Rothin lause

Heikki Pitkänen

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2012

Tiivistelmä: Heikki Pitkänen, *Rothin lause*. Matematiikan pro gradu -tutkielma, 47 sivua, Jyväskylän Yliopiston matematiikan ja tilastotieteen laitos, kevät 2012.

Tämän pro gradu -tutkielman tarkoituksena on esitellä Diofantoksen approksimoinnin tuloksia ja antaa todistus Rothin lauseelle. Diofantoksen approksimoinnissa ollaan kiinnostuneita siitä, kuinka hyvin irrationaalilukuja voidaan arvioida rationaaliluvuilla. Näiden rationaalilukuarvioiden määrän perusteella voidaan antaa riittävä ja välttävä ehto luvun irrationaalisuudesta. Osoittautuu, että ainoastaan irrationaaliluvuilla on ääretön määrä ”hyviä” arvioita. Tämän ehdon riittävyys ja välttävyys todistetaan ja lisäksi esitellään tehokas menetelmä näiden arvioiden laskemiseksi ketjumurtolukujen avulla.

Kun on todettu, että näitä hyviä arvioita on olemassa ja niitä voidaan laskea, voidaan kysyä, olisiko niitä mahdollista löytää vielä tehokkaammin. Tätä ongelmaa lähestyy Liouvillen lause, joka antaa rajan algebrallisten lukujen rationaaliarvioiden hyvyydelle ja mahdollistaa transkendenttilukujen konstruoinnin. Lopulta ratkaisun ongelmaan antaa Rothin lause, jonka nojalla vastaus on kielteinen algebrallisten lukujen kohdalla. Tutkielman toisen puoliskon pääpaino on Rothin lauseen todistuksessa.

Lisäksi tutkielmassa esitellään muutama Rothin lauseen sovellus ja tutustutaan siihen, kuinka lausetta voitaisiin parantaa.

Avainsanat: Lukuteoria, Rothin lause, Diofantoksen approksimointi, Diofantoksen yhtälöt, ketjumurtoluvut

Kiitokset

Kiitokset Lassi Kuritulle tutkielmani ohjaamisesta ja Jere Lehtoselle kommenteista ja korjausehdotuksista. Omistan työni Mimmille, sillä ilman hänen toistuvaa kyselyään graduni valmistumisesta en olisi varmaan koskaan saanut tätä valmiiksi.

Sisältö

Johdanto

Voidaan sanoa, että irrationaaliluku on luku, jonka desimaalikehitelmä on epäsäännöllinen ja päättymätön. Käytännössä tällaisen luvun desimaalikehitelmää on mahdotonta kirjoittaa. Kun huomataan, että irrationaalilukuja on niiden konstruktiosta johtuen mahdollista arvoida äärettömän tarkasti rationaaliluvuilla, sovelluksissa voidaan tyytyä käyttämään rationaalilukuapproksimaatioita. Ongelmaksi muodostuu, kuinka tällaisia arvioita voidaan löytää tehokkaasti. Käytettäessä alkeellista haarukointia työmäärä kasvaa jyrkästi arvion tarkkuuden kasvaessa. Kun aikaisemmin käytössä ei ollut tietokoneita, oli kehitettävä jokin tehokas menetelmä. Ketjumurtoluvut tarjosivat ratkaisun tähän ongelmaan eikä niiden merkitys ole kadonnut tietotekniikan kehityksen myötä — vain arvioinnin tarkkuus on parantunut.

Irrationaalilukuja tutkittaessa havaitaan kuitenkin pian, ettei kaikkia lukuja voida arvioida yhtä hyvin. Huomataan, että reaaliluvut voidaan jakaa algebrallisiin ja transkendenttisiin lukuihin. Näistä jälkimmäisten olemassaolo todistettiin vasta vuonna 1844. Tämä aloitti reilun vuosisadan kehityksen, joka huipentui Rothin[1] lauseeseen. Lausetta pidettiin niin merkittävänä, että Roth sai tästä Fieldsin mitalin vuonna 1958.

Tutkielman rakenne seuraa järjestykseltään kirjan Exploring the number jungle: A journey into Diophantine analysis [**2**] järjestystä. Kahdessa ensimmäisessä luvussa tutkitaan yksinkertaisia arviointimenetelmiä ja kolmannessa luvussa kehitetään tehokas arviointimenetelmä ketjumurtolukujen avulla. Kahdessa viimeisessä luvussa todistetaan Liouvillen ja Rothin lauseet ja käsitellään niiden seurauksia.

[1] Klaus Roth, 1925 —

LUKU 1

Reaalilukujen approksimointia

Oletetaan lukujärjestelmien $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{R}$ konstruktio tunnetuksi. Sovitaan, että luonnollisiksi luvuiksi kutsutaan vain aidosti positiivisia lukuja, jolloin rationaalilukujen joukko voidaan kirjoittaa:

$$\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N} \right\}.$$

Sanotaan, että rationaaliluku $\frac{p}{q}$ on *supistetussa muodossaan*, kun p:llä ja q:lla ei ole yhteisiä tekijöitä lukuja ± 1 lukuunottamatta. Tällöin voidaan sanoa, että luvun $\frac{p}{q}$ *taso* on q. Etsittäessä "hyviä" arvioita irrationaaliluvulle ollaan kiinnostuneita juurikin rationaaliapproksimaation tasosta.

LAUSE 1.1. *Luvun $\frac{p}{q} \in \mathbb{Q}$ supistettu muoto on yksikäsitteinen.*

TODISTUS. Todistus perustuu lukujen p ja q alkulukuesityksen yksikäsitteisyyteen ja joukon $\mathbb{Q}$ määritelmään. □

SOPIMUS 1.2. Kun sekaannuksen vaaraa ei ole, merkitään jatkossa pelkästään $\frac{p}{q}$, kun tarkoitetaan, että $\frac{p}{q} \in \mathbb{Q}$ ja $\frac{p}{q}$ on supistetussa muodossaan.

Aloitetaan arvioiden etsiminen toteamalla seuraava tulos.

LEMMA 1.3. *Olkoon $\alpha \in \mathbb{R}$. Tällöin on olemassa $r \in \mathbb{Z}$ siten, että*

$$|\alpha - r| \leq \frac{1}{2}.$$

TODISTUS. Väite seuraa suoraan reaalilukujen ominaisuuksista. □

Tästä voidaan helposti johtaa seuraava vahvempi tulos.

LAUSE 1.4. *Olkoon $\alpha \in \mathbb{R}$ ja $N \in \mathbb{N}$. Tällöin on olemassa $\frac{p}{q} \in \mathbb{Q}$ siten, että $0 < q \leq N$ ja*

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{2N}.$$

TODISTUS. Koska lemma 1.3 pätee kaikille reaaliluvuille, niin se pätee myös luvulle $N\alpha \in \mathbb{R}$. Tällöin on olemassa $r \in \mathbb{Z}$ siten, että

$$|N\alpha - r| \leq \frac{1}{2}$$

Tämä on yhtäpitävää väitteen

$$\left| \alpha - \frac{r}{N} \right| \leq \frac{1}{2N}$$

kanssa. Voidaan siis valita $\frac{p}{q} = \frac{r}{N}$. □

HUOMAUTUS 1.5. Huomattavaa lauseessa 1.4 on, että luvun $\frac{p}{q}$ taso on korkeintaan N. Tämä on varsin intuitiivista: Jos jana jaetaan $\frac{1}{N}$-mittaisiin osiin, on jokainen janan piste korkeintaan $\frac{1}{2N}$ etäisyydellä jostain osajanan päätepisteestä.

SEURAUS 1.6. *Olkoon $\alpha \in \mathbb{R}\setminus\mathbb{Q}$. Tällöin on äärettömän monta lukua $\frac{p}{q} \in \mathbb{Q}$ siten, että*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q}.$$

TODISTUS. Väite seuraa lauseesta 1.4. Jos näitä lukuja $\frac{p}{q}$ olisi äärellinen määrä, olisi olemassa ε siten, että kaikilla $\frac{p}{q}$ pätisi

$$\left|\alpha - \frac{p}{q}\right| > \varepsilon,$$

sillä α ei irrationaalisuudestaan johtuen voi olla mikään näistä luvuista $\frac{p}{q}$. Kuitenkin on olemassa $N \in \mathbb{N}$ siten, että $\frac{1}{N} < \varepsilon$ ja lauseen 1.4 nojalla löydetään $\frac{p}{q}$ siten, että

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2N} < \frac{1}{N} < \varepsilon,$$

mikä on ristiriita. □

HUOMAUTUS 1.7. Seuraus 1.6 vaikuttaa edelleen varsin intuitiiviselta: Jos irrationaalilukua α lähestytään rationaaliluvuilla $\frac{p_n}{q_n}$, lukua α ei saavuteta koskaan, siis kaikilla $n \in \mathbb{N}$ pätee $\frac{p_n}{q_n} \neq \alpha$, ja tehty virhe voi olla korkeintaan $\frac{1}{q_n}$.

LUKU 2

Dirichlet'n ja Hurwitzin lauseet

Seuraus 1.6 antaa melko hyvän tuloksen irrationaalilukujen arvioille. Kuitenkin, jos tarkkuutta $\frac{1}{q}$ halutaan parantaa, kasvaa työmäärä suoraan verrannollisesti siihen. Liikuttaessa tietokoneen suorituskyvyn rajoilla ja erityisesti laskettaessa käsin on huomattava merkitys sillä, paraneeko tarkkuus verrannollisesti lukuun q vai q^2. Onko mahdollista löytää murtolukuja $\frac{p}{q}$ siten, että tehty virhe olisikin korkeintaan $\frac{1}{q^2}$? Tähän kysymykseen antaa vastauksen Dirichlet'n[1] lause.

LAUSE 2.1 (Dirichlet'n lause, 1842). *Olkoon α reaaliluku ja $N \in \mathbb{N}$. Tällöin on olemassa rationaaliluku $\frac{p}{q}$ siten, että $0 < q \leq N$ ja*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q(N+1)}.$$

Dirichlet'n lauseen todistus perustuu niin sanottuun *kyyhkyslakkaperiaatteeseen*:

LAUSE 2.2 (Kyyhkyslakkaperiaate). *Olkoon $a_1, \ldots, a_n \geq 0$ kokonaislukuja siten, että $\sum_{i=1}^{n} a_i = n + 1$. Tällöin $a_i > 1$ jollakin i.*

TODISTUS. Jos olisi $a_i \leq 1$ kaikilla i, niin

$$\sum_{i=1}^{n} a_i \leq \sum_{i=1}^{n} 1 = n < n + 1,$$

mikä on ristiriita. □

Määritellään Dirichlet'n lauseen todistusta ja jatkoa varten käsite *kokonaisosa* kaikille reaaliluvuille.

MÄÄRITELMÄ 2.3 (Kokonaisosa). Luvun $x \in \mathbb{R}$ *kokonaisosaksi* $\lfloor x \rfloor \in \mathbb{Z}$ sanotaan lukua

$$\lfloor x \rfloor = \max\{k \in \mathbb{Z} : k \leq x\}.$$

HUOMAUTUS 2.4. Kokonaisosa on hyvin määritelty, sillä maksimi on aina olemassa ja se on yksikäsitteinen. Kokonaisosan määritelmästä seuraa heti: $x - \lfloor x \rfloor \in [0, 1[$.

DIRICHLET'N LAUSEEN TODISTUS. Todistuksessa käytetään samaa ideaa kuin lauseen 1.4 todistuksessa. Oletetaan, että $N \geq 2$. Riittää osoittaa, että jollakin $q \in \{1, \ldots, N\}$ on $p \in \mathbb{Z}$ siten, että

$$|q\alpha - p| \leq \frac{1}{N+1}.$$

[1] Johann Peter Gustav Lejeune Dirichlet, 1805—1859

Määritellään kaikille $q \in \{1, \ldots, N\}$ luvut $p_q = \lfloor q\alpha \rfloor$ ja $\alpha_q = q\alpha - \lfloor q\alpha \rfloor = q\alpha - p_q$. Voidaan olettaa, että

$$\frac{1}{N+1} < \alpha_q < \frac{N}{N+1},$$

sillä muutoin väite seuraa, kun valitaan $p = p_q$ tai $p = p_q + 1$ vastaavasti. Oletetaan lisäksi, että pisteet α_q ovat eri pisteitä kaikilla $q \in \{1, \ldots, N\}$. Jos nimittäin olisi $q_1 < q_2$ siten, että $\alpha_{q_1} = \alpha_{q_2}$, olisi $q_2 - q_1 \in \{1, \ldots, N\}$ ja pätisi

$$0 = |\alpha_{q_2} - \alpha_{q_1}| = |q_2\alpha - \lfloor q_2\alpha \rfloor - (q_1\alpha - \lfloor q_1\alpha \rfloor)| = |\alpha(q_2 - q_1) - (p_{q_2} - p_{q_1})|$$

ja voitaisiin valita $p = (p_{q_2} - p_{q_1}) \in \mathbb{Z}$.
Nyt siis välillä $[\frac{1}{N+1}, \frac{N}{N+1}]$ on N kappaletta eri lukuja α_{q_i}, $i \in \{1, \ldots, N\}$ ja voidaan käyttää kyyhkyslakkaperiaatetta: Olkoon kaikilla $j \in 1, \ldots, N-1$

$$A_j = [\frac{j}{N+1}, \frac{j+1}{N+1}]$$

ja

$$a_j = \#\{\alpha_{q_n} \in A_j : n \in \{1, \ldots, N\}\}$$

Koska osajoukot A_j peittävät välin $[\frac{1}{N+1}, \frac{N}{N+1}]$, kun $j \in 1, \ldots, N-1$, niin pätee $\sum_{j=1}^{N-1} a_j = N$. Kyyhkyslakkaperiaatteen nojalla on oltava tällöin $a_k > 1$ jollain $k \in \{1, \ldots, N-1\}$. Koska osavälin A_k pituus on $\frac{1}{N+1}$ ja joillekin $q_1 < q_2$ pätee $\alpha_{q_1} \in A_k$ ja $\alpha_{q_2} \in A_k$, niin

$$|\alpha(q_2 - q_1) - (p_{q_2} - p_{q_1})| = |\alpha_{q_2} - \alpha_{q_1}| \leq \frac{1}{N+1}$$

ja voidaan valita $p = p_{q_2} - p_{q_1} \in \mathbb{Z}$, sillä $q_2 - q_1 \in \{1, \ldots, N\}$. □

Huomautus 2.5. Dirichlet'n lause kertoo vain sen, että irrationaalilukuja on mahdollista arvioida tason q murtoluvuilla tarkkuudella $\frac{1}{q^2}$, mutta se ei anna tehokasta menetelmää näiden lukujen löytämiseksi. Luvussa 3 tutustutaan tehokkaseen algoritmiin, jolla näitä lukuja voidaan tuottaa.

Seuraus 2.6. *Olkoon $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Tällöin on äärettömän monta lukua $\frac{p}{q}$ siten, että*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Todistus. Todistus on analoginen seurauksen 1.6 todistuksen kanssa. Erona on vain, että arvion $\frac{1}{2N}$ sijaan käytetään arviota $\frac{1}{q(N+1)}$. □

Seuraus 2.6 antaa välttämättömän ehdon luvun α irrationaalisuudelle. Osoitetaan seuraavaksi, että tämä on lisäksi riittävä ehto.

Lause 2.7. *Luku on α on irrationaalinen, jos ja vain jos on olemassa äärettömän monta rationaalilukua $\frac{p}{q}$ siten, että*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

TODISTUS. "⇒ " Tämä seuraa suoraan seurauksesta 2.6.
"⇐" Tehdään antiteesi: $\alpha = \frac{m}{n}$ jollakin $\frac{m}{n} \in \mathbb{Q}$. Olkoon $\frac{p}{q}$ jokin luku siten, että arvio $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ pätee. Tällöin

$$\begin{aligned} \left|\frac{p}{q} - \alpha\right| &\leq \frac{1}{q^2} \\ \Leftrightarrow -\frac{1}{q^2} \leq \frac{p}{q} - \alpha &\leq \frac{1}{q^2} \\ \Leftrightarrow -\frac{1}{q^2} + \alpha \leq \frac{p}{q} &\leq \frac{1}{q^2} + \alpha \\ \Rightarrow -\frac{1}{q^2} - |\alpha| \leq \frac{p}{q} &\leq \frac{1}{q^2} + |\alpha| \\ \Rightarrow \left|\frac{p}{q}\right| \leq |\alpha| + \frac{1}{q^2} &\leq |\alpha| + 1 \end{aligned} \tag{2.1}$$

ja kullekin q tämä voi päteä vain äärelliselle määrälle lukuja $p \in \mathbb{Z}$. Koska oletuksen nojalla arvio pätee äärettömän monelle $\frac{p}{q}$, sen on pädettävä äärettömän monelle luvulle $\frac{p}{q} \neq \frac{m}{n}$, joissa kussakin on eri nimittäjä q. Tällöin on olemassa $q > n$ siten, että $\frac{p}{q} \neq \frac{m}{n}$ ja arvio (2.1) pätee. Olkoon $\frac{p}{q}$ tällainen luku. Tällöin

$$\begin{aligned} \left|\frac{m}{n} - \frac{p}{q}\right| &< \frac{1}{q^2} \\ \Leftrightarrow \left|\frac{mq - pn}{nq}\right| &< \frac{1}{q^2} \\ \Leftrightarrow \left|\frac{mq - pn}{n}\right| &< \frac{1}{q} \end{aligned} \tag{2.2}$$

Koska $q > n$, niin $\frac{1}{q} < \frac{1}{n}$, jolloin arvion (2.2) nojalla pätee

$$\begin{aligned} \frac{|mq - pn|}{n} &< \frac{1}{n} \\ \Leftrightarrow |mq - pn| &< 1 \end{aligned}$$

Koska mq ja pn ovat kokonaislukuja, tämä voi päteä vain, jos $|mq - pn| = 0$, mikä on ristiriita valinnan $\frac{m}{n} \neq \frac{p}{q}$ kanssa. Antiteesi on siten väärä ja väite tosi. □

Voidaan kysyä, olisiko Dirichlet'n lauseen arviota mahdollista parantaa kertomalla se jollakin vakiolla m. Hurwitz[2] todisti vuonna 1891, että arviota voidaan parantaa kertomalla se luvulla $m = \frac{1}{\sqrt{5}}$.

LAUSE 2.8 (Hurwitzin lause, 1891). *Olkoon $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Tällöin on olemassa äärettömän monta rationaalilukua $\frac{p}{q}$ siten, että*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$$

[2]Adolf Hurwitz, 1859—1919

TODISTUS. Todistus [**11**, s. 6] vaatii muutaman aputuloksen sekä tuntemusta Farey-jonoista, joten sivuutetaan se. □

SEURAUS 2.9. *Luku on α on irrationaalinen, jos ja vain jos on olemassa äärettömän monta rationaalilukua $\frac{p}{q}$ siten, että*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

TODISTUS. "⇒" Seuraa Hurwitzin lauseesta.
"⇐" Seuraa lauseesta 2.7. Jos on äärettömän monta rationaalilukua $\frac{p}{q}$ siten, että $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$, niin näillä luvuille pätee $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2} < \frac{1}{q^2}$, jolloin lauseen 2.7 nojalla α on irrationaalinen. □

Hurwitzin lauseen arvio on paras, mikä voidaan tehdä *kaikille irrationaaliluvuille*:

LAUSE 2.10. *Hurwitzin lauseessa esiintyvä vakio $m = \frac{1}{\sqrt{5}}$ on pienin luku, jolle väite* "Jokaiselle $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ on olemassa äärettömän monta rationaalilukua $\frac{p}{q}$ siten, että $\left|\alpha - \frac{p}{q}\right| < \frac{m}{q^2}$." *pätee.*

TODISTUS. Todistus [**12**, s.35] perustuu *kultaisen leikkauksen suhdeluvun*, $\varphi = \frac{1+\sqrt{5}}{2}$, approksimointiin. Osoittautuu, että valinta $m < \frac{1}{\sqrt{5}}$ johtaa ristiriitaan arvioitaessa tätä lukua. □

LUKU 3

Approksimointia ketjumurtoluvuilla

Dirichlet'n lause kertoo vain sen, että irrationaaliluvulle α on olemassa äärettömän monta rationaalilukuapproksimaatiota $\frac{p}{q}$ siten, että tehty virhe on korkeintaan $\frac{1}{q^2}$. Seuraavaksi kehitetään koneistoa, jolla näitä approksimaatioita voidaan tuottaa. Ketjumurtoluvut tarjoavat menetelmän tällaisten lukujen löytämiseksi.

Suurin osa tämän luvun tuloksista todistuksineen on Lassi Kuritun luentomonisteesta [**7**].

Tutkitaan aluksi lukua $\frac{459}{182}$. Tämä luku voidaan kirjoittaa muodossa

$$\frac{459}{182} = 2 + \frac{95}{182}.$$

Edelleen huomataan, että $\frac{95}{182}$ voidaan kirjoittaa muodossa

$$\frac{95}{182} = \frac{1}{\frac{182}{95}} = \frac{1}{1 + \frac{87}{95}}.$$

Tällöin

$$\frac{459}{182} = 2 + \frac{95}{182} = 2 + \frac{1}{\frac{182}{95}} = 2 + \frac{1}{1 + \frac{87}{95}}.$$

Jatkamalla näin saadaan esitys

$$\frac{459}{182} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{10 + \cfrac{1}{1 + \frac{1}{7}}}}}.$$

Tämä on luvun $\frac{459}{182}$ *ketjumurtolukuesitys*. Merkitään tätä esitystä yksinkertaisesti

$$\frac{459}{182} = [2, 1, 1, 10, 1, 7]\,.$$

MÄÄRITELMÄ 3.1. Ketjumurtoluvut määritellään rekursiivisesti: Olkoot $x_0, x_1, x_2, \ldots$ reaalilukuja ja oletetaan, että $x_n > 0$ kaikilla $n \geq 1$.

(1) Alkuaskel: Määritellään aluksi $[x_0] = x_0$.
(2) Rekursioaskel: Oletetaan, että tunnetaan merkintä $[x_0, x_1, \ldots, x_{n-1}]$, missä $x_i > 0$, kun $i \geq 1$ ja että $[x_0, x_1, \ldots, x_{n-1}] > 0$, jos $x_0 > 0$. Määritellään nyt

$$[x_0, x_1, \ldots, x_{n-1}, x_n] = x_0 + \frac{1}{[x_1, \ldots, x_{n-1}, x_n]}.$$

Aloitetaan ketjumurtolukujen tutkiminen määrittelemällä aluksi reaalilukujonot $(p_n)_{n=0}^{\infty}$ ja $(q_n)_{n=0}^{\infty}$ ja osoittamalla niiden yhteys ketjumurtolukuihin. Myöhemmin rajoitutaan tutkimaan vain kokonaislukujonoja, joilla todistetaan ketjumurtolukujen ominaisuuksia.

LEMMA 3.2. *Olkoon $(x_n)_{n=0}^{\infty}$ jono reaalilukuja siten, että $x_n > 0$, kun $n \geq 1$. Määritellään jonot $(p_n)_{n=0}^{\infty}$ ja $(q_n)_{n=0}^{\infty}$ rekursiivisesti:*

(1) Asetetaan ensin $q_0 = 1$ ja $q_1 = x_1$
sekä $p_0 = x_0$ ja $p_1 = x_0x_1 + 1$.
(2) Oletetaan, että $q_0, \ldots, q_n$ ja $p_0, \ldots, p_n$ tunnetaan, kun $n \geq 1$ ja asetetaan

$$q_{n+1} = x_{n+1}q_n + q_{n-1}$$

ja

$$p_{n+1} = x_{n+1}p_n + p_{n-1}.$$

Tällöin kaikille $n \in \mathbb{N} \cup \{0\}$ pätee

$$\frac{p_n}{q_n} = [x_0, \ldots, x_n].$$

TODISTUS. Tehdään todistus induktiolla:
(1) $n = 0$: $\dfrac{p_0}{q_0} = \dfrac{x_0}{1} = x_0 = [x_0]$.
$n = 1$: $\dfrac{p_1}{q_1} = \dfrac{x_0x_1 + 1}{x_1} = x_0 + \dfrac{1}{x_1} = [x_0, x_1]$.
(2) Oletetaan, että väite pätee, kun $n = k$.
(3) Todistetaan tapaus $n = k + 1$: Muodostetaan jono $(a_i)_{i=0}^{\infty}$ siten, että $a_i = x_i$ kaikilla $i \neq k$ ja $a_k = x_k + \frac{1}{x_{k+1}}$. Muodostetaan edelleen tästä jonot p' ja q' kuten jonot p ja q muodostettiin. Tällöin $p_i = p'_i$ ja $q_i = q'_i$ kaikilla $i \leq k - 1$. Nyt oletuksen mukaan pätee

$$\frac{p'_k}{q'_k} = [a_0, \ldots, a_k] = [x_0, \ldots, x_k + \frac{1}{x_{k+1}}] = [x_0, \ldots, x_k, x_{k+1}],$$

missä ensimmäinen yhtälö seuraa induktio-oletuksesta ja jälkimmäinen ketjumurtolukujen määritelmästä. Riittää siis osoittaa, että $\dfrac{p'_k}{q'_k} = \dfrac{p_{k+1}}{q_{k+1}}$.
Nimittäjälle saadaan

$$\begin{aligned}
p_{k+1} &= x_{k+1}p_k + p_{k-1} \\
&= x_{k+1}(x_kp_{k-1} + p_{k-2}) + p_{k-1} \\
&= (x_{k+1}x_k + 1)p_{k-1} + x_{k+1}p_{k-2} \\
&= x_{k+1}\left[\left(x_k + \frac{1}{x_{k+1}}\right)p_{k-1} + p_{k-2}\right] \\
&= x_{k+1}\left[a_kp'_{k-1} + p'_{k-2}\right] \\
&= x_{k+1}p'_k
\end{aligned}$$

ja vastaavasti osoittajalle

$$q_{k+1} = x_{k+1}q'_k,$$

joten

$$\frac{p_{k+1}}{q_{k+1}} = \frac{x_{k+1}p'_k}{x_{k+1}q'_k} = \frac{p'_k}{q'_k}.$$

Väite seuraa nyt induktioperiaatteesta. □

HUOMAUTUS 3.3. Jonon q_n määritelmästä seuraa suoraan, että $q_n > 0$ kaikilla $n \in \mathbb{N} \cup \{0\}$.

LEMMA 3.4. *Olkoon $(x_n)_{n=0}^{\infty}$ jono reaalilukuja. Määritellään jonot $(p_n)_{n=0}^{\infty}$ ja $(q_n)_{n=0}^{\infty}$ kuten lemmassa 3.2. Tällöin kaikille $n \geq 1$ pätee*

$$p_{n-1}q_n - p_nq_{n-1} = (-1)^n.$$

TODISTUS. Tehdään tämäkin todistus induktiolla: (1) $n = 1$: $p_{n-1}q_n - p_nq_{n-1} = p_0q_1 - p_1q_0 = x_0x_1 - (x_0x_1 + 1) \cdot 1 = -1$

(2) Oletetaan, että väite pätee, kun $n = k - 1$.

(3) Todistetaan tapaus $n = k$:

$$\begin{aligned} p_{k-1}q_k - p_kq_{k-1} &= p_{k-1}(x_kq_{k-1} + q_{k-2}) - (x_kp_{k-1} + p_{k-2})q_{k-1} \\ &= p_{k-1}x_kq_{k-1} + p_{k-1}q_{k-2} - p_{k-1}x_kq_{k-1} - q_{k-1}p_{k-2} \\ &= -(q_{k-1}p_{k-2} - p_{k-1}q_{k-2}) \\ &= -(-1)^{k-1} \\ &= (-1)^k. \end{aligned}$$

Väite seuraa nyt induktioperiaatteesta. □

LEMMA 3.5. *Olkoon $(x_n)_{n=1}^{\infty}$ jono reaalilukuja. Määritellään jonot $(p_n)_{n=0}^{\infty}$ ja $(q_n)_{n=0}^{\infty}$ kuten lemmassa 3.2. Tällöin kaikille $n \geq 2$ pätee*

$$q_np_{n-2} - p_nq_{n-2} = (-1)^{n-1}x_n.$$

TODISTUS. Lemman 3.4 nojalla

$$\begin{aligned} q_np_{n-2} - p_nq_{n-2} &= (x_nq_{n-1} + q_{n-2})p_{n-2} - (x_np_{n-1} + p_{n-2})q_{n-2} \\ &= x_nq_{n-1}p_{n-2} + q_{n-2}p_{n-2} - x_np_{n-1}q_{n-2} - p_{n-2}q_{n-2} \\ &= x_n(q_{n-1}p_{n-2} + p_{n-1}q_{n-2}) \\ &= (-1)^{n-1}x_n. \end{aligned}$$

□

LEMMA 3.6. *Lemman 3.2 oletuksin kaikille $n \geq 1$ pätee*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots < \frac{p_{2n}}{q_{2n}} < \frac{p_{2n+1}}{q_{2n+1}} < \ldots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

TODISTUS. Huomataan ensin, että $\frac{p_0}{q_0} = x_0 < x_0 + \frac{1}{x_1} = \frac{p_1}{q_1}$, sillä $x_1 > 0$. Oletetaan siten, että $n \geq 2$. Lemman 3.5 nojalla

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1}x_n}{q_{n-2}q_n}.$$

Nyt parillisille $n \geq 2$ saadaan $\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} < 0$ ja parittomille $n \geq 1$ saadaan $\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} > 0$, sillä huomautuksen 3.3 nojalla $q_{n-2}q_n > 0$ ja $x_n \geq 2$. Riittää siis osoittaa, että $\frac{p_n}{q_n} < \frac{p_m}{q_m}$ aina kun n on parillinen ja m pariton.

Oletetaan aluksi, että $n < m$. Koska $\frac{p_n}{q_n} \leq \frac{p_{m-1}}{q_{m-1}}$, riittää osoittaa, että $\frac{p_{m-1}}{q_{m-1}} < \frac{p_m}{q_m}$. Tämä pätee, sillä lemman 3.4 nojalla $q_m p_{m-1} - p_m q_{m-1} = (-1)^m < 0$ (kun m on pariton), joten väite pitää paikkansa.

Tapaus $n > m$ todistetaan vastaavasti. □

Esimerkki 3.7. Kappaleen alussa johdettiin ketjumurtolukuesitys

$$\frac{459}{182} = [2, 1, 1, 10, 1, 7].$$

Tutkimalla tätä huomataan ensin, että $\frac{459}{182} \approx 2,52197802198$. Laskemalla hieman lisää huomataan

$$\begin{aligned}
\frac{p_0}{q_0} &= 2 < \frac{459}{182} \\
\frac{p_1}{q_1} &= 2 + \frac{1}{1} > \frac{459}{182} \\
\frac{p_2}{q_2} &= 2 + \frac{1}{1 + \frac{1}{1}} = 2 + \frac{1}{2} < \frac{459}{182} \\
\frac{p_3}{q_3} &= 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{10}}} = 2 + \frac{11}{21} \approx 2.52380952381 > \frac{459}{182} \\
\frac{p_4}{q_4} &= 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{10 + \frac{1}{1}}}} = 2 + \frac{12}{23} \approx 2.52173913043 < \frac{459}{182} \\
\frac{p_5}{q_5} &= \frac{459}{182}.
\end{aligned}$$

Luvun ylä- ja alaraja-arviot näyttäisivät suppenevan melko nopeasti kohti lukua itseään. Lisäksi on helppo todeta, että kunkin arvion $\frac{p_n}{q_n}$ virhe näyttäisi olevan korkeintaan $\frac{1}{q_n^2}$. Tämä ei ole sattumaa, vaan pätee ketjumurtoluvuille yleisesti, mikä todistetaan jatkossa.

Rajoitutaan nyt tutkimaan vain kokonaislukujonosta $(a_n)_{n=0}^{\infty}$ muodostettuja lukujonoja $(p_n)_{n=0}^{\infty}$ ja $(q_n)_{n=0}^{\infty}$. Tällainen rajoitus on mielekästä tehdä, sillä muutoin luvut $\frac{p_n}{q_n}$ voisivat olla irrationaalisia, eikä toivottua hyötyä saavutettaisi. Seuraavaksi osoitetaan, että tällöin luvut $\frac{p_n}{q_n}$ todella ovat rationaalilukuja.

Lemma 3.8. *Olkoon $(a_n)_{n=0}^{\infty}$ jono* kokonais*lukuja siten, että $a_n > 0$, kun $n \geq 1$. Määritellään jonot $(p_n)_{n=0}^{\infty}$ ja $(q_n)_{n=0}^{\infty}$ (kuten lemmassa 3.2) rekursiivisesti:*

(1) Asetetaan ensin $q_0 = 1$ ja $q_1 = a_1$
sekä $p_0 = a_0$ ja $p_1 = a_0 a_1 + 1$.

(2) Oletetaan, että $q_0, \ldots, q_n$ ja $p_0, \ldots, p_n$ tunnetaan, kun $n \geq 1$ ja asetetaan

$$q_{n+1} = a_{n+1}q_n + q_{n-1}$$

ja

$$p_{n+1} = a_{n+1}p_n + p_{n-1}.$$

Tällöin kaikille $n \geq 1$ pätee $p_n \in \mathbb{Z}$ ja $q_n \in \mathbb{N}$ sekä $q_n \geq \sqrt{2^{n-1}}$.

TODISTUS. Ensimmäinen väite seuraa siitä, että $\mathbb{Z}$ ja $\mathbb{N}$ ovat suljettuja kertolaskun ja summan suhteen.

Osoitetaan toinen väite induktiolla: Oletuksen nojalla luvut a_n ovat kokonaislukuja, joille pätee $a_n > 0$, kun $n \geq 1$, eli $a_n \geq 1$, kun $n \geq 1$.

(1) $n = 1$: $q_1 = a_1 \geq 1 \geq \sqrt{2^0} = 1$.

(2) Oletetaan, että väite pätee kun $n = k - 1$.

(3) Todistetaan tapaus $n = k$:

$$\begin{aligned} q_k &= a_k q_{k-1} + q_{k-2} \\ &\geq 1 \cdot \sqrt{2^{k-2}} + \sqrt{2^{k-3}} \\ &= \frac{1}{\sqrt{2}}\sqrt{2^{k-1}} + \frac{1}{\sqrt{2^2}}\sqrt{2^{k-1}} \\ &\geq \frac{1}{2}\sqrt{2^{k-1}} + \frac{1}{2}\sqrt{2^{k-1}} \\ &= \sqrt{2^{k-1}}. \end{aligned}$$

Väite seuraa induktioperiaatteesta. □

LEMMA 3.9. *Lemmassa 3.8 määritelty lukujono (q_n) on aidosti kasvava, kun $n \geq 2$.*

TODISTUS. Oletuksen nojalla $a_n \geq 1$, kun $n \geq 1$. Tällöin kaikille $k \geq 2$ pätee

$$\begin{aligned} q_k &= a_k q_{k-1} + q_{k-2} \\ &\geq q_{k-1} + q_{k-2} \\ &> q_{k-1}, \end{aligned}$$

sillä $q_{k-1}, q_{k-2} > 0$. □

LAUSE 3.10. *Olkoon $(a_n)_{n=0}^{\infty}$ jono kokonaislukuja siten, että $a_n > 0$, kun $n \geq 1$. Tällöin on olemassa irrationaalinen raja-arvo*

$$\lim_{n\to\infty} [a_0, a_1, \ldots, a_n] = a \in \mathbb{R} \setminus \mathbb{Q}.$$

Lisäksi, jos jonot $(p_n)_{n=0}^{\infty}$ ja $(q_n)_{n=0}^{\infty}$ määritelty kuten lemmassa 3.8, niin kaikilla $n \in \mathbb{N}$ pätee

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

TODISTUS. Riittää osoittaa raja-arvon olemassaolo ja lauseen toisen osan arvio. Raja-arvon irrationaalisuus seuraa tällöin lauseesta 2.7, sillä lemman 3.6 nojalla $\frac{p_n}{q_n}$ ovat eri lukuja ja lemman 3.9 nojalla (q_n) on aidosti kasvava, kun $n \geq 2$..

Osoitetaan ensin raja-arvon olemassaolo: Koska $\frac{p_1}{q_1}$ on yläraja jonolle $\left(\frac{p_{2n}}{q_{2n}}\right)$ ja tämä jono on kasvava, se suppenee. Olkoon siten $\beta = \lim_{n\to\infty} \frac{p_{2n}}{q_{2n}}$. Vastaavasti $\frac{p_0}{q_0}$ on alaraja jonolle $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)$ ja tämä jono on laskeva, joten se suppenee. Olkoon siten $\gamma = \lim_{n\to\infty} \frac{p_{2n+1}}{q_{2n+1}}$. Osoitetaan, että $\beta = \gamma$.

Lemman 3.6 nojalla

$$\frac{p_{2n}}{q_{2n}} \leq \beta \leq \gamma \leq \frac{p_{2n+1}}{q_{2n+1}}$$

kaikilla $n \in \mathbb{N}$. Riittää siis osoittaa, että

$$\lim_{n\to\infty} \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = 0.$$

Lemman 3.4 nojalla

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{(-1)^{2n}}{q_{2n}q_{2n+1}} = \frac{1}{q_{2n}q_{2n+1}}.$$

Nyt lemman 3.8 nojalla $q_{2n}q_{2n+1} \geq \sqrt{2^{2n-1}}\sqrt{2^{2n}} > 2^n$ ja tällöin kaikille $n \in \mathbb{N}$

$$\left|\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}}\right| \leq \frac{1}{2^n},$$

mistä väite $\beta = \gamma$ seuraa.

Olkoon siis $\beta = \gamma = \alpha = \lim_{n\to\infty} \frac{p_n}{q_n}$, mikä on lemman 3.2 nojalla yhtäpitävää väitteen

$$\alpha = \lim_{n\to\infty} [a_0, a_1, \ldots, a_n]$$

kanssa.

Lauseen toinen osa seuraa lemmasta 3.4. Olkoon n parillinen, $n = 2k$. Tällöin

$$\frac{p_{2k}}{q_{2k}} < \alpha < \frac{p_{2k+1}}{q_{2k+1}}$$

ja kuten edellä

$$\frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k}}{q_{2k}} = \frac{(-1)^{2k}}{q_{2k}q_{2k+1}} = \frac{1}{q_nq_{n+1}}.$$

Vastaavasti parittomalle n, $n = 2k+1$ pätee

$$\frac{p_{2k+2}}{q_{2k+2}} < \alpha < \frac{p_{2k+1}}{q_{2k+1}}$$

ja

$$\frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k+2}}{q_{2k+2}} = \frac{(-1)^{2k+2}}{q_{2k+1}q_{2k+2}} = \frac{1}{q_nq_{n+1}}.$$

Siispä $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}}$ kaikilla $n \in \mathbb{N}$. □

Merkitään jatkossa lauseen 3.10 raja-arvoa $\alpha = \lim_{n\to\infty}[a_0, a_1, a_2, \ldots, a_n]$ yksinkertaisesti

$$\alpha = [a_0, a_1, a_2, \ldots]$$

ja sanotaan, että tämä on irrationaaliluvun α *jatkuva ketjumurtolukuesitys*. Kokonaislukua a_n sanotaan luvun α n.:ksi *ketjutekijäksi* ja rationaalilukua $\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n]$ α:n n.:ksi *konvergentiksi*.

Sopimus 3.11. Oletetaan jatkossa, että α on irrationaalinen, ellei erikseen muuta mainita ja kun sekaannuksen vaaraa ei ole.

Puhuttaessa luvun α konvergenteista, olisi mielekästä, jos jokainen $\frac{p_n}{q_n}$ olisi yksikäsitteinen eli jos irrationaaliluvun ketjumurtolukuesitys $[a_0, a_1, \ldots]$ olisi yksikäsittäinen. Jos näin on, voidaan puhua luvun α n.:stä konvergentista määrittelemättä erikseen, mistä jonosta (a_n) se on laskettu.

Vastauksen yksikäsitteisyyskysymykseen antaa seuraava lause.

Lause 3.12. *Olkoon α irrationaalinen ja kokonaislukujonot $(a_n)_{n=0}^{\infty}$ ja $(b_n)_{n=0}^{\infty}$ siten, että $a_n, b_n > 0$, kun $n \geq 1$ ja*

$$[a_0, a_1, a_2, \ldots] = \alpha = [b_0, b_1, b_2, \ldots].$$

Tällöin $a_n = b_n$ kaikilla, $n \in \mathbb{N}$.

Todistus. Tehdään todistus neljässä osassa:

(1) Huomataan ensin, että

$$[c_0, c_1, c_2, \ldots, c_n] = c_0 + \frac{1}{[c_1, c_2, \ldots, c_n]},$$

missä $[c_1, c_2, \ldots, c_n] > 0$, jolloin

$$c_0 \leq [c_0, c_1, c_2, \ldots, c_n] \leq c_0 + 1.$$

Tämä pätee kaikille $n \in \mathbb{N}$, ja siten myös yleisemmässä tapauksessa, sillä $[c_0, c_1, c_2, \ldots] = \lim_{n\to\infty}[c_0, c_1, c_2, \ldots, c_n]$. Toisin sanoen

$$c_0 \leq [c_0, c_1, c_2, \ldots] \leq c_0 + 1.$$

(2) Huomataan, että $[c_0, c_1, c_2, \ldots] = c_0 + [0, c_1, c_2, \ldots]$

(3) Osoitetaan, että lauseen oletuksin $a_0 = b_0$. Nyt kohdan 2 nojalla $[a_0, a_1, a_2, \ldots] = a_0 + [0, a_1, a_2, \ldots]$ ja vastaavasti $[b_0, b_1, b_2, \ldots] = b_0 + [0, b_1, b_2, \ldots]$. Oletuksen nojalla pätee nyt

$$b_0 - a_0 = [0, b_1, b_2, \ldots] - [0, a_1, a_2, \ldots].$$

Tälle saadaan kohdan 1 nojalla arvio

$$-1 \leq [0, b_1, b_2, \ldots] - [0, a_1, a_2, \ldots] \leq 1.$$

Koska $\alpha = b_0 + [0, b_1, b_2, \ldots] = a_0 + [0, a_1, a_2, \ldots]$ on irrationaalinen, ovat myös luvut $[0, b_1, b_2, \ldots]$ ja $[0, a_1, a_2, \ldots]$ irrationaalisia. Tällöin edellisen arvion epäyhtälöiden on oltava aidot ja saadaan arvio

$$-1 < [0, b_1, b_2, \ldots] - [0, a_1, a_2, \ldots] < 1,$$

josta saadaan

$$-1 < b_0 - a_0 < 1.$$

Koska $b_0 - a_0 \in \mathbb{Z}$, on oltava $a_0 = b_0$.

(4) Todistetaan itse väite induktiolla. Alkuaskel otettiin kohdassa 3. Oletetaan siis, että väite pätee, kun $n = k - 1$. Huomaa, että a_0 on ensimmäinen ketjutekijä. Oletetaan siis väitteen pätevän k:lle ensimmäiselle ketjutekijälle.

Todistetaan, että väite pätee kun $n = k$.
Nyt induktio-oletuksen nojalla $a_0 = b_0$, jolloin ehdosta

$$\alpha = a_0 + \frac{1}{[a_1, a_2, \ldots]} = b_0 + \frac{1}{[b_1, b_2, \ldots]}$$

seuraa $[a_1, a_2, \ldots] = [b_1, b_2, \ldots] =: \gamma$. Nyt edelleen γ on irrationaalinen, jolloin induktio-oletuksen nojalla sen ketjumurtolukuesityksen k ensimmäistä ketjutekijää ovat yksikäsitteisiä. Toisin sanoen luvun a_0 lisäksi luvut $a_1, \ldots, a_k$ ovat yksikäsitteisiä, jolloin induktioväite on todistettu. □

Huomautus 3.13. Oletus luvun α irrationaalisuudesta on oleellinen. Rationaaliluvulle pätee nimittäin $\frac{p}{q} = [a_0, a_1, a_2, \ldots, a_n] = [a_0, a_1, a_2, \ldots, a_n - 1, 1]$ ja kokonaisluvulle $k = [k] = [k - 1, 1]$.

Lause 3.12 kertoo siis vain, että jos irrationaaliluvulla on ketjumurtolukuesitys, niin se on yksikäsitteinen. Seuraava kysymys onkin, onko jokaisella irrationaaliluvulla tällainen esitys. Tähän kysymykseen vastaamiseksi esitellään algoritmi luvun α ketjumurtolukuesityksen muodostamiseksi.

Algoritmi 3.14. Olkoon $\alpha \in \mathbb{R}$. Sanotaan, että α on algoritmin *siemenluku*. Määritellään luvut $\alpha_0, \alpha_1, \alpha_2, \ldots \in \mathbb{R}$ ja $a_0, a_1, a_2, \ldots \in \mathbb{Z}$ rekursiivisesti:

(1) Asetetaan $a_0 = \lfloor \alpha \rfloor$ ja $\alpha_0 = \alpha$.
(2) Oletetaan, että α_{n-1} ja a_{n-1} on määritelty ja $\alpha_{n-1} \notin \mathbb{Z}$. Tällöin määritellään ensin $\alpha_n = \dfrac{1}{\alpha_{n-1} - a_{n-1}}$ ja tämän avulla $a_n = \lfloor \alpha_n \rfloor$. Jos $\alpha_{n-1} \in \mathbb{Z}$ niin sanotaan, että algoritmi päättyy vaiheessa $n - 1$, eikä lukuja a_k määritellä, kun $k \geq n$.

Lause 3.15. *Oletetaan, että jollakin siemenluvulla α algoritmi 3.14 ei pääty missään vaiheessa. Tällöin*

$$\alpha = \lim_{n \to \infty} [a_0, a_1, a_2, \ldots, a_n] = [a_0, a_1, a_2, \ldots].$$

Todistus. Lauseen 3.10 nojalla on olemassa raja-arvo $\lim_{n\to\infty}[a_0, a_1, a_2, \ldots, a_n]$. Riittää siis osoittaa, että kaikille $n \in \mathbb{N} \cup \{0\}$ pätee

$$[a_0, a_1, \ldots, a_{2n}] \leq \alpha \leq [a_0, a_1, \ldots, a_{2n+1}].$$

Osoitetaan tämä induktiolla.

(1) Osoitetaan tapaus $n = 0$. Kokonaisosan määritelmän nojalla

$$a_0 = \lfloor \alpha \rfloor \leq \alpha$$

ja tästä seuraa

$$[a_0, a_1] = a_0 + \frac{1}{a_1} \geq a_0 + \frac{1}{\lfloor \alpha \rfloor} = a_0 + \alpha_0 - a_0 = \alpha.$$

(2) Oletetaan, että väite pätee kun $n = k - 1$, missä $k \geq 1$. Oletetaan siis, että

$$[a_0, a_1, \ldots, a_{2k-2}] \leq \alpha$$

ja

$$[a_0, a_1, \ldots, a_{2k-1}] \geq \alpha.$$

(3) Osoitetaan tapaus $n = k$. Huomataan ensin, että

$$[a_0, a_1, \ldots, a_{2k}] = a_0 + \frac{1}{[a_1, \ldots, a_{2k}]}$$

Soveltamalla induktio-oletusta nyt lukuun $[a_1, \ldots, a_{2k}]$, joka saadaan algoritmista siemenluvulla α_1, saadaan (kun huomataan uudelleenindeksoinnin jälkeen, että tämän luvun viimeisen ketjutekijän indeksi on pariton) $[a_1, \ldots, a_{2k}] \geq \alpha_1$, jolloin

$$\frac{1}{[a_1, \ldots, a_{2k}]} \leq \frac{1}{\alpha_1}.$$

Siispä

$$[a_0, a_1, \ldots, a_{2k}] = a_0 + \frac{1}{[a_1, \ldots, a_{2k}]} \leq a_0 + \frac{1}{\alpha_1} = \alpha.$$

Ensimmäinen arvio on siis todistettu. Jälkimmäinen arvio saadaan, kun kirjoitetaan

$$[a_0, a_1, a_2 \ldots, a_{2k}, a_{2k+1}] = a_0 + \frac{1}{a_1 + \frac{1}{[a_2 \ldots, a_{2k}, a_{2k+1}]}}$$

ja sovelletaan induktio-oletusta lukuun $[a_2 \ldots, a_{2k}, a_{2k+1}]$, joka saadaan algoritmista siemenluvulla α_2. Tällöin saadaan (kuten edellä uudelleenindeksoinnin jälkeen)

$$[a_2 \ldots, a_{2k}, a_{2k+1}] \geq \alpha_2.$$

Käyttämällä tätä tietoa hyväksi

$$\begin{array}{rcccl} [a_0, a_1, a_2 \ldots, a_{2k}, a_{2k+1}] & = & a_0 + \dfrac{1}{a_1 + \frac{1}{[a_2 \ldots, a_{2k}, a_{2k+1}]}} & \geq & a_0 + \dfrac{1}{a_1 + \frac{1}{\alpha_2}} \\ & = & a_0 + \dfrac{1}{a_1 + \alpha_1 - a_1} & = & a_0 + \dfrac{1}{\alpha_1} \\ & = & a_0 + \alpha - a_0 & = & \alpha. \end{array}$$

Väite seuraa nyt induktioperiaatteesta. □

Esimerkki 3.16. (1) Kehitetään luvun $\sqrt{2}$ ketjumurtolukuesitys.

$$\begin{array}{l|l} \alpha_0 = \sqrt{2} & a_0 = 1 \\ \alpha_1 = \dfrac{1}{\sqrt{2}-1} = \dfrac{\sqrt{2}+1}{1} & a_1 = 2 \\ \alpha_2 = \dfrac{1}{\sqrt{2}+1-2} = \alpha_1 = \sqrt{2}+1 & a_2 = a_1 = 2 \\ \alpha_3 = \dfrac{1}{\sqrt{2}+1-2} = \alpha_2 = \alpha_1 = \sqrt{2}+1 & a_3 = a_2 = a_1 = 2 \end{array}$$

Huomataan, että algoritmissa alkavat toistua samat luvut, jolloin saadaan

$$\sqrt{2} = [1, 2, 2, 2, \ldots].$$

(2) Vastaavasti luvulle $\varphi = \frac{1+\sqrt{5}}{2}$ saadaan

$$\begin{array}{l|l} \alpha_0 = \frac{1+\sqrt{5}}{2} & a_0 = 1 \\ \alpha_1 = \dfrac{1}{\frac{1+\sqrt{5}}{2} - 1} = \dfrac{2}{\sqrt{5}-1} = \dfrac{2(\sqrt{5}+1)}{5-1} = \dfrac{1+\sqrt{5}}{2} & a_1 = a_0 = 1 \\ \alpha_2 = \dfrac{1}{\frac{1+\sqrt{5}}{2} - 1} = \dfrac{1+\sqrt{5}}{2} & a_2 = a_1 = 1 \end{array}$$

Algoritmissa alkavat toistua heti samat luvut, joten

$$\frac{1+\sqrt{5}}{2} = [1, 1, 1, \ldots].$$

(3) Määritellään vielä aiemmin tutuksi tulleen luvun $\frac{459}{182}$ ketjumurtolukuesitys käyttäen algoritmia 3.14.

$$\begin{array}{l|l} \alpha_0 = \frac{459}{182} & a_0 = 2 \\ \alpha_1 = \dfrac{1}{\frac{459}{182} - 2} = \dfrac{182}{95} & a_1 = 1 \\ \alpha_2 = \dfrac{1}{\frac{182}{95} - 1} = \dfrac{95}{87} & a_2 = 1 \\ \alpha_3 = \dfrac{1}{\frac{95}{87} - 1} = \dfrac{87}{8} & a_3 = 10 \\ \alpha_4 = \dfrac{1}{\frac{87}{8} - 10} = \dfrac{8}{7} & a_4 = 1 \\ \alpha_5 = \dfrac{1}{\frac{8}{7} - 1} = \dfrac{7}{1} & a_5 = 7 \end{array}$$

Koska $\alpha_5 \in \mathbb{Z}$, algoritmi pättyy vaiheessa 5. Ei liene yllätys, että luvulle saadaan sama ketjumurtolukuesitys kuin kappaleen alussa.

LAUSE 3.17. *Luvun α kahdesta peräkkäisestä konvergentista ainakin toiselle pätee*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

TODISTUS. Koska parittomat konvergentit ovat suurempia kuin α ja parilliset pienempiä kuin α, voidaan kirjoittaa

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\frac{p_n}{q_n} - \alpha\right| + \left|\frac{p_{n+1}}{q_{n+1}} - \alpha\right|.$$

Jos väite olisi nyt epätosi, niin lemman 3.4 nojalla saadaan

$$\frac{1}{q_n q_{n+1}} = \left|\frac{p_{n+1}q_n - p_n q_{n+1}}{q_n q_{n+1}}\right| = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}.$$

Tästä seuraa

$$\begin{array}{rcl} \dfrac{q_{n+1}^2 + q_n^2}{2q_n q_{n+1}} & \geq & \dfrac{1}{q_n q_{n+1}} \\ \Leftrightarrow \quad \dfrac{q_{n+1}^2 - 2q_n q_{n+1} + q_n^2}{2q_n q_{n+1}} & \leq & 0 \\ \Rightarrow \quad (q_{n+1} - q_n)^2 & \leq & 0, \end{array}$$

mikä on ristiriita lukuunottamatta erikoistapausta

$$n = 0,\ q_1 = q_0 = 1,\ a_1 = 1.$$

Tässä tapauksessa

$$0 < \frac{p_1}{q_1} - \alpha = 1 - \frac{1}{1 + \dfrac{1}{a_2 + \ldots}} < 1 - \frac{a_2}{a_2 + 1} = \frac{1}{a_2 + 1} \leq \frac{1}{2},$$

joten väite pätee. □

Esimerkki 3.18. Edellä laskettiin luvulle $\sqrt{2}$ ketjumurtolukuesitys

$$\sqrt{2} = [1, 2, 2, 2, \ldots].$$

Tästä esityksestä saadaan seuraavat konvergentit:

$$\frac{p_0}{q_0} = 1,\ \frac{p_1}{q_1} = \frac{3}{2},\ \frac{p_2}{q_2} = \frac{7}{5},\ \frac{p_3}{q_3} = \frac{17}{12},\ \frac{p_4}{q_4} = \frac{41}{29}\ \frac{p_5}{q_5} = \frac{99}{70},\ \frac{p_6}{q_6} = \frac{239}{169},\ \ldots$$

Näitä vastaaville virheille $R(n) = \left|\sqrt{2} - \dfrac{p_n}{q_n}\right|$ saadaan arviot

$$\begin{aligned}
&R(0) < 0,5 = \frac{1}{2 \cdot 1^2}, && R(1) < 0,01 < \frac{1}{2 \cdot 2^2},\\
&R(2) < 0,01 < \frac{1}{5^2}, && R(3) < 0,003 < \frac{1}{2 \cdot 12^2},\\
&R(4) < 0,000421 < \frac{1}{2 \cdot 29^2}, && R(5) < 0,000073 < \frac{1}{2 \cdot 70^2}\\
&R(6) < 1,24 \cdot 10^{-6} < \frac{1}{2 \cdot 169^2}, && \ldots
\end{aligned}$$

On siis todettu, että irrationaaliluvuille on mahdollista löytää äärettömän monta approksimaatioita $\frac{p}{q}$ siten, että tehty virhe on pienempi kuin $\frac{1}{q^2}$. Seuraavissa luvuissa tutkitaan, voidaanko luvun q eksponenttia kasvattaa suuremmaksi kuin 2. Tällöin arvion tarkkuus paranisi entistä nopeammin.

Ketjumurtoluvuilla on lisäksi joitakin mielenkiintoisia sovelluksia, joita ei tämän tutkielman puitteissa tutkita tarkemmin. Ketjumurtolukuja voidaan käyttää esimerkiksi

(1) Luonnollisten lukujen p ja q suurimman yhteisen tekijän laskemiseen [**7**],
(2) Markovin[1] lukujen laskemiseen ja yhtälön
$$k^2 + l^2 + m^2 = 3klm, \quad (0 \leq k, l \leq m)$$
ratkaisemiseen [**2**],
(3) Pellin yhtälön[2]
$$x^2 - dy^2 = \pm 1$$
ratkaisemiseen [**2**] sekä
(4) pienillä avainluvuilla RSA-salauksen purkamiseen käyttäen Wienerin hyökkäystä [**4**, **15**].

[1] Andrei Andrejevitš Markov, 1856—1922

[2] Tämä yhtälö kantaa Pellin nimeä, vaikka kunnia kuuluisi Lordi Brounckerille.

LUKU 4

Liouvillen lause

Toisen asteen yhtälön irrationaalisia juuria eli niin sanottuja kvadraattisia lukuja tutkittaessa huomataan, että on olemassa vakio $c = c(\alpha) > 0$ siten, että

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^2}$$

kaikilla supistetussa muodossa olevilla rationaaliluvuilla $\frac{p}{q} \in \mathbb{Q}$. Tämä on kuitenkin vain seuraus yleisemmästä tuloksesta, jonka Liouville[1] todisti vuonna 1844.

MÄÄRITELMÄ 4.1 (Algebrallinen ja transkendenttinen luku). Sanotaan, että luku $\alpha \in \mathbb{R}$ on *algebrallinen*, jos se on kokonaislukukertoimisen polynomin

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots a_1 x + a_0, \quad a_n, \dots, a_0 \in \mathbb{Z}, \quad a_n \neq 0$$

nollakohta. Sanotaan, että luku on *transkendenttinen*, jos se ei ole algebrallinen.

MÄÄRITELMÄ 4.2 (Minimaalipolynomi ja algebrallisen luvun aste). Sanotaan, että polynomi

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \dots a_1 x + a_0, \quad a_n, \dots, a_0 \in \mathbb{Z}, \quad a_n \neq 0$$

on algebrallisen luvun α *minimaalipolynomi*, jos kertoimilla a_i ei ole yhteistä kokonaislukutekijää (lukuja ± 1 lukuunottamatta) ja P on pienintä astetta oleva polynomi, joka toteuttaa yhtälön

$$P(\alpha) = 0.$$

Sanotaan, että algebrallisen luvun *aste* on sen minimaalipolynomin asteluku.

HUOMAUTUS 4.3. Jokaisella algebrallisella luvulla on minimaalipolynomi, jonka aste on yksikäsitteinen.

LEMMA 4.4. *Olkoon $P(x)$ kokonaislukukertoiminen polynomi, jonka aste on n ja $\frac{p}{q} \in \mathbb{Q}$ siten, että $P(\frac{p}{q}) = 0$. Tällöin on olemassa kokonaislukukertoiminen polynomi $Q(x)$, jonka aste on $n-1$ ja jolle pätee*

$$P(x) = \left(x - \frac{p}{q}\right) Q(x).$$

TODISTUS. Väite seuraa polynomin $P(x)$ jaollisuudesta polynomilla $\left(x - \frac{p}{q}\right)$ ja Gaussin lemman seurauksesta. Katso [**13**, s. 33] ja [**3**, s. 161-162]. □

LEMMA 4.5. *Olkoon α algebrallinen luku, jonka aste on $d \geq 2$ ja P sen minimaalipolynomi. Tällöin polynomilla P ei ole rationaalisia juuria.*

[1] Joseph Liouville, 1809—1882

TODISTUS. Tehdään antiteesi: Olemassa $\frac{p}{q} \in \mathbb{Q}$ siten, että $P(\frac{p}{q}) = 0$. Tällöin lemman 4.4 nojalla on olemassa kokonaislukukertoiminen polynomi Q, jonka aste on $d-1$ ja jolle pätee

$$P(x) = \left(x - \frac{p}{q}\right) Q(x). \tag{4.1}$$

Koska P on luvun α minimaalipolynomi, pätee $P(\alpha) = (\alpha - \frac{p}{q})Q(\alpha) = 0$. Edelleen koska $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ja $\frac{p}{q} \in \mathbb{Q}$, niin $\alpha - \frac{p}{q} \neq 0$, joten $Q(\alpha) = 0$. Tämä on ristiriita, sillä polynomin Q aste on $d-1$ ja oletuksen mukaan luvun α aste on d. Antiteesi on siis epätosi ja väite pätee. □

LAUSE 4.6 (Liouvillen lause, 1844). *Olkoon α algebrallinen irrationaaliluku, jonka aste on $d \geq 2$. Tällöin on olemassa vakio $c = c(\alpha) > 0$ siten, että*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^d}$$

kaikilla rationaaliluvuilla $\frac{p}{q} \in \mathbb{Q}$.

TODISTUS. a) Olkoon $P(x)$ luvun α minimaalipolynomi ja d sen aste.
b) Polynomin P Taylorin sarjasta saadaan

$$\begin{aligned}
\left|P\left(\frac{p}{q}\right)\right| &= \left|\sum_{k=1}^{d} \frac{1}{k!} P^{(k)}(\alpha) \left(\frac{p}{q} - \alpha\right)^k\right| \\
&\leq \left|\sum_{k=1}^{d} \frac{1}{k!} P^{(k)}(\alpha)\right| \left|\left(\frac{p}{q} - \alpha\right)\right| \\
&< \frac{1}{c(\alpha)} \left|\alpha - \frac{p}{q}\right|,
\end{aligned}$$

kun $\left|\alpha - \frac{p}{q}\right| \leq 1$. Tämä oletus voidaan tehdä, sillä väite pätee kaikille vakioille $0 < c(\alpha) < 1$, jos $\left|\alpha - \frac{p}{q}\right| > 1$.

c) Koska $P(x)$ on kokonaislukukertoiminen polynomi, jonka aste on $d \geq 2$, niin $q^d P(\frac{p}{q})$ on kokonaisluku. Lisäksi lemman 4.5 nojalla kaikilla $\frac{p}{q} \in \mathbb{Q}$ pätee $P(\frac{p}{q}) \neq 0$. Siispä $\left|q^d P(\frac{p}{q})\right| \geq 1$, eli

$$\left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}.$$

Yhdistämällä tämä edelliseen arvioon saadaan väite

$$\begin{aligned}
\frac{1}{c(\alpha)} \left|\alpha - \tfrac{p}{q}\right| &> \left|P(\tfrac{p}{q})\right| \geq \frac{1}{q^d} \\
\Rightarrow \qquad \left|\alpha - \tfrac{p}{q}\right| &> \frac{c(\alpha)}{q^d}.
\end{aligned}$$

□

HUOMAUTUS 4.7. Luku c on vakio siinä mielessä, että se riippuu vain luvusta α eikä ollenkaan luvusta $\frac{p}{q}$, jolla arvio tehdään. Vakio c sopii siis *kaikille* luvuille $\frac{p}{q}$.

Liouvillen lause ratkaisi yhden 1800-luvun suurimmista matemaattisista ongelmista, sillä se mahdollistaa transkendenttilukujen konstruoinnin. Tämä tapahtuu siten, että muodostetaan reaaliluku, jota voidaan arvioida rationaaliluvuilla tarkemmin kuin mitään astetta d olevaa algebrallista lukua, jonka arviointitarkkuudelle Liouvillen lause antaa rajan.

Esimerkki 4.8 ([**7**], s. 145). Osoitetaan, että luku

$$\alpha := \sum_{n=1}^{\infty} 10^{-n!} = 0.11000100000000000000000001000\ldots$$

on transkendenttinen.

Todistus. Huomataan ensin, että sarja suppenee johonkin reaalilukuun majoranttiperiaatten nojalla, sillä $10^{-n!} < 10^{-n}$ ja tunnetusti gemetrinen sarja $\sum_{n=1}^{\infty} 10^{-n}$ suppenee.
Merkitään kaikille $n \in \mathbb{N}$ äärellistä summaa

$$S_n = \sum_{k=1}^{n} 10^{-k!} = \frac{1}{10} + \frac{1}{100} + \ldots + \frac{1}{10^{(n-1)!}} + \frac{1}{10^{n!}}.$$

Tällöin $S_n \in \mathbb{Q}$ kaikilla $n \in \mathbb{N}$ ja $S_n \to \alpha$, kun $n \to \infty$. Siis

$$S_n = \frac{1}{10^{n!}}(10^{n!-1} + 10^{n!-2} + 10^{n!-6} + \ldots + 10^{n!-(n-1)!} + 1),$$

joten $S_n = \frac{p_n}{q_n}$, missä $p_n = 10^{n!-1} + 10^{n!-2} + 10^{n!-6} + \ldots + 10^{n!-(n-1)!} + 1 \in \mathbb{N}$
ja $q_n = 10^{n!} \in \mathbb{N}$. Lisäksi

$$|\alpha - S_n| = \sum_{k=n+1}^{\infty} 10^{-k!} = \frac{1}{10^{(n+1)!}}(1 + \frac{1}{10^{(n+2)!-(n+1)!}} + \frac{1}{10^{(n+3)!-(n+1)!}} + \ldots).$$

Kun huomataan, että kaikilla $k \geq n+2$ pätee $k! - (n+1)! \geq k - (n+1)$, niin voidaan tehdä arvio

$$|\alpha - S_n| \leq \frac{1}{10^{(n+1)!}}(1 + \frac{1}{10^{(n+2)-(n+1)!}} + \frac{1}{10^{(n+3)-(n+1)}} + \ldots) = \frac{1}{10^{(n+1)!}} \sum_{k=0}^{\infty} \frac{1}{10^k}.$$

Geometrisen summakaavan nojalla $\sum_{k=0}^{\infty} \frac{1}{10^k} = \frac{10}{9}$, jolloin voidaan arvioida edelleen

$$|\alpha - S_n| \leq \frac{1}{10^{(n+1)!}} \frac{10}{9} < \frac{2}{10^{(n+1)!}}.$$

Suurilla $n \in \mathbb{N}$ pätee $\dfrac{2}{10^{(n+1)!}} = \dfrac{2}{(10^{n!})^{(n+1)}} < \dfrac{1}{(10^{n!})^2}$, jolloin siis

$$|\alpha - S_n| = \left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n^2}.$$

Koska rationaaliluvut $S_n = p_n/q_n$ ovat eri lukuja ja edellinen arvio pätee, on α lauseen 2.7 nojalla irrationaalinen. Osoitetaan, että α on transkendenttinen.
Antiteesi: α on algebrallinen. Olkoon sen aste $d \geq 2$. Liouvillen lauseen nojalla on tällöin vakio $c > 0$ siten, että kaikilla $n \in \mathbb{N}$

$$\left|\alpha - \frac{p_n}{q_n}\right| > \frac{c}{q_n^d}.$$

Edellisten arvioiden nojalla kaikilla $n \in \mathbb{N}$ pätee

$$\begin{array}{ccccc} \frac{2}{10^{(n+1)!}} & > & \left|\alpha - \frac{p_n}{q_n}\right| & > & \frac{c}{(10^{n!})^d} \\ \Rightarrow & & \frac{1}{10^{(n+1-d)n!}} & > & \frac{c}{2}. \end{array}$$

Tämä on kuitenkin ristiriita, sillä kaikille $c > 0$ löytyy $n_c \in \mathbb{N}$ siten, että

$$\frac{1}{10^{(n_c+1-d)n_c!}} < \frac{c}{2}.$$

Antiteesi on siis väärä ja luku α on transkendenttinen. □

LUKU 5

Rothin lause

1. Historiaa

Liouvillen lausetta voidaan parantaa. Olkoon α algebrallinen luku, jonka aste on $d \geq 2$. Haluamme löytää parhaan mahdollisen eksponentin $\lambda(\alpha)$ siten, että on olemassa luku $c = c(\alpha) > 0$ ja kaikilla rationaaliluvuilla $\frac{p}{q} \in \mathbb{Q}$ pätee

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{\lambda(\alpha)}}.$$

Liouvillen lauseen nojalla voidaan ainakin valita $\lambda(\alpha) = d$. Arviota luvulle $\lambda(\alpha)$ on parannettu vuosien varrella useaan otteeseen

- 1844 Liouville: $\lambda(\alpha) = d$
- 1909 Thue: $\lambda(\alpha) > \frac{1}{2}d + 1$
- 1921 Siegel: $\lambda(\alpha) > 2\sqrt{d}$
- 1947 Dyson: $\lambda(\alpha) > \sqrt{2d}$
- 1955 Roth: $\lambda(\alpha) > 2$

Rothin tulos on siitä merkittävä, että se poisti kokonaan riippuvuuden luvun α asteesta d. Tämän työnsä ansiosta hän sai Fieldsin mitalin vuonna 1958. Rothin lause voidaan kirjottaa kahdessa keskenään ekvivalentissa muodossa.

LAUSE 5.1 (Rothin lause, 1955). *Olkoon α algebrallinen luku, jonka aste on $d \geq 2$ ja $\varepsilon > 0$. Tällöin on olemassa vakio $c(\alpha, \varepsilon) > 0$ siten, että kaikilla $\frac{p}{q} \in \mathbb{Q}$*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha, \varepsilon)}{q^{2+\varepsilon}}.$$

LAUSE 5.2. *Olkoon α algebrallinen luku, jonka aste on $d \geq 2$ ja $\varepsilon > 0$. Tällöin on korkeintaan* äärellisen *monta lukua $\frac{p}{q} \in \mathbb{Q}$ siten, että*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}.$$

HUOMAUTUS 5.3.
(1) Huomataan ensin, että jos luvun α aste on $d = 2$ (eli kun luku on kvadraattinen), antaa Liouvillen lause vahvemman tuloksen kuin Rothin lause.
(2) Lauseesta 5.2 huomataan kuitenkin, että arvio $\lambda(\alpha) = 2 + \varepsilon$, $\varepsilon > 0$ on paras mahdollinen, joka voidaan tehdä *kaikille* irrationaalisille algebrallisille luvuille, sillä lauseen 2.7 nojalla kaikille irrationaaliluvuille α on olemassa äärettömän monta rationaalilukua $\frac{p}{q} \in \mathbb{Q}$ siten, että

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Toisin sanoen, jos lauseen 5.2 arvio pätisi jollakin algebrallisella luvulla α, kun $\lambda(\alpha) = 2$, olisi luvun α oltava rationaalinen eli astetta $d = 1$.

2. Esitietoja

Rothin lauseen todistus on moniosainen ja sen tekemiseen tarvitaan useampi aputulos. Todistus voidaan jakaa karkeasti kahteen osaan (vertaa Liouvillen lauseen todistukseen):

I) Oletetaan, että antiteesi pätee ja muodostetaan m muuttujan polynomi R, joka *katoaa vahvasti* pisteessä $(\alpha, \alpha, \ldots, \alpha) \in \mathbb{R}^m$. Tämä tarkoittaa sitä, että itse funktion arvon lisäksi myös *monet* sen osittaisderivaatat ovat 0 tässä pisteessä. Tällöin sen graafi on erittäin tasainen pisteen $(\alpha, \alpha, \ldots, \alpha)$ ympäristössä, eli polynomin P on kadottava *melko vahvasti* pisteessä $(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_m}{q_m})$.

II) Seuraavaksi todistetaan, että jos polynomin R asteet kasvavat eksponentiaalisesti, niin se ei voi kadota *liian vahvasti* pisteessä $(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_m}{q_m})$. Tätä tulosta kutsutaan Rothin lemmaksi ja se on ristiriidassa edellisen kohdan kanssa.

Tässä tehtävä todistus seuraa melko tarkasti Schmidtin todistusta [**11**], joka vuorostaan seuraa Casselsin todistusta [**3**]. Alkuperäinen todistus löytyy lähteestä [**10**]. Todistetaan tarvittavat lemmat aluksi, jolloin Rothin lauseen todistus voidaan lopulta kasata niistä kappaleessa 7.

Aloitetaan todistamalla, että lauseet 5.1 ja 5.2 ovat ekvivalentteja.

Lemma 5.4. *Lauseet 5.1 ja 5.2 ovat ekvivalentteja.*

Todistus. Olkoon α algebrallinen luku, jonka aste on $d \geq 2$ ja $\varepsilon > 0$.

Oletetaan ensin, että lause 5.2 on tosi. Olkoot $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m} \in \mathbb{Q}$ ne rationaaliluvut, jotka toteuttavat epäyhtälön

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^{2+\varepsilon}} \tag{5.1}$$

kaikilla $1 \leq n \leq m$. Voidaan olettaa, että näitä lukuja $\frac{p_n}{q_n}$ on ainakin yksi. Jos näin ei olisi, voitaisiin valita $C(\alpha, \varepsilon) = 1$. Koska lukuja $\frac{p_n}{q_n}$ on äärellinen määrä, voidaan valita $1 \leq k \leq m$ siten, että kaikilla $\frac{p_n}{q_n}$ pätee

$$\left|\alpha - \frac{p_k}{q_k}\right| \leq \left|\alpha - \frac{p_n}{q_n}\right|.$$

Merkitään $r = \left|\alpha - \frac{p_k}{q_k}\right|$. Koska α on irrationaalinen, pätee $r > 0$ ja koska $\frac{p_k}{q_k}$ toteuttaa epäyhtälön (5.1), niin pätee $r < 1$. Nyt voidaan valita $C(\alpha, \varepsilon) = r$, jolloin kaikilla $\frac{p_n}{q_n}$

$$\frac{C(\alpha, \varepsilon)}{q_n^{2+\varepsilon}} = \frac{r}{q_n^{2+\varepsilon}} < r \leq \left|\alpha - \frac{p_n}{q_n}\right|.$$

Tällöin kaikilla $\frac{p}{q} \in \mathbb{Q}$ pätee

$$\left|\alpha - \frac{p}{q}\right| > \frac{C(\alpha, \varepsilon)}{q^{2+\varepsilon}}.$$

Oletetaan seuraavaksi, että Rothin lause on tosi. Tehdään antiteesi: On olemassa äärettömän monta epäyhtälön

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^{2+\varepsilon}} \tag{5.2}$$

toteuttavaa rationaalilukua $\frac{p_n}{q_n}$. Voidaan olettaa, että kaikilla $n, m \in \mathbb{N}$ pätee $\frac{p_n}{q_n} \neq \frac{p_m}{q_m}$, kun $n \neq m$. Koska kullakin q_n epäyhtälö (5.2) voi toteutua vain äärellisellä määrällä p_n, on olemassa jonon q_n osajono, $q_{\varphi(n)}$, jolle $q_{\varphi(n)} \to \infty$. Merkitään tätä osajonoa $(q_{\varphi(n)})$ yksinkertaisesti (q_n).

Koska $\varepsilon > 0$, voidaan valita luku $\gamma > 0$ siten, että $0 < \gamma < \varepsilon$. Nyt Rothin lauseen nojalla on olemassa vakio $C(\alpha, \gamma) > 0$ siten, että kaikilla $\frac{p}{q} \in \mathbb{Q}$ pätee

$$\frac{C(\alpha,\gamma)}{q^{2+\gamma}} < \left|\alpha - \frac{p}{q}\right|. \tag{5.3}$$

Tämä pätee erityisesti luvuilla $\frac{p_n}{q_n}$. Yhdistämällä epäyhtälöt (5.2) ja (5.3) saadaan

$$\frac{C(\alpha,\gamma)}{q_n^{2+\gamma}} < \frac{1}{q_n^{2+\varepsilon}},$$

josta saadaan edelleen

$$C(\alpha,\gamma) < \frac{1}{q_n^{\varepsilon-\gamma}}$$

kaikilla $n \in \mathbb{N}$. Koska $\varepsilon - \gamma > 0$, niin $\dfrac{1}{q_n^{\varepsilon-\gamma}} \to 0$, kun $q_n \to \infty$. Tämä on ristiriita, sillä $C(\alpha, \gamma)$ on aidosti positiivinen vakio. Antiteesi on siten väärä ja väite tosi. □

MÄÄRITELMÄ 5.5 (Algebrallinen kokonaisluku). Sanotaan, että α on *algebrallinen kokonaisluku*, jos se toteuttaa jonkin kokonaislukukertoimisen yhtälön

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

HUOMAUTUS 5.6. Nimitys algebrallinen kokonaisluku tulee siitä, että kokonaisluku α toteuttaa yhtälön, joka on muotoa

$$\alpha + a_0 = 0,$$

Jokainen kokonaisluku on siis algebrallinen kokonaisluku.

LAUSE 5.7. *Olkoon α algebrallinen kokonaisluku ja n sen aste. Tällöin $a_n = 1$ luvun α minimaalipolynomissa.*

TODISTUS. Katso [**5**, lause 236, s. 265] □

LEMMA 5.8. *Rothin lause on tosi, jos se pätee algebrallisille kokonaisluvuille.*

TODISTUS. Olkoon α algebrallinen luku ja olkoon $f(x) = a_n x^n + \cdots + a_0$ sen minimaalipolynomi. Merkitään $z = a_n\alpha$. Tällöin pätee

$$z^n + a_{n-1}z^{n-1} + a_{n-2}a_n z^{n-2} + \ldots + a_n^{n-1}a_0 = a_n^{n-1}f(\alpha) = 0,$$

siis z on algebrallinen kokonaisluku.

Jos

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}, \tag{5.4}$$

niin

$$\left|z - a_n \frac{p}{q}\right| < |a_n| \frac{1}{q^{2+\varepsilon}} < \frac{1}{q^{2+\frac{1}{2}\varepsilon}}, \tag{5.5}$$

kun q on tarpeeksi iso. Jos epäyhtälöllä (5.4) on äärettömän monta ratkaisua, niin myös epäyhtälöllä (5.5) on. Koska ε on mielivaltainen, olisi z ristiriidassa Rothin lauseen kanssa, jos α olisi. Siispä väite pätee algebrallisille luvuille, jos se pätee algebrallisille kokonaisluvuille. □

Puhuttaessa jatkossa algebrallisesta luvusta α, voidaan olettaa, että α on algebrallinen kokonaisluku, jonka minimaalipolynomi on f ja polynomin f johtava kerroin on 1.

3. Polynomin indeksi

Todistaakseen lauseensa Roth käyttää usean muuttujan polynomeja, jotka ovat muotoa

$$R(x_1, \ldots, x_m) = \sum_{0 \le j_h \le r_h} C(j_1, \ldots, j_m) x_1^{j_1} \cdots x_m^{j_m},$$

missä luvut $C(j_1, \ldots, j_m)$ ovat kokonaislukukertoimia ja luku r_h muuttujan x_h suurin potenssi.

MÄÄRITELMÄ 5.9. Sanotaan, että polynomin R *korkeus* on

$$\lceil R \rceil = \max |C(j_1, \ldots, j_m)|$$

ja kirjoitetaan

$$R_{i_1,\ldots,i_m} = \frac{1}{i_1! \cdots i_m!} \frac{\partial^{i_1} \cdots \partial^{i_m}}{\partial x_1^{i_1} \cdots \partial x_m^{i_m}} R$$

kaikilla ei-negatiivisilla konaisluvuilla i_h, $1 \le h \le m$. Merkintöjen yksinkertaistamiseksi käytetään merkintään $R_{\underline{i}}$, kun $\underline{i} = (i_1, \ldots, i_m)$ on yhteydestä selvä.

LEMMA 5.10. *i) Jos R on kokonaislukukertoiminen, niin myös $R_{i_1,\ldots,i_m}$ on sitä.*
ii) Jos muuttujan x_h aste polynomissa R on r_h, niin sen aste polynomissa $R_{\underline{i}}$ on korkeintaan $r_h - i_h$. Lisäksi pätee $R_{\underline{i}} \equiv 0$, jos $i_h > r_h$ kaikilla $1 \le h \le m$.
iii) Lopuksi

$$\lceil R_{\underline{i}} \rceil \le 2^{r_1 + \cdots + r_m} \lceil R \rceil.$$

TODISTUS. i) Huomataan ensin, että Taylorin kaavasta saadaan

$$R_{\underline{i}} = \sum_{i_h \le j_h \le r_h} \binom{j_1}{i_1} \cdots \binom{j_m}{i_m} C(j_1, \ldots, j_m) x^{j_1 - i_1} \cdots x_m^{j_m - i_m}, \tag{5.6}$$

missä binomikertoimet $\binom{j}{i}$ ovat kokonaislukuja.

ii) Seuraa yhtälöstä (5.6).

iii) Koska

$$\binom{j}{i} \le \sum_{0 \le i \le j} \binom{j}{i} = (1+1)^j \le 2^r,$$

kun $0 \le i \le j \le r$, niin väite seuraa yhtälöstä (5.6).

□

LEMMA 5.11.

$$R(x_1+y_1,\ldots,x_m+y_m) \;=\; \sum_{0\le i_h\le r_h} y_1^{i_1}\cdots y_m^{i_m} R_{\underline{i}}(x_1,\ldots,x_m) \tag{5.7}$$

TODISTUS. Yhtälö (5.7) seuraa Taylorin lauseesta, sillä R on polynomi. Katso [**9**, s.7]. □

MÄÄRITELMÄ 5.12. Olkoot $\alpha_1,\ldots,\alpha_m$ reaalilukuja ja $r_1,\ldots,r_m$ positiivisia kokonaislukuja. Sanotaan, että *polynomilla* $R\not\equiv 0$ *on indeksi* $I =: \operatorname{ind}_{\underline{\alpha},\underline{r}} R$ *pisteessä* $\underline{\alpha}=(\alpha_1,\ldots,\alpha_m)$ *pisteen* $\underline{r}=(r_1,\ldots,r_m)$ *suhteen*, jos I on pienin summa

$$\sum_{h=1}^{m}\frac{i_h}{r_h},$$

jolle $R_{\underline{i}}(\alpha_1,\ldots,\alpha_m)$ ei katoa. Toisin sanoen,

$$\operatorname*{ind}_{\underline{\alpha},\underline{r}} R = \min\left\{\sum_{1\le h\le m}\frac{i_h}{r_h} \;:\; \underline{i}=(i_1,\ldots,i_m) \text{ s.e } i_h\in\mathbb{Z}_+ \text{ ja } R_{\underline{i}}(\alpha)\neq 0\right\}.$$

Jos $R\equiv 0$, niin sanotaan, että indeksi I on $+\infty$.

HUOMAUTUS 5.13. Indeksin määritelmä on mielekäs, sillä kirjoittamalla

$$R(\alpha_1,\ldots,\alpha_m) = R(r_1+(\alpha_1-r_1),\ldots,r_m+(\alpha_m-r_m))$$

huomataan, että yhtälön (5.7) nojalla on olemassa $\underline{i}=(i_1,\ldots,i_m)$ siten, että $R_{\underline{i}}$ ei katoa paitsi erikoistapauksessa $R\equiv 0$. Huomataan myös, että erityisesti $\operatorname{ind}_{\underline{\alpha},\underline{r}} R = 0$, jos $R(\alpha_1,\ldots,\alpha_m)\neq 0$.

ESIMERKKI 5.14. (1) Olkoot $R(x)=x^2$, $\underline{\alpha}=\alpha=0$ ja $\underline{r}=r=1$. Tällöin $R(\alpha)=0$ ja $R_1(\alpha)=0$, mutta $R_2(\alpha)=\frac{1}{2}\frac{\partial^2}{\partial x^2}R(\alpha)=1\neq 0$, jolloin $\sum_{h=1}^{1}\frac{i_h}{r_h}=\frac{2}{1}=2$, joten $\operatorname{ind}_{\underline{\alpha},\underline{r}} R=2$.

(2) Olkoot $R(x_1,x_2)=x_1x_2+x_2^2$, $\underline{\alpha}=(1,-1)$ ja $\underline{r}=(1,2)$. Tällöin
   i) $R(\underline{\alpha})=0$,
   ii) $R_{1,0}(\underline{\alpha})=-1\neq 0$,
   iii) $R_{0,1}(\underline{\alpha})=1-2=-1\neq 0$,
   Kohdasta ii) saadaan summaksi $\sum_{h=1}^{2}\frac{i_h}{r_h}=\frac{1}{1}+\frac{0}{2}=1$ ja kohdasta iii) $\sum_{h=1}^{2}\frac{i_h}{r_h}=\frac{0}{1}+\frac{1}{2}=\frac{1}{2}$. Muita osittaisderivaattoja ei tarvitse laskea, sillä lukujen i_h kasvattaminen vain kasvattaa summaa $\sum_{h=1}^{2}\frac{i_h}{r_h}$ lukujen r_h ollessa kiinnitettyjä. Siispä $\operatorname{ind}_{\underline{\alpha},\underline{r}} R=\frac{1}{2}$.

SOPIMUS 5.15. Merkitään yksinkertaisesti $\operatorname{ind} R$, kun tarkoitetaan $\operatorname{ind}_{\underline{\alpha},\underline{r}} R$ ja sekaannuksen vaaraa ei ole.

LEMMA 5.16. *i)* $\operatorname{ind} R_{\underline{i}} \ge \operatorname{ind} R - \sum_{h=1}^{m}\frac{i_h}{r_h}$
ii) $\operatorname{ind}(R+T)\ge\min(\operatorname{ind} R,\operatorname{ind} T)$
iii) $\operatorname{ind}(R\cdot T)=\operatorname{ind} R+\operatorname{ind} T$

TODISTUS. i) Olkoon $T=R_{\underline{i}}$ ja oletetaan, että $T_{\underline{j}}(\alpha_1,\ldots,\alpha_m)\neq 0$. Siis $R_{\underline{i}+\underline{j}}(\alpha_1,\ldots,\alpha_m)\neq 0$. Tällöin

$$\frac{i_1+j_1}{r_1}+\ldots+\frac{i_m+j_m}{r_m}\ge\operatorname{ind} R,$$

joten

$$\frac{j_1}{r_1} + \ldots + \frac{j_m}{r_m} \geq \operatorname{ind} R - \sum_{h=1}^{m} \frac{i_h}{r_h}$$

eli

$$\operatorname{ind} R_{\underline{i}} = \operatorname{ind} T \geq \operatorname{ind} R - \sum_{h=1}^{m} \frac{i_h}{r_h}.$$

ii) Oletetaan, että $(R+T)_{\underline{i}}(\alpha_1, \ldots, \alpha_m) \neq 0$. Tällöin pätee $R_{\underline{i}}(\alpha_1, \ldots, \alpha_m) \neq 0$ tai $T_{\underline{i}}(\alpha_1, \ldots, \alpha_m) \neq 0$. Siispä joko

$$\sum_{h=1}^{m} \frac{i_h}{r_h} \geq \operatorname{ind} R$$

tai

$$\sum_{h=1}^{m} \frac{i_h}{r_h} \geq \operatorname{ind} T,$$

joten

$$\operatorname{ind}(R+T) \geq \min(\operatorname{ind} R, \operatorname{ind} T).$$

iii) Huomataan, että

$$(R \cdot T)_{\underline{k}}(\alpha_1, \ldots, \alpha_m) = \sum_{\underline{i}+\underline{j}=\underline{k}} C(\underline{i}, \underline{j}) R_{\underline{i}}(\alpha_1, \ldots, \alpha_m) T_{\underline{j}}(\alpha_1, \ldots, \alpha_m), \tag{5.8}$$

kun $\underline{k} = (k_1, \ldots, k_m)$ ja $k_h \geq 0$ kaikilla $1 \leq h \leq m$. Oletetaan, että $\underline{k}$ on valittu siten, että $\sum_{h=1}^{m} \frac{k_h}{r_h} = \operatorname{ind}(R \cdot T)$ ja $(R \cdot T)_{\underline{k}}(\alpha_1, \ldots, \alpha_m) \neq 0$. Yhtälön (5.8) nojalla on olemassa $\underline{i}$ ja $\underline{j}$ siten, että $\underline{i} + \underline{j} = \underline{k}$ ja $R_{\underline{i}}(\alpha_1, \ldots, \alpha_m) \neq 0$ ja $T_{\underline{j}}(\alpha_1, \ldots, \alpha_m) \neq 0$. Tällöin $\sum_{h=1}^{m} \frac{i_h}{r_h} \geq \operatorname{ind} R$ ja $\sum_{h=1}^{m} \frac{j_h}{r_h} \geq \operatorname{ind} T$, joten

$$\operatorname{ind}(R \cdot T) = \sum_{h=1}^{m} \frac{k_h}{r_h} = \sum_{h=1}^{m} \frac{i_h}{r_h} + \sum_{h=1}^{m} \frac{j_h}{r_h} \geq \operatorname{ind} R + \operatorname{ind} T. \tag{5.9}$$

Toisaalta, on olemassa ainakin yksi $\underline{i} = (i_1, \ldots, i_m)$ siten, että $\sum_{h=1}^{m} \frac{i_h}{r_h} = \operatorname{ind} R$ ja $R_{\underline{i}}(\alpha_1, \ldots, \alpha_m) \neq 0$. Olkoon $\underline{i}$ siten, että se on näistä vektoreista ensimmäinen leksikografisessa järjestyksessä[1]. Toisin sanoen sen ensimmäisten indeksien arvot ovat mahdollisimman pienet. Olkoon vastaavasti $\underline{j} = (j_1, \ldots, j_m)$ leksikografisessa järjestyksessä ensimmäinen $\underline{j}$, jolle $\sum_{h=1}^{m} \frac{j_h}{r_h} = \operatorname{ind} T$ ja $T_{\underline{j}}(\alpha_1, \ldots, \alpha_m) \neq 0$. Asetetaan $\underline{k} = \underline{i} + \underline{j}$.

Tutkitaan seuraavaksi, mitkä tapaukset vaikuttavat summaan (5.8). Jos olisi $\tilde{\underline{i}} = (\tilde{i}_1, \ldots, \tilde{i}_m)$, joka olisi leksikografisessa järjestyksessä aidosti pienempi kuin $\underline{i}$ ja jolle pätisi sekä $R_{\tilde{\underline{i}}}(\alpha_1, \ldots, \alpha_m) \neq 0$ että $\sum_{h=1}^{m} \frac{\tilde{i}_h}{r_h} \neq \operatorname{ind} R$, niin indeksin määritelmän

[1]Leksikografinen järjestys eli niin sanottu ”sanakirjajärjestys”: $(a_1, \ldots, a_m) \leq (b_1, \ldots, b_m)$, jos ja vain jos on olemassa indeksi k $(m \geq k \geq 1)$ siten, että $a_i = b_i$ kaikilla $i < k$ ja $a_k \leq b_k$.

nojalla olisi oltava $\sum_{h=1}^{m} \frac{\tilde{i}_h}{r_h} > \sum_{h=1}^{m} \frac{i_h}{r_h}$. Muutoin $\underline{\tilde{i}}$ olisi ristiriidassa vektorin i valinnan kanssa. Olkoon $\underline{\tilde{j}}$ siten, että $\underline{k} = \underline{\tilde{i}} + \underline{\tilde{j}}$. Tällöin

$$\sum_{h=1}^{m} \frac{\tilde{j}_h}{r_h} = \sum_{h=1}^{m} \frac{j_h + i_h - \tilde{i}_h}{r_h} = \sum_{h=1}^{m} \frac{j_h}{r_h} + \sum_{h=1}^{m} \frac{i_h}{r_h} - \sum_{h=1}^{m} \frac{\tilde{i}_h}{r_h} < \sum_{h=1}^{m} \frac{j_h}{r_h} = \operatorname{ind} T, \tag{5.10}$$

joten $T_{\underline{\tilde{j}}}(\alpha_1, \ldots, \alpha_m) = 0$ ja $R_{\underline{\tilde{i}}} T_{\underline{\tilde{j}}}(\alpha_1, \ldots, \alpha_m) = 0$.

Vastaavasti, jos olisi $\underline{\tilde{i}}$, joka olisi leksikografisessa järjestyksessä aidosti suurempi kuin $\underline{i}$ ja jolle pätisi $R_{\underline{\tilde{i}}}(\alpha_1, \ldots, \alpha_m) \neq 0$, niin tälle vektorille $\sum_{h=1}^{m} \frac{\tilde{i}_h}{r_h} \geq \operatorname{ind} R$. Olkoon $\underline{\tilde{j}}$ kuten edellä. Tällöin yhtälöstä (5.10) saadaan

$$\sum_{h=1}^{m} \frac{\tilde{j}_h}{r_h} \leq \operatorname{ind} T.$$

Jos $\sum_{h=1}^{m} \frac{\tilde{j}_h}{r_h} < \operatorname{ind} T$, niin $T_{\underline{\tilde{j}}}(\alpha_1, \ldots, \alpha_m) = 0$ ja jos $\sum_{h=1}^{m} \frac{\tilde{j}_h}{r_h} = \operatorname{ind} T$, niin tulee päteä $T_{\underline{\tilde{j}}}(\alpha_1, \ldots, \alpha_m) = 0$, muutoin $\underline{\tilde{j}}$ olisi ristiriidassa vektorin $\underline{j}$ valinnan kanssa, sillä $\underline{\tilde{j}}$ on leksikografisesti pienempi kuin $\underline{j}$.

Nyt vektoreiden $\underline{i}$ ja $\underline{j}$ valinnoista johtuen yhtälö (5.8) saa muodon

$$(R \cdot T)_{\underline{k}}(\alpha_1, \ldots, \alpha_m) = C(\underline{i}, \underline{j}) R_{\underline{i}}(\alpha_1, \ldots, \alpha_m) T_{\underline{j}}(\alpha_1, \ldots, \alpha_m) \neq 0.$$

Siispä

$$\operatorname{ind}(R \cdot T) \leq \sum_{h=1}^{m} \frac{k_h}{r_h} = \sum_{h=1}^{m} \frac{i_h}{r_h} + \sum_{h=1}^{m} \frac{j_h}{r_h} = \operatorname{ind} R + \operatorname{ind} T. \tag{5.11}$$

Väite seuraa nyt epäyhtälöistä (5.9) ja (5.11).

□

4. Polynomin R konstruktio

Polynomin R konstruktio seuraavan lauseen todistuksessa vastaa Liouvillen lauseen todistuksen kohtaa a), jossa luvun α minimaalipolynomi otetaan tutkittavaksi. Lauseen todistamiseksi tarvitaan muutama lemma, jotka todistetaan aluksi.

LEMMA 5.17. *Olkoot $r_1, \ldots, r_m$ positiivisia kokonaislukuja ja $0 < \varepsilon < 1$. Tällöin kokonaislukupisteitä $(i_1, \ldots, i_m)$, joille*

$$0 \leq i_h \leq r_h, \tag{5.12}$$

kun $(1 \leq h \leq m)$ ja

$$\left| \left(\sum_{h=1}^{m} \frac{i_h}{r_h} \right) - \frac{m}{2} \right| \geq \varepsilon m, \tag{5.13}$$

on korkeintaan

$$(r_1 + 1) \cdots (r_m + 1) \cdot 2e^{-\varepsilon^2 \cdot m/4}$$

kappaletta.

TODISTUS. Olkoon M_+ niiden kokonaislukupisteiden lukumäärä, joille pätee ehto (5.12) ja

$$\left(\sum_{h=1}^{m} \frac{i_h}{r_h}\right) - \frac{m}{2} \geq \varepsilon m$$

sekä vastaavasti M_- niiden kokonaislukupisteiden lukumäärä, joille pätee (5.12) ja

$$\left(\sum_{h=1}^{m} \frac{i_h}{r_h}\right) - \frac{m}{2} \leq -\varepsilon m.$$

Lemman todistamiseksi riittää osoittaa, että

$$M_\pm \leq (r_1 + 1) \cdots (r_m + 1) \cdot e^{-\varepsilon^2 \cdot m/4}, \tag{5.14}$$

missä merkinnällä $M_\pm$ tarkoitetaan, että epäyhtälö (5.14) pätee sekä luvulle M_+ että luvulle M_-.

Lukujen M_+ ja M_- määritelmästä seuraa suoraan, että

$$M_\pm = \sum_{\underline{c}} 1, \tag{5.15}$$

missä summassa $\sum_{\underline{c}}$ lasketaan yhteen niiden vektorien $\underline{c} = (c_1, \ldots, c_m)$, $0 \leq c_j \leq r_j$, lukumäärä, joille summa

$$\left(\sum_{h=1}^{m} \frac{c_h}{r_h}\right) - \frac{m}{2}$$

on joko yli εm tai vastaavasti alle $-\varepsilon m$. Olkoon j ja c_j kokonaislukuja siten, että $1 \leq j \leq m$ ja $0 \leq c_j \leq r_j$. Tällöin

$$\begin{aligned} M_\pm \exp\left(\varepsilon^2 m/2\right) &\leq \sum_{c_1=0}^{r_1} \cdots \sum_{c_m=0}^{r_m} \exp\left(\pm\frac{\varepsilon}{2}\left(\left(\sum_{h=1}^{m} \frac{c_h}{r_h}\right) - \frac{m}{2}\right)\right) \\ &= \prod_{j=1}^{m} \left(\sum_{c_j=0}^{r_j} \exp\left(\pm\frac{\varepsilon}{2}\left(\frac{c_j}{r_j} - \frac{1}{2}\right)\right)\right), \end{aligned} \tag{5.16}$$

missä merkintöjen yksinkertaistamiseksi käytetään merkintää $\exp(x) = e^x$.

Huomataan, että kullekin $0 \leq j \leq m$ pätee

$$\sum_{c_j=0}^{r_j} 1 = (r_j + 1) \tag{5.17}$$

Arvioimalla $e^x \leq 1 + x + x^2$, mikä pätee, kun $|x| \leq 1$, saadaan kullekin $0 \leq j \leq m$ arvio

$$\begin{aligned}
\sum_{c_j=0}^{r_j} \exp\left(\pm\frac{\varepsilon}{2}\left(\frac{c_j}{r_j} - \frac{1}{2}\right)\right) &\leq \sum_{c_j=0}^{r_j}\left(1 \pm \frac{\varepsilon}{2}\left(\frac{c_j}{r_j} - \frac{1}{2}\right) + \frac{\varepsilon^2}{4}\left(\frac{c_j}{r_j} - \frac{1}{2}\right)^2\right) \\
&\leq \sum_{c_j=0}^{r_j}\left(1 + \frac{\varepsilon^2}{4}\right) \pm \frac{\varepsilon}{2r_j}\left(\sum_{c_j=0}^{r_j} c_j - \frac{r_j}{2}\sum_{c_j=0}^{r_j} 1\right) \\
&= \sum_{c_j=0}^{r_j}\left(1 + \frac{\varepsilon^2}{4}\right) \pm \frac{\varepsilon}{2r_j}\left(\sum_{c_j=0}^{r_j} c_j - \frac{r_j(r_j+1)}{2}\right) \\
&= (r_j+1)(1+\frac{\varepsilon^2}{4}), \qquad (5.18)
\end{aligned}$$

missä viimeinen yhtäsuuruus seuraa siitä, että luvun $\pm\frac{\varepsilon}{2r_j}$ kerroin on 0, sillä $\sum_{c_j=0}^{r_j} c_j = \frac{r_j(r_j+1)}{2}$. Nyt epäyhtälöistä (5.18) ja (5.16) seuraa

$$M_{\pm}\exp\left(\varepsilon^2 m/2\right) \leq (r_1+1)\cdots(r_m+1)(1+\frac{\varepsilon^2}{4})^m \leq (r_1+1)\cdots(r_m+1)\exp\left(\varepsilon^2 m/4\right),$$

sillä $(1+x)^m \leq e^{xm}$, kun $0 \leq x \leq 1$. Tämä on yhtäpitävää epäyhtälön (5.14) kanssa. Väite on siten todistettu. □

LEMMA 5.18. *Olkoon α algebrallinen kokonaisluku ja*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

sen minimaalipolynomi. Tällöin kaikilla luvuilla $k \geq 0$ on olemassa kokonaisluvut $c_{n-1}(k), \ldots, c_0(k)$ siten, että

$$\alpha^k = c_{n-1}(k)\alpha^{n-1} + \cdots + c_1(k)\alpha + c_0(k)$$

ja

$$|c_i(k)| \leq (\lceil f \rceil + 1)^k$$

kaikilla $1 \leq i \leq n$.

TODISTUS. Tehdään todistus induktiolla luvun k suhteen. Väite pätee selvästi kaikilla luvuilla $k \leq n$. Oletetaan, että väite pätee jollakin luvulla k. Tällöin

$$\begin{aligned}
\alpha^{k+1} &= \alpha^k \cdot \alpha = \left(c_{n-1}(k)\alpha^{n-1} + \cdots + c_0(k)\right)\cdot\alpha \\
&= c_{n-1}(k)\alpha^n + c_{n-2}(k)\alpha^{n-1} + \cdots + c_0(k)\alpha \\
&= c_{n-1}(k)\left(-a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0\right) \\
&\quad + c_{n-2}(k)\alpha^{n-1} + \cdots + c_0(k)\alpha \\
&= -c_{n-1}(k)a_{n-1}\alpha^{n-1} - c_{n-1}(k)a_{n-2}\alpha^{n-2} - \cdots - c_{n-1}(k)a_1\alpha - c_{n-1}(k)a_0 \\
&\quad + c_{n-2}(k)\alpha^{n-1} + \ldots + c_0(k)\alpha \\
&= \left(c_{n-2}(k) - a_{n-1}c_{n-1}(k)\right)\alpha^{n-1} + \cdots + \left(c_0(k) - a_1 c_{n-1}(k)\right)\alpha - a_0 c_{n-1}(k),
\end{aligned}$$

mistä merkintöjä vaihtamalla saadaan

$$\alpha^{k+1} = c_{n-1}(k+1)\alpha^{n-1} + \cdots + c_1(k+1)\alpha + c_0(k+1).$$

Kullekin $1 \leq i \leq n-1$ saadaan arvio

$$|c_i(k+1)| \leq (\lceil f \rceil + 1)^k + \lceil f \rceil (\lceil f \rceil + 1)^k = (\lceil f \rceil + 1)^{k+1}.$$

□

LEMMA 5.19 (Siegelin lemma). *Olkoot $M, N \in \mathbb{N}$ siten, että $N > M$. Olkoot lisäksi*

$$L_j(z_1, \ldots, z_N) = \sum_{k=1}^{N} a_{jk} z_k$$

kokonaislukukertoimisia lineaarikuvauksia, kun $1 \leq j \leq M$, siten, että

$$|a_{jk}| \leq A$$

jollakin luonnollisella luvulla A. Tällöin on olemassa kokonaislukupiste $\underline{z} = (z_1, \ldots, z_N) \neq \underline{0}$ siten, että

$$L_j(\underline{z}) = \underline{0} \tag{5.19}$$

ja

$$|z_j| \leq (NA)^{\frac{M}{N-M}} \tag{5.20}$$

kaikilla $1 \leq j \leq M$.

TODISTUS. Koska $N > M$, on olemassa ei-triviaali rationaalinen ratkaisu $\underline{z}$ yhtälöille (5.19). Koska $\underline{z}$ on ratkaisu, on $\lambda \underline{z}$ myös ratkaisu kaikilla reaaliluvuilla λ. Täten on olemassa joukko kokonaislukupisteitä, jotka kaikki toteuttavat yhtälöt (5.19).

Osoitetaan, että jokin näistä pisteistä toteuttaa epäyhtälön (5.20). Tämän todistamiseksi käytetään Dirichlet'n lauseen todistuksesta tuttua kyyhkyslakkaperiaatetta.

Merkitään $Z := (NA)^{\frac{M}{N-M}}$. Tällöin $Z+1 > (NA)^{\frac{M}{N-M}}$, jolloin $NA < (Z+1)^{\frac{N-M}{M}}$ ja edelleen

$$NAZ + 1 \leq NA(Z+1) < (Z+1)^{\frac{N}{M}}.$$

Kaikille kokonaislukupisteille $\underline{z} = (z_1, \ldots, z_N)$, jotka toteuttavat ehdon

$$0 \leq z_i \leq Z, \tag{5.21}$$

pätee

$$L_j^- Z \leq L_j(\underline{z}) \leq L_j^+ Z,$$

missä L_j^- ja L_j^+ ovat kuvauksen $L_j(\underline{z})$ negatiivisten ja positiivisten kertoimien summa vastaavasti. Nyt $\left|L_j^- + L_j^+\right| \leq NA$, joten kukin kuvapiste $L_j(\underline{z})$ sijaitsee janalla, jonka pituus on korkeintaan NAZ. Kun päätepisteet lasketaan mukaan, kukin $L_j(\underline{z})$ voi saada korkeintaan $NAZ+1$ eri arvoa. Tällöin kuvapisteiden muodostama vektori $(L_1(\underline{z}), \ldots, L_M(\underline{z}))$ voi saada korkeintaan

$$(NAZ+1)^M < (Z+1)^N$$

eri arvoa.

Toisaalta, ehdon (5.21) toteuttavien kokonaislukupisteiden $\underline{z}$ lukumäärä on $(Z+1)^N$. Kyyhkyslakkaperiaatteen nojalla tällöin on oltava ainakin kaksi ehdon (5.21) toteuttavaa kokonaislukupistettä $\underline{z_1} \neq \underline{z_2}$ siten, että

$$L_j(\underline{z_1}) = L_j(\underline{z_2})$$

kaikilla $1 \leq j \leq M$.

Piste $\underline{z} = \underline{z_1} - \underline{z_2}$ toteuttaa lemman väitteen. □

LAUSE 5.20 (Indeksilause). *Olkoon α algebrallinen kokonaisluku ja $d \geq 2$ sen aste. Merkitään $\underline{\alpha} = (\alpha, \alpha, \ldots, \alpha)$. Olkoon lisäksi $\varepsilon > 0$ ja m kokonaisluku siten, että*

$$m > \frac{16}{\varepsilon^2} \log 4d \tag{5.22}$$

ja $\underline{r} = (r_1, \ldots, r_m)$ kokonaislukupiste, jolle $r_h \geq 1$, kun $1 \leq h \leq m$. Tällöin on olemassa kokonaislukukertoiminen polynomi $R(x_1, \ldots, x_m) \not\equiv 0$ siten, että

i) muuttujan x_h aste polynomissa R on korkeintaan r_h,

ii)

$$\operatorname*{ind}_{\underline{\alpha},\underline{r}} R \geq \frac{m}{2}(1-\varepsilon)$$

ja

iii)

$$\lceil R \rceil \leq B^{r_1+\ldots+r_m},$$

missä $B = B(\alpha)$.

TODISTUS. Polynomi, jota etsitään on muotoa

$$R(x_1, \ldots, x_m) = \sum_{j_1=0}^{r_1} \cdots \sum_{j_m=0}^{r_m} C(j_1, \ldots, j_m) x_1^{j_1} \cdots x_m^{j_m},$$

missä luvut $C(j_1, \ldots, j_m)$ ovat kokonaislukuja siten, että ii) ja iii) pätevät. Näiden määriteltävien kertoimien lukumäärä on

$$N = (r_1 + 1) \cdots (r_m + 1). \tag{5.23}$$

Jos

$$R_{i_1,\ldots,i_m}(\alpha, \alpha, \ldots, \alpha) = 0, \tag{5.24}$$

aina, kun

$$\left(\sum_{h=1}^{m} \frac{i_h}{r_h} \right) - \frac{m}{2} < -\frac{m\varepsilon}{2}, \tag{5.25}$$

niin kohta ii) pätee. Lemman 5.17 nojalla tällaisten vektoreiden $\underline{i}$ määrä on korkeintaan $(r_1+1) \cdots (r_m+1) \cdot 2e^{-\varepsilon^2 m/16}$. Oletuksen (5.22) nojalla näiden tapausten määräksi saadaan korkeintaan

$$N \cdot \frac{2}{4d} = \frac{N}{2d}. \tag{5.26}$$

Kukin yhtälön 5.24) toteuttavista tapauksista vastaa lineaariyhtälöä, jossa muuttujina ovat kokonaisluvut $C(j_1, \ldots, j_m)$ ja kertoimina luvun α potenssit kerrottuna jollakin kokonaisluvulla. Koska α on algebrallinen, on se potenssien $\alpha^{d-1}, \ldots, \alpha, 1$ kokonaislukukertoiminen lineaarikombinaatio, sillä $f(\alpha) = 0$. Täten kukin yhtälön (5.24) toteuttavista tapauksista seuraa lineaariyhtälöistä, joiden lukumäärä on d. Kaiken kaikkiaan lukujen $C(j_1, \ldots, j_m)$ määrittelevien kokonaislukukertoimisten yhtälöiden lukumääräksi saadaan

$$M \leq d \cdot \frac{N}{2d} = \frac{N}{2}.$$

Olkoon A suurin näiden kokonaislukukertoimien itseisarvoista. Esityksestä (5.6) saadaan

$$R_{\underline{i}}(\alpha,\dots,\alpha)=\sum_{i_h\le j_h\le r_h}\binom{j_1}{i_1}\cdots\binom{j_m}{i_m}C(j_1,\dots,j_m)\underbrace{\alpha^{j_1-i_1}\cdots\alpha^{j_m-i_m}}_{=\alpha^{j_1-i_1+\cdots+j_m-i_m}}.$$

Tällöin lemman 5.18 nojalla

$$A\le\binom{j_1}{i_1}\cdots\binom{j_m}{i_m}(\lceil f\rceil+1)^k\le 2^{j_1+\cdots+j_m}(\lceil f\rceil+1)^k,$$

missä f on luvun α minimaalipolynomi ja $k=(j_1-i_1)+\cdots+(j_m-i_m)$. Siten

$$A\le(2(\lceil f\rceil+1))^{r_1+\cdots+r_m}.$$

Lemman 5.19 nojalla on olemassa yhtälöryhmän toteuttava ei-triviaali kokonaislukuratkaisu, jolle pätee

$$\begin{aligned}|C(j_1,\dots,j_m)| &\le (NA)^{\frac{M}{N-M}}\le NA\\ &\le 2^{r_1+\cdots+r_m}\,(2(\lceil f\rceil+1))^{r_1+\cdots+r_m}=:B^{r_1+\cdots+r_m}\end{aligned}$$

kaikilla $\underline{j}=(j_1,\dots,j_m)$. Nyt polynomi R, jolla on nämä kertoimet $C(j_1,\dots,j_m)$, toteuttaa epäyhtälön

$$\lceil R\rceil\le B^{r_1+\cdots+r_m},$$

missä $B=B(\alpha)=4(\lceil f\rceil+1)$ ja siten kohtien i) - iii) ehdot täyttyvät. □

5. Polynomin R käyttäytyminen rationaalipisteissä

Seuraava lause vastaa vuorostaan Liouvillen lauseen todistuksen osaa b), jossa tutkitaan polynomin käyttäytymistä rationaalipisteissä lähellä lukua α.

LAUSE 5.21. *Olkoot α, d, m ja $\underline{r}=(r_1,\dots,r_m)$ kuten lauseen 5.20 oletuksissa. Merkitään $\underline{\alpha}=(\alpha,\dots,\alpha)$.*

Olkoon lisäksi $0<\delta<1$ ja

$$0<\varepsilon<\frac{\delta}{36}\tag{5.27}$$

sekä $\underline{p}=(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m})$, missä $\frac{p_h}{q_h}$ on luvun α rationaalilukuapproksimaatio siten, että kaikilla $1\le h\le m$ pätee

$$\left|\alpha-\frac{p_h}{q_h}\right|<\frac{1}{q_h^{2+\delta}}\tag{5.28}$$

ja siten, että

$$q_h^{\delta}>D\tag{5.29}$$

jollakin $D=D(\alpha)>0$. Oletetaan lisäksi, että

$$r_1\log q_1\le r_h\log q_h\le(1+\varepsilon)r_1\log q_1,\tag{5.30}$$

kun $1\le h\le m$. Oletetaan nyt, että R on lauseen 5.20 antama polynomi.

Tällöin

$$\operatorname*{ind}_{\underline{p},\underline{r}}R\ge\varepsilon m.$$

TODISTUS. Olkoon $j_1, \ldots, j_m$ ei-negatiivisia kokonaislukuja siten, että

$$\sum_{h=1}^{m} \frac{j_h}{r_h} < \varepsilon m.$$

Merkitään $T(x_1, \ldots, x_m) = R_{\underline{j}}(x_1, \ldots, x_m)$, missä $\underline{j} = (j_1, \ldots, j_m)$. Tällöin tulee osoittaa, että $T\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right) = 0$.

Indeksilauseen nojalla pätee

$$\lceil R \rceil \leq B^{r_1+\cdots+r_m},$$

jolloin lemman 5.10 kohdan iii) nojalla

$$\lceil T \rceil \leq (2B)^{r_1+\cdots+r_m}.$$

Soveltamalla samaa tulosta edelleen saadaan

$$\lceil T_{\underline{i}} \rceil \leq (4B)^{r_1+\cdots+r_m}$$

kaikille vektoreille $\underline{i} = (i_1, \ldots, i_m)$, missä $i_h \geq 0$, kun $1 \leq h \leq m$. Täten kunkin monomin itseisarvo polynomissa $T_{\underline{i}}(\underline{\alpha})$ on korkeintaan

$$(4B)^{r_1+\cdots+r_m} \left(\max(1, |\alpha|)\right)^{r_1+\cdots+r_m}.$$

Koska monomien lukumäärä polynomissa $T_{\underline{i}}(\underline{\alpha})$ on korkeintaan

$$(r_1 + 1) \cdots (r_m + 1) \leq 2^{r_1+\cdots+r_m},$$

saadaan

$$|T_{\underline{i}}(\underline{\alpha})| \leq (8B \max(1, |\alpha|))^{r_1+\cdots+r_m} =: C^{r_1+\cdots+r_m}, \tag{5.31}$$

missä $C = C(\alpha)$.

Indeksilauseen nojalla

$$\operatorname*{ind}_{\underline{\alpha},\underline{r}} R \geq \frac{m}{2}(1 - \varepsilon). \tag{5.32}$$

Lemman 5.16 kohdasta i) seuraa

$$\operatorname*{ind}_{\underline{\alpha},\underline{r}} T \geq \frac{m}{2}(1 - \varepsilon) - \sum_{h=1}^{m} \frac{j_h}{r_h} > \frac{m}{2}(1 - 3\varepsilon). \tag{5.33}$$

Taylorin lauseen nojalla

$$T\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right) = \sum_{i_1=0}^{r_1} \cdots \sum_{i_m=0}^{r_m} T_{i_1,\cdots,i_m}(\underline{\alpha}) \cdot \left(\frac{p_1}{q_1} - \alpha\right)^{i_1} \ldots \left(\frac{p_m}{q_m} - \alpha\right)^{i_m}.$$

Epäyhtälön (5.33) nojalla summattavat katoavat paitsi, jos $\sum_{h=1}^{m} \frac{i_h}{r_h} > \frac{m}{2}(1 - 3\varepsilon)$. Oletuksen (5.28) ja epäyhtälön (5.31) nojalla saadaan

$$\left| T\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right) \right| \leq \sum_{\underline{i}} C^{r_1+\cdots+r_m} \frac{1}{\left(q_1^{i_1} q_2^{i_2} \cdots q_m^{i_m}\right)^{2+\delta}}, \tag{5.34}$$

missä $\sum_{\underline{i}}$ tarkoittaa summaa yli kaikkien niiden vektoreiden $\underline{i}$, joille $\sum_{h=1}^{m} \frac{i_h}{r_h} > m(\frac{1}{2} - 2\varepsilon)$ ja $0 \leq i_h \leq r_h$, kun $1 \leq h \leq m$. Näille vektoreille pätee oletusten (5.30) ja (5.27) nojalla

$$\begin{aligned} q_1^{i_1} q_2^{i_2} \cdots q_m^{i_m} &= q_1^{r_1 \frac{i_1}{r_1}} q_2^{r_2 \frac{i_2}{r_2}} \cdots q_m^{r_m \frac{i_m}{r_m}} \geq q_1^{r_1\left(\frac{i_1}{r_1} + \cdots + \frac{i_m}{r_m}\right)} \\ &> q_1^{r_1 m(\frac{1}{2} - 2\varepsilon)} \geq (q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m})^{(\frac{1}{2} - 2\varepsilon)/(1+\varepsilon)} \\ &> (q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m})^{\frac{1}{2}(1-6\varepsilon)}. \end{aligned}$$

Koska summattavien määrä epäyhtälön (5.34) summassa on korkeintaan $2^{r_1+\cdots+r_m}$, seuraa

$$\begin{aligned} \left| T\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right) \right| &\leq 2^{r_1+\cdots+r_m} C^{r_1+\cdots+r_m} \cdot \prod_{h=1}^{m} q_h^{i_h \cdot (-2-\delta)} \\ &\leq 2^{r_1+\cdots+r_m} C^{r_1+\cdots+r_m} \cdot \prod_{h=1}^{m} q_h^{r_h \cdot \left(-\frac{1}{2}(1-6\varepsilon)(2+\delta)\right)} \\ &\leq \prod_{h=1}^{m} \left(2C \cdot q_h^{-\frac{1}{2}(1-6\varepsilon)(2+\delta)}\right)^{r_h}. \end{aligned}$$

Nyt oletuksen (5.27) nojalla

$$\frac{1}{2}(1-6\varepsilon)(2+\delta) > 1 + \frac{\delta}{4},$$

joten

$$2C \cdot q_h^{-\frac{1}{2}(1-6\varepsilon)(2+\delta)} < 2C \cdot q_h^{-1-\frac{\delta}{4}} < q_h^{-1},$$

jos $q_h^{\delta} > (2C)^4$. Tämä pätee, kun valitaan $D = (2C)^4$, joka riippuu vain luvusta α, sillä luku $C = C(B) = C(B(\alpha))$ riippuu vain siitä. Tästä seuraa

$$\left| T\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right) \right| < \frac{1}{q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m}}.$$

Koska muuttujan x_h aste polynomissa T, on lemman 5.10 kohdan ii) nojalla korkeintaan r_h, kaikilla $1 \leq h \leq m$ ja koska T on lemman 5.10 kohdan i) nojalla kokonaislukukertoiminen, pätee

$$\left| T\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right) \right| = \frac{N}{q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m}}$$

jollakin kokonaisluvulla N. Edellisen epäyhtälön nojalla on oltava $N = 0$, joten

$$\left| T\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right) \right| = 0.$$

Tämä päättää lauseen todistuksen. □

6. Rothin lemma

Kohdan c) tulos Liouvillen lauseen todistuksessa seurasi helposti yksinkertaisesta arviosta. Rothin lauseen tapauksessa vastaavan arvion tuottaminen on kuitenkin todistuksen vaikein kohta. Arvion tuottamiseksi tarvitaankin kahta aputulosta, joista toinen todistetaan aluksi ja toinen itse Rothin lemman todistuksen yhteydessä.

Olkoot jatkossa $\varphi_1, \ldots, \varphi_k$ reaalikertoimisia *rationaalifunktioita*, joissa on m muuttujaa. Toisin sanoen funktio φ_j voidaan esittää muodossa

$$\varphi_j(x_1, \ldots, x_m) = \frac{P_j(x_1, \ldots, x_m)}{Q_j(x_1, \ldots, x_m)},$$

missä P_j ja Q_j ovat polynomeja kaikilla $1 \leq j \leq k$.

Edelleen, jatkossa käsitellään differentiaalioperaattoreita, joista käytetään merkintää

$$\Delta = \frac{\partial^{i_1+\cdots+i_m}}{\partial x_1^{i_1} \cdots \partial x_m^{i_m}}.$$

Sanotaan, että tällaisen operaattorin *aste* on $i_1 + \cdots + i_m$.

MÄÄRITELMÄ 5.22 (Yleistetty Wronskin determinantti). Funktioiden $\varphi_1, \ldots, \varphi_k$ *yleistetyksi Wronskin determinantiksi* kutsutaan mitä tahansa determinanttia, joka on muotoa

$$\det(\Delta_i \varphi_j) = \begin{vmatrix} \Delta_1\varphi_1 & \Delta_1\varphi_2 & \cdots & \Delta_1\varphi_k \\ \Delta_2\varphi_1 & \Delta_2\varphi_2 & \cdots & \Delta_2\varphi_k \\ \vdots & \vdots & & \vdots \\ \Delta_k\varphi_1 & \Delta_k\varphi_2 & \cdots & \Delta_k\varphi_k \end{vmatrix}, \tag{5.35}$$

missä operaattorin Δ_i aste on korkeintaan $i-1$ kaikilla $1 \leq i \leq k$.

HUOMAUTUS 5.23. Koska differentiaalioperaattorin Δ_1 aste on korkeintaan $1-1 = 0$, niin determinantti (5.35) voidaan kirjoittaa muodossa

$$\begin{vmatrix} \varphi_1 & \varphi_2 & \cdots & \varphi_k \\ \Delta_2\varphi_1 & \Delta_2\varphi_2 & \cdots & \Delta_2\varphi_k \\ \vdots & \vdots & & \vdots \\ \Delta_k\varphi_1 & \Delta_k\varphi_2 & \cdots & \Delta_k\varphi_k \end{vmatrix}. \tag{5.36}$$

ESIMERKKI 5.24. (1) Olkoot φ_1 ja φ_2 rationaalifunktioita, joissa on m muuttujaa ja olkoot $1 \leq i \leq m$. Merkitään

$$W = \begin{vmatrix} \varphi_1 & \varphi_2 \\ \frac{\partial}{\partial x_i}\varphi_1 & \frac{\partial}{\partial x_i}\varphi_2 \end{vmatrix} = \varphi_1 \frac{\partial}{\partial x_i}\varphi_2 - \varphi_2 \frac{\partial}{\partial x_i}\varphi_1.$$

Olkoon f myös rationaalifunktio. Tällöin

$$\begin{aligned} \begin{vmatrix} f\varphi_1 & f\varphi_2 \\ \frac{\partial}{\partial x_i}(f\varphi_1) & \frac{\partial}{\partial x_i}(f\varphi_2) \end{vmatrix} &= f\varphi_1 \tfrac{\partial}{\partial x_i}(f\varphi_2) - f\varphi_2 \tfrac{\partial}{\partial x_i}(f\varphi_1) \\ &= f\varphi_1(\tfrac{\partial}{\partial x_i} f\varphi_2 + f\tfrac{\partial}{\partial x_i}\varphi_2) - f\varphi_2(\tfrac{\partial}{\partial x_i} f\varphi_1 + f\tfrac{\partial}{\partial x_i}\varphi_1) \\ &= f\varphi_1 \tfrac{\partial}{\partial x_i} f\varphi_2 + f\varphi_1 f\tfrac{\partial}{\partial x_i}\varphi_2 - f\varphi_2 \tfrac{\partial}{\partial x_i} f\varphi_1 - f\varphi_2 f\tfrac{\partial}{\partial x_i}\varphi_1 \\ &= f\varphi_1 f\tfrac{\partial}{\partial x_i}\varphi_2 - f\varphi_2 f\tfrac{\partial}{\partial x_i}\varphi_1 \\ &= f^2 W. \end{aligned}$$

(2) Kehittämällä determinantti kolmannen rivin suhteen ja käyttämällä hyväksi edellistä tulosta rationaalifunktioille $\varphi_1, \varphi_2, \varphi_3$ ja f, joissa on m muuttujaa, saadaan

$$\begin{vmatrix} f\varphi_1 & f\varphi_2 & f\varphi_3 \\ \frac{\partial}{\partial x_i}(f\varphi_1) & \frac{\partial}{\partial x_i}(f\varphi_2) & \frac{\partial}{\partial x_i}(f\varphi_3) \\ \frac{\partial}{\partial x_j \partial x_k}(f\varphi_1) & \frac{\partial}{\partial x_j \partial x_k}(f\varphi_2) & \frac{\partial}{\partial x_j \partial x_k}(f\varphi_3) \end{vmatrix} = f^3 \begin{vmatrix} \varphi_1 & \varphi_2 & \varphi_3 \\ \frac{\partial}{\partial x_i}\varphi_1 & \frac{\partial}{\partial x_i}\varphi_2 & \frac{\partial}{\partial x_i}\varphi_3 \\ \frac{\partial}{\partial x_j \partial x_k}\varphi_1 & \frac{\partial}{\partial x_j \partial x_k}\varphi_2 & \frac{\partial}{\partial x_j \partial x_k}\varphi_3 \end{vmatrix}$$
$$+ f^2 \tfrac{\partial}{\partial x_j} f \begin{vmatrix} \varphi_1 & \varphi_2 & \varphi_3 \\ \frac{\partial}{\partial x_i}\varphi_1 & \frac{\partial}{\partial x_i}\varphi_2 & \frac{\partial}{\partial x_i}\varphi_3 \\ \frac{\partial}{\partial x_k}\varphi_1 & \frac{\partial}{\partial x_k}\varphi_2 & \frac{\partial}{\partial x_k}\varphi_3 \end{vmatrix}$$
$$+ f^2 \tfrac{\partial}{\partial x_k} f \begin{vmatrix} \varphi_1 & \varphi_2 & \varphi_3 \\ \frac{\partial}{\partial x_i}\varphi_1 & \frac{\partial}{\partial x_i}\varphi_2 & \frac{\partial}{\partial x_i}\varphi_3 \\ \frac{\partial}{\partial x_j}\varphi_1 & \frac{\partial}{\partial x_j}\varphi_2 & \frac{\partial}{\partial x_j}\varphi_3 \end{vmatrix},$$

kun $1 \leq i, j, k \leq m$ ja kun luvut i, j ja k ovat keskenään erisuuria.

LEMMA 5.25. *Olkoot $\varphi_1, \ldots, \varphi_k$ reaalikertoimisia rationaalifunktioita, joissa on m muuttujaa ja jotka ovat lineaarisesti riippumattomia. Tällöin ainakin yksi funktioiden $\varphi_1, \ldots, \varphi_k$ yleistetyistä Wronskin determinanteista ei ole identtisesti nolla.*

HUOMAUTUS 5.26. Lemman 5.25 käänteinen tulos on myös tosi: Jos $\varphi_1, \ldots, \varphi_k$ ovat lineaarisesti riippuvia, niin kaikille funktioiden $\varphi_1, \ldots, \varphi_k$ yleistetyille Wronskin determinanteille W pätee $W = 0$. Todistus seuraa suoraan lineaarisesta riippuvuudesta.

LEMMAN 5.25 TODISTUS. Tehdään todistus induktiolla luvun k suhteen:

(1) $k = 1$: Kun $k = 1$ determinantti (5.36) saa muodon $|\varphi_1| = \varphi_1$. Koska oletuksen nojalla φ_1 on lineaarisesti riippumaton, ei se voi olla identtisesti nolla.

(2) Oletetaan, että väite pätee, kun $k = n - 1$, jollakin $n \geq 2$.

(3) Todistetaan tapaus $k = n$: Olkoot $\varphi_1, \ldots, \varphi_n$ lineaarisesti riippumattomia rationaalifunktioita, jotka täyttävät väitteen oletukset. Olkoon $f(x_1, \ldots, x_m)$ mielivaltainen reaalikertoiminen rationaalifunktio siten, että $f \not\equiv 0$. Olkoot kaikilla $1 \leq i \leq n$ funktiot

$$\hat{\varphi}_i = f\varphi_i.$$

Tällöin rationaalifunktiot $\hat{\varphi}_1, \ldots, \hat{\varphi}_n$ ovat edelleen lineaarisesti riippumattomia. Kaikki funktioiden $\hat{\varphi}_1, \ldots, \hat{\varphi}_n$ yleistetyt Wronskin determinantit ovat funktioiden $\varphi_1, \ldots, \varphi_n$ yleistettyjen Wronskin determinanttien lineaarikombinaatioita, joissa painokertoimet ovat rationaalifunktioita, joissa esintyy funktio f ja sen osittaisderivaattoja.

Lemman todistamiseksi riittää siis osoittaa, että jokin funktioiden $\hat{\varphi}_1, \ldots, \hat{\varphi}_n$ Wronskin determinanteista ei katoa identtisesti. Valitaan $f = \frac{1}{\varphi_1}$, jolloin $\hat{\varphi}_1 = 1, \hat{\varphi}_2 = \frac{\varphi_2}{\varphi_1}, \ldots, \hat{\varphi}_n = \frac{\varphi_n}{\varphi_1}$. Tämän nojalla voidaan olettaa, että annetuista funktioista $\varphi_1, \ldots, \varphi_n$ funktiolle φ_1 pätee $\varphi_1 \equiv 1$.

Rationaalifunktioiden $\varphi_1, \ldots, \varphi_n$ joukko muodostaa n-ulotteisen vektoriavaruuden V kannan. Koska $n > 1$ ja koska $\varphi_1 \equiv 1$ ja φ_2 ovat lineaarisesti riippumattomia, φ_2 ei ole vakio, siispä $\frac{\partial \varphi_2}{\partial x_j} \not\equiv 0$ jollakin j. Edelleen ilman yleisyyden menetystä voidaan valita $j = 1$, jolloin siis $\frac{\partial \varphi_2}{\partial x_1} \not\equiv 0$.

Olkoon

$$W = \left\{ v \in V : v = \sum_{j=1}^{n} c_j \varphi_j, \frac{\partial}{\partial x_1} v \equiv 0, c_j \in \mathbb{R}, \text{ kaikilla } 1 \leq j \leq n \right\}.$$

Huomataan, että W on vektoriavaruuden V alivektoriavaruus. Erityisesti $W \neq \{0\}$, sillä $\varphi_1 \in W$. Lisäksi $W \neq V$, sillä $\varphi_2 \notin W$. Merkitään $t = \dim W$, jolloin $1 \leq t \leq n-1$.

Valitaan funktiot $\Psi_1, \ldots, \Psi_n$ siten, että funktiot $\Psi_1, \ldots, \Psi_t$ ovat avaruuden W kanta ja funktiot $\Psi_1, \ldots, \Psi_n$ ovat avaruuden V kanta. Induktio-oletuksen nojalla on olemassa differentiaalioperaattorit $\Delta'_1, \ldots, \Delta'_t$ siten, että operaattorin Δ'_i aste on korkeintaan $i-1$ kaikilla $1 \leq i \leq t$ ja

$$W_1 := \det(\Delta'_i \Psi_j) \not\equiv 0. \tag{5.37}$$

Olkoot $c_{t+1}, \ldots, c_n$ reaalilukuja siten, että $c_h \neq 0$ jollakin $t+1 \leq h \leq n$. Tällöin

$$(c_{t+1}\Psi_{t+1} + \cdots + c_k \Psi_n) \not\equiv 0,$$

sillä funktiot $\Psi_{t+1}, \ldots, \Psi_n$ ovat lineaarisesti riippumattomia. Koska funktiot $\Psi_1, \ldots, \Psi_t$ virittävät avaruuden W, olisi yhtälö

$$\frac{\partial}{\partial x_1}(c_{t+1}\Psi_{t+1} + \cdots + c_k \Psi_n) \equiv 0$$

ristiriidassa avaruuden V kannan valinnan kanssa. Erityisesti rationaalifunktiot

$$\frac{\partial}{\partial x_1}\Psi_{t+1}, \ldots, \frac{\partial}{\partial x_1}\Psi_n$$

ovat lineaarisesti riippumattomia. Edelleen induktio-oletuksen nojalla on olemassa differentiaalioperaattorit $\Delta'_{t+1}, \ldots, \Delta'_n$ siten, että operaattorin Δ'_i aste on korkeintaan $i-1-t$ kaikilla $t+1 \leq i \leq n$ ja

$$W_2 := \det\left(\Delta'_i \frac{\partial}{\partial x_1}\Psi_j\right) \not\equiv 0. \tag{5.38}$$

Määritellään nyt differentiaalioperaattorit Δ_i kaikille $1 \leq i \leq n$ seuraavasti:

$$\Delta_i = \begin{cases} \Delta'_i & , \text{kun } 1 \leq i \leq t \\ \Delta'_i \dfrac{\partial}{\partial x_1} & , \text{kun } t+1 \leq i \leq n. \end{cases}$$

Tällöin kunkin differentiaalioperaattorin Δ_i aste on korkeintaan $i-1$ ja kohdista (5.37) ja (5.38) seuraa

$$\begin{aligned} \det(\Delta_i \Psi_j) &= \det \begin{pmatrix} \Delta'_1\Psi_1 & \cdots & \Delta'_1\Psi_t & \Delta'_1\Psi_{t+1} & \cdots & \Delta'_1\Psi_n \\ \vdots & & \vdots & \vdots & & \vdots \\ \Delta'_t\Psi_1 & \cdots & \Delta'_t\Psi_t & \Delta'_t\Psi_{t+1} & \cdots & \Delta'_t\Psi_n \\ 0 & \cdots & 0 & \Delta'_{t+1}\frac{\partial}{\partial x_1}\Psi_{t+1} & \cdots & \Delta'_{t+1}\frac{\partial}{\partial x_1}\Psi_n \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \Delta'_n\frac{\partial}{\partial x_1}\Psi_{t+1} & \cdots & \Delta'_n\frac{\partial}{\partial x_1}\Psi_n \end{pmatrix} \\ &= W_1 W_2 \not\equiv 0, \end{aligned}$$

missä matriisiin muodostuva nolla-alimatriisi seuraa differentiaalioperaattoreiden Δ_i ja joukon W määrittelystä.

Koska funktiot $\Psi_1, \ldots, \Psi_n$ ovat funktioiden $\varphi_1, \ldots, \varphi_n$ virittämän vektoriavaruuden kanta, diffrentiaalioperaattoreiden lineaarisuuden nojalla pätee

$$\det(\Delta_i \varphi_j) \not\equiv 0.$$

Induktioaskel on nyt otettu ja väite seuraa induktioperiaatteesta. □

LAUSE 5.27 (Rothin lemma, 1955). *Olkoon m positiivinen kokonaisluku ja olkoon*

$$0 \leq \varepsilon \leq \frac{1}{12}. \tag{5.39}$$

Merkitään

$$\omega = \omega(m, \varepsilon) = 24 \cdot 2^{-m} \left(\frac{\varepsilon}{12}\right)^{2^{m-1}}. \tag{5.40}$$

Olkoon $\underline{r} = (r_1, \ldots, r_m)$, missä $r_h \geq 1$, kun $0 \leq h \leq m$ ja

$$\omega r_h \geq r_{h+1}, \tag{5.41}$$

kun $1 \leq h < m$. Edelleen, olkoon $\underline{p} = (\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m})$ siten, että p_h ja q_h ovat keskenään jaottomia, $q_h > 0$ ja lisäksi

$$q_h^{r_h} \geq q_1^{r_1}, \tag{5.42}$$

sekä

$$q_h^{\omega} \geq 2^{3m}, \tag{5.43}$$

kun $0 \leq h \leq m$. Oletetaan nyt, että $R(x_1, \ldots, x_m) \not\equiv 0$ on kokonaislukukertoiminen polynomi, jossa muuttujan x_h aste on korkeintaan r_h ja jolle pätee

$$\lceil R \rceil \leq q_1^{\omega r_1}. \tag{5.44}$$

Tällöin

$$\operatorname*{ind}_{\underline{p},\underline{r}} R \leq \varepsilon.$$

TODISTUS. Tehdään todistus induktiolla luvun m suhteen:

(1) $m = 1$: Voidaan olettaa, että pätee $R(\frac{p_1}{q_1}) = 0$, sillä muutoin $\operatorname{ind}_{\underline{p},\underline{r}} R = 0$ ja väite pätee. Tällöin $R(x)$ voidaan esittää muodossa

$$R(x) = \left(x - \frac{p_1}{q_1}\right)^l M(x),$$

missä l on juuren $\frac{p_1}{q_1}$ kertaluku ja $M(x)$ rationaalilukukertoiminen polynomi siten, että $M\left(\frac{p_1}{q_1}\right) \neq 0$. Näin ollen

$$R(x) = (q_1 x - p_1)^l Q(x), \tag{5.45}$$

missä $Q(x) = q_1^{-l} M(x)$. Gaussin lemman nojalla $Q(x)$ on kokonaislukukertoiminen polynomi.

Yhtälön (5.45) nojalla polynomin $R(x)$ korkeimman potenssin kerroin on jaollinen luvulla q_1^l. Tällöin oletusten (5.44), (5.40) ja $m = 1$ nojalla

$$\begin{aligned} q_1^l \leq \lceil R \rceil &\leq q_1^{\omega r_1} \\ &= q_1^{24 \cdot 2^{-m} \left(\frac{\varepsilon}{12}\right)^{2^{m-1}} \cdot r_1} \\ &= q_1^{\varepsilon r_1}, \end{aligned}$$

joten $\frac{l}{r_1} \leq \varepsilon$, sillä oletuksen (5.43) nojalla $q_1 > 1$. Nyt l on pienin luku, jolla $f^{(l)}(\frac{p_1}{q_1}) \neq 0$, joten

$$\operatorname*{ind}_{\underline{p},\underline{r}} R = \frac{l}{r_1} \leq \varepsilon.$$

Väite siis pätee, kun $m = 1$.

(2) Oletetaan, että väite pätee jollakin luvulla $m-1$, kun $m > 2$.

(3) Todistetaan, että väite pätee luvulla m: Olkoot $\varphi_1, \ldots, \varphi_k$ ja $\Psi_1, \ldots, \Psi_k$ rationaalilukukertoimisia polynomeja siten, että

$$R(x_1, \ldots, x_m) = \sum_{j=1}^{k} \varphi_j(x_1, \ldots, x_{m-1})\Psi_j(x_m). \tag{5.46}$$

Valitaan funktiot $\varphi_1, \ldots, \varphi_k$ ja $\Psi_1, \ldots, \Psi_k$ niin, että luku k on pienin mahdollinen esityksessä (5.46). Tällöin $k \leq r_m + 1$, sillä luvulle $k = r_m + 1$ tällainen esitys on olemassa.

Koska esitys (5.46) on valittu niin, että k on pienin mahdollinen, ovat funktiot $\varphi_1, \ldots, \varphi_k$ lineaarisesti riippumattomia. Muutoin olisi olemassa reaaliluvut $c_1, \ldots, c_k$ siten, että ainakin jokin niistä on erisuuri kuin 0 ja

$$c_1\varphi_1 + \ldots + c_k\varphi_k \equiv 0.$$

Koska $\varphi_1, \ldots, \varphi_k$ ovat rationaalilukukertoimisia, voitaisiin luvut $c_1, \ldots, c_k$ valita rationaaliluvuiksi. Tällöin olettaen esimerkiksi, että $c_k \neq 0$, pätisi

$$R(x_1, \ldots, x_m) = \sum_{j=1}^{k-1} \varphi_j\Psi_j + \underbrace{\left(-\frac{\Psi_k}{c_k}\sum_{j=1}^{k-1} c_j\varphi_j\right)}_{=\varphi_k\Psi_k} = \sum_{j=1}^{k-1} \varphi_j \left(\Psi_j - \frac{c_j}{c_k}\Psi_k\right).$$

Tämä olisi kuitenkin ristiriita luvun k valinnan kanssa. Vastaavasti voidaan osoittaa, että funktiot $\Psi_1, \ldots, \Psi_m$ ovat lineaarisesti riippumattomia.

Merkitään

$$U(x_m) = \det\left(\frac{1}{(i-1)!}\frac{\partial^{i-1}}{\partial x_m^{i-1}}\Psi_j(x_m)\right),$$

kun $1 \leq i, j \leq k$. Lemman 5.25 ja huomautuksen 5.26 nojalla pätee

$$U(x_m) \not\equiv 0.$$

Edelleen lemman 5.25 nojalla on olemassa differentiaalioperaattorit $\Delta_1, \ldots, \Delta'_k$,

$$\Delta'_i = \frac{1}{i_1! \cdots i_{m-1}!}\frac{\partial^{i_1+\cdots+i_{m-1}}}{\partial x_1^{i_1} \cdots \partial x_{m-1}^{i_{m-1}}}$$

siten, että operaattorin Δ_i aste on korkeintaan

$$i_1 + \cdots + 1_{m-1} \leq i - 1 \leq k - 1 \leq r_m \tag{5.47}$$

kaikilla $1 \leq i \leq k$ ja

$$V(x_1, \ldots, x_{m-1}) := \det_{1 \leq i,j \leq k}(\Delta'_i\varphi_j) \not\equiv 0.$$

Asetetaan

$$W(x_1, \ldots, x_m) := \det_{1 \leq i,j \leq k}\left(\frac{1}{(j-1)!}\frac{\partial^{j-1}}{\partial x_m^{j-1}}\Delta'_i R\right).$$

Tällöin

$$\begin{aligned} W(x_1,\ldots,x_m) &= \det\left(\sum_{r=1}^{k}(\Delta_i'\varphi_r)\left(\frac{1}{(j-1)!}\frac{\partial^{j-1}}{\partial x_m^{j-1}}\Psi_r\right)\right) \\ &= V(x_1,\ldots,x_{m-1})U(x_m) \\ &\not\equiv 0. \end{aligned} \tag{5.48}$$

Determinantin W määrittelevän matriisin alkiot ovat polynomeja $R_{i_1,\ldots,i_{m-1},i_{j-1}}$ (määritelmä 5.9), joten lemman 5.10 kohdan i) nojalla ne ovat kokonaislukukertoimisia. Näin ollen W on kokonaislukukertoiminen polynomi. Todistuksen loppuun viemiseksi tarvitaan arvio funktion W indeksille.

LEMMA 5.28. *Olkoon* $I = \operatorname{ind}_{\underline{p},\underline{r}} W$. *Tällöin*

$$I \leq \frac{k\varepsilon^2}{6}.$$

Lemman 5.28 todistus: Polynomeilla U ja V ei välttämättä ole kokonaislukukertoimia, mutta koska W on kokonaislukukertoiminen, Gaussin lemman seurauksen [**3**, s. 162] nojalla on olemassa kokonaisluku t siten, että polynomit $V' := tV$ ja $U' := t^{-1}U$ ovat kokonaislukukertoimisia. Näille funktioille pätee

$$W(x_1,\ldots,x_m) = V'(x_1,\ldots,x_{m-1})U'(x_m).$$

Huomataan, että lemman 5.10 ja oletuksen (5.44) nojalla

$$\begin{aligned} \lceil R_{i_1,\ldots,i_{m-1},i_{j-1}} \rceil &\leq 2^{r_1+\cdots+r_m}\lceil R \rceil \\ &\leq 2^{r_1+\cdots+r_m} q_1^{\omega r_1}. \end{aligned}$$

Lisäksi termien määrä polynomissa $R_{i_1,\ldots,i_{m-1},i_{j-1}}$ on korkeintaan $2^{r_+\cdots+r_m}$ ja termien määrä summassa (5.48) on $k! \leq k^{k-1} \leq k^{r_m} \leq 2^{kr_m}$. Tällöin

$$\lceil W \rceil \leq 2^{kr_m}\left(2^{r_1+\cdots+r_m}2^{r_1+\cdots+r_m}q_1^{\omega r_1}\right)^k \leq \left(2^{3mr_1}q_1^{\omega r_1}\right)^k,$$

sillä $r_1 \geq r_2 \geq \cdots \geq r_m$ oletusten (5.40) ja (5.41) nojalla. Oletuksesta (5.43) seuraa silloin

$$\lceil W \rceil \leq \left(q_1^{2\omega r_1}\right)^k = q_1^{2\omega r_1 k}.$$

Näin saadaan arviot

$$\lceil U' \rceil \leq q_1^{2\omega r_1 k} \leq q_m^{2\omega r_m k} \quad \text{ja} \quad \lceil V' \rceil \leq q_1^{2\omega r_1 k} \tag{5.49}$$

Sovelletaan nyt induktio-oletusta funktioon V' sekä lukuihin $kr_1,\ldots,kr_{m-1}$ ja $\frac{\varepsilon^2}{12}$. Tällöin $\omega(m-1,\frac{\varepsilon^2}{12}) = 2\omega(m,\varepsilon)$. Nyt kohdat (5.41) ja (5.43) pätevät oletuksen nojalla luvulla $\omega(m,\varepsilon)$ ja edellisen huomion nojalla myös luvulla $\omega(m-1,\frac{\varepsilon^2}{12})$. Myös kohdat (5.39) ja (5.42) pätevät luvulla $\frac{\varepsilon^2}{12}$. Arvion (5.49) nojalla myös kohta (5.44) pätee, sillä

$$\lceil V' \rceil \leq q_1^{\omega\left(m-1,\frac{\varepsilon^2}{12}\right)(kr_1)}.$$

Olkoot $\underline{p'} = (\frac{p_1}{q_1},\ldots,\frac{p_{m-1}}{q_{m-1}})$ ja $k\underline{r'} = (kr_1,\ldots,kr_{m-1})$. Induktio-oletuksen nojalla

$$\operatorname*{ind}_{\underline{p'},k\underline{r'}} V' \leq \frac{\varepsilon^2}{12},$$

joten

$$\operatorname*{ind}_{\underline{p'},\underline{r'}} V' \leq \frac{k\varepsilon^2}{12}.$$

Laajentamalla polynomin V' määrittelyjoukkoa voidaan se mieltää polynomiksi $V' = V'(x_1, \ldots, x_m)$. Tällöin muuttuja x_m ei vaikuta kuvaukseen ja edelleen

$$\operatorname*{ind}_{\underline{p},\underline{r}} V' \leq \frac{k\varepsilon^2}{12}.$$

Sovelletaan nyt alkuaskeleessa todistettua tapauksen $m = 1$ tulosta funktioon $U'(x_m)$ sekä lukuihin kr_m ja $\frac{\varepsilon^2}{12}$. Oletuksien päteminen on helppo todeta, jolloin kuten edellä saadaan

$$\operatorname*{ind}_{\underline{p},\underline{r}} U' \leq \frac{k\varepsilon^2}{12}.$$

Koska $W = U'V'$, niin lemman 5.16 kohdan iii) nojalla

$$I = \operatorname*{ind}_{\underline{p},\underline{r}} W \leq \frac{k\varepsilon^2}{12} + \frac{k\varepsilon^2}{12} = \frac{k\varepsilon^2}{6}.$$

Tämä päättää lemman 5.28 todistuksen.

Lemman 5.27 todistuksen päätös: Olkoon $J = \operatorname{ind}_{\underline{p},\underline{r}} R$. Tällöin

$$\begin{aligned}
\operatorname{ind} R_{i_1,\ldots,i_{m-1},j-1} \geq\ & J - \tfrac{i_1}{r_1} - \cdots - \tfrac{i_{m-1}}{r_{m-1}} - \tfrac{j-1}{r_m} && \text{(lemma 5.16)} \\
\geq\ & J - \tfrac{i_1+\cdots+i_{m-1}}{r_{m-1}} - \tfrac{j-1}{r_m} && (r_1 \geq \cdots \geq r_{m-1}) \\
\geq\ & J - \tfrac{r_m}{r_{m-1}} - \tfrac{j-1}{r_m} && \text{(oletus (5.47)} \\
\geq\ & J - \omega - \tfrac{j-1}{r_m} && \text{(oletus (5.41)} \\
\geq\ & J - \tfrac{\varepsilon^2}{24} - \tfrac{j-1}{r_m} && \text{(oletus (5.40) ja } m \geq 2).
\end{aligned}$$

Muistetaan, että polynomin W määrittelevän matriisin alkiot ovat kussakin sarakkeessa j muotoa $R_{i_1,\ldots,i_{m-1},j-1}$ sekä lemman 5.16 yhtälö

$$\operatorname{ind}(R \cdot T) = \operatorname{ind} R + \operatorname{ind} T$$

ja epäyhtälö

$$\operatorname{ind}(R + T) \geq \min(\operatorname{ind} R, \operatorname{ind} T).$$

Koska W on summa, jossa on k alkiota, yksi kustakin sarakkeesta, saadaan

$$\begin{aligned}
I = \operatorname{ind} W \ &\geq \ \sum_{j=1}^{k} \max\left(J - \frac{\varepsilon^2}{24} - \frac{j-1}{r_m}, 0\right) \\
&\geq \ -\frac{k\varepsilon^2}{24} + \sum_{i=1}^{k-1} \max\left(J - \frac{i}{r_m}, 0\right).
\end{aligned}$$

Näin ollen

$$\sum_{i=0}^{k-1} \max\left(J - \frac{i}{r_m}, 0\right) \leq I + \frac{k\varepsilon^2}{24} \leq \frac{k\varepsilon^2}{6} + \frac{k\varepsilon^2}{24} < \frac{k\varepsilon^2}{4}. \tag{5.50}$$

Tutkitaan kahta mahdollista tapausta. Tapaus 1: $J - \frac{k-1}{r_m} > 0$. Tällöin epäyhtälö (5.50) saa muodon

$$\begin{aligned} & \tfrac{k}{2}\left(J + \left(J - \tfrac{k-1}{r_m}\right)\right) && < \frac{k\varepsilon^2}{4} \\ \Leftrightarrow \quad & J + \left(J - \tfrac{k-1}{r_m}\right) && < \frac{\varepsilon^2}{2}. \end{aligned}$$

Koska oletettiin, että $J - \frac{k-1}{r_m} > 0$, niin

$$J \leq J + \left(J - \frac{k-1}{r_m}\right) < \frac{\varepsilon^2}{2} < \varepsilon.$$

Tapaus 2: $J - \frac{k-1}{r_m} \leq 0$. Tällöin epäyhtälö (5.50) saa muodon

$$\begin{aligned} & \textstyle\sum_{i=0}^{\lfloor Jr_m \rfloor}\left(J - \frac{i}{r_m}\right) && < \frac{k\varepsilon^2}{4} \\ \Rightarrow \quad & \tfrac{J}{2}\left(\lfloor Jr_m \rfloor + 1\right) && < \frac{k\varepsilon^2}{4} \\ \Rightarrow \quad & \tfrac{J^2}{2} r_m && < \frac{k\varepsilon^2}{4}. \end{aligned}$$

Koska nyt kohdan (5.47) nojalla $k \leq r_m + 1 \leq 2r_m$, niin $\frac{1}{2}J^2 r_m < \frac{1}{2}\varepsilon^2 r_m$, joten $J < \varepsilon$.

Molemmissa tapauksissa päädytään siis arvioon $\operatorname{ind}_{\underline{p},\underline{r}} R = J < \varepsilon$. Tämä päättää lauseen 5.27 todistuksen.

□

7. Rothin lauseen todistus

ROTHIN LAUSEEN TODISTUS. Lemman 5.4 nojalla riittää todistaa lause 5.2. Edelleen lemman 5.8 nojalla voidaan rajoittua todistamaan lause pelkästään algebrallisille kokonaisluvuille.

Tehdään antiteesi: Olkoon α algebrallinen kokonaisluku, jonka aste on $d \geq 2$ ja jolle on olemassa $\delta > 0$ siten, että on äärettömän monta lukua $\frac{p}{q} \in \mathbb{Q}$, joille pätee epäyhtälö

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}}. \tag{5.51}$$

Muodostetaan tästä nyt ristiriita käyttäen hyväksi edellä todistettuja tuloksia.

(1) Voidaan olettaa ilman yleisyyden menetystä, että $0 < \delta < 1$.

(2) Valitaan ε siten, että $0 < \varepsilon < \dfrac{\delta}{36}$. Tällöin antiteesi pätisi myös luvulla ε. Tämä valinta täyttää oletuksen (5.27) ja lisäksi oletuksen (5.39), sillä $0 < \varepsilon < \dfrac{1}{12}$.

(3) Valitaan kokonaisluku m siten, että $m > 16\varepsilon^{-2} \log 4d$. Tällöin oletus (5.22) täyttyy. Määritellään $\omega = \omega(m, \varepsilon)$ kuten kohdassa (5.40).

(4) Olkoot $\dfrac{p_1}{q_1}$ epäyhtälön (5.51) ratkaisu siten, että $\operatorname{syt}(p_1, q_1) = 1$ ja $q_1 > 0$ siten, että $q_1^{\omega} > B^m$, missä $B = B(\alpha)$ on indeksilauseen todistuksessa määritetty ja siten, että oletukset (5.29) ja (5.43) pitävät, kun $h = 1$. Tämä valinta voidaan tehdä, sillä

antiteesin mukaan lukuja $\frac{p}{q}$ on äärettömän monta ja kullakin q epäyhtälö (5.51) voi päteä vain äärellisellä määrällä lukuja p.

(5) Valitaan epäyhtälön (5.51) ratkaisuista luvut $\frac{p_2}{q_2}, \ldots, \frac{p_m}{q_m}$ siten, että $\operatorname{syt}(p_h, q_h) = 1$ ja $q_h > 0$ kaikilla $2 \leq h \leq m$ ja siten, että

$$\omega \log q_{h+1} \geq 2 \log q_h.$$

Tällöin $q_1 < q_2 < \cdots < q_m$, joten kohdat (5.29) ja (5.43) pätevät, kun $h = 1, 2, \ldots, m$.

(6) Olkoon r_1 kokonaisluku, siten että $\varepsilon r_1 \log q_1 \geq \log q_m$.

(7) Määritellään luvut $r_2, \ldots, r_m$ asettamalla kaikille $2 \leq h \leq m$

$$r_h = \left\lfloor \frac{r_1 \log q_1}{\log q_h} \right\rfloor + 1.$$

Tällöin kaikilla $2 \leq h \leq m$ on voimassa epäyhtälöt

$$\begin{aligned} r_1 \log q_1 &< r_h \log q_h \\ &\leq r_1 \log q_1 + \log q_h \\ &\leq (1+\varepsilon) r_1 \log q_1, \end{aligned}$$

missä viimeinen arvio seuraa kohdasta (6). Tällöin kohdat (5.30) ja (5.42) pitävät. Edelliset arviot yhdistämällä saadaan kaikille $1 \leq h \leq m-1$

$$r_{h+1} \log q_h + 1 \leq (1+\varepsilon) r_h \log q_h.$$

Vastaavasti kohdan 5 nojalla

$$\begin{aligned} \omega r_h &\geq \omega \frac{r_{h+1} \log q_{h+1}}{(1+\varepsilon) \log q_h} \\ &\geq \frac{2}{1+\varepsilon} r_{h+1}, \end{aligned}$$

joten $\omega r_h \geq r_{h+1}$ kaikilla $1 \leq h \leq m-1$. Tällöin myös oletus (5.41) täyttyy.

Lauseen 5.20 (Indeksilause) oletukset täyttyvät, sillä (5.22) pitää. Olkoon R indeksilauseen antama polynomi. Myös lauseen 5.21 oletukset ((5.27), (5.28), (5.29), (5.30)) täyttyvät, joten

$$\operatorname*{ind}_{\underline{p},\underline{r}} R \geq \varepsilon m. \tag{5.52}$$

Toisaalta myös lauseen 5.27 (Rothin lemma) oletukset ((5.39), (5.40), (5.41), (5.42), (5.43), (5.44)) pitävät. Erityisesti (5.44) pitää, sillä indeksilauseen ja kohdan (3) nojalla

$$\begin{aligned} \lceil R \rceil &\leq B^{r_1 + \cdots + r_m} \\ &\leq B^{m r_1} \leq q_1^{\omega r_1}. \end{aligned}$$

Tällöin Rothin lemmasta saadaan

$$\operatorname*{ind}_{\underline{p},\underline{r}} R \leq \varepsilon.$$

Tämä on kuitenkin ristiriidassa epäyhtälön (5.52) kanssa, sillä $m > 1$. Tämä ristiriita päättää Rothin lauseen todistuksen. □

8. Rothin lauseen sovelluksia ja parannuksia

Koska Rothin lause on huomattava parannus Liouvillen lauseeseen, voidaan sen avulla konstruoida uusia transkendenttilukuja.

LAUSE 5.29. *Olkoon α irrationaaliluku, jonka ketjumurtolukuesitys on $\alpha = [a_0, a_1, a_2, \ldots]$. Olkoon $\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$ luvun α n. konvergentti ja olkoon $\lambda > 2$. Oletetaan, että äärettömän monelle $n \in \mathbb{N}$ pätee*

$$a_n \geq q_{n-1}^{\lambda-2}.$$

Tällöin α on transkendenttiluku.

TODISTUS. Todistus perustuu ketjumurtolukujen ominaisuuksiin ja Rothin lauseeseen. Katso [**7**, s. 134]. □

ESIMERKKI 5.30. Määritellään rekursiivisesti kokonaislukujono $(a_n)_{n=1}^{\infty}$ siten, että asetetaan ensin $a_0 = 0$ ja $a_1 = 1$. Jos luvut $a_0, \ldots, a_{n-1}$, joille pätee $a_1, \ldots, a_{n-1} \in \mathbb{N}$, on määritelty, kun $n \geq 2$, määritellään

$$a_n = \prod_{k=1}^{n-1}(1 + a_k) = (1 + a_1) \cdot (1 + a_2) \cdots (1 + a_{n-1}).$$

Lauseen 3.10 nojalla on olemassa raja-arvo

$$[a_0, a_1, a_2, \ldots] = \lim_{n\to\infty}[a_0, a_1, a_2, \ldots, a_n] = \alpha \in \mathbb{R} \setminus \mathbb{Q}.$$

Tällöin α on transkendenttiluku.

TODISTUS. Todistus seuraa lauseesta 5.29. Katso [**7**, s. 135]. □

LAUSE 5.31. *Olkoot m ja n kokonaislukuja siten, että $n > 0$ ja $\sqrt[3]{n} \notin \mathbb{Q}$. Tällöin Diofantoksen*[2] *yhtälöllä*

$$x^3 - ny^3 = m \tag{5.53}$$

on vain äärellinen määrä ratkaisuja $(x, y) \in \mathbb{Z}^2$.

TODISTUS. Tehdään antiteesi: Yhtälöllä (5.53) on ääretön määrä ratkaisuja. Tällöin myös yhtälöllä

$$\begin{aligned} & |x^3 - ny^3| && = |m| \\ \Leftrightarrow \quad & \left|\left(\tfrac{x}{y}\right)^3 - n\right| && = \frac{|m|}{|y^3|} \\ \Leftrightarrow \quad & \tfrac{1}{|m|}\left|\left(\tfrac{x}{y}\right)^2 + \left(\tfrac{x}{y}\right)\sqrt[3]{n} + \sqrt[3]{n}^2\right|\left|\tfrac{x}{y} - \sqrt[3]{n}\right| && = \frac{1}{|y^3|} \end{aligned} \tag{5.54}$$

on ääretön määrä ratkaisuja. Koska yhtälö (5.53) voi kullakin luvulla x päteä vain yhdellä luvulla y, on kaikille $M \in \mathbb{N}$ olemassa ratkaisu (x, y) siten, että $|y| > M$. Oletuksen nojalla on oltava $n > 1$, joten saadaan arvio $\frac{x}{y} = \sqrt[3]{\frac{m}{y^3} + n} > 1$, kun $|y|$ on tarpeeksi suuri. Oletuksen nojalla $\sqrt[3]{n}$ on algebrallinen luku, jonka aste on $d = 3$. Tällöin Rothin lauseen mukaan kaikille $\varepsilon > 0$ on olemassa luku $C(n, \varepsilon) > 0$ siten, että

$$\frac{C(n,\varepsilon)}{|y^{2+\varepsilon}|} < \left|\frac{x}{y} - \sqrt[3]{n}\right|.$$

[2]Yhtälöä, joka on muotoa $ax^k - by^k = m$, $k \geq 3$, kutsutaan kirjallisuudessa Thuen yhtälöksi.

Olkoot $0 < \varepsilon < 1$. Tällöin yhtälön (5.54) vasen puoli saa arvion

$$\frac{1}{|m|}\frac{C(n,\varepsilon)}{|y^{2+\varepsilon}|} < \frac{1}{|m|}\left|\left(\frac{x}{y}\right)^2 + \left(\frac{x}{y}\right)\sqrt[3]{n} + \sqrt[3]{n}^2\right|\left|\frac{x}{y} - \sqrt[3]{n}\right|$$

ja oikea puoli arvion

$$\frac{1}{|y^3|} = \frac{1}{|y^{1-\varepsilon}|}\frac{1}{|y^{2+\varepsilon}|} < \frac{1}{|m|}\frac{C(n,\varepsilon)}{|y^{2+\varepsilon}|}, \tag{5.55}$$

kun $|y|$ on tarpeeksi suuri. Siispä $C(n,\varepsilon) < C(n,\varepsilon)$, mikä on ristiriita. □

Huomautus 5.32. Koska Rothin lause koskee vain luvun $C(n,\varepsilon)$ olemassaoloa eikä anna lukua eksplisiittisesti, ei yhtälön (5.53) ratkaisujen lukumäärää tai kokoa voida arvioida.

Rothin lauseen niin sanotun tehokkaan version tuottaminen on avoin ongelma. Lang[3] esitti vuonna 1964 nimeänsä kantavan konjektuurin. [**8**]

Konjektuuri 5.33 (Langin konjektuuri). *Olkoot α algebrallinen luku, jonka aste on $d \geq 3$, ja $\varepsilon > 0$. Tällöin on vain äärellinen määrä lukuja $\frac{p}{q} \in \mathbb{Q}$ siten, että*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2(\log q)^{1+\varepsilon}}.$$

Joillekin luvuille α on kuitenkin onnistuttu todistamaan heikompia mutta tehokkaita tuloksia. Baker[4] todisti vuonna 1964 seuraavan lauseen.

Lause 5.34 (Bakerin lause, 1964). *Kaikille rationaaliluvuille $\frac{p}{q} \in \mathbb{Q}$ pätee*

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{10^{-6}}{q^{2{,}955}}.$$

Todistus. Katso [**1**]. □

Seuraus 5.35. *Olkoon $m \in \mathbb{Z}$. Tällöin Diofantoksen yhtälöllä*

$$x^3 - 2y^3 = m \tag{5.56}$$

on vain äärellinen määrä ratkaisuja $(x,y) \in \mathbb{Z}^2$. Lisäksi näille ratkaisuille pätee

$$|y| < \left(|m| \cdot 10^6\right)^{\frac{1}{0{,}045}} \tag{5.57}$$

ja

$$|x| < |m| + 2\left(|m| \cdot 10^6\right)^{\frac{3}{0{,}045}}. \tag{5.58}$$

Todistus. Väitteen ensimmäinen osa seuraa lauseesta 5.31. Arvio (5.57) seuraa epäyhtälöstä (5.55), kun siihen sovelletaan Rothin lauseen sijaan Bakerin lausetta. Arvio (5.58) seuraa arviosta (5.57), sillä $x = \sqrt[3]{m + 2y^3}$, joten

$$|x| \leq \sqrt[3]{|m| + |2y^3|} \leq |m| + \left|2y^3\right| < |m| + 2\left(|m| \cdot 10^6\right)^{\frac{3}{0{,}045}}.$$

□

Bakerin lauseen parannuksia ja muotoa $\sqrt[k]{a/b}$ olevien lukujen arvioinnista löytyy lisää lähteistä [**6**] ja [**14**].

[3] Serge Lang, 1927 — 2005

[4] Alan Baker, 1939 —

Lähdeluettelo

[1] Baker, Alan: *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers.* The Quarterly Journal of Mathematics, Oxford, 15:375-383, 1964.

[2] Burger, Edward B.: *Exploring the number jungle: A journey into Diophantine analysis.* American Mathematical Society, 2000.

[3] Cassels, J. W. S.: *Diophantine approximation.* Cambridge University Press, 1957.

[4] Dujella, Andrej: *Continued fractions and RSA with small secret exponent.* Tatra Mountains Mathematical Publications, 29:101–112, 2004.

[5] Hardy, G. H. and Wright, E. M.: *An Introduction to theory of numbers.* 6th edition, Oxford University Press, Great Britain, 2008.

[6] Heimonen, Ari: *On effective irrationality measures for some values of certain hypergeometric functions.* Väitöskirja, Oulun Yliopisto, Oulu, 1997.

[7] Kurittu, Lassi: *Ketjumurtoluvut.* `http://users.jyu.fi/~lkurittu/ketjumurtoluvut.pdf`, luettu 10.2.2010.

[8] Lang, Serge: *Report on diophantine approximations.* Bulletin de la Société Mathématique de France, 93:117-192, 1965.

[9] Purmonen, Veikko T.: *Differentiaalilaskentaa 2.* Jyväskylän yliopiston Matematiikan ja tilastotieteen laitoksen luentomoniste 54, 2011.

[10] Roth, Klaus: *Rational approximation to algebraic numbers.* Mathematika 2:1-20, 1955.

[11] Schmidt, Wolfgang M.: *Diophantine Approximation.* Springer Lecture Notes in Mathematics 785, 1980.

[12] Schmidt, Wolfgang M.: *Diophantine Approximation and Diophantine Equations.* Springer Lecture Notes in Mathematics 1467, 1991.

[13] Stolarsky, Kenneth B.: *Algebraic numbers and Diophantine approximation.* Marcel Dekker, Inc. New York, 1974.

[14] Voutier, Paul M.: *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers revised.* Journal de Théorie des Nombres de Bordeaux 19:263-288, 2007.

[15] Wiener, M.J.: *Cryptanalysis of short RSA secret exponents.* IEEE Trans. Inform. Theory, 36:553–558, 1990.