Luku 1

Algebralliset operaatiot ja kunnat

Lineaarialgebran peruskursseilla tarkastellaan ainoastaan sellaisia lineaarisia otuksia, joiden *skalaarikunta* on reaalilukujen kunta $\mathbb{R}$, esimerkiksi lineaariset yhtälöryhmät oletetaan reaalikertoimisiksi, vektoriavaruuden alkioita kerrotaan reaaliluvuilla jne. Kuitenkin abstraktin algebran näkökulmasta reaalikertoiminen lineaarialgebra on vain erikoistapaus. Itse asiassa, hieman erikoisempaa sisätulon teoriaa lukuunottamatta, kaikki lineaariagebralliset käsitteet ja tulokset, joita käydään läpi peruskurssilla, toimivat sellaisenaan kun reaalilukujen systeemi $\mathbb{R}$ korvataan mielivaltaisella *kunnalla*.

Kunnan käsitteeseen voi päätyä luonnollisella tavalla lineaarialgebran kautta, jos tutkii minkälaisia reaalilukujen ominaisuuksia reaalikertoimisessa lineaarialgebrassa käytetään hyväksi. Osoittautuu, että merkitystä on ainoastaan reaalilukujen neljällä *algebrallisella operaatiolla*, jotka ovat yhteenlasku, vähennyslasku, kertolasku ja jakolasku, sekä niiden *ominaisuuksilla*. Minkälaisista ominaisuuksista on kyse?

Tarkastellaan esimerkiksi lineaaristen yhtälöryhmien ratkaisumenetelmien teoriasta tuttua alkeisrivitoimitusta $Y_i + rY_j$, johon perustuu muuttujan eliminointialgoritmi. Otetaan yksinkertaisuuden vuoksi kahden muuttujan x, y tapaus. Olkoot Y_1 ja Y_2 lineaariset yhtälöt

$$(Y_1) \qquad a_{11}x + a_{12}y = b_1,$$

$$(Y_2) \qquad a_{21}x + a_{22}y = b_2.$$

Oletamme edelleenkin, että kertoimet $a_{11}, a_{12}, a_{21}, a_{22}$ ja vakiotermit b_1, b_2 ovat reaalilukuja. Olkoon myös r reaaliluku. Jokainen koulua käynyt osaa suoraan päässäkin laskea, että operaation $Y_1 + rY_2$ (kerrotaan Y_2 luvulla r ja lisätään yhtälöön Y_1) seurauksena saadaan lineaarinen yhtälö

$$(a_{11} + ra_{21})x + (a_{12} + ra_{22})y = b_1 + rb_2.$$

Katsotaan kuitenkin tarkemmin mistä me oikeastaan tiedämme tämän ja mihin reaalilukujen ominaisuuksiin tämä ”itsestäänselvä” johtopäätös perustuu. Edetään yksi välivaihe kerrallaan. Aloitetaan siitä, että kerrotaan yhtälö Y_2 luvulla r. Tämähän tarkoittaa sitä, että yhtälön molemmat puolet kerrotaan luvulla r, jolloin yhtälö säilyy (miksi?) ja päädytään yhtälöön

$$r(a_{21}x + a_{22}y) = rb_2.$$

Seuraavaksi *avataan sulut* yhtälön vasemmalla puolella. Tämä välivaihe perustuu reaalilukujen **osittelulakiin**

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

Sijoittamalla tässä säännössä $a = r, b = a_{21}x$, $c = a_{22}y$, saadaan

$$r(a_{21}x) + r(a_{22}y) = r(a_{21}x + a_{22}y) = rb_2.$$

Huomaa erityisesti sulut, esimerkiksi ensimmäisessä yhteenlaskettavassa kyse on siitä, että luku $a_{21}x$ kerrotaan (vasemmalta) luvulla r. Tietysti me tiedämme, että pätee $r(a_{21}x_1) = (ra_{21})x_1$, mutta tämä tosiasia perustuu reaalilukujen **kertolaskun liitännäisyyteen**

$$a(bc) = (ab)c.$$

Samalla tavalla kertolaskun liitännäisyyteen on vedottava, jos haluaa korvata lausekkeen $r(a_{22}x_2)$ lausekkeella $(ra_{22})x_2$. Näin päästään seuraavassa välivaiheessa kirjoittamaan yhtälö rY_2 muotoon

$$(ra_{21})x + (ra_{22})y = rb_2. \tag{1.1}$$

Huomaa, että itse asiassa *vasta tässä vaiheessa* paljastuu, että *yhtälö rY_2 on itse lineaarinen yhtälö*. Ilman osittelulakia ja kertolaskun liitännäyisyyttä emme olisi voineet osoittaa todeksi näinkin yksinkertaista ja itsestään selvältä tuntuvaa väitettä.

Seuraavaksi lisätään yhtälö (1.1) yhtälöön Y_1 eli suoritetaan alkeisrivitoimitus $Y_1 + rY_2$. Merkintöjen yksinkertaistamiseksi merkitään yhtälön rY_2 kertoimia $ra_{21} = a'_{21}$, $ra_{22} = a'_{22}$, $rb_2 = b'_2$. Lasketaan siis yhtälöt $a_{11}x + a_{12}y = b_1$ ja $a'_{21}x + a'_{22}y = b'_2$ yhteen. Tämä tarkoittaa sitä, että yhtälöiden Y_1, rY_2 molemmat puolet lasketaan yhteen, jolloin yhtälö säilyy (miksi?) ja saadaan uusi yhtälö

$$(a_{11}x + a_{12}y) + (a'_{21}x + a'_{22}y) = b_1 + b'_2.$$

Seuraavaksi haluaisimme kerätä yhtälön vasemmalla puolella kaikki muuttujan x kertoimet ”yhteen”, yhdeksi muuttujan x kertoimeksi, ja vastaavasti muuttujan y kohdalla. Tätä varten meidän pitää ”avata sulut” ja ”järjestää termit uudestaan”. Tämä vaatii kuitenkin sekä **yhteenlaskun liitännäisyyden**

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

että myös **yhteenlaskun vaihdannaisuuden**

$$a + b = b + a$$

käyttöä. Nimittäin soveltamalla näitä algebrallisia lakeja saadaan

$$\begin{aligned}(a_{11}x + a_{12}y) + (a'_{21}x + a'_{22}y) &\overset{(i)}{=} (a_{11}x + a_{12}y) + (a'_{22}y + a'_{21}x)\\ &\overset{(ii)}{=} a_{11}x + (a_{12}y + (a'_{22}y + a'_{21}x)) \overset{(iii)}{=} a_{11}x + ((a_{12}y + a'_{22}y) + a'_{21}x)\\ &\overset{(iv)}{=} a_{11}x + (a'_{21}x + (a_{12}y + a'_{22}y))\\ &\overset{(iv)}{=} (a_{11}x + a'_{21}x) + (a_{12}y + a'_{22}y).\end{aligned}$$

Välivaiheden selitykset:

(i) Vaihdannaisuuden nojalla pätee $a'_{21}x + a'_{22}y = a'_{22}y + a'_{21}x$.

(ii) Sovelletaan yhteenlaskun liitännäisyyttä.

(iii) Sovelletaan yhteenlaskun liitännäisyyttä sisemmässä lauseekkessa, saadaan

$$a_{12}y + (a'_{22}y + a'_{21}x) = (a_{12}y + a'_{22}y) + a'_{21}x.$$

(iv) Sovelletaan yhteenlaskun vaihdannaisuutta sisemmässä lauseekkessa.

(v) Vaihdetaan sulkujen paikkaa yhteenlaskun liitännäisyyden avulla.

Nyt voidaan käyttää osittelulakia, jolloin saadaan vihdoinkin

$$(a_{11}x + a_{12}y) + (a'_{21}x + a'_{22}y) = (a_{11}x + a'_{21}x) + (a_{12}y + a'_{22}y) = (a_{11} + a'_{21})x + (a_{12} + a'_{22})y$$

ja päästään siihen, mihin haluttiin. Sijoittamalla takaisin $ra_{21} = a'_{21}$, $ra_{22} = a'_{22}$, $rb_2 = b'_2$, voidaan todeta, että yhtälö $Y_1 + rY_2$ on lineaarinen yhtälö

$$(a_{11} + ra_{21})x + (a_{12} + ra_{22})y = b_1 + rb_2.$$

Enemmän kuin kahden muuttujan tapauksessa välivaiheet ovat oleellisesti samanlaisia.

Näin ollen, sen osoittamiseksi, että tyyppiä (II) olevan alkeisrivitoimituksen tuloksena lineaarinen yhtälöryhmä edes säilyy lineaarisena yhtälöryhmänä, tarvitaan yhteenlaskun vaihdannaisuutta ja liitännäisyyttä, kertolaskun liitännäisyyttä sekä osittelulakia. Lisäksi samanlaisia laskuja (sekä vähennyslaskua, josta ei vielä ollut puhetta) joudutaan käymään läpi sen osoittamiseksi, että tyyppiä (II) oleva alkeisrivitoimitus säilyttää yhtälöryhmän ratkaisujoukon. Tämä on tietysti hyvin tärkeä tulos - jos alkeisrivitoimitus ei säilyttäisi ratkaisuja, siitä ei olisi mitään hyötyä yhtälöryhmien ratkaisemisen kannalta.

Katsotaan vielä tarkemmin mitä tapahtuu seuraavassa vaiheessa, eli *muuttujan eliminoinnissa*. Jos haluamme seuraavaksi eliminoida ensimmäisestä yhtälöstä muuttujan y, on yhtälössä $Y_1 + rY_2$ sijoitettava $r = -a_{12}a_{22}^{-1}$. Tässä tarvitaan sekä *vähennyslaskun*, että *jakolaskun* käsitteitä sekä niiden ominaisuuksia. Katsotaan ensin, mistä syistä tämä toimenpide todellakin eliminoi muuttujan y. Tämän muuttujan kerroin yhtälössä $Y_1 + rY_2$, missä $r = -a_{12}a_{22}^{-1}$, on

$$a_{12} + ra_{22} = a_{12} - (a_{12}a_{22}^{-1})a_{22} \overset{(i)}{=} a_{12} - a_{12}(a_{22}^{-1}a_{22})$$

$$\overset{(ii)}{=} a_{12} - a_{12} \cdot 1 \overset{(iii)}{=} a_{12} - a_{12} \overset{(iv)}{=} 0.$$

Välivaiheiden selitykset:

(i) Kertolaskun liitännäisyys.

(ii) *Käänteisluvun* määritelmä: $aa^{-1} = 1$ kaikilla reaaliluvulla a.

(iv) *Ykkösalkion* 1 määrittelevä ominaisuus: $a \cdot 1 = a$ kaikilla reaaliluvulla a.

(v) *Vasta-luvun* määritelmä: $a + (-a) = a - a = 0$ kaikilla reaaliluvuilla a.

Olemme näyttäneet, että yhtälö Y_1 muuntuu alkeisrivitoimituksen $Y_1 - a_{12}a_{22}^{-1}Y_2$ avulla muotoon

$$a_{11}''x + 0y = b_1''.$$

Tässä ei ole vielä kaikki - nyt pitäisi vielä päätellä, että

(1) $0y = 0$ ja

(2) $a_{11}''x + 0y = a_{11}''x + 0 = a_{11}''$.

Vasta tämän jälkeen voidaan todeta, että muuttuja y on todellakin eliminoitu ensimmäisestä yhtälöstä, jolloin voimme ratkaista muutujan x arvo, $x = b_1''/a_{11}''$. Väitteiden (1) ja (2) perustelemista varten meidän on palautettava mieleen, että luku 0 on niin sanottu *yhteenlaskun neutraalialkio*, mikä tarkoittaa yksinkertaisesti sitä, että $a + 0 = a$ kaikilla reaaliluvuilla a. Väite (2) seuraa tällöin suoraan, kunhan ensin osoitetaan ensin todeksi väite (1). Tämä taas voidaan johtaa osittelulain ja luvun 0 edellä mainitun määritelmän avulla. Palataan tähän tarkemmin myöhemmin yleisesti renkaiden tasolla.

Kootaan yhteen saadut havainnot. Jotta Gaussin eliminointimenetelmä olisi loogisesti pätevä, tarvitsemme seuraavia reaalilukujen *algebrallisten operaatioden* yhteen- ja kertolaskun ominaisuuksia: yhteenlaskun vaihdannaisuus ja liitännäisyys, kertolaskun liitännäisyys, osittelulaki. Lisäksi tarvitsemme *nolla-alkion* 0, sekä *ykkösalkion* käsitteitä. Nolla-alkio 0 on sellainen alkio, joka ei muuta lukua *yhteenlaskussa*, $x + 0 = 0 + x$ kaikilla reaaliluvuilla x. Ykkösalkiolla 1 on samantyyppinen ominaisuus *kertolaskun* suhteen, $x \cdot 1 = 1 \cdot x = x$ kaikilla $x \in \mathbb{R}$.

Olemme myös käyttäneet vähennys- ja jakolaskua. Näita sovelletaan Gaussin eliminointimenetelmässä paitsi muuttujan eliminointivaiheessa, myös laskun lopussa. Nimittäin päämuuttuja ratkaistaan vapaiden muuttujien avulla yhtälöryhmän porrasmuodossa siirrtämällä termejä yhtälön toiselle puolelle, mikä perustuu vähennyslaskuun. Tämän jälkeen päämuuttujan arvo ratkaistaan *jakamalla* se (nollasta eroavalla) kertoimella.

Vähennys- ja jakolasku voidaan palauttaa yhteen- ja kertolaskun *vasta-luvun* ja *käänteisluvun* käsitteisiin. Luvun $x \in \mathbb{R}$ vasta-luku $-x$ on sellainen reaaliluku, jolle pätee $x + (-x) = (-x) + x = 0$, missä 0 on jo edellä mainittu nolla-alkio. Nollasta eroavan reaaliluvun x käänteisluku x^{-1} on sellainen reaaliluku, jolle pätee $x \cdot x^{-1} = x^{-1} \cdot x = 1$. Nollan käänteisluku ei ole määritely (renkaiden teorian yhteydessä palataan kohta yleisellä tasolla kysymykseen miksi "nollalla ei saa jakaa"). Kun vasta-alkiot ja käänteisluvut ovat määriteltyjä, voidaan määritellä vähennys- ja jakolaskut, kaavoilla

$$x - y = x + (-y),$$

$$\frac{x}{y} = xy^{-1}.$$

Reaalilukujen kertolaskulla on vielä yksi ominaisuus, jota emme mainineet yllä kertaakaan, nimittäin *kertolaskun vaihdannaisuus* $xy = yx$. Itse asiassa se ei ole lineaarialgebran

kannalta yhtä tärkeä kuin muut yhteen- ja kertolaskun ominaisuudet, esimerkiksi Gaussin eliminointimenetelmässä sitä ei tosiaankaan tarvita. Tästä syystä joskus kirjallisuudessa otetaankin vektoriavaruuksien skalaarien lähtökohdaksi niin sanottuja *vinokuntia*, joissa kertolaskun vaihdannaisuutta ei oleteta. Suurin osa teoriasta toimii vinokuntien tapauksessa samalla tavalla kuin kuntien tapauksessa, mutta on kuitenkin myös tärkeitä tuloksia, joissa tarvitaan myös kertolaskun vaihdannaisuutta. Siksi kurssin ensimmäisessä osassa, joissa tarkastellaan vektoriavaruuksia, teemme yhteistyötä nimenomaan kuntien kanssa. Kurssin loppupuolella tutustumme myös yleisempään *modulien* teoriaan. Näissä skalaarit ovat niin sanottujen *renkaiden* alkiota.

1.1. Algebralliset operaatiot

Reaalilukujen yhteen- ja kertolasku ovat esimerkkejä *algebrallisista operaatioista* (reaalilukujen joukossa $\mathbb{R}$).

Olkoon X mielivaltainen joukko. **Algebrallinen operaatio** joukossa X on kuvaus $f\colon X \times X \to X$. Toinen nimitys, jota käytetään algebrallisen operaation synonyyminä, on **laskutoimitus** joukossa X. Palautetaan mieleen, että **karteesinen tulo** $X \times X$ on joukko, joka koostuu kaikista *järjestetyistä pareista* (x, y), missä $x, y \in X$,

$$X \times X = \{(x, y) \mid x, y \in X\}.$$

Tapausta $x = y$ sallitaan eli on olemassa pareja (x, x), $x \in X$. On tärkeätä ymmärtää, että pari (x, y) eroaa joukosta $\{x, y\}$, sillä parissa (x, y) alkiot x, y luetellaan *järjestyksessä* - x on parin (x, y) *ensimmäinen komponentti*, y on parin *toinen komponentti*. Erityisesti (x, y) ja (y, x) ovat *eri pareja*, paitsi silloin kun $x = y$. Joukossa taas alkioiden luettelojärjestyksellä ei ole merkitystä, joukot $\{x, y\}$ ja $\{y, x\}$ ovat aina sama joukko.

Näin ollen joukossa X määritelty laskutoimitus $f\colon X \times X \to X$ voidaan ajatella eräänä tapana liittää kahteen joukon X alkioihin a, b (tässä järjestyksessä) tämän laskutoimituksen *tulos* $f(a, b)$, joka on myös joukon X alkio. Vaikka laskutoimitus onkin kuvaus, tämäntyyppistä "funktionaalista" merkintää käytetään harvoin. Sen sijaan algebrassa on tapana käyttää laskutoimituksen symboleina merkkejä $+, \cdot, \times, \circ, \oplus, \otimes$ jne. Tällöin laskutoimituksen tulosta **ei** merkitä $+(a, b)$, $\cdot(a, b)$ jne., vaan tuttuun tapaan $a + b$, $a \cdot b$ ja niin poispäin, eli laittamalla laskutoimitusta vastaava symboli alkioiden väliin. Kun laskutoimituksen symbolina on sovittu $+$ eli *plusmerkki*, puhutaan alkioiden a ja b **summasta** $a + b$. Laskutoimitusta tällöin sanotaan *yhteenlaskuksi* ja merkintätapaa $a + b$ sanotaan *additiiviseksi*. Kun laskutoimituksen symbolina käytetään pistettä $\cdot$ puhutaan alkioiden a ja b **tulosta** $a \cdot b$. Laskutoimitus on tällöin *kertolasku* tai *tulo*. Tällaista merkintätapaa sanotaan myös *multiplikatiiviseksi*. Multiplikatiivisesti merkityn laskutoimituksen tapauksessa on varsin tavallista, että jätetään laskutoimitus jopa kokonaan merkitsemättä, jolloin alkioiden a ja b tuloa merkitään yksinkertaisesti ab.

Näiden symbolien ja merkintöjen käyttötavoista on olemassa kutakuinkin vakiintuneita käytäntöjä ja perinteitä, jotka selviävät kokemuksen ja kontekstin myötä. Esimerkiksi koulusta asti olemme tottuneet merkitsemään reaalilukujen yhteenlaskua symbolilla $+$ ja

kertolaskua symbolilla $\cdot$. Tällaisia perinteitä on syytä noudattaa, mutta samalla on pidettävää mielessä, että kyse on vain merkintätavoista ja matemaattinen sisältö ei riipu siitä, mitä merkintöjä on missäkin asianyhteydessä sovittu käyttämään. Puhtaan matematiikan näkökulmasta yhteen- ja kertolasku ovat laskutoimituksina "samanarvosia", molemmat ovat vain esimerkkejä joukon laskutoimituksesta. Koska kuitenkin törmäämme niihin usein samassa yhteydessa, niille on pakko ottaa käyttöön erilaisia merkintöjä tai sopimuksia, esimerkiksi koulusta tuttu laskutoimitusten *laskujärjestyssopimus*, jonka mukaan kertolaskulla on monimutkaisissa lausekkeissa *prioriteetti* yhteenlaskun suhteen.

Kun joukossa X on annettu jokin laskutoimitus $\cdot$, sanomme myös, että X on *varustettu* laskutoimituksella $\cdot$. Sama joukko voidaan yleensä varustaa hyvin monella erilaisella laskutoimituksella.

Esimerkki 1.2. *1. Vanhimpia ihmiselle tunnettuja laskutoimituksia on melko varmasti positiivisten kokonaislukujen yhteenlasku. Tämä on siis joukossa* $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$ *määritelty laskutoimitus* $+$*. Ihmiset tiesivät että lukumääriä voi laskea yhteen ennen kirjallisuuden keksimistäkin. Sen sijaan luvun nolla "keksiminen" kesti pitkään, nollan käyttö vakiintui länsimaissa vasta noin 500 vuotta sitten.*

2. Vähennyslasku $-$ *on laskutoimitus* kokonaislukujen *joukossa* $\mathbb{Z}$*. Sen sijaan luonnollisten lukujen joukossa* $\mathbb{N}$ *vähennyslaskua ei voida määritellä, sillä on olemassa luonnollisten lukujen pareja* (a, b)*, joille* $a - b$ *ei ole enää luonnollinen luku, esimerkiksi* $1 - 2 = -1 \notin \mathbb{N}$*. Jotta vähennyslasku olisi mahdollista määritellä yleisesti, tarvitaan myös* negatiivisia *lukuja. Nämä ovat suurinpiirtein yhtä vanha keksintö kuin nolla.*

Määritelmän mukaan laskutoimitus joukossa X on kuvaus $f\colon X \times X \to X$. On selvää, että tällä tavalla määritelty algebrallisen operaation käsite on liian laaja ollakseen mielenkiintoinen - sellaiseksi kelpaa *mikä tahansa* kuvaus $X \times X \to X$ eikä tällaisesta yleisesti voida sanoa mitään sen enempää. Algebrassa rajoitutaankin tutkimaan tarkemmin ainoastaan sellaisia algebrallisia operaatioita, jotka toteuttavat tiettyjä lisäominaisuuksia, yleensä sellaisia, jotka voidaan muotoilla pelkästään operaation ja joukon alkioiden avulla. Tällaisia ominaisuuksia on luonnollista kutsua *algebrallisiksi*. Esimerkiksi yhteenlaskun vaihdannaisuutta ilmaiseva ominaisuus "$a + b = b + a$ kaikilla a, b" on esimerkki tyyppillisestä laskutoimituksen algebrallista ominaisuudesta. Sen sijaan ominaisuus "reaalilukujen joukon $\mathbb{R}$ yhteenlasku on jatkuva operaatio" ei ole algebrallinen, sillä sen muotoilussa esiintyy topologinen jatkuvuuden käsite.

Annetaan muutama esimerkki tärkeistä algebrallisista ominaisuuksista. Käytämme laskutoimitukselle ensisijaisesti multiplikatiivista merkintätapaa, mutta annamme jokaiselle uudelle käsitteelle myös "addiitivisen tulkinnan".

Assosiatiivisuus/Liitännäisys.
Olkoon $\cdot$ joukossa X määritelty laskutoimitus. Sitä sanotaan *assosiatiiviseksi* tai *liitännäiseksi* jos kaikilla $a, b, c \in X$ pätee

$$(ab)c = a(bc).$$

Jos laskutoimitus merkitään additiivisesti symbolilla $+$, liitännäisyys tarkoittaa sitä, että

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

kaikilla $a, b, c \in X$.

Lähtökohtaisesti jokainen laskutoimitus $\cdot$ määrittelee vain **kahden alkion** a, b laskutoimituksen tulosta ab. Jos haluaa "kertoa" keskenään kolme tai enemmän alkiota eli muodostaa esimerkiksi tulon abc, täytyy ensin kertoa mitä tämä tarkoittaa, eli miten tämä tulo määritellään ja ymmärretään, sillä laskutoimitus sinänsä ei sano tästä mitään. Yleensä tällaisessa tapauksessa asetetaan

$$abc = (ab)c$$

eli abc saadaan kun ensin lasketaan tulo $ab = d$ ja sen jälkeen lasketaan tulo dc. Jos "välilaskuja" suorittaa toisessa järjestyksessä, eli ensin bc ja sitten $a(bc)$, lopputulos voi, yleisesti ottaen, olla erilainen. *Liittänäisen* laskutoimituksen kohdalla tällaista ongelmaa ei ole, sillä siinä pätee $(ab)c = a(bc)$, toisin sanoen kolmen alkion tulo abc voidaan laskea suorittamalla välilaskuja missä tahansa järjestyksessä.

Yleisesti laskutoimituksen $\cdot$ ollessa liitännäinen voidaan puhua mielivaltaisen monen alkion $a_1, \ldots, a_n$ tulosta $a_1 a_2 \ldots a_n$. Virallisesti tämä tulo määritellään *induktiivisesti* kaavalla

$$a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n,$$

mutta koska laskutoimitus on liitännäinen, tämän laskun lopputulos ei riipu siitä, millä tavalla järjestää sulkuja alkioiden ympärille. Esimerkiksi neljän alkion tapauksessa liitännäisyys implikoi, että

$$a_1 a_2 a_3 a_4 = ((a_1 a_2) a_3) a_4 = (a_1 a_2)(a_3 a_4) = a_1 (a_2 (a_3 a_4)) = a_1 ((a_2 a_3) a_4).$$

Ei-liitännäisessä laskutoimituksessa tällaiset laskut eivät ole päteviä ja kolmen tai useamman alkion tulo voi riippua välivaiheiden suoritusjärjestyksestä. Tällä kurssilla kaikki laskutoimitukset, joihin törmämme, tulevat olemaan liitännäisiä.

Esimerkkejä 1.3. *1. Reaalilukujen yhteen-ja kertolasku ovat tunnetusti liitännäisiä. Sen sijaan esimerkiksi vähennyslasku ei ole liitännäinen, sillä esimerkiksi*

$$7 - (5 - 2) = 4 \neq 0 = (7 - 5) - 2.$$

2. Tärkeimpiä esimerkkejä assosiatiivisista laskutoimituksista on **kuvausten yhdistäminen**. *Palutetaan mieleen, että kun $f \colon X \to Y$ ja $g \colon Y \to Z$ ovat kuvauksia siten, että kuvauksen f* maalijoukko Y *on sama kuin kuvauksen g* lähtöjoukko, *voidaan muodostaa* yhdistetty kuvaus $g \circ f$ *kaavalla*

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

Kuvausten yhdistäminen on liitännäinen operaatio, sillä

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

aina kun kaikki molemmalla puolella esiintyvät yhdistetyt kuvaukset ovat määriteltyjä, eli kun $f \colon X \to Y$, $g \colon Y \to Z$, $h \colon Z \to W$. Tämän näkee laskemalla yhtälön molemman puolen arvo mielivaltaisessa pisteessä $x \in X$ (HT, tuttu matematiikan

peruskursseilta).

Vaikka kuvausten yhdistäminen on liitännäinen operaatio, näin määriteltynä se ei ole laskutoimitus missään joukossa, sillä se ei ole määritelty kaikilla pareilla (f, g), missä f ja g ovat kuvauksia. Saadaksemme tästä laskutoimituksen kiinnitetään jokin joukko X ja rajoitetaan tarkastelu joukkoon $Y = X^X$, jonka muodostavat kaikki kuvaukset $f\colon X \to X$ (sekä lähtö-, että maalipuoli sama joukko X). Tällöin kuvausten yhdistäminen $(f, g) \mapsto g \circ f$ on joukossa Y määritelty liitännäinen laskutoimitus.

Summan ja tulon merkit

Olkoon + additiivisesti merkitty *liitännäinen* laskutoimitus jossakin joukossa X. Olemme todenneet, että tällöin voidaan puhua myös kolmen tai useamman alkion summasta, eli yleisesti alkioiden $a_1, \ldots, a_n \in X$ summasta

$$a_1 + a_2 + \ldots + a_n.$$

Toinen, täsmällisempi ja lyhyempi, tapa merkitä *samantyyppisten alkioiden* summaa on niin sanottu summan $\sum$-*merkki* (luetaan "sigma-merkki"):

$$a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i.$$

Tällaisessa merkinnässä summattavat indeksoidaan jollakin mielekkäällä tavalla, esimerkiksi yllä indeksoidaan summan jäsenet alaindeksin i avulla, jonka oletetaan saavan kokonaislukuarvoja. Tämä indeksi käy läpi kaikki arvot luvusta 1 (tähän alarajaan viittää $\sum$-symbolin alapuolella oleva merkki $i = 1$) lukuun n (tämä yläraja laitetaan $\sum$-symbolin yläpuolella). Esimerkiksi

$$\sum_{i=2}^{5} i^2$$

tarkoittaa summaa

$$2^2 + 3^2 + 4^2 + 5^2.$$

Toinen esimerkki - "Johdanto"-mateeriaalissa esitetyn lineaarisen yhtälöryhmän (3) i:nnes yhtälö

$$a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{im}x_m = b_i$$

voidaan kirjoittaa $\sum$-merkinnän avulla lyhyesti muotoon $\sum_{j=1}^{m} a_{ij}x_j = b_i$.

Indeksejä voi olla enemmän kuin yksi ja sen sijaan, että annetaan indeksille ala-ja ylärajoja, summausmerkissä voidaan antaa jokin ehto, jonka indeksien on toteuttavaa. Esimerkiksi *binomikaava* voidaan kirjoittaa muotoon

$$(a + b)^n = \sum_{i+j=n} \binom{n}{i} a^i b^j.$$

Tässä siis oletetaan, että i ja j saavat ei-negatiivisia kokonaislukuarvoja siten, että $i+j = n$. Summa muodostetaan käymällä läpi kaikki vaihtoehdot, esimerkiksi

$$(a + b)^3 = \sum_{i+j=3} \binom{3}{i} a^i b^j = a^0b^3 + 3a^1b^2 + 3a^2b^1 + a^3b^3.$$

Yleensä indeksien mahdollisten arvojen joukko selviää asianyhteydestä.

Jos liitännäiselle laskutoimitukselle käytetään multiplikatiivista merkintää $\cdot$, summan sigma-merkinnän sijasta käytetään *tulon pii-merkintää* $\prod$. Esimerkiksi luonnollisen luvun n *kertoma* voidaan määritellä kaavalla

$$n! = \prod_{i=1}^{n} i.$$

Kommutatiivisuus/Vaihdannaisuus.
Joukon X laskutoimitus $\cdot$ on *kommutatiivinen* eli *vaihdannainen* jos kaikilla $a, b \in X$ pätee

$$ab = ba.$$

Jos laskutoimituksen merkintätapa on additiivinen, vaihdannaisuuden ehto tarkoittaa, että kaikilla $a, b \in X$ pätee

$$a + b = b + a.$$

Itse asiassa matematiikassa on vakiintunut tapana käyttää additiivista merkintätapaa $+$ *ainoastaan* vaihdannaisille operaatioille.

Koulusta tutut luvuille määritellyt laskutoimitukset eli reaalilukujen yhteenlasku ja kertolasku ovat tunnetusti kommutatiivisia. Korkeassa matematiikassa sen sijaan vaihdannaiset operaatiot ovat paljon harvinaisempia kuin koulumatematiikassa. Olennainen syy tähän on oikeastaan se, että *kuvausten yhdistäminen* ei ole yleisesti ottaen vaihdannainen operaatio. Esimerkiksi jos kuvauksille $f, g\colon \mathbb{R} \to \mathbb{R}$ pätee $f(x) = x + 1$, $g(x) = x^2$, niin

$$f \circ g(x) = (x + 1)^2 \neq x^2 + 1 = g \circ f(x),$$

kun $x \neq 0$, joten $f \circ g \neq g \circ f$.

Suurin osa matematiikassa esiintyvistä mielenkiintoisista laskutoimituksista ”polveutuvat” tavalla tai toisella kuvausten yhdistämisestä (vaikka tätä ei aina huomaa päällepäin). Tästä syystä ominaisuudet, joita kuvausten yhdistämisoperaatiolla ei ole, ovat vähemmän yleisiä kuin sellaiset ominaisuudet, joita kuvausten yhdistämisellä luonnostaan on (esimerkiksi liitännäisyys). Tällä kurssilla törmäämme luonnollisella tavalla eivaihdannaisiin laskutoimituksiin ensimmäistä kertaa *matriisien kertolaskun* yhteydessä.

Neutraalialkio ja käänteisalkiot

Neutraalialkio.
Olkoon $\cdot$ joukon X laskutoimitus. Alkiota $e \in X$ sanotaan tämän laskutoimituksen *neutraalialkioksi* jos kaikilla $x \in X$ pätee

$$ex = x = xe.$$

Havainnollisesti neutraalialkio ”pitää alkion x paikallaan laskutoimituksessa”.

Esimerkkejä 1.4. *(1) Positiivisten kokonaislukujen joukossa* $\mathbb{N}_+ = \{1, 2, 3, \ldots, \}$ *määritellyllä yhteenlasku-operaatiolla ei ole neutraalialkiota - sehän on nimenomaan nollan rooli. Kun joukkoon* $\mathbb{N}_+$ *lisätään nolla, eli tarkastellaan yhteenlaskua luonnollisten lukujen joukossa* $\mathbb{N} = \{0, 1, 2, \ldots\}$*, tällä laskutoimituksella on neutraalialkiona* 0*.*

(2) *Luku* 1 *on reaalilukujen kertolaskun neutraalialkio.*

(3) *Kuvausten* $f\colon X \to X$ *yhdistämisoperaatiolla on neutraalialkiona* identtinen *kuvaus* $\mathrm{id}\colon X \to X$*, joka on määritelty kaavalla* $\mathrm{id}(x) = x$ *kaikilla* $x \in X$*.*

Neutraalialkio on aina *yksikäsitteinen*, jos se on olemassa, eli *laskutoimituksella voi olla korkeintaan yksi neutraalialkio.* Tämä nähdään seuraavasti. Olkoot $e, e' \in X$ molemmat laskutoimituksen $\cdot$ neutraalialkioita. Tällöin neutraalialkion määritelmästä seuraa suoraan, että

$$e = e'e = e'.$$

Kun laskutoimitusta $\cdot$ merkitään *multiplikatiivisesti*, neutraalialkiolle usein käytetään merkintää 1. Tällöin tätä alkiota sanotaan myös laskutoimituksen *ykkösalkioksi.* Kun laskutoimitusta merkitään additiivisesti symbolilla +, neutraalialkiota merkitään tavallisesti symbolilla 0 ja sitä sanotaan *nollaksi* tai nolla-alkioksi.

Käänteisalkio/Vasta-alkio.
Olkoon $\cdot$ joukossa X määritelty laskutoimitus, *jolla on neutraalialkio* e. Olkoon $x \in X$. Alkiota $y \in X$ sanotaan x:n *käänteisalkioksi* jos pätee

$$xy = e = yx.$$

Käänteisalkio on aina yksikäsitteinen, **jos oletetaan lisäksi**, että laskutoimitus on liitännäinen.

Lemma 1.5. *Olkoon* $\cdot$ *joukossa* X *määritelty liitännäinen laskutoimitus, jolla on neutraalialkio* e*. Olkoon* $x \in X$*. Oletetaan, että* $y, z \in X$ *molemmat toteutuvat alkion* x *käänteisalkion määritelmän. Tällöin* $y = z$*.*

Todistus. Oletusten nojalla pätee

$$y = ye = y(xz) = (yx)z = ez = z.$$

□

Kun laskutoimitus $\cdot$ on liitännäinen, alkion x känteisalkiota merkitään, jos se on olemassa, symbolilla x^{-1}. Lisäksi sanomme tällöin, että x on *kääntyvä* laskutoimituksen $\cdot$ suhteen.

Jos laskutoimituksen symbolina käytetään + merkkiä, käänteisalkion sijaan puhutaan x:n *vasta-alkiosta.* Vasta-alkio merkitään symbolilla $-x$. Tällöin siis pätee

$$x + (-x) = (-x) + x = 0.$$

Esimerkkejä 1.6. *(1) Tarkastellaan luonnollisten lukujen joukossa* $\mathbb{N}$ *määriteltyä yhteenlaskua. Tällä laskutoimituksella on neutraalialkio* 0*, mutta se onkin ainoa alkio, jolla on vasta-alkio - tässä tapauksessa nolla on itsensä vasta-alkio. Jos halutaan kaikille alkioille vasta-alkiot, joukkoon on lisättävää negatiivisia kokonaislukuja. Näin päädytään luonnollisella tavalla* kokonaisten lukujen joukkoon $\mathbb{Z}$*. Joukossa* $\mathbb{Z}$ *jokaisella alkiolla on vasta-alkio yhteenlaskun suhteen.*

(2) *Tarkastellaan kuvausten yhdistämisoperaatiota kuvausten $f\colon X \to X$ joukossa. Voidaan osoittaa (HT), että kuvauksella $f\colon X \to Y$ on olemassa tämän laskutoimituksen suhteen käänteisalkio jos ja vain jos f on* bijektio. *Tällöin kuvauksen f käänteisalkiota f^{-1} sanotaan f:n* käänteiskuvaukseksi. *Alkioiden tasolla käänteiskuvaus on määritelty seuraavasti. Olkoon $y \in X$ mielivaltainen. Koska f on surjektio, on olemassa $x \in X$ jolle pätee $f(x) = y$. Lisäksi, koska f on injektio, tällainen x on yksikäsitteinen. Asettamalla $g(y) = x$ saadaan hyvin määritelty kuvaus $g\colon X \to X$, jolle pätee (HT)*

$$f \circ g = g \circ f = \mathrm{id}_X\,.$$

Koska identtinen kuvaus id_X on laskutoimituksen $\circ$ neutraalialkio, tästä seuraa, että $g = f^{-1}$.

Seuraava Lemma sanoo sen, että käänteisalkion ottaminen tulosta "kääntää" kerrottavien järjestystä.

Lemma 1.7. *Olkoon $\cdot$ joukossa X määritelty liitännäinen laskutoimitus, jolla on neutraalialkio e. Olkoot $x, y \in X$. Oletetaan että sekä x, että y ovat kääntyviä laskutoimituksen $\cdot$ suhteen. Tällöin myös tulo xy on kääntyvä ja pätee*

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Todistus. Liitännäisyyden ja käänteisalkioiden määritelmän nojalla saadaan suoraan laskemalla

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e.$$

Samalla tavalla osoitetaan, että $(y^{-1}x^{-1})xy = e$. Näin ollen $y^{-1}x^{-1}$ toteuttaa alkion xy käänteisalkion määritelmää. □

Mihin käänteisalkioita tarvitaan?
Olkoon $\cdot$ joukossa X määritelty *liitännäinen* laskutoimitus. Yhtälöä, joka on muotoa $ax = b$ tai $xa = b$ (missä $a, b \in X$ ovat annettuja vakiota ja x on tuntematon), sanotaan *lineaariseksi* (laskutoimituksen $\cdot$ suhteen). Tarkastellaan lineaarista yhtälöä $ax = b$ ja oletetaan, että laskutoimituksella $\cdot$ on neutraalialkio $e \in X$ ja tuntemattoman *kertoimella* a on X:ssä käänteisalkio a^{-1}. Tällöin kertomalla yhtälön $ax = b$ molemmat puolet *vasemmalta* alkiolla a^{-1} saadaan

$$x = ex = (a^{-1}a)x \overset{(i)}{=} a^{-1}(ax) = a^{-1}b.$$

Huomaa, että kohdassa (i) on käytetty hyväksi laskutoimituksen liitännäisyytta. Kääntäen sijoittamalla tuntemattoman x paikalle $a^{-1}b$ nähdään, että $x = a^{-1}b$ todellakin on lineaarisen yhtälön $ax = b$ ratkaisu. Näin ollen saadaan seuraava johtopäätös.

Lemma 1.8. *Olkoon $\cdot$ joukossa X määritelty liitännäinen laskutoimitus, jolla on neutraalialkio e. Olkoot $a, b \in X$. Oletetaan, että alkiolla a on X:ssä käänteisalkio a^{-1}. Tällöin lineaarisella yhtälöllä $ax = b$ on X:ssä* yksikäsitteinen *ratkaisu $x = a^{-1}b$.*

Vastaavasti lineaarisella yhtälöllä $xa = b$ on X:ssä yksikäsitteinen ratkaisu $x = ba^{-1}$.

Edellisessä lemmassa lineaarista yhtälöä $xa = b$ koskeva väite todistetaan samalla tavalla kuin yhtälön $ax = b$ kohdalla. Huomaa, että jos kertolasku on vaihdannainen, nämä yhtälöt ovat samoja, mutta yleisesti ottaen ne ovat eri yhtälöitä.

Näin ollen käänteisalkioiden olemassaolo helpottaa lineaaristen yhtälöiden ratkaisemista.

Potenssit ja monikerrat.
Olkoon X laskutoimituksella $\cdot$ varustettu joukko. Olkoon $x \in X$ ja oletetaan, että $n = 1, 2, 3, \ldots$ on *positiivinen kokonaisluku*. Alkion x *n's potenssi* x^n määritellään jokaisella positiivisella luonnollisella luvulla rekursiivisesti *induktiolla* asettamalla

$$x^1 = x,$$

$$x^{n+1} = x^n \cdot x.$$

Esimerkiksi $x^2 = x \cdot x$, $x^3 = (x \cdot x) \cdot x$ jne. Jos laskutoimitus on liitännäinen, emme tarvitse sulkuja ja voimme kirjoittaa

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ kertaa}},$$

mikä vastaa potenssin intuitiivista tulkintaa. Liitännäisen laskutoimituksen tapauksessa pätee myös tärkeä *potenssisääntö*

$$x^n \cdot x^m = x^{n+m}, \tag{1.9}$$

kaikilla $x \in X$, $n, m \in \mathbb{N}_+ = 1, 2, 3, \ldots$. Tässä yhteenlasku yhtälön toisella puolella on tavallinen kokonaislukujen yhteenlasku. Sääntö (1.9) voidaan todistaa esimerkiksi induktiolla luvun m suhteen (jätetään harjoitustehtäväksi).

Toinen potenssisääntö, joka on voimassa liitännäiselle laskutoimitukselle $\cdot$, on kaava

$$(x^n)^m = x^{nm}, \tag{1.10}$$

$x \in X$, $n, m \in \mathbb{N}_+ = 1, 2, 3, \ldots$. Tässä yhtälön toisella puolella esiintyvä tulo nm tarkoittaa tavallista kokonaislukujen kertolaskua. Tämänkin säännön todistus jätetään harjoitustehtäväksi.

Oletetaan, että liitännäisellä laskutoimituksella $\cdot$ on neutraalialkio e. Tällöin jokaiselle $x \in X$ määritellään myös *nollas* potenssi asettamalla $x^0 = e$. Motivaationa tällaiselle määritelmälle on se tosiasia, että tällöin potenssisäännöt (1.9) ja (1.10) pätevät myös kun $n = 0$ tai $m = 0$ (tarkistus harjoitustehtävänä).

Oletetaan, että liitännäisellä laskutoimituksella $\cdot$ on neutraalialkio e. Lisäksi oletetaan, että jollakin $x \in X$ on olemassa käänteisalkio x^{-1}. Tällöin x^n määritellään myös kun $n \in \mathbb{Z}$ on *negatiivinen*, asettamalla (kun $n < 0$)

$$x^n = (x^{-1})^{-n}.$$

Tämänkin säännön motivaationa ovat potenssisäännöt (1.9) ja (1.10), jotka pysyvät tällöin voimassa myös negatiivisilla kokonaislukujen n, m arvoilla (tarkistus harjoitustehtävänä).

Alkion potensseista puhutaan, ja merkintää x^n käytetään, silloin kun laskutoimituksen merkintätapa on multiplikatiivinen. Jos laskutoimituksen + merkintätapa on additiivinen, puhutaan potenssin sijaan x:n **monikerroista**, joita merkitään symbolisesti nx. Induktiivinen määritelmä on tällöin

$$1 \cdot x = 1x = x,$$

$$(n+1)x = nx + x.$$

Havainnollisesti tällöin

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ kpl}}$$

Jos liitännäisellä laskutoimituksella + on nolla-alkio $0 = 0_X$, asetetaan jokaisella $x \in X$

$$0x = 0_X.$$

Huomaa, että tässä vasemmalla puolella symboli 0 tarkoittaa ”tavallista” kokonaislukua nolla eli joukon $\mathbb{Z}$ alkiota, kun taas 0_X oikealla puolella on laskutoimituksen + nolla-alkio. Juuri välttäkseen sekannusta symbolin 0 kahden merkityksen välillä, olemme tässä yhteydessä hetkellisesti käyttäneet joukon X abstraktille nolla-alkiolle merkintää 0_X, eikä pelkkää 0. Tällaiset tilanteet, joissa eri asiolle saatetaan käyttää samaa merkintää, ovat matematiikassa varsin yleisiä. Yleensä on pyrittävää välttää tällaista ”tupla-notaatiota”, esimerkiksi samalla tavalla jota olemme juuri käyttäneet. Tämä ei ole kuitenkaan aina mahdollista, mistä syystä on myös opittavaa ymmärtämään symbolien merkitykset kontekstista riippuen.

Jos liitännäisellä laskutoimituksella + on nolla-alkio 0, ja jollakin alkiolla $x \in X$ on olemassa vasta-alkio $-x$ laskutoimtuksen + suhteen, voidaan alkiolla x määritellä myös monikerrat nx negatiivisilla kokonaisluvuilla n, kaavalla

$$nx = (-n)(-x).$$

Potenssisäännöt (1.9) ja (1.10) muuttuvat additiivisessa merkintätavassa *monikertasäännöiksi*

$$(n+m)x = nx + mx, \tag{1.11}$$

$$n(mx) = (nm)x. \tag{1.12}$$

Nämä säännät on helppo muistaa, sillä ensimmäinen ”näyttää osittelulailta” ja toinen ”näyttää kertolaskun liitännäisyydeltä”. Täytyy kuitenkin ymmärtää, että kyseessä ei ole välttämättä minkään joukon X laskutoimituksiin liityvistä säännöistä, sillä kaavoissa esiintyvät alkiot otetaan eri joukoista - n ja m ovat kokonaislukuja, kun taas x on abstraktin joukon X alkio. Myös laskutoimitukset, jotka esiintyvät molemman yhtälön (1.11) ja (1.12) kahdella puolella ovat erilaisia laskutoimituksia, vaikka niitä merkitäänkin samalla tavalla. Nimittäin, yhtälössä (1.11) symboli + vasemmalla puolella tarkoittaa *kokonaislukujen yhteenlaskua*, kun taas yhtälön toisella puolella sama symboli tarkoittaakin joukon X laskutoimitusta. Samalla tavalla yhtälössä 1.12 esiintyviä ”kertolaskuja” täytyy tulkita oikein, esimerkiksi yhtälön vasemmalla puolella ”tulo” mx tarkoittaa monikerran

ottamista joukossa X, samoin $n(mx)$ on alkion mx n's monikerta ja $(nm)x$ on alkion x nm's monikerta. Yhtälön toisella puolella esiintyvä tulo nm on taas "tavallinen" kokonaislukujen kertolasku (tosin sekin voidaan tulkita monikerraksi yllä annetun määritelmän mielessä, miksi?).

1.2. Ryhmät

Olkoon $\cdot$ joukossa G määritelty laskutoimitus. Paria $(G, \cdot)$ sanotaan *ryhmäksi* jos laskutoimitus $\cdot$ on liitännäinen, sillä on neutraalialkio e ja jokaisella joukon G alkiolla $g \in G$ on käänteisalkio g^{-1} laskutoimituksen $\cdot$ suhteen.

Jos ryhmän G laskutoimitus on vaihdannainen, ryhmää sanotaan **Abelin ryhmäksi**. Abelin ryhmän laskutoimitusta on tapana merkitä yleisesti additiivisesti eli symbolilla $+$, paitsi tietysti silloin kun laskutoimitukselle on jostakin syystä sovittu toinen merkintätapa. Esimerkiksi nollasta eroavat reaaliluvut muodostavat Abelin ryhmän reaalilukujen kertolaskun $\cdot$ suhteen, mutta olisi hullua merkitä tästä syystä reaalilukujen kertolaskua symbolilla $+$, koska tämä on jo varattu reaalilukujen kohdalla tarkoittamaan lukujen yhteenlaskua.

Kuten yleensäkin additiivisen merkinnän tapauksessa on tapana, jos Abelin ryhmän G laskutoimituksen symbolina käytetään merkintää $+$, ryhmän neutraalialkio merkitään symbolilla 0 ja sanotaan ryhmän nolla-alkioksi. Lisäksi alkion $g \in G$ käänteisalkioita sanotaan tällöin sen vasta-alkioiksi ja sitä merkitään $-g$. Lisäksi addiivisen merkintätavan tapauksessa Abelin ryhmässä voidaan määritellä *vähennyslaskutoimitus*. Täsmällisesti se määritellään seuraavasti. Olkoon $(G, +)$ Abelin ryhmä ja olkoot $x, y \in G$. Tällöin asetetaan

$$x - y = x + (-y),$$

missä $-y$ on alkion y vasta-alkio Abelin ryhmässä G.

Esimerkkejä 1.13.

(1) Lukujen yhteenlasku $+$ luonnollisten lukujen joukossa $\mathbb{N} = \{0, 1, \ldots\}$ on liitännäinen operaatio ja sillä on neutraalialkio 0. Pari $(\mathbb{N}, +)$ ei ole kuitenkaan ryhmä, sillä sen alkioilla (nollaa lukuunottamatta) ei ole $\mathbb{N}$:ssä vasta-alkioita.

Lisämällä joukkoon negatiivisia kokonaislukuja, eli tarkastelemalla yhteenlaskua kokonaislukujen joukossa $\mathbb{Z}$ saadaan kokonaislukujen Abelin ryhmä $(\mathbb{Z}, +)$.

Muita tuttuja esimerkkejä Abelin ryhmistä ovat rationaalilukujen Abelin ryhmä $(\mathbb{Q}, +)$ ja reaalilukujen Abelin ryhmä $(\mathbb{R}, +)$.

(2) Olkoon $\cdot$ reaalilukujen kertolasku. Tällöin pari $(\mathbb{R}, \cdot)$ **ei ole** *ryhmä, koska nollalla ei ole käänteisalkiota kertolaskun suhteen. Tämä johtuu siitä, että nollan käänteisluvulle $x = 0^{-1}$ pitäisi määritelmän mukaan päteä $0x = 1$. Kuitenkin $0x = 0 \neq 1$ kaikilla reaaliluvuilla x.*

(3) Edellisessä esimerkissä nolla on ainoa "ongelmakohta", sillä muilla reaaliluvuilla on käänteisluku kertolaskun suhteen. Tästä syystä on luonnollista tarkastella kertolaskun laskutoimitusta nollasta eroavien reaalilukujen muodostamassa joukossa $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Tämä laskutoimitus on hyvin määritelty, sillä kahden nollasta eroavan reaaliluvun tulo on myös nollasta eroava luku.

Pari $(\mathbb{R}^*, \cdot)$ *on Abelin ryhmä. Tämä on esimerkki tilanteesta, jossa Abelin ryhmässä* **ei** *ole järkevää käyttää additiivista merkintätapaa. Vaikka tämän ryhmän kertolasku on vaihdannainen, sen kohdalla puhutaan edelleenkin neutraalialkiosta (joka on tässä tapauksessa reaaliluku* 1*) ja alkioiden käänteisalkioista.*

Esimerkki 1.14. *Olkoon* X *mielivaltainen joukko ja tarkastellaan joukossa* X^X *määriteltyä kuvausten yhdistämisoperaatiota* $\circ$ *. Jos joukossa* X *on ainakin kaksi alkiota, on olemassa kuvauksia* $X \to X$ *jotka eivät ole bijektioita (HT). Koska bijektiot* $f\colon X \to X$ *ovat ainoat kuvaukset joukossa* X^X*, joilla ylipäätän voi olla käänteisalkioita (kts. esimerkki 1.6, 2), pari* $(X^X, \circ)$ *ei tällöin voi olla ryhmä. Saadaksemme ryhmän meidän on rajoitettava tarkastelu pelkästään bijektioihin. Tästä syystä määritellään niin sanottu* X*:n* permutaatiojoukko*,*

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

eli kaikkien bijektioiden $f\colon X \to X$ *muodostama joukko.*

Jos $g, f \in \mathrm{Perm}(X)$*, myös yhdistetty kuvaus* $g \circ f\colon X \to X$ *on bijektio, eli myös joukon* $\mathrm{Perm}(X)$ *alkio. Näin ollen* $\circ$ *on hyvin määritelty laskutoimitus joukossa* $\mathrm{Perm}(X)$*. Tämä laskutoimitus on liitännäinen, sillä kuvausten yhdistämisen tiedetään olevan liitännäinen operaatio. Identtinen kuvaus* $\mathrm{id}\colon X \to X$ *on bijektio ja toimii tämän laskutoimituksen neutraalialkiona. Viimeiseksi huomataan, että jokaisella bijektiolla* $f\colon X \to X$ *on käänteiskuvaus* $f^{-1}\colon X \to X$*, joka on myös bijektio. Tämä kuvaus on käänteisalkio laskutoimituksen* $\circ$ *suhteen. Näin ollen* $(\mathrm{Perm}(X), \circ)$ *on ryhmä. Helposti nähdään (HT), että jos joukossa* X *on vähintään* 3 *alkiota, tämä ryhmä ei ole vaihdannainen.*

Lemmasta 1.7 saadaan ryhmän tapauksessa seuraava tulos.

Lemma 1.15. *Olkoon* $(G, \cdot)$ *ryhmä ja olkoot* $x, y \in G$*. Tällöin*

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Lemmasta 1.8 seuraa, että ryhmässä lineaarisilla yhtälöillä on aina yksikäsitteinen ratkaisu.

Lemma 1.16. *Olkoon* $(G, \cdot)$ *ryhmä. Olkoot* $a, b \in G$*. Tällöin lineaarisella yhtälöllä* $ax = b$ *on ryhmässä* G *yksikäsitteinen ratkaisu* $x = a^{-1}b$ *ja lineaarisella yhtälöllä* $xa = b$ *on ryhmässä* G *yksikäsitteinen ratkaisu* $x = ba^{-1}$*.*

Esimerkissä (1.14) yllä olemme muodostaneet ryhmän rajoittamalla tarkastelun joukon käänteisalkioiden muodostamaan osajoukkoon. Samalla tavalla meneteltiin myös esimerkissä (1.13), jossa paljastui, että kertolaskun suhteen kääntyvät reaaliluvut muodostavat ryhmän. Osoittautuu, että samanlainen temppu onnistuu mille tahansa liitännäiselle laskutoimitukselle, jolla on neutraalialkio.

Lemma 1.17. *Oletetaan, että* $\cdot$ *on joukossa* X *määritelty liitännäinen laskutoimitus, jolla on neutraalialkio* $e \in X$*. Olkoon*

$$X^* = \{x \in X \mid x \text{ on kääntyvä laskutoimituksen } \cdot \text{ suhteen}\}.$$

Tällöin laskutoimituksen $\cdot$ rajoittuma *joukkoon* $X^* \times X^*$ *on hyvinmääritelty laskutoimitus joukossa* X^**. Lisäksi* $(X^*, \cdot)$ *on tällöin ryhmä.*

Todistus. Ensin on osoitettava, että laskutoimitus $\cdot$ on hyvinmääritelty osajoukossa X^*, toisin sanoen, että aina kun $x, y \in X^*$ myös $xy \in X^*$. Mutta tämähän on osoitettu Lemmassa 1.7.

Seuraavaksi tarkistetaan, että pari $(X^*, \cdot)$ on todellakin ryhmä. Olkoot $x, y, z \in X^*$. Tällöin

$$(xy)z = x(yz),$$

koska laskutoimitus $\cdot$ on liitännäinen jopa isomassa joukossa X. Näin ollen se myös pysyy liitännäisenä pienemmässä osajoukossa X^*.

Neutraalialkio $e \in X$ on kääntyvä, sillä $ee = e$, joten $e^{-1} = e$. Näin ollen $e \in X^*$. Koska jokaisella $x \in X^*$ pätee $ex = xe = x$, e on neutraalialkio myös joukossa X^*.

Lopuksi on vielä tarkistettavaa, että jokaisella $x \in X^*$ on joukossa X^* käänteisalkio laskutoimituksen $\cdot$ suhteen. Olkoon $y = x^{-1} \in X$, joka on olemassa, koska $x \in X^*$. Tällöin $xy = yx = e$ käänteisalkion määritelmän mukaan. Tämä ei kuitenkaan vielä riittää, koska emme tiedä, kuuluuko alkio y joukkoon X^*. Kuitenkin, koska $xy = yx = e$, x toteuttaa y:n käänteisalkion määritelmää. Erityisesti y on kääntyvä eli on joukon X^* alkio. Näin ollen jokaisella $x \in X^*$ on joukossa X^* käänteisalkio laskutoimituksen $\cdot$ suhteen (sama käänteisalkio, joka sillä on isommassa joukossa X). □

Esimerkkejä 1.18. *(1) Soveltamalla edellisen Lemman tulosta reaalilukujen joukossa $\mathbb{R}$ määriteltyyn kertolaskuoperaatioon, saadaan ryhmä $(\mathbb{R}^*, \cdot)$, kuten esimerkissä (1.13.3). Soveltemalla tulosta joukossa X^X määriteltyyn kuvausten yhdistämisoperaatioon $\circ$, saadaan permutaatioryhmä* $(\mathrm{Perm}(X), \circ)$*, kuten esimerkissä (1.14).*

(2) Tarkastellaan kertolaskua kokonaislukujen joukossa $\mathbb{Z}$. Ainoat alkiot, jotka ovat $\mathbb{Z}$:ssä kääntyviä kertolaskun suhteen ovat luvut 1 *ja* -1*. Edellisen Lemman nojalla tästä seuraa, että on olemassa kahden alkion ryhmä $(\{1, -1\}, \cdot)$. Abstraktisti ajatelleen tämä ryhmä koostuu neutraalialkiosta e (alkio* 1*) ja toisesta alkiosta x (alkio* -1*), jolle pätee $x^2 = e$.*

(3) Luonnollisten lukujen joukossa $\mathbb{N}$ ainoa yhteenlaskun suhteen kääntyvä alkio on 0*. Näin ollen edellisen Lemman antama ryhmä $(\mathbb{N}^*, +)$ on niin sanottu* triviaali ryhmä*, joka koostuu tasan yhdestä alkiosta.*

Ryhmien teoria muodostaa tärkeän perustan nykyalgebralle. Törmäämme ryhmiin silloin tällöin myös tälläkin kurssilla, esimerkiksi $(n \times n)$-kokoisten kääntyvien neliömatriisien joukko muodostaa ryhmän matriisien kertolaskun suhteen. Meidän kannalta kuitenkin tärkeämpiä algebrallia otuksia ovat *renkaat* ja erityisesti *kunnat*, sillä vektoriavaruuksien ja modulien teoria perustuu, ainakin osittain, niihin.

1.3. Renkaat

Usein joudutaan tilanteeseen, jossa samassa joukossa X määritellään ja tarkastellaan samanaikaisesti kahta (tai jopa enemmänkin) algebrallista operaatiota kerrallaan. Esimerkiksi reaalilukujen joukossa lukuja voidaan sekä laskea yhteen että kertoa lukuja keskenään. Tällöin on pakko ottaa näille laskutoimituksille käyttöön erilaisia merkintätapoja ja varsin tavallista on, että tällaisessa tilanteessa toista laskutoimitusta merkitään additiivisesti symbolilla $+$ ja toista laskutoimitusta merkitään multiplikatiivisesti symbolilla

$\cdot$. Tämä merkintätapa luonnollisesti johtaa myös siihen, että laskutoimitusta $+$ tällöin sanotaan joukon X *yhteenlaskuksi* ja laskutoimitusta $\cdot$ sanotaan joukon X *kertolaskuksi*. Yleensä lisäksi tehdään implisiittisesti oletus, että monimutkaisissa lausekkeissa kertolaskulla on *prioreteetti* yhteenlaskun nähden. Toisin sanoen esimerkiksi lauseke $a + bc$ ymmärretään tarkoittavan "ensin muodostetaan tulo $bc = d$ ja sen jälkeen lasketaan summa $a + d$". Jos haluaa muodostaa lausekkeen, joka tarkottaa "lasketaan yhteen a ja b ja sitten kerrotaan näin saatu summa $a+b$ alkiolla c oikealta", on käytettävää sulkuja - $(a+b)c$.

Kahden operaation läsnäollessa voimme tarkastella sellaisia algebrallisia ominaisuuksia, jotka *sitovat* erilaisia laskutomituksia yhteen. Oletetaan, että $+$ ja $\cdot$ ovat joukossa X määriteltyjä laskutoimituksia. Sanomme, että laskutoimitus $\cdot$ *on ositteleva vasemmalta* laskutoimituksen $+$ suhteen, jos kaikilla $a, b, c \in X$ pätee niin sanottu *vasemmanpuoleinen* osittelulaki

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

Vastaavasti laskutoimitus $\cdot$ *on ositteleva oikealta* laskutoimituksen $+$ suhteen, jos kaikilla $a, b, c \in X$ pätee niin sanottu *oikeanpuoleinen* osittelulaki

$$(a + b)c = ac + bc.$$

Jos laskutoimitus $\cdot$ on ositteleva sekä vasemmalta, että oikealta laskutoimituksen $+$ suhteen, sanotaan yksinkertaisesti, että laskutoimitus $\cdot$ on ositteleva laskutoimituksen $+$ suhteen.

Esimerkki 1.19. *Reaalilukujen kertolasku on tunnetusti ositteleva reaalilukujen yhteelaskun suhteen. Jos yhteen- ja kertolaskun rooleja vaihdetaan, huomataan, että reaalilukuyhteenlasku ei ole ositteleva kertolaskun suhteen. Esimerkiksi vasemmanpuoleinen osittelulaki tällöin tarkoittaisi, että yhtälö*

$$a + bc = (a + b)(a + c),$$

pätisi kaikilla reaaliluvuilla a, b, c, mikä ei tietystikään ole totta.

Esimerkki 1.20. *Olkoon $X = \mathbb{R}^{\mathbb{R}}$ kaikkien kuvausten $f\colon \mathbb{R} \to \mathbb{R}$ muodostama joukko. Määritellään tässä joukossa* pisteittäinen yhteenlaskuoperaatio $+$ *seuraavasti. Olkoot $f, g\colon \mathbb{R} \to \mathbb{R}$ ja olkoon $x \in \mathbb{R}$ mielivaltainen. Tällöin asetetaan*

$$(f + g)(x) = f(x) + g(x).$$

Tämä sääntö määrittelee kuvauksen $f + g\colon \mathbb{R} \to \mathbb{R}$.

Joukossa X on olemassa myös toinen laskutoimitus, nimittäin kuvausten yhdistäminen $\circ$. Tutkitaan onko operaatio $\circ$ ositteleva yhteenlaskun $+$ suhteen joukossa X vasemmalta tai oikealta. Olkoot $f, g, h\colon \mathbb{R} \to \mathbb{R}$ ja olkoon $x \in X$ mielivaltainen. Tällöin

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

kun taas

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

Näin ollen vasemmanpuoleinen osittelulaki $f \circ (g + h) = f \circ g + f \circ h$ pätee funktioille f, g, h jos ja vain jos jokaisella $x \in X$ pätee

$$f(g(x) + h(x)) = f(g(x)) + f(h(x)).$$

Valitsemalla esimerkiksi f:ksi vakiokuvaus $f(x) = 1$,$x \in \mathbb{R}$ ja funktioiksi g, h mielivaltaisia funktioita $\mathbb{R} \to \mathbb{R}$, nähdään, että ehto ei päde, sillä $1 \neq 1 + 1 = 2$. Näin ollen $\circ$ ei ole ositteleva laskutoimituksen $+$ suhteen vasemmalta.

Operaatio $\circ$ on kuitenkin ositteleva laskutoimituksen $+$suhteen oikealta, eli kaikilla $f, g, h \in X$ pätee

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

Nimittäin olkoon $x \in \mathbb{R}$ mielivaltainen. Tällöin

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

Koska funktioilla $(f + g) \circ h$ ja $f \circ h + g \circ h$ on sama arvo jokaisella $x \in \mathbb{R}$, funktiot ovat samat.

Määritelmä 1.21. *Olkoon R joukko, jossa on määritelty kaksi laskutoimitusta, yhteenlasku $+$ ja kertolasku $\cdot$. Kolmikko $(R, +, \cdot)$ on* rengas, *jos seuraavat ehdot pätevät.*

A(i) *Kaikilla $x, y \in R$ pätee $x + y = y + x$ (yhteenlaskun vaihdannaisuus).*

A(ii) *Kaikilla $x, y, z \in R$ pätee $(x + y) + z = x + (y + z)$ (yhteenlaskun liitännäisyys).*

A(iii) *On olemassa alkio $0 \in R$ siten, että kaikilla $x \in R$ pätee $x + 0 = x$ (yhteenlaskun neutraalialkion olemassaolo).*

A(iv) *Jokaisella $x \in R$ on olemassa alkio $-x \in K$ siten, että pätee $x + (-x) = 0$ (vastaalkioiden olemassaolo).*

B(i) *Kaikilla $x, y, z \in R$ pätee $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (kertolaskun liitännäisyys).*

B(ii) *On olemassa alkio $1 \in R$ siten, että kaikilla $x \in R$ pätee $x \cdot 1 = x = 1 \cdot x$ (kertolaskun neutraalialkion olemassaolo).*

C(i) *Kaikilla $x, y, z \in R$ pätee (vasemmanpuoleinen osittelulaki)*

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

C(ii) *Kaikilla $x, y, z \in R$ pätee (oikeanpuoleinen osittelulaki)*

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Rengas on siis joukko R, joka on varustettu kahdella laskutoimituksella, jotka toteuttavat määritelmässä mainitut ehdot A(i)-(iv)(yhteenlaskun ominaisuudet), B(i)-(ii) (kertolaskun ominaisuudet) ja C(i)-(ii) (osittelulait, ainoat ehdot jotka koskevat molempaa laskutoimitusta samanaikaisesti). Vaikka formaalisti määritelmän mukaan rengas ei

ole joukko R, vaan "systeemi" $(R, +, \cdot)$, jonka muodostavat joukko R ja sen kaksi laskutoimitusta, käytännössä usein puhutaan yksinkertaisesti lyhyesti "renkaasta R". Tällöin ajatellaan, että laskutoimituksia joko oletetaan olevan olemassa määritelmän mukaisesti, tai ne ovat muuten tunnettuja/annettuja ennestään. Tällainen sanontatapa ei ole täsmällinen, mutta hyvin yleinen käytännön syistä.

Renkaan yhteenlaskun neutraalialkiota, jonka olemassaolo posturoidaan määritelmän ehdossa A(iii) merkitään symbolilla 0 ja sanotaan renkaan *nolla-alkioksi*. Jos haluamme korostaa, että kyseessä on jonkun tietyn kunnan R nolla-alkio, se voidaan merkitä symbolilla 0_R. Huomaa, että ehdossa A(iii) nolla-alkiosta vaaditaan ainoastaan, että yhtälö $x + 0 = x$ toteuttuisi kaikilla $x \in R$, vaikka neutraalialkion määritelmän mukaan pitäisi vielä vaatia, että pätisi myös yhtälö $0 + x = x$. Tämä ei kuitenkaan ole tarpeellista, koska ehdon A(i) nojalla renkaan yhteenlasku oletetaan olevan vaihdannainen, jolloin ehto $x + 0 = x$ implikoi, että myös yhtälö $0 + x = x$ on totta. Samasta syystä vasta-alkion olemassaoloa koskevassa ehdossa A(iv) riittää, että vasta-alkio toteuttaa ehdon $x+(-x) = 0$, sillä vaihdannaisuuden nojalla tämä on sama asia kuin $(-x)+x = 0$. Yhdessä ehdot A(i)-(iv) tarkoittavat yksinkertaisesti sitä, että pari $(R, +)$ on Abelin ryhmä.

Sen sijaan renkaan kertolaskuoperaatiota *ei yleisesti ottaen* oleteta vaihdannaiseksi. Tästä syystä aksioomissa B(ii) kertolaskun neutraalialkiosta vaaditaan molemmat yhtälöt $x1 = x$ ja $1x = x$. Renkaan kertolaskun neutraalialkiota 1 sanotaan renkaan *ykkösalkioksi*. Sillekin voidaan tarvittaessa käyttää merkintää 1_R, jos haluaa jossakin kontekstissa korostaa, että kyseessä on nimenomaan jonkun tietyn renkaan R ykkösalkio.

Jos renkaan kertolasku saattuu olemaan myös *vaihdannainen*, sanotaan koko rengasta *vaihdannaiseksi renkaaksi*. Vaihdannaisen renkaan tapauksessa riittää olettaa kahdesta osittelulaista C(i) ja C(ii) vain toisen olevan voimassa, sillä tällöin toinen on myös voimassa. Myös yksikköalkiolle riittää olettaa määritelmässä ehto $x1 = x$, sillä tällöin myös ehto $1x = x$ on automaattisesti voimassa.

Esimerkkejä 1.22. *1. Olkoot $+$ ja $\cdot$ "tavalliset" reaalilukujen yhteen- ja kertolaskuoperaatiot. Kolmikko $(\mathbb{N}, +, \cdot)$ (luonnollisten lukujen joukko näillä laskutoimituksilla varustettuna) ei ole rengas. Se toteuttaa kaikki renkaan määritelmän ehdot, lukuunottamatta ehtoa A(iv) - nollasta eroavalla luonnollisella luvulla ei ole vasta-lukua, joka olisi myös luonnollinen luku. Kun tämä luonnollisten lukujen "puute" yritetään "korjata", päädytään luonnollisella tavalla kokonaislukujen käsitteseen.*

Koska kokonaislukujen joukossa $\mathbb{Z}$ jokaisella luvulla on vasta-luku, kolmikko $(\mathbb{Z}, +, \cdot)$ (kokonaislukujen joukko yhteen- ja kertolaskulla varustettuna) on rengas. Samoin rationaalilukujen joukko $\mathbb{Q}$ ja $\mathbb{R}$ yhteen- ja kertolaskuilla varustettuina ovat renkaita.

Kaikki tässä esimerkissä tarkastellut renkaat ovat vaihdannaisia, sillä reaalilukujen kertolasku on tunnetusti vaihdannainen.

2. Olkoon $2\mathbb{Z}$ parillisten *kokonaislukujen muodostama joukko,*

$$2\mathbb{Z} = \{2n \mid n \in \mathbb{N}\}.$$

Tämä joukko on suljettu kokonaislukujen tavallisen yhteen- ja kertolaskun suhteen, koska kahden parillisen kokonaisluvun summa ja tulo ovat edelleenkin parillisia kokonaislukuja. Näin ollen voidaan tarkastella joukossa $2\mathbb{Z}$ määriteltyjä laskutoimi-

tuksia $+$, $\cdot$. Kolmikko $(2\mathbb{Z}, +, \cdot)$ toteuttaa kaikki renkaan määritelmän ehdot, lukuunottamatta ehtoa B(ii), sillä joukolla $2\mathbb{Z}$ ei ole neutraalialkiota kertolaskun suhteen (huomaa, että kokonauslukujen neutraalialkio 1 ei ole nyt tarkasteltavassa joukossa). Näin ollen $(2\mathbb{Z}, +, \cdot)$ ei ole rengas tämän kurssin määritelmän mukaan.

Joissakin alan lähteissä annetaan termille rengas *yleisempi määritelmä, jossa ei vaadita kertolaskun neutraalialkion olemassaoloa. Tällöin tämän kurssin määritelmän mukaisia renkaita sanotaan* ykkösellisiksi. *Tällaisen yleisemmän määritelmän mukaan $(2\mathbb{Z}, +, \cdot)$ olisi rengas, mutta ei ykkösellinen rengas. Tällä kurssilla tarkastelemme kuitenkin ainoastaan määritelmän (1.21) mukaisia renkaita, eli erityisesti vaadimme renkaassa aina ykkösalkon olemassaolon.*

3. *Lineaarialgebran peruskurssilla määritellään (reaalikertoimisille)* matriiseille *laskutoimitukset - matriisien yhteenlasku $+$ ja matriisien kertolasku $\cdot$. Nämä eivät ole kaikille matriisipareille määriteltyjä, vaan laskea yhteen saa ainoastaan samankokoisia matriisia ja tulo AB on määritelty ainoastaan silloin kun matriisissa A on saman verran sarakkeita kuin matriisissa B rivejä. Erityisesti tästä seuraa, että kiinteällä luonnollisella luvulla $n \in \mathbb{N}$ $(n \times n)$-kokoisten neliömatriisien yhteenlasku ja kertolasku ovat aina määriteltyjä. Merkitään tätä kaikkien $(n \times n)$-kokoisten (reaalikertoimisten) matriisien muodostamaa joukkoa symbolilla $M(n \times n; \mathbb{R})$. Joukossa $M(n \times n; \mathbb{R})$ on siis määritelty kaksi laskutoimitusta eli $+$ (matriisien yhteenlasku) ja $\cdot$ (matriisien kertolasku).*

   Kolmikko $(M(n \times n; \mathbb{R}), +, \cdot)$ on rengas eli toteuttaa määritelmän (1.21) kaikki ehdot. Tämä tosiasia osoitetaan lineaarialgebran peruskurssilla. Me palaamme siihen uudestaan tämän kurssin seuraavassa luvussa yleisemmässä kontekstissa.

   Renkaan $(M(n \times n; \mathbb{R}), +, \cdot)$ nolla-alkio on $(n \times n)$-kokoinen nollamatriisi *(kaikki alkiot nollia). Renkaan ykkösalkio on niin sanottu $(n \times n)$-*yksikkömatriisi I_n, *jonka* lävistäjäalkiot *ovat ykkösiä ja muut alkiot nollia. Koska matriisien kertolasku ei tunnetusti ole vaihdannainen, $(M(n \times n; \mathbb{R}), +, \cdot)$ on esimerkki ei-vaihdannaisesta renkaasta (kun $n > 1$).*

4. *Esimerkissä (1.20) yllä olemme määritelleet kuvausten $f \colon \mathbb{R} \to \mathbb{R}$ joukossa $\mathbb{R}^{\mathbb{R}}$ laskutoimitukset $+$ (pisteittäinen yhteenlasku) ja $\circ$ (kuvausten yhdistäminen). Samassa esimerkissä todettiin, että $\circ$ ei ole vasemmalta ositteleva yhteenlaskun $+$ suhteen eli ei toteutaa renkaan määritelmän ehtoa C(i). Näin ollen $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ ei ole rengas.*

   Voidaan kuitenkin osoittaa, että kolmikko $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ toteuttaa kaikki muut renkaan ehdot määritelmässä (1.21). Tämän todistus jätetään harjoitustehtäväksi.

   Olkoon Y joukon $\mathbb{R}^{\mathbb{R}}$ osajoukko, jonka muodostavat sellaiset kuvaukset $f \colon \mathbb{R} \to \mathbb{R}$, jotka toteuttavat ehdon

$$f(x + y) = f(x) + f(y)$$

   kaikilla $x, y \in \mathbb{R}$. Tällaisia kuvauksia sanotaan homomorfismeiksi *yhteenlaskun suhteen, koska ne "säilyttävät yhteenlaskun". Voidaan osoittaa, että kun $f, g \in Y$ myös $f + g$ ja $f \circ g$ ovat joukon Y alkioita. Toisin sanoen jos laskutoimitukset $+$ ja $\circ$ rajoitetaan joukkoon Y, saadaan hyvinmääritellyt algebralliset operaatiot joukossa*

Y. Kolmikko $(Y, +, \cdot)$ osoittautuu renkaaksi. Tämänkin väitteen todistus jätetään harjoitustehtäväksi.

5. *Tarkastellaan uudestaan edellisessä esimerkissä mainittua joukkoa $\mathbb{R}^{\mathbb{R}}$. Varustetaan se samalla pistettäisellä yhteenlaskuoperaatiolla $+$ kuten edellä. Kertolaskuksi $\cdot$ otetaan operaation $\circ$ sijaan* pistettäinen kertolaskuoperaatio*, joka määritellään kaavalla*

$$(f \cdot g)(x) = f(x)g(x), x \in \mathbb{R}$$

(yhtälön oikealla puolella reaalilukujen kertolasku). Tällöin kolmikko $(\mathbb{R}^{\mathbb{R}}, +, \cdot)$ on rengas.

Samanlainen temppu onnistuu itse asiassa mielivaltaiselle renkaalle seuraavassa yleisemmässä mielessä. Olkoon X mielivaltainen joukko ja olkoon $(R, +, \cdot)$ rengas. Tarkastellaan kaikkien kuvausten $f\colon X \to R$ muodostamaa joukkoa R^X,

$$R^X = \{f\colon X \to R\}.$$

Huomaa, että tässä siis X:ssä ei oleteta olevan mitään algebrallista rakenmetta. Olkoot $f, g \in R^X$. Tällöin voidaan määritellä kuvausten f ja g summakuvauksen *$f + g \in R^X$ ja* tulokuvauksen *$fg \in R^X$ pisteittäin,*

$$(f + g)(x) = f(x) + g(x),$$

$$(fg)(x) = f(x) \cdot g(x)$$

kaikilla $x \in X$. Tässä yhtälöiden toisella puolella esiintyvät renkaan R yhteen- ja kertolasku. Nämä konstruktiot määrittelevät joukossa R^X laskutoimitukset $+$ ja $\cdot$. Kolmikko $(R^X, +, \cdot)$ on rengas. Tämän väitteen verifikaatio jätetään lukijalle harjoitustehtäväksi. Esimerkiksi yhteenlaskun vaihdannaisuus osoitetaan seuraavasti. Olkoot $f, g\colon X \to R$ ja olkoon $x \in X$. Tällöin, koska yhteenlaksu renkaassa R on vaihdannainen, pätee

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x).$$

Koska tämä pätee kaikilla $x \in X$, on voimassa $f + g = g + f$ (kaksi kuvausta $X \to Y$ ovat samoja jos niillä on samat arvot kaikilla $x \in X$). Muut renkaan ehdot todistetaan samalla tavalla palauttamalla ne pisteittäin renkaan R vastaaviin ominaisuuksiin.

6. *Tarkastellaan yhden alkion joukkoa $X = \{a\}$. Ainoa mahdollisuus määritellä tässä joukossa laskutoimitukset $+$ ja $\cdot$ on asettaa $a + a = a = a \cdot a$. Kolmikko $(\{a\}, +, \cdot)$ on tällöin rengas. Tällaista yhden alion rengasta sanotaan* triviaaliksi *renkaaksi. Triviaalin renkaan ainoa alkio a on samanaikaisesti renkaan nolla-alkio ja sen ykkösalkio.*

Koulusta tiedetään, että ainakin reaalilukualueessa pätee yhtälö $0x = 0 = x0$ kaikilla $x \in \mathbb{R}$. Osoittautuu, että sama väite on tosi mielivaltaisessa renkaassa.

Lemma 1.23. *Olkoon $(R, +, \cdot)$ rengas ja olkoon $x \in R$. Tällöin*

$$0_R x = 0_R = x 0_R.$$

Todistus. Koska 0_R on yhteenlaskun neutraalialkio, erityisesti pätee $0_R + 0_R = 0_R$. Soveltamalla vasemmanpuoleista osittelulakia saadaan

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

Lisätään yhtälöön molempiin puoliin alkion $0_R x$ vasta-alkio $-0_R x$ (joka on olemassa renkaan määritelmän ehdon A(iv) nojalla). Tällöin vasta-alkion ja nolla-alkion määritelmän, sekä yhteenlaskun liitännäisyyden nojalla saadaan

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

Yhtälö $x0_R = 0_R$ osoitetaan samalla tavalla oikeanpuoleisen osittelulain avulla. □

Semifilosofinen huomautus: Edellisen Lemman todistuksessa lähdettiin liikeelle yhdestä kahdesta osittelulaista. Mistä voi keksiä, että näin pitää tehdä? Vai onko kenties muita todistustapoja? Itse asiassa oleellisesti muita todistuksia ei ole. Sen tietää siitä, että nolla-alkio 0_R on määritelty *yhteenlaskun* avulla. Ainoa mitä me tiedetään siitä on sen yhteenlaskun neutraalialkion ominaisuus. Lemman johtopäätös taas koskee ainoastaan renkaan *kertolaskua*. Koska osittelulait ovat renkaan määritelmän *ainoat* ehdot, joissa esiintyvät sekä yhteen-, että kertolasku, niitä on pakko käyttää tällöin jokaisen sellaisen väitteen todistuksessa, joka koskee sekä yhteen-, että kertolaskua.

Esimerkissä (1.22.5) yllä olemme todenneet, että *triviaalissa* yhden alkion renkaassa R nolla-alkio ja ykkösalkio yhtyvät, $0_R = 1_R$. Edellisen tuloksen avulla voidaan nyt näyttää, että ei-trivialissa renkaassa taas nolla-alkio ja ykkösalkio ovat aina eri alkiota. Nimittäin, olkoon R sellainen rengas, jossa pätee $0_R = 1_R$ ja olkoon $x \in R$. Tällöin edellisen Lemman ja ykkösalkion määritelmän nojalla pätee

$$x = x \cdot 1_R = x \cdot 0_R = 0_R.$$

Toisin sanoen renkaassa on vain yksi alkio 0_R eli rengas on triviaali.

Koska renkaan jokaisella alkiolla on ehdon A(iv) nojalla olemassa vasta-alkio, renkaassa voidaan puhua *vähennyslaskusta*, joka määritellään, kuten (additiivisesti merkittyjen) Abelin ryhmissä yleensäkin kaavalla

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

Lemma 1.24. *Olkoon $(R, +, \cdot)$ rengas ja olkoot $x, y, z \in R$. Tällöin seuraavat väitteet ovat tosia.*

(i) $(-x)y = -(xy) = x(-y)$.

(ii) $(-x)(-y) = xy$.

(iii) $x(y - z) = xy - xz$ *(vähennyslaskun vasemmanpuoleinen osittelulaki).*

(iv) $(x - y)z = xz - yz$ *(vähennyslaskun oikeanpuoleinen osittelulaki).*

Todistus. Oikeanpuoleisen osittelulain C(i), vasta-alkion määritelmän ja edellisen Lemman nojalla pätee

$$xy + (-x)y = (x + (-x))y = 0_R y = 0.$$

Vasta-alkion määritelmän nojalla tämä yhtälö implikoi, että $(-x)y$ on alkion xy vasta-alkio, eli

$$-(xy) = (-x)y.$$

Yhtälö $-(xy) = (-x)y$ osoitetaan samalla tavalla.

Soveltamalla kohdan (i) tulosta toistuvasti saadaan

$$(-x)(-y) = -(x(-y)) = -(-(xy)) = xy,$$

eli väite (ii).

Osittelulakien (iii) ja (iv) osoittaminen jätetään harjoitustehtäväksi. □

Koska renkaassa on käytössä sekä yhteen-, että kertolasku, renkaassa on luonnollista puhua alkioiden monikerroista na, potensseista a^n sekä *polynomilausekkeista*. Tarkemmin, olkoon $(R, +, \cdot)$ rengas ja olkoon $x \in R$, $a_0, \ldots, a_n \in R$, missä n on luonnollinen luku. Tällöin voidaan muodostaa polynomilauseke

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0.$$

Jos $a_0, \ldots, a_n$ ovat kiinteitä vakiota ja x käy läpi kaikki R:n alkiot, muodostuu *yhden muuttujan polynomifunktio* $f\colon R \to R$, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$. Tämä voidaan yleistää kahden, kolmen tai useamman muuttujan tapaukseen.

Vaihdannaisessa renkaassa pätevät koulusta tutut ”muistisäännöt” ja yleisemmin *binomikaava*.

Lemma 1.25. *Olkoon $(R, +, \cdot)$ vaihdannainen rengas ja olkoot $a, b \in R$. Tällöin*

$$a^2 - b^2 = (a - b)(a + b),$$

$$(a + b)^2 = a^2 + 2ab + b^2.$$

Yleisemmin jokaisella $n \in \mathbb{N}$ pätee binomikaava

$$(a + b)^n = \sum_{i+j=n} \binom{n}{i} a^i b^j.$$

Tässä

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

on binomikerroin ja indiksien i, j oletetaan saavan ei-negatiivisia kokonaislukuarvoja.

Todistus. Osittelulain ja edellisen Lemman nojalla saadaan

$$(a - b)(a + b) = a(a + b) - b(a + b) = a^2 + ab - ba - b^2.$$

Koska oletamme, että kertolasku on vaihdannainen pätee $ab = ba$, joten $ab - ba = ab - ab = 0$. Ensimäinen väite seuraa tästä. Toinen osoitetaan samalla tavalla. Binomikaava osoitetaan induktiolla luvun n suhteen, tarkka todistus sivuutetaan. □

Kertolaskun vaihdannaisuus on oleellinen edellisessä Lemmassa ja sen väitteet eivät yleisesti ottaen päde renkaissa yleisesti.

Olkoon $(R, +, \cdot)$ rengas. Määritelmän mukaan tällöin $(R, +)$ on (jopa Abelin) ryhmä. Luonnollisesti nousee kysymys siitä, voiko samanlainen väite päteä renkaan kertolaskulle, eli voiko myös $(R, \cdot)$ olla ryhmä? Osoittautuu, että vastaus on "melkein ei", eli tämä on mahdollista ainoastaan *triviaalin* yhden alkion renkaan tapauksessa. Nimittäin, jos nolla-alkiolla 0 olisi renkaassa R käänteisalkio $a = 0^{-1} \in R$, pätisi silloin määritelmän mukaan $1 = 0 \cdot a$. Kuitenkin toisaalta Lemman (1.23) nojalla renkaassa R pätee yhtälö $0 \cdot x = 0$ kaikilla $x \in R$, erityisesti $0 \cdot a = 0$. Näin ollen, nollan käänteisalkion olemassaolo renkaassa R implikoi sen, että $1_R = 0_R$. Tiedämme jo, että tämä on mahdollista ainoastaan kun R on yhden alkion triviaali rengas. Epätriviaalissa renkaassa nolla-alkiolla ei voi olla käänteisalkiota. Juuri tätä tarkoitetaan, kun sanotaan, että "nollalla ei saa jakaa".

Näin ollen, jos rengas R on epätriviaali, sen kääntyvien alkioiden joukko

$$R^* = \{x \in R \mid x \text{ on kääntyvä renkaan kertolaskun suhteen}\}$$

on R:n aito osajoukko. Se on myös epätyhjä, sillä ykkösalkio 1 on aina kääntyvä. Itse asiassa, koska renkaan kertolasku oletetaan olevan liitännäinen, Lemmasta 1.17 seuraa heti seuraava tulos.

Lemma 1.26. *Olkoon $(R, +, \cdot)$ rengas. Tällöin $(R^*, \cdot)$ on ryhmä.*

Renkaan R kääntyviä alkioita eli joukon R^* alkioita sanotaan kirjallisuudessa usein renkaan *yksikkö-alkioiksi* tai yksinkertaisesti renkaan *yksiköiksi*.

Olemme todenneet, että epätriviaalin renkaan tapauksessa nolla-alkio ei ole koskaan kääntyvä. Näin ollen parasta mitä voi tässä tapauksessa tapahtua on se, että kaikilla nollasta eroavilla alkioilla on käänteisalkio kertolaskun suhteen. Vaihdannaisia renkaita, joissa tämä ehto toteuttuu sanotaan *kunniksi*. Kunnat ovat tämän kurssin näkökulmasta tärkeimpiä algebrallisia olioita.

1.4. Kunnat

Tämän luvun alussa olemme huomanneet, että lineaaristen yhtälöryhmien ratkaisumenetelmien toimivuuden kannalta oleellisia ovat seuraavat reaalilukujen yhteen- ja kertolaskun ominaisuudet: yhteen- ja kertolaskun vaihdannaisuus ja liittännäisyys, osittelulaki, joka sitoo yhteen nämä lasutoimitukset, nolla- ja ykkösalkioiden 0 ja 1 olemassaolo sekä vasta- ja käänteislukujen olemassaolo. Nämä havainnot motivoivat *kunnan* määritelmän.

Määritelmä 1.27. *Olkoon K joukko ja olkoot $+$ ja $\cdot$ laskutoimituksia joukossa K. Kolmikko $(K, +, \cdot)$ on* kunta*, jos seuraavat ehdot pätevät.*

A(i) Kaikilla $x, y \in K$ pätee $x + y = y + x$ (yhteenlaskun vaihdannaisuus).

A(ii) Kaikilla $x, y, z \in K$ pätee $(x + y) + z = x + (y + z)$ (yhteenlaskun liitännäisyys).

A(iii) *On olemassa alkio $0 \in K$ siten, että kaikilla $x \in K$ pätee $x + 0 = x$ (yhteenlaskun neutraalialkion olemassaolo).*

A(iv) *Jokaisella $x \in K$ on olemassa $-x \in K$ siten, että pätee $x + (-x) = 0$ (vastaalkioiden olemassaolo).*

B(i) *Kaikilla $x, y \in K$ pätee $x \cdot y = y \cdot x$ (kertolaskun vaihdannaisuus).*

B(ii) *Kaikilla $x, y, z \in \mathbb{R}$ pätee $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (kertolaskun liitännäisyys).*

B(iii) *On olemassa alkio $1 \in K$, $1 \neq 0$ siten, että kaikilla $x \in K$ pätee $x \cdot 1 = x$ (kertolaskun olemassaolo).*

B(iv) *Jokaisella $x \in K$, $x \neq 0$, on olemassa alkio x^{-1} siten, että $x \cdot x^{-1} = 1$ (käänteialkioiden olemassaolo).*

C *Kaikilla $x, y, z \in K$ pätee (osittelulaki)*

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Edellisen aliluvun terminologian avulla kunta K voidaan määritellä yksinkertaisesti **vaihdannaisena ei-triviaalina renkaana, jossa jokaisella nollasta eroavalla alkiolla on käänteisalkio kertolaskun suhteen**. Koska kunta on, näin ollen, erikoistapaus (vaihdannaisesta) renkaasta, voimme käyttää sille kaikkia sopimuksia ja tuloksia, jotka ovat meille jo tuttuja edellisestä aliluvusta.

Esimerkkejä 1.28. *1. Kokonaislukujen joukko $\mathbb{Z}$ varustettuna tavallaisella lukujen yhteen- ja kertolaskulla on vaihdannainen rengas, mutta ei ole kunta. Ainoat $\mathbb{Z}$:n alkiot jotka kääntyvät $\mathbb{Z}$:ssä ovat 1 ja -1. Tämä ongelma "korjataan" ottamalla käyttöön murtolukuja. Näin päädytään rationaalilukujen joukkoon $\mathbb{Q}$.*

Kolmikko $(\mathbb{Q}, +, \cdot)$, eli rationaaliluvut yhteen-ja kertolaskulla varustettuna, muodostaa kunnan.

2. Vaikka algebran näkökulmasta rationaalilukujen systeemi muodostaa jo mainion kunnan eli on siis algebrallisesti hyvin rikas, osoittautuu, että se ei riitä analyysin *tarpeisiin. Tästä syystä $\mathbb{Q}$ laajennetaan* reaalilukujen joukkoon $\mathbb{R}$*, tämä on yksi nykymatematiikan tärkeämpiä konstruktioita. Kolmikko $(\mathbb{R}, +, \cdot)$ on kunta. Lineaarialgebran peruskurssilla tarkastellaan ainoastaan vektorivaruuksia, joiden* skalaarikunta *on $\mathbb{R}$.*

3. Vaikka reaalilukujen joukko riittää jo kehittämään esimerkiksi toimivaa differentiaali- ja integraalilaskentaa, sillä (ja oikeastaan jo rationaalilukujen kunnalla) on algebrallisia puutteita, jotka motivoivat kompleksilukujen kunnan $\mathbb{C}$ *konstruktion. Tästä puhutaan tarkemmin alaluvussa 1.5.*

Koska kunta on erikoistapaus renkaasta, kunnassa voidaan puhua vähennyslaskusta. Koska kunnassa jokaisella nollasta eroavalla alkiolla on olemassa käänteisalkio, kunnassa

on luonnollista puhua myös *jakolaskusta* ja *murtoluvusta*. Nämä määritellään seuraavasti - olkoot $a, b \in K$, missä K on kunta. Oletetaan, että $b \neq 0_K$. Tällöin asetetaan

$$a/b = \frac{a}{b} = ab^{-1}.$$

Mielivaltaisen kunnan murtolausekkeille pätevät samat laskusäännöt kuin tavalliselle murtolausekkeille reaailuvuilla. Olkoon $(K, +, \cdot)$ kunta ja olkoot $a, b, c, d \in K$, $b, d \neq 0_K$. Tällöin

$$\frac{a}{b} + \frac{c}{d} = \frac{ac + bd}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

lisäksi kun $a \neq 0_K$ on voimassa

$$\left(\frac{a}{b}\right)^{-1} = \frac{b^{-1}}{a^{-1}}.$$

Lineaariset yhtälöt kunnassa.
Lemmasta 1.8 saadaan kuntien tapauksessa seuraava tulos.

Lemma 1.29. *Olkoon $(K, +, \cdot)$ kunta. Olkoot $a, b \in K$. Tällöin (yhteenlaskun suhteen) lineaarisella yhtälöllä $x + a = b$ on renkaassa K yksikäsitteinen ratkaisu $x = b - a$.*

(Kertolaskun suhteen) lineaarisella yhtälöllä $ax = b$ on kunnassa K yksikäsitteinen ratkaisu $x = ba^{-1}$ edellyttäen, *että $a \neq 0$.*

1.5. Kompleksilukujen kunta

Algebrallisesta näkökulmasta yksi reaalilukujen kunnan ”puutteista” on se tosiasia, että kaikilla ei-triviaaleilla *polynomiyhtälöillä* $\mathbb{R}$:n yli ei ole reaalilukuratkaisuja. Polynomiyhtälö kunnassa K on yhtälö, joka on muotoa

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

missä $a_n, a_{n-1}, \ldots, a_1, a_0 \in K$ ovat annettuja vakioita, $a_n \neq 0_K$ ja x on tuntematon. Luonnollinen luku $n \geq 1$ on polynomiyhtälön *aste*.

Tunnetusti reaalilukujen joukossa jo toisen asteen polynomiyhtälöllä ei välttämättä ole ratkaisuja $\mathbb{R}$:ssä, mikä johtuu siitä, että negatiivisilla reaaliluvuilla ei ole neliöjuurta. Yksinkertaisin toisen asteen yhtälö, jolla ei ole $\mathbb{R}$:ssä ratkaisua, on yhtälö

$$x^2 + 1 = 0.$$

Kompleksilukujen konstruktion idea on siinä, että reaalilukujen joukko $\mathbb{R}$ laajennetaan, lisäämällä siihen ”kuvitteellinen” alkio i, joka on luvun (-1) neliöjuuri. Koska haluamme, että uudessa joukossa lukuja voi edelleenkin laskea yhteen ja kertoa keskenään, sen on sisällettävä myös kaikki muotoa $a + bi$ olevat ”luvut”, missä $a, b \in \mathbb{R}$. Kutsumme tällaista muotoa olevia ”lukuja” *kompleksiluvuiksi*. Oletetaan hetkellisesti, että tällaisten uusien ”kompleksilukujen” muodostama systeemi on todellakin olemassa ja siinä muotoa $a+bi$ olevia lukuja voidaan laskea yhteen ja kertoa keskenään. Lisäksi oletetaan, että näille laskutoimituksille pätevät kaikki tutut säännöt, kuten laskutoimitusten liitännäisyys,

vaihdannaisuus, osittelulaki jne. Toisin sanoen oletetaan, että kompleksiluvuilla voidaan laskea samalla tavalla kuin olemme tottuneet laskemaan reaaliluvuilla. Tällöin kahdelle uudelle kompleksiluvulle $a + bi$ ja $c + di$ pitäisi päteä

$$(a + bi) + (c + di) = (a + c) + (bi + di) = (a + c) + (b + d)i, \tag{1.30}$$

(1.31)
$$(a+bi)\cdot(c+di) = a(c+di)+bi(c+di) = ac+adi+bic+bidi = ac+(ad)i+(bc)i+bdi^2 = (ac-bd)+i(ad+bc),$$

missä viimeisessä välivaiheessa käytimme myös oletusta $i^2 = -1$. Havaitaan, että tällöin kahden muotoa $a+bi$ olevan kompleksiluvun summa ja kertolasku on sama muotoa, eli on myös kompleksiluku. Tällä havainnolla motivoituneena voidaan määritellä lausekkeiden $a + bi$, $a, b \in \mathbb{R}$, muodostamassa kompleksilukujen joukossa yhteenlasku-operaatio $+$ ja kertolasku operaatio $\cdot$ kaavoilla

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \tag{1.32}$$

$$(a + bi) \cdot (c + di) = (ac - bd) + i(ad + bc). \tag{1.33}$$

Tämän jälkeen voidaan ruveta tutkimaan, mitä algebrallisia ominaisuuksia nämä laskutoimitukset toteuttavat. Jää kuitenkin vähän epäselväksi, miten sanonta ”muotoa $a + bi$ oleva lauseke” tulkitaan, toisin sanoen mitä alkiot $a + bi$ tarkoittavat ja mistä voidaan ollaan varmoja, että ne ”ovat olemassa”. Miten kompleksiluku $a + bi$ koodatan joukko-opillisesti?

Yksi mahdollisuus on sopia, että kompleksiluku yksinkertaisesti ON formaali symbolien muodostama jono $a + bi$, missä a ja b ovat reaalilukuja. Matemaattisesti on kuitenkin tyydyttävämpää *konstruoida* kompleksilukujen joukko reaalilukujen joukon avulla joukko-opillisella konstruktiolla. On selvä, että kompleksiluku $a+bi$ määräytyy täysin kun tunnetaan reaaliluvut a ja b, tässä järjestyksessä. Tästä seuraa, että kompleksiluku $a+bi$ voidaan yhtä hyvin ajatella reaalilukujen *parina* (a, b) eli karteesisen tulon $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ alkiona.

Pidetään edellisten kappaleiden sisältö mielessä motivaationa ja annetaan puhtaalta pöytältä täysin formaali määritelmä kompleksilukujen joukolle $\mathbb{C}$ ja sen laskutoimituksille. Joukkona kompleksilukujen joukko $\mathbb{C}$ on sama kuin reaalilukuparien $(x, y), x, y \in \mathbb{R}$ muodostama joukko eli karteesinen tulo

$$\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}.$$

Geometrisesti tämä joukko mieltään usein kaksiulotteiseksi *tasoksi*. Kompleksilukujen joukko $\mathbb{C}$ siis ON meille kirjaimellisesti sama joukko kuin $\mathbb{R}^2$.

Kompleksilukujen joukossa $\mathbb{C}$ määrittelemme formaalisti laskutoimitukset $+$ ja $\cdot$ kaavoilla

$$(a, b) + (c, d) = (a + c, b + d), \tag{1.34}$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc). \tag{1.35}$$

Formaalista näkökulmasta näitä määritelmiä ei tarvitse perustella mitenkään (kuten ei määritelmiä yleensäkin), mutta tässä vaiheessa on selvää, että näiden määritelmien takana on yhtälöt (1.32) ja (1.33), joissa olemme "johtaneet" kaavat kompleksilukujen laskutoimituksille.

Propositio 1.36. *Kolmikko* $(\mathbb{C}, +, \cdot)$ *on kunta.*

Yhteenlaskun nolla-alkio on kompleksiluku $(0,0)$ *ja kompleksiluvun* (x,y) *vasta-alkio on* $(-x,-y)$.

Kertolaskun neutraalialkio on kompleksiluku $(1,0)$ *ja kompleksiluvun* $(a,b) \neq (0,0)$ *käänteisalkio kertolaskun suhteen on kompleksiluku*

$$\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right).$$

Todistus. Käydään läpi kunnan määritelmän 1.27 ehdot.

A(i). Olkoot a, b, c, d reaalilukuja. Tällöin

$$(a,b) + (c,d) = (a+c, b+d) \overset{(i)}{=} (c+a, d+b) = (c,d) + (a,b).$$

Huomaa, että kohdassa (i) olemme käyttäneet reaalilukujen yhteenlaskun vaihdannaisuutta.

A(ii)-A(iv). Nämä kohdat, sekä sen osoittaminen, että yhteenlaskun nolla-alkio on kompleksiluku $(0,0)$ ja kompleksiluvun (x,y) vasta-alkio on $(-x,-y)$ jätetään harjoitustehtäväksi.

B(i). Olkoot a, b, c, d reaalilukuja. Tällöin

$$(a,b) \cdot (c,d) = (ac-bd, ad+bc) \overset{(i)}{=} (ca-db, da+cb) = (c,d) \cdot (a,b).$$

Kohdassa (i) käytämme reaalilukujen kertolaskun vaihdannaisuutta.

B(ii). Kertolaskun liitännäisyyden tarkistus suoraan kertolaskun määritelmästä (1.35) on tylsä ja pitkä lasku, joten se jätetään lukijalle harjoitustehtäväksi. Myöhemmin esitetään matriisien teorian yhteydessä tapa ajatella kompleksilukujen kertolasku eräiden matriisien kertolaskuna. Tämä tekisi kompleksilukujen kertolaskun liitännäisyyden osoittamisesta paljon helpompaa. Asiaan palataan kurssin seuraavassa luvussa.

B(iii). Olkoon $(c,d) \in \mathbb{R}^2$ kompleksiluku. Tutkitaan millä ehdoilla tämä luku olisi kompleksilukujen kertolaskun neutraalialkio. Olkoon $(a,b) \in \mathbb{R}^2$ mielivaltainen. Jos (c,d) on kertolaskun neutraalialkio, pitäisi päteä

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

eli

$$\begin{cases} ac - bd = a, \\ bc + ad = b. \end{cases}$$

Tämä voidaan ajatella reaalikertoimisena lineaarisena yhtälöparina, jossa a ja b ovat vakioita ja c, d ovat tuntemattomia. Kerrotaan ensimmäinen yhtälö b:llä, toinen yhtälö a:llä ja vähennetään ensimmäinen yhtälö toisesta. Tällöin muuttuja c eliminoituu ja saadaan yhtälö $(a^2 + b^2)d = 0$. Tästä seuraa, että $d = 0$, paitsi jos $(a, b) = (0, 0)$. Jos taas ensimmäinen yhtälö kerrotaan a:lla, toinen kerrotaan b:llä ja yhtälöt lasketaan yhteen, saadaan

$$(a^2 + b^2)c = a^2 + b^2,$$

mistä seuraa, että $c = 1$, paitsi jos jos $(a, b) = (0, 0)$. Näin ollen, jos halutaan, että yhtälö $(a, b) \cdot (c, d) = (a, b)$ pätisi kaikilla $(a, b) \in \mathbb{C}$, on pakko olla $(c, d) = (1, 0)$. Kääntäen helposti tarkistetaan suoraan laskemalla, että $(1, 0)$ todellakin on neutraalialkio kompleksilukujen kertolaskun suhteen. Lisäksi $(1, 0) \neq (0, 0)$, missä $(0, 0)$ on yhteenlaskun neutraalialkio.

B(iv). Olkoon $(a, b) \in \mathbb{R}^2$ kompleksiluku, $(a, b) \neq 0$. Tutkitaan millä ehdoilla toinen kompleksiluku (c, d) on luvun (a, b) käänteisalkio kompleksilukujen kertolaskun suhteen. Koska tiedämme jo, että kertolaskun neutraalialkio on $(1, 0)$, tämä tarkoittaisi, että yhtälö

$$(ac - bd, ad + bc) = (a, b) \cdot (c, d) = (1, 0)$$

pätee. Tämä voidaan esittää lineaarisena yhtälöparina

$$\begin{cases} ac - bd = 1, \\ bc + ad = 0, \end{cases}$$

jossa a ja b ovat vakioita ja c, d ovat tuntemattomia. Kerrotaan ensimmäinen yhtälö b:llä, toinen yhtälö a:lla ja vähennetään ensimmäinen yhtälö toisesta. Tällöin muuttuja c eliminoituu ja saadaan yhtälö $(a^2 + b^2)d = -b$. Koska oletamme, että $(a, b) \neq (0, 0)$, eli $a^2 + b^2 \neq 0$, tästä seuraa, että

$$d = -\frac{b}{a^2 + b^2}.$$

Jos taas ensimmäinen yhtälö kerrotaan a:lla, toinen kerrotaan b:llä ja yhtälöt lasketaan yhteen, saadaan $(a^2 + b^2)c = a$, mistä seuraa, että

$$c = \frac{a}{a^2 + b^2}.$$

Näin ollen, jos halutaan, että yhtälö $(a, b) \cdot (c, d) = (1, 0)$, on pakko olla

$$(c, d) = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right).$$

Koska edelliset välivaiheet eivät ole välttämättä ekvivalentteja (esimerkiksi jos yllä a sattukin olla nolla, niin yhtälön kertominen a:llä **ei** säilytä ratkaisuja), lopussa pitäisi vielä tarkistaa, että näin löydetty käänteisluvun kandidaatti todellakin on luvun (a, b) käänteisalkio. Tämä on suora lasku, joka jätetään lukijalle.

C. Osittelulain todistus jätetään harjoitustehtäväksi. □

Vaikka formaalisti kompleksiluvut määritellään reaalilukupareina (a, b), käytännössä niitä ajatellaan ja käsitellään lausekkeina $a+bi$, missä a ja b ovat reaalilukuja ja i on niin sanottu "imaginäärinen yksikkö". Tähän merkintätapaan liittyy läheisesti myös ajatus siitä, että jokainen reaaliluku x voidaan ajatella kompleksilukuna $x + 0i$, eli kunta $\mathbb{C}$ onkin reaalilukujen kunnan $\mathbb{R}$ "laajennus". Laitetaan näitä ideoita täsmälliselle pohjalle.

Tarkastellaan kompleksilukuja, jotka ovat muotoa $(a, 0)$, eli sellaisia reaalilukupareja, joiden *toinen komponentti* on nolla. Havaitaan, että tällaisten kompleksilukjen joukko on "suljettu" kompleksilukujen laskutoimitusten suhteen, sillä kaikilla a, a' pätee (tarkista!)

$$(a, 0) + (a', 0) = (a + a', 0) \text{ ja}$$

$$(a, 0) \cdot (a', 0) = (aa', 0).$$

Lisäksi näistä yhtälöistä nähdään, että tällaisten kompleksilukujen yhteen- ja kertolaskut "näyttävät" samoilta kuin reaalilukujen yhteen- ja kertolasku. Tästä johtuen on luonnollista "samaistaa" kompleksiluku $(x, 0)$ reaaliluvun x kanssa. Tämä samastus on bijektiivinen vastavuus $(x, 0) \mapsto x$. Lisäksi se "säilyttää" molemmat laskutoimitukset. Näin ollen, voidaan ajatella jokainen muotoa $(x, 0)$ oleva kompleksiluku reaalilukuna x ja merkitäänkin sitä jatkossa yksinkertaisesti x:llä.

Seuraavaksi etsitään kompleksilukujen kunnassa $\mathbb{C}$ imaginääriyksikkö eli sellainen kompleksiluku z jolle pätee $z^2 = -1$. Tässä yhtälön oikealla puolella käytämme jo edellisessä kappaleessa tehtyä sopimusta, (-1) tarkoittaa tässä formaalisti kompleksilukua $(-1, 0)$. Merkitsemällä $z = (a, b)$ (missä $a, b \in \mathbb{R}$) nähdään, että ehto $z^2 = -1$ on yhtäpitävä ehtojen

$$(a^2 - b^2, 2ab) = (a, b)^2 = (-1, 0)$$

kanssa. Tämä on yhtäpitävä ehtojen $a^2 - b^2 = -1$ ja $2ab = 0$ kanssa. Kahden reaaliluvun tulo on nolla jos ja vain jos ainakin toinen luvuista on nolla, joten ehto $2ab = 0$ tarkoittaa sitä, että $a = 0$ tai $b = 0$. Jos $b = 0$, ensimmäisestä ehdosta tulee $a^2 = -1$, ja mikään reaaliluku a ei toteuda sitä. Näin ollen $a = 0$, jolloin $b^2 = 1$ eli $b = \pm 1$. Olemme näyttäneet, että yhtälöllä $z^2 = -1$ on kompleksilukujen kunnassa tasan kaksi ratkaisua - kompleksiluku $(0, 1)$ ja sen vasta-alkio $(0, -1)$. Imaginääriyksiköksi sovitaan virallisesti niistä ensimmäinen, määrittelemme siis $i = (0, 1)$ ja sanomme tätä kompleksilukua *imaginääriyksiköksi*.

Lemma 1.37. *Jokainen kompleksiluku $z \in \mathbb{C}$ voidaan esittää muodossa $a + bi$, missä $a, b \in \mathbb{R}$ ja $i = (0, 1)$ täsmälleen yhdellä tavalla. Tarkemmin sanottuna yhtälö $z = a + bi$ pätee jos ja vain jos $z = (a, b)$.*

Todistus. Olkoot $a, b \in \mathbb{R}$. Tällöin kompleksilukujen laskutoimitusten määritelmien nojalla

$$a + ib = (a, 0) + (0, 1) \cdot (b, 0) = (a, 0) + (0, b) = (a, b).$$

Tästä seuraa, että kompleksiluvulle z pätee $z = a + ib$ jos ja vain jos $z = (a, b)$. Tällainen esitys on yksikäsitteinen, sillä parin määritelmän mukaan pari (a, b) määräytyy yksikäsitteisesti komponenteistaan a ja b. □

Lemman nojalla voidaan tästä lähtien halutessaan unohtaa kompleksilukujen joukon esitys reaalilukujen pareina ja käyttää niille sen sijaan merkintää $a + ib$, jolle on nyt esitetty täsmällinen looginen pohja.

Kuntaa K sanotaan *algebrallisesti suljetuksi* jos jokaisella epätriviaalilla polynomiyhtälöllä

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$$

on kunnassa K ainakin yksi ratkaisu. Reaalilukujen kunta $(\mathbb{R}, +, \cdot)$ ei tunnetusti ole algebrallisesti suljettu - onhan juuri yhtälö

$$x^2 + 1 = 0$$

sellainen polynomiyhtälö, jolla ei ole ratkaisuja reaalilukujen joukossa. Tämä havainto oli alkuperäinen motivaatiomme kompleksilukujen konstruktioon. Olemme edellä osoittaneet, että kompleksilukujen kunnassa $\mathbb{C}$ yhtälöllä $x^2+1 = 0$ on jo ratkaisuja. Itse asiassa ei ole vaikeata tarkistaa (tämä sivutetaan), että kompleksikunnassa $\mathbb{C}$ jokaisella alkiolla z on olemassa neliöjuuri $w = \sqrt{z}$, eli sellainen luku, jolle pätee $w^2 = z$. Tästä puolestaan seuraa, että $\mathbb{C}$:ssä jokainen toisen asteen yhtälö $ax^2 + bx + c = 0$, $a \neq 0$, voidaan ratkaista samalla kaavalla kuin $\mathbb{R}$:ssä,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Erityisesti siis jokaisella toisen asteen polynomiyhtälöllä on ratkaisuja $\mathbb{C}$:ssä. Onko kenties kaikilla (epätriviaaleilla) polynomiyhtälöillä ratkaisu $\mathbb{C}$:ssä eli onko $\mathbb{C}$ algebrallisesti suljettu? Osoittautuu, että vastaus tähän kysymykseen on ”kyllä, on”. Tämä tärkeä tulos tunnetaan nimellä ”Algebran peruslause”. Palaamme algebran peruslauseeseen ja algebrallisesti suljettuihin kuntiin myöhemmin, kun tutkimme kurssin Luvussa 4 lineaarikuvauksia äärellisulotteisten vektoriavaruuksien välillä.

1.6. Homomorfismit ja isomorfismit

Edeltävissä alaluvuissa olemme nähneet paljon esimerkkejä erilaisilla laskutoimituksilla varustetuista joukoista - ryhmät, renkaat, kunnat. Samassa joukossa X voidaan määritellä erilaisia laskutoimituksia. Tällaista ”systeemiä”, jonka muodostavat joukko X ja jokin kokoelma $(\tau_i)_{i \in I}$ sen laskutoimituksia sanotaan yleisesti *algebralliseksi struktuuriksi*. Kaksi algebrallista struktuuria voidaan sanoa olevan *samaa tyyppiä*, jos niissä on sama määrä samantyyppisiä laskutoimituksia, jotka mahdollisesti toteuttavat joitakin lisäehtoja. Esimerkiksi, jos joukossa X on määritelty yksi laskutoimitus $\cdot$, joka on liitännäinen, jossa on neutraalialkio ja jossa jokaisella alkiolla on käänteisalkio, kyseessä on algebrallinen struktuuri $(X, \cdot)$, jonka tyyppi on *ryhmä*. Kaikki ryhmät siis voidaan ajatella kuuluvaan samaan algebrallisten struktuurien tyyppiin eli ryhmän tyyppiin. Samalla tavalla voidaan puhua renkaan $(R, +, \cdot)$ tai kunnan $(K, +, \cdot)$ tyypistä. Näissä algebrallisissa struktuureissa on kaksi laskutoimitusta.

Huomattava osa nykymatematiikkaa on juuri erilaisilla struktuureilla varustettujen joukkojen tutkimista. Esimerkiksi topologiassa tutkitaan joukkoja, joissa on määritelty

topologia eli eräs tapa ajatella tämä joukko geometriseksi olioksi. Algebrassa taas olemme kiinnostuneita algebrallisilla struktuureilla varustetuista joukoista.

Joukot ja niiden sisäiset struktuurit eivät kuitenkaan riitä yksinään. Yhtä tärkeitä ovat struktuureilla varustettujen joukkojen väliset *kuvaukset* ja muut relaatiot. Tällöin mitkä tahansa tällaisten joukkojen väliset kuvaukset eivät ole kiinnostavia, vaan tarkastelu rajoitetaan ainoastaan sellaisiin kuvauksiin, jotka ovat jossakin mielessä "*yhteensopivia*" joukkojen struktuurien kanssa. Tällaisia kuvauksia sanotaan yleisesti matematiikassa *morfismeiksi*. Esimerkiksi topologiassa luonnolliset morfismit ovat jatkuvat kuvaukset.

Mitä tämä "struktuurien yhteensopivuus" voisi tarkoittaa algebrassa, eli algebrallisilla laskutoimituksilla varustettujen joukkojen maailmassa? Tarkastellaan ensin yksinkertaista tapausta, jossa kummassakin joukossa X ja Y on määritelty yksi laskutoimitus. Merkitään joukon X laskutoimitusta symbolilla $\cdot$ ja joukon Y laskutoimitusta symbolilla $\cdot'$. Olkoon $f\colon X \to Y$ jokin joukkojen välinen *kuvaus*. Tällöin sanomme, että kuvaus f on *yhteensopiva* annettujen joukkojen X ja Y laskutoimitusten kanssa, jos kaikilla $x, x' \in X$ pätee

$$f(x \cdot x') = f(x) \cdot' f(x').$$

Myös sanontaa "*laskutoimitukset säilyttävä kuvaus*" käytetään. Jos lähtö ja maalipuolella on sama joukko X samalla laskutoimituksella $\cdot$ varustettuna, sanomme yksinkertaisesti, että $f\colon X \to X$ säilyttää laskutoimituksen $\cdot$ tai on yhteensopiva laskutoimituksen $\cdot$ kanssa.

Esimerkkejä 1.38. *(1) Olkoon $+$ tavallinen reaalilukujen yhteenlasku joukossa $\mathbb{R}$ ja olkoon $\cdot$ kompleksilukujen kertolasku joukossa $\mathbb{C}$. Määritellään kuvaus $f\colon \mathbb{R} \to \mathbb{C}$ kaavalla $f(x) = (\cos x, \sin x)$. Sinin ja kosinin yhteenlaskukaavat implikoivat tällöin, että kaikilla $x, y \in \mathbb{R}$ pätee*

$$f(x+y) = (\cos(x+y), \sin(x+y)) = (\cos x \cos y - \sin x \sin y, \sin x \cos y + \cos x \sin y) =$$

$$(\cos x, \sin x) \cdot (\cos y, \sin y) = f(x) \cdot f(y).$$

Näin ollen f on yhteensopiva tarkasteltavien laskutoimitusten kanssa.

(2) Olkoon $r \in \mathbb{R}$ kiinteä reaaliluku. Määritellään kuvaus $f\colon \mathbb{R} \to \mathbb{R}$ kaavalla $f(x) = rx$. Tällöin kaikilla $x, y \in \mathbb{R}$ pätee (kertolaskun osittelulain nojalla)

$$f(x + y) = r(x + y) = rx + ry = f(x) + f(y).$$

Näin ollen kuvaus f on yhteensopiva reaalilukujen yhteenlaskun kanssa (lähtö- ja maalipuolella nyt sama laskutoimitus).

Itse asiassa samalla tavalla nähdään, että jos $(R, +, \cdot)$ on mielivaltainen rengas ja $r \in R$, kuvaus $f\colon R \to R$, $f(x) = rx$ on yhteensopiva renkaan yhteenlaskun kanssa. Tämä johtuu (vasemmanpuoleisesta) osittelulaista.

Koska laskutoimitusten kanssa yhteensopiva kuvaus $f\colon X \to Y$ säilyttää laskutoimiksia, voisi myös odottaa, että se säilyttää laskutoimitusten ominaisuuksia, ainakin kuvajoukossaan $f(X)$. Muotoillaan ja todistetaan tämä tulos täsmällisesti meitä kiinnostavien agebrallisten ominaisuuksien kohdalla.

Lemma 1.39. *Oletetaan, että joukossa X on määritelty laskutoimitus $\cdot$ ja joukossa Y on määritelty laskutoimitus $\cdot'$. Olkoon $f\colon X \to Y$* **surjektiivinen** *kuvaus, joka on yhteensopiva laskutoimitusten $\cdot$ ja $\cdot'$ kanssa. Tällöin seuraavat väitteet pätevät*

(i) Jos laskutoimitus $\cdot$ on liitännäinen, myös laskutoimitus $\cdot'$ on liitännäinen.

(ii) Jos laskutoimitus $\cdot$ on vaihdannainen, myös laskutoimitus $\cdot'$ on vaihdannainen.

(ii) Oletetaan, että joukolla X on neutraalialkio e laskutoimituksen $\cdot$ suhteen. Tällöin $f(e)$ on joukon Y neutraalialkio laskutoimituksen $\cdot$ suhteen. Erityisesti tällöin myös joukolla Y on neutraalialkio laskutoimituksen $\cdot$ suhteen.

(v) Olkoon $x \in X$. Oletetaan, että x:llä on joukossa X käänteisalkio x^{-1} laskutoimituksen $\cdot$ suhteen. Tällöin alkiolla $y = f(x)$ on joukossa Y käänteisalkio laskutoimituksen $\cdot$ suhteen. Lisäksi tällöin pätee

$$f(x)^{-1} = f(x^{-1}).$$

Todistus. Oletetaan, että $\cdot$ on liitännäinen laskutoimitus ja osoitetaan, että $\cdot'$ on myös liitännäinen. Olkoot $y_1, y_2, y_3 \in Y$. Koska f oletetaan olevan surjektio, voidaan valita $x_1, x_2, x_3 \in X$ siten, että $f(x_i) = y_i$, $i = 1, 2, 3$. Koska $\cdot$ on liitännäinen,

$$(x_1x_2)x_3 = x_1(x_2x_3).$$

Ottamalla f yhtälön molemmasta puolesta ja käyttämällä hyväksi oletusta saadaan

$$(y_1y_2)y_3 = (f(x_1)f(x_2))f(x_3) = f(x_1x_2)f(x_3) = f((x_1x_2)x_3) =$$

$$= f(x_1(x_2x_3)) = f(x_1)f(x_2x_3) = f(x_1)(f(x_2)f(x_3)) = y_1(y_2y_3).$$

Näin ollen $\cdot'$ on liitännäinen.

Kohdan (ii) väite osoitetaan samalla tavalla.

Oletetaan, että $e \in X$ on laskutoimituksen $\cdot$ neutraalialkio. Osoitetaan, että $e' = f(e)$ on tällöin Y:ssä laskutoimituksen $\cdot'$ neutraalialkio. Olkoon $y \in Y$ mielivaltainen. Koska f on surjektio, on olemassa $x \in X$ siten, että $f(x) = y$. Oletusten nojalla

$$e'y = f(e)f(x) = f(ex) = f(x) = y,$$

samalla tavalla nähdään, että $ye' = y$.

Oletetaan, että alkiolla $x \in X$ on käänteisalkio $x^{-1} \in X$. Soveltamalla yhtälön $xx^{-1} = e$ molemmasta puolesta kuvausta f, saadaan

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e',$$

missä e' on edellisen nojalla neutraalialkio Y:ssä. Samalla tavalla näytetään, että

$$f(x^{-1})f(x) = e'.$$

□

Erityisesti ryhmät/renkaat/kunnat ”säilyvät” sujektiivisissa laskutoimituksia säilyttävissä kuvauksissa.

Seuraus 1.40. *Olkoon $(G, \cdot)$ ryhmä. Olkoon $\cdot'$ laskutoimitus joukossa G'. Oletetaan, että on olemassa* surjektiivinen *kuvaus $f\colon G \to G'$ jolle pätee*

$$f(x \cdot y) = f(x) \cdot' f(y)$$

kaikilla $x, y \in G$. Tällöin $(G', \cdot')$ on myös ryhmä.

Jos $(G, \cdot)$ on Abelin ryhmä, myös $(G', \cdot)$ on Abelin ryhmä.

Seuraus 1.41. *Olkoon $(R, +, \cdot)$ rengas. Olkoot $+', \cdot'$ laskutoimituksia joukossa R'. Oletetaan, että on olemassa* surjektiivinen *kuvaus $f\colon R \to R'$ jolle pätee*

$$f(x + y) = f(x) +' f(y).$$

$$f(x \cdot y) = f(x) \cdot' f(y).$$

Tällöin $(R', +, \cdot)$ on myös rengas.

Jos R on kommutatiivinen, myös R' on kommutatiivinen. Jos R on kunta ja R' ei ole triviaali, R' on myös kunta.

Todistus. Kaikki renkaan/kommutatiivisen renkaan/kunnan ehdot R' seuraavat Lemmasta 1.39, paitsi osittelulait. Niitä voi todistaa samalla tavalla kuin Lemmassa 1.39 on tehty muiden ehtojen kohdalla. Kunnan tapauksessa oletusta ”R' ei triviaali” tarvitaan varmistakseen, että sen ykkösalkio eroaa sen nolla-alkiosta (mikä on yksi kunnan vaatimuksista). □

Nyt voidaan palata kysymykseen, mitä ”morfismit” algebrallisten struktuurien välillä ovat. Olkoot X ja Y joukkoja, joissa molemmissa on määritelty samantyyppiset algebralliset struktuurit. Tällöin näiden struktuurien välinen **homomorfismi** on kuvaus $f\colon X \to Y$, joka on yhteensopiva kaikkien molemman struktuurin vastaavien laskutoimitusten kanssa ja lisäksi *”säilyttää struktuuriin liittyviä ehtoja”*, esimerkiksi neutraalialkiot, käänteisalkiot jne, koska tällaiset ehdot ovat osaa struktuuria. Jälleen kerran emme anna tässä mitään sen täsmällisempää formaalia määritelmää sille, mitä ”struktuuriin liityvien ehtojen säilyttäminen tarkoittaa”, vaan tyydymme sen sijaan käymään asia formaalisti läpi meitä kiinnostavien struktuurien, eli ryhmien, renkaiden ja kuntien tapauksessa.

Ryhmien tapaus.

Määritelmä 1.42. *Olkoot $(G, \cdot)$ ja $(G', \cdot')$ molemmat ryhmiä. Sanomme, että kuvaus $f\colon G \to G'$ on* ryhmien välinen homomorfismi*, jos se on yhteensopiva ryhmien G ja G' laskutoimitusten kanssa, eli jos ja vain jos kaikilla $g, h \in G$ pätee*

$$f(gh) = f(g)f(h). \tag{1.43}$$

Laskutoimitusten kanssa yhteensopivuus on siis ainoa ehto, jonka vaadimme ryhmien välisen homomorfismin virallisessa määritelmässä. Periaatteessa yleisen homomorfismin idean mukaan meidän pitäisi vielä vaatia, että f säilyttäisi neutraalialkion ja kaikkien alkioiden käänteisalkiot, eli että pätisi myös

$$f(e_G) = e_H \text{ ja } f(g^{-1}) = (f(g))^{-1} \text{ kaikilla } g \in G. \tag{1.44}$$

Tämä ei kuitenkaan ole tarpeellista, sillä osoittautuu, että ryhmien erikoistapauksessa yhtälöt (1.44) seuraavat homomorfismin määritelmästä eli ehdosta 1.43. Tämän osoittaminen jätetään harjoitustehtäväksi.

Esimerkkejä 1.45. *(1) Edellisessä esimerkissä tarkasteltu kuvaus* $f\colon (\mathbb{R},+) \to (\mathbb{C},\cdot)$, $f(x) = (\cos x, \sin x)$ *ei formaalista näkökulmasta voi olla ryhmähomomorfismi, sillä vaikka* $(\mathbb{R},+)$ *on ryhmä,* $(\mathbb{C},\cdot)$ *ei ole sellainen - nollalla ei ole käänteisalkiota kertolaskun suhteen.*

Kuitenkin, koska $\mathbb{C}$ *on kunta, Lemman 1.17 mukaan joukossa* $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$ *(kunnan* $\mathbb{C}$ *kääntyvät alkiot) voidaan määritellä samanlainen kertolasku kuin* $\mathbb{C}$*:ssä. Lisäksi saman lemman mukaan* $(\mathbb{C}^*,\cdot)$ *on tällöin ryhmä. Kuvauksen* f *määritelmästä seuraa, että* $f(x) \neq 0$ *kaikilla* $x \in \mathbb{R}$*. Näin ollen, vaihtamalla kuvauksen* f *maalijoukkoa, voidaan* f *ajatella kuvauksena* $\mathbb{R} \to \mathbb{C}^*$*. Tällöin sekä lähtö-, että maalijoukko ovat molemmat ryhmiä, ja* f *säilyttää laskutoimituksen, joten* f *on ryhmähomomorfismi.*

(2) Olkoon $(G,\cdot)$ *mikä tahansa ryhmä ja olkoon* $x \in G$ *kiinnitetty. Määritellään kuvaus* $f\colon \mathbb{Z} \to G$ *kaavalla* $f(x) = x^n$*. Tällöin potenssisääntö 1.9 implikoi, että kuvaus* f *on ryhmähomomorfismi ryhmien* $(\mathbb{Z},+)$ *ja* $(G,\cdot)$ *välillä, sillä kaikilla* $n, m \in \mathbb{Z}$ *pätee*

$$f(n+m) = x^{n+m} = x^n x^m = f(n)f(m).$$

Renkaiden tapaus.

Määritelmä 1.46. *Olkoot* $(R,+,\cdot)$ *ja* $(R',+,\cdot)$ *renkaita. Kuvausta* $f\colon R \to R'$ *sanotaan* rengashomomorfismiksi*, jos* f *on yhteensopiva sekä yhteenlaskun, että kertolaskun suhteen, eli jos kaikilla* $x, y \in R$ *pätee*

$$f(x+y) = f(x) + f(y) \text{ ja } f(xy) = f(x)f(y), \tag{1.47}$$

ja lisäksi f *säilyttää kertolaskun neutraalialkiot, eli pätee yhtälö*

$$f(1_R) = 1_{R'}. \tag{1.48}$$

Tällä kertaa vaatimus 1.48 on yleisesti ottaen tarpeellinen, sillä se ei seuraa välttämättä ehdoista 1.47, katso esimerkkejä alla. Huomaa, että Lemman 1.39 nojalla yhtälö (1.48) kyllä *seuraa* ehdoista 1.47), jos kuvaus $f\colon R \to R'$ on *surjektiivinen*.

Yhteenlaskun neutraalialkion eli nolla-alkion säilymistä ei tarvitse rengashomomorfismin määritelmässä vaatia erikseen, sillä $(R,+)$ on ryhmä ja rengashomomorfismi $f\colon R \to R'$ on erityisesti myös ryhmien $(R,+)$ ja $(R',+)$ ryhmähomomorfismi, joten (kts. yllä) se säilyttää yhteenlaskun neutraalialkion.

Kuntien tapaus

Olkoot $(K,+,\cdot)$ ja $(K',+,\cdot)$ kuntia. Koska kunta on erikoistapaus renkaasta, määritelemme yksinkertaisesti, että kuvaus $f\colon K \to K'$ on *kuntahomomorfismi*, jos ja vain jos se on rengashomomorfismi renkaiden $(K,+,\cdot)$ ja $(K',+,\cdot)$ välillä. Mitään muuta ei tällöin tarvitse vaatia, sillä näin määriteltynä kuntahomorfismi tällöin säilyttää yhteen- ja kertolaskun neutraalialkiot. Lisäksi voidaan osoittaa, että tällöin kaikille $x \neq 0$ pätee

$$f(x^{-1}) = (f(x))^{-1}.$$

Viimeisen väitteen todistaminen jätetään lukijalle harjoitustehtäväksi.

Esimerkkejä 1.49. *(1) Edellisessä aliluvussa olemme kompleksilukujen konstruktion yhteydessä sovinneet reaaliluvun x ja kompleksiluvun $(x,0)$ "samaistamisesta". Lisäksi totesimme, että tämä samaistus "kunnioittaa laskutoimituksia". Nyt voidaan tehdä jälkimmäisestä väitteestä täsmällinen rengashomomorfismin käsitteen avulla. Edellä mainittu samastus voidaan ajatella tapahtuvan kuvauksen $f\colon \mathbb{R} \to \mathbb{C}$, $f(x) = (x,0)$ välityksellä. Kaikilla $x, y \in \mathbb{R}$ tällöin pätee*

$$f(x+y) = (x+y, 0) = (x+y, 0+0) = (x,0) + (y,0),$$

$$f(xy) = (xy, 0) = (x \cdot y - 0 \cdot 0, x \cdot 0 + 0 \cdot y) = (x,0) \cdot (y,0) = f(x) \cdot f(y).$$

Lisäksi $f(1_{\mathbb{R}}) = (1,0) = 1_{\mathbb{C}}$. Näin ollen f on esimerkki rengashomomorfismista. Koska $\mathbb{R}$ ja $\mathbb{C}$ ovat itse asiassa kuntia, kyseessä on jopa kuntahomomorfismi.

(2) Esimerkissä 1.38 olemme todenneet, että kun $(R, +, \cdot)$ on rengas ja $r \in R$ on sen kiinteä alkio, kuvaus $f\colon R \to R$, $f(x) = rx$ (eli r:llä kertominen vasemmalta) on yhteensopiva renkaan yhteenlaskun kanssa, $f(x+y) = f(x) + f(y)$. Tämä kuvaus ei yleensä kuitenkaan ole rengashomomorfismi. Ensinnäkin $f(1_R) = r$, joten f säilyttää kertolaskun neutraalialkion jos ja vain jos $r = 1_R$, jolloin $f = \mathrm{id}_R$ on joukon R identtinen kuvaus. Kuvaus f ei myöskään yleensä ole yhteensopiva renkaan kertolaskun kanssa. Esimerkiksi jos $R = \mathbb{R}$ on reaalilukujen rengas ja $r = 2$

$$f(xy) = 2xy \neq 4xy = (2x)(2y) = f(x)f(y)$$

kun $x, y \neq 0$.

(3) Oletetaan tunnetuksi, että (2×2)-kokoisten matriisien joukko $M(2\times2;\mathbb{R})$ muodostaa renkaan $(M(2\times 2;\mathbb{R}), +, \cdot)$, kun se varustetaan matriisien yhteen- ja kertolaskulla. Määritellään kuvaus $f\colon \mathbb{Z} \to M(2\times 2;\mathbb{R})$ kaavalla

$$f(n) = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}, n \in \mathbb{Z}$$

Tällöin f säilyttää sekä yhteen-, että kertolaskun, sillä

$$f(n+m) = \begin{pmatrix} n+m & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = f(n) + f(m),$$

$$f(nm) = \begin{pmatrix} nm & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = f(n) \cdot f(m)$$

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

$$f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

ei ole matriisirenkaan $M(2\times 2;\mathbb{R})$ kertolaskun neutraalialkio. Näin ollen f ei ole rengashomomorfismi. Tämä esimerkki osoittaa myös, että oletus kuvauksen surjektiivisuudesta on tarpeellinen Lemmassa 1.39.

(4) Olkoon X joukko ja $(R, +, \cdot)$ rengas. Esimerkissä (1.22, 5) olemme todenneet, että on olemassa rengas $(R^X, +, \cdot)$, jonka alkioiden joukko R^X on kaikkien kuvausten $f\colon X \to R$ muodostama joukko ja jonka laskutoimitukset määritellään pisteittäin. Olkoon $a \in R$ mielivaltainen kiinnitetty alkio. Määritellään kuvaus $G\colon R^X \to R$ kaavalla $G(f) = f(a)$. Tällöin G on renkaiden välinen homomorfismi, sillä kaikilla $f, g \in R^X$ pätee pisteittäisten laskutoimitusten määritelmien nojalla

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

$$G(fg) = (fg)(a) = f(a) \cdot g(a) = G(f) \cdot G(g),$$

lisäksi G kuvaa kertolaskun neutraalialkio kertolaskun neutraalialkioksi (tämän tarkistus harjoitustehtävänä).

Isomorfismit

Olkoot X ja Y joukkoja, jotka ovat varustettuja samantyyppisillä algebrallisilla struktuureilla, esimerkiksi molemmat ryhmiä tai molemmat kuntia. Olkoon $f\colon X \to Y$ näiden struktuurien välinen homomorfismi. Koska f on erityisesti kuvaus, voidaan kysyä onko f mahdollisesti injektio, surjektio tai bijektio.

Bijektiivista homomorfismia $f\colon X \to Y$ sanotaan **isomorfismiksi**. Jos kahden algebrallisilla struktuureilla varustetun joukon X ja Y välillä on olemassa jokin isomorfismi $f\colon X \to Y$, sanomme, että X ja Y ovat *isomorfisia*. Tällöin merkitään $X \cong Y$. Jos halutaan korostaa, että kuvaus f on isomorfismi, käytetään sille merkintää $f\colon X \xrightarrow{\cong} Y$.

Isomorfisilla struktuureilla varustetut joukot ovat ”täysin samanlaisia” algebran näkökulmasta. Voidaan ajatella, että ne eroavat vain alkioiden nimeämiseen suhteen tai edustavat samaa abstraktia algebrallista oliota. Algebra ei pysty näkemään kahden isomorfisen struktuurin välillä mitään eroa.

Esimerkki 1.50. *Olkoon $(\mathbb{R}, +)$ reaalilukujen ryhmä yhteenlaskulla varustettuna ja olkoon $(\mathbb{R}_+, \cdot)$* positiivisten reaalilukujen *muodostama joukko reaalilukujen kertolaskulla varustettuna. Koska kahden positiivisen reaaliluvun tulo on myös positiivinen, $\cdot$ on hyvin määritelty laskutoimitus joukossa $\mathbb{R}$.*

Määritellään kuvaus $f\colon \mathbb{R} \to \mathbb{R}_+$ kaavalla $f(x) = 2^x$. Analyysistä tiedetään, että tämä kuvaus on bijektio. Lisäksi

$$f(x+y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$$

kaikilla reaaliluvuilla x, y. Näin ollen f on bijektiivinen kuvaus, joka on yhteensopiva laskutoimitusten kanssa. Koska bijektio on erityisesti surjektio, Seurauksen 1.40 nojalla $(\mathbb{R}_+, \cdot)$ on myös ryhmä. Näin ollen f on bijektiivinen ryhmien välinen homomorfismi eli ryhmien välinen isomorfismi. *Ryhmät $(\mathbb{R}, +)$ ja $(\mathbb{R}_+, \cdot)$ ovat isomorfisia. Havainnollisesti ajatelleen niillä on samanalainen algebrallinen struktuuri. Kumpaakin ryhmää voidaan pitää saman algebrallisen olion eräänä* mallina.

Koska isomorfismi $f\colon X \to Y$ on bijektio, sillä on käänteiskuvaus $f^{-1}\colon Y \to X$. Osoittautuu, että tämä käänteiskuvaus on aina myös isomorfismi. Tämä seuraa seuraavasta Lemmasta. Tässä mielessä algebra eroaa esim. topologiasta, jossa bijektiivisen "morfismin" eli bijektiivisen jatkuvan kuvauksen käänteiskuvauksen ei tarvitse olla enää jatkuva.

Lemma 1.51. *Oletetaan, että joukossa X on määritelty laskutoimitus $\cdot$ ja joukossa Y on määritelty laskutoimitus $\cdot'$. Olkoon $f\colon X \to Y$ bijektiivinen kuvaus, joka on yhteensopiva laskutoimistuen $\cdot$ ja $\cdot'$ kanssa. Tällöin kuvauksen f käänteiskuvaus $f^{-1}\colon Y \to X$ on myös bijektiivinen kuvaus, joka on yhteensopiva laskutoimisten $\cdot'$ ja $\cdot$ kanssa.*

Todistus. Olkoot $y, y' \in Y$. Tällöin, koska f on bijektio on olemassa yksikäsitteiset $x, x' \in X$ siten, että $f(x) = y$ ja $f(x') = y'$. Käänteiskuvauksen määritelmän nojalla $x = f^{-1}(y)$ ja $x' = f^{-1}(y')$. Lisäksi oletusten mukaan

$$f(x \cdot x') = f(x) \cdot' f(x') = yy',$$

mistä seuraa, että $x \cdot x' = f^{-1}(y \cdot' y')$. Näin ollen

$$f^{-1}(y \cdot' y') = x \cdot x' = f^{-1}(y) \cdot f^{-1}(y').$$

Olemme osoittaneet, että kuvaus $f^{-1}\colon Y \to X$ on yhteensopiva laskutoimisten $\cdot'$ ja $\cdot$ kanssa. □

Seuraus 1.52. *Olkoon $f\colon X \to Y$ isomorfismi ryhmien/renkaiden/kuntien X, Y välillä. Tällöin $f^{-1}\colon Y \to X$ on myös ryhmien/renkaiden/kuntien välinen isomorfismi.*

Näin ollen isomorfiarelaatio "X ja Y ovat isomorfisia" on symmetrinen - jos on olemassa isomorfismi $f\colon X \to Y$, niin on olemassa myös isomorfismi $Y \to X$ ja päinvastoin.

Koska isomorfiset struktuurit ovat "algebrallisesti samanlaisia", niillä on "samanlaisia algebrallisia ominaisuuksia", sillä isomorfismi "säilyttää" kaikki algebralliset ominaisuudet. Tätä periaatetta voi käyttää sen osoittamiseksi, että kaksi struktuuria X, Y **eivät ole** isomorfisia - tällöin riitää löytää toisessa struktuurissa jokin algebrallinen ominaisuus, joka ei ole voimassa toisessa.

Esimerkki 1.53. *Reaalilukujen kunta $\mathbb{R}$ ja kompleksilukujen kunta $\mathbb{C}$ eivät voi olla isomorfisia kuntina, koska $\mathbb{C}$:ssä luvulla -1 on neliöjuuri, mutta $\mathbb{R}$:ssä ei ole. Täsmällinen perustelu menisi seuraavasti. Jos kunnat $\mathbb{R}$ ja $\mathbb{C}$ olisi isomorfisia, olisi olemassa isomorfismi, eli bijektiivinen homomorfismi $f\colon \mathbb{C} \to \mathbb{R}$. Tällöin erityisesti $f(0) = 0$ ja $f(1) = 1$ renkaan homomorfismin määritelmän nojalla. Olkoon $i \in \mathbb{C}$ imäginääriyksikkö jolle pätee $i^2 + 1 = 0$. Soveltamalla f tämän yhtälön molemmalle puolelle saadaan*

$$f(i)^2 + 1 = f(i^2) + f(1) = f(i^2 + 1) = f(0) = 0.$$

Erityisesti on olemassa reaaliluku $r = f(i) \in \mathbb{R}$ jolle pätee $r^2 + 1 = 0$. Tämä tiedätään olevan mahdotonta. Saatu ristiriitä osoittaa sen, että kuvausta f ei voi olla olemassa.

1.7. Alistruktuurit

Olkoon X jollakin matemaattisella struktuurilla varustettu joukko ja olkoon $Y \subset X$ sen osajoukko. On kiinnostavaa tutkia määrittelekö X:n struktuuri samantyyppisen struktuurin osajoukkoon Y. Jos vastaus on myönteinen, on luonnollista sanoa Y:tä struktuurin X *alistruktuuriksi*.

Esimerkiksi tasossa $\mathbb{R}^2$ on määritelty luonnollinen geometrinen struktuuri - voimme laskea pisteiden välisiä etäisyyksiä, määritellä avoimet joukot, puhua kulmista. Jos Y on tason osajoukko, esimerkiksi kolmio tai paraabeli, tämä tason geometrinen struktuuri määrittelee, ainakin osittain, samantyyppisen struktuurin Y:hyn - voidaan ajatella myös Y geometrisena oliona.

Tällä kurssilla meitä kiinnostaa kuitenkin mitä alistruktuuri tarkoittaisi algebrassa. Aloitetaan tarkastelu taas mahdollisimman yksinkertaisestä tilanteesta. Olkoon X laskutoimituksella $\cdot$ varustettu joukko ja olkoon Y jokin joukon X osajoukko, $Y \subset X$. Sanomme, että Y on *vakaa* laskutoimituksen $\cdot$ suhteen jos kaikilla $x, y \in Y$ pätee $xy \in Y$. On selvää, että jos Y on vakaa, niin X:n laskutoimituksen $\cdot$ *rajoittuma* karteesiseen tuloon $Y \times Y$ määrittelee luonnollisella tavalla kuvauksen $\cdot\colon Y \times Y \to Y$, joka on laskutoimitus joukossa Y. Tällöin voimme puhua algebrallisesta struktuurista $(Y, \cdot)$. Jos Y ei ole vakaa laskutoimituksen $\cdot$ suhteen, tämä laskutoimitus ei määrittele mitään laskutoimitusta joukossa Y.

Termin ”vakaa” (laskutoimituksen suhteen) synonyymina käytetään myös termiä ”suljettu” (laskutoimituksen suhteen).

Esimerkki 1.54. *Tarkastellaan kokonaislukujen joukkoa $\mathbb{Z}$ varustettuna yhteenlaskulla $+$. Tällöin positiivisten kokonaislukujen osajoukko $\mathbb{N}_+ = \{1, 2, 3, \dots, \}$ on vakaa $\mathbb{Z}$:ssä. Myös ei-negatiivisten kokonaislukujen osajoukko $\mathbb{N} = \{0, 1, \dots, \}$ on vakaa $\mathbb{Z}$:ssä. Parillisten kokonaislukujen joukko on vakaa, sillä kahden parillisen luvun summa on myös parillinen. Sen sijaan parittomien kokonaislukujen summa ei itse asiassa koskaan ole pariton. Esimerkiksi $1+3 = 4$. Näin ollen parittomien kokonaislukujen joukko ei ole suljettu yhteenlaskun suhteen.*

Olkoon X jollakin algebrallisella struktuurilla varustettu joukko ja olkoon $Y \subset X$. Tällöin Y sanotaan struktuurin X *alistruktuuriksi* jos se on vakaa jokaisen X:n laskutoimituksen suhteen ja lisäksi” toteuttaa samat mahdolliset lisäehdot, jotka X toteuttaa”. Tällöin merkitään myös $Y \leq X$. Annamme alla täsmällisen määritelmän alistruktuurin käsitteille meitä kiinnostavissa tilanteissa eli ryhmien, renkaiden ja kuntien tapauksessa. Sitä ennen mietitään yleisellä tasolla mitä ”laskutoimituksen ominaisuuksien periytyyvyys osajoukkoon” tarkoittaa.

Sellaiset ominaisuudet kuin laskutoimitusten *liitännäisyys*, *vaihdannaisuus* tai *osittelulaki* ”periytyvät” automaattisesti X:n vakaisiin osajoukkoihin. Tämä on melkein itsestään selvä, joten emme anna tälle väitteelle mitään todistusta. Kuittaamme tämän tuloksen kuitenkin virallisena Lemmana selkeyden vuoksi.

Lemma 1.55. *Olkoon $\cdot$ joukossa X määritelty laskutoimitus ja olkoon $Y \subset X$ vakaa laskutoimituksen $\cdot$ suhteen. Tällöin seuraavat ehdot pätevät*

- *Jos $\cdot$ on liitännäinen X:ssä, se on liitännäinen myös Y:ssä.*

- *Jos $\cdot$ on vaihdannainen X:ssä, se on vaihdannainen myös Y:ssä.*

Oletetaan, että joukossa X on määritelty laskutoimitukset $+$, $\cdot$ ja olkoon $Y \subset X$ vakaa laskutoimitusten $+$ ja $\cdot$ suhteen. Tällöin jos $\cdot$ on ositteleva laskutoimituksen $+$ suhteen X:ssä, se on myös ositteleva $+$:n suhteen Y:ssä.

Sen sijaan erilaiset "olemassaolo"-ominaisuudet, kuten neutraalialkion tai vasta/käänteisalkioiden olemassaolo eivät välttämättä "periydy" vakaisiin osajoukkoihin. Esimerkiksi parillisten kokonaislukujen joukko $2\mathbb{Z}$ on vakaa reaaliukujen kertolaskun suhteen, mutta sillä ei ole tämän laskutoimituksen suhteen neutraalialkiota, vaikka $\mathbb{R}$:ssä sellainen on olemassa (luku 1). Myös jokaisella joukon $2\mathbb{Z}$ nollasta eroavalla alkiolla on $\mathbb{R}$:ssä olemassa käänteisalkio kertolaskun suhteen, mutta ei $2\mathbb{Z}$:ssä. On hyvin selvä mistä nämä ongelmat johtuvat - $\mathbb{R}$:n kertolaskun neutraalialkio 1 ei ole joukon $2\mathbb{Z}$ alkio, samoin jokaisen joukon $2\mathbb{Z}$ alkion $2n$ käänteisalkio $1/2n$ ei yksinkertaisesti ole enää joukon $2\mathbb{Z}$ alkio.

Joskus voi käydä myös niinkin, että joukolla X ja sen vakaalla osajoukolla Y on jonkun laskutoimituksen suhteen olemassa neutraalialkiot $e \in X$ ja $e' \in Y$, mutta ne eivät ole samoja, $e \neq e'$. Tällöin Y:tä **ei lasketa** X:n alistruktuuriksi, vaikka se olisikin "samaa tyyppiä". Samoin alistruktuurissa on oltava samat vasta/käänteisalkiot kuin isommassa struktuurissa jne.

Esimerkki 1.56. *Olkoon $M(2 \times 2; \mathbb{R})$ kaikkien (reaalikertoimisten) (2×2)-matriisien muodostama joukko, joka on tunnetusti rengas matriisien yhteen- ja kertolaskun suhteen. Olkoon R sen osajoukko, joka koostuu kaikista muotoa*

$$\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}$$

olevista matriiseista, $n \in \mathbb{Z}$. Koska kaikilla $n, m \in \mathbb{Z}$ pätee

$$\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n+m & 0 \\ 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} nm & 0 \\ 0 & 0 \end{pmatrix},$$

R on vakaa matriisrenkaan $M(2\times 2)$ laskutoimitusten suhteen. Lisäksi kuvaus $f\colon \mathbb{Z} \to R$,

$$f(n) = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}$$

on bijektiivinen kuvaus, joka säilyttää sekä yhteen-, että kertolaskun (vrt. esim. 1.49, 3). Seurauksesta 1.41 seuraa tällöin, että $(R, +, \cdot)$ on rengas, koska $(\mathbb{Z}, +, \cdot)$ on sellainen. Tämän renkaan ykkösalkio on matriisi

$$f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Tämä ei ole sama kuin renkaan $M(2 \times 2; \mathbb{R})$ ykkösalkio, joka on matriisi

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Näin ollen R on renkaan $(M(2\times 2;\mathbb{R}),+,\cdot)$ osajoukko, joka on vakaa molempien laskutoimitusten $+$ ja $\cdot$ kanssa ja on itse rengas näillä laskutoimituksilla varustettuna. Kuitenkin R:n ykkösalkio ei ole sama kuin isomman renkaan $M(2\times 2;\mathbb{R})$ ykkösalkio.

Näiden yleisten periaatteiden jälkeen annetaan vielä täsmällisiä määritelmiä alistruktuurille ryhmän, renkaan ja kunnan tapauksessa.

Ryhmien tapaus.
Olkoon $(G,\cdot)$ ryhmä ja $H\subset G$. Tällöin osajoukkoa H sanotaan ryhmän G *aliryhmäksi* jos seuraavat ehdot toteutuvat.

- $xy\in H$ kaikilla $x,y\in H$, eli H on vakaa laskutoimituksen $\cdot$ suhteen.
- $e\in H$, missä e on ryhmän G neutraalialkio.
- H on suljettu käänteisalkioiden suhteen, eli $x^{-1}\in H$ kaikilla $x\in H$. Tässä x^{-1} on alkion x käänteisalkio ryhmässä G.

Kun H on ryhmän $(G,\cdot)$ ryhmä, pari $(H,\cdot)$ muodostaa itse ryhmän. Jos ryhmä G on vaihdannainen eli Abelin ryhmä, myös H on vaihdannainen.

Esimerkki 1.57. *Tarkastelemme ryhmän $(\mathbb{Z},+)$ vakaita osajoukkoja esimerkistä (1.54), eli osajoukkoja $\mathbb{N}_+$, $\mathbb{N}$ sekä parillisten kokonaislukujen joukkoa $2\mathbb{Z}$. Näistä $\mathbb{N}_+$ ei ole ryhmän $(\mathbb{Z},+)$ aliryhmä, sillä se ei sisällä edes yhteenlaskun neutraalialkiota 0. Luonnollisten lukujen joukko $\mathbb{N}$ sisältää kyllä neutraalialkion, mutta ei ole suljettu vasta-alkioiden suhteen, sillä esimerkiksi $1\in\mathbb{N}$, mutta $-1\notin\mathbb{N}$. Näin ollen ei sekään ole aliryhmä.*

Parillisten kokonaislukujen osajoukko $2\mathbb{Z}=\{2n\mid n\in\mathbb{Z}\}$ sen sijaan on aliryhmä - se on vakaa yhteenlaskun suhteen, sisältää neutraalialkion 0 ja on suljettu vasta-alkioiden suhteen, sillä parillisen kokonaisluvun vastaluku on parillinen kokonaisluku.

Esimerkki 1.58. *Olkoon $(\mathbb{C}^*,\cdot)$ nollasta eroavien kompleksilukujen ryhmä (kompleksilukujen kertolaskulla varustettuna). Väitämme, että osajoukko*

$$G=\{1,-1,i,-i\}\subset\mathbb{C}^*$$

on ryhmän $\mathbb{C}^*$ aliryhmä. Renkaan kertolaskun "merkkisäännöistä" (Lemma 1.24) seuraa, että

$$(\pm i)\cdot(\pm 1)=\pm 1,$$
$$(\pm 1)\cdot(\pm i)=\pm i,$$
$$(\pm i)\cdot(\pm i)=\pm i^2=\pm 1,$$

joten G on todellakin vakaa kertolaskun suhteen. Määritelmänsä mukaan se sisältää kertolaskun neutraalialkion 1. Lisäksi G on suljettu käänteisalkioiden suhteen, sillä $1^{-1}=1$, $(-1)^{-1}=-1$, $i^{-1}=-i$, $(-i)^{-1}=i$ (tarkista). Näin ollen G on ryhmän $(\mathbb{C}^*,\cdot)$ aliryhmä. Huomaa, että tämä on esimerkki epätriviaalista äärellisestä ryhmästä.

Esimerkki 1.59. *Kokonaislukujen joukko* $(\mathbb{Z}, +)$ *on Abelin ryhmä. Jokaisella* $m \in \mathbb{N}$ *määritellään osajoukko*

$$m\mathbb{Z} = \{mn \mid m \in \mathbb{Z}\}.$$

Tällöin $m\mathbb{Z}$ *on* $\mathbb{Z}$*:n aliryhmä (yhteenlaskun suhteen), sillä*

$$0 = m \cdot 0 \in m\mathbb{Z},$$

$$mn + mn' = m(n + n'), \text{ joten } m\mathbb{Z} \text{ on suljettu yhteenlaskun suhteen,}$$

$$-(mn) = m(-n) \text{ joten } m\mathbb{Z} \text{ on suljettu vasta-alkioiden suhteen.}$$

Kääntäen voidaan osoittaa, että nämä ovat kaikki ryhmän $(\mathbb{Z}, +)$ *aliryhmät. Tämän tärkeän tuloksen todistus jätetään harjoitustehtäväksi.*

Renkaiden tapaus
Olkoon $(R, +, \cdot)$ rengas ja olkoon $R' \subset R$. Tällöin R' on renkaan R *alirengas* jos seuraavat ehdot toteutuvat

- $(R', +)$ on Abelin ryhmän $(R, +)$ aliryhmä.
- R' on vakaa kertolaskun suhteen.
- $1_R \in R'$. Tässä 1_R on renkaan R neutraalialkio kertolaskun suhteen.

Jos R' on renkaan R alirengas, kolmikko $(R', +, \cdot)$ on rengas.

Kuntien tapaus
Olkoon $(K, +, \cdot)$ kunta ja olkoon $K' \subset K$. Tällöin K' on kunnan R *alikunta* jos seuraavat ehdot toteutuvat

- $(K', +, \cdot)$ on renkaan $(K, +, \cdot)$ alirengas.
- K' on suljettu kertolaskun käänteisalkioiden suhteen eli kaikilla $k \in K', k \neq 0$ pätee $k^{-1} \in K'$. Tässä k^{-1} on alkion k käänteisalkio kunnassa K.

Jos K' on kunnan K alikunta, kolmikko $(K', +, \cdot)$ on kunta.

Esimerkkejä 1.60. *(1) Rengas* $(\mathbb{Z}, +, \cdot)$ *on renkaan* $(\mathbb{R}, +, \cdot)$ *alirengas. Jos rengasta* $(\mathbb{R}, +, \cdot)$ *ajatellaan kuntana,* $(\mathbb{Z}, +, \cdot)$ *ei ole kunnan* $(\mathbb{R}, +, \cdot)$ *alikunta, sillä* $\mathbb{Z}$ *ei ole suljettu käänteisalkioiden suhteen - esimerkiksi* $2 \in \mathbb{Z}$*, mutta* $\frac{1}{2} \notin \mathbb{Z}$*.*

(2) $(\mathbb{R}, +, \cdot)$ *on kompleksilukukunnan* $(\mathbb{C}, +, \cdot)$ *alikunta. Tässä samaistetaan* $x \in \mathbb{R}$ *kompleksiluvun* $(x, 0)$ *kanssa.*

(3) Parillisten lukujen joukko $2\mathbb{Z}$ *on kokonaislukujen ryhmän* $(\mathbb{Z}, +)$ *aliryhmä . Se on myös vakaa kokonaislukujen kertolaskun suhteen. Kuitenkin* $2\mathbb{Z}$ *ei ole renkaan* $(\mathbb{Z}, +, \cdot)$ *alirengas, sillä* $1 = 1_Z \notin 2\mathbb{Z}$*. Itse asiassa* $(2\mathbb{Z}, +, \cdot)$ *ei edes ole rengas, koska sillä ei ole ykkösalkiota.*

(4) Esimerkissä (1.56) annettiin esimerkki (2×2) *reaalikertoimisten matriisien muodostaman renkaan* $(M(2 \times 2; \mathbb{R}), +, \cdot)$ *osajoukosta* R'*, joka on vakaa molempien renkaan* $M(2 \times 2; \mathbb{R})$ *laskutoimitusten* $+$ *ja* $\cdot$ *suhteen, ja joka on rengas niillä varustettuna, mutta joka ei kuitenkaan ole renkaan* $M(2 \times 2; \mathbb{R})$ *alirengas.*

(5) Kaikkien muotoa

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, a, b, d \in \mathbb{R},$$

olevat (2×2) *reaalikertoimiset matriisit muodostavat matriisirenkaan* $(M(2\times2;\mathbb{R}),+,\cdot)$ *alirenkaan. Yksityiskohdat jätetään harjoitustehtäväksi.*

1.7.1. Alistruktuurit ja homomorfismit

Palautetaan ensin mieleen joukko-oppilliset *kuvan* ja *alkukuvan* käsitteet. Olkoot X ja Y joukkoja ja olkoon $f\colon X \to Y$ kuvaus. Huomaa, että emme tässä vaiheessa vielä oleta, että joukoilla X tai Y olisi mitään algebrallista rakennetta.

Olkoot $A \subset X$ ja $B \subset Y$ osajoukkoja. Joukon A *kuva(joukko)* kuvauksessa f on joukon Y osajoukko

$$f(A) = \{f(a) \mid a \in A\}.$$

Toisin sanoen $y \in Y$ on kuvan $f(A)$ alkio jos ja vain jos on olemassa $a \in A$ siten, että $f(a) = y$.

Joukon $B \subset Y$ *alkukuva* on joukon X osajoukko

$$f^{-1}(A) = \{x \in X \mid f(x) \in B\}.$$

Toisin sanoen alkukuvassa $f^{-1}(B)$ on tasan ne x:n alkiot joita f kuvaa joukkoon B.

Kun f on bijektio on määritelty, sen käänteiskuvaus $f^{-1}\colon Y \to X$ on myös kuvaus, joten symboli $f^{-1}(B)$ voidaan tulkita kahdella tavalla - joko joukon B *kuvana* kuvauksessa f^{-1} tai joukon B alkukuvana kuvauksessa f. Onneksi molemmat tulkinnat kuitenkin tuottavat täsmälleen saman joukon, joten tuplanotaation vaaraa ei synny.

Tarkastellaan seuraavaksi kuvan ja alkukuvan ominaisuuksia algebrallisilla struktuureilla rikastetussa tilanteessa. Aloitetaan yksinkertaisista yleisistä tuloksista.

Lemma 1.61. *Olkoon* $\cdot$ *joukon* X *laskutoimitus ja* $\cdot'$ *joukon* Y *laskutoimitus. Olkoon* $f\colon X \to Y$ *kuvaus, joka on yhteensopiva näiden laskutoimitusten kanssa. Oletetaan, että* $A \subset X$ *on vakaa laskutoimituksen* $\cdot$ *suhteen ja* $B \subset Y$ *on vakaa laskutoimituksen* $\cdot'$ *suhteen. Tällöin* kuvajoukko $f(A) \subset Y$ *on vakaa laskutoimituksen* $\cdot'$ *suhteen ja* alkukuva $f^{-1}(B) \subset X$ *on on vakaa laskutoimituksen* $\cdot$ *suhteen.*

Toisin sanoen vakaiden osajoukkojen kuvat/alkukuvat laskutoimituksia säilyttävän kuvauksen suhteen ovat vakaita.

Todistus. Osoitetaan väite alkukuville ja jätetään (helpompi) kuvien tapaus harjoitustehtäväksi. Olkoon $B \subset Y$ vakaa ja olkoot $x, x' \in f^{-1}(B)$. On osoitettavaa, että $x \cdot x' \in f^{-1}(B)$. Alkukuvan määritelmän mukaan tämä on sama asia kuin $f(x \cdot x') \in B$. Mutta, koska f on yhteensopiva laskutoimitusten kanssa, pätee

$$f(x \cdot x') = f(x) \cdot' f(x') \in B,$$

koska B on vakaa laskutoimituksen $\cdot'$ suhteen. Väite on osoitettu. □

Yllä tarkastellussa tilanteessa X on itseensä osajoukkona aina vakaa. Näin olleen erityisesti edellisestä Lemmasta seuraa, että laskutoimituksia säilyttävän kuvauksen $f\colon X \to Y$ *kuvajoukko*

$$\operatorname{Im} f = \{f(x) \mid x \in X\} \subset Y$$

on vakaa joukon Y laskutoimituksen suhteen.

Usein tarkastellaan tapausta, jossa joukolla Y on laskutoimituksen $\cdot'$ suhteen olemassa neutraalialkio $e' \in Y$. Neutraalialkion määritelmästä seuraa helposti, että tällöin yksiö $B = \{e\}$ on Y:n vakaa osajoukko. Edellisestä Lemmasta seuraa, että tämän joukon *alkukuva*

$$\operatorname{Ker} f = \{x \in X \mid f(x) = e'\}$$

on joukon X vakaa osajoukko. Tätä joukkoa sanotaan kuvauksen f **ytimeksi** (engl. *kernel*, tästä merkintä Ker tulee). Huomaa, että ydin on määritelty ainoastaan silloin kun joukolla Y on neutraalialkio, kun taas kuvajoukko on aina määritelty.

Tarkastellaan tarkemmin kuvia ja ytimiä meitä kiinnostavissa tilanteissa, eli ryhmien, renkkaiden ja kuntien kohdalla.

Ryhmien tapaus.

Lemma 1.62. *Olkoot $(G, \cdot)$ ja $(G', \cdot')$ ryhmiä ja olkoon $f\colon G \to G'$ ryhmähomomorfismi. Olkoon $H \subset G$ ryhmän G aliryhmä ja $H' \subset G'$ vastaavasti ryhmän G' aliryhmä. Tällöin* kuvajoukko $f(H) \subset G'$ *on ryhmän G' aliryhmä ja* alkukuva $f^{-1}(H') \subset G$ *on ryhmän G aliryhmä.*

Toisin sanoen aliryhmien kuvat/alkukuvat ryhmähomomorfismin suhteen ovat aliryhmiä.

Todistus. Harjoitustehtävä. □

Ryhmä G on selvästi itsensä aliryhmä. Helposti nähdään, että neutraalialkion muodostama yksiö $\{e'\}$ on ryhmän G' aliryhmä (niin sanottu *triviaali aliryhmä*). Edellisestä Lemmasta seuraa, että jos $f\colon G \to G'$ on ryhmien välinen homomorfismi, kuvajoukko $f(G)$ on ryhmän G' aliryhmä ja homomofismin f **ydin** $\operatorname{Ker} f = f^{-1}(e')$ on ryhmän G aliryhmä. Osoittautuu, että ydin on aina jopa niin sanottu *normaali aliryhmä*. Normaalista aliryhmistä puhutaan seuraavassa aliluvussa tekijäryhmien yhteydessä.

Esimerkki 1.63. *Tarkastellaan esimerkissä 1.45, 1 mainittua ryhmähomomorfismia $f\colon (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$, $f(x) = (\cos x, \sin x)$. Tässä $\mathbb{C}^*$ on nollasta eroavien kompleksilukujen joukko, joka muodostaa ryhmän kompleksilukujen kertolaskun suhteen.*

Tämän kuvauksen kuvajoukko $\operatorname{Im} f$ *koostuu tason pisteistä (a, b), jotka voidaan esittää muodossa $(\cos x, \sin x)$ jollakin $x \in \mathbb{R}$. Tason geometriasta tiedetään, että tämä on niiden tason pisteiden joukko, joiden etäisyys origosta on tasan* 1*, toisin sanoen* 1*-säteisen origokeskeinen ympyrä,*

$$\operatorname{Im} f = S^1 = \{(a, b) \in \mathbb{R}^2 \mid a^2 + b^2 = 1\}.$$

Edellisen Lemman mukaan S^1 muodostaa ryhmän kompleksilukujen kertolaskun suhteen, tämä on ryhmän $(\mathbb{C}^*, \cdot)$ aliryhmä.

Olkoon $G = \{1, -1, i, -i\}$, tällöin G on ryhmän $(\mathbb{C}^*, \cdot)$ aliryhmä (kts. esimerkki 1.58). Kuvauksen f määritelmästä seuraa, että joukon G alkukuva $f^{-1}(G)$ koostuu kaikista luvun $\pi/2$ monikerroista,

$$f^{-1}(G) = \{n\pi/2 \mid n \in \mathbb{Z}\}.$$

Edellisen Lemman nojalla tämä on $\mathbb{R}$:n aliryhmä (yhteenlaskun suhteen). Tämä väite on helppoa nähdä todeksi myös suoraan.

Homomorfismin kuvajoukon ja ytimen käsitteiden avulla voidaan luonnehtia homomorfismin surjektiivisyyttä tai injektiivisyyttä.

Lemma 1.64. *Olkoot $f\colon G \to G'$ ryhmien välinen homomorfismi. Tällöin*

- *f on injektio jos ja vain jos* $\operatorname{Ker} f = \{e\}$ *on triviaali (eli sisältää vain neutraalialkion).*
- *f on surjektio jos ja vain jos* $\operatorname{Im} f = G'$.
- *f on isomorfismi jos ja vai jos* $\operatorname{Im} f = G'$ *ja* $\operatorname{Ker} f = \{e\}$.

Todistus. Oletetaan, että f on injektio ja olkoon $x \in \operatorname{Ker} f$. Tällöin $f(x) = e'$, missä e' on ryhmän G' neutraalialkio. Toisaalta myös $f(e) = e'$. Oletuksesta seuraa tällöin, että $x = e$. Näin ollen $\operatorname{Ker} f = \{e\}$ sisältää vain neutraalialkion.

Oletetaan kääntäen, että $\operatorname{Ker} f = \{e\}$. Olkoot $x, y \in G$ siten, että $f(x) = f(y)$. Tällöin, koska f on homomorfismi

$$f(xy^{-1}) = f(x)f(y)^{-1} = e',$$

joten $xy^{-1} = e$, mistä seuraa, että $x = y$. Olemme osoittaneet, että f on injektio.

Lemman toinen väite on triviaali ja kolmas on ensimmäisen ja toisen suora yhdistelmä. □

Renkaiden/Kuntien tapaus.

Samalla tavalla kuin ryhmien tapauksessa voidaan osoittaa, että alirenkaiden/alikuntien kuvat ja alkukuvat rengas/kuntahomomorfismeissa ovat alirenkaita/alikuntia. Tarkat todistukset jätetään lukijalle.

Lemma 1.65. *Olkoot $(R, +, \cdot)$ ja $(R', +', \cdot')$ renkaita ja olkoon $f\colon R \to R'$ rengashomomorfismi. Olkoon $P \subset R$ renkaan R alirengas ja $P' \subset R'$ vastaavasti renkaan R' alirengas. Tällöin* kuvajoukko $f(P) \subset R'$ *on renkaan R' alirengas ja* alkukuva $f^{-1}(P') \subset R$ *on renkaan R alirengas.*

Lemma 1.66. *Olkoot $(K, +, \cdot)$ ja $(K', +', \cdot')$ kuntia ja olkoon $f\colon K \to K'$ kuntahomomorfismi. Olkoon $Q \subset K$ kunnan K alikunta ja $Q' \subset K'$ vastaavasti kunnan K' alikunta. Tällöin* kuvajoukko $f(K) \subset K'$ *on kunnan K' alikunta ja* alkukuva $f^{-1}(Q') \subset K$ *on kunnan K alikunta.*

Rengas R on selvästi itsensä alirengas. Edellisestä Lemmasta seuraa, että jos $f\colon R \to R'$ on renkaiden välinen homomorfismi, kuvajoukko $f(R)$ on renkaan R' alirengas. **Sen sijaan rengashomomorfismin** $f\colon R \to R'$ *ydin* yhteenlaskun suhteen eli joukko

$$\operatorname{Ker} f = f^{-1}(0_{R'}) = \{r \in R \mid f(r) = 0_{R'}\}$$

ei yleensä ole renkaan R alirengas. Se on kyllä vakaa renkaan R yhteen- ja kertolaskun suhteen, mutta ei sisällä renkaan ykkösalkiota 1_R, paitsi jos R' on triviaali rengas, koska muuten $f(1_R) = 1_{R'} \neq 0_{R'}$. Tästä huolimatta rengashomomorfismin ydin (yhteenlaskun suhteen) on tärkeä renkaan R osajoukko ja esimerkki niin sanotusta renkaan *ideaalista*. Renkaan ideaaleista ja rengashomomorfismin ytimestä puhutaan tarkemmin seuraavassa aliluvussä tekijärenkaiden yhteydessä. Huomaa, että rengashomomorfismin $f\colon R \to R'$ ydin on sama asia kuin *ryhmien* $(R, +)$, $(R', +)$ välisen homomomorfismin f ydin. Näin ollen kaikki rengashomomorfismin f ytimen koskevat väitteet voidasan palauttaa ryhmien homomorfismien ytimen teoriaan. Erityisesti Lemmasta 1.64 seuraa suoraan, että vastaava yhteys ytimien ja homomorfismien injektiivisyyden kanssa on voimassa myös renkaiden tapauksessa.

Lemma 1.67. *Olkoot $f\colon R \to R'$ renkkaiden välinen homomorfismi. Tällöin*

- *f on injektio jos ja vain jos $\operatorname{Ker} f = \{0_R\}$ on triviaali.*
- *f on surjektio jos ja vain jos $\operatorname{Im} f = R'$.*
- *f on isomorfismi jos ja vai jos $\operatorname{Im} f = R'$ ja $\operatorname{Ker} f = \{0_R\}$.*

Esimerkki 1.68. *Olkoon R muotoa*

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, a, b, d \in \mathbb{R}$$

olevien reaalikertoimisten (2×2)-matriisien muodostama joukko. Tämä on rengas, koska se on matriisirenkaan $(M(2 \times 2; \mathbb{R}), +, \cdot)$ alirengas (kts. esim. 1.60). Varustetaan karteesinen tulo

$$\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$$

yhteen- ja kertolaskutoimituksilla $+$, $\cdot$ "koordinaateittain",

$$(x, y) + (x', y') = (x + x', y + y'),$$

$$(x, y) \cdot (x', y') = (xx', yy').$$

Huomaa, että jos $\mathbb{R}^2$ ajatellaan kompleksilukujen joukkona, edellä määritelty yhteenlasku on sama kuin kompleksilukujen yhteenlasku, mutta kertolasku ei ole sama.
Voidaan osoittaa, että näilla laskutoimituksilla varustettuna $(\mathbb{R}^2, +, \cdot)$ on rengas (HT). Määritellään kuvaus $f\colon R \to \mathbb{R}^2$ kaavalla

$$f(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}) = (a, d).$$

Tällöin f on rengashomorfismi (HT). Koska renkaan $(\mathbb{R}^2, +, \cdot)$ nolla-alkio on pari $(0,0)$, tämän kuvauksen ytimelle pätee

$$\text{Ker } f = \{\begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \mid b \in \mathbb{R}\}.$$

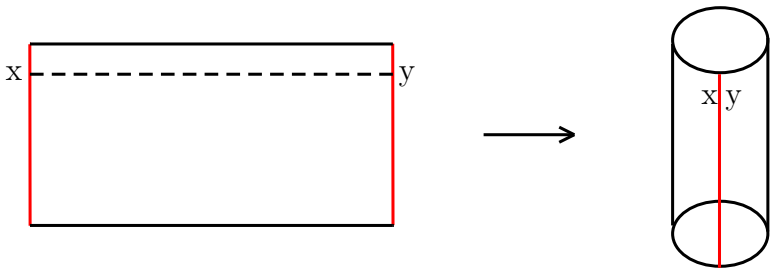
Tämä ei sisällä renkaan R ykkösalkiota

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Erityisesti Ker f *ei ole renkaan R alirengas.*

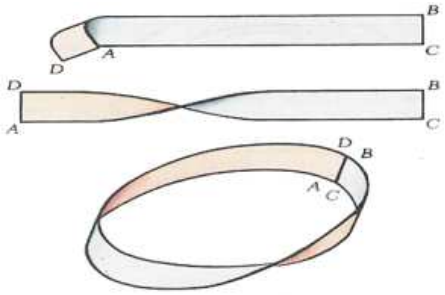
1.8. Tekijästruktuurit

Matematiikassa on usein hyödyllistä tai tarpeellista ”samaistaa” jonkun joukon X erilaisia alkioita ”samaksi alkioksi”. Esimerkiksi kellotauluaritmetiikan näkökulmasta klo 3 ja klo 15 on sama asia, vaikka luvut 3 ja 15 ovat eri lukuja. Topologiassa uusia geometrisia muotoja saadaan vanhoista ”liimamalla” eri pisteitä toisiinsa. Esimerkiksi olkoon X tasossa sijaitseva suorakulmio (kts. kuva 2 alla). Taivuttamalla X kolmiulotteisessa avaruudessa ja yhdistämällä sen pystyreunoja yhteen saadaan aikaan ontto putki eli *sylenteri* (ympyrälieriö). Voidaan ajatella, että sylenteri syntyy kun pystyreunoilla sijaitsevat vastakkaiset pisteet ”samastetaan samaksi pisteeksi” (kuvassa pistepari x, y on tällainen) . Tällöin sylenterissa kaksi tällaista pistettä vastaavat samaa pistettä eli niistä tulee sama alkio, vaikka alunperin ne olivat suorakulmion pisteinä eri alkiota.



Kuva 2

Jos suorakolmion taivutuksessa kierretäänkin sen toinen pystyreunoista ilmassa 180 asteen verran ja liimataan pystyreunat yhteen ainoastaan sen jälkeen, saadaan kuuluisa *Möbiuksen nauha* (kts. kuva 3).



Kuva 3

Teknisellä, formaalilla tasolla alkioiden samastuksen idea voidaan koodata matemaattisesti *ekvivalenssirelaation* käsitteen avulla. Tämän pitäisi olla matematiikan peruskursseilta tuttu, mutta kerrataan asiaa kuitenkin. Olkoon X joukko. Joukon X *relaatio* R on mikä tahansa karteesisen tulon $X \times X$ osajoukko R. Toisin sanoen joukon R relaatio on mikä tahansa kokoelma pareja (x, y), missä $x, y \in X$. Kun $(x, y) \in R$, missä R on relaatio, merkitään myös xRy ja sanotaan, että alkio x on relaatiossa R alkion y. Relaatio siis ilmaisee jonkinlaisen *suhteen* joukon X alkioiden välillä (mistä nimitys tuleekin).

Määritelmä 1.69. *Joukossa X määriteltyä relaatiota $\sim \subset X \times X$ sanotaan* ekvivalenssirelaatioksi*, jos*

(i) $\sim$ *on* refleksiivinen*, eli $x \sim x$ kaikilla $x \in X$,*

(ii) $\sim$ *on* symmetrinen*, eli jos $x \sim y$ joillakin $x, y \in X$, niin myös $y \sim x$,*

(iii) $\sim$ *on* transitiivinen*, eli jos $x \sim y$ ja $y \sim z$, niin tällöin aina $x \sim z$.*

Ekvivalenssirelaation avulla tietyssä tilanteessa haluttu joukon alkioiden ”samastus” hoidetaan määrittelemällä ekvivalenssirelaatio $\sim$ ehdolla $x \sim y$ jos ja vain jos x ja y samastetaan samaksi alkioksi eli jos x:stä ja y:stä ”tulee sama alkio” samastuksen jälkeen. Ehdot (i)-(iii) ovat tällöin luonnollisia samastuksen ominaisuuksia. Ehto (i) vastaa triviaalia havantoa siitä, että joka tapauksessa jokainen alkio samastuu (muun muassa) itseensä kanssa. Ehto (ii) sanoo, että jos x samastetaan y:n kanssa, niin yhtä hyvin y samastetaan x:n kanssa. Tällainen symmetrisyys on selvä vaatimus - ei ole järkevää sanoa, että x:stä ja y:stä tulee sama alkio, mutta y:stä ja x:stä ei tule. Ehto (iii) taas sanoo, että jos samastuksen jälkeen alkiot x, y ”edustavat” samaa alkiota ja alkiot y, z myös ”edustavat” samaa alkiota, niin x ja z yhtä hyvin edustavat samaa alkiota. Tämähän johtuu siitä, että tällöin kaikki kolme alkiota x, y, z pakosti edustavat samaa alkiota samastuksen jälkeen. Näin ollen samastus voidaan havainnollisesti ajatella tapana ”määritellä alkioiden yhtäsuuruus joukossa uudelleen”. Ekvivalenssirelaation ehdot (i)-(iii) tulevat tämän näkökulman mukaan vastaavista yhtäsuuruusrelaation $=$ luonnollisista ominaisuuksista.

Esimerkiksi, jos halutaan puhua kellotauluaritmetiikan tunnista, jolloin, esimerkiksi 3 ja 15 ajatellaan samana alkiona, on määriteltävä kokonaislukujen joukossa $\mathbb{Z}$ relaatio $\sim$ ehdolla $x \sim y$ jos ja vain jos x ja y eroavat toisistaan luvun 12 monikerran verran. Sama ehto voidaan ilmaistaa ehtona ”erotus $x - y$ on jaollinen luvulla 12”. Itse asiassa hyödyllinen konstruktio saadaan tarkastelemalla sama asetelma yleisemmin, korvamaamalla luku 12 millä tahansa positiivisella kokonaisluvulla n.

Esimerkki 1.70. *Olkoon $n \in \mathbb{N}_+ = \{1, 2, 3, \ldots\}$. Määritellään kokonaislukujen joukossa $\mathbb{Z}$ relaatio $\equiv_n$ ehdolla $x \equiv_n y$ jos ja vain jos erotus $x - y$ on jaollinen luvulla n, toisin sanoen jos ja vain jos on olemassa $k \in \mathbb{N}$ siten, että $x - y = kn$.*

Osoitetaan, että relaatio $\sim$ on ekvivalenssirelaatio joukossa $\mathbb{Z}$.

(i) Jokainen $x \in \mathbb{Z}$ on relaatiossa itsensä kanssa, sillä $x - x = 0 = n \cdot 0$ on jaollinen n:llä. Näin ollen $\equiv_n$ on refleksiivinen.

(ii) Oletetaan, että $x \equiv_n y$ eli $x - y = kn$ jollakin $k \in \mathbb{Z}$. Tällöin

$$y - x = -kn = (-k) \cdot n.$$

mistä seuraa, että $y \equiv_n x$. Näin ollen relaatio $\equiv_n$ on symmetrinen.

(iii) Oletetaan, että $x \equiv_n y$ ja $y \equiv_n z$. Tämä tarkoittaa sitä, että $x-y = kn$ ja $y-z = ln$ joillakin $k, l \in \mathbb{Z}$. Tällöin

$$x - z = (x - y) + (y - z) = kn + ln = (k + l)n.$$

Näin ollen relaatio $\equiv_n$ on transitiivinen.

Olemme näyttäneet, että $\equiv_n$ on ekvivalenssirelaatio joukossa $\mathbb{Z}$, jokaisella $n \geq 1$.

Olkoon esimerkiksi $n = 5$. Tällöin $13 \equiv_5 -2$, koska $13-(-2) = 15 = 3 \cdot 5$ on jaollinen 5:llä. $7 \not\equiv_5 20$, koska $7 - 20 = -13$ ei ole jaollinen 5:llä.

Kun $n = 2$ väite $a \equiv_2 b$ tarkoittaa sitä, että joko a ja b ovat molemmat parillisia kokonaislukuja tai molemmat parittomia kokonaislukuja.

Olkoon $\sim$ ekvivalenssirelaatio joukossa X ja olkoon $x \in X$. Joukon X osajoukkoa

$$\bar{x} = \{y \in X \mid x \sim y\}$$

sanotaan alkion x *ekvivalenssiluokaksi* (ekvivalenssirelaatiossa $\sim$). Alkion x ekvivalenssiluokka koostuu siis tasan niistä X:n alkioista, jotka ovat relaatiossa $\sim$ alkion x kanssa. Koska relaatio $\sim$ on refleksiivinen, alkio x kuuluu aina omaan ekvivalenssiluokkaan, $x \in \bar{x}$. Koska $\sim$ on symmetrinen, $y \in \bar{x}$ jos ja vain jos $y \sim x$. Havainnollisesti ajatelleen samaan ekvivalenssiluokkaan kootaan kaikki alkiot, jotka halutaan samaistaa keskenään, eikä mitään muuta. Seuraavan Lemman mukaan erilaiset ekvivalenssiluokat eivät koskaan ”mene päällekkäin”.

Lemma 1.71. *Olkoon $\sim$ joukossa X määritelty ekvivalenssirelaatio. Tällöin sen alkioiden ekvivalenssiluokat muodostavat joukon X* osituksen*. Tarkemmin sanottuna jokainen $x \in X$ kuuluu* tasan yhteen *ekvivalenssiluokkaan A, jolloin $A = \bar{x}$. Jos $x, y \in X$, niin*

$$\bar{x} \cap \bar{y} \neq \emptyset$$

jos ja vain jos $x \sim y$, jolloin $\bar{x} = \bar{y}$.

Todistus. Tunnettua matematiikan peruskursseilta, harjoitustehtävä. □

Olkoon $A \subset X$ ekvivalenssirelaation $\sim$ ekvivalenssiluokka. Tällöin jokaisella $x \in A$ pätee $A = \bar{x}$. Kun ekvivalenssiluokka A esitetään muodossa $\bar{x}$ jollakin sen alkiolla x, tämä alkio sanotaan kyseisen luokan *edustajaksi*. Jokainen ekvivalenssiluokan alkio voidaan valita tämän luokan edustajaksi.

Esimerkkejä 1.72. *(1) Määritellään reaalilukujen joukossa $\mathbb{R}$ relaatio R ehdolla xRy jos $xy = 1$. Tällöin R ei ole refleksiivinen, joten se ei ole ekvivalenssirelaatio.*

(2) Määritellään reaalilukujen joukossa $\mathbb{R}$ relaatio $\sim$ ehdolla $x \sim y$ jos $x^2 = y^2$. Tällöin $\sim$ on ekvivalenssirelaatio. Alkion x ekvivalenssiluokka $\bar{x}$ on joukko $\{x, -x\}$, koska $y^2 = x^2$ jos ja vai jos $y = \pm x$. Kun $x = 0$ ekvivalenssiluokka $\bar{x}$ on yksiö $\{0\}$, muuten ekvivalenssiluokka $\bar{x}$ on aina kaksio.

(3) Olkoon $n \geq 1$ positiivinen kokonaisluku. Esimerkissä 1.70 olemme määritelleet kokonaislukujen joukossa $\mathbb{Z}$ relaatio $\equiv_n$ ehdolla $x \equiv_n y$ jos ja vain jos $x-y$ on jaollinen luvulla n. Olemme osoittaneet, että $\equiv_n$ on ekvivalenssirelaatio.

Todetaan ensin, että jokaisella $x \in \mathbb{Z}$ pätee

$$\bar{x} = \{x + kn \ \ | k \in \mathbb{Z}\}$$

eli ekvivalenssiluokka $\bar{x}$ koostuu luvuista jotka saadaan lisäämällä x:ään luvun n monikertoja. Tämä seuraa suoraan relaation $\equiv_n$ määritelmästä, nimittäin $y \in \bar{x}$ jos ja vain jos $y \equiv_n x$ eli jos ja vain jos $y - x = kn$ jollakin $k \in \mathbb{Z}$. Tämä on yhtäpitävä sen kanssa, että $y = x + kn$ jollakin $k \in \mathbb{Z}$. Näin ollen

$$\bar{x} = \{x + kn \ \ | k \in \mathbb{Z}\}.$$

Koska $n \geq 1$, tästä seuraa, että $\bar{x}$ sisältää "mielivaltaisen suuria" kokonaislukuja, erityisesti se sisältää myös ei-negatiivisia kokonaislukuja, eli joukon $\mathbb{N} = \{0, 1, 2, \ldots\}$ alkiota. Yksi luonnollisten lukujen joukon $\mathbb{N}$ tärkeimpiä ominaisuuksia on se tosiasia, että jokainen sen epätyhjä osajoukko sisältää pienemmän *luvun. Voimme siis valita kaikista ekvivalenssiluokaan $\bar{x}$ kuuluvista luonnollisista luvuista* **pienimmän** *luonnollisen luvun $l \in \bar{x} \cap \mathbb{N}$. Osoitetaan, että tällöin $l \in \{0, 1, \ldots, n-1\}$ eli toisin sanoen $l < n$. Tehdään vasta-oletus, $l \geq n$. Koska $l \in \bar{x}$, edellä osoitetun nojalla $l = x + kn$ jollakin $k \in \mathbb{Z}$. Tästä seuraa, että*

$$l' = l - n = x + (k-1)n \in \bar{x}.$$

Lisäksi, koska oletamme, että $l \geq n$, pätee $l' \geq 0$. Toisaalta $l' < l$ ja päädytään ristiriitaan sen kanssa, että l oli **pienin** *luonnollinen luku luokassa $\bar{x}$. Näin ollen vasta-oletus ei voi pitää paikkaansa, joten $l < n$. Koska toisaalta $l \geq 0$, saadaan $l \in \{0, 1, \ldots, n-1\}$. Koska $l \in \bar{x}$, edellisen Lemman nojalla pätee $\bar{n} = \bar{l}$. Erityisesti $x = l + kn$ jollakin $k \in \mathbb{Z}$, mistä nähdään, että l ei ole itse asiassa mitään muuta kuin x:n* jakojäännös *luvulla n jaettaessa.*

Näin ollen relaatiolla $\equiv_n$ on vain äärellinen määrä ekvivalenssiluokkia - kaikki luokat ovat muotoa $\bar{l}$, missä $l = 0, 1, \ldots, n-1$. Osoitetaan vielä, että nämä luokat ovat kaikki erilaisia. Olkoot $l, l' \in \{0, 1, \ldots, n-1\}$ sellaisia, että $\bar{l} = \bar{l'}$. Tällöin erityisesti $l' = l + kn$ jollakin $k \in \mathbb{Z}$. Jos $k < 0$, saadaan

$$l' = l + kn < n + kn = (k+1)n \leq 0 \cdot n = 0,$$

eli $l' < 0$, mikä on vastoin oletusta. Samoin, jos $k > 0$ eli jos $k \geq 1$ saadaan

$$l' = l + kn \geq 0 + 1 \cdot n = n,$$

mikä on myöskin mahdotonta. Näin ollen ainoa mahdollisuus on $k = 0$, jolloin $l' = l$.

Olemme osoittaneet, että kokonaislukujen joukon $\mathbb{Z}$ ekvivalenssirelaatiolla $\equiv_n$ on tasan n ekvivalenssiluokkaa. Ne ovat täsmälleen lukujen $0, 1, \ldots, n-1$ ekvivalenssiluokat. Jokaiselle $k \in \mathbb{Z}$ pätee $\bar{k} = \bar{l}$, missä l on luvun k jakojäännös luvulla n

jaettaessa.

Relaation $\equiv_n$ tapauksessa käytämme ekvivalenssiluokalle $\bar{x}$ myös merkintää x_n. Esimerkiksi

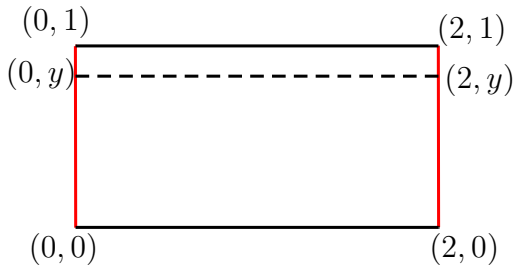
$$5_3 = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\} = 2_3.$$

Olkoon $\sim$ ekvivalenssirelaatio joukossa X. Tämän relaation määrittelemä **tekijäjoukko** $X/\sim$ on kaikkien relaation $\sim$ ekvivalenssiluokkien muodostama kokoelma, eli kaavan muodossa

$$X/\sim = \{\bar{x} \mid x \in X\}.$$

Tekijäjoukon *alkiot* ovat siis aina eräitä joukon X *osajoukkoja*. Juuri tekijäjoukko $X/\sim$ on se joukko, joka saadaan alkioiden samastuksen jälkeen.

Esimerkiksi palataan sylenterin kosntruktioon suorakulmiosta. Otetaan suorakulmioksi tason $\mathbb{R}^2$ osajoukko $X = [0, 2] \times [0, 1]$ (toki mikä tahansa muu suorakulmio kelpaisi). Tällöin suorakulmion X vasemmanpuoleisen pystyreunan pisteet ovat muotoa $(0, y)$, jossa y käy läpi lukuja väliltä $[0, 1]$. Vastaavasti oikeanpuoleisen pystyreunan pisteet ovat muotoa $(2, y)$, $0 \leq y \leq 1$ (kts. kuva 4). Sylenteri saadaan kun samastetaan jokaisella $y \in [0, 1]$ pisteet $(0, y)$ ja $(2, y)$. Teknisesti samastus tehdään määrittelemällä joukossa X ekvivalenssirelaatio $\sim$ ehdoilla $(a, b) \sim (c, d)$ jos ja vain jos joko $(a, b) = (c, d)$ tai toinen pisteistä $(a, b), (c, d)$ on muotoa $(0, y)$ ja toinen muotoa $(2, y)$, jollakin $y \in [0, 1]$. Huomaa, että teknisistä syistä relaation $\sim$ määritelmässä on mainittava kaikki muotoa $(a, b) \sim (a, b)$ olevat suhteet, sillä ekvivalenssirelaation pitää olla refleksiivinen määritelmän mukaan. Asian ydin on kuitenkin epätriviaaleissa samastuksissa $(0, y) \sim (2, y)$ ja $(2, y) \sim (0, y)$, jotka ilmaisevat juuri sitä "liimausta" jonka tarvitsemme. Taas teknisistä syistä täytyy ottaa nämä samastukset molemmin päin, jotta relaatiosta tulisi symmetrinen. Sen tarkistaminen, että näin määritelty relaatio $\sim$ todellakin on ekvivalenssirelaatio jätetään lukijalle harjoitustehtäväksi.



Kuva 4

Nyt voidaan muodostaa tekijäjoukko $X/\sim$. Sen alkiot ovat yksiöitä $\{(a, b)\}$, missä $a \neq 0, 2$, jotka vastaavat pisteitä, jotka samastuvat vain itseensä kanssa, sekä kaksiot $\{(0, y), (2, y)\}$, missä $y \in [0, 1]$. Nämä vastaavat suorakulmion X pystyreunojen liimausta, jossa kahdesta eri pisteestä tulee aina yksi.

Esimerkki 1.73. *Esimerkkeissä 1.70 ja 1.72, 3) olemme määritelleet kokonaislukujen joukossa $\mathbb{Z}$ ekvivalenssirelaation $\equiv_n$ (missä $n \geq 1$ on kiinteä positiivinen kokonaisluku). Olemme myös osoittaneet, että tällä relaatiolla on tasan n ekvivalenssiluokkaa, jotka ovat luokat*

$$\overline{0}, \overline{1}, \ldots, \overline{n-1}.$$

Tekijäjoukkoa $\mathbb{Z}/\equiv_n$ *merkitään lyhyesti* $\mathbb{Z}_n$. *Edellisen nojalla* $\mathbb{Z}_n$ *on äärellinen joukko, jossa on tasan* n *alkiota* $0_n, 1_n, \ldots, (n-1)_n$. *Esimerkiksi*

$$\mathbb{Z}_3 = \{0_3, 1_3, 2_3\},$$

$$\mathbb{Z}_7 = \{0_7, 1_7, 2_7, 3_7, 4_7, 5_7, 6_7\}$$

jne. Joukon $\mathbb{Z}_n$ *alkioita sanotaan* **kokonaisluvuiksi modulo** n.

Olkoon $\sim$ ekvivalenssirelaatio joukossa X. **Kanoninen projektio** $p\colon X \to X/\sim$ on kuvaus joukolta X tekijäjoukolle $X/\sim$, joka määritellään kaavalla $p(x) = \bar{x}$. Tämä kuvaus siis kuvaa alkion sen ekvivalenssiluokalle. Tekijäjoukon määritelmästä seuraa, että kanoninen projektio on aina surjektio.

Ekvivalenssirelaatiot algebrassa

Kun joukolla X on jokin algebrallinen struktuuri, ollaan erityisesti kiinnostuneita sellaisista sen ekvivalenssirelaatioista, jotka ovat ”yhteensopivia” tämän struktuurin kanssa, sillä tällöin tekijäjoukostakin tulee (uusi ja mahdollisesti mielenkiintoinen) algebrallinen olio.

Olkoon X laskutoimituksella $\cdot$ varustettu joukko. Olkoon $\sim$ joukon X ekvivalenssirelaatio. Tällöin on olemassa tekijäjoukko $X/\sim$. Haluaisimme määritellä tekijäjoukossa $X/\sim$ alkuperäisestä joukon X laskutoimituksesta ”luonnollisella tavalla periytyvään laskutoimituksen” $\cdot'$. Tämä tarkoittaa sitä, että laskesimme ekvivalenssiluokilla tekijäjoukossa $X/\sim$ ”samalla tavalla” kuin vastaavilla alkioilla joukossa X, eli kaikille $x, y \in X$ pätisi

$$\bar{x} \cdot' \bar{y} = \overline{x \cdot y}. \tag{1.74}$$

Ongelma on siinä, että tällä kaavalla annettu laskutoimitus ei välttämättä ole *hyvinmääritelty*. Nimittäin yhtälön 1.74 molemmat puolet *riipuvat luokkien edustajiin valinnoista*. Laskutoimituksen tuloksen ei kuitenkaan pitäisi riippua siitä, missä muodossa laskettavia ekvivalenssiluokkia esitetään. Tarkemmin sanottuna, olkoot yllä $x' \sim x$, $y' \sim y$. Tällöin x' on yhtä hyvin luokan $\bar{x}$ edustaja, eli pätee $\bar{x'} = \bar{x}$. Samalla tavalla pätee $\bar{y'} = \bar{y}$. Jos ekvivalenssiluokkien $A = \bar{x'} = \bar{x}$ ja $B = \bar{y'} = \bar{y}$ tulo lasketaan kaavalla 1.74 käyttämällä A:lle edustajaa x ja B:lle edustajaa y, saadaan

$$A \cdot' B = \bar{x} \cdot' \bar{y} = \overline{x \cdot y}.$$

Jos taas käytetään A:n edustajana alkioita x' ja B:n edustajana alkiota y', saadaan kaavalla 1.74

$$A \cdot' B = \bar{x'} \cdot' \bar{y'} = \overline{x' \cdot y'}.$$

Lopputuloksen $A \cdot' B$ pitää tietysti olla yksikäsitteisesti määrätty. Näin ollen, jotta kaavalla 1.74 olisi mahdollista määritellä tekijäjoukossa $X/\sim$ laskutoimituksen $\cdot'$, pitäisi päteä

$$\overline{x \cdot y} = \overline{x' \cdot y'}$$

aina kun $x \sim x'$ ja $y \sim y'$. Mielivaltainen ekvivalenssirelaatio ei välttämättä toteuta tätä ehtoa. Annetaan virallinen määritelmä sellaisille ekvivalenssirelaatioille, jotka toteutavat sen.

Määritelmä 1.75. *Olkoon $\cdot$ laskutoimitus joukossa X. Olkoon $\sim$ joukon X ekvivalenssirelaatio. Sanomme, että $\sim$ on* yhteensopiva *laskutoimituksen $\cdot$ kanssa, jos ehdoista $x \sim x', y \sim y'$ aina seuraa, että $xy \sim x'y'$.*

Määritelmää edeltävän pohdinnan pohjalta saadaan seuraava tulos.

Lemma 1.76. *Olkoon $\cdot$ laskutoimitus joukossa X. Olkoon $\sim$ joukon X ekvivalenssirelaatio, joka on yhteensopiva laskutoimituksen $\cdot$ kanssa. Tällöin tekijäjoukossa $X/\sim$ on olemassa yksikäsitteinen laskutoimitus $\cdot'$, siten, että kaikilla $x, y \in X$ pätee*

$$\bar{x} \cdot' \bar{y} = \overline{x \cdot y}. \tag{1.77}$$

Kanoninen projektio $p\colon (X, \cdot) \to (X/\sim, \cdot')$ on laskutoimitukset säilyttävä.

Todistus. Olkoot A, B tekijäjoukon $X/\sim$ alkioita. Määritelmän mukaan A ja B ovat tällöin ekvivalenssirelaation $\sim$ ekvivalenssiluokkia. Valitaan $x, y \in X$ siten, että $A = \bar{x}$ ja $B = \bar{y}$ ja asetetaan

$$A \cdot' B = \overline{x \cdot y}.$$

Koska $\sim$ on yhteensopiva laskutoimituksen $\cdot$ suhteen, tämän määritelmän lopputulos ei riipu edustajin x, y valinnoista, joten $\cdot'$ on hyvinmääritelty laskutoimitus joukossa $X/\sim$.

Kanonisen projektion $p\colon X \to X/\sim$ yhteensopivuus laskutoimitusten $\cdot$ ja $\cdot'$ kanssa tarkoittaa sitä, että kaikilla $x, y \in X$ pätee

$$p(x) \cdot' p(y) = p(x \cdot y).$$

Koska $p(a) = \bar{a}$ määritelmän mukaan, tämä yhtälö on täsmälleen sama asia kuin yhtälö 1.77, jonka voidaan pitää laskutoimituksen $\cdot'$ määritelmänä. □

Edellisessä Lemmassa konstruoitua tekijäjoukon laskutoimitusta sanotaan myös laskutoimituksen $\cdot$ *indusoimaksi* laskutoimitukseksi.

Esimerkkejä 1.78. *(1) Määritellään kokonaislukujen joukossa $\mathbb{Z}$ ekvivalenssirelaatio $x \sim y$ ehdolla $x = \pm y$. Tällöin $\sim$* **ei ole** *yhteensopiva kokonaislukujen yhteenlaskun kanssa. Esimerkiksi $\mathbb{Z}$:ssä pätee $1 \sim -1$, $1 \sim 1$ mutta $1+1 = 2 \nsim 0 = 1+(-1)$. Näin ollen tekijäjoukossa $\mathbb{Z}/\sim$ ei voida määritellä mielekkäällä tavalla kokonaislukujen yhteenlaskusta periytyvää laskutoimitusta.*

(2) Tarkastellaan joukossa $\mathbb{Z}$ ekvivalenssirelaatiota $\equiv_n$, jossa $x \equiv ny$ tarkoittaa, että $x - y$ on jaollinen luvulla n, missä $n \in \mathbb{N}_+ = 1, 2, \ldots$ on kiinteä luku. Esimerkissä 1.70 olemme osoittaneet, että $\equiv_n$ on ekvivalenssirelaatio joukossa $\mathbb{Z}$. Osoitetaan, että $\equiv_n$ on yhteensopiva kokonaislukujen yhteenlaskun kanssa. Oletetaan, että $x \equiv_n x'$, $y \equiv_n y'$. Tämä tarkoittaa sitä, että $x - x' = kn$ ja $y - y' = ln$ joillakin $k, l \in \mathbb{Z}$. Tällöin

$$(x + y) - (x' + y') = (x - x') + (y - y') = nk + ln = (k + l)n.$$

Relaation määritelmän nojalla tästä seuraa, että $(x + y) \equiv_n (x' + y')$, mikä pitikin todistaa.

Näin ollen tekijäjoukossa $\mathbb{Z}/\equiv_n = \mathbb{Z}_n$ eli kokonaislukujen modulo n muodostamassa joukossa voidaan määritellä laskutoimitus $+'$, joka periytyy kokonaislukujen yhteenlaskusta. Käytännössä tätäkin laskutoimitusta merkitään yksinkertaisesti symbolilla $+$ ja sanotaan kokonaislukujen modulo n yhteenlaskuoperaatioksi. Kokonaisluvuilla modulo n lasketaan samalla tavalla kuin kokonaisluvuilla, paitsi, että otetaan myös relaatio huomioon tarvittaessas. Esimerkiksi

$$2_4 + 5_4 = 7_4 = 3_4.$$

Tekijäjoukon indusoimaan laskutoimitukseen periytyvät luonnollisella tavalla joukon X alkuperäisen laskutoimituksen ominaisuudet.

Lemma 1.79. *Olkoon $\cdot$ laskutoimitus joukossa X. Olkoon $\sim$ joukon X ekvivalenssirelaatio, joka on yhteensopiva laskutoimituksen $\cdot$ kanssa. Olkoon $\cdot'$ laskutoimituksen $\cdot$ indusoima laskutoimitus tekijäjoukossa $X/\sim$. Tällöin seuraavat väitteet pätevät.*

(i) Jos laskutoimitus $\cdot$ on liitännäinen, myös laskutoimitus $\cdot'$ on liitännäinen.

(ii) Jos laskutoimitus $\cdot$ on vaihdannainen, myös laskutoimitus $\cdot'$ on vaihdannainen.

(ii) Oletetaan, että joukolla X on neutraalialkio e laskutoimituksen $\cdot$ suhteen. Tällöin $\bar{e}$ on joukon $X/\sim$ neutraalialkio laskutoimituksen $\cdot'$ suhteen. Erityisesti tällöin myös joukolla $X/\sim$ on neutraalialkio laskutoimituksen $\cdot'$ suhteen.

(v) Olkoon $x \in X$. Oletetaan, että x:llä on joukossa X käänteisalkio x^{-1} laskutoimituksen $\cdot$ suhteen. Tällöin sen ekvivalenssiluokalla $\bar{x}$ on joukossa $X/\sim$ käänteisalkio laskutoimituksen $\cdot'$ suhteen, itse asiassa tällöin pätee

$$\bar{x}^{-1} = \bar{x^{-1}}.$$

Todistus. Koska kanoninen projektio $p\colon X \to X/\sim$ on yhteensopiva laskutoimitusten $\cdot$ ja $\cdot'$ suhteen, Lemman väitteet seuravat suoraan Lemmasta 1.39. □

Erityisesti sellaiset struktuurit kuin ryhmät ja renkaat ”säilyvät” kun siirrytään tekijäjoukkoon laskutoimitusten kanssa yhteensopivan ekvivalenssirelaation suhteen.

Seuraus 1.80. *Olkoon $(G, \cdot)$ ryhmä ja olkoon $\sim$ joukon X ekvivalenssirelaatio, joka on yhteensopiva laskutoimituksen $\cdot$ kanssa. Tällöin tekijäjoukko $G/\sim$ indusoidulla laskutoimituksella $\cdot'$ varustettuna on ryhmä $(G/\sim, \cdot')$. Sanomme tätä ryhmää ryhmän G* tekijäryhmäksi. *Kanoninen kuvaus $p\colon G \to G/\sim$ on tällöin ryhmähomomorfismi.*

Jos $(G, \cdot)$ on Abelin ryhmä, myös $(G/\sim, \cdot')$ on Abelin ryhmä.

Seuraus 1.81. *Olkoon $(R, +, \cdot)$ rengas ja olkoon $\sim$ joukon X ekvivalenssirelaatio, joka on yhteensopiva sekä laskutoimituksen $+$, että laskutoimituksen $\cdot$ kanssa. Tällöin tekijäjoukko $R/\sim$ indusoiduilla laskutoimituksilla $+'$ ja $\cdot'$ varustettuna on rengas $(R/\sim, +', \cdot')$. Sanomme tätä rengasta renkaan R* tekijärenkaaksi. *Kanoninen kuvaus $p\colon R \to R/\sim$ on tällöin rengashomomorfismi.*

Jos rengas R on kommutatiivinen, myös tekijärengas $R/\sim$ on kommutatiivinen rengas.

Todistus. Kaikki renkaan/kommutatiivisen renkaan ehdot kolmikolle $(R/\sim, +', \cdot')$ seuraavat Lemmasta 1.79 osittelulakien lukuunottamatta. Niitä voi todistaa samalla tavalla kuin Lemmassa 1.79 on tehty muiden ehtojen kohdalla (HT). □

Esimerkki 1.82. *Esimerkissä 1.78 olemme näyttäneet, että relaatio $\equiv_n$ kokonaislukujen $\mathbb{Z}$ joukossa on yhteensopiva kokonaislukujen yhteenlaskun kanssa. Koska $(\mathbb{Z}, +)$ on Abelin ryhmä, Seurauksesta 1.80 seuraa, että kokonaisluvut modulo n muodostavat Abelin ryhmän $(\mathbb{Z}_n, +)$ yhteenlaskun suhteen. Tämän ryhmän neutraalialkio on 0_n eli nollan ekvivalenssiluokka. Alkion a_n vasta-alkio on $(-a)_n$. Koska kyseessä on additiivisesti merkitty ryhmälaskutoimitus, voidaan puhua vähennyslaskusta. Esimerkiksi*

$$5_7 - 6_7 = (-1)_7 = -1_7 = -8_1.$$

Ryhmä $(\mathbb{Z}_n, \cdot)$ antaa esimerkin äärellisestä ryhmästä. Tässä ryhmässä on tasan n alkiota.

Ekvivalenssirelaatio $\equiv_n$ on yhteensopiva myös kokonaislukujen kertolaskun *kanssa. Tämän todistaminen jätetään harjoitustehtäväksi. Koska $(\mathbb{Z}, +, \cdot)$ on kommutatiivinen rengas, Seurauksesta 1.81 seuraa, että kokonaislukujen modulo n muodostama joukko $\mathbb{Z}_n$ muodostaa* kommutatiivisen renkaan *$(\mathbb{Z}_n, +, \cdot)$ indusoidun yhteenlaskun ja kertolaskun suhteen. Tämä on esimerkki äärellisestä renkaasta, jossa on n alkiota. Kertolaskun neutraalialkio on 1_n. Esimerkiksi renkaassa $\mathbb{Z}_6$ pätee*

$$2_6 \cdot 3_6 = 6_6 = 0_6.$$

Huomaa, että $2_6, 3_6 \neq 0_6$ renkaassa $\mathbb{Z}_6$. Näin ollen renkaassa kahden nollasta eroavan alkion tulo voi olla nolla eli koulusta tuttu nollasääntö *ei välttämälttä päde mielivaltaisessa renkaassa.*

Normaalit aliryhmät ja ideaalit

Algebrassa ei yleensä esitetä tekijäryhmiä ja -renkaita muodossa $G/\sim$ tai $R/\sim$, vaan sen sijaan on tapana käsitellä niitä niin sanottujen *normaalien aliryhmien* (ryhmien tapauksessa) tai *ideaalien* (renkaiden tapauksessa) kautta.

Ryhmien tapaus - Normaalit aliryhmät

Olkoon G *ryhmä* ja olkoon $N < G$ sen aliryhmä. Sanomme, että N on **normaali** aliryhmä jos kaikilla $x \in G$ ja $n \in N$ pätee $xnx^{-1} \in N$. Jos $N < G$ on normaali aliryhmä, merkitään myös $N \triangleleft G$. Tällä kurssilla emme motivoi tätä ehtoa ja normaalin aliryhmän käsitettä kunnolla, tämä tehdään algebran peruskursseilla. Mainitsemme kuitenkin seuraavaa osittain motivaationa toimivaa tärkeätä tulosta.

Lemma 1.83. *Olkoon $f\colon (G, \cdot) \to (G', \cdot')$ ryhmähomomorfismi. Tällöin sen ydin $N = \operatorname{Ker} f$ on ryhmän G normaali aliryhmä.*

Todistus. Se, että ydin on aina aliryhmä, todettiin homomorfismien yhteydessä aikaisemmin.

Oletetaan, että $n \in \operatorname{Ker} f$ ja $x \in G$. Ensimmäinen ehto tarkoittaa sitä, että $f(n) = e'$, missä e' on ryhmän G' neutraalialkio. Koska f on homomorfismi, saadaan

$$f(xnx^{-1}) = f(x)f(n)f(x)^{-1} = f(x)e'f(x)^{-1} = f(x)f(x)^{-1} = e'.$$

Näin ollen $xnx^{-1} \in N$. □

Myöhemmin nähdään, että edellisen lemman väitteen käänteinen väite myös pitää paikkaansa - jokainen normaali aliryhmä on jonkun homomorfismin ydin. Näin ollen normaalit aliryhmät ovat täsmälleen sama asia kuin ryhmähomomorfismien ytimet. Tämä selittää, ainakin osittain, miksi normaalit aliryhmät ovat tärkeitä.

Esimerkki 1.84. *Oletetaan tunnetuksi lineaarialgebran peruskurssilta, että* (2×2)*-matriiseille määritelty* determinanttikuvaus $\det\colon M(2\times 2;\mathbb{R}) \to \mathbb{R}$ *on yhteensopiva matriisen kertolaskun ja reaalilukujen kertolaskun suhteen,*

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

kaikilla $A, B \in M(2\times 2;\mathbb{R})$*. Lisäksi kääntyvän matriisin determinantti on aina nollasta eroava. Rajoittamalla determinanttikuvaus kääntyvien* (2×2)*-matriisien muodostamaan ryhmään* $GL(2;\mathbb{R})$ *saadaan* ryhmähomomorfismi $\det\colon GL(2;\mathbb{R}) \to \mathbb{R}^*$*. Edellisen lemman nojalla tämän homomorfismin ydin*

$$SL(2;\mathbb{R}) = \{A \in M(2\times 2;\mathbb{R}) \mid \det A = 1\}$$

on ryhmän $GL(2;\mathbb{R})$ *normaali aliryhmä. Tätä ryhmä sanotaan* erikoiseksi lineaariseksi ryhmäksi *(engl. special linear group).*

Olkoon $H \subset GL(2;\mathbb{R})$ *sellaisten kääntyvien matriisien joukko, joka ovat muotoa*

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

Helposti nähdään, että $H < GL(2;\mathbb{R})$ *(HT). Kuitenkin* H *ei ole ryhmän* $GL(2;\mathbb{R})$ *normaali aliryhmä. Esimerkiksi valitsemalla*

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in H$$

ja

$$B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in GL(2;\mathbb{R}),$$

saadaan

$$BAB^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \notin H$$

(tarkista).

Siirrytään ekvivalenssirelaatioihin. Olkoon G *ryhmä* ja olkoon $\sim$ joukon G ekvivalenssirelaatio, joka on yhteensopiva G:n laskutoimituksen kanssa. Tällöin, edellisen aliluvun nojalla, tekijäjoukossa $G/\sim$ voidaan määritellä indusoitu laskutoimitus $\cdot'$, siten että $(G/\sim, \cdot')$ on ryhmä ja kanoninen homomorfismi $p\colon G \to G/\sim$ on *ryhmähomomorfismi.* Tekijäryhmän $G/\sim$ neutraalialkio on ryhmän G neutraalialkion e ekvivalenssiluokka $\bar{e}$. Kuten jokaisella ryhmähomomorfismilla, homomorfismilla p on *ydin*

$$N = \operatorname{Ker} p = p^{-1}(\bar{e}) = \{x \in G \mid p(x) = \bar{e} = p(e)\} = \{x \in G \mid x \sim e\} = \bar{e}, \tag{1.85}$$

joka Lemman 1.83 mukaan on ryhmän G *normaali aliryhmä*. Yhtälöstä (1.85) nähdään, toisaalta, että $\operatorname{Ker} p$ ei ole mitään muuta, kuin neutraalialkion e ekvivalenssiluokka $\bar{e}$.

Olkoot $x, y \in X$. Koska relaatio $\sim$ on yhteensopiva ryhmän laskutoimituksen kanssa, ehdoista $x \sim y$, $y^{-1} \sim y^{-1}$ saadaan ehto $xy^{-1} \sim yy^{-1} = e$. Kääntäen, jos pätee $xy^{-1} \sim e$, niin samalla tavalla käyttämällä hyväksi myös ehtoa $y \sim y$, saadaan, että $x = xy^{-1}y \sim ey = y$. Olemme näyttäneet, että $x \sim y$ on yhtäpitävä ehdon $xy^{-1} \in N$ kanssa. Näin ollen, ekvivalenssirelaatio $\sim$ voidaan määritellä *puhtaasti algebrallisesti* erään normaalin aliryhmän $N = \operatorname{Ker} p$ avulla, ehdolla $xy^{-1} \in N$. Osoittautuu, että käänteinen konstruktio tuottaa myös tekijäryhmän.

Lemma 1.86. *Olkoon N ryhmän G* mielivaltainen normaali *aliryhmä. Määritellään joukossa G relaatio $\sim_N$ ehdolla $x \sim_N y$ jos ja vain jos $xy^{-1} \in N$. Tällöin*

(i) Relaatio $\sim_N$ on ekvivalenssirelaatio.

(ii) Relaatio $\sim_N$ on yhteensopiva laskutoimituksen $\cdot$ kanssa.

(iii) $N = \bar{e}$ on neutraalialkion e ekvivalenssiluokka relaation $\sim_N$ suhteen.

(iv) Alkion $x \in G$ ekvivalenssiluokka on

$$\bar{x} = xN = Nx,$$

missä

$$xN = \{xn \mid n \in N\}$$

ja vastaavasti

$$Nx = \{nx \mid n \in N\}.$$

Todistus. Ensimmäisen väitteen todistus jätetään harjoitustehtävänä. Osoitetaan, että $\sim_N$ on yhteensopiva laskutoimituksen $\cdot$ kanssa. Oletetaan, että $x \sim_N y$, $x' \sim_N y'$ eli $xy^{-1} = n \in N$ ja $x'y'^{-1} = n' \in N$. Tällöin suorana laskuna (jossa ensimmäisessä välivaiheessa käytetään myös Lemmaa 1.7) saadaan

$$(xx')(yy')^{-1} = xx'y'^{-1}y^{-1} = (xn'x^{-1})(xy^{-1}),$$

Tässä $xn'x^{-1} \in N$, koska N on normaali, ja $xy^{-1} \in N$ oletuksen nojalla. Koska N on aliryhmänä suljettu laskutoimituksen suhteen, saadaan

$$(xx')(yy')^{-1} = (xn'x^{-1})(xy^{-1}) \in N.$$

Relaation $\sim$ määritelmän nojalla tämä tarkoittaa sitä, $xx' \sim_N yy'$. Näin ollen $\sim_N$ on yhteensopiva ryhmän laskutoimituksen kanssa.

Ehdon (iv) osoittaminen jätetään harjoitustehtäväksi. Ehto (iii) on ehdon (iv) erikoistapaus kun $x = e$.

□

Edellinen lemma ja sitä edeltävä pohdinta osoittavat, että kaikki ryhmän G tekijäryhmät ovat täsmälleen muotoa $G/\sim_N$, missä N on jokin ryhmän G *normaali* aliryhmä ja $\sim_N$ on ehdolla $xy^{-1} \in N$ määritelty relaatio. Tekijäryhmää $G/\sim_N$ on tapana merkitä yksinkertaisesti G/N. Tekijäryhmän G/N neutraalialkio on ekvivalenssiluokka $\bar{e}$, joka

on edellisen lemman nojalla sama kuin joukko N. Alkion $x \in G$ ekvivalenssiluokka on puolestaan joukko

$$xN = \{xn \mid n \in N\}.$$

Tekijäryhmän G/N alkiot ovat tämän nojalla muotoa xN. Tällä merkintätavalla tekijäryhmässä G/N pätee

$$xN \cdot' yN = (xy)N,$$
$$(xN)^{-1} = x^{-1}N.$$

Huomaa, että normaali aliryhmä N on kanonisen projektion $p\colon G \to G/N$ *ydin*. Tästä seuraa jo edellä luvattu Lemman 1.83 käänteinen tulos - jokainen normaali aliryhmä on jonkun ryhmähomomorfismin ydin. Näin ollen normaalit aliryhmät ja ryhmähomomorfismien ytimet ovat sama asia.

Olkoon $(G, +)$ *vaihdannainen* (eli Abelin) ryhmä, jonka laskutoimitus $+$ on merkitty additiivisesti. Olkoon H mikä tahansa ryhmän G aliryhmä. Tällöin normaalisuuden ehto tarkoittaa sitä, että $x + h + (-x) \in H$ kaikilla $h \in H$ ja $x \in G$. Mutta vaihdannaisuuden nojalla

$$x + h + (-x) = h + x + (-x) = h + 0 = h \in H.$$

Toisin sanoen *mikä tahansa Abelin ryhmän G aliryhmä H on normaali*, joten voimme aina muodostaa myös tekijäryhmän G/H. Vastaava ekvivalenssirelaatio on tällöin määritelty ehdolla $x - y \in H$. Alkion $x \in G$ ekvivalenssiluokka on tällöin $x + H$, tekijäryhmän G/H nolla-alkio on $0 + H = H$ ja alkion $x + H$ vasta-alkio on $-x + H$. Ekvivalenssiluokilla lasketaan seuraavasti:

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

Renkaiden tapaus - Ideaalit

Olkoon $(R, +, \cdot)$ *rengas* ja olkoon $I \subset R$ sen osajoukko. Sanomme, että I on renkaan R **ideaali** jos seuraavat ehdot toteuttuvat.

(1) $(I, +)$ on Abelin ryhmän $(R, +)$ aliryhmä.

(2) Kaikilla $x \in I$ ja $a \in R$ pätee $xa \in I$ ja $ax \in I$.

Ideaalit toimivat renkkaiden maailmassa samalla tavalla kuin normaalit aliryhmät ryhmien maailmassa. Tämän osion sisältö onkin täysin analoginen edellisen, jossa käsittelemme ryhmien ekvivalenssirelaatiota normaalien aliryhmien kautta, kanssa.

Nolla-alkion muodostama yksiö $\{0_R\}$ on aina renkaan R ideaali, niin sanottu *triviaali ideaali*. Myös koko rengas eli R on itsensä ideaali.

Lemma 1.87. *Olkoon $f\colon (R, +, \cdot) \to (R', +', \cdot')$ rengashomomorfismi. Tällöin sen ydin*

$$I = \operatorname{Ker} f = \{r \in R \mid f(r) = 0_R\}$$

on renkaan R ideaali.

Todistus. Harjoitustehtävä. □

Esimerkki 1.88. *Kokonaislukujen renkaan $(\mathbb{Z}, +, \cdot)$ kaikki ideaalit ovat muotoa $n\mathbb{Z}$ jollakin $n \in \mathbb{Z}$. Nimittäin, olkoon I renkaan $\mathbb{Z}$ ideaali. Tällöin $(I, +)$ on erityisesti ryhmän $(\mathbb{Z}, +)$ aliryhmä. Esimerkin 1.59 mukaan $I = n\mathbb{Z}$ jollakin $n \in \mathbb{Z}$. Kääntäen helposti nähdään, että osajoukko $n\mathbb{Z}$ toteuttaa ideaalin määritelmän 1.8. Vaihtoehtoisesti voidaan todeta, että edellisessä aliluvussa konstruoidun projektion $p\colon \mathbb{Z} \to \mathbb{Z}/\equiv_n$ ydin on tasan $n\mathbb{Z}$, jolloin väite seuraa edellisestä lemmasta.*

Olkoon R rengas ja olkoon $\sim$ joukon R ekvivalenssirelaatio, joka on yhteensopiva sekä renkaan yhteenlaskun, että renkaan kertolaskun suhteen. Tällöin Lemman 1.81 nojalla tekijäjoukossa $R/\sim$ voidaan määritellä indusoidut laskutoimitukset $+'$, $\cdot'$, siten, että $(R/\sim, +', \cdot')$ on rengas ja kanoninen homomorfismi $p\colon R \to R/\sim$ on *rengashomomorfismi*. Tekijärenkaan $R/\sim$ nolla-alkio on tällöin renkaan R nolla-alkion 0_R ekvivalenssiluokka $\overline{0_R}$. Kuten jokaisella rengashomomorfismilla, homomorfismilla p on *ydin*

$$I = \operatorname{Ker} p = p^{-1}(\overline{0_R}) = \{x \in R \mid p(x) = \overline{0_R} = p(0_R)\} = \{x \in R \mid x \sim 0_R\} = \overline{0_R}, \tag{1.89}$$

joka Lemman 1.87 mukaan on renkaan R *ideaali*. Yhtälöstä (1.89) nähdään, toisaalta, että $\operatorname{Ker} p$ ei ole mitään muuta, kuin nolla-alkion 0_R ekvivalenssiluokka $\overline{0_R}$.

Olkoot $x, y \in R$. Koska relaatio $\sim$ on yhteensopiva renkaan laskutoimitusten kanssa, se on erityisesti yhteensopiva yhteenlaskun $+$ suhteen. Koska $(I, +)$ on Abelin ryhmän $(R, +)$ (normaali) aliryhmä, edellisen osion normaalien aliryhmien ja ryhmien ekvivalenssirelaatioiden yhteys pätee erityisesti ekvivalenssirelaatiolle $\sim$ ryhmässä $(R, +)$. Erityisesti tiedämme jo, että $x \sim y$ jos ja vain jos $x - y \in I$. Näin ollen, ekvivalenssirelaatio $\sim$ voidaan määritellä *puhtaasti algebrallisesti* erään ideaalin $I = \operatorname{Ker} p$ avulla. Kuten ryhmien tapauksessa, osoittautuu, että myös renkkaille yhtä hyvin toimii käänteinen konstruuktio.

Lemma 1.90. *Olkoon I renkaan R* ideaali. *Määritellään joukossa R relaatio $\sim_I$ ehdolla $x \sim_I y$ jos ja vain jos $x - y \in I$. Tällöin*

(i) Relaatio $\sim_I$ on ekvivalenssirelaatio.

(ii) Relaatio $\sim_I$ on yhteensopiva renkaan laskutoimitusten $+$ ja $\cdot$ kanssa.

(iii) $I = \overline{0_R}$ on nolla-alkion 0_R ekvivalenssiluokka relaation $\sim_I$ suhteen.

(iv) Alkion $x \in R$ ekvivalenssiluokka on

$$\bar{x} = x + I = I + x.$$

Todistus. Soveltamalla Lemman 1.86 tulosta ryhmään $(R, +)$ (jonka normaalina aliryhmänä I on), saadaan melkein kaikki tämänkin Lemman väitteet ilmaiseksi kaupan päälle osoitettua. Ainoa, mikä ei Lemmasta 1.86 ei seura, on se, että relaatio $\sim_I$ on yhteensopiva renkaan kertolaskun $\cdot$ kanssa. Osoitetaan tämä. Olkoot $x, y, x', y' \in R$ ja oletetaan, että $x \sim_I x'$, $y \sim_I y'$. Tällöin $x - x' \in I$ ja $y - y' \in I$. Saadaan

$$xy - x'y' = xy - xy' + xy' - x'y' = x(y - y') + (x - x')y'.$$

Koska $y - y' \in I$, ideaalin määritelmän ehdosta (2) nähdään, että $x(y - y') \in I$. Samalla tavalla nähdään, että $(x - x')y' \in I$. Koska I on aliryhmä, eli erityisesti suljettu yhteenlaskun suhteen, saadaan, että

$$xy - x'y' = x(y - y') + (x - x')y' \in I.$$

Tämä tarkoittaa sitä, että $xy \sim_I x'y'$, mitä pitikin todistaa. □

Edellinen Lemma ja sitä edeltävä pohdinta osoittavat, että kaikki renkaan R tekijärenkaat ovat täsmälleen muotoa $R/\sim_I$, missä I on jokin renkaan R *ideaali* ja $\sim_I$ on ehdolla $x - y \in I$ määritelty relaatio. Tekijäengasta $R/\sim_I$ on tapana merkitä yksinkertaisesti R/I. Tekijärenkaan R/I neutraalialkio on ekvivalenssiluokka $\overline{0_R} = 0 + I = I$. Alkion $x \in R$ ekvivalenssiluokka on puolestaan joukko

$$x + I = \{x + a \mid a \in I\}.$$

Tekijärenkaan R/I alkiot ovat tämän nojalla muotoa $x + I$. Tällä merkintätavalla tekijärenkaassa R/I pätee

$$(x + I) + (y + I) = (x + y) + I,$$
$$(x + I) \cdot (y + I) = (xy) + I,$$
$$-(x + I) = (-x) + I.$$

Kertolaksun ykkösalkio tekijärenkaassa R/I on renkaan R ykkösalkion 1_R ekvivalenssiluokka $1_R + I$.

Huomaa, että ideaali I on kanonisen projektion $p\colon R \to R/I$ *ydin*. Tästä seuraa jo edellä luvattu Lemman 1.87 käänteinen tulos - jokainen renkaan ideaali on jonkun rengashomomorfismin ydin. Näin ollen ideaalit ja rengashomomorfismien ytimet ovat sama asia.

Esimerkki 1.91. *Esimerkin (1.88) mukaan $n\mathbb{Z}$ on renkaan $(\mathbb{Z}, +, \cdot)$ ideaali jokaisella $n \in \mathbb{Z}$. Tekijärengas $\mathbb{Z}/n\mathbb{Z}$ ei ole mitään muuta kuin edellisessä aliluvussa tarkasteltu tekijärengas $\mathbb{Z}_n$ (kokonaisluvut modulo n).*

Tässä vaiheessa lukija saattaa ihmetellä, miksi emme puhuneet mitään erikseen kunnista ja niiden tekijäkunnista. Tämä johtuu siitä, että kunnalla ei ole mielenkiintoisia ideaaleja ja ainoa kunnan K "tekijäkunta" on (isomorfian vaille) kunta K itse. Osoitetaan tämä hieman yleisemmän tuloksen kautta.

Lemma 1.92. *Olkoon I renkaan R ideaali, joka sisältää ainakin yhden renkaassa R (kertolaskun suhteen) kääntyvän alkion $x \in I$. Tällöin $I = R$.*

Erityisesti kunnan K ainoat ideaalit ovat triviaali ideaali $\{0_K\}$ ja kunta K itse.

Todistus. Olkoon I renkaan R ideaali ja oletetaan, että on olemassa sellainen $x \in I$, jolla renkaassa R on olemassa käänteisalkio $x^{-1} \in R$. Tällöin, ideaalin määritelmän 1.8 nojalla pätee $1_R = xx^{-1} \in I$. Olkoon $r \in R$ mielivaltainen. Saman ideaalin määritelmän nojalla tällöin saadaan $y = y1_R \in I$. Näin ollen oletus johti siihen, että $I = R$.

Olkoon I kunnan K ideaali. Tällöin joko $I = \{0_K\}$ tai sisältää ainakin yhden $x \neq 0_K$. Jälkimmäisessä tapauksessa, koska K on kunta, K:ssä alkiolla x on olemassa käänteisalkio x^{-1}. Todistuksen ensimmäisen osan nojalla $I = K$. □

Edellisestä Lemmasta seuraa, että jos K on kunta, niin kaikki sen tekijärenkaat ovat muotoa $K/\{0_K\}$ tai K/K. Näistä edellinen on isomorfinen kunnan K kanssa ja jälkimmäinen on triviaali yhden alkion rengas.

Seuraus 1.93. *Olkoon $f\colon K \to K'$ kuntahomomorfismi. Tällöin f on injektiivinen ja kunta K on isomorfinen kunnan $f(K')$ kanssa.*

Todistus. Koska jokainen kuntahomomorfismi on erityisesti rengashomomorfismi, kuvauksen f ydin $I = f^{-1}(0_{K'})$ on kunnan K ideaali (Lemma 1.87). Edellisen Lemman nojalla $I = \{0_K\}$ tai $I = K$. Jälkimmäinen vaihtoehto ei kuitenkaan ole mahdollinen, sillä se tarkoittaisi, että $f(k) = 0$ kaikilla $k \in K$, mikä on vastoin oletusta $f(1_K) = 1_{K'}$. Näin ollen $I = \{0_K\}$ on triviaali ideaali. Osoitetaan, että f on injektio. Olkoot $x, y \in K$ siten, että $f(x) = f(y)$. Tällöin, koska f on rengashomomorfismi, saadaan

$$f(x - y) = f(x) - f(y) = 0_{K'},$$

joten $x - y \in I = \{0_K\}$. Tämä tarkoittaa sitä, että $x = y$. Näin ollen f on injektio.

Jos kuvauksen f maalijoukko rajoitetaan kuvauksen f kuvajoukkoon $f(K)$ (joka on kunnan K' alikunta), saadaan bijektiivinen kuntahomomorfismi $f\colon K \to f(K)$, eli kuntien välinen isomorfismi. □

Kokonaisluvut modulo n

Vaikka kunnista ei saada uusi mielenkiintoisia kuntia tekijäkunta-käsitteen avulla, joskus on mahdollista konstruoida kuntia muiden renkaiden tekijärenkaina. Tässä osiossa tutkimme milloin renkaan $(\mathbb{Z}, +, \cdot)$ tekijärengas $(\mathbb{Z}_n, +, \cdot)$ (kokonaisluvut modulo n) on kunta.

Olkoot $n, m \in \mathbb{Z}$. Esimerkin (1.88) mukaan $n\mathbb{Z}$ ja $m\mathbb{Z}$ ovat molemmat renkaan $\mathbb{Z}$ ideaaleja. Ei ole vaikeata osoittaa yleisesti, että renkaan R kahden ideaalin I, J *summa*

$$I + J = \{a + b \mid a \in I, b \in J\}$$

on myös renkaan R ideaali. Erityisesti

$$n\mathbb{Z} + m\mathbb{Z} = \{nk + ml \mid k, l \in \mathbb{Z}\}$$

on renkaan $\mathbb{Z}$ ideaali. Toisaalta esimerkin 1.88 nojalla kaikki $\mathbb{Z}$:n ideaalit ovat muotoa $r\mathbb{Z}$ jollakin $r \in \mathbb{Z}$. Näin ollen kaikilla $n, m \in \mathbb{Z}$ on olemassa $r \in \mathbb{Z}$ jolle pätee $n\mathbb{Z} + m\mathbb{Z} = r\mathbb{Z}$. Koska $r\mathbb{Z} = (-r)\mathbb{Z}$, voimme lisäksi olettaa, että $r \geq 0$.

Palautetaan mieleen, että kahden kokonaisluvun $n, m \in \mathbb{Z}$ *suurin yhteinen tekijä* $d = \mathrm{syt}(n, m)$ on sellainen ei-negatiivinen kokonaisluku, joka toteuttaa seuraavat ehdot:

- d on sekä luvun n, että luvun m tekijä.
- jos $c \in \mathbb{Z}$ on lukujen n ja m yhteinen tekijä, niin c on myös luvun d tekijä.

Lemma 1.94. *Olkoot $n, m \in \mathbb{Z}$ ja olkoon $r \in \mathbb{Z}_+$ sellainen, että $n\mathbb{Z} + m\mathbb{Z} = r\mathbb{Z}$. Tällöin r on lukujen n, m* suurin yhteinen tekijä*, merkitään $r = \mathrm{syt}(n, m)$. Erityisesti on olemassa $k, l \in \mathbb{Z}$ joille pätee*

$$\mathrm{syt}(n, m) = nk + ml.$$

Todistus. Koska $n \in n\mathbb{Z} \subset n\mathbb{Z} + m\mathbb{Z} = r\mathbb{Z}$, on olemassa $q \in \mathbb{Z}$ siten, että $n = rq$, toisin sanoen r on luvun n tekijä. Samalla tavalla nähdään, että r on luvun m tekijä. Näin ollen r on lukujen n ja m yhteinen tekijä. Koska $r \in r\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z}$, on olemassa $k, l \in \mathbb{Z}$ joille pätee

$$r = nk + ml.$$

Olkoon c jokin toinen lukujen n ja m yhteinen tekijä, $n = sq$, $m = tq$, $s, t \in \mathbb{Z}$. Tällöin

$$r = (sk)q + (tl)q = (sq + tl)q$$

eli q on luvun r tekijä. Olemme osoittaneet, että r todellakin on suurin lukujen n ja m yhteinen tekijä. □

Kokonaislukuja n, m sanotaan *suhteelliseksi alkuluvuiksi*, jos $\text{syt}(n, m) = 1$. Edellisestä Lemmasta seuraa, että jos n ja m ovat suhteellisia alkulukuja, on olemassa $k, l \in \mathbb{Z}$ siten, että

$$1 = nk + ml.$$

Myös käänteinen väite pätee - jos kahdelle kokonaisluvuille m, n on olemassa $k, l \in \mathbb{Z}$ siten, että $1 = nk + ml$, m ja n ovat suhteellisia alkulukuja. Nimittäin jokainen lukujen n ja m yhteinen tekijä c on välttämättä myös luvun $nk + ml = 1$ tekijä. Tämä on mahdollista jos ja vain jos $c = \pm 1$.

Lause 1.95. *Olkoon $n \geq 1$ ja tarkastellaan kokonaislukujen modulo n muodostamaa rengasta $(\mathbb{Z}_n, +, \cdot)$. Tällöin sen kääntyvien alkioiden ryhmä on*

$$\mathbb{Z}_n^* = \{m_n \mid m \text{ ja } n \text{ ovat suhteellisia alkulukuja}\}.$$

Todistus. Oletetaan, että m ja n ovat suhteellisia alkulukuja. Tällöin edellisen nojalla on olemassa $k, l \in \mathbb{Z}$ siten, että $1 = nk + ml$. Siirtymällä tässä yhtälössä lukuihin modulo n saadaan

$$1_n = n_n k_n + m_n l_n = m_n l_n,$$

koska $n_n = 0_n$. Näin ollen $m_k l_k = 1_n$, mistä seuraa, että alkiolla m_n on renkaassa $\mathbb{Z}_n$ käänteisluku l_k.

Kääntäen, olkoon m_n kääntyvä renkaassa $\mathbb{Z}_n$. Tällöin on olemassa $l_n \in \mathbb{Z}$ siten, että $m_n l_n = 1_n$, mikä tarkoittaa sitä, että $ml - 1 \in n\mathbb{Z}$. Tästä seuraa, että on olemassa kokonaisluku luku k, siten, että

$$ml - 1 = nk$$

eli $ml + n(-k) = 1$. Edellisen nojalla $\text{syt}(n, m) = 1$. □

Seuraus 1.96. *Kokonaislukujen modulo n rengas $(\mathbb{Z}_n, +, \cdot)$ on kunta jos ja vain jos n on alkuluku.*

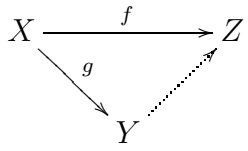
Todistus. $\mathbb{Z}_n$ on kunta jos ja vain jos $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0_n\}$. Edellisen Lauseen mukaan tämä on yhtäpitävä sen kanssa, että n on suhteellinen alkuluku jokaisen sellaisen $m \in \mathbb{Z}$, joka ei ole jaollinen n:llä. Tämä on mahdollista jos ja vain jos n on alkuluku. □

Esimerkiksi $\mathbb{Z}_2$ ja $\mathbb{Z}_5$ ovat kuntia, kun taas $\mathbb{Z}_4$ tai $\mathbb{Z}_{12}$ eivät ole.

Isomorfialauseet

Tekijästruktuurien tärkeimpiä sovelluksia ovat niin sanotut *isomorfialauseet* ja, yleisemmin, *hajoitelmalauseet*.

Aloitetaan tarkastelu yksinkertaisesta joukko-opillisesta tilanteesta, jossa ei vielä oteta algebraa huomioon. Olkoot X, Y, Z joukkoja ja olkoot $f\colon X \to Z$ ja $g\colon X \to Y$ kuvauksia, joilla on siis sama lähtöjoukko. Asetelma voidaan havainnollisesti esittää *diagrammina*



Jos tässä diagrammissa voidaan katkoviivan paikalle asettaa kuvaus $h\colon Y \to Z$, joka "tekee sitä kommutoivan", eli, täsmällisesti sanottuna, jos on olemassa sellainen $h\colon Y \to Z$ siten, että $h \circ g = f$, sanomme, että *kuvaus f voidaan hajottaa kuvauksen g kautta*.

Lemma 1.97. *Olkoot X, Y, Z joukkoja ja olkoot $f\colon X \to Z$ ja $g\colon X \to Y$ kuvauksia. Oletamme lisäksi, että on olemassa g on surjektio. Tällöin on olemassa kuvaus $h\colon Y \to Z$ siten, että $h \circ g = f$ jos ja vain jos seurava ehto toteutuu:*

- *Aina kun joillakin $x, x' \in X$ pätee $g(x) = g(x')$, pätee myös $f(x) = f(x')$.*

Lisäksi, jos kyseinen kuvaus h on olemassa, se on yksikäsitteinen.

Todistus. Oletetaan, että kuvaus $h\colon Y \to Z$ toteuttaa ehdon $h \circ g = f$. Olkoot $x, x' \in X$ sellaisia, että $g(x) = g(x')$. Tällöin

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

Näin ollen Lemman ehto toteutuu.

Kääntäen oletetaan, että $f(x) = f(x')$ aina kun $g(x) = g(x)'$. Olkoon $y \in Y$. Koska g on surjektio, on olemassa $x \in X$ siten, että $g(x) = y$. Jos $h\colon Y \to Z$ on sellainen, että pätee $h \circ g = f$, tästä saadaan, että

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

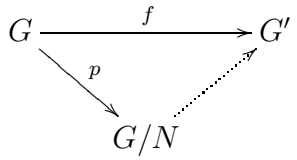
Tästä seuraa, että tällainen kuvaus h on yksikäsitteinen ja sen pitää olla määritelty säännöllä $h(y) = f(x)$, missä $x \in X$ on sellainen, että $g(x) = y$. Ongelma on siinä, että vaikka tällainen x on aina olemassa g:n surjektiivisuuden nojalla, se ei ole välttämättä yksikäsitteinen. Jos haluaa määritellä kuvauksen h kaavalla $h(y) = f(x)$, on tarkistettavaa, että tämä määritelmä ei riipu x:n valinnasta, eli jos $x' \in X$ on toinen alkio, jolla on ominaisuus $g(x') = y$, saadaan sama tulos eli $f(x) = f(x')$. Mutta jos $g(x) = y = g(x')$, oletuksesta seuraa, että $f(x) = f(x')$. Näin ollen yllä konstruoitu $h\colon X \to Y$ on hyvinmääritelty kuvaus. On vielä osoitettavaa, että $h \circ g = f$. Olkoon $x \in X$ ja olkoon $y = g(x) \in Y$. Tällöin x on sellainen, jolle pätee $g(x) = y$, joten kuvauksen h määritelmän mukaan

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

□

Siirrytään tarkastelemaan homomoforfisten kuvausten hajottamista algebrallisilla struktuureilla varustettujen joukkojen tapauksessa.

Ryhmien tapaus
Olkoot $(G, \cdot)$ ja $(G', \cdot')$ ryhmiä. Olkoon $f\colon G \to G'$ ryhmähomomorfismi. Olkoon $N \lhd G$ ryhmän G normaali aliryhmä ja olkoon $p\colon G \to G/N$ kanoninen projektio tekijäryhmälle. Tällöin kuvaukset f ja p muodostavat diagramin

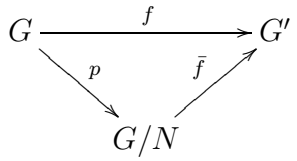


On tärkeätä tietää milloin homomorfismi f voidaan hajottaa kanonisen projektion p kautta, toisin sanoen, milloin homomorfismi f *indusoi* homomorfismin $\bar{f}\colon G/N \to G'$. Tälle indusoidulle homomorfismille, jos se on olemassa, pätee tällöin $\bar{f} \circ p = f$. Tämä voidaan kirjoittaa myös kaavana

$$\bar{f}(\bar{x}) = f(x)$$

kaikilla $x \in G$. Tämä määrittelee kuvauksen $\bar{f}$ alkioiden tasolla.

Lause 1.98. Ryhmähomomorfismien hajotelmalause
Olkoot $(G, \cdot)$ ja $(G', \cdot')$ ryhmiä. Olkoon $f\colon G \to G'$ ryhmähomomorfismi. Olkoon $N \lhd G$ normaali aliryhmä ja olkoon $p\colon G \to G/N$ kanoninen projektio. Tällöin on olemassa indusoidu ryhmähomomorfismi $\bar{f}\colon G/N \to G'$ jolle pätee $f = \bar{f} \circ p$,



jos ja vain jos $N \subset \operatorname{Ker} f$.
Jos tällainen kuvaus $\bar{f}$ on olemassa, niin se on yksikäsitteinen. Lisäksi pätee $\operatorname{Im} \bar{f} = \operatorname{Im} f$. Erityisesti $\bar{f}$ on surjektio jos ja vain jos f on surjektio.

Lisäksi $\bar{f}$ on injektio jos ja vain jos $N = \operatorname{Ker} f$.

Todistus. Unohdetaan aluksi algebra ja tutkitaan ensin, milloin on olemassa kuvaus $\bar{f}\colon G/N \to G'$ jolle pätee $f = \bar{f} \circ p$. Koska kanoninen projektio p on surjektio, voidaan soveltaa Lemman 1.97 tulosta. Sen mukaan kuvaus $\bar{f}$ on olemassa jos ja vain jos kaikilla $x, x' \in G$ yhtälöstä $p(x) = p(x')$ seuraa yhtälö $f(x) = f(x')$. Osoitetaan, että tämä ehto on yhtäpitävä ehdon $N \subset \operatorname{Ker} f$ kanssa.

Oletetaan, että kaikilla $x, x' \in G$ yhtälöstä $p(x) = p(x')$ seuraa yhtälö $f(x) = f(x')$. Olkoon $x \in N$. Tällöin $p(x) = \bar{x} = N = \bar{e}$, missä e on ryhmän G neutraalialkio, joten oletuksen nojalla $f(x) = f(e) = e'$, missä e' on ryhmän G' neutraalialkio. Olemme näyttäneet, että kaikilla $x \in N$ pätee $x \in \operatorname{Ker} f$, eli $N \subset \operatorname{Ker} f$.

Kääntäen oletetaan, että $N \subset \operatorname{Ker} f$ ja osoitetaan, että kaikilla $x, x' \in G$ yhtälöstä $p(x) = p(x')$ seuraa yhtälö $f(x) = f(x')$. Oletetaan, että $\bar{x} = p(x) = p(x') = \bar{x'}$. Tekijäryhmän G/N määritelmän nojalla tästä seuraa, että $xx'^{-1} \in N = \bar{e}$. Oletuksen nojalla

$xx'^{-1} \in \operatorname{Ker} f$ eli

$$f(x)f(x')^{-1} = f(xx'^{-1}) = e'.$$

Kertomalla tämän yhtälön molemmat puolet $f(x')$:llä oikealta saadaan $f(x) = f(x')$, mikä pitikin todistaa.

Olemme osoittaneet, että hajottava kuvaus $\bar{f}\colon G/N \to G'$ on olemassa (joukkojen välisenä kuvauksena) jos ja vain jos $N \subset \operatorname{Ker} f$. Lisäksi Lemman 1.97 nojalla tällainen $\bar{f}$ on yksikäsitteinen. Olkoot $A = \bar{x}$, $B = \bar{x'} \in G/N$, missä $x, x' \in G$ ovat luokkien A, B edustajat. Tällöin, koska f on ryhmähomomorfismi, saadaan kuvauksen $\bar{f}$ määritelmän nojalla

$$\bar{f}(AB) = \bar{f}(\overline{xx'}) = \bar{f}(p(xx')) = f(xx') = f(x)f(x') = \bar{f}(p(x))\bar{f}(p(x)) = \bar{f}(A)\bar{f}(B).$$

Näin ollen $\bar{f}$ on ryhmähomomorfismi.

Koska kanoninen projektio p on surjektio, indusoidun kuvauksen $\bar{f}$ kuvajoukolle pätee

$$\operatorname{Im} \bar{f} = \bar{f}(G/N) = \bar{f}(p(G)) = f(G) = \operatorname{Im} f.$$

Erityisesti $\bar{f}$ on surjektio tasan silloin kun f on surjektio.

Oletetaan, että $N \subsetneq \operatorname{Ker} f$ ja olkoon $x \in \operatorname{Ker} f$ sellainen, että $x \notin N$. Tällöin

$$\bar{f}(\bar{x}) = f(x) = e' = \bar{f}(\bar{e}),$$

vaikka $\bar{x} \neq \bar{e} = N$. Näin ollen tässä tapauksessa $\bar{f}$ ei ole injektio.

Oletetaan kääntäen, että $N = \operatorname{Ker} f$. Oletetaan, että $x, x' \in X$ ovat sellaisia, että

$$\bar{f}(\bar{x}) = f(x) = f(x') = \bar{f}(\bar{x'}).$$

Tällöin erityisesti $f(x^{-1}x') = f(x)^{-1}f(x) = e'$, joten $x^{-1}x \in \operatorname{Ker} f = N$. Tästä seuraa, että tekijäryhmässä pätee $\bar{x} = \bar{x'}$. Olemme osoittaneet, että $\bar{f}$ on injektio.

Näin ollen $\bar{f}$ on injektio jos ja vain jos $N = \operatorname{Ker} f$. □

Ottamalla hajotelmalauseessa tapauksen $N = \operatorname{Ker} f$, saadaan hajoitelmalauseen seurauksena niin sanottu *(ensimmäinen) isomorfialause*, joka kuuluu abstraktin algebran tärkeämpiin perustuloksiin.

Lause 1.99. Ryhmien Isomorfialause *Olkoot G, G' ryhmiä ja olkoon $f\colon G \to G'$ ryhmähomomorfismi. Tällöin indusoitu kuvaus $\bar{f}\colon G/\operatorname{Ker} f \to \operatorname{Im} f$, joka on määritelty ehdolla $\bar{f}(\bar{x}) = f(x)$, on* **ryhmäisomorfismi**.

Näin ollen *jokainen ryhmähomomorfismi* antaa synnyn eräälle ryhmäisomorfismille.

Esimerkkejä 1.100. *(1) Esimerkissä (1.45) olemme tarkastelleet ryhmähomomorfismia* $f\colon (\mathbb{R},+) \to (\mathbb{C}^*,\cdot)$, $f(x) = (\cos x, \sin x)$. *Esimerkissä (1.63) olemme todenneet, että kuvauksen* f *kuva* $f(\mathbb{R})$ *on ryhmä* $(S^1,\cdot)$ *(yksikköympyrällä sijaitsevat kompleksiluvut kertolaskulla varustettuna). Koska kompleksilukujen kertolaskun neutraalialkio on* $1_{\mathbb{C}} = (1,0)$, *trigonometriasta päätellään, että*

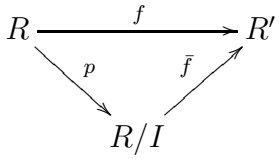
$$\operatorname{Ker} f = \{x \in \mathbb{R} \mid \cos x = 1, \sin x = 0\} = (2\pi)\mathbb{Z}$$

on luvun 2π *monikerroista koostuva ryhmä. Isomorfialauseesta saadaan, että tekijäryhmä* $(\mathbb{R}/(2\pi\mathbb{Z}),+)$ *on isomorfinen ryhmän* $(S^1,\cdot)$ *kanssa.*

Renkkaiden tapaus

Renkaille pätevät täysin analogiset hajotelma- ja isomorfismilauseet, kuten ryhmien teoriassa. Todistukset ovat samanlaisia, joten yksityiskohtien tarkastelu jätetään lukijalle harjoitustehtäväksi.

Lause 1.101. Rengashomomorfismien hajotelmalause
Olkoot $(R,+,\cdot)$ *ja* $(R',+',\cdot')$ *renkaita. Olkoon* $f\colon R \to R'$ *rengashomomorfismi. Olkoon* I *renkaan* R *ideaali ja olkoon* $p\colon R \to R/I$ *kanoninen projektio tekijärenkaalle. Tällöin on olemassa indusoidu rengashomomorfismi* $\bar{f}\colon R/I \to R'$ *jolle pätee* $f = \bar{f} \circ p$,



jos ja vain jos $I \subset \operatorname{Ker} f$.
Jos tällainen kuvaus $\bar{f}$ *on olemassa, niin se on yksikäsitteinen. Lisäksi pätee* $\operatorname{Im}\bar{f} = \operatorname{Im} f$. *Erityisesti* $\bar{f}$ *on surjektio jos ja vain jos* f *on surjektio.*

Lisäksi $\bar{f}$ *on injektio jos ja vain jos* $I = \operatorname{Ker} f$.

Lause 1.102. Renkaiden Isomorfialause *Olkoot* R, R' *renkaita ja olkoon* $f\colon R \to R'$ *rengashomomorfismi. Tällöin indusoitu kuvaus* $\bar{f}\colon R/\operatorname{Ker} f \to \operatorname{Im} f$, *joka on määritelty ehdolla* $\bar{f}(\bar{x}) = f(x)$, *on* **rengasisomorfismi**.

Näin ollen *jokainen rengashomomorfismi* antaa synnyn eräälle rengasisomorfismille.

Esimerkki 1.103.

Olkoon $p\colon \mathbb{Z} \to \mathbb{Z}_3$ *kanoninen projektio tekijärenkaalle, joka on renkaiden välinen homomorfismi. Olkoon* $I = 6\mathbb{Z}$. *Esimerkin (1.88) nojalla* I *on renkaan* $\mathbb{Z}$ *ideaali. Lisäksi* $I = 6\mathbb{Z} \subset 3\mathbb{Z} \operatorname{Ker} p$, *sillä* $6k = 3(2k)$ *kaikilla* $k \in \mathbb{Z}$. *Renkaiden hajotelmalauseen 1.101 nojalla on olemassa homomorfismin* p *indusoima rengashomomorfismi* $\bar{p}\colon \mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}_3$. *Alkioiden tasolla tämä on määritelty seuraavasti,*

$$\bar{p}(0_6) = 0_3,$$

$$\bar{p}(1_6) = 1_3,$$

$$\bar{p}(2_6) = 2_3,$$
$$\bar{p}(3_6) = 3_3 = 0_3,$$
$$\bar{p}(4_6) = 4_3 = 1_3,$$
$$\bar{p}(5_6) = 5_6 = 2_3,$$

Koska sisältyvyys $12\mathbb{Z} \subset 3\mathbb{Z}$ *on aito, kuvaus* $\bar{p}$ *ei ole injektio Lauseen 1.101 nojalla. Tämän näkee suoraan myös kuvauksen arvoista yllä, esim.* $\bar{p}(1_6) = \bar{p}(4_6)$*, vaikka* $1_6 \neq 4_6$*.*

Renkaan kokonaisluvut

Olkoon $(R, +, \cdot)$ rengas. Tällöin erityisesti $(R, +)$ on Abelin ryhmä, joten voimme muodostaa renkaan ykkösalkion $1_R \in R$ *monikerrat* $m \cdot 1_R$ jokaisella kokonaisluvulla $m \in \mathbb{Z}$. Määritellään kuvaus $\phi\colon \mathbb{Z} \to R$ kaavalla $\phi(m) = m \cdot 1$. Tällöin ϕ on renkaiden välinen homomorfismi (HT). Tämän kuvaksen kuvajoukko

$$\mathbb{Z}1_R = \{m1_R \mid m \in \mathbb{Z}\}$$

on kaikkien ykkösten monikertojen muodostama joukko ja ydin $\operatorname{Ker}\phi$ on jokin renkaan $\mathbb{Z}$ ideaali. Esimerkin (1.88) nojalla $\operatorname{Ker}\phi = n\mathbb{Z}$ jollakin $n \in \mathbb{Z}$. Koska $(-n)\mathbb{Z} = n\mathbb{Z}$, voimme olettaa, että $n \geq 0$. Isomorfialauseesta 1.99 seuraa, että on olemassa indusoidu **isomorfismi** tekijärenkaasta $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ renkaan R alirenkaalle $\mathbb{Z}1_R$. Tämän renkaan $\mathbb{Z}1_R$ alkiota sanotaan *renkaan kokonaisluvuiksi*. Ei ole vaikeata nähdä, että tämä on renkaan R *pienin alirengas*, siinä mielessä, että jokainen renkaan R alirengas sisältää alirenkaan $\mathbb{Z}1_R$.

Luonnollista lukua $n \in \mathbb{N}$ sanotaan renkaan R **karakteristikaksi**.

Renkaan kokonaislukua $m1_R$ merkitään usein yksinkertaisesti symbolilla m eli ”samastetaan” renkaan kokonaisluku $m1_R$ vastaavan ”tavallisen kokonaisluvun” kanssa. Nämä renkaan kokonaisluvut käyttäytävät algebrallisesti samalla tavalla kuin tavalliset kokonaisluvut, koska ϕ on renkaiden homomorfismi eli säilyttää yhteen-ja kertolaskun. On kuitenkin tärkeätä muistaa, että kuvauksen ϕ ei tarvitse olla injektio, joten renkaassa R voi käydä niin, että renkaan alkioina $k = l$, vaikka vastaavat kokonaisluvut k ja l ovatkin eri lukuja. Esimerkiksi renkaassa $\mathbb{Z}_3$ pätee näillä merkinnöillä $1 = 4$.

Tarkemmin sanottuna on olemassa kaksi mahdollisuutta.

Vaihtoehto 1: Yllä $n = 0$ eli renkaan R karakteristika on 0. Tällöin $\operatorname{Ker}\phi = 0\mathbb{Z} = 0$. Tässä tapauksessa ϕ on injektio, joten

$$\mathbb{Z}1_R \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\{0\} \cong \mathbb{Z}$$

ja erilaisia kokonaislukuja vastaavat erilaiset renkaan kokonaisluvut. Erityisesti R sisältää alirenkaan, joka on isomorfinen renkaan $\mathbb{Z}$ kanssa. Renkaan R ykkösalkiolle pätee $n1_R = 0_R$ jos ja vain jos $n = 0$.

Vaihtoehto 2: Yllä $n > 0$ eli renkaan R karakteristika n on positiivinen kokonaisluku. Tällöin $\operatorname{Ker}\phi = n\mathbb{Z}$. Tässä tapauksessa

$$\mathbb{Z}1_R \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

eli renkaan kokonaislukujen rengas on isomorfinen äärellisen renkaan $\mathbb{Z}_n$ kanssa. Renkaan ykkösalkiolle pätee

$$n1_R = \underbrace{1 + 1 + \ldots + 1}_{n \text{ kertaa}} = 0_R$$

ja renkaan karakteristika n on itse asiassa *pienin* positiivinen kokonaisluku k jolla on ominaisuus $k1_R = 0_R$.

Voidaan osoittaa, että kunnan karakteristika on aina joko nolla tai alkuluku (HT). Esimerkki nollakarakteristisesta kunnasta on rationaalilukujen kunta $\mathbb{Q}$ tai kompleksilukujen kunta $\mathbb{C}$. Kunta $\mathbb{Z}_p$, jossa p on alkuluku, on taas yksinkertainen esimerkki kunnasta, jonka karakteristika on alkuluku p.