TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Tommi Kuusisto

Äärellisistä kunnista

Matematiikan ja tilastotieteen laitos
Matematiikka
Huhtikuu 2008

Tampereen yliopisto

Matematiikan, tilastotieteen ja filosofian laitos

Tommi Kuusisto: Äärellisistä kunnista

Pro gradu -tutkielma, 43 s.
Matematiikka
Huhtikuu 2008

TIIVISTELMÄ

Algebra on yksi matematiikan päähaaroista. Sen tutkimuskohteina ovat lukujen ja laskutoimitusten yleiset ominaisuudet. Tutkimus onkin ollut viime vuosikymmeninä vilkasta.

Tämän työn tarkoituksena on esitellä äärellisiä kuntia ja niiden ominaisuuksia. Äärellisten kuntien tutkimus on yksi modernin algebran tutkimuskohteista. Äärelliset kunnat ovat tärkeässä osassa myös nyky-yhteiskunnassa. Suuri osa ihmisistä on käyttänyt esimerkiksi verkkopankin palveluita, joissa salataan tietoliikenne turvallisen käytön takaamiseksi. Tämän tyyppisten sovellusten tutkimiseen on käytetty paljon aikaa, ja äärellisten kuntien tutkiminen on yksi sen tärkeä osa-alue.

Työssä esitetään aluksi työn kannalta tärkeitä algebran peruskäsitteitä, kuten algebrallinen struktuuri, ryhmä ja rengas. Seuraavaksi perehdytään kuntiin ja tarkemmin äärellisiin kuntiin. Tämän jälkeen käsitellään kuntalaajennuksia, äärellisten kuntien ominaisuuksia, sekä lopuksi puhutaan hieman kryptologiasta ja sen käytöstä ennen ja nykyään.

Tutkielman rakenne noudattaa pääosin Lidlin ja Niederreiterin kirjan Finite Fields lukuja 1 ja 2.1.

Sisältö

Johdanto

Historiaa

Algebra on yksi matematiikan päähaaroista. Sen tutkimuskohteina ovat lukujen ja laskutoimitusten yleiset ominaisuudet. Tutkimus onkin ollut viime vuosikymmeninä vilkasta.

Kreikkalaisten matemaatikkojen ja filosofien voidaan sanoa ottaneen käyttöön abstraktisuuden ja aksiomatisoinnin ideat 600-300 eKr. 1800-luvulla algebrassa esiintyi kasvavassa määrin konkreettisia systeemejä, jotka olivat näennäisesti erilaisia, mutta muistuttivat syvällisemmin tarkasteltuina toisiaan. Kiinnittämällä huomio systeemin yhteisiin piirteisiin saatiin muotoiltua vastaava "abstraktin"systeemin käsite ja sitä kautta luokiteltua eri systeemejä. Esimerkiksi ryhmän käsitteen käyttö tekee mahdolliseksi useiden eri asioiden käsittelyn yhtenäisiä sääntöjä soveltaen.

Klassinen algebra käsitteli polynomiyhtälöitä, erityisesti yrittäen antaa ratkaisukaavoja. Vuonna 1824 norjalainen Niels Henrik Abel todisti, että viidennen asteen yhtälöllä ei ole yleistä algebrallista ratkaisukaavaa. Tämän jälkeen hän tutki, miten karakterisoida ne yhtälöt, jotka voidaan ratkaista rationaalisilla operaatioilla (yhteen- ja vähennyslasku, kertominen sekä jakaminen) ja ottamalla juuria. Ongelman ratkaisi 1832 ranskalainen Evariste Galois. Ratkaisuun liittyy kommutatiivisen ryhmän käsite, ja vuosia myöhemmin tälle ryhmälle annettiin nimeksi Abelin ryhmä. Galois esitti myös normaalin aliryhmän käsitteen ja tutki äärellisiä kuntia, jotka ovat tämän työn pääaiheena.

Kahden edellä mainitun matemaatikon nimet tulevat esiin tässä työssä, mutta tulee huomioida, että he olivat vain algebran tutkimuksen alulle panijoita.

Monet tunnetut matemaatikot, kuten Hilbert, Steinitz ja Brauer, ovat tutkineet tätä matematiikan osa-aluetta, ja tutkimus jatkuu edelleen.

Työstä

Tämän työn tarkoituksena on esitellä äärellisiä kuntia ja niiden ominaisuuksia. Kuntatutkimus on yksi matematiikan tärkeä tutkimuskohde. Äärelliset kunnat ovat tärkeässä osassa myös nyky-yhteiskunnassa, vaikka sitä ei heti niin selvästi havaitsisikaan. Suuri osa ihmisistä on käyttänyt esimerkiksi verkkopankin palveluita, joissa salataan tietoliikenne turvallisen käytön takaamiseksi. Tämän tyyppisten sovellusten tutkimiseen on käytetty paljon aikaa, ja äärellisten kuntien tutkiminen on yksi sen tärkeä osa-alue.

Tämän työn ensimmäisessä luvussa esitellään laajalti algebran peruskäsitteitä, jotka on tarpeen tuntea työtä luettaessa. Lukijalta siis vaaditaan vain lukion perustietojen osaaminen algebran osalta.

Tutkielman rakenne noudattaa pääosin Lidlin ja Niederreiterin kirjan [4] lukuja 1 ja 2.1.

Luku 1

Esitiedot

1.1 Algebrallinen struktuuri

Määritelmä 1.1 *Olkoon S ei-tyhjä joukko. Kuvausta $S \times S \to S$ sanotaan binäärioperaatioksi joukossa S. Usein käytetään myös nimitystä laskutoimitus joukossa S. Binäärioperaatio liittää siis jokaiseen järjestettyyn pariin $(s,t) \in S \times S$ täsmälleen yhden alkion joukosta S. Merkitään tätä alkiota jatkossa $s * t$.*

Laskutoimitus on siis sulkeutuva, mikä tarkoittaa, että $s*t \in S$ aina, kun $s,t \in S$.

Määritelmä 1.2 *Algebrallisen struktuurin muodostaa joukko S ja sen yksi tai useampi laskutoimitus.*

Määritelmä 1.3 *Alkio $e \in A$ on algebrallisen struktuurin $(S,*)$ neutraalialkio, jos jokaiselle joukon S alkiolle a pätee*

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

Lause 1.1 *Algebrallisen struktuurin neutraalialkio on yksikäsitteinen.*

Todistus Olkoot e ja e' algebrallisen struktuurin $(A, *)$ neutraalialkioita. Silloin

$$a * e = a \qquad \forall a \in A$$

ja

$$e' * b = b \qquad \forall b \in A.$$

Jos valitaan $a = e'$ ja $b = e$, niin saadaan

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

□

Määritelmä 1.4 *Olkoon $(A, *)$ algebrallinen struktuuri ja $a \in A$. Jos on olemassa sellainen alkio $a' \in A$, että*

$$a * a' = a' * a = e,$$

missä e on neutraalialkio, niin alkiota a' sanotaan alkion a käänteisalkioksi. Usein tätä merkitään $a' = a^{-1}$.

1.2 Ryhmä

Määritelmä 1.5 *Ryhmä $(G, *)$ on joukon G ja sen laskutoimituksen $*$ muodostama algebrallinen struktuuri, jossa seuraavat kolme ominaisuutta pätevät:*

1. *$*$ on assosiatiivinen, eli kaikilla joukon G alkioilla a, b, c*

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

2. *joukossa G on neutraalialkio e,*

3. *jokaisella joukon G alkiolla a on käänteisalkio $a' \in G$.*

Lause 1.2 *Ryhmän $(G, *)$ alkion a käänteisalkio a^{-1} on yksikäsitteinen.*

Todistus Olkoot x ja y alkion a käänteisalkioita. Nyt

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

ja

$$a * y = y * a = e.$$

Nyt koska laskutoimitus $*$ on assosiatiivinen, voidaan päätellä

$$x = e * x = (y * a) * x = y * (a * x) = y * e = y.$$

Täten siis

$$x = y.$$

□

Määritelmä 1.6 *Ryhmä $(G, *)$ on Abelin ryhmä, jos laskutoimitus $*$ on kommutatiivinen eli kaikilla joukon G alkioilla a ja b pätee*

$$a * b = b * a.$$

Esimerkki 1.1 Olkoon $(G, *)$ Abelin ryhmä ja $a \in G$. Määritellään G:n laskutoimitus $\circ$ seuraavasti:

$$x \circ y = x * y * a$$

jokaisella joukon G alkiolla x ja y. Todista, että $(G, \circ)$ on Abelin ryhmä.

Olkoot $x, y, z \in G$ mielivaltaisia. Ryhmä $(G, \circ)$ on kommutatiivinen, koska $(G, *)$ on Abelin ryhmä. Ryhmän $(G, \circ)$ neutraalialkio on a^{-1}, sillä

$$x \circ a^{-1} = x * a^{-1} * a = x = a^{-1} \circ x,$$

koska $(G, *)$ on Abelin ryhmä. Alkion x käänteisalkio on $a^{-1} * a^{-1} * x^{-1}$, sillä

$$a^{-1} * a^{-1} * x^{-1} \circ x = a^{-1} * a^{-1} * x^{-1} * x * a = a^{-1}.$$

Nyt

$$x\circ(y\circ z) = x\circ(y*z*a) = x*(y*z*a)*a = (x*y*a)*z*a = (x*y*a)\circ z = (x\circ y)\circ z,$$

joten $(G, \circ)$ on assosiatiivinen. Täten $(G, \circ)$ on Abelin ryhmä. □

Usein käytetään tavallista kertolaskun merkintätapaa ab tarkoittamaan binäärioperaatiota $a * b$. Assosiatiivisuuden nojalla käytetään usein myös potenssimerkintää
$a^n = \underbrace{a * a * a \cdots * a}_{n}$.
Toisaalta jos binäärioperaatio on yhteenlaskun kaltainen, potenssin sijaan puhutaan monikerrasta ja merkitään tätä $na = \underbrace{a + a + \cdots + a}_{n}$.

Määritelmä 1.7 *Ryhmä $(G, *)$ on syklinen, jos on olemassa sellainen $a \in G$, että jokaisella alkiolla $b \in G$ pätee $b = a^j$ jollain $j \in \mathbf{Z}$. Tällaista alkiota a kutsutaan syklisen ryhmän generaattoriksi ja tätä merkitään $G = \langle a \rangle$.*

Syklisellä ryhmällä voi olla useampi kuin yksi generaattori.
Esimerkiksi ryhmällä $(\mathbf{Z}, +)$ generaattoreita ovat alkiot -1 ja 1.

Ryhmien ominaisuuksia käsiteltäessä tulee usein vastaan termi ekvivalenssirelaatio. Joukon $S \times S$ osajoukkoa R kutsutaan ekvivalenssirelaatioksi joukossa S, jos seuraavat kolme ominaisuutta ovat voimassa:

1. $(s, s) \in R$ jokaisella $s \in S$ (refleksiivisyys).
2. Jos $(s, t) \in R$, niin $(t, s) \in R$ (symmetrisyys).
3. Jos $(s, t), (t, u) \in R$, niin $(s, u) \in R$ (transitiivisuus).

Yksinkertaisin esimerkki ekvivalenssirelaatiosta on yhtäsuuruus.

Alkion $s \in S$ kanssa ekvivalentit alkiot muodostavat joukon S osajoukon, jota kutsutaan alkion a ekvivalenssiluokaksi ja sitä merkitään

$$[s] = \{t \in S : (s, t) \in R\}.$$

Nyt huomataan, että $[s] = [t]$ vain silloin kun $(s, t) \in R$.

Koodausteoriassa eräs tärkeä käsite on kongruenssi. Kongruenssi mahdollistaa jaollisuuteen liittyvien asioiden käsittelyn tavalla, joka muistuttaa yhtälöiden käsittelyä. Määritellään se seuraavaksi.

Määritelmä 1.8 *Olkoon m positiivinen kokonaisluku. Jos $a, b \in \mathbf{Z}$ ja $a - b$ on jaollinen luvulla m, sanotaan, että a on kongruentti b:n kanssa modulo m, ja merkitään*

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

Kun a ei ole kongruentti b:n kanssa modulo m, merkitään sitä $a \not\equiv b \pmod{\text{m}}$. Tällöin sanotaan, että a on epäkongruentti b:n kanssa modulo m. Kongruenssi $a \equiv b \pmod{m}$ voidaan esittää myös muodossa

$$m \mid (a - b).$$

Tämä merkintä tarkoittaa siis, että luku $(a - b)$ on jaollinen luvulla m, eli on olemassa sellainen luku $c \in \mathbf{Z}$, että $a - b = mc$.

Annetaan muutama esimerkki kongruenssista.

Esimerkki 1.2 $42 \equiv 2 \pmod{8}$, $7 \equiv -8 \pmod{5}$, $40 \not\equiv 1 \pmod{10}$.

Lause 1.3 *Kongruenssi $\equiv$ on ekvivalenssirelaatio eli*

1. $a \equiv a \pmod{m}$,
2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$,
3. $a \equiv b \pmod{m}$ *ja* $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Todistus
Kohta 1. seuraa selvästi relaatiosta $m \mid 0$.
2. Oletetaan, että $a \equiv b \pmod{m}$. Silloin $m \mid (a - b)$, joten $m \mid (b - a)$. Siis $b \equiv a \pmod{m}$.
3. Oletetaan, että $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$. Nyt $m \mid (a - b)$

ja $m \mid (b-c)$. Tällöin $m \mid (a-b)+(b-c)$, joten $m \mid (a-c)$. Täten siis $a \equiv c \pmod{m}$. □

Mietitään nyt minkälaisiin ekvivalenssiluokkiin kongruenssi modulo m jakaa kokonaislukujen joukon $\mathbf{Z}$. Joukot ovat

$$[0] = \{\ldots, -2m, -m, 0, m, 2m, \ldots\},$$

$$[1] = \{\ldots, -2m+1, -m+1, 1, m+1, 2m+1, \ldots\},$$

$$\vdots$$

$$[m-1] = \{\ldots, -m-1, -1, m-1, 2m-1, 3m-1 \ldots\}.$$

Näitä joukkoja kutsutaan jäännösluokiksi.
Alkion a määräämä jäännösluokka $[a] = \{a + km \mid k \in \mathbf{Z}\}$. Nyt voidaan määritellä laskutoimitus ekvivalenssiluokkien $\{[0], [1], \ldots, [m-1]\}$ joukossa:

$$[a] + [b] = [a+b], \tag{1.1}$$

missä yhtälön oikealla puolella oleva laskutoimitus $a+b$ on tavallinen yhteenlaskutoimitus. Laskutoimitus on hyvin määritelty: Valitaan mielivaltaiset alkiot $a' \in [a]$ ja $b' \in [b]$. Tällöin $a' = km + a$ ja $b' = lm + b$, missä $k, l \in \mathbf{Z}$. Nyt

$$a' + b' = (km + a) + (lm + b) = (k+l)m + (a+b).$$

Siis $a' + b' \in [a+b]$, joten tulos ei riipu siitä, mitkä alkiot jäännösluokista valitaan.
Samaan tapaan voidaan määritellä kertolasku

$$[a][b] = [ab].$$

Lause 1.4 *Algebrallista struktuuria, jonka muodostavat ekvivalenssiluokkien modulo m joukko* $\{[0], [1], \ldots, [m-1]\}$ *ja laskutoimitus* (1.1)*, kutsutaan kokonaislukujen modulo m määräämäksi ryhmäksi ja sitä merkitään* $\mathbf{Z}_{\mathrm{m}}$.

Todistus
Todistetaan, että joukko $\mathbf{Z}_m = \{[0], [1], \ldots, [m-1]\}$ ja sen laskutoimitus (1.1) muodostavat ryhmän.
Olkoon mielivaltaiset $a, b, c \in \mathbf{Z}$ ja

$$[a], [b], [c] \in \{[0], [1], \ldots, [m-1]\}.$$

Ryhmän neutraalialkio on [0], sillä

$$[a] + [0] = [a + 0] = [a] = [0] + [a]$$

ja alkion $[a]$ käänteisalkio on $[-a]$, sillä

$$[a] + [-a] = [a + (-a)] = [0] = [-a] + [a].$$

Ryhmä on lisäksi assosiatiivinen, koska

$$[a]+([b]+[c]) = [a]+[b+c] = [a+(b+c)] = [(a+b)+c] = [a+b]+[c] = ([a]+[b])+[c].$$

□

Ryhmä $\mathbf{Z}_m$ on itse asiassa syklinen ryhmä ja sen yksi generaattori on ekvivalenssiluokka [1].

Ryhmän $\mathbf{Z}_5$ kertolaskutaulu on

*	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Määritelmä 1.9 *Ryhmää kutsutaan äärelliseksi, jos siinä on äärellinen määrä alkioita. Joukon G alkioiden lukumäärää merkitään $\mid G \mid$ ja sanotaan joukon kertaluvuksi.*

Määritelmä 1.10 *Olkoot $(G, *)$ ja $(H, \bullet)$ ryhmiä. Kuvaus $f : G \to H$ on homomorfismi, jos*

$$f(a * b) = f(a) \bullet f(b)$$

kaikilla alkioilla $a, b \in G$.

Lause 1.5 *Olkoot $(G, *)$ ja $(H, \bullet)$ ryhmiä ja olkoon kuvaus $f : G \to H$ homomorfismi. Olkoon lisäksi e ryhmän $(G, *)$ ja e' ryhmän $(H, \bullet)$ neutraalialkio. Silloin*

1. $f(e) = e'$,
2. $f(a^{-1}) = f(a)^{-1}$

kaikilla alkioilla $a \in G$.

Todistus
1. Ensiksi $f(e) = f(e * e) = f(e) \bullet f(e)$. Nyt voidaan kertoa molemmat puolet $f(e)$:n käänteisalkiolla, jolloin saadaan $f(e) = e'$.
2. Toiseksi $f(a) \bullet f(a^{-1}) = f(a * a^{-1}) = f(e) = e'$ ja samoin $f(a^{-1}) \bullet f(a) = e'$, joten $f(a^{-1}) = f(a)^{-1}$ käänteisalkion yksikäsitteisyyden mukaan. □

Määritelmä 1.11 *Olkoot $(G, *)$ ja $(H, \bullet)$ ryhmiä. Kuvaus $f : G \to H$ on isomorfismi, jos se on bijektio ja homomorfismi.*

Esimerkki 1.3 Olkoot $\mathbf{R}$ reaalilukujen joukko ja $\mathbf{R}_+ = \{x \in \mathbf{R} \mid x > 0\}$. Tällöin $(\mathbf{R}, +)$ ja $(\mathbf{R}_+, \cdot)$ ovat ryhmiä (jotka oletetaan tunnetuiksi). Osoita, että nämä ryhmät ovat isomorfiset.

Määritellään $f : \mathbf{R} \to \mathbf{R}_+$

$$f(x) = e^x.$$

Todistetaan, että f on homomorfismi. Olkoot $x, y \in \mathbf{R}$ mielivaltaisia alkioita. Tällöin

$$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y).$$

Siis f on homomorfismi. Osoitetaan seuraavaksi, että f on bijektio. Jokaisella alkiolla $x \in \mathbf{R}$ kuvaus

$$f'(x) = e^x > 0,$$

joten f on aidosti kasvava ja täten siis injektio. Koska $\lim_{x\to\infty} f(x) = \infty$ ja $\lim_{x\to-\infty} = 0$ sekä f on jatkuva, niin f on surjektio. Täten siis f on bijektiivinen homomorfismi eli isomorfismi.

Määritelmä 1.12 *Homomorfismin $f : G \to H$ ydin ryhmästä G ryhmään H on joukko*

$$kerf = \{a \in G : f(a) = e'\},$$

missä e' ryhmän H neutraalialkio.

1.3 Rengas ja sen ominaisuuksia

Määritelmä 1.13 *Rengas $(R, +, \cdot)$ on algebrallinen struktuuri, jossa on määritelty kaksi laskutoimitusta $+$ ja $\cdot$, ja seuraavat kohdat pätevät:*

1. *$(R, +)$ on Abelin ryhmä,*

2. *Laskutoimitus $\cdot$ on assosiatiivinen, eli kaikilla alkioilla $a, b, c \in R$*

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

3. *osittelulait ovat voimassa, eli kaikilla alkioilla $a, b, c \in R$*

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

ja

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

Laskutoimitukset $+$ ja $\cdot$ eivät välttämättä ole tavallisia yhteen- ja kertolaskutoimituksia. Ryhmän $(R, +)$ neutraalialkiota kutsutaan nolla-alkioksi ja merkitään symbolilla 0.

Määritelmä 1.14 *Rengasta $(R, +, \cdot)$ kutsutaan 1-renkaaksi, jos joukossa R on olemassa ykkösalkio* 1 *kertolaskun suhteen, eli*

$$\forall a \in R : a \cdot 1 = 1 \cdot a = a.$$

Määritelmä 1.15 *Rengasta $(R, +, \cdot)$ kutsutaan kommutatiiviseksi, jos kertolasku $\cdot$ on kommutatiivinen, eli*

$$\forall a, b \in R : a \cdot b = b \cdot a.$$

Lause 1.6 *Renkaan perusominaisuuksia:*
Olkoon $(R, +, \cdot)$ rengas ja olkoon $a, b, c \in R$. Silloin

1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$,
3. $-(-a) = a$,
4. $(-a)(-b) = ab$,
5. $a(b - c) = ab - ac$ *ja* $(a - b)c = ac - bc$, *missä* $a - b = a + (-b)$.

Todistus Vrt. [3], s. 103.
1. Koska $0a = (0 + 0)a = 0a + 0a$, niin vähentämällä saadun yhtälön molemmilta puolilta $0a$, saadaan yhtälö $0 = 0a$. Vastaavasti $a0 = 0$.
2. Koska $ab + a(-b) = a(b + (-b)) = a0 = 0$, niin tulo $a(-b)$ on tulon ab vasta-alkio. Vastaavasti $(-a)b$ on tulon (ab) vasta-alkio.
3. Kaava on yleisesti voimassa ryhmässä.
4. Seuraa kohdista 2. ja 3. siten, että $(-a)(-b) = -((-a)b) = -(-(ab)) = ab$.
5. $a(b - c) = ab + a(-c) = ab + (-(ac)) = ab - ac$; vastaavasti toinen. □

Esimerkki 1.4 Todista, että jos $(R, +, \cdot)$ on kommutatiivinen rengas, niin $a^2 - b^2 = (a + b)(a - b)$.

Renkaan ominaisuuksien perusteella saadaan

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

$$= a^2 - (ab) + ab + (-b^2) = a^2 + 0 + (-b^2) = a^2 - b^2.$$

Määritelmä 1.16 *Rengasta* $(R, +, \cdot)$ *kutsutaan jakorenkaaksi, jos* $(R\backslash\{0\}, \cdot)$ *muodostaa ryhmän.*

Määritelmä 1.17 *Kommutatiivinen jakorengas on kunta.*

Täten ollaan päädytty käsitteeseen kunta, joka on tämän tutkielman pääkäsite. Määritellään kuitenkin vielä muutama kuntien tarkastelussa tarvittava käsite.

Määritelmä 1.18 *Olkoon* S *epätyhjä joukko ja olkoon se lisäksi joukon* R *osajoukko. (Siis* $\emptyset \neq S \subseteq R$*).* $(S, +, \cdot)$ *on renkaan* $(R, +, \cdot)$ *alirengas, jos* S *on suljettu laskutoimitusten* $+$ *ja* $\cdot$ *suhteen sekä* $(S, +, \cdot)$ *on rengas.*

Määritelmä 1.19 *Olkoon* R *rengas. Joukon* R *osajoukkoa* J *sanotaan ideaaliksi, jos* J *on* R*:n alirengas ja kaikille alkioille* $a \in J$ *ja* $r \in R$ *pätee* $ar \in J$ *ja* $ra \in J$*.*

Määritelmä 1.20 *Olkoon* R *kommutatiivinen rengas ja* $a \in R$*. Tällöin suppeinta ideaalia, joka sisältää alkion* a*, kutsutaan* a*:n generoimaksi pääideaaliksi. Pääideaalia merkitään* $J = (a)$*.*

Koska ideaalit ovat renkaan yhteenlaskun suhteen aliryhmiä, niin renkaan R ideaali J jakaa renkaan R erillisiin joukkoihin, joita kutsutaan jäännösluokiksi ideaalin J suhteen. Jos J on renkaan R ideaali ja alkiot $a, b \in R$, niin alkio a on *kongruentti* b:n kanssa *modulo* J, eli

$$a \equiv b \pmod{J},$$

jos $a - b \in J$. Nyt osoittautuu, että kongruenssi on ekvivalenssi (ks. [4, s. 13]). Jäännösluokat ovat J:n määrittelemiä ekvivalenssiluokkia. Renkaan R alkion a jäännösluokkia J:n suhteen merkitään $[a] = a + J$, koska niiden alkiot ovat R:n alkioita, jotka ovat muotoa $a + c$ jollain $c \in J$.

Määritelmä 1.21 *Ideaalin* J *renkaasta* R *muodostamien jäännösluokkien rengasta, jossa on seuraavat laskutoimitukset voimassa: kun* $a, b \in R$*, niin*

$$(a + J) + (b + J) = (a + b) + J$$

ja

$$(a + J)(b + J) = ab + J,$$

sanotaan R:n jäännösluokkarenkaaksi ideaalin J suhteen. Tätä merkitään R/J.

Osoitetaan, että määritelmän jäännösluokkien kertolasku on hyvinmääritelty (yhteenlasku samaan tapaan): Olkoon $a + J = a' + J$ ja $b + J = b' + J$. Nyt $a = a' + j_1$ ja $b = b' + j_2$ joillain $j_1, j_2 \in J$. Silloin

$$ab = (a' + j_1)(b' + j_2) = a'b' + a'j_2 + j_1b' + j_1j_2.$$

Koska J on renkaan R ideaali, se sisältää tulot $a'j_2, j_1b'$ ja j_1j_2 sekä niiden summan. Siis $ab = a'b' + j$, missä $j \in J$. Täten siis $ab \in a'b' + J$ eli $ab + J = a'b' + J$.

Lause 1.7 *Jäännösluokkarengas* $\mathbf{Z}/(p)$*, jolla tarkoitetaan alkuluvun p generoimaa pääideaalin suhteen muodostuvaa jäännösluokkien rengasta, on kunta.*

Todistus Ks. [4, s. 14].

Homomorfismin käsite voidaan laajentaa ryhmien tasolta renkaan tasolle. Kuvaus $\varphi : R \to S$ renkaasta R renkaaseen S on rengashomomorfismi, jos kaikille $a, b \in R$ pätee

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad ja \quad \varphi(ab) = \varphi(a)\varphi(b).$$

Rengashomomorfismin $\varphi : R \to S$ ydin on

$$\ker\varphi = \{a \in R : \varphi(a) = 0 \in S\}.$$

Esimerkki 1.5 Olkoot R_1, R_2 ja R_3 renkaita ja $f : R_1 \to R_2$ ja $g : R_2 \to R_3$ rengashomomorfismeja. Osoita, että $g \circ f$ on rengashomomorfismi.

Olkoot $x, y \in R_1$ mielivaltaiset alkiot. Nyt koska f ja g ovat rengashomomorfismeja, niin

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

ja

$$(g\circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g\circ f)(x)(g\circ f)(y),$$

joten $g \circ f$ on rengashomomorfismi.

Lause 1.8 *(Homomorfismilause renkaille)*
Jos φ on homomorfismi renkaasta R renkaaseen S, niin $ker\varphi$ on renkaan R ideaali ja S on homomorfinen jäännösluokkarenkaan $R/(ker\varphi)$ kanssa. Toisaalta, jos J on renkaan R ideaali, niin kuvaus $\psi : R \to R/J$, joka on määritelty $\psi(a) = a + J$ kaikilla $a \in R$, on homomorfismi R:ltä R/J:lle ja $ker\psi = J$.

Todistus Ks. [4, s. 15].

Määritelmä 1.22 *Olkoon p alkuluku ja olkoon $F_p = \{0, 1, \ldots, p-1\}$. Olkoon lisäksi $\varphi : \mathbf{Z}/(p) \to F_p$ kuvaus siten, että $\varphi([a]) = a$, kun $a \in F_p$. Nyt F_p on äärellinen kunta ja sitä kutsutaan Galois'n kunnaksi (kertalukua p).*

Kuvaus $\varphi : \mathbf{Z}/(p) \to F_p$ on isomorfismi siten, että

$$\varphi([a] + [b]) = \varphi([a]) + \varphi([b]) \quad ja \quad \varphi([a][b]) = \varphi([a])\varphi([b]).$$

Ks. [4, s. 15].

Äärellisessä kunnassa F_p on nolla-alkio 0, ykkösalkio 1 ja sen struktuuri on täysin samanlainen kuin $\mathbf{Z}/(p)$:n struktuuri. Galois'n kuntia käytetään esimerkiksi koodausteoriassa. Se onkin yksi tärkeimpiä käytännön sovellusalueita, jossa kuntien tutkimista tarvitaan.

Määritelmä 1.23 *Jos R on rengas ja sillä on olemassa positiivinen kokonaisluku n siten, että jokaisella renkaan R alkiolla r*

$$nr = 0,$$

niin pienintä tällaista lukua n kutsutaan renkaan R karakteristikaksi ja merkitään $\mathrm{char}(R)$.

Jos tällaista positiivista kokonaislukua ei löydy, sanotaan, että renkaan R karakteristika on 0.

Esimerkki 1.6 $\mathrm{char}(F_p) = p$ *ja* $\mathrm{char}(\mathbf{Q}) = 0$.

Määritelmä 1.24 *Olkoon* $(R, +, \cdot)$ *rengas. Silloin* $a \in R$ *on nollanjakaja, jos*

1. $a \neq 0$ *ja*

2. *on olemassa alkio* $b \in R \setminus \{0\}$ *siten, että* $ab = 0$ *tai* $ba = 0$.

Yllä olevassa määritelmässä myös alkio b on nollanjakaja.

Lause 1.9 *Renkaan* $R \neq \{0\}$*, jolla on positiivinen karakteristika ja ei ole nollanjakajia, karakteristika on alkuluku.*

Todistus Koska joukko R sisältää nollasta poikkeavia alkioita, niin R:n karakteristika $n \geq 2$. Jos n ei ole alkuluku, niin voidaan kirjoittaa $n = km$, missä $k, m \in \mathbf{Z}, 1 < k, m < n$. Nyt $0 = ne = (km)e = (ke)(me)$, joten tulee olla $ke = 0$ tai $me = 0$, koska R:ssä ei ole nollanjakajia. Tästä seuraa, että joko jokaisella alkiolla $r \in R : kr = (ke)r = 0$ tai jokaisella $r \in R : mr = (me)r = 0$, mikä on ristiriita karakteristikan määritelmän kanssa. □

Määritelmä 1.25 *Kommutatiivista 1-rengasta, jossa ei ole nollanjakajia, sanotaan kokonaisalueeksi.*

Luku 2

Äärellinen kunta

2.1 Kunta

Kuten edellä määritelmässä 1.17 ollaan esitetty, kommutatiivinen 1-rengas $(F, +, \cdot)$ on kunta, jos jokaisella joukon $F \setminus \{0\}$ alkiolla on käänteisalkio.

Lause 2.1 *Jokainen äärellinen kokonaisalue on kunta.*

Todistus Olkoot äärellisen kokonaisalueen R alkiot $a_1, a_2, \ldots, a_n$. Olkoon alkio $a \in R$ ja $a \neq 0$. Kerrotaan joukon R alkiot alkiolla a ja saadaan $aa_1, aa_2, \ldots, aa_n$. Saadut alkiot ovat erisuuria, sillä jos olisi $aa_i = aa_j$, niin olisi $a(a_i - a_j) = 0$, ja koska $a \neq 0$, tulisi olla $a_i - a_j = 0$, jolloin $a_i = a_j$, mikä on mahdotonta. Nyt jokainen joukon R alkioista on muodossa aa_i ja erityisesti joukon R neutraalialkio $e = aa_i$ jollain $1 \leq i \leq n$. Koska R on kommutatiivinen, on $a_i a = e$. Täten alkiolla a_i on käänteisalkio a. Täten joukon R alkiot $(\neq 0)$ muodostavat kommutatiivisen ryhmän, joten R on kunta. □

2.2 Äärellinen kunta

Määritelmä 2.1 *Kuntaa, jossa on äärellinen määrä alkioita, sanotaan äärelliseksi kunnaksi.*

Lause 2.2 *Äärellisen kunnan karakteristika on alkuluku.*

Todistus Lauseen 1.9 perusteella riittää osoittaa, että äärellisellä kunnalla F on positiivinen karakteristika. Tarkastellaan alkioita $e, 2e, 3e, \ldots$, missä e on neutraalialkio. Koska F:ssä on äärellinen määrä erisuuria alkioita, on olemassa alkiot k ja m, missä $1 \leq k < m$, siten, että $ke = me$. Nyt $(m-k)e = 0$ ja täten F:llä on positiivinen karakteristika. □

Lause 2.3 *Olkoon R kommutatiivinen rengas ja sen karakteristika alkuluku p. Tällöin*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \quad ja \quad (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

kaikilla $a, b \in R$ ja $n \in \mathbf{N}$.

Jotta saamme tämän lauseen todistettua, meidän tulee ensin todistaa tärkeä teoreema, jota usein kutsutaan binomilauseeksi.

Lause 2.4 (Binomilause)

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

missä

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

ja $n!$ tarkoittaa luvun n kertomaa.

Todistus Tehdään todistus induktiolla alkion n suhteen. Tehdään alkuaskel, että $n = 0$. Nyt

$$(a+b)^0 = 1 = \sum_{k=0}^{0} \binom{0}{k} a^{0-k} b^k.$$

Täten siis alkuaskel on voimassa. Tehdään seuraavaksi induktio-oletus, että binomilause pätee, kun $n = m$. Induktioaskeleessa tutkitaan tapausta, kun $n = m + 1$.

$$(a+b)^{m+1} = (a+b)(a+b)^m = a(a+b)^m + b(a+b)^m$$

$$= a\sum_{k=0}^{m}\binom{m}{k}a^{m-k}b^k + b\sum_{j=0}^{m}\binom{m}{j}a^{m-j}b^j \qquad \text{induktio-oletuksen mukaan}$$

$$= \sum_{k=0}^{m}\binom{m}{k}a^{m-k+1}b^k + \sum_{j=0}^{m}\binom{m}{j}a^{m-j}b^{j+1} \qquad \text{kertomalla } a \text{ ja } b \text{ summiin}$$

$$= a^{m+1} + \sum_{k=1}^{m}\binom{m}{k}a^{m-k+1}b^k + \sum_{j=0}^{m}\binom{m}{j}a^{m-j}b^{j+1} \qquad \text{poist. summasta termi } k = 0$$

$$= a^{m+1} + \sum_{k=1}^{m}\binom{m}{k}a^{m-k+1}b^k + \sum_{k=1}^{m+1}\binom{m}{k-1}a^{m-k+1}b^k \qquad \text{asetetaan } j = k-1$$

$$= a^{m+1} + \sum_{k=1}^{m}\binom{m}{k}a^{m-k+1}b^k + \sum_{k=1}^{m}\binom{m}{k-1}a^{m-k+1}b^k + b^{m+1} \qquad \text{poist. } k = m+1$$

$$= a^{m+1} + b^{m+1} + \sum_{k=1}^{m}\left[\binom{m}{k} + \binom{m}{k-1}\right]a^{m-k+1}b^k \qquad \text{yhdistämällä summat}$$

$$= a^{m+1} + b^{m+1} + \sum_{k=1}^{m}\binom{m+1}{k}a^{m-k+1}b^k \qquad \text{koska } \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

$$= \sum_{k=1}^{m+1}\binom{m+1}{k}a^{m-k+1}b^k \qquad \text{lisäämällä termit } m+1 \text{ sisälle summaan}$$

□

Edellisen lauseen todistuksen perustelussa esiintyi kohta

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

joka on niin sanottu Pascalin sääntö. Todistetaan vielä se ennen lauseen 2.3 todistusta.

Lause 2.5 (Pascalin sääntö)

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

Todistus Yhtälön vasen puoli voidaan kirjoittaa muodossa

$$\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-(k-1))!}.$$

Nyt saadaan

$$\begin{aligned}
\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-(k-1))!} &= \frac{(n-k+1)n!}{(n-k+1)k!(n-k)!} + \frac{kn!}{k(k-1)!(n-k+1)!} \\
&= \frac{(n-k+1)n! + kn!}{k!(n-k+1)!} \\
&= \frac{(n+1)n!}{k!((n+1)-k)!} \\
&= \frac{(n+1)!}{k!((n+1)-k)!} \\
&= \binom{n+1}{k}.
\end{aligned}$$

□

Todistetaan seuraavaksi lause 2.3.

Todistus Tiedetään, että

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\cdots(p-i+1)}{1\cdot 2\cdot\cdots\cdot i} \equiv 0 \pmod{p}$$

kaikilla $i \in \mathbf{Z}$ ja $0 < i < p$, mikä seuraa siitä, että $\binom{p}{i}$ on kokonaisluku ja siitä, että tekijää p ei voida supistaa osoittajasta. Nyt binomilauseesta seuraa, että

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p = a^p + b^p,$$

ja induktiolla alkion n suhteen saadaan ensimmäinen kohta todistettua. Nyt edellä osoitetun mukaan saadaan

$$a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n},$$

ja näin on toinenkin kohta saatu todistettua. □

Esimerkki 2.1 Ratkaistaan kunnassa $(K, +, \cdot)$ toisen asteen yhtälö $x^2 + ax + b = 0$, missä $a, b \in K$, olettaen, että $\text{char}(K) \neq 2$.

Koska $\text{char}(K) \neq 2$, on kunnan K alkiolla $2 = 1 + 1$ käänteisalkio $2^{-1} = \frac{1}{2}$. (Merkinnällä $\frac{a}{b}$ tarkoitetaan muotoa ab^{-1}, missä $b \neq 0$.) Nyt myös luvulla $4 = 2 + 2 \neq 0$ on käänteisalkio, nimittäin $(\frac{1}{2})^2$. Nyt

$$x^2 + ax + b = x^2 + ax + \frac{a^2}{4} - \frac{a^2}{4} + b = (x + \frac{a}{2})^2 - (\frac{a^2}{4} - b).$$

Täten yhtälöllä $x^2 + ax + b = 0$ on ratkaisu kunnassa K, jos ja vain jos on olemassa sellainen kunnan K alkio y, että $y^2 = \frac{a^2}{4} - b$. Oletetaan, että tällainen y on olemassa. Silloin

$$x^2 + ax + b = 0 \Leftrightarrow (x + \frac{a}{2})^2 - y^2 = 0 \Leftrightarrow ((x + \frac{a}{2}) - y)((x + \frac{a}{2}) + y) = 0.$$

Koska kunta on kokonaisalue, tämä tarkoittaa, että joko

$$x + \frac{a}{2} - y = 0 \quad \text{tai} \quad x + \frac{a}{2} + y = 0.$$

Täten ratkaisuksi saadaan

$$x = -\frac{a}{2} \pm y,$$

missä

$$y \in K : y^2 = \frac{a^2}{4} - b.$$

2.3 Polynomeista

Olkoon R rengas. Polynomi renkaassa R on

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

missä n on ei-negatiivinen kokonaisluku ja kertoimet a_i, $0 \leq i \leq n$, ovat R:n alkiota ja x on muuttuja, jonka arvot voivat olla laajemmassakin joukossa kuin R. Vertaillaan renkaan R kahta polynomia $f(x)$ ja $g(x)$. Polynomit

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad ja \qquad g(x) = \sum_{i=0}^{n} b_i x^i$$

ovat samat, jos ja vain jos $a_i = b_i$, kun $0 \leq i \leq n$. Polynomien $f(x)$ ja $g(x)$ summa määritellään

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i.$$

Polynomien

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad ja \qquad g(x) = \sum_{j=0}^{m} b_j x^j$$

tulo määritellään

$$f(x)g(x) = \sum_{i=0}^{n+m} c_k x^k,$$

missä

$$c_k = \sum_{i+j=k,} a_i b_j \quad \text{ja} \quad 0 \leq i \leq n, \quad 0 \leq j \leq m.$$

Voidaan helposti osoittaa, että polynomien joukko ja sen edellä mainitut laskutoimitukset R:ssä muodostavat renkaan.

Määritelmä 2.2 *Renkaan R polynomeista ja niiden laskutoimituksista (summa ja tulo) muodostuvaa rengasta kutsutaan R:n polynomirenkaaksi ja sitä merkitään $R[x]$.*

Polynomirenkaan $R[x]$:n nolla-alkio on se polynomia, jonka jokainen kerroin on 0. Sen asteeksi määritellään $-\infty$. Tässä $-\infty$ ajatellaan lukuna, joka on pienempi kuin kaikki reaaliluvut.

Määritelmä 2.3 *Olkoon $f(x) = \sum_{i=0}^{n} a_i x^i$ renkaan R polynomi, joka ei ole nollapolynomi. Oletetaan lisäksi, että $a_n \neq 0$. Tällöin a_n on $f(x)$:n korkeimman asteen kerroin (joskus puhutaan johtavasta kertoimesta). Termi a_0 on vakiokerroin ja n on $f(x)$:n aste ja sitä merkitään $n = \deg(f(x)) = \deg(f)$. Polynomeja, joiden aste on nolla, sanotaan vakiopolynomeiksi. Jos R:n neutraalialkio on 1 ja $f(x)$:n johtava kerroin on 1, niin $f(x)$:ää kutsutaan pääpolynomiksi.*

Lause 2.6 *Olkoon $f, g \in R[x]$. Nyt*

$$\textit{jos } f(x)g(x) \neq 0, \textit{niin } \deg(fg) \leq \deg(f) + \deg(g) \qquad (1)$$

ja

$$\textit{jos } f(x) + g(x) \neq 0, \textit{niin } \deg(f+g) \leq \max\{\deg(f), \deg(g)\}. \qquad (2)$$

Todistus [1, s. 285] Olkoon $\deg(f(x)) = n$ ja $\deg(g(x)) = m$ sekä

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

ja

$$g(x) = b_0 + b_1 x + \cdots + b_m x^m.$$

(1) Nyt

$$f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{m+n}.$$

Koska $f(x)g(x) \neq 0$, niin ainakin yksi polynomin $f(x)g(x)$ kertoimista tulee olla nollasta eroava. Jos $a_n b_m \neq 0$, niin

$$\deg(f(x)g(x)) = n + m = \deg(f(x)) + \deg(g(x)).$$

Jos taas $a_n b_m = 0$, niin polynomin $f(x)g(x)$ asteen määrää polynomin nollasta poikkeava, suurimman eksponentin omaava termi. Nyt

$$\deg(f(x)g(x)) < \deg(f(x)) + \deg(g(x)).$$

(2) Kokonaislukujen ominaisuus on, että vain joko $m > n$, $m = n$ tai $m < n$. Jos $m < n$, niin

$$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_m+b_m)x^m+a_{m+1}x^{m+1}+\cdots+a_nx^n$$

ja

$$\deg(f(x)+g(x)) = n = \max\{\deg(f(x)), \deg(g(x))\}.$$

Vastaavasti käsitellään $m > n$. Jos taas $m = n$, niin

$$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_m)x^n.$$

Nyt koska $f(x)+g(x) \neq 0$, on polynomin termien kertoimista jonkin oltava nollasta poikkeava. Jos $a_n + b_n \neq 0$, niin

$$\deg(f(x)+g(x)) = n = \max\{\deg(f(x)), \deg(g(x))\}.$$

Jos $a_n+b_n = 0$, niin polynomin $f(x)+g(x)$ asteen määrää polynomin nollasta poikkeava, suurimman eksponentin omaava termi. Tällöin

$$\deg(f(x)+g(x)) < \max\{\deg(f(x)), \deg(g(x))\}.$$

□

Esimerkki 2.2 Tarkastellaan polynomeja $f(x) = 1 + x$ ja $g(x) = 1 - x$ yli mielivaltaisen kommutatiivisen renkaan R. Tällöin siis

$$f(x)+g(x) = 2 = 1+1 \quad \text{ja} \quad f(x)g(x) = 1-x^2.$$

Nyt $\deg(f(x)) = \deg(g(x)) = 1$ ja edelleen $\deg(f(x)+g(x)) = 0$. Kuitenkin $\deg(f(x)g(x)) = 2$.

Määritelmä 2.4 *Olkoon F kunta. Polynomi $g \in F[x]$ jakaa polynomin $f \in F[x]$, jos on olemassa polynomi $h \in F[x]$ siten, että $f = gh$.*

Lause 2.7 (Jakoyhtälö)
Olkoon $g \neq 0$ polynomi ja $g \in F[x]$. Jokaisella polynomilla $f \in F[x]$ on olemassa polynomit $q, r \in F[x]$ siten, että

$$f = qg + r, \quad deg(r) < deg(g).$$

Todistus Ks. [1, s. 289].

Esimerkki 2.3 Jaetaan polynomi $f(x) = x^5 + 2x^4 + 4x^2 + 2x + 3 \in F_5[x]$ polynomilla $g(x) = 2x^2 + 2 \in F_5[x]$ jakokulmassa.

$$\begin{array}{rl} & 3x^3 + x^2 + 2x + 1 \\ 2x^2 + 2 \;\big\lceil & x^5 + 2x^4 + 0x^3 + 4x^2 + 2x + 3 \\ & \underline{-x^5 - 0x^4 - x^3} \\ & \quad 2x^4 + 4x^3 + 4x^2 + 2x + 3 \\ & \quad \underline{-2x^4 - 0x^3 - 2x^2} \\ & \qquad 4x^3 + 2x^2 + 2x + 3 \\ & \qquad \underline{-4x^3 - 0x^2 - 4x} \\ & \qquad\quad 2x^2 + 3x + 3 \\ & \qquad\quad \underline{-2x^2 - 0x - 2} \\ & \qquad\qquad 3x + 1 \end{array}$$

Nyt polynomi voidaan kirjoittaa myös muotoon

$$x^5 + 2x^4 + 4x^2 + 2x + 3 = (2x^2 + 2)(3x^3 + x^2 + 2x + 1) + 3x + 1.$$

Määritelmä 2.5 *Olkoon $p \in F[x]$ sellainen polynomi, jonka aste on positiivinen, ja jos $p = bc$, missä $b, c \in F[x]$, niin b tai c on vakiopolynomi. Tällöin polynomia $p \in F[x]$ sanotaan jaottomaksi polynomiksi F:ssä.*

Määritelmä 2.6 *Alkiota $b \in F$ sanotaan polynomin $f \in F[x]$ juureksi, jos $f(b) = 0$.*

Esimerkki 2.4 Osoita, että polynomi $x^2 - 2$ on jaoton polynomirenkaassa $\mathbf{Q}[x]$.

Huomataan, että polynomilla $x^2 - 2$ on tekijä $\mathbf{Q}$:ssa. Tekijä on 1. Koska polynomi on astetta 2, sillä on silloin myös nollakohta $x_0 \in \mathbf{Q}$. Tällöin $x_0^2 = 2$. Tämä on mahdotonta, koska $\pm\sqrt{2} \notin \mathbf{Q}$.
Polynomi $x^2 - 2$ ei ole sen sijaan jaoton renkaassa $\mathbf{R}[x]$, koska $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Lause 2.8 *Olkoon $f \in F[x]$. Jäännösluokkarengas $F[x]/(f)$ on kunta, jos ja vain jos f on jaoton polynomi F:ssä.*

Todistus Ks. [4, s. 25].

Luku 3

Kuntalaajennuksista

3.1 Kuntalaajennus

Määritelmä 3.1 *Olkoon F kunta. Olkoon K kunnan F osajoukko, joka on myös kunta ja jossa on samat laskutoimitukset voimassa kuin kunnassa F. Tällöin K:ta sanotaan kunnan F alikunnaksi. Kuntaa F taas kutsutaan kunnan K laajennukseksi. Jos $K \neq F$, niin K on F:n aito alikunta.*

Esimerkki 3.1 **Q** *on* **R***:n alikunta, ja* **R** *on puolestaan* **C***:n alikunta.*

Olkoon p alkuluku. Jos K on äärellisen kunnan F_p alikunta, niin K sisältää alkiot 0 ja 1 ja täten muutkin F_p :n alkiot, koska K on suljettu yhteenlaskun suhteen. Täten kunnalla F_p ei ole aitoja alikuntia.

Määritelmä 3.2 *Kuntaa, jolla ei ole aitoja alikuntia, sanotaan alkukunnaksi.*

Kuten edellä pääteltiin, kaikki äärelliset kunnat kertalukua p, jossa p on alkuluku, ovat alkukuntia. Toinen hyvä esimerkki alkukunnasta on rationaalilukujen kunta **Q**. Kun otetaan leikkaus annetun kunnan F joistakin alikuntien muodostamasta epätyhjästä joukosta, muodostuu jälleen F:n alikunta. Jos taas otetaan leikkaus kaikista F:n alikunnista, muodostuu F:n suppein alikunta, joka on selvästi alkukunta.

Lause 3.1 *Kunnan F suppein alikunta on isomorfinen joko F_p:n tai $\mathbf{Q}$:n kanssa, sen mukaan, onko F:n karakteristika alkuluku vai* 0.

Todistus Ks. [4, s. 30].

Määritelmä 3.3 *Olkoon K kunnan F alikunta ja M mikä tahansa F:n osajoukko. Tällöin kunta $K(M)$ on leikkaus kaikista F:n alikunnista, jotka sisältävät sekä K:n, että M:n. Sitä kutsutaan K:n laajennukseksi, joka on saatu adjungoimalla M:n alkiot. Jos M on äärellinen ja $M = \{\theta_1, \ldots, \theta_n\}$, niin merkitään $K(M) = K(\theta_1, \ldots, \theta_n)$. Jos joukko M on yksiö sisältäen vain alkion $\theta \in F$, niin $L = K(\theta)$:aa sanotaan K:n yksinkertaiseksi laajennukseksi ja alkiota θ kutsutaan L:n määräväksi alkioksi yli K:n .*

Kunta $K(M)$ on F:n pienin alikunta, joka sisältää sekä K:n, että M:n. Määritellään seuraavaksi tärkeä laajennuksen tyyppi.

Määritelmä 3.4 *Oletetaan, että K on kunnan F alikunta ja $\theta \in F$. Jos θ on ratkaisu polynomiyhtälöön, jonka kertoimet ovat alkioina K:ssa (siis jos $a_n\theta^n + \cdots + a_1\theta + a_0 = 0$ ja $a_n \neq 0$), niin θ:n sanotaan olevan algebrallinen yli K:n. Kunnan K laajennuksen L sanotaan olevan algebrallinen yli K:n, jos jokainen L:n alkio on algebrallinen yli K:n.*

Määritelmä 3.5 *Jos $\theta \in F$ on algebrallinen yli K:n, niin pääpolynomia $g \in K[x]$, joka generoi $K[x]$:n ideaalin $J = \{f \in K[x] : f(\theta) = 0\}$, kutsutaan θ yli K:n minimipolynomiksi. Laajennuksen θ yli K:n asteella tarkoitetaan g:n astetta.*

Lause 3.2 *Jos $\theta \in F$ on algebrallinen yli K:n, niin minimipolynomilla g yli K:n on seuraavat ominaisuudet:*

1. *g on jaoton $K[x]$:ssa.*
2. *Kun $f \in K[x]$, niin $f(\theta) = 0$, jos ja vain jos g jakaa f:n.*

Todistus Ensimmäinen kohta seuraa siitä, että minimipolynomin g aste $deg(g(x)) = 1$. Toinen kohta seuraa g:n määritelmästä.

Jos L on K:n kuntalaajennus, niin L voidaan ajatella K:n vektoriavaruutena, (eli sellaisena vektoriavaruutena, jonka skalaarikunta on K). Tällöin L:n alkiot ('vektorit') muodostavat Abelin ryhmän yhteenlaskun suhteen. Lisäksi jokainen 'vektori' $\alpha \in L$ voidaan kertoa skalaarilla $r \in K$ siten, että $r\alpha \in L$ ja kertolaskun lait skalaarilla kerrottaessa säilyvät: $r(\alpha+\beta) = r\alpha+r\beta, (r+s)\alpha = r\alpha + s\alpha, (rs)\alpha = r(s\alpha)$ ja $1\alpha = \alpha$, kun $r, s \in K$ ja $\alpha, \beta \in L$.

3.2 Kunnan äärellinen laajennus

Määritelmä 3.6 *Olkoon L kunnan K:n laajennus. Ajatellaan laajennus L vektoriavaruutena. Jos L:n dimensio on äärellinen, niin L:ää kutsutaan kunnan K äärelliseksi laajennukseksi. Laajennuksen L vektoriavaruuden dimensiota kutsutaan L:n asteeksi yli K:n ja merkitään $[L : K]$.*

Lause 3.3 *Jos L on kunnan K äärellinen laajennus ja M on L:n äärellinen laajennus, niin M on K:n äärellinen laajennus siten, että*

$$[M : K] = [M : L][L : K].$$

Todistus Olkoon $[M : L] = m, [L : K] = n$ ja olkoon lisäksi $\{\alpha_1, \cdots, \alpha_m\}$ laajennuksen M yli L kanta sekä $\{\beta_1, \cdots, \beta_n\}$ laajennuksen L yli K kanta. Tällöin jokaisella $\alpha \in M$ on olemassa lineaarikombinaatio $\alpha = \gamma_1\alpha_1 + \cdots + \gamma_m\alpha_m$, missä $\gamma_i \in L$ ja $1 \leq i \leq m$. Kirjoitetaan jokainen γ_i kannan alkioiden β_j avulla, jolloin saadaan

$$\alpha = \sum_{i=1}^{m} \gamma_i\alpha_i = \sum_{i=1}^{m}(\sum_{j=1}^{n} r_{ij}\beta_j)\alpha_i = \sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\beta_j\alpha_i,$$

missä kertoimet $r_{ij} \in K$. Osoitetaan, että alkiot $\beta_j\alpha_i$, $1 \leq i \leq m$ ja $1 \leq j \leq n$, ovat lineaarisesti riippumattomia kunnassa K. Oletetaan, että

$$\sum_{i=1}^{m}\sum_{j=1}^{n} s_{ij}\beta_j\alpha_i = 0,$$

missä kertoimet $s_{ij} \in K$. Nyt

$$\sum_{i=1}^{m}(\sum_{j=1}^{n} s_{ij}\beta_j)\alpha_i = 0$$

ja α_i:den lineaarisesta riippumattomuudesta kunnassa L saadaan

$$\sum_{j=1}^{n} s_{ij}\beta_j = 0 \qquad 1 \leq i \leq m.$$

Nyt koska β_j:t ovat lineaarisesti riippumattomia kunnassa K, niin tulee olla, että kaikki kertoimet $s_{ij} = 0$. □

Lause 3.4 *Jokainen kunnan K äärellinen laajennus on algebrallinen yli K:n.*

Todistus Oletetaan, että L on kunnan K äärellinen laajennus ja $[L : K] = m$. Nyt jos $\theta \in L$, niin $m+1$ alkion (alkiot $1, \theta, \ldots, \theta^m$) tulee olla lineaarisesti riippuvia K:ssa ja näin saadaan relaatio $a_0 + a_1\theta + \cdots + a_m\theta^m = 0$, missä jokin $a_i \neq 0$. Täten θ on algebrallinen yli K:n. □

Lause 3.5 *Oletetaan, että $\theta \in F$ on algebrallinen yli kunnan K. Olkoon laajennus astetta n. Olkoon g lisäksi θ:n minimipolynomi yli K:n. Nyt*

1. *$K(\theta)$ on isomorfinen $K[x]/(g)$:n kanssa.*
2. *$[K(\theta) : K] = n$ ja $\{1, \theta, \ldots, \theta^{n-1}\}$ on $K(\theta)$ yli K:n kanta.*
3. *Jokainen $\alpha \in K(\theta)$ on algebrallinen yli K:n ja sen aste yli K:n on alkion n jakaja.*

Jos R on kommutatiivinen rengas, niin alkio $a \in R$ on alkion $b \in R$ jakaja, jos on olemassa $c \in R$ siten, että $ac = b$.

Todistus

1. Olkoon kuvaus $\tau : K[x] \to K(\theta)$ siten, että $\tau(f) = f(\theta)$, kun $f \in K[x]$, jonka huomataan olevan rengashomomorfismi. Minimipolynomin määritelmästä saadaan, että $ker\tau = \{f \in K[x] : f(\theta) = 0\} = (g)$. Olkoon S τ:n kuva, eli S on θ:n polynomisten lausekkeiden joukko siten, että niiden kertoimet kuuluvat joukkoon K. Tällöin homomorfismilauseen renkaille (kts. lause 1.8) mukaan S on isomorfinen $K[x]/(g)$:n kanssa. Lauseiden 2.8 ja 3.2 kohdan 1. mukaan $K[x]/(g)$ on kunta, joten myös S on kunta. Koska $K \subseteq S \subseteq K(\theta)$ ja $\theta \in S$, niin $K(\theta)$:n määritelmästä seuraa, että $S = K(\theta)$, joten kohta 1. on todistettu.

2. Koska $S = K(\theta)$, niin jokainen $\alpha \in K(\theta)$ voidaan kirjoittaa muodossa $\alpha = f(\theta)$ jollain $f \in K[x]$. Nyt jakoyhtälön (kts. lause 2.7) mukaan $f = qg + r$, missä $q, r \in K[x]$ ja $deg(r) < deg(g) = n$. Nyt $\alpha = f(\theta) = q(\theta)g(\theta) + r(\theta) = r(\theta)$. Täten α on $1, \theta, \ldots, \theta^{n-1}$:n lineaarikombinaatio, jonka kertoimet ovat K:ssa. Toisaalta, jos $a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} = 0$ joillakin $a_i \in K$, niin polynomilla $h(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in K[x]$ on juuri θ ja se on täten g:n monikerta lauseen 3.2 kohdan 2 mukaan. Koska $deg(h) < n = deg(g)$, niin tulee olla $h = 0$, eli jokainen kerroin $a_i = 0$. Siis alkiot $1, \theta, \ldots, \theta^{n-1}$ ovat lineaarisesti riippumattomia. Täten kohta 2 on todistettu.

3. Kunta $K(\theta)$ on K:n äärellinen laajennus kohdan 2 mukaan ja täten $\alpha \in K(\theta)$ on algebrallinen yli K:n lauseen 3.4 mukaan. Lisäksi $K(\alpha)$ on $K(\theta)$:n alikunta. Olkoon d $K(\alpha)$ yli K:n aste, jolloin kohdan 2. ja lauseen 3.3 mukaan $n = [K(\theta) : K] = [K(\theta) : K(\alpha)][K(\alpha) : K] = [K(\theta) : K(\alpha)]d$ ja täten d jakaa n:n.

□

Lause 3.6 *Olkoon $f \in K[x]$ jaoton kunnassa K. Tällöin on olemassa kunnan K algebrallinen laajennus, jonka määräävänä alkiona on f:n juuri.*

Todistus Tarkastellaan jäännösluokkarengasta $L = K[x]/(f)$. Se on lauseen 2.8 mukaan kunta. L:n alkioita ovat jäännösluokat $[h] = h + (f)$, missä $h \in K[x]$. Jokaista alkiota $a \in K$ kohti voidaan muodostaa jäännösluokka $[a]$, jonka määrää vakiopolynomi a. Jos alkiot $a, b \in K$ ovat toisistaan eroavia,

niin $[a] \neq [b]$, koska f:n aste on positiivinen. Kuvaus $a \mapsto [a]$ antaa isomorfismin kunnalta K jäännösluokkarenkaan L alikunnalle K'. Voidaan ajatella, että L on kunnan K laajennus. Tällöin jokaiselle polynomille

$$h(x) = a_0 + a_1 x + \cdots + a_m x^m \in K[x]$$

saadaan

$$[h] = [a_0 + a_1 x + \cdots + a_m x^m] = [a_0] + [a_1][x] + \cdots + [a_m][x]^m = a_0 + a_1[x] + \cdots + a_m[x]^m$$

jäännösluokkien laskusääntöjen ja säännön $[a_i] = a_i$ mukaan. Täten jokainen L:n alkio voidaan kirjoittaa polynomilausekkeena jäännösluokan $[x]$ ja kunnan K alkioina olevien kertoimien avulla. Jokaisen kunnan, joka sisältää sekä K:n, että $[x]$:n, tulee sisältää edellä mainitut polynomilausekkeet. Täten siis L on kunnan K laajennus, joka on saatu adjungoimalla siihen $[x]$. Jos

$$f(x) = b_0 + b_1 x + \cdots + b_n x^n,$$

niin

$$f([x]) = b_0 + b_1[x] + \cdots + b_n[x]^n = [b_0 + b_1 x + \cdots + b_n x^n] = [f] = [0],$$

joten $[x]$ on f:n juuri ja L on kunnan K algebrallinen laajennus. □

Määritelmä 3.7 *Oletetaan, että $f \in K[x]$ ja f:n aste on positiivinen. Olkoon lisäksi F kunnan K laajennus. Tällöin f:n sanotaan hajoavan F:ssä, jos f voidaan kirjoittaa $F[x]$:n lineaaristen tekijöiden avulla, eli jos on olemassa alkiot $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ siten, että*

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

missä a on f:n johtava kerroin. Kunta F on f:n hajoamiskunta yli K:n, jos f hajoaa F:ssä ja jos lisäksi $F = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Lause 3.7 *(Hajoamiskunnan olemassaolo ja yksikäsitteisyys)*
Oletetaan, että K on kunta ja f mikä tahansa polynomi, jonka aste on positiivinen polynomirenkaassa $K[x]$. Tällöin on olemassa f:n hajoamiskunta yli K:n. Mitkä tahansa kaksi eri f:n hajoamiskuntaa yli K:n ovat isomorfisia ja täten f:n juuret kuvautuvat toisilleen.

Todistus Ks. [4, s. 35].

Luku 4

Äärellisten kuntien ominaisuuksia

4.1 Äärellisten kuntien ominaisuuksia

Lause 4.1 *Olkoon F äärellinen kunta, jolla on on alikunta K, jossa on q alkiota. Tällöin kunnassa F on q^m alkiota, missä $m = [F : K]$.*

Todistus Kunta F on vektoriavaruus yli alikunnan K. Koska F on äärellinen, niin myös sen dimensio on äärellinen. Jos $[F : K] = m$, niin F:llä on kanta yli K:n, jossa on m alkiota. Merkitään näitä $b_1, b_2, \cdots, b_m$. Nyt jokainen F:n alkio voidaan esittää muodossa $a_1b_1+a_2b_2+\cdots+a_mb_m$, missä $a_1, a_2, \cdots, a_m \in K$. Koska jokaisella a_i:lla voi olla q eri arvoa, niin F:ssä on tasan q^m alkiota. □

Lause 4.2 *Olkoon F äärellinen kunta. Tällöin F:ssä on p^n alkiota, missä alkuluku p on F:n karakteristika ja n on F:n aste yli sen suppeimman alikunnan.*

Todistus Koska F on äärellinen, niin sen karakteristika on alkuluku p lauseen 2.2 mukaan. Täten F:n suppein alikunta K on isomorfinen F_p:n

kanssa lauseen 3.1 mukaan. Täten K:ssa on p alkiota. Lauseen 4.1 nojalla lause on todistettu. □

Lause 4.3 *Jos F on äärellinen kunta ja sillä on q alkiota, niin jokaiselle $a \in F$ pätee $a^q = a$.*

Todistus Kun $a = 0$, niin triviaalisti $a^q = a$. Toisaalta F:n nollasta eroavat alkiot muodostavat ryhmän kertolaskun suhteen ja tämä ryhmä on kertalukua $q-1$. Tällöin $a^{q-1} = 1$ kaikilla $a \in F$ (ks.[3], s.75, seurauslause 2) ja $a \neq 0$ ja tällöin kun kerrotaan tämä alkiolla a, niin saadaan haluttu tulos. □

Lause 4.4 *Jos F on äärellinen kunta ja siinä on q alkiota sekä K on F:n alikunta, niin $K[x]$:n polynomi $x^q - x$ jakautuu $F[x]$:ssä tekijöihin siten, että*

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

ja F on $(x^q - x)$:n hajoamiskunta yli K:n.

Todistus Polynomin $x^q - x$ aste on q, joten sillä on korkeintaan q juurta F:ssä. Lauseen 4.3 mukaan tiedetään q tällaista juurta, nimittäin F:n alkiot. Täten polynomi $x^q - x$ hajoaa F:ssä edellä mainituiksi alkioiksi ja F onkin pienin kunta, jossa se voi hajota. □

Nyt voidaan esittää äärellisten kuntien pääominaisuus seuraavassa lauseessa. Määritellään kuitenkin ensiksi derivaatan käsite. Olkoon $b \in F$ polynomin $f \in F[x]$ juuri. Jos k on positiivinen kokonaisluku siten, että $f(x)$ on jaollinen $(x-b)^k$:lla, mutta ei $(x-b)^{k+1}$:llä, niin k:ta kutsutaan juuren b monikerraksi. Jos $k = 1$, b:tä kutsutaan yksinkertaiseksi juureksi ja jos $k \geq 2$, niin b:tä kutsutaan monikertaiseksi juureksi.

Määritelmä 4.1 *Jos polynomi $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in F[x]$, niin f:n derivaatta f' on $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in F[x]$.*

Alkio $b \in F$ on moninkertainen juuri, jos ja vain jos se on sekä f:n että f':n juuri. (Ks. [4], s.27.)

Lause 4.5 (Äärellisten kuntien olemassaolo ja yksikäsitteisyys)
Jokaista alkulukua p ja jokaista positiivista kokonaislukua n kohti on olemassa äärellinen kunta, jossa on p^n alkiota. Jokainen äärellinen kunta, jossa on $q = p^n$ alkiota, on isomorfinen $(x^q - x)$:n hajoamiskunnan yli F_p:n kanssa.

Todistus (Olemassaolo) Olkoon $q = p^n$ ja polynomi $x^q - x$ polynomirenkaassa $F_p[x]$. Olkoon lisäksi F $(x^q - x)$:n hajoamiskunta yli F_p:n. Polynomilla $x^q - x$ on q erisuurta juurta F:ssä, koska sen derivaatta on $qx^{q-1} - 1 = -1 \in F_p[x]$ jolloin derivaatalla ei voi olla yhteisiä juuria $x^q - x$:n kanssa. Olkoon $S = \{a \in F : a^q - a = 0\}$. Tällöin S on F:n alikunta, koska: (i) $0, 1 \in S$; (ii) $a, b \in S$, jolloin lauseen 2.3 mukaan $(a-b)^q = a^q - b^q = a - b$, joten $a - b \in S$; (iii) jokaiselle $a, b \in S$ ja $b \neq 0$ pätee $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, joten $ab^{-1} \in S$. Toisaalta polynomin $x^q - x$ tulee hajota S:ssä, koska S sisältää sen kaikki juuret. Täten $F = S$, ja koska S:ssä on q alkiota, niin F on äärellinen kunta, jossa on q alkiota.
(Yksikäsitteisyys) Olkoon F äärellinen kunta, jossa on $q = p^n$ alkiota. Tällöin F:n karakteristika on lauseen 4.2 mukaan p ja täten F_p on F:n alikunta. Lauseesta 4.4 seuraa, että F on $(x^q - x)$:n hajoamiskunta yli F_p:n. Täten haluttu tulos seuraa hajoamiskuntien yksikäsitteisyydestä, joka on esitetty lauseessa 3.7. □

Jatkossa äärellistä kuntaa, jossa on q alkiota, merkitään F_q.

Lause 4.6 *Olkoon F_q äärellinen kunta, jossa on alkioita $q = p^n$. Tällöin jokainen F_q:n alikunta on kertalukua p^m, missä m on alkion n positiivinen jakaja. Kääntäen, jos m on alkion n positiivinen jakaja, niin on olemassa täsmälleen yksi F_q:n alikunta, jossa on p^m alkiota.*

Todistus On selvää, että F_q:n alikunta K on kertalukua p^m jollain positiivisella kokonaisluvulla $m \leq n$. Lauseen 4.1 mukaan $q = p^n$:n tulee olla p^m:n potenssi, jolloin m on välttämättä alkion n jakaja.
Kääntäen, jos m on alkion n positiivinen jakaja, niin $p^m - 1$ jakaa $p^n - 1$:n ja täten $x^{p^m-1} - 1$ jakaa $x^{p^n-1} - 1$:n polynomirenkaassa $F_p[x]$. Tällöin $x^{p^m} - x$

jakaa $x^{p^n} - x = x^q - x$:n $F_p[x]$:ssä. Nyt jokainen $x^{p^m} - x$:n juuri on myös $x^q - x$:n juuri ja täten F_q sisältää kyseisen juuren. Tästä seuraa, että F_q:n tulee alikuntana sisältää $(x^{p^n} - x)$:n hajoamiskunta yli F_p:n ja tällöin, kuten lauseen 4.5 todistuksessa, hajoamiskunnan kertaluku on p^m. Jos F_p:ssä olisi kaksi eri alikuntaa kertalukua p^m, ne yhdessä sisältäisivät enemmän kuin p^m polynomin $x^{p^m} - x$ juurta F_q:ssa, mikä olisi ristiriita. □

Lauseen 4.6 todistus osoittaa, että F_{p^n}:n kertalukua p^m (m on n:n positiivinen jakaja) oleva yksikäsitteinen alikunta koostuu täsmälleen polynomin $x^{p^m} - x \in F_p[x]$ juurista F_{p^n}:ssä.

Määritellään äärelliselle kunnalle F_q merkintä F_q^*, millä tarkoitetaan F_q:n nollasta eroavien alkioiden ryhmää kertolaskun suhteen.

Lause 4.7 *Ryhmä F_q^* on syklinen.*

Todistus Tapaus $q = 2$ on triviaali, joten voidaan olettaa, että $q \geq 3$. Olkoon $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ ryhmän F_q^* kertaluvun $h = q-1$ jako alkutekijöihin. Jokaiselle i, $1 \leq i \leq m$, polynomilla $x^{h/p_i} - 1$ on korkeintaan h/p_i juurta F_q:ssa. Koska $h/p_i < h$, niin F_q:ssa on nollasta eroavia alkioita, jotka eivät ole tämän polynomin juuria. Olkoon a_i tällainen alkio ja olkoon $b_i = a_i^{h/p_i^{r_i}}$. Tällöin $b_i^{p_i^{r_i}} = 1$, koska b_i:n kertaluku on $p_i^{r_i}$:n jakaja ja se on tällöin muotoa $p_i^{s_i}$, missä $0 \leq s_i \leq r_i$. Toisaalta

$$b_i^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1,$$

joten b_i on kertalukua $p_i^{r_i}$. Nyt voidaan tehdä väitös, että alkio $b = b_1 b_2 \cdots b_m$ on kertalukua h. Tehdään vastaoletus, että b:n kertaluku on h:n jakaja ja jakaa tällöin myös ainakin yhden kokonaisluvun h/p_i, $1 \leq i \leq m$. Merkitään tätä kokonaislukua h/p_1. Tällöin

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1}.$$

Nyt, jos $2 \leq i \leq m$, niin $p_i^{r_i}$ jakaa h/p_1:sen ja tällöin $b_i^{h/p_1} = 1$. Nyt $b_1^{h/p_1} = 1$. Tällöin taas b_1:n kertaluvun tulee jakaa h/p_1, mikä on mahdotonta, koska b_1:n kertaluku on $p_1^{r_1}$. Täten ryhmä F_q^* on syklinen ja sen generaattori on b. □

Määritelmä 4.2 *Syklisen ryhmän F_q^* generaattoria kutsutaan F_q:n primitiivialkioksi.*

Lause 4.8 *Olkoot F_q äärellinen kunta ja F_r äärellinen kuntalaajennus. Tällöin F_r on F_q:n yksinkertainen algebrallinen laajennus ja jokainen F_r:n primitiivialkio on F_r:n määräävä alkio yli F_q:n.*

Todistus Olkoon ζ F_r:n primitiivialkio. Tällöin selvästi $F_q(\zeta) \subseteq F_r$. Toisaalta $F_q(\zeta)$ sisältää alkion 0 ja kaikki ζ:n potenssit ja täten myös kaikki F_r:n alkiot. Siis $F_r = F_q(\zeta)$. □

Lause 4.9 *Jokaista äärellistä kuntaa F_q ja jokaista positiivista kokonaislukua n kohti on olemassa $F_q[x]$:n jaoton polynomi, joka on astetta n.*

Todistus Olkoon F_r F_q:n kertalukua q^n oleva kuntalaajennus siten, että $[F_r : F_q] = n$. Nyt lauseen 4.8 mukaan $F_r = F_q(\zeta)$ jollain $\zeta \in F_r$. Tällöin ζ:n minimipolynomi yli F_q:n on $F_q[x]$:n jaoton polynomi ja se on astetta n lauseen 3.2 kohdan 1. ja lauseen 3.5 kohdan 2. mukaan. □

4.2 Kryptologiaa ja sen historiaa

Äärellisiä kuntia kutsutaan usein myös Galois'n kunniksi ranskalaisen matemaatikon Evariste Galois'n (1811-1832) mukaan. Hän oli ensimmäinen matemaatikko, joka tutki täysin yleisesti äärellisiä kuntia. Viime aikoina äärellisten kuntien tutkimus on jälleen yleistynyt, koska sillä on useita tärkeitä sovellusalueita, kuten koodausteoria tiedonsiirron salaamiseksi esimerkiksi matkapuhelinliikenteessä.
([2], s. 175)

Tietoverkkojen käyttö on levinnyt monille eri aloille nyky-yhteiskunnassa. Yksi tärkeä ala on kaupankäynti. Kun käydään elektronista kaupankäyntiä verkon välityksellä, on tietoturva tärkeässä osassa. Salakirjoitusmenetelmillä saadaan estettyä luottamuksellisten tietojen leviäminen vääriin käsiin kun

viestejä välitetään verkossa. Niillä turvataan myös tietojen eheys ja luottamuksellisuus.

Erilaisia salakirjoitusmenetelmiä on käytetty viestien salaamiseen jo muinaisen Egyptin ja Rooman ajoilta lähtien. Menetelmät ovat kehittyneet aikojen saatossa ja myöhemmin kehittyi tieteenala kryptologia, joka tutkii salakirjoitusta. Muinaisen Egyptin salakirjoitusmenetelmä oli tavallisesta poikkeavien hieroglyfien käyttö kirjoituksessa. Yksi historiallisesti tunnettu salausmenetelmä on Gaius Julius Caesarin kehittämä Caesarin systeemi.
(Vrt. [2], s. 52)

Määritelmä 4.3 *Kun luku a jaetaan jakoyhtälön mukaisesti luvulla* $m(>0)$*, niin saadaan*

$$a = qm + r,$$

missä $0 \leq r < m$*. Lukua* r *sanotaan jäännökseksi ja tarkemmin jäännökseksi modulo* m*. Tätä merkitään* $r = a(\mathrm{mod} m)$*.*

Kryptologia tutkii systeemejä, joiden avulla muunnetaan kaikkien osapuolten ymmärtämä sanoma sellaiseen muotoon, jonka ymmärtävät vain ne, jotka pystyvät purkamaan salakirjoituksen. Alkuperäistä selväkielistä viestiä sanotaan selvätekstiksi ja se salaataan eli kryptataan kryptotekstiksi.
Viestin vastaanottaja dekryptaa kryptotekstin, jolloin hän saa viestin jälleen selvätekstiksi.

Caesarin systeemissä selväteksti koostuu kirjainjonoista, jotka aluksi muutetaan lukujonoiksi niin, että jokainen kirjain $(A, \ldots, Z)$ muutetaan luvuiksi siten, että $A \leftarrow 0, \ldots, Z \leftarrow 25$. Olkoon nyt p jokin selvätekstin luku $(0 \leq p \leq 25)$ ja merkitään vastaavaa kryptotekstin lukua $f(p)$. Kryptaaminen Caesarin systeemissä muodostetaan kirjaimittain kaavalla

$$f(p) = (p + 3) \bmod 26$$

ja täten $f(p) \in \{0, 1, \ldots, 25\}$.

Esimerkki 4.1 Kryptataan sana TOMMI.

$$TOMMI \rightarrow 19 \quad 14 \quad 12 \quad 12 \quad 8 \rightarrow 22 \quad 17 \quad 15 \quad 15 \quad 11 \rightarrow WRPPL.$$

Dekryptaaminen Caesarin systeemissä tapahtuu kaavalla

$$p = (f(p) - 3) \bmod 26.$$

Esimerkki 4.2 Dekryptataan sana HQG.

$$HQG \leftarrow 7 \quad 16 \quad 6 \leftarrow 4 \quad 13 \quad 3 \leftarrow END.$$

Eräs toinen salausmenetelmä on tietoverkkojen, erityisesti internetin, tiedon siirron turvaamiseen käytetty Diffie-Hellman -avaimenvaihtoprotokolla. Se julkaistiin vuonna 1976. Protokolla perustuu osapuolien yhteiseen salaisuuteen. Tällöin sitä voidaan käyttää viestien salaamiseen perinteisillä salausmenetelmillä.
Protokolla käyttää kokonaislukujen jäännösluokkarenkaan multiplikatiivista ryhmää modulo jokin alkuluku p kertolaskun suhteen ja sen primitiivistä alkiota g. Osapuolet sopivat käytettävästä äärellisestä syklisestä ryhmästä G ja sen generoivasta alkiosta g. Osapuoli A valitsee satunnaisen luonnollisen luvun a ja laskee ryhmän G alkion g^a, ja lähettää sen osapuolelle B. Osapuoli B valitsee myös satunnaisen luonnollisen luvun b, laskee G:n alkion g^b, ja lähettää sen A:lle. Tämän jälkeen osapuoli A laskee ryhmän G alkion $(g^b)^a$ ja B laskee G:n alkion $(g^a)^b$. Ryhmän G alkiot $(g^b)^a$ ja $(g^a)^b$ ovat keskenään yhtäsuuret, koska ryhmässä on voimassa assosiatiivisuus. Nyt molemmat osapuolet tietävät alkion g^{ab}, joka toimii heidän salaisena avaimenaan.

Esimerkki 4.3 (Vrt. [5])
Aarne ja Bertta sopivat käyttävänsä alkulukua $p = 23$ ja primitiivistä alkiota $g = 5$. Aarne valitsee kokonaisluvun $a = 6$ ja lähettää Bertalle luvun $g^a \bmod p$, joka on 8, sillä $5^6 \bmod 23 = 8$. Bertta valitsee kokonaisluvun $b = 15$ ja lähettää Aarnelle luvun 19 ($5^{15} \bmod 23 = 19$). Tämän jälkeen Aarne laskee luvun $(g^b \bmod p)^a \bmod p$ eli $19^6 \bmod 23 = 2$. Samaan tapaan Bertta laskee luvun $(g^a \bmod p)^b \bmod p$ eli $8^{15} \bmod 23 = 2$. Nyt Aarne ja Bertta ovat saaneet saman luvun, koska g^{ab} ja g^{ba} ovat yhtäsuuret. Täten siis ainoastaan luvut a, b, g^{ab} ja g^{ba} ovat salassa pidettäviä.

Edellisessä esimerkissä oli siis kyse salaisen avaimen vaihtamisesta, eikä niinkään itse viestin vaihtamisesta.
Käytännössä luvuiksi a, b ja p valittaisiin paljon suuremmat luvut. Jos alkuluku p olisi yli 300 numeroinen ja a ja b yli 100 numeroisia lukuja, niin tällä hetkellä tunnetut algoritmit eivät pystyisi lukujen a ja b laskemiseen vaikka tiedettäisiin luvut $g, p, g^a \bmod p$ ja $g^b \bmod p$. Huomattavaa on, että luvun g ei tarvitse olla suuri, yleensä käytetään arvoja 2 tai 5.

Kirjallisuutta

[1] Bland, P.E.: The Basics of Abstract Algebra.
W.H. Freeman and Company, 2001.

[2] Hardy, D., Walker, C.: Applied algebra: codes, ciphers and discrete algorithms.
Pearson Education Inc., 2003.

[3] Metsänkylä, T., Näätänen, M. : Algebra.
Limes ry, 2003.

[4] Lidl, R., Niederreiter, H.: Finite Fields.
Cambridge University Press, 1997.

[5] http://en.wikipedia.org/wiki/Diffie-Hellman