13.3. Transkendenttisuudesta. Luvun todistamiseksi algebralliseksi riittää löytää polynomi, jonka juuri kyseinen luku on. Transkendenttisuuden todistaminen on sen sijaan työläämpää. Jotkut tapaukset ovat kuitenkin selkeitä: Oletetaan esimerkiksi, että K on kunta, ja tarkastellaan polynomialgebran $K[X]$ jakokuntaa $K(X)$. Tämä kunta on K:n laajennos, ja alkio $X \in K(X)$ on selvästi transkendenttinen K:n suhteen. Kaikkien K-kertoimisten polynomien joukko $K[X]$ nimittäin sisältyy kuntaan $K(X)$, ja alkioon X liittyvä sijoitushomomorfismi $K[X] \to K(X)$ on inkluusiokuvaus. Toisin sanoen, sijoitettaessa alkio X polynomiin f tuloksena on f. Siispä $f(X) = 0$ jos ja vain jos $f = 0$.

Useimmiten transkendenttisista luvuista puhuttaessa tarkoitetaan reaali- tai kompleksilukuja, jotka ovat transkendenttisia rationaalilukujen kunnan suhteen. Nykyään on selvää, että transkendenttisia lukuja on olemassa, vieläpä runsain mitoin. On nimittäin varsin helppo osoittaa, että $\mathbb{Q}$-kertoimisia polynomeja on vain numeroituva määrä, jolloin myös niiden juuria on numeroituvan monta (ks. lemma 14.11). Siispä *algebrallisten lukujen joukko*

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

on numeroituva. Toisaalta kompleksilukujen joukko on ylinumeroituva, joten valtaosa kompleksiluvuista (tai yhtä hyvin reaaliluvuista) on transkendenttisia.

Yllä esitetty päättely on mahdollista tehdä vain, jos kompleksilukujen joukon ylinumeroituvuus tunnetaan. Tämän todisti Georg Cantor vuonna 1878. Kuitenkin jo ennen sitä — tarkemmin sanoen vuonna 1844 — Joseph Liouville oli osoittanut, että hänen nimeään kantavat Liouvillen luvut ovat transkendenttisia reaalilukuja. Tämä oli ensimmäinen osoitus transkendenttiseten lukujen olemassaolosta. Tunnetumpi esimerkki transkendenttisesta luvusta saatiin vuonna 1873, kun Charles Hermite osoitti Neperin luvun e transkendenttisuuden. Hieman myöhemmin, eli vuonna 1882, Ferdinand von Lindemann onnistui Hermiten menetelmää mukaillen osoittamaan, että myös luku π on transkendenttinen rationaalilukujen suhteen. Lindemannin ja Hermiten todistukset käyttävät analyyttisiä menetelmiä.

Avoimeksi ongelmaksi on jäänyt muun muassa se, onko e algebrallinen vai transkendenttinen laajennoksen $\mathbb{Q}(\pi)$ suhteen eli onko olemassa polynomia, jonka kertoimissa saa hyödyntää piin potensseja ja jolla on juurena e.

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 $\alpha_1, \ldots, \alpha_n \in L$ ovat polynomin f juuret, voidaan määritellä, että $K(\alpha_1, \ldots, \alpha_n)$ 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 $f = (X - \alpha) \cdot g + r$, 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 $\deg(f) = 0$, niin 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 $n + 1$. □

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 $\mathbb{Q}(\sqrt[3]{2})$.

ESIMERKKI 14.4. Olkoon $f = X^2 + X + 1 \in \mathbb{F}_2[X]$. Koska f on jaoton, tekijärengas $K = \mathbb{F}_2[X]/\langle f\rangle$ on kunnan $\mathbb{F}_p$ laajennos. Merkitään $\alpha = \overline{X}$. Nyt $\alpha^2 + \alpha = 1$, sillä $\alpha^2 + \alpha + 1 = 0$, ja $1 = -1$ kunnassa K. Täten

$$\begin{aligned}(X+\alpha)(X+(\alpha+1)) &= X^2 + (2\alpha+1)X + \alpha^2 + \alpha \\ &= X^2 + X + \alpha^2 + \alpha = X^2 + X + 1.\end{aligned}$$

Siispä f jakautuu renkaassa $K[X]$ ensimmäisen asteen tekijöihin $X+\alpha$ ja $X+\alpha+1$. Lisäksi $K = \mathbb{F}_2[\alpha] = \mathbb{F}_2[\alpha, \alpha+1]$, joten K on polynomin f juurikunta alkukunnan $\mathbb{F}_2$ suhteen.

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

LAUSE 14.5. *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 $\alpha = \overline{X}$. Sijoitettaessa muuttujan X paikalle $\overline{X}$ polynomi p muuttuu polynomiksi $\overline{p}$. Täten $p(\alpha) = \overline{p} = 0$, 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 M:n suhteen ensimmäisen asteen tekijöihin, ja lisäksi $[L : K] = [L : K_1] \cdot \deg(p) < \infty$. □

KOROLLAARI 14.6. *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. □

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

14.2. Algebrallinen sulkeuma. Tarkastellaan seuraavaksi niitä 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) *K on algebrallisesti suljettu.*

b) *Jokaisella polynomilla $f \in K[X]$ on juuri K:ssa.*
c) *K:lla ei ole aitoja algebrallisia laajennoksia.*
d) *K:lla 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. $\square$

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 pienin algebrallisesti suljettu kunta, joka sisältää alkuperäisen kunnan. Jos nimittäin algebrallisesta sulkeumasta poistaa yhdenkin alkion, poistuu samalla jonkin polynomin juuri, koska jokainen sulkeuman alkio on algebrallinen. Toisaalta algebrallinen sulkeuma on algebrallisista laajennoksista suurin, koska se on algebrallisesti suljettu.

ESIMERKKI 14.10. Kompleksilukujen kunta $\mathbb{C}$ on algebrallisesti suljettu. Tämä tulos, jonka Gauss todisti vuonna 1799, tunnetaan *algebran peruslauseen* nimellä.[20] Sille on lukuisia todistuksia, jotka yleensä perustuvat kompleksianalyysiin. On olemassa myös Galois'n teoriaa käyttävä todistus, jossa tarvitaan algebrallisten menetelmien lisäksi vain väliarvolausetta. Koska $\mathbb{C}$ on algebrallisesti suljettu ja algebrallinen reaalilukujen suhteen, se on $\mathbb{R}$:n algebrallinen sulkeuma.

Tarkastellaan algebrallisten lukujen joukkoa

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

On helppo nähdä, että 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 $\mathbb{A}$ 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 isomorfiaa 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 $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ voidaan samastaa äärellisen jonon $(a_0, \ldots, a_n)$ 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 $|K[X]| \leq \max\{|K|, |\mathbb{N}|\}$.

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

Koska L/K on algebrallinen, jokainen L:n alkio on jonkin K-kertoimisen polynomin juuri. Indeksöidään jokaisen K-kertoimisen polynomin juuret $\alpha_1, \ldots, \alpha_r$ jossain mielivaltaisessa järjestyksessä, jolloin kutakin L:n alkiota 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 $\max\{|K[X]|, |\mathbb{N}|\} = \max\{|K|, |\mathbb{N}|\}$. $\square$

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 määritellä 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.

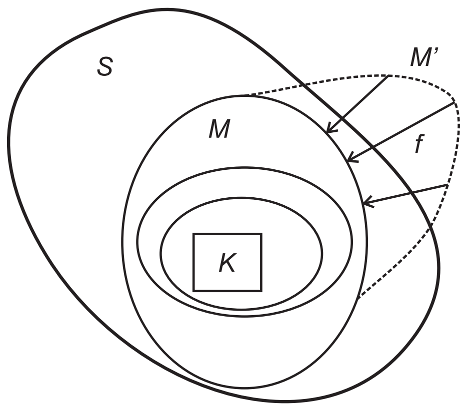
On helppo nähdä, että osittaisjärjestyksessä $(\mathcal{A}, \leq)$ jokaisella ketjulla on yläraja. Zornin lemmasta seuraa tällöin, että $\mathcal{A}$:ssa on maksimaalinen alkio M. Riittää osoittaa, että M on algebrallisesti suljettu. Olkoon sitä varten M' jokin M:n algebrallinen laajennos. Edellisen lemman 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 $f : M' \to S$, jolle lisäksi pätee $f|_M = \mathrm{id}$. Kun määritellään kuvassa $f(M')$ 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 $f|_M = \mathrm{id}$ ja f on injektio. Siispä M on algebrallisesti suljettu ja kunnan K algebrallinen sulkeuma.



KUVA 27. Maksimaalinen algebrallinen laajennos M on kunnan K algebrallinen sulkeuma.

$\square$

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. $\square$