

14. Juurikunnat

Mielivaltaisella polynomilla ei välttämättä ole juuria tarkasteltavassa kunnassa. Tässä luvussa tutkitaan sellaisia algebrallisia laajennoksia, jotka saadaan lisäämällä polynomeille juuria. Ääritapauksessa voidaan muodostaa laajennos, johon lisätään kaikkien polynomien kaikki mahdolliset juuret.

14.1. Määritelmä ja olemassaolo. Tarkastellaan aluksi esimerkkiä. Oletetaan, että K on kunta ja $f \in K[X]$ jokin polynomi, jolla on juuria kunnan K laajennoksessa L . Jos $\alpha_1, \dots, \alpha_n \in L$ ovat polynomin f juuret, voidaan määritellä, että $K(\alpha_1, \dots, \alpha_n)$ on f :n *juurikunta* laajennoksessa L . Juurikunta on siis pienin L :n alilaajennos, joka sisältää polynomin f juuret. Määritelmä on kuitenkin hieman kömpelö, koska siinä viitataan ympäröivään laajennokseen L , jossa polynomilla jo tiedetään olevan juuria. Lisäksi jää avoimeksi, sisältääkö L kaikki f :n juuret vai jääkö osa juurista mahdollisesti juurikunnan ulkopuolelle.

Seuraava tuttu lemma antaa juurten olemassaololle kriteerin, joka perustuu vain polynomin jaollisuusominaisuuksiin.

LEMMA 14.1. *Olkoon K kunta ja $f \in K[X]$ nollasta poikkeava polynomi.*

- a) *Alkio α on polynomin f juuri, jos ja vain jos $X - \alpha$ jakaa f :n.*
- b) *Polynomin f juurten lukumäärä missä tahansa K :n laajennoksessa on korkeintaan $\deg(f)$.*

TODISTUS. a) Jakoyhtälöstä saadaan $f = q(X - \alpha) + r$, missä r on vakio. Nyt $f(\alpha) = r$, joten $f(\alpha) = 0$, jos ja vain jos $X - \alpha$ jakaa f :n.

b) Olkoon L kunnan K laajennos. Käytetään induktiota polynomin f asteen suhteen. Jos $\deg(f) = 0$, väite pätee selvästi. Oletetaan sitten, että väite pätee astetta n olevilla polynomeilla ja että f :n aste on $n + 1$. Jos f :llä ei ole juuria laajennoksessa L , niin väite pätee. Muussa tapauksessa voidaan valita juuri $\alpha \in L$ ja kirjoittaa $f = (X - \alpha) \cdot g$. Jokainen f :n juuri on nyt joko α tai jokin g :n juurista. Jälkimmäisiä on induktio-oletuksen mukaan korkeintaan n kappaletta, joten yhteensä juuria on korkeintaan $n + 1$. \square

Lemman avulla päästään juurikunnan määritelmässä eroon viittauksesta ympäröivään kuntaan. Mikäli ympäröivää kuntaa ei ole, ei voida tietää, minkälaisia juuria annetulla polynomilla on eri laajennoksissa. Kuitenkin sellainen laajennos, jonka suhteen polynomi jakautuu ensimmäisen asteen tekijöihin, sisältää joka tapauksessa maksimaalisen määrän kyseisen polynomin juuria.

MÄÄRITELMÄ 14.2. Olkoon $f \in K[X]$ jokin polynomi. Kunnan K laajennos L on f :n *juurikunta* kunnan K suhteen, jos seuraavat ehdot toteutuvat:

- (JK1) Polynomi f jakautuu 1. asteen polynomien tuloksi renkaassa $L[X]$.
- (JK2) $L = K(\alpha_1, \dots, \alpha_n)$, missä $\alpha_1, \dots, \alpha_n \in L$ ovat polynomin f juuret.

Huomaa, että ehto (JK1) takaa, että polynomilla on suurin mahdollinen määrä juuria laajennoksessa L . Ehdolla (JK2) puolestaan varmistetaan, että L ei sisällä mitään ylimääräistä kyseisten juurten lisäksi.

Yleisemmin, jos $S \subset K[X]$ on joukko polynomeja, sanotaan, että L on joukon S juurikunta, jos jokainen $f \in S$ jakautuu ensimmäisen asteen tekijöihin L :n suhteen ja lisäksi $L = K(A)$, missä A koostuu kaikkien S :n polynomien juurista.

Polynomijoukon juurikunta ei ole yksikäsitteinen. Myöhemmin tullaan kuitenkin osoittamaan, että kaikki tietyn joukon juurikunnat ovat keskenään isomorfiset.

ESIMERKKI 14.3. Kompleksilukujen kunta \mathbb{C} on polynomin $X^2 + 1$ juurikunta \mathbb{R} :n suhteen, sillä $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i, -i)$. Yleisesti, jos L on kunnan K laajennos ja $\alpha^2 \in K$ jollain $\alpha \in L$, niin laajennos $K(\alpha) \subset L$ on polynomin $X^2 - \alpha^2$ juurikunta K :n suhteen. Toisaalta esimerkiksi $\mathbb{Q}(\sqrt[3]{2})$ ei ole polynomin $X^3 - 2$ juurikunta \mathbb{Q} :n suhteen, sillä

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$$

eikä polynomilla $X^2 + \sqrt[3]{2}X + \sqrt[3]{4}$ ole reaalisia juuria; siis erityisesti sillä ei ole juuria kunnassa $\mathbb{Q}(\sqrt[3]{2})$.

Voidaan osoittaa, että millä tahansa polynomilla on olemassa juurikunta. Sellainen löydetään jo tutuksi tulleella menetelmällä.

LAUSE 14.4. *Olkoon K kunta, ja olkoon $f \in K[X]$ jokin polynomi, joka ei ole vakio. Tällöin löytyy K :n äärellinen laajennos L , jonka suhteen f jakautuu ensimmäisen asteen tekijöihin.*

TODISTUS. Käytetään induktiota polynomin f asteen suhteen. Jos $\deg(f) = 1$, tapaus on selvä. Oletetaan sitten, että väite pätee tapauksessa n . Olkoon $f \in K[X]$ polynomi, jonka aste on $n + 1$. Valitaan jokin f :n jaoton tekijä p ja konstruoidaan kunta $K_1 = K[X]/\langle p \rangle$. Lähtökunta K voidaan samastaa K_1 :n alikunnan kanssa, jolloin K_1 on K :n laajennos.

Merkitään $\alpha = \bar{X} = X + \langle p \rangle$. Sijoitettaessa muuttujan X paikalle \bar{X} polynomi p muuttuu polynomiksi \bar{p} . Täten $p(\alpha) = \bar{p} = 0$, eli α on polynomin p juuri ja siten myös f :n juuri. Näin ollen $f = (X - \alpha) \cdot g$ jollain $g \in K_1[X]$. Nyt polynomin g aste on n , joten induktio-oletuksen perusteella löytyy K_1 :n äärellinen laajennos L , jonka suhteen g jakautuu 1. asteen tekijöihin. Siispä myös f jakautuu L :n suhteen ensimmäisen asteen tekijöihin, ja lisäksi $[L : K] = [L : K_1] \cdot \deg(p) < \infty$. \square

KOROLLAARI 14.5. *Jokaisella polynomilla $f \in K[X]$ on juurikunta kunnan K suhteen.*

TODISTUS. Edellisen lauseen avulla löydetään K :n laajennos L , jonka suhteen f jakautuu ensimmäisen asteen tekijöihin. Olkoot $\alpha_1, \dots, \alpha_n \in L$ polynomin f juuret. Nyt $K(\alpha_1, \dots, \alpha_n) \subset L$ on etsitty juurikunta. \square

ESIMERKKI 14.6. Tarkastellaan polynomia $f = X^4 + 3X^2 + 2 \in \mathbb{Q}[X]$. Pienellä vaivalla löydetään polynomin jaottomat tekijät $p_1 = X^2 + 2$ ja $p_2 = X^2 + 1$. Sovelletaan edellisen lauseen todistusta juurikunnan löytämiseksi.

Valitaan ensimmäiseksi laajennokseksi $K_1 = \mathbb{Q}[X]/\langle p_1 \rangle$. Merkitään tässä laajennoksessa $\alpha = \bar{X}$, jolloin $K_1 = \mathbb{Q}(\alpha)$, ja

$$\alpha^2 = \bar{X}^2 = -2 + \bar{p}_1 = -2.$$

Nyt pätee

$$(X - \alpha)(X + \alpha) = X^2 - \alpha^2 = X^2 + 2,$$

joten p_1 jakautuu ensimmäisen asteen tekijöihin renkaassa $K_1[X]$. Toisaalta voidaan osoittaa, että p_2 on edelleen jaoton laajennetussa renkaassa $K_1[X]$. (Tämä nähdään tarkistamalla, että mikään luku $x\alpha + y$, missä $x, y \in \mathbb{Q}$, ei voi olla p_2 :n juuri.) Siispä voidaan valita seuraavaksi laajennokseksi $K_2 = K_1[X]/\langle p_2 \rangle$. Merkitään $\beta = \overline{X}$ (sivuluokka nyt ideaalin $\langle p_2 \rangle$ suhteen), jolloin $\beta^2 = -1$. Polynomirenkaassa $K_1[X]$ alkio α on vakio, joten samastetaan tavalliseen tapaan $\overline{\alpha} = \alpha$. Nyt renkaassa $K_2 = K_1[X]$ pätee

$$f = (X - \alpha)(X + \alpha)(X - \beta)(X + \beta).$$

Lisäksi $K_2 = \mathbb{Q}(\alpha, \beta)$, joten K_2 on polynomien f juurikunta kunnan \mathbb{Q} suhteen.

Yllä kuvattua metodia voidaan soveltaa kaikissa tapauksissa. Toisinaan voidaan kuitenkin edetä suoraviivaisemminkin, jos tunnetaan kunta, joka sisältää varmasti kaikki tarvittavat juuret. Esimerkiksi kompleksilukujen kunta \mathbb{C} sisältää kaikki rationaalipolynomien juuret, joten voidaan yksinkertaisesti ratkaista yhtälö $f(x) = 0$ kunnassa \mathbb{C} , jolloin saadaan juuriksi luvut $i\sqrt{2}$, $-i\sqrt{2}$, i ja $-i$. Juurikunnaksi tulee siten $\mathbb{Q}(i, \sqrt{2})$, sillä tämä kunta sisältää mainitut juuret, ja toisaalta, jos jokin kunta sisältää juuret $i\sqrt{2}$ ja i , se sisältää myös luvun $\sqrt{2} = i\sqrt{2}/i$.

Edellä viitattiin siihen, että kaikki annetun polynomien juurikunnat ovat isomorfisia. Tämän esimerkin tapauksessa eräs isomorfismi saadaan kaavasta

$$a + b\alpha + c\beta + d\alpha\beta \mapsto a + bi\sqrt{2} + ci - d\sqrt{2}.$$

Kaava määrittelee lineaarikuvauksen, koska joukko $\{1, \alpha, \beta, \alpha\beta\}$ on laajennoksen K_2/\mathbb{Q} kanta. Isomorfian tarkistaminen jätetään harjoitustehtäväksi.

Mielivaltaisen äärellisen polynomijoukon $\{f_1, \dots, f_n\}$ juurikunta löydetään soveltamalla edellistä lausetta tulon $f_1 \cdots f_n$. Jos polynomeja on ääretön määrä, todistus on vaikeampi, ja se jätetään myöhemmäksi.

14.2. Algebrallinen sulkeuma. Tarkastellaan seuraavaksi sellaisia laajennoksia, jotka sisältävät kaikkien polynomiensa juuret.

MÄÄRITELMÄ 14.7. Kunta K on *algebrallisesti suljettu*, jos jokainen polynomi $f \in K[X]$ jakautuu ensimmäisen asteen tekijöihin renkaassa $K[X]$.

Algebrallisesti suljetut kunnat voidaan karakterisoida monella tapaa.

LAUSE 14.8. *Olkoon K kunta. Seuraavat ehdot ovat yhtäpitäviä.*

- a) *Kunta K on algebrallisesti suljettu.*
- b) *Jokaisella polynomilla $f \in K[X]$ on juuri K :ssa.*
- c) *Kunnalla K ei ole aitoja algebrallisia laajennoksia.*
- d) *Kunnalla K ei ole aitoja äärellisiä laajennoksia.*
- e) *Jos L on K :n laajennos, niin K koostuu täsmälleen niistä L :n alkioista, jotka ovat algebrallisia K :n suhteen.*

TODISTUS. Harjoitustehtävä. □

MÄÄRITELMÄ 14.9. Kunnan K laajennosta L nimitetään K :n *algebralliseksi sulkeumaksi*, jos se on algebrallisesti suljettu ja algebrallinen K :n suhteen.

Kunnan algebrallinen sulkeuma on sen suurin mahdollinen algebrallinen laajennos, koska sulkeuma on algebrallisesti suljettu eikä sillä itsellään siis voi olla algebrallisia laajennoksia. Algebrallinen sulkeuma on toisaalta myös pienin algebrallisesti suljettu kunta, joka sisältää alkuperäisen kunnan. Jos nimittäin sulkeumasta poistaa yhdenkin alkion, poistuu samalla jonkin polynomin juuri, koska jokainen sulkeuman alkio on algebrallinen.

ESIMERKKI 14.10. Kompleksilukujen kunta \mathbb{C} on algebrallisesti suljettu. Tämä tulos, jonka Gauss todisti vuonna 1799²², tunnetaan *algebran peruslauseen* nimellä. Sille on lukuisia todistuksia, jotka yleensä nojautuvat kompleksianalyysiin tai algebralliseen topologiaan. On olemassa myös Galois'n teoriaa käyttävä todistus, jossa tarvitaan algebrallisten menetelmien lisäksi vain väliarvolauseetta. Koska \mathbb{C} on algebrallisesti suljettu ja algebrallinen reaalilukujen suhteen, se on \mathbb{R} :n algebrallinen sulkeuma.

Tarkastellaan algebrallisten lukujen joukkoa

$$\mathbb{A} = \{\alpha \in \mathbb{C} \mid \alpha \text{ on algebrallinen } \mathbb{Q}\text{:n suhteen}\}.$$

Määritelmän perusteella jokaisen \mathbb{A} -kertoimisen polynomin kaikki kompleksijuuret löytyvät \mathbb{A} :sta. Koska \mathbb{C} on algebrallisesti suljettu, myös \mathbb{A} on täten algebrallisesti suljettu. Lisäksi on helppo näyttää, että \mathbb{A} on kunnan \mathbb{Q} algebrallinen laajennos. Algebralliset luvut muodostavat siis \mathbb{Q} :n algebrallisen sulkeuman.

Voidaan osoittaa, että mielivaltaisella kunnalla K on algebrallinen sulkeuma ja että tämä sulkeuma on isomorfaa vaille yksikäsitteinen. Tässä esitettävän olemassaolotodistuksen perusidea on käyttää Zornin lemmaa kaikkien K :n algebrallisten laajennosten kokoelmassa. Kyseinen kokoelma on kuitenkin liian laaja ollakseen joukko, joten sitä on rajoitettava jollain tapaa. Samalla on silti pidettävä huolta siitä, että kokoelma sisältää riittävän määrän kuntia, jotta todistus menee läpi. Tähän käytetään seuraavaa joukko-opillista lemmaa.

LEMMA 14.11. *Jos L/K on algebrallinen laajennos, niin $|L| \leq \max\{|K|, |\mathbb{N}|\}$.*

TODISTUS. Jokainen polynomi $f = a_0 + a_1X + \dots + a_nX^n \in K[X]$ voidaan samastaa äärellisen jonon (a_0, \dots, a_n) kanssa. Astetta n olevien K -kertoimisten polynomien joukon $K_n[X]$ mahtavuus on siis $|K|^n$. Jos K on äärellinen, tämä mahtavuus on $|K|^n$, muuten $|K|^n = |K|$. Koska $K[X]$ on numeroituva yhdiste joukoista $K_n[X]$, joukko-opin perustuloksista seuraa, että $|K[X]| \leq \max\{|K|, |\mathbb{N}|\}$.

Koska L/K on algebrallinen, jokainen L :n alkio on jonkin K -kertoimisen polynomin juuri. Indeksoidaan jokaisen K -kertoimisen polynomin juuret $\alpha_1, \dots, \alpha_r$ jossain mielivaltaisessa järjestyksessä, jolloin kutakin L :n alkioita α vastaa yksikäsitteinen pari $(p, i) \in K[X] \times \mathbb{N}$, missä $p = \min(K, \alpha)$ ja α :n indeksi polynomin p juurten joukossa on i . Näiden parien muodostaman joukon mahtavuus on korkeintaan $\max\{|K[X]|, |\mathbb{N}|\} = \max\{|K|, |\mathbb{N}|\}$. \square

²²Oikeastaan Gaussin väitöskirjassaan esittämä todistus sisältää aukon. Jean-Robert Argand esitti täydellisen todistuksen vuonna 1814, ja Gauss julkaisi myöhemmin useitakin erilaisia aukottomia versioita.

LAUSE 14.12. *Jokaisella kunnalla on algebrallinen sulkeuma.*

TODISTUS. Olkoon K mielivaltainen kunta. Olkoon S jokin joukko, joka sisältää kunnan K ja jolle pätee $|S| > \max\{|K|, |\mathbb{N}|\}$. Joillekin S :n osajoukoille voidaan määrittellä kuntarakenne, jonka suhteen niistä tulee K :n algebrallisia laajennoksia. Olkoon \mathcal{A} nyt kaikkien tällaisten joukkoon S sisältyvien K :n algebrallisten laajennosten kokoelma. (Sama osajoukko voi esiintyä kokoelmassa useamman kerran erilaisilla kuntarakenteilla varustettuna.) Selvästi $K \in \mathcal{A}$, joten $\mathcal{A} \neq \emptyset$. Merkitään $L_1 \leq L_2$, kun L_2 on L_1 :n laajennos. Tämä relaatio tekee kokoelmasta \mathcal{A} osittaisjärjestyksen.

On helppo nähdä, että osittaisjärjestyksessä (\mathcal{A}, \leq) jokaisella ketjulla on ylärajanaan ketjun yhdiste. Zornin lemmasta seuraa tällöin, että \mathcal{A} :ssa on maksimaalinen alkio M . On osoitettava, että M on algebrallisesti suljettu. Olkoon sitä varten M' jokin M :n algebrallinen laajennos. Edellisen lemmän perusteella

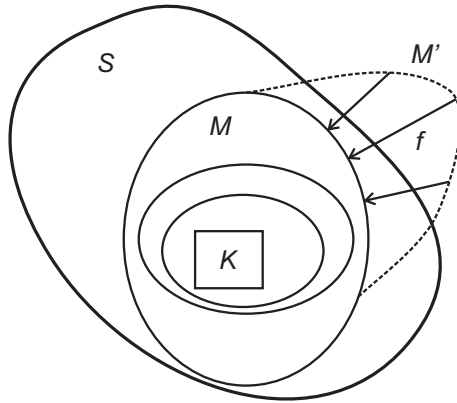
$$|M'| \leq \max\{|M|, |\mathbb{N}|\} \leq \max\{|K|, |\mathbb{N}|\} < |S|,$$

koska sekä M'/M että M/K ovat algebrallisia laajennoksia. Näin ollen löytyy jokin injektio $f: M' \rightarrow S$, jolle lisäksi pätee $f|_M = \text{id}$.

Kun määritellään kuvajoukossa $f(M')$ laskutoimitukset kaavoilla

$$f(a) + f(b) = f(a + b) \quad \text{ja} \quad f(a)f(b) = f(ab),$$

joukosta $f(M') \subset S$ tulee M :n algebrallinen laajennos. Nyt M :n maksimaalisuudesta seuraa, että $f(M') = M$, joten $M' = M$, koska $f|_M = \text{id}$ ja f on injektio. Siispä M on algebrallisesti suljettu ja kunnan K algebrallinen sulkeuma.



KUVA 26. Maksimaalinen algebrallinen laajennos M on kunnan K algebrallinen sulkeuma.

□

KOROLLAARI 14.13. *Jokaisella polynomijoukolla $S \subset K[X]$ on juurikunta kunnan K suhteen.*

TODISTUS. Olkoon M kunnan K algebrallinen sulkeuma. Tällöin jokainen polynomi $f \in S$ jakautuu ensimmäisen asteen tekijöihin M :n suhteen. Olkoon A joukko, joka sisältää kaikki S :n polynomien juuret. Nyt $K(A)$ on etsitty juurikunta. □