Renkaista kuntia ja ryhmäteorian historiaa

Pro Gradu
Erkki Lohiniva
2124049
Matemaattisten tieteiden laitos
Oulun yliopisto
Syksy 2016

Sisältö

Johdanto

Tässä pro gradu -tutkielmassa syvennytään yhteen ryhmäteorian keskeisimmistä tuloksista ja tarkastellaan aihetta hieman historian valossa. Tarkoituksena on herättää lukijan mielenkiinto aihepiiriä kohtaan ja toisaalta ymmärtää kuinka tässäkin tutkielmassa käsiteltyyn teoriaan on päästy.

Vaikka matemaattiset määritelmät ja tulokset todistuksineen esitetään tässä tutkielmassa varsin sujuvasti, on niiden matka ollut pitkä 1700-luvun lopulta tähän päivään. Ensimmäinen luku pyrkiikin avaamaan sitä, kuinka paljon työtä ja eri matemaatikoiden panosta kokonaan uuden matematiikan osa-alueen syntyminen on todellisuudessa vaatinut. Ryhmäteorian perustan luoneelle Evariste Galois'lle annetaan tutkielmassa oma erityishuomio. Luvun 1 ryhmäteorian historian läpileikkauksen tekemiseen on käytetty lähdeteoksia [4] – [7].

Jatkossa siirrytään kohti ryhmäteorian tärkeää tulosta eli kuntalaajennusta. Se antaa meille mahdollisuuden konstruoida kommutatiivisesta renkaasta kunta sen maksimaalisen ideaalin avulla. Matkalla kuntalaajennukseen käsitellään tarvittavia peruskäsitteitä ekvivalenssirelaation, ryhmien, renkaiden ja kuntien teoriasta. Kuntalaajennusta ja sen taustateoriaa avataan esimerkein, jotta sen käyttömahdollisuudet selkiytyisivät paremmin. Esimerkeissä käytetään pitkälti hyödyksi jäännösluokkia, mutta kuntalaajennuksesta tarjotaan myös erilainen esimerkki Gaussin kokonaislukujen avulla.

Lopuksi käsitellään eräs toisenlainen laajennus osamääräkunnan muodossa. Tarkoituksena on osoittaa, kuinka kokonaisalueen avulla voidaan konstruoida uusi kuntarakenne. Tämä tapahtuu määrittelemällä uusi relaatio kokonaisalueessa ja siihen liittyvät ekvivalenssiluokat laskutoimituksineen. Tämän lisäksi esitellään osamääräkuntaan liittyviä tuloksia, kuten rationaalilukujen joukon muodostaminen kokonaislukujoukon osamääräkuntana, jonka todistus käydään lopuksi läpi.

Lukijalle on eduksi matemaattisen käsitteistön hallitseminen ja tiedot algebran perusteista. Tutkielman matemaattisen osan tekemiseen on käytetty lähdeteoksia [1] – [3].

1 Ryhmäteorian historiaa

Matematiikan historia on täynnä mielenkiintoisia yksityiskohtia, kuten minkä tahansa aiheen historia. Matematiikka tieteenä on hyvin konstruoivaa ja harvemmin innovaatiot ovat syntyneet yhden henkilön tai ryhmän toimesta. Näiden innovaatioiden taakse kätkeytyy lukuisia matemaatikoita mitä erilaisempien tarinoiden kera. Kuten seuraavissa kappaleissa kerrotaan, ryhmäteoria on kehittynyt vuosikymmenten tutkimustyön tuloksena eri matemaatikoiden työn tuloksena. Toisaalta esimerkiksi joukko-opin tarina on yksinkertaisempi.

Seuraavaksi tutustutaan ryhmäteorian taustoihin joukko-opin, ryhmäteorian ja abstraktin ryhmän käsitteiden historian kautta.

1.1 Joukko-opin synty

Joukko-opilla on tärkeä osa ryhmäteorian, johon kuntalaajennuskin kuuluu, synnyssä. Sen historia on erilainen verrattuna moniin muihin matematiikan osa-alueisiin, sillä yleensä matematiikan alueet ovat muotoutuneet pitkällisen tutkimuksen tuloksena, jossa eri ideat ovat kehittyneet lukuisten matemaatikkojen toimesta lopulliseen muotoonsa. Tästä poiketen joukko-oppi on käytännössä yhden miehen, venäläisen matemaatikon Georg Cantorin ($1845 - 1918$) työn tulosta.

Cantor työskenteli varhaisvuosiensa aikana lukuteorian parissa ja hän julkaisi lukuisia artikkeleita lukuteorian aihepiiristä vuosina $1867 - 1871$. Joukko-opin kannalta merkittävä vuosi oli 1872, jolloin Cantor matkusti Sveitsiin ja tapasi saksalaisen matemaatikon Richard Dedekindin ($1831 - 1916$). Cantor ja Dedekind ystävystyivät ja he lähettivät toisilleen lukuisia kirjeitä vuosien 1873-1879 aikana. Näillä keskusteluilla oli iso rooli Cantorin ajatuksien kehittymisessä ja Cantorin siirtymisessä lukuteoriasta trigonometrisiin sarjoihin. Näiden tutkimusten parissa Cantor esitti ensimmäiset ideansa joukko-opista sekä tärkeitä tuloksia irrationaalisista numeroista, joiden parissa Dedekind työskenteli. Vuonna 1874 Cantorin artikkeli, joka käsitteli ainakin kahta erilaista äärettömyyttä, julkaistiin saksalaisen matemaatikon August Crellen ($1780 - 1855$) lehdessä. Tätä voidaan pitää joukko-opin syntynä.

Seuraavassa kirjoituksessaan Cantor esitteli joukkojen ekvivalenttisuuden idean ja määritteli kahden joukon olevan ekvivalentteja eli "omaavan saman voiman", jos ne voidaan osoittaa yksi yhteen vastaaviksi. Termin "voima" Cantor omaksui sveitsiläisen matemaatikon Jakob Steinerin ($1796 - 1863$) julkaisuista. Artikkeli julkaistiin Crellen lehdessä. Samaisessa kirjoituksessa Cantor todisti, että joukko $\mathbb{R}^n$ on ekvivalentti joukon $\mathbb{R}$ kanssa. Näihin ai-

koihin Cantorin ajatuksia alettiin vastustaa niin matemaattisissa piireissä kuin Crellen julkaisun toimituksessa, joten Cantorin ystävä Dedekind joutuikin suostuttelemaan epäröivää Cantoria julkaisemaan kirjoituksensa. Tämä kirjoitus jäi hänen viimeisekseen Crellen julkaisussa.

Vuosien 1879 – 1884 aikana Cantor julkaisi kuusi osaa sisältävän tutkielman joukko-opista matematiikkaa käsittelevässä lehdessä Mathematische Annalen. Tutkimuksen julkaisua voidaan pitää rohkeana, sillä Cantorin ajatukset keräsivät yhä suurempaa vastustusta konstruktiivisen matematiikan nimeen vannovan tiedeyhteisön parissa.

Cantor kuitenkin jatkoi työtään joukko-opin parissa esitellen uusia määritelmiä ja antaen näin pohjan kokonaan uudelle matematiikan ajattelulle. [4]

1.2 Ryhmäteorian alku

Jos joukko-oppi voidaan määrittää yhden henkilön aikaansaannokseksi, ryhmäteorian alkuperän määritys on huomattavasti haasteellisempaa. Ryhmäteoria on enemmän lukuisten eri ideoiden luomus, jotka kumpuavat eri matemaattisten osa-alueiden kautta toisiinsa. Kolme merkittävintä matematiikan osa-aluetta ryhmäteorian kannalta ovat 1800-luvun alun geometria, 1700-luvun lopun lukuteoria sekä algebrallisten yhtälöiden teoria 1700-luvun lopulta aina permutaatioiden tutkimukseen saakka.

Geometriaa on tutkittu matematiikan historiaa tarkasteltaessa todella pitkään. Onkin mielenkiintoista tietää, mitä oleellista geometrian tutkimuksessa tapahtui 1900-luvun alussa, niin että se vaikutti ryhmäteorian syntyyn. Geometria oli alkanut menettää pelkästään metristä luonnettaan, kun projektiivisen ja epäeuklidisen geometrian tutkimus lisääntyi. Lisäksi muutos geometrian tutkimisesta n-ulotteisessa avaruudessa teki siitä abstraktia. Saksalainen matemaatikko August Möbius (1790 – 1868) alkoi vuonna 1827 luokitella geometrioita sen perusteella, että tietyn ryhmän sisällä tietyn geometrian tutkimat ehdot pysyvät muuttumattomina, vaikkei hänellä ollut mitään tietoa ryhmän käsitteestä. Vuonna 1832 sveitsiläinen matemaatikko Jakob Steiner (1796 – 1863) tutki aksiomaattisen geometrian käsitteitä, mistä tuli myöhemmin osa isometristen kuvausten ryhmän tutkintaa.

Vuonna 1761 sveitsiläinen matemaatikko Leonhard Euler (1707 – 1783) tutki modulaariaritmetiikkaa ja tarkemmin ottaen korkeampaan potenssiin korotettujen lukujen jakojäännöksiä modulossa n. Eulerin työ ei ymmärrettävästi sisältänyt ryhmäteorian termejä, mutta hän esitti esimerkin Abelin ryhmän hajotelmasta aliryhmien sivuluokkien avulla ja todisti, että aliryhmän kertaluku jakaa ryhmän kertaluvun. Vuonna 1801 saksalainen matemaatikko Johann Gauss (1777 – 1855) vei Eulerin tutkimuksia vielä pidemmälle

ja teki huomattavan paljon työtä modulaariaritmetiikan parissa lisäten reilusti Abelin ryhmän taustateoriaa. Hän tutki alkioiden kertalukuja ja todisti, ei kylläkään tässä asiayhteydessä, että jokaiselle syklisen ryhmän kertaluvun jakavalle luvulle on olemassa vastaavan kertaluvun omaava aliryhmä. Gauss tutki myös muita Abelin ryhmiä sekä kahden muuttujan toisen asteen yhtälöä $ax^2+2bxy+cy^2$, missä a, b, c ovat kokonaislukuja. Gauss tutki näiden yhtälöiden käyttäytymistä eri muunnoksilla ja muuttujan vaihdoilla. Hän jakoi yhtälöt omiin luokkiinsa ja sitten määritteli luokkien yhdistämisoperaation ja osoitti, ettei kolmen luokan yhdistämisen järjestyksellä ole väliä. Tämä tunnetaan nykyisin assosiaatiolain voimassaolona. Itseasiassa Gauss muodosti äärellisen Abelin ryhmän ja myöhemmin vuonna 1869 saksalainen matemaatikko Ernst Schering $(1824-1897)$, joka julkaisi Gaussin työt, löysi perustan Abelin ryhmille.

Vaikka tässä työssä ei tarkemmin käsitellä permutaatioita tai algebrallisia yhtälöitä, on niiden tutkimuksella tärkeä osa ryhmäteorian synnyssä. Ryhmäteorian kannalta merkittävänä voidaan pitää italialaisen matemaatikon Joseph-Louis Lagrangen $(1736-1813)$ aloittamia tutkimuksia siitä, miksi kolmannen ja neljännen asteen yhtälöt voidaan ratkaista algebrallisesti. Vaikka Lagrangen työssä voidaan nähdä permutaatioiden ryhmäteorian alkeita, Lagrange ei ikinä koonnut permutaatioitaan ylös, joten niiden yhteydessä ei puhuta ryhmistä.

Korkeamman asteen yhtälöiden parissa seuraavia merkittäviä askeleita otti italialainen matemaatikko Paolo Ruffini $(1765-1822)$, joka ensimmäisenä esitti, ettei viidennen asteen yhtälölle ole olemassa algebrallista ratkaisua. Vuonna 1799 hän julkaisi työn, jonka perustana toimi Lagrangen varhaisemmat työt, mutta lisäksi Ruffini esitti permutaatioiden ryhmän. Tarkoituksena oli demonstroida viidennen asteen yhtälön ratkaisemattomuus. Työ sisälsi sulkeumaominaisuuden, eli assosiaatiolain pätemisen permutaatioille. Ruffini jakoi permutaatioryhmänsä kahteen tyyppiin, joista voidaan käyttää modernin matematiikan termejä syklinen ryhmä ja ei-syklinen ryhmä. Ei-sykliset ryhmät Ruffini jakoi edelleen kolmeen tyyppiin, joita nykypäivän termeillä kutsutaan ei-transitiiviseksi ryhmäksi, transitiiviseksi ei-primitiiviseksi ryhmäksi ja transitiiviseksi primitiiviseksi ryhmäksi. Ruffinin työ viidennen asteen yhtälön ratkaisemattomuuden osoittamisessa sisälsi joitain puutteita ja pettyneenä kiinnostuksen puutteeseen työtäänsä kohtaan, Ruffini julkaisi lisää todistuksia. Vuonna 1802 julkaistussa tutkimuksessa hän esitti, että permutaatioiden ryhmä varustettuna jaottomilla yhtälöillä on transitiivinen, mikä vei hänen ymmärryksensä korkeammalle kuin Lagrangen.

Yhtenä suurena tekijänä permutaatioiden teorian kehityksessä pidetään ranskalaista matemaatikkoa Augustin Cauchya $(1789-1857)$. Hän julkaisi ensimmäisen tutkimuksen liittyen permutaatioihin vuonna 1815. Vuonna

1844 Cauchy julkaisi suurimman työnsä, jossa perustana oli permutaatioiden teoria itsessään. Hän esitti työssään merkintätavan permutaatioiden positiivisille ja negatiivisille potensseille, joka sisälsi potenssin nolla antaman identiteettikuvauksen, määritteli permutaation kertaluvun, esitteli syklimerkinnän ja käytti termiä "système des substitutions conjuguées"ryhmälle. Cauchy kutsui myös kahta permutaatiota samanlaisiksi, jos niiden syklirakenne oli sama sekä todisti, että ne ovat silloin myös konjugoituneita.

Vuonna 1824 norjalainen matemaatikko Niels Abel ($1802 - 1829$) esitti ensimmäisen hyväksytyn todistuksen viidennen asteen yhtälön ratkaisemattomuudelle. Abel hyödynsi todistuksessaan jo aiemmin esitettyjä ajatuksia juurien permutaatioista, mutta hänen työnsä ei vielä tuonut paljon uutta ryhmäteorian kehitykseen.

Ranskalainen matemaatikko Evariste Galois ($1811 - 1832$) teki läpimurron ryhmäteorian kehityksessä vuonna 1831. Hän oli ensimmäinen, joka todella ymmärsi, että yhtälön algebrallinen ratkaisu oli yhteydessä permutaatioiden ryhmän rakenteeseen. Vuonna 1832 hän huomasi, että eräät erikoiset aliryhmät, joita nykyään kutsutaan normaaleiksi aliryhmiksi, ovat keskeisessä osassa ongelmaa. Hän kutsui ryhmän hajotelmaa aliryhmän sivuluokkiin "varsinaiseksi hajotelmaksi", jos vasemmat ja oikeat sivuluokkahajotelmat ovat yhteneviä. Myöhemmin hän osoitti, että pienimmän kertaluvun yksinkertainen ei-Abelin ryhmä on kertaluvultaan 60. [5]

Galois eli hyvin poikkeuksellisen elämän. Hän oli erittäin älykäs nuori, jonka intohimona oli matematiikka. Hänen koulunsa kuvaili häntä ainutlaatuiseksi, oudoksi ja sulkeutuneeksi. Galois'n omat tutkimukset ajoivat koulutöiden edelle. Hänen ensimmäinen matematiikan opettajansa kirjoitti hänestä seuraavaa: "älykäs, merkittävää kehitystä, mutta ei riittävästi työskentelytekniikkaa". Lausunto kuvastaa hänen omapäisyyttään opiskelun suhteen. Galois'n elämä kohtasi ensimmäisen tragedian vuonna 1829, kun hänen isänsä teki itsemurhan. Galois jatkoi opintojaan ja tutkimuksiaan vaikeimpien matemaattisten ongelmien parissa. Hänet kuitenkin pidätettiin kahteen otteeseen. Ensimmäisellä kerralla pidätyksen syynä oli kuningas Ludvig Filip I uhkaaminen ja toisella kerralla kielletyn uniformun käyttö. Vankilassa hän yritti itsemurhaa toisten vankien onnistuessa estämään tämän. Galois menehtyi myöhemmin vain kaksikymmentävuotiaana kaksintaistelussa saamiinsa vammoihin, johon todennäköisesti liittyi Stephanie-Felice du Mote, Galois'n ihastuksen kohde. Kaksintaistelua edeltävänä iltana Galois kirjoitti ryhmäteoriaa käsitelleitä muistiinpanoja ja niistä löytyy merkintä "tässä esityksessä on jotain täydennettävää. Minulla ei ole aikaa". Vaikka tästä illasta liikkuu liioiteltuja huhuja, joiden mukaan Galois kirjoitti illan aikana kaiken mitä tiesi ryhmäteoriasta, niin juuri nämä paperit osoittautuivat tärkeiksi vuosia myöhemmin.

Galois'n kuoleman jälkeen hänen veljensä kopioi ja toimitti Galois'n matematiikkaa käsittelevät paperit muille matemaatikoille. Galois'n toiveena oli, että esimerkiksi Gauss olisi sanonut oman mielipiteensä hänen työstään. Kuitenkin vasta vuonna 1843 ranskalainen Joseph Liouville ($1809-1882$) sai käsiinsä nämä paperit. Hän ilmoitti Ranskan tiedeakatemialle, että Galois'n papereista oli löytynyt lyhyt ratkaisu vanhaan ongelmaan: "jaottoman polynomiyhtälön voi ratkaista radikaalien avulla". Liouville julkaisi nämä muistiinpanot lehdessään vuonna 1846. Vaikka Liouville ei suoraan tajunnutkaan kuinka merkittävästä asiasta oli kyse, voidaan tätä hetkeä pitää merkittävänä ryhmäteorian kannalta. Galois'n papereissa esittämää teoriaa kutsutaan tänä päivänä Galois'n teoriaksi. [6]

Vuonna 1851 italialainen matemaatikko Enrico Betti ($1823-1892$) alkoi julkaista töitä, joissa permutaatioiden teoria yhdistyi yhtälöiden teoriaan. Itseasiassa Betti oli ensimmäinen, joka todisti, että Galois'n ryhmä varustettuna yhtälöllä on oikeastaan permutaatioiden ryhmä moderneilla käsitteillä.

Ryhmäteoria jatkoi kehittymistään pienin askelin, mutta vuonna 1849, ennen Bettin julkaisuja otettiin mahdollisesti merkittävimmät kehitysaskeleet. Tuolloin englantilainen matemaatikko Arthur Cayley ($1821-1895$) julkaisi artikkelin, jossa hän yhdisti ajatuksensa permutaatioista Cauchyn työhön. Vuonna 1854 Cayley kirjoitti kaksi artikkelia, jotka ovat merkittäviä niiden abstraktia ryhmää koskevan käsityksen vuoksi. Tuohon aikaan ainoat tunnetut ryhmät olivat permutaatioryhmiä joten tämä olikin täysin uutta matematiikan aluetta. Cayley määritteli abstraktin ryhmän ja esitteli laskutaulut, jotka auttoivat abstraktin ryhmän käsitteen esittelyssä. Hän myös huomasi, että matriisit ja kvaterniot ovat ryhmiä. Vielä ilmestyessään Cayleyn artikkelit olivat edellä aikaansa, eivätkä ne saaneet paljon vaikutusta aikaan. Cayleyn palatessa aiheeseen vuonna 1878 julkaisemalla neljä artikkelia ryhmistä, joista yksi oli "ryhmien teoria", aika oli kypsä abstraktin ryhmän käsitteen nousulle matemaattisen tutkimuksen keskiöön. Cayley todisti mm. että kaikki äärelliset ryhmät voidaan esittää permutaatioiden ryhmänä.

Lukuisat matemaatikot jatkoivat ryhmäteorian parissa ja kaikki kulminoitui englantilaisen matemaatikon William Burnsiden ($1852-1927$) vuonna 1897 julkaisemaan kirjaan "Äärellisten ryhmien teoria" ja saksalaisen matemaatikon Heinrich Weberin ($1842-1913$) kaksiosaiseen algebran kirjaan, jotka julkaistiin vuosina 1895 ja 1896. Nämä kirjat vaikuttivat tulevien sukupolvien matemaatikoihin tehden ryhmäteoriasta ehkä merkittävimmän teorian 1900-luvun matemaatikoille. [5]

1.3 Abstraktin ryhmän käsite

Moderni määritelmä ryhmälle, joka löytyy myös tämän pro gradu -tutkielman luvusta 3, on varmasti kaikille matematiikkaa opiskelleille tuttu. Mistä tämä nykyään itsestään selvä määritelmä on tullut? Abstraktin ryhmän määritelmä oli itseasiassa vain pieni sivulinja ryhmäteorian kehityksessä 1800-luvulla.

Todetaan alkuun, että abstraktille ryhmälle oli itseasiassa kaksi eri merkitystä vuosien 1905 ja 1955 välillä. Ensimmäisen mukaan ryhmä määriteltiin neljän aksiooman kautta, kuten nykyään. Toisen mukaan ryhmä määriteltiin generaattoreiden ja relaatioiden kautta. Tässä kappaleessa tutustutaan ensimmäisen merkityksen kehitykseen.

Abstraktin ryhmän käsitteen syntyminen oli erittäin hidas prosessi. Sen juuret ulottuvat Galois'n ja Cauchyn työhön ja yhteydenpitoon. Galois määritteli ryhmän vuonna 1832, vaikka se julkaistiinkin vuosia myöhemmin Liouvillen toimesta, kuten tiedämme. Ensimmäinen versio Galois'n tärkeästä yhtälön algebrallisen ratkaisun sisältävästä tutkimuksesta oli jätetty Ranskan tiedeakatemiaan jo vuonna 1829. On löydetty todisteita tiedeakatemian arkistoista, että Cauchy yritti suostutella Galois'ta vetämään tutkimuksensa takaisin ja tuomaan uuden version siitä vuoden 1830 Grand Prixiin. Tiedetään myös, että Galois antoi uuden version tutkimuksestaan ranskalaiselle matemaatikolle Joseph Fourierille ($1768 - 1830$), jotta hän harkitsisi sitä Grand Prixiin vuoden 1830 maaliskuussa. Fourier kuitenkin menehtyi pian tämän jälkeen ja Galois'n artikkeli katosi samoihin aikoihin. Sitä ei siis ikinä otettu huomioon Gran Prixin voittajaa valittaessa. Palkinto myönnettiin sekä Abelille postuumisti että Jacobille heinäkuussa 1830.

Ranskalainen matemaatikko Siméon Poisson ($1781-1840$) kuitenkin pyysi Galois'ta jättämään kolmannen version työstään akatemialle ja työ jätettiin 17. tammikuuta 1831. Poisson arvosteli tämän version ja hylkäsi sen, mutta kirjoitti siitä myötämielisen raportin. Galois oli todistanut tulokset yleisesti, mutta artikkelissa käsiteltiin vain yhtälöitä joiden aste oli alkuluku. Poisson ei ymmärtänyt artikkelia ja ehdotti perustelujen viemistä vielä pidemmälle. Hänelle oli epäselvää kuinka Galois luokitteli radikaalien avulla ratkeavat yhtälöt.

Päivä ennen kohtalokseen koitunutta kaksintaistelua, Galois'n kirjoittamista muistiinpanoista löytyy merkintä, että: "jos eräs ryhmä sisältää substantit S ja T, sitten se sisältää myös substantin ST". Galois käytti hyvin laajasti ryhmiä paperissaan, joka käsitteli yhtälöitä, mutta ei antanut niille mitään määritelmiä. Ei siis ole ihme, ettei Poisson ymmärtänyt täysin Galois'n työtä, sillä se sisälsi monia tarkkoja laskuja ryhmässä, ennen kuin koko käsitettä oli edes määritelty.

Vuosi ennen kuin Liouville julkaisi Galois'n paperit, eli vuonna 1845,

Cauchy antoi ryhmälle oman määritelmänsä. Hän tutki substantteja (Cauchyn nimitys permutaatioille), joissa oli n kappaletta kirjaimia $x, y, z, ...$ ja määritteli johdetuiksi substanteiksi kaikki ne, jotka voidaan muodostaa kertomalla näitä substantteja keskenään missä tahansa järjestyksessä. Myöhemmin hän kutsui substanttien joukkoa yhdessä johdettujen substanttien kanssa "substanttien konjugaattisysteemiksi". Jonkin aikaa näitä kahta identtistä konseptia, ryhmää ja substanttien konjugaattisysteemiä, käytettiin yhtä aikaa. Vuodesta 1863 alkaen termistä ryhmä tuli standardi nimitys, kun ranskalainen matemaatikko Marie Jordan ($1838 - 1922$) kirjoitti arvostelun Galois'n työstä. Termi vahvistui Jordanin julkaistua päätyönsä ryhmäteoriasta, "Traité des substitutions et des algebraique" vuonna 1870. Kuitenkin Cauchyn termin "substanttien konjugaattisysteemi" käyttö jatkui 1880-luvulle asti.

Herää kysymys, kuinka paljon Cauchy sai vaikutteita omaan ryhmän määritelmäänsä Galois'n työstä? Tiedetään, että hän oli nähnyt Galois'n paperit Ranskan tiedeakatemiassa, mutta ne eivät sisältäneet tarkkaa ryhmän määritelmää. Toisaalta, hänen täytyi olla vähintään tiedostamattomasti ottanut vaikutteita Galois'n työstä. Sekä Galois että Cauchy määrittelivät ryhmän suljettuna omilla tahoillaan. Tänä päivänä tutut aksioomat assosiatiivisuus, ykkösalkio ja käänteisalkio eivät esiinny heidän määritelmissään. Tämä johtuu siitä, että molemmat työskentelivät permutaatioiden parissa, joten sulkeumaominaisuus oli ainoa välttämätön ominaisuus määritellä, muut seurasivat automaattisesti tästä. Cauchy kirjoittikin 25 artikkelia aiheesta syyskuun 1845 ja joulukuun 1846 välillä.

Ensimmäinen, joka yritti antaa abstraktia määritelmää ryhmälle oli Cayley. Hän kirjoitti artikkelin ryhmistä vuonna 1854, joka julkaistiin uudestaan kahdessa erillisessä julkaisussa vuonna 1878. Vuoden 1854 artikkelissa hän yritti antaa abstraktia määritelmää, jossa symboli θ operoi joukossa $(x, y, ...)$ siten, että $\theta(x, y, ...) = (x', y', ...)$, missä alkiot $x', y', ...$ ovat alkioiden $x, y, ...$ funktioita. Cayley määritteli identiteettisymbolin 1, joka jättää muut alkiot muuttamatta. Hän määritteli termin $\theta\varphi$ terminä, joka syntyy, kun ensin operoidaan symbolilla θ ja sitten symbolilla φ. Hän myös merkitsi, ettei $\theta\varphi$ tarvitse olla yhtä kuin $\varphi\theta$. Caley myös vaati, että assosiaatiolaki oli voimassa. Lopuksi hän linjasi, että mikä tahansa joukko vastaavilla symboleilla, joille pätee myös se, että minkä tahansa kahden alkion operaation tulos on joukon sisällä, on nimeltään ryhmä.

Tämä on tärkeä yritys ryhmän abstraktille määritelmälle, mutta silti Cayley ylisuoritti omiin taitoihinsa nähden. Se, mitä hän oli luonut oli hyvin sekavaa, sillä ei ollut ihan selvää, miksi hän vaati assosiaatiolain voimassaoloa, kun symbolit olivat operaattoreita. Kuten permutaatioille, assosiaatiolain voimassaolo seuraa automaattisesti operaatioille. Määritelmä ei ollut

kaikilta osin kovin onnistunut.

Vuonna 1878 Cayley kirjoitti, että: "ryhmä on määritelty alkioidensa kokoamien lakien pohjalta". Tämä ajatus oli peräisin Burnsidelta, saksalaiselta matemaatikolta Walter von Dyckiltä ($1856-1934$) ja muilta matemaatikoilta. Kirjassaan "Äärellisten ryhmien teoria" vuonna 1897 Burnside esitti seuraavanlaisen määritelmän: "Olkoon $A, B, C, ...$ operaatioiden joukon edustus, joka voidaan esittää samoilla olioilla tai olioiden joukkona." Lisäksi hän oletti, että mitkä tahansa kaksi operaatiota ovat erilliset siten, että ne eivät tuota samaa vaikutusta. Hän edellytti samoja ominaisuuksia kuin Cayley, eli sulkeumaa, assosiaatiolakia ja käänteisalkiota. Kuitenkin tämä määritelmä sai samaa kritiikkiä kuin Cayleyn määritelmä. Jos alkiot ovat operaatioita, miksi niiltä pitää edellyttää assosiaatiolakia? Hieman outoa on myös se, ettei Burnside vaatinut identiteettialkion olemassaoloa, vaikka sen olemassaolo voitiin päätellä alkion ja käänteisalkion olemassaolosta ja joukon sulkeutuneisuudesta. Burnside toisti täsmälleen saman määritelmän myös toisessa painoksessa kirjastaan, joka ilmestyi vuonna 1911.

On myös merkille pantavaa, että Cayley ja Burnside eivät kumpikaan vaatineet ryhmiltään äärellisyyttä. Määritelmät antoivat tarkoituksellisesti mahdollisuuden äärettömille ryhmille ja Burnside oli erityisesti kiinnostunut äärettömistä ryhmistä.

Tähän asti käytyä abstraktin ryhmän kehitystä voidaan pitää "englantilaisen koulun" tuotoksena. Seuraavaksi siirrytään käsittelemään samoihin aikoihin tapahtunutta ryhmäteorian kehitystä, jota voidaan pitää "eurooppalaisen koulun" työnä.

Vuonna 1870 preussilainen (nyk. Puola) matemaatikko Leopold Kronecker ($1823-1891$) antoi määritelmän ryhmälle täysin eri kontekstissa kuin aiemmin, eli jäännösluokkaryhmä lukuteoriassa. Hän tutki erityisesti äärellistä joukkoa, missä mistä tahansa kahdesta alkiosta voidaan tietyllä metodilla muodostaa kolmas alkio. Hän myös edellytti, että kommutatiivisuus ja assosiaatiolaki ovat voimassa. Tämän lisäksi oli voimassa, että $\theta'\theta'' \neq \theta'\theta'''$, jos $\theta'' \neq \theta'''$. Kroneckerin työ osoittautui erilliseksi kehitystyöksi, sillä hän ei sitonut sitä aiemmin ilmestyneeseen ryhmien parissa tehtyyn työhön. Kuitenkin, saksalainen matemaatikko Heinrich Weber ($1842-1913$) antoi vuonna 1882 hyvin samanlaisen määritelmän kuin Kronecker, mutta hän linkitti sen aiemmin tehtyyn työhön ryhmien parissa.

Weber määritteli ryhmän astetta h ja aivan kuten Kronecker jäännösluokkien parissa, joukko oli äärellinen. Hän vaati, että kahdesta systeemin alkiosta voidaan muodostaa kolmas systeemin alkio, siten että seuraavat lait pätevät: $(\theta_r\theta_s)\theta_t = \theta_r(\theta_s\theta_t) = \theta_r\theta_s\theta_t$ ja jos $\theta\theta_r = \theta\theta_s$, niin $\theta_r = \theta_s$. Varsinkin ensimmäisessä nähdään selkeitä yhteneväisyyksiä modernin ajan assosiaatiolain määritelmään.

Myös Weberin määritelmässä voidaan nähdä lieviä selkeyden puutteita. Hän itseasiassa määritteli puoliryhmän (ryhmä, joka on suljettu ja assosiaatiolaki on voimassa) varustettuna yhteisen tekijän ottamisella. Lisäksi määritellessään ryhmän äärelliseksi, se takaa ykkösalkion ja käänteisalkioiden olemassaolon. Weber itse osoitti, ettei määritelmä toimi äärettömille systeemeille kuuluisassa kirjassaan "Lehrbuch der Algebra", joka julkaistiin vuonna 1895. Hän osoitti, että määritelmä toimii vain äärellisille ryhmille ja ääretömille ryhmille vain, jos käänteisalkiot määritellään selvästi.

Abstraktin ryhmän käsite jatkoi kehittymistään 1900-luvulla englantilaisen ja eurooppalaisen tutkimustyön yhdistyessä. Kappaleessa mainittujen matemaatikkojen työ, kuten Weberin, vaikuttivat vielä pitkään ryhmäteorian kehittymiseen lopulta saaden nykyisen modernin muotonsa. [7]

2 Ekvivalenssirelaatio

Jotta päästäisiin niin sanotusti maaliin asti, täytyy lähteä perusteista liikkeelle. On tärkeää ymmärtää ekvivalenssirelaation määritelmä ja ekvivalenssiluokilla laskeminen, jotta ymmärrettäisiin tulevia määritelmiä paremmin.

2.1 Ekvivalenssirelaation teoria

Siirrytään ekvivalenssirelaation ja -luokan määritelmään.

Määritelmä 2.1.1. Joukon A binäärinen relaatio R on *ekvivalenssirelaatio*, jos

1. xRx aina, kun $x \in A$. Tätä ominaisuutta kutsutaan *refleksiivisyydeksi*, eli jokainen joukon A alkio on relaatiossa itsensä kanssa.

2. Jos xRy, niin yRx aina, kun $x, y \in A$. Tätä ominaisuutta kutsutaan *symmetrisyydeksi*, eli jos alkio x on relaatiossa alkion y kanssa, täytyy myös alkion y olla relaatiossa alkion x kanssa.

3. Jos xRy ja yRz, niin xRz aina, kun $x, y, z \in A$. Tätä ominaisuutta kutsutaan *transitiivisuudeksi*, eli jos alkio x on relaatiossa alkion y kanssa ja alkio y on relaatiossa alkion z kanssa, täytyy myös alkion x olla relaatiossa alkion z kanssa.

Jos R on ekvivalenssirelaatio ja $a \in A$, niin joukkoa

$$[a] = \{x \in A | xRa\}$$

sanotaan *alkion a määräämäksi ekvivalenssiluokaksi*.

Esitellään lopuksi kaksi hyödyllistä lausetta ekvivalenssirelaatioon liittyen.

Lause 2.1.2. *Jos R on ekvivalenssirelaatio, niin aRb jos ja vain jos $[a] = [b]$.*

Lause 2.1.3. *Jos R on joukon A ekvivalenssirelaatio, niin kaikkien ekvivalenssiluokkien yhdiste, eli unioni, on koko joukko A. Lisäksi, jos $[a] \neq [b]$, niin $[a] \cap [b] = \emptyset$.*

3 Ryhmät

Jotta päästään määrittelemään renkaiden kuntalaajennus, tarvitaan esitietoja, kuten ryhmän ja renkaan määritelmät. Ryhmä, rengas ja kunta muodostavat ketjun, jossa määritelmät täydentävät toisiaan.

3.1 Ryhmien teoria

Määritellään nyt jäännösluokat.

Määritelmä 3.1.1. Kokonaislukujen joukossa $\mathbb{Z}$ määritellyn ekvivalenssirelaation

$$xRy \Leftrightarrow x \equiv y \ (mod\ m) \Leftrightarrow m|\ x - y$$

ekvivalenssiluokkia kutsutaan *jäännösluokiksi modulo m.* Luvun y määräämästä jäännösluokasta *modulo m* käytetään merkintää

$$\begin{aligned}[y] &= \{x \in \mathbb{Z} | x \equiv y(m)\} \\ &= \{x \in \mathbb{Z} | x = y + km\}.\end{aligned}$$

Kaikki erilliset jäännösluokat (mod m) ovat $[0], [1], [2], ..., [m-1]$. Tästä joukosta käytetään merkintää $\mathbb{Z}_m = \{[0], [1], [2], ..., [m-1]\}$.

Määritelmä 3.1.2. Jäännösluokkaa $[a]$ (mod m) sanotaan *alkuluokaksi modulo m*, mikäli $syt(a,m) = 1$. Alkuluokkien joukkoa merkitään $\mathbb{Z}_m^*$.

Jäännösluokat tulevat olemaan olennaisessa asemassa mitä pidemmälle mennään ryhmien teoriaa, kuten myös renkaiden ja kuntien teoriaan tultaessa. Onkin syytä käydä läpi jäännösluokkien avulla laskeminen.

Jos $x \equiv a\ (m)$ ja $y \equiv b\ (m)$, niin $x+y \equiv a+b\ (m)$. Edelleen, jos $x \equiv a\ (m)$ ja $y \equiv b\ (m)$, niin $x \cdot y \equiv a \cdot b\ (m)$. Näin ollen

$$\begin{aligned}[a] + [b] &= [a + b]\ ja \\ [a] \cdot [b] &= [a \cdot b].\end{aligned}$$

Nyt kun on määritelty jäännösluokat ja niiden väliset laskutoimitukset, voidaan siirtyä kohti ryhmän määritelmää.

Määritelmä 3.1.3. Olkoot $G \neq \emptyset$ ja $(*)$ joukon G operaatio. Pari $(G, *)$ on *ryhmä*, mikäli seuraavat ehdot toteutuvat:

1. Operaatio $(*)$ on *binäärinen*, eli $a * b \in G$ aina, kun $a, b \in G$.

2. Operaatio $(*)$ on *assosiatiivinen* eli

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

aina, kun $a, b, c \in G$.

3. Joukossa G on sellainen alkio e, että

$$a * e = e * a = a$$

aina, kun $a \in G$. Alkiota e kutsutaan ryhmän *neutraali-* eli *ykkösalkioksi*.

4. Aina, kun $a \in G$, on olemassa sellainen alkio $a^{-1} \in G$, että

$$a * a^{-1} = a^{-1} * a = e.$$

Alkiota a^{-1} kutsutaan *alkion a käänteisalkioksi*.

Jos lisäksi $(G, *)$ toteuttaa ehdon

5. $a * b = b * a$ aina, kun $a, b \in G$ eli operaatio $(*)$ on *kommutatiivinen*, niin kyseessä on *Abelin ryhmä* eli kommutatiivinen ryhmä.

Seuraava lause osoittaa, että esimerkiksi seuraavat parit ovat Abelin ryhmiä.

Lause 3.1.4.

1. *Pari* $(\mathbb{Z}, +)$ *on Abelin ryhmä, kun taas pari* $(\mathbb{Z}, \cdot)$ *ei ole ryhmä.*
2. *Pari* $(Z_m, +)$ *on Abelin ryhmä.*
3. *Pari* $(Z_m^*, \cdot)$ *on Abelin ryhmä.*

Jatkon kannalta hyödyllisiä ovat myös aliryhmän ja tekijäryhmän määritelmät, joihin tutustutaan seuraavassa kappaleessa.

3.2 Tekijäryhmä

Tekijäryhmää varten tarvitaan hieman lisää ryhmien tarkastelua. Ensimmäisenä täytyy määritellä ryhmän aliryhmä.

Määritelmä 3.2.1. Olkoon $(G, *)$ ryhmä ja $H \subseteq G$ ja $H \neq \emptyset$. Jos $(H, *)$ on ryhmä, sitä kutsutaan *ryhmän* $(G, *)$ *aliryhmäksi*, jota merkitään $(H, *) \leq (G, *)$ tai lyhyemmin $H \leq G$.

Aliryhmiin liittyvät oleellisesti myös sivuluokat.

Määritelmä 3.2.2. Olkoon $H \leq G$ ja $a \in G$. Joukkoa

$$aH = a * H = \{a * h |\ h \in H\}$$

sanotaan *alkion a määräämäksi aliryhmän H vasemmaksi sivuluokaksi.*

Vastaavalla tavalla määritellään myös *alkion a määräämä aliryhmän H oikea sivuluokka*

$$Ha = H * a = \{h * a |\ h \in H\}.$$

Ryhmiä tarkasteltaessa ja tunnistettaessa erittäin käyttökelpoinen on Lagrangen lauseena tunnettu tulos.

Lause 3.2.3. (Lagrangen lause) *Olkoon G äärellinen ryhmä, $H \leq G$ ja n aliryhmän H vasempien sivuluokkien lukumäärä ryhmässä G. Tällöin*

$$|G| = n|H|,$$

ts. äärellisessä ryhmässä aliryhmän kertaluku jakaa ryhmän kertaluvun.

Lagrangen lauseen lisäksi toinen tapa tutkia mahdollisia aliryhmiä saadaan seuraavasta lauseesta.

Lause 3.2.4. *Olkoon $(G, *)$ ryhmä ja $H \subseteq G$, $H \neq \emptyset$. Tällöin $H \leq G$, jos ja vain jos ehdosta $a, b \in H$ seuraa $a * b^{-1} \in H$.*

Aliryhmän määritelmää voidaan laajentaa vielä sivuluokkien kautta normaalin aliryhmän määritelmään.

Määritelmä 3.2.5. Olkoon $N \leq G$. Aliryhmää N sanotaan *normaaliksi*, mikäli $aN = Na$ aina, kun $a \in G$. Tällöin merkitään $N \trianglelefteq G$.

Kun $N \trianglelefteq G$, niin aliryhmän N vasempien sivuluokkien välillä voidaan määritellä operaatio seuraavasti:

$$aN \cdot bN = abN.$$

Normaalin aliryhmän ja sivuluokkien avulla saadaan matkalla kuntalaajennukseen erittäin tärkeä tulos.

Lause 3.2.6. *Olkoon G ryhmä ja $N \trianglelefteq G$. Tällöin $(\{aN |\ a \in G\}, \cdot)$ on ryhmä.*

Tämän tuloksen perusteella voidaan määrittää tekijäryhmä.

Määritelmä 3.2.7. Paria $(\{aN | a \in G\}, \cdot)$ kutsutaan *ryhmän G tekijäryhmäksi normaalin aliryhmän N suhteen.* Kyseisestä ryhmästä käytetään merkintää G/N.

4 Renkaat

Kun ryhmän määritelmä on käsitelty, voidaan sen määritelmää hieman laajentaa. Ottamalla mukaan yksi operaatio lisää, saadaan rengas. Käsitellään siis seuraavaksi renkaiden teoriaa.

4.1 Renkaiden teoria

Määritelmä 4.1.1. Olkoon R epätyhjä joukko. $(R, +, \cdot)$ on *rengas*, jos seuraavat ehdot toteutuvat:

1. $(R, +)$ on Abelin ryhmä:

   - Operaatio $(+)$ on joukon R binäärinen operaatio, eli $a + b \in R$ aina, kun $a, b \in R$.
   - Operaatio $(+)$ on assosiatiivinen, eli

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

   aina, kun $a, b, c \in R$.
   - Joukko R sisältää *nolla-alkion* $\mathbf{0}_R$, eli

   $$a + \mathbf{0}_R = \mathbf{0}_R + a = a$$

   aina, kun $a \in R$. Nolla-alkio $\mathbf{0}_R$ on joukon R neutraalialkio *operaation* $(+)$ suhteen.
   - Aina, kun $a \in R$, sille on olemassa *vasta-alkio* $-a \in R$, eli

   $$a + (-a) = -a + a = \mathbf{0}_R.$$

   Vasta-alkio on käänteisalkio operaation $(+)$ suhteen.
   - Ryhmän R täytyy olla kommutatiivinen operaation $(+)$ suhteen, eli $a + b = b + a$ aina, kun $a, b \in R$.

2. $(R, \cdot)$ on monoidi:

   - Operaatio $(\cdot)$ on binäärinen operaatio joukossa R, eli $a \cdot b \in R$ aina, kun $a, b \in R$.
   - Operaatio $(\cdot)$ on assosiatiivinen, eli

   $$(a \cdot b) \cdot c = a \cdot b \cdot c = a \cdot (b \cdot c)$$

aina, kun $a, b, c \in R$.
- Joukko R sisältää *ykkösalkion* $\mathbf{1}_R$, eli

$$a \cdot \mathbf{1}_R = \mathbf{1}_R \cdot a = a$$

aina, kun $a \in R$. Ykkösalkio $\mathbf{1}_R$ on joukon R neutraalialkio *operaation* $(\cdot)$ suhteen.

3. Joukon R alkioille pätee seuraavat osittelulait:

   $a \cdot (b + c) = a \cdot b + a \cdot c$ ja

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

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

Rengas on *kommutatiivinen*, jos se on kommutatiivinen kertolaskun $(\cdot)$ suhteen, eli $a \cdot b = b \cdot a$ kaikilla $a, b \in R$.

Seuraavat kolmikot ovat myös kommutatiivisia renkaita.

Lause 4.1.2.

1. *Kolmikko* $(\mathbb{Z}, +, \cdot)$ *on kommutatiivinen rengas.*

2. *Kolmikko* $(\mathbb{Z}_m, +, \cdot)$ *on kommutatiivinen rengas.*

Kuten ryhmille voidaan määritellä aliryhmä, myös renkaille voidaan määritellä alirengas.

Määritelmä 4.1.3. Olkoot $(R, +, \cdot)$ rengas ja $\emptyset \neq S \subseteq R$. Jos $(S, +, \cdot)$ on rengas ja sillä on sama ykkösalkio kuin renkaalla R, niin sitä kutsutaan renkaan R *alirenkaaksi*.

Alirenkaan tunnistamiseksi ei välttämättä tarvitse käydä läpi kaikkia renkaan ehtoja. Seuraava tulos helpottaa alirenkaiden löytämistä.

Lause 4.1.4. (Alirengaskriteeri) *Renkaan* $(R, +, \cdot)$ *osajoukko* $S \neq \emptyset$ *on renkaan* R *alirengas jos ja vain jos seuraavat ehdot pätevät*:

1. *Jos* $a, b \in S$, *niin* $a + (-b) \in S$.

2. *Jos* $a, b \in S$, *niin* $ab \in S$.

3. $\mathbf{1}_R \in S$.

Renkaille voidaan määritellä myös eräs toinen osajoukko, joka on tärkeässä osassa kuntalaajennusta.

Määritelmä 4.1.5. Renkaan $(R, +, \cdot)$ epätyhjä osajoukko I on *ideaali*, jos

1. $(I, +) \leq (R, +)$.
2. $r \cdot a \in I$ ja $a \cdot r \in I$ kaikilla $a \in I$ ja $r \in R$.

Ideaali I on *aito ideaali*, jos $I \neq R$.

Seuraava tulos kertoo, milloin ideaali on itseasiassa koko rengas.

Lause 4.1.6. *Olkoon $(R, +, \cdot)$ rengas ja I sen ideaali. Jos renkaan ykkösalkio $\mathbf{1} \in I$, niin $I = R$.*

Keskenään erilaisille ideaaleille saadaan myös hyödyllinen tulos, jonka mukaan niiden summa ja leikkaus on aina uusi ideaali.

Lause 4.1.7. *Jos I ja J ovat renkaan R ideaaleja, niin tällöin myös niiden*

$$\textit{leikkaus } I \cap J \textit{ ja summa } I + J = \{a + b |\ a \in I, b \in J\}$$

ovat ideaaleja.

Ideaaleja voi olla erilaisia ja niitä voidaan myös määritellä tietyn generaattorin mukaan.

Määritelmä 4.1.8. Jos $(R, +, \cdot)$ on rengas ja $a \in R$, niin suppeinta ideaalia, joka sisältää alkion a, kutsutaan alkion a generoimaksi *pääideaaliksi* ja sitä merkitään (a). Alkion a generoima pääideaali on siis kaikkien sellaisten ideaalien leikkaus, jotka sisältävät alkion a.

Pääideaali voidaan määritellä myös toisella, hieman eksaktimmalla tavalla.

Määritelmä 4.1.9. Ideaalia P kutsutaan alkion a generoimaksi pääideaaliksi, mikäli

1. $a \in P$.
2. Jos ideaali I sisältää alkion a, niin $P \subseteq I$.

Tällöin merkitään $P = (a)$.

Pääideaaleille saadaan myös seuraavanlainen tulos.

Lause 4.1.10. *Jos $(R, +, \cdot)$ on kommutatiivinen rengas ja $a \in R$, niin*

$$(a) = Ra = \{ra |\ r \in R\}.$$

Aidoille ideaaleille on olemassa suurin mahdollinen ideaali, jota isommaksi ne eivät voi enää kasvaa ilman, että niistä tulisi itse rengas.

Määritelmä 4.1.11. Renkaan $(R, +, \cdot)$ ideaali M on *maksimaalinen ideaali*, mikäli

1. $M \neq R$.
2. Jos I on renkaan R ideaali ja $M \subset I \subseteq R$, niin $I = R$.

Tarkastellaan ideaaleja vielä esimerkin kautta.

Esimerkki 4.1.12. Tarkastellaan kommutatiivista rengasta $(\mathbb{Z}_{12}, +, \cdot)$ ja alkion $[2]$ generoimaa pääideaalia, eli pääideaalia $([2])$. Käydään läpi kaikki renkaan alkiot lauseen 4.1.10 mukaan, jolloin saamme kaikki pääideaalin $([2])$ alkiot.

$$\begin{array}{ll} [0] \cdot [2] = [0 \cdot 2] = [0], & [6] \cdot [2] = [12] = [0], \\ [1] \cdot [2] = [2], & [7] \cdot [2] = [14] = [2], \\ [2] \cdot [2] = [4], & [8] \cdot [2] = [16] = [4], \\ [3] \cdot [2] = [6], & [9] \cdot [2] = [18] = [6], \\ [4] \cdot [2] = [8], & [10] \cdot [2] = [20] = [8], \\ [5] \cdot [2] = [10], & [11] \cdot [2] = [22] = [10]. \end{array}$$

Eli pääideaalin $([2])$ alkioiksi saadaan $\{[0], [2], [4], [6], [8], [10]\}$. Pääideaali $([2])$ on myös selvästi maksimaalinen ideaali, sillä ideaalin määritelmän nojalla $(([2]), +) \leq (\mathbb{Z}_{12}, +)$ ja lagrangen lauseen nojalla aliryhmän kertaluvun täytyy jakaa ryhmän kertaluku. Nyt $|([2])| = 6$, eli ideaalia ei voida laajentaa enää suuremmaksi ideaaliksi tekemättä siitä joukkoa $\mathbb{Z}_{12}$, jonka kertaluku on 12.

Renkaiden maksimaalisia ideaaleja etsiessä lagrangen lauseen hyödyntäminen voi joskus osoittautua vaikeaksi. Esimerkiksi ryhmän $(\mathbb{Z}_{99}, +)$ kertaluku 99 on niin suuri, ettei kertalukua 3 olevasta ideaalin I muodostamasta aliryhmästä $(I, +)$ voida suoraan sanoa onko ideaali I maksimaalinen. Tällaisia tilanteita varten voi auttaa seuraava tulos.

Lause 4.1.13. *Olkoon p alkuluku joka jakaa luvun m. Tällöin $([p])$ on renkaan $(\mathbb{Z}_m, +, \cdot)$ maksimaalinen ideaali.*

4.2 Tekijärengas

Tekijärenkaan muodostaminen sisältää samoja elementtejä kuin tekijäryhmän määritteleminen. Siinä missä tekijäryhmät muodostetaan normaalien

aliryhmien avulla ja näin saadaan mahdollisuus määrittää laskutoimitus sivuluokkien joukossa, täytyy tekijärenkaan kohdalla pystyä määrittämään sekä yhteen- että kertolasku. Tekijärenkaiden muodostamiseen tarvitaan ideaaleja.

Olkoon I renkaan $(R,+,\cdot)$ ideaali, jolloin $(I,+) \leq (R,+)$. Nyt tiedetään, että $(R,+)$ on Abelin ryhmä, joten $(I,+) \trianglelefteq (R,+)$. Tällöin tekijäryhmä $(R/I,+)$ on olemassa. Tekijäryhmän alkioina toimivat sivuluokat $r+I = \{r+x|\ x \in I\}$, missä $r \in R$, ja sivuluokkien yhteenlasku voidaan määritellä

$$(r_1+I)+(r_2+I) = (r_1+r_2)+I$$

aina, kun $r_1, r_2 \in R$. Tällöin ryhmän $(R/I,+)$ nolla-alkio on $\mathbf{0}+I = I$ ja alkion $a+I \in R/I$ vasta-alkio on $(-a)+I$.

Kuten edellä todettiin, myös sivuluokkien välinen kertolasku täytyy pystyä määrittämään. Sivuluokkien välinen kertolasku määritellään siten, että

$$(r_1+I)\cdot(r_2+I) = (r_1r_2)+I$$

aina, kun $r_1, r_2 \in R$. Tällöin joukon R/I ykkösalkio on $\mathbf{1}+I$.

Nyt edellä määritellyt laskutoimitukset sivuluokille antavat mahdollisuuden tekijärenkaan muodostamiseen.

Lause 4.2.1. *Olkoon I renkaan $(R,+,\cdot)$ ideaali ja $R/I = \{r+I|\ r \in R\}$, missä $r+I = \{r+x|\ x \in I\}$. Tällöin $(R/I,+,\cdot)$ on rengas, missä laskutoimitukset $(+)$ ja $(\cdot)$ ovat edellä määritellyt sivuluokkien yhteen- ja kertolasku.*

Vastaavasti kuten tekijäryhmän kohdalla, tämän tuloksen perusteella voidaan määrittää tekijärengas.

Määritelmä 4.2.2. Kolmikkoa $(R/I,+,\cdot)$ kutsutaan *renkaan R tekijärenkaaksi ideaalin I suhteen.*

Todettakoon vielä, että jos rengas $(R,+,\cdot)$ on kommutatiivinen, myös tekijärengas $(R/I,+,\cdot)$ on kommutatiivinen.

Tutkitaan tekijärenkaan muodostamista esimerkin avulla.

Esimerkki 4.2.3. Jatketaan kommutatiivisen renkaan $(\mathbb{Z}_{12},+,\cdot)$ parissa. Esimerkissä 4.1.10. osoitettiin, että pääideaali $([2]) = \{[0],[2],[4],[6],[8],[10]\}$ on kommutatiivisen renkaan $\mathbb{Z}_{12}$ maksimaalinen ideaali. Lauseen 4.2.1 nojalla saadaan muodostettua tekijärengas $\mathbb{Z}_{12}/([2]) = \{r+([2])|\ r \in \mathbb{Z}_{12}\}$.

Tekijärenkaan alkioita ei ole tässä tapauksessa kuin kaksi, $\mathbb{Z}_{12}/([2]) = \{[0]+([2]),[1]+([2])\}$, sillä kaikki renkaan ja ideaalin alkioiden yhteenlaskut palautuvat näihin:

$$[0]+([2]) = \{[0],[2],[4],[6],[8],[10]\}$$

ja

$$[1] + ([2]) = \{[1], [3], [5], [7], [9], [11]\}.$$

Tekijärenkaan alkiot voidaan esittää laskutaulukossa operaation $(+)$ suhteen.

$+$	$[0] + ([2])$	$[1] + ([2])$
$[0] + ([2])$	$[0] + ([2])$	$[1] + ([2])$
$[1] + ([2])$	$[1] + ([2])$	$[0] + ([2])$

Laskutaulukosta nähdään, että tekijärenkaan nolla-alkio on $[0] + ([2]) = \mathbf{0}_{\mathbb{Z}_{12}} + ([2])$.

Vastaavanlainen laskutaulukko voidaan tehdä myös operaation $(\cdot)$ suhteen.

$\cdot$	$[0] + ([2])$	$[1] + ([2])$
$[0] + ([2])$	$[0] + ([2])$	$[0] + ([2])$
$[1] + ([2])$	$[0] + ([2])$	$[1] + ([2])$

Laskutaulukosta nähdään, että tekijärenkaan ykkösalkio on $[1] + ([2]) = \mathbf{1}_{\mathbb{Z}_{12}} + ([2])$.

4.3 Rengashomomorfismi

Renkaan alkioita voidaan kuvata jonkin toisen renkaan alkioiksi sopivan kuvauksen avulla. Tähän tarkoitukseen määritellään seuraavaksi rengashomomorfismi.

Määritelmä 4.3.1. Olkoon $(R, +, \cdot)$ ja $(R', \oplus, \odot)$ renkaita. Tällöin kuvausta $f : R \to R'$ kutsutaan *rengashomomorfismiksi*, jos se täyttää seuraavat ehdot:

1. $f(a + b) = f(a) \oplus f(b)$ kaikilla $a, b \in R$.
2. $f(a \cdot b) = f(a) \odot f(b)$ kaikilla $a, b \in R$.
3. $f(\mathbf{1}_R) = \mathbf{1}_{R'}$.

Nyt kun rengashomomorfismi on määritelty, voidaan määritellä rengasisomorfismi.

Määritelmä 4.3.2. Rengashomomorfismia $f : R \to R'$ sanotaan *rengasisomorfismiksi*, jos f on bijektio. Rengasta R sanotaan *isomorfiseksi* renkaan R' kanssa, jos on olemassa jokin isomorfismi $R \to R'$. Keskenään isomorfisia renkaita merkitään $R \cong R'$.

5 Kokonaisalue

Tässä luvussa määritellään uusi renkaan muoto eli kokonaisalue. Kokonaisalue on kommutatiivinen rengas, mutta sillä on oma erityisominaisuutensa.

5.1 Kokonaisalueiden teoria

Aluksi täytyy määritellä käsite nollanjakaja, josta päästään kokonaisalueen määritelmään.

Määritelmä 5.1.1. Renkaan $(R, +, \cdot)$ nolla-alkiosta eroava alkio a on renkaan R *nollanjakaja*, jos renkaassa R on sellainen nolla-alkiosta eroava alkio b, että $ab = \mathbf{0}_R$ tai $ba = \mathbf{0}_R$.

Määritelmä 5.1.2. Kommutatiivista rengasta, jossa ei ole nollanjakajia, kutsutaan *kokonaisalueeksi*.

Seuraava lause antaa esimerkin renkaasta, joka on kokonaisalue ja auttaa tunnistamaan milloin jäännösluokkarengas on kokonaisalue.

Lause 5.1.3.

1. *Rengas* $(\mathbb{Z}, +, \cdot)$ *on kokonaisalue.*
2. *Jäännösluokkarengas* $(\mathbb{Z}_m, +, \cdot)$ *on kokonaisalue jos ja vain jos* m *on alkuluku.*

Käydään läpi kokonaisalueen tarkastelua esimerkin avulla.

Esimerkki 5.1.4. Tiedetään, että $(\mathbb{Z}_{12}, +, \cdot)$ on kommutatiivinen rengas, mutta onko se myös kokonaisalue? Kokonaisalueen määritelmän 4.4.2 mukaan, kommutatiivinen rengas on kokonaisalue, jos se ei sisällä nollanjakajia. Eli, jos löydetään yksikin nollanjakaja renkaasta, tiedetään, että se ei ole kokonaisalue.

Nyt $[2] \neq \mathbf{0}_{\mathbb{Z}_{12}}$ ja $[6] \neq \mathbf{0}_{\mathbb{Z}_{12}}$. Kuitenkin $[2] \cdot [6] = [12] = [0] = \mathbf{0}_{\mathbb{Z}_{12}}$, eli kommutatiivinen rengas $(\mathbb{Z}_{12}, +, \cdot)$ sisältää ainakin yhden nollanjakajan. Näin ollen se ei ole kokonaisalue.

Lopuksi käydään läpi hyödyllinen lause kokonaisalueita käsiteltäessä.

Lause 5.1.5. *Olkoon* $(R, +, \cdot)$ *kokonaisalue ja* $a \in R, a \neq \mathbf{0}_R$. *Tällöin*

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

6 Kunnat

Tähän asti on käyty läpi ryhmän muodostamista laajentaen sitä eteenpäin renkaaksi ja edelleen kokonaisalueeksi. Tässä luvussa käsitteiden laajentamista jatketaan määrittelemällä kunta.

6.1 Kuntien teoria

Määritellään alkuun hyödyllinen merkintätapa tulevaisuutta ajatellen.

Määritelmä 6.1.1. Olkoon $(R, +, \cdot)$ rengas ja $a \in R$. Kun n on positiivinen kokonaisluku, niin merkintä na on lyhennetty merkintä summasta $a + \ldots + a$, missä alkioita a on n kappaletta. Alkio na on renkaan alkion a n. *monikerta*. Ykkösalkiota käyttäen voidaan alkio na esittää renkaan operaationa, sillä $na = (\mathbf{1}_R + \ldots + \mathbf{1}_R) \cdot a = (n\mathbf{1}_R) \cdot a$. Negatiivisilla kokonaisluvun n arvoilla alkio na on alkion $-a$ $|n|$. monikerta.

Nyt voidaan siirtyä itse luvun aiheeseen, eli kunnan määritelmään.

Määritelmä 6.1.2. Kommutatiivista rengasta $(K, +, \cdot)$ sanotaan *kunnaksi*, mikäli $(K \setminus \{\mathbf{0}_K\}, \cdot)$ on Abelin ryhmä. Ryhmää $(K \setminus \{\mathbf{0}_K\}, \cdot)$ kutsutaan kunnan *multiplikatiiviseksi ryhmäksi* ja ryhmää $(K, +)$ kunnan *additiiviseksi ryhmäksi*.

Avataan tarkemmin kunnan multiplikatiivisen ryhmän ehtoja. Ryhmä $(K, +)$ on selvästi Abelin ryhmä, koska $(K, +, \cdot)$ on kommutatiivinen rengas ja samasta syystä osittelulait ovat voimassa, eikä niitä ole tarvetta enää avata.

Ryhmä $(K \setminus \{\mathbf{0}_K\}, \cdot)$ on Abelin ryhmä:

1. Operaatio $(\cdot)$ on binäärinen joukossa $K \setminus \{\mathbf{0}_K\}$, eli $a \cdot b \in K \setminus \{\mathbf{0}_K\}$ aina, kun $a, b \in K \setminus \{\mathbf{0}_K\}$.

2. Operaatio $(\cdot)$ on assosiatiivinen, eli

$$(a \cdot b) \cdot c = a \cdot b \cdot c = a \cdot (b \cdot c)$$

   aina, kun $a, b, c \in K \setminus \{\mathbf{0}_K\}$.

3. Joukossa $K \setminus \{\mathbf{0}_K\}$ on ykkösalkio $\mathbf{1}_K$, eli

$$a \cdot \mathbf{1}_K = \mathbf{1}_K \cdot a = a$$

   aina, kun $a \in K \setminus \{\mathbf{0}_K\}$.

4. Aina, kun $a \in K \setminus \{\mathbf{0}_K\}$, sille on olemassa *käänteisalkio* $a^{-1} \in K \setminus \{\mathbf{0}_K\}$, siten että
$$a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1}_K.$$
On syytä huomata, että tämä ehto on siis voimassa vain, kun joukosta K otetaan pois sen nolla-alkio $\mathbf{0}_K$.

5. Operaatio $(\cdot)$ on kommutatiivinen, eli $a \cdot b = b \cdot a$ aina, kun $a, b \in K \setminus \{\mathbf{0}_K\}$.

Kunnan määritelmälle saadaan myös hyödyllinen tulos, joka antaa uusia mahdollisuuksia kuntien tunnistamiseen.

Lause 6.1.3. *Kolmikko $(K, +, \cdot)$ on kunta, jos ja vain jos seuraavat ehdot toteutuvat:*

1. *$(K, +)$ on Abelin ryhmä.*
2. *$(K \setminus \{\mathbf{0}\}, \cdot)$ on Abelin ryhmä.*
3. *Joukon K alkoille pätee seuraavat osittelulait:*
$a \cdot (b + c) = a \cdot b + a \cdot c$ *ja*
$(a + b) \cdot c = a \cdot c + b \cdot c$
kaikilla $a, b, c \in K$.

Aivan kuten renkaillekin, myös kunnille voidaan määritellä kuntahomomorfismi ja kuntaisomorfismi.

Määritelmä 6.1.4. Olkoot $(K, +, \cdot)$ ja $(K', \oplus, \odot)$ kuntia. Jos on olemassa kuvaus $f : K \to K'$ niin, että se on rengashomomorfismi, on se tällöin *kuntahomomorfismi*. Jos kuvaus $f : K \to K'$ on lisäksi rengasisomorfismi, on se tällöin *kuntaisomorfismi*. Keskenään isomorfisista kunnista käytetään merkintää $K \cong K'$.

Tutkitaan seuraavaksi kommutatiivisen renkaan ja kunnan välistä suhdetta esimerkin kautta.

Esimerkki 6.1.5. Edellisissä esimerkeissä käytetty joukko $(\mathbb{Z}_{12}, +, \cdot)$ on kommutatiivinen rengas, mutta täyttääkö se myös kunnan ehdot? Käytännössä riittää tutkia onko $(\mathbb{Z}_{12} \setminus \{\mathbf{0}_{\mathbb{Z}_{12}}\}, \cdot)$ Abelin ryhmä, sillä muut ehdot sisältyvät kommutatiivisen renkaan ehtoihin.

Tehdään joukolle $\mathbb{Z}_{12} \setminus \{\mathbf{0}_{\mathbb{Z}_{12}}\}$ laskutaulu operaation $(\cdot)$ suhteen:

$\cdot$	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
[2]	[2]	[4]	[6]	[8]	[10]	[0]	[2]	[4]	[6]	[8]	[10]
[3]	[3]	[6]	[9]	[0]	[3]	[6]	[9]	[0]	[3]	[6]	[9]
[4]	[4]	[8]	[0]	[4]	[8]	[0]	[4]	[8]	[0]	[4]	[8]
[5]	[5]	[10]	[3]	[8]	[1]	[6]	[11]	[4]	[9]	[2]	[7]
[6]	[6]	[0]	[6]	[0]	[6]	[0]	[6]	[0]	[6]	[0]	[6]
[7]	[7]	[2]	[9]	[4]	[11]	[6]	[1]	[8]	[3]	[10]	[5]
[8]	[8]	[4]	[0]	[8]	[4]	[0]	[8]	[4]	[0]	[8]	[4]
[9]	[9]	[6]	[3]	[0]	[9]	[6]	[3]	[0]	[9]	[6]	[3]
[10]	[10]	[8]	[6]	[4]	[2]	[0]	[10]	[8]	[6]	[4]	[2]
[11]	[11]	[10]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Kuten laskutaulusta selvästi nähdään, operaatio $(\cdot)$ ei ole binäärinen joukossa $\mathbb{Z}_{12} \setminus \{\mathbf{0}_{\mathbb{Z}_{12}}\}$, esimerkiksi $[4], [6] \in \mathbb{Z}_{12} \setminus \{\mathbf{0}_{\mathbb{Z}_{12}}\}$, mutta $[4] \cdot [6] = [24] = [0] \notin \mathbb{Z}_{12} \setminus \{\mathbf{0}_{\mathbb{Z}_{12}}\}$, eli $(\mathbb{Z}_{12} \setminus \{\mathbf{0}_{\mathbb{Z}_{12}}\}, \cdot)$ ei ole Abelin ryhmä eikä $(\mathbb{Z}_{12}, +, \cdot)$ näin ollen ole kunta.

Nyt kun on käsitelty ryhmän, renkaan ja kunnan teoriaa, voidaan siirtyä itse tutkielman aiheeseen, eli renkaan laajentamiseen kunnaksi.

7 Kuntalaajennus

Kuten edellisessä luvussa nähtiin, on olemassa kommutatiivisia renkaita, jotka eivät ole kuntia, mutta voisiko olla jokin tapa, jolla niistä voidaan muokata kunta? Tähän saadaan vastaus seuraavassa kappaleessa.

7.1 Kuntalaajennuslauseen teoria

Kommutatiivisesta renkaasta voidaan aina laajentaa kunta sen maksimaalisen ideaalin avulla. Tätä tulosta kutsutaan *kuntalaajennuslauseeksi.*

Lause 7.1.1. (Kuntalaajennuslause) *Olkoon* $(R, +, \cdot)$ *kommutatiivinen rengas ja* M *renkaan* R *maksimaalinen ideaali. Tällöin tekijärengas* R/M *on kunta.*

Todistus. Koska R on kommutatiivinen rengas, niin myös tekijärenkaan R/M täytyy olla kommutatiivinen. Näin ollen tiedetään, että $(R/M, +)$ on Abelin ryhmä ja osittelulait ovat voimassa. Osoitetaan, että $(R/M \setminus \{\mathbf{0} + M\}, \cdot)$ on Abelin ryhmä, jolloin kaikki kunnan ehdot toteutuvat.

Nyt koska R/M on kommutatiivinen rengas, tiedetään varmasti, että assosiatiivisuus on voimassa myös joukossa $(R/M \setminus \{\mathbf{0} + M\}, \cdot)$ ja sieltä löytyy ykkösalkio $\mathbf{1} + M$. Binäärisyys ja käänteisalkion olemassaolo sen sijaan eivät ole itsestäänselviä. Osoitetaan ensin, että jokaiselle tekijärenkaan nollaalkiosta eroavalle alkiolle löytyy käänteisalkio joukossa $R/M \setminus \{\mathbf{0} + M\}$.

Olkoon $a + M \in R/M$ ja $a + M \neq \mathbf{0} + M$. Tällöin $a \notin \mathbf{0} + M = M$, eli $(a) \neq M$. Lauseen 4.1.7 nojalla $M + (a)$ on renkaan R ideaali ja $M \subset M + (a)$. Koska M on renkaan R maksimaalinen ideaali, niin $M + (a) = R$ ja edelleen lauseen 4.1.10 nojalla $R = M + Ra$.

Nyt $\mathbf{1} \in R$ eli $\mathbf{1} \in M + Ra$, joten $\mathbf{1} = m + ra$ joillakin $m \in M$ ja $r \in R$. Tällöin tekijärenkaan R/M ykkösalkio voidaan esittää muodossa

$$\begin{aligned} \mathbf{1} + M &= (m + ra) + M = (m + M) + (ra + M) \\ &= (\mathbf{0} + M) + (ra + M) = ra + M = (r + M) \cdot (a + M). \end{aligned}$$

Koska tekijärengas R/M on kommutatiivinen, niin myös

$$(a + M) \cdot (r + M) = \mathbf{1} + M.$$

Näin ollen $r + M$ on alkion $a + M$ käänteisalkio ja selvästi $r + M \neq \mathbf{0} + M$.

Nyt kun tiedetään, että käänteisalkio on olemassa, voidaan sen seurauksena osoittaa sivuluokkien tulon binäärisyys joukossa $R/M \setminus \{\mathbf{0} + M\}$. Olkoon

$a_1 + M$ ja $a_2 + M \in R/M \setminus \{\mathbf{0} + M\}$. Olkoon

$$(a_1 + M) \cdot (a_2 + M) = (\mathbf{0} + M).$$

Nyt alkiolla $a_2 + M$ on olemassa käänteisalkio, jolla operoimalla saadaan

$$\begin{aligned}(a_1 + M) \cdot (a_2 + M) \cdot (a_2 + M)^{-1} &= (\mathbf{0} + M) \cdot (a_2 + M)^{-1},\\ (a_1 + M) \cdot (\mathbf{1} + M) &= (\mathbf{0} + M),\\ (a_1 + M) &= (\mathbf{0} + M),\end{aligned}$$

mikä on ristiriita alkuehdon kanssa, eli kahden alkion tulo joukossa $R/M \setminus \{\mathbf{0} + M\}$ ei voi olla nolla-alkio ja näin ollen sivuluokkien tulo on binäärinen joukossa $R/M \setminus \{\mathbf{0} + M\}$.

Näin ollen $(R/M \setminus \{\mathbf{0}+M\}, \cdot)$ on Abelin ryhmä ja tekijärengas $(R/M, +, \cdot)$ on kunta.

□

Käydään vielä läpi toinen, hieman perusteellisempi todistus kuntalaajennuslauseelle.

Todistus. Todistetaan, että $(R/M, +, \cdot)$ on kunta tutkimalla kunnan ehtojen täyttyminen.

1. Osoitetaan aluksi, että $(R/M, +, \cdot)$ on kommutatiivinen rengas.

   Nyt $(R/M, +)$ on Abelin ryhmä, jos

   1^o Operaatio $(+)$ on binäärinen joukossa R/M.

   Nyt

   $$(a_1 + M) + (a_2 + M) = (a_1 + a_2) + M \in R/M,$$

   sillä $a_1 + a_2 \in R$ kaikilla $(a_1 + M), (a_2 + M) \in R/M$.

   2^o Operaatio $(+)$ on assosiatiivinen joukossa R/M.

   Nyt

   $$\begin{aligned}&(a_1 + M) + [(a_2 + M) + (a_3 + M)]\\ &= (a_1 + M) + ((a_2 + a_3) + M)\\ &= (a_1 + (a_2 + a_3)) + M\\ &= ((a_1 + a_2) + a_3) + M\\ &= ((a_1 + a_2) + M) + (a_3 + M)\\ &= [(a_1 + M) + (a_2 + M)] + (a_3 + M)\end{aligned}$$

kaikilla $(a_1 + M), (a_2 + M), (a_3 + M) \in R/M$.

3^o Joukossa R/M on nolla-alkio.

Nyt $\mathbf{0} + M$ on joukon R/M nolla-alkio, sillä

$$(\mathbf{0} + M) + (a + M) = (\mathbf{0} + a) + M = a + M,$$

$$(a + M) + (\mathbf{0} + M) = (a + \mathbf{0}) + M = a + M$$

kaikilla $a + M \in R/M$.

Nolla-alkio on selvästi yksikäsitteinen, sillä $\mathbf{0}$ on renkaan R yksikäsitteinen nolla-alkio, jolloin myös $\mathbf{0} + M$ on yksikäsitteinen.

4^o Jokaisella joukon R/M alkiolla on vasta-alkio joukossa R/M.

Olkoon $a + M \in R/M$. Nyt $(-a) + M \in R/M$ ja

$$(a + M) + ((-a) + M) = (a + (-a)) + M = \mathbf{0} + M,$$

$$((-a) + M) + (a + M) = ((-a) + a) + M = \mathbf{0} + M$$

kaikilla $a + M \in R/M$.

5^o Operaatio $(+)$ on kommutatiivinen joukossa R/M.

Nyt

$$\begin{aligned}(a_1 + M) + (a_2 + M) &= (a_1 + a_2) + M \\ &= (a_2 + a_1) + M \\ &= (a_2 + M) + (a_1 + M)\end{aligned}$$

kaikilla $(a_1 + M), (a_2 + M) \in R/M$.

Kohtien $1^o - 5^o$ nojalla $(R/M, +)$ on Abelin ryhmä.

Nyt $(R/M, \cdot)$ on monoidi, jos

1^o Operaatio $(\cdot)$ on binäärinen joukossa R/M.

Nyt

$$(a_1 + M) \cdot (a_2 + M) = a_1 a_2 + M \in R/M,$$

sillä $a_1 a_2 \in R$ kaikilla $(a_1 + M), (a_2 + M) \in R/M$.

2^o Operaatio $(\cdot)$ on assosiatiivinen joukossa R/M.

Nyt

$$\begin{aligned}
&(a_1 + M) \cdot [(a_2 + M) \cdot (a_3 + M)] \\
&= (a_1 + M) \cdot (a_2 a_3 + M) \\
&= (a_1(a_2 a_3)) + M \\
&= ((a_1 a_2)a_3) + M \\
&= (a_1 a_2 + M) \cdot (a_3 + M) \\
&= [(a_1 + M) \cdot (a_2 + M)] \cdot (a_3 + M)
\end{aligned}$$

kaikilla $(a_1 + M), (a_2 + M), (a_3 + M) \in R/M$.

3^o Joukossa R/M on ykkösalkio.

Nyt $\mathbf{1} + M$ on joukon R/M ykkösalkio, sillä

$$(\mathbf{1} + M) \cdot (a + M) = (\mathbf{1} \cdot a) + M = a + M,$$

$$(a + M) \cdot (\mathbf{1} + M) = (a \cdot \mathbf{1}) + M = a + M$$

kaikilla $a + M \in R/M$.

Ykkösalkio on selvästi yksikäsitteinen, sillä $\mathbf{1}$ on renkaan R yksikäsitteinen ykkösalkio, jolloin myös $\mathbf{1} + M$ on yksikäsitteinen.

Kohtien $1^o - 3^o$ nojalla $(R/M, \cdot)$ on monoidi.

Tarkistetaan päteekö joukon R/M alkioille osittelulait.

Nyt

$$\begin{aligned}
(a_1 + M) \cdot [(a_2 + M) + (a_3 + M)] &= (a_1 + M) \cdot ((a_2 + a_3) + M) \\
&= (a_1 \cdot (a_2 + a_3)) + M \\
&= (a_1 a_2 + a_1 a_3) + M \\
&= (a_1 a_2 + M) + (a_1 a_3 + M) \\
&= (a_1 + M) \cdot (a_2 + M) + (a_1 + M) \cdot (a_3 + M)
\end{aligned}$$

ja

$$\begin{aligned}
[(a_1 + M) + (a_2 + M)] \cdot (a_3 + M) &= ((a_1 + a_2) + M) \cdot (a_3 + M) \\
&= ((a_1 + a_2) \cdot a_3) + M \\
&= (a_1 a_3 + a_2 a_3) + M \\
&= (a_1 a_3 + M) + (a_2 a_3 + M) \\
&= (a_1 + M) \cdot (a_3 + M) + (a_2 + M) \cdot (a_3 + M)
\end{aligned}$$

kaikilla $(a_1 + M), (a_2 + M), (a_3 + M) \in R/M$.

Lopuksi tarkistetaan onko joukko R/M kommutatiivinen operaation $(\cdot)$ suhteen.

Nyt

$$\begin{aligned}(a_1 + M) \cdot (a_2 + M) &= (a_1 a_2) + M \\ &= (a_2 a_1) + M \\ &= (a_2 + M) \cdot (a_1 + M)\end{aligned}$$

kaikilla $(a_1 + M), (a_2 + M) \in R/M$.

Eli edellä täyttyneiden ehtojen nojalla $(R/M, +, \cdot)$ on kommutatiivinen rengas.

2. Osoitetaan lopuksi, että $(R/M \setminus \{\mathbf{0} + M\}, \cdot)$ on Abelin ryhmä.

   Nyt $(R/M \setminus \{\mathbf{0} + M\}, \cdot)$ on Abelin ryhmä, jos

   1^o Operaatio $(\cdot)$ on binäärinen joukossa $R/M \setminus \{\mathbf{0} + M\}$.

   Nyt

   $$(a_1 + M) \cdot (a_2 + M) = a_1 a_2 + M,$$

   tutkitaan onko sivuluokkien tulo aina eri suuri kuin $\mathbf{0} + M$, kun $(a_1 + M), (a_2 + M) \in R/M \setminus \{\mathbf{0} + M\}$.

   Oletetaan, että joukon $R/M \setminus \{\mathbf{0} + M\}$ kaikille alkioille löytyy käänteisalkio. Olkoon

   $$(a_1 + M) \cdot (a_2 + M) = (\mathbf{0} + M).$$

   Tällöin

   $$\begin{aligned}(a_1 + M) \cdot (a_2 + M) \cdot (a_2 + M)^{-1} &= (\mathbf{0} + M) \cdot (a_2 + M)^{-1}, \\ (a_1 + M) \cdot (\mathbf{1} + M) &= (\mathbf{0} + M), \\ (a_1 + M) &= (\mathbf{0} + M),\end{aligned}$$

   mikä on ristiriita alkuehdon kanssa, eli kahden alkion tulo joukossa $R/M \setminus \{\mathbf{0} + M\}$ ei voi olla nolla-alkio, jos pystytään osoittamaan, että kaikille joukon $R/M \setminus \{\mathbf{0} + M\}$ alkioille on olemassa käänteisalkio, mikä osoitetaan kohdassa 4^o.

2^o Operaatio $(\cdot)$ on assosiatiivinen joukossa $R/M \setminus \{\mathbf{0}+M\}$.

Nyt

$$\begin{aligned}
&(a_1+M)\cdot[(a_2+M)\cdot(a_3+M)]\\
&=(a_1+M)\cdot(a_2a_3+M)\\
&=(a_1(a_2a_3))+M\\
&=((a_1a_2)a_3)+M\\
&=(a_1a_2+M)\cdot(a_3+M)\\
&=[(a_1+M)\cdot(a_2+M)]\cdot(a_3+M)
\end{aligned}$$

kaikilla $(a_1+M),(a_2+M),(a_3+M) \in R/M \setminus \{\mathbf{0}+M\}$.

3^o Joukossa $R/M \setminus \{\mathbf{0}+M\}$ on ykkösalkio.

Nyt $\mathbf{1}+M$ on joukon $R/M \setminus \{\mathbf{0}+M\}$ ykkösalkio, sillä

$$(\mathbf{1}+M)\cdot(a+M) = (\mathbf{1}\cdot a)+M = a+M,$$

$$(a+M)\cdot(\mathbf{1}+M) = (a\cdot\mathbf{1})+M = a+M$$

kaikilla $a+M \in R/M$.

Ykkösalkio on selvästi yksikäsitteinen, sillä $\mathbf{1}$ on renkaan R yksikäsitteinen ykkösalkio, jolloin myös $\mathbf{1}+M$ on yksikäsitteinen ja $\mathbf{1}+M \in R/M \setminus \{\mathbf{0}+M\}$.

4^o Jokaisella joukon $R/M \setminus \{\mathbf{0}+M\}$ alkiolla on käänteisalkio joukossa $R/M \setminus \{\mathbf{0}+M\}$.

Olkoon $a+M \in R/M$ ja $a+M \neq \mathbf{0}+M$. Tällöin $a \notin \mathbf{0}+M = M$, eli $(a) \neq M$. Lauseen 4.1.7 nojalla $M+(a)$ on renkaan R ideaali ja $M \subset M+(a)$. Koska M on renkaan R maksimaalinen ideaali, niin $M+(a)=R$ ja edelleen lauseen 4.1.10 nojalla $R = M+Ra$.

Nyt $\mathbf{1} \in R$ eli $\mathbf{1} \in M+Ra$, joten $\mathbf{1} = m+ra$ joillakin $m \in M$ ja $r \in R$. Tällöin tekijärenkaan R/M ykkösalkio voidaan esittää muodossa

$$\begin{aligned}
\mathbf{1}+M &= (m+ra)+M = (m+M)+(ra+M)\\
&= (\mathbf{0}+M)+(ra+M) = ra+M = (r+M)\cdot(a+M).
\end{aligned}$$

Koska tekijärengas R/M on kommutatiivinen, niin myös

$$(a+M)\cdot(r+M) = \mathbf{1}+M.$$

Näin ollen $r+M$ on alkion $a+M$ käänteisalkio ja selvästi $r+M \neq \mathbf{0}+M$.

5^o Operaatio $(\cdot)$ on kommutatiivinen joukossa $R/M \setminus \{\mathbf{0}+M\}$.

Nyt

$$\begin{aligned}(a_1+M)\cdot(a_2+M) &= (a_1a_2)+M \\ &= (a_2a_1)+M \\ &= (a_2+M)\cdot(a_1+M)\end{aligned}$$

kaikilla $(a_1+M),(a_2+M) \in R/M \setminus \{\mathbf{0}+M\}$.

Kohtien $1^o - 5^o$ nojalla $(R/M \setminus \{\mathbf{0}+M\}, \cdot)$ on Abelin ryhmä.

Eli kohtien 1. ja 2. nojalla $(R/M, +, \cdot)$ on kunta.

□

Kuntalaajennuslause voidaan esittää myös toiseen suuntaan, mikä laajentaa sen käyttömahdollisuuksia.

Lause 7.1.2. *Olkoon $(R,+,\cdot)$ rengas ja M renkaan R ideaali. Jos tekijärengas R/M on kunta, niin ideaali M on renkaan R maksimaalinen ideaali.*

Todistus. Olkoon I ideaali, joka aidosti sisältää ideaalin M, eli $M \subset I$. Pyritään osoittamaan, että $I = R$, jolloin M on maksimaalinen ideaali.

Olkoon $a \in I$, mutta $a \notin M$. Nyt $a+M$ ei voi olla kunnan R/M nolla-alkio, sillä kunnan nolla-alkio on muotoa $\mathbf{0}+M = M$, joten kunnan ehtojen mukaan alkiolla $a+M$ on oltava käänteisalkio. Tällöin on olemassa alkio $b \in R$ jolla $(a+M)\cdot(b+M) = ab+M = (\mathbf{1}+M)$. Täytyy siis olla sellainen alkio $m \in M$, että $ab = \mathbf{1}+m \in \mathbf{1}+M$.

Nyt $\mathbf{1} = ab+(-m)$ ja koska $a \in I$, niin $ab \in I$. Lisäksi $m \in M$ ja $M \subset I$, joten myös $m \in I$ ja siten myös $-m \in I$. Näin ollen $\mathbf{1} = ab+(-m) \in I$ ja lauseen 4.1.6 nojalla tämä on mahdollista vain, jos $I = R$. Näin ollen M on renkaan R maksimaalinen ideaali.

□

Kuntalaajennuslause antaa oivan mahdollisuuden sellaisten kommutatiivisten renkaiden laajentamiseen, jotka eivät ole kuntia. Näin voidaan toimia esimerkiksi kommutatiivisen renkaan $(\mathbb{Z}_{12},+,\cdot)$ tapauksessa.

Esimerkki 7.1.3. Aiemmin todettiin esimerkissä 5.1.4., että kommutatiivinen rengas $(\mathbb{Z}_{12},+,\cdot)$ ei ole kunta. Nyt kuntalaajennuslauseen nojalla siitä

voidaan kuitenkin laajentaa kunta sen maksimaalisen ideaalin avulla. Esimerkissä 4.2.3. muodostettu tekijärengas $\mathbb{Z}_{12}/([2]) = \{[0] + ([2]), [1] + ([2])\}$ on juuri tällainen, sillä pääideaali $([2])$ on myös maksimaalinen ideaali. Tekijärenkaan $(\mathbb{Z}_{12}/([2]), +, \cdot)$ kunnaksi osoittaminen on helppoa, sillä joukko $\mathbb{Z}_{12}/([2]) \setminus \{[0] + ([2])\}$ sisältää vain yhden alkion $[1] + ([2])$ ja näin ollen ryhmän $(\mathbb{Z}_{12}/([2]) \setminus \{[0] + ([2])\}, \cdot)$ osoittaminen Abelin ryhmäksi on itsestäänselvyys. Näin ollen tekijärengas $(\mathbb{Z}_{12}/([2]), +, \cdot)$ todellakin on kunta, aivan kuten kuntalaajennuslauseen mukaan pitääkin.

Jatketaan kuntalaajennuksen havainnollistamista hieman suuremman tekijärenkaan parissa.

Esimerkki 7.1.4. Tarkastellaan jäännösluokkarengasta $\mathbb{Z}_{21}$. Nyt lauseen 4.1.2 nojalla $(\mathbb{Z}_{21}, +, \cdot)$ on kommutatiivinen rengas. Sille voidaan myös muodostaa alkion $[7]$ generoima pääideaali eli pääideaali $([7])$. Pääideaalin $([7])$ alkiot saadaan käymällä läpi kaikki renkaan alkiot lauseen 4.1.10 mukaisesti:

$$
\begin{array}{lll}
[0] \cdot [7] = [0 \cdot 7] = [0], & [7] \cdot [7] = [49] = [7], & [14] \cdot [7] = [98] = [14], \\
[1] \cdot [7] = [7], & [8] \cdot [7] = [56] = [14], & [15] \cdot [7] = [105] = [0], \\
[2] \cdot [7] = [14], & [9] \cdot [7] = [63] = [0], & [16] \cdot [7] = [112] = [7], \\
[3] \cdot [7] = [21] = [0], & [10] \cdot [7] = [70] = [7], & [17] \cdot [7] = [119] = [14], \\
[4] \cdot [7] = [28] = [7], & [11] \cdot [7] = [77] = [14], & [18] \cdot [7] = [126] = [0], \\
[5] \cdot [7] = [35] = [14], & [12] \cdot [7] = [84] = [0], & [19] \cdot [7] = [133] = [7], \\
[6] \cdot [7] = [42] = [0], & [13] \cdot [7] = [91] = [7], & [20] \cdot [7] = [140] = [14].
\end{array}
$$

Eli pääideaalin $([7])$ alkioiksi saadaan $\{[0], [7], [14]\}$. Pääideaali $([7])$ on myös selvästi maksimaalinen ideaali lauseen 4.1.13 nojalla. Nyt kuntalaajennuslauseen 7.1.1 nojalla tekijärengas $\mathbb{Z}_{21}/([7])$ on rakenteeltaan kunta.

Muodostetaan tekijärenkaan $\mathbb{Z}_{21}/([7])$ alkiot lauseen 4.2.1 mukaisesti.

$$
\begin{aligned}
\mathbb{Z}_{21}/([7]) &= \{r + ([7]) \mid r \in \mathbb{Z}_{21}\} \\
&= \{[0] + ([7]), [1] + ([7]), [2] + ([7]), [3] + ([7]), [4] + ([7]), [5] + ([7]), \\
&\quad [6] + ([7])\}.
\end{aligned}
$$

Tekijärenkaan $\mathbb{Z}_{21}/([7])$ nolla-alkio on $[0]+([7])$ ja ykkösalkio on $[1]+([7])$.

Nyt kun tekijärenkaan $\mathbb{Z}_{21}/([7])$ alkiot on muodostettu, tarkastellaan tekijärengasta $\mathbb{Z}_{21}/([7])$ hieman tarkemmin. Kaikille tekijärenkaan alkioille löytyy vasta-alkiot, aivan kuten kunnan ehtoihin kuuluu. Koska tekijärenkaan yhteenlasku on kommutatiivinen, tämä riittää osoittaa vain toiseen suuntaan.

Nyt

$$([0]+([7]))+([0]+([7]))=([0]+[0])+([7])=[0]+([7]),$$
$$([1]+([7]))+([6]+([7]))=([1]+[6])+([7])=[7]+([7])=[0]+([7]),$$
$$([2]+([7]))+([5]+([7]))=([2]+[5])+([7])=[7]+([7])=[0]+([7]),$$
$$([3]+([7]))+([4]+([7]))=([3]+[4])+([7])=[7]+([7])=[0]+([7]).$$

Eli

$$\begin{aligned}
-([0]+([7]))&=[0]+([7]), & -([4]+([7]))&=[3]+([7]),\\
-([1]+([7]))&=[6]+([7]), & -([5]+([7]))&=[2]+([7]),\\
-([2]+([7]))&=[5]+([7]), & -([6]+([7]))&=[1]+([7]),\\
-([3]+([7]))&=[4]+([7]).
\end{aligned}$$

Vastaavasti kaikille joukon $\mathbb{Z}_{21}/([7]) \setminus \{[0]+([7])\}$ alkioille on olemassa kunnan ehtojen mukaiset käänteisalkiot. Aivan kuten yhteenlaskun tapauksessa, tekijärenkaan kommutatiivisuuden perusteella kertolasku riittää tarkastella vain toiseen suuntaan.

Nyt

$$([1]+([7]))\cdot([1]+([7]))=([1]\cdot[1])+([7])=[1]+([7]),$$
$$([2]+([7]))\cdot([4]+([7]))=([2]\cdot[4])+([7])=[8]+([7])=[1]+([7]),$$
$$([3]+([7]))\cdot([5]+([7]))=([3]\cdot[5])+([7])=[15]+([7])=[1]+([7]),$$
$$([6]+([7]))\cdot([6]+([7]))=([6]\cdot[6])+([7])=[36]+([7])=[1]+([7]).$$

Eli

$$\begin{aligned}
([1]+([7]))^{-1}&=[1]+([7]), & ([4]+([7]))^{-1}&=[2]+([7]),\\
([2]+([7]))^{-1}&=[4]+([7]), & ([5]+([7]))^{-1}&=[3]+([7]),\\
([3]+([7]))^{-1}&=[5]+([7]), & ([6]+([7]))^{-1}&=[6]+([7]).
\end{aligned}$$

Käänteisalkioiden löytyminen takaa yhdessä kommutatiivisen renkaan määritelmän ohella kunnan ehtojen täyttymisen.

Tarkastellaan kuntalaajennusta vielä hieman erilaisen rakenteen kautta. Vaikka tässä pro gradu -tutkielmassa käsitellään lähinnä jäännösluokkia, samat ryhmäteorian tulokset pätevät myös muiden lukujoukkojen parissa.

Esimerkki 7.1.5. Määritellään aluksi uusi lukujoukko *Gaussin kokonaisluvut*. Gaussin kokonaislukuja merkitään

$$\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\},$$

missä i on imaginääriyksikkö, jolle pätee $i^2=-1$.
Gaussin kokonaisluvuilla yhteenlasku määritellään seuraavalla tavalla:

$$(a+bi)+(c+di)=(a+b)+(b+d)i,$$

kaikilla $(a+bi),(c+di) \in \mathbb{Z}[i]$.
Gaussin kokonaisluvuilla kertolasku määritellään seuraavalla tavalla:

$$\begin{aligned}(a+bi)\cdot(c+di) &= ac+adi+bci+bdi^2\\ &= ac+adi+bci-bd\\ &= (ac-bd)+(ad+bc)i,\end{aligned}$$

kaikilla $(a+bi),(c+di) \in \mathbb{Z}[i]$.

Osoitetaan, että $(\mathbb{Z}[i],+,\cdot)$, missä yhteen- ja kertolasku ovat edellä määritellyt, täyttää kommutatiivisen renkaan ehdot määritelmän 4.1.1. mukaisesti.

$(\mathbb{Z}[i],+,\cdot)$ on kommutatiivinen rengas, jos

1. $(\mathbb{Z}[i],+)$ on Abelin ryhmä. Tämä toteutuu, jos

   1^o Operaatio $(+)$ on binäärinen joukossa $\mathbb{Z}[i]$.

   Nyt
   $$(a_1+b_1i)+(a_2+b_2i) = (a_1+a_2)+(b_1+b_2)i \in \mathbb{Z}[i],$$
   sillä $(a_1+a_2),(b_1+b_2) \in \mathbb{Z}$ kaikilla $(a_1+b_1i),(a_2+b_2i) \in \mathbb{Z}[i]$.

   2^o Operaatio $(+)$ on assosiatiivinen joukossa $\mathbb{Z}[i]$.

   Nyt

   $$\begin{aligned}&(a_1+b_1i)+[(a_2+b_2i)+(a_3+b_3i)]\\ &= (a_1+b_1i)+((a_2+a_3)+(b_2+b_3)i)\\ &= (a_1+(a_2+a_3))+(b_1+(b_2+b_3))i\\ &= ((a_1+a_2)+a_3)+((b_1+b_2)+b_3)i\\ &= ((a_1+a_2)+(b_1+b_2)i)+(a_3+b_3i)\\ &= [(a_1+b_1i)+(a_2+b_2i)]+(a_3+b_3i),\end{aligned}$$

   kaikilla $(a_1+b_1i),(a_2+b_2i),(a_3+b_3i) \in \mathbb{Z}[i]$.

   3^o Joukossa $\mathbb{Z}[i]$ on nolla-alkio.

   Nyt $0+0i=0$ on joukon $\mathbb{Z}[i]$ nolla-alkio, sillä

   $$\begin{aligned}0+(a+bi) &= (0+a)+bi = a+bi,\\ (a+bi)+0 &= (a+0)+bi = a+bi\end{aligned}$$

kaikilla $a + bi \in \mathbb{Z}[i]$.

Nolla-alkio 0 on selvästi yksikäsitteinen, sillä 0 on yksikäsitteinen kokonaislukujoukossa $\mathbb{Z}$, jolloin se on myös Gaussin kokonaisluvuissa yksikäsitteinen.

4^o Jokaisella joukon $\mathbb{Z}[i]$ alkiolla on vasta-alkio joukossa $\mathbb{Z}[i]$.

Olkoon $a + bi \in \mathbb{Z}[i]$. Nyt $(-a) + (-b)i \in \mathbb{Z}[i]$ ja

$$(a + bi) + ((-a) + (-b)i) = (a + (-a)) + (b + (-b))i = (0 + 0i) = 0,$$

$$((-a) + (-b)i) + (a + bi) = ((-a) + a) + ((-b) + b)i = (0 + 0i) = 0$$

kaikilla $a + bi \in \mathbb{Z}[i]$.

5^o Operaatio $(+)$ on kommutatiivinen joukossa $\mathbb{Z}[i]$.

Nyt

$$\begin{aligned}(a_1 + b_1 i) + (a_2 + b_2 i) &= (a_1 + a_2) + (b_1 + b_2)i \\ &= (a_2 + a_1) + (b_2 + b_1)i \\ &= (a_2 + b_2 i) + (a_1 + b_1 i)\end{aligned}$$

kaikilla $(a_1 + b_1 i), (a_2 + b_2 i) \in \mathbb{Z}[i]$.

Kohtien $1^o - 5^o$ nojalla $(\mathbb{Z}[i], +)$ on Abelin ryhmä.

2. $(\mathbb{Z}[i], \cdot)$ on monoidi. Tämä toteutuu, jos

1^o Operaatio $(\cdot)$ on binäärinen joukossa $\mathbb{Z}[i]$.

Nyt

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i \in \mathbb{Z}[i],$$

sillä $(a_1 a_2 - b_1 b_2), (a_1 b_2 + b_1 a_2) \in \mathbb{Z}$ kaikilla $(a_1 + b_1 i), (a_2 + b_2 i) \in \mathbb{Z}[i]$.

2^o Operaatio $(\cdot)$ on assosiatiivinen joukossa $\mathbb{Z}[i]$.

Nyt

$$
\begin{aligned}
&(a_1 + b_1 i) \cdot [(a_2 + b_2 i) \cdot (a_3 + b_3 i)] \\
&= (a_1 + b_1 i) \cdot (a_2 a_3 + a_2 b_3 i + b_2 a_3 i + b_2 b_3 i^2) \\
&= a_1(a_2 a_3) + a_1(a_2 b_3)i + a_1(b_2 a_3)i + a_1(b_2 b_3)i^2 + b_1(a_2 a_3)i + b_1(a_2 b_3)i^2 \\
&\quad + b_1(b_2 a_3)i^2 + b_1(b_2 b_3)i^3 \\
&= (a_1 a_2)a_3 + (a_1 a_2)b_3 i + (a_1 b_2)a_3 i + (a_1 b_2)b_3 i^2 + (b_1 a_2)a_3 i + (b_1 a_2)b_3 i^2 \\
&\quad + (b_1 b_2)a_3 i^2 + (b_1 b_2)b_3 i^3 \\
&= (a_1 a_2 + a_1 b_2 i + b_1 a_2 i + b_1 b_2 i^2) \cdot (a_3 + b_3 i) \\
&= [(a_1 + b_1 i) \cdot (a_2 + b_2 i)] \cdot (a_3 + b_3 i)
\end{aligned}
$$

kaikilla $(a_1 + b_1 i), (a_2 + b_2 i), (a_3 + b_3 i) \in \mathbb{Z}[i]$.

3^o Joukossa $\mathbb{Z}[i]$ on ykkösalkio.

Nyt $1 + 0i = 1$ on joukon $\mathbb{Z}[i]$ ykkösalkio, sillä

$$1 \cdot (a + bi) = (1 \cdot a) + (1 \cdot b)i = a + bi,$$

$$(a + bi) \cdot 1 = (a \cdot 1) + (b \cdot 1)i = a + bi$$

kaikilla $a + bi \in \mathbb{Z}[i]$.

Ykkösalkio 1 on selvästi yksikäsitteinen, sillä 1 on yksikäsitteinen kokonaislukujoukossa $\mathbb{Z}$, jolloin se on myös Gaussin kokonaisluvuissa yksikäsitteinen.

Kohtien $1^o - 3^o$ nojalla $(\mathbb{Z}[i], \cdot)$ on monoidi.

3. Joukon $\mathbb{Z}[i]$ alkioille pätee määritelmän mukaiset osittelulait.

   Nyt

$$
\begin{aligned}
&(a_1 + b_1 i) \cdot [(a_2 + b_2 i) + (a_3 + b_3 i)] \\
&= (a_1 + b_1 i) \cdot ((a_2 + a_3) + (b_2 + b_3)i) \\
&= a_1(a_2 + a_3) + a_1(b_2 + b_3)i + b_1 i(a_2 + a_3) + b_1(b_2 + b_3)i^2 \\
&= a_1 a_2 + a_1 a_3 + a_1 b_2 i + a_1 b_3 i + b_1 a_2 i + b_1 a_3 i + b_1 b_2 i^2 + b_1 b_3 i^2 \\
&= a_1 a_2 + a_1 b_2 i + b_1 a_2 i + b_1 b_2 i^2 + a_1 a_3 + a_1 b_3 i + b_1 a_3 i + b_1 b_3 i^2 \\
&= (a_1 + b_1 i) \cdot (a_2 + b_2 i) + (a_1 + b_1 i) \cdot (a_3 + b_3 i)
\end{aligned}
$$

ja

$$\begin{aligned}
&[(a_1 + b_1 i) + (a_2 + b_2 i)] \cdot (a_3 + b_3 i) \\
&= ((a_1 + a_2) + (b_1 + b_2)i) \cdot (a_3 + b_3 i) \\
&= (a_1 + a_2)a_3 + (a_1 + a_2)b_3 i + (b_1 + b_2)a_3 i + (b_1 + b_2)b_3 i^2 \\
&= a_1 a_3 + a_2 a_3 + a_1 b_3 i + a_2 b_3 i + b_1 a_3 i + b_2 a_3 i + b_1 b_3 i^2 + b_2 b_3 i^2 \\
&= a_1 a_3 + a_1 b_3 i + b_1 a_3 i + b_1 b_3 i^2 + a_2 a_3 + a_2 b_3 i + b_2 a_3 i + b_2 b_3 i^2 \\
&= (a_1 + b_1 i) \cdot (a_3 + b_3 i) + (a_2 + b_2 i) \cdot (a_3 + b_3 i)
\end{aligned}$$

kaikilla $(a_1 + b_1 i), (a_2 + b_2 i), (a_3 + b_3 i) \in \mathbb{Z}[i]$.

Lopuksi tarkistetaan onko joukko $\mathbb{Z}[i]$ kommutatiivinen operaation $(\cdot)$ suhteen.

Nyt

$$\begin{aligned}
(a_1 + b_1 i) \cdot (a_2 + b_2 i) &= a_1 a_2 + a_1 b_2 i + b_1 a_2 i + b_1 b_2 i^2 \\
&= a_2 a_1 + a_2 b_1 i + b_2 a_1 i + b_2 b_1 i^2 \\
&= (a_2 + b_2 i) \cdot (a_1 + b_1 i)
\end{aligned}$$

kaikilla $(a_1 + b_1 i), (a_2 + b_2 i) \in \mathbb{Z}[i]$.

Eli edellä täyttyneiden ehtojen nojalla $(\mathbb{Z}[i], +, \cdot)$ on kommutatiivinen rengas.

Nyt kun tiedetään, että $(\mathbb{Z}[i], +, \cdot)$ on kommutatiivinen rengas, sille täytyy löytyä jokin ideaali.

Olkoon $M = \{2x + 2yi \mid x, y \in \mathbb{Z}\}$. Osoitetaan seuraavaksi, että M on kommutatiivisen renkaan $(\mathbb{Z}[i], +, \cdot)$ ideaali.

M on ideaali, jos se täyttää määritelmän 4.1.5 mukaiset ehdot, eli

1. $(M, +) \leq (\mathbb{Z}[i], +)$.

   Osoitetaan tämä ehto todeksi lauseen 3.2.4 nojalla, eli olkoon a ja b joukon M alkioita. Tällöin $a = 2x+2yi$ ja $b = 2v+2wi$, missä $x, y, v, w \in \mathbb{Z}$.

   Nyt

$$\begin{aligned}
a + (-b) &= (2x + 2yi) + ((-2v) + (-2w)i) \\
&= (2x + (-2v)) + (2y + (-2w))i \\
&= 2(x + (-v)) + 2(y + (-w))i \in M,
\end{aligned}$$

   sillä $(x + (-v)), (y + (-w)) \in \mathbb{Z}$. Eli $(M, +) \leq (\mathbb{Z}[i], +)$.

2. $r \cdot a \in M$ ja $a \cdot r \in M$ kaikilla $a \in M$ ja $r \in \mathbb{Z}[i]$.

   Olkoon $r = k + li$ ja $a = 2x + 2yi$. Tällöin

$$\begin{aligned} r \cdot a &= (k + li) \cdot (2x + 2yi) \\ &= 2kx + 2kyi + 2lxi + 2lyi^2 \\ &= 2kx + 2kyi + 2lxi - 2ly \\ &= 2kx - 2ly + 2kyi + 2lxi \\ &= 2(kx - ly) + 2(ky + lx)i \in M, \end{aligned}$$

   sillä $(kx - ly), (ky + lx) \in \mathbb{Z}$.

   Vastaavasti

$$\begin{aligned} a \cdot r &= (2x + 2yi) \cdot (k + li) \\ &= 2xk + 2xli + 2yki + 2yli^2 \\ &= 2xk + 2xli + 2yki - 2yl \\ &= 2xk - 2yl + 2xli + 2yki \\ &= 2(xk - yl) + 2(xl + yk)i \in M, \end{aligned}$$

   sillä $(xk - yl), (xl + yk) \in \mathbb{Z}$.

Kohtien 1 ja 2 nojalla M on renkaan $(\mathbb{Z}[i], +, \cdot)$ ideaali.
Nyt kommutatiivisen renkaan $(\mathbb{Z}[i], +, \cdot)$ ja sen ideaalin $M = \{2x+2yi \mid x, y \in \mathbb{Z}\}$ avulla voidaan muodostaa tekijärengas $\mathbb{Z}[i]/M$. Tekijärenkaan $\mathbb{Z}[i]/M$ alkiot ovat ideaalin M sivuluokat:

$$\begin{aligned} 0 + M &= \{2x + 2yi \mid x, y \in \mathbb{Z}\} \\ &= \{x + yi \in \mathbb{Z}[i] \mid x \text{ ja } y \text{ ovat parillisia kokonaislukuja}\}, \\ 1 + M &= \{(2x + 1) + 2yi \mid x, y \in \mathbb{Z}\} \\ &= \{x + yi \in \mathbb{Z}[i] \mid x \text{ on pariton ja } y \text{ on parillinen kokonaisluku}\}, \\ i + M &= \{2x + (2y + 1)i \mid x, y \in \mathbb{Z}\} \\ &= \{x + yi \in \mathbb{Z}[i] \mid x \text{ on parillinen ja } y \text{ on pariton kokonaisluku}\}, \\ 1 + i + M &= \{(2x + 1) + (2y + 1)i \mid x, y \in \mathbb{Z}\} \\ &= \{x + yi \in \mathbb{Z}[i] \mid x \text{ ja } y \text{ ovat parittomia kokonaislukuja}\}. \end{aligned}$$

Eli tekijärenkaan alkiot ovat $\mathbb{Z}[i]/M = \{0 + M, 1 + M, i + M, 1 + i + M\}$. Nyt kun on muodostettu kommutatiivinen tekijärengas $(\mathbb{Z}[i]/M, +, \cdot)$, voidaan kysyä, että onko se myös kunta. Kuntalaajennuslauseen mukaan tekijärengas $\mathbb{Z}[i]/M$ on kunta, jos M on maksimaalinen ideaali. Toisaalta, mistä tiedetään onko M maksimaalinen ideaali?

Tutkitaan tekijärenkaan alkioiden kertolaskutaulua ilman nolla-alkiota $0 + M$.

Nyt

$\cdot$	$1 + M$	$i + M$	$1 + i + M$
$1 + M$	$1 + M$	$i + M$	$1 + i + M$
$i + M$	$i + M$	$1 + M$	$1 + i + M$
$1 + i + M$	$1 + i + M$	$1 + i + M$	$0 + M$

Kuten kertolaskutaulusta ilman nolla-alkiota voidaan päätellä, tekijärenkaan alkiolla $1 + i + M$ ei ole käänteisalkiota, eikä tekijärengas näin ollen voi olla kunta. Näin ollen ideaali M ei voi myöskään olla maksimaalinen ideaali.

Seuraavassa luvussa perehdytään kokonaisalueen laajentamiseen kunnaksi uusien määritelmien avulla.

8 Osamääräkunta

Vaikka edellisessä luvussa käsiteltiinkin tämän pro gradu -tutkielman keskeinen asia, tämä luku laajentaa sen teoriaa uudella, mielenkiintoisella tavalla.

8.1 Osamääräkuntien teoria

Osamääräkuntaa tutkittaessa täytyy määritellä uusi relaatio kokonaisalueen D avulla muodostetussa joukossa, jonka jälkeen päästään käsiksi ekvivalenssiluokkiin ja niiden välisiin laskuoperaatioihin. Aloitetaan kuitenkin määrittelemällä kokonaisalueen D avulla uusi joukko $\mathcal{D}$.

$$\mathcal{D} = D \times (D \setminus \{\mathbf{0}\}) = \{(a, b) \mid a \in D, b \in D \setminus \{\mathbf{0}\}\}.$$

Nyt voimme määritellä uuden relaation joukossa $\mathcal{D}$ ja todistaa, että se on myös ekvivalenssirelaatio.

Määritelmä 8.1.1. Olkoon D kokonaisalue ja $a, b, c, d \in D, b \neq \mathbf{0}, d \neq \mathbf{0}$. Asetetaan relaatio

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

Lause 8.1.2. *Relaatio* $(\sim)$ *on ekvivalenssirelaatio joukossa* $\mathcal{D}$.

Todistus. Tarkastellaan toteuttaako relaatio $\sim$ ekvivalenssirelaation ehdot:

1. Ensimmäisenä tarkastellaan relaation refleksiivisyyttä.

   Nyt $(a, b) \sim (a, b)$, koska $ab = ba$, eli tulo on kommutatiivinen kokonaisalueessa D.

2. Toisena tarkastellaan relaation symmetrisyyttä.

   Jos $(a, b) \sim (c, d)$, niin $ad = bc$. Koska tulo on kommutatiivinen kokonaisalueessa D, voidaan päätellä, että $cb = da$ ja näin ollen $(c, d) \sim (a, b)$.

3. Kolmanneksi tarkastellaan relaation transitiivisuutta.

   Jos $(a, b) \sim (c, d)$ ja $(c, d) \sim (r, s)$, niin $ad = bc$ ja $cs = dr$. Käyttäen näitä relaatioita ja muistaen, että tulo on kommutatiivinen kokonaisalueessa D, saadaan

   $$asd = sad = sbc = bcs = bdr = brd.$$

   Tiedetään, että $d \neq \mathbf{0}$ ja D on kokonaisalue. Nyt $asd = brd$ ja lauseen 5.1.5 nojalla saadaan $as = br$. Näin ollen $(a, b) \sim (r, s)$.

□

Seuraavaksi määritellään ekvivalenssiluokille merkintätapa.

Määritelmä 8.1.3. Asetetaan ekvivalenssiluokka

$$[(a,b)] = [a,b] = \{(c,d) \in \mathcal{D} \mid (c,d) \sim (a,b)\}.$$

Tällöin

$$(c,d) \in [a,b] \Leftrightarrow [c,d] = [a,b].$$

Määritellään ekvivalenssiluokkien välinen yhteenlasku

$$[a,b] + [c,d] = [ad + cb, bd].$$

Vastaavasti määritellään kertolasku

$$[a,b][c,d] = [ac, bd].$$

Nämä operaatiot pätevät aina, kun $(a,b), (c,d) \in \mathcal{D}$. Osoitetaan, että operaatiot ovat hyvin määritellyt, eli ekvivalenssiluokkien välinen yhteenlasku ja kertolasku ovat riippumattomia alkioiden a, b, c, d valinnasta.

Valitaan toiset sellaiset alkiot a', b', c', d', että $[a,b] = [a',b']$ ja $[c,d] = [c',d']$. Jos operaatiot ovat hyvin määritellyt, niin $[a,b]+[c,d] = [a',b']+[c',d']$ ja $[a,b][c,d] = [a',b'][c',d']$.

Aloitetaan ekvivalenssiluokkien välisestä yhteenlaskusta. Kuten edellä todettiin, täytyy osoittaa, että $[a,b] + [c,d] = [a',b'] + [c',d']$ eli $[ad + bc, bd] = [a'd' + b'c', b'd']$. Nyt ekvivalenssiluokkien ja relaation määritelmän nojalla täytyy olla, että $(ad+bc)b'd' = bd(a'd'+b'c')$. Vastaavasti, kun $[a,b] = [a',b']$ ja $[c,d] = [c',d']$, niin $ab' = ba'$ ja $cd' = dc'$. Tällöin $(ad + bc)b'd' = ab'dd' + bb'cd' = ba'dd' + bb'dc' = (a'd' + b'c')bd$, aivan kuten pitääkin. Näin ollen ekvivalenssiluokkien välinen yhteenlasku on hyvin määritelty joukossa $\mathcal{D}$.

Jatketaan ekvivalenssiluokkien välisestä kertolaskusta. Täytyy siis osoittaa, että $[a,b][c,d] = [a',b'][c',d']$, eli $[ac,bd] = [a'c', b'd']$. Kuten aiemmin todettiin, tiedetään, että $ab' = ba'$ ja $cd' = dc'$. Ekvivalenssiluokkien ja relaation määritelmän nojalla täytyy olla, että $acb'd' = bda'c'$. Lähtien yhtälön vasemmalta puolen saadaan $acb'd' = ab'cd' = ba'dc' = bda'c'$, aivan kuten pitääkin. Näin ollen ekvivalenssiluokkien välinen kertolasku on hyvin määritelty joukossa $\mathcal{D}$.

Merkitään vielä

$$Q(D) = \{[a,b] \mid (a,b) \in \mathcal{D}\} = \{\frac{a}{b} \mid (a,b) \in \mathcal{D}\}.$$

Nyt voidaan seuraavassa lauseessa osoittaa, että $(Q(D), +, \cdot)$ todellakin on kunta.

Lause 8.1.4. *Kolmikko* $(Q(D), +, \cdot)$ *on kunta.*

Todistus. Osoitetaan lause todeksi lauseen 6.1.3 ehtojen kautta kolmessa vaiheessa.

1. Osoitetaan aluksi, että $(Q(D), +)$ on Abelin ryhmä.

   Nyt $(Q(D), +)$ on Abelin ryhmä, jos

   1^o Operaatio $(+)$ on binäärinen joukossa $Q(D)$.

   Nyt

   $$[a_1, b_1] + [a_2, b_2] = [a_1 b_2 + a_2 b_1, b_1 b_2] \in Q(D),$$

   sillä $a_1 b_2 + a_2 b_1 \in D$ ja $b_1 b_2 \in D \setminus \{\mathbf{0}\}$ kaikilla $[a_1, b_1], [a_2, b_2] \in Q(D)$.

   2^o Operaatio $(+)$ on assosiatiivinen joukossa $Q(D)$.

   Nyt

   $$\begin{aligned} &[a_1, b_1] + ([a_2, b_2] + [a_3, b_3]) \\ &= [a_1, b_1] + [a_2 b_3 + a_3 b_2, b_2 b_3] \\ &= [a_1 b_2 b_3 + a_2 b_1 b_3 + a_3 b_1 b_2, b_1 b_2 b_3] \\ &= [a_1 b_2 + a_2 b_1, b_1 b_2] + [a_3, b_3] \\ &= ([a_1, b_1] + [a_2, b_2]) + [a_3, b_3] \end{aligned}$$

   kaikilla $[a_1, b_1], [a_2, b_2], [a_3, b_3] \in Q(D)$.

   3^o Joukossa $Q(D)$ on nolla-alkio.

   Nyt huomataan, että kaikki alkiot muotoa $[\mathbf{0}, a] \in Q(D)$ ovat nolla-alkioita, sillä

   $$[c, d] + [\mathbf{0}, a] = [ca + \mathbf{0} \cdot d, da] = [ca + \mathbf{0}, da] = [ca, da] = [c, d],$$

   sillä ekvivalenssiluokkien ja relaation määritelmän nojalla, jos $[ca, da] = [c, d]$, niin $cad = dac = cad$, mikä pitää paikkansa.

   Vastaavasti

   $$[\mathbf{0}, a] + [c, d] = [\mathbf{0} \cdot d + ca, ad] = [\mathbf{0} + ac, ad] = [ac, ad] = [c, d],$$

   sillä aivan kuten edellä $acd = adc$, mikä pitää paikkansa.

Edellä olleet yhteenlaskut pätevät kaikilla $[c,d] \in Q(D)$.

Kuitenkin nolla-alkio on yksikäsitteinen, sillä $[\mathbf{0},a] = [\mathbf{0},\mathbf{1}]$. Tämä seuraa siitä, että $(\mathbf{0},a) \in [\mathbf{0},\mathbf{1}]$, sillä $(\mathbf{0},a) \sim (\mathbf{0},\mathbf{1})$ kaikilla $a \in D \setminus \{\mathbf{0}\}$.

4^o Jokaisella joukon $Q(D)$ alkiolla on vasta-alkio joukossa $Q(D)$.

Olkoon $[a,b] \in Q(D)$. Nyt $[-a,b] \in Q(D)$ ja

$$[a,b]+[-a,b] = [ab+(-a)b, b^2] = [(a-a)b, b^2] = [\mathbf{0}\cdot b, b^2] = [\mathbf{0}, b^2] = [\mathbf{0},\mathbf{1}],$$

$$[-a,b]+[a,b] = [(-a)b+ab, b^2] = [((-a)+a)b, b^2] = [\mathbf{0}\cdot b, b^2] = [\mathbf{0}, b^2] = [\mathbf{0},\mathbf{1}]$$

kaikilla $[a,b] \in Q(D)$.

Näin ollen alkion $[a,b]$ vasta-alkio $-[a,b] = [-a,b]$.

5^o Operaatio $(+)$ on kommutatiivinen joukossa $Q(D)$.

Nyt

$$\begin{aligned}[a_1,b_1] + [a_2,b_2] &= [a_1b_2 + a_2b_1, b_1b_2] \\ &= [a_2b_1 + a_1b_2, b_2b_1] \\ &= [a_2,b_2] + [a_1,b_1]\end{aligned}$$

kaikilla $[a_1,b_1], [a_2,b_2] \in Q(D)$.

Kohtien $1^o - 5^o$ nojalla $(Q(D),+)$ on Abelin ryhmä.

2. Osoitetaan seuraavaksi, että $(Q(D) \setminus \{[\mathbf{0},\mathbf{1}]\},\cdot)$ on Abelin ryhmä.

   Nyt $(Q(D) \setminus \{[\mathbf{0},\mathbf{1}]\},\cdot)$ on Abelin ryhmä, jos

   1^o Operaatio $(\cdot)$ on binäärinen joukossa $Q(D) \setminus \{[\mathbf{0},\mathbf{1}]\}$.

   Nyt

   $$[a_1,b_1] \cdot [a_2,b_2] = [a_1a_2, b_1b_2] \in Q(D) \setminus \{[\mathbf{0},\mathbf{1}]\},$$

   sillä $a_1a_2 \in D \setminus \{\mathbf{0}\}$ ja $b_1b_2 \in D \setminus \{\mathbf{0}\}$ kaikilla $[a_1,b_1], [a_2,b_2] \in Q(D) \setminus \{[\mathbf{0},\mathbf{1}]\}$.

   2^o Operaatio $(\cdot)$ on assosiatiivinen joukossa $Q(D) \setminus \{[\mathbf{0},\mathbf{1}]\}$.

Nyt

$$\begin{aligned}
&[a_1, b_1] \cdot ([a_2, b_2] \cdot [a_3, b_3]) \\
&= [a_1, b_1] \cdot [a_2 a_3, b_2 b_3] \\
&= [a_1 a_2 a_3, b_1 b_2 b_3] \\
&= [a_1 a_2, b_1 b_2] \cdot [a_3, b_3] \\
&= ([a_1, b_1] \cdot [a_2, b_2]) \cdot [a_3, b_3]
\end{aligned}$$

kaikilla $[a_1, b_1], [a_2, b_2], [a_3, b_3] \in Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$.

3^o Joukossa $Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$ on ykkösalkio.

Nyt huomataan, että kaikki alkiot muotoa $[a, a] \in Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$ ovat ykkösalkioita, sillä

$$[c, d] \cdot [a, a] = [ca, da] = [c, d],$$

$$[a, a] \cdot [c, d] = [ac, ad] = [c, d]$$

kaikilla $[c, d] \in Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$. Viimeiset yhtäsuuruudet voidaan olettaa kohdan 1.3^o perustelujen nojalla.

Kuitenkin ykkösalkio on yksikäsitteinen, sillä $[a, a] = [\mathbf{1}, \mathbf{1}]$. Tämä seuraa siitä, että $(a, a) \in [\mathbf{1}, \mathbf{1}]$, sillä $(a, a) \sim (\mathbf{1}, \mathbf{1})$ kaikilla $a \in D \setminus \{\mathbf{0}\}$.

4^o Jokaisella joukon $Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$ alkiolla on käänteisalkio joukossa $Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$.

Olkoon $[a, b] \in Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$. Nyt $[b, a] \in Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$ ja

$$[a, b] \cdot [b, a] = [ab, ba] = [ab, ab] = [\mathbf{1}, \mathbf{1}],$$

$$[b, a] \cdot [a, b] = [ba, ab] = [ab, ab] = [\mathbf{1}, \mathbf{1}]$$

kaikilla $[a, b] \in Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$.

Näin ollen alkion $[a, b]$ käänteisalkio $[a, b]^{-1} = [b, a]$.

5^o Operaatio $(\cdot)$ on kommutatiivinen joukossa $Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$.

Nyt

$$\begin{aligned}
[a_1, b_1] \cdot [a_2, b_2] &= [a_1 a_2, b_1 b_2] \\
&= [a_2 a_1, b_2 b_1] \\
&= [a_2, b_2] \cdot [a_1, b_1]
\end{aligned}$$

kaikilla $[a_1, b_1], [a_2, b_2] \in Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}$.

Kohtien $1^o - 5^o$ nojalla $(Q(D) \setminus \{[\mathbf{0}, \mathbf{1}]\}, \cdot)$ on Abelin ryhmä.

3. Osoitetaan lopuksi, että osittelulait ovat voimassa.

   Nyt

$$\begin{aligned}[a_1,b_1]\cdot([a_2,b_2]+[a_3,b_3]) &= [a_1,b_1]\cdot[a_2b_3+a_3b_2,b_2b_3]\\ &= [a_1a_2b_3+a_1a_3b_2,b_1b_2b_3]\\ &= [a_1a_2b_1b_3+a_1a_3b_1b_2,b_1b_2b_1b_3]\\ &= [a_1a_2,b_1b_2]+[a_1a_3,b_1b_3]\\ &= [a_1,b_1]\cdot[a_2,b_2]+[a_1,b_1]\cdot[a_3,b_3]\end{aligned}$$

   ja

$$\begin{aligned}([a_1,b_1]+[a_2,b_2])\cdot[a_3,b_3] &= [a_1b_2+a_2b_1,b_1b_2]\cdot[a_3,b_3]\\ &= [a_1b_2a_3+a_2b_1a_3,b_1b_2b_3]\\ &= [a_1a_3b_2b_3+a_2a_3b_1b_3,b_1b_3b_2b_3]\\ &= [a_1a_3,b_1b_3]+[a_2a_3,b_2b_3]\\ &= [a_1,b_1]\cdot[a_3,b_3]+[a_2,b_2]\cdot[a_3,b_3]\end{aligned}$$

   kaikilla $[a_1,b_1],[a_2,b_2],[a_3,b_3]\in Q(D)$.

Eli kohtien 1. 2. ja 3. nojalla $(Q(D),+,\cdot)$ on kunta.

□

Nyt voidaan esittää kunnalle $Q(D)$ seuraavanlainen määritelmä.

Määritelmä 8.1.5. Olkoon $(D,+,\cdot)$ kokonaisalue. Tällöin kunta $Q(D)$ on kokonaisalueen D *osamääräkunta*.

Tällöin pätee myös seuraava rengasisomorfiatulos.

Lause 8.1.6. *Olkoon $(D,+,\cdot)$ kokonaisalue. Tällöin on voimassa tulos*

$$\{[a,\mathbf{1}] \mid a\in D\} = \{\frac{a}{\mathbf{1}} \mid a\in D\} \cong D.$$

Todistus. Merkitään $A=\{[a,\mathbf{1}] \mid a\in D\}$ ja osoitetaan aluksi, että A on renkaan $Q(D)$ alirengas alirengaskriteerin avulla.

1. Olkoon $[a,\mathbf{1}],[b,\mathbf{1}]\in A$. Tällöin

   $$[a,\mathbf{1}]+(-[b,\mathbf{1}]) = [a,\mathbf{1}]+[-b,\mathbf{1}] = [a\cdot\mathbf{1}+(-b)\cdot\mathbf{1},\mathbf{1}\cdot\mathbf{1}] = [a+(-b),\mathbf{1}]\in A.$$

2. Olkoon $[a,\mathbf{1}],[b,\mathbf{1}]\in A$. Tällöin $[a,\mathbf{1}]\cdot[b,\mathbf{1}] = [a\cdot b,\mathbf{1}\cdot\mathbf{1}] = [ab,\mathbf{1}]\in A$.

3. Renkaan $Q(D)$ ykkösalkio on $[\mathbf{1},\mathbf{1}]$ ja $[\mathbf{1},\mathbf{1}] \in A$.

Kohtien $1-3$ nojalla alirengaskriteeri toteutuu, eli A on renkaan $Q(D)$ alirengas.
Määritellään kuvaus $f : (A,+,\cdot) \to (D,+,\cdot)$ siten, että

$$f([a,\mathbf{1}]) = a$$

kaikilla $a \in D$.
Osoitetaan, että kuvaus f on rengasisomorfismi $A \to D$ osoittamalla, että kuvaus f toteuttaa rengashomomorfismin ehdot ja on bijektio.

1. Aloitetaan rengashomomorfismin ehdoista.

   1^o Olkoon $[a,\mathbf{1}],[b,\mathbf{1}] \in A$. Tällöin

   $$f([a,\mathbf{1}]+[b,\mathbf{1}]) = f([(a+b),\mathbf{1}]) = a+b = f([a,\mathbf{1}]) + f([b,\mathbf{1}]).$$

   2^o Olkoon $[a,\mathbf{1}],[b,\mathbf{1}] \in A$. Tällöin

   $$f([a,\mathbf{1}]\cdot[b,\mathbf{1}]) = f([(a\cdot b),\mathbf{1}]) = a\cdot b = f([a,\mathbf{1}])\cdot f([b,\mathbf{1}]).$$

   3^o Renkaan $(A,+,\cdot)$ ykkösalkio on $[\mathbf{1},\mathbf{1}]$, missä $\mathbf{1} \in D$ on renkaan $(D,+,\cdot)$ ykkösalkio. Nyt $f([\mathbf{1},\mathbf{1}]) = \mathbf{1}$.

   Kohtien $1^o - 3^o$ nojalla kuvaus f on rengashomomorfismi.

2. Tutkitaan onko kuvaus f surjektio ja injektio.

   1^o Olkoon $x \in D$. Tällöin $[x,\mathbf{1}] \in A$ ja $f([x,\mathbf{1}]) = x$, joten f on surjektio.

   2^o Olkoon $[a,\mathbf{1}],[b,\mathbf{1}] \in A$ ja $f([a,\mathbf{1}]) = f([b,\mathbf{1}])$. Tällöin $a = b$, joten $[a,\mathbf{1}] = [b,\mathbf{1}]$. Siispä f on injektio.

   Kohtien 1^o ja 2^o nojalla kuvaus f on bijektio.

Kohtien 1 ja 2 nojalla kuvaus f on rengasisomorfismi $A \to D$, joten

$$A = \{[a,\mathbf{1}] \mid a \in D\} \cong D.$$

□

Rengasisomorfiatuloksen nojalla voidaan merkitä $a = \dfrac{a}{\mathbf{1}}$. Jos $a,b \in D$ ja b^{-1} on olemassa, niin

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

Voidaan myös osoittaa, että merkinnälle pätee supistamis- ja laventamislait.

Lause 8.1.7. *Olkoon D kokonaisalue. Tällöin on voimassa seuraavat tulokset:*

$$\frac{ac}{bc} = \frac{a}{b} \text{ ja } \frac{a}{b} = \frac{da}{db},$$

kaikilla $a, b, c, d \in D$, $b, c, d \neq 0$.

Todistus. Nyt

$$\begin{aligned}
\frac{ac}{bc} &= \frac{a}{\mathbf{1}} \cdot \frac{c}{\mathbf{1}} \cdot \frac{\mathbf{1}}{b} \cdot \frac{\mathbf{1}}{c} \\
&= \frac{a}{\mathbf{1}} \cdot \frac{c}{\mathbf{1}} \cdot (\frac{b}{\mathbf{1}})^{-1} \cdot (\frac{c}{\mathbf{1}})^{-1} \\
&= \frac{a}{\mathbf{1}} \cdot (\frac{b}{\mathbf{1}})^{-1} \cdot \frac{c}{\mathbf{1}} \cdot (\frac{c}{\mathbf{1}})^{-1} \\
&= \frac{a}{\mathbf{1}} \cdot (\frac{b}{\mathbf{1}})^{-1} \cdot \frac{\mathbf{1}}{\mathbf{1}} \\
&= \frac{a}{\mathbf{1}} \cdot (\frac{b}{\mathbf{1}})^{-1} \\
&= \frac{a}{\mathbf{1}} \cdot \frac{\mathbf{1}}{b} = \frac{a}{b}
\end{aligned}$$

ja

$$\begin{aligned}
\frac{a}{b} &= \frac{a}{\mathbf{1}} \cdot \frac{\mathbf{1}}{b} \\
&= \frac{a}{\mathbf{1}} \cdot \frac{d}{\mathbf{1}} \cdot (\frac{d}{\mathbf{1}})^{-1} \cdot \frac{\mathbf{1}}{b} \\
&= \frac{d}{\mathbf{1}} \cdot \frac{a}{\mathbf{1}} \cdot (\frac{d}{\mathbf{1}})^{-1} \cdot \frac{\mathbf{1}}{b} \\
&= \frac{d}{\mathbf{1}} \cdot \frac{a}{\mathbf{1}} \cdot \frac{\mathbf{1}}{d} \cdot \frac{\mathbf{1}}{b} = \frac{da}{db}.
\end{aligned}$$

□

Seuraava lause esittelee yhden tutun osamääräkunnan.

Lause 8.1.8. *Rationaalilukujen joukko $\mathbb{Q}$ on kokonaislukujoukon $\mathbb{Z}$ osamääräkunta, eli $\mathbb{Q} = Q(\mathbb{Z})$.*

Todistus. Nyt $(\mathbb{Z}, +, \cdot)$ on kokonaisalue ja $(\mathbb{Q}, +, \cdot)$ on kunta. Osoitetaan väite todeksi kuntaisomorfismin avulla. Jos löydetään kuvaus $f : Q(\mathbb{Z}) \to \mathbb{Q}$, joka on kuntaisomorfismi, niin väite on tosi.

Olkoon kuvaus $f : Q(\mathbb{Z}) \to \mathbb{Q}$ sellainen, että $f([a, b]) = \frac{a}{b}$. Osoitetaan kuvaus f kuntaisomorfismiksi kahdessa vaiheessa. Kuvaus f on kuntaisomorfismi, jos

1. Kuvaus f toteuttaa rengashomomorfismin ehdot.

   1^o Olkoon $[a_1, b_1], [a_2, b_2] \in Q(\mathbb{Z})$. Tällöin

$$\begin{aligned} f([a_1, b_1] + [a_2, b_2]) &= f([a_1b_2 + a_2b_1, b_1b_2]) \\ &= \frac{a_1b_2 + a_2b_1}{b_1b_2} = \frac{a_1b_2}{b_1b_2} + \frac{a_2b_1}{b_1b_2} \\ &= \frac{a_1}{b_1} + \frac{a_2}{b_2} = f([a_1, b_1]) + f([a_2, b_2]) \end{aligned}$$

   kaikilla $a_1, a_2 \in \mathbb{Z}$, $b_1, b_2 \in \mathbb{Z} \setminus \{0\}$.

   2^o Olkoon $[a_1, b_1], [a_2, b_2] \in Q(\mathbb{Z})$. Tällöin

$$\begin{aligned} f([a_1, b_1] \cdot [a_2, b_2]) &= f([a_1a_2, b_1b_2]) \\ &= \frac{a_1a_2}{b_1b_2} = \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} \\ &= f([a_1, b_1]) \cdot f([a_2, b_2]) \end{aligned}$$

   kaikilla $a_1, a_2 \in \mathbb{Z}$, $b_1, b_2 \in \mathbb{Z} \setminus \{0\}$.

   3^o Olkoon $[a, a] \in Q(\mathbb{Z})$ osamääräkunnan $Q(\mathbb{Z})$ ykkösalkio. Tällöin

$$f([a, a]) = \frac{a}{a} = \frac{1}{1} = 1$$

   kaikilla $a \in \mathbb{Z} \setminus \{0\}$ ja 1 on kunnan $\mathbb{Q}$ ykkösalkio.

   Kohtien $1^o - 3^o$ nojalla kuvaus f on kuntashomomorfismi.

2. Kuvaus f on bijektio. Tämä toteutuu, jos kuvaus f on sekä surjektio että injektio.

   1^o Olkoon $\frac{a}{b} \in \mathbb{Q}$. Tällöin $a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}$ ja $f([a, b]) = \frac{a}{b}$, missä $[a, b] \in Q(\mathbb{Z})$. Näin ollen f on surjektio.

2^o Olkoot $[a_1, b_1], [a_2, b_2] \in Q(\mathbb{Z})$ ja $f([a_1, b_1]) = f([a_2, b_2])$. Tällöin

$$\begin{aligned} f([a_1, b_1]) &= f([a_2, b_2]), \\ \frac{a_1}{b_1} &= \frac{a_2}{b_2}, \\ \frac{a_1}{b_1} \cdot b_1 b_2 &= \frac{a_2}{b_2} \cdot b_1 b_2, \\ \frac{a_1 b_1 b_2}{b_1} &= \frac{a_2 b_1 b_2}{b_2}, \\ a_1 b_2 &= a_2 b_1, \\ [a_1, b_1] &= [a_2, b_2]. \end{aligned}$$

Viimeinen vaihe seuraa ekvivalenssiluokkien määritelmästä 8.1.3. Näin ollen f on injektio.

kohtien 1^o ja 2^o nojalla kuvaus f on bijektio.

Kohtien 1 ja 2 nojalla kuvaus $f : Q(\mathbb{Z}) \to \mathbb{Q}$ on isomorfismi ja tarkemmin ottaen kuntaisomorfismi $Q(\mathbb{Z}) \to \mathbb{Q}$, joten $Q(\mathbb{Z}) \cong \mathbb{Q}$. Eli $\mathbb{Q}$ on kokonaislukujoukon $\mathbb{Z}$ osamääräkunta.

□

Lähdeluettelo

[1] Fraleigh, J.B: *A First Course in Abstract Algebra.* 6e. Addison-Wesley. 1998.

[2] Herstein, I.N.:*Abstract Algebra.* 3e. Prentice-Hall,Inc. 1996.

[3] Niemenmaa, M., Myllylä, K., Tirilä, J., Torvikoski, A & Törmä, T.: *Luentomoniste*: 802355A Renkaat, kunnat ja polynomit. Oulun yliopisto. 2013.

[4] O'Connor, J.J., Robertson, E.F., *Mactutor History of Mathematics*, (University of St Andrews, Scotland, Helmikuu 1996) http://www-history.mcs.st-andrews.ac.uk/HistTopics/Beginnings_of_set_theory.html

[5] O'Connor, J.J., Robertson, E.F., *Mactutor History of Mathematics*, (University of St Andrews, Scotland, Toukokuu 1996) http://www-history.mcs.st-andrews.ac.uk/HistTopics/Development_group_theory.html

[6] O'Connor, J.J., Robertson, E.F., *Mactutor History of Mathematics*, (University of St Andrews, Scotland, Joulukuu 1996) http://www-history.mcs.st-andrews.ac.uk/Biographies/Galois.html

[7] O'Connor, J.J., Robertson, E.F., *Mactutor History of Mathematics*, (University of St Andrews, Scotland, Maaliskuu 2001) http://www-history.mcs.st-andrews.ac.uk/HistTopics/Abstract_groups.html