Algebrallisesti suljetuista kunnista

Tutkielma kurssilla *Äärellisulotteinen lineaarialgebra*

Tekijä: Kaisa Pohjonen

Tämä tutkielma käsittelee kuntien algebrallisia laajennoksia, erityisesti kuntien algberallisia sulkeumia. Ensimmäiseen osaan on koottu tutkielmassa tarvittavia esitietoja. Toisessa osassa käsitellään algebrallisten laajennosten teoriaa ja todistetaan, että jokaisella kunnalla on algebrallinen sulkeuma. Kolmannessa osassa käsitellään esimerkkinä kompleksilukujen kuntaa ja osoitetaan, että se on algebrallisesti suljettu.

1. Algebrallisia esitietoja

Tässä osassa käsitellään sellaisia algebrallisia määritelmiä ja tuloksia, joita tarvitaan tutkielmassa myöhemmin. Käsiteltäviä aihealueita ovat ideaalit ja tekijärenkaat, usean muuttujan polynomialgebrat, yleiset kuntalaajennokset sekä algebralliset laajennokset ja minimipolynomit. Osa seuraa Häsän ja Suomisen esityksiä [1, 4].

1.1. Ideaalit ja tekijärenkaat.

Määritelmä 1.1. Olkoon R vaihdannainen rengas ja I jokin sen additiivisen ryhmän aliryhmä. Tällöin I on renkaan R *ideaali*, jos kaikilla $r \in R$ pätee $rI = Ir = I$.

Esimerkki 1.2. Olkoon $R = \mathbb{Z}$. Tällöin kaikki sen ideaalit ovat muotoa $n\mathbb{Z}$ jollain luonnollisella luvulla n, ja kaikki tätä muotoa olevat osajoukot ovat ideaaleja.

Renkaan ideaali on samantyyppinen konstruktio kuin ryhmän normaali aliryhmä. Erityisesti ideaalin sivuluokat muodostavat alkuperäisen renkaan tekijärenkaan.

Lause 1.3. *Olkoon R vaihdannainen rengas ja I sen ideaali. Tällöin ideaalin I sivuluokat $r + I$ muodostavat renkaan R/I, yhteenlaskuna $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ ja kertolaskuna $(r_1 + I)(r_2 + I) = (r_1 r_2) + I$. Tätä rengasta kutsutaan renkaan R* tekijärenkaaksi. □

Yksi ideaalien alaluokka on maksimaaliset ideaalit.

Määritelmä 1.4. Renkaan R ideaali I on *maksimaalinen*, jos $I \neq R$ eikä ole olemassa renkaan R ideaalia J, jolle pätisi $I \subsetneq J \subsetneq R$.

Esimerkki 1.5. Olkoon K kunta, jolloin polynomialgebra $K[X]$ on rengas. Tällöin jokaisen jaottoman polynomin $p \in K[X]$ virittämä ideaali $\langle p \rangle$ on maksimaalinen.

Maksimaaliset ideaalit ovat kiinnostavia, sillä niiden avulla voidaan konstruoida kuntia.

Lause 1.6. *Olkoon R rengas ja I sen ideaali. Tällöin ideaali I on maksimaalinen, jos ja vain jos tekijärengas R/I on kunta.* □

Edellisen lauseen jälkeen kiinnostava kysymys on, onko kaikilla renkailla ainakin yksi maksimaalinen ideaali. Varsinainen Krullin lause sanoo, että tämä on totta jokaisella epätriviaalilla renkaalla. Sen todistus perustuu Zornin lemmaan, joka antaa maksimaalisen alkion ketjussa, jonka muodostavat renkaan aidot ideaalit sisältymisen suhteen. Lauseesta voidaan osoittaa seurauksena seuraava lause, jota toisinaan myös näkee kutsuttavan Krullin lauseeksi.

Lause 1.7 (Krullin lause)**.** *Olkoon R rengas ja I sen aito ideaali. Tällöin on olemassa maksimaalinen ideaali M, joka sisältää ideaalin I.* □

Seuraava esimerkki havainnollistaa lauseita 1.6 ja 1.7.

Esimerkki 1.8. Olkoon rengas $R = \mathbb{Z}$. Kuten esimerkissä 1.2 todettiin, kaikki sen ideaalit ovat muotoa $n\mathbb{Z}$ jollain luonnollisella luvulla n.

Tutkitaan renkaan $\mathbb{Z}$ maksimaalisia ideaaleja. Olkoot $M = m\mathbb{Z}$ ja $N = n\mathbb{Z}$ ideaalit, joille pätee $M \subseteq N \subseteq \mathbb{Z}$. Koska M sisältää kaikki luvulla m jaolliset kokonaisluvut ja N kaikki luvulla n jaolliset kokonaisluvut, eli kaikki luvulla n jaolliset kokonaisluvut ovat jaollisia myös luvulla m, täytyy päteä $m \mid n$. Osoitetaan, että ideaali M on maksimaalinen täsmälleen silloin, kun m on alkuluku.

Jos m on alkuluku, pätee $m \geq 2$ eli M on aito ideaali. Lisäksi luvun m ainoat tekijät ovat 1 ja m, eli ainoat ideaalit N, jolle pätee $M \subseteq N \subseteq \mathbb{Z}$, ovat $N = 1\mathbb{Z} = \mathbb{Z}$ ja $N = m\mathbb{Z} = M$. Täten M on maksimaalinen ideaali.

Toisaalta jos m ei ole alkuluku, voidaan kirjoittaa $m = kl$, missä $k, l \in \mathbb{N}$ ja $1 < k, l < m$. Tällöin ideaali $k\mathbb{Z}$ on aito ja lisäksi M sisältyy aidosti ideaaliin $k\mathbb{Z}$. (Sisältyvyys on aito, koska esimerkiksi $k \notin M$.)

Niinpä renkaan $\mathbb{Z}$ maksimaaliset ideaalit ovat täsmälleen ne ideaalit $p\mathbb{Z}$, missä p on alkuluku. Tämä on linjassa lauseen 1.6 kanssa, sillä tunnetusti tekijärengas $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ on kunta, jos ja vain jos n on alkuluku.

Mikäli $n > 1$ ja n ei ole alkuluku, luvulla n on alkulukuesitys $n = p_1^{e_1} \cdots p_k^{e_k}$, missä kukin p_i on eri alkuluku. Tällöin esimerkiksi p_1 jakaa luvun n, eli pätee $n\mathbb{Z} \subseteq p_1\mathbb{Z}$. Nyt koska $n > 1$, ideaali $n\mathbb{Z}$ on aito, ja koska p_1 on alkuluku, ideaali $p_1\mathbb{Z}$ on maksimaalinen. Siis saatu tulos on linjassa Krullin lauseen 1.7 kanssa.

Luvun n alkulukuesitys osoittaa, että Krullin lauseen takaama maksimaalinen ideaali ei välttämättä ole yksikäsitteinen. Ideaali $n\mathbb{Z}$ nimittäin sisältyy luvun n jokaisen alkulukutekijän virittämään maksimaaliseen ideaaliin. Tärkeää kuitenkin on, että aina on olemassa *jokin* maksimaalinen ideaali, johon aito ideaali sisältyy.

1.2. **Usean muuttujan polynomialgebrat.** Tässä kappaleessa yleistetään yhden muuttujan polynomialgebra $K[X]$ usean muuttujen polynomialgebraksi $K[(X_i)_{i\in I}]$.

Olkoon I mielivaltainen indeksijoukko ja $M = \mathbb{N}^{(I)}$ joukko, joka koostuu jonoista $\nu = (\nu_i)_{i\in I}$, joissa $\nu_i \in \mathbb{N}$ kaikilla $i \in I$ ja $\nu_i \neq 0$ vain äärellisen monella indeksillä $i \in I$. (Tässä tutkielmassa $0 \in \mathbb{N}$.) Joukossa M voidaan määritellä yhteenlasku komponenteittain. Tällöin joukolla M on vapaa virittäjäjoukko $(\delta_i)_{i\in I}$, jossa $\delta_i = (0, \ldots, 1, 0, \ldots)$, missä 1 on i:nnellä paikalla.

Olkoon sitten K kunta ja $P_K(I) = K^{(M)}$ joukon M algebra kunnan K suhteen. Sillä on kanta $(e^\nu)_{\nu\in M}$, ja sen alkiot ovat lineaarikombinaatiot $\sum_{\nu\in M} c_\nu e^\nu$, missä $(c_\nu)_{\nu\in M}$ on äärelliskantajainen perhe kunnan K alkioita. Algebran kertolasku määräytyy kanta-alkioiden kertolaskusta $e^\nu e^\mu = e^{\nu+\mu}$.

Nyt joukon M kanta-alkiot vastaavat usean muuttujen polynomialgebran muuttujia, joten merkitään $\delta_i = X_i$, ja joukon M alkiot polynomialgebran monomeja: $X^\nu = \prod_{i\in I} X_i^{\nu_i}$. Monomin aste on $|\nu| = \sum_{i\in I} \nu_i$, joka on hyvinmääritelty, sillä $\nu_i \neq 0$ vain äärellisen monella $i \in I$.

Tällöin polynomialgebran kanta voidaan kirjoittaa $(X^\nu)_{\nu\in M}$ ja kukin algebran alkio $p = \sum_{\nu\in M} c_\nu X^\nu$, missä $(c_\nu)_{\nu\in M}$ on äärelliskantajainen perhe kunnan K alkioita. Nyt algebra $P_K(I)$ koostuu K-kertoimisista polynomeista muuttujien X_i suhteen, eli $P_K(I) = K[(X_i)_{i\in I}]$. Polynomin $p = \sum_{\nu\in M} c_\nu X^\nu \in K[(X_i)_{i\in I}]$, $p \neq 0$ aste $\deg(p)$ on suurin niiden monomien X^ν asteista $|\nu|$, joiden kertoimet $c_\nu \neq 0$. Nollapolynomin aste on tuttuun tapaan $-\infty$.

Algebran $K[(X_i)_{i\in I}]$ ykkösalkio on X^0. Koska kunta K on myös K-algebra ja kanoninen algebrahomomorfismi $K \to K[(X_i)_{i\in I}]$, $c \mapsto cX^0$ on injektio, niin kunta K voidaan samastaa vakiopolynomien kanssa. Koska kunnan ykkösalkio kuvautuu algebran ykkösalkioksi, saadaan siis samastus huomioiden $1 = X^0$.

Kuten yhden muuttujen polynomeille, myös usean muuttujen polynomeille pätee universaalisuus:

Lause 1.9. *Olkoon K kunta, A ykkösellinen K-algebra ja $(x_i)_{i\in I}$ perhe algebran A alkioita. Tällöin on olemassa yksikäsitteinen algebrahomomorfismi $S_x : K[(X_i)_{i\in I}] \to A$, jolle pätee $S_x(X_i) = x_i$ kaikilla $i \in I$.*

Tätä homomorfismia kutsutaan sijoitushomomorfismiksi *ja polynomin $p = \sum_{\nu\in M} c_\nu X^\nu = \sum_{\nu\in M} c_\nu \prod_{i\in I} X_i^{\nu_i}$ arvo homomorfismissa on $S_x(p) = \sum_{\nu\in M} c_\nu \prod_{i\in I} x^{\nu_i}$, missä $\nu = (\nu_i)_{i\in I}$. Tätä arvoa merkitään myös $p((x_i)_{i\in I})$.* □

1.3. **Kuntalaajennokset.**

Määritelmä 1.10. Olkoon K kunta. Tällöin kunta L on sen *laajennos*, jos K on kunnan L alikunta. Laajennosta merkitään L/K.

Laajennoksen L/K *aste* $[L : K]$ on kunnan L dimensio K-vektoriavaruutena. Jos laajennoksen aste on äärellinen, laajennosta kutsutaan *äärelliseksi laajennokseksi*. Muussa tapauksessa kyseessä on *ääretön laajennos*.

Esimerkki 1.11.
(1) Reaalilukujen kunta $\mathbb{R}$ on rationaalilukujen kunnan $\mathbb{Q}$ ääretön laajennos.
(2) Kompleksilukujen kunta $\mathbb{C}$ on reaalilukujen kunnan $\mathbb{R}$ äärellinen laajennos, $[\mathbb{C} : \mathbb{R}] = 2$.

Määritelmä 1.12. Olkoot K kunta ja L_1 sekä L_2 sen laajennoksia. Tällöin laajennosten L_1/K ja L_2/K sanotaan olevan isomorfiset, jos on olemassa isomorfismi $\theta : L_1 \to L_2$, joka kiinnittää alikunnan K: $\theta(K) = K$.

Määritelmä 1.13. Olkoot K kunta, L sen laajennos ja $A \subseteq L$. Tällöin joukon A virittämä laajennoksen L/K alirengas $K[A]$ on pienin kunnan L alirengas, johon sisältyy sekä kunta K että joukko A.

Vastaavasti joukon A virittämä laajennoksen L/K alilaajennos $K(A)$ on pienin kunnan L alikunta, johon sisältyy sekä kunta K että joukko A.

1.4. **Algebralliset laajennokset ja minimipolynomit.**

Määritelmä 1.14. Olkoot K kunta, L sen laajennos ja $x \in L$. Alkiota x sanotaan *algebralliseksi* kunnan K suhteen, jos on olemassa jokin (nollasta poikkeava) polynomi $p \in K[X]$, jolle pätee $p(x) = 0$. Jos luku ei ole algebrallinen, se on *transkendenttinen* kunnan K suhteen.

Jos kaikki laajennoksen L alkiot ovat algebrallisia kunnan K suhteen, sanotaan, että kunta L on algebrallinen kunnan K suhteen. Tällöin laajennosta L/K kutsutaan *algebralliseksi laajennokseksi*.

Määritelmä 1.15. Olkoon alkio $x \in L$ algebrallinen kunnan K suhteen. Tällöin alkion x *minimipolynomi* kunnan K suhteen on sellainen (nollasta poikkeava) pääpolynomi $p \in K[X]$, jolle pätee $p(x) = 0$ ja jonka aste on pienin mahdollinen. Minimipolynomia merkitään $p = \min(K, x)$.

Esimerkki 1.16.
(1) Luku $\sqrt{2}$ on algebrallinen kunnan $\mathbb{Q}$ suhteen, sillä se on polynomin $X^2 - 2$ juuri. Tällä polynomilla ei ole ensimmäisen asteen tekijöitä algebrassa $\mathbb{Q}[X]$, joten sen on oltava jaoton. Niinpä se on luvun $\sqrt{2}$ minimipolynomi. Saman luvun minimipolynomi kunnan $\mathbb{R}$ on suhteen on $\min(\mathbb{R}, \sqrt{2}) = X - \sqrt{2}$. Yleisesti kaikki kunnan K alkiot ovat algebrallisia kunnan K suhteen.

(2) Luku i on algebrallinen kunnan $\mathbb{R}$ suhteen, sillä se on polynomin $X^2 + 1$ juuri. Koska polynomilla ei voi olla ensimmäisen asteen tekijöitä algebrassa $\mathbb{R}[X]$, se on jaoton ja siten luvun i minimipolynomi.

Muutamia hyödyllisiä ja myöhemmin tarvittavia tuloksia minimipolynomeista on koottu seuraavaan lauseeseen, jota ei todisteta tässä tutkielmassa tilan puutteen vuoksi.

Lause 1.17. *Olkoon K kunta, L sen laajennos ja $a \in L$ algebrallinen kunnan K suhteen. Tällöin seuraavat väitteet ovat voimassa:*

(1) Minimipolynomi $\min(K, a)$ on jaoton algebrassa $K[X]$
(2) Jos $p \in K[X]$, niin $p(a) = 0$, jos ja vain jos $\min(K, a)$ jakaa polynomin p
(3) $K[a]$ on kunta, ja $K[a] = K(a)$
(4) Jos polynomin $\min(K, a)$ aste on n, niin alkiot $1, a, \ldots, a^{n-1}$ muodostavat laajennoksen $K(a)$ kannan. Tällöin siis $[K(a) : K] = n$.

Todistus. Katso esimerkiksi [1, s. 99]. □

2. Kuntien algebrallisista sulkeumista

Tämä osa seuraa Häsän ja Suomisen esityksiä [1, 4].

2.1. **Juurikunnat.** Polynomien juuria ja tekijöitä tarkasteltaessa riittää tutkia pääpolynomeja, sillä polynomin $p \in K[X]$ juuret eivät muutu, jos polynomi kerrotaan vakiolla $a \in K$, $a \neq 0$. Erityisesti siis jos a_n on polynomin p johtava kerroin (jolloin $a_n \neq 0$), niin polynomeilla p ja $q = \frac{p}{a_n}$ on samat juuret.

Polynomilla $p \in K[X]$ ei välttämättä ole juuria kunnassa K. Seuraavaksi tutkitaan kunnan K laajennoksia, jotka sisältävät haluttujen polynomien juuret. Yleisesti ottaen tällainen laajennos ei tietenkään ole yksikäsitteinen, mutta jos sitä rajoitetaan ehdolla, että se ”ei sisällä mitään ylimääräistä” haluttujen polynomien juurien lisäksi, saadaan käsitteestä hyvinmääritelty.

Määritelmä 2.1. Olkoon K kunta ja $(p_i)_{i \in I}$ perhe algebran $K[X]$ polynomeja. Perheen *juurikunta* kunnan K suhteen on laajennos L/K, joka toteuttaa seuraavat ehdot:

(1) Jokainen p_i jakautuu ensimmäisen asteen polynomien tuloksi algebrassa $L[X]$
(2) $L = K(\bigcup_{i \in I} A_i)$, missä joukko A_i koostuu polynomien p_i juurista

Esimerkki 2.2. (1) Polynomin $X^2 - 2$ juurikunta kunnan $\mathbb{Q}$ suhteen on $\mathbb{Q}(\sqrt{2})$. Polynomilla on kaksi juurta $\sqrt{2}$ ja $-\sqrt{2}$, joista jälkimmäinen kuuluu laajennokseen $\mathbb{Q}(\sqrt{2})$. Niinpä pätee

$\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ ja polynomi $X^2 - 2$ jakautuu ensimmäisen asteen polynomien tuloksi laajennoksessa $\mathbb{Q}(\sqrt{2})$.

(2) Vastaavalla tavalla voidaan osoittaa, että polynomin $X^2 + 1$ juurikunta kunnan $\mathbb{R}$ suhteen on $\mathbb{R}(i)$.

Seuraavat kaksi lausetta takaavat, että riippumatta kunnasta ja valituista polynomeista juurikunta on aina olemassa ja se on lisäksi isomorfiaa vaille yksikäsitteinen. Tässä tutkielmassa todistetaan tilan puutteen vuoksi vain juurikunnan olemassaolo.

Lause 2.3. *Olkoon K kunta ja $(p_i)_{i\in I}$ perhe algebran $K[X]$ polynomeja, jotka eivät ole vakioita. Tällöin on olemassa perheen $(p_i)_{i\in I}$ juurikunta.*

Todistus. Voidaan olettaa, että jokainen p_i on pääpolynomi. Lisäksi voidaan olettaa, että $I \neq \emptyset$, sillä jos $I = \emptyset$, niin juurikunta on K itse.

Osoitetaan väite todeksi kolmessa osassa: kun perheessä on vain yksi polynomi, kun perheessä on äärellinen määrä polynomeja ja kun perheessä on ääretön määrä polynomeja.

Oletetaan siis ensin, että perheessä on vain yksi polynomi p, ja osoitetaan juurikunnan olemassaolo induktiolla tämän polynomin asteen $n \geq 1$ suhteen. Jos $n = 1$, on polynomi $p = X - a$ jollain $a \in K$ ja juurikunta $E = K(a) = K$.

Kun $n > 1$, valitaan jokin polynomin p jaoton tekijä $q \in K[X]$. Polynomin q virittämä ideaali $\langle q \rangle$ on maksimaalinen, joten tekijäalgebra $L = K[X]/\langle q \rangle$ on kunta. Kunta K voidaan samastaa erääseen kunnan L alikuntaan (vakiopolynomien sivuluokat), joten L on kunnan K laajennos. Merkitään $a = \overline{X}$. Kanoninen projektio on homomorfismi, joten koska polynomeissa on vain tuloja ja summia, $r(\overline{X}) = \overline{r(X)}$ kaikilla $r \in L$. Erityisesti siis $q(a) = q(\overline{X}) = \overline{q(X)} = 0$. Niinpä a on polynomin q ja siten myös polynomin p juuri, ja p voidaan kirjoittaa tulona $p = (X - a)r$ jollain $r \in L[X]$. Nyt polynomin r aste on $n - 1$, joten induktio-oletuksen nojalla on olemassa kunnan L laajennos M, joka on polynomin r juurikunta. Tällöin siis r voidaan kirjoittaa algebrassa $M[X]$ tulona

$$r \prod_{i=1}^{n-1} (X - a_i),$$

ja kunta M voidaan kirjoittaa laajennoksena $M = L(a_1, \ldots, a_{n-1})$. Jos lisäksi merkitään $a_0 = a$, voidaan polynomi p kirjoittaa algebrassa $M[X]$ tulona

$$p = \prod_{i=0}^{n-1} (X - a_i).$$

Lisäksi $L = K(a_0)$, joten $M = K(a_0)(a_1, \ldots, a_{n-1}) = K(a_0, \ldots, a_{n-1})$, joten M on polynomin p juurikunta.

Oletetaan seuraavaksi, että perheessä on äärellinen määrä polynomeja. Tällöin voidaan muodostaa tulo

$$p = \prod_{i \in I} p_i \in K[X],$$

joka ei ole vakio ja jonka juuret ovat täsmälleen polynomien p_i juuret. Edellä esitetyn nojalla polynomilla p on juurikunta M, joka on siten myös perheen $(p_i)_{i \in I}$ juurikunta.

Oletetaan viimeiseksi, että indeksijoukko I on ääretön. Osoitetaan ensin, että kunnalla K on laajennos L, jossa kullakin polynomilla p_i on jokin (yksi) juuri. Tätä varten tarkastellaan polynomialgebraa $A = K[(X_i)_{i \in I}]$. Kuhunkin polynomiin p_i yhdistetään algebran A polynomi $p_i(X_i)$. Olkoon $a = \langle (p_i(X_i))_{i \in I} \rangle \subset A$ perheen $(p_i(X_i))_{i \in I}$ virittämä ideaali. Näytetään, että se on aito.

Jos $1 \in a$, se voidaan kirjoittaa muodossa

$$1 = \sum_{j \in J} n_j p_j(X_j), \tag{1}$$

missä $J \subset I$ on äärellinen ja $n_j \in A$. Edellä esitetyn nojalla äärellisellä perheellä $(p_j)_{j \in J}$ on juurikunta E. Siis kullakin $j \in J$ on olemassa sellainen $x_j \in E$, että $p_j(x_j) = 0$. Joukko $(x_i)_{i \in I}$ voidaan täydentää mielivaltaisilla alkioilla $x_i \in E$, kun $i \in I \setminus J$. Kun arvot x_i sijoitetaan yhtälöön (1), saadaan yhtälö

$$1 = \sum_{j \in J} n_j((x_i)_{i \in I}) p_j(x_j) = 0.$$

Tämä on ristiriita, joten täytyy päteä $1 \notin a$ eli $a \neq A$.

Koska a on aito ideaali, Krullin lauseen nojalla se sisältyy johonkin algebran A maksimaaliseen ideaaliin m. Tällöin tekijäalgebra $K_1 = A/m$ on kunta ja lisäksi K sisältyy siihen, joten K_1 on kunnan K laajennos. Koska polynomit $p_i(X_i)$ sisältyvät ideaaliin m, luokat $x_i = \overline{X_i} \in L$ toteuttavat ehdot $p_i(x_i) = 0$. Niinpä ne ovat algebrallisia kunnan K suhteen ja laajennos K_1 on niiden virittämä: $K_1 = K[(x_i)_{i \in I}] = K((x_i)_{i \in I})$.

Polynomit p_i voidaan siis kirjoittaa tuloina $p_i = (X - x_{i1})p_{1i}$, missä $x_{i1} = x_i \in K_1$ ja $p_{1i} \in K_1[X]$. Jos polynomin p_i aste on 1, polynomi p_{1i} on vakio ($p_{1i} = 1$, koska p_i on pääpolynomi). Toistetaan konstruktio niillä polynomeilla p_{1i}, jotka eivät ole vakioita.

Tällöin saadaan jono laajennoksia $K \subset K_1 \subset K_2 \subset \cdots$, joissa polynomit p_i hajoavat seuraavanlaisiksi tuloiksi:

(1) Jos $\deg(p_i) > n$, niin

$$p_i = \prod_{k=1}^{n} (X - x_{ik}) p_{ni},$$

missä $x_{ik} \in K_k$ ja $p_{ni} \in K_n[X]$

(2) Jos $\deg(p_i) = m \leq n$, niin

$$p_i = \prod_{k=1}^{m} (X - x_{ik}),$$

missä $x_{ik} \in K_k$.

Lisäksi jokaisen kunnan K_n virittää ne polynomien p_i juuret x_{ik}, joilla $1 \leq k \leq \min\{n, \deg(p_i)\}$. Tällöin perheen $(p_i)_{i \in I}$ juurikunta on yhdiste

$$L = \bigcup_{n \in \mathbb{N}} K_n.$$

□

Juurikuntien merkittävin ominaisuus on se, että ne ovat isomorfiaa vaille yksikäsitteisiä. Tästä seuraa myöhemmin myös algebrallisten sulkeumien yksikäsitteisyys. Tulos perustuu siihen, että polynomien hajotus ensimmäisen asteen tekijöihin on yksikäsitteinen. Isomorfismi kuvaa tällöin polynomin juuret yhdessä juurikunnassa sen juuriksi toisessa juurikunnassa.

Lause 2.4. *Olkoon K kunta ja $(p_i)_{i \in I}$ perhe algebran $K[X]$ polynomeja, jotka eivät ole vakioita. Olkoot L_1 ja L_2 kunnan K laajennoksia, jotka kumpikin ovat perheen $(p_i)_{i \in I}$ juurikuntia. Tällöin $L_1 \simeq L_2$.*

Todistus. Katso esimerkiksi [4, s. 133–135]. □

2.2. **Algebrallisesti suljetut kunnat ja algebralliset sulkeumat.** Lopuksi käsittelemme algebrallisesti suljettuja kuntia ja kuntien algebrallisia sulkeumia. Algebrallisesti suljettu kunta sisältää kaikkien polynomiensa juuret, eli sitä ei tarvitse (eikä voi) laajentaa juurikuntien avulla. Lopuksi osoitetaan, että kaikille kunnille voidaan määritellä algebrallinen sulkeuma, joka on kunnan pienin algebrallisesti suljettu laajennos, ja että sulkeuma on isomorfiaa vaille yksikäsitteinen.

Määritelmä 2.5. Olkoon K kunta. Se on *algebrallisesti suljettu*, jos jokaisella algebran $K[X]$ polynomilla, joka ei ole vakio, on ainakin yksi juuri kunnassa K.

Esimerkki 2.6.
(1) Jäljempänä todistetaan, että kompleksilukujen kunta $\mathbb{C}$ on algebrallisesti suljettu.
(2) Algebrallisten lukujen kunta $\mathbb{A} = \{a \in \mathbb{C} \mid a$ on algebrallinen kunnan $\mathbb{Q}$ suhteen $\}$ on algebrallisesti suljettu. (Katso tarkemmin [4, s. 130].)

Algebrallisesti suljettu kunta voidaan karakterisoida monella tapaa. Seuraavassa lauseessa on esitetty neljä keskenään yhtäpitävää määritelmää.

Lause 2.7. *Olkoon K kunta. Tällöin seuraavat ehdot ovat yhtäpitäviä:*
(i) K on algebrallisesti suljettu

(ii) Jokainen algebran $K[X]$ polynomi, joka ei ole vakio, jakautuu ensimmäisen asteen tekijöihin algebrassa $K[X]$
(iii) Jokaisen algebran $K[X]$ jaottoman polynomin aste on 1
(iv) Jokaisen kunnan K algebrallisen laajennoksen aste on 1.

Todistus. $(i) \Rightarrow (ii)$: Olkoon $p \in K[X]$ polynomi, joka ei ole vakio. Osoitetaan induktiolla polynomin p asteen n suhteen, että p on tulo ensimmäisen asteen tekijöistä. Jos $n = 1$, väite on selvä.

Olkoon sitten $n > 1$ ja $a \in K$ jokin polynomin p juuri. Tällöin $p = (X - a)q$, missä $q \in K[X]$ ja $\deg(q) = n - 1$. Induktio-oletuksen nojalla q voidaan esittää tulona

$$q = \prod_{k=1}^{n-1} r_k,$$

missä jokaisen polynomin $r_k \in K[X]$ aste on 1. Asetetaan $r_n = X - a$, jolloin saadaan

$$p = (X - a)q = r_n \prod_{k=1}^{n-1} r_k = \prod_{k=1}^{n} r_k,$$

missä jokaisen tekijän aste on 1.

$(ii) \Rightarrow (iii)$: Olkoon $p \in K[X]$ jaoton. Sillä on siis vain yksi tekijä. Toisaalta oletuksen nojalla tämän tekijän aste on 1. Siis polynomin p aste on 1.

$(iii) \Rightarrow (i)$: Olkoon $p \in K[X]$ polynomi, joka ei ole vakio. Olkoon $q \in K[X]$ sen tekijä, jonka aste on pienin mahdollinen mutta joka ei ole vakio. Tällöin q on jaoton, joten sen aste on 1. Niinpä voidaan kirjoittaa $q = aX + b$, missä $a, b \in K$ ja $a \neq 0$. Nyt $x = -ba^{-1} \in K$ ja $q(x) = 0$. Koska q jakaa polynomin p, sen juuri x on myös polynomin p juuri.

$(iii) \Rightarrow (iv)$: Olkoon L kunnan K algebrallinen laajennos. Tällöin kaikki sen alkiot ovat algebrallisia kunnan K suhteen. Valitaan jokin mielivaltainen $x \in L$ ja olkoon p sen minimipolynomi kunnan K suhteen. Lauseen 1.17 nojalla p on jaoton algebrassa $K[X]$ ja siis oletuksen nojalla ensimmäisen asteen polynomi. Niinpä se voidaan kirjoittaa muodossa $p = X - a$ jollain $a \in K$. Toisaalta koska x on polynomin p juuri, pätee $p(x) = x - a = 0$ eli $x = a$. Siispä täytyy olla $L = K$, jolloin saadaan $[L : K] = 1$.

$(iv) \Rightarrow (iii)$: Olkoon $p \in K[X]$ jaoton polynomi, jonka aste on n. Tällöin sen virittämä ideaali $\langle p \rangle$ on maksimaalinen ja tekijäalgebra $L = K[X]/\langle p \rangle$ kunta, joka on kunnan K laajennos. Merkitään $a = \overline{X}$. Tällöin pätee $p(a) = 0$ ja $L = K(a)$, eli alkio a ja sen virittämä laajennos L ovat algebrallisia kunnan K suhteen.

Koska p on jaoton, se on lauseen 1.17 nojalla vakiokerrointa lukuunottamatta sama kuin alkion a minimipolynomi. Niinpä polynomin p aste n on sama kuin polynomin $\min(K, a)$ aste, joka on sama kuin laajennoksen L aste. Oletuksen nojalla siis $n = 1$. □

Määritelmä 2.8. Olkoon K kunta ja L sen laajennos. Tällöin laajennosta L kutsutaan kunnan K *algebralliseksi sulkeumaksi*, jos se on algebrallisesti suljettu ja algebrallinen kunnan K suhteen.

Esimerkki 2.9. (1) Kompleksilukujen kunta $\mathbb{C}$ on reaalilukujen kunnan $\mathbb{R}$ algebrallinen sulkeuma.
(2) Algebrallisten lukujen kunta $\mathbb{A}$ on rationaalilukujen kunnan $\mathbb{Q}$ algebrallinen sulkeuma.

Lemma 2.10. *Olkoon K kunta ja L sen laajennos. Tällöin L on kunnan K algebrallinen sulkeuma, jos ja vain jos L on algebrallinen kunnan K suhteen sekä jokainen algebran $K[X]$ polynomi, joka ei ole vakio, jakautuu algebrassa $L[X]$ ensimmäisen asteen tekijöihin.*

Todistus. Jos L on kunnan K algebrallinen sulkeuma, jos on määritelmän mukaisesti algebrallinen kunnan K suhteen. Kunta L on lisäksi algebrallisesti suljettu, ja koska $K[X] \subseteq L[X]$, jokainen algebran $K[X]$ polynomi, joka ei ole vakio, jakautuu algebrassa $L[X]$ ensimmäisen asteen tekijöihin.

Oletetaan sitten, että laajennos L on algebrallinen kunnan K suhteen ja että jokainen algebran $K[X]$ polynomi, joka ei ole vakio, jakautuu algebrassa $L[X]$ ensimmäisen asteen tekijöihin. Riittää osoittaa, että kunta L on algebrallisesti suljettu. Käytetään lausetta 2.7: olkoon L' jokin kunnan L algebrallinen laajennos. Osoitetaan, että $[L' : L] = 1$.

Algebrallisuus on transitiivinen ominaisuus [4, s. 124], joten L' on algebrallinen myös kunnan K suhteen. Olkoon $x \in L'$ mielivaltainen alkio ja $p \in K[X]$ sen minimipolynomi. Nyt oletuksen nojalla se voidaan kirjoittaa tulona

$$p = \prod_{i=1}^{n} (X - x_i),$$

missä $x_i \in L$. Koska x on polynomin p juuri, täytyy päteä $x = x_i$ jollain i. Niinpä saadaan $x \in L$ ja $L' = L$, jolloin pätee $[L' : L] = 1$. □

Lause 2.11. *Jokaisella kunnalla on isomorfiaa vaille yksikäsitteinen algebrallinen sulkeuma.*

Todistus. Olkoon $(p_i)_{i \in I}$ perhe, johon kuuluu jokainen algebran $K[X]$ polynomi, joka ei ole vakio. Lauseen 2.3 nojalla sillä on juurikunta L. Juurikunnan virittävät polynomien p_i juuret, joten se on algebrallinen kunnan K suhteen. Lisäksi juurikunnan määritelmän nojalla kukin polynomi p_i hajoaa algebrassa $L[X]$ ensimmäisen asteen tekijöihin. Niinpä lauseen 2.10 perusteella kunta L on kunnan K algebrallinen sulkeuma.

Jos L_1 ja L_2 ovat kaksi kunnan K algebrallista sulkeumaa, niin ne molemmat ovat perheen $(p_i)_{i \in I}$ juurikuntia. Niinpä lauseen 2.4 nojalla ne ovat isomorfiset. □

3. Kompleksilukujen kunta on algebrallisesti suljettu

Tulosta, että kompleksilukujen kunta on algebrallisesti suljettu, kutsutaan *algebran peruslauseeksi*. Ensimmäisen, joskin siinä vaiheessa vielä virheellisen, todistuksen sille esitti Gauss vuonna 1799. [1, s. 108] Tulokselle tunnetaan useita hyvin erilaisia todistuksia[1]. Koska reaaliluvut ja sitä myöten myös kompleksiluvut ovat pohjimmiltaan analyyttinen konstruktio, yhtäkään täysin algebrallista todistusta algebran peruslauseelle ei kuitenkaan ole. Eräs minimaalisesti ei-algebrallisia menetelmiä käyttävä tulos hyödyntää Galois'n teorian lisäksi vain väliarvolausetta. [1, s. 108; 2, s. 355]

Tässä esitelmässä tulos osoitetaan yksinkertaisten analyyttisten ja topologisten havaintojen avulla. Todistus seuraa Rudinin esitystä [3, s. 170].

Lause 3.1 (Algebran peruslause)**.** *Olkoon* $P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$ *polynomi, jossa* $n \geq 1$*,* $a_i \in \mathbb{C}$ *kaikilla* $i \in \{1, \ldots, n\}$ *ja* $a_n \neq 0$*. Tällöin* $P(z) = 0$ *jollain* $z \in \mathbb{C}$*.*

Todistus. Voidaan olettaa, että $a_n = 1$.

Merkitään $\mu = \inf\{|P(z)| \mid z \in \mathbb{C}\}$.

Kolmioepäyhtälöstä seuraa, että epäyhtälö $\|x + y\| \geq \|x\| - \|y\|$ pätee kaikilla normeilla, erityisesti kompleksilukujen itseisarvolla. Jos $|z| = R$, saadaan

$$
\begin{aligned}
|P(z)| &= |z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0| \\
&\geq |z^n| - |a_{n-1} z^{n-1}| - \ldots - |a_0| \\
&= R^n - |a_{n-1}| R^{n-1} - \ldots - |a_0| \\
&= R^n (1 - |a_{n-1}| R^{-1} - \ldots - |a_0| R^{-n}).
\end{aligned} \tag{2}
$$

Kun $R \to \infty$, epäyhtälön (2) oikea puoli kasvaa rajatta. Niinpä on olemassa jokin raja R_0, jolle pätee, että $|P(z)| > \mu$, kun $|z| > R_0$. Niinpä riittää tarkastella nollakeskistä R_0-säteistä kiekkoa, kun tutkitaan suurinta alarajaa μ.

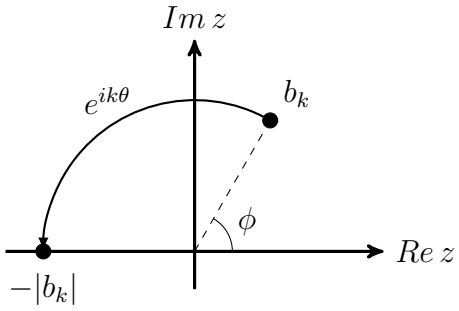
Tämä kiekko on kompakti ja funktio $|P|$ on siinä jatkuva, joten funktiolla $|P|$ on kiekossa pienin (ja suurin) arvo. Olkoon z_0 kiekon piste, jossa funktio $|P|$ saavuttaa pienimmän arvonsa. Jos joukolla on minimi, kyseinen arvo on myös joukon suurin alaraja. Niinpä $\mu = |P(z_0)|$.

Osoitetaan, että $\mu = 0$. Tehdään vastaoletus, että $\mu > 0$ (itseisarvo on aina positiviinen). Asetetaan $Q(z) = \frac{P(z+z_0)}{P(z_0)}$. Tällöin Q on astetta n oleva polynomi, $Q(0) = 1$ ja koska $|P(z_0)|$ on funktion $|P|$ pienin arvo, $|Q(z)| \geq |Q(0)| = 1$ kaikilla $z \in \mathbb{C}$.

Voidaan siis kirjoittaa $Q(z) = 1 + b_k z^k + \ldots + b_n z^n$, missä k on pienin kokonaisluku välillä $1 \leq k \leq n$, jolle $b_k \neq 0$.

[1]Kymmenen erilaista todistusta on esitetty, paikoin painovirheiden kera, osoitteessa `http://adamazzam.wordpress.com/category/algebra/`

Jos $z \in \mathbb{C}$, voidaan luku $e^{i\theta}z$ tulkita geometrisesti siten, että kompleksitason pistettä z kierretään kulman θ verran $|z|$-säteisen ympyrän kaarta pitkin. Niinpä on olemassa sellainen θ, että $e^{ik\theta}b_k = -|b_k|$. (Jos ϕ on kompleksiluvun b_k argumentti, $-\pi \leq \phi \leq \pi$, saadaan $\theta = \frac{1}{k}(\pi - \phi)$.)



Olkoon $r > 0$ ja lisäksi $r^k < \frac{1}{|b_k|}$. Tällöin saadaan

$$
\begin{aligned}
|Q(re^{i\theta})| &= |1 + b_k r^k e^{ik\theta} + \ldots + b_n r^n e^{in\theta}| \\
&\leq |1 + b_k r^k e^{ik\theta}| + \sum_{j=k+1}^{n} |b_j r^j e^{ij\theta}| \\
&= |1 - r^k |b_k|| + \sum_{j=k+1}^{n} r^j |b_j| \\
&= 1 - r^k |b_k| + r^{k+1}|b_{k+1}| + \ldots + r^n |b_n| \\
&= 1 - r^k(|b_k| - r|b_{k+1}| - \ldots - r^{n-k}|b_n|).
\end{aligned} \tag{3}
$$

Kun r on riittävän pieni, epäyhtälön (3) viimeisen rivin sulkulausekkeen arvo on positiivinen, eli $1 \leq |Q(re^{i\theta})| < 1$, mikä on ristiriita. Niinpä vastaoletus on väärä, ja on osoitettu, että $P(z_0) = \mu = 0$. Siis z_0 on polynomin P juuri. □

Viitteet

[1] Jokke Häsä, *Algebra II.* Luentomoniste, Helsingin yliopisto.

[2] I. Martin Isaacs, *Algebra: A Graduate Course.* American Mathematical Society, 2009.

[3] Walter Rudin, *Principles of Mathematical Analysis.* 2nd Edition, McGraw-Hill, 1964.

[4] Kalevi Suominen, *Algebra II.* Luentomoniste, Helsingin yliopisto.