Ortogonaalit latinalaiset neliöt

M. Tamminen

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Syksy 2013

Tiivistelmä: M. Tamminen, *Ortogonaalit latinalaiset neliöt* (engl. *Orthogonal Latin squares*), matematiikan pro gradu -tutkielma, 27. s., Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, syksy 2013.

Tässä tutkielmassa perehdytään ortogonaaleihin latinalaisiin neliöihin, niiden muodostamiseen äärellisten kuntien avulla, äärellisiin kuntiin ja kuntalaajennuksiin sekä niiden taustalla olevaan rengasteoriaan.

Kertaluvun k latinalainen neliö on taulukko, johon jonkin k alkion joukon S alkiot on järjestetty siten, että kukin alkio esiintyy taulukon jokaisella rivillä ja sarakkeella täsmälleen kerran. Kaksi saman kertaluvun latinalaista neliötä taas ovat keskenään ortogonaalit, jos ne päällekäin asetettuna muodostavat taulukon, jossa jokainen ensimmäisen neliön alkio esiintyy jokaisen toisen neliön alkion kanssa täsmälleen kerran. Kahdesta keskenään ortogonaalista latinalaisesta neliöstä päällekäin asettamalla saatua neliötä kutsutaan Eulerin neliöksi. Nimi juontuu Eulerin ongelmista tällaisen neliön muodostamisessa kertaluvuilla 6, 10, 14 ....

Eulerin aikojen jälkeen on todistettu, että tällaisia neliöitä voidaan muodostaa kaikilla muilla kuin kertaluvuilla 2 ja 6. Tässä tutkielmassa käsitellään kuitenkin lähinnä Eulerin neliöitä, jotka ovat kertalukua $q = p^m$, missä p on alkuluku ja m luonnollinen luku. Kertaluvun q neliöitä voidaan muodostaa äärellisten kuntien laskutauluista. Siksi tässä tutkielmassa perehdytään myös kunta- ja rengasteoriaan ja opitaan konstruoimaan q alkion kuntia kaikilla alkuluvuilla p ja luonnollisilla luvuilla m. Yhtenä esimerkkinä tutkielmassa käytetään pelikorttiongelmaa, jossa korteista on muodostettava 4. kertaluvun Eulerin neliö. Ongelmalle annetaan ratkaisu tutkielman loppupuolella ja sen kaikki vaiheet selvitetään matkan varrella. Lopuksi Eulerin neliöiden avulla muodostetaan myös nk. taikaneliöitä.

Kuten todettu, äärellisten kuntien yhteenlaskutaulut ovat latinalaisia neliöitä. Jos $x_0 = 0, x_1 = 1, x_2, \ldots, x_n$ ovat kunnan F alkiot, on laskun $x_k x_i + x_j$ laskutaulu n. kertaluvun latinalainen neliö kaikilla $1 \leq k \leq n$. Selvästi siis n alkion kunnan F alkioista voidaan muodostaa $n-1$ n. kertaluvun latinalaista neliötä. Nämä neliöt ovat kaikki vieläpä pareittain ortogonaaleja. Kun tiedetään, että äärellisessä kunnassa on aina p^m alkiota jollain alkuluvulla p ja luonnollisella luvulla m, tiedetään myös kertaluvun $q = p^m$ pareittain ortogonaalien latinalaisten neliöiden maksimilukumäärä. Laskutaulujen avulla nuo neliöt saadaan myös muodostettua, kunhan tiedetään mistä alkioista kyseinen kunta koostuu ja mitkä ovat sen laskutoimitukset.

Tässä kirjoitelmassa esitellään p^m alkion kunnan konstruointi kuntalaajennuksena kunnasta $\mathbb{Z}_p$. Kuntateorian pohjustamiseksi kirjoitelma alkaa abstraktin algebran perusasioiden ja erityisesti renkaisiin liittyvien asioiden kertaamisella. Kuntalaajennusta varten muodostetaan ensin euklidinen polynomirengas $\mathbb{Z}_p[x]$. Etsitään jokin m. asteen jaoton polynomi $p(x) \in \mathbb{Z}_p[x]$ ja muodostetaan tekijärengas $\mathbb{Z}_p[x]/p(x)$. Tämä rengas $\mathbb{Z}_p[x]/p(x)$ on kunta, jossa on täsmälleen p^m alkiota. Kunnan $\mathbb{Z}_p[x]/p(x)$ alkioista voidaan siis muodostaa pareittain ortogonaaleja latinalaisia neliöitä sen laskutaulujen avulla. Laskeminen on kuitenkin helpompaa kunnan $\mathbb{Z}_p(\alpha)$ avulla, joka saadaan myös kunnasta $\mathbb{Z}_p$ liittämällä siihen polynomin $p(x)$ juuri α. Nämä kunnat ovat keskenään isomorfisia. Kun taulut on saatu laskettua, voidaan kunnan alkiot korvata millä tahansa p^m erilaisella symbolilla taulujen pysyessä edelleen pareittain ortogonaaleina latinalaisina neliöinä.

Sisältö

Johdanto

Etsipä käsiisi korttipakka. Jos tavallista korttipakkaa ei löydy, esimerkiksi Uno-Ligretto- tai Skippo-kortitkin käyvät. Poimi pakasta neljä arvokkainta korttia jokaisesta maasta - tai neljä suurinta lukua kaikilla väreillä, jos kädessäsi on esimerkiksi Uno-kortit. Levitä nyt poimimasi yhteensä 16 korttia eteesi pöydälle ja yritä järjestää ne neljään riviin ja neljään sarakkeeseen niin, että muodostuu 4×4 -taulukko, jonka jokaisella rivillä ja jokaisella sarakkeella on yksi kortti kustakin maasta ja yksi kortti kutakin arvoa. Tai vastaavasti Uno-korteilla, järjestä kortit taulukkoon, jonka jokaisella rivilllä ja jokaisella sarakkeella sekä jokainen väri että jokainen luku on edustettuna täsmälleen kerran. Korttien järjestäminen tällä tavalla saattaa vaatia useita yrityksiä ja erehdyksiä, mutta on kyllä mahdollista monellakin eri tavalla.

Korttien järjestäminen pelkästään maiden perusteella niin, että jokainen maa on edustettuna jokaisella rivillä ja sarakkeella täsmälleen kerran, on melko helppoa. Samoin korttien järjestäminen pelkästään niiden arvon perusteella on helppoa. Tällainen yhden ominaisuuden perusteella järjestetty neliö on esimerkki 4. kertaluvun latinalaisesta neliöstä. Kummankin ominaisuuden, sekä maan että arvon, järjestäminen vaaditulla tavalla yhteen ja samaan neliötaulukkoon on vaikeampaa, mutta kun siinä onnistut, on sinulla edessäsi esimerkki kahdesta päällekäin asetetusta keskenään ortogonaalista (4. kertaluvun) latinalaisesta neliöstä. Kertaluvun k latinalainen neliö on siis taulukko, johon jonkin k alkion joukon S alkiot on järjestetty siten, että kukin alkio esiintyy taulukon jokaisella rivillä ja sarakkeella täsmälleen kerran. Kaksi saman kertaluvun latinalaista neliötä taas ovat keskenään ortogonaalit, jos ne päällekäin asetettuna muodostavat taulukon, jossa jokainen ensimmäisen neliön alkio esiintyy jokaisen toisen neliön alkion kanssa täsmälleen kerran. Poimimissasi pelikorteissa jokainen alkiopari (kortin maa ja arvo -yhdistelmä) esiintyy vain kerran, samanlaisia kortteja ei ole useita.

Jos sinulla on kaksi erilaista korttipakkaa, esimerkiksi sekä tavalliset pelikortit että Uno-kortit, voit yrittää muodostaa myös 5. kertaluvun keskenään ortogonaaleja latinalaisia neliöitä poimimalla pakoista vaikkapa luvut 1-5 kustakin maasta ja yhdestä väristä. Tai voit yrittää muodostaa vastaavanlaisia 6. kertaluvun neliöitä neljän maan ja kahden värin korteista. Viidennen kertaluvun neliön muodostaminen voi olla helpompaa kuin neljännen. Sen sijaan kuudennen kertaluvun neliön muodostamiseen ei aikaa kannata tuhlata. Edes Leonard Euler (1707-1783) ei onnistunut siinä ja myöhemmin onkin osoitettu tehtävän olevan mahdoton. Eulerin ongelma tosin oli muotoiltu toisella tavalla:

Valitaan kuudesta eri rykmentistä kuusi upseeria kuudella eri sotilasarvolla. Halutaan järjestää nämä yhteensä 36 upseeria paraatiin 6×6 -neliömuodostelmaan siten, että jokaisessa rivissä ja jokaisessa jonossa on edustettuna kaikki kuusi rykmenttiä ja

sotilasarvoa. Siis siten, että jokaisessa rivissä ja jokaisessa jonossa olisi yksi upseeri kutakin sotilasarvoa kustakin rykmentistä. Onko tämä mahdollista?

Euler yritti vuonna 1779 järjestää upseereita pyydetyllä tavalla, mutta ei onnistunut siinä, ja arvasi lopulta tehtävän olevan mahdoton. Itseasiassa Euler otaksui vastaavanlaisen neliön muodostamisen olevan mahdotonta kaikilla muotoa $2 + 4k$ ($k = 1, 2, 3, ...$), olevilla määrillä rykmenttejä ja sotilasarvoja. Hän muotoilikin siitä nk. Eulerin konjektuurin, jota ei kuitenkaan kyennyt todistamaan [**6**].

Eulerin 36 upseerin ongelma voidaan uudelleenmuotoilla seuraavasti: Onko olemassa kahta tai useampaa keskenään ortogonaalia 6. kertaluvun latinalaista neliötä? Tältä osin Eulerin otaksuma osui oikeaan. Ei ole. Tämän todisti G. Tarry vuonna 1900 käymällä läpi pitkällisen tapaustutkimuksen. Kuudennen kertaluvun latinalaisia neliöitä on yli 800, mutta yksikään niistä ei ole ortogonaali minkään toisen kanssa. [**4**], [**6**] Käytännössä tämä tarkoittaa sitä, että halutunlaisessa 36 upseerin neliömuodostelmassa osan upseereista pitäisi olla useassa paikassa yhtä aikaa samalla kun osalle upseereista ei löytyisi paraatista paikkaa ollenkaan.

Eulerin konjektuuri pätee kuitenkin vain luvulle kuusi. Vuonna 1959 Bose ja Shrikhande konstruoivat kaksi ortogonaalia 22. kertaluvun latinalaista neliötä ja pian he jo osoittivatkin Eulerin konjektuurin pätemättömyyden äärettömän monella sitä suuremmalla luvulla [**3**]. Samoihin aikoihin Parker osoitti vähintään kahden pareittain ortogonaalin latinalaisen neliöiden olemassaolon kaikille kertaluvuille $v = 1/2(3q-1)$, missä q on joku luvun 3 kanssa kongruentti alkulukupotenssi modulo 4. Esimerkiksi luku 10 on tätä muotoa. Yhdessä Bose, Shrikhande ja Parker sitten konstruoivat 10. kertaluvun Eulerin neliön ja todistivat, että n. kertaluvun pareittain ortogonaaleja latinalaisia neliöitä on vähintään kaksi kaikilla $n = 2 + 4k > 6$ [**3**], [**4**]. Niitä on kuitenkin aina enintään $n-1$, ja joillain kertaluvuilla täsmälleen $n-1$. Tässä tutkielmassa keskitytään juuri niiden $n-1$ pareittain ortogonaalin n. kertaluvun latinalaisen neliön olemassaoloon ja konstruointiin.

Käy ilmi, että äärellisten kuntien yhteenlaskutaulut ovat latinalaisia neliöitä. Jos $x_0 = 0, x_1 = 1, x_2, \ldots, x_n$ ovat kunnan F alkiot, on laskun $x_k x_i + x_j$ laskutaulu n. kertaluvun latinalainen neliö kaikilla $1 \leq k \leq n$. Selvästi siis n alkion kunnan F alkioista voidaan muodostaa $n-1$ n. kertaluvun latinalaista neliötä. Myöhemmin osoitetaan vielä, että ne ovat kaikki pareittain ortogonaaleja. Kun tiedetään, että äärellisessä kunnassa on aina p^m alkiota jollain alkuluvulla p ja luonnollisella luvulla m, tiedetään kertaluvun $q = p^m$ pareittain ortogonaalien latinalaisten neliöiden maksimilukumäärä. Laskutaulujen avulla nuo neliöt saadaan myös muodostettua, kunhan tiedetään mistä alkioista kyseinen kunta koostuu ja mitkä ovat sen laskutoimitukset.

Tässä kirjoitelmassa esitellään p^m alkion kunnan konstruointi kuntalaajennuksena kunnasta $\mathbb{Z}_p$. Sitä varten on jonkin verran perehdyttävä paitsi kunta-, myös rengasteoriaan, ja niinpä kirjoitelma alkaakin abstraktin algebran perusasioiden ja erityisesti renkaisiin liittyvien asioiden kertaamisella. Kuntalaajennusta varten muodostetaan ensin euklidinen polynomirengas $\mathbb{Z}_p[x]$. Sitten etsitään jokin m. asteen jaoton polynomi $p(x) \in \mathbb{Z}_p[x]$ ja muodostetaan tekijärengas $\mathbb{Z}_p[x]/p(x)$. Tämä rengas $\mathbb{Z}_p[x]/p(x)$ on itseasiassa kunta, jossa on täsmälleen p^m alkiota. Kunnan $\mathbb{Z}_p[x]/p(x)$ alkioista voidaan siis jo muodostaa keskenään ortogonaaleja latinalaisia neliöitä sen laskutaulujen avulla. Laskeminen on kuitenkin helpompaa kunnan $\mathbb{Z}_p(\alpha)$ avulla. Kunta $\mathbb{Z}_p(\alpha)$ saadaan

myös kunnasta $\mathbb{Z}_p$ liittämällä siihen polynomin $p(x)$ juuri α ja se on isomorfinen kunnan $\mathbb{Z}_p[x]/p(x)$ kanssa. Itseasiassa kaikki saman kertaluvun kunnat ovat keskenään isomorfisia, joten ei ole väliä missä kunnassa laskutauluja muodostaa. Kun taulut on saatu laskettua, voidaan kunnan alkiot korvata millä tahansa p^m erilaisella symbolilla taulujen pysyessä edelleen pareittain ortogonaaleina latinalaisina neliöinä.

Kahdesta keskenään ortogonaalista latinalaisesta neliöstä päällekäin asettamalla muodostetusta neliöstä käytetään yleisesti ainakin kahta erilaista nimeä; Eulerin neliö ja latinalais-kreikkalainen neliö. Eulerin neliö -nimi lienee Eulerin upseeri-ongelman innoittama. Latinalais-kreikkalainen neliö taas on saanut nimensä siitä, että ensimmäisen neliön alkiot on usein nimetty latinalaisin kirjaimin $A, B, C \ldots$ ja toisen neliön alkiot kreikkalaisin aakkosin $\alpha, \beta, \gamma \ldots$ Tässä kirjoitelmassa käytetään nimeä Eulerin neliö.

Eulerin neliöillä ja latinalaisilla neliöillä ylipäätään on useita hyödyllisiä sovelluksia. Niitä käytetään monien eri tieteenalojen tutkimuksissa koeasetelmien suunnittelussa. Jos halutaan tutkia vaikkapa, miten eri kesäkurpitsalajikkeet kasvavat erilaisissa kasvualustoissa, voi koejärjestely olla latinalainen neliö. Tässä kirjoitelmassa sovelluksista kuitenkin käsitellään tarkemmin vain yhtä hieman matemaattisempaa sovellusta; taikaneliötä. Kertaluvun n taikaneliö on $n \times n$-taulukko, jossa on luvut $1, 2, \ldots, n^2$ järjestettynä siten, että taulukon jokaisen rivin, sarakkeen ja diagonaalin summa on sama. Tällaisia taulukoita voidaan muodostaa sopivasti valittujen keskenään ortogonaalien latinalaisten neliöiden avulla. Taikaneliöihin ja siihen, millaiset latinalaiset neliöt niiden muodostamiseksi on valittava, palataan kirjoitelman lopussa.

Tutkielman teossa käytetystä kirjallisuudesta mainittakoon erityisesti päälähteen asemassa ollut W. J. Gilbertin kirja Modern Algebra with Applications [**7**]. Se on helppolukuinen ja avaa aihetta hyvin, vaikka ei käsittelekään kaikkia asioita kovin syvällisesti. Perusteellisemmin asioita todistetaan mm. M. Artinin ja S. Warnerin kirjoissa [**1**] ja [**9**]. Näistä Warnerin kirja on sujuvammin kirjoitettu ja siksi kevyempi lukea. Erityisesti Eulerin neliöiden ja taikaneliöiden konstruointia minulle avasi hyvin myös Alexander Bogomolnyn kirjoitus latinalaisista neliöistä Cut The Knot-sivustolla [**2**]. Eulerin ongelmasta ja Eulerin konjektuurin kumoamisesta taas voit lukea lisää esimerkiksi artikkeleista [**3**], [**4**] ja [**6**].

LUKU 1

Algebrallisia taustoja

1.1. Abstraktin algebran perusasioita

MÄÄRITELMÄ 1.1. Laskutoimituksella varustettu joukko $(G, *)$ on ryhmä, jos
i) laskutoimitus $*$ on assosiatiivinen
$(a * (b * c) = (a * b) * c \quad \forall a, b, c \in G)$.
ii) sillä on neutraalialkio $e \in G$
$(e * a = a = a * e \quad \forall a \in G)$
iii) ja jokaisella $g \in G$ on laskutoimituksen $*$ suhteen käänteisalkio $g^{-1} \in G$
$(g^{-1} * g = e = g * g^{-1})$.
Jos lisäksi laskutoimitus $*$ on kommutatiivinen ($a * b = b * a$ kaikilla $a, b \in G$), niin $(G, *)$ on Abelin ryhmä.

MÄÄRITELMÄ 1.2. Kahdella laskutoimituksella varustettu joukko $(R, *, \circ)$ on rengas, jos $(R, *)$ on Abelin ryhmä, ja jos
i) laskutoimitus $\circ$ on assosiatiivinen,
i) se on $*$:n suhteen distributiivinen
$(a \circ (b * c) = a \circ b * a \circ c$ ja $(b * c) \circ a = b \circ a * c \circ a$ kaikilla $a, b, c \in R)$
ii) ja sillä on neutraalialkio $I \in R$
$(I \circ a = a = a \circ I \quad \forall a \in R)$.
Jos lisäksi laskutoimitus $\circ$ on kommutatiivinen, niin R on kommutatiivinen rengas.

Kutsutaan jatkossa renkaan ensimmäistä laskutoimitusta (jota nyt on merkitty $*$) yhteenlaskuksi ja toista laskutoimitusta ($\circ$) kertolaskuksi, vaikka ne olisivat eri laskutoimituksia kuin perinteisesti yhteen- ja kertolaskuna pitämämme laskutoimitukset. Vastaavasti käytetään yhteenlaskun käänteisalkiosta termiä vasta-alkio ja merkitään sitä miinusmerkillä alkion edessä. Käytetään myös yhteenlaskun neutraalialkiolle merkintää 0 ja kertolaskun neutraalialkiolle merkintää 1. Alaindeksit kertovat tarvittaessa minkä ryhmän tai renkaan neutraalialkioista on kyse. Siis esimerkiksi Abelin ryhmässä jokaisella $g \in G$ on yhteenlaskun suhteen käänteis- eli vasta-alkio $-g \in G$, jolla $-g * g = 0_G = g * (-g)$.

Ryhmän $(G, +)$ epätyhjä osajoukko H on ryhmän G aliryhmä, jos se samalla laskutoimituksella $+$ varustettuna täyttää ryhmän ehdot eli on itsekin ryhmä $(H, +)$. Vastaavasti renkaan $(R, +, \cdot)$ alirengas $(S, +, \cdot)$ on sen epätyhjä osajoukko, joka kaikilla $a, b \in S$ toteuttaa ehdot i) $a - b \in S$, ii) $a \cdot b \in S$ ja iii) $1_R \in S$.

MÄÄRITELMÄ 1.3. Kommutatiivinen rengas $(F, *, \circ)$ on kunta, jos sen jokaisella nollasta eroavalla alkiolla $g \in F$ on kertolaskun $\circ$ suhteen käänteisalkio $g^{-1} \in F$.

Esimerkki 1.4. $(\mathbb{Z}, +)$ on Abelin ryhmä ja $(\mathbb{Z}, +, \cdot)$ on kommutatiivinen rengas, mutta ei kunta, sillä käänteisalkioita kertolaskun suhteen ei löydy kuin luvuille ± 1. Sen sijaan esimerkiksi $(\mathbb{Z}_5, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ ja $(\mathbb{R}, +, \cdot)$ ovat kuntia.

Jos $ab = 0$ joillain renkaan nollasta poikkeavilla alkioilla a ja b, niin sanotaan, että a ja b ovat nollanjakajia. Kommutatiivinen rengas, jossa ei ole nollanjakajia on kokonaisalue. Kunnassa ei ole nollanjakajia, joten kunta on aina kokonaisalue, mutta kaikki kokonaisalueet eivät ole kuntia. Äärellinen kokonaisalue kuitenkin on kunta [**7**, 172].

Määritelmä 1.5. Renkaan R epätyhjä osajoukko I on renkaan R ideaali, jos kaikilla $x, y \in I$ ja $r \in R$ pätee
i) $x - y \in I$ (eli $(I, +)$ on ryhmän $(R, +)$ aliryhmä) ja
ii) $x \cdot r, r \cdot x \in I$.

Lause 1.6. *Olkoon R kommutatiivinen rengas ja olkoon $a \in R$. Kaikkien alkion a monikertojen joukko*

$$(a) = \{ar : r \in R\}$$

on renkaan R ideaali. Kutsutaan sitä alkion a virittämäksi pääideaaliksi.

Todistus. Olkoot $ar, as \in (a)$ ja $t \in R$. Nyt $ar - as = a(r - s) \in (a)$ ja $(ar)t = a(rt) \in (a)$, joten (a) on renkaan R ideaali. □

Jos renkaan kaikki ideaalit ovat pääideaaleja, rengasta kutsutaan pääideaalirenkaaksi.

Olkoon nyt I jokin (kommutatiivisen) renkaan R ideaali. Jäännösluokkien joukko $R/I = \{I + r : r \in R\}$ varustettuna tekijälaskutoimituksilla

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

$$\text{ja} \quad (I + r_1)(I + r_2) = I + (r_1 r_2)$$

muodostaa (kommutatiivisen) renkaan $(R/I, +, \cdot)$ [**7**, 223–224]. Kutsutaan rengasta $(R/I, +, \cdot)$ tekijärenkaaksi.

Pääideaalirenkaasta R voidaan siis ottaa mikä tahansa alkio $a \in R$ ja muodostaa sen virittämän ideaalin (a) avulla tekijärengas $R/(a)$. Juuri näin on saatu aiemmin esimerkkinä käytetty rengas ja kunta

$$\mathbb{Z}_5 = \mathbb{Z}/(5) = \{(5) + k : k \in \mathbb{Z}\} = \{[0], [1], [2], [3], [4]\},$$

joka on siis ekvivalenssiluokkien joukko modulo 5.

1.2. Homomorfismeista

Laskutoimituksen säilyttävää kuvausta kutsutaan homomorfismiksi. Jos $(G, *)$ ja $(H, \circ)$ ovat ryhmiä, niin kuvausta $f : G \to H$ sanotaan ryhmähomomorfismiksi, jos $f(a * b) = f(a) \circ f(b)$ kaikilla $a, b \in G$. Jos ryhmähomomorfismi f on bijektio, sitä sanotaan ryhmäisomorfismiksi ja ryhmät G ja H ovat isomorfisia keskenään. Merkitään ryhmien isomorfisuutta $G \cong H$. Määritellään ryhmähomomorfismille nyt ydin ja kuva, tutustutaan pariin lemmaan ja todistetaan ryhmien isomorfismilause. Lemmojen todistukset löytyvät mm. Gilbertin kirjasta [**7**, 93–94].

MÄÄRITELMÄ 1.7. Ryhmähomomorfismin $f : G \to H$ ydin $\operatorname{Ker} f$ on niiden ryhmän G alkioiden joukko, jotka kuvautuvat ryhmän H neutraalialkioksi. Siis

$$\operatorname{Ker} f = \{g \in G : f(g) = 0_H\}.$$

LEMMA 1.8. *Olkoon $f : G \to H$ ryhmähomomorfismi. Tällöin*
i) $\operatorname{Ker} f$ *on ryhmän G normaali aliryhmä ja*
ii) kuvaus f on injektio jos ja vain jos $\operatorname{Ker} f = \{0_G\}$.

LEMMA 1.9. *Ryhmähomomorfismin $f : G \to H$ kuva* $\operatorname{Im} f = \{f(g) : g \in G\}$ *on ryhmän H aliryhmä (joskaan ei välttämättä normaali).*

LAUSE 1.10. *Olkoon K ryhmähomomorfismin $f : G \to H$ ydin. Tällöin tekijäryhmä G/K on isomorfinen kuvan* $\operatorname{Im} f$ *kanssa ja ryhmäisomorfismi näiden välille määritellään $\varphi : G/K \to \operatorname{Im} f$, $\varphi(K + g) = f(g)$.*

TODISTUS. Kuvaus φ määriteltiin nyt vain yhden edustajan avulla, joten on varmistettava, että se on hyvin määritelty, eikä ole väliä sillä, mitä luokan alkiota käytetään. Jos $K + g = K + g'$, niin $g \equiv g' \mod K$ ja niiden erotus $g' + (-g) = k \in K = \operatorname{Ker} f$. Siten

$$f(g') = f(k + g) = f(k) + f(g) = 0_H + f(g) = f(g)$$

ja φ on hyvin määritelty tekijäluokissa.

Funktio φ on homomorfismi, koska

$$\varphi(K+g_1+K+g_2) = \varphi(K+g_1+g_2) = f(g_1+g_2) = f(g_1)+f(g_2) = \varphi(K+g_1)+\varphi(K+g_2).$$

Jos $\varphi(K + g) = 0_H$, niin $f(g) = 0_H$ ja $g \in K$. Siis $\operatorname{Ker} \varphi = K$ (tekijäryhmän G/K neutraalialkio) ja lemman 1.6. nojalla φ on injektio. Kuvauksen φ määritelmästä seuraa, että $\operatorname{Im} \varphi = \operatorname{Im} f$, joten φ on myös surjektio. Siis φ on bijektiivinen homomorfismi ja $G/K \cong \operatorname{Im} f$. □

Määritellään sitten rengashomomorfismi ja tarkastellaan vastaavia tuloksia sille.

MÄÄRITELMÄ 1.11. Olkoot $(R, +, \cdot)$ ja $(S, *, \circ)$ renkaita. Funktio $f : R \to S$ on rengashomomorfismi, jos kaikille $a, b \in R$ pätee
i)$f(a + b) = f(a) * f(b)$
ii) $f(a \cdot b) = f(a) \circ f(b)$ ja
iii) $f(1_R) = 1_S$.

Esimerkiksi funktio $f : \mathbb{Z} \to \mathbb{Z}_5, f(x) = (5) + x = [x]$, joka kuvaa jokaisen kokonaisluvun sen ekvivalenssiluokaksi modulo 5, on rengashomomorfismi.

Jälleen bijektiivistä rengashomomorfismia kutsutaan rengasisomorfismiksi, ja renkaan R isomorfisuutta renkaan S kanssa merkitään $R \cong S$. Jos renkaat R ja S ovat kuntia, yllä määriteltyä kuvausta f voidaan kutsua myös kuntahomo-/isomorfismiksi. Tässä tutkielmassa termillä isomorfismi tarkoitetaan yleensä rengasisomorfismia.

Koska rengashomomorfismi $f : R \to S$ on erityisesti myös ryhmähomomorfismi $f : (R, +) \to (S, *)$, se kuvaa renkaan R yhteenlaskun neutraalialkion 0_R neutraalialkioksi 0_S renkaassa S. Lisäksi $f(-a) = -f(a)$, eli alkion a vasta-alkio kuvautuu sen kuvan $f(a)$ vasta-alkioksi. Rengashomomorfismin ydin määritelläänkin täsmälleen kuten ryhmähomomorfismin ydin:

MÄÄRITELMÄ 1.12. Rengashomomorfismin $f : R \to S$ ydin $\operatorname{Ker} f$ on niiden renkaan R alkioiden joukko, jotka kuvautuvat renkaan S neutraalialkioksi yhteenlaskun suhteen. Siis

$$\operatorname{Ker} f = \{g \in R : f(g) = 0_S\}.$$

Jo tutuksi tulleen rengashomomorfismin $f : \mathbb{Z} \to \mathbb{Z}_5, f(x) = [x]$ ydin on luvun 5 monikertojen joukko. Nyt siis $\operatorname{Ker} f = \{5n : n \in \mathbb{Z}\} = (5)$.

LAUSE 1.13. *Olkoon $f : R \to S$ rengashomomorfismi. Tällöin sen ydin* $\operatorname{Ker} f$ *on renkaan R ideaali.*

TODISTUS. Koska rengashomomorfismi on aina myös ryhmähomomorfismi, lemmasta 1.8 seuraa, että $\operatorname{Ker} f$ on ryhmän $(R, +)$ normaali aliryhmä. Kun lisäksi kaikilla $x \in \operatorname{Ker} f$ ja $r \in R$ pätee $f(xr) = f(x)f(r) = 0_S \cdot f(r) = 0_S$ eli $xr \in \operatorname{Ker} f$ ja vastaavasti $rx \in \operatorname{Ker} f$, niin $\operatorname{Ker} f$ on renkaan R ideaali. □

Jos R on pääideaalirengas, niin $\operatorname{Ker} f$ on pääideaali, ts. $\operatorname{Ker} f = (q)$ jollain $q \in R$. Toisaalta mikä tahansa renkaan R ideaali I on jonkin rengashomomorfismin ydin. Tämän osoittamiseksi käy esimerkiksi luonnollinen homomorfismi $g : R \to R/I$, $g(r) = I + r$. On myös helppo nähdä, että homomorfismin $f : R \to S$ kuva $\operatorname{Im} f$ on renkaan S alirengas.

LAUSE 1.14. *Olkoon $f : R \to S$ rengashomomorfismi. Tällöin $R/\operatorname{Ker} f \cong \operatorname{Im} f$.*

TODISTUS. Olkoon $K = \operatorname{Ker} f$. Ryhmien isomorfismilauseesta 1.10 seuraa, että kuvaus $\varphi : R/K \to \operatorname{Im} f$, $\varphi(K + r) = f(r)$ on ryhmähomomorfismi. Niinpä täytyy enää osoittaa, että φ on myös rengashomomorfismi ja sitä se on, sillä:

$$\varphi[(K + r)(K + s)] = \varphi(K + rs) = f(rs) = f(r)f(s) = \varphi(K + r)\varphi(K + s).$$

□

1.3. Renkaista

Missä tahansa kokonaisalueessa (siis kommutatiivisessa renkaassa, jossa ei ole nollanjakajia) D voidaan määritellä alkioiden jaollisuus kuten kokonaisluvuille on totuttu määrittelemään: Olkoot $a, b, q, \in D$. Jos $a = qb$, sanotaan että alkio b jakaa alkion a, tai että b on alkion a tekijä, ja merkitään sitä $b|a$.

Nyt kaikilla $a, b, c \in D$ pätee:
i) Jos $a|b$ ja $a|c$, niin $a|(b + c)$.
ii) Jos $a|b$, niin $a|br$ millä tahansa $r \in D$.
iii) Jos $a|b$ ja $b|c$, niin $a|c$.

Määritellään kokonaisalueen D alkioille myös suurin yhteinen tekijä:

MÄÄRITELMÄ 1.15. Olkoot $a, b \in D$. Alkio $g \in D$ on alkioiden a ja b suurin yhteinen tekijä $\operatorname{syt}(a, b)$, jos
i) $g|a$ ja $g|b$ ja jos
ii) siitä, että $c|a$ ja $c|b$ seuraa että $c|g$.

Toisin kuin alkeislukuteoriassa, tämä suurimman yhteisen tekijän määritelmä ei ole yksikäsitteinen. Kuten ei myöskään seuraavassa määritelmässä esiteltävä jakoyhtälö. Suurimman yhteisen tekijän monikäsitteisyyteen palataan myöhemmin lemmassa 1.23.

MÄÄRITELMÄ 1.16. Kokonaisalue R on euklidinen rengas, jos voidaan määritellä euklidinen funktio $d : R \to \{0, 1, 2, \dots\}$ siten että
(i) kun $a, b \in R$ ovat nollasta eroavia, $d(a) \leq d(ab)$ ja
(ii) kaikille $a, b \in R$, $b \neq 0$, löytyy alkiot $q, r \in R$ siten että $a = qb + r$, missä $r = 0$ tai $d(r) < d(b)$ (jakoyhtälö).

Esimerkiksi $\mathbb{Z}$ on euklidinen rengas, kun valitaan $d(a) = |a|$. Nyt esimerkiksi luvuille 5 ja 3 löytyy luvut 2, 1 ja -1 siten että $5 = 1 \cdot 3 + 2$, $d(2) = 2 < 3 = d(3)$, tai toisaalta $5 = 2 \cdot 3 - 1$ ja jälleen $d(-1) = 1 < 3 = d(3)$. Määritelmän 1.15 mukaan luvuilla 5 ja 3 on siis kaksi suurinta yhteistä tekijää, 1 ja -1.

Myös kaikki kunnat F ovat triviaalisti euklidisia renkaita, sillä voidaan valita $d(a) = 1$ kaikille nollasta poikkeaville kunnan alkioille a. Tällöin kaikilla $a, b \in F$ $d(a) = 1 \leq 1 = d(ab)$ ja $a = qb + r$, kun $q = ab^{-1} \in F$ ja $r = 0$.

Yksi merkittävä euklidinen rengas on F-kertoiminen polynomirengas $F[x]$, missä F on kunta. Sen lähempää tarkastelua varten määritellään kuitenkin ensin polynomirengas ja polynomin aste.

MÄÄRITELMÄ 1.17. Olkoon R kommutatiivinen rengas. Kaikkien R-kertoimisten polynomien joukkoa

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in R, n \in \mathbb{N}\}$$

varustettuna polynomilaskutoimituksilla

$$p(x) + q(x) = \sum_{i=0}^{\max(n,m)} (a_i + b_i)x^i \quad \text{ja}$$

$$p(x) \cdot q(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ missä } c_k = \sum_{i+j=k} a_i b_j,$$

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad \text{ja} \quad q(x) = \sum_{i=0}^{m} b_i x^i,$$

kutsutaan R-kertoimiseksi polynomirenkaaksi.

MÄÄRITELMÄ 1.18. Polynomin $p(x) = a_0 + a_1 x + \dots a_n x^n \in R[x]$ aste $\deg p(x)$ on suurin luonnollinen luku i, jolla $a_i \neq 0$. Samalla se on siis myös muuttujan x suurin eksponentti polynomissa $p(x)$.

Jos R on kokonaisalue, niin renkaan $R[x]$ polynomeille $p(x), q(x) \neq 0$

$$\deg(p(x) \cdot q(x)) = \deg p(x) + \deg q(x)$$

[**7**, 179]. Niinpä kuntakertoiminen polynomirengas $F[x]$ on euklidinen rengas, kun valitaan luvuksi $d(g(x))$ polynomin $g(x) \in F[x]$ aste $\deg g(x)$. Jakoyhtälön päteminen tälle polynomirenkaalle ei ole triviaalia, mutta se on todistettu algebran kurssilla ja todistus löytyy myös lähteestä [**7**, 195].

LAUSE 1.19. *Euklidisessa renkaassa R kaikilla alkioilla a ja b on suurin yhteinen tekijä $g \in R$. Lisäksi on olemassa alkiot $s, t \in R$, joilla $g = sa + tb$.*

TODISTUS. Jos a ja b ovat kumpikin nolla-alkioita, niiden suurin yhteinen tekijä on 0, koska mikä tahansa renkaan alkio jakaa nollan. Oletetaan nyt, että vähintään toinen alkioista on nollasta poikkeava. Olkoon

$$g \in I = \{i = xa + yb : x, y \in R\}$$

nollasta poikkeava alkio, jonka $d(g)$ on pienin arvoista $d(i)$. Kirjoitetaan $g = sa + tb$, $s, t \in R$.

Koska R on euklidinen rengas, niin $a = hg + r$, missä $r = 0$ tai $d(r) < d(g)$. Nyt

$$r = a - hg = a - h(sa + tb) = (1 - hs)a - htb \in I.$$

Koska $d(g)$ jo on pienin mahdollinen luvuista $d(i), i \in I \setminus \{0\}$, on oltava $r = 0$. Siten $g|a$. Vastaavasti $g|b$.

Jos $c|a$ ja $c|b$, siten että $a = kc$ ja $b = lc$, niin

$$g = sa + tb = skc + tlc = (sk + tl)c \quad \text{ja} \quad c|g.$$

Näin kaikki suurimman yhteisen tekijän määritelmän ehdot täyttyvät ja $g = syt(a, b)$. □

MÄÄRITELMÄ 1.20. Olkoon R kommutatiivinen rengas. Alkiota $u \in R$ kutsutaan yksiköksi, jos on olemassa alkio $v \in R$, jolla $uv = 1$.

Yksiköllä u on siis käänteisalkio kertalaskun suhteen renkaassa R ja kunta voitaisiin määritellä myös kommutatiivisena renkaana R, jonka jokainen nollasta eroava alkio on yksikkö.

LEMMA 1.21. *Jos $a|b$ ja $b|a$ kokonaisalueessa R, niin $a = ub$ jollain yksiköllä $u \in R$.*

TODISTUS. Koska $a|b$, $b = va$ jollain $v \in R$ ja koska $b|a$, $a = ub$ jollain $u \in R$. Siis $a = ub = uva$, mistä seuraa että $a(uv - 1) = 0$. Jos nyt $a = 0$, niin myös $b = 0$. Jos taas $a \neq 0$, niin $uv = 1$, sillä kokonaisalueessa R ei ole nollanjakajia. Siis u on yksikkö. □

MÄÄRITELMÄ 1.22. Olkoon R euklidinen rengas. Alkio $p \in R$ on renkaan jaoton alkio, jos $p = ab$ vain kun $a \in R$ tai $b \in R$ on yksikkö.

Kun polynomi $f(x)$ on jaollinen tai jaoton euklidisessa renkaassa $F[x]$, voidaan sanoa myös, että se on jaollinen tai vastaavasti jaoton kunnan F suhteen.

LEMMA 1.23. *Olkoon g_1 alkioiden a ja b suurin yhteinen tekijä euklidisessa renkaassa R. Nyt $g_2 \neq g_1$ on myös a:n ja b:n suurin yhteinen tekijä jos ja vain jos $g_2 = ug_1$ jollain yksiköllä $u \in R$.*

TODISTUS. Olkoon ensin $g_1 = \text{syt}(a, b)$ ja $g_2 = \text{syt}(a, b)$, $g_1 \neq g_2$. Suurimman yhteisen tekijän määritelmästä seuraa nyt, että $g_2|g_1$ ja toisaalta myös $g_1|g_2$. Lemman 1.21 nojalla $g_2 = ug_1$ jollain yksiköllä $u \in R$.

Oletetaan sitten, että $g_2 = ug_1$ jollain yksiköllä $u \in R$. Tällöin on siis olemassa alkio $v \in R$, jolla $uv = 1$. Kun kerrotaan yhtälö $g_2 = ug_1$ puolittain alkiolla v, saadaan $vg_2 = g_1$. Siis taas $g_1|g_2$ ja $g_2|g_1$ ja kun $g_1 = \text{syt}(a, b)$, niin nyt myös g_2 täyttää suurimman yhteisen tekijän määritelmän ehdot ja siten myös $g_2 = \text{syt}(a, b)$. □

LEMMA 1.24. *Olkoot R euklidinen rengas ja $a, b \in R$. Tällöin $d(a) = d(ab)$ jos ja vain jos b on yksikkö. Muutoin $d(a) < d(ab)$.*

TODISTUS. Jos b on yksikkö ja $bc = 1$, niin $d(a) \leq d(ab) \leq d(abc) = d(a)$. Siis $d(a) = d(ab)$. Jos taas b ei ole yksikkö, ab ei jaa lukua a ja $a = qab + r$, missä $d(r) < d(ab)$. Nyt $r = a(1 - qb)$, joten

$$d(a) \leq d(a(1 - qb)) = d(r).$$

Siis $d(a) < d(ab)$. □

LAUSE 1.25. *Euklidinen rengas on pääideaalirengas.*

TODISTUS. Olkoon I mikä tahansa euklidisen renkaan R ideaali. Jos $I = \{0\}$, niin $I = (0)$ on 0-alkion virittämä pääideaali. Jos taas I sisältää nollasta eroavia alkioita, olkoon b niistä jokin sellainen, jolla $d(b)$ on pienin mahdollinen. Olkoon a mikä tahansa muu ideaalin I alkio. Tällöin jakoyhtälön perusteella on olemassa $q, r \in R$, joilla

$$a = q \cdot b + r \text{ , missä } r = 0 \text{ tai } d(r) < d(b).$$

Nyt $a \in I$ ja $q \cdot b \in I$, joten myös $r = a - q \cdot b \in I$. Koska b valittiin niin, että $d(b)$ on pienin mahdollinen, on oltava $r = 0$. Siis $a = q \cdot b \in (b)$ kaikilla $a \in I$ ja siten $I \subseteq (b)$.

Toisaalta jokainen joukon (b) alkio on muotoa $q \cdot b$ jollain $q \in R$ ja $q \cdot b \in I$. Siis $I \supseteq (b)$ ja niinpä $I = (b)$. Siis kaikki renkaan R ideaalit ovat pääideaaleja ja R on pääideaalirengas. □

Aiemmin todettiin, että $\mathbb{Z}$ ja $F[x]$, missä F on kunta, ovat euklidisia renkaita. Nyt tiedetään siis, että ne ovat myös pääideaalirenkaita.

LAUSE 1.26. *Olkoon R euklidinen rengas ja $a \in R$. Tekijärengas $R/(a)$ on kunta jos ja vain jos a on jaoton.*

TODISTUS. Olkoon $a \in R$ jaoton ja olkoon $(a) + b$ tekijärenkaan $R/(a)$ joku nollasta eroava alkio. Nyt siis b ei ole a:n monikerta, ja koska a on jaoton, $syt(a, b) = 1$. Lauseen 1.19 nojalla on siis olemassa $s, t \in R$, joilla $sa + tb = 1$. Tällöin $tb = 1 - sa$ ja koska $sa \in (a)$, niin

$$[(a) + t] \cdot [(a) + b] = (a) + tb = (a) + 1 - sa = (a) + 1.$$

$(a) + 1$ on renkaan $R/(a)$ neutraalialkio kertolaskun suhteen, joten $(a) + t \in R/(a)$ on alkion $(a) + b$ käänteisalkio. Siis $R/(a)$ on kunta.

Lauseen oletuksen mukaan rengas R on euklidinen, joten sen kertolasku on kommutatiivinen. Oletetaan nyt, että $a \in R$ ei ole jaoton, vaan on olemassa $s, t \in R$, jotka eivät ole yksiköitä, mutta joilla $st = a$. Nyt lemman 1.24 nojalla $d(s) < d(st) = d(a)$ ja $d(t) < d(st) = d(a)$. Siten s ei ole jaollinen a:lla eli $s \notin (a)$. Vastaavasti $t \notin (a)$ ja näin sekä $(a) + s$ että $(a) + t$ ovat renkaan $R/(a)$ nollasta eroavia alkioita. Kuitenkin

$$[(a) + s] \cdot [(a) + t] = (a) + st = (a),$$

joka on renkaan $R/(a)$ nolla-alkio. Siis renkaassa $R/(a)$ on nollanjakajia eikä se voi olla kunta. □

LAUSE 1.27. *$\mathbb{Z}_n$ on kunta, jos ja vain jos n on alkuluku.*

TODISTUS. Tämä seuraa suoraan edellisestä lauseesta, sillä kaikki jaottomat kokonaisluvut ovat alkulukuja tai niiden vastalukuja.

□

LAUSE 1.28. *Olkoon F kunta. Tekijärengas $F[x]/(p(x))$ on kunta jos ja vain jos $p(x) \in F[x]$ on jaoton. Lisäksi renkaalla $F[x]/(p(x))$ on aina alirengas, joka on isomorfinen kunnan F kanssa.*

TODISTUS. Lauseen ensimmäinen väite seuraa nyt suoraan lauseesta 1.26. Olkoon $F' = \{(p(x)) + r : r \in F\}$. Selvästi F' on renkaan $F[x]/(p(x))$ alirengas. Sen isomorfisuuden kunnan F kanssa osoittamiseksi määritellään kuvaus

$$f : F \to F', f(r) = (p(x)) + r.$$

Nyt

$$f(r+s) = (p(x)) + r + s = (p(x)) + r + (p(x)) + s = f(r) + f(s),$$
$$f(rs) = (p(x)) + rs = [(p(x)) + r] \cdot [(p(x)) + s] = f(r) \cdot f(s)$$
$$\text{ja } f(1_F) = (p(x)) + 1_F = 1_{F'} \ ,$$

joten kuvaus on rengashomomorfismi. Se on myös injektio, sillä

$$f(r) = f(s) \Leftrightarrow (p(x)) + r = (p(x)) + s \Leftrightarrow r = s,$$

ja surjektio, sillä $\operatorname{Im} f = \{(p(x)) + r : r \in F\} = F'$. Näin siis kuvaus $f : F \to F'$ on isomorfismi ja väite pätee. □

Määritellään nyt kongruenssirelaatio

$$f(x) \equiv g(x) \mod (p(x)) \text{ jos ja vain jos } f(x) - g(x) \in (p(x)).$$

Renkaan $F[x]/(p(x))$ alkiot ovat siis tämän relaation ekvivalenssiluokkia. Jakoyhtälön perusteella $f(x)$ ja $g(x)$ voidaan kirjoittaa muotoon $f(x) = q(x)p(x) + r(x)$ ja $g(x) = s(x)p(x) + t(x)$, missä $r(x)$ ja $t(x)$ ovat joko nollapolynomeja tai niiden aste on pienempi kuin polynomin $p(x)$.

LEMMA 1.29. *Yllä olevin merkinnöin $f(x) \equiv g(x) \mod (p(x))$ jos ja vain jos jäännöspolynomit $r(x)$ ja $t(x)$ ovat samat.*

TODISTUS.

$$\begin{aligned} f(x) \equiv g(x) \mod (p(x)) &\Leftrightarrow f(x) - g(x) \in (p(x)) \\ &\Leftrightarrow p(x) | f(x) - g(x) \\ &\Leftrightarrow p(x) | [q(x) - s(x)]p(x) + r(x) - t(x) \\ &\Leftrightarrow p(x) | r(x) - t(x) \\ &\Leftrightarrow r(x) = t(x). \end{aligned}$$

□

LAUSE 1.30. *Olkoon F kunta ja olkoon $p(x)$ jokin renkaan $F[x]$ n. asteen polynomi. Tällöin tekijärenkaan $F[x]/(p(x))$ alkiot ovat yksikäsitteisesti muotoa*

$$(p(x)) + a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \ , \text{ missä } a_0, a_1, \ldots, a_{n-1} \in F.$$

TODISTUS. Olkoon $(p(x))+f(x)$ mikä tahansa renkaan $F[x]/(p(x))$ alkio ja olkoon $r(x)$ jäännöspolynomi, joka muodostuu, kun $f(x)$ jaetaan polynomilla $p(x)$. Edellisen lemman perusteella $(p(x))+f(x) = (p(x))+r(x)$. Alkio $(p(x))+r(x)$ taas on lauseen antamaa muotoa, sillä $r(x) = 0$ tai $\deg r(x) < \deg p(x)$.

Yksikäsitteisyyden osoittamiseksi oletetaan että $(p(x)) + r(x) = (p(x)) + t(x)$, missä $r(x)$ ja $t(x)$ ovat joko nollapolynomeja tai niiden aste on pienempi kuin n. Nyt siis $r(x) \equiv t(x) \mod (p(x))$ ja jälleen lemman 1.29 nojalla $r(x) = t(x)$. □

1.4. Lineaarialgebrasta

Otetaan esiin muutamia lineaarialgebran määritelmiä, jotka on hyvä muistaa kuntalaajennuksia käsiteltäessä. Lineaarialgebran ja -geometrian kurssilla määriteltiin yleinen reaalilukukertoiminen vektoriavaruus. Reaalilukujen tilalle voidaan kuitenkin laittaa mikä tahansa kunta W ja määritellä W-kertoiminen vektoriavaruus vastaavalla tavalla.

MÄÄRITELMÄ 1.31. Joukko V on W-kertoiminen lineaarinen vektoriavaruus eli lineaariavaruus, jos siinä on määritelty summaoperaatio $+$

$$V \times V \to V : (x, y) \mapsto x + y$$

ja kerto-operaatio $\cdot$

$$W \times V \to V : (\lambda, x) \mapsto \lambda \cdot x,$$

jotka kaikilla $x, y, z, \in V$ ja $\lambda, \mu \in W$ toteuttavat ehdot

i) $x + y = y + x$
ii) $x + (y + z) = (x + y) + z$
iii) joukossa V on nolla-alkio 0, jolle $x + 0 = x$ kaikilla x
iv) alkiolla x on vasta-alkio x', jolle $x + x' = 0$
v) $\lambda \cdot (\mu \cdot x) = (\lambda \cdot \mu) \cdot x$
vi) $1_W \cdot x = x = x \cdot 1_W$
vii) $(\lambda + \mu)x = \lambda x + \mu x$
viii) $\lambda(x + y) = \lambda x + \lambda y$.

Huomataan, että ehtojen i)-iv) täyttyessä $(V, +)$ on Abelin ryhmä.

Määritellään sitten W-kertoimisen lineaariavaruuden V äärellisen monen vektorin lineaarinen riippumattomuus:

MÄÄRITELMÄ 1.32. Lineaariavaruuden V vektorit $v_1, \ldots, v_n$, $v \geq 1$, ovat lineaarisesti riippumattomia, jos vektoreiden W-kertoiminen lineaariyhdistely

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0 \text{ , jos ja vain jos } \lambda_i = 0 \text{ kaikilla } i \in \{1, \ldots n\}.$$

Tällöin sanotaan että joukko $S = \{v_1, \ldots, v_n\}$ on lineaarisesti riippumaton.

Joukon $S = \{v_1, \ldots, v_n\} \subset V$ virittämän aliavaruuden

$$\langle S \rangle = \langle v_1, \ldots, v_n \rangle = \{\lambda_1 v_1 + \cdots + \lambda_n v_n : v_i \in S, \lambda_i \in W\}$$

jokaisen vektorin x esitys muodossa $x = \lambda_1 v_1 + \cdots + \lambda_n v_n$ joillain $\lambda_1, \ldots, \lambda_n \in W$ on yksikäsitteinen täsmälleen silloin kun S on lineaarisesti riippumaton. [**5**, 186]

Jos lineaarisesti riippumattoman joukon S virittämä W-kertoiminen aliavaruus $\langle S\rangle$ täyttää koko avaruuden V, eli jos $\langle S\rangle = V$, sanotaan että joukko S on lineaariavaruuden V kanta. Kannan S vektoreita sanotaan avaruuden V kantavektoreiksi. Jos avaruudella V on äärellinen kanta $S = \{v_1, \ldots, v_n\}$ ja toinenkin kanta $T = \{u_1, \ldots, u_p\}$, niin $n = p$ eli kummassakin kannassa on vektoreita yhtä monta. [**5**, 185] Lineaariavaruuden V kantavektoreiden lukumäärää kutsutaan avaruuden V dimensioksi ja sitä merkitään dim V. Kaikki nämä määritelmät ja tulokset löytyvät mm. Deanin kirjasta [**5**, 177-186].

Esimerkiksi kompleksilukujen joukko $\mathbb{C}$ on $\mathbb{R}$-kertoiminen vektoriavaruus, jonka kanta on joukko $\{1, i\}$ ja dimensio dim $\mathbb{C} = 2$. Reaalilukujen joukko $\mathbb{R}$ taas on ääretönulotteinen rationaalinen eli $\mathbb{Q}$-kertoiminen vektoriavaruus.

1.5. Kuntalaajennuksista

MÄÄRITELMÄ 1.33. Kunnan K alikunta on alirengas F, joka myös on kunta. Jos F on kunnan K alikunta, niin K on kunnan F kuntalaajennus.

Kuntalaajennusta voidaan tarkastella myös vektoriavaruutena.

LAUSE 1.34. *Olkoon K kunnan F kuntalaajennus. Tällöin K on F-kertoiminen vektoriavaruus.*

TODISTUS. Vektoriavaruuden määritelmän neljä ensimmäistä ehtoa toteutuvat, koska kunta K on Abelin ryhmä yhteenlaskun suhteen. Kuntalaajennus K sisältää tietysti alikuntansa F, joten kunnan K alkioita voidaan kertoa kunnan F alkioilla ja määritelmän kertolaskuoperaatio on hyvin määritelty. Tarkistetaan, että vektoriavaruuden määritelmän ehdot (v)-(viii) toteutuvat: Olkoot $\lambda, \mu \in F$ ja $k, l \in K$. Nyt

v) $\lambda \cdot (\mu \cdot k) = (\lambda \cdot \mu) \cdot k$, koska kunnassa kertolasku on assosiatiivinen

vi) kertolaskun neutraalialkio $1 \in F \subset K$, joten $1 \cdot k = k$ kaikilla $k \in K$

vii) $(\lambda + \mu)k = \lambda k + \mu k$ ja

viii) $\lambda(x+y) = \lambda x + \lambda y$, sillä kunnassa kertolasku on distributiivinen yhteenlaskun suhteen.

Siten K on F-kertoiminen vektoriavaruus ja kaikki sen alkiot voidaan yksikäsitteisesti ilmaista lineaarikombinaationa sen kanta-alkioiden avulla. □

MÄÄRITELMÄ 1.35. Kuntalaajennuksen aste $[K : F]$ on kunnan K dimensio F-kertoimisena vektoriavaruutena. Kuntalaajennus K on äärellinen, jos $[K : F]$ on äärellinen.

LAUSE 1.36. *Jos $p(x) \in F[x]$ on n. asteen jaoton polynomi, niin $K = F[x]/(p(x))$ on kunnan F kuntalaajennus ja sen aste $[K : F] = n$.*

TODISTUS. Lauseen 1.30 perusteella kunnan $K = F[x]/(p(x))$ alkiot ovat yksikäsitteisesti muotoa

$$(p(x)) + a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}, \text{ missä } a_0, \ldots, a_{n-1} \in F.$$

Siis $K = \{(p(x))a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} : a_i \in F\}$ ja vektoriavaruutena sen kanta on $\{1, x, x^2, \ldots, x^{n-1}\}$. Avaruuden K dimensio on sen kanta-alkioiden lukumäärä, tässä n, joten kuntalaajennuksen aste $[K : F] = n$. □

MÄÄRITELMÄ 1.37. Olkoot K kunnan F kuntalaajennus ja $a \in K$. Otetaan pienin kunnan K alikunta, joka sisältää sekä kunnan F että alkion a ja merkitään sitä $F(a)$. Sanotaan, että $F(a)$ on kunta, joka saadaan aikaan liittämällä alkio a kuntaan F.

Tällainen kunta on aina olemassa, sillä alikuntien leikkaus on aina myös alikunta ja $F(a)$ on kaikkien sellaisten kunnan K alikuntien leikkaus, jotka sisältävät sekä kunnan F että alkion a [**7**, 238]. Esimerkiksi pienin kunta, joka sisältää sekä reaaliluvut $\mathbb{R}$ että imaginaariyksikön i, on koko kompleksilukujen joukko, sillä siihen on kuuluttava kaikki alkiot, jotka ovat muotoa $a + ib$, missä $a, b \in \mathbb{R}$. Niinpä $\mathbb{R}(i) = \mathbb{C}$.

MÄÄRITELMÄ 1.38. Olkoon kunta K kunnan F laajennus. Alkio $k \in K$ on algebrallinen kunnan F suhteen, jos se on jonkin nollasta poikkeavan polynomin $p(x) \in F[x]$ juuri ts. $a_0 + a_1 k + \dots a_n k^n = 0$ jollain kertoimilla $a_i \in F$.

Äsken todettiin, että kompleksiluvut ovat reaalilukujen kuntalaajennus, joka saadaan aikaan liittämällä kuntaan $\mathbb{R}$ alkio i. Yllä olevan määritelmän mukaan alkio $i \in \mathbb{C}$ on algebrallinen reaalilukujen suhteen, sillä se on polynomin $x^2 + 1 \in \mathbb{R}[x]$ juuri. Koska 2. asteen polynomi $x^2 + 1$ on jaoton renkaassa $\mathbb{R}[x]$, on tekijärengas $\mathbb{R}[x]/(x^2 + 1) = \{a + bx : a, b \in \mathbb{R}\}$ kunta. Nyt on helppo uskoa että $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{R}(i) = \mathbb{C}$ ja itse asiassa seuraava lause todistaakin näin olevan.

LAUSE 1.39. *Olkoon α algebrallinen kunnan F suhteen ja olkoon $p(x) \in F[x]$ jokin sellainen jaoton n. asteen polynomi, jonka juuri α on. Tällöin*

$$F(\alpha) \cong F[x]/(p(x))$$

ja kunnan $F(\alpha)$ alkiot voidaan yksikäsitteisesti kirjoittaa muotoon

$$c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-1}\alpha^{n-1}, \text{ missä } c_i \in F.$$

TODISTUS. Määritellään rengashomomorfismi

$$f : F[x] \to F(\alpha) : f(q(x)) = q(\alpha).$$

Koska nyt F on kunta ja siten $F[x]$ on lauseen 1.25 nojalla pääideaalirengas, kuvauksen ydin $\operatorname{Ker} f$ on jokin renkaan $F[x]$ pääideaali. Siis $\operatorname{Ker} f = (r(x))$ jollain $r(x) \in F[x]$. Koska nyt $p(\alpha) = 0$, niin $p(x) \in \operatorname{Ker} f$ ja $r(x)|p(x)$. Koska $p(x)$ on jaoton, $p(x) = kr(x)$ jollain nollasta eroavalla $k \in F$. Siten $\operatorname{Ker} f = (r(x)) = (p(x))$.

Lauseen 1.14 nojalla $F[x]/(p(x)) \cong \operatorname{Im} f \subseteq F(\alpha)$. Koska $F[x]/(p(x))$ on kunta, niin nyt myös $\operatorname{Im} f$ on kunta ja siten kunnan $F(\alpha)$ alikunta. Nythän $f(x) = \alpha \in \operatorname{Im} f$ ja $f(p(x) + r) = r \in \operatorname{Im} f$ kaikilla $r \in F$ eli $\operatorname{Im} f$ sisältää sekä kunnan F että alkion α. Kuitenkin $F(\alpha)$ on määritelmänsä mukaan pienin nämä alkiot sisältävä kunta, joten $\operatorname{Im} f$ ei voi olla kuntaa $F(\alpha)$ pienempi, vaan on oltava $\operatorname{Im} f = F(\alpha)$. Siten $F[x]/(p(x)) \cong F(\alpha)$.

Kunnan $F(\alpha)$ alkioiden muodon yksikäsitteisyys taas seuraa ylläesitetystä isomorfismista ja tekijärenkaan $F[x]/(p(x))$ alkioiden yksikäsitteisyydestä (lause 1.30). □

SEURAUS 1.40. *Olkoon n. asteen polynomi $p(x) \in F[x]$ jaoton ja olkoon α sen juuri. Tällöin $[F(\alpha) : F] = n$.*

TODISTUS. Äsken todistettiin, että kunnan $F(\alpha)$ alkiot voidaan yksikäsitteisesti kirjoittaa muotoon $c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-1}\alpha^{n-1}$, missä $c_i \in F$. Siis $\{1, \alpha, \alpha^2, \dots \alpha^{n-1}\}$ muodostaa kunnan $F(\alpha)$ kannan, ja vektoriavaruutena sen dimensio on n. Siten $[F(\alpha) : F] = n$. □

LUKU 2

Äärellisistä kunnista

2.1. Alkioiden lukumäärä

Mille tahansa renkaalle R voidaan määritellä rengashomomorfismi $f : \mathbb{Z} \to R$:

$$f(n) = \begin{cases} 1 + 1 + \cdots + 1 & (n \text{ kpl}), \text{ jos } n > 0 \\ 0 & \text{jos } n = 0 \\ -1 - 1 - \cdots - 1 & (n \text{ kpl}), \text{ jos } n < 0. \end{cases} \tag{2.1}$$

Funktion f ydin on nyt siis renkaan $\mathbb{Z}$ jokin ideaali ja koska $\mathbb{Z}$ on pääideaalirengas, $\operatorname{Ker} f = (q)$ jollain $q \geq 0$.

MÄÄRITELMÄ 2.1. Renkaan R karakteri on yllämääritellyn homomorfismin f ytimen $\operatorname{Ker} f$ virittäjä $q \geq 0$.

LAUSE 2.2. *Renkaan R karakteri on pienin kokonaisluku $q > 0$, jolla $qa = 0$ kaikilla $a \in R$. Jos tällaista lukua q ei ole, karakteri on 0.*

TODISTUS. Olkoon $q > 0$ renkaan R karakteri. Siis $\operatorname{Ker} f = (q)$. Nyt $f(q) = q \cdot 1_R = 0_R$ ja tällöin myös $qa = q \cdot 1_R \cdot a = 0_R$ kaikilla $a \in R$. Olkoon nyt toinenkin kokonaisluku $p > 0$, jolla $pa = 0_R$ kaikilla $a \in R$. Tällöin erityisesti $p \cdot 1_R = 0$. Tämä taas tarkoittaa sitä, että $f(p) = 0_R$ eli että $p \in \operatorname{Ker} f = (q)$. Tällöin $p = sq$ jollain $s \in \mathbb{Z}$. Koska $\mathbb{Z}$ on euklidinen rengas, niin nyt $d(q) \leq d(sq) = d(p)$, ja koska luvut p ja q ovat positiivisia, $q \leq p$. □

LAUSE 2.3. *Kokonaisalueen karakteri on joko nolla tai alkuluku.*

TODISTUS. Olkoon q kokonaisalueen D karakteri. Määritellään rengashomomorfismi $f : \mathbb{Z} \to D$ kuten yllä kuvaus 2.1. Soveltamalla nyt renkaiden isomorfismilausetta nähdään, että

$$\operatorname{Im} f = f(\mathbb{Z}) \cong \mathbb{Z}/(q) = \begin{cases} \mathbb{Z}_q & \text{jos } q \neq 0 \\ \mathbb{Z} & \text{jos } q = 0. \end{cases}$$

Mutta koska $f(\mathbb{Z})$ on kokonaisalueen alirengas, siinä ei ole nollanjakajia. Jos $f(\mathbb{Z})$ on äärellinen, se on kunta ja lauseen 1.27 nojalla q on alkuluku. Muutoin $q = 0$. □

LAUSE 2.4. *Jos kunnalla F on alkulukukarakteri p, niin kunnalla F on alikunta, joka on isomorfinen kunnan $\mathbb{Z}_p$ kanssa.*

TODISTUS. Olkoon nyt p kunnan F karakteri. Kuten edellisessäkin lauseessa nähtiin, renkaiden isomorfismilauseen nojalla kunnalla F on alirengas $f(\mathbb{Z}) \cong \mathbb{Z}_p$. □

LAUSE 2.5. *Äärellisessä kunnassa F on aina p^m alkiota jollain alkuluvulla p ja luonnollisella luvulla m.*

TODISTUS. Koska F on äärellinen kunta, sen karakteri on joku alkuluku p ja sillä on $\mathbb{Z}_p$:n kanssa isomorfinen alikunta. Samastetaan tämä alikunta $\mathbb{Z}_p$:hen, jolloin F on $\mathbb{Z}_p$:n kuntalaajennus. Laajennuksen aste on äärellinen, koska F on äärellinen kunta. Olkoon $[F : \mathbb{Z}_p] = m$ ja olkoon $\{f_1, f_2, \dots f_m\}$ F:n kanta, niin että $F = \{a_1 f_1 + a_2 f_2 + \cdots + a_m f_m | a_i \in \mathbb{Z}_p\}$. Jokaiselle a_i:lle on nyt p eri vaihtoehtoa, joten F:ssä on p^m alkiota. □

Äärellisen kunnan alkioiden lukumäärään liittyy eräs tässä tutkielmassa hyvin olennainen tulos, lause 2.9. Tuon lauseen todistusta varten otetaan ensin pari aputulosta. Ensimmäistä niistä ei tässä todisteta, mutta sille löytyy helposti luettava todistus mm. Gilbertin kirjasta [**7**, 248].

LEMMA 2.6. *Olkoon K q alkion kunta. Tällöin multiplikatiivinen ryhmä $K^\times = K \setminus \{0\}$ on kertaluvun $q-1$ syklinen ryhmä.*

LEMMA 2.7. *Olkoon K q alkion kunta. Tällöin kunnan K alkiot ovat polynomin $x^q - x$ juuria ja polynomi $x^q - x$ voidaan jakaa lineaarisiin tekijöihin kunnassa K.*

TODISTUS. Multiplikatiivisen ryhmän $K^\times = K \setminus \{0\}$ kertaluku on nyt $q-1$ ja $a^{q-1} = 1$ kaikilla $a \in K^\times$. Niinpä myös $a^q = a$ eli $a^q - a = 0$, mikä tarkoittaa, että a on polynomin $x^q - x$ juuri kaikilla $a \in K^\times$. Koska myös 0 on polynomin $x^q - x$ juuri, on $a^q - a = 0$ kaikilla $a \in K$ ja polynomi $x^q - x$ voidaan jakaa lineaarisiin tekijöihin

$$x^q - x = \prod_{a \in K} (x - a).$$

□

LEMMA 2.8. *Olkoot $f(x)$ ja $g(x)$ F-kertoimisia polynomeja ja olkoon K kunnan F laajennus. Jos $f(x) \in F[x]$ on jaoton ja jos polynomeilla $f(x)$ ja $g(x)$ on yhteinen juuri kunnassa K, niin $f(x)$ jakaa polynomin $g(x)$.*

TODISTUS. Olkoot nyt $f(x) \in F[x]$ jaoton ja $\alpha \in K$ polynomien $p(x)$ ja $g(x)$ yhteinen juuri. Jakoyhtälön nojalla polynomit $p(x)$ ja $g(x)$ voidaan nyt polynomirenkaassa $K[x]$ kirjoittaa muotoon $f(x) = q(x)(x - \alpha)$ ja $g(x) = r(x)(x - \alpha)$ joillain $q(x), r(x) \in K[x]$. Siis $(x - \alpha) | f(x)$ ja $(x - \alpha) | g(x)$ ja näin ollen $\text{syt}(f(x), g(x)) \neq 1$ renkaassa $K[x]$. Polynomien suurin yhteinen tekijä on kuitenkin sama sekä renkaassa $K[x]$ että $F[x]$ [**1**, 507], joten $\text{syt}(f(x), g(x)) \neq 1$ myös renkaassa $F[x]$. Koska nyt $f(x)$ on oletuksen mukaan jaoton kunnan F suhteen, on oltava $\text{syt}(f(x), g(x)) = f(x)$. Siis $f(x) | g(x)$. □

LAUSE 2.9. *Kaikki äärelliset kunnat, joissa on $q = p^m$ alkiota, ovat keskenään isomorfisia.*

TODISTUS. Olkoot K ja K' q alkion kuntia ja olkoon α syklisen ryhmän $K^\times$ virittäjä. Siten K on saatu kuntalaajennuksena p alkion kunnasta F liittämällä siihen α. Siis $K = F(\alpha)$. Olkoon nyt $f(x) \in F[x]$ se m. asteen jaoton polynomi, jonka juuri α on. Tällöin $K \cong F[x]/(f(x))$. Nyt α on sekä polynomin $f(x)$ että polynomin $x^q - x$ juuri. Lisäksi, koska $f(x)$ on jaoton, se jakaa polynomin $x^q - x$. Tarkastellaan sitten kuntaa K'. Polynomi $x^q - x$ voidaan jakaa lineaarisiin tekijöihin myös kunnassa K', ja koska $f(x)$ edelleen jakaa polynomin $x^q - x$, niin polynomilla $f(x)$ on juuri $\alpha' \in K'$. Siten $K \cong F[x]/(f(x)) \cong F(\alpha')$. Koska nyt myös K' on q alkion kunta, $F(\alpha') = K'$ ja siten $K \cong K'$ eli K ja K' ovat keskenään isomorfiset. □

MÄÄRITELMÄ 2.10. Kutsutaan p^m alkion kuntaa kertaluvun p^m Galois'n kunnaksi Évariste Galois'n (1811-1832) mukaan ja merkitään sitä $\mathrm{GF}(p^m)$.

Koska siis kaikissa äärellisissä kunnissa on aina p^m alkiota jollain alkuluvulla p ja luonnollisella luvulla m, kaikki äärelliset kunnat ovat isomorfisia jonkin kunnan $\mathrm{GF}(p^m)$ kanssa.

2.2. Äärellisten kuntien konstruointi

Keinot minkä tahansa äärellisen kunnan konstruointiin on nyt kerätty. Kun p on alkuluku ja m mikä tahansa luonnollinen luku, voidaan muodostaa kunta, jossa on täsmälleen p^m alkiota.

Lähdetään liikkeelle p alkion kunnasta $\mathbb{Z}_p$. Muodostetaan polynomirengas $\mathbb{Z}_p[x]$, joka nyt on euklidinen, koska $\mathbb{Z}_p$ on kunta. Valitaan renkaasta $\mathbb{Z}_p[x]$ jokin m. asteen jaoton polynomi $q(x)$ ja muodostetaan sen virittämän ideaalin avulla tekijärengas $\mathbb{Z}_p[x]/(q(x)) = \{(q(x)) + a_0 + a_1x + \cdots + a_{m-1}x^{m-1} : a_i \in \mathbb{Z}_p\}$. Lauseen 1.36 nojalla tämä tekijärengas on kunnan $\mathbb{Z}_p$ kuntalaajennus ja lauseen 2.5 nojalla siinä on täsmälleen p^m alkiota. Toisaalta lauseen 1.39 mukaan $\mathbb{Z}_p[x]/(q(x))$ on isomorfinen kunnan $\mathbb{Z}_p(\alpha)$ kanssa, joka saadaan kuntalaajennuksena kunnasta $\mathbb{Z}_p$, kun liitetään siihen polynomin $q(x)$ juuri α.

Sitä, löytyykö renkaasta $\mathbb{Z}_p[x]$ varmasti jokin m. asteen jaoton polynomi, ei tässä tutkielmassa ole tarkasteltu, mutta sellaisen polynomin löytyminen on kyllä osoitettu mm. Simmonsin artikkelissa [**8**]. Kun $m \in \{2, 3\}$, niin jaottoman polynomin löytäminen on helppoa. Seuraavat lauseet antavat keinoja 2. tai 3. asteen jaottoman polynomin etsimiseen.

LAUSE 2.11. *Olkoon $p(x) \in \mathbb{Z}_p[x]$. Jos $m = \deg p(x) \in \{2, 3\}$, niin $p(x)$ on jaoton, jos ja vain jos sillä ei ole juuria.*

TODISTUS. Jos polynomilla $p(x)$ olisi juuri $\alpha \in \mathbb{Z}_p([x])$, niin sillä olisi tekijä $(x-\alpha)$ eli se olisi jaollinen. Vastaavasti, jos $p(x)$ olisi jaollinen, niin, koska $\deg p(x) \leq 3$, sillä olisi vähintään yksi 1. asteen tekijäpolynomi $(x - \beta)$ jollain $\beta \in \mathbb{Z}_p([x])$, mikä taas tarkoittaa sitä, että sillä olisi juuri. □

LAUSE 2.12. *Jos alkuluku $p \equiv 3 \mod 4$, niin polynomi $x^2 + 1 \in \mathbb{Z}_p[x]$ on jaoton.*

TODISTUS. Jos $x^2 + 1$ olisi jaollinen, sillä olisi juuri $\alpha \in \mathbb{Z}_p$, jolloin siis $\alpha^2 + 1 = 0$ eli $\alpha^2 = -1$. Selvästikin nyt $\alpha \neq \pm 1$. Kuitenkin nyt $\alpha^4 = 1$, mikä tarkoittaa sitä, että juuren α kertaluku $\operatorname{ord} \alpha = 4$ multiplikatiivisessa ryhmässä $\mathbb{Z}_p^\times$. Lagrangen lauseen [**9**, 239] mukaan $\operatorname{ord} \alpha$ jakaa ryhmän kertaluvun $\#\mathbb{Z}_p^\times = p - 1 \equiv 2 \mod 4$. Nyt näin ei kuitenkaan ole, joten alkuperäinen väite pätee. □

ESIMERKKI 2.13. Halutaan muodostaa neljän alkion kunta $\mathrm{GF}(2^2)$. On siis laajennettava kunta $\mathbb{Z}_2 = \{0, 1\}$ polynomirenkaan $\mathbb{Z}_2[x]$ tekijärenkaaksi $\mathbb{Z}_2[x]/(p(x))$, missä $p(x)$ on jokin renkaan $\mathbb{Z}_2[x]$ jaoton polynomi. Tähän käy esimerkiksi polynomi $x^2 + x + 1$, sillä sillä ei ole juuria kunnassa $\mathbb{Z}_2$. Nyt tekijärengas

$$\mathbb{Z}_2[x]/(p(x)) = \{(p(x)) + 0, (p(x)) + 1, (p(x)) + x, (p(x)) + x + 1\}$$

on neljän alkion kunta $\mathrm{GF}(4)$. Tekijäluokkien edustajien avulla voidaan siitä käyttää myös lyhyempää merkintää $\mathrm{GF}(4) = \{0, 1, x, x+1\}$, mutta merkinnän tausta on syytä muistaa kunnan alkioilla laskettaessa.

Neljän alkion kunta voidaan muodostaa myös liittämällä kuntaan $\mathbb{Z}_2$ polynomin $x^2 + x + 1$ juuret α ja $\alpha^2 = \alpha + 1$, jolloin lauseen 1.39 nojalla

$$\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha^2\} \cong \{0, 1, x, x + 1\} = \mathrm{GF}(4).$$

LUKU 3

Ortogonaalit latinalaiset neliöt

3.1. Latinalaiset neliöt

MÄÄRITELMÄ 3.1. Olkoot n ja m luonnollisia lukuja. Tällöin nm alkiota a_{ij} järjestettynä n riviin ja m sarakkeeseen muodostavat $n \times m$-taulukon. Alaindeksit i ja j, $1 \leq i \leq n$, $1 \leq j \leq m$, ilmaisevat kunkin alkion paikan taulukossa.

Taulukko on siis matriisin kaltainen järjestys, jolle ei kuitenkaan määritellä laskutoimituksia ja jota ei operoida kuten matriisia.

MÄÄRITELMÄ 3.2. Olkoon S n alkion joukko. Joukkoon S perustuva kertalukua n oleva latinalainen neliö on $n \times n$ -taulukko, jossa jokainen joukon S alkio esiintyy taulukon jokaisella rivillä ja jokaisella sarakkeella täsmälleen kerran.

Latinalaisen neliön jokainen rivi ja jokainen sarake on siis jokin joukon S alkioiden permutaatio.

ESIMERKKI 3.3.

$$\begin{array}{|ccc|} \hline a & b & c \\ c & a & b \\ b & c & a \\ \hline \end{array} \quad \text{ja} \quad \begin{array}{|ccc|} \hline a & b & c \\ b & c & a \\ c & a & b \\ \hline \end{array}$$

ovat joukkoon $\{a, b, c\}$ perustuvia kolmannen kertaluvun latinalaisia neliöitä.

LAUSE 3.4. *Minkä tahansa äärellisen ryhmän $(G, +)$ yhteenlaskutaulu on G:hen perustuva latinalainen neliö.*

TODISTUS. Olkoot $x_1, x_2, \ldots, x_n$ ryhmän G alkiot. Jos taulun jollain rivillä joku G:n alkio esiintyisi kahdesti, niin olisi $x_i + x_j = x_i + x_k$ joillain $x_i, x_j, x_k \in G$. Koska G on ryhmä, alkiolla x_i on käänteisalkio $(-x_i)$, jolla $(-x_i) + x_i = 0$. Lisäämällä tämä käänteisalkio yhtälöön puolittain saadaan $(-x_i) + (x_i + x_j) = (-x_i) + (x_i + x_k)$, josta laskutoimituksen assosiatiivisuuden perusteella seuraa $x_j = x_k$. Siten mikään G:n alkio ei voi esiintyä samalla rivillä useampaan kertaan. Vastaavasti voidaan todistaa, että kukin alkio esiintyy jokaisella sarakkeella täsmälleen kerran. Niinpä laskutaulu on latinalainen neliö. □

Luonnollisesti tulos pätee myös äärellisten kuntien $(F, +, \cdot)$ yhteenlaskutauluille. Äärellisen kunnan alkioista voidaan latinalaisia neliöitä muodostaa toisellakin tavalla.

LAUSE 3.5. *Olkoon $(F, +, \cdot)$ n alkion kunta. Valitaan joku alkio $x_k \in F$, $1 \leq k \leq n-1$, $x_k \neq 0$. Tällöin laskun $x_k x_i + x_j$, (missä $x_i, x_j \in F$), $0 \leq i, j \leq n-1$, laskutaulu on latinalainen neliö.*

TODISTUS. Rivin i kahden alkion erotus on $(x_k x_i + x_j) - (x_k x_i + x_q) = x_j - x_q \neq 0$, kun $j \neq q$. Siis taulun jokainen rivi on joukon F permutaatio. Sarakkeen j kahden

alkion erotus on $(x_k x_i + x_j) - (x_k x_r + x_j) = x_k(x_i - x_r) \neq 0$, kun $i \neq r$, sillä kunnassa ei ole nollanjakajia. Siten myös jokainen taulun sarake on joukon F permutaatio ja F:n jokainen alkio esiintyy jokaisella taulun rivillä ja sarakkeella täsmälleen kerran. □

3.2. Ortogonaalit latinalaiset neliöt

MÄÄRITELMÄ 3.6. Kaksi n. kertaluvun latinalaista neliötä ovat ortogonaaleja, jos ne päällekäin asetettuna muodostavat neliön, jossa jokainen ensimmäisen neliön alkio esiintyy (järjestys huomioonottaen) jokaisen toisen neliön alkion kanssa täsmälleen kerran.

ESIMERKKI 3.7. Ensimmäisen esimerkin latinalaiset neliöt

$$\begin{array}{|ccc|}\hline a & b & c \\ c & a & b \\ b & c & a \\ \hline\end{array} \quad \text{ja} \quad \begin{array}{|ccc|}\hline a & b & c \\ b & c & a \\ c & a & b \\ \hline\end{array}$$

ovat ortogonaaleja, sillä päällekäin asetettuna ne muodostavat neliön

$$\begin{array}{|ccc|}\hline aa & bb & cc \\ cb & ac & ba \\ bc & ca & ab \\ \hline\end{array},$$

jossa mikään kirjainpari ei esiinny kahta kertaa.

ESIMERKKI 3.8. Sen sijaan latinalaiset neliöt

$$\begin{array}{|ccc|}\hline a & b & c \\ c & a & b \\ b & c & a \\ \hline\end{array} \quad \text{ja} \quad \begin{array}{|ccc|}\hline a & c & b \\ b & a & c \\ c & b & a \\ \hline\end{array}$$

eivät ole ortogonaaleja keskenään, sillä niiden päällekäin asetettuna muodostama neliö koostuu vain kolmesta toistuvasta kirjainparista.

$$\begin{array}{|ccc|}\hline aa & bc & cb \\ cb & aa & bc \\ bc & cb & aa \\ \hline\end{array}$$

MÄÄRITELMÄ 3.9. Jos $L_1, \ldots, L_r$ ovat n. kertaluvun latinalaisia neliöitä ja jos L_i on ortogonaali L_j:n kanssa kaikilla $i \neq j$, $i, j \in \{1, \ldots, r\}$, niin $\{L_1, \ldots, L_r\}$ on n. kertaluvun pareittain ortogonaalien latinalaisten neliöiden joukko. Merkitään tällaisen joukon alkioiden maksimilukumäärää $N(n)$.

Pareittain ortogonaalien n. kertaluvun latinalaisten neliöiden joukkoja voi siis olla useita, mutta niissä on kussakin enintään $N(n)$ alkiota.

ESIMERKKI 3.10. Kolmannen kertaluvun pareittain ortogonaalien latinalaisten neliöiden joukoissa on aina enintään kaksi neliötä eli $N(3) = 2$. Esimerkin 3.3 neliöt muodostavat pareittain ortogonaalien latinalaisten neliöiden joukon

$$\left\{ \begin{array}{|ccc|}\hline a & b & c \\ c & a & b \\ b & c & a \\ \hline\end{array}, \begin{array}{|ccc|}\hline a & b & c \\ b & c & a \\ c & a & b \\ \hline\end{array} \right\}.$$

Samoin neliöt

$$\boxed{\begin{matrix} a & b & c \\ b & c & a \\ c & a & b \end{matrix}} \quad \text{ja} \quad \boxed{\begin{matrix} a & c & b \\ b & a & c \\ c & b & a \end{matrix}}$$

muodostavat toisen 3. kertaluvun pareittain ortogonaalien latinalaisten neliöiden joukon, mutta siinäkin on vain kaksi alkiota.

LAUSE 3.11. *Kertaluvun n pareittain ortogonaalien latinalaisten neliöiden joukossa on aina enintään $n-1$ alkiota eli $N(n) \leq n-1$.*

TODISTUS. Olkoot $L_1, L_2, \ldots L_r$ n. kertaluvun pareittain ortogonaaleja latinalaisia neliöitä. Neliön L_i alkioiden uudelleen nimeäminen ei vaikuta neliön ortogonaalisuuteen minkään neliön L_j kanssa $(1 \leq i, j \leq r)$, joten voimme kirjoittaa kaikki neliöt uudelleen niin, että neliön ylin rivi on aina $1, 2, \ldots n$.

$$L_1 = \boxed{\begin{matrix} 1 & 2 & \ldots & n \\ x_1 & - & \ldots & - \\ \vdots & \vdots & & \vdots \\ - & - & \ldots & - \end{matrix}}, \; L_2 = \boxed{\begin{matrix} 1 & 2 & \ldots & n \\ x_2 & - & \ldots & - \\ \vdots & \vdots & & \vdots \\ - & - & \ldots & - \end{matrix}}, \; \ldots, \; L_r = \boxed{\begin{matrix} 1 & 2 & \ldots & n \\ x_r & - & \ldots & - \\ \vdots & \vdots & & \vdots \\ - & - & \ldots & - \end{matrix}}$$

Nyt neliöiden toisen rivin ensimmäisen sarakkeen alkioista $x_1, x_2, \ldots, x_r$ mikään ei voi olla 1, koska luku 1 on jo ensimmäisellä sarakkeella ensimmäisellä rivillä. Koska ensimmäisen rivin alkiot ovat jo kaikissa neliöissä samat, on myös oltava $x_i \neq x_j$ kaikilla $i \neq j$, mutta toisistaan eroavia alkioita on jäljellä enää $n-1$ kappaletta. Siten $r \leq n-1$.

□

LAUSE 3.12. *Kunnan $(F, +, \cdot)$ n alkiosta muodostetut latinalaiset neliöt $L_k = a_{ij}^k$, missä $a_{ij}^k = x_k x_i + x_j$,$x_k \neq 0$, $1 \leq k \leq n-1$ ja $0 \leq i, j \leq n-1$, muodostavat n. kertaluvun pareittain ortogonaalien latinalaisten neliöiden joukon $\{L_1, \ldots, L_{n-1}\}$.*

TODISTUS. Lauseessa 3.5 jo osoitettiin, että näin muodostetut neliöt ovat latinalaisia neliöitä. Nyt on siis vielä todistettava, että L_k ja L_l ovat keskenään ortogonaaleja kaikilla $k \neq l$. Oletetaan, että kun neliöt L_k ja L_l asetetaan päällekkäin, muodostuu kaksi samaa alkioparia paikoille (i, j) ja (r, q). Siis $(a_{ij}^k, a_{ij}^l) = (a_{rq}^k, a_{rq}^l)$. Nyt $a_{ij}^k = a_{rq}^k$ ja $a_{ij}^l = a_{rq}^l$ eli

$$\begin{aligned} & x_k \cdot x_i + x_j = x_k \cdot x_r + x_q \\ \text{ja} \quad & x_l \cdot x_i + x_j = x_l \cdot x_r + x_q. \end{aligned}$$

Vähentämällä ylempi yhtälö alemmasta saadaan $(x_k - x_l)x_i = (x_k - x_l)x_r$, josta edelleen $(x_k - x_l)(x_i - x_r) = 0$. Koska kunnassa ei ole nollanjakajia, on oltava $x_k - x_l = 0$ tai $x_i - x_r = 0$ eli $x_k = x_l$ tai $x_i = x_r$. Siis joko $k = l$ tai $i = r$. Nyt oletuksena on, että $k \neq l$. Jos olisi $i = r$, niin olisi $a_{ij}^k = a_{iq}^k$ eli neliön L_k rivillä i joku alkio esiintyisi kahteen kertaan. Tämä ei kuitenkaan ole mahdollista, sillä L_k on latinalainen neliö.

Siten mikään päällekkäin asetettujen neliöiden L_k ja L_l muodostamista lukupareista ei esiinny neliössä useampaan kertaan, vaan jokainen L_k:n alkio esiintyy jokaisen L_l:n alkion kanssa täsmälleen kerran ja neliöt L_k ja L_l ovat ortogonaaleja keskenään. □

Lauseen 3.11 mukaan $N(n) \leq n-1$ kaikilla $n \in \mathbb{N}$. Toisaalta on helppo nähdä, että kaikille $n = p^m$ pareittain ortogonaaleja latinalaisia neliöitä löytyy vähintään $n-1$. Näitä ovat juurikin edellisen lauseen antamat neliöt $L_1, \ldots, L_{n-1}$. Siispä $N(p^m) = p^m - 1$, mutta muille kertaluvuille pareittain ortogonaalien latinalaisten neliöiden lukumäärää on vaikeampi määrittää. Bose, Shrinkhande ja Parker osoittivat, että $N(n) \geq 2$ kaikilla $n > 6$ ja tiedetään, että esimerkiksi $N(10) \geq 2$, $N(14) \geq 3$ ja $N(18) \geq 3$. Näidenkin kertalukujen ortogonaaleja latinalaisia neliöitä etsitään yhä lisää ja tulevaisuudessa lukumäärät voivatkin tarkentua. [**4**]

Esimerkki 3.13. Koska $\mathbb{Z}_5$ on kunta, sen alkioista voidaan nyt helposti muodostaa neljä pareittain ortogonaalia 5. kertaluvun latinalaista neliötä L_1, L_2, L_3 ja L_4. Nyt $x_0 = 0, x_1 = 1, x_2 = 2, x_3 = 3$ ja $x_4 = 4$, joten esimerkiksi taulussa L_3 $a_{ij}^3 = 3x_i + x_j$ ja taulussa L_4 $a_{ij}^4 = 4x_i + x_j$. Taulut näyttävät tältä:

$$L_3 = \begin{array}{|ccccc|}\hline 0&1&2&3&4\\ 3&4&0&1&2\\ 1&2&3&4&0\\ 4&0&1&2&3\\ 2&3&4&0&1\\ \hline\end{array} \quad L_4 = \begin{array}{|ccccc|}\hline 0&1&2&3&4\\ 4&0&1&2&3\\ 3&4&0&1&2\\ 2&3&4&0&1\\ 1&2&3&4&0\\ \hline\end{array}\,.$$

Päällekäin asetettuna ne muodostavat neliön

$$\begin{array}{|ccccc|}\hline 00&11&22&33&44\\ 34&40&01&12&23\\ 13&24&30&41&02\\ 42&03&14&20&31\\ 21&32&43&04&10\\ \hline\end{array}\,.$$

Näitä kuntaan $\mathbb{Z}_5$ perustuvia 5. kertaluvun latinalaisia neliöitä voidaan nyt käyttää hyväksi muodostettaessa ortogonaaleja latinalaisia mistä tahansa viiden alkion joukosta. Alkiot $x_0, \ldots, x_4$ voidaan uudelleennimetä eli lukujen $1, \ldots, 5$ paikalle voidaan sijoittaa mitkä tahansa viisi erilaista symbolia ja neliöt pysyvät latinalaisina neliöinä ja niiden ortogonaalisuus säilyy.

Kun halutaan muodostaa ortogonaaleja latinalaisia neliöitä vaikkapa neljän tai kahdeksan alkion joukosta, on tekemistä hieman enemmän. Lauseen 1.27 mukaan $\mathbb{Z}_4$ ja $\mathbb{Z}_8$ eivät ole kuntia, joten ennen latinalaisten neliöiden muodostamista yllä esitellyllä tavalla on muodostettava neljän tai vastaavasti kahdeksan alkion kunta. Neljän alkion Galois'n kunta $\mathrm{GF}(4) = \{0, 1, x, x+1\}$ konstruoitiinkin jo esimerkissä 2.13.

3.3. Eulerin neliöiden konstruointi äärellisten kuntien avulla

Muodostetaan nyt kuntaan $\mathrm{GF}(4)$ perustuvat pareittain ortogonaalit 4. kertaluvun latinalaiset neliöt L_1, L_2 ja L_3. Merkitään $x_0 = 0, x_1 = 1, x_2 = x$ ja $x_3 = x+1$ ja lasketaan ensin neliön L_1 alkiot $a_{ij} = x_1 x_i + x_j = x_i + x_j$. Muistetaan, että laskutoimitukset on tehtävä kunnassa $\mathbb{Z}_2[x]/(x^2 + x + 1)$, vaikka merkinnöissä käytetäänkin edustajia tekijäluokkien esittämiseen. Näin ensimmäiseksi neliöksi saadaan:

$$L_1 = \begin{array}{|cccc|}\hline 0 & 1 & x & x+1 \\ 1 & 0 & x+1 & x \\ x & x+1 & 0 & 1 \\ x+1 & x & 1 & 0 \\ \hline\end{array}\,.$$

Neliöiden L_2 ja L_3 alkiot taas saadaan laskemalla $a_{ij}^2 = x_2 x_i + x_j = x \cdot x_i + x_j$ ja vastaavasti $a_{ij}^3 = x_3 x_i + x_j = (x+1)x_i + x_j$:

$$L_2 = \begin{array}{|cccc|}\hline 0 & 1 & x & x+1 \\ x & x+1 & 0 & 1 \\ x^2 & x^2+1 & x^2+x & x^2+x+1 \\ x^2+x & x^2+x+1 & x^2 & x^2+1 \\ \hline\end{array}\,,$$

$$L_3 = \begin{array}{|cccc|}\hline 0 & 1 & x & x+1 \\ x+1 & x & 1 & 0 \\ x^2+x & x^2+x+1 & x^2 & x^2+1 \\ x^2+1 & x^2 & x^2+x+1 & x^2+x \\ \hline\end{array}\,.$$

Neliöt L_2 ja L_3 näyttävät nyt aika hankalilta, mutta se on silkkaa silmänlumetta. Muistetaan, että kunta GF(4) on isomorfinen kunnan $\mathbb{Z}_2(\alpha)$ kanssa, kun α on polynomin $x^2 + x + 1$ juuri. Siis $\alpha^2 + \alpha + 1 = 0$, mistä seuraa myös, että $\alpha + 1 = \alpha^2$, $\alpha^2 + \alpha = 1$ ja $\alpha^2 + 1 = \alpha$. Sijoittamalla nyt α muuttujan x paikalle saadaan neliöt L_1, L_2 ja L_3 sievennettyä näin:

$$L_1 = \begin{array}{|cccc|}\hline 0 & 1 & \alpha & \alpha^2 \\ 1 & 0 & \alpha^2 & \alpha \\ \alpha & \alpha^2 & 0 & 1 \\ \alpha^2 & \alpha & 1 & 0 \\ \hline\end{array}\,,\; L_2 = \begin{array}{|cccc|}\hline 0 & 1 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & 0 & 1 \\ \alpha^2 & \alpha & 1 & 0 \\ 1 & 0 & \alpha^2 & \alpha \\ \hline\end{array}\,,\; L_3 = \begin{array}{|cccc|}\hline 0 & 1 & \alpha & \alpha^2 \\ \alpha^2 & \alpha & 1 & 0 \\ 1 & 0 & \alpha^2 & \alpha \\ \alpha & \alpha^2 & 0 & 1 \\ \hline\end{array}\,.$$

Nyt neliöt ovat kauniit ja käytännölliset. Päällekäin asettamalla niistä saadaan Eulerin neliöitä ja esimerkiksi alussa esitetty pelikorttiongelma voidaan ratkaista vaikkapa asettamalla kortit seuraavasti:

$$\begin{array}{|cccc|}\hline \clubsuit A & \diamondsuit K & \heartsuit Q & \spadesuit J \\ \heartsuit J & \spadesuit Q & \clubsuit K & \diamondsuit A \\ \spadesuit K & \heartsuit A & \diamondsuit J & \clubsuit Q \\ \diamondsuit Q & \clubsuit J & \spadesuit A & \heartsuit K \\ \hline\end{array}\,.$$

Vastaavasti kahdeksan alkion kunta $\mathrm{GF}(8) = \mathrm{GF}(2^3)$ saadaan polynomilaajennuksena kunnasta $\mathbb{Z}_2$ muodostamalla tekijärengas $\mathbb{Z}_2[x]/q(x)$, missä $q(x) \in \mathbb{Z}_2[x]$ on joku 3. asteen jaoton polynomi. Voidaan valita esimerkiksi $q(x) = x^3 + x + 1$. Kahdeksan alkion kunta voidaan myös muodostaa lisäämällä kuntaan $\mathbb{Z}_2$ polynomin $q(x)$ juuri α, ja latinalaisia neliöitä muodostettaessa laskuissa ja neliöiden sieventämisessä voi käyttää apuna yhtälöä $\alpha^3 + \alpha + 1 = 0$.

Tässä tutkielmassa on nyt esitelty n. kertaluvun Eulerin neliöiden muodostaminen n alkion kunnan laskutaulujen avulla. Tätä menetelmää voidaan siis käyttää kun $n = p^m$ jollain alkuluvulla p ja luonnollisella luvulla m. Kaikki luvut $n \in \mathbb{N}$ eivät

tietenkään ole tuota muotoa, mutta kuten todettu, kertaluvun n Eulerin neliöitä löytyy kaikilla $n > 6$. Esimerkiksi kymmenen alkion kuntaa ei ole olemassa, mutta kuitenkin on ainakin kaksi keskenään ortogonaalia 10. kertaluvun latinalaista neliötä, joista saatu Eulerin neliö näyttää tältä:

11	24	37	49	56	68	70	82	93	05
79	33	04	57	41	86	62	20	15	98
60	71	55	94	87	43	26	09	38	12
06	69	73	88	14	27	45	91	52	30
48	96	61	75	22	34	07	13	80	59
97	42	16	63	78	00	54	35	29	81
84	17	40	36	65	72	99	58	01	23
32	50	89	21	03	95	18	44	77	66
53	85	28	02	90	19	31	76	64	47
25	08	92	10	39	51	83	67	46	74

Luonnollisesti myös 10. kertaluvun pareittain ortogonaalien latinalaisten neliöiden joukkoja on useita, vaikka toistaiseksi yhteenkään niistä ei ole löytynyt kuin kaksi neliötä. Tuo yllä esitetty 10×10-neliö on kuitenkin eri neliö kuin Bosen, Shrikhanden ja Parkerin vuonna 1960 artikkelissaan [**3**] esittelemä neliö.

3.4. Taikaneliöt

Ortogonaalien latinalaisten neliöiden hyödyllisten sovellustapojen lisäksi ortogonaaleilla latinalaisilla neliöillä on myös ainakin yksi sinänsä hauska, mutta melko hyödytön sovellus. Paitsi Eulerin neliöitä, pareittain ortogonaalien latinalaisten neliöiden avulla voidaan muodostaa myös niin kutsuttuja taikaneliöitä.

MÄÄRITELMÄ 3.14. Kertaluvun n taikaneliö koostuu kokonaisluvuista $1, 2, \ldots n^2$ järjestettynä $n \times n$ -taulukkoon siten, että taulukon jokaisen rivin, sarakkeen ja diagonaalin luvut summautuvat samaksi luvuksi $n(n^2 + 1)/2$.

Taikaneliön voisi määritellä vastaavalla tavalla myös luvuille $0, 1, \ldots, n^2 - 1$. Tällöin rivien, sarakkeiden ja diagonaalien lukujen summa vain on $n(n^2 + 1)/2 - n = n(n^2 - 1)/2$.

Tällaisia neliöitä voi muodostaa kahden sopivasti valitun keskenään ortogonaalin latinalaisen neliön avulla. Jo ottamalla mitkä tahansa kaksi n. kertaluvun joukkoon $\{0, 1, \ldots, n-1\}$ perustuvaa keskenään ortogonaalia latinalaista neliötä ja asettamalla ne päällekäin saadaan jokaisen rivin ja sarakkeen suhteen taianomainen neliö. Siis minkä tahansa luvuista $0, 1, \ldots, n-1$ muodostetun Eulerin neliön rivit ja sarakkeet summautuvat samaksi luvuksi, kun ajatellaan Eulerin neliön lukuparit n-kantaisina kaksinumeroisina lukuina. Kun muutetaan neliön n-kantaiset luvut 10-kantaisiksi, koostuu neliö täsmälleen luvuista $0, 1, \ldots, n^2 - 1$. Diagonaalit eivät kuitenkaan välttämättä vielä summaudu rivien ja sarakkeiden kanssa samaksi luvuksi.

ESIMERKKI 3.15. Neliöt $\begin{array}{|ccc|}\hline 0&1&2\\2&0&1\\1&2&0\\\hline\end{array}$ ja $\begin{array}{|ccc|}\hline 2&1&0\\1&0&2\\0&2&1\\\hline\end{array}$ muodostavat neliön $\begin{array}{|ccc|}\hline 02&11&20\\21&00&12\\10&22&01\\\hline\end{array}$,

joka

kymmenkantaiseksi muutettuna näyttää tältä:

$$\begin{array}{|ccc|}\hline 2 & 4 & 6 \\ 7 & 0 & 5 \\ 3 & 8 & 1 \\ \hline\end{array}$$

Nyt kaikkien rivien ja sarakkeiden summaksi tulee luku 12, mutta toisen diagonaalin summa on 9 ja toisen 3.

Sen sijaan neliöiden $\begin{array}{|ccc|}\hline 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \\ \hline\end{array}$ ja $\begin{array}{|ccc|}\hline 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \\ \hline\end{array}$ muodostaman kymmenkantaan muunnetun neliön

$$\begin{array}{|ccc|}\hline 3 & 8 & 1 \\ 2 & 4 & 6 \\ 7 & 0 & 5 \\ \hline\end{array}$$

diagonaalitkin summautuvat luvuksi 12. Kun tämän neliön jokaiseen alkioon lisätään luku 1, saadaan täsmälleen määritelmän mukainen taikaneliö

$$\begin{array}{|ccc|}\hline 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \\ \hline\end{array},$$

jonka jokainen rivi, sarake ja diagonaali summautuu luvuksi $3(3^2+1)/2 = 15$.

Mikä on se olennainen ero näissä neliöissä? Mistä tietää, mitkä keskenään ortogonaalit neliöt kelpaavat taikaneliön muodostamiseen? Seuraava lause antaa vastauksen. Esitellään kuitenkin ensin lauseessa käytettävät merkinnät.

Olkoot $K = (k_{ij})$ ja $L = (l_ij)$ joukkoon $\{0, 1, \ldots, n-1\}$ perustuvia keskenään ortogonaaleja n. kertaluvun latinalaisia neliöitä. Muodostetaan näistä Eulerin neliö, jonka alkiot ovat 2-numeroisia n-kantaisia lukuja, joiden ensimmäinen numero on neliöstä K ja toinen neliöstä L. Muunnetaan luvut kymmenkantaisiksi ja merkitään saatua neliötä $M = (m_{ij})$, missä nyt siis $m_{ij} = n \cdot k_{ij} + l_{ij}$. Lisätään vielä luku 1 kaikkiin neliön M lukuihin m_{ij} ja merkitään näin viimeisteltyä neliötä M'.

LAUSE 3.16. *Jos K ja L ovat n. kertaluvun joukkoon $\{0, 1, \ldots, n-1\}$ perustuvia keskenään ortogonaaleja latinalaisia neliöitä ja jos kummankin neliön kumpikin diagonaali summautuu luvuksi*

$$n(n-1)/2,$$

niin yllä esitetyllä tavalla muodostettu neliö M' on n. kertaluvun taikaneliö.

TODISTUS. Muodostuneessa Eulerin neliössä jokaisella rivillä ja sarakkeella kaikki luvut $0, 1, \ldots n-1$ esiintyvät täsmälleen kerran jonkun alkion ensimmäisenä numerona ja täsmälleen kerran jonkun alkion toisena kirjaimena. Siten neliön M minkä tahansa rivin tai sarakkeen lukujen summa on

$$\begin{aligned} n(0+1+\cdots+n-1) + (0+1+\cdots+n) &= (n+1)(0+1+\cdots+n-1) \\ &= (n+1)(n-1)n/2 \\ &= n(n^2-1)/2 \end{aligned}$$

ja neliön M' rivien ja sarakkeiden summa taas on $n(n^2-1)/2+n = n(n^2+1)/2$. Lauseen oletuksen mukaan Eulerin neliön diagonaaleilla ensimmäisten numeroiden summa on $n(n-1)/2$, samoin kuin diagonaalialkioiden toistenkin numeroiden summa, joten neliön M diagonaaleilla olevien lukujen summa on

$$n \cdot n(n-1)/2 + n(n-1)/2 = (n+1) \cdot n(n-1)/2 = n(n^2-1)/2$$

ja näin neliön M' diagonaalisummiksi saadaan $n(n^2-1)/2+n = n(n^2+1)/2$. Siten kaikki rivit, sarakkeet ja diagonaalit summautuvat samaksi luvuksi ja M' on taikaneliö. □

Halutessasi muodostaa n. kertaluvun taikaneliön, sinun ei välttämättä tarvitse laskea kaikkien muodostamiesi latinalaisten neliöiden diagonaalisummia löytääksesi sopivat neliöt taikaneliöön. Jos diagonaalit ovat joukon $\{0, 1, \ldots, n-1\}$ permutaatioita, niiden summa on $n(n-1)/2$. Lisäksi jos kertaluku n on pariton, voit valita ortogonaalit latinalaiset neliöt, joissa toinen diagonaali koostuu pelkästään luvusta $(n-1)/2$.

Esimerkki 3.17. Tarkastellaan luvussa 3.3 konstruoituja 4. kertaluvun pareittain ortogonaaleja latinalaisia neliöitä L_1, L_2 ja L_3, joissa α on korvattu luvulla 2 ja α^2 luvulla 3.

$$L_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, L_2 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{bmatrix}, L_3 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{bmatrix}.$$

Nyt ensimmäisen neliön toinen diagonaalisumma on 0 ja toinen 12. Kumpikaan ei ole $4(4-1)/2 = 6$, eikä neliö L_1 siis kelpaa taikaneliön muodostamiseen. Sen sijaan sekä toisessa että kolmannessa neliössä diagonaalit ovat joukon $\{0, 1, 2, 3\}$ permutaatioita, joten niistä taikaneliön muodostaminen onnistuu. Kymmenkantaan muutettuna näistä muodostettu taikaneliö näyttää tältä:

$$M = \begin{bmatrix} 0 & 5 & 10 & 15 \\ 11 & 14 & 1 & 4 \\ 13 & 8 & 7 & 2 \\ 6 & 3 & 12 & 9 \end{bmatrix} \quad \text{ja} \quad M' = \begin{bmatrix} 1 & 6 & 11 & 16 \\ 12 & 15 & 1 & 5 \\ 14 & 9 & 8 & 3 \\ 7 & 4 & 13 & 10 \end{bmatrix}.$$

Vaikka tämä on ainoa 4. kertaluvun taikaneliö, joka tässä kirjoitelmassa esitetyin keinoin voidaan konstruoida, ei tämä suinkaan ole ainoa maailmassa. Kuten aiemmin todettiin, pareittain ortogonaalien latinalaisten neliöiden joukkoja on useita. Esimerkiksi eräs renesanssiajan taiteilija, Albrecht Dürer, sisällytti kuparikaiverrustyöhönsä Melancholia I:een neliön, jonka alimmalle riville muodostui työn kaiverrusvuosi 1514 [**7**, 267].

$$\begin{bmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{bmatrix}$$

Kirjallisuutta

[1] Michael Artin: *Algebra*, Prentice-Hall, 1991.

[2] Alexander Bogomolny: *Orthogonal Latin Squares*, `http://www.cut-the-knot.org/arithmetic/latin3.shtml`

[3] R. C. Bose, S. S. Shrikhande ja E. T. Parker: *Further results on the construction of mutually orthogonal latin squares and the falsity of euler's conjecture*, Canadian Journal of Mathematics 12 (1960) 189-203.

[4] Charles J. Colbourn ja Jeffrey H. Dinitz: *Mutually orthogonal latin squares: a brief survey of constructions*, Journal of Statistical Planning and Inference 95 (2001) 9-48.

[5] Richard A. Dean: *Elements of Abstract Algebra*, kolmas painos, John Wiley & Sons, 1967.

[6] Trevor Evans: *Universal Algebra and Euler's Officer Problem*, The American Mathematical Monthly Vol 86, No 6 (Jun.-Jul.,1979), pp.466-473.

[7] William J. Gilbert: *Modern Algebra with Applications*, John Wiley & Sons, 1976.

[8] G. J. Simmons: *The Number of Irreducible Polynomials of Degree n Over GF(p)*, The American Mathematical Monthly Vol 77, No 7 (Aug.-Sep.,1970), pp.743-745.

[9] Seth Warner: *Modern Algebra*, Prentice-Hall, 1965.