TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Leo Majaranta

Algebrallisista ja transkendenttisista luvuista

Informaatiotieteiden yksikkö
Matematiikka
Toukokuu 2011

Tampereen yliopisto
Informaatiotieteiden yksikkö

MAJARANTA, LEO: Algebrallisista ja transkendenttisista luvuista

Pro gradu -tutkielma, 40 s.

Matematiikka

Toukokuu 2011

Tiivistelmä

Tämän tutkielman tarkoituksena on esitellä algebralliset- ja transkendenttiset luvut, sekä joitakin näitä lukuja koskevia lauseita. Tässä tutkielmassa algebrallisella luvulla tarkoitetaan useimmiten sellaista algebrallista lukua, joka määritellään rationaalilukukertoimisen polynomin juurena. Vastaavasti transkendenttisellä luvulla tarkoitetaan lukua, joka ei ole minkään rationaalilukukertoimisen polynomin juuri. Algebrallisen luvun käsite voidaan määritellä yleisemmin siten, että algebrallinen luku määritetään jonkin sellaisen polynomin juureksi, jonka kertoimet ovat kunnassa K, missä tämä kunta K ei ole välttämättä rationaalilukujen kunta. Osa tutkielmassa esitetyistä lauseista on esitetty muodossa, jossa puhutaan algebrallisista luvuista tässä laajemmassa merkityksessä. Tärkeimmät tutkielmassa esitetyt lauseet ovat Liouvillen lukujen transkendenttisuutta koskeva lause, yleistetty Lindemannin lause ja Gelfondin-Schneiderin lause. Näissä lauseissa algebrallisuudella ja transkendenttisuudella on perinteinen rationaalilukujen kuntaan liittyvä merkitys. Lauseiden perusteella on osoitettu lukujen π ja e transkendenttisuus. Tärkeimpänä lähteenä on käytetty Nivenin kirjaa *Irrational Numbers*.

Sisältö

1 Johdanto **7**

2 Algebralliset ja transkendenttiset luvut **7**
2.1 Algebrallisten ja transkendenttisten lukujen määrittely 7
2.2 Algebrallisten lukujen ominaisuuksia 8
2.3 Liouvillen luvut 11
2.4 Lisää algebrallisten ja transkendenttisten lukujen ominaisuuksia 12
2.5 Joitakin polynomeja koskevia lauseita 13

3 Yleistetty Lindemannin lause **16**
3.1 Yleistetyn Lindemannin lauseen esittely 16
3.2 Yleistetyn Lindemannin lauseen todistamiseen tarvittavia lauseita 17
3.3 Yleistetyn Lindemannin lauseen todistus 26
3.4 Yleistetyn Lindemannin lauseen seurauksia 27
3.5 Ympyrän neliöiminen 28

4 Gelfondin-Schneiderin lause **28**
4.1 Gelfondin-Schneiderin lauseen esittely 28
4.2 Gelfondin-Schneiderin lauseen todistamiseen tarvittavia lauseita 29
4.3 Gelfondin-Schneiderin lauseen todistuksen valmistelua 33
4.4 Gelfondin-Schneiderin lauseen todistus 37

Viitteet **40**

1 Johdanto

Tämä tutkielma käsittelee algebrallisia ja transkendenttisia lukuja. Lukijalla oletetaan olevan perustiedot lukuteoriasta ja abstraktista algebrasta.

Lukujen jako rationaalilukuihin ja irrationaalilukuihin oli tunnettu jo ennen ajanlaskumme alkua. Edellä mainittua jakoa käytettäessä puhutaan yleensä reaaliluvuista. Luvut voidaan jakaa myös algebrallisista ja transkendenttisiin lukuihin, jolloin on luonnollista käsitellä reaalilukujen lisäksi kompleksilukuja, koska algebrallinen luku määritellään rationaalilukukertoimisen polynomin juurena, ja tälläinen juuri voi olla kompleksiluku. Transkendenttinen luku on reaaliluku tai kompleksiluku, joka ei ole minkään edellä mainitun polynomin juuri. Tunnetuimpia transkendenttisia lukuja ovat luvut π ja e. Reaalinen algebrallinen luku voi olla rationaaliluku tai irrationaaliluku. Transkendenttinen reaaliluku on aina irrationaaliluku. Algebrallisista ja transkendenttisistä luvuista puhuttiin jo 1700-luvulla, mutta ensimmäisen todistuksen transkendenttisten lukujen olemassaolosta esitti Liouville vuonna 1844. Luvun e transkendenttisuuden todisti Hermite vuonna 1873 ja luvun π transkendenttisuuden todisti Lindemann vuonna 1882.

Tässä tutkielmassa esitellään algebralliset- ja transkendenttiset luvut, sekä joitakin näitä lukuja koskevia lauseita. Tärkeimmät lauseet ovat Liouvillen lukujen transkendenttisuutta koskeva lause, yleistetty Lindemannin lause ja Gelfondin-Schneiderin lause.

Tärkeimpänä lähteenä on käytetty Nivenin kirjaa *Irrational Numbers*.

2 Algebralliset ja transkendenttiset luvut

2.1 Algebrallisten ja transkendenttisten lukujen määrittely

Seuraavassa esitetään algebrallisten ja transkendenttisten lukujen määrittely.

Määritelmä 2.1. Lukua, joka toteuttaa muotoa

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \tag{2.1}$$

olevan rationaalilukukertoimisen polynomiyhtälön sanotaan *algebralliseksi*. Jos luku ei toteuta mitään tällaista polynomiyhtälöä, niin lukua sanotaan *transkendenttiseksi*.

Huomautus. Edellä olevassa määritelmässä korkeimman asteen termin kerroin on 1. Jos tätä vaatimusta ei aseteta, niin edellisen kanssa yhtäpitävä määrittely saadaan, jos vaaditaan, että kertoimet ovat kokonaislukuja. Tällöin edellistä määritelmää vastaava yhtälö saataisiin jakamalla kaikki termit ylimmän asteen termin kertoimella.

Määritelmä 2.2. Jos algebrallinen luku α toteuttaa muotoa (2.1) olevan yhtälön, missä kertoimet a_i ovat kokonaislukuja, niin sanotaan, että luku α on *algebrallinen kokonaisluku*.

Esimerkki 2.1. Jokainen rationaaliluku $\frac{m}{n}$ toteuttaa muotoa $nx - m = 0$ olevan polynomiyhtälön. Täten rationaaliluvut ovat algebrallisia.

Määritelmä 2.3. Polynomia, jonka korkeimman asteen termin kerroin on 1, sanotaan pääpolynomiksi. Jos $f(x)$ on pienintä astetta oleva pääpolynomi siten, että algebrallinen luku α toteuttaa polynomiyhtälön $f(x) = 0$, niin polynomia sanotaan luvun α minimaalipolynomiksi ja sen astetta sanotaan luvun α asteeksi.

2.2 Algebrallisten lukujen ominaisuuksia

Oletetaan tunnetuksi seuraava lause.

Lause 2.1. *Mitkä tahansa $r+1$ r:n muuttujan rationaalilukukertoimista lineaarista funktionaalia ovat lineaarisesti riippuvia yli rationaalilukujen joukon.*

Lause 2.2. *Algebrallisten lukujen joukko varustettuna yhteenlaskulla ja kertolaskulla on kunta .*

Todistus. Vrt. [1, s. 84]. Oletetaan, että α ja β ovat algebrallisia lukuja joiden asteet ovat vastaavasti m ja n. Tällöin α toteuttaa astetta m olevan algebrallisen yhtälön

$$\alpha^m = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \cdots + a_1\alpha + a_0, \tag{2.2}$$

missä kertoimet a_j ovat rationaalilukuja. Siis α^m on lukujen $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ lineaarikombinaatio siten, että kertoimet ovat rationaalilukuja. Kertomalla yhtälö luvulla α ja käyttämällä yhtälöä korvaamaan termi $a_{m-1}\alpha^m$ alemman asteen termeillä, voidaan todeta, että sama pätee myös luvulle α^{m+1}. Toistamalla edellä olevaa prosessia todetaan, että kaikki luvut $\alpha^m, \alpha^{m+1}, \alpha^{m+2}, \ldots$ ovat esitettävissä lukujen $1, \alpha, \ldots, \alpha^{m-1}$ rationaalilukukertoimisena lineaarikombinaationa. Samoin luvut $\beta^n, \beta n + 1, \beta^{n+2}, \ldots$ ovat esitettävissä lukujen $1, \beta, \beta^2, \ldots, \beta^{n-1}$ rationaalilukukertoimisena lineaarikombinaationa.

Tarkastellaan lukuja

$$1, \alpha + \beta, (\alpha + \beta)^2, \ldots, (\alpha + \beta)^{mn}, \tag{2.3}$$

joita on $mn+1$ kappaletta. Laajentamalla nämä ja korvaamalla korvaamalla luvun α korkeammat potenssit lähtien potenssista m alemmilla potensseilla ja samoin korvaamalla luvun β korkeammat potenssit lähtien potenssista n todetaan, että nämä $mn+1$ lukua voidaan kirjoittaa rationaalilukukertoimisina lukujen

$$\alpha^j\beta^k, \qquad j = 0, 1, \ldots, m-1, \qquad k = 0, 1, \ldots, n-1,$$

lineaarikombinaatioina. Nämä mn lukua voidaan korvata lauseen 2.1 muuttujilla r jonka perusteella voidaan päätellä, että luvut (2.3) ovat lineaarisesti riippumattomia yli rationaalilukujen. Tämä todistaa, että $\alpha+\beta$ on algebrallinen luku.

Vastaavasti voidaan todistaa tulon $\alpha\beta$ algebrallisuus korvaamalla luettelossa (2.3) lukujen $\alpha+\beta$ potenssit lukujen $\alpha\beta$ potensseilla.

Jos luku α astetta m olevan polynomiyhtälön $f(x)=0$, niin luku $-\alpha$ toteuttaa yhtälön $f(-x)=0$ ja jos $\alpha!=0$, niin α^{-1} toteuttaa yhtälön $x^m f(1/x)=0$, joten algebrallisten lukujen joukko on suljettu vähennyslaskun ja jakolaskun suhteen.

Lause 2.3. *Jos luvut a ja b ovat reaalilukuja, niin kompleksiluku $a+bi$ on algebrallinen, jos ja vain jos luvut a ja b ovat algebrallisia.*

Todistus. Vrt. [1, s. 85]. Luku i on algebrallinen, koska se on polynomiyhtälön $x^2+1=0$ ratkaisu. Tällöin myös $a+bi$ on lauseen 2.1 perusteella algebrallinen, jos luvut a ja b ovat algebrallisia. Oletetaan suraavaksi, että $a+bi$ on algebrallinen. Tällöin on olemassa rationaalilukukertoiminen polynomi $f(x)$, jolle on voimassa yhtälö $f(a+bi)=0$. Tällöin on voimassa myös $f(a-bi)=0$, joten myös luku $a-bi$ on algebrallinen. Tällöin lukujen $a+bi$ ja $a-bi$ summa $2a$ ja erotus $2bi$ ovat algebrallisia. Kertomalla nämä algebrallisilla luvuilla $1/2$ ja $-i/2$ todetaan, että luvut a ja b ovat algebrallisia. Siis lause on todistettu.

Määritelmä 2.4. Reaaliluvulla ξ sanotaan olevan kertalukua n oleva rationaalilukuapproksimaatio, jos on olemassa vain luvusta ξ riippuva kiinteä positiivinen luku c siten, että epäyhtälöllä

$$\left|\xi-\frac{h}{k}\right|<\frac{c}{k^n} \tag{2.4}$$

on äärettömän monta rationaalilukuratkaisua h/k, joille on voimassa $k>0$ ja $(h,k)=1$.

Lause 2.4. *Jokaiselle rationaaliluvulle on olemassa kertalukua 1 oleva rationaalilukuapproksimaatio, mutta ei korkeampaa kertalukua olevaa approksimaatiota.*

Todistus. Vrt. [1, s. 89]. Tarkastellaan rationaalilukua a/b, jolle on voimassa ehdot $(a,b)=1$ ja $b\geq 1$. Yhtälölle $ax-by=1$ on olemassa äärettömän monta kokonaislukuratkaisua. Jos $x=x_0, y=y_0$ on yhtälön ratkaisu, niin yleinen ratkaisu on $x=x_0+bt, \quad y=y_0+at$, missä t on mikä tahansa kokonaisluku. Yhtälöille

$$ax-by=1, \qquad \left|\frac{a}{b}-\frac{y}{x}\right|=\frac{1}{bx}$$

ja epäyhtälölle

$$\left|\frac{a}{b} - \frac{y}{x}\right| < \frac{2}{x},$$

missä $x > 0$, on siis äärettömän monta kokonaislukuratkaisua. Tämä voidaan tulkita siten, että rationaaliluvulle a/b on olemassa kertalukua 1 oleva approksimaatio, mikä todetaan kun tehdään epäyhtälöön (2.4) sijoitukset $n = 1, \xi = a/b, h/k = y/xjac = 2$.

Toisaalta jos tutkitaan mitä tahansa rationaalilukua $y/x \neq a/b$ todetaan, että on voimassa

$$\left|\frac{a}{b} - \frac{y}{x}\right| = \left|\frac{ax - by}{bx}\right| \geq \frac{1}{bx}.$$

Tällöin ei ole olemassa kiinteää lukua c siten, että olisi voimassa $1/bx < c/x^2$ äärettömän monella kokonaisluvulla x. Siis luvulle a/b ei ole olemassa approksimaatiota, jonka kertalukua olisi suurempi kuin 1. Lause on siis todistettu.

Lause 2.5. *Algebralliselle astetta n olevalle reaaliluvulle ei ole kertalukua n korkeampaa approksimaatiota.*

Todistus. Vrt. [1, s. 90]. Tapaus $n = 1$ käsiteltiin lauseessa 2.4. Oletetaan, että $n \geq 2$. Oletetaan, että astetta n oleva algebrallinen luku ξ toteuttaa polynomiyhtälön

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = 0,$$

missä $f(x)$ on rationaalilukukertoiminen polynomi, joka on jaoton rationaalilukujen kunnassa. Jos $x \in (\xi - 1, \xi + 1)$, niin on voimassa $|x| < |\xi| + 1$. Derivaatalle $f'(x)$ on tällöin voimassa

$$\begin{aligned} |f'(x)| &= |na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1}| \\ &\leq |na_0x^{n-1}| + |(n-1)a_1x^{n-2}| + \cdots + |a_{n-1}| \\ &< n|a_0|(|\xi| + 1)^{n-1} + (n-1)|a_1|(|\xi| + 1)^{n-2} \\ &\quad + \cdots + |a_{n-1}| = A \end{aligned} \tag{2.5}$$

Edellä oleva yhtälö määrittelee vakion A. Jos h/k on jokin luvun ξ rationaalilukuapproksimaatio, niin voidaan olettaa, että $h/k \in (\xi - 1, \xi + 1)$. Koska $f(x)$ oli jaoton rationaalilukujen kunnassa, niin oltava $f(h/k) \neq 0$, sillä muuten $x - h/k$ olisi polynomin $f(x)$ tekijä. Tällöin on voimassa

$$\left|f\left(\frac{h}{k}\right)\right| = \frac{|a_0h^n + a_1h^{n-1}k + \cdots + a_nk^n|}{k^n} \geq \frac{1}{k^n}. \tag{2.6}$$

Väliarvolauseen perusteella on olemassa luku $x \in (\xi, h/k)$ siten, että on voimassa

$$f\left(\frac{h}{k} - f(\xi\right) = \left(\frac{h}{k} - \xi\right) f'(x).$$

Ottamalla itseisarvot yhtälön kummastakin puolesta ja käyttämällä yhtälöitä ja epäyhtälöita (2.5) ja (2.6), saadaan

$$\left|\frac{h}{k} - \xi\right| = \frac{|f(h/k)|}{|f'(x)|} > \frac{1}{Ak^n}.$$

Ei ole olemassa kiinteä luku c siten, että olisi voimassa $1/(Ak^n) < c/k^{n+1}$ äärettömän monella positiivisella kokonaisluvulla k, ja siis luvulle ξ ei ole olemassa approksimaatioita jonka ketaluku on $n+1$ tai korkeampi. Lause on siis todistettu.

2.3 Liouvillen luvut

Määritelmä 2.5. Reaalilukua ξ sanotaan Liouvillen luvuksi, jos jokaista positiivista kokonaislukua m kohti löytyy rationaaliluku h_m/k_m, missä $k_m > 1$ siten, että on voimassa

$$|\xi - h_m/k_m| < (k_m)^{-m}. \tag{2.7}$$

Lause 2.6. *Jokainen Liouvillen luku on transkendenttinen.*

Todistus. Vrt. [1, s. 92]. Tehdään vastaoletus, että Liouvillen luku ξ on astetta n oleva algebrallinen luku. Tällöin kaikille kokonaisluvuille $m \geq n+1$ olisi epäyhtälön (2.7) perusteella voimassa

$$|\xi - h_m/k_m| < (k_m)^{-n-1}.$$

Tällöin luvulle ξ on olemassa kertaluokan $n+1$ approksimaatio, mikä on ristiriidassa lauseen 2.5 kanssa. Siis vastaoletus on väärä ja lause on todistettu.

Esimerkki 2.2. Tarkastellaan lukua

$$\xi_1 = \sum_{i=1}^{\infty} \frac{1}{10^{i!}}$$

Osasumma

$$\sum_{i=1}^{m} \frac{1}{10^{i!}}$$

voidaan esittää rationaalilukuna h_m/k_m, missä $k_m = 10^{m!}$. Tällöin on voimassa

$$|\xi_1 - h_m/k_m| = \sum_{i=m+1}^{\infty} \frac{1}{10^{i!}} < 2 \cdot 10^{-(m+1)!} < (10^{m!})^{-m} = (k_m)^{-m}.$$

Siis ehto (2.7) on voimassa ja luku ξ_1 on Liouvillen luku ja siten transkendenttinen.

2.4 Lisää algebrallisten ja transkendenttisten lukujen ominaisuuksia

Määritelmä 2.6. Jos joukko S on reaalilukujen osajoukko ja luvut α ja β ovat kaksi erisuurta reaalilukua, joille on voimassa $\alpha < \beta$, niin joukon S sanotaan olevan kaikkialla tiheä, jos aina löytyy $s \in S$ siten, että on voimassa $\alpha < s < \beta$.

Lause 2.7. *Reaalisten algebrallisten kokonaislukujen joukko, joiden aste on $n \geq 2$, on kaikkialla tiheä.*

Todistus. Vrt. [1, s. 85]. Olkoon α ja β kaksi erisuurta reaalilukua, joille on voimassa $\alpha < \beta$. On todistettava, että löytyy astetta n oleva reaalinen algebrallinen kokonaisluku, jolle on voimassa $\alpha < \gamma < \beta$. Havaitaan, että on voimassa

$$(x+\beta)^n - (x+\alpha)^n = ((x+\alpha) - (\beta-\alpha))^n - (x+\alpha)^n > n(x+\alpha)^{n-1}(\beta-\alpha)$$

kaikilla sellaisilla reaaliluvuilla x, joille on voimassa $x + \alpha > 0$. Edellä oleva epäyhtälö saatiin hylkäämällä binomikehitelmässä toisen termin jälkeiset termit. Lausekkeen $n(x+\alpha)^{n-1}(\beta-\alpha)$ arvo saadaan mielivaltaisen suureksi valitsemalla suuri luku x. On siis olemassa positiivinen kokonaisluku j siten, että on voimassa epäyhtälöt

$$(j+\beta)^n - (j+\alpha)^n > 5, \qquad j+\alpha > 0, \qquad j+\beta > 0.$$

Tällöin avoin väli $((j+\alpha)^n, (j+\beta)^n)$ sisältää ainakin neljä perättäistä positiivista kokonaislukua, joten väliin täytyy sisältyä kokonaisluku joka on muotoa $2 + 4k$. Jatkuvuudesta johtuen on olemassa reaaliluku γ jolle on voimassa ehdot $(j+\gamma)^n = 2 + 4k$ ja $\alpha < \gamma < \beta$. Tällöin luku γ toteuttaa polynomiyhtälön

$$f(x) = (x+j)^n - 2(1+2k) = 0,$$

missä kertoimet ovat kokonaislukuja. Korkeimman asteen termin kerroin on yksi, joten luku γ on algebrallinen kokonaisluku.

On vielä todistettava, että algebrallinen kokonaisluku γ on astetta n. On osoitettava, että polynomi $f(x)$ on jaoton polynomi rationaalilukujen suhteen. Tämä on yhtäpitävä sen kanssa, että osoitetaan, että polynomi $f(x-j) = x^n - 2(1+2k)$ on jaoton. Polynomin $f(x-j)$ nollakohdat ovat kompleksiluvut

$$\sqrt[n]{2(1+2k)} \cdot \xi^s, \qquad s = 1, 2, \ldots, n,$$

missä ξ on primitiivinen n:s yksikön juuri. Tehdään vastaoletus, että polynomi $f(x-j)$ on jaollinen. Tällöin sillä on rationaalilukukertoiminen astetta $w < n$ oleva tekijäpolynomi $g(x)$. Polynomi $g(x)$ on tulo, jossa on w kappaletta muotoa

$$x - \sqrt[n]{2(1+2k)} \cdot \xi^s$$

olevia tekijöitä. Tarkastellaan tälläisen polynomin vakiotermin itseisarvoa. Tämä itseisarvo on $(2(1+2k))^{w/n}$, koska luvun ξ^s itseisarvo on 1 kaikilla luvun s arvoilla. Oletuksen perusteella tämä on rationaaliluku. Merkitään tätä rationaalilkukua a/b. Tällöin saadaan

$$(2(1+2k))^{w/n} = a/b \quad tai \quad 2^w(1+2k)^w b^n = a^n.$$

Jälkimmäinen yhtälö on mahdoton, koska luvun 2 potenssit eivät voi olla samat yhtälön oikealla ja vasemmalla puolella. Siis vastaoletus on väärä ja polynomi $f(x-j)$ on jaoton. Lause on siis todistettu.

Lause 2.8. *Algebrallisten lukujen joukko on numeroituva.*

Todistus. Jokainen algebrallinen luku toteuttaa jonkin muotoa

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$$

olevan polynomiyhtälön, missä kertoimet a_i ovat kokonaislukuja ja $a_0 \neq 0$. Voidaan olettaa, että $a_0 \geq 1$. Määritellään, että polynomin $f(x)$ indeksi on positiivinen kokonaisluku

$$n + a_0 + |a_1| + |a_2| + \cdots + |a_n|.$$

Koska on voimassa $n \geq 1$ ja $a_0 \geq 1$, niin minkä tahansa polynomin indeksi on väintään 2. Ainoastaan polynomin x indeksi on 2. Algebrallinen luku 0 toteuttaa polynomiyhtälön $f(x) = x = 0$. Polynomien $x^2, x+1, x-1, 2x$ indeksi on 3. Näiden polynomien perusteella saadaan uudet algebralliset luvut 1 ja -1. Vastaavasti polynomeista, joiden indeksi on 4, saadaan uudet algebralliset luvut $\pm 2, \pm\frac{1}{2}, \pm i$. Nähdään, että kutakin indeksiä kohden on äärellinen määrä polynomeja ja siten myös äärellinen määrä algebrallisia lukuja. Antamalla indeksin kulkea läpi luonnolliset luvut, ja listaamalla uudet algebralliset kuvut kussakin vaiheessa, saadaan numeroitu jono algebrallisia lukuja. Koska kaikilla polynomeilla on indeksi, niin kaikki algebralliset luvut ovat tässä jonossa. Siis algebrallisia lukuja on numeroituva määrä. Lause on siis todistettu.

Kun tiedetään, että kompleksilukujen joukko on ylinumeroituva, niin edellisen lauseen perusteella voidaan päätellä, että transkendenttisten lukujen joukko on ylinumeroituva.

2.5 Joitakin polynomeja koskevia lauseita

Lause 2.9. *Oletetaan, että $f(x)$ ja $g(x)$ ovat polynomeja yli kunnan K siten, että niiden asteet ovat vastaavasti n ja m, ja on voimassa $n \geq m$. Tällöin on olemassa luku $c \in K$ siten, että lauseke*

$$f(x) - cx^{n-m}g(x)$$

on identtisesti nolla, tai se on polynomi, jonka aste on pienempi kuin n.

Todistus. Vrt. [2, s. 28] Olkoon polynomit $f(x)$ ja $g(x)$ määritelty seuraavasti:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0,$$

missä $a_n \neq 0$ ja $b_m \neq 0$. Määritellään $c = a_n/b_m$. Tällöin on voimassa

$$f(x) - cx^{n-m}g(x) = (a_n x^n + \cdots) - \frac{a_n}{b_m}x^{n-m}(b_m x^m + \cdots),$$

mistä termi x^n häviää. On mahdollista, että kaikki termit häviävät, mutta jäjelle jää ainoastaan termejä, jotka ovat pienempää astetta kuin x^n. Lause on siis todistettu.

Lause 2.10. *Oletetaan, että $f(x)$ ja $g(x) \neq 0$ ovat polynomeja yli kunnan K. Tällöin on olemassa polynomit $q(x)$ ja $r(x)$ yli kunnan K siten, että*

$$f(x) = q(x)g(x) + r(x),$$

missä $r(x) \neq 0$ tai $r(x)$ on alempaa astetta kuin $g(x)$.

Todistus. Vrt. [2, s. 29] Jos polynomi $f(x)$ on identtisesti nolla tai alempaa astetta kuin polynomi $g(x)$, niin voidaan asettaa $q(x) = 0$ ja $r(x) = f(x)$. Oletetaan, että $g(x)$ on astetta m. Todistetaan lause induktiolla kaikille polynomeille $f(x)$ joiden aste on $n \geq m$. Oletetaan, että lause on tosi kaikille polynomeille $f(x)$, joiden aste on $0, \ldots, n-1$. Lauseen 2.9 perusteella on olemassa luku $c \in K$ siten, että polynomi

$$f(x) - cx^{n-m}g(x) = f_1(x)$$

on identtisesti nolla tai korkeintaan astetta $n-1$. Siis $f_1(x) = 0$ tai jos $f(x) \neq 0$, niin induktio-oletuksen perusteella

$$f_1(x) = q_1(x)g(x) + r(x),$$

missä $r(x) = 0$ tai $r(x)$ on alempaa astetta kuin $g(x)$. Tällöin saadaan

$$\begin{aligned} f(x) &= f_1(x) + cx^{n-m}g(x) \\ &= (cx^{n-m} + q_1(x))g(x) + r(x) \\ &= q(x)g(x) + r(x). \end{aligned}$$

Lause on siis todistettu.

Lause 2.11. *Oletetaan, että $f(x)$ ja $g(x)$ ovat nollasta eroavia polynomeja yli kunnan K siten, että ne ovat keskenään jaottomia yli kunnan K. Tällöin on olemassa polynomit $s_0(x)$ ja $t_0(x)$ yli kunnan K siten, että on voimassa*

$$1 = s_0(x)f(x) + t_0(x)g(x).$$

Todistus. Vrt. [2, s. 29] Tarkastellaan joukkoa T, joka koostuu kaikista muotoa $s(x)f(x) + t(x)g(x) \neq 0$ olevista polynomeista, missä polynomien $s(x)$ ja $t(x)$ kertoimet ovat kunnassa K. Valitaan joukosta T alinta astetta oleva alkio $d(x)$. Tämä voi olla vakio tai nolla.

Lauseen 2.10 perusteella on olemassa polynomit $q(x)$ ja $r(x)$ siten, että on voimassa

$$r(x) = f(x) - q(x)d(x),$$

missä $r(x) \equiv 0$ tai $r(x)$ on alempaa astetta kuin $d(x)$. Toinen vaihtoehto on pois suljettu, sillä $r(x)$ kuuluu selvästi joukkoon T ja mikään joukkoon T kuuluva polynomi ei oel alempaa astetta kuin $d(x)$. Siis on oltava voimassa $r(x) \equiv 0$. Tällöin on voimassa $f(x) = q(x)d(x)$. Vastaavasti saadaan, että on voimassa $g(x) = q_1(x)d(x)$ jollakin polynomilla $q_1(x)$. Koska polynomit $f(x)$ ja $g(x)$ ovat keskenään jaottomia, niin polynomin $d(x)$ on oltava nollasta eroava vakio. Koska d kuuluu joukkon T, niin se voidaan esittää muodossa

$$d = s_0(x)f(x) + t_0(x)g(x).$$

Jakamalla tämä yhtälö vakiolla d nähdään, että lause on todistettu.

Aikaisemmin on määritelty algebrallinen luku rationaalilukukertoimisen polynomin juurena. Käsite algebrallinen luku voidaan yleistää siten, että puhutaan algebrallisesta luvusta yli kunnan K, jos luku on sellaisen polynomin juuri, jonka kertoimet ovat kunnassa K.

Lause 2.12. *Jos luku θ on algebrallinen yli kunnan K, niin luvun θ minimaalipolynomi on yksikäsitteinen.*

Todistus. Vrt. [2, s. 44] Oletetaan, että luvun θ minimaalipolynomi on $p(x)$ ja polynomi $q(x)$ on mikä tahansa polynomi, jonka kertoimet ovat kunnassa K ja jonka juuri θ on. Tällöin on lauseen 2.10 perusteella olemassa polynomit $g(x)$ ja $h(x)$ yli kunnan K siten, että on voimassa

$$q(x) = g(x)p(x) + h(x),$$

missä $h(x) \equiv 0$ tai $h(x)$ on alempaa astetta kuin p(x). Asetetaan $x = \theta$. Koska on voimassa $p(\theta) = q(\theta) = 0$, niin on oltava $h(\theta) = 0$. Tällöin oltava $h(x) \equiv 0$, sillä muuten $p(x)$ ei olisi minimaalinen. On siis oltava voimassa $p(x)|q(x)$.

Jos $q(x)$ olisi mikä tahansa luvun θ minimaalipolynomi, niin vastaavasti saataisiin, että on voimassa $q(x)|p(x)$. Tällöin olisi oltava voimassa $p(x) = cq(x)$. Koska minimaalipolynomi on pääpolynomi, niin tästä seuraa, että on oltava voimassa $p(x) = q(x)$. Lause on siis todistettu.

Lause 2.13. *Jos $f(x)$ on polynomi yli kunnan K ja θ on algebrallinen luku yli kunnan K siten, että θ on polynomin $f(x)$ juuri, niin luvun θ minimaalipolynomi yli kunnan K on tämän polynomin tekijä.*

Todistus. Todistus seuraa suoraan lauseen 2.12 todistuksesta.

Lause 2.14. *Jos polynomit $f(x)$ ja $g(x)$ ovat keskenään jaottomia yli kunnan K, niin niillä ei ole yhteisiä juuria.*

Todistus. Vrt. [2, s. 45] Jos luku θ olisi polynomien yhteinen juuri, niin luvun θ minimaalipolynomi yli kunnan K jakaisi sekä polynomin $f(x)$ että polynomin $g(x)$, jolloin ne siis eivät olisi keskenään jaottomia. Lause on siis todistettu.

Lause 2.15. *Jaottomalla astetta n olevalla polynomilla yli kunnan K on n kappaletta toisistaan eroavia juuria.*

Todistus. Vrt. [2, s. 45] Tehdään vastaoletus, että jaottomalla polynomilla $f(x)$ on kaksi juurta, jotka ovat samat. Tällöin voidaan kirjoittaa

$$f(x) = a_n(x-r)^2 g(x).$$

Derivoimalla edellinen saadaan

$$f'(x) = a_n(x-r)^2 g'(x) + 2a_n(x-r)g(x),$$

mistä nähdään, että $f'(r) = 0$. Lauseen 2.13 perusteella f on luvun r minimaalipolynomin monikerta. Tämä ei voi pitää paikkaansa, koska $f'(x)$ on alempaa astetta kuin $f(x)$. Lause on siis todistettu.

Määritelmä 2.7. Oletetaan, että luku θ on algebrallinen luku yli kunnan K ja polynomi $p(x)$ on luvun θ minimaalipolynomi yli kunnan K. Polynomin $p(x)$ juuria $\theta_1, \theta_2, \ldots, \theta_n$, missä $\theta_1 = \theta$, sanotaan luvun θ *konjugaateiksi yli kunnan K*.

Algebrallisen luvun θ minimaalipolynomi $p(x)$ on jaoton polynomi, koska muuten polynomilla olisi tekijä, jonka juuri luku θ on, ja tämä tekijä olisi alempaa astetta kuin $p(x)$. Lauseen 2.15 perusteella luvun θ konjugaatit ovat toisistaan eroavia.

3 Yleistetty Lindemannin lause

3.1 Yleistetyn Lindemannin lauseen esittely

Seuraava lause on yleistetty Lindemannin lause.

Lause 3.1. *Jos luvut $\alpha_1, \alpha_2, \ldots, \alpha_m$ ovat toisistaan eroavia algebrallisia lukuja, niin luvut $e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_m}$ ovat lineaarisesti riippumattomia yli algebrallisten lukujen kunnan. Toisin sanoen yhtälöllä*

$$\sum_{j=1}^{m} a_j e^{\alpha_j} = 0, \tag{3.1}$$

missä luvut a_j ovat algebrallisia, ei ole sellaista ratkaisua, että jokin a_j olisi nollasta eroava.

Edellä olevan lauseen todistus esitetään jatkossa. Seuraavassa esitetään lauseen todistamiseksi tarvittavia lauseita.

3.2 Yleistetyn Lindemannin lauseen todistamiseen tarvittavia lauseita

Lause 3.2. *Oletetaan, että luvut $\beta_1, \beta_2, \ldots, \beta_n$ ovat rationaalilukukertoimisen polynomiyhtälön*

$$f(x) = bx^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_n = 0$$

juuret. Jos $P(x_1, x_2, \ldots, x_n)$ on muuttujien $x_1, x_2, \ldots, x_n$ symmetrinen rationaalilukukertoiminen polynomi, niin $P(\beta_1, \beta_2, \ldots, \beta_n)$ on rationaaliluku. Lisäksi jos polynomi P on kokonaislukukertoiminen ja astetta t, niin $b^tP(\beta_1, \beta_2, \ldots, \beta_n)$ on kokonaisluku.

Todistus. Vrt. [1, s. 119]. Luvut $b\beta_1, b\beta_2, \ldots, b\beta_n$ ovat polynomiyhtälön

$$b^{n-1}f(x/b) = x^n + c_1x^{n-1} + bc_2x^{n-2} + \cdots + b^{n-1}c_n = 0$$

juuret, joten lukujen $b\beta_1, b\beta_2, \ldots, b\beta_n$ symmetriset alkeisfunktiot ovat kokonaislukuja. Jos $p(x_1, x_2, \ldots, x_n)$ on rationaalilukukertoiminen homogeeninen symmetrinen polynomi, jonka aste $r \leq t$, niin on voimassa

$$b^r p(\beta_1, \beta_2, \ldots, \beta_n) = p(b\beta_1, b\beta_2, \ldots, b\beta_n),$$

joten $b^t p(\beta_1, \beta_2, \ldots, \beta_n)$ on kokonaisluku. Jakamalla polynomi P homogeenisten polynomien p summaksi todetaan, että myös $b^tP(\beta_1, \beta_2, \ldots, \beta_n)$ on kokonaisluku. Lause on siis todistettu.

Lause 3.3. *Tutkitaan muuttujien $y_1, y_2, \ldots, y_m$ polynomeja $P_1, P_2, \ldots, P_q$,*

$$P_j = f_1(x_j)y_1 + f_2(x_j)y_2 + \cdots + f_m(x_j)y_m, \qquad j = 1, 2, \ldots, q,$$

missä kertoimet $f_i(x_j)$ ovat polynomeja yli kunnan K. Jos muodostetaan näiden polynomien tulo siten, että y termit kootaan yhteen, niin kertoimet ovat muuttujien $x_1, x_2, \ldots, x_q$ symmetrisiä polynomeja.

Todistus. Vrt. [1, s. 119]. Tarkastellaan tuloa

$$P_1P_2 \cdots P_q = \sum_{\substack{i_j=1 \\ i_1 \leq i_2 \leq \cdots \leq i_q}}^{m} cy_{i_1}y_{i_2} \cdots y_{i_q}. \tag{3.2}$$

Ehto $i_1 \leq i_2 \leq \cdots \leq i_q$ johtuu siitä, että termit on yhdistetty. On todistettava, että kertoimet $c = c(x_1, \ldots, x_q)$ ovat symmetrisiä muuttujien $x_1, \ldots, x_q$ suhteen. Mikä tahansa muuttujien $x_1, \ldots, x_q$ permutaatio kohdistettuna yhtälöön (3.2) jättää vasemman puolen ennalleen, koska se vain permutoi polynomeja $P_1, P_2, \ldots, P_q$. Siis myös oikean puolen on säilyttävä samana, joten kertoimet c pysyvät samana. Siis kertoimet ovat symmetrisiä polynomeja ja lause on siis todistettu.

Seuraavassa oletetaan tunnetuksi kuntalaajennuksen käsite.

Määritelmä 3.1. Jos kunta K on rationaalilukujen kunnan $\mathbb{Q}$ äärellinen laajennus, niin sanotaan, että K on algebrallinen kunta.

Lause 3.4. *Jos K on algebrallinen kunta ja luku θ on algebrallinen yli kunnan K, niin mikä tahansa kuntalaajennuksen $K(\theta)$ alkio β voidaan esittää yksikäsitteisesti muodossa*

$$\beta = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1},$$

missä $a_i \in K$ ja n on luvun θ aste/K.

Todistus. Vrt. [2, s. 47]. Voidaan olettaa, että $\beta = f(\theta)/g(\theta)$, missä $g(\theta) \neq 0$. Oletetaan, että luvun θ minimaalipolynomi yli kunnan K on $p(x)$. Tällöin $p(x)$ on jaoton ja $p(x) \nmid g(x)$, koska muuten olisi $g(\theta) = 0$. Siis polynomit $p(x)$ ja $g(x)$ ovat keskenään jaottomia. Lauseen 2.11 perusteella tällöin on olemassa polynomit $s(x)$ ja $t(x)$ siten, että $s(x)p(x)+t(x)g(x) = 1$. Asetetaan $x = \theta$. Koska $p(\theta) = 0$, niin on voimassa $1/g(\theta) = t(\theta)$. Tällöin saadaan

$$\beta = \frac{f(\theta)}{g(\theta)} = f(\theta)t(\theta),$$

mikä on siis on luvun θ polynomi. Merkitään $\beta = h(\theta)$.

Lauseen 2.10 perusteella on olemassa polynomit $q(x)$ ja $r(x)$ siten, että on voimassa $h(x) = q(x)p(x) + r(x)$, missä $r(x) \equiv 0$ tai polynomin $r(x)$ aste on pienempi kuin polynomin $p(x)$. Koska on voimassa $p(\theta) = 0$, niin saadaan

$$\beta = h(\theta) = r(\theta).$$

Siis luku β voidaan kirjoittaa luvun θ polynomina ja tämän polynomin aste on korkeintaan $n - 1$.

On vielä osoitettava, että tämä polynomi on yksikäsitteinen. Tehdään vastaoletus, että on olemassa polynomista $r(x)$ eroava korkeintaan astetta $n - 1$ oleva polynomi $r_1(x) \in K[x]$ ja $\beta = r_1(\theta)$. Tällöin on voimassa $r(\theta) - r_1(\theta) = 0$, joten luku θ toteuttaa polynomiyhtälön $r(x) - r_1(x) = 0$. Koska luku θ ei toteuta mitään polynomiyhtälöä, jonka aste on pienempi kuin n, niin polynomien $r_1(x)$ ja $r(x)$ on oltava samat. Siis vastaoletus on väärä, joten polynomi $r(x)$ on yksikäsitteinen. Lause on siis todistettu,

Lause 3.5. *Oletetaan, että K on algebrallinen kunta. Jos luvut $\alpha_1, \alpha_2, \ldots, \alpha_s$ ovat algebrallisia yli kunnan K, niin on olemassa luku γ, joka on algebrallinen yli kunnan K siten, että luvun γ määräämä kuntalaajennus on sama kuin lukujen $\alpha_1, \alpha_2, \ldots, \alpha_s$ määrämä laajennus, toisin sanoen on voimassa*

$$K(\gamma) = K(\alpha_1, \alpha_2, \ldots, \alpha_s).$$

Todistus. Vrt. [2, s. 48]. Lauseen todistamiseksi riittää osoittaa, että jos luvut α ja β ovat algebrallisia yli kunnan K, niin on olemassa luku γ joka on algebrallinen yli kunnan K ja on voimassa $K(\gamma) = K(\alpha, \beta)$. Tämä seuraa siitä, että jos $L = K(\alpha_1, \alpha_2, \alpha_3)$, niin voidaan kirjoittaa $L = K(\alpha_1, \alpha_2)(\alpha_3)$, ja käyttää lausetta kahdesti.

Oletetaan, että $\alpha_1, \ldots, \alpha_l$ ja $\beta_1, \ldots, \beta_m$ ovat vastaavasti lukujen α ja β konjugaatit yli kunnan K, numeroituna siten, että $\alpha_1 = \alpha$ ja $\beta_1 = \beta$. Jos $k \neq 1$, niin $\beta_k \neq \beta$, koska konjugaatit yli kunnan K ovat toisistaan eroavia. Tällöin on voimassa jokaiselle indeksille i ja jokaiselle indeksille $k \neq 1$, että yhtälöllä

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1$$

on korkeintaan yksi ratkaisu $x \in F$. Koska näitä yhtälöitä on äärellinen määrä, on ratkaisuja x vain äärellinen määrä. Tällöin voidaan valita kuntaan K kuuluva luku $c \neq 0$ siten, että se eroaa kaikista ratkaisuista x. Tällöin on voimassa

$$\alpha_i + c\beta_k \neq \alpha + c\beta$$

kaikilla indekseillä i ja kaikilla indekseillä $k \neq 1$. Asetetaan $\gamma = \alpha + c\beta$. Näytetään, että on voimassa $K(\gamma) = K(\alpha, \beta)$, jolloin lause on todistettu.

Ensiksi todetaan, että jokainen kunnan $K(\gamma)$ alkio kuuluu kuntaan $K(\alpha, \beta)$, sillä lauseen 3.4 perusteella jokainen kunnan $K(\gamma)$ alkio voidaan kirjoittaa muodossa

$$a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1} = a_0 + a_1(\alpha + c\beta) + \cdots + a_{n-1}(\alpha + c\beta)^{n-1},$$

missä oikea puoli kuuluu selvästi kuntaan $K(\alpha, \beta)$.

On näytettävä, että jokainen kunnan $K(\alpha, \beta)$ alkio kuuluu kuntaan $K(\gamma)$. Tämä voidaan osoittaa, jos voidaan todistaa, että luvut α ja β kuuluvat kuntaan $K(\gamma)$. Tällöin ne voidaan esittää muodoissa $\alpha = r(\gamma)$ ja $\beta = s(\gamma)$, missä polynomien $r(x)$ ja $s(x)$ kertoimet kuuluvat kuntaan K. Jokainen kunnan $F(\alpha, \beta)$ alkio on tällöin muotoa

$$\frac{u(\alpha, \beta)}{v(\alpha, \beta)} = \frac{u(r(\gamma), s(\gamma))}{v(r(\gamma), s(\gamma))},$$

missä $u(x, y)$ ja $v(x, y)$ ovat polynomeja, joiden kertoimet ovat kunnassa K. Tämä osamäärä kuuluu varmasti kuntaan $K(\gamma)$. Riittää osoittaa, että luku β kuuluu kuntaan $K(\gamma)$, sillä tällöin myös $\alpha = \gamma - c\beta$ kuuluu.

Oletetaan, että $f(x)$ ja $g(x)$ ovat vastaavasti lukujen α ja β minimaalipolynomit. Koska on voimassa $f(\gamma - c\beta) = f(\alpha) = 0$, niin luku β toteuttaa yhtälöt $g(x) = 0$ ja $f(\gamma - cx) = 0$. Luku β on polynomien $g(x)$ ja $f(\gamma - cx)$ ainoa yhteinen juuri, sillä polynomin $g(x)$ juuret ovat $\beta_1, \ldots, \beta_m$, ja jos olisi voimassa $f(\gamma - c\beta_i) = 0$ jollakin indeksillä $i \neq 1$, niin luku $\gamma - c\beta_i$ olisi yksi luvuista α_j, mikä on ristiriidassa luvun c valinnan kanssa.

Polynomit $g(x)$ ja $f(\gamma - cx)$ ovat muuttujan x polynomeja, joiden kertoimet ovat kunnassa $K(\gamma)$, ja luku β on niiden ainoa yhteinen juuri. Oletetaan, että $h(x)$ on luvun β minimipolynomi yli kunnan $K(\gamma)$. Lauseen 2.13 perusteella on oltava voimassa $h(x)|g(x)$ ja $h(x)|f(\gamma - cx)$, kun kertoimet ovat kunnassa $K(\gamma)$. Polynomi $h(x)$ ei voi korkeampaa kuin ensimmäistä astetta, koska muuten polynomeilla $g(x)$ ja $f(\gamma - cx)$ olisi yhteisiä juuria enemmän kuin yksi. Täten oltava $h(x) = \xi x + \delta$, missä luvut ξ ja δ kuuluvat kuntaan $K(\gamma)$. Koska $h(\beta) = 0$, niin $\beta = -\delta/\xi$, joten siis luku β kuuluu kuntaan $K(\gamma)$. Lause on siis todistettu.

Määritelmä 3.2. Algebrallista kuntaa $\mathbb{Q}(\theta)$ sanotaan *normaaliksi*/$\mathbb{Q}$, jos kunnassa $\mathbb{Q}$ jaottomalla polynomilla, jolla on yksi juuri kunnassa $\mathbb{Q}(\theta)$, on kaikki juuret kunnassa $\mathbb{Q}(\theta)$.

Lause 3.6. *Oletetaan, että $\alpha_1, \alpha_2, \ldots \alpha_s$ ovat algebrallisia lukuja yli kunnan $\mathbb{Q}$. Tällöin on olemassa algebrallinen luku θ yli kunnan $\mathbb{Q}$ siten, että kuntalaajennuksille on voimassa $\mathbb{Q}(\alpha_1, \alpha_2, \ldots \alpha_s) \subseteq \mathbb{Q}(\theta)$, ja $\mathbb{Q}(\theta)$ on normaali.*

Todistus. Vrt. [1, s. 121]. Lauseen 3.5 perusteella on olemassa algebrallinen luku γ siten, että $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha_1, \ldots \alpha_s)$. Oletetaan, että $h(x)$ on luvun γ minimaalipolynomi/ $\mathbb{Q}$, jonka juuret ovat $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_m$. Edelleen lauseen 3.5 perusteella on olemassa luku θ, jolle on voimassa

$$\mathbb{Q}(\theta) = \mathbb{Q}(\gamma_1, \gamma_2, \ldots, \gamma_m) \supset \mathbb{Q}(\gamma_1) = \mathbb{Q}(\alpha_1, \alpha_2, \ldots \alpha_s).$$

On todistettava, että $\mathbb{Q}(\theta)$ on normaali. Oletetaan, että $g(x)$ on jaoton polynomi / $\mathbb{Q}$ jolla on juuri $\rho \in \mathbb{Q}(\theta)$. Tällöin $g(x)$ on luvun ρ minimaalipolynomi. Lauseen 3.4 yleistyksen perusteella on olemassa rationaalilukukertoiminen polynomi f siten, että $\rho = f(\gamma_1, \gamma_2, \ldots \gamma_m)$. Muodostetaan polynomi

$$G(x) = \prod (x - f(\gamma_{i_1}, \gamma_{i_2}, \ldots, \gamma_{i_m})),$$

joka on muuttujan x astetta $m!$ oleva polynomi ja jossa tulo on otettu yli kaikkien indeksien $i_j \in 1, 2, \ldots, m$ permutaatioiden. Polynomin $G(x)$ kertoimet ovat juurien $f(\gamma_{i_1}, \gamma_{i_2}, \ldots \gamma_{i_m})$ symmetrisiä polynomeja. Mikä tahansa lukujen $\gamma_{i_1}, \gamma_{i_2}, \ldots \gamma_{i_m}$ permutaatio permutoi polynomit $f(\gamma_{i_1}, \gamma_{i_2}, \ldots \gamma_{i_m})$ keskenään. Siis polynomin $G(x)$ kertoimet ovat lukujen $\gamma_1, \gamma_2, \ldots \gamma_m$ symmetrisiä polynomeja ja ovat siis lauseen 3.2 perusteella rationaalilukuja. Luku ρ on polynomien $g(x)$ ja $G(x)$ yhteinen juuri, ja siten minimaalipolynomi $g(x)$ on polynomin $G(x)$ tekijä. Koska polynomin $G(x)$ kaikki juuret ovat kunnassa $\mathbb{Q}(\theta)$, niin myös polynomin $g(x)$ juurten täytyy olla kunnassa $\mathbb{Q}(\theta)$. Lause on siis todistettu.

Oletetaan, että normaalin kuntalaajennuksen $\mathbb{Q}(\theta)/\mathbb{Q}$ aste on n. Siis luvun θ minimaalipolynomi $f(x)$ yli kunnan $\mathbb{Q}$ on jaoton polynomi yli kunnan $\mathbb{Q}$, joka voidaan esittää muodossa

$$f(x) = x^n + b_1 x^{n-1} + b_2 x^{n-2} + \cdots + b_n. \tag{3.3}$$

Jokainen kunnan $\mathbb{Q}(\theta)$ alkio voidaan esittää luvun θ polynomina, jonka aste on korkeintaan $n-1$. Merkitään polynomin (3.3) juuria seuraavasti: $\theta = \theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$. Koska kuntalaajennus $\mathbb{Q}(\theta)$ / $\mathbb{Q}$ on normaali, niin kaikki juuret ovat kunnassa $\mathbb{Q}(\theta)$. Täten nämä *konjugaatit* voidaan kirjoittaa muodossa

$$\theta^{(j)} = h_j(\theta) \qquad j = 1, 2, \ldots, n, \tag{3.4}$$

missä polynomien $h_j(\theta)$ kertoimet ovat kunnassa $\mathbb{Q}$. Polynomien $h_1(\theta), h_2(\theta), \ldots, h_n(\theta)$ symmetriset alkeispolynomit ovat myös luvun θ polynomeja siten, että kertoimet ovat kunnassa $\mathbb{Q}$. Täten ne saadaan palautettua rationaaliluvuiksi $-b_1, b_2, -b_3, \ldots, (-1)^n b_n$ kun eliminoidaan θ^n ja korkeammat potenssit käyttämällä yhtälöä

$$\theta^n = -b_1\theta^{n-1} - b_2\theta^{n-2} - \cdots - b_n.$$

Luku $\theta^{(2)}$ toteuttaa saman yhtälön, ja siksi polynomien

$$h_1(\theta^{(2)}), h_2(\theta^{(2)}), \ldots, h_n(\theta^{(2)})$$

symmetriset alkeispolynomit ovat myös $-b_1, b_2, -b_3, \ldots, (-1)^n b_n$. Täten todetaan, että luvut

$$h_1(\theta^{(2)}), h_2(\theta^{(2)}), \ldots, h_n(\theta^{(2)})$$

ovat myös polynomin (3.3) juuria ja siten jossain järjestyksessä samat kuin $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$. Toisinsanoen, jos lukuja $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ käsitellään luvun θ polynomeina, niin korvaamalla luku θ luvulla $\theta(2)$ sadaan joku konjugaattien $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ permutaatio. Koska $\theta^{(2)}$ ei ole missään erityisasemassa, niin sama pätee kaikkiin lukuihin $\theta^{(i)}$.

Lause 3.7. *Olkoon $\mathbb{Q}(\theta)/\mathbb{Q}$ normaali algebrallinen astetta n oleva kuntalaajennus ja olkoot luvun θ konjugaatit $\theta = \theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$. Nämä konjugaatit käsitettynä luvun θ polynomeiksi permutoituvat, jos luku θ korvataan luvulla $\theta^{(i)}$. Yleisemmin, jos $F(x)$ on rationaalinen polynomi, niin joukko*

$$F(\theta^{(1)}), F(\theta^{(2)}), \ldots, F(\theta^{(n)}) \tag{3.5}$$

permutoituu, jos luku θ korvataan luvulla $\theta^{(i)}$.

Todistus. Vrt. [1, s. 123]. Joukkoa (3.5) voidaan pitää luvun θ polynomeina yhtälön (3.4) perusteella. Ennen lausetta tehtyjen tarkastelujen perusteella, korvaamalla θ luvulla $\theta^{(i)}$ permutoidaan konjugaatit $\theta^{(1)}, \ldots, \theta^{(n)}$ ja siten myös luvut (3.5). Lause on siis todistettu.

Mikä tahansa kunnan $\mathbb{Q}(\theta)$ alkio γ voidaan esittää luvun θ rationaalilukukertoimisena polynomina $\gamma = F(\theta)$. Lukuja (3.5) sanotaan luvun γ konjugaateiksi kunnassa $\mathbb{Q}(\theta)$. Nämä konjugaatit voidaan kirjoittaa $\gamma = \gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(n)}$. Näiden konjugaattien symmetriset alkeispolynomit ovat myös lukujen $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ symmetrisiä polynomeja ja siten rationaalilukuja. Tämä todistaa seuraavan lauseen. Vrt. [1, s. 123].

Lause 3.8. *Mikä tahansa kunnan $\mathbb{Q}(\theta)$ alkio γ, ja sen konjugaatit kunnassa $\mathbb{Q}(\theta)$, toteuttavat astetta n olevan kokonaislukukertoimisen polynomiyhtälön $g(x) = 0$.*

Lause 3.9. *Tarkastellaan funktioita*

$$f(x) = \sum_{j=1}^{m} a_j x^{\alpha_j}, \qquad g(x) = \sum_{j=1}^{t} b_j x^{\beta_j},$$

missä kertoimet a_j ja b_j ovat nollasta eroavia kompleksilukuja ja eksponentit α_j ja β_j ovat algebrallisia lukuja. Lisäksi luvut α_j ovat keskenään erisuuria ja samoin luvut β_j. Jos muodostetaan tulo $f(x)g(x)$ ja yhdistetään kaikki termit joissa on sama eksponentti, niin tuloksena syntyvässä lausekkeessa on ainakin yksi nollasta eroava kerroin.

Todistus. Vrt. [1, s. 124]. Soveltamalla lausetta 3.6 lukuihin

$$\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_t$$

todetaan, että on olemassa normaali kuntalaajennus $\mathbb{Q}(\theta)/\mathbb{Q}$, joka sisältää kaikki nämä luvut. Merkitään kuntalaajennuksen astetta luvulla n. Lauseen 3.4 perusteella voidaan jokainen luvuista α_j kirjoittaa yksikäsitteisesti luvun θ rationaalilukukertoimisena polynomina

$$\alpha_j = \sum_{i=0}^{n-1} r_{j_i} \theta^i.$$

Järjestetään luvut α_j siten, että α_j edeltää lukua α_k, jos ensimmäinen nollasta eroa termi jonossa

$$r_{j_0} - r_{j_0}, r_{j_1} - r_{j_1}, r_{j_2} - r_{j_2}, \ldots$$

on positiivinen. Muutetaan merkintöjä vastaamaan tätä järjestystä siten, että α_1 on ensimmäinen luvuista α_j ja vastaavasti β_1 on ensimmäinen luvuista β_j. Tällöin $\alpha_1 + \beta_1$ on ensimmäinen summista $\alpha_j + \beta_k$. Tällöin tulon $f(x)g(x)$ termin $a_1 b_1 x^{\alpha_1 + \beta_1}$ eksponentti on poikkeaa muista eksponenteista, joten tätä termiä ei voi yhdistää muiden termien kanssa, joten tämä termi ei katoa. Lause on siis todistettu.

Lause 3.10. *Jos luvut $\alpha_1, \alpha_2, \ldots, \alpha_m$ ovat keskenään erisuuria algebrallisia lukuja, niin luvut $e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_m}$ ovat lineaarisesti riippumattomia rationaalilukujen kunnassa.*

Todistus. Vrt. [1, s. 124]. Tehdään vastaoletus, että on voimassa

$$\sum_{j=1}^{m} a_j e^{\alpha_j} = 0, \tag{3.6}$$

missä kertoimet ovat rationaalilukuja ja ainakin yksi kerroin on nollasta eroava. Jättämällä pois termit joissa kerroin on nolla, ja muuttamalla vastaavasti merkintöjä, voidaan olettaa, että mikään kertoimista ei ole nolla. Kertomalla (3.6) sopivalla kokonaisluvulla saadaan yhtälö, jossa kaikki kertoimet ovat nollasta eroavia kokonaislukuja. Lauseen 3.6 perusteella voidaan muodostaa normaali kuntalaajennus $\mathbb{Q}(\theta)$, joka sisältää luvut $\alpha_1, \alpha_2, \ldots, \alpha_m$. Oletetaan kuntalaajennuksen asteen olevan n, jolloin jokainen α_j voidaan esittää yksikäsitteisenä luvun θ rationaalilukukertoimisena polynomina

$$\alpha_j = \sum_{i=0}^{n-1} r_{j_i}\theta^i \qquad j = 1, 2, \ldots, m.$$

Kuten aikaisemmin, niin merkitään luvun θ konjugaatteja

$$\theta = \theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}.$$

Tällöin lukujen α_j konjugaatit kunnassa $\mathbb{Q}(\theta)$ ovat

$$\alpha_j^{(k)} = \sum_{i=0}^{n-1} r_{j_i}(\theta^{(k)})^i, \qquad j = 1, 2, \ldots, m, \qquad k = 1, 2, \ldots, n.$$

Samoin kuin θ, jokainen $\theta^{(k)}$ on astetta n oleva algebrallinen luku, joten nämä lukujen $\theta^{(k)}$ polynomit ovat yksikäsitteisiä. Täten oletuksesta, että luvut α_j ovat toisistaan eroavia, seuraa, että kiinteällä luvun k arvolla luvut $\alpha_j^{(k)}$ ovat toisistaan eroavia.

Muodostetaan tulo

$$0 = \prod_{k=1}^{n} \sum_{j=1}^{m} a_j e^{\alpha_j^{(k)}} = \sum_{j=0}^{r} c_j e^{\beta_j}. \tag{3.7}$$

Tulo on nolla yhtälön (3.6) perusteella, sillä $\alpha_j^{(1)}$ on vain toinen merkintätapa luvulle α_j. Yhtälön (3.7) oikeapuoli saadaan suorittamalla kertominen ja keräämällä yhteen kaikki termit joissa on sama eksponentti. Siten kertoimet β_j ovat toisistaan eroavia. Koska kertoimet a_j ovat kokonaislukuja, niin samoin ovat myös kertoimet c_j. Koska kertoimet a_j ovat nollasta eroavia, niin laajentamalla lause 3.9 k-kertaiselle tulolle voidaan todeta, että ainakin yksi kertoimista c_j on nollasta eroava. Oletetaan, että $c_0 \neq 0$.

Lauseen 3.7 perusteella, kiinteällä luvun j arvolla, n konjugaattia $\alpha_j^{(k)}$ permutoituvat kun luku θ korvataan luvulla $\theta^{(i)}$. Kyseisen lauseen todistuksen perusteella permutaatio ei riipu indeksistä j. Siis luvun θ korvaaminen luvulla $\theta^{(i)}$ permutoi tekijät tulossa (3.7) niin, että tulo kokonaisuudessaan pysyy samana. Luvun θ korvaaminen luvulla $\theta^{(i)}$ aiheuttaa yhtälön (3.7) oikeassa puolessa lukujen β_j korvautumisen konjugaateilla $\beta_j^{(i)}$. Täten yhtälön (3.7) perusteella saadaan

$$0 = \sum_{j=0}^{r} c_j e^{\beta_j^1} = \sum_{j=0}^{r} c_j e^{\beta_j^2} = \cdots = \sum_{j=0}^{r} c_j e^{\beta_j^n}. \tag{3.8}$$

Aikaisemmin todettiin, että luvut $\beta_j^{(1)}$ ovat toisistaan eroavia. Täten luvut $\beta_j^{(i)}$ ovat toisistaan eroavia kiinteällä indeksin i arvolla.

Kerrotaan yhtälössä (3.8) ensimmäinen summa luvulla $e^{-\beta_0^{(1)}}$, toinen summa luvulla $e^{-\beta_0^{(2)}}$, ..., viimeinen summa luvulla $e^{-\beta_0^{(n)}}$. Määritellään

$$\gamma_j^{(i)} = \beta_j^{(i)} - \beta_0^{(i)}, \qquad i = 1, 2, \ldots, n, \qquad j = 1, 2, \ldots, r. \tag{3.9}$$

Koska luvut $\beta_j^{(i)}$ ovat toisistaan eroavia kiinteällä indekisn i arvolla, niin mikään luvuista $\gamma_j^{(i)}$ ei ole nolla. Täten yhtälö (3.8) voidaan kirjoittaa

$$0 = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(1)}} = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(2)}} = \cdots = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(n)}} \tag{3.10}$$

Lauseen 3.8 perusteella konjugaatit $\gamma_j^{(1)}, \gamma_j^{(2)}, \ldots, \gamma_j^{(n)}$ ovat kokonaislukukertoimisen polynomin juuria. Merkitään tätä polynomia

$$g_j(z) = b_j z^n + \cdots = b_j \prod_{i=1}^{n} (z - \gamma_j^i), \qquad j = 1, 2, \ldots, r. \tag{3.11}$$

Voidaan olettaa, että kokonaisluvut $b_j > 0$. Koska kaikki luvut γ_j^i) ovat nollasta eroavia, niin polynomien vakiotermit $g_j(0)$ ovat nollasta eroavia kokonaislukuja.

Edellä on todistettu lauseen 3.10 algebrallinen osuus. Seuraavaksi tarkastellaan analyyttistä osuutta. Oletetaan, että $F(z)$ on mielivaltaisen polynomin $f(z)$ ja sen derivaattojen summa. Siis

$$F(z) = f(z) + f'(z) + f^{(2)}(z) + \cdots .$$

Tällöin saadaan yhtälöt

$$(F(z)e^{-z})' = -f(z)e^{-z},$$

$$F(b) - F(0)e^b = -e^b \int_0^b f(z)e^{-z}dz.$$

Korvaamalla b luvuilla $\gamma_j^{(i)}$, kertomalla saadut yhtälöt luvulla c_j ja summaamalla yli indeksien $j = 1, \ldots, r$ ja $i = 1, \ldots, n$ saadaan

$$\sum_{j=1}^{r}\sum_{i=1}^{n} c_j F(\gamma_j^{(i)}) - F(0)\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} = -\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z)e^{-z}dz.$$

Käyttämällä yhtälöä (3.10) edellä olevan lausekkeen toiseen termiin saadaan

$$\sum_{j=1}^{r} c_j \left(\sum_{i=1}^{n} F(\gamma_j^{(i)}) \right) - nc_0F(0) = -\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z)e^{-z}dz. \tag{3.12}$$

Määritellään polynomi $f(z)$ seuraavasti

$$f(z) = (b_1 b_2 \cdots b_r)^{prn} z^{p-1} \left(\prod_{j=1}^{r} g_j(z) \right)^p /(p-1)!, \tag{3.13}$$

missä luku p on myöhemmin määriteltävä alkuluku. Kun alkuluku p valitaan riittäävän suureksi, niin yhtälön (3.13) vasenpuoli on nollasta eroava kokonaisluku, kun taas oikea puoli on itseisarvoltaan mielivaltaisen pieni. Täten saadan ristiriita, joka todistaa lauseen oikeaksi.

Johtuen tekijästä z^{p-1} polynomin $f(z)$ lausekkeessa, on voimassa yhtälöt

$$0 = f(0) = f'(0) = f^{(2)}(0) = \cdots = f^{(p-2)}(0),$$
$$f^{(p-2)}(0) = (b_1 b_2 \cdots b_r)^{prn} \prod_{j=1}^{r} (g_j(z))^p.$$

Valitaan alkuluku p siten, että on voimassa epäyhtälöt $p > b_j$ ja $p > g_j(0)$, kun $j = 1, 2, \ldots, r$. Tällöin p ei ole nollasta eroavan kokonaisluvun $f^{(p-2)}(0)$ jakaja.

Osoitetaan, että kun $t \geq p$, niin $f^{(t)}(0)$ on luvulla p jaollinen kokonaisluku. Polynomia $f(z)$ voidaan pitää muuttujan z potenssien summana, siten, että polynomin $f^{(t)}(z)$ jokaisen termin kertoimessa on t kappaletta peräkkäistä kokonaislukua seurauksena derivoinneista. Kun $t \geq p$, niin tulo, jossa on t kappaletta peräkkäisiä kokonaislukuja, on jaollinen luvulla $p!$, ja tällöin jakaja $(p-1)!$ polynomin $f(z)$ lausekkeessa kumoutuu. Voidaan kirjoittaa

$$f^{(t)} = p(b_1 b_2 \cdots b_r)^{prn} G_t(z), \tag{3.14}$$

missä $G_t(z)$ on kokonaislukukertoiminen polynomi, jonka asteluku on korkeintaan $prn - 1$. Siis $f^{(t)}(0)$ on kokonaisluku joka on jaollinen luvulla p. Asetetaan luvulle p ehdot $p > n$ ja $p > c_0$, jolloin p ei jaa kokonaislukua $nc_0F(0)$ yhtälössä (3.12).

Seuraavaksi osoitetaan, että yhtälön (3.12) vasemman puolen termi

$$\sum_{j=1}^{r} c_j \left(\sum_{i=1}^{n} F(\gamma_j^{(i)}) \right)$$

on kokonaisluku, joka on jaollinen luvulla p. Osoitetaan, että summa

$$\sum_{i=1}^{n} F(\gamma_j^{(i)}) = \sum_{i=1}^{n} f(\gamma_j^{(i)}) + \sum_{i=1}^{n} f'(\gamma_j^{(i)}) + \sum_{i=1}^{n} f^{(2)}(\gamma_j^{(i)}) + \cdots$$

on luvun p monikerta. Koska $f(z)$ sisältää tekijän $(g_j(z))^p$, niin yhtälön (3.11) perusteella saadaan

$$f(\gamma_j^{(i)}) = 0, f'(\gamma_j^{(i)}) = 0, \ldots, f^{(p-1)}(\gamma_j^{(i)}) = 0.$$

Korkeammille derivaatoille saadaan yhtälön (3.14) perusteella

$$\sum_{i=1}^{n} f^{(t)}(\gamma_j^{(i)}) = p\sum_{i=1}^{n}(b_1 b_2 \cdots b_r)^{prn} G_t(\gamma_j^{(i)}), \qquad t \geq p. \tag{3.15}$$

Polynomi $G_t(z)$ on korkeintaan astetta $prn-1$, joten ottaen huomioon tekijän b_j^{prn} saadaan lauseen 3.2 perusteella, että (3.15) on kokonaisluku, joka on jaollinen luvulla p.

On siis osoitettu, että kaksi lauseketta yhtälön (3.12) vasemmalla puolella ovat kokonaislukuja, ja ensimmäinen on luvun p monikerta ja toinen ei ole jaollinen luvulla p. Siis yhtälön (3.12) vasen puoli on nollasta eroava kokonaisluku. Siis jos yhtälön puolista otetaan itseisarvo, on voimassa

$$1 \leq \left| \sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z)e^{-z}dz \right|. \tag{3.16}$$

Määritellään luvut

$$m1 = max|c_j|, \qquad m_2 = max|e^{\gamma_j^{(i)}}|, \qquad m_3 = |\gamma_j^{(i)}|,$$

kaikilla indeksien i ja j arvoilla. Määritellään pisteiden $z = 0$ ja $z = \gamma_j^{(i)}$ välisellä suoralla

$$m_4 = max|e^{-z}|, \qquad m_5 = max|\prod_{j=1}^{r} g_j(z)|,$$

kaikilla indeksien i ja j arvoilla. Huomataan, että $m_3^{p-1} = max|z^{p-1}|$ samalla suoralla. Tällöin epäyhtälön (3.16) ja yhtälön (3.13) perusteella saadaan

$$\begin{aligned} 1 &\leq rnm_1m_2m_3m_4(b_1b_2\cdots b_r)^{prn}m_3^{p-1}m_5^p/(p-1)! \\ &= rnm_1m_2m_4(b_1^{rn}b_2^{rn}\cdots b_r^{rn}m_3m_5)^p/(p-1)!. \end{aligned}$$

Luvut $r, n, m_1, m_2, m_3, m_5, b_1, b_2, \cdots, b_r$ eivät riipu luvusta p, joten jälkimmäinen lauseke lähenee nollaa, kun p lähenee ääretöntä. Tämä on ristiriita, ja lause on siis todistettu.

Voidaan osoittaa, että lause 3.1 on lauseen 3.10 seuraus.

3.3 Yleistetyn Lindemannin lauseen todistus

Lauseen 3.1 todistus.

Vrt. [1, s. 130]. Tehdään vastaoletus, että on voimassa yhtälö (3.1) siten, että mikään algebrallisista luvuista a_j ei ole nolla. Lauseen 3.6 perusteella voidaan määrittää normaali algebrallinen kuntalaajennus $\mathbb{Q}(\theta)/\mathbb{Q}$, joka sisältää

algebralliset luvut a_j. Konjugaatit $a_j^{(i)}$ sisältyvät kuntaan $\mathbb{Q}(\theta)$. Merkitään kuntalaajennuksen astetta luvulla q. Muodostetaan tulo

$$\prod_{i=1}^{q} \left(a_1^{(i)} e^{\alpha_1} + a_2^{(i)} e^{\alpha_2} + \cdots + a_m^{(i)} e^{\alpha_m} \right) = 0.$$

Jos kertoimet $a_j^{(i)}$ tulkitaan lukujen $\theta^{(i)}$ polynomeiksi, niin lauseen 3.3 perusteella todetaan, kertoimet ovat lukujen $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(q)}$ symmetrisiä polynomeja, ja siis lauseen 3.2 perusteella rationaalilukuja. Lauseen 3.9 perusteella tulo ei ole identtisesti nolla. Täten todetaan, että yhtälön (3.1) perusteella on voimassa vastaava yhtälö rationaalilukukertoimilla, mikä todettiin lauseen 3.10 perusteella mahdottamaksi. Vastaoletus on siis väärä, joten lause 3.1 on todistettu.

3.4 Yleistetyn Lindemannin lauseen seurauksia

Lause 3.11. *Jos luku β on nollasta eroava algebrallinen luku, niin luku e^β on transkendenttinen.*

Todistus. Tehdään vastaoletus, että luku e^β on algebrallinen. Tällöin luku e^β toteuttaa muotoa

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0$$

olevan polynomiyhtälön, missä kertoimet b_i ovat rationaalilukuja. Kun merkitään $a_1 = 1, a_2 = b_1, \ldots, a_{n+1} = b_n$, $\alpha_1 = n, \alpha_2 = n-1, \ldots, \alpha_{n+1} = 0$ ja $m = n+1$, niin on siis voimassa

$$\sum_{j=1}^{m} a_j e^{\beta \alpha_j} = 0,$$

missä luvut a_j ja $\beta\alpha_j$ ovat algebrallisia, luvut $\beta\alpha_j$ ovat toisistaan eroavia ja ainakin yksi luvuista a_j on nollasta poikkeava. Tämä on ristiriidassa lauseen 3.1 kanssa. Vastaoletus on siis väärä, joten lause on todistettu.

Lause 3.12. *Luku π on transkendenttinen.*

Todistus. Tehdään vastaoletus, että π on algebrallinen. Tällöin luku $i\pi$ on lauseen 2.2 perusteella algebrallinen, koska luku i on algebrallinen. Tällöin luku $e^{i\pi}$ on lauseen 3.11 perusteella transkendenttinen. Tämä on ristiriita, koska tiedetään, että $e^{i\pi} = -1$. Vastaoletus on siis väärä, joten lause on todistettu.

Lause 3.13. *Jos luku α on nollasta eroava algebrallinen luku, niin* $\sin\alpha$ *on transkendenttinen.*

Todistus. Tiedetään, että $\sin\alpha = (e^{i\alpha} - e^{-i\alpha})/2i$. Tehdään vastaoletus, että $\sin\alpha$ on algebrallinen. Merkitään $a = \sin\alpha$. Tällöin saadaan

$$e^{i\alpha} - e^{-i\alpha} - 2iae^0 = 0,$$

missä kertoimet ja eksponentit ovat algebrallisia. Tämä on ristiriidassa lauseen 3.1 kanssa. Vastaoletus on siis väärä, joten lause on todistettu.

Lause 3.14. *Jos luku α on nollasta eroava algebrallinen luku ja $\alpha \neq 1$, niin $\log\alpha$ on transkendenttinen.*

Todistus. Tehdään vastaoletus, että $\log\alpha = a$, missä a on algebrallinen. Tällöin olisi $e^a = \alpha$, mikä on mahdollista vain jos $a = 0$ ja $\alpha = 1$. Lause on siis todistettu.

3.5 Ympyrän neliöiminen

Sellaisen neliön muodostaminen viivoitinta ja harppia käyttäen, jolla on sama pinta-ala kuin annetulla ympyrällä, on klassinen ongelma antiikin ajalta. Tämän ongelman Lindemann osoitti mahdottomaksi ratkaista, kun hän todisti, että luku π on transkendenttinen luku. Tämä perustuu siihen, että toisaalta kaikilla janoilla, jotka voidaan muodostaa annetusta pituusyksiköstä käyttäen äärellisen monta kertaa harppia ja viivoitinta, on pituutena algebrallinen luku. Toisaalta ympyrällä, jonka säde on yksikön pituinen, on pinta-ala, joka ilmaistaan luvun π yksikköinä. Siten tämä neliön muodostaminen vastaa ongelmaa, missä pitäisi annetun yksikön pituisen janan perusteella muodostaa jana, jonka pituus on $\sqrt{\pi}$. Tämä on mahdotonta, koska luku $\sqrt{\pi}$ on transkendenttinen. Jos $\sqrt{\pi}$ olisi algebrallinen, niin lauseen 2.2 perusteella luku $\pi = \sqrt{\pi} \cdot \sqrt{\pi}$ olisi algebrallinen.

4 Gelfondin-Schneiderin lause

4.1 Gelfondin-Schneiderin lauseen esittely

Seuraava lause on Gelfondin-Schneiderin lause.

Lause 4.1. *Jos α on algebrallinen luku, jolle on voimassa $\alpha \neq 0$ ja $\alpha \neq 1$, ja β on algebrallinen luku, joka ei ole rationaaliluku, niin lausekkeen α^β arvot ovat transkendenttisia lukuja.*

Lauseen todistus esitetään jatkossa. Lauseen kanssa yhtäpitävä on seuraava lause.

Lause 4.2. *Jos α ja γ ovat nollasta eroavia algebarallisia lukuja ja $\alpha \neq 1$, niin lausekkeen $(\log\gamma)/(\log\alpha)$ arvo on joko rationaalinen tai transkendenttinen.*

Yhäpitävyyden toteamiseksi merkitään $\beta = (\log \gamma)/(\log \alpha)$, jolloin $\gamma = \alpha^\beta$. Oletetaan, että jälkimmäisen lauseen oletukset ovat voimassa ja β on algebrallinen, mutta ei rationaalinen. Tällöin γ on lauseen 4.1 perusteella transkendenttinen, mikä on riistiriita.

Jos oletetaan, että lauseen 4.1 oletukset ovat voimassa, mutta lauseen väite ei voimassa, niin luku α^β on nollasta poikkeava algebrallinen luku. Lauseen 4.2 perusteella todetaan, että luku β on joko transendenttinen tai rationaalinen, ja tämä on ristiriita. Siis lause 4.1 seuraa lauseesta 4.2. Lauseet ovat siis yhtäpitäviä.

Lauseesta 4.2 seuraa, että positiivisten rationaalilukujen 10-kantaiset logaritmit ovat joko rationaalisia tai transkendentaalisia lukuja. Tämä nähdään yhtälöstä

$$\log_{10} r = \frac{\log r}{\log 10}.$$

4.2 Gelfondin-Schneiderin lauseen todistamiseen tarvittavia lauseita

Lause 4.3. *Tarkastellaan determinanttia, jossa rivin j ja sarakkeen $1 + a$ alkio on ρ_j^a. Tämän kaltaista determinanttia kutsutaan Vandermonden determinantiksi. Tämä determinantti on nolla, jos ja vain jos on olemassa sellaiset i ja j, että $i \neq j$ ja $\rho_i = \rho_j$.*

Todistus. Voidaan osoittaa (vrt. [3, s. 215]), että tämä determinantti voidaan kirjoittaa muodossa

$$\prod_{1 \leq i < j \leq n} (\rho_j - \rho_i),$$

mistä nähdään, että lauseen väite pitää paikkansa.

Lause 4.4. *Olkoon α ja β algebrallisia lukuja kuntalaajennuksessa $K/\mathbb{Q}$, jonka aste on h. Jos lukujen α ja β konjugaatit kunnassa K ovat $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_h$ ja $\beta = \beta_1, \beta_2, \ldots, \beta_h$, niin lukujen $\alpha\beta$ ja $\alpha + \beta$ konjugaatit ovat $\alpha_1\beta_1, \ldots, \alpha_h\beta_h$ ja $\alpha_1 + \beta_1, \ldots, \alpha_h + \beta_h$.*

Todistus. Sivuutetaan. Kts. [2, s. 65].

Lause 4.5. *Jos α on algebrallinen luku, niin on olemassa positiivinen kokonaisluku r siten, että $r\alpha$ on algebrallinen kokonaisluku.*

Todistus. Vrt. [2, s. 77]. Koska luku α on algebrallinen, niin se toteuttaa muotoa

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + a_{n-3} x^{n-3} + \cdots + a_0 = 0,$$

missä kertoimet a_i ovat kokonaislukuja. On siis voimassa

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + a_{n-2} \alpha^{n-2} + a_{n-3} \alpha^{n-3} + \cdots + a_0 = 0.$$

Voidaan olettaa, että korkeimman asteen termin kerroin on positiivinen. Kerrotaan yhtälön molemmat puolet luvulla a_n^{n-1}, jolloin saadaan

$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_{n-2}a_n(a_n\alpha)^{n-2} + a_{n-3}a_n^2(a_n\alpha)^{n-3} + \cdots + a_n^{n-1}a_0 = 0.$$

Tästä nähdään, että luku $a_n\alpha$ toteuttaa polynomiyhtälön, jossa korkeimman asteen termin kerroin on yksi ja muut kertoimet ovat kokonaislukuja. Luku $a_n\alpha$ on siis algebrallinen kokonaisluku ja lause on todistettu.

Lause 4.6. *Jos $K/\mathbb{Q}$ on algebrallinen kuntalaajennus, jonka aste on h, niin on olemassa algebralliset kokonaisluvut $\beta_1, \beta_2, \ldots, \beta_h \in K$ siten, että jokainen algebrallinen kokonaisluku $n \in K$ voidaan ilmaista yksikäsitteisesti muodossa $k = g_1\beta_1 + \cdots + g_h\beta_h$, missä kertoimet g_i ovat kokonaislukuja. Lukuja β_i kutsutaan kunnan K kokonaislukukannaksi, ja tämän kannan diskriminantti on kokonaisluku.*

Todistus. Sivuutetaan. Kts. [2, ss. 79-81].

Lause 4.7. *Jos α on algebrallinen luku, joka kuuluu astetta h olevaan kuntalaajennukseen $K/\mathbb{Q}$, ja normi $N(\alpha)$ määritellään luvun α ja sen konjugaattien tulona, niin normi toteuttaa ehdon $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$. Lisäksi on voimassa $N(\alpha) = 0$, jos ja vain jos $\alpha = 0$. Jos α on algebrallinen kokonaisluku, niin $N(\alpha)$ on kokonaisluku. Jos α on rationaaliluku, niin $N(\alpha) = \alpha^h$.*

Todistus. Sivuutetaan. Kts. [2, s. 89].

Lause 4.8. *Tarkastellaan seuraavia yhtälöitä, joita on m kappaletta, ja jotka sisältävät n tuntematonta.*

$$a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n = 0, \qquad k = 1, 2, \ldots, m, \tag{4.1}$$

missä kertoimet a_{ij} ovat kokonaislukuja, ja on voimassa $0 < m < n$. Olkoon A positiivinen kokonaisluku, joka on kertoimien itseisarvojen yläraja. Siis $A \geq |a_{ij}|$ kaikilla i ja j. Tällöin yhtälöillä (4.1) on ei-triviaali kokonaislukuratkaisu $x_1, x_2, \ldots, x_n$ siten, että

$$|x_j| < 1 + (nA)^{m/(n-m)}, \qquad j = 1, 2, \ldots, n.$$

Todistus. Vrt. [1, s. 137]. Merkintään $y_k = a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n$, jolloin jokaista pistettä $x = (x_1, x_2, \ldots, x_n)$ vastaa piste $y = (y_1, y_2, \ldots, y_n)$. Pistettä x sanotaan hilapisteeksi, jos koordinaatit x_j ovat kokonaislukuja. Jos x on hilapiste, niin vastaava y on myös hilapiste, koska kertoimet a_{ij} ovat kokonaislukuja. Olkoon q mielivaltainen positiivinen kokonaisluku. Jos x saa arvot, joille on voimassa $|x_j| \leq q$ kaikilla indeksin j arvoilla, niin tällöin vastaavat luvut y_k toteuttavat ehdon

$$|y_k| = \left| \sum_{j=1}^{n} a_{kj}x_j \right| \leq \sum_{j=1}^{n} |a_{kj}| \cdot |x_j| \leq \sum_{j=1}^{n} Aq = nAq.$$

Tällöin x on jokin hilapisteistä, joita on $(2q+1)^n$ kappletta. Vastaavien hilapisteiden y koordinaatit y_k koordinaatit ovat kokonaislukuja jotka voivat saada $2nAq+1$ arvoa joukossa $-nAq, \ldots, -2, -1, 0, 1, 2, \ldots, nAq$. Mahdollisia hilapisteitä y on siis korkeintaan $(2nAq+1)^m$. Osoitetaan, että ainakin kaksi näistä hilapisteistä y on samat. Tämä voidaan tehdä osoittamalla, että jollakin luvun q arvolla on enemmän pisteitä kuin mahdollisia sijainteja. Siis osoitettava, että on voimassa

$$(2q+1)^n > (2nAq+1)^m. \tag{4.2}$$

Määritetään kokonaisluku q. Määritellään, että $2q$ on yksikäsitteinen parillinen kokonaisluku välillä, jonka pituus on 2 sueraavasti

$$(nA)^{m/(n-m)} - 1 \leq 2q < (nA)^{m/(n-m)} + 1. \tag{4.3}$$

Edellä olevan epäyhtälön ensimmäisen osan perusteella on voimassa $(nA)^m \leq (2q+1)^{n-m}$, jolloin saadaan

$$\begin{aligned}(2nAq+1)^m = (nA)^m \left(2q + \frac{1}{nA}\right)^m &< (nA)^m (2q+1)^m \\ &\leq (2q+1)^{n-m}(2q+1)^m = (2q+1)^n.\end{aligned}$$

Siis epäyhtälö (4.2) on voimassa. Siis kun x käy läpi $(2q+1)^n$ hilapistettä, jotka ehto $|x_j| \leq q$ määrittelee, niin vastaavat hilapisteet y eivät ole kaikki toisistaan eroavia. Oletetaan, että hilapisteet y ovat samat kun $x = (x'_1, \ldots, x'_n)$ ja $x = (x''_1, \ldots, x''_n)$. Tällöin $x = (x'_1 - x''_1, \ldots x'_n - x''_n)$ on lauseessa mainittu ei-trivialli ratkaisu yhtälöryhmälle (4.1), koska epäyhtalön (4.3) perusteella on voimassa

$$|x'_j - x''_j| \leq |x'_j| - |x''_j| \leq q + q < (nA)^{m/(n-m)} + 1.$$

Merkintä. Jos algebrallinen luku α kuuluu kuntaan K, niin merkinnällä $\|\alpha\|$ tarkoitetaan maksimiarvoa luvun α ja sen konjugaattien itseisarvoista. Lauseen 4.4 perusteella todetaan, että on voimassa $\|\alpha+\beta\| \leq \|\alpha\| + \|\beta\|$ ja $\|\alpha\beta\| \leq \|\alpha\| \cdot \|\beta\|$.

Lause 4.9. *Tarkastellaan seuraavia yhtälöitä, joita on p kappaletta ja jotka sisältävät q tuntematonta.*

$$\alpha_{k1}\xi_1 + \alpha_{k2}\xi_2 + \cdots + \alpha_{kq}\xi_q = 0 \qquad k = 1, 2, \ldots, p, \tag{4.4}$$

missä kertoimet alpha$_{ij}$ ovat kokonaislukuja ja kuuluvat algebralliseen kuntaan K, joka on äärellistä astetta. Oletetaan, että on voimassa $0 < p < q$. Olkoon $A \geq 1$ on yläraja kertoimien ja niiden konjugaattien/K itseisarvoille . Siis on voimassa $A \geq \|\alpha_{ij}\|$ kaikilla indeksien i ja j arvoilla. Tällöin

on olemassa kunnasta K riippuva positiivinen vakio c, joka ei riipu luvuista α_{ij}, p ja q siten, että yhtälöillä (4.4) *on kuntaan K kuuluva ei-triviaali kokonaislukuratkaisu $\xi_1, \xi_2, \ldots, \xi_q$ ja on voimassa*

$$\|\xi_k\| < c + c(cqA)^{p/(q-p)}, \qquad k = 1, 2, \ldots, p.$$

Todistus. Vrt. [1, s. 139]. Olkoon kuntalaajennuksen $K/\mathbb{Q}$ aste h ja $\beta_1, \beta_2, \ldots, \beta_h$ kunnan kokonaislukukanta. Jos $\alpha \in K$ on mielivaltainen kokonaisluku, niin lauseen 4.6 perusteella luku α voidaan esittää yksikäsitteisesti tämän kannan lineaarikombinaatioina

$$\alpha = g_1\beta_1 + g_2\beta_2 + \cdots + g_h\beta_h,$$

missä kertoimet g_j ovat kokonaislukuja. Merkitään luvun α konjugaatteja/K $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(h)}$ ja käytetään vastaavaa merkintää lukujen β_j konjugaateille. Tällöin saadaan edellisen yhtälön ja lauseen 4.4 perusteella

$$\alpha^{(i)} = g_1\beta_1^{(i)} + g_2\beta_2^{(i)} + \cdots + g_h\beta_h^{(i)}, \qquad i = 1, 2, \ldots, h.$$

Determinantti $|\beta_j^{(i)}|$ on kannan diskriminantti ja lauseen 4.6 perusteella nollasta eroava. Yhtälöryhmä voidaan siten ratkaista. Ottamalla ratkaisuista itseisarvot saadaan

$$|g_j| < c_1\|\alpha\|, \qquad j = 1, 2, \ldots, h, \tag{4.5}$$

missä positiivinen vakio c_1 riippuu kunnasta K, mutta ei riipu luvusta α.

Kokonaisluvuille ξ_i, jotka toteuttavat yhtälöt (4.4), voidaan kirjoittaa

$$\xi_i = \sum_{j=1}^{h} x_{ij}\beta_j, \qquad i = 1, 2, \ldots, q. \tag{4.6}$$

Pitää siis löytää sopivat kokonaisluvut x_{ij}. Yhtälöt (4.4) voidaan kirjoittaa muotoon

$$\sum_{i=1}^{q} \alpha_{ki}\xi_i = \sum_{i=1}^{q}\sum_{j=1}^{h} \alpha_{ki}\beta_j x_{ij} = 0, \qquad k = 1, 2, \ldots, p. \tag{4.7}$$

Kokonaisluvut $\alpha_{ki}\beta_j$ voidaan lauseen 4.6 perusteella ilmaista kokonaislukukannan avulla muodossa

$$\alpha_{ki}\beta_j = \sum_{r=1}^{h} m_{kijr}\beta_r, \qquad k = 1, \ldots, p, \quad i = 1, \ldots, q, \quad j = 1, \ldots, h, \tag{4.8}$$

missä luvut m_{kijr} ovat kokonaislukuja. Yhtälöstä (4.7) sadaan tällöin

$$\sum_{i=1}^{q}\sum_{j=1}^{h}\sum_{r=1}^{h} m_{kijr}x_{ij}\beta_r = 0, \qquad k = 1, 2, \ldots, p.$$

Luvut β_r ovat lineaarisesti riippumattomia kuunan $\mathbb{Q}$ suhteen, joten asetetaan kunkin luvun β_r kertoimet nollaksi, jolloin saadaan

$$\sum_{i=1}^{q}\sum_{j=1}^{h} m_{kijr}x_{ij} = 0, \qquad k = 1, 2, \ldots, p, \quad r = 1, 2, \ldots, h. \tag{4.9}$$

On saatu ph yhtälöä, joissa on qh tuntematonta x_{ij}. Jotta voidaan käyttää lausetta 4.8, tarvitaan yläraja kerrointen m_{kijr} itseisarvoille. Käytetään epäyhtälöä (4.5) siten, että luvut α korvataan luvuilla $\alpha_{ki}\beta_j$ ja luvut g_j korvataan luvuilla m_{kijr}. Tällöin saadaan

$$\|m_{kijr}\| < c_1\|\alpha_{ki}\beta_j\| \leq c_1\|\alpha_{ki}\| \cdot \|\beta_j\| \leq c_1 A\|\beta_j\| \leq c_2 A,$$

missä A yläraja, joka on annettu lauseessa, ja c_2 on vakio, joka on valittu siten, että $c_2 A$ on kokonaisluku ja on voimassa ehto $c_2 \geq c_1\|\beta_j\|$ kaikilla indeksin j arvoilla. Koska $A \geq 1$, niin reaaliluku c_2 voidaan valita väliltä

$$1 + c_1 \cdot \max_j \|\beta_j\| > c_2 \geq c_1 \cdot \max_j \|\beta_j\|$$

siten, että $c_2 A$ on kokonaisluku.

Voidaan siis käyttää lausetta 4.8 yhtälöihin (4.9) siten, että luvut m, n ja A korvataan luvuilla ph, qh ja $c_2 A$. Yhtälöille (4.9) on siis ei-triviaali ratkaisu siten, että kokonaisluvut x_{ij} täyttävät ehdon

$$|x_{ij}| < 1 + (qhc_2 A)^{ph/(qh-ph)} = 1 + (hc_2 qA)^{p/(q-p)}.$$

Käyttämällä näitä arvioita ja yhtälöä (4.6) saadaan yhtälöille (4.4) ratkaisu joka täyttää ehdot

$$\|\xi_i\| < h \cdot \max_j \|\beta_\|(1 + (hc_2 qA)^{p/(q-p)}) < c + c(cqA)^{p/(q-p)},$$

kunhan luku c valitaan siten, että se on suurempi kuin luvut hc_2 ja $h\|\beta_j\|$ kaikilla indeksin j arvoilla. Täten luku c riippuu kunnasta K, mutta ei riipu luvuista α_{ij}, p ja q. Lisäksi, koska ainakin yksi luvuista x_{ij} on nollasta eroava, niin yhtälön (4.6) perusteella ainakin yksi ξ_i tässä rakaisussa on nollasta poikkeava, sillä luvut β_j ovat lineaarisesti riippumattomia rationaalilukujen suhteen.

4.3 Gelfondin-Schneiderin lauseen todistuksen valmistelua

Tehdään vastaoletus, että algebralliset luvut α ja β täyttävät lauseen 4.1 ehdot, mutta luku α^β on algebrallinen. Todistetaan, että tämä oletus johtaa

ristiriitaan. Merkitään $\gamma = \alpha^\beta = e^{\beta \log \alpha}$. Olkoon $K/\mathbb{Q}$ astetta h oleva kuntalaajennus, joka sisältää luvut α, β ja γ. Tehdään seuraavat määritykset

$$\begin{aligned} &m = 2h+3, \qquad q > 4m^2, \qquad n = q^2/2m \\ &t = q^2 = 2mn, \qquad n > q. \end{aligned} \tag{4.10}$$

Ensimmäisenä määritellään m siten, että m ja h ovat seuraavassa kiinnitettyjä. Kokonaisluku q valitaan suuremmaksi kuin $4m^2$ siten, että q^2 on luvun $2m$ monikerta ja kokonaisluku n näiden osamäärä. Luku t määritellään samaksi kuin q^2. Epäyhtälö $n > q$ seuraa muista ehdoista. Näitä lukujen q, n ja t määrityksiä täydennetään myöhemmin siten, että näiden kokonaislukujen on oltava suurempia kuin tietyt vakiot. Näitä vakioita merkitään $c, c_1, c_2, c_3, \ldots$, ja ne kaikki ovat riippumattomia luvuista n, q, t. Määritellään luvut $\rho_1, \rho_2, \ldots, \rho_t$ siten, että ne ovat lukuja

$$(r + k\beta)\log\alpha, \qquad r = 1, 2, \ldots, q, \quad k = 1, 2, \ldots, q. \tag{4.11}$$

Ei ole tarvetta määrittää mikä näistä on ρ_1, mikä ρ_2 jne. Määritellään kokonainen funktio

$$F(z) = \sum_{j=1}^{t} \eta_j e^{z\rho_j}, \tag{4.12}$$

missä luvut η_j ovat algebrallisia kokonaislukuja kunnassa K.

Lauseen 4.5 perusteella on olemassa kokonaisluku $c_1 > 0$ siten, että luvut $c_1\alpha$, $c_1\beta$ ja $c_1\gamma$ ovat algebrallisia kokonaislukuja. Tarkastellaan seuraavia yhtälöitä, joita on mn kappaletta ja joissa on $2mn$ tuntematonta η_j,

$$c_1^{n+2mq}(\log\alpha)^{-a}F^{(a)}(b) = 0, \qquad a = 0, 1, \ldots, n-1, \quad b = 1, 2, \ldots, m. \tag{4.13}$$

Jotta voitaisiin käyttää lausetta 4.9, näihin yhtälöihin, on tarkistettava, että lauseen oletukset ovat voimassa. Kertoimet η_j yhtälöissä (4.13) ovat (4.11) perusteella seuraavat

$$\begin{aligned} c_1^{n+2mq}(\log\alpha)^{-a}\rho_j^a e^{b\rho_j} &= c_1^{n+2mq}(r+k\beta)^a e^{b(r+k\beta)\log\alpha} \\ &= c_1^{n+2mq}(r+k\beta)^a \alpha^{rb}\gamma^{kb}. \end{aligned} \tag{4.14}$$

Yhtälön perusteella kertoimet η_j yhtälöissä (4.13) ovat algebrallisia kokonaislukuja kunnassa K. Tämä nähdään kun huomataan, että yhtälön (4.14) jälkimmäisessä lausekkeessa on lukujen α, β, γ astetta $a + rb + kb$ oleva polynomi. Lukujen a, b, r, k maksimit ovat vastaavassa järjestyksessä $n-1, m, q, q$, joten on voimassa $a + rb + kb \le n - 1 + 2mq$. Kerroin c_1^{n+2mq} takaa, että (4.14) on algebrallinen kokonaisluku.

Jotta löydettäisiin rajat kertoimille (4.14) ja niiden konjugaateille, todetaan, että on voimassa

$$\|r + k\beta\| \le \|r\| + \|k\| \cdot \|\beta\| \le q + q\|\beta\| = q(1 + \|\beta\|). \tag{4.15}$$

Määritellään c_2 maksimiksi luvuista $\|\alpha\|, \|\gamma\|, 1+\|\beta\|$. Tällöin voidaan sanoa, että kerrointen (4.14) ja niiden konjugaattien itseisarvoja rajoittaa yhtälöiden ja epäyhtälöiden (4.10) perusteella

$$c_1^{n+2mq}(qc_2)^n c_2^{2mq} = (c_1c_2)^n((c_1c_2)^{2m})^q(\sqrt{2m})^n n^{n/2}.$$

Määritellään $c_3 = (c_1c_2)^{2m+1}\sqrt{2m}$, jolloin tämä raja voidaan korvata lausekkeella $c_3^n n^{n/2}$, koska $q < n$. Huomataan, että luku c_3, samoin kuin luvut c_1, c_2 ja m, on riippumaton luvusta n. Voimme nyt soveltaa lausetta 4.9 yhtälöihin (4.13) siten, että A korvataan lausekkeella $c_3^n n^{n/2}$, ja todetaan, että näillä yhtälöillä' on ei-triviaali ratkaisu η_j siten, että on voimassa

$$\|\eta_j\| < c + c(c(2mn)c_3^n n^{n/2})^{mn/(2mn-mn)} = c + 2c^2 mnc_3^n n^{n/2} < 3c^2 mnc_3^n n^{n/2}$$

kaikilla indeksin j arvoilla.

Vakio c riippuu kunnasta K, mutta ei luvusta n. On voimassa $2^n > n > q > m$, joten jälkimmäisessä epäyhtälössä voidaan korvata mn luvulla 4^n, ja voidaan yhdistää kaikki vakiot, jolloin saadaan

$$\|\eta_j\| < c_4^n n^{n/2}, \tag{4.16}$$

missä c_4 on riippumaton luvusta n. Tätä ei-triviaalia yhtälöiden (4.13) kokonaislukuratkaisua η_j kunnassa K sovelletaan yhtälöön (4.12), jolloin $F(z)$ on täydellisesti määritelty.

Lause 4.10. *On olemassa kokonaisluvut $p > n$ ja B, joka kuuluu väliin $1 \le B \le m$ siten, että on voimassa $F^{(a)}(b) = 0$, kun $a = 0, 1, \ldots, p-1$ ja $b = 1, 2, \ldots, m$ ja $F^{(p)}(B) \neq 0$.*

Todistus. Vrt. [1, s. 144]. Jos tälläinen p on olemassa , on sen täytettävä yhtälöiden (4.13) perusteella ehto $p \ge n$. Riittää todistaa, että $F^{(a)}(1)$ ei ole nolla kaikilla arvoilla $a = 0, 1, 2, \ldots, t-1$. Tehdään vastaoletus, että $F^{(a)}(1)$ on nolla kaikilla näillä arvoilla, jolloin (4.12) perusteella saadaan

$$\sum_{j=1}^{t} \eta_j \rho_j^a e^{\rho_j} = 0, \qquad 0 \le a \le t-1.$$

Mutta luvut η_j eivät ole kaikki nollia, joten determinanti jonka arvo on nolla.

$$0 = \det|\rho_j^a e^{\rho_j}| = \det|\rho_j^a| \cdot \prod_j e^{\rho_j}, \qquad 0 = \det|\rho_j^a|.$$

Jälkimmäinen yhtälö saadaan, koska $e^{\rho_j} \neq 0$. Lauseen 4.3 perusteella siitä että tämän Vandermonden determinantti on nolla, seuraa, että kahden luvuista ρ_j täytyy olla samat, eli $\rho_j = \rho_k, j \neq k$. Kun huomoidaan (4.11) ja se, että oletuksen perusteella $\log\alpha \neq 0$, niin seuraa, että luku β on rationaaliluku. Tämä on ristiriidassa lauseen 4.1 oletusten kanssa. Siis lause 4.10 on todistettu.

Seuraavaksi määritellään lauseen 4.10 perusteella nollasta eroava arvo

$$\begin{aligned}\zeta &= (\log\alpha)^{-p}F^{(p)}(B) \\ &= \sum_{j=1}^{t}\eta_j(\log\alpha)^{-p}\rho_j^p e^{B\rho_j} \\ &= \sum_{j=1}^{t}\eta_j(r+k\beta)^p\alpha^{Br}\gamma^{Bk},\end{aligned} \tag{4.17}$$

missä jälkimmäinen lauseke saadaan (4.12) ja (4.11) perusteella. Viimeisimmässä summassa luvut r ja k riippuvat indeksistä j, mutta seuraavaa varten ei tarvitse tietää tarkkaa riippuvuutta.

Lause 4.11. *On olemassa luvuista n ja p riippumaton positiivinen vakio C, jolle on voimassa*

$$|N(\zeta)| \geq C^{-p}.$$

Todistus. Vrt. [1, s. 145]. Muistetaan kokonaisluvut $\eta_j \in K$ ja kokonaisluku c_1 oli valittu siten, että $c_1\alpha, c_1\beta$ ja $c_1\gamma$ ovat kokonaislukuja, jotka kuuluvat kuntaan K. Tästä seuraa yhtälön (4.17) perusteella, että $c_1^{p+2mq}\zeta$ on algebrallinen kokonaisluku, kun huomioidaan, että q on sekä luvun r että luvun k maksimiarvo kohdassa (4.11), ja luku m on luvun B maksimiarvo lauseen 4.10 perusteella. On voimassa $q < n \leq p$, joten saadaan

$$c_1^{p+2mq} < (c_1^{1+2m})^p = c_5^p,$$

missä c_5 samoin kuin c_1 ja m on riippumaton luvuista p ja n. Luku $c_5^p\zeta$ on myös algebrallinen kokonaisluku, jolloin lauseen 4.7 saadaan

$$\begin{aligned}&1 \leq |N(c_5^p\zeta)| = |N(c_5^p\zeta)N(\zeta)| = c_5^{ph}|N(\zeta)|, \\ &|N(\zeta)| \geq (c_5^h)^{-p}.\end{aligned}$$

Koska h on riippumaton luvuista n ja p, niin lause on todistettu.

Lause 4.12. *On olemassa luvuista n ja p riippumaton positiivinen vakio c, jolle on voimassa $\|\zeta\| < c^p p^p$*

Todistus. Vrt. [1, s. 146]. Yhälön (4.17) perusteella saadaan

$$\|\zeta\| \leq t \cdot \max_j(\|\eta_j\| \cdot \|r+k\beta\|^p \cdot \|\alpha\|^{Br} \cdot \|\gamma\|^{Bk}),$$

missä lukujen r ja k arvot riippuvat indeksistä j, kuten yhtälössä (4.11). Kun luku n on riittävän suuri, niin on voimassa $q < n \leq p$ ja $t = 2mn < 2^n$. Käytetään epäyhtälöä (4.16) ja korvataan luvut $r, k, B, \|\alpha\|, \|\gamma\|, 1+\|\beta\|$ maksimiarvoilla q, q, m, c_2, c_2, c_2, jolloin saadaan

$$\|\zeta\| < 2^n c_4^n n^{n/2}(qc_2)^p c_2^{mq} c_2^{mq} \leq (2c_4c_2^{1+2m})^p n^{n/2} q^p.$$

Yhtälöiden ja epäyhtälöiden (4.10) perusteella saadaan

$$q^p = (\sqrt{2m})^p n^{p/2} \leq (\sqrt{2m})^p p^{p/2} \quad \text{ja} \quad n^{n/2} \leq p^{p/2}.$$

Näitä käyttämällä saadaan

$$\|\zeta\| < (2c_4 c_2^{1+2m}\sqrt{2m})^p p^p = c^p p^p.$$

4.4 Gelfondin-Schneiderin lauseen todistus

Lauseen 4.10 perusteella yhtälöllä (4.12) määritellyllä kokonaisella funktiolla $F(z)$ on vähintään kertalukua p olevat nollakohdat pisteissä $z = 1, 2, \ldots, m$. Määritellään kokonainen funktio $S(z)$ seuraavasti

$$S(z) = p!F(z)\prod_{b=1}^{m}(z-b)^{-p}\prod_{\substack{b=1\\ b\neq B}}^{m}(B-b)^p. \tag{4.18}$$

Kirjoittamalla $F(z)$ Taylorin sarjakehitelmänä lausekkeen $z - B$ potensseina saadaan

$$f(z) = \frac{(z-B)^p F^{(p)}(B)}{p!} + \frac{(z-B)^{p+1}F^{(p+1)}(B)}{(p+1)!} + \cdots .$$

Sijoittamalla tämä yhtälöön (4.18) ja asettamalla $z = B$, saadaan

$$S(B) = F^{(p)}(B), \qquad \zeta = (\log\alpha)^{-p}S(B), \tag{4.19}$$

missä jälkimmäinen yhtälö saadaan yhtälön (4.17) perusteella. Cauchyn integraalikaavan perusteella saadaan

$$S(B) = \frac{1}{2\pi i}\oint_C \frac{S(z)}{z-B}dz, \tag{4.20}$$

missä C on jokin suljettu käyrä pisteen $z = B$ ympäri. Oletetaan, että C on ympyrä $|z| = p/q$. Tämä sulkee sisäänsä pisteen $z = B$, koska yhtälöiden ja epäyhtälöiden (4.10) perusteella on voimassa

$$\frac{p}{q} > \frac{p}{2q} \geq \frac{n}{2q} = \frac{q}{4m} > m \geq B. \tag{4.21}$$

Luvulle ζ saadaan nyt yläraja käyttämällä yhtälöitä (4.19) ja (4.20). Jos u on mielivaltainen kompleksiluku, niin on voimassa $|e^u| \leq e^{|u|}$. Käyttämällä yhtälöitä (4.11) saadaan seuraava epäyhtälö luvuille z ympyrällä $|z| = p/q$

$$|e^{z\rho_j}| \leq e^{|z\rho_j|} \leq \exp(\frac{p}{q}(q + q|\beta|)\cdot|\log\alpha|) = c_6^p,$$
$$c_6 = e^{(1+|\beta|)\cdot|\log\alpha|},$$

missä vakio c_6 ei riipu luvuista n ja p. Yhtälön (4.12) ja epäyhtälön (4.16) perusteella saadaan, kun $|z| = p/q$,

$$|F(z)| \leq t c_4^n n^{n/2} c_6^p < (2c_4 c_6)^p n^{n/2} \leq c_7^p p^{p/2}, \tag{4.22}$$

missä on käytetty tietoa, että on voimassa $t = 2mn < 2^n \leq 2^p$, kun n on riittävän suuri. Käyttämällä epäyhtälöä (4.21) saadaan

$$\begin{aligned} |z-b| &\geq |z| - |b| \geq \frac{p}{q} - m \geq \frac{p}{2q}, \\ |z-b|^{-p} &\leq \left(\frac{2q}{p}\right)^p, \end{aligned} \tag{4.23}$$

kun $b = 1, 2, \ldots, m$.

Epäyhtälöiden(4.22), (4.23) ja yhtälön (4.18) perusteella ympyrällä $|z| = p/q$ on voimassa

$$\begin{aligned} |S(z)| &< p! c_7^p p^{p/2} \left(\frac{2q}{p}\right)^{mp} \prod_{\substack{b=1 \\ b \neq B}}^{m} |B-b|^p \\ &= \left(c_7 2^m (2m)^{m/2} \prod_{\substack{b=1 \\ b \neq B}}^{m} |B-b| \right)^p p! p^{p/2} \left(\frac{\sqrt{n}}{p}\right)^{mp} \\ &= c_8^p p! p^{p/2} \left(\frac{\sqrt{n}}{p}\right)^{mp}. \end{aligned}$$

On voimassa $p! < p^p$ ja $\sqrt{n}/p \leq 1/\sqrt{p}$, koska $n \leq p$. Saadaan

$$|S(z)| < c_8^p p^{p(3-m)/2}, \tag{4.24}$$

kaikille luvuille z ympyrällä $|z| = p/q$. Käyttämällä yhtälöitä (4.19) ja (4.20) saadaan

$$|\zeta| \leq |\log \alpha|^{-p} \cdot |S(B)| = \frac{1}{2\pi} |\log \alpha|^{-p} \cdot \left| \oint_C \frac{S(z)}{z-B} dz \right|.$$

Integrointipolun pituus on $2\pi p/q$. Käyttämällä epäyhtälöitä (4.24) ja (4.24) saadaan

$$\begin{aligned} |\zeta| &< |\log \alpha|^{-p} \cdot \frac{p}{q} \cdot c_8^p p^{p(3-m)/p} \cdot \frac{2q}{p} \\ &< (2c_8 |\log \alpha|^{-1})^p p^{p(3-m)/2} \\ &= c_9^p p^{p(3-m)/2}. \end{aligned}$$

Käyttämällä tätä arvioita luvulle $|\zeta|$ ja lauseen 4.12 mukaista arvioita sen konjugaateille, ja käyttämällä yhtälöitä ja epäyhtälöitä (4.10) saadaan

$$|N(\zeta)| < c_9^p p^{p(3-m)/2}(c^p p^p)^{h-1} = (c_9 c^{h-1})^p p^{-p} = c_0^p p^{-p},$$

missä $c_0 = c_9 c^{h-1}$. Tästä ja lauseesta 4.11 seuraa, että on voimassa

$$c_0^p p^{-p} > C^{-p}, \qquad Cc_0 > p,$$

joillakin positiivisilla vakioilla, jotka eivät riipu luvuista n ja p. Tämä on ristiriita, koska $p \geq n$, ja luku n voidaan valita mielivaltaisen suureksi. Lause 4.1 on siis todistettu.

Esimerkki 4.1. Luku $(\sqrt{2})^{\sqrt{2}}$ on lauseen 4.1 oletusten mukainen, joten se on transkendenttinen luku.

Jos lauseessa 4.1 mainitun luvun α paikalla oleva luku ei ole algebrallinen, niin α^β ei välttämättä ole transkendenttinen luku. Tästä esimerkkinä $((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = 2$.

Viitteet

[1] I. Niven *Irrational Numbers*. New Jersey: Quinn & Boden Company, Inc. 1990.

[2] H. Pollard, H.G. Diamond *The Theory of Algebraic Numbers, second edition*. The Mathematical Association of America 1975.

[3] J.V. Uspensky *Theory of Equations*. McGraw-Hill Book Company, Inc 1948.