujen kunta $\mathbb{Q}$ on alkukunta, koska se on suppein lukukunta (VI.1:n esimerkki 7). Jäännösluokkakunta $\mathbb{Z}_p$ päätellään alkukunnaksi seuraavasti: Jos F on $\mathbb{Z}_p$:n alikunta, niin ajattelemalla additiivisia ryhmiä saadaan Lagrangen lauseesta, että $\#F$ jakaa alkuluvun p. Koska $\#F$ toisaalta on > 1, se on siis $= p$.

Se, ettei ole olemassa muita alkukuntia, seuraa (ii)-kohdasta.

(ii) Väitetyn kunnan P olemassaolo todistettiin lauseessa 7. Osoitetaan vielä yksikäsitteisyys. Jos P_1 ja P_2 ovat kuntaan K sisältyviä alkukuntia, niin lauseen 5 mukaan myös $P_1 \cap P_2$ on kunta. Koska se on P_1:n ja P_2:n alikunta, niin alkukunnan määritelmän perusteella se on $= P_1$ ja $= P_2$. Tästä nähdään, että $P_1 = P_2$. □

Tämä lause osoittaa, että kunnan K karakteristika on ratkaisevassa asemassa K:n tyyppiä määritettäessä.

Lauseesta 8 seuraa myös, että *kunta ja sen alikunta sisältävät saman alkukunnan.*

ESIMERKKI 4. Äärellisen kunnan $GF(p^k)$ sisältämä alkukunta P on $\simeq \mathbb{Z}_p$. Tämä seuraa esim. siitä, että $\#P \mid p^k$ (Lagrangen lause).

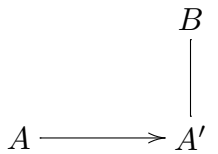
ESIMERKKI 5. Funktiokunnan $\mathbb{R}(x)$ (ks. VI.1:n esimerkki 2) sisältämä alkukunta on $\mathbb{Q}$. Esimerkki äärettömästä kunnasta, jonka karakteristika on p ja alkukunta siis $\mathbb{Z}_p$, esitetään pykälässä VI.6.

Harjoitustehtäviä

1. Oletetaan, että kunnan K karakteristika on 3. Tutki, onko joukko $\{a^9 \mid a \in K\}$ kunnan K alikunta.

VI.3 Kokonaisalueen osamääräkunta

Algebrassa esiintyy usein seuraava probleema: on annettu algebrallinen systeemi A mutta siltä puuttuu jokin haluttu ominaisuus. Voidaanko konstruoida sellainen systeemi B, jolla on tämä ominaisuus ja joka sisältää A:n? Koska isomorfiset systeemit voidaan algebrassa samaistaa, "sisältämistä" ei tässä tarvitse ottaa sananmukaisesti; riittää, että B sisältää A:n kanssa isomorfisen systeemin A'.



Esimerkki 1. Klassinen esimerkki edellisestä on lukualueen laajentaminen vaiheittain: $\mathbb{N} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$.

Tarkastellaan lähemmin vaihetta $\mathbb{Z} \to \mathbb{Q}$. Palautetaan mieleen, että rationaalilukujen konstruointi tapahtuu pääkohdittain seuraavasti:

- Muodostetaan kaikkien kokonaislukuparien (a, b), $b \neq 0$, joukko.
- Sovitaan, että parit (a, b) ja (c, d) ovat ekvivalentteja jos ja vain jos $ad = bc$.
- Otetaan käyttöön merkintä $\dfrac{a}{b}$ edustamaan paria (a, b) ja kaikkia sen kanssa ekvivalentteja pareja.
- Merkitään alkioiden $\dfrac{a}{b}$ joukkoa $\mathbb{Q}$:lla (ja nimitetään nämä alkiot *rationaaliluvuiksi*).
- Määritellään yhteen- ja kertolasku joukossa $\mathbb{Q}$.
- Samaistetaan alkiot $\dfrac{a}{1}$ kokonaislukujen a kanssa.

Lisäksi tämän konstruktion algebralliseen käsittelyyn kuuluu sen todistaminen, että saatu joukko $\mathbb{Q}$ on kunta. Konstruktion viimeinen kohta merkitsee täsmällisesti ilmaistuna, että $\mathbb{Q}$:n osajoukko $\left\{ \dfrac{a}{1} \;\middle|\; a \in \mathbb{Z} \right\}$ on kokonaisalue ja $\simeq \mathbb{Z}$.

Algebrassa on tärkeää, että *jokainen* kokonaisalue D voidaan "laajentaa" edellistä vastaavalla konstruktiolla erääksi kunnaksi $Q(D)$, ns. D:n *osamääräkunnaksi eli jakokunnaksi*. Seuraavassa suoritetaan tämä konstruktio.

Olkoon siis D kokonaisalue. Muodostetaan joukko

$$X = \{\, (a,b) \mid a,b \in D,\ b \neq 0 \}$$

ja määritellään tässä joukossa relaatio seuraavasti:

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

Tämä on ekvivalenssirelaatio (tarkista ehdot E1-E3; pane merkille, että tarvitaan supistamislakia). Näin syntyy siis joukon X ositus ekvivalenssiluokkiin $[(a,b)]$; näitä sanotaan *formaalisiksi osamääriksi* ja merkitään $\frac{a}{b}$:llä:

$$\frac{a}{b} = \{\, (x,y) \mid (x,y) \sim (a,b) \} = \{\, (x,y) \mid x,y \in D,\ y \neq 0,\ xb = ya \}\,.$$

Erityisesti

$$\frac{a}{b} = \frac{c}{d} \qquad \Longleftrightarrow \qquad ad = bc.$$

Merkitään kaikkien formaalisten osamäärien joukkoa $Q(D)$:llä:

$$Q(D) = \left\{ \frac{a}{b} \mid a,b \in D,\ b \neq 0 \right\}.$$

Määritellään joukossa $Q(D)$ yhteen- ja kertolasku:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Huomaa ensiksikin, että $bd \neq 0$. Lisäksi on varmistuttava, että nämä laskutoimitukset ovat hyvinmääriteltyjä. Osoitetaan tämä yhteenlaskusta (kertolasku samoin): Olkoon $\frac{a}{b} = \frac{a'}{b'}$ ja $\frac{c}{d} = \frac{c'}{d'}$, jolloin siis $ab' = ba'$ ja $cd' = dc'$. Väitetään, että

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

toisin sanoen $(ad+bc)b'd' = bd(a'd'+b'c')$. Tämä todetaankin helposti: vasen puoli $= (ab')dd' + bb'(cd') = (ba')dd' + bb'(dc') =$ oikea puoli.

Lause 9. *Joukko $Q(D)$ on kunta. Sen osajoukko*

$$D' = \left\{ \frac{a}{1} \mid a \in D \right\}$$

on $Q(D)$:n alirengas; tämä on kokonaisalue ja isomorfinen D:n kanssa.

Todistus. $Q(D)$ on kommutatiivinen rengas, nolla-alkiona $\frac{0}{1}$, ykkösalkiona $\frac{1}{1}$ ja alkion $\frac{a}{b}$ vasta-alkiona $\frac{-a}{b}$; rengaspostulaattien tarkistaminen on suoraviivaista (käy läpi esim. distributiivisuus).

Jos $\frac{a}{b} \neq \frac{0}{1}$, niin $a\cdot 1 \neq b\cdot 0$ eli $a \neq 0$. Täten $Q(D)$ sisältää alkion $\frac{b}{a}$. Tämä on $\frac{a}{b}$:n käänteisalkio, sillä $\frac{a}{b}\cdot\frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$. Näin ollen rengas $Q(D)$ on kunta.

Muodostetaan kuvaus

$$j : D \longrightarrow Q(D), \qquad j(a) = \frac{a}{1}.$$

Se on rengashomomorfismi (tarkista postulaatit RH1-RH3). Lisäksi j on injektio, koska yhtälöstä $\frac{a}{1} = \frac{b}{1}$ seuraa, että $a\cdot 1 = 1\cdot b$ eli $a = b$. Saadaan siis, että

$$D \simeq \mathrm{Im}(j) = \left\{ \frac{a}{1} \;\middle|\; a \in D \right\}.$$

Tämä todistaa lauseen jälkimmäiset väitteet. □

On luonnollista *samaistaa* D ja D' merkitsemällä alkiota $\frac{a}{1}$ yksinkertaisesti a:lla. (Sanotaan myös, että D *upotetaan* kuntaan $Q(D)$ kuvauksella j.) Silloin kunnassa $Q(D)$ on

$$ab^{-1} = \frac{a}{1}\cdot\left(\frac{b}{1}\right)^{-1} = \frac{a}{1}\cdot\frac{1}{b} = \frac{a\cdot 1}{1\cdot b} = \frac{a}{b},$$

joten merkintä $\frac{a}{b}$ tarkoittaa myös kunnan alkioiden a ja b *todellista* osamäärää.

MÄÄRITELMÄ. Edellä konstruoitua kuntaa $Q(D)$ sanotaan kokonaisalueen D *osamääräkunnaksi* tai *jakokunnaksi* (quotient field, field of fractions).

ESIMERKKI 2. Polynomirengas $\mathbb{R}[x]$ on kokonaisalue (mieti, milloin polynomien tulo $= 0$). Sen osamääräkunta on rationaalifunktioiden kunta $\mathbb{R}(x)$ (VI.1:n esimerkki 2).

Jos konstruoidaan osamääräkunta $Q(D)$ kokonaisalueelle D, joka sisältyy johonkin kuntaan K, niin $Q(D)$:stä tulee isomorfinen edellisessä pykälässä (lause 6) esiintyvän kunnan

$$K_D = \left\{ \frac{a}{b} \;\middle|\; a, b \in D,\ b \neq 0 \right\} \tag{1}$$

kanssa. On luonnollista samaistaa $Q(D)$ ja K_D ja nimittää siis myös kuntaa K_D kokonaisalueen D osamääräkunnaksi. (Ajattele esim. $\mathbb{Z}$:aa reaalilukujen kunnassa $\mathbb{R}$: silloin osamääräkunta $\mathbb{Q}$ on $= K_{\mathbb{Z}}$.)

Tämän jälkeen nähdäänkin, että osamääräkunnan käsite on helppo: Koska D äsken todistetun mukaan joka tapauksessa sisältyy kuntaan $K = Q(D)$, osamääräkuntaa voidaan

aina ajatella muodossa (1). Itse konstruktiota ei siis yleensä tarvitse ajatella sen jälkeen, kun se kerran on tehty!

Edellisestä nähdään myös, että *kokonaisalueen D osamääräkunta on suppein kunta, johon D sisältyy.* Jos nimittäin $D \subset K$ (= kunta), niin $D \subset K_D \subset K$.

Palataan lopuksi pykälän alussa esitettyyn yleiseen probleemaan. Oletetaan, että systeemi A saadaan laajennetuksi mainitulla tavalla systeemiksi B. Silloin B on algebrallisesti tyydyttävä vain, jos se on *yksikäsitteinen* seuraavassa mielessä: jos A on isomorfinen systeemin A_0 kanssa, niin myös niiden vastaavat laajennukset B ja B_0 ovat isomorfiset.

On helppo todistaa (vaikka se sivuutetaan tässä), että kokonaisalueen osamääräkunnalla on tämä yksikäsitteisyysominaisuus.

Esimerkki 3. Olkoon $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Osoita, että $\mathbb{Z}[i]$:n osamääräkunta on isomorfinen kunnan $\mathbb{Q}(i) = \{r + si \mid r, s \in Q\}$ kanssa. (Osoita, ensin, että jokainen kunta, joka sisältää $\mathbb{Q}$:n ja i:n, sisältää $\mathbb{Q}(i)$:n. Osoita sitten, että $(a + bi)(c + di) \in \mathbb{Q}(i)$ kun $a, b, c, d \in \mathbb{Z}$.)

VI.4 Laajennuskunta

Määritelmä. Jos K on kunnan L alikunta, sanotaan että L on kunnan K *laajennuskunta* tai *kuntalaajennus* (extension field, field extension).

Erityisesti siis jokainen kunta L on alkukuntansa P laajennuskunta.

Kunnan L osajoukon S *virittämä* alikunta K määritellään samoin kuin vastaavat käsitteet aikaisemmin:

$$K = \bigcap_{\substack{S \subset F \\ F \text{ on } L\text{:n alikunta}}} F.$$

Nyt tämä määritelmä ei kuitenkaan sellaisenaan ole käytännöllinen, sillä ei ole olemassa yksinkertaista sääntöä, jolla K:n alkiot voitaisiin muodostaa, kun S on esimerkiksi mielivaltainen äärellinen joukko L:ssä.

Muista, että L:n alikunta K sisältää aina L:n alkukunnan P. Siksi on luonnollista ottaa P mukaan virittäjäjoukkoon S, ts. valita $S = P \cup S_1$, missä S_1 on jokin L:n osajoukko. Itse asiassa on osoittautunut hyödylliseksi hyväksyä tässä P:n paikalle muitakin L:n alikuntia ja asettaa seuraava määritelmä.

Määritelmä. Olkoon F kunnan L alikunta ja S jokin L:n osajoukko. Silloin joukko $F \cup S$ virittää (yllä esitetyssä mielessä) L:n alikunnan, josta käytetään merkintää $F(S)$:

$$F \subset F(S) \subset L.$$

Kuntaa $F(S)$ sanotaan joukon S *virittämäksi eli generoimaksi* F:n *laajennuskunnaksi* (L:ssä) tai myös kunnaksi, joka saadaan *liittämällä* (adjoin) joukko S kuntaan F.

Määritelmästä seuraa myös, että $F(S)$ on L:n suppein alikunta, joka sisältää F:n ja S:n. Huomaa, että $F(S)$ on myös suppein kunnan F laajennuskunta (L:ssä), joka sisältää joukon S. Tosiasiassa vain niillä S:n alkioilla, jotka ovat F:n ulkopuolella, on merkitystä.

Jos S on äärellinen, $S = \{a_1, \ldots, a_n\}$, merkitään $F(S) = F(a_1, \ldots, a_n)$ ja sanotaan, että $F(S)$ on kunnan F *äärellisesti viritetty* laajennus. Yhden alkion virittämää laajennusta $F(a)$ sanotaan *yksinkertaiseksi*. On helppo osoittaa, että jokainen äärellisesti viritetty laajennus saadaan rakennetuksi peräkkäisistä yksinkertaisista laajennuksista.

Yhteenvetona edellisestä: Jos F ja L ovat kuntia, $F \subset L$, sekä $a \in L$, niin $F(a)$ on suppein L:n alikunta, joka sisältää F:n ja a:n; kyseessä on F:n laajennuskunta, joka saadaan liittämällä alkio a kuntaan F.

Esimerkki 1. Jos rationaalilukujen kuntaan $\mathbb{Q}$ liitetään luku $\sqrt{2}$, saadaan $\mathbb{R}$:n alikunta

$$\mathbb{Q}(\sqrt{2}\,) = \left\{ a + b\sqrt{2} \;\mid\; a, b \in \mathbb{Q} \right\}$$

(vrt. VI.2:n esimerkki 1).

Esimerkki 2. Jos reaalilukujen kuntaan liitetään imaginaariyksikkö i, saadaan koko kompleksilukujen kunta: $\mathbb{R}(i) = \mathbb{C}$.

Edellä pohdittiin kunnan F laajentamista jonkin laajemman kunnan L "sisällä". Vielä kiinnostavammaksi kuntalaajennusten teoria osoittautuu tapauksissa, joissa tällaista kuntaa L ei ole. Silloin kyseessä on sama tilanne, joka esiintyi edellisen pykälän alussa yleisenä probleemana.

Esimerkiksi kompleksilukujen kunta $\mathbb{C}$ saadaan *muodostetuksi* lähtemällä reaalilukujen kunnasta $\mathbb{R}$ ja polynomin $x^2 + 1$ nollakohdasta, jota merkitään i:llä. Näin syntyvä kunta ei sellaisenaan ole $\mathbb{R}$:n laajennus; se muodostuu "uusista" alkioista, jotka voidaan kirjoittaa esim. muodossa (a, b) tai $a + bi$, missä $a, b \in \mathbb{R}$ ja jossa on kunnan laskusääntöjen lisäksi voimassa $i^2 = -1$. Se kuitenkin sisältää $\mathbb{R}$:n kanssa isomorfisen alikunnan R_0, joka koostuu kaikista muotoa $(a, 0)$ (tai $a + 0i$) olevista alkioista. Kuten edellisessä pykälässä, on luonnollista samaistaa $\mathbb{R}$ ja R_0 eli siis merkitä $a = a + 0i$.

Samalla periaatteella muodostetaan annetun kunnan F laajennuksia $F(a)$ yleisestikin. Laajennuksen ominaisuudet riippuvat tällöin siitä polynomista (F:ssä), jonka nollakohta kuntaan F liitetään. Polynomit kytkeytyvätkin olennaisesti kuntalaajennusten teoriaan.

Tässä kurssissa esitetään vain eräät perustulokset kuntalaajennusten muodostamisesta mainitulla menetelmällä ja sovelletaan niitä äärellisten kuntien konstruointiin. Sitä ennen käsitellään tarvittavassa määrin polynomeja.

VI.5 Maksimaalinen ideaali

Seuraavassa esitetään, miten kommutatiivisesta renkaasta voidaan muodostaa kuntia *maksimaalisten ideaalien* avulla.

MÄÄRITELMÄ. Renkaan R ideaalia M sanotaan *maksimaaliseksi*, jos se on aito (ts. $M \neq R$) ja jos mikään muu R:n ideaali I ei täytä ehtoa $M \subsetneq I \subsetneq R$.

Määritelmän jälkimmäinen ehto on usein mukava ajatella muodossa

$$I \text{ on } R\text{:n ideaali ja } M \subsetneq I \qquad \Longrightarrow \qquad I = R.$$

ESIMERKKI 1. Renkaan $\mathbb{Z}_8$ ideaali $\langle \overline{2} \rangle = \{ \overline{0}, \overline{2}, \overline{4}, \overline{6} \}$ on maksimaalinen, koska sen additiivisen ryhmän indeksi ryhmässä $(\mathbb{Z}_8, +)$ on 2.

ESIMERKKI 2. Renkaan $\mathbb{Z}$ maksimaaliset ideaalit ovat ideaalit $p\mathbb{Z}$, missä p on alkuluku. Koska näet $\mathbb{Z}$ on PIR, sen kaikki ideaalit ovat muotoa $m\mathbb{Z}$, $m \geq 0$, ja

$$m_1\mathbb{Z} \subsetneq m_2\mathbb{Z} \qquad \Longleftrightarrow \qquad m_2 \mid m_1 \quad \text{ja} \quad m_2 < m_1.$$

Vertaa tämän esimerkin antamaa tietoa siihen, että jäännösluokkarengas $\mathbb{Z}/m\mathbb{Z}$ on kunta jos ja vain jos $m = p$ on alkuluku. Seuraava lause yleistää tämän tuloksen.

Lause 10. *Olkoon I kommutatiivisen renkaan R ideaali. Silloin*

$$R/I \text{ on kunta} \qquad \Longleftrightarrow \qquad I \text{ on } R\text{:n maksimaalinen ideaali.}$$

Todistus. ($\Longrightarrow$) Oletetaan, että R/I on kunta. Koska kunnassa on ainakin kaksi alkiota, niin $I \neq R$. Ideaalin I maksimaalisuuden todistamiseksi on siis vielä otettava R:n ideaali J, joka sisältää aidosti I:n, ja näytettävä että $J = R$.

Koska I on J:n aito osajoukko, on olemassa $a \in J \setminus I$. Silloin $a + I \neq I$, ts. $a + I$ ei ole kunnan R/I nolla-alkio. Sillä on siis käänteisalkio $b + I$:

$$(a + I)(b + I) = 1 + I.$$

Tästä saadaan, että $1 = ab + i$, missä $i \in I$. Mutta tällöin $1 \in J$, sillä $a \in J$ ja $i \in J$ (muista ehto I2 ideaalin määritelmässä). Se todistaa väitteen.

($\Longleftarrow$) Oletetaan nyt ideaali I maksimaaliseksi. Jäännösluokkarengas R/I on joka tapauksessa kommutatiivinen rengas. Pitää siis enää osoittaa, että sen mielivaltaisella alkiolla $a + I \neq I$ on käänteisalkio.

Koska $a \notin I$, ideaalien I ja Ra summa sisältää aidosti I:n (ks. luvun V lause 6). Ideaalin I maksimaalisuudesta seuraa silloin, että $I + Ra = R$. Erityisesti siis $1 \in I + Ra$, joten $1 = i + ra$, missä $i \in I$ ja $r \in R$. Tästä saadaan

$$1 + I = ra + I = (r + I)(a + I).$$

Alkio $r + I$ on siis $(a + I)$:n käänteisalkio renkaassa R/I. □

Kurssin loppuosan yhtenä tavoitteena on konstruoida kuntia edelliseen lauseeseen nojautuen. Sopiviksi renkaiksi ovat osoittautuneet polynomirenkaat: niissä ideaalien maksimaalisuus palautuu polynomien *jaottomuuteen.*

Tämän pykälän jäljellä oleva osa muodostaa kuitenkin oman kokonaisuutensa, joka ei tähtää kuntien konstruointiin. Tarkoituksena on liittää ideaalin maksimaalisuuden käsite yleisempään matemaattiseen yhteyteensä.

Palauta mieleen järjestetyn joukon määritelmä ja siihen liittyvät peruskäsitteet (pykälä II.8).

MÄÄRITELMÄ. Osittain järjestetyn joukon A alkiota m sanotaan *maksimaaliseksi*, jos m ei ole A:n minkään muun alkion edeltäjä, ts. jos

$$m \leq a, \quad a \in A \qquad \Longrightarrow \qquad m = a.$$

ESIMERKKI 3. Jos A on jokin reaalilukujoukko ja $\leq$ on tavallinen suuruusjärjestys, A:n suurin luku (mikäli sellainen on olemassa) on ainoa maksimaalinen alkio A:ssa.

Yleisemmin jokaisessa totaalisesti järjestetyssä joukossa on enintään yksi maksimaalinen alkio.

ESIMERKKI 4. Joukossa $\{ 1, 2, \ldots, 9 \}$, järjestettynä jaollisuusrelaation mukaan, maksimaaliset alkiot ovat 5, 6, 7, 8, 9.

Tällaista riittävän pientä osittain järjestettyä joukkoa on mukava havainnollistaa Hassen diagrammalla.

ESIMERKKI 5. Tämä esimerkki kytkee maksimaalisen alkion käsitteen pykälän alkuosaan: Renkaan R kaikkien aitojen ideaalien joukossa, järjestettynä sisältymisrelaation $\subset$ mukaan, maksimaaliset alkiot ovat R:n maksimaaliset ideaalit.

Kysymys, milloin renkaalla on (ainakin yksi) maksimaalinen ideaali, johtaa siis yleisempään kysymykseen: *Milloin osittain järjestetyllä joukolla A on maksimaalisia alkioita?*

Pohtimalla erilaisia esimerkkejä havaitaan, ettei tähän kysymykseen ole yksinkertaista vastausta (ajattele äärettömiä joukkoja). Erään käyttökelpoisen riittävän ehdon maksimaalisen alkion olemassaololle lausuu seuraava ns. *Zornin lemma.* Se voidaan todistaa joukkoteorian kuuluisan *valinta-aksiooman* avulla. Todistusta ei kuitenkaan tässä esitetä; itse asiassa valinta-aksiooma on kääntäen johdettavissa Zornin lemmasta, joten näitä kahta voidaan pitää ekvivalentteina aksioomeina joukkoteoriassa.

Zornin lemmaa varten tarvitaan seuraava käsite osittain järjestetyssä joukossa $(A, \leq)$: alkiota $y \in A$ sanotaan A:n *osajoukon S ylärajaksi*, jos $s \leq y \quad \forall \ s \in S$.

ESIMERKKI 6. Joukossa $\mathbb{Z}_+$, järjestettynä jaollisuusrelaation mukaan, osajoukon $S = \{1, 2, \ldots, 9\}$ eräs yläraja on 9!. Etsi myös jokin pienempi yläraja.

Zornin lemma. *Olkoon A osittain järjestetty joukko. Jos A:n jokaisella totaalisesti järjestetyllä osajoukolla on yläraja A:ssa, niin A:ssa on ainakin yksi maksimaalinen alkio.*

Seuraus. *Olkoon $\mathcal{P}$ jokin epätyhjä parvi joukon X osajoukkoja varustettuna sisältymisrelaation antamalla osittaisella järjestyksellä. Oletetaan, että $\mathcal{P}$:n jokaisen totaalisesti järjestetyn osaparven $\{ A_\alpha \mid \alpha \in T \}$ joukkojen unioni $\bigcup_{\alpha \in T} A_\alpha$ kuuluu $\mathcal{P}$:hen. Silloin $\mathcal{P}$:ssä on ainakin yksi maksimaalinen joukko, ts. sellainen joukko $M \subset X$, että*

$$M \subset A, \quad A \in \mathcal{P} \qquad \Longrightarrow \qquad M = A.$$

(Tässä T on indeksijoukko, joka voi olla ylinumeroituva. Mitä merkitsee oletus, että $\{ A_\alpha \mid \alpha \in T \}$ on totaalisesti järjestetty? Ajattele sitä helpompaa tapausta, että T on äärellinen tai numeroituva, esim. $T = \{1, 2, \ldots\}$; silloin ko. parvi on jono "laajenevia" joukkoja: $A_1 \subset A_2 \subset \ldots$)

Todistus. Koska jokainen joukko A_α sisältyy unioniin $\bigcup_\alpha A_\alpha$, tämä unioni on parven $\{ A_\alpha \mid \alpha \in T \}$ yläraja. Väite seuraa siis Zornin lemmasta sovellettuna parveen $\mathcal{P}$. □

Lause 11. *Jokaisessa renkaassa on ainakin yksi maksimaalinen ideaali. Tarkemmin: renkaan R jokainen aito ideaali I sisältyy ainakin yhteen R:n maksimaaliseen ideaaliin.*

Todistus. Lauseen edellinen väite seuraa jälkimmäisestä, koska R:llä on joka tapauksessa $\{0\}$ aitona ideaalina.

Jälkimmäisen väitteen todistamiseksi sovelletaan seurauslausetta parveen

$$\mathcal{P} = \{ J \mid I \subset J, \ \ J \ \text{ on } R\text{:n aito ideaali } \}.$$

$\mathcal{P}$ on epätyhjä, koska se sisältää I:n. Olkoon $\{ J_\alpha \mid \alpha \in T \}$ jokin totaalisesti järjestetty parvi $\mathcal{P}$:n joukkoja. On näytettävä, että myös unioni $\bigcup_\alpha J_\alpha$ kuuluu $\mathcal{P}$:hen; silloin $\mathcal{P}$ sisältää maksimaalisen joukon M ja tämä on haettu maksimaalinen ideaali.

Ensiksikin $\bigcup_\alpha J_\alpha$ sisältää I:n, koska jokainen J_α (yksikin riittäisi!) sisältää I:n.

Toiseksi $\bigcup_\alpha J_\alpha$ on renkaan R ideaali, kuten todetaan ideaalikriteerin avulla. Olkoon nimittäin $a, b \in \bigcup_\alpha J_\alpha$. Silloin esim. $a \in J_\alpha$ ja $b \in J_\beta$, missä $\alpha, \beta \in T$. Koska parvi $\mathcal{P}$ on totaalisesti järjestetty, niin $J_\alpha \subset J_\beta$ tai $J_\beta \subset J_\alpha$; voidaan olettaa, että $J_\alpha \subset J_\beta$. Nyt a ja b kuuluvat molemmat ideaaliin J_β, joten myös $a - b \in J_\beta$. Näin ollen $a - b \in \bigcup_\alpha J_\alpha$. Mieti itse, miksi myös alkiot ra ja ar kuuluvat tähän unioniin aina kun $r \in R$.

Kolmanneksi on varmistuttava, että ideaali $\bigcup_\alpha J_\alpha$ on aito eli $\neq R$. Tämä seuraa siitä, ettei renkaan ykkösalkio 1 kuulu mihinkään ideaaleista J_α eikä siis myöskään niiden unioniin. □

Harjoitustehtäviä

1. Etsi kaikki seuraavien renkaiden maksimaaliset ideaalit:
   a) $\mathbb{Z}_8$, b) $\mathbb{Z}_{10}$, c) $\mathbb{Z}_{12}$, d) $\mathbb{Z}_n$.
2. Olkoon $R = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ jatkuva}\}$. Osoita, että $A = \{f \in R \,|\, f(0) = 0\}$ on R:n maksimaalinen ideaali.
3. Ajatellaan tason $\mathbb{R}^2$ pisteet järjestetyksi tehtävässä II.8.3 annettuun tulojärjestykseen. Etsi osajoukosta
$$A = \{(x, y) \in \mathbb{R}^2 \mid x, y \in \mathbb{Z},\ x^2 + y^2 \leq 2\}$$
maksimaaliset alkiot.
4. Renkaan R aitoa ihannetta P sanotaan *alkuihanteeksi*, jos P täyttää ehdon $a, b \in R,\ ab \in P \implies a \in P$ tai $b \in P$. Todista, että kommutatiivisen renkaan maksimaalinen ihanne on alkuihanne. (Ohje: Tarkastele jäännösluokkarengasta R/P.)

VI.6 Polynomirengas

Edellä on useissa esimerkeissä käsitelty reaalikertoimisia polynomeja $a_0 + a_1x + \cdots + a_nx^n$ ja niiden muodostamaa rengasta. Nyt yleistetään polynomin käsite korvaamalla reaaliluvut $a_0, \ldots, a_n$ annetun (kommutatiivisen) renkaan R alkioilla. Tällöin polynomien yhteen- ja kertolasku voidaan suorittaa aivan samoin kuin reaalisessa tapauksessa soveltaen kertoimiin renkaan R laskutoimituksia.

Kaikkien tällaisten polynomien joukkoa merkitään $R[x]$:llä; siis

$$R[x] = \left\{ a_0 + a_1x + \cdots + a_nx^n \;\middle|\; n \geq 0,\ a_k \in R \quad (k = 0, \ldots, n) \right\}.$$

Joukon alkioita sanotaan *polynomeiksi yli renkaan* R (tai *renkaan* R *suhteen*). Täsmällisemmin sanottuna kyseessä ovat *yhden muuttujan* (indeterminate) x polynomit.

Miten määritellään kahden polynomin

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \tag{1}$$

$$g(x) = b_0 + b_1x + \cdots + b_mx^m \tag{2}$$

yhtäsuuruus? Reaalikertoimisia polynomeja ajateltiin funktioina $\mathbb{R} \to \mathbb{R}$, jolloin niiden yhtäsuuruus palautuu funktioiden yhtäsuuruuteen: polynomit $f(x)$, $g(x) \in \mathbb{R}[x]$ ovat yhtäsuuret, jos niiden *arvot* ovat samat kaikilla reaaliluvuilla x.

Yleisessä tapauksessa tämä funktioajattelu on korvattava "algebrallisella" lähestymistavalla. Sen mukaan polynomi $a_0 + a_1x + \cdots + a_nx^n$ on yksinkertaisesti lauseke, jonka R:n alkiot $a_0, \ldots, a_n$ määrittävät. Tällöin on luonnollista sanoa polynomeja (1) ja (2) yhtäsuuriksi, jos niillä on samat kertoimet. Siis

$$f(x) = g(x) \qquad \Longleftrightarrow \qquad n = m \quad \text{ja} \quad a_k = b_k \quad (k = 0, \ldots, n), \quad a_n \neq 0.$$

Tämä ekvivalenssi pätee siinäkin erikoistapauksessa, että $f(x), g(x) \in \mathbb{R}[x]$, joten mitään ristiriitaa ei synny (ajattele reaalikertoimisia polynomeja lineaarialgebran kannalta: $\{\, 1, x, \ldots, x^n \,\}$ on enintään astetta n olevien polynomien polynomiavaruuden P_{n+1} kanta). Yleisesti polynomin arvot eivät kuitenkaan aina määritä polynomia yksikäsitteisesti, vrt. harjoitustehtävä 4.

HUOMAUTUS. Polynomin määritteleminen "lausekkeena" $a_0 + a_1x + \cdots + a_nx^n$ ei ole aivan täsmällistä. Jos haluat täsmällisen määritelmän, ajattele polynomia äärettömänä *jonona*

$$(a_0, a_1, \ldots, a_n, 0, 0, \ldots),$$

jonka jäsenet jostain kohdasta alkaen ovat $= 0$. Jotta tällaista jonoa sitten olisi helpompi käsitellä (mm. jotta voitaisiin käyttää hyväksi tuttuja polynomien yhteydestä opittuja laskumenetelmiä), sille otetaan käyttöön merkintä $a_0 + a_1x + \cdots + a_nx^n$, missä symboli x^k ilmaisee sen, että a_k on jonon $(k+1)$:s jäsen ($k \geq 0$; symboli x^0 jätetään usein kirjoittamatta). Siis esim.

$$4 + 2x^3 - x^4 = (4, 0, 0, 2, -1, 0, 0, \ldots).$$

Lause 12. *Jos R on kommutatiivinen rengas, myös kaikki polynomit yli R:n muodostavat kommutatiivisen renkaan $(R[x], +, \cdot)$ tavalliseen tapaan määriteltyjen yhteen- ja kertolaskun suhteen.*

Polynomit $ax^0 = a$ $(a \in R)$ muodostavat $R[x]$:n alirenkaan, joka voidaan luonnollisella tavalla samaistaa renkaan R kanssa.

Renkaasta $R[x]$ käytetään nimitystä *polynomirengas (yli R:n)*. Tässä ovat täydellisyyden vuoksi polynomien summan ja tulon muodostamissäännöt näkyviin kirjoitettuina (polynomit $f(x)$ ja $g(x)$ kuten (1):ssä ja (2):ssa, $n \leq m$):

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_mx^m,$$
$$f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_mx^{n+m}.$$

Polynomeja $ax^0 = a$ sanotaan *vakiopolynomeiksi.*

Lauseen todistus. On tarkistettava, että polynomien yhteen- ja kertolasku noudattavat kommutatiivisen renkaan postulaatteja. Useimpien postulaattien kohdalla asia todetaan välittömästi; esim. nolla-alkio on vakiopolynomi 0 (*nollapolynomi*), ykkösalkio on vakiopolynomi 1 ja polynomin $f(x)$ vasta-alkio on $-f(x)$. Eräiden postulaattien tarkistaminen vaatii enemmän kirjoitustyötä (mieti esim. tulon assosiatiivisuutta).

Lauseen loppuosa on ilmeinen. □

Kun polynomien laskutoimitukset on näin määritelty, todetaan että myös alkuperäisessä polynomin lausekkeessa $a_0 + a_1x + \cdots + a_nx^n$ esiintyvät summa- ja tulomerkinnät voidaan tulkita näiden mukaisesti: esim. $a_0 + a_1x$ = vakiopolynomin a_0 ja polynomin a_1x summa ja a_kx^k = vakiopolynomin a_k ja polynomin (monomin) $x^k = 1 \cdot x^k$ tulo. Merkinnöissä ei siis synny monikäsitteisyyttä.

MÄÄRITELMÄ. Jos polynomissa $f(x) = a_0 + a_1x + \cdots + a_nx^n$ on $a_n \neq 0$, kerrointa a_n sanotaan $f(x)$:n *johtavaksi kertoimeksi* ja lukua n sanotaan $f(x)$:n *asteeksi* (degree), merkitään $n = \deg f(x)$.

Polynomia $f(x)$ sanotaan *pääpolynomiksi* (monic polynomial), jos sen johtava kerroin $= 1$.

Näin tulee määritellyksi jokaiselle polynomille $\neq 0$ johtava kerroin ja aste ≥ 0.

Sopimus: nollapolynomin aste $\deg(0) = -\infty$. (Symbolien ∞ ja $-\infty$ merkitykseen matemaattisissa kaavoissa on yleensä suhtauduttava erityisen varovasti. Polynomien asteiden välisissä kaavoissa $-\infty$ kuitenkin yksinkertaisesti ajatellaan "lukuna", joka on pienempi kuin kaikki reaaliluvut; vrt. pykälän II.6 loppu.)

ESIMERKKI 1. Tarkastellaan polynomeja $f(x) = 1+x$ ja $g(x) = 1-x$ yli mielivaltaisen kommutatiivisen renkaan R. Todetaan, että

$$f(x) + g(x) = 2, \qquad f(x)g(x) = 1 - x^2.$$

Nyt siis $\deg f(x) = \deg g(x) = 1$ ja edelleen $\deg(f(x) + g(x)) = 0$ (tai $-\infty$, jos R:ssä on $2 = 0$) sekä $\deg f(x)g(x) = 2$.

Lause 13. *Jos R on kokonaisalue, niin myös polynomirengas $R[x]$ on kokonaisalue ja*

$$\deg f(x)g(x) = \deg f(x) + \deg g(x) \quad \forall \ f(x),\, g(x) \in R[x]. \tag{3}$$

Todistus. Olkoot $f(x)$:n ja $g(x)$:n johtavat kertoimet a_n ja b_m. Tulossa $f(x)g(x)$ esiintyvä korkein termi on $a_nb_mx^{n+m}$; tässä nimittäin $a_nb_m \neq 0$, koska R:ssä ei ole nollanjakajia. Nähdään siis ensiksikin, että tulopolynomin aste $= n+m$. Mutta silloin erityisesti tulopolynomi $\neq 0$, joten myöskään $R[x]$:ssä ei ole nollanjakajia. Polynomirengas $R[x]$ on siis kokonaisalue.

Jos $f(x) = 0$ tai $g(x) = 0$, myös tulo $= 0$ ja yhtälön (3) molemmat puolet ovat $= -\infty$. □

ESIMERKKI 2. Koska $\mathbb{Z}_p$ (p alkuluku) on kokonaisalue, lauseen 13 mukaan myös polynomirengas $\mathbb{Z}_p[x]$ on kokonaisalue ja sillä siis on osamääräkunta

$$\mathbb{Z}_p(x) = \left\{ \frac{p(x)}{q(x)} \;\middle|\; p(x),\, q(x) \in \mathbb{Z}_p[x],\; q(x) \neq \text{ nollapolynomi} \right\}.$$

Tätä sanotaan *rationaalifunktioiden kunnaksi yli kunnan* $\mathbb{Z}_p$ (vrt. VI.1:n esimerkki 2). Huomaa, että $\text{char}(\mathbb{Z}_p(x)) = p$, vaikka $\mathbb{Z}_p(x)$ on ääretön kunta.

Harjoitustehtäviä

1. Laske renkaan $\mathbb{Z}_7[x]$ polynomeilla $a = 1 + 2x + x^2$ ja $b = x^2 + 2$ polynomit $a + b$, ab ja b^5.
2. Määritä polynomien $1 - 4x + 6x^2$ ja $x + 2x^2 + 10x^3$ tulon aste polynomirenkaissa $\mathbb{R}[x]$, $\mathbb{Z}_4[x]$, $\mathbb{Z}_5[x]$.
3. Etsi polynomin $2x + 1 \in \mathbb{Z}_4[x]$ käänteispolynomi.
4. Tutki, mitä arvoja $\mathbb{Z}_3[x]$:n polynomit $x^4 + x$ ja $x^2 + x$ saavat.
5. Millä polynomeilla on käänteispolynomi $\mathbb{Z}[x]$:ssä? (Tutki ensin vakiopolynomit ja käytä sitten lausetta 13).
6. Näytä, että polynomilla $F = 1 - 2x$ on käänteispolynomi renkaassa $\mathbb{Z}_{16}[x]$.
   (Ohje: Ratkaise $G \in \mathbb{Z}_{16}[x]$ yhtälöstä $FG = 1$.)

VI.7 Polynomien jaollisuus

Tästedes oletetaan, että polynomien kertoimet kuuluvat *kuntaan* K.

Äskeistä lausetta 13 ajatellen on nyt ensimmäinen luonnollinen kysymys: Kun K on kunta, onko myös polynomirengas $K[x]$ kunta? Vastaus on kielteinen. Polynomilla $f(x) \in K[x]$ on näet käänteisalkio $K[x]$:ssä vain siinä tapauksessa, että $f(x)$ on nollasta eroava vakiopolynomi. Tämä todetaan päättelemällä lauseen 13 avulla seuraavasti:

$$f(x)g(x) = 1 \quad \Longrightarrow \quad \deg f(x) + \deg g(x) = 0 \quad \Longrightarrow \quad \deg f(x) = \deg g(x) = 0.$$

Polynomirenkaalla $K[x]$ on siis samanlainen algebrallinen rakenne kuin kokonaislukujen renkaalla $\mathbb{Z}$: se on kokonaisalue mutta ei kunta. Tästä seuraa, että polynomeille (yli kunnan K) saadaan samanlainen jaollisuusteoria kuin kokonaisluvuille. Seuraavassa esitetään tämän teorian pääkohdat; useimmat asiat ovat tuttuja koulukurssista kunnan $K = \mathbb{R}$ tapauksessa.

MÄÄRITELMÄ. Olkoot $a(x)$, $b(x) \in K[x]$. Jos on olemassa sellainen polynomi $c(x) \in K[x]$, että $a(x) = b(x)c(x)$, sanotaan, että polynomi $a(x)$ on *jaollinen* polynomilla $b(x)$; merkitään $b(x) \mid a(x)$. Käytetään myös sanontoja: $b(x)$ *jakaa* $a(x)$:n, $b(x)$ on $a(x)$:n *tekijä*, $a(x)$ on $b(x)$:n *monikerta.*

ESIMERKKI 1. (1) $(x-1) \mid (x^2-1)$ $K[x]$:ssä, missä K on mielivaltainen kunta;

(2) $(x+1) \mid (x^2+1)$ $\mathbb{Z}_2[x]$:ssä, koska tässä renkaassa $x^2+1 = (x+1)^2$;

(3) $(x+1) \nmid (x^2+1)$ $\mathbb{R}[x]$:ssä.

HUOMAUTUS. Seuraavassa käsitellään usein esimerkkejä, joissa kunta K on jokin jäännösluokkakunta $\mathbb{Z}_p$ (p alkuluku). Kuten edellisessä esimerkissä, $\mathbb{Z}_p[x]$:n polynomien kertoimista jätetään tällöin yleensä jäännösluokkamerkintä (yläviiva) kirjoittamatta näkyviin; siis esim. merkinnällä $2 + 5x - x^3$ tarkoitetaan polynomia $\overline{2} + \overline{5}x - x^3$. Huomaa, että

$$\begin{aligned} 2 + 5x - x^3 &= x - x^3 = x + x^3 && \mathbb{Z}_2[x] \text{ :ssä,} \\ 2 + 5x - x^3 &= 2 - x^3 = 2 + 4x^3 && \mathbb{Z}_5[x] \text{ :ssä.} \end{aligned}$$

Jaollisuusrelaatiolla on useita samoja perusominaisuuksia kuin kokonaislukujen tapauksessa, mm. aina $a(x) \mid a(x)$ ja

$$\begin{aligned} a(x) \mid b(x), \quad b(x) \mid c(x) \quad &\Longrightarrow \quad a(x) \mid c(x), \\ a(x) \mid b(x), \quad a(x) \mid c(x) \quad &\Longrightarrow \quad a(x) \mid (b(x) + c(x)). \end{aligned}$$

Eräät ominaisuudet ovat nyt hiukan toisenlaisia, esim.

$$a(x) \mid b(x), \quad b(x) \mid a(x) \quad \Longrightarrow \quad a(x) = k \cdot b(x), \quad \text{missä } \; k \in K \setminus \{0\}.$$

(Jos haluat miettiä, mistä eroavuus $\mathbb{Z}$:aan verrattuna johtuu, ajattele renkaiden $\mathbb{Z}$ ja $K[x]$ yksikköryhmiä: $\mathbb{Z}^* = \{\pm 1\}$ ja $K[x]^* = K \setminus \{0\}$.)

Tutkittaessa annetun polynomin $a(x)$ jaollisuutta toisella polynomilla $b(x)$ voidaan käyttää samanlaista jakoalgoritmia ("jakokulmalaskua") kuin kokonaisluvuilla. Vertaa seuraavaa lausetta lauseeseen I.2.

Lause 14 (Jakoyhtälö). *Jos $a(x)$, $b(x) \in K[x]$ ja $b(x) \neq 0$, on olemassa yksikäsitteiset polynomit $q(x)$ ja $r(x)$ (= "jakojäännös"), joilla*

$$a(x) = q(x)b(x) + r(x), \qquad \deg r(x) < \deg b(x). \tag{1}$$

Todistus. Valitaan joukosta $S = \{\, a(x) - k(x)b(x) \mid k(x) \in K[x] \,\}$ polynomi

$$r(x) = a(x) - q(x)b(x),$$

jonka aste on mahdollisimman pieni. Jos $r(x) = 0$, niin sen aste on $-\infty$ ja (1) on siis voimassa. Muussa tapauksessa on näytettävä, että luku $n = \deg r(x)$ on pienempi kuin $m = \deg b(x)$. Olkoot $r(x)$:n ja $b(x)$:n johtavat kertoimet vastaavasti r_n ja b_m. Jos nyt n olisi $\geq m$, niin voitaisiin muodostaa polynomi

$$s(x) = a(x) - \left(q(x) + \frac{r_n}{b_m} \cdot x^{n-m}\right) b(x) = r(x) - \frac{r_n}{b_m} \cdot x^{n-m} b(x),$$

joka kuuluu joukkoon S ja jossa n:nnen asteen termin kerroin on

$$r_n - \frac{r_n}{b_m} \cdot b_m = 0.$$

Tästä nähdään, että $s(x)$ on pienempää astetta kuin $r(x)$, mikä on vastoin polynomin $r(x)$ valintaa. Näin ollen $n < m$.

Yksikäsitteisyys: Jos myös $a(x) = q'(x)b(x) + r'(x)$, missä $\deg r'(x) < \deg b(x)$, niin

$$r(x) - r'(x) = (q'(x) - q(x))b(x), \qquad \deg(r(x) - r'(x)) < \deg b(x).$$

Toisaalta lauseen 13 mukaan $\deg(r(x) - r'(x)) = \deg(q'(x) - q(x)) + \deg b(x)$, joten $\deg(q'(x) - q(x)) < 0$. Silloin välttämättä $q'(x) - q(x) = 0$. Tästä seuraa, että $r(x) - r'(x) = 0 \cdot b(x) = 0$. Siis $q'(x) = q(x)$ ja $r'(x) = r(x)$. $\square$

Esimerkki 2. Renkaan $\mathbb{Q}[x]$ polynomeihin $a(x) = 2x^3 + x^2 - x - 1$ ja $b(x) = x^2 - 2$ sovellettuna jakoalgoritmi antaa tuloksen

$$2x^3 + x^2 - x - 1 = (2x + 1)(x^2 - 2) + (3x + 1).$$

Siis $q(x) = 2x + 1$ ja $r(x) = 3x + 1$.

Entä jos tarkastellaan näitä polynomeja $a(x)$ ja $b(x)$ yli jonkin kunnan $\mathbb{Z}_p$? Mieti miksi saatu kaava pätee silloinkin. Kirjoita tulos erityisesti $\mathbb{Z}_2[x]$:ssä ja $\mathbb{Z}_3[x]$:ssä sieventäen polynomit yksinkertaisempaan muotoon.

Esimerkki 3. Sovelletaan jakoalgoritmia $\mathbb{Z}_5[x]$:n polynomeihin $3x^2 + 1$ ja $2x + 3$.

Jos $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ ja $c \in K$, merkitään

$$f(c) = a_0 + a_1c + \cdots + a_nc^n.$$

Huomaa, että $f(c)$ on kunnan K alkio; se voidaan lukea "f arvolla c". Näin saadaan analyysista tuttu *polynomikuvaus*

$$K \longrightarrow K, \qquad c \mapsto f(c).$$

Jos erityisesti $f(c) = 0$, sanotaan, että c on polynomin $f(x)$ *nollakohta* tai yhtälön $f(x) = 0$ *juuri.*

Jos $a(x) = f(x) + g(x)$ ja $b(x) = f(x)\cdot g(x)$ (missä $f(x)$, $g(x) \in K[x]$), niin nähdään, että

$$a(c) = f(c) + g(c), \qquad b(c) = f(c)\cdot g(c).$$

Tuloksena on "sijoitusperiaate": *Jokainen $K[x]$:n polynomien toteuttama yhtälö toteutuu kunnassa K, kun x:n paikalle sijoitetaan mikä tahansa kunnan K alkio c.*

Lause 15. *Olkoon $f(x) \in K[x]$ ja $c \in K$. Silloin*

$$f(c) = 0 \qquad \Longleftrightarrow \qquad (x - c) \mid f(x).$$

Todistus. ($\Longrightarrow$) Jakoalgoritmin nojalla $f(x) = q(x)(x-c)+r(x)$, missä $\deg r(x) < 1$. Täten $r(x)$ on vakiopolynomi, $r(x) = r \in K$. Kun nyt yhtälöön sijoitetaan $x = c$, saadaan $r = f(c) = 0$. Siis $f(x)$ on jaollinen polynomilla $x - c$.

($\Longleftarrow$) Oletuksen mukaan $f(x) = (x - c)g(x)$, missä $g(x) \in K[x]$. Sijoittamalla jälleen $x = c$ saadaan tulos $f(c) = 0$. $\square$

Lauseesta saadaan seuraus: *n:nnen asteen polynomilla $f(x)$ yli kunnan K on enintään n eri nollakohtaa K:ssa.* Olkoot nimittäin $c_1, \ldots, c_k$ tällaisia nollakohtia. Silloin lauseen mukaan $f(x) = (x - c_1)g(x)$, missä $g(x) \in K[x]$. Sijoittamalla $x = c_2$ saadaan

$$(c_2 - c_1)g(c_2) = 0.$$

Koska $c_2 - c_1 \neq 0$, eikä kunnassa ole nollanjakajia, tästä seuraa, että $g(c_2) = 0$. Soveltamalla lausetta uudelleen saadaan $g(x) = (x - c_2)h(x)$, missä $h(x) \in K[x]$, ja jatkamalla samoin päädytään tulokseen

$$(x - c_1)(x - c_2)\cdots(x - c_k) \mid f(x).$$

Polynomin $f(x)$ aste on siis $\geq k$.

Esimerkki 4. Olkoon p alkuluku. Näytetään, että polynomirenkaassa $\mathbb{Z}_p[x]$ on

$$x^{p-1} - 1 = \prod_{a=1}^{p-1} (x - a).$$

Päätellään tästä lukuteorian *Wilsonin lause*: $(p-1)! \equiv -1 \pmod{p}$.

Edellisestä yhtälöstä seuraa myös, että polynomin $f(x) = x^p - x \in \mathbb{Z}_p[x]$ nollakohtia ovat kunnan $\mathbb{Z}_p$ *kaikki* alkiot, toisin sanoen $f(x)$ on identtisesti 0 vaikka se ei ole nollapolynomi. (Tällainen tilanne olisi absurdi $\mathbb{R}[x]$:ssä. Katso uudestaan yleistä polynomien yhtäsuuruuden määritelmää pykälästä VI.6.)

Määritelmä. Polynomia $f(x) \in K[x]$ sanotaan *jaottomaksi* (irreducible), jos $f(x)$ ei ole vakiopolynomi eikä kahden positiivista astetta olevan polynomin ($\in K[x]$) tulo.

Käytetään myös sanontaa: $f(x)$ on jaoton *kunnan K suhteen* (tai *yli*).

Tämän mukaan kaikki 1. asteen polynomit ovat jaottomia.

Jos $\deg f(x) > 1$ ja $f(x)$:llä on nollakohta K:ssa, lauseesta 15 seuraa, ettei $f(x)$ ole jaoton K:n suhteen.

Esimerkki 5. Polynomi $x^2 + 1$ on jaoton $\mathbb{R}$:n suhteen, sillä muuten sillä olisi ensimmäisen asteen tekijä $x - c \in \mathbb{R}[x]$ (huomaa että $ax + b = a\left(x + \frac{b}{a}\right)$) ja siis lauseen 15 mukaan nollakohta $c \in \mathbb{R}$.

Mutta $x^2 + 1$ ei ole jaoton $\mathbb{C}$:n suhteen: $x^2 + 1 = (x + i)(x - i)$.

Tämän esimerkin päättelyä soveltaen nähdään, että 2. *ja* 3. *asteen polynomit $K[x]$:ssä ovat jaottomia jos ja vain jos niillä ei ole nollakohtaa K:ssa.* (Ajattele, millä tavoilla 3 voidaan kirjoittaa positiivisten kokonaislukujen summana.)

Jos $\deg f(x) > 3$, $f(x)$ voi luonnollisesti olla kahden sellaisen jaottoman polynomin tulo, joiden asteet ovat > 1; esim.

$$x^4 + 2x^2 + 1 = (x^2 + 1)^2 \in \mathbb{R}[x].$$

Tällöin $f(x)$ ei ole jaoton mutta sillä ei myöskään ole nollakohtia.

Esimerkki 6. Tutkitaan, onko $x^3 + 3x + 2$ jaoton kuntien $\mathbb{Z}_3$ ja $\mathbb{Z}_5$ suhteen.

Palauta mieleen koulukurssista tuttu menetelmä polynomin $f(x) \in \mathbb{Q}[x]$ rationaalisten nollakohtien löytämiseksi.

Algebran peruslause sanoo, että jokaisella polynomilla $f(x) \in \mathbb{C}[x] \setminus \mathbb{C}$ on nollakohta $\mathbb{C}$:ssä; $f(x)$ hajoaa siis 1. asteen tekijöihin $\mathbb{C}[x]$:ssä. Algebran peruslause todistetaan mukavimmin kompleksifunktioiden teorian avulla (alkeellisempiakin todistuksia sille on kyllä keksitty). Pitää myös paikkansa, että jokainen polynomi $f(x) \in K[x] \setminus K$ voidaan esittää jaottomien polynomien tulona ja esitys on yksikäsitteinen näiden polynomien järjestystä ja vakiotekijöitä vaille. (Ei todisteta tässä.)

Harjoitustehtäviä

1. Jaa polynomi $3x^4 + x^3 + 2x^2 + 1$ polynomilla $x^2 + 4x + 2$ renkaassa $\mathbb{R}[x]$. Muuttuuko vastaus, jos jako tehdään renkaassa $\mathbb{Z}_5[x]$?
2. Mitkä ovat polynomin $x^2 + 3x + 2$ nollakohdat $\mathbb{Z}_6$:ssa?
3. Tutki polynomin $x^2 + 1$ tekijöihinjakoa kunnan $\mathbb{Z}_5$ suhteen.
4. Olkoon F kunta ja $a \neq 0$, $a \in F$. Todista:
   a) Jos $af(x)$ on jaoton F:n suhteen, niin $f(x)$ on jaoton F:n suhteen.
   b) Jos $f(ax)$ on jaoton F:n suhteen, niin $f(x)$ on jaoton F:n suhteen.
   c) Jos $f(x + a)$ on jaoton F:n suhteen, niin $f(x)$ on jaoton F:n suhteen.
5. Hajota polynomi $x^4 - 2$ alkutekijöihinsä renkaissa $\mathbb{Q}[x]$, $\mathbb{R}[x]$ ja $\mathbb{C}[x]$. (Ohje: Alkutekijäesityksen yksikäsitteisyys.)
6. Määritä renkaan $\mathbb{Z}_7[x]$ alkioiden $F = 2x^4 + 1$ ja $G = x^5 + 2x^4 + x^3 + 5$ suurin yhteinen tekijä $D \in \mathbb{Z}_7[x]$.
7. Näytä, ettei osajoukon $\{2, x\}$ virittämä renkaan $\mathbb{Z}[x]$ ideaali I ole pääideaali. (Ohje: Näytä, että I:n jokaisen nollasta poikkeavan alkion vakiotermi on parillinen ja käytä epäsuoraa todistusta.)
8. Etsi tehtävässä 6 sellaiset polynomit $U, V \in \mathbb{Z}_7[x]$, että $D = UF + VG$.
9. Näytä, että tekijärengas $A = \mathbb{Z}_3[x]/I$, missä I on alkion $F = x^2 + 1$ virittämä pääideaali, on yhdeksän alkion kunta. (Ohje: Näytä, että F on jaoton renkaassa $\mathbb{Z}_3[x]$, ja etsi käänteisalkiot Eukleideen algoritmilla.)

VI.8 Miten jaottomat polynomit tuottavat kuntia

Muista, että kommutatiivisen renkaan R jäännösluokkarengas R/I on kunta, jos ideaali I on maksimaalinen (lause 10). Seuraavassa valitaan $R = K[x]$, missä K on annettu kunta, ja näytetään, että jaottomien polynomien virittämät $K[x]$:n pääideaalit ovat maksimaalisia. Näin saadaan muodostetuksi uusia kuntia.

Polynomin $f(x) \in K[x]$ virittämä pääideaali on lauseen V.7 mukaan muotoa

$$\langle f(x) \rangle = \left\{ k(x)f(x) \;\middle|\; k(x) \in K[x] \right\}.$$

Huomaa, että $\langle f(x) \rangle = \langle cf(x) \rangle$, olipa c mikä tahansa kunnan K alkio $\neq 0$.

Lemma. *Kaikki polynomirenkaan $K[x]$ ideaalit I ovat pääideaaleja, ts. $K[x]$ on PIR.*

Todistus. (Vertaa lauseiden IV.5 ja IV.6 todistuksiin.) Jos $I = \{0\}$, se on pääideaali, nimittäin $\langle 0\rangle$. Oletetaan, että $I \neq \{0\}$. Olkoon $b(x)$ sellainen nollapolynomista eroava polynomi I:ssä, jonka aste on mahdollisimman pieni. Näytetään, että $I = \langle b(x)\rangle$.

Koska $b(x) \in I$, niin $\langle b(x)\rangle \subset I$. Kääntäen, jos $a(x) \in I$, niin jakoalgoritmi antaa

$$a(x) = q(x)b(x) + r(x), \qquad \deg r(x) < \deg b(x).$$

Nyt $r(x) = a(x) - q(x)b(x) \in I$, joten $b(x)$:n valinnan nojalla $r(x) = 0$. Tästä saadaan, että $a(x) = q(x)b(x) \in \langle b(x)\rangle$. Siis tuloksena on $I \subset \langle b(x)\rangle$. $\square$

Lause 16. *Jos $p(x)$ on $K[x]$:n jaoton polynomi, niin ideaali $I = \langle p(x)\rangle$ on $K[x]$:n maksimaalinen ideaali.*

Todistus. Koska $\deg p(x) \geq 1$, I ei sisällä vakiopolynomeja $\neq 0$. Se on siis aito ideaali.

Olkoon J $K[x]$:n ideaali, joka sisältää aidosti I:n. On osoitettava, että $J = K[x]$.

Lemman mukaan J on pääideaali, siis $J = \langle b(x)\rangle$, missä $b(x) \in K[x]$. Koska $I \subsetneq J$, polynomi $p(x)$ on muotoa $k(x)b(x)$, missä $k(x) \in K[x]$. Mutta $p(x)$ oletettiin jaottomaksi; täten $k(x)$ tai $b(x)$ on vakiopolynomi. Jos $k(x)$ on vakio, nähdään että $\langle p(x)\rangle = \langle b(x)\rangle$, toisin sanoen $I = J$, mikä on vastoin J:n valintaa. Näin ollen $b(x)$ on vakio, $b(x) = b \in K \setminus \{0\}$. Silloin saadaan

$$J = \langle b\rangle = \langle 1\rangle = K[x] \cdot 1 = K[x] \quad \square$$

Seuraus. *Jos $p(x)$ on $K[x]$:n jaoton polynomi, niin jäännösluokkarengas $K[x]\,/\langle p(x)\rangle$ on kunta.*

Millainen kunta $K[x]\,/\langle p(x)\rangle$ on? Merkitään $I = \langle p(x)\rangle$ ja $d = \deg p(x)$. Kuten kaikki jäännösluokkarenkaat, $K[x]\,/\,I$ voidaan esittää muodossa

$$K[x]\,/\,I = \big\{\, f(x) + I \;\big|\; f(x) \in K[x]\big\} = \big\{\, f(x) + I \;\big|\; f(x) \in D\big\}\,,$$

missä D on jokin jäännösluokkien edustajisto. Huomaa, että $f_1(x)$ ja $f_2(x)$ kuuluvat samaan jäännösluokkaan jos ja vain jos $f_1(x) - f_2(x)$ on jaollinen $p(x)$:llä. Tästä seuraa jakoalgoritmin avulla, että edustajistoksi kelpaa

$$D = \big\{\, r(x) \in K[x] \;\big|\; \deg r(x) < d\big\}\,.$$

Täten

$$\begin{aligned} K[x]\,/\,I &= \big\{\, r(x) + I \;\big|\; r(x) \in K[x],\ \deg r(x) < d\big\} \\ &= \big\{\, a_0 + a_1x + \cdots + a_{d-1}x^{d-1} + I \;\big|\; a_i \in K \quad \forall\ i\,\big\}\,. \end{aligned}$$

Jäännösluokkien $r_1(x) + I$ ja $r_2(x) + I$ summa ja tulo muodostetaan tavalliseen tapaan laskemalla niiden edustajien summa ja tulo; tulopolynomi $r_1(x)r_2(x)$ palautetaan muotoon $a_0 + a_1x + \cdots + a_{d-1}x^{d-1}$ vähentämällä siitä sopiva $p(x)$:n monikerta (käyttäen esim. jakoalgoritmia).

Lause 17. *Kunta $K[x]\,/\langle p(x)\rangle$ sisältää alikunnan K', joka on isomorfinen kunnan K kanssa; kun K samaistetaan K':n kanssa, tulee kunnasta $K[x]\,/\langle p(x)\rangle$ siis K:n laajennus. Tässä laajennuksessa polynomilla $p(x)$ on nollakohta.*

Todistus. Kuten edellä merkitään $I = \langle p(x)\rangle$. Kuvaus

$$j : K \longrightarrow K[x]\,/\,I, \qquad j(a) = a + I,$$

on kuntahomomorfismi (tarkista). Sen kuva $K' = \mathrm{Im}(j)$ on siis pykälän VI.2 lemman 1 nojalla isomorfinen K:n kanssa:

$$K \simeq K' = \left\{ a + I \;\middle|\; a \in K \right\}.$$

Kuntien K ja K' samaistaminen merkitsee nyt, että K:n alkiot a samaistetaan jäännösluokkiin $a + I$.

Erityisesti siis polynomin $p(x) \in K[x]$ kertoimia voidaan pitää myös kunnan $K[x]\,/\,I$ alkioina. Koska symboli x sai edellä tietyn merkityksen tämän kunnan alkioiden merkinnässä, on parempi kirjoittaa polynomin määräämättömäksi esim. y, siis $p(y) \in (\,K[x]\,/\,I)[y]$. Mikä kunnan alkioista on tämän nollakohta? Yksinkertaisesti alkio $x + I$, sillä jäännösluokkien laskusääntöjen mukaan

$$p(x + I) = p(x) + I = 0 + I. \quad \square$$

Esimerkki 1. Valitaan $K = \mathbb{R}$ ja $p(x) = x^2 + 1$. Edellisen mukaan tällöin saadaan seuraava kunta (missä $I = \langle x^2 + 1\rangle$):

$$\mathbb{R}[x]\,/\,I = \left\{\, a + bx + I \;\middle|\; a, b \in \mathbb{R} \right\},$$

$$\begin{aligned}(a + bx + I) + (a' + b'x + I) &= (a + a') + (b + b')x + I,\\ (a + bx + I)\cdot(a' + b'x + I) &= (aa' - bb') + (ab' + a'b)x + I\end{aligned}$$

(tuloa laskettaessa vähennettiin jäännösluokan edustajasta $bb'(x^2 + 1)$). Lisäksi tiedetään siis, että tämä kunta on $\mathbb{R}$:n laajennus, joka sisältää yhtälön $x^2 + 1 = 0$ juuren.

Näin muodostettu kunta on mikäpä muu kuin – kompleksilukujen kunta $\mathbb{C}$. Näet sen välittömästi, jos merkitset $a + bx + I = (a, b)$ tai $= a + bi$.

Lauseen todistuksessa saatiin polynomin $y^2 + 1$ nollakohdaksi $x + I$, siis "parempia" merkintöjä käyttäen $(0, 1)$ eli $0 + 1\cdot i = i$, kuten pitääkin.

Esimerkki 2. Polynomi x^2+x+1 on jaoton kunnan $\mathbb{Z}_2$ yli (tarkista), joten saadaan kunta

$$\begin{aligned}\mathbb{Z}_2[x]\,/\,I &= \left\{\, a+bx+I \;\middle|\; a,b\in\mathbb{Z}_2 \right\} \qquad (I=\langle x^2+x+1\rangle)\\ &= \{\, I,\, 1+I,\, x+I,\, 1+x+I \,\}\,.\end{aligned}$$

Kyseessä on siis 4 alkion kunta $GF(2^2)$. Jos kunnan alkioita merkitään $0 = I$ (nolla-alkio), $1 = 1+I$ (ykkösalkio), $\alpha = x+I$ ja $\beta = 1+x+I$, saadaan sen additiiviselle ja multiplikatiiviselle ryhmälle seuraavat taulut:

$$\underline{GF\left(2^2\right) = \{\ 0\ ,\ 1\ ,\, \alpha,\, \beta\,\}}$$

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	1	α	β
1	1	α	β
α	α	β	1
β	β	1	α

Tässä esimerkiksi tulo $\alpha\beta$ laskettiin näin:

$$\alpha\beta = x(1+x)+I = x+x^2+I = -1+I = 1+I = 1\,.$$

Tarkistetaan vielä (taulujen avulla), että α on alkuperäisen polynomin nollakohta:

$$\alpha^2+\alpha+1 = \beta+\alpha+1 = 1+1 = 0\,.$$

Vastaavanlainen konstruktio voidaan tehdä lähtien mistä tahansa polynomista $q(x)$, joka on jaoton yli jonkin kunnan $\mathbb{Z}_p$. Tuloksena on silloin äärellinen kunta $GF\left(p^d\right)$, missä $d = \deg q(x)$.

Vertaa edellistä yhteenlaskutaulua Kleinin 4-ryhmään luvussa III.2.

LIITE 1

Reaaliluvut

1. Reaalilukujen määrittely aksiomaattisesti

Reaalilukujen joukko $\mathbb{R}$ on tässä kirjassa esiintynyt vain esimerkeissä ja harjoitustehtävissä. Näissä on riittänyt ajatella reaalilukuja intuitiiviselta pohjalta, lukuina jotka jokainen tuntee. Mutta $\mathbb{R}$ voidaan määritellä myös täsmällisesti. Määrittely on mahdollista tehdä joko joukko-opillisesti konstruoimalla $\mathbb{R}$ luonnollisten lukujen avulla tai aksiomaattisesti ilman luonnollisia lukuja. Tässä liitteessä määritellään $\mathbb{R}$ aksiomaattisesti.

Olkoon annettuna joukko $\mathbb{R}$, jossa on määritelty *yhteenlasku* ja *kertolasku*, täsmällisemmin sanottuna kuvaukset

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ (x, y) \mapsto x + y,$$
$$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ (x, y) \mapsto x \cdot y$$

siten, että seuraavat aksioomat ovat voimassa:

(R1) $x + y = y + x \quad \forall x, y \in \mathbb{R}$;
(R2) $x + (y + z) = (x + y) + z \quad \forall x, y, z \in \mathbb{R}$;
(R3) $\exists 0 \in \mathbb{R} : \quad x + 0 = x \quad \forall x \in \mathbb{R}$;
(R4) $\forall x \in \mathbb{R}\ \exists x' \in \mathbb{R} : \quad x + x' = 0$;
(R5) $xy = yx \quad \forall x, y \in \mathbb{R}$;
(R6) $x(yz) = (xy)z \quad \forall x, y, z \in \mathbb{R}$;
(R7) $\exists \quad 1 \in \mathbb{R} : \quad x \cdot 1 = x \quad \forall x \in \mathbb{R}; \qquad 1 \neq 0$;
(R8) $\forall (x \in \mathbb{R},\ x \neq 0)\ \exists x' \in \mathbb{R} : \quad xx' = 1$;
(R9) $x(y + z) = xy + xz \quad \forall x, y, z \in \mathbb{R}$.

Joukon $\mathbb{R}$ alkioita sanotaan reaaliluvuiksi. Aksioomassa R4 mainittua lukua x' sanotaan luvun x *vastaluvuksi* ja sitä merkitään $-x$. Aksioomassa R8 mainittua lukua x' sanotaan luvun x *käänteisluvuksi* ja merkitään $1/x$ tai x^{-1}.

2. Reaalilukujen järjestys

Oletetaan, että laskutoimitusten lisäksi joukossa $\mathbb{R}$ on määritelty suuruusjärjestys, jolla on seuraavat ominaisuudet (R10)–(R14) (vrt. myös II.8).

(R10) Ehdoista $x < y,\ y < x,\ x = y$ on voimassa täsmälleen yksi;
(R11) $x < y \wedge y < z \Rightarrow x < z$ (*transitiivisuus*);
(R12) $x < y \Rightarrow x + z < y + z\ \forall z \in \mathbb{R}$;
(R13) $0 < x \wedge 0 < y \Rightarrow 0 < xy$.

Viimeisen aksiooman (R14) esittämistä varten tarvitaan differentiaali- ja integraalilaskennasta tuttu pienimmän ylärajan käsite.

MÄÄRITELMÄ. Luku G on joukon S *supremum* eli *pienin yläraja*, jos

(1) $x \leq G\ \ \forall x \in S$,
(2) $x \leq M\ \ \forall x \in S \Rightarrow G \leq M$.

Luku g on joukon S *infimum* eli *suurin alaraja*, jos

(1) $x \geq g\ \forall x \in S$,
(2) $x \geq m\ \forall x \in S \Rightarrow g \geq m$.

Näille käytetään merkintöjä $G = \sup S,\ g = \inf S$.

Jos joukon S suurin alkio eli *maksimi* $\max S$ on olemassa, niin $\max S = \sup S$. Supremum sen sijaan voi olla olemassa, vaikka maksimia ei olisikaan. Aina on voimassa $\max S \in S$, kun taas $\sup S$ voi kuulua joukkoon tai olla kuulumatta. Vastaava pätee pienimmällä alkiolla eli *minimillä* ja infimumilla.

ESIMERKKI 1.A. Jos $S = [0, 1]$, niin $\sup S = \max S = 1,\ \inf S = \min S = 0$.

ESIMERKKI 1.B. Jos $S = (0, 1)$, niin $\sup S = 1,\ \inf S = 0$, mutta $\max S$ ja $\min S$ eivät ole olemassa.

Pienimmän ylärajan käsitteen avulla voidaan nyt formuloida viimeinen tarvittava aksiooma:

(R14) Jokaisella joukolla $S \subset \mathbb{R}$, $S \neq \emptyset$,
jolla on jokin yläraja, on pienin yläraja.

Joukkoa $S \subset \mathbb{R}$ sanotaan *ylhäältä rajoitetuksi*, jos sillä on jokin yläraja, ja *alhaalta rajoitetuksi*, jos sillä on jokin alaraja.

Lause. *Jokaisella alhaalta rajoitetulla epätyhjällä reaalilukujoukolla S on suurin alaraja.*

Todistus. Olkoon m joukon S alaraja. Tarkastellaan joukkoa

$$T = \{y \in \mathbb{R} \mid -y \in S\}.$$

Koska $S \neq \emptyset$, on $T \neq \emptyset$. Ehdosta $x \geq m\ \forall x \in S$ seuraa $-x \leq -m\ \forall x \in S$, toisin sanoen $y \leq -m\ \forall y \in T$.

Joukolla T on siten aksiooman R14 mukaan olemassa supremum $G = \sup T$. Määritelmän mukaan

$$y \leq G\ \ \forall y \in T,$$
$$y \leq M\ \ \forall y \in T \Rightarrow G \leq M,$$

siis

$$x \geq -G \quad \forall x \in S,$$
$$x \geq -M \quad \forall x \in S \Rightarrow -G \geq -M,$$

missä $y = -x$. Täten $\inf S = -G$. $\square$

Em. neljästätoista aksioomasta voidaan johtaa kaikki reaalilukujen ominaisuudet. (Näitä on jo käytettykin edellä olevan lauseen todistamisessa.) Yksinkertaistenkin tulosten todistaminen voi olla pitkän tien takana, kuten seuraava esimerkki osoittaa.

Esimerkki 2. Todistetaan, että $0 < 1$. Todistuksen eri kohdissa käydään läpi mm. seuraavien kaavojen todistukset:

b) $0 \cdot x = 0$, d) $-x = (-1)x$, e) $(-1)(-1) = 1$.

a) Ensin osoitetaan, että alkion x vasta-alkio $-x$ on yksikäsitteinen. Väitetään siis, että jos vasta-alkioita olisi kaksi, nimittäin x' ja x'', nämä olisivat samoja, ts.

$$\left.\begin{aligned} x + x' &= 0 \\ x + x'' &= 0 \end{aligned}\right\} \Rightarrow x' = x''.$$

Tämä nähdään yhtälöketjulla

$$x' = x' + 0 = x' + (x + x'') = (x' + x) + x'' = (x + x') + x'' = 0 + x'' = x'' + 0 = x'',$$

missä yhtäläisyysmerkkien perusteluina ovat aksioomat R3, R4, R2, R1, R4, R1 ja R3.

Itse asiassa vasta tämän yksikäsitteisyystodistuksen jälkeen vasta-alkiolle voidaan ottaa käyttöön merkintä $-x$.

b) Osoitetaan, että kertomalla mikä tahansa reaaliluku nollalla saadaan nolla: Aksioomien R3, R5, R9 ja R5 perusteella on

$$0 \cdot x = (0 + 0) \cdot x = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0 = 0 \cdot x + 0 \cdot x$$

ja edelleen

$$0 = 0 \cdot x + (-0 \cdot x) = [0 \cdot x + 0 \cdot x] + (-0 \cdot x) = 0 \cdot x + [0 \cdot x + (-0 \cdot x)] = 0 \cdot x + 0 = 0 \cdot x,$$

perusteina aksiooma R4, edellä oleva päättely sekä aksioomat R2, R4 ja R3.

c) Aksiooman R4 mukaan alkiolla 1 on vasta-alkio, -1.

d) Osoitetaan, että x:n vasta-alkio $-x$ täyttää ehdon $-x = (-1)x$: Aksioomien ja edellä todistettujen kohtien (R7, R5, R9, c, R5 ja b) perusteella

$$x + (-1)x = x \cdot 1 + (-1)x = x \cdot 1 + x(-1) = x \cdot [1 + (-1)] = x \cdot 0 = 0 \cdot x = 0.$$

e) Edelleen $(-1)(-1) = 1$: Aksioomien R1 ja R4 mukaan on

$$(-1) + 1 = 1 + (-1) = 0,$$

joten alkion -1 vasta-alkio on 1. Toisaalta kohdan d mukaan on $-(-1) = (-1)(-1)$, mistä a-kohdan perusteella seuraa väitös.

f) Lopullinen väitös $0 < 1$: Aksiooman R7 perusteella $0 \neq 1$. Jos olisi $1 < 0$, olisi aksiooman R12 perusteella

$$1 + (-1) < 0 + (-1),$$

mikä aksioomien R4, R1 ja R3 perusteella sievenee muotoon

$$0 < -1.$$

Aksiooman R13 ja kohdan e perusteella on

$$0 < (-1)(-1) = 1.$$

On siis saatu implikaatio $1 < 0 \Rightarrow 0 < 1$, mikä aksiooman R10 perusteella on ristiriita.

Koska ei päde $1 = 0$ eikä $1 < 0$, ainoaksi mahdollisuudeksi jää $0 < 1$ aksiooman R10 mukaan.

Huomaa, etteivät ∞ ja $-\infty$ ole reaalilukuja, ts. ne eivät kuulu joukkoon $\mathbb{R}$. Joskus puhutaan *laajennetusta reaalilukujoukosta* $\bar{\mathbb{R}}$, johon reaalilukujen lisäksi kuuluvat symbolit $\infty = +\infty$ ja $-\infty$. Tämä joukko ei toteuta edellä esitettyjä reaalilukujen aksioomia. Laskutoimitukset laajennetussa reaalilukujoukossa $\bar{\mathbb{R}}$ määritellään luonnollisella tavalla; esimerkiksi

$$x + \infty = \infty$$

kaikilla reaaliluvuilla x. Kaikkien $\bar{\mathbb{R}}$:n alkioiden välillä ei laskutoimituksia kuitenkaan voida määritellä joutumatta ristiriitoihin: $-\infty + \infty$ ei ole määritelty, ts. ∞ ja $-\infty$ eivät ole "vastalukuja". Määriteltyjä eivät ole myöskään $\frac{\infty}{\infty}$ ja $0 \cdot \infty$.

Kaikki differentiaali- ja integraalilaskennan lauseet voidaan todistaa reaalilukujen ominaisuuksien pohjalta, lähtien esitetyistä neljästätoista aksioomasta.

3. Reaalilukujen osajoukot

Aksiooman R7 mukaan reaalilukujoukossa on kertolaskun neutraalialkio, jota merkitään 1; tämä on $\neq 0$. Mitkä tahansa kaksi reaalilukua voidaan laskea yhteen, joten voidaan muodostaa luku $1 + 1$. Aksioomista seuraa, että tämä on eri alkio kuin 0 tai 1, ja sille annetaan nimeksi 2. Vastaavasti muodostetaan $1 + 2 = 3$, $1 + 3 = 4$ jne. Tällä tavalla syntyvää reaalilukujen osajoukkoa

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$$

sanotaan *luonnollisiksi luvuiksi*. Voidaan osoittaa, että se toteuttaa Peanon aksioomat ja on siis malli pykälässä II.2 määritellylle joukolle $\mathbb{N}$.

Luonnollisten lukujen joukolla on seuraavat kolme ominaisuutta.

a) Jokaisessa $\mathbb{N}$:n epätyhjässä osajoukossa on pienin alkio.

b) Olipa n mikä hyvänsä luonnollinen luku, jokaisessa joukon $\{k \in \mathbb{N} \mid k \leq n\}$ epätyhjässä osajoukossa on suurin alkio.

c) Joukossa $\mathbb{N}$ ei ole suurinta alkiota.

Kun luonnollisten lukujen joukkoon liitetään kaikkien sen lukujen vastaluvut, saadaan *kokonaisluvut*:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

Muodostamalla luonnollisten lukujen $\neq 0$ käänteislukujen ja kokonaislukujen tulot saadaan *rationaalilukujen joukko*:

$$\mathbb{Q} = \{\frac{p}{q} \mid \frac{p}{q} = \frac{1}{q}\, p,\ p \in \mathbb{Z},\ q \in \mathbb{N} \setminus \{0\}\}.$$

Joukko $\mathbb{Q}$ ei toteuta aksioomaa R14. Todetaan nimittäin, ettei esimerkiksi joukolla $\{x \in \mathbb{Q} \mid x^2 < 2\}$ ole supremumia joukossa $\mathbb{Q}$. Merkitään

$$\sqrt{2} = \sup\{x \in \mathbb{Q} \mid x^2 < 2\};$$

tämä kuuluu aksiooman R14 mukaan joukkoon $\mathbb{R}$. Jos se kuuluisi myös joukkoon $\mathbb{Q}$, saataisiin yhtälö

$$(p/q)^2 = 2 \qquad (p \in \mathbb{Z},\ q \in \mathbb{N} \setminus \{0\}),$$

joka johtaa helposti ristiriitaan kokonaislukujen yksikäsitteisen alkutekijöihinjaon kanssa.

LIITE 2

Lukujen uusi maailma: p-adiset luvut

Kun kokonaislukujen $0, 1, 2, \ldots$ joukkoa laajennetaan vaiheittain ottamalla mukaan negatiiviset kokonaisluvut, murtoluvut, irrationaaliluvut ja lopulta imaginaariluvut, saadaan rakennetuksi kompleksilukujen joukko $\mathbf{C}$. Tämä on laajin mahdollinen "lukujen maailma", kuten Solmussakin hiljattain [2] kerrottiin: sitä ei voida enää laajentaa, jos sen halutaan säilyttävän totutut yhteen-, vähennys-, kerto- ja jakolaskusäännöt. Joukkoa, jossa nämä säännöt pätevät, sanotaan matematiikan kielellä *kunnaksi*, ja erityisesti $\mathbf{C}$ on *algebrallisesti suljettu kunta*.

Mutta tässä ei ole koko tarina lukualueiden laajentamisesta ja "hyvistä" lukumaailmoista. Lähtemällä liikkeelle rationaalilukujen joukosta ja käyttämällä toisenlaista laajentamistapaa päädytään uudenlaisiin joukkoihin, joiden alkioita voidaan hyvästä syystä myös nimittää luvuiksi. Myös niistä muodostuu nimittäin kunta, jolla on monia samanlaisia ominaisuuksia kuin reaalilukukunnalla $\mathbf{R}$ ja kompleksilukukunnalla $\mathbf{C}$. Lisäksi sillä on useita jännittävällä tavalla erilaisia ominaisuuksia.

Kyseessä ovat *p-adiset luvut*. Tässä p tarkoittaa mitä tahansa alkulukua eli jaotonta lukua, joka on valittu kiinteäksi. Tapauksissa $p = 2$ ja $p = 3$ puhutaan myös *dyadisista* ja *triadisista* luvuista, mikä ehkä saa oudonnäköisen "adinen"-päätteen (englanniksi *adic*) kuulostamaan luontevammalta.

Tällaiset p-adiset luvut eivät ole mikään pelkkä kuriositeetti. Ne ovat päin vastoin osoittautuneet hyvin käyttökelpoisiksi usealla matematiikan alalla, erityisesti lukuteoriassa.

Etäisyyksiä ja itseisarvoja

Ajatellaan ensin reaalilukujoukkoa $\mathbf{R}$. Sen alkioiden kesken voidaan paitsi suorittaa tavallisia laskutoimituksia myös ajatella *etäisyyksiä*: kahden luvun a ja b etäisyys on $|a-b|$. Tämä ns. *euklidinen* etäisyys vastaa arkielämän etäisyyskäsitettä, kun reaalilukuja kuvataan lukusuoran pisteinä.

Etäisyys näyttelee keskeistä osaa monissa matematiikan tarkasteluissa. Siksi on luonnollista kysyä, olisiko euklidisella etäisyydellä vaihtoehtoja ja mitä seurauksia sellaisesta olisi.

Ensiksi on syytä miettiä, mitä ominaisuuksia etäisyydellä pitää olla. Ilmeisesti ainakin kahden eri luvun etäisyyden on oltava positiivinen ja luvun etäisyyden itsestään on oltava 0. Lisäksi etäisyyden täytyy suhtautua lukujen laskutoimituksiin "oikealla" tavalla. Euklidisen etäisyyden tapauksessa nämä etäisyyden ominaisuudet palautuvat seuraaviin itseisarvon ominaisuuksiin: aina kun $a, b \in \mathbf{R}$,

E1. $|a| > 0$, jos $a \neq 0$; $\quad |0| = 0$,
E2. $|ab| = |a| \cdot |b|$,
E3. $|a + b| \leq |a| + |b|$.

Viimeksi mainittu ominaisuus on tärkeä *kolmioepäyhtälö*. Tämän nimityksen voi ymmärtää ajattelemalla hetkeksi a ja b kompleksilukuina ja esittämällä ne kompleksitason pisteinä (tai vektoreina); silloin ehto E3 sanoo, että kolmion sivu on pienempi (tai yhtäsuuri) kuin kahden muun sivun summa.

Kysymystä uudenlaisesta etäisyydestä voidaan nyt pohtia kysymällä, voitaisiinko luvuille ensin määritellä jokin toinen ehdot E1–E3 täyttävä "itseisarvo". Tällaisia mahdollisuuksia kyllä onkin, mutta ne eivät johda mihinkään mielenkiintoiseen etäisyyskäsitteeseen. Tilanne muuttuu paremmaksi, kun hylätään ajatus, että lukualueena on koko $\mathbf{R}$. Sen takia muutetaan lähtötilannetta siten, että otetaan $\mathbf{R}$:n tilalle sen osajoukko $\mathbf{Q}$, pelkät rationaaliluvut. Ajatellaan siis lähtökohtana vain rationaalilukujen välistä euklidista etäisyyttä sekä tätä etäisyyttä luonnehtivia ehtoja E1–E3, missä nyt $a, b \in \mathbf{Q}$.

Osoittautuu, että tässä tapauksessa ehdot E1–E3 pysyvät voimassa, kun tavallinen itseisarvo $|a|$ korvataan *p-adisella itseisarvolla* $|a|_p$. Tämä määritellään seuraavasti. Kiinnitetään alkuluku p ja kirjoitetaan rationaaliluku $a = \frac{t}{u}$ supistettuna murtolukuna, missä siis t ja u ovat kokonaislukuja, joilla ei ole yhteisiä tekijöitä. Tässä on tietysti oletettava, että $a \neq 0$. Katsotaan, onko jompikumpi luvuista t, u jaollinen p:llä, ja kirjoitetaan a muotoon

$$a = p^k \frac{t_1}{u_1},$$

missä t_1 ja u_1 ovat p:llä jaottomia. Eksponenttia k, joka siis on positiivinen, negatiivinen tai 0, sanotaan luvun a *p-eksponentiksi*. Otetaan sille käyttöön merkintä $k = v_p(a)$. Voidaan sanoa, että a on *jaollinen* alkuluvun p potenssilla $p^{v_p(a)}$ (sillä siitähän on kysymys, jos a sattuu itse olemaan kokonaisluku). Nyt asetetaan määritelmä

$$|a|_p = (\tfrac{1}{2})^{v_p(a)} \qquad (a \neq 0) \tag{1}$$

ja lisäksi $|0|_p = 0$. Silloin ehdot E1–E3 ovat voimassa, kun $|.|$:n tilalla on $|.|_p$. Ensimmäinen ehtohan nähdään suoraan määritelmästä ja E2 ja E3 seuraavat (tapauksessa $a \neq 0$, $b \neq 0$) siitä, että

$$v_p(ab) = v_p(a) + v_p(b),$$

$$v_p(a+b) \geq \min(v_p(a),\, v_p(b)). \tag{2}$$

Tässä jälkimmäinen ehto siis lausuu, että summasta $a+b$ voidaan ottaa yhteiseksi tekijäksi vähintään se p:n potenssi, jolla molemmat yhteenlaskettavat ovat jaollisia. Voit myös varmistua näistä kirjoittamalla

$$a = p^{v_p(a)} \frac{t_1}{u_1}, \quad b = p^{v_p(b)} \frac{t_2}{u_2}$$

ja muodostamalla näiden lukujen tulon ja summan.

Summan tapauksessa ehdosta (2) seuraa edelleen, että

$$|a+b|_p \leq \max(|a|_p,\, |b|_p) \leq |a|_p + |b|_p. \tag{3}$$

Täydellisyyden vuoksi ehdot E2 ja E3 on tarkistettava myös tapauksessa, jossa esim. $a = 0$. Silloin näiden ehtojen paikkansapitävyys nähdään välittömästi.

Luvun $\frac{1}{2}$ valinta kaavassa (1) on pitkälti mielivaltainen; mikä tahansa luku r väliltä $0 < r < 1$ kelpaisi. Tämän luvun vaihteleminen merkitsisi vain eräänlaista mittakaavan vaihtelua. Usein tehdään mittakaavan normalisointi valitsemalla $r = \frac{1}{p}$.

Esimerkiksi alkuluvulla $p = 5$ saadaan

$$|\tfrac{75}{88}|_5 = |5^2 \cdot \tfrac{3}{88}|_5 = (\tfrac{1}{2})^2 = \tfrac{1}{4},$$
$$|\tfrac{11}{15}|_5 = |5^{-1} \cdot \tfrac{11}{3}|_5 = (\tfrac{1}{2})^{-1} = 2,$$
$$|1250|_5 = |5^4 \cdot 2|_5 = (\tfrac{1}{2})^4 = \tfrac{1}{16},$$
$$|\tfrac{261}{13}|_5 = (\tfrac{1}{2})^0 = 1.$$

Näin määritelty p-adinen itseisarvo $|.|_p$ antaa rationaalilukujen a ja b *p-adisen etäisyyden* $|a - b|_p$. Sanotaan myös, että $|.|_p$ määrittelee rationaalilukujen joukossa *p-adisen metriikan*. Huomaa, että a ja b ovat "lähekkäin", kun $a - b$ on jaollinen korkealla p:n potenssilla. Tämä on p-adisen metriikan tyypillinen piirre, joka kannattaa muotoilla erityisesti näkyville:

Kahden rationaaliluvun p-adinen etäisyys on sitä pienempi, mitä korkeammalla p:n potenssilla niiden erotus on jaollinen.

Erityisesti siis p:n kasvavien potenssien jonossa $p, p^2, p^3, \ldots$ lukujen etäisyys nollasta pienenee eli tässä metriikassa nämä luvut lähestyvät nollaa.

On myös tärkeä huomata, että (3):n nojalla kolmioepäyhtälölle saadaan nyt vahvempi muoto

$$|a + b|_p \leq \max(|a|_p, |b|_p). \tag{4}$$

Katsomalla tarkemmin sitä, miten (3) edellä pääteltiin oikeaksi, havaitaan lisäksi, että

$$|a + b|_p = \max(|a|_p, |b|_p), \qquad \text{jos } |a|_p \neq |b|_p. \tag{5}$$

Näillä kahdella kaavalla on kauaskantoiset seuraukset p-adisten lukujen maailmassa. Kaavan (4) perusteella p-adista metriikkaa sanotaan myös *epäarkhimediseksi*; siltä nimittäin puuttuu eräs euklidisen metriikan yksinkertainen ominaisuus, jota matemaatikot sanovat "Arkhimedeen ominaisuudeksi".

Käytetään myös nimitystä *ultrametriikka*. Tämä johtuu siitä, että tällä metriikalla on oudontuntuisia ominaisuuksia. Esimerkiksi kun $|a|_p$, $|b|_p$ ja $|a + b|_p$ tulkitaan vastaavasti kuin edellä kolmion sivujen pituuksiksi, niin (5):stä nähdään, että jokainen kolmio p-adisessa metriikassa on tasakylkinen! Kolmiossa nimittäin joko $|a|_p = |b|_p$ tai muussa tapauksessa $|a + b|_p = |a|_p$ tai $|b|_p$.

Uusia lukuja

Tähän mennessä olemme siis löytäneet rationaalilukujen joukossa uuden metriikan mutta toistaiseksi ei ole saatu vielä aikaan yhtään uutta "lukua". Nyt on niiden vuoro.

Jos "tavallisessa" matematiikassa halutaan selvittää annetun murtoluvun suuruus, niin luku kannattaa yleensä muuttaa desimaaliluvuksi: esim. $\frac{109}{8} = 13,625$ eli

$$\frac{109}{8} = 1 \cdot 10^1 + 3 \cdot 10^0 + 6 \cdot 10^{-1} + 2 \cdot 10^{-2} + 5 \cdot 10^{-3}.$$

Tässä desimaalien vaikutus luvun suuruuteen vähenee oikealle mentäessä, koska potenssit 10^{-1}, 10^{-2}, 10^{-3} pienenevät. Näin siis euklidisessa metriikassa.

Vastaavasti p-adisessa metriikassa kannattaa lausua annettu luku p:n *kasvavien* potenssien mukaan, esim. (kun $p = 5$)

$$199 = 4 + 4 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3,$$

sillä potenssit p, p^2, $p^3, \ldots$ lähenevät nollaa p-adisessa metriikassa. (Käytännössä edellisen kehitelmän määrittäminen kannattaa tosin tehdä "takaperin", aloittamalla siitä, että 5^3 on korkein 5:n potenssi, joka ei ylitä lukua 199.)

Edellisten esimerkkien luvut oli valittu siten, että kehitelmät ovat päättyviä. Mutta rationaaliluvun desimaaliesitys voi tietysti myös olla päättymätön (jolloin se on jostain kohdasta alkaen jaksollinen), esim.

$$\frac{249}{110} = 2,2363636\ldots .$$

Samoin rationaaliluvun p-adinen kehitelmä, esim.

$$\frac{29}{40} = 3 \cdot 5^{-1} + 2 \cdot 5^0 + 4 \cdot 5 + 1 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4 + \cdots .$$

Tämä kirjoitelma luonnollisesti tarkoittaa, että oikealla puolella oleva summa on sitä lähempänä (p-adisessa metriikassa) lukua $\frac{29}{40}$, mitä enemmän siihen on otettu mukaan termejä, toisin sanoen mitä kauempaa se on katkaistu. Tarkemmin sanottuna: jos katkaisu on tehty potenssin p^n jälkeen, niin summan etäisyys ko. rationaaliluvusta on $\leq (\frac{1}{2})^{n+1}$. Esimerkiksi

$$\left|\frac{29}{40} - 3 \cdot 5^{-1} - 2 - 4 \cdot 5 - 1 \cdot 5^2\right|_5 = \left|-\frac{375}{8}\right|_5 = \left|-5^3 \cdot \frac{3}{8}\right|_5 = (\tfrac{1}{2})^3 = \tfrac{1}{8}.$$

(Eri asia on, miten kehitelmä saadaan määritetyksi. Siihen palataan tuonnempana.)

Rationaalilukujen joukon $\mathbf{Q}$ laajentaminen perinteiseksi reaalilukujoukoksi $\mathbf{R}$ on matemaattisesti melko monimutkainen prosessi, mutta prosessin tulos on yksinkertaista kuvailla lukusuoran avulla: uudet luvut, irrationaaliluvut, täyttävät rationaalilukujen väliset "aukot", niin että alkujaan erillisistä pisteistä muodostunut rationaalilukujen joukko on täydentynyt yhtenäiseksi suoraksi. Reaalilukuja esittävät *kaikki mahdolliset desimaaliluvut*; irrationaalisia näistä ovat ne, jotka ovat päättymättömiä ja jaksottomia. Avainasemassa tässä laajentamisprosessissa on ilmeisesti euklidinen metriikka.

Analoginen laajentaminen voidaan suorittaa p-adista metriikkaa käyttäen. Tällöin tulosta ei voida havainnollistaa lukusuoraa käyttäen, mutta joka tapauksessa tuloksena on rationaalilukujen joukkoa $\mathbf{Q}$ paljon laajempi joukko, *p-adisten lukujen joukko* $\mathbf{Q}_p$, jonka muodostavat *kaikki mahdolliset p-adiset kehitelmät*. Uusia, ei-rationaalisia lukuja näistä ovat jälleen ne, jotka ovat päättymättömiä ja jaksottomia. Yleisessä muodossa tällainen kehitelmä on muotoa

$$a_{-k}p^{-k} + a_{-k+1}p^{-k+1} + \cdots + a_0p^0 + a_1p^1 + a_2p^2 + \cdots , \tag{6}$$

missä kertoimet siis ovat kokonaislukuja välillä $0 \leq a_i \leq p - 1$ ja summa jatkuu oikealle äärettömiin (joskin rationaaliluvun tapauksessa kertoimet a_i voivat jostain kohdasta alkaen kaikki olla $= 0$). Tässä voi k tietysti olla myös negatiivinen, jolloin kehitelmä alkaa

p:n positiivisella potenssilla. Tavallista desimaalilukuesitystä jäljitellen lukua (6) voidaan merkitä

$$a_{-k}a_{-k+1}\ldots a_0, a_1a_2\ldots$$

ja siinä tapauksessa, että k on negatiivinen, $k = -h$,

$$0,00\ldots 0a_ha_{h+1}\ldots .$$

Kertoimia a_i voidaan sanoa luvun "numeroiksi". Siis esimerkiksi

$$\frac{29}{40} = 32,4141\ldots$$

5-adisesti.

Näin saatuja lukuja voidaan laskea yhteen, vähentää, kertoa ja jakaa aivan samoin kuin tavallisia desimaalilukuja. Tätä valaistaan seuraavassa pykälässä muutamin esimerkein. Tuloksena oleva joukko $\mathbf{Q}_p$ onkin kunta aivan kuten $\mathbf{R}$. Lisäksi se on *täydellinen*, toisin sanoen se täyttää ehdon, joka on analoginen $\mathbf{R}$:n täydellisyysaksiooman kanssa (eräs muoto tästä reaalilukujen aksioomasta on R14 edellisessä Liitteessä 1).

Edellä määritelty p-adinen itseisarvo joukossa $\mathbf{Q}$ laajenee luonnollisella tavalla myös joukkoon $\mathbf{Q}_p$:

$$|a_{-k}a_{-k+1}\ldots a_0, a_1a_2\ldots|_p = (\tfrac{1}{2})^{-k},$$

jos $a_{-k} \neq 0$. Tarkista tämän kaavan paikkansapitävyys edellisen luvun $\frac{29}{40}$ tapauksessa. Itseisarvo $|.|_p$ antaa joukkoon $\mathbf{Q}_p$ p-adisen etäisyyden, jolla on samat ominaisuudet kuin edellä. Erityisesti voimassa ovat ehdot (4) ja (5) eli metriikka on ultrametriikka.

Niiden p-adisten lukujen x joukkoa, jotka täyttävät ehdon $|x - a|_p = r$ (missä a on annettu p-adinen luku ja r jokin $|.|_p$:n arvo), on luonnollista sanoa a-keskiseksi r-säteiseksi ympyräksi. Jos b on tämän ympyrän sisällä, toisin sanoen jos $|b - a|_p < r$, niin ehtoa (5) käyttäen saadaan

$$|x - b|_p = |x - a + a - b|_p = \max(|x - a|_p,\, |a - b|_p) = r$$

aina, kun x on ympyrällä. Tämä merkitsee, että myös b on ympyrän keskipiste. Siis jokainen ympyrän sisällä oleva piste on ympyrän keskipiste!

Samoin kuin reaalilukujen kunnassa $\mathbf{R}$ myös p-adisten lukujen kunnassa $\mathbf{Q}_p$ voidaan ratkaista sellaisia yhtälöitä, joilla ei ole rationaalilukuratkaisuja. Esimerkiksi yhtälöllä $x^2 = 6$ on ratkaisut $x = \pm 1,3042\ldots$ (päättymätön) kunnassa $\mathbf{Q}_5$. Yhtälöllä $x^4 = 1$ on tässä kunnassa maksimimäärä eli neljä ratkaisua. Kunta $\mathbf{Q}_5$ on siis tässä suhteessa parempi kuin kunta $\mathbf{R}$; tämähän on laajennettava kompleksilukukunnaksi $\mathbf{C}$ ennen kuin saadaan yhtälölle $x^4 = 1$ kaikki neljä ratkaisua ± 1, $\pm i$.

Kunta $\mathbf{Q}_p$ voidaan algebran yleisten periaatteiden mukaan laajentaa sellaiseksi kunnaksi, joka on algebrallisesti suljettu. Siinä jokaisella n:nnen asteen yhtälöllä on n ratkaisua. Lisäksi tämä kunta voidaan valita siten, että se on täydellinen yllä mainitussa mielessä. Siinä voidaan kehittää samanlaista funktioiden teoriaa kuin $\mathbf{R}$:ssä ja $\mathbf{C}$:ssä, alkaen derivoinnista ja integroinnista. Hyvän yleiskuvan asiasta saa selailemalla esim. kirjaa [1]. Näin muodostettua kuntaa, josta usein käytetään merkintää $\mathbf{C}_p$, on luonnollista pitää kompleksilukukunnan p-adisena analogiana.

Laskutoimituksia

Palataan takaisin p-adisten lukujen kuntaan $\mathbf{Q}_p$. Yksinkertaiset numerolaskut p-adisilla luvuilla sujuvat aivan vastaavasti kuin tavallisilla desimaaliluvuilla. Seuraavissa esimerkeissä aina $p = 5$.

Yhteenlasku voidaan tehdä kirjoittamalla luvut tavalliseen tapaan alakkain, mutta laskujen suunta on nyt vasemmalta oikealle, koska "muistinumero" siirretään aina korkeamman potenssin kohdalle eli oikealle, siis esimerkiksi

$$\begin{array}{r} {\scriptstyle 1} \\ 1\,,\,2\,1 \\ 2\,,\,4\,2 \\ \hline 3\,,\,1\,4 \end{array} + \qquad \begin{array}{r} {\scriptstyle 1\ 1} \\ 3\,3\,,\,2\,2 \\ 2\,,\,4\,2 \\ \hline 3\,0\,,\,2\,0\,1 \end{array} +$$

Vähennyslaskussa on samoin edettävä vasemmalta oikealle, koska "lainaaminen" tapahtuu korkeamman potenssin kohdalta. Vähennyslaskun voi myös muuttaa yhteenlaskuksi vaihtamalla vähentäjän ensin vastaluvukseen. Luvun vastaluku saadaan korvaamalla ensimmäinen numero $a_{-k}(\neq 0)$ numerolla $p - a_{-k}$ ja jokainen seuraava numero a_i numerolla $p-1-a_i$. Tämä on helppo perustella laskemalla, että näiden lukujen summaksi tulee 0. Esimerkiksi

$$-3,421 = 2,02344\ldots, \qquad -0,01134 = 0,0431044\ldots$$

(kehitelmät ovat päättymättömiä). Tässä vähennyslasku molemmilla tavoilla:

$$\begin{array}{r} 4\,,\,1\,\cancel{1}\,\cancel{3} \\ 3\,,\,4\,2\,1 \\ \hline 1\,,\,2\,3\,1 \end{array} - \qquad \begin{array}{r} {\scriptstyle 1\ 1\ 1} \\ 4\,,\,1\,1\,3 \\ 2\,,\,0\,2\,3\,4\,4\ldots \\ \hline 1\,,\,2\,3\,1\,0\,0\ldots \end{array} +$$

Myös lukujen kertominen alakkain (tämäkin vasemmalta oikealle) on helppoa. Laskuja helpottaa, jos välituloksissa (eli kerrottaessa yksittäisellä numerolla) jätetään numerot redusoimatta välille $0,\ldots,4$, siis kirjoitetaan esimerkiksi tulo $3 \cdot 1,32$ muodossa $3,96$. Redusoitunahan, eli ns. *kanonisessa* muodossa, se olisi $3,421$. Redusointi tehdään sitten näiden lukujen yhteenlaskussa.

Tehtävä. Tarkista, että 5-adinen luku $2,1213$ kerrottuna itsellään antaa tulokseksi luvun -1 viiden numeron tarkkuudella (siis 5-adisessa muodossa $4,4444$). Kyseessä on kompleksilukujen kunnan imaginaariyksikköä $i = \sqrt{-1}$ vastaavan 5-adisen luvun likiarvo eli samalla myös yhtälön $x^4 = 1$ yhden ratkaisun likiarvo (vrt. edellisen pykälän loppuun).

Jos edellisessä pykälässä annettu yhtälön $x^2 = 6$ ratkaisun likiarvo $1,3042$ kunnassa $\mathbf{Q}_5$ on oikea, niin $1,3042$ korotettuna neliöön antaa viiden numeron tarkkuudella luvun 6 (eli 5-adisessa muodossa $1,1$). Tarkista tämä.

Jakolasku (jakokulmassa) on vähän vaativampaa, koska siinä tavallaan ratkaistaan *kongruensseja* modulo p. Jos lasketaan esim. $\frac{4,01}{0,31}$, on aloitettava selvittämällä, montako kertaa 3 (jakajan ensimmäinen nollasta eroava numero) "menee" 4:ään. Vastaus on 3,

koska $3 \cdot 3$ antaa välille $0, \ldots, 4$ redusoituna tulokseksi 4. Tällöin on tosiasiassa ratkaistu kongruenssi $3x \equiv 4 \pmod 5$. Helpointa on luonnollisesti laatia ensin valmiiksi pieni taulukko tuloista $3x$ laskettuna modulo 5, kun $x = 0, \ldots, 4$.

Tehtävä. Suorita edellistä jakolaskua jakokulmassa pitemmälle. Kyseessä on edellisessä pykälässä esiintynyt luku 29/40, jossa osoittaja ja nimittäjä on vain kirjoitettu 5-adiseen muotoon. Sille pitää siis tulla kehitelmä $32,4141\ldots$.

Vähän historiaa – ja muutakin

Kunnia p-adisten lukujen keksimisestä kuuluu matemaatikko *Kurt Henselille* (1861–1941), joka toimi professorina Saksassa Marburgin yliopistossa. Hensel ei päätynyt keksintöönsä yllä esitetyllä ajattelutavalla, vaan otti lähtökohdakseen funktioiden sarjakehitelmät (kompleksialueessa). Ajatuksena oli, että samoin kuin sarjakehitelmä tietyssä kompleksitason pisteessä kuvaa funktion käyttäytymistä tämän pisteen läheisyydessä, eli funktion *lokaalia* (paikallista) käyttäytymistä, myös luvun p-adinen kehitelmä kertoo luvusta lokaalista tietoa "paikassa p". Kuntia $\mathbf{Q}_p$ sanotaankin *lokaaleiksi kunniksi*.

Hensel julkaisi p-adisia lukuja koskevan teoriansa vuoden 1900 paikkeilla, mutta sen merkitystä ei aluksi oikein ymmärretty. Teorian varsinainen läpimurto tapahtui noin 20 vuotta myöhemmin, kun Henselin oppilas Helmut Hasse ratkaisi kuuluisan neliömuotoja koskevan probleeman p-adisia lukuja käyttäen.

Koska p-adisten lukujen varsinaiset sovellukset vaativat melko syvällistä matematiikkaa, näistä luvuista ei yleensä puhuta lukuteorian alkeiden kirjoissa. Joitakin helppolukuisia esityksiä voi löytää esim. Googlen avulla, yksinkertaisesti haulla *p-adic numbers*.

Lukijalle, joka on kiinnostunut matematiikan ja musiikin yhteyksistä ja/tai naisten aseman historiallisesta kehityksestä, vielä pieni lisäys. Kurt Henselin isoäiti oli *Fanny Hensel*, tyttönimeltään Mendelssohn, säveltäjä *Felix Mendelssohnin* sisar. Fanny oli itsekin säveltäjä, mutta tuohon aikaan sellaista pidettiin sopimattomana naiselle. Niinpä Fanny sävelsi pääasiassa pöytälaatikkoon, tai joissakin tapauksissa julkaisi sävellyksensä veljensä nimissä. Mutta nyttemmin hänen sävellyksensä on löydetty ja tunnistettu, ja ne ovat päässeet julkisuuteen. Monet niistä ovat erinomaisia – pankaapa vain merkille, jos satutte kuulemaan niitä esim. radiossa.

Viitteet

[1] Schikhof, W.H.: *Ultrametric Calculus: An Introduction to p-Adic Analysis*. Cambridge University Press, 1982.

[2] Valmari, Antti: *Onko* $\sqrt{-1}$ *olemassa?*, 1. osa, Solmu 1/2008, 18–24; 2. osa, Solmu 2/2008, 13–20.

Tämä kirjoitus on ilmestynyt matematiikkalehti Solmun numerossa 3/2008.

LIITE 3

Algebran soveltamisesta koodausteoriaan

IIRO HONKALA

Lähetetään jokin viesti kanavassa, jossa viestiin saattaa tulla virheitä. Tavoitteena on, että vastaanottaja pystyisi korjaamaan viestiin mahdollisesti tulleet virheet. Viesti on muotoa

$$0010\,1000\,0000\,1110\,\ldots,$$

ts. viesti on binäärimuodossa ja jaettu 4-pituisiin paloihin. Kirjaimet 0 ja 1 tulkitaan joukon $\mathbb{Z}_2$ alkioiksi $\overline{0}$ ja $\overline{1}$. Koodausteoriassa nämä yläviivat on tapana jättää kirjoittamatta. Viesti lähetetään neljän kirjaimen (= bitin) paloissa, ts. joukon $\mathbb{Z}_2^4$ alkio kerrallaan (vrt. $\mathbb{R}^4$).

Olkoon

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

Matriisissa A jokainen nollasta poikkeava sarake esiintyy tarkalleen kerran. Määritellään

$$C = \{Y = (y_1, y_2, \ldots, y_7)^T \in \mathbb{Z}_2^7 \mid AY = 0\}.$$

Joukkoa C kutsutaan 7-pituiseksi Hammingin koodiksi. Määritelmän yhtälöiden

$$\begin{array}{lllll} y_4 = & & y_5 & +y_6 & +y_7 \\ y_2 = & y_3 & & +y_6 & +y_7 \\ y_1 = & y_3 & +y_5 & & +y_7 \end{array}$$

nojalla y_3, y_5, y_6, y_7 voidaan valita vapaasti (kullekin kaksi vaihtoehtoa), minkä jälkeen y_1, y_2, y_4 määräytyvät yksikäsitteisesti. Näin joukossa C on 16 *koodisanaa* $(0,0,0,0,0,0,0)$, $(1,1,0,1,0,0,1), \ldots, (1,1,1,1,1,1,1)$.

Lähettäjä suorittaa *koodauksen*: viestin (y_3, y_5, y_6, y_7) sijasta lähetetäänkin kanavaan vektori $(y_1, y_2, y_3, y_4, y_5, y_6, y_7)$, missä y_1, y_2, y_4 saadaan edellä olevista yhtälöistä. Jos viesti on esimerkiksi $(0,1,1,0)$, lähetetään kanavaan vektori $(1,1,0,0,1,1,0)$. Koska $\mathbb{Z}_2$ on äärellinen kunta, on koodaus itse asiassa lineaarikuvaus $f : \mathbb{Z}_2^4 \mapsto \mathbb{Z}_2^7$, $f((y_3, y_5, y_6, y_7)) = (y_3 + y_5 + y_7, y_3 + y_6 + y_7, y_3, y_5 + y_6 + y_7, y_5, y_6, y_7)$.

Tehdään nyt seuraava oletus:

- kanavassa kuhunkin lähetettyyn 7-pituiseen sanaan tulee enintään yksi virhe.

Tämä on järkevä oletus, jos virheiden syntymisen todennäköisyys on pieni.

Vastaanottaja saa kanavasta vektorin $R = (r_1, \ldots, r_7) \in \mathbb{Z}_2^7$. Oletuksen nojalla

- joko R on koodiin C kuuluva sana ja $AR = 0$
- tai $R = Y + E$, missä $Y \in C$ (ja siis $AY = 0$) ja E on virhevektori, jonka kaikki komponentit yhtä lukuunottamatta ovat nollia. Jos ko. ykkönen on koordinaatissa i, niin
$$AR = A(Y + E) = AY + AE = AE = \text{matriisin } A \text{ } i\text{:s sarake.}$$

Vastaanottajan riittää siis laskea vektori AR: jos $AR = 0$, virhettä ei ole tapahtunut; jos AR on matriisin A i:s sarake, virhe on tapahtunut koordinaatissa i, ja se voidaan korjata!

Jos esimerkiksi lähetetyssä sanassa $(1, 1, 0, 0, 1, 1, 0)$ kolmas koordinaatti vaihtuu kanavassa ykköseksi, saa vastaanottaja kanavasta vektorin $(1, 1, 1, 0, 1, 1, 0)$. Vastaanottaja laskee vektorin $A(1, 1, 1, 0, 1, 1, 0)^T = (0, 1, 1)^T$, joka on matriisin A kolmas sarake, ja tietää että alunperin lähetetty sana saadaan vaihtamalla kolmas koordinaatti nollaksi.

Edellä kuvattu koodi on *yhden virheen korjaava koodi*. Suurempia äärellisiä kuntia käyttämällä voidaan konstruoida useampia virheitä korjaavia koodeja. Jos esimerkiksi F on 16-alkioinen äärellinen kunta ja α sen primitiivinen alkio (ts. multiplikatiivisen ryhmän generoiva alkio), niin voidaan osoittaa, että yhtälöt

$$\sum_{i=0}^{14} a_i \alpha^i = 0$$

$$\sum_{i=0}^{14} a_i \alpha^{3i} = 0$$

toteuttavat vektorit $(a_0, a_1, \ldots, a_{14})$, missä $a_i \in \{0, 1\}$, muodostavat kaksi virhettä korjaavan koodin.

LIITE 4

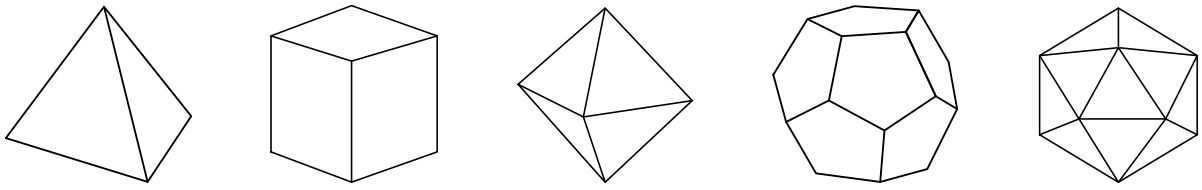
Symmetriaryhmät

Symmetriaa esiintyy merkittävässä määrin sekä taiteessa että luonnossa. Sen perustana on matematiikka, ja olisikin vaikea löytää parempaa tapaa esitellä matemaattisen älyn toimintaa.

Hermann Weyl

Kreikkalaiset ja säännöllisten kappaleiden symmetriaryhmät

Antiikin kreikkalaiset (600-200 eKr) huomasivat, että ainoat säännölliset kappaleet (kaikki tahot yhtenevät ja kaikki kulmat kärjissä samat) ovat tetraedri, kuutio, oktaedri, dodekaedri ja ikosaedri. Eukleides käsitteli näitä yksityiskohtaisesti kirjassaan Elementa, Platon ja Pythagoras kehittelivät säännöllisiin kappaleisiin, materiaan ja kosmokseen liittyviä mystisvivahteisia teorioita. Nykykielellä sanotaan, että $\mathbb{R}^3$:lla on tarkalleen viisi kiertoryhmää. Nämä ovat säännöllisen tetraedrin, kuution, oktaedrin, dodekaedrin ja ikosaedrin symmetriaryhmät.



Tetraedri Kuutio Oktaedri Dodekaedri Ikosaedri

Neliön symmetriaryhmää on käsitelty luvussa IV.6. Tässä on vähän kertausta. Oletetaan, että tasosta irrotetaan neliö, sitä liikutellaan ja se sijoitetaan takaisin alkuperäiselle paikalleen. Tarkoituksena on nyt esittää kaikki mahdolliset tavat, joilla tämä voidaan tehdä. Asia käsitellään kuvausten avulla, kiinnittämällä huomio itse kuvauksen asemesta kuvauksen vaikutukseen. (Esimerkiksi $90°$ kierto ja $450°$ kierto aiheuttavat saman vaikutuksen, vaikka ovatkin eri kuvauksia.)

Kuvitellaan, että neliömme on läpinäkyvä, esimerkiksi lasia, ja että sen kärjet on merkitty neljällä värillä tai numeroilla $1, 2, 3, 4$. Näin voimme seurata kuvausten vaikutusta ja löytää kaikki mahdolliset tavat asettaa neliö paikalleen. Nämä ovat luvussa IV.6 mainitut kierrot ja peilaukset.

Vastaava havainnollinen geometrinen tarkastelu voidaan tehdä tasasivuiselle kolmiolle tai säännölliselle viisikulmiolle sekä yleisesti säännölliselle n-kulmiolle ($n \geq 3$). Kuten

aikaisemmin, vastaavaa ryhmää merkitään D_n ja sanotaan kertalukua $2n$ olevaksi diedriryhmäksi. (Neliön tapauksessa siis $n = 4$ ja ryhmässä on 8 alkiota).

Diedriryhmät esiintyvät usein myös taiteessa ja luonnossa. Tapeteissa, lattioissa, keramiikassa ja rakennuksissa käytetään koristemalleja, joiden symmetriaryhmä on diedriryhmä. Lumihiutaleen symmetriaryhmä on D_6. Goottilaisten katedraalien ruusuikkunoiden symmetriaryhminä esiintyy esim. D_{12}, D_{16}, D_{24}, D_{30}, mutta yleisimmät ovat D_{12} ja D_{24}, koska luku 12 oli erityisen merkittävä keskiajan kristityille. Se oli täydellisyyden, maailmankaikkeuden, apostolien ja Israelin heimojen luku.

Harjoitustehtäviä:

1. Esitä tasasivuisen kolmion kärjet numeroimalla ryhmän D_3 kuvaukset ja kirjoita D_3:n kertotaulu. Onko D_3 Abelin ryhmä?

2. Esitä säännöllisen viisikulmion symmetriat numeroimalla kärjet.

3. Millaisia alkioita on ryhmässä D_n, $n \geq 3$? (Tutki tapaukset n parillinen ja n pariton erikseen). Montako alkiota on ryhmässä D_n?

4. Selitä kuvausten kiintopisteiden avulla, miksi D_n:ssä kierto yhdistettynä kiertoon on kierto.

5. Selitä kuvausten kiintopisteiden avulla, miksi D_n:ssä peilaus yhdistettynä peilaukseen on kierto.

6. Selitä kuvausten kiintopisteiden avulla, miksi D_n:ssä kierron ja peilauksen yhdistetty kuvaus on peilaus.

7. Tee kuvaus $D_n \to \{-1, +1\}$ liittämällä $+1$ kiertoon ja -1 peilaukseen. Saadaanko näin homomorfismi, kun $\{-1, +1\}$ varustetaan lukujen kertolaskulla? Tulkitse kuvaus käyttämällä suunnistuksen säilymistä tai kääntymistä.

8. Etsi suorakulmion symmetriat ja tee kertotaulu tapauksessa, jolloin suorakulmio ei ole neliö.

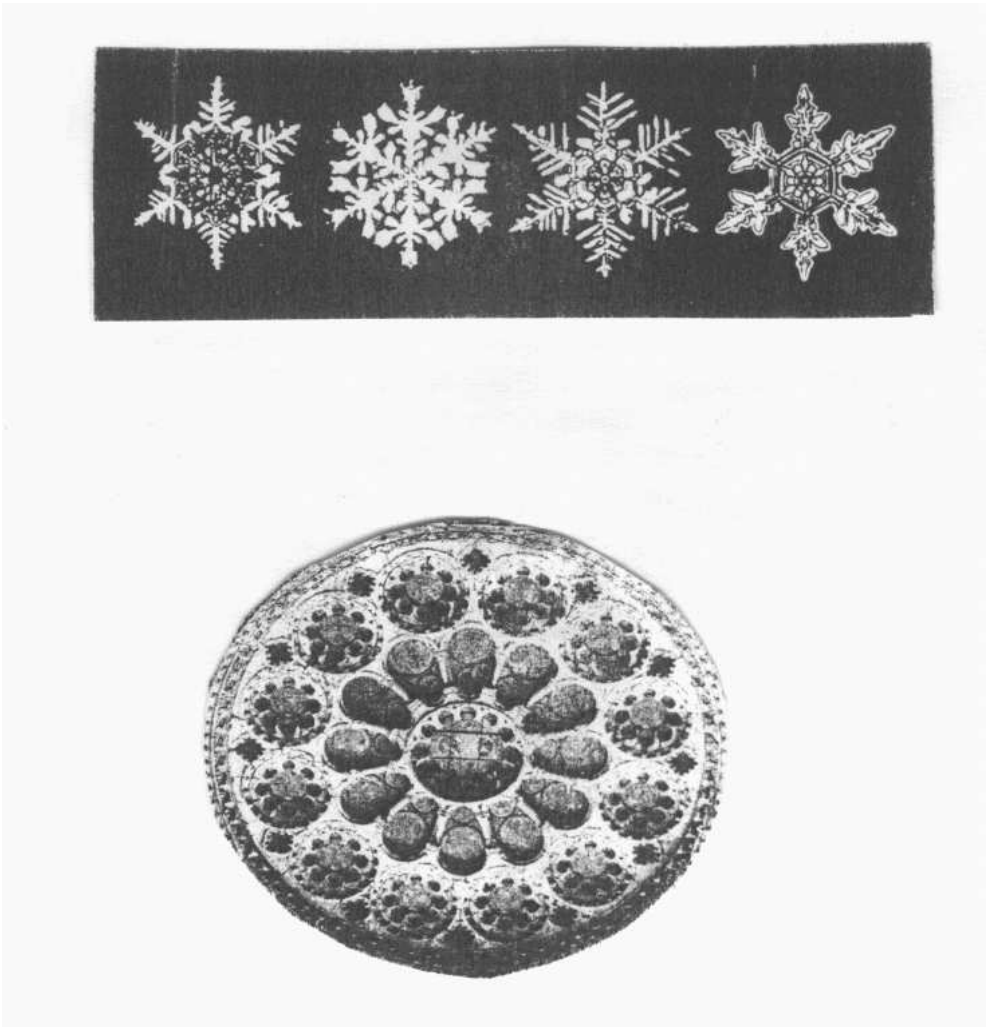
9. Tutki aakkosten yksittäisten kirjainten symmetriaryhmiä.

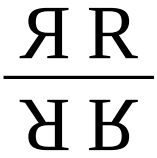
10. Tutki kuvion

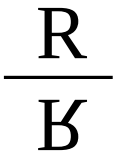
    E E E E

    symmetrioita. Entä jos jonoa jatketaan?

11. Mitkä ovat seuraavien kuvioiden symmetriaryhmät? Etsi kaikki peilausakselit.







LIITE 5

Sanat ja matriisit

JUHANI KARHUMÄKI

Matemaatikko näkee jonon 121 lukuna "satakaksikymmentäyksi". Tietokone puolestaan näkee tämän jonona "yksi–kaksi–yksi". Näin siksi, että tietokone operoi merkkijonoilla myös silloin, kun se suorittaa aritmeettisia laskuja. Ylläsanotusta seuraa, että äärellisen joukon alkioista koostuvat äärelliset jonot, eli *sanat*, ovat keskeisessä asemassa tietojenkäsittelyn matemaattisia perusteita tutkittaessa, esimerkiksi algoritmien teoriassa.

Formalisoidaan tarvittavat käsitteet seuraavasti. Olkoon A äärellinen aakkosto, esimerkiksi $A = \{a, b\}$. Äärellistä jonoa $w = a_1, \ldots, a_n$, missä kukin $a_i \in A$, kutsutaan aakkoston A *sanaksi*. Sen *pituus* $|w|$ on n. Merkitään A^+:lla kaikkien aakkoston A sanojen muodostamaa joukkoa. Määritellään A^+:ssa binäärinen operaatio *tulo*, eli *sanojen yhdistäminen*, ehdosta

$$a_1 \ldots a_n \cdot b_1 \ldots b_m = a_1 \ldots a_n b_1 \ldots b_m.$$

Kyseinen operaatio on *assosiatiivinen*, joten A^+ on *puoliryhmä*. Edelleen se on A:n *vapaasti generoima*, koska kullakin sanalla on yksikäsitteinen esitys aakkoston A alkioiden tulona. Puoliryhmä A^+ voidaan laajentaa *monoidiksi* A^* liittämällä siihen 1–alkio, ts. sana jonka pituus on nolla, siis jono jossa ei ole yhtään alkiota.

Tämän esityksen tarkoituksena on valottaa sanojen ja matriisien välisiä yhteyksiä kolmella yleisluontoisella esimerkillä. Esimerkeistä kaksi ensimmäistä korostaa matriisien hyödyllisyyttä sanoja tutkittaessa, kun taas kolmas esimerkki korostaa käänteistä yhteyttä.

Esim. 1. Olkoon $M_{2\times 2}(\mathbb{N})$ ei–negatiivialkioisten 2×2 kokonaislukumatriisien muodostama joukko. Ajatellaan tätä puoliryhmänä, missä operaationa on matriisien tulo. Olkoon edelleen A^+ aakkoston $A = \{a, b\}$ generoima vapaa puoliryhmä. Osoitamme, että homomorfismi $\varphi : A^+ \to M_{2\times 2}(\mathbb{N})$, joka määritellään ehdoista

$$\varphi(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{ja} \quad \varphi(b) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

on injektiivinen.

Ensinnäkin, koska φ on homomorfismi, on jokaisen sanan kuva yksikäsitteisesti määrätty, esim. $\varphi(aba) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$. Toiseksi huomataan, että $\varphi(a)$ ja $\varphi(b)$ ovat *unitaarisia*, ts. niiden determinantti on 1. Näinollen, koska unitaaristen

matriisien tulo on unitaarinen, on φ itse asiassa kuvaus A^+:lta $M_{2\times 2}(\mathbb{N})$:n unitaarisista matriiseista koostuvaan alipuoliryhmään. Erikoisesti siis matriisilla $\varphi(w)$, missä $w \in A^+$, on aina (unitaarinen) käänteismatriisi.

Osoitetaan nyt φ:n injektiivisyys. Oletetaan, että $\varphi(w) = \varphi(w')$, missä $w, w' \in A^+$ ja $w \neq w'$. Edellä sanotun nojalla voimme olettaa, että $w = av$ ja $w' = bv'$, missä $a, b \in A$ ja $v, v' \in A^+$. Olkoot nyt $\varphi(v) = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ ja $\varphi(v') = \begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix}$. Silloin ehdosta $\varphi(w) = \varphi(w')$ seuraa, että

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix},$$

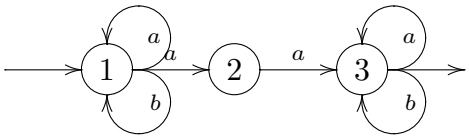
tai ekvivalentisti,

$$\begin{cases} p + r = p' \\ r = p' + r' \end{cases} \quad \text{ja} \quad \begin{cases} q + s = q' \\ s = q' + s' \end{cases}.$$

Täten välttämättä $p = r' = s = q' = 0$ ja $r = p'$ sekä $q = s'$. Kuitenkin matriiseista $\begin{pmatrix} 0 & q \\ r & 0 \end{pmatrix}$ ja $\begin{pmatrix} r & 0 \\ 0 & q \end{pmatrix}$ vain jälkimmäinen voi olla unitaarinen, joten injektiivisyys on todistettu.

Edellä todistettu osoittaa, että sanojen ominaisuuksien tutkiminen voidaan palauttaa kokonaislukumatriisien tutkimiseen. Yllä tarkastelimme vain binäärisanoja, mutta tarkastelut voidaan yleistää mielivaltaisia sanoja koskeviksi.

Esim. 2. Tarkastellaan esimerkin valossa *äärellisten automaattien* ja matriisien välistä yhteyttä. Olkoon $\mathcal{A}$ oheinen leimattu graafi, ts. suunnattu graafi, jonka jokainen nuoli on leimattu aakkoston A symbolilla,



.

Tässä piste (1) on nk. *alkupiste* ja (3) nk. *loppupiste*. Olkoon edelleen $L(\mathcal{A})$ kaikkien niiden sanojen joukko, jotka saadaan $\mathcal{A}$:n alkupisteestä loppupisteeseen johtavien polkujen leimoina. Esimerkiksi sana *abaaabb* on $L(\mathcal{A})$:ssa, mutta sana *abbabab* ei ole.

Määritellään nyt matriisit

$$M_a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{ja} \quad M_b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Jätetään lukijan pohdittavaksi, miten M_a ja M_b määräytyvät $\mathcal{A}$:sta. Edelleen jätetään lukijan todistettavaksi (esim. induktiolla), että lauseke

$$(1, 0, 0) M_w (0, 0, 1)^\top,$$

missä $w \in A^+$ ja, jos $w = aw'$, niin $M_w = M_a \cdot M_{w'}$, ilmoittaa montako erilaista w:llä leimattua polkua johtaa alkupisteestä loppupisteeseen.

Esitetyt tarkastelut voidaan yleistää koskemaan mielivaltaisia leimattuja (suunnattuja) graafeja, ts. *äärellisiä automaatteja*. Matriisit ovat siten erittäin tärkeitä automaattien teoriassa.

Esim. 3. Tämän vuosisadan suuria matemaattisia saavutuksia on *algoritmisen laskettavuuden formalisointi*. Tämä puolestaan on tehnyt mahdolliseksi osoittaa, että tietyt luonnollisella tavalla määritellyt probleemat ovat *algoritmisesti ratkeamattomia*. Tämä tarkoittaa, että niitä *ei voida edes periaatteessa ratkaista tietokoneilla*.

Eräs tunnetuimmista tällaisista probleemoista on nk. *Post'n vastaavuusprobleema*. Probleeman syöttönä on kaksi homomorfismia $h, h' : A^+ \to B^+$, ja tehtävänä on selvittää, onko olemassa sellaista sanaa $w \in A^+$, että $h(w) = h'(w)$. Tämän selvittäminen yleisesti siis on algoritmisesti mahdotonta. Tässä voidaan olettaa, että B (mutta ei A) koostuu vain kahdesta aakkosesta.

Ylläolevaan tulokseen nojautuen osoitamme, että monet yksinkertaiset kysymykset matriisien ominaisuuksista ovat niinikään algoritmisesti ratkeamattomia. Olkoot h ja h' kuten edellä, missä $B = \{1, 2\}$. Liitetään homomorfismiin h matriisit

$$M_a = \begin{pmatrix} 10^{|h(a)|} & 0 \\ h(a) & 1 \end{pmatrix}, \ a \in A, \tag{1}$$

missä $h(a)$ ajatellaan $h(a)$:n esittämänä 10–järjestelmän lukuna. Määrittelemällä

$$M_w = M_a \cdot M_{w'}$$

aina kun $w = aw'$ ja $a \in A$, nähdään helposti induktiolla, että

$$M_w = \begin{pmatrix} 10^{|h(w)|} & 0 \\ h(w) & 1 \end{pmatrix} \quad \text{aina, kun} \quad w \in A^+. \tag{2}$$

Olkoot nyt $\{M_a \mid a \in A\}$ ja $\{M'_a \mid a \in A\}$ homomorfismeihin h ja h' liitetyt matriisijoukot (1). Silloin (2):n nojalla kysymys siitä, onko olemassa sellaista indeksijonoa, eli sanaa, w että

$$(M_w)_{1,2} = (M'_w)_{1,2}$$

on algoritmisesti ratkeamaton.

Vastaavalla metodilla voidaan todistaa monia muita matriisiteoreettisia probleemoja algoritmisesti ratkeamattomiksi. Erikoisen kiintoisa on seuraava variantti: Annettuna äärellinen joukko 3×3 kokonaislukumatriiseja. Selvitettävä, saadaanko näiden jonakin tulona nollamatriisi.

LIITE 6

Algebran historiaa

Sana algebra johtuu arabiankielisestä sanasta *al-jabr*, joka esiintyy 800-luvulla persialaisen matemaatikon Mohammed Al-Khowarizmin (tästä tulee sana algoritmi!) kirjoittamassa kirjassa. Kirjan latinankielisellä käännöksellä oli suuri vaikutus Euroopassa. Se käsitteli tehtäviä, jotka liittyivät polynomiyhtälöiden ratkaisemiseen, ja aiheutti, että algebra-sana liitettiin erityisesti yhtälöihin.

Algebra voidaan jakaa historiansa mukaan kolmeen vaiheeseen: klassinen, moderni ja abstrakti. Klassinen algebra tarkoittaa yhtälöiden teoriaa; siinä käytetään symboleja, jotka tarkoittavat reaali- tai kompleksilukuja. Moderni algebra tarkoittaa myöhempää kehitysvaihetta, jossa symbolien ei enää tarvitse olla lukuja (Cauchy määritteli 1815 *permutaatioiden* kertomisen ja Gauss 1801 kokonaisluvut *modulo p*). Abstrakti algebra käsittelee algebrallisia systeemejä, jotka on määritelty aksioomein (näitä ei ole valittu mielivaltaisesti, vaan pitäen mielessä konkreettisia esimerkkejä); käsiteltäville symboleille ei anneta erityistä merkitystä.

Abstraktisuus ja aksiomatisointi

Kreikkalaisten matemaatikkojen ja filosofien voidaan sanoa ottaneen käyttöön abstraktisuuden ja aksiomatisoinnin ideat 600-300 eKr. Abstrahoinnista on se hyöty, että poistamalla objekteilta epäolennaiset piirteet niistä saadaan matemaattiseen käsittelyyn sopivampia. Näin myös paranee mahdollisuus havaita näennäisesti erilaisissa asioissa samanlaisuutta: yhdellä matematiikan alalla saavutettu tulos voi antaa viitteen samanlaisesta tuloksesta toisella alalla. Lisäksi voidaan käsitellä useita konkreettisia teorioita samanaikaisesti käyttämällä yleistä teoriaa, jonka erikoistapauksia ne ovat. Yksinkertainen esimerkki tämän havainnollistamiseksi on seuraava babylonialaisten esittämä tehtävä: mikä on neliön sivun pituus, jos ala vähennettynä sivun pituudella on 870? Kun tehtävän ratkaisussa korvataan numerot kirjaimilla, saadaan ratkaisumenetelmä, joka soveltuu äärettömän moneen samantyyppiseen tehtävään: yhtälönä on $ax^2 + bx + c = 0$ ja ratkaisu saadaan toisen asteen yhtälön yleisestä ratkaisukaavasta (alkuperäisessä tehtävässä siis $a = 1,\ b = -1,\ c = -870$).

Aksiomaattinen menetelmä hylkää pelkkään intuitioon perustuvan todistamisen ja soveltaa teoreemojen johtamiseen logiikan sääntöihin perustuvaa päättelyä, lähtien alkuoletuksista (aksioomista), jotka hyväksytään lähtökohdiksi. Yleisimmin esitetty esimerkki tämän menetelmän käytöstä on Eukleideen *Elementa* (n. 300 eKr). Aksiomaattisen menetelmän tarpeellisuus tuli esiin jo varhain mm. eräiden ongelmia aiheuttaneiden *paradoksien*

yhteydessä – nehän osoittivat, ettei intuitio olekaan aina luotettava. Tästä huolimatta konkreettisempi intuitiivinen lähestymistapa oli vallalla parintuhannen vuoden ajan Eukleideen jälkeen.

Vuonna 1829 Lobatševski julkaisi *epäeuklidisen geometrian* perusteet. Tässä geometriassa ei yhdensuuntaisaksiooma ole voimassa, seikka jonka olisi pitänyt heti kääntää matemaatikkojen huomio aksioomien tärkeyteen. Moniin vuosiin ei Lobatševskin työhön kuitenkaan kiinnitetty suurta huomiota. Seuraavina vuosikymmeninä alettiin perustaa analyysin tuloksia aritmetiikkaan (jonka perusteita pidettiin luotettavina). Vuonna 1889 Peano määritteli aksiomaattisesti kokonaisluvut käyttäen joukko-opin piiriin kuuluvia käsitteitä, joita hän ei määritellyt. Cantor määritteli joukon käsitteen, mutta määritelmä osoittautui liian laaja-alaiseksi ja johti jälleen kerran matematiikan perusteita koskevaan kriisiin (Russellin paradoksi). Yhtenä tuloksena oli Zermelon yritys (1908) rakentaa aksiomaattinen perusta formaalille joukko-opille.

1800-luvulla algebrassa esiintyi kasvavassa määrin konkreettisia systeemejä, jotka olivat näennäisesti erilaisia mutta muistuttivat syvällisemmin tarkasteltuna toisiaan. Kiinnittämällä huomio systeemin yhteisiin piirteisiin saatiin muotoilluksi vastaava "abstraktin" systeemin käsite ja sitä kautta luokitelluksi ja vertailluksi eri systeemejä. Esimerkiksi *ryhmän* käsitteen käyttö tekee mahdolliseksi useiden eri asioiden (permutaatio-, matriisi-, lukuryhmät) käsittelyn yhtenäisiä sääntöjä soveltaen.

Algebran historiallinen kehitys

Klassinen algebra käsitteli siis polynomiyhtälöitä, erityisesti yrittäen antaa ratkaisukaavoja. Toisen asteen yhtälön ratkaisukaavan tunsivat jo babylonialaiset, joskin he hyväksyivät vain positiiviset ratkaisut. Vasta 1824 Abel todisti, ettei viidennen asteen yhtälöllä ole *yleistä* ratkaisukaavaa, jossa esiintyisi vain yhteen-, vähennys-, kerto- ja jakolaskua sekä juurenottoa. Toisaalta joidenkin yhtälöiden, kuten $x^5 = 1$, juuret saadaan lasketuksi mainitulla tavalla. Vuonna 1832 Galois selvitti, liittämällä kuhunkin yhtälöön tietyn ryhmän, mitkä yhtälöt voidaan ratkaista. Galois esitti myös (olennaisesti) normaalin aliryhmän käsitteen ja tutki äärellisiä kuntia (joissa on p^n alkiota, p alkuluku). 1800-luvun alun vaiheilla Gauss saavutti tuloksia, joilla oli sittemmin huomattava merkitys algebran kehityksessä. Monet tuloksista hän esitti kirjassaan Disquisitiones Arithmeticae. Gaussilta on myös peräisin ensimmäinen tyydyttävä todistus algebran peruslauseelle. Noihin aikoihin *kompleksilukuja* käytettiin intuitiiviseen tapaan, kunnes Hamilton korvasi merkinnän $a + ib$ järjestetyllä reaalilukuparilla (a, b); itse asiassa hän tällöin toisti Gaussin julkaisemattoman työn.

1800-luvun alussa Peacock esitti kaksi algebran käsitettä, aritmeettisen algebran ja symbolisen algebran. Esimerkiksi $a - b$ on aritmeettisessa algebrassa merkityksetön, jos $a < b$, symbolisessa taas aina merkityksellinen, ja laskusäännöt jälkimmäisessä ovat samat kuin aritmeettisessa algebrassa. Peacock oletti, että aina $ab = ba$. Vuonna 1843 Hamilton keksi *kvaternionit*, joihin pätevät kaikki muut aritmetiikan säännöt paitsi $ab = ba$. Samaan aikaan Grassmann yleisti kompleksiluvun käsitteen vielä pitemmälle, mutta koska hänen työnsä oli vaiketajuinen, Hamiltonin kvaternionit saivat enemmän huomiota. Ne eivät

kuitenkaan olleet täsmälleen se, mitä fyysikot tarvitsivat. Näille näytti sopivan paremmin Gibbsin ja Heavisiden kehittämä vektorilaskenta. 1840-luvulla kvaternionit inspiroivat matemaatikkoja kehittämään muitakin systeemejä, joissa kaikki aritmetiikan lait eivät päteneet.

1847 Boole formalisoi logiikkaa ja kehitti *Boolen algebrat*. Näillä on sovelluksia logiikkkaan, todennäköisyyslaskentaan ja tietotekniikan matematiikkaan.

Gauss kehitti 1800-luvulla lukuteoriaa. Hän käytti tutkimuksissaan muotoa $a + ib$ ja $a + gb$ olevia lukuja, missä a, b ovat kokonaislukuja ja g on kompleksinen kolmas ykkösenjuuri. Olennaiseksi probleemaksi osoittautui kysymys näiden lukujen alkutekijäesityksistä. Alkutekijöihin jaon yksikäsitteisyys on ratkaisevan tärkeä esimerkiksi Fermat'n probleeman yhteydessä.

Yhtälön $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = 0$ (missä a_i:t ovat kokonaislukuja) ratkaisuja sanotaan *algebrallisiksi luvuiksi*. Jos lisäksi $a_n = 1$, niitä sanotaan *algebrallisiksi kokonaisluvuiksi*. Esimerkiksi $(-7 + \sqrt{-11})/2$ on sellainen, koska se on yhtälön $x^2 + 7x + 15 = 0$ juuri.

Kunnan käsitteen syntyyn vaikutti havainto, että algebralliset luvut toteuttavat kunnan aksioomat, mutta algebralliset kokonaisluvut eivät; niiden osamäärän ei nimittäin tarvitse olla algebrallinen kokonaisluku. Nykyiseen renkaiden teoriaan puolestaan liittyy *algebrallisten invarianttien* käsite. Algebralliset suureet, jotka säilyvät koordinaattimuunnoksessa, ovat koordinaatteja käyttävässä geometriassa tärkeitä, koska ne liittyvät tutkittavan objektin sisäisiin, koordinaattiesityksestä riippumattomiin geometrisiin ominaisuuksiin. Cayley, joka oli kiinnostunut projektiivisesta geometriasta algebralliselta kannalta katsottuna, alkoi etsiä kahden ja useamman muuttujan n-asteisten homogeenisten muotojen invariantteja (sana invariantti tulee Sylvesteriltä). Invarianttien teorialla on huomattava asema algebrallisessa geometriassa. Algebrallinen geometria tutkii n-ulotteisen avaruuden niitä käyriä ja pintoja, jotka voidaan määritellä algebrallisilla yhtälöillä. Se käyttää algebraa, geometriaa, kompleksianalyysia, topologiaa ja lukuteoriaa. Noin 1930 Emmy Noether ja B.L. van der Waerden rakensivat sille abstraktia algebraa käyttäen vankan perustan. Algebrallinen lukuteoria ja algebrallinen geometria ovat kommutatiivisten renkaiden teorian tärkeitä käyttöalueita.

Vaikka Galois oli esittänyt ryhmän käsitteen, hän oli käyttänyt sitä epäjohdonmukaisesti. Vuonna 1854 Cayley määritteli eksplisiittisesti ryhmän. Vuoteen 1867 asti käsiteltiin vain äärellisiä ryhmiä.

Vuonna 1872 Klein luokitteli geometriat transformaatioryhmien avulla, jotka säilyttivät tiettyjä geometrisia ominaisuuksia. Kun hyväksyttiin äärettömän pienet tason siirrot ja kierrot, syntyi äärettömän, *jatkuvan ryhmän* käsite. Näitä ryhmiä tutki norjalainen Sophus Lie. Lien ryhmät ja Lien algebrat ovat nykyisen teoreettisen fysiikan työkaluja. Vuonna 1882 H. Weber esitti nykyisen ryhmän määritelmän.

1900-luvulla Dyck paneutui ryhmän virittäjiin ja niiden toteuttamiin relaatioihin. Nämä vaikuttivat ratkaisevasti epäkommutatiivisten ryhmien käyttöönottoon topologiassa. Frobenius, Schur ja Burnside kehittivät ryhmien esitysteoriaa, jossa ryhmiä esitetään homomorfismeja käyttäen kompleksialkioisten matriisien avulla.

Hilbertin suorittama euklidisen geometrian täydellinen aksiomatisointi inspiroi 1900-luvulla kuntien ja ryhmien aksiomatisointiyrityksiä. Steinitz kehitti kuntien luokittelun. Kunnat jakautuvat kahteen kategoriaan sen mukaan, onko niiden yksikäsitteinen alkukunta (olennaisesti) rationaalilukujen kunta vai p:n alkion äärellinen kunta. Jokainen kunta voidaan muodostaa alkukunnastaan tietyllä laajentamismenetelmällä.

Vuonna 1914 määriteltiin aksiomaattisesti rengas ja myöhemmin Emmy Noether kehitti renkaiden aksiomatisointia edelleen. Hän oli aikaisemmin tutkinut kvanttimekaniikan differentiaalioperaattoreita ja esittänyt niiden perusominaisuudet abstraktissa muodossa aksioomina, johtaen seurauksia tältä pohjalta. Samaa lähestymistapaa Noether sovelsi algebrassa. Renkaita, joita hän oppilaineen käsitteli, sanotaan nykyään Noetherin renkaiksi.

Tällä vuosisadalla on kehitetty ryhmien esitysteoriaa myös käyttäen matriiseja, joiden alkiot kuuluvat äärelliseen kuntaan (Brauer). Äärettömiä ryhmiä ovat tutkineet mm. venäläiset Golod, Kostrikin, Novikov ja Adjan.

LIITE 7

Algebran käytöstä

Algebran tarjoamien merkintöjen ja käsitteiden avulla voidaan esittää kätevästi tiettyjä konkreettisia ideoita. Matemaatikot käyttävät mieluummin *kokonaislukujen renkaan* käsitettä kuin *kaikkien kokonaislukujen joukkoa*, silloinkin, kun rengasstruktuuria ei tarvita. Algebrallinen terminologia antaa asiasta täydellisemmän ja täsmällisemmän kuvan. Tietenkin voitaisiin babylonialaisten tavoin ratkaista kukin ongelma erikseen, mutta algebran koneisto tarjoaa mahdollisuuden kehittää tehokkaampia menetelmiä.

Ryhmäteoriaa, jossa on osittain kyse symmetrian formuloinnista, käytetään fysiikassa ja kemiassa (kristallografia, spektroskopia, yleinen suhteellisuusteoria, molekyylivärähtelyt, molekyyliorbitaalit, kiinteän aineen fysiikka, alkeishiukkasteoria).

Matriisialgebrat ja polynomialgebrat esiintyvät monissa sovelluksissa. Kvanttimekaniikassa käsitellään polynomialgebroja, joissa on kaksi symbolia, x ja y, jotka täyttävät kommutatiivilain sijasta ehdon $xy = yx + 1$. Rationaali-, reaali- ja kompleksilukujen taustalla on kuntien teoria. Äärelliset kunnat, polynomirenkaat ja potenssisarjojen renkaat tulevat käyttöön mm. kehitettäessä (kustannuksia säästäviä) virheitä etsiviä ja korjaavia koodeja tietoliikenteeseen. Äärellisillä kunnilla on yhteys myös tilastotieteeseen *latinalaisten neliöiden* kautta. Boolen kehittämää algebraa, jolla hän halusi mallintaa logiikkaa matemaattisesti, sovelletaan tietokoneiden sekä puhelimien kytkentäpiirien suunnittelussa.

Lähde: Tässä ja edellisessä liitteessä on käytetty lähteenä R. Allenbyn kirjaa Rings, Fields and Groups (Arnold 1991).

LIITE 8

Henkilökuvia algebran historiasta

Pierre Fermat (1601-1665)

Olen löytänyt paljon äärettömän kauniita teoreemoja (P. Fermat)

Ranskalainen Fermat opiskeli Toulousessa ja valmistui virkamieheksi. Hän eli koko elämänsä rauhallisesti, työteliäästi ja hiljaisesti. Hänen rakkain harrastuksensa oli matematiikka, mutta hän hallitsi myös Euroopan pääkielet ja niiden kirjallisuuden. Hän on differentiaalilaskennan luojia. Hän sovelsi analyyttistä geometriaa kolmiulotteiseen avaruuteen ja kehitti valo-oppia matemaattisesti. Lukuteoriassa hän tutki erityisesti Diofantoksen yhtälöitä. Vuonna 1637 hän kirjoitti kirjan laitaan: "... on mahdotonta jakaa kuutio kahdeksi kuutioksi ... ja yleisesti mikään kahta korkeampi potenssi kahden samankorkuisen

potenssin summaksi. Olen keksinyt tälle todella ihmeellisen todistuksen, mutta se ei mahdu tähän marginaaliin". Yhtälöllä esitettynä väite on, ettei muotoa $x^n + y^n = z^n,\ n > 2$, olevalla yhtälöllä ole positiivisia kokonaislukuratkaisuja $x,\ y,\ z$. Tätä ns. Fermat'n suurta lausetta yrittivät todistaa Euler, Lagrange, Legendre, Gauss sekä lukemattomat muut matemaatikot ja harrastelijat. Saksalaisen Kummerin todistusyritykset johtivat ideaalien teorian syntymiseen. Sitä varhaisemmat yritykset sisälsivät usein virheellisen oletuksen, että alkutekijöihinjako lukurenkaissa on ilman muuta yksikäsitteinen. Fermat'n suuren lauseen todisti vasta Andrew Wiles vuonna 1994.

Niels Henrik Abel (1802-1829)

Abel on jättänyt matemaatikoille jotain, joka työllistää heidät viideksisadaksi vuodeksi (Charles Hermite)

Norjalainen Abel alkoi 16-vuotiaana tutkia Newtonin, Eulerin, Lagrangen ja Gaussin matemaattisia julkaisuja. Isän kuoltua 18-vuotias Abel joutui huolehtimaan perheen toimeentulosta; hän opetti yksityisoppilaita ja jatkoi matematiikan tutkimusta. 19-vuotiaana hän ratkaisi satoja vuosia avoimena olleen ongelman: Päinvastoin kuin enintään neljännen asteen yhtälöllä, ei yhtälöllä $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$ ole yleistä algebrallista

ratkaisukaavaa. Tämän jälkeen hän tutki, miten karakterisoida ne yhtälöt, jotka *voidaan* ratkaista rationaalisilla operaatioilla (yhteen- ja vähennyslasku, kertominen, jakaminen) ja ottamalla juuria. Ongelman ratkaisi Evariste Galois. Ratkaisuun liittyy kommutatiivisen ryhmän käsite, ja vuosia myöhemmin tälle ryhmälle annettiinkin nimi Abelin ryhmä. Abel tutki myös elliptisiä funktioita, elliptisiä integraaleja, Abelin integraaleja ja sarjoja. Abel lähti Berliiniin 1825 ja tutustui siellä August Crelleen, joka oli päättänyt perustaa omalla kustannuksellaan ensimmäisen yksinomaan matemaattiselle tutkimustyölle omistetun aikakauslehden. Crelle huomasi Abelin lahjat ja teki kaiken voitavansa saadakseen Abelille tunnustusta. Abelista tuli uuden aikakauslehden kirjoittajia, ja Crellen ja Abelin seurassa oli usein myös itseoppinut sveitsiläinen geometrikko Steiner. Kun Crellen ystävät näkivät tämän tulevan molempien nerojensa kanssa, he totesivat: "Taas tulee Aatami poikiensa Kainin ja Abelin kanssa." Juuri kun Abelin työ alkoi saavuttaa ansaitsemaansa huomiota, hän sai tuberkuloosin ja kuoli 26-vuotiaana. Kaksi päivää hänen kuolemansa jälkeen saapui kirje, jossa ilmoitettiin hänen nimittämisestään Berliiniin professoriksi. Vuosi kuolemansa jälkeen hän sai Ranskan tiedeakatemian palkinnon ansioistaan matemaatikkona ja myöhemmin hänelle pystytettiin patsas Osloon.

Evariste Galois (1811-1832)

Ranskalainen Galois aloitti matematiikan opiskelun 15-vuotiaana ja opiskeli Legendren ja Lagrangen töitä. Seuraavana vuonna hänet hylättiin l'Ecole Polytechniquen pääsy-

kokeessa, mutta hän tutustui pian Louis-Paul-Emile Richardiin; tämä tunnisti Galois'n nerouden. Richardin rohkaisemana Galois jätti Ranskan tiedeakatemialle julkaistavaksi käsikirjoituksen. Cauchy luki kirjoituksen ja se teki häneen niin suuren vaikutuksen, että hän lupasi esittää sen julkaisemista – mitä hän ei kuitenkaan koskaan tehnyt. 18-vuotiaana Galois pyrki jälleen l'Ecole Polytechniqueen. Hänet hylättiin taas. Ilmeisesti hän ei osannut esittää ajatuksiaan selvästi. Tarinan mukaan Galois raivostui niin, että heitti sienellä kuulustelijaa. 19-vuotiaana Galois osallistui Ranskan tiedeakatemian kilpailuun. Hänen kirjoituksensa annettiin luettavaksi Fourierille, joka kuoli pian sen jälkeen. Galois'n kirjoitus hävisi sille tielle. Galois aloitti vallankumouksellisen poliittisen toiminnan, hänet erotettiin koulusta ja tuomittiin vankilaan. Sinne hän sai tiedon Poissonilta käsikirjoituksensa hylkäämisestä. Tämän jälkeen Galois ei halunnut olla enää missään tekemisissä tiedeakatemian kanssa. Vankilassa hän yritti itsemurhaa ja ennusti kuolevansa kaksintaistelussa, mikä tapahtuikin. Legenda kertoo, että kuolemaansa edeltävänä iltana hän kirjoitti ystävilleen tutkimustensa tuloksia. Hautajaisissa oli läsnä 2000-3000 poliittista aatetoveria. Galois otti käyttöön mm. normaalin aliryhmän, isomorfian ja äärellisen kunnan käsitteet sekä kehitti ns. Galois'n teorian. Galois'n teorian avulla voidaan todistaa esimerkiksi, että on kulmia, joita ei voida jakaa kolmeen osaan harpilla ja viivottimella.

Emmy Noether (1882-1935)

Emmy Noether syntyi Saksassa, missä hänen isänsä Max Noether oli Erlangenin yliopiston matematiikan professori. Emmy Noether opiskeli ja työskenteli Erlangenissa ilman

virkaa, kunnes oli 1915 saanut niin paljon mainetta, että Felix Klein ja David Hilbert kutsuivat hänet Göttingeniin. Vuosina 1915-1923 hän antoi Göttingenissä Hilbertin nimelle merkittyä opetusta, koska naisena hänen ei sallittu käyttää omaa nimeään. Hilbertin oli taisteltava, jotta Noetherin annettiin edes ilmaiseksi opettaa ja työskennellä Göttingenissä. Noether on abstraktin aksiomaattisen algebran kehittäjiä. Hänen tunnetuimmat työnsä liittyvät renkaiden ja ideaalien teoriaan (rengasta, jonka ideaalit täyttävät ns. nousevan ketjun ehdon, sanotaan hänen kunniakseen Noetherin renkaaksi). Noether kehitti myös epäkommutatiivisten algebrojen ja niiden esitysten yhtenäisen teorian. Hermann Weyl, joka tuli Göttingeniin 1930, sanoi Noetherin olleen sikäläisen matematiikan voimakkain keskushahmo, sekä tutkimuksen luovuuden että oppilaspiirin laajuuden takia. Vuonna 1933 Noether joutui juutalaisena luopumaan virastaan ja siirtyi USA:han. 51-vuotiaana tämä loistava matemaatikko sai ensimmäisen kerran viran, josta hänelle maksettiin normaalia palkkaa. Seuraavana vuonna hän kuoli USA:ssa leikkaukseen.

LIITE 9

Matematiikan monet kasvot[1]

KARI ASTALA

Matematiikka on tieteistä abstraktein, usein tieteiden kuningattareksi kutsuttu ja sellaisena helposti viileä ja etäinen. Pyrin tämän vuoksi hahmottamaan alaa sitä tuntemattomalle tai sitä harrastamattomalle; erityisesti tarkoitukseni on pyrkiä luomaan mielikuvia matematiikan luonteenpiirteistä, sen tutkimuksesta ja siitä miltä nämä saattavat näyttää matemaatikon näkökulmasta.

Monesti tuntuu siltä, että nykypäivän matematiikkaa ja aikamme suhtautumista siihen leimaa kaksi vahvaa piirrettä: Ensinnäkin matematiikasta ja matemaattisista menetelmistä on tullut yhä vahvempi osa luonnontieteitä, tekniikkaa ja jopa elinkeinoelämäämme. Jokainen meistä käyttää ja joutuu käyttämään päivittäin tekniikan tuotteita, joissa matematiikkaa on sovellettu olennaisella tavalla. Myös arkielämässämme sekaannumme säännöllisesti matemaattisiin ilmiöihin, vaikkemme niitä sellaisiksi aina huomaisikaan. Toisaalta yhä useammin alan tutkija saa vastaansa kysymyksen, onko matematiikasta nykyään mitään hyötyä. Pelkistäen voimme kysyä kuten vanhassa tarinassa, eikö kaikki numerot ole jo keksitty? Mitä siis voisi olla matematiikan tutkimuskaan?

Kuinka nämä kaksi näin vastakkaista näkemystä voivat elää niin vahvasti ja rinnakkain? Ensimmäinen, jopa triviaali osasyy on tietysti matematiikan oma kieli, alaa tuntemattomalle käsittämättömältä näyttävä symbolien järjestelmä. Mutta miettimättä enempää hyödyn käsitettä tai sen mahdollisia moderneja variaatioita uskoisin kuitenkin, että enemmmänkin syynä on syvällisempi ilmiö, nimittäin matemaattisten sovellusten tyypillinen luonne: ei ole mitenkään poikkeuksellista, että vahvankin matemaattisen idean tai teorian sovellus lasketaan tietokoneen tiliin.

Matemaatikolle tuttuna esimerkkinä mainitsen vaikkapa lääketieteen röntgentomografialaitteen: eri suunnista lähetetyistä röntgensäteistä laite konstruoi tietokoneen avulla poikkileikkauksen halutusta, tutkittavasta kohteesta. Mutta jos yrittää mielessään hahmottaa laitteen toimintaa, huomaa helposti, ettei kuvaa voikaan rakentaa suoraan tai sellaisenaan eri suunnista mitattujen röntgensäteiden vahvuuksia vain numeerisesti laskemalla. Kohteen läpäisseiden säteiden vahvuusarvot täytyykin muuntaa eräällä matemaattisella teorialla, nk. Radonin muunnoksella, muotoon, josta poikkileikkaus on lopulta mahdollista määrätä. Toisin sanoen, laitteen toiminta ylipäätään tulee mahdolliseksi vasta tällaisen matemaatisen muunnoksen avulla.

[1] Virkaanastujaisesitelmä Jyväskylän yliopistossa 18.10.1995

Mielikuviimme matematiikasta eivät voi olla vaikuttamatta myöskään omat kokemuksemme alan opetuksesta: 12 kouluvuotemme matematiikan tunneista vietämme yli puolet aritmeettisten numerolaskujen parissa. Tosiasiassahan ei edes lukuteorialla, sillä matematiikan alalla, joka tutkii lukujen ominaisuuksia, ole paljonkaan tekemistä luvuilla laskemisen kanssa. Siksi paremman mielikuvan matematiikan tutkimuksen luonteesta antaisikin geometria, jolla valitettavasti ei enää ole ansaitsemaansa asemaa kouluopetuksessa. Geometristen mielikuvien tärkeyttä matemaatikolle on mielestäni mahdotonta ylikorostaa. Erityisesti symmetriat ja erilaiset tavat hyödyntää symmetroiden ominaisuuksia leimaavat vahvasti modernia matematiikkaa.

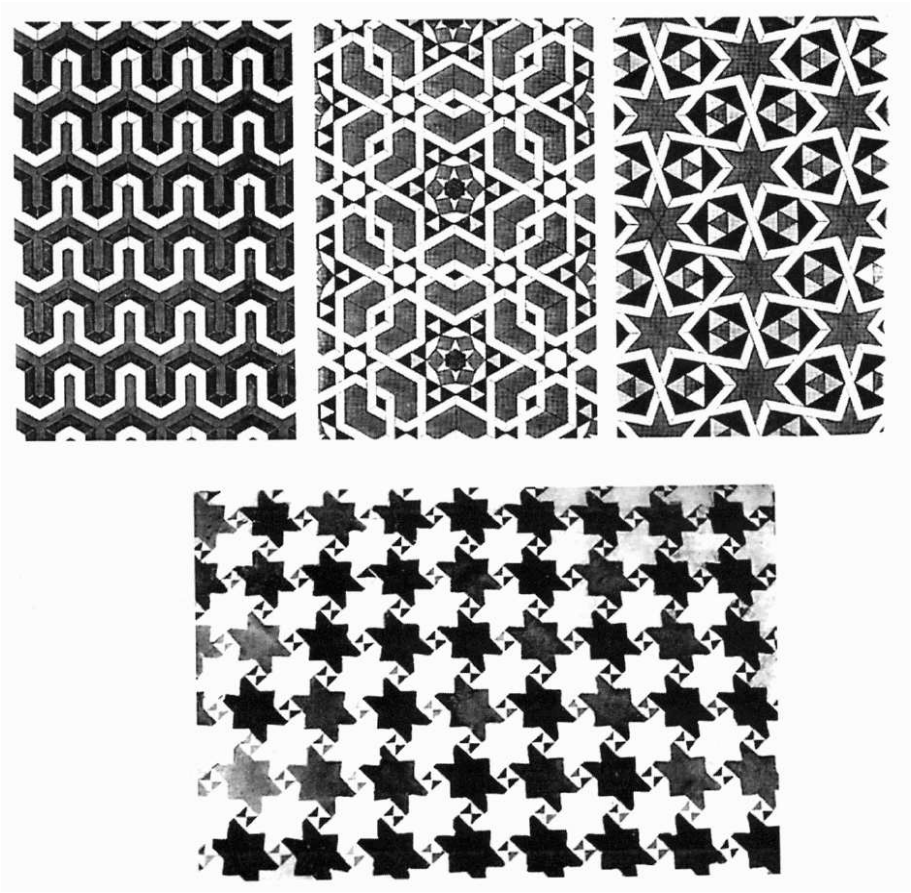
Symmetria ja laatoitukset

Matematiikkaa tuntemattomalle yritän havainnollistaa tätä esimerkillä, symmetrisellä laatoituksella tai kaakeloinnilla, jollaista jokainen meistä on tavalla tai toisella, ehkä useammallakin, joskus soveltanut. Hyviä esimerkkejä kuviosymmetrioista löytyy vaikkapa monista historiallisista rakennuksista. Kuuluisassa Alhambran linnoituksessa Espanjassa, josta kuvat 1.a ovat peräisin, ei voi olla kiinnittämättä huomiota kauniisiin ornamentteihin, joilla palatsin seinät on koristeltu. Ornamenttien monimuotoisuus viehättää ja kiehtoo, mutta niitä tarkastellessa huomaa pian vahvan järjestyksen: vaikka säännöllisesti toistuvaa kuviota voidaan muuttaa ja vaihtaa mielivaltaisen monella erilaisella ja mielikuvituksellisella tavalla, järjestelytapoja, siis tapoja limittää kuviot toisiinsa, näyttää olevan vain muutamia.

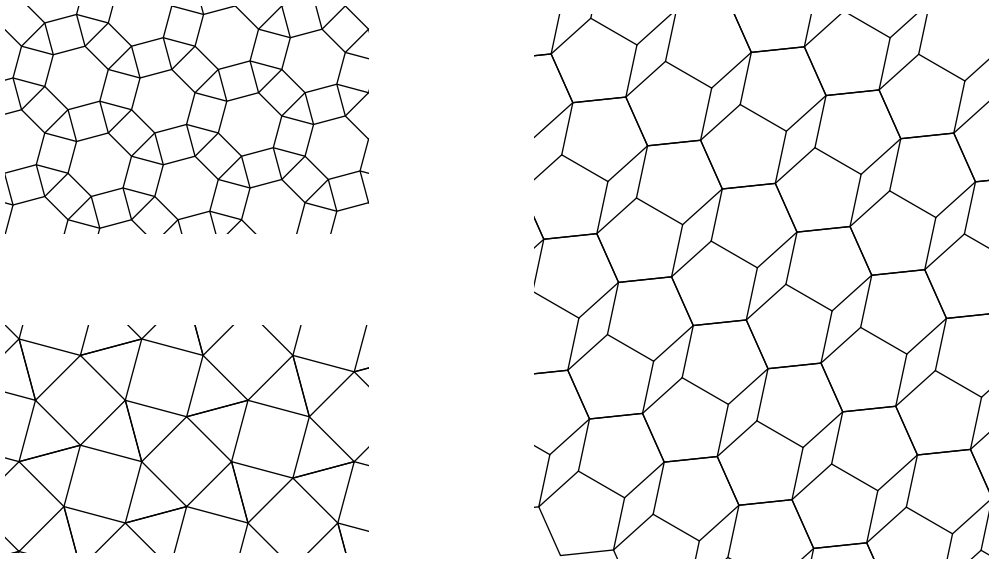
Kuinka monta erilaista symmetriaa tai symmetriaryhmää voi siis löytää laatoitetusta seinästä? Alhambrasta näitä tapoja löytyy kaikkiaan kolmetoista erilaista. Tämä viittaa selvästi siihen, että jo linnoituksen taiteilijat ovat yrittäneet hahmottaa kaikki erilaiset mahdollisuudet rakentaa symmetriakombinaatioita. Nykyään tiedämme, ja moderneilla matemaattisilla käsitteillä tätä ei ole vaikeatakaan osoittaa, että säännöllisiä tapoja tiilien järjestämiseksi on kaikkiaan seitsemäntoista. Itse asiassa puuttuvat neljä symmetriaryhmää ovat löydettävissä muista myöhemmistä islamin ornamenteista.

Matemaattisena käsitteenä laatoitus koostuu tavasta peittää taso yhdellä tai useammalla, kuitenkin äärellisen monella kuviolla, joita siirtämällä, kiertämällä tai peilaamalla saadaan koko ääretön taso täytetyksi, kuitenkin niin että kuviot voivat olla päällekkäin korkeintaan reunapisteissään. Kuvassa 1.b olen esittänyt kolme eri tason laatoitustapaa. Kaikki eri mahdollisuudet tason laatoittamiseksi säännöllisillä monikulmioilla siten, että ne leikkaavat kärkipisteissään aina samalla tavalla, onnistui luokittelemaan jo Johannes Kepler, tähtitieteestään paremmin tunnettu. Tälläisia laatoituksia, joita Kepler nimitti arkimeedisiksi, ovat kuvan 1b laatoituksista kaksi vasemmanpuoleista, mutta ei oikeanpuoleinen (siinä esimerkiksi neliö on vinoneliö, ei siis säännöllinen nelikulmio).

Keplerin jälkeen laatoituksien ominaisuuksien selvittäminen jäi unholaan, kunnes vuosisatamme alussa topologian nousun myötä symmetriaryhmiä alettiin ymmärtää paremmin; tällöin myös luokiteltiin edellä mainitut 17 symmetriaryhmää. Symmetriaryhmistä tärkeimmät ovat ne, joiden avulla tasosta voidaan rakentaa muitakin pintoja. Tässä yhteydessä mielenkiintoinen ja havainnollinen vuorovaikutus matemaattisten ideoitten ja maailmamme hahmotuksen välillä löytyy maailmankuulun taiteilijan, Martin Escherin töistä.



Kuva 1. a



Kuva 1. b

Juuri Alhambran innoittamana Escher pyrki taiteessaan hakemaan eri tapoja, joilla taso voitaisiin jakaa osiin. Alkuun hän käytti euklidisia laatoituksia (vrt. kuvan 2 ylemmät vasemmanpuoleiset kuvat), mutta matemaatikko H.S.M. Coxeter osoitti hänelle muidenkin

mahdollisten maailmojen, toisenlaisten geometrioiden olemassaolon, ja erityisesti hyperbolisen, epäeuklidisen geometrian. Tätä kuvassa 2 esittävät ylemmät oikeanpuoleiset kuviot, keskellä Escherin tulkitsemana.

Matemaatikon kannalta kuvassa 2 ylinnä olevien laatoitusten symmetrioiden avulla voimme rakentaa, ja siis ymmärtää, uusia pintoja: neliön vastakkaiset sivut yhteen liimaamalla voimme rakentaa toruksen, autonrenkaan, vrt kuva 2 alhaalla vasemmalla. Escherin hyödyntämän geometrian ja symmetriaryhmän pinta on taas esitetty kuvassa 2 alhaalla oikealla.

On selvää, että säännöllisyysominaisuuksista luopumalla saadaan numeroimaton joukko erilaisia laatoituksia, eikä kaikkien sellaisten luokitteleminen ole mahdollista. Sen sijaan voimme kysyä, onko kaikilla laatoituksilla yhteisiä ominaisuuksia: esimerkiksi jos olemme riittävän huolellisia, voimmeko aina järjestää kuviomme jaksolliseksi eli tasavälein itseään toistavaksi. Yksinkertaisetkin palat on usein mahdollista järjestää epäjaksollisesti (kuten kuvassa 3.a on tehty tasasivuiselle kolmiolle), mutta nyt kysymme, onko sellaisia paloja, joilla taso voidaan laatoittaa ja joilla kuitenkin jokaisesta laattajärjestelystä tulee aina ja välttämättä epäjaksollinen. Kauneimman ratkaisun ongelmaan antoi brittimatemaatikko Roger Penrose rakentamalla kaksi vinoneliötä, joiden kaikki järjestelyt johtavat välttämättä epäperiodiseen laatoitukseen (kuva 3.b). Myöhemmin kävi ilmi, että itse asiassa tämä Penrosen kuvio saadaankin sopivalla projektiolla viipaleesta, joka on leikattu viisiulotteisen avaruuden säännöllisestä suorakulmaisesta jaosta eli viisiulotteisesta neliölaatoituksen vastineesta(N.G.de Bruijn, 1981; ks. kuva 4).

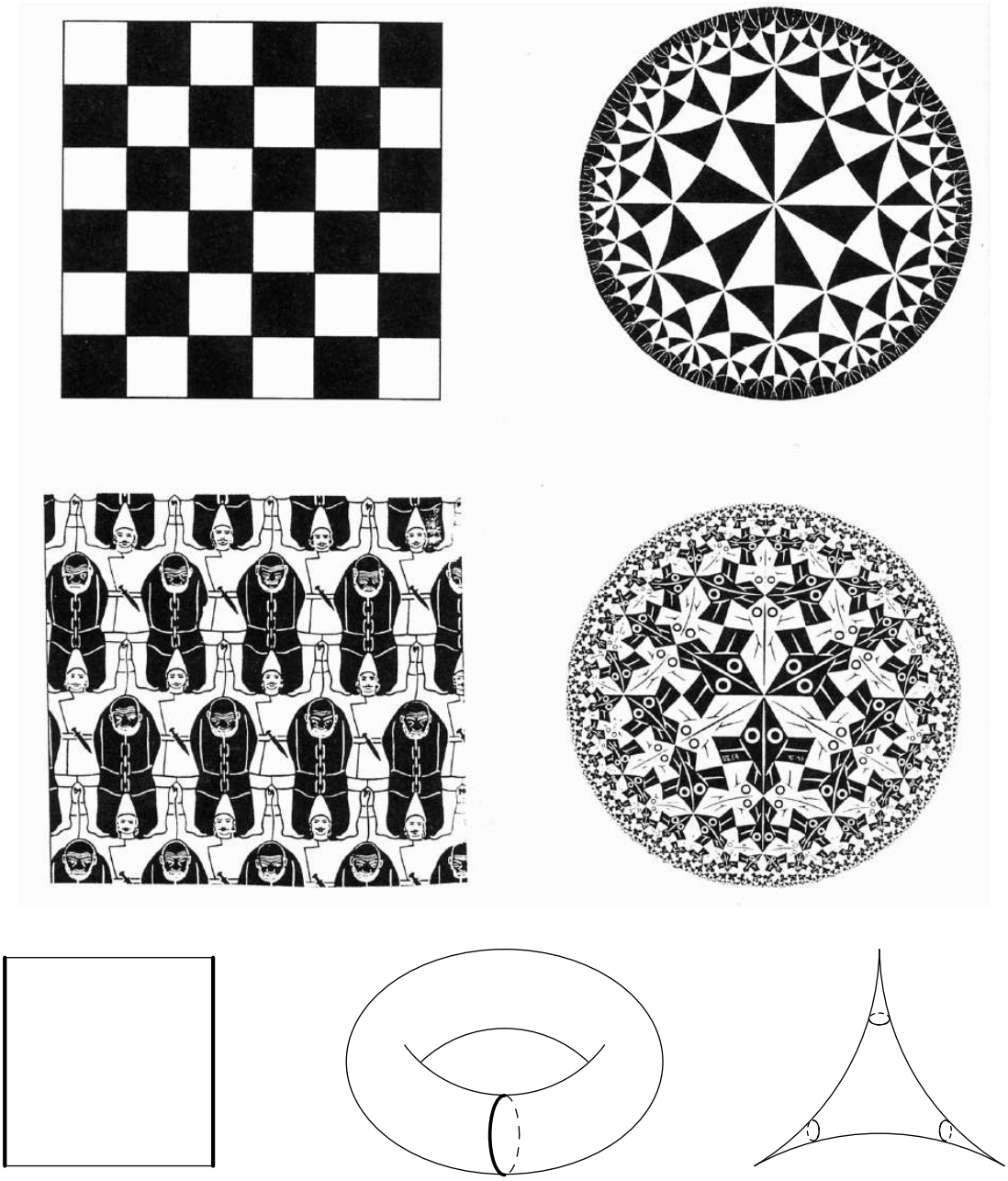
Tässä meillä on matemaattinen selitys parhaimmillaan! Saamme nopean, tehokkaan ja selkeän geometrisen mielikuvan samoin kuin selityksen Penrosen kaakeleiden olemassaololle ja samoin niiden monille ominaisuuksille. Sivujuonena joudumme tosin mieltämään ehkä abstraktilta tuntuvaa viiden ulottuvuuden geometriaa. Matemaattisin peruskäsittein tämä on kuitenkin helposti hallittavissa.

Lopuksi todettakoon, että Penrose rakensi kuvioitaan puhtaasta matemaattisesta mielenkiinnosta ja leikkimielelläkin, mutta viime vuosikymmenellä löydettyjen kvasikristallien, uusien fysikaalisten ilmiöiden ymmärryksessä nämä rakenteet ja niiden kolmiulotteiset vastineet ovat löytäneet keskeisen sijan.

Jaffen syklit

Olen yllä selittänyt varsin pitkään laatoituksen matematiikkaa antaakseni mielikuvan siitä, kuinka matematiikka toimii, mistä sen kysymykset saavat alkunsa, miten se etenee, miten se auttaa meitä hahmottamaan ympäröivää maaailmaamme, ja myös kuinka yllättäviä, ennalta aavistamattomia sovelluksia se tässä löytää.

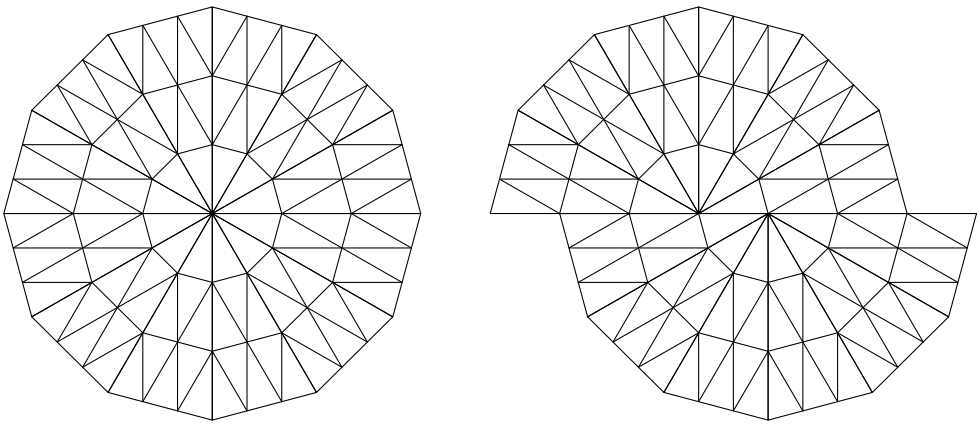
Tämä on tyypillistä paitsi yllä esitetylle suhteellisen konkreettiselle esimerkille matematiikasta, myös koko tieteelle. Esimerkiksi Radon ei aikoinaan kehittänyt teoriaansa



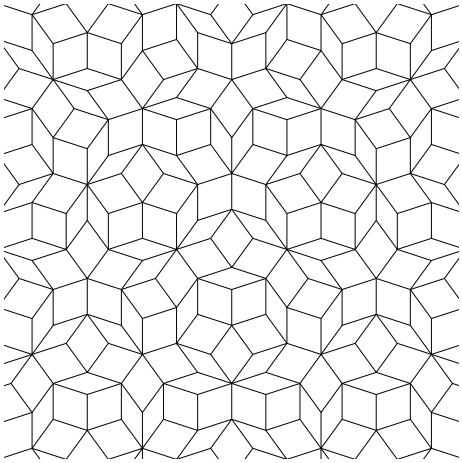
Kuva 2.

röntgenkoneita ja röntgentomografiaa silmällä pitäen, vaan aivan puhtaan matemaattisia ilmiöitä ymmärtääkseen. Perustutkimuksessa ei teorian kehittämisellä tarvitse useinkaan olla välitöntä yhteyttä sille löydettäviin sovelluksiin; erityisen vahvasti tämä ilmenee matematiikan kohdalla. Joskus uusi matemaattinen teoria löytää heti sovelluskohteensa, mutta varsin usein se saa odottaa hyödyntäjäänsä kymmeniä ja joskus jopa satoja vuosia.

Näin on ollut ainakin tähän asti. Onko tilanne muuttunut esimerkiksi uusien tekniikan tuomien mahdollisuuksien vuoksi ja onko ylipäätään odotettavissa abstrakteilta matemaattisilta teorioilta enää uutta annettavaa käytäntöön. Ehkä löydetyt sovellukset



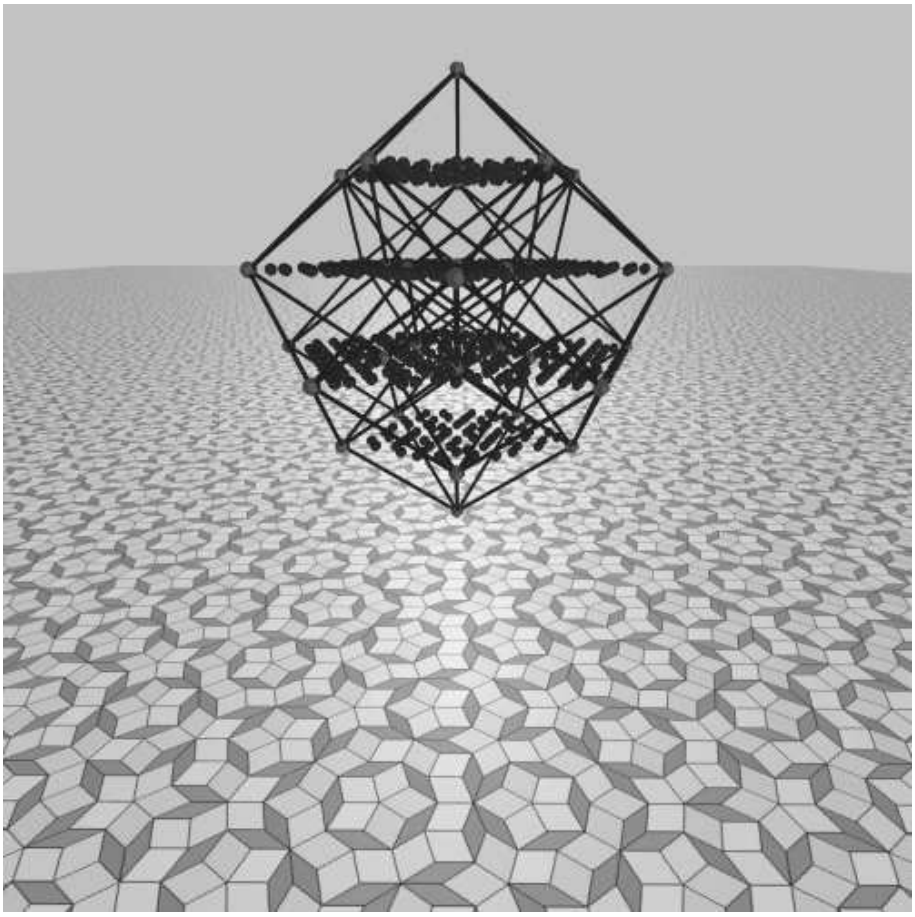
Kuva 3. a



Kuva 3. b

ovatkin olleet onnellista sattumaa? Harvardin yliopiston matematiikan professori Andrew Gleasonin esittämä seuraava kiteytys selittää mainiosti, miksi matemaattiset metodit ovat olleet ja lienevät vastakin tehokkaita niin monessa odottamattomassakin yhteydessä:

”Matematiikka on järjestyksen tiedettä - sen kohteena on löytää, kuvata ja ymmärtää järjestystä päällisin puolin äärimmäisen monimutkaisissakin tilanteissa. Matematiikan tärkeimmät työkalut ovat käsitteitä, jotka mahdollistavat tämän järjestyksen kuvailun. Ja juuri siksi, koska matemaatikot ovat vuosisatoja etsineet tehokkaimpia mahdollisia käsitteitä kuvailla järjestystä eriskummallisissakin tilanteissa, heidän työkalujaan voi hyödyntää ympäröivässä maailmassamme; sillä reaalimaailmahan on malliesimerkki mutkikkaasta tilanteesta, josta löytyy paljon järjestystä.” Toinen harvardilainen, matemaattinen fyysikko Arthur Jaffe on tiivistänyt matemaattisen tutkimuksen ja ulkopuolisen maailman vuorovaikutuksen kahteen periaatteeseen. Ensimmäinen, ns. Jaffen syklin mukaan korkeatasoinen matematiikka, abstraktikin, johtaa aikanaan arkielämän sovelluksiin. Luonnonilmiöiden ymmärtäminen on puolestaan virikkeenä matemaattiselle tutkimukselle. Tätä abstraktion ja sovellusten vuorovaikutusta voi havainnollistaa syklillä, johon voi liittyä kummaltakin puolelta. Esimerkiksi planeettojen liikkeen ymmärtäminen johti differentiaalilaskennan syntyyn ja kompleksiluvut sekä abstraktien Hilbertin avaruuksien teoria taas on kvantti-



Kuva 4. Kuvassa laattojen kärkipisteet ja viisiulotteisen kuution särmät projisoituna kolmeen ulottuvuuteen, lisäksi tasossa Penrosen laatoitus.

mekaniikan, atomaarisen maailman ymmärtämisen perustana.

Toisen Jaffen periaatteen mukaan on mahdotonta ennustaa, missä jokin matemaattinen menetelmä on hyödynnettävissä; jopa teorian luojat voivat yllättyä työnsä käyttömahdollisuuksista. Lineaarialgebra, joka kehitettiin alun perin korkeampiulotteisten avaruuksien geometrian ymmärtämiseen on nyt olennainen osa teollisten prosessien optimointia.

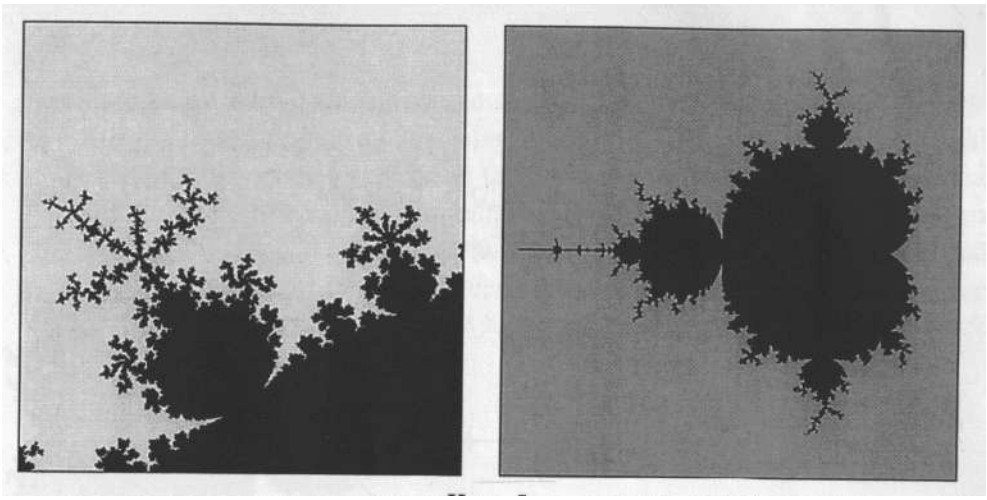
Matemaattisten ilmiöiden ymmärtäminen

Jos ei käytännön sovellus siis olekaan ainoa eikä välttämättä paraskaan neuvo matematiikan tutkimuksen suunnan valitsemiseen, niin mikä ohjaa matemaatikkoa hänen valitessaan tutkimusaiheitaan? Tähän ei tietenkään ole yksikäsitteistä, kaikkia matemaatikkoja kattavaa, yksinkertaista vastausta. Tyypillisesti puhtaan matematiikan tutkimus, jota itsekin edustan, saa tutkimusaiheensa tutkijan halusta ymmärtää kohtaamiansa keskeisiä matemaattista ilmiöitä. Tämä ei kuitenkaan sulje pois ulkomatemaattiseen sovellukseen liittyvää ongelmaa. Erityisesti on huomattava, että tämä ei merkitse, ettei puhtaan matematiikan tutkija olisi kiinnostunut työnsä tai osaamisensa sovelluksista, päinvastoin!

Mutta mitä ovat ne matemaattiset ilmiöt, joita tutkija kohtaa ja joihin tarmonsa kohdistaa. Olen edellä yrittänyt antaa tästä muutamia lyhyitä mielikuvia, esimerkkejä, vaik-

kakin välttämättä vajavaisia. Yleisellä tasolla parhaiten asian ytimeen pääsevät Andrew Gleasonin teesit: kalkyyleja suorittaessaan tai geometrisia ilmiöitä hahmottaessaan tutkijan tavoitteena on järjestyksen, yhteyksien ja sitä kautta ymmärryksen etsiminen. Haluan havainnollistaa tätä esimerkillä, joka on meille kaikille tuttu, ja valitsen sellaiseksi laajalle levinneet fraktaalikuviot.

Mandelbrotin joukon ja muiden fraktaalien kuvat ovat jättäneet tuskin ketään kylmäksi (kuva 5). Kuvioiden alati toistuvat itsensä näköiset mutta kuitenkin kaoottisesti muuttuvat yksityiskohdat ja ornamentit ovat kiehtoneet meitä kaikkia jo kymmenkunta vuotta. sanomattakin on selvää että nämä vetävät tietysti puoleensa myös matemaatikkoa. Mutta näkeekö hän nämä kuvat jotenkin erilailla kuin kadunmies. Kuinka järjestys on löydettävissä tässä väriloistossa ja mielivaltaisilta tuntuvissa kuviorykelmissä?



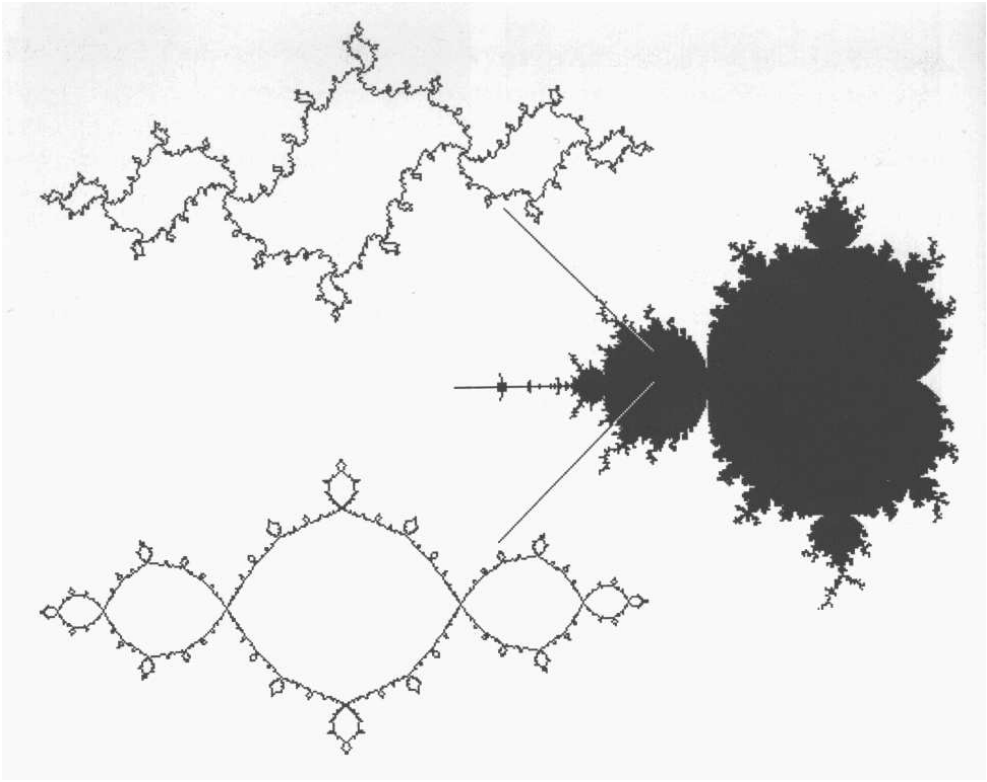
Kuva 5.

Itse asiassa Mandelbrotin joukko on kartta. Kartta, joka kuvaa, kuinka yksinkertaiset dynaamiset järjestelmät toimivat pitkän aikaskaalan muutoksissa. Tätä kautta joukon rakenne on myös hahmotettavissa: jokainen joukon piste c vastaa tilannetta, jossa aikakehitystä kuvataan iteroimalla kompleksilukupolynomia $P(z) = z^2 + c$, siis toistamalla polynomilla operointia.

Järjestelmän muutosta kuvaavan polynomin "pitkien aikaskaalojen" käytöksessä keskeinen on taas ns. täytetty Julia-joukko, joka koostuu niistä pisteistä, jotka eivät karkaa äärettömiin polynomilla operoitaessa. Tämän joukon reunalla, varsinaisella Julia-joukolla, polynomin toiminta on kaoottista.

Käy ilmi, että kussakin Mandelbrotin joukon "pallurassa" tai "kuplassa", eli sen sisäpisteiden komponentissa, kukin vastaava Julia-joukko on rakenteeltaan samanlainen , ja sitä kautta ymmärrettävissä. Esimerkiksi kuvan 6 Julia-joukot voi rekonstruoida kiekosta yhden reunapisteparin ja sen iteroitujen kuvien yhteenliimauksella. Kuvan konfiguraatio on siis helposti selitettavissä, ja lisäksi se esiintyy ainoastaan tässä kyseisessä Mandelbrotin joukon komponentissa. Tätä kautta myös itse Mandelbrotin joukko hahmottuu: kartan

eri pisteet on luonnollisella tavalla lueteltavissa niiden määräämien konfiguraatioiden, liimaustapojen avulla. Näiden ja ns. renormalisaatio-ominaisuuksien avulla Mandelbrotin joukon ja sen kuvioiden toisto-ominaisuuskin on saanut luonnollisen selityksen.



Kuva 6.

Mitä muuta matemaatikko saattaisi miettiä näitä kuvia katsellessaan? Tärkeitä kysymyksiä voisivat olla vaikkapa Julia-joukkojen geometria, niiden reunan dimensio jne. Kuvasta huomaamme myös, että polynomin parametria hieman muutettaessa Julia-joukon rakenne ja osin jopa geometriakin muuttuu hallitusti. Kuinka tämä on selitettävissä? Käy ilmi, että selitys on löydetty yllättävää kautta, niin kutsuttujen kvasikonformikuvausten avulla, jotka nousivat alun perin aivan toisenlaisista matemaattisista kysymyksistä. Näiden kuvauksien teoriaa on huomattavissa määrin kehitetty Suomessa perinteisen kompleksianalyysin koulukunnassa. Mainitsen vielä lopuksi, että dynamiikan avulla on vastaavasti selvitetty kvasikonformikuvausten ominaisuuksia, ja edelleen, että äskettäin näin saatu ymmärrys löysi hyödyntäjänsä huokoisten materiaalien ominaisuuksia tutkivassa homogenisaatioteoriassa. Yhteenvetona voidaan todeta, että Jaffen teesit matemaattisen ymmärryksen kiertokulusta ja yllättävistä sovelluksista toimivat vahvasti myös matematiikan sisällä!

Matematiikka luonnontieteenä

Useimmat matematiikoista kokevat selvittävänsä työssään olemassa olevaisen olemusta monessa mielessä samalla tavalla kuin luonnontieteilijä, joka kokeillaan selvittää luonnonilmiöiden rakennetta. Tämä Platonilta peräisin oleva matematiikan tulkinta tuntuu saavan yhä kasvavaa hyväksyntää. Ehkä matemaatikkojen suhtautuminen tieteensä filosofiaan riippuukin paljolti ajankohtaisista tutkimuskohteista ja -menetelmistä. Abstrakteja rakenteita ylikorostava bourbakismi, joka toi joukko-opinkin kouluihimme, oli aikanaan ilmeisesti sopivaa maaperää formalismille, käsitykselle, että matematiikan lauseet ovat vain tautologioita, loogisia itsestäänselvyyksiä, jotka eivät kerro olemassa olevaisesta mitään. Toisaalta esimerkiksi yllä esitetyn tai yleisempien dynaamisten systemien ominaisuuksia selvittäessään ja niitä tietokoneella testatessaan tai havainnollistaessaan tutkijan on vaikea välttää tuntemusta meistä riippumattomaan luonnonilmiöön törmäämisestä. Päinvastoin, tutkijalle tämä näkökulma tekee omalta osaltaan hyvin ymmärrettäväksi matemaattisten käsitteiden tai teorioiden soveltuvuuden monissa eri tilanteissa, vaikkapa tekniikan tai luonnonilmiöiden ja sitä kautta myös arkimaailman alueella.

Viitteitä

N.G. de Bruijn, Algebraic theory of Penrose's nonperiodic tilings of the plane. I,II.Nederl. Akad.Wetensch. Indag.Math.43 (1981),no.1, 39-52, 53-66.

B.Grünbaum, G.C. Shephard, Tilings and patterns. W.H.Freeman and Company, New York, 1989

Kuva 4: Tekijä E.Durand, Geometry Center, Minnesota, USA

Summary

The many faces of mathematics

This talk, intended to non-mathematicians, describes the nature of modern mathematics and discusses how and why it helps to understand the world around us. Emphasis is on discussions on symmetry, especially symmetric tilings, aspects on applicability of mathematics and how a mathematician chooses his/her research goals.

Tämä kirjoitus on ilmestynyt lehdessä Arkhimedes 4, 1995.

LIITE 10

Suomeksi ilmestynyttä kirjallisuutta:

Guzmán, M. de: *Matemaattisia seikkailuja*, Finn Lectura, 1990 (suom. Marjatta Näätänen). Tied: Marjatta.Naatanen@Helsinki.Fi

Ekeland, I.: *Ennakoimattoman matematiikkaa*, Art House, 1989 (suom. Klaus ja Helka Vala).

Perelman, J., Boltjanski V. ja Höijer, M.: *Elävää matematiikkaa: matemaattisia kertomuksia ja pähkinöitä*, MIR, Moskova, 1981.

Gardner, M.: *Älyniekka, jokamiehen ongelmakirja*, Weilin & Göös, 1965.

Väisälä, K.: *Lukuteorian ja korkeamman algebran alkeet*, Otava, 2. painos 1961.

Nevanlinna, V.: *Matematiikkaa harrastajille*, Gummerus, 1958.

Hogben, L.: *Matematiikkaa kaikille*, WSOY, 4. painos 1955 (suom. Risto Niini).

Nevanlinna, F.: *Johdatus lukuteoriaan ja algebraan*, Otava, 1944.

Singh, S.: *Fermat'n viimeinen teoreema*, Tammi, 1998.

Karttunen, H.: *Matematiikka* (sarjassa Tiedettä kaikille), Ursa 2006.

Matematiikan käsikirja (toim. Jan Thompson), Tammi, 2. painos 1994.

Matematiikan historiaa:

Katsauksia matematiikan historiaan (toim. Juha Oikkonen), Gaudeamus, 1982.

Bell, E. T.: *Matematiikan miehiä*, WSOY, 1963 (suom. Klaus ja Helka Vala).

Boyer, Carl B.: *Tieteiden kuningatar: matematiikan historia, osat* 1 *ja* 2, Arthouse, 1994 (suom. Kimmo Pietiläinen).

Matematiikan historiasta on ilmestynyt ruotsiksi

Sjöberg, B.: Från Euklides till Hilbert, Åbo Akademis förlag, 1995.

Matematiikkaan liittyvää julkaisutoimintaa harjoittavat erityisesti Art House ja Terra Cognita.

Katso myös matematiikkalehti Solmu, `http://solmu.math.helsinki.fi/`

LIITE 11

Ratkaistuja harjoitustehtäviä

Luku I.1

Esimerkkejä jakoyhtälöstä ja jaollisuudesta

1. **Jakoyhtälö** $a = bq + r, \quad 0 \leq r < b$**:**
   Tapauksessa $a = 17$, $b = 5$ saadaan $17 = 5 \cdot 3 + 2$. Luvuilla $a = -23$, $b = 6$ saadaan $-23 = -4 \cdot 6 + 1$.
2. Syt $(4, 15) = 1$, syt $(4, 10) = 2$, syt $(2^2 \cdot 3^2 \cdot 5,\ 2 \cdot 3^3 \cdot 7^2) = 2 \cdot 3^2$. Luvut 4 ja 15 ovat suhteellisesti jaottomia ja $4 \cdot 4 + 15(-1) = 1$. Luvut 4 ja 10 eivät ole suhteellisesti jaottomia ja $(-2)4 + 1 \cdot 10 = 2$.
3. Syt $(2520, 154)$ lasketaan Eukleideen algoritmilla näin:
$$\begin{aligned} 2520 &= 154 \cdot 16 + 56 \\ 154 &= 56 \cdot 2 + 42 \\ 56 &= 42 \cdot 1 + 14 \\ 42 &= 14 \cdot 3. \end{aligned}$$
   Koska 14 on viimeinen nollasta poikkeava jakojäännös, on syt $(2520, 154) = 14$. Edellisistä yhtälöistä saadaan myös syt (a, b) a:n ja b:n lineaariyhdisteenä:
$$\begin{aligned} 56 &= 2520 + 154(-16) \\ 42 &= 154 + 56(-2) \\ 14 &= 56 + 42(-1) = 56 + [154 + 56(-2)](-1) \\ &= 56 \cdot 3 + 154(-1) = [2520 + 154(-16)]3 + 154(-1) \\ &= 2520 \cdot 3 + 154(-49). \end{aligned}$$
4. Pyj $(4, 6) = 12$, pyj $(10, 12) = 60$, pyj $(2^2 \cdot 3^2 \cdot 5,\ 2 \cdot 3^3 \cdot 7^2) = 2^2 \cdot 3^3 \cdot 5 \cdot 7^2$.
5. **Olkoon** p **alkuluku ja** $p > 3$**. Osoita, että** p^2 **on luvun** 12 **monikerran ja ykkösen summa.**
   Todistus. On osoitettava, että $12 \mid (p^2 - 1)$ eli että $12 \mid (p-1)(p+1)$. Koska $12 = 3 \cdot 4$, on siis osoitettava, että $3 \mid (p-1)(p+1)$ ja että $4 \mid (p-1)(p+1)$. Oletuksen mukaan

p on alkuluku, siis pariton, joten $2 \mid (p+1)$ ja $2 \mid (p-1)$ ja siis $4 \mid (p+1)(p-1)$. Koska p on alkuluku, on $3 \nmid p$. Siis $p = 3k+1$ tai $p = 3k'+2$ joillain luvuilla $k, k' \in \mathbb{Z}$. Edellisessä tapauksessa $3 \mid (p-1)$, jälkimmäisessä $p+1 = 3k'+3$, joten $3 \mid (p+1)$. Kummassakin tapauksessa siis $3 \mid (p-1)(p+1)$.

6. **Olkoon n luonnollinen luku ja $2n+1$ kokonaisluvun neliö. Todista, että $n+1$ on kahden kokonaisluvun neliöiden summa.**

   Todistus. Oletuksen mukaan on olemassa $q \in \mathbb{Z}$, jolla $2n+1 = q^2$. Tämä on yhtäpitävä kaavan $2n = (q+1)(q-1)$ kanssa. Luvut $q+1$ ja $q-1$ ovat yhtäaikaa joko parillisia tai parittomia. Edellisen kaavan perusteella $2 \mid (q+1)(q-1)$, joten sekä $q+1$ että $q-1$ ovat parillisia. Olkoon $q+1 = 2h$, missä $h \in \mathbb{Z}$. Sijoittamalla tämä kaavaan $2n = (q+1)(q-1)$ saadaan $2n = 2h(2h-2)$, joten $n = h(2h-2)$ ja $n+1 = 2h^2 - 2h + 1 = h^2 + (h-1)^2$.

Luku I.2

Laskeminen $\bmod n$

1. $7+4 \equiv 2 (\mathrm{mod}\ 3)$, $\quad 7 \cdot 4 \equiv 1 (\mathrm{mod}\ 3)$, sillä
   $7+4 = 11 = 3 \cdot 3 + 2$, $\quad 7 \cdot 4 = 28 = 3 \cdot 9 + 1$.
   Toinen ratkaisutapa, joka on edullinen varsinkin suurilla luvuilla: Koska $7 \equiv 1 (\mathrm{mod}\ 3)$, ja $4 \equiv 1 (\mathrm{mod}\ 3)$, niin $7+4 \equiv 1+1 \equiv 2 (\mathrm{mod}\ 3)$ ja $7 \cdot 4 \equiv 1 \cdot 1 = 1 (\mathrm{mod}\ 3)$.
2. $-10 \equiv 4 (\mathrm{mod}\ 7)$, sillä $-10 - 4 = -14 = 2 \cdot 7$.
3. **Ratkaise kongruenssi $x \equiv 1 (\mathrm{mod}\ 5)$.**

   Luku x on tehtävän ratkaisu jos ja vain jos $x = 1 + 5k$, missä $k \in \mathbb{Z}$. Siis $x \in \{\ldots, -9, -4, 1, 6, 11, \ldots\}$.
4. **Ratkaise kongruenssi $2x \equiv 5 (\mathrm{mod}\ 6)$.**

   Yhtälön $2x = 5 + 6k$ vasen puoli on parillinen ja oikea pariton $\forall k \in \mathbb{Z}$, joten ei ole ratkaisua.

Luku II.6

Ekvivalenssirelaatio

Yhdenmuotoisuus on ekvivalenssirelaatio tason kolmioiden joukossa:

Olkoon S tason kolmioiden joukko. Määritellään $a \sim b$ jos kolmiot a ja b ovat yhdenmuotoiset (eli vastinkulmat ovat yhtäsuuret). Jokainen kolmio on yhdenmuotoinen itsensä kanssa, ts. aina $a \sim a$. Jos a on yhdenmuotoinen b:n kanssa eli $a \sim b$, niin b on yhdenmuotoinen a:n kanssa eli $b \sim a$. Oletetaan, että $a \sim b$ ja $b \sim c$. Silloin a:n

kulmat ovat yhtäsuuret kuin b:n vastinkulmat ja nämä puolestaan yhtäsuuret kuin c:n vastinkulmat. Siis a:lla ja c:llä on yhtäsuuret vastinkulmat, joten $a \sim c$.

Luku III.1

Ryhmä

Positiivisten rationaalilukujen joukko $\mathbb{Q}_+$ on ryhmä kertolaskun suhteen:

Jokainen luku $a \in \mathbb{Q}_+$ voidaan kirjoittaa muotoon $a = \frac{p}{q}$, missä p ja q ovat positiivisia kokonaislukuja.
G0 Jos $a, b \in \mathbb{Q}_+$, on $a = \frac{p_1}{q_1}, \quad b = \frac{p_2}{q_2}$. Silloin $ab = \frac{p_1}{q_1}\,\frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2} \in \mathbb{Q}_+$.

G1 Reaalilukujen kertominen on assosiatiivinen.

G2 $1 \in \mathbb{Q}_+$ ja $1 \cdot a = a = a \cdot 1 \quad \forall a \in \mathbb{Q}_+$.

G3 Jos $a \in \mathbb{Q}_+$ ja $a = \frac{p}{q}$, on $a^{-1} = \frac{q}{p}$, sillä $\frac{q}{p} \in \mathbb{Q}_+$ ja $\frac{p}{q} \cdot \frac{q}{p} = 1 = \frac{q}{p} \cdot \frac{p}{q}$.

Matriisien laskutoimitukset.

Matriisiyhteenlasku joukossa $M_{2\times 2}(\mathbb{R})$ määritellään kaavalla

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}.$$

Matriisikertolasku:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}.$$

Esimerkki ei–kommutatiivisesta ryhmästä

Olkoon $G = \{f_1, \ldots, f_6\}$, missä $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = 1 - x$, $f_4(x) = \frac{x-1}{x}$, $f_5(x) = \frac{x}{x-1}$, $f_6(x) = \frac{1}{1-x}$, $\forall x \in \mathbb{R} \setminus \{0, 1\}$. Laskutoimituksena on funktioiden yhdistäminen. Esimerkiksi $(f_2 \circ f_6)(x) = f_2(f_6(x)) = f_2(\frac{1}{1-x}) = 1 - x = f_3(x)$, joten $f_2 \circ f_6 = f_3$, mutta $(f_6 \circ f_2)(x) = f_6(f_2(x)) = f_6(\frac{1}{x}) = \frac{1}{1-\frac{1}{x}} = \frac{x}{x-1} = f_5(x)$, joten $f_6 \circ f_2 = f_5$. Laskutoimitus ei siis ole kommutatiivinen. Kuvausten yhdistäminen on aina assosiatiivista ja tekemällä laskutoimitukselle "kertotaulu"nähdään, että $f_i \circ f_j$ on aina jokin f_k, siis kuuluu joukkoon G. Kuvaus f_1 on neutraalialkio ja käänteisalkiot ovat $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_6$, $f_5^{-1} = f_5$, $f_6^{-1} = f_4$.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_2	f_1	f_3	f_4

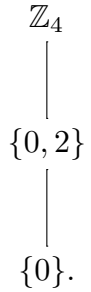
Luku III.2

Aliryhmät

Mitkä ovat $(\mathbb{Z}_4, +)$:n aliryhmät?

Merkitään $\mathbb{Z}_4$:n alkiota $\overline{a}$ lyhyyden vuoksi a:lla ($a = 0, 1, 2, 3$).

Olkoon $H \leq \mathbb{Z}_4$. Silloin $0 \in H$. Joka tapauksessa $\{0\}$ on aliryhmä ($-0 = 0$). Tämä on ainoa yhden alkion käsittävä aliryhmä. Jos $1 \in H$, on $H = \mathbb{Z}_4$, koska $2 = 1 + 1 \in H$ ja $3 = 2+1 \in H$. Olkoon $2 \in H$. Koska $2+2 = 0$, niin $-2 = 2$. $\{0, 2\}$ on siis aliryhmä. $\{0, 3\}$ ei ole aliryhmä, koska $3 + 3 = 2 \notin \{0, 3\}$. Jos $3 \in H$, on $2 = 3 + 3 \in H$ ja $1 = 3 - 2 \in H$, joten $H = \mathbb{Z}_4$. Sisältymiskaaviolla esitettynä $\mathbb{Z}_4$:n aliryhmät ovat



($\mathbb{Z}_4$:n virittäjät, ks. luku III.3, ovat 1 ja 3.)

Luku III.3

Syklinen ryhmä

Näytetään, että ryhmän $(\mathbb{Z}_8, +)$ virittää 3_8 mutta ei 2_8:

Joukko $\langle 3_8 \rangle = \{3_8, 6_8,\ 9_8 = 1_8,\ 4_8, 7_8,\ 10_8 = 2_8,\ 5_8, 0_8\} = \mathbb{Z}_8$. Jälkimmäinen väite $\mathbb{Z}_8 \neq \langle 2_8 \rangle$ todetaan siitä, että $\langle 2_8 \rangle = \{0_8, 2_8, 4_8, 6_8\} \neq \mathbb{Z}_8$.

Luku III.4

Ryhmien homomorfia ja isomorfia

1. **Olkoon $G = (\mathbb{R}, +)$ ja $H = (\mathbb{R}_+, \cdot)$. Määritellään kuvaus $\phi : G \to H$ kaavalla $\phi(x) = 2^x$. Todista, että ϕ on isomorfismi.**

   Todistus: ϕ on injektio: $\phi(x_1) = \phi(x_2) \Rightarrow 2^{x_1} = 2^{x_2} \Rightarrow x_1 \ln 2 = x_2 \ln 2 \Rightarrow x_1 = x_2$.

   ϕ on surjektio: $y \in \mathbb{R}_+$ on pisteen $\frac{\ln y}{\ln 2} \in \mathbb{R}$ kuvapiste, sillä $2^{\ln y / \ln 2} = y$.

   ϕ toteuttaa homomorfiaehdon: $\phi(a + b) = 2^{a+b} = 2^a \cdot 2^b = \phi(a)\phi(b) \quad \forall\ a, b \in \mathbb{R}$. Siis ϕ on isomorfismi.

   (Koska ϕ on homomorfismi, sen injektiivisyys voidaan todeta myös ytimen avulla: $x \in \mathrm{Ker}(\phi) \Rightarrow 2^x = 1 \Rightarrow x = 0$, siis ydin $= \{0\}$.)

Luku III.5

Sivuluokat

1. **Mitkä ovat ryhmän $\mathbb{Z}_9$ aliryhmän $H = \{0, 3, 6\}$ sivuluokat?**

   H:n sivuluokat ovat

$$0 + H = \{0, 3, 6\} (= 3 + H = 6 + H),$$
$$1 + H = \{1, 4, 7\} (= 4 + H = 7 + H),$$
$$2 + H = \{2, 5, 8\} (= 5 + H = 8 + H).$$

2. **Olkoon H ryhmän G aliryhmä. Osoita, että $aH = H$ jos ja vain jos $a \in H$.**

   Todistus. "$\Rightarrow$"Oletetaan, että $aH = H$. Nyt $a = a \cdot 1 \in aH$, koska $1 \in H$. Siis oletuksen nojalla $a \in H$.

   "$\Leftarrow$"Oletetaan, että $a \in H$. Silloin $ah \in H \quad \forall\ h \in H$, koska H on aliryhmänä suljettu laskutoimituksen suhteen. Siis $aH \subset H$. Toisaalta jokainen $h \in H$ voidaan kirjoittaa muotoon $h = 1 \cdot h = (aa^{-1})h = a(a^{-1}h)$. Tässä $a^{-1}h \in H$ koska $a, h \in H$ ja H on aliryhmä. Saadaan siis $h = a(a^{-1}h) \in aH \quad \forall h \in H$. Täten $H \subset aH$.

Luku IV.1

Tekijäryhmä

1. **Konstruoidaan tekijäryhmä $\mathbb{Z}/4\mathbb{Z}$:**

$4\mathbb{Z} = \{0, \pm 4, \pm 8, \dots\}$, lasketaan ensin $4\mathbb{Z}$:n sivuluokat $\mathbb{Z}$:ssa:

$$\begin{aligned} 0 + 4\mathbb{Z} &= 4\mathbb{Z} = \{0, \pm 4, \pm 8, \dots\}, \\ 1 + 4\mathbb{Z} &= \{\dots, -11, -7, -3, 1, 5, 9, \dots\}, \\ 2 + 4\mathbb{Z} &= \{\dots, -10, -6, -2, 2, 6, 10, \dots\}, \\ 3 + 4\mathbb{Z} &= \{\dots, -9, -5, -1, 3, 7, 11, \dots\}. \end{aligned}$$

Väitetään, että muita ei ole. Olkoon $k \in \mathbb{Z}$. Silloin $k = 4q + r$, missä $0 \leq r < 3$. Siis $k + 4\mathbb{Z} = r + 4q + 4\mathbb{Z} = r + 4\mathbb{Z}$. Seuraavaksi tehdään yhteenlaskutaulu käyttämällä kaavaa $(a + 4\mathbb{Z}) + (b + 4\mathbb{Z}) = (a + b) + 4\mathbb{Z}$.

	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

Totea vertaamalla yhteenlaskutauluja, että $\mathbb{Z}/4\mathbb{Z}$ on isomorfinen $\mathbb{Z}_4$:n kanssa. (Itse asiassa kyseessä on sama ryhmä.)

Normaali aliryhmä

Palataan kohdan III.1 esimerkkiin epäkommutatiivisesta ryhmästä. Olkoon aliryhmä $H = \{f_1, f_4, f_6\}$. Laskemalla sivuluokat saadaan, että

$$\begin{aligned} f_k \circ H &= \{f_1, f_4, f_6\} = H \circ f_k, \quad \text{kun } k = 1, 4, 6, \\ f_k \circ H &= \{f_2, f_3, f_5\} = H \circ f_k, \quad \text{kun } k = 2, 3, 5. \end{aligned}$$

Siis H on G:n normaali aliryhmä. (Normaalisuus seuraa myös siitä, että $[G : H] = 2$; ks. IV.1 esimerkki 1.) Sen sijaan aliryhmä $\{f_1, f_2\}$ ei ole normaali, sillä esimerkiksi

$$f_4 \circ f_2 \circ f_4^{-1} = f_4 \circ f_2 \circ f_6 = f_5 \notin \{f_1, f_2\},$$

joten pykälän IV.1 lauseen 1 ehto ei toteudu.

Luku IV.2

Esimerkkejä ryhmien homomorfialauseesta

Tarkastellaan ryhmiä $(\mathbb{Z},+)$ ja $(\{1,-1\},\cdot)$ ja homomorfismia $f:\mathbb{Z}\to\{1,-1\}$, missä

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

$\mathrm{Ker}(f)$ on siis $2\mathbb{Z}$, joten

$$\mathbb{Z}/\mathrm{Ker}(f)=\mathbb{Z}/2\mathbb{Z}=\{2\mathbb{Z},1+2\mathbb{Z}\}.$$

Sivuluokat ovat siis parilliset kokonaisluvut ja parittomat kokonaisluvut. Homomorfialauseen mukaan $(\{2\mathbb{Z},1+2\mathbb{Z}\},+)$ ja $(\{1,-1\},\cdot)$ ovat isomorfisia ryhmiä. Niiden ryhmätaulut ovat merkintöjä vaille samat, kuten pitää:

$+$	$2\mathbb{Z}$	$1+2\mathbb{Z}$
$2\mathbb{Z}$	$2\mathbb{Z}$	$1+2\mathbb{Z}$
$1+2\mathbb{Z}$	$1+2\mathbb{Z}$	$2\mathbb{Z}$

$\cdot$	1	-1
1	1	-1
-1	-1	1

Indusoitu isomorfismi F on

$$F(2\mathbb{Z})=F(0+2\mathbb{Z})=f(0)=1,$$
$$F(1+2\mathbb{Z})=f(1)=-1.$$

Osoitetaan, että ryhmät $(\mathbb{Z},+)$ ja $(\mathbb{Q}\setminus\{0\},\cdot)$ eivät ole isomorfiset:

Olkoon $f:\mathbb{Z}\to\mathbb{Q}\setminus\{0\}$ bijektio, jolla $f(a+b)=f(a)\cdot f(b)\quad\forall\, a,b\in\mathbb{Z}$. Jos $x\in\mathbb{Z}$ toteuttaa ehdon $f(x)=-1$, niin $f(2x)=f(x+x)=f(x)f(x)=(-1)(-1)=1$. Isomorfismeissa neutraalialkiot kuvautuvat toisilleen, joten $2x=0$ eli $x=0$. Silloin $f(0)=1$ ja $f(0)=-1$, siis $1=-1$. Tämä ristiriita osoittaa, etteivät $(\mathbb{Z},+)$ ja $(\mathbb{Q}\setminus\{0\},\cdot)$ ole isomorfiset.

Osoitetaan, että ainoat isomorfismit $(\mathbb{Z},+)\to(\mathbb{Z},+)$ ovat $\mathrm{id}_{\mathbb{Z}}$ ja $-\mathrm{id}_{\mathbb{Z}}$:

Olkoon f isomorfismi $(\mathbb{Z},+)\to(\mathbb{Z},+)$. Osoitetaan ensin, että alkion $f(1)$ virittämä aliryhmä on koko $(\mathbb{Z},+)$. Triviaalisti $\langle f(1)\rangle\subset\mathbb{Z}$. Olkoon $n\in\mathbb{Z}$. Koska f on isomorfismi, on $n=f(m)$ jollain kokonaisluvulla $m\in\mathbb{Z}$, siis $n=f(m)=mf(1)$. Täten $n\in\langle f(1)\rangle$. Saatiin siis tulos $\mathbb{Z}\subset\langle f(1)\rangle$. Yhdessä edellisen kanssa tämä antaa $\mathbb{Z}=\langle f(1)\rangle$, joten $f(1)$ virittää $\mathbb{Z}$:n. Ryhmän $(\mathbb{Z},+)$ ainoat virittäjät ovat 1 ja -1, joten $f(1)=1$ tai $f(1)=-1$. Kuten edellä, on silloin $f(n)=nf(1)\quad\forall\, n\in\mathbb{Z}$, joten $f=\mathrm{id}_{\mathbb{Z}}$ tai $f=-\mathrm{id}_{\mathbb{Z}}$ sen mukaan, onko $f(1)=1$ vai $f(1)=-1$.

Luku IV.3

Sykliset ryhmät

Olkoon G Abelin ryhmä ja $g, h \in G$. Oletetaan, että $\mathrm{ord}(g) = m$ **ja** $\mathrm{ord}(h) = n$ **ovat keskenään jaottomia, ts.** $\mathrm{syt}(m, n) = 1$**. Näytä, että** $\mathrm{ord}(gh) = mn$**.**

Todistus. Olkoon $(gh)^r = 1$. Silloin $g^r h^r = 1$, joten $k = g^r = h^{-r} \in \langle g \rangle \cap \langle h \rangle$. Merkitään $l = \mathrm{ord}(k)$. Silloin III.5:n seurauslause 1 antaa $l \mid m$ ja $l \mid n$, koska $\#\langle g \rangle = m$ ja $\#\langle h \rangle = n$. Oletuksen mukaan $\mathrm{syt}(m, n) = 1$, joten $l = 1$. Siis $k = g^r = h^{-r} = 1$, joten $m \mid r$ ja $n \mid r$. Silloin $mn \mid r$, koska $\mathrm{syt}(m, n) = 1$. Toisaalta $(gh)^{mn} = g^{mn} h^{mn} = (g^m)^n (h^n)^m = 1$. Näistä yhdessä seuraa, että $\mathrm{ord}(gh) = mn$.

Luku V.1

Renkaat

Todistetaan, että Boolen rengas (esimerkki 5) toteuttaa kaikilla $A, B, C \subset S$ **osittelulain** $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$:
$A \cap (B \triangle C) = A \cap [(B \setminus C) \cup (C \setminus B)] = [A \cap (B \setminus C)] \cup [A \cap (C \setminus B)] = [(A \cap B) \setminus (A \cap C)] \cup [(A \cap C) \setminus (A \cap B)] = (A \cap B) \triangle (A \cap C)$.

Tässä nojauduttiin kaavaan $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$, joka todistetaan kaavan $A \setminus B = A \cap B^c$ ja de Morganin kaavojen avulla (ks. tehtävä luvun 0 teht. 20).

Boolen rengas ei ole kokonaisalue (V.6): siinä voi olla $A \cap B = \emptyset$, vaikka $A \neq \emptyset$ ja $B \neq \emptyset$. Renkaan jokaisen alkion $A \neq \emptyset$ kertaluku additiivisessa ryhmässä on $= 2$, koska

$$2A = A \triangle A = (A \setminus A) \cup (A \setminus A) = \emptyset.$$

Luku V.3

Alirengas ja ideaali

1. **Todetaan, että lävistäjämatriisien joukko** $S = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R}\}$ **on** $M_2(\mathbb{R})$**:n alirengas:**

   (a) $1_{M_2(\mathbb{R})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ on lävistäjämatriisi.

   (b) Jos $A, B \in S$, on $A = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix}$, $B = \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix}$ ja $A - B = \begin{pmatrix} a_1 - a_2 & 0 \\ 0 & b_1 - b_2 \end{pmatrix} \in S$.

   (c) $AB = \begin{pmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{pmatrix} \in S$.

Luku V.4

Jäännösluokkarengas

1. $\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$. Lasketaan yhteen ja kerrotaan alkiot $2 + 4\mathbb{Z}$ ja $3 + 4\mathbb{Z}$:

$$(2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4 + 4\mathbb{Z} = 1 + 4\mathbb{Z},$$
$$(2 + 4\mathbb{Z})(3 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4 + 4\mathbb{Z} = 2 + 4\mathbb{Z}.$$

Luku V.5

Renkaiden homomorfia ja isomorfia

Todetaan, ettei kuvaus $f : \mathbb{Z} \to 2\mathbb{Z}$**,** $f(a) = 2a$**, toteuta ehtoa RH2:**

Olkoon $a = 1,\ b = 3$. Silloin $f(1 \cdot 3) = 2(1 \cdot 3) = 6$, mutta $f(1)f(3) = 2 \cdot 6 = 12$. Sensijaan f toteuttaa ehdon RH1: $f(a+b) = 2(a+b) = 2a+2b = f(a)+f(b) \quad \forall\, a, b \in \mathbb{Z}$.

Luku VI.2

Alikunta, alkukunta

Osoitetaan, että rationaalilukujen kunta on alkukunta.

Olkoon $(F, +, \cdot)$ rationaalilukujen kunnan $(\mathbb{Q}, +, \cdot)$ alikunta. Jokainen kunta sisältää ykkösalkion, siis $1 \in F$. Tästä seuraa, että $n \in F \quad \forall\ n \in \mathbb{Z}$ ja $\frac{n}{m} = n \cdot m^{-1} \in F \quad \forall\ n \in \mathbb{Z}, m \in \mathbb{Z} \setminus \{0\}$. Siis $F = \mathbb{Q}$.

Luku VI.5

Maksimaalinen ideaali

Osoita, että kokonaisluvun $n > 1$ virittämä pääideaali $\langle n \rangle$ on maksimaalinen jos ja vain jos n on alkuluku.

Todistus. Ellei n ole alkuluku, on $n = n_1 n_2$, missä $1 < n_1 \leq n_2 < n$. Silloin

$$\langle n \rangle \subsetneq \langle n_1 \rangle \subsetneq \mathbb{Z},$$

joten $\langle n \rangle$ ei ole maksimaalinen. Oletetaan sitten, että n on alkuluku. Ellei $\langle n \rangle$ ole maksimaalinen ideaali, on joko $\langle n \rangle = \mathbb{Z}$ tai on olemassa $m \in \mathbb{Z}$, jolla $\langle n \rangle \subsetneq \langle m \rangle \subsetneq \mathbb{Z}$. Ensimmäinen tapaus on mahdoton, koska $1 \in \mathbb{Z}$ mutta toisaalta $n > 1$. Jos taas $\langle n \rangle \subsetneq \langle m \rangle$, on $n = km$ jollain kokonaisluvulla $k > 1$. Tämä on ristiriidassa sen oletuksen kanssa, että n on alkuluku.

Luku VI.7

Polynomien jaollisuus

Osoitetaan, että $x^2 - 2$ on jaoton renkaassa $\mathbb{Q}[x]$:

Koska $\mathbb{Q}$ on kokonaisalue, on $\mathbb{Q}[x]$ kokonaisalue ja $\deg f(x)g(x) = \deg f(x) + \deg g(x)$ $\forall\ f(x), g(x) \in \mathbb{Q}[x]$. Ainoat mahdolliset tekijät ovat siis ensimmäistä astetta: $x^2 - 2 = (ax + b)(cx + d) = (ac)x^2 + (ad + bc)x + bd$, missä $a, b, c, d \in \mathbb{Q}$. Tällöin $ac = 1$, $ad + bc = 0$, $bd = -2$, joten $c = \frac{1}{a}$, $d = -\frac{2}{b}$ ja sijoittamalla kaavaan $ad + bc = 0$ saadaan $0 = (-2a^2 + b^2)/ab$. Silloin $-2a^2 + b^2 = 0$ eli $(b/a)^2 = 2$, mutta tämä on mahdotonta, koska $\pm\sqrt{2} \notin \mathbb{Q}$.

Toinen ratkaisu: Oletetaan, että polynomilla $x^2 - 2$ on epätriviaali tekijä $\mathbb{Q}$:ssa. Koska polynomi on astetta 2, sillä on silloin myös nollakohta $x_0 \in \mathbb{Q}$. Tällöin $x_0^2 = 2$. Tämä on mahdotonta, koska $\pm\sqrt{2} \notin \mathbb{Q}$.

Polynomi $x^2 - 2$ ei ole sen sijaan jaoton renkaassa $\mathbb{R}[x]$: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Luku VI.8

Miten jaottomat polynomit tuottavat kuntia

Olkoon $\mathbb{R}[x]$ reaalikertoimisten polynomien joukko ja $\langle x^2+1\rangle$ pääideaali, jonka virittää x^2+1. Silloin

$$\langle x^2+1\rangle = \{f(x)(x^2+1) \mid f(x) \in \mathbb{R}[x]\}$$

(lause V.7). Väitetään, että rengas

$$\mathbb{R}[x]/\langle x^2+1\rangle = \{g(x)+\langle x^2+1\rangle \mid g(x) \in \mathbb{R}[x]\} = \{ax+b+\langle x^2+1\rangle \mid a,b \in \mathbb{R}\}.$$

Tämä todetaan seuraavasti: Olkoon $g(x) \in \mathbb{R}[x]$. Kirjoitetaan $g(x)$ muotoon $q(x)(x^2+1)+r(x)$ jakoyhtälöä käyttämällä. Erityisesti $\deg r(x) < 2$, joten $r(x) = ax+b$, missä $a,b \in \mathbb{R}$. Edelleen

$$g(x)+\langle x^2+1\rangle = q(x)(x^2+1)+r(x)+\langle x^2+1\rangle = r(x)+\langle x^2+1\rangle,$$

koska $q(x)(x^2+1) \in \langle x^2+1\rangle$.

Nyt esimerkiksi $(x+3+\langle x^2+1\rangle)(2x+5+\langle x^2+1\rangle) = 2x^2+11x+15+\langle x^2+1\rangle = 11x+13+\langle x^2+1\rangle$.

Lauseen 16 nojalla $\langle x^2+1\rangle$ on $\mathbb{R}[x]$:n maksimaalinen ideaali (koska ko. polynomi on jaoton), joten tutkittava jäännösluokkarengas on kunta. Edellisen mukaan tämän kunnan alkiot ovat muotoa $ax+b+\langle x^2+1\rangle$, missä $x^2+\langle x^2+1\rangle = -1+\langle x^2+1\rangle$. Onkin helppo todeta, että näin polynomien avulla konstruoitu kunta on isomorfinen kompleksilukujen kunnan kanssa.

LIITE 12

Sanasto : englanti-suomi-ruotsi

Abelian group = Abelin ryhmä, kommutatiivinen ryhmä : abelsk grupp, kommutativ grupp
absolute value = itseisarvo : absolut belopp
addition = yhteenlasku : addition, summa
additive = additiivinen : additiv
algebraic multiplicity = algebrallinen kertaluku : algebraisk ordning, multiplicitet
algorithm = algoritmi : algoritm
alternating group = alternoiva ryhmä : alternerande grupp
arithmetic = aritmeettinen : aritmetisk
arithmetic mean = aritmeettinen keskiarvo : aritmetiskt medeltal
associative law = liitäntälaki : associativitetslagen, den associativa lagen
associativity = liitännäisyys, assosiatiivisuus : associativitet
axiom = aksiooma : axiom
axiom of choice = valinta-aksiooma : urvalsaxiomet
axis (plural axes) = akseli : axel
base, basis = kanta : bas
bijection, 1-1 correspondence = bijektio, kääntäen yksikäsitteinen kuvaus : bijektion
bijective, one-to-one and onto = bijektiivinen, kääntäen yksikäsitteinen : bijektiv
binomial coefficient = binomikerroin : binomialkoefficient
bounded = rajoitettu : begränsad
cancel = supistaa : eliminera
canonical = kanoninen : kanonisk
canonical projection = kanoninen projektio : kanonisk projektion
cardinality = mahtavuus : kardinalitet
Cartesian product = karteesinen tulo : kartesisk produkt
chain = ketju : kedja
characteristic = karakteristinen; karakteristika (kunnan) : karakteristisk, karakteristika
circle = ympyrä : cirkel
column = sarake, pystyrivi : kolumn
combination = kombinaatio, yhdistely, yhdistelmä : kombination
combinatorial = kombinatorinen : kombinatorisk
commutative law = vaihdantalaki : den kommutativa lagen
commutativity = vaihdannaisuus, kommutatiivisuus : kommutativitet
commute = kommutoida : kommutera
comparability = vertailtavuus : jämförbarhet

complex conjugate = liittoluku : komplex konjugat
complex number = kompleksiluku : komplext tal
complex plane = kompleksitaso : komplexa planet
composite mapping = yhdistetty kuvaus (merkintä $f \circ g$, $f(g(x))$) : sammansatt avbildning
composite number = yhdistetty luku : sammansatt tal
congruence = kongruenssi : kongruens
congruent = kongruentti, yhtenevä : kongruent
conjecture = otaksuma, konjektuuri : konjektur, gissning
conjugacy class = konjugaattiluokka : konjugatklass
conjunction = konjunktio ("p ja q") : konjunktion
constant = vakio : konstant
construction = konstruointi, muodostaminen : konstruktion
contain = sisältää : innehålla
coordinate axes = koordinaattiakselit : koordinataxlar
coset = sivuluokka, jäännösluokka : restklass
countable, enumerable, denumerable = numeroituva : uppräknelig, numrerbar
cover = peite, peittää : täcka (verbi), täcke (subst.)
criterion = kriteeri : kriterium
cyclic = syklinen : cyklisk
decimal number = kymmenjärjestelmän luku; desimaaliluku : decimaltal
decomposition = hajotelma, tekijöihinjako; ositus : delning, partition
decreasing = vähenevä, aidosti vähenevä : avtagande, strängt avtagande
denominator = nimittäjä : nämnare
diagonal = lävistäjä, diagonaali : diagonal
diagonal matrix = lävistäjämatriisi : diagonal matris
diagonalizable = diagonalisoituva : diagonaliserbar
diagram = diagrammi, kaavio : diagram
dihedral (group) = diedri- (diedriryhmä) : diedergruppen
difference = erotus, differenssi : differens, skillnad
dimension = ulottuvuus, dimensio : dimension
direct product = suora tulo : direkt produkt
direct sum = suora summa : direkt summa
disjunction, alternation = disjunktio ("p tai q") : disjunktion ("p eller q")
division = jakolasku, jakaminen : division
division algorithm = jakoalgoritmi : divisionsalgoritm
divisor = jakaja, tekijä : divisor, nämnare
domain = määrittelyjoukko; alue : definitionsmängd, område
dot product = pistetulo, skalaaritulo, sisätulo : skalär produkt
eigenvalue = ominaisarvo : egenvärde
eigenvector = ominaisvektori : egenvektor
element, member = alkio, jäsen : element
elimination = eliminointi : eliminering
embedding, imbedding = upotus : inbädda
empty set = tyhjä joukko : tom mängd

endomorphism = endomorfismi : endomorfism
entry, element = alkio (matriisin) : element
equal = yhtäsuuri : lika stor
equation = yhtälö : ekvation
equivalence = ekvivalenssi : ekvivalens
equivalent = ekvivalentti, yhtäpitävä : ekvivalent
Euclidean space = euklidinen avaruus : euklidiskt rum
even = parillinen : jämn
example = esimerkki : exempel
exercise = tehtävä : övningsuppgift
exist = olla olemassa : existera
existence = olemassaolo : existens
existential quantifier = eksistenssikvanttori (esim. ”on olemassa x”) : existentiell kvantor
exponential function = eksponenttifunktio : exponentialfunktion
expression = lauseke : uttryck
extended = laajennettu : utvidgad
extension = laajennus, jatke : utvidgning
extension field = laajennuskunta : utvidgningskropp
factor group, quotient group = tekijäryhmä, jäännösluokkaryhmä : restklassgrupp
factor ring = jäännösluokkarengas : restklassring
factor(noun) = tekijä : faktor
factor(verb) = jakaa tekijöihin : faktorisera
factorial = kertoma ($n!$) : fakultet
factorization = tekijöihinjako : faktorisering
field = kunta : kropp
field extension = kuntalaajennus : utdvidgning av en kropp
field of fractions = (kokonaisalueen) osamääräkunta, jakokunta : kvotkropp
finite = äärellinen : ändlig
finitely generated = äärellisesti viritetty (generoitu) : ändligt genererad
fixed point = kiintopiste : fixpunkt
formal = formaali, muodollinen : formell
formula = kaava : formel
fraction = murtoluku, osamäärä : bråktal, kvot
function = funktio : funktion
Gaussian integer = Gaussin kokonaisluku : gaussiskt heltal
general = yleinen : allmän
general linear group = yleinen lineaarinen ryhmä : allmän lineär grupp
generalization = yleistys : generalisering
generate = virittää, generoida : generera
generator = virittäjä, generaattori : generator
geometric mean = geometrinen keskiarvo : geometriskt medeltal
graph = kuvaaja; verkko, graafi : graf
great = suuri : stor
greatest common divisor, GCD = suurin yhteinen tekijä : största gemensamma faktor

grid, lattice = hila; verkko : gitter
group = ryhmä : grupp
half-open interval = puoliavoin väli : halvöppet intervall
homeomorphism = homeomorfismi : homeomorfism
homogeneous = homogeeninen : homogen
ideal = ideaali, ihanne : ideal
identification = samaistus : identifikation
identity (mapping) = identiteetti(kuvaus) : identitet
identity element = ykkösalkio : enhetselement, etta
identity matrix = identiteettimatriisi, matriisirenkaan ykkösalkio : enhetsmatris
iff = jos ja vain jos, silloin ja vain silloin : omm, om och endast om
image = kuva, kuvajoukko, arvojoukko : bildmängd
imaginary = imaginaarinen : imaginär
imaginary axis = imaginaariakseli : imaginära axelen
imaginary part = imaginaariosa : imaginär del
imaginary unit = imaginaariyksikkö (i) : imaginär enhet
imbedding, embedding = upotus : inbäddning
implication = seuraus, implikaatio : följd, impliktion
implicit = implisiittinen : implicit
implies = (lausekkeesta, teoreemasta tms.) seuraa : följer av
increasing = kasvava; aidosti kasvava : växande
indefinite = indefiniitti (matriisi, neliömuoto) : indefinit
independence = riippumattomuus : oberoende
independent = riippumaton : oberoende
index = indeksi : index
induction = induktio : induktion
inequality = epäyhtälö : olikhet
infimum = infimum, suurin alaraja : infimum, största undre gräns
infinite = ääretön : oändlig
infinite sequence = ääretön jono : oändlig följd
injection = injektio : injektion
injective, one-to-one = injektiivinen : injektiv
integer = kokonaisluku, kokonais- : heltal, heltals-
integral domain = kokonaisalue : heltalsområde
interval = väli : intervall
invariant = invariantti : invariant
inverse = käänteinen, käänteis- : invers
inverse element = käänteisalkio, vasta-alkio : inverst element
inverse function = käänteisfunktio : invers funktion
inverse image = alkukuva : urbild
inverse matrix = käänteismatriisi : invers matris
inversion = käänteismuunnos : invers transformation
invertible = kääntyvä, säännöllinen : inverterbar, reguljär
isometry = isometria (etäisyydet säilyttävä kuvaus) : isometri

isomorphic = isomorfinen : isomorfisk
isomorphism = isomorfismi, isomorfia : isomorfism
iteration = iteraatio, iterointi : iteration
kernel, null space = ydin : kärna
lattice, grid = hila; verkko : gitter
leading coefficient = johtava kerroin : ledande koefficient
least common multiple, LCM = pienin yhteinen monikerta : minsta gemensamma multipel
left = vasen : vänster
left inverse = vasemmanpuoleinen käänteisalkio : vänsterinvers, invers element från vänster
left inverse matrix = vasemmanpuoleinen käänteismatriisi : vänster inversmatris, invers matris från vänster
lemma = lemma, apulause : lemma
length = pituus : längd
limit = raja-arvo : gränsvärde
line segment = jana : sträcka
line, straight line = suora : rät linje
linear algebra = lineaarialgebra : lineär algebra
linear combination = lineaarikombinaatio, lineaariyhdistelmä : lineär kombination
linear space, vector space = lineaariavaruus, vektoriavaruus : lineärt rum, vektorrum
linear transformation = lineaarikuvaus, lineaarimuunnos : lineär transformation
linearly independent = lineaarisesti riippumaton : lineärt oberoende
local = lokaali, paikallinen : lokal
logic = logiikka : logik
lower bound = alaraja : undre gräns
map, mapping = kuvaus : avbildning
mapping, function = kuvaus, funktio : avbildning, funktion
mathematical = matemaattinen : matematisk
mathematics = matematiikka : matematik
matrix = matriisi : matris
matrix norm = matriisinormi : matrisnorm
maximal ideal = maksimaalinen ideaali : maximalt ideal
mean = keskiarvo : medeltal
member, element = alkio (joukon), jäsen : element
metric = metriikka : metrik
metric space = metrinen avaruus : metriskt rum
minimum = minimi : minimum
monic polynomial = pääpolynomi : huvudpolynom
monoid = monoidi : monoid
monotonic, monotone = monotoninen : monoton
multiple = monikerta : multipel
multiplication = kertolasku : multiplikation
multiplication table = kertotaulu : multiplikationstabell
multiplicity = kertaluku (juuren) : multiplicitet
multiplier = kerroin : koefficient

n-tuple = n-jono : n-tupel
natural number = luonnollinen luku : naturligt tal
necessary = välttämätön : nödvändig
negation = negaatio : negation
negative definite = negatiividefiniitti, negatiivisesti definiitti : negativt definit
neutral element = neutraalialkio : neutralelement
network = verkko : nät
non-Euclidean geometry = epäeuklidinen geometria : icke-euklidisk geometri
nonempty = epätyhjä : icke tom
nonhomogeneous = epähomogeeninen : ickehomogen
nonlinear = epälineaarinen : ickelineär
norm = normi : norm
normal subgroup = normaali aliryhmä : normal undergrupp
null space, kernel = ydin : kärna
number = luku; numero : tal
number field = lukukunta : talkropp
number theory = lukuteoria : talteori
numerator, dividend = osoittaja, jaettava : täljare
numerical = numeerinen :numerisk
odd = pariton : udda
one-to-one, injective = injektiivinen : injektiv
onto, surjective = surjektiivinen : surjektiv
orbit = rata : bana
order = kertaluku; järjestys : ordning, ordningstal, multiplicitet
ordered pair = järjestetty pari : ordnat par
ordering = järjestys : ordning
orientation = suunnistus : orientering
orientation preserving = suunnan säilyttävä : som bibehåller orientering
orientation reversing = suunnan kääntävä : som inverterar orientering
oriented = suunnistettu; suunnattu : orienterad
origin = origo : origo
orthogonal = kohtisuora, ortogonaalinen : ortogonal
orthogonal matrix = ortogonaalinen matriisi : ortogonal matris
pairwise = par(e)ittain : parvis
parallelogram law = suunnikassääntö : parallellogramregel
partial fraction decomposition = osamurtokehitelmä : partialbråksutveckling
partial order(ing) = osittainen järjestys : partiell ordning
partition = ositus, partitio : delning, partition
period = jakso : period
periodic = jaksollinen : periodisk
periodicity = jaksollisuus : periodicitet
permutation = permutaatio, permutointi : permutation
perpendicular = kohtisuora : vinkelrät, ortogonal
piecewise = paloittain : styckevis

pigeon-hole principle = lokeroperiaate : boxprincipen
plane = taso : plan
point = piste : punkt
pointwise = pisteittäin : punktvis
polar coordinates = napakoordinaatit : polära koordinater
polygon = monikulmio : månghörning, polygon
polyhedron = monitahokas, tahokas : polyeder
polynomial = polynomi : polynom
polynomial ring = polynomirengas : polynomring
positive = positiivinen : positiv
positive definite = positiividefiniitti, positiivisesti definiitti : positiv definit
power = potenssi; mahtavuus : potens
power set = potenssijoukko : potensmängd
preimage = alkukuva : urbild
presentation = esitys : framställning
prime (number) = alkuluku, jaoton (luku) : primtal
prime factorization = alkutekijähajotelma, alkutekijöihinjako : primtalsfaktorisering
prime field = alkukunta : irreducibel kropp
prime ideal = alkuideaali : irreducibelt ideal
prime polynomial = jaoton polynomi : irreducibelt polynom
principal ideal = pääideaali : huvudideal, principalideal
principal ideal ring = pääideaalirengas : huvudideal ring, principalideal ring
product = tulo : produkt
product space = tuloavaruus : produktrum
projection = projektio : projektion
proof = todistus : bevis
proper = aito (osajoukko, aliavaruus) : äkta
proper subset = aito osajoukko : äkta delmängd
proposition = propositio : proposition
prove = todistaa : bevisa
pure(ly) imaginary = puhtaasti imaginaarinen (reaaliosa on 0) : rent imaginär
quadratic approximation = neliöllinen approksimaatio, kvadraattinen approksimaatio : kvadratisk approximation
quadratic form = neliömuoto : kvadratisk form
quadrilateral = nelikulmio : fyrhörning
quaternion = kvaternio : kvaternion
quotient = osamäärä : kvot
quotient field, field of fractions = (kokonaisalueen) osamääräkunta, jakokunta : kvotkropp
quotient group = tekijäryhmä : faktorgrupp
quotient ring = tekijärengas, jakorengas, jäännösluokkarengas : kvotring, faktorring, ring av restklasser
quotient space = tekijäavaruus : faktorrum
range = maalijoukko; kuva-avaruus : bildrum, målrum, målmängd
rank = säännöllisuusaste, aste, rangi; sijaluku, rankiluku : rang

rational = rationaalinen : rationell
rational function = rationaalifunktio : rationell funktion
rational number = rationaaliluku : rationellt tal
real = reaalinen, reaali- : reell
real axis = reaaliakseli : reella axelen
real number = reaaliluku : realdel
real part = reaaliosa : reell del
real vector space = reaalikertoiminen vektoriavaruus, reaalinen vektoriavaruus : reellt vektorrum
real-valued = reaaliarvoinen : reellvärdig, med reella värden
reciprocal (number) = käänteisluku : inverst tal
reciprocal = käänteis-, käännetty, resiprookkinen : inverst
reciprocity law = resiprookkilaki : reciprocitetssats
rectangle = suorakulmio : rektangel
rectangular = suorakulmainen : rektangulär
reduced residue class = alkuluokka : reducerad residyklass
reflexive = refleksiivinen :reflexiv
regular = säännöllinen : reguljär
regular representation = säännöllinen esitys : reguljär representation
relation = relaatio, suhde : relation
relatively prime = keskenään jaottomat : relativt prima, sinsemellan odelbar
remainder term, remainder = jäännöstermi, jäännös : restterm
represent = edustaa : representant
representation = esitys : representation
residual = residuaali, jäännös- : residual, rest-
residue = jäännös; residy : residy
residue class = jäännösluokka : residual klass, restklass
restriction = rajoittuma : restriktion
right = oikea : höger
ring = rengas : ring
root = juuri (yhtälön) : rot
root of unity = ykkösenjuuri : enhetsrot
row = rivi, vaakarivi : rad
scalar = skalaari, luku : skalär
scalar field = kerroinkunta : koefficientkropp
scalar-valued = skalaariarvoinen, lukuarvoinen : skalärvärdig
semigroup = puoliryhmä : halvgrupp
sense preserving = suunnistuksen säilyttävä : som bevarar orientering
sense reversing = suunnistuksen kääntävä : som inverterar orientering
sequence = jono (lukujono) : talföljd
set = joukko : mängd
set theory = joukko-oppi : mängdlära
shift = siirto : translation
show = näyttää : visa

sign, signum (abbr. sgn) = etumerkki; merkki : tecken
similar = similaarinen; yhdenmuotoinen; samanlainen : similär
simple group = yksinkertainen ryhmä : enkel grupp
simplify = sieventää : hyfsa, förenkla
skew field = vinokunta : vridkropp
small = pieni : liten
solution = ratkaisu : lösning
solvable, soluble = ratkeava : lösbar
span = viritelmä : genererad
span = virittää, generoida : genererad
square = neliö : kvadrat
square free = neliövapaa : kvadratfri
square matrix = neliömatriisi : kvadratisk matris
square root = neliöjuuri : kvadratrot
stable = vakaa, stabiili : stabil
standard basis = luonnollinen kanta : standard bas
strictly decreasing = aidosti vähenevä : strängt avtagande
strictly increasing = aidosti kasvava : strängt växande
subdivision = jako, alijako : delning
subfield = alikunta : delkropp
subgroup = aliryhmä : undergrupp
subinterval = osaväli : delintervall
submonoid = alimonoidi : undermonoid
subring = alirengas : underring
subset = osajoukko : delmängd
subspace = aliavaruus : underrum
substitution = sijoitus : substitution
subtraction = vähennyslasku; vähennys : subtraktion
sufficient = riittävä; tyhjentävä : tillräcklig
sum = summa, yhteenlasku : summa
surjection = surjektio : surjektion
surjective, onto = surjektiivinen : surjektiv
survey = katsaus : översikt
symmetric = symmetrinen : symmetrisk
symmetry = symmetria : symmetri
system of equations = yhtälöryhmä : ekvationssystem
tautology = tautologia, aina tosi lause : tautologi
tetrahedron = tetraedri : tetraeder
theorem = lause, teoreema : sats, teorem
theory = teoria : teori
total order(ing) = totaalinen järjestys, täydellinen järjestys, lineaarinen järjestys : fullständing ordning, lineär ordning
trace = jälki (matriisin) : spår
transformation = muunnos : transformation

transitive = transitiivinen : transitiv
translation = translaatio, siirto : translation
transpose = transpoosi : transpos
transposition = transpositio : transposition
triangle = kolmio : triangel
triangle inequality = kolmioepäyhtälö : triangelolikhet
triangular matrix = kolmiomatriisi : triangulär matris
trigonometric = trigonometrinen : trigonometrisk
trigonometry = trigonometria : trigonometri
trivial = triviaali : trivial
truth value = totuusarvo : sanningsvärde
uncountable = ylinumeroituva : oupräknelig
union = yhdiste, unioni : union
unique = yksikäsitteinen : entydig
uniqueness = yksikäsitteisyys : entydighet
unit = yksikkö (mittayksikkö) : enhet
unit, unit element = yksikkö (alkio jolla on käänteisalkio) : enhetselement, etta
unity = ykkönen; ykkösalkio : enhet
universal = universaali : universal
universal quantifier = universaalikvanttori (esim. ”kaikilla alkioilla x”) : all-kvantor
unknown = tuntematon (muuttuja tms.) : okänd
upper bound = yläraja : övre grans
valid = pätevä : gällande
value = arvo : värde
vanish = hävitä : försvinna
variable = muuttuja : variabel
vector = vektori : vektor
vector field = vektorikenttä : vektorfält
vector space, linear space = vektoriavaruus, lineaariavaruus : vektorrum
vertex = kärki : hörn
vertical = pystysuora : vertikal
void set = tyhjä joukko : tom mängd
volume = tilavuus : volym
well defined = hyvin määritelty : väl definierad
well-posed = hyvin asetettu (tehtävä tms.) : väl formulerad
zero = nolla, nollakohta, juuri (funktion) : nolla
zero vector = nollavektori : nollvektor

Sanaston pohjana on käytetty Juha Haatajan ja Kalle Mikkolan Internetissä aloittamaa matematiikan sanastoa: http://www.csc.fi/math_topics/data/math_words

Ruotsinkielisen sanaston tarkistuksen suorittivat Gustaf Gripenberg ja Sören Illman.

Hakemisto

Aakkosellinen hakemisto