Sveučilište u Zagrebu

PMF - Matematički odjel

Tomislav Pejković

ROTHOV TEOREM

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, studeni 2005.

Sadržaj

Pregled rada

Osnovna tema ovog diplomskog rada je aproksimacija algebarskih brojeva racionalnim brojevima. Budući da je i tako određeno područje dosta opsežno, usredotočeni smo na aproksimaciju jednog algebarskog broja. Točnije, zanima nas kakva može biti udaljenost

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

u ovisnosti o algebarskom broju α i racionalnom broju $\frac{p}{q}$.

Dirichletov teorem povlači da za α stupnja $d \geq 2$ nejednadžba

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

ima beskonačno mnogo rješenja $\frac{p}{q}$. S druge strane, Liouvilleov teorem pokazuje da

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\varepsilon}}$$

ima najviše konačno rješenja za svaki $\varepsilon > 0$. Ti rezultati izloženi su zajedno s nekim zanimljivim partikularnim slučajevima u prvom poglavlju.

Rothov teorem poništio je razliku eksponenata 2 i $d + \varepsilon$ u prethodnim nejednadžbama. Roth je pokazao da već

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

ima konačno mnogo rješenja za svaki $\varepsilon > 0$. Dokaz Rothovog teorema je središnji dio ovog rada i izložen je u drugom poglavlju.

Iako je Rothov teorem na neki način riješio pitanje aproksimacija o kojima je riječ, ipak ostaju važni problemi. Najvažniji od njih svakako je to što nam Rothov teorem ne omogućuje da nađemo sva rješenja pripadne nejednadžbe. U tom smjeru nije se otišlo puno dalje od Liouvilleovog rezultata. U trećem poglavlju se govori više o tome. Ondje su izložene i različite primjene Rothovog teorema. Ograničavamo se na razmatranje određenih diofantskih jednadžbi i dokazivanje transcendentnosti nekih brojeva.

Konačno, u posljednjem poglavlju osvrćemo se na probleme aproksimacija više algebarskih brojeva i ključni rezultat u tom području, teorem o potprostorima.

Predložak u pisanju ovog rada bila je knjiga W.M. Schmidta *Diophantine Approximation* [Sch 80]. Također su često korištene i [Sch 91, Du 99, Bu 04]. Najdetaljniji i najpotpuniji popis literature vezane uz ovu tematiku nalazi se u [Bu 04]. Spomenute četiri knjige najčešće ne navodimo izričito u tekstu.

Osnovne oznake i pojmovi

$\mathbb{N}$	skup prirodnih brojeva $\{1, 2, 3, \dots\}$
$\mathbb{N}_0$	skup nenegativnih cijelih brojeva $\{0, 1, 2, \dots\}$
$\mathbb{Z}$	prsten cijelih brojeva
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$	redom polja racionalnih, realnih i kompleksnih brojeva
$[a, b]$	segment, tj. zatvoreni interval $\{x \in \mathbb{R} : a \leq x \leq b\}$
$[a, b\rangle$	poluotvoreni interval $\{x \in \mathbb{R} : a \leq x < b\}$
$\mathscr{S}^n$	Kartezijeva potencija skupa $\mathscr{S}$, $\{(x_1, \dots, x_n) : x_i \in \mathscr{S}, i = 1, \dots, n\}$
$\setminus$	označava skupovnu razliku, $A \setminus B = \{x : x \in A, x \notin B\}$
$\lfloor \alpha \rfloor$	cijeli dio realnog broja α, tj. najveći cijeli broj $\leq \alpha$
$\{\alpha\}$	razlomljeni dio od α, $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$
$\|\alpha\|$	udaljenost od α do najbližeg cijelog broja, $\|\alpha\| = \min\big\{\{\alpha\}, 1 - \{\alpha\}\big\}$
$\underline{\underline{x}}, \underline{\underline{y}}, \dots$	vektori, npr. $\underline{\underline{x}} = (x_1, \dots, x_n) \in \mathbb{R}^n$ ili $\underline{\underline{y}} = (y_1, \dots, y_m) \in \mathbb{Z}^m$
$\boxed{\underline{\underline{x}}}$	norma vektora $\underline{\underline{x}}$ koja se inače često označava $\big\|\underline{\underline{x}}\big\|_\infty$, za $\underline{\underline{x}} = (x_1, \dots, x_n)$ je $\boxed{\underline{\underline{x}}} = \max\{\|x_1\|, \dots, \|x_n\|\}$
$M(a_1, \dots, a_m)$	najveći zajednički djelitelj, tj. mjera od $a_1, \dots, a_m$; za dva broja pišemo i (a_1, a_2), pa primjerice $(a_1, a_2) = 1$ znači da su brojevi a_1 i a_2 relativno prosti
$c = c(\alpha, \delta)$	konstanta c ovisi samo o brojevima α i δ
$:=$	koristi se za definiranje lijeve strane u jednakosti
$\log, \exp$	logaritamska i eksponencijalna funkcija s bazom e
$\deg P$	stupanj polinoma P
$\mathrm{H}(P)$	*visina* polinoma P, za $P(X) = a_n X^n + \dots + a_1 X + a_0$ je $\mathrm{H}(P) = \max\{\|a_i\| : i = 0, 1, \dots, n\}$
$\star$	teoreme i propozicije označene zvjezdicom ne dokazujemo
$\blacksquare$	kraj dokaza
$\clubsuit$	kraj rješenja

algebarski broj, transcendentan broj

Kompleksan broj α zove se *algebarski broj* ako postoji polinom $P(X)$ s racionalnim koeficijentima, različit od nul-polinoma takav da je $P(\alpha) = 0$. Kompleksan broj se zove *transcendentan* ako nije algebarski.

algebarski cijeli broj

Kompleksan broj se naziva *algebarski cijeli broj* ako je korijen nekog normiranog polinoma s koeficijentima iz $\mathbb{Z}$.

minimalni polinom, stupanj algebarskog broja

Za svaki algebarski broj α postoji jedinstveni ireducibilni normirani polinom $P(X)$ s racionalnim koeficijentima takav da je $P(\alpha) = 0$. Takav polinom naziva se *minimalni polinom* od α (nad $\mathbb{Q}$). *Stupanj* algebarskog broja je stupanj njegovog minimalnog polinoma.

definirajući polinom, minimalni polinom nad $\mathbb{Z}$

Za algebarski broj α postoji jedinstveni polinom $Q(X)$ s cjelobrojnim koeficijentima koji je ireducibilan nad $\mathbb{Q}$, koeficijenti su mu relativno prosti, a vodeći koeficijent je pozitivan i $Q(\alpha) = 0$. Takav polinom naziva se *minimalni polinom* od α nad $\mathbb{Z}$ ili *definirajući polinom* od α.

Očito je minimalni polinom od α nad $\mathbb{Z}$ cjelobrojni višekratnik minimalnog polinoma od α nad $\mathbb{Q}$.

Gaussova lema

Za polinom $f(X)$ s cjelobrojnim koeficijentima (oznaka $f \in \mathbb{Z}[X]$) označimo najveći zajednički djelitelj koeficijenata od f s $\mathrm{cont}(f)$. Ako su $f, g \in \mathbb{Z}[X]$, onda je

$$\mathrm{cont}(fg) = \mathrm{cont}(f)\,\mathrm{cont}(g).$$

Odavde slijedi: ako su $f, g \in \mathbb{Z}[X]$ i $h \in \mathbb{Q}[\mathrm{X}]$ polinomi tako da je $f = gh$ i $\mathrm{cont}(g) = 1$, onda je i $h \in \mathbb{Z}[X]$ (v. [Ma 77, La 02]).

brojevno polje (number field)

Brojevno polje je potpolje od $\mathbb{C}$ koje ima konačan stupanj (tj. dimenziju kao vektorski prostor) nad $\mathbb{Q}$.

1 Uvod

1.1 Dirichletov teorem

Za dani realni broj α s $\lfloor\alpha\rfloor$ ćemo označavati *cijeli dio* od α, tj. najveći cijeli broj $\leq \alpha$, a s $\{\alpha\} := \alpha - \lfloor\alpha\rfloor$ ćemo označavati *razlomljeni dio* od α koji očito zadovoljava $0 \leq \{\alpha\} < 1$.

Teorem 1.1 (Dirichlet, 1842.). *Neka su α i Q realni brojevi i $Q > 1$. Tada postoje cijeli brojevi p,q takvi da je $1 \leq q < Q$ i $|\alpha q - p| \leq \frac{1}{Q}$.*

Dokaz. Pretpostavimo najprije da je Q prirodan broj. Promotrimo sljedećih $Q+1$ brojeva:

$$0, 1, \{\alpha\}, \{2\alpha\}, \ldots, \{(Q-1)\alpha\}.$$

Svi ovi brojevi leže u segmentu $[0,1]$. Podijelimo taj segment na Q disjunktnih podintervala duljine $\frac{1}{Q}$:

$$[0, \frac{1}{Q}\rangle, [\frac{1}{Q}, \frac{2}{Q}\rangle, \ldots, [\frac{Q-1}{Q}, 1].$$

Prema Dirichletovom principu, barem jedan podinterval sadrži dva (ili više) od gornjih $Q+1$ brojeva. Dakle, postoje cijeli brojevi r_1,r_2,s_1,s_2 takvi da je $0 \leq r_i < Q$ $(i = 1, 2)$, $r_1 \neq r_2$ i da vrijedi

$$|(r_1\alpha - s_1) - (r_2\alpha - s_2)| \leq \frac{1}{Q}.$$

Možemo pretpostaviti da je $r_1 > r_2$. Stavimo $q = r_1 - r_2$, $p = s_1 - s_2$. Tada je $1 \leq q < Q$ i $|\alpha q - p| \leq \frac{1}{Q}$, čime je tvrdnja teorema dokazana u slučaju $Q \in \mathbb{N}$.

Pretpostavimo sada da Q nije prirodan broj. Neka je $Q' = \lfloor Q\rfloor + 1$. Prema prije dokazanom, postoje cijeli brojevi p, q takvi da je $1 \leq q < Q'$ i $|\alpha q - p| \leq \frac{1}{Q'}$. No sada je $|\alpha q - p| < \frac{1}{Q}$, a $1 \leq q < Q'$ povlači da je $1 \leq q \leq \lfloor Q\rfloor$, odnosno $1 \leq q < Q$. ■

Korolar 1.2. *Ako je α iracionalan broj, onda postoji beskonačno mnogo parova p, q relativno prostih cijelih brojeva takvih da je*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{1.1}$$

Dokaz. Tvrdnja teorema 1.1 očito vrijedi i ukoliko zahtijevamo da su p i q relativno prosti. Dakle, za $Q > 1$ postoje relativno prosti cijeli brojevi p, q takvi da je $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{Qq} < \frac{1}{q^2}$. Budući je α iracionalan, to je $\alpha q - p \neq 0$.

Pretpostavimo da postoji samo konačno mnogo racionalnih brojeva $\frac{p}{q}$ koji zadovoljavaju (1.1). Neka su to brojevi $\frac{p_j}{q_j}$, $j = 1, \ldots, n$. Izaberimo prirodan broj m tako da je $\frac{1}{m} < \left|\alpha q_j - p_j\right|$ za sve $j = 1, \ldots, n$. Primjenimo sada teorem 1.1 uz $Q = m$, pa dobivamo racionalan broj $\frac{p}{q}$ koji zadovoljava (1.1) i za koji vrijedi $|\alpha q - p| \leq \frac{1}{m}$. Prema tome, $\frac{p}{q}$ je različit od $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$, što je kontradikcija. ■

Propozicija 1.3. *Ako je α racionalan broj, onda za sve racionalne $\frac{p}{q} \neq \frac{a}{b}$ s $q > 0$ vrijedi*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{|b|q}. \tag{1.2}$$

■

Iz ove trivijalne propozicije slijedi da za $\alpha \in \mathbb{Q}$ nejednakost (1.1) može biti zadovoljena samo za konačno parova p, q relativno prostih cijelih brojeva.

Korolar 1.2 i propozicija 1.3 daju nam koristan kriterij iracionalnosti: realan broj ima beskonačno mnogo *dobrih* racionalnih aproksimacija ako i samo ako je iracionalan.

1.2 Aproksimabilnost i verižni razlomci

Korolar 1.2 je 1891. poboljšao Hurwitz.

Teorem* 1.4 (Hurwitz). *Za svaki iracionalni broj α postoji beskonačno mnogo racionalnih brojeva p/q takvih da je*

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

Vidi [Sch 80] za dva različita dokaza; jedan preko Fareyjevih nizova, a drugi pomoću verižnih razlomaka.

Definicija. Za iracionalan broj α kažemo da je *kvadratna iracionalnost* ako je α korijen kvadratne jednadžbe s racionalnim koeficijentima. Drugim riječima, kvadratne iracionalnosti su algebarski brojevi stupnja 2.

Sljedeću lemu možemo iskoristiti kako bismo pokazali da je konstanta $\sqrt{5}$ u teoremu 1.4 najbolja moguća.

Lema 1.5. *Neka je α realna kvadratna iracionalnost koja zadovoljava jednadžbu $a\alpha^2 + b\alpha + c = 0$, s koeficijentima $a, b, c \in \mathbb{Z}$, vodećim koeficijentom $a > 0$ i diskriminantom $D = b^2 - 4ac$. Tada za $A > \sqrt{D}$ postoji najviše konačno racionalnih brojeva p/q takvih da vrijedi*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}. \tag{1.3}$$

Dokaz. Zapišimo $P(X) = aX^2 + bX + c = a(X-\alpha)(X-\alpha')$ iz čega dobivamo da je $D = a^2(\alpha-\alpha')^2$. Ako je $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$, onda vrijedi

$$\begin{aligned}\frac{1}{q^2} \leq \left|P\Big(\frac{p}{q}\Big)\right| &= \left|a\Big(\frac{p}{q}-\alpha\Big)\Big(\frac{p}{q}-\alpha'\Big)\right| \\ &< \frac{a}{Aq^2}\left|\alpha-\alpha'+\frac{p}{q}-\alpha\right| < \frac{\sqrt{D}}{Aq^2} + \frac{a}{A^2q^4}.\end{aligned}$$

Oduzimanjem $\frac{\sqrt{D}}{Aq^2}$ od obje strane dobivamo

$$\frac{1}{q^2}\left(1 - \frac{\sqrt{D}}{A}\right) < \frac{a}{A^2q^4},$$

što povlači

$$q^2 < \frac{a}{A(A-\sqrt{D})}.$$

Time je lema dokazana jer postoji najviše konačno mnogo $q \in \mathbb{Z}$, pa samim tim i $p \in \mathbb{Z}$ za koje je (1.3) istinita. ■

Napomena.
Promotrimo algebarsku jednadžbu $\alpha^2 - \alpha - 1 = 0$. Ovdje je $D = 5$ i $\alpha = \frac{1+\sqrt{5}}{2}$. Iz leme 1.5 slijedi da za $A > \sqrt{5}$ postoji najviše konačno mnogo rješenja od $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$. Zato je Hurwitzov rezultat najbolji mogući.

Kombinirajući lemu 1.5 i korolar 1.2, vidimo da je problem racionalnih aproksimacija realnih kvadratnih iracionalnosti, na neki način riješen.

Korolar 1.6. *Neka je α realna kvadratna iracionalnost. Tada postoji pozitivan realan broj $c(\alpha)$ tako da vrijedi*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^2} \qquad \textit{za sve racionalne brojeve } \frac{p}{q},$$

dok je

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2} \qquad \textit{za beskonačno mnogo racionalnih brojeva } \frac{p}{q}. \qquad ■$$

Definicija. Za realan broj α kažemo da je *loše aproksimabilan* ako postoji pozitivna konstanta $c(\alpha)$ takva da je

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^2} \qquad \text{za svaki racionalni broj } \frac{p}{q} \text{ različit od } \alpha. \tag{1.4}$$

Prema propoziciji 1.3 i korolaru 1.6, racionalni brojevi i realne kvadratne iracionalnosti su loše aproksimabilni. Možemo se zapitati postoje li i drugi takvi brojevi. Odgovor je potvrdan, a to se pokazuje pomoću teorije verižnih razlomaka.

Verižni razlomci

Slijedeći [Du 99], ukratko ćemo izreći neke definicije i teoreme vezane uz verižne razlomke. Detaljniji prikaz ove teorije nalazi se primjerice u [Hi 64, Sch 80, Du 99, Bu 04].

Neka je α proizvoljan realan broj. Stavimo: $a_0 = \lfloor \alpha \rfloor$. Ako je $a_0 \neq \alpha$, onda zapišimo α u obliku $\alpha = a_0 + \frac{1}{\alpha_1}$, tako da je $\alpha_1 > 1$, i stavimo $a_1 = \lfloor \alpha_1 \rfloor$. Ako je $a_1 \neq \alpha_1$, onda α_1 zapišimo u obliku $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, tako da je $\alpha_2 > 1$, i stavimo $a_2 = \lfloor \alpha_2 \rfloor$. Ovaj proces možemo nastaviti u nedogled, ukoliko nije $a_n = \alpha_n$ za neki n. Jasno, ako je $a_n = \alpha_n$ za neki n, onda je α racionalan broj. Naime, tada je

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}. \tag{1.5}$$

Ovo ćemo kraće zapisivati u obliku $\alpha = [a_0, a_1, \ldots, a_n]$.

Pretpostavimo da je $a_n \neq \alpha_n$ za sve n. Definirajmo racionalne brojeve $\frac{p_n}{q_n}$ sa

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n], \qquad q_n > 0.$$

Pokazuje se da vrijedi:

Teorem* 1.7. *Brojevi p_n, q_n zadovoljavaju rekurzije*

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, & p_0 &= a_0, & p_1 &= a_0 a_1 + 1; \\ q_n &= a_n q_{n-1} + q_{n-2}, & q_0 &= 1, & q_1 &= a_1. \end{aligned}$$

Propozicija* 1.8. *Za sve $n \in \mathbb{N}$ vrijedi $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$.*

Propozicija* 1.9.

1) $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots,$
2) $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \ldots,$
3) *Ako je n paran, a m neparan, onda je $\frac{p_n}{q_n} < \frac{p_m}{q_m}$.*

Propozicija* 1.10.

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$$

Sada možemo zaključiti da za racionalan α mora biti $a_n = \alpha_n$ za neki n. Zaista, u protivnom bi, zbog toga što α leži između $\frac{p_n}{q_n}$ i $\frac{p_{n+1}}{q_{n+1}}$, imali

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\frac{(-1)^n}{q_{n+1}q_n}\right| = \frac{1}{q_{n+1}q_n} < \frac{1}{q_n^2} \tag{1.6}$$

za svaki n. To bi značilo da postoji beskonačno mnogo racionalnih brojeva $\frac{p}{q}$ takvih da je $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$, što je u suprotnosti s propozicijom 1.3.

Definicija. Ako je a_0 cijeli broj, $a_1, \ldots, a_n$ prirodni brojevi, te ako je $\alpha = [a_0, a_1, \ldots, a_n]$, onda ovaj izraz zovemo razvoj broja α u *konačni jednostavni verižni (neprekidni) razlomak*; $\frac{p_i}{q_i}$ je i-ta *konvergenta* od α, a_i je i-ti *parcijalni kvocijent* od α, a $\alpha_i = [a_i, a_{i+1}, \ldots, a_n]$ je i-ti *potpuni kvocijent* od α.

Ako je α iracionalan broj, onda uvodimo oznaku $\lim\limits_{n\to\infty} [a_0, a_1, \ldots, a_n] = [a_0, a_1, a_2, \ldots]$. Ako je $\alpha = [a_0, a_1, a_2, \ldots]$, onda ovaj izraz zovemo razvoj od α u *(beskonačni) jednostavni verižni razlomak*; $\frac{p_i}{q_i}$ je i-ta konvergenta od α, a_i je i-ti *parcijalni kvocijent*, a $\alpha_i = [a_i, a_{i+1}, \ldots]$ je i-ti *potpuni kvocijent* od α.

Ovim smo završili kratak pregled temeljnih pojmova iz teorije verižnih razlomaka i možemo iskazati karakterizaciju loše aproksimabilnih brojeva.

Teorem* 1.11. *Iracionalan broj α je loše aproksimabilan ako i samo ako je niz njegovih parcijalnih kvocijenata omeđen. Iz ovoga slijedi da je skup svih loše aproksimabilnih brojeva neprebrojiv.*

Svi racionalni brojevi i kvadratne iracionalnosti su algebarski brojevi (stupnja 1, odnosno 2). Kako algebarskih brojeva ima prebrojivo mnogo, prethodni teorem nam govori da ima neprebrojivo mnogo loše aproksimabilnih brojeva koji ne spadaju u dvije već poznate skupine.

Spomenimo još da kvadratne iracionalnosti zadovoljavaju i puno više nego što nam daje teorem 1.11. Naime, niz njihovih parcijalnih kvocijenata je periodičan. Nužnost je u sljedećem teoremu dokazao Euler, a dovoljnost je dokazao Lagrange 1770.

Teorem* 1.12. *Da bi razvoj u jednostavni verižni razlomak iracionalnog broja $\alpha = [a_0, a_1, a_2, \ldots]$ bio periodičan (tj. da bi postojali cijeli brojevi $k \geq 0$ i $n \geq 1$ takvi da je $a_{m+n} = a_m$ za sve $m \geq k$), nužno je i dovoljno da α bude realna kvadratna iracionalnost.*

Gotovo ništa nije poznato o razvoju u jednostavni verižni razlomak realnih algebarskih brojeva stupnja ≥ 3. Ne zna se odgovor niti na jedno od sljedeća dva pitanja:

(1?) Postoji li realni algebarski broj stupnja ≥ 3 s omeđenim parcijalnim kvocijentima? (Prema teoremu 1.11 ovo je ekvivalentno s lošom aproksimabilnošću.)

(2?) Postoji li realni algebarski broj stupnja ≥ 3 s neomeđenim parcijalnim kvocijentima?

Obično se predviđa ([Wa 04]) da verižni razlomak realnog algebarskog broja stupnja barem 3 uvijek ima neomeđene parcijalne kvocijente.

1.3 Liouvilleov teorem

Teorem 1.13 (Liouville, 1844.). *Neka je α realni algebarski broj stupnja d. Tada postoji konstanta $c(\alpha) > 0$ tako da vrijedi*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d} \tag{1.7}$$

za sve racionalne brojeve $\frac{p}{q}$ različite od α.

(U nejednakosti (1.7) i u drugim nejednakostima tog tipa, prešutno se pretpostavlja da je $q > 0$.)

Dokaz. Prilično jednostavan dokaz razdvojit ćemo u tri koraka koji će biti važni u kasnijem poboljšanju Liouvilleovog teorema.

(a) Neka je $P(X)$ *definirajući polinom* od α. Dakle, $\deg P = d$, koeficijenti od P su u $\mathbb{Z}$ (tj. $P(X) \in \mathbb{Z}[X]$) i $P(\alpha) = 0$.

(b) Bez smanjenja općenitosti možemo pretpostaviti da je $\left|\alpha - \frac{p}{q}\right| \leq 1$ (inače možemo staviti $c(\alpha) = 1$). Razvijemo li $P(X)$ u Taylorov red oko α, dobivamo

$$\left|P\Big(\frac{p}{q}\Big)\right| = \left|\sum_{i=1}^{d} \Big(\frac{p}{q} - \alpha\Big)^i \frac{1}{i!} P^{(i)}(\alpha)\right| < \frac{1}{c(\alpha)} \left|\alpha - \frac{p}{q}\right|, \tag{1.8}$$

gdje je $c(\alpha) = \frac{1}{2\sum_{i=1}^{d} \frac{1}{i!}|P^{(i)}(\alpha)|}$.

(c) Budući je polinom $P(X)$ ireducibilan i $\frac{p}{q} \neq \alpha$, to je $P\big(\frac{p}{q}\big) \neq 0$. Stoga je broj $q^d\big|P\big(\frac{p}{q}\big)\big|$ prirodan, pa je $\big|P\big(\frac{p}{q}\big)\big| \geq \frac{1}{q^d}$. Usporedimo li ovo sa (1.8), dobivamo tvrdnju teorema. ■

Korolar 1.14. *Broj $\alpha = \sum_{n=1}^{\infty} 10^{-n!}$ je transcendentan.*

Dokaz. Budući da mu decimalni prikaz nije periodičan, α je iracionalan. Ako za $k \geq 2$ stavimo $q_k = 10^{(k-1)!}$ i $p_k = q_k \sum_{n=1}^{k-1} 10^{-n!}$, onda je

$$\left|\alpha - \frac{p_k}{q_k}\right| = \sum_{n=k}^{\infty} \frac{1}{10^{n!}} \leq \frac{2}{10^{k!}} = \frac{2}{q_k^k}.$$

Odavde slijedi da za svaki prirodni broj d i za svaki $c > 0$ postoji $k_0 \in \mathbb{N}$ takav da za sve $k \geq k_0$ vrijedi $\left|\alpha - \frac{p_k}{q_k}\right| < \frac{c}{q_k^d}$. Po Liouvilleovom teoremu, α ne može biti algebarski broj stupnja d niti za jedan d, pa je α transcendentan. ■

Liouville je bio prvi koji je dokazao egzistenciju transcendentnih brojeva. Učinio je to dajući za takve brojeve primjere poput α iz korolara. Kasnije je Cantor dokazao neprebrojivost skupa realnih brojeva, pa je tako dobiven i drugi dokaz, ovaj puta nekonstruktivan, da postoje transcendentni brojevi.

Korolar 1.14 ilustrira kako se teorem 1.13 može primijeniti u dokazu transcendentnosti za veliku klasu realnih brojeva koje nazivamo Liouvilleovi brojevi.

Definicija. Za realni broj α kažemo da je *Liouvilleov broj* ako za svaki pozitivni realni broj $w > 0$ postoji racionalni broj p/q tako da je

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^w}.$$

Laganom modifikacijom dokaza korolara 1.14 možemo pokazati da je svaki realan broj oblika $\sum_{n=1}^{\infty} a_n 10^{-n!}$, gdje je a_n iz $\{1, 2\}$, Liouvilleov broj. Stoga postoji neprebrojivo mnogo Liouvilleovih brojeva. No, Liouvilleovi brojevi čine skup Lebesgueove mjere 0 (v. Hinčinov teorem 3.4), pa to djelomično objašnjava zašto Liouvilleov teorem nije dovoljno jak da bi se dokazala transcendentnost klasičnih brojeva kao što su e ili π.

Teorem 1.13 nam daje sljedeći koristan kriterij transcendentnosti.

Primjer 1.1. *Ako nazivnici q_n konvergenata realnog broja α zadovoljavaju*

$$\limsup_{n\to\infty} \frac{\log\log q_n}{n} = +\infty,$$

onda je α transcendentan.

Rješenje. Ovu ćemo tvrdnju dokazati indirektno.

Pretpostavimo da je α algebarski broj stupnja d. Tada prema Liouvilleovom teoremu postoji konstanta $c(\alpha) > 0$ takva da je $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$ za sve racionalne brojeve $\frac{p}{q}$ različite od α.

Neka je k po volji izabran prirodan broj. Tvrdimo da je skup $A_k = \{n \in \mathbb{N} : q_n^k < q_{n+1}\}$ beskonačan.

> Pretpostavimo suprotno, tj. neka postoji $n_0 \in \mathbb{N}$ tako da za sve $n \geq n_0$ vrijedi $q_n^k \geq q_{n+1}$, tj. $k \log q_n \geq \log q_{n+1}$. Iteracijom dobivamo da za sve $i \in \mathbb{N}$ vrijedi $k^i \log q_{n_0} \geq \log q_{n_0+i}$, iz čega slijedi $i \log k + \log\log q_{n_0} \geq \log\log q_{n_0+i}$ (primjetimo da je za $m \geq 1$ nužno $q_m > 1$, pa je i $\log q_m > 0$). Sada je
>
> $$\frac{i \log k}{n_0 + i} + \frac{\log\log q_{n_0}}{n_0 + i} \geq \frac{\log\log q_{n_0+i}}{n_0 + i} \qquad \text{za sve } i \in \mathbb{N},$$
>
> što je u kontradikciji sa činjenicama:
>
> $$\frac{i \log k}{n_0 + i} < \log k, \quad \lim_{i\to\infty} \frac{\log\log q_{n_0}}{n_0 + i} = 0, \quad \limsup_{i\to\infty} \frac{\log\log q_{n_0+i}}{n_0 + i} = \infty.$$

Uzmimo prirodan broj k tako da je $2^k > \frac{1}{c(\alpha)}$ i uzmimo $n \in A_{k+d}$ tako da je $q_n > 2$. Onda vrijedi

$$\left|\alpha - \frac{p_n}{q_n}\right| \overset{(1.6)}{<} \frac{1}{q_n q_{n+1}} \overset{(n\in A_{k+d})}{<} \frac{1}{q_n^{k+d+1}} < \frac{1}{q_n^{k+d}} = \frac{1}{q_n^k} \cdot \frac{1}{q_n^d} \overset{(q_n>2)}{<} \frac{1}{2^k} \cdot \frac{1}{q_n^d} < \frac{c(\alpha)}{q_n^d}.$$

Došli smo do kontradikcije, što pokazuje da α ne može biti algebarski broj. ♣

1.4 Rothov teorem

Neka je α realan algebarski broj stupnja $d \geq 2$. Iz Liouvilleovog teorema 1.13 slijedi da nejednadžba

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\mu} \tag{1.9}$$

ima konačno mnogo racionalnih rješenja $\frac{p}{q}$ ako je $\mu > d$. Veliki norveški matematičar Thue dokazao je 1909. da (1.9) ima konačno rješenja ako je $\mu > \frac{1}{2}d + 1$. (Njegov rezultat iskoristit ćemo u §3.6 kod proučavanja jedne vrste diofantskih jednadžbi koja sada nosi njegovo ime.) Godine 1921. Siegel je u svojoj disertaciji znatno poboljšao Thueov rezultat pokazavši da tvrdnja vrijedi već za

$$\mu > \min_{1 \leq j \leq d} \Big(\frac{d}{j+1} + j \Big),$$

što, uzmemo li $j = \lfloor \sqrt{d} \rfloor$, povlači malo slabiji rezultat $\mu > 2\sqrt{d}$. Neznatno poboljšanje $\mu > \sqrt{2d}$ dali su 1947. Dyson[1]i neovisno o njemu Geljfand. Konačno je Roth[2] 1955. dokazao[3] da (1.9) ima najviše konačno rješenja ako je $\mu > 2$. Za ovaj rezultat je Roth 1958. dobio Fieldsovu medalju.[4] Dirichletov teorem, tj. korolar 1.2, pokazuje da je

[1] Izgleda da je ovaj problem imao presudan utjecaj na Dysonovu karijeru. Donosimo isječak iz njegovih komentara vlastitih izabranih radova [Dy 96]:
"At that time I had tentatively decided to switch my activities from mathematics to physics... I thought then that it would be more exciting to solve one of the basic mysteries of nature than to continue proving theorems that were of interest only to a small coterie of number-theorists. But Davenport's friendliness tempted me to stay with mathematics. I decided to launch an all-out attack on the Siegel conjecture and to let the result determine my future. If I succeeded in proving it, I would be a mathematician. If I failed, I would be a physicist. After three months of intensive work, I admitted failure. I would after all be a physicist. The result of the three month's work is recorded in paper /'The Approximation to Algebraic Numbers by Rationals'/. All I could achieve was an inconsequential strengthening of Siegel's theorem, replacing Siegel's bound $2\sqrt{n}$ by $\sqrt{2n}$. I was still infinitely far away from the conjectured bound 2. Eight years later K. F. Roth, helped like me by Davenport's encouragement, succeeded brilliantly where I had failed. Roth converted Siegel's conjecture into Roth's theorem. Roth's smashing victory confirmed my feeling that I had made a wise choice when I switched to physics."

[2] Klaus Friedrich Roth (Brestlau=Wroclaw, 29.10.1925.–) je engleski matematičar njemačkog podrijetla. Kratki životopis nalazi se na
`http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Roth_Klaus.html`

[3] Na internet stranici [Co 04] profesora J.B. Cosgravea nalaze se i neke zanimljivosti vezane uz Rothov teorem. Ovdje prenosimo jednu njegovu anegdotu koja opisuje okolnosti u kojima je Roth došao do svog važnog rezultata:
"When I was a student in London, I once asked Roth (in his office at Imperial College) what were the circumstances in which he proved his famous 1955 result. Roth told me that when he worked with Davenport in University College London in the early 50's, Davenport had a practice of inviting colleagues to read up on some difficult piece of work, and then explain it in a seminar talk. Davenport asked him to read the Thue-Siegel result. He read it, understood it, explained it to everyone, and then (after all that effort) decided to give himself one year (Roth's standard practice) to solve Siegel's conjectured improvement. His year was almost up, he was just about to give up, when..."

[4] Iz govora H. Davenporta povodom dodjele Fieldsove medalje Rothu (prema [Co 04]): "The achievement /of Roth/ is one that speaks for itself: it closes a chapter, and a new chapter is now opened. Roth's theorem settles a question which is both of a fundamental nature and of extreme difficulty. It will stand as a landmark in mathematics for as long as mathematics is cultivated."

Rothov rezultat najbolji mogući.

Teorem 1.15 (Roth). *Za svaki algebarski broj α i svaki $\delta > 0$ nejednadžba*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}} \tag{1.10}$$

ima samo konačno mnogo rješenja u racionalnim brojevima $\frac{p}{q}$.
Ekvivalentno, za svaki $\delta > 0$ postoji konstanta $c(\alpha, \delta) > 0$ takva da za sve $\frac{p}{q} \in \mathbb{Q}\backslash\{\alpha\}$ vrijedi

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha, \delta)}{q^{2+\delta}}. \tag{1.11}$$

Napomene.

(i) Rothov rezultat je istinit, ali trivijalan za $\alpha \in \mathbb{C}\backslash\mathbb{R}$, pa će nam ubuduće α uvijek biti realan broj.

(ii) Ako je α stupnja 2, onda je prema Liouvilleovom teoremu

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^2}. \tag{1.12}$$

U ovom slučaju je Liouvilleov teorem jači od Rothovog. Naravno, (1.12) slijedi već iz leme 1.5.

Prije nego što započnemo s dokazom, dat ćemo nekoliko uvodnih komentara.

Pokušajmo dokazati Rothov teorem modifikacijom dokaza Liouvilleovog teorema. U koraku (a) izabiremo polinom $P(X)$ stupnja r s cjelobrojnim koeficijentima, kojemu je α korijen s kratnošću i. Nadalje, u koraku (b) pretpostavljamo da vrijedi (1.9), pa razvoj u Taylorov red oko α

$$P\Big(\frac{p}{q}\Big) = \sum_{j=i}^{r} \Big(\frac{p}{q} - \alpha\Big)^j \frac{1}{j!} P^{(j)}(\alpha)$$

povlači $\big|P\big(\frac{p}{q}\big)\big| \leq cq^{-\mu i}$. Konačno u (c) dijelu dokaza imamo $P\big(\frac{p}{q}\big) \neq 0$, pa je $\big|P\big(\frac{p}{q}\big)\big| \geq q^{-r}$ za sve osim konačno mnogo racionalnih brojeva $\frac{p}{q}$. Dakle, ako (1.9) ima beskonačno rješenja, onda je $\mu i \leq r$, odnosno $\mu \leq \big(\frac{i}{r}\big)^{-1}$. Zato želimo $\frac{i}{r}$ učiniti što je moguće većim. No, uvijek je $\frac{i}{r} \leq \frac{1}{d}$ i $\frac{i}{r} = \frac{1}{d}$ vrijedi samo ako je $P(X)$ potencija definirajućeg polinoma od α. Zaključujemo da nam ova metoda daje $\mu \leq d$, što nije nimalo bolje od Liouvilleovog rezultata.

Kako bi poboljšao ovu ocjenu, Thue upotrebljava polinom $X_2Q(X_1) - P(X_1)$ u dvije varijable, a Siegel upotrebljava općenitiji polinom $P(X_1, X_2)$ u dvije varijable. Roth koristi polinom $P(X_1, \ldots, X_m)$ u više varijabli.

Ako su sada $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$ vrlo dobre aproksimacije od α, uvrstimo ih u $P(X_1, \ldots, X_m)$. Veliki problem predstavlja to što je teško utvrditi da je $P\big(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\big) \neq 0$. Ovu poteškoću prevladava Rothova lema u kojoj se zahtijeva da bude $q_1 < q_2 < \cdots < q_m$.

Posljedica je da do kontradikcije dolazimo samo ako imamo barem m vrlo dobrih racionalnih aproksimacija. Kod Thueovog i Siegelovog rezultata je $m = 2$, pa trebamo dvije vrlo dobre racionalne aproksimacije.

Osnovni nedostatak metode Thuea, Siegela i Rotha je u tome što ne daje ogradu na veličinu nazivnika q racionalnih rješenja od (1.10) ili, ekvivalentno tome, ne daje eksplicitnu konstantu u (1.11). Ova je metoda stoga *neefektivna*. Ne omogućava nam pronalaženje svih rješenja od (1.10).

Efektivni rezultati su nažalost slabiji i od Thueovog, pa samim tim i od Rothovog rezultata. Feljdman je 1971. koristeći Bakerovu teoriju linearnih formi u logaritmima dao efektivna poboljšanja Liouvilleovog teorema. Ta su poboljšanja ovog tipa

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^{d-c_1(\alpha)}},$$

gdje su $c(\alpha) > 0$ i $c_1(\alpha) > 0$ efektivne. Tako dobiven $c_1(\alpha)$ je vrlo mali, a bolji rezultati poznati su samo za posebne algebarske brojeve α, primjerice za kubne iracionalnosti i k-te korijene racionalnih brojeva. Detaljniji pregled efektivnih aproksimacija može se naći u [Bu 04].

2 Dokaz Rothovog teorema

Dokaz Rothovog teorema prenosimo, uz sitne nadopune, iz [Sch 80], gdje je vrlo pregledno i detaljno izložen.

2.1 Kombinatorne leme

Lema 2.1. *Neka su $r_1, \ldots, r_m$ prirodni brojevi i neka je $0 < \varepsilon < 1$. Tada m-torki cijelih brojeva $\underline{\underline{i}} = (i_1, \ldots, i_m)$ koje zadovoljavaju*

$$0 \leq i_h \leq r_h \qquad (1 \leq h \leq m) \tag{2.1}$$

i

$$\left| \left(\sum_{h=1}^{m} \frac{i_h}{r_h} \right) - \frac{m}{2} \right| \geq \varepsilon m \tag{2.2}$$

ima najviše

$$(r_1 + 1) \cdots (r_m + 1) \cdot 2e^{-\frac{\varepsilon^2 m}{4}}. \tag{2.3}$$

Napomene.

(i) Ovoj lemi možemo dati vjerojatnosnu interpretaciju. Promatramo $i_1, \ldots, i_m$ kao nezavisne slučajne varijable takve da svaki i_h ima uniformnu distribuciju na $\{0, 1, \ldots, r_h\}$ $(1 \leq h \leq m)$. Stavimo li

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

vidimo da je X slučajna varijabla kojoj je lako izračunati očekivanje $\mathrm{E}(X) = \frac{m}{2}$ i varijancu

$$\mathrm{Var}(X) = \sum_{h=1}^{m} \mathrm{Var}\left(\frac{i_h}{r_h}\right) = \sum_{h=1}^{m} \left(\frac{2r_h + 1}{6r_h} - \frac{1}{4}\right) \leq \sum_{h=1}^{m} \frac{1}{4} = \frac{m}{4}.$$

Koristit ćemo Čebiševljevu nejednakost

$$\mathrm{P}\left(|X - \mathrm{E}(X)| \geq \xi\right) \leq \frac{\mathrm{Var}(X)}{\xi^2}$$

uz $\xi = \varepsilon m$. Očekivani broj m-torki $\underline{\underline{i}}$ koje zadovoljavaju (2.1) i (2.2) očito je jednak umnošku broja svih m-torki koje zadovoljavaju (2.1) i vjerojatnosti za

(2.2), tj.

$$(r_1+1)\cdots(r_m+1)\,\mathrm{P}\left(|X-\mathrm{E}(X)|\geq \varepsilon m\right) \leq (r_1+1)\cdots(r_m+1)\frac{\mathrm{Var}(X)}{(\varepsilon m)^2} \leq (r_1+1)\cdots(r_m+1)\frac{1}{4\varepsilon^2 m}. \tag{2.4}$$

Dobivena ograda za broj takvih m-torki zaista vrijedi jer radimo s konačnim vjerojatnosnim modelom (usp. [Ve 01, str. 343]). Ta je ograda za $m > \frac{21}{\varepsilon^2}$ lošija, a za $m < \frac{20}{\varepsilon^2}$ bolja od (2.3).

(ii) Lema 2.1 je neposredna posljedica leme 2.3 koju ćemo uskoro dokazati.

Lema 2.2. *Neka su $n \geq 1$, $r \geq 0$ cijeli brojevi. Broj n-torki $(i_1, \ldots, i_n)$ nenegativnih cijelih brojeva takvih da vrijedi $i_1 + \cdots + i_n = r$ je*

$$N(n,r) = \binom{r+n-1}{r}. \tag{2.5}$$

Dokaz se može provesti indukcijom po n i r, ali mi ćemo dati kombinatorni dokaz koji pruža bolje razumijevanje (v. [Ve 01, str. 68]).

Dokaz. Postoji bijekcija između n-torki nenegativnih cijelih brojeva $(i_1, \ldots, i_n)$ koje su rješenja jednadžbe $i_1 + \cdots + i_n = r$ i nizova sastavljenih samo od nula i jedinica koji imaju točno $n-1$ nulu i r jedinica. Naime, rješenju $(i_1, \ldots, i_n)$ dane jednadžbe pridružujemo niz koji se sastoji od i_1 jedinica, pa 1 nula, i_2 jedinica, pa 1 nula, itd. do i_{n-1} jedinica, 1 nula i na kraju i_n jedinica. Ilustrirajmo to na primjeru u kojem je $n = 4$, $r = 10$.

$\downarrow$	$5+1+0+4=10$	0111111100111	$\uparrow$
$\downarrow$	$\|\|\|\|\|+\|++\|\|\|\|$	$+\|\|\|\|\|\|+++\|\|\|$	$\uparrow$
$\downarrow$	1111101001111	$0+7+0+3=10$	$\uparrow$

Lako se pokaže da je ovakvo pridruživanje bijektivno, pa zaključujemo da je $N(n,r) = \binom{r+n-1}{r}$. ∎

Lema 2.3. *Neka su $r_1, \ldots, r_m$ prirodni brojevi i $0 < \varepsilon < 1$. Neka je i $n \geq 2$ prirodan broj. Tada je broj nm-torki nenegativnih cijelih brojeva*

$$\begin{matrix} i_{11}, \ldots, i_{1n} \\ i_{21}, \ldots, i_{2n} \\ \vdots \\ i_{m1}, \ldots, i_{mn} \end{matrix}$$

koje zadovoljavaju

$$\sum_{k=1}^{n} i_{hk} = r_h \qquad (1 \le h \le m) \tag{2.6}$$

i

$$\left| \left(\sum_{h=1}^{m} \frac{i_{h1}}{r_h} \right) - \frac{m}{n} \right| \ge \varepsilon m$$

najviše

$$\binom{r_1 + n - 1}{r_1} \cdots \binom{r_m + n - 1}{r_m} \cdot 2e^{-\frac{\varepsilon^2 m}{4}}.$$

Napomena.
Lema 2.1 slijedi iz leme 2.3 uzmemo li $n = 2$ i $2m$-torku

$$\begin{matrix} i_1, r_1 - i_1 \\ \vdots \\ i_m, r_m - i_m. \end{matrix}$$

Dokaz leme 2.3. Neka je M_+ broj nm-torki za koje vrijedi (2.6) i

$$\left(\sum_{h=1}^{m} \frac{i_{h1}}{r_h} \right) - \frac{m}{n} \ge \varepsilon m,$$

a neka je M_- broj nm-torki za koje vrijedi (2.6) i

$$\left(\sum_{h=1}^{m} \frac{i_{h1}}{r_h} \right) - \frac{m}{n} \le -\varepsilon m.$$

Za dokaz leme očito je dovoljno pokazati da je

$$M_\pm \le \binom{r_1 + n - 1}{r_1} \cdots \binom{r_m + n - 1}{r_m} e^{-\frac{\varepsilon^2 m}{4}}. \tag{2.7}$$

Za cijele brojeve j i c_j, takve da je $1 \le j \le m$ i $0 \le c_j \le r_j$, sa $f_j(c_j)$ označavamo broj $(n-1)$-torki nenegativnih cijelih brojeva $i_{j2}, \ldots, i_{jn}$ koje zadovoljavaju $i_{j2} + \cdots + i_{jn} = r_j - c_j$. Iz definicija od M_+ i M_- dobivamo

$$M_\pm = \sum_{\underline{c}} f_1(c_1) \cdots f_m(c_m), \tag{2.8}$$

gdje suma ide po svim $\underline{c} = (c_1, \ldots, c_m)$ sa $0 \le c_j \le r_j$ $(1 \le j \le m)$ za koje je

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

$\geq \varepsilon m$ ili $\leq -\varepsilon m$, respektivno. Stoga je

$$\begin{aligned} M_{\pm} e^{\frac{\varepsilon^2 m}{2}} &\leq \sum_{c_1=0}^{r_1} \cdots \sum_{c_m=0}^{r_m} f_1(c_1) \cdots f_m(c_m) \exp\left(\pm \frac{\varepsilon}{2} \left(\left(\sum_{h=1}^{m} \frac{c_h}{r_h} \right) - \frac{m}{n} \right) \right) \\ &= \prod_{j=1}^{m} \left(\sum_{c_j=0}^{r_j} f_j(c_j) \exp\left(\pm \frac{\varepsilon}{2} \left(\frac{c_j}{r_j} - \frac{1}{n} \right) \right) \right). \end{aligned} \tag{2.9}$$

Uzmimo na trenutak fiksan j. Iz definicija je jasno da vrijedi

$$\sum_{c=0}^{r_j} f_j(c) = \sum_{c+i_2+\cdots+i_n=r_j} 1 = N(n, r_j) \overset{\text{lema 2.2}}{=} \binom{r_j + n - 1}{r_j}. \tag{2.10}$$

Prisjetimo se da je $e^x \leq 1 + x + x^2$ za $|x| \leq 1$. Zato je

$$\begin{aligned} \sum_{c=0}^{r_j} f_j(c) \exp\left(\pm \frac{\varepsilon}{2} \left(\frac{c}{r_j} - \frac{1}{n} \right) \right) &\leq \sum_{c=0}^{r_j} f_j(c) \left(1 \pm \frac{\varepsilon}{2} \left(\frac{c}{r_j} - \frac{1}{n} \right) + \frac{\varepsilon^2}{4} \Big(\underbrace{\frac{c}{r_j} - \frac{1}{n}}_{<1} \Big)^2 \right) \\ &\leq \sum_{c=0}^{r_j} f_j(c) \left(1 + \frac{\varepsilon^2}{4} \right) \pm \frac{\varepsilon}{2r_j} \left(\sum_{c=0}^{r_j} c f_j(c) - \frac{r_j}{n} \sum_{c=0}^{r_j} f_j(c) \right) \\ &= \binom{r_j + n - 1}{r_j} \left(1 + \frac{\varepsilon^2}{4} \right), \end{aligned} \tag{2.11}$$

pri čemu zadnja jednakost slijedi iz (2.10) i činjenice da je koeficijent uz $\pm\frac{\varepsilon}{2r_j}$ u predzadnjem redu jednak 0. Kako bismo pokazali da taj koeficijent uistinu jest 0, uočimo

$$f_j(c) = \sum_{\substack{i_2,\ldots,i_n \\ i_2+\cdots+i_n=r_j-c}} 1 = \sum_{\substack{i_1,\ldots,i_n \\ i_1+\cdots+i_n=r_j \\ i_1=c}} 1,$$

iz čega je

$$c f_j(c) = \sum_{\substack{i_1,\ldots,i_n \\ i_1+\cdots+i_n=r_j \\ i_1=c}} i_1.$$

Zato je

$$\begin{aligned} \sum_{c=0}^{r_j} c f_j(c) &= \sum_{\substack{i_1,\ldots,i_n \\ i_1+\cdots+i_n=r_j}} i_1 = \frac{1}{n} \sum_{\substack{i_1,\ldots,i_n \\ i_1+\cdots+i_n=r_j}} (i_1 + \cdots + i_n) \\ &= \frac{r_j}{n} \sum_{\substack{i_1,\ldots,i_n \\ i_1+\cdots+i_n=r_j}} 1 = \frac{r_j}{n} \sum_{c=0}^{r_j} f_j(c), \end{aligned}$$

kao što smo i tvrdili.

Iz (2.9) i (2.11) slijedi

$$M_{\pm}e^{\frac{\varepsilon^2 m}{2}} \leq \binom{r_1+n-1}{r_1}\cdots\binom{r_m+n-1}{r_m}\left(1+\frac{\varepsilon^2}{4}\right)^m \overset{1+x\leq e^x}{\leq} \binom{r_1+n-1}{r_1}\cdots\binom{r_m+n-1}{r_m}e^{\frac{\varepsilon^2 m}{4}}.$$

Ova nejednakost je ekvivalentna (2.7), pa je lema dokazana. ■

2.2 Daljnje leme

Od sad pa do kraja ovog poglavlja promatrat ćemo polinome u m varijabli s cjelobrojnim koeficijentima. Pišemo

$$P(X_1,\ldots,X_m) = \sum C(j_1,\ldots,j_m)X_1^{j_1}\cdots X_m^{j_m},$$

pri čemu se sumira po svim m-torkama nenegativnih cijelih brojeva $(j_1,\ldots,j_m)$ i svi osim konačno mnogo koeficijenata $C(j_1,\ldots,j_m)$ su 0. Definiramo *visinu* od P sa

$$\mathrm{H}(P) := \max_{j_1,\ldots,j_m} |C(j_1,\ldots,j_m)|.$$

Ako su $i_1,\ldots,i_m$ nenegativni cijeli brojevi, pišemo

$$P_{i_1\ldots i_m} = \frac{1}{i_1!\cdots i_m!}\cdot\frac{\partial^{i_1+\cdots+i_m}}{\partial {X_1}^{i_1}\cdots\partial {X_m}^{i_m}}P. \tag{2.12}$$

Često će biti praktičnije pisati $P_{\underline{\underline{i}}}$ umjesto $P_{i_1\ldots i_m}$, a tada se podrazumijeva da je $\underline{\underline{i}} = (i_1,\ldots,i_m)$.

Lema 2.4. *Ako P ima cjelobrojne koeficijente, onda su i koeficijenti od $P_{\underline{\underline{i}}}$ cijeli brojevi. Nadalje, ako je P stupnja $\leq r_h$ u varijabli X_h $(1\leq h\leq m)$, onda je*

$$\mathrm{H}(P_{\underline{\underline{i}}}) \leq 2^{r_1+\cdots+r_m}\,\mathrm{H}(P).$$

Dokaz. Možemo pisati

$$P(X_1,\ldots,X_m) = \sum_{j_1=0}^{r_1}\cdots\sum_{j_m=0}^{r_m} C(j_1,\ldots,j_m)X_1^{j_1}\cdots X_m^{j_m},$$

pa je

$$P_{\underline{\underline{i}}}(X_1,\ldots,X_m) = \sum_{j_1=0}^{r_1}\cdots\sum_{j_m=0}^{r_m}\binom{j_1}{i_1}\cdots\binom{j_m}{i_m}C(j_1,\ldots,j_m)X_1^{j_1-i_1}\cdots X_m^{j_m-i_m}. \tag{2.13}$$

Novi koeficijenti su također cijeli brojevi jer su binomni koeficijenti cijeli brojevi. (Dogovorno uzimamo da je $\binom{m}{n} = 0$ za $m < n$.) Kako je[1]

$$\binom{j_k}{i_k} \leq 2^{j_k} \leq 2^{r_k} \qquad (1 \leq k \leq m),$$

to druga tvrdnja leme slijedi iz (2.13). ■

Lema 2.5 (Siegelova lema). *Neka je dano M linearnih formi s cjelobrojnim koeficijentima:*

$$L_j(\underline{\underline{z}}) = \sum_{k=1}^{N} a_{jk} z_k \qquad (1 \leq j \leq M).$$

Ako je $N > M$ i vrijedi

$$|a_{jk}| \leq A, \qquad (1 \leq j \leq M,\ 1 \leq k \leq N)$$

gdje je A neki prirodan broj, onda postoji cjelobrojna točka $\underline{\underline{z}} = (z_1, \ldots, z_N) \neq \underline{\underline{0}}$ takva da je

$$L_j(\underline{\underline{z}}) = 0 \qquad (1 \leq j \leq M) \tag{2.14}$$

i

$$\boxed{\underline{\underline{z}}} \leq \left\lfloor (NA)^{\frac{M}{N-M}} \right\rfloor = Z. \tag{2.15}$$

Dokaz. Budući da je $N > M$, racionalna rješenja $\underline{\underline{z}} \neq \underline{\underline{0}}$ od (2.14) uvijek postoje. No, ako je $\underline{\underline{z}}$ rješenje od (2.14), onda je i $\lambda\underline{\underline{z}}$ rješenje za svaki $\lambda \in \mathbb{R}$. Prema tome, postoje cjelobrojne točke $\underline{\underline{z}} \neq \underline{\underline{0}}$ koje zadovoljavaju (2.14).

Preostaje pokazati da postoji takva točka koja bi uz (2.14) zadovoljavala i (2.15). Naš dokaz ove tvrdnje vrlo je sličan dokazu Dirichletovog teorema 1.1. Najprije imamo $Z + 1 > (NA)^{\frac{M}{N-M}}$, pa je $NA < (Z+1)^{\frac{N-M}{M}}$ i stoga vrijedi

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

Za svaku cjelobrojnu točku $\underline{\underline{z}} = (z_1, \ldots, z_N)$ iz $[0, Z]^N$ vrijedi

$$-C_j^- Z \leq L_j(\underline{\underline{z}}) \leq C_j^+ Z, \qquad (1 \leq j \leq M)$$

gdje je $-C_j^-$ suma negativnih, a C_j^+ suma pozitivnih koeficijenata linearne forme L_j. Iz $C_j^- + C_j^+ \leq NA$ slijedi da svaki $L_j(\underline{\underline{z}})$ leži u intervalu duljine $\leq NAZ$. Zato svaki $L_j(\underline{\underline{z}})$ može imati najviše $NAZ + 1$ različitih vrijednosti, pa M-torka $\big(L_1(\underline{\underline{z}}), \ldots, L_M(\underline{\underline{z}})\big)$ može imati najviše

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

[1] Ova nejednakost ima očitu kombinatornu interpretaciju: podskupova od $\{1, \ldots, j_k\}$ koji imaju i_k elemenata očito je manje od svih podskupova skupa $\{1, \ldots, j_k\}$, v. [Ve 01]

različitih vrijednosti.

S druge strane, postoji $(Z+1)^N$ vektora $\underline{\underline{z}} \in \{0, 1, \ldots, Z\}^N$. Zaključujemo da postoje N-torke $\underline{\underline{z}}^{(1)} \neq \underline{\underline{z}}^{(2)}$ iz $\{0, 1, \ldots, Z\}^N$ za koje vrijedi

$$L_j(\underline{\underline{z}}^{(1)}) = L_j(\underline{\underline{z}}^{(2)}) \qquad (1 \leq j \leq M).$$

Cjelobrojna točka $\underline{\underline{z}} = \underline{\underline{z}}^{(1)} - \underline{\underline{z}}^{(2)}$ zadovoljava tražene uvjete iz leme. ■

Ako je α algebarski broj stupnja d, onda zadovoljava jednadžbu $a_0\alpha^d + \cdots + a_d = 0$ s cjelobrojnim koeficijentima $a_0, \ldots, a_d$, pa je $\beta = a_0\alpha$ algebarski stupnja d i vrijedi $\beta^d + a_1\beta^{d-1} + a_2a_0\beta^{d-2} + \cdots + a_da_0^{d-1} = 0$, što znači da je β algebarski cijeli broj. Nejednakosti $\left|\alpha - \frac{p}{q}\right| < q^{-2-\delta}$ i $\left|\beta - \frac{a_0p}{q}\right| < a_0q^{-2-\delta}$ su ekvivalentne. Stoga tvrdnja Rothovog teorema vrijedi za β ako i samo ako vrijedi za α. Zato je *dovoljno teorem dokazati za algebarske cijele brojeve.*

Lema 2.6. *Neka je α algebarski cijeli broj s minimalnim polinomom $Q(X) = X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d$. Tada za svaki $\ell \in \mathbb{N}_0$ postoje cijeli brojevi $a_1^{(\ell)}, \ldots, a_d^{(\ell)}$ takvi da je*

$$\alpha^\ell = a_1^{(\ell)}\alpha^{d-1} + \cdots + a_{d-1}^{(\ell)}\alpha + a_d^{(\ell)},$$

a pritom vrijedi

$$\left|a_i^{(\ell)}\right| \leq \big(\mathrm{H}(Q) + 1\big)^\ell \qquad (1 \leq i \leq d).$$

Dokaz. Lemu dokazujemo indukcijom po ℓ. Tvrdnja je trivijalno ispunjena za $\ell < d$. Pretpostavimo da lema vrijedi za $\ell - 1$. Imamo

$$\begin{aligned}
\alpha^\ell &= \alpha^{\ell-1} \cdot \alpha = \Big(a_1^{(\ell-1)}\alpha^{d-1} + \cdots + a_d^{(\ell-1)}\Big)\alpha \\
&= a_1^{(\ell-1)}\alpha^d + a_2^{(\ell-1)}\alpha^{d-1} + \cdots + a_d^{(\ell-1)}\alpha \\
&= a_1^{(\ell-1)}\big(-a_1\alpha^{d-1} - \cdots - a_{d-1}\alpha - a_d\big) + a_2^{(\ell-1)}\alpha^{d-1} + \cdots + a_d^{(\ell-1)}\alpha \\
&= \Big(a_2^{(\ell-1)} - a_1a_1^{(\ell-1)}\Big)\alpha^{d-1} + \cdots + \Big(a_d^{(\ell-1)} - a_{d-1}a_1^{(\ell-1)}\Big)\alpha - a_da_1^{(\ell-1)},
\end{aligned}$$

pa je

$$\alpha^\ell = a_1^{(\ell)}\alpha^{d-1} + \cdots + a_{d-1}^{(\ell)}\alpha + a_d^{(\ell)}$$

uz očite oznake. Za svaki i, $1 \leq i \leq d$, imamo ocjenu

$$\left|a_i^{(\ell)}\right| \leq \big(\mathrm{H}(Q) + 1\big)^{\ell-1} + \mathrm{H}(Q)\big(\mathrm{H}(Q) + 1\big)^{\ell-1} = \big(\mathrm{H}(Q) + 1\big)^\ell.$$ ■

2.3 Indeks polinoma

Neka je $P(X_1, \ldots, X_m)$ polinom s cjelobrojnim koeficijentima, neka su $r_1, \ldots, r_m$ prirodni brojevi i neka je $(\alpha_1, \ldots, \alpha_m)$ proizvoljna točka iz $\mathbb{R}^m$.

Definicija. Pretpostavimo najprije da je $P \not\equiv 0$.
Indeks od P s obzirom na[2] $(\alpha_1, \ldots, \alpha_m; r_1, \ldots, r_m)$ je najmanja vrijednost od

$$\frac{i_1}{r_1} + \cdots + \frac{i_m}{r_m}$$

za koju $P_{i_1 \ldots i_m}(\alpha_1, \ldots, \alpha_m)$ ne iščezava. Indeks od P označavamo $\operatorname{Ind}(P)$. Dakle,

$$\operatorname{Ind}(P) := \inf \left\{ \sum_{h=1}^{m} \frac{i_h}{r_h} : P_{\underline{\underline{i}}}(\alpha_1, \ldots, \alpha_m) \neq 0 \right\}. \tag{2.16}$$

Ako je $P \equiv 0$, definiramo da je indeks od P jednak $+\infty$.

Pogledamo li Taylorov razvoj od P oko $(\alpha_1, \ldots, \alpha_m)$,

$$P(X_1, \ldots, X_m) = \sum_{\substack{i_1, \ldots, i_m \\ 0 \leq i_h \leq \deg_h P \\ (1 \leq h \leq m)}} P_{\underline{\underline{i}}}(\alpha_1, \ldots, \alpha_m)(X_1 - \alpha_1)^{i_1} \cdots (X_m - \alpha_m)^{i_m},$$

vidimo da se indeks za $P \not\equiv 0$ postiže, pa je infimum u (2.16) zapravo minimum. $\operatorname{Ind}(P) = 0$ ako je $P(\alpha_1, \ldots, \alpha_m) \neq 0$. Ako P iščezava do visokog reda u $(\alpha_1, \ldots, \alpha_m)$, onda je i indeks velik. Indeks je neka vrsta mjere za iščezavanje od P. To opravdava i stavljanje $\operatorname{Ind}(P) = +\infty$ za $P \equiv 0$.

Lema 2.7. *Neka su $(\alpha_1, \ldots, \alpha_m) \in \mathbb{R}^m$ i $r_1, \ldots, r_m \in \mathbb{N}$. S obzirom na ove parametre vrijedi:*

(i) $\operatorname{Ind} P_{\underline{\underline{i}}} \geq \operatorname{Ind} P - \sum_{h=1}^{m} \frac{i_h}{r_h}$,

(ii) $\operatorname{Ind}\left(P^{(1)} + P^{(2)}\right) \geq \min\left\{\operatorname{Ind} P^{(1)}, \operatorname{Ind} P^{(2)}\right\}$,

(iii) $\operatorname{Ind}\left(P^{(1)} P^{(2)}\right) = \operatorname{Ind} P^{(1)} + \operatorname{Ind} P^{(2)}$.

Dokaz.
(i) Neka je $T = P_{\underline{\underline{i}}}$ te pretpostavimo da je $T_{\underline{\underline{j}}}(\alpha_1, \ldots, \alpha_m) \neq 0$ za neki $\underline{\underline{j}}$. Tada je[3] $P_{\underline{\underline{i}}+\underline{\underline{j}}}(\alpha_1, \ldots, \alpha_m) \neq 0$, pa slijedi

$$\frac{i_1 + j_1}{r_1} + \cdots + \frac{i_m + j_m}{r_m} \geq \operatorname{Ind} P, \quad \text{tj.}$$

$$\frac{j_1}{r_1} + \cdots + \frac{j_m}{r_m} \geq \operatorname{Ind} P - \sum_{h=1}^{m} \frac{i_h}{r_h},$$

[2] Ponekad se govori: *indeks od P u točki $(\alpha_1, \ldots, \alpha_m)$ s obzirom na $(r_1, \ldots, r_m)$*.
[3] Primjetimo da je $T_{\underline{\underline{j}}} = (P_{\underline{\underline{i}}})_{\underline{\underline{j}}} = c P_{\underline{\underline{i}}+\underline{\underline{j}}}$, gdje je $c = \binom{i_1+j_1}{i_1} \cdots \binom{i_m+j_m}{i_m}$.

iz čega dobivamo

$$\operatorname{Ind} T \geq \operatorname{Ind} P - \sum_{h=1}^{m} \frac{i_h}{r_h}.$$

(ii) Pretpostavimo da je $\big(P^{(1)} + P^{(2)}\big)_{\underline{\underline{j}}}(\alpha_1, \ldots, \alpha_m) \neq 0$. Tada je

$$P^{(1)}_{\underline{\underline{j}}}(\alpha_1, \ldots, \alpha_m) \neq 0 \quad \text{ili} \quad P^{(2)}_{\underline{\underline{j}}}(\alpha_1, \ldots, \alpha_m) \neq 0, \qquad \text{pa je}$$
$$\frac{j_1}{r_1} + \cdots + \frac{j_m}{r_m} \geq \operatorname{Ind} P^{(1)} \quad \text{ili} \quad \frac{j_1}{r_1} + \cdots + \frac{j_m}{r_m} \geq \operatorname{Ind} P^{(2)}.$$

Zaključujemo da je

$$\operatorname{Ind}\big(P^{(1)} + P^{(2)}\big) \geq \min\big\{\operatorname{Ind} P^{(1)}, \operatorname{Ind} P^{(2)}\big\}.$$

(iii) Uz očitu notaciju, vrijedi

$$\big(P^{(1)}P^{(2)}\big)_{\underline{\underline{j}}} = \sum_{\underline{\underline{i}}+\underline{\underline{i}}'=\underline{\underline{j}}} C(\underline{\underline{i}}, \underline{\underline{i}}') P^{(1)}_{\underline{\underline{i}}} P^{(2)}_{\underline{\underline{i}}'} \tag{2.17}$$

za svaku cjelobrojnu točku $\underline{\underline{j}} = (j_1, \ldots, j_m)$ kojoj je $j_h \geq 0$ $(1 \leq h \leq m)$.[4]

Neka je sad $\underline{\underline{j}}$ izabran tako da bude $\sum_{h=1}^{m} \frac{j_h}{r_h} = \operatorname{Ind}\big(P^{(1)}P^{(2)}\big)$ i $\big(P^{(1)}P^{(2)}\big)_{\underline{\underline{j}}}(\alpha_1, \ldots, \alpha_m) \neq 0$. Zbog (2.17) postoje $\underline{\underline{i}}$ i $\underline{\underline{i}}'$ za koje je $\underline{\underline{i}}+\underline{\underline{i}}' = \underline{\underline{j}}$ te vrijedi $P^{(1)}_{\underline{\underline{i}}}(\alpha_1, \ldots, \alpha_m) \neq 0$ i $P^{(2)}_{\underline{\underline{i}}'}(\alpha_1, \ldots, \alpha_m) \neq 0$. Tada je $\sum_{h=1}^{m} \frac{i_h}{r_h} \geq \operatorname{Ind} P^{(1)}$ i $\sum_{h=1}^{m} \frac{i'_h}{r_h} \geq \operatorname{Ind} P^{(2)}$, pa dobivamo

$$\operatorname{Ind}\big(P^{(1)}P^{(2)}\big) = \sum_{h=1}^{m} \frac{j_h}{r_h} = \sum_{h=1}^{m} \frac{i_h}{r_h} + \sum_{h=1}^{m} \frac{i'_h}{r_h} \geq \operatorname{Ind} P^{(1)} + \operatorname{Ind} P^{(2)}. \tag{2.18}$$

S druge strane, postoje m-torke $\underline{\underline{i}}$ za koje je $\sum_{h=1}^{m} \frac{i_h}{r_h} = \operatorname{Ind} P^{(1)}$ i $P^{(1)}_{\underline{\underline{i}}}(\alpha_1, \ldots, \alpha_m) \neq 0$. Od ovih $\underline{\underline{i}}$, neka je $\overline{\underline{\underline{i}}} = \big(\overline{i}_1, \ldots, \overline{i}_m\big)$ prva po leksikografskom uređaju. Analogno, neka je $\overline{\underline{\underline{i}}'} = \big(\overline{i'}_1, \ldots, \overline{i'}_m\big)$ leksikografski prva m-torka $\underline{\underline{i}}'$ za koju vrijedi $\sum_{h=1}^{m} \frac{i'_h}{r_h} = \operatorname{Ind} P^{(2)}$ i $P^{(2)}_{\underline{\underline{i}}'} \neq 0$. Stavimo li $\underline{\underline{j}} = \overline{\underline{\underline{i}}} + \overline{\underline{\underline{i}}'}$, iz (2.17) slijedi

$$\big(P^{(1)}P^{(2)}\big)_{\underline{\underline{j}}}(\alpha_1, \ldots, \alpha_m) = C\big(\overline{\underline{\underline{i}}}, \overline{\underline{\underline{i}}'}\big) P^{(1)}_{\overline{\underline{\underline{i}}}}(\alpha_1, \ldots, \alpha_m) P^{(2)}_{\overline{\underline{\underline{i}}'}}(\alpha_1, \ldots, \alpha_m) \neq 0.$$

Ovo dokazuje obratnu nejednakost u (2.18). ■

[4] Zapravo, može se pokazati da je $C(\underline{\underline{i}}, \underline{\underline{i}}') = 1$, tj.

$$\Big(\frac{\partial}{\partial X_1}\Big)^{j_1} \cdots \Big(\frac{\partial}{\partial X_m}\Big)^{j_m} \big(P^{(1)}P^{(2)}\big) =$$
$$= \sum_{i_1=0}^{j_1} \cdots \sum_{i_m=0}^{j_m} \binom{j_1}{i_1} \cdots \binom{j_m}{i_m} \Big(\Big(\frac{\partial}{\partial X_1}\Big)^{i_1} \cdots \Big(\frac{\partial}{\partial X_m}\Big)^{i_m} P^{(1)}\Big) \Big(\Big(\frac{\partial}{\partial X_1}\Big)^{j_1-i_1} \cdots \Big(\frac{\partial}{\partial X_m}\Big)^{j_m-i_m} P^{(2)}\Big).$$

Ovo je očita prednost našeg $P_{\underline{\underline{i}}}$ u odnosu na samo parcijalne derivacije.

2.4 Teorem o indeksu

Teorem 2.8. *Neka je α algebarski cijeli broj stupnja $d \geq 2$ i neka je $\varepsilon > 0$, a m cijeli broj koji zadovoljava nejednakost*

$$m > \frac{16 \log 4d}{\varepsilon^2}. \tag{2.19}$$

Nadalje, neka su $r_1, \ldots, r_m$ prirodni brojevi.

Tada postoji polinom $P(X_1, \ldots, X_m) \not\equiv 0$ s cjelobrojnim koeficijentima takav da vrijedi:

(i) P *je stupnja* $\leq r_h$ *u* X_h $(1 \leq h \leq m)$,

(ii) P *ima indeks* $\geq \frac{m}{2}(1-\varepsilon)$ *s obzirom na* $(\alpha, \alpha, \ldots, \alpha; r_1, \ldots, r_m)$ *i*

(iii) $\mathrm{H}(P) \leq B^{r_1+\cdots+r_m}$, *gdje je* $B = B(\alpha)$ *neka konstanta (koja ovisi samo o* α*).*

Dokaz. Tražimo polinom

$$P(X_1, \ldots, X_m) = \sum_{j_1=0}^{r_1} \cdots \sum_{j_m=0}^{r_m} C(j_1, \ldots, j_m) X_1^{j_1} \cdots X_m^{j_m}$$

s cjelobrojnim koeficijentima $C(j_1, \ldots, j_m)$ tako da su ispunjeni uvjeti (ii) i (iii). Koeficijenata ima

$$N = (r_1 + 1) \cdots (r_m + 1)$$

i to su cijeli brojevi koje trebamo odrediti. Prema (ii) mora

$$P_{\underline{i}}(\alpha, \alpha, \ldots, \alpha) = 0 \tag{2.20}$$

vrijediti čim je

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

Iz leme 2.1 slijedi da je broj takvih m-torki $\underline{i}$ najviše $(r_1+1) \cdots (r_m+1) \cdot 2e^{\frac{-\varepsilon^2 m}{16}}$. Zato je broj uvjeta izraženih u jednadžbama oblika (2.20) najviše

$$N \cdot 2e^{-\frac{\varepsilon^2 m}{16}} \overset{(2.19)}{\leq} N \cdot \frac{2}{4d} = \frac{N}{2d}.$$

Svaki od uvjeta (2.20) je linearna jednadžba u nepoznanicama $C(j_1, \ldots, j_m)$. Koeficijenti ovih jednadžbi su umnošci cijelih brojeva i potencija od α, pa su algebarski. Ali, svaka potencija od α je linearna kombinacija od $1, \alpha, \ldots, \alpha^{d-1}$ s cjelobrojnim koeficijentima. Kako su brojevi $1, \alpha, \ldots, \alpha^{d-1}$ linearno nezavisni nad $\mathbb{Q}$, vidimo da je svaki od uvjeta (2.20) ekvivalentan s d linearnih relacija u $C(j_1, \ldots, j_m)$ s cjelobrojnim koeficijentima. Sve zajedno dobivamo

$$M \leq d \cdot \frac{N}{2d} = \frac{N}{2} \tag{2.21}$$

linearnih jednadžbi za $C(j_1,\dots,j_m)$ kojima su koeficijenti cijeli brojevi.

Neka je A maksimum apsolutnih vrijednosti ovih cjelobrojnih koeficijenata. Za svaki $C(j_1,\dots,j_m)$ u (2.20), koeficijenti o kojim govorimo imaju apsolutnu vrijednost najviše

$$\binom{j_1}{i_1}\cdots\binom{j_m}{i_m}\big(\mathrm{H}(Q)+1\big)^{\ell}\le 2^{j_1+\cdots+j_m}\big(\mathrm{H}(Q)+1\big)^{\ell}$$

prema lemi 2.6. Ovdje je $Q(X)$ minimalni polinom od α i $\ell=(j_1-i_1)+\cdots+(j_m-i_m)$. Stoga je

$$A\le\Big(2\big(\mathrm{H}(Q)+1\big)\Big)^{r_1+\cdots+r_m}. \tag{2.22}$$

Prema lemi 2.5, naš sustav linearnih jednadžbi ima netrivijalno cjelobrojno rješenje takvo da je

$$|C(j_1,\dots,j_m)|\le\Big\lfloor(NA)^{\frac{M}{N-M}}\Big\rfloor\le(NA)^{\frac{M}{N-M}}\overset{(2.21)}{\le}NA=(r_1+1)\cdots(r_m+1)A$$
$$\overset{\substack{r+1\le 2^r\\(2.22)}}{\le}2^{r_1+\cdots+r_m}\Big(2\big(\mathrm{H}(Q)+1\big)\Big)^{r_1+\cdots+r_m}=B^{r_1+\cdots+r_m}.$$

za svaku m-torku $(j_1,\dots,j_m)$. Polinom P s ovim koeficijentima $C(j_1,\dots,j_m)$ zadovoljava

$$\mathrm{H}(P)\le B^{r_1+\cdots+r_m},$$

gdje je $B=B(\alpha)=4\big(\mathrm{H}(Q)+1\big)$. ■

Konstrukcija polinoma P u ovom odjeljku odgovara dijelu (a) u dokazu Liouvilleovog teorema 1.13. Idući odjeljak će odgovarati dijelu (b).

2.5 Indeks od $P(X_1,\dots,X_m)$ u racionalnim točkama bliskim $(\alpha,\alpha,\dots,\alpha)$

Neka je α algebarski cijeli broj stupnja $d\ge 2$. Za svaki $\varepsilon>0$, neka je $m=m(\alpha,\varepsilon)$ cijeli broj koji zadovoljava

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

Neka su $r_1,\dots,r_m$ prirodni brojevi i neka je P polinom koji ispunjava zaključke teorema 2.8.

Teorem 2.9. *Neka je $0<\delta<1$ i*

$$0<\varepsilon<\frac{\delta}{36}. \tag{2.23}$$

Neka su $\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}$ racionalne aproksimacije od α tako da je

$$\left|\alpha-\frac{p_h}{q_h}\right|\le\frac{1}{q_h^{2+\delta}}\qquad(1\le h\le m) \tag{2.24}$$

i

$$q_h^{\delta} > D, \qquad (1 \le h \le m) \tag{2.25}$$

gdje je $D = D(\alpha) > 0$. *Nadalje, pretpostavimo da vrijedi*

$$r_1 \log q_1 \le r_h \log q_h \le (1+\varepsilon) r_1 \log q_1 \qquad (1 \le h \le m). \tag{2.26}$$

Tada indeks od P *s obzirom na* $\left(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}; r_1, \dots, r_m\right)$ *mora biti* $\ge \varepsilon m$.

Dokaz. Neka su $j_1, \dots, j_m$ nenegativni cijeli brojevi tako da je

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

Stavimo $T(X_1, \dots, X_m) = P_{\underline{j}}(X_1, \dots, X_m)$, gdje je $\underline{j} = (j_1, \dots, j_m)$. Trebamo pokazati da je $T\left(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}\right) = 0$.

Prema teoremu o indeksu (teorem 2.8) imamo

$$\mathrm{H}(P) \le B^{r_1+\cdots+r_m}, \qquad B = B(\alpha)$$

iz čega je

$$\mathrm{H}(T) \le (2B)^{r_1+\cdots+r_m}$$

zbog leme 2.4. Ponovno primjenjujući lemu 2.4, dobivamo

$$\mathrm{H}(T_{\underline{i}}) \le (4B)^{r_1+\cdots+r_m}$$

za svaku m-torku $\underline{i} = (i_1, \dots, i_m)$ nenegativnih cijelih brojeva. Zato u $T_{\underline{i}}(\alpha, \alpha, \dots, \alpha)$ svaki monom ima apsolutnu vrijednost

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

Budući da je $T_{\underline{i}}$ suma od najviše

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

monoma, slijedi

$$\left|T_{\underline{i}}(\alpha, \alpha, \dots, \alpha)\right| \le \left(8B \max\{1, |\alpha|\}\right)^{r_1+\cdots+r_m} = C^{r_1+\cdots+r_m}, \tag{2.27}$$

gdje je $C = C(\alpha) = 8B \max\{1, |\alpha|\}$.

Prema teoremu o indeksu, indeks od P s obzirom na $(\alpha, \alpha, \dots, \alpha; r_1, \dots, r_m)$ je $\ge \frac{m}{2}(1-\varepsilon)$. Iz dijela (i) leme 2.7 zaključujemo da je indeks od T s obzirom na $(\alpha, \alpha, \dots, \alpha; r_1, \dots, r_m)$ nužno

$$\ge \frac{m}{2}(1-\varepsilon) - \sum_{h=1}^{m} \frac{j_h}{r_h} > \frac{m}{2}(1-3\varepsilon).$$

Upotrebom Taylorove formule dobivamo

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

Iz prethodnog odlomka vidimo da pribrojnici iščezavaju ako nije $\sum_{h=1}^{m}\frac{i_h}{r_h}>\frac{m}{2}(1-3\varepsilon)$. Uključimo li nejednakosti (2.24) i (2.27), polučujemo

$$\left|T\Big(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\Big)\right|\le\sum_{\underline{i}}{}'C^{r_1+\dots+r_m}\big(q_1^{i_1}q_2^{i_2}\cdots q_m^{i_m}\big)^{-2-\delta},\tag{2.28}$$

gdje $\sum'$ označava da se sumira po svim m-torkama $(i_1,\dots,i_m)$ cijelih brojeva, $0\le i_h\le r_h$ $(1\le h\le m)$, za koje je $\sum_{h=1}^{m}\frac{i_h}{r_h}>m\big(\frac12-2\varepsilon\big)$.

Za takve m-torke zbog (2.26) i (2.23) vrijedi

$$\begin{aligned}q_1^{i_1}q_2^{i_2}\cdots q_m^{i_m}&=q_1^{r_1\frac{i_1}{r_1}}q_2^{r_2\frac{i_2}{r_2}}\cdots q_m^{r_m\frac{i_m}{r_m}}\overset{(2.26)}{\ge}q_1^{r_1\left(\frac{i_1}{r_1}+\dots+\frac{i_m}{r_m}\right)}\\&>q_1^{r_1m\left(\frac12-2\varepsilon\right)}\overset{(2.26)}{\ge}\big(q_1^{r_1}q_2^{r_2}\cdots q_m^{r_m}\big)^{\frac{\frac12-2\varepsilon}{1+\varepsilon}}\\&\overset{(2.23)}{>}\big(q_1^{r_1}q_2^{r_2}\cdots q_m^{r_m}\big)^{\frac12(1-6\varepsilon)}.\end{aligned}$$

Broj pribrojnika u (2.28) je $\le(r_1+1)\cdots(r_m+1)\le 2^{r_1+\dots+r_m}$, pa vrijedi

$$\begin{aligned}\left|T\Big(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\Big)\right|&\le 2^{r_1+\dots+r_m}C^{r_1+\dots+r_m}\big(q_1^{r_1}q_2^{r_2}\cdots q_m^{r_m}\big)^{-\frac12(1-6\varepsilon)(2+\delta)}\\&=\prod_{h=1}^{m}\Big(2Cq_h^{-\frac12(1-6\varepsilon)(2+\delta)}\Big)^{r_h}.\end{aligned}\tag{2.29}$$

U skladu s (2.23) je

$$\frac12(1-6\varepsilon)(2+\delta)=1+\frac{\delta}{2}-6\varepsilon-3\varepsilon\delta\overset{\delta<1}{>}1+\frac{\delta}{2}-9\varepsilon\overset{(2.23)}{>}1+\frac{\delta}{4},$$

pa imamo

$$2Cq_h^{-\frac12(1-6\varepsilon)(2+\delta)}<2Cq_h^{-1-\frac{\delta}{4}}<q_h^{-1},$$

ako je $q_h^{\delta}>(2C)^4$, a to je prema (2.25) točno ako stavimo $D=(2C)^4$. Iz (2.29) sada je

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

Prisjetimo se da P, a onda i T, ima stupanj $\le r_h$ u X_h $(1\le h\le m)$. Zato je

$$T\Big(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m}\Big)=\frac{N}{q_1^{r_1}q_2^{r_2}\cdots q_m^{r_m}}$$

za neki cijeli broj N. No, prethodna nejednakost pokazuje da je $N = 0$. Stoga je

$$T\Big(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\Big) = 0. \qquad \blacksquare$$

Dio (c) u dokazu Liouvilleovog teorema bio je trivijalan. U ovom kontekstu taj dio je najteži i bit će razriješen u Rothovoj lemi, §2.7.

2.6 Generalizirani Wronskijani

Neka su $\varphi_1, \ldots, \varphi_k$ racionalne funkcije u m varijabli $X_1, \ldots, X_m$. Promatramo diferencijalne operatore

$$\Delta = \frac{\partial^{i_1+\cdots+i_m}}{\partial {X_1}^{i_1} \cdots \partial {X_m}^{i_m}}.$$

Red takvog diferencijalnog operatora je $i_1 + \cdots + i_m$.

Definicija. *Generalizirani Wronskijan* od $\varphi_1, \ldots, \varphi_k$ je svaka determinanta oblika

$$\det(\Delta_i \varphi_j)_{1 \le i,j \le k} \tag{2.30}$$

gdje su $\Delta_1, \ldots, \Delta_k$ operatori kao gore, a red od Δ_i je $\le i - 1$ $(1 \le i \le k)$.[5]

Napomena.
Uzmimo $m = 1$. Tada je Δ_1 identitetski operator, Δ_2 je identiteta ili $\frac{\partial}{\partial X}$, Δ_3 je identiteta ili $\frac{\partial}{\partial X}$ ili $\frac{\partial^2}{\partial X^2}$ itd. Kako generalizirani Wronskijan (2.30) ne bi svuda iščezavao, nužno je da bude Δ_1 identiteta, $\Delta_2 = \frac{\partial}{\partial X}$, $\Delta_3 = \frac{\partial^2}{\partial X^2}$, ... U ovom slučaju (2.30) postaje

$$\det \begin{pmatrix} \varphi_1 & \varphi_2 & \cdots & \varphi_k \\ \varphi_1' & \varphi_2' & \cdots & \varphi_k' \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_1^{(k-1)} & \varphi_2^{(k-1)} & \cdots & \varphi_k^{(k-1)} \end{pmatrix},$$

a to je (obični) Wronskijan od $\varphi_1, \ldots, \varphi_k$.

Lema 2.10. *Neka su $\varphi_1, \ldots, \varphi_k$ racionalne funkcije u varijablama $X_1, \ldots, X_m$ s realnim koeficijentima i neka su te funkcije linearno nezavisne nad $\mathbb{R}$. Tada bar jedan generalizirani Wronskijan od $\varphi_1, \ldots, \varphi_k$ nije identički jednak 0.*

Napomena.
Obrat leme 2.10 je trivijalno istinit: ako su $\varphi_1, \ldots, \varphi_k$ linearno zavisne nad skupom realnih brojeva, onda su svi generalizirani Wronskijani identički jednaki 0.

[5] Primjetimo da se, osim u konstanti, ovaj diferencijalni operator i onaj u (2.12) razlikuju i u označavanju. Naime, ovdje nam je indeks u Δ_i skalar i koji omeđuje red diferencijalnog operatora, pa ovakvo označavanje nije jednoznačno. U (2.12) je u indeksu bio vektor koji je određivao jedinstveni diferencijalni operator.

Dokaz. Provodimo dokaz indukcijom po k.

Za $k = 1$ je Δ_1 nužno identiteta, a generalizirani Wronskijan je φ_1. Ali φ_1 je linearno nezavisna nad $\mathbb{R}$, pa je $\varphi_1 \neq 0$.

Neka su sada $\varphi_1, \ldots, \varphi_k$ $(k \geq 2)$ racionalne funkcije koje zadovoljavaju uvjete leme. Neka je Ω proizvoljna racionalna funkcija u $X_1, \ldots, X_m$ s realnim koeficijentima, $\Omega \neq 0$. Promotrimo funkcije

$$\varphi_i^* = \Omega\varphi_i \qquad (1 \leq i \leq k).$$

Tada su $\varphi_1^*, \ldots, \varphi_k^*$ također linearno nezavisne nad $\mathbb{R}$. Svaki generalizirani Wronskijan od $\varphi_1^*, \ldots, \varphi_k^*$ je linearna kombinacija generaliziranih Wronskijana od $\varphi_1, \ldots, \varphi_k$. (Koeficijenti u ovoj linearnoj kombinaciji su racionalne funkcije koje sadrže parcijalne derivacije od Ω.) Zato je za dokaz leme dovoljno pokazati da neki generalizirani Wronskijan od $\varphi_1^*, \ldots, \varphi_k^*$ ne iščezava. Ako stavimo $\Omega = \varphi_1^{-1}$, onda je $\varphi_1^* = 1$, $\varphi_2^* = \frac{\varphi_2}{\varphi_1}$, $\ldots$, $\varphi_k^* = \frac{\varphi_k}{\varphi_1}$. To nam pokazuje da nije nikakvo smanjenje općenitosti pretpostaviti da je u našem popisu racionalnih funkcija $\varphi_1, \ldots, \varphi_k$, funkcija φ_1 identički jednaka 1.

Skup svih linearnih kombinacija

$$c_1\varphi_1 + \cdots + c_k\varphi_k$$

s realnim koeficijentima $c_1, \ldots, c_k$ čini realni vektorski prostor V dimenzije k. Budući da je $k > 1$, a $\varphi_1 = 1$ i φ_2 su linearno nezavisne, funkcija φ_2 nije konstantna. Stoga je $\frac{\partial\varphi_2}{\partial X_j} \neq 0$ za neki j (v. npr. [Un 94]). Bez smanjenja općenitosti možemo pretpostaviti da je $\frac{\partial\varphi_2}{\partial X_1} \neq 0$. Neka je W potprostor od V koji sadrži sve elemente $c_1\varphi_1 + \cdots + c_k\varphi_k$ za koje je

$$\frac{\partial}{\partial X_1}(c_1\varphi_1 + \cdots + c_k\varphi_k) = 0.$$

W je pravi potprostor, tj. $W \neq \{0\}$ jer je $\varphi_1 \in W$ i $W \neq V$ jer $\varphi_2 \notin W$. Prema tome, ako stavimo $t = \dim W$, onda je $1 \leq t \leq k-1$.

Izaberimo racionalne funkcije $\psi_1, \ldots, \psi_k$ tako da je $(\psi_1, \ldots, \psi_t)$ baza za W, a $(\psi_1, \ldots, \psi_k)$ baza za V. Prema pretpostavci indukcije, postoje operatori $\Delta_1^*, \ldots, \Delta_t^*$ reda $\leq 0, 1, \ldots, t-1$, respektivno, tako da je

$$W_1 = \det(\Delta_i^*\psi_j)_{1\leq i,j\leq t} \neq 0.$$

Ako su $c_{t+1}, \ldots, c_k$ realni brojevi koji nisu svi jednaki 0, onda je

$$\frac{\partial}{\partial X_1}(c_{t+1}\psi_{t+1} + \cdots + c_k\psi_k) \neq 0.$$

Ovo vrijedi jer potprostor razapet sa $\{\psi_{t+1}, \ldots, \psi_k\}$ ima u presjeku s W samo konstantnu funkciju 0. Drugim riječima, racionalne funkcije

$$\frac{\partial}{\partial X_1}\psi_{t+1}, \ldots, \frac{\partial}{\partial X_1}\psi_k$$

su linearno nezavisne nad $\mathbb{R}$. Pretpostavka indukcije povlači da postoje operatori Δ_{t+1}^*, $\ldots, \Delta_k^*$ reda $\leq 0, 1, \ldots, k-t-1$, respektivno, za koje je

$$W_2 = \det\left(\Delta_i^* \frac{\partial}{\partial X_1}\psi_j\right)_{t<i,j\leq k} \neq 0$$

Definiramo operatore Δ_i $(1 \leq i \leq k)$ na sljedeći način:

$$\Delta_i = \begin{cases} \Delta_i^* & \text{za} \quad 1 \leq i \leq t, \\ \Delta_i^* \frac{\partial}{\partial X_1} & \text{za} \quad t < i \leq k. \end{cases}$$

Primjetimo da je svaki Δ_i reda $\leq i-1$. Imamo

$$\begin{aligned} \det(\Delta_i\psi_j)_{1\leq i,j\leq k} &= \det \begin{pmatrix} \Delta_i^*\psi_j & \Delta_i^*\psi_j \\ 0 & \Delta_i^*\frac{\partial}{\partial X_1}\psi_j \end{pmatrix} \begin{matrix} 1\leq i\leq t \\ t<i\leq k \end{matrix} \\ &\quad \begin{matrix} 1\leq j\leq t & t<j\leq k \end{matrix} \\ &= W_1 W_2 \neq 0. \end{aligned}$$

Kako je $(\psi_1, \ldots, \psi_k)$ baza vektorskog prostora razapetog sa $(\varphi_1, \ldots, \varphi_k)$, slijedi[6]

$$\det(\Delta_i\varphi_j)_{1\leq i,j\leq k} \neq 0. \qquad \blacksquare$$

2.7 Rothova lema

Teorem 2.11. *Neka je*

$$0 < \varepsilon < \frac{1}{12}. \tag{2.31}$$

Neka je $m \in \mathbb{N}$ fiksan. Stavimo

$$\omega = \omega(m, \varepsilon) = 24 \cdot 2^{-m}\left(\frac{\varepsilon}{12}\right)^{2^{m-1}}. \tag{2.32}$$

Neka su $r_1, \ldots, r_m$ prirodni brojevi za koje vrijedi

$$\omega r_h \geq r_{h+1} \qquad (1 \leq h < m). \tag{2.33}$$

[6]Neka je A matrica prijelaza iz baze $(\psi_1, \ldots, \psi_k)$ u bazu $(\varphi_1, \ldots, \varphi_k)$. To znači da je i-ti stupac od A koordinatni prikaz vektora φ_i u bazi $(\psi_1, \ldots, \psi_k)$. Matrica A je očito regularna i vrijedi

$$\begin{pmatrix} \varphi_1 \\ \vdots \\ \varphi_k \end{pmatrix} = A^\tau \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_k \end{pmatrix}$$

Sada koristeći linearnost diferencijalnih operatora nije teško pokazati

$$(\Delta_i\varphi_j)_{1\leq i,j\leq k} = (\Delta_i\psi_j)_{1\leq i,j\leq k} \cdot A,$$

pa iz Binet-Cauchyjevog teorema slijedi tražena tvrdnja.

Neka su $(p_1, q_1), \ldots, (p_m, q_m)$ *parovi relativno prostih cijelih brojeva tako da vrijedi*

$$q_h^{r_h} \geq q_1^{r_1} \qquad (1 \leq h \leq m), \tag{2.34}$$

$$q_h^{\omega} \geq 2^{3m} \qquad (1 \leq h \leq m). \tag{2.35}$$

Nadalje, pretpostavimo da je $P(X_1, \ldots, X_m) \neq 0$ *polinom stupnja* $\leq r_h$ *u* X_h $(1 \leq h \leq m)$ *s cjelobrojnim koeficijentima i visinom*

$$\mathrm{H}(P) \leq q_1^{\omega r_1}. \tag{2.36}$$

Tada indeks od P *s obzirom na* $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}; r_1, \ldots, r_m\right)$ *mora biti* $\leq \varepsilon$.

Dokaz. Provodimo dokaz indukcijom po m.

$\mathsf{m} = 1$. Možemo pisati

$$P(X) = \left(X - \frac{p_1}{q_1}\right)^{\ell} M(X),$$

gdje je $M(X)$ polinom s racionalnim koeficijentima za koji je $M\left(\frac{p_1}{q_1}\right) \neq 0$. Stoga je

$$P(X) = (q_1 X - p_1)^{\ell} R(X), \tag{2.37}$$

gdje je $R(X) = q_1^{-\ell} M(X)$. Gaussova lema povlači da $R(X)$ ima cjelobrojne koeficijente.

Sada iz (2.37) slijedi da je vodeći koeficijent od $P(X)$ djeljiv sa q_1^{ℓ}. Zato vrijedi

$$q_1^{\ell} \leq \mathrm{H}(P) \overset{(2.36)}{\leq} q_1^{\omega r_1} \overset{\substack{m=1 \\ (2.32)}}{=} q_1^{\varepsilon r_1},$$

pa je $\frac{\ell}{r_1} \leq \varepsilon$, jer je $q_1 > 1$ prema (2.35). Ali, $\frac{\ell}{r_1}$ je indeks od P s obzirom na $\left(\frac{p_1}{q_1}; r_1\right)$. Teorem, dakle, vrijedi za $m = 1$.

Korak indukcije $\mathsf{m} - 1 \Rightarrow \mathsf{m}$. Promotrimo dekompoziciju

$$P(X_1, \ldots, X_m) = \sum_{j=1}^{k} \varphi_j(X_1, \ldots, X_{m-1}) \psi_j(X_m), \tag{2.38}$$

gdje su $\varphi_1, \ldots, \varphi_k$ i $\psi_1, \ldots, \psi_k$ polinomi s racionalnim koeficijentima. Izaberimo dekompoziciju za koju je k minimalan. Uzmemo li u obzir mogućnost $\psi_j(X_m) = X_m^{j-1}$ $(1 \leq j \leq r_m + 1)$, vidimo da vrijedi

$$k \leq r_m + 1. \tag{2.39}$$

Funkcije $\varphi_1, \ldots, \varphi_k$ su linearno nezavisne nad $\mathbb{Q}$ budući da je izabrana dekompozicija u kojoj je k minimalan. U protivnom bi postojali racionalni brojevi $c_1, \ldots, c_k$ koji nisu svi 0, tako da je

$$c_1 \varphi_1 + \cdots + c_k \varphi_k = 0.$$

Ako bi, recimo, bilo $c_k \neq 0$, onda bismo imali

$$P = \sum_{j=1}^{k-1} \varphi_j\psi_j + \varphi_k\psi_k = \sum_{j=1}^{k-1} \varphi_j\psi_j - \frac{1}{c_k}\Big(\sum_{j=1}^{k-1} c_j\varphi_j\Big)\psi_k = \sum_{j=1}^{k-1} \varphi_j\Big(\psi_j - \frac{c_j}{c_k}\psi_k\Big),$$

što je u kontradikciji s minimalnošću od k.

No, vrijedi i više: funkcije $\varphi_1, \ldots, \varphi_k$ su linearno nezavisne nad $\mathbb{R}$. U dokazu te činjenice presudno je da su to polinomi s racionalnim koeficijentima.

Pretpostavimo da postoje $c_1, \ldots, c_k \in \mathbb{R}$, ne svi 0, tako da za polinome $\varphi_1, \ldots, \varphi_k \in \mathbb{Q}[X_1, \ldots, X_{m-1}]$ vrijedi $\sum_{j=1}^{k} c_j\varphi_j = 0$. Želimo pokazati da postoje $d_1, \ldots, d_k \in \mathbb{Q}$ tako da je $\sum_{j=1}^{k} d_j\varphi_j = 0$. Uzmemo li u obzir definiciju jednakosti dvaju polinoma i stavimo li da ima sveukupno n monoma različitih stupnjeva u ovim polinomima $\varphi_1, \ldots, \varphi_k$, vidimo da je sljedeća tvrdnja ekvivalentna onoj koju želimo dokazati:

Ako za matricu

$$A = \begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1k} \\ \vdots & & \vdots \\ \alpha_{n1} & \ldots & \alpha_{nk} \end{pmatrix} \in \mathbb{Q}^{n\times k}$$

postoji $\underline{\underline{c}} = (c_1, \ldots, c_k)^\tau \in \mathbb{R}^k\backslash\{\underline{\underline{0}}\}$ *takav da je* $A\underline{\underline{c}} = \underline{\underline{0}}$, *onda postoji i* $\underline{\underline{d}} \in \mathbb{Q}^k\backslash\{\underline{\underline{0}}\}$ *takav da je* $A\underline{\underline{d}} = \underline{\underline{0}}$. Drugim riječima,

$$\ker A \cap \big(\mathbb{R}^k\backslash\{\underline{\underline{0}}\}\big) \neq \varnothing \;\Rightarrow\; \ker A \cap \big(\mathbb{Q}^k\backslash\{\underline{\underline{0}}\}\big) \neq \varnothing.$$

Promatrajmo vektorski potprostor od $\mathbb{R}$ nad $\mathbb{Q}$ koji je generiran skupom $\{c_1, \ldots, c_k\}$. Bez smanjenja općenitosti možemo pretpostaviti da je $(c_1, \ldots, c_l)$ baza tog potprostora (inače renumeriramo vektore c_j). Tada postoje racionalni brojevi d_{i_1,i_2} $(l+1 \leq i_1 \leq k,\ 1 \leq i_2 \leq l)$ takvi da za matricu

$$D = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ d_{l+1,1} & \ldots & d_{l+1,l} \\ \vdots & & \vdots \\ d_{k,1} & \ldots & d_{k,l} \end{pmatrix} \in \mathbb{Q}^{k\times l}$$

(prvih k redova ove matrice čini jediničnu matricu reda l) i vektor $\widetilde{\underline{\underline{c}}} = (c_1, \ldots, c_l)^\tau \in \mathbb{R}^l$ vrijedi $\underline{\underline{c}} = D\widetilde{\underline{\underline{c}}}$, pa je $\underline{\underline{0}} = A\underline{\underline{c}} = AD\widetilde{\underline{\underline{c}}}$. Zbog linearne nezavisnosti od $\{c_1, \ldots, c_l\}$ nad $\mathbb{Q}$ je $AD = 0$. Sada za $\underline{\underline{d}}$ možemo uzeti bilo koji stupac iz D.

Analogno se pokazuje da su $\psi_1, \ldots, \psi_k$ linearno nezavisne nad $\mathbb{R}$.

Definirajmo

$$U(X_m) = \det\Big(\frac{1}{(i-1)!}\frac{\partial^{i-1}}{\partial {X_m}^{i-1}}\psi_j(X_m)\Big)_{1\le i,j\le k}.$$

Prema lemi 2.10 i napomeni koja joj prethodi,

$$U(X_m) \neq 0.$$

Također prema lemi 2.10, postoje operatori

$$\Delta_i' = \frac{1}{i_1!\cdots i_{m-1}!}\frac{\partial^{i_1+\cdots+i_{m-1}}}{\partial {X_1}^{i_1}\cdots\partial {X_{m-1}}^{i_{m-1}}} \qquad (1\le i\le k)$$

kojima su redovi

$$i_1+\cdots+i_{m-1} \le i-1 \le k-1 \overset{(2.39)}{\le} r_m \tag{2.40}$$

tako da je

$$V(X_1,\dots,X_{m-1}) := \det(\Delta_i'\varphi_j)_{1\le i,j\le k} \neq 0.$$

Stavimo

$$W(X_1,\dots,X_m) = \det\Big(\frac{1}{(j-1)!}\frac{\partial^{j-1}}{\partial {X_m}^{j-1}}\Delta_i' P\Big)_{1\le i,j\le k}.$$

Tada je

$$W(X_1,\dots,X_m) \overset{(2.38)}{=} \det\left(\sum_{r=1}^{k}\Big(\Delta_i'\varphi_r\cdot\frac{\partial^{j-1}}{(j-1)!\partial {X_m}^{j-1}}\psi_r\Big)\right)_{1\le i,j\le k}$$

$$= \det\Bigg(\begin{pmatrix}\Delta_1'\varphi_1 & \dots & \Delta_1'\varphi_k\\ \vdots & \ddots & \vdots\\ \Delta_k'\varphi_1 & \dots & \Delta_k'\varphi_k\end{pmatrix}\begin{pmatrix}\psi_1 & \dots & \psi_k\\ \frac{\partial}{\partial X_m}\psi_1 & \dots & \frac{\partial}{\partial X_m}\psi_k\\ \vdots & & \vdots\\ \frac{\partial^{k-1}}{(k-1)!\partial {X_m}^{k-1}}\psi_1 & \dots & \frac{\partial^{k-1}}{(k-1)!\partial {X_m}^{k-1}}\psi_k\end{pmatrix}^{\tau}\Bigg)$$

$$\overset{\substack{\text{Binet-Cauchyjev teorem}\\ \text{i } \det M^{\tau}=\det M}}{=} V(X_1,\dots,X_{m-1})U(X_m) \neq 0$$

Elementi u matrici čija determinanta definira W su oblika $P_{i_1\dots i_{m-1}j-1}$, pa ti elementi imaju cjelobrojne koeficijente. Zato je W polinom s cjelobrojnim koeficijentima. Prije nego što nastavimo dokaz, trebamo sljedeću lemu.

Lema 2.12. *Ako je Θ indeks od W s obzirom na $\big(\frac{p_1}{q_1},\dots,\frac{p_m}{q_m};r_1,\dots,r_m\big)$, onda vrijedi*

$$\Theta \le \frac{k\varepsilon^2}{6}.$$

Dokaz leme. Polinomi U i V imaju racionalne koeficijente koji nisu nužno cijeli. No, iz Gaussove leme zaključujemo da postoji faktorizacija

$$W(X_1,\dots,X_m) = V^*(X_1,\dots,X_{m-1})U^*(X_m),$$

gdje su U^* i V^* polinomi s cjelobrojnim koeficijentima.

Ocijenimo sada visine od U^* i V^*. Najprije imamo

$$\mathrm{H}(P_{i_1\dots i_{m-1}j-1}) \overset{\text{lema 2.4}}{\leq} 2^{r_1+\cdots+r_m}\,\mathrm{H}(P) \overset{(2.36)}{\leq} 2^{r_1+\cdots+r_m} q_1^{\omega r_1}.$$

Nadalje, broj članova u $P_{i_1\dots i_{m-1}j-1}$ je $\leq 2^{r_1+\cdots+r_m}$, a broj pribrojnika u razvoju determinante za W je

$$k! \leq k^{k-1} \overset{(2.39)}{\leq} k^{r_m} \leq 2^{kr_m}.$$

Slijedi

$$\mathrm{H}(W) \leq 2^{kr_m}(2^{r_1+\cdots+r_m}2^{r_1+\cdots+r_m}q^{\omega r_1})^k \leq (2^{3mr_1}q_1^{\omega r_1})^k,$$

jer je $r_1 \geq r_2 \geq \cdots \geq r_m$ prema (2.32) i (2.33). Iz (2.35) dobivamo

$$\mathrm{H}(W) \leq (q_1^{2\omega r_1})^k = q_1^{2\omega r_1 k}.$$

Ovo povlači ocjene[7]

$$\mathrm{H}(U^*) \leq q_1^{2\omega r_1 k} \overset{(2.34)}{\leq} q_m^{2\omega r_m k}, \qquad \mathrm{H}(V^*) \leq q_1^{2\omega r_1 k}. \tag{2.41}$$

Sada primjenjujemo pretpostavku indukcije. Točnije, primjenit ćemo teorem 2.11 za $m-1$ umjesto m, za $kr_1, \dots, kr_{m-1}$ umjesto $r_1, \dots, r_m$ i $\frac{\varepsilon^2}{12}$ umjesto ε, te sa $V^*(X_1, \dots, X_{m-1})$ umjesto $P(X_1, \dots, X_m)$. Pogledajmo zašto su ispunjeni uvjeti teorema u ovom slučaju. Nejednakosti (2.33) i (2.35) prema pretpostavci vrijede za $\omega = \omega(m, \varepsilon)$, pa pogotovo vrijede za $\omega\big(m-1, \frac{\varepsilon^2}{12}\big) = 2\omega(m, \varepsilon)$. Jasno je da vrijedi (2.34) i da je (2.31) ispunjeno za $\frac{\varepsilon^2}{12}$ umjesto ε. Ograda analogna (2.36) vrijedi prema (2.41) jer je

$$\mathrm{H}(V^*) \leq q_1^{\omega\left(m-1, \frac{\varepsilon^2}{12}\right)(kr_1)}.$$

Zaključujemo da je indeks od V^* s obzirom na $\big(\frac{p_1}{q_1}, \dots, \frac{p_{m-1}}{q_{m-1}}; kr_1, \dots, kr_{m-1}\big)$ nužno $\leq \frac{\varepsilon^2}{12}$, pa indeks od V^* s obzirom na $\big(\frac{p_1}{q_1}, \dots, \frac{p_{m-1}}{q_{m-1}}; r_1, \dots, r_{m-1}\big)$ mora biti $\leq \frac{k\varepsilon^2}{12}$. Ako sada V^* gledamo kao polinom u $X_1, \dots, X_m$, i dalje V^* ima indeks $\leq \frac{k\varepsilon^2}{12}$ s obzirom na $\big(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}; r_1, \dots, r_m\big)$.

Lako je provjeriti da su uvjeti iz Rothove leme ispunjeni i s $m = 1$, za kr_m umjesto $r_1, \dots, r_m$, za $\frac{\varepsilon^2}{12}$ umjesto ε i za $U^* = U^*(X_m)$ na mjestu $P(X_1, \dots, X_m)$. (Primjetimo da je $\omega\big(1, \frac{\varepsilon^2}{12}\big) \geq 2\omega(m, \varepsilon)$.) Budući da je Rothova lema dokazana u slučaju $m = 1$, U^* ima indeks $\leq \frac{k\varepsilon^2}{12}$ s obzirom na $\big(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}; r_1, \dots, r_m\big)$. Kako je $W = U^*V^*$, iz dijela (iii) leme 2.7 slijedi

$$\Theta \leq \frac{k\varepsilon^2}{12} + \frac{k\varepsilon^2}{12} = \frac{k\varepsilon^2}{6}.$$

[7] Važno je primjetiti da su U^* i V^* polinomi u različitim varijablama. Inače ne bismo iz $W = V^*U^*$ mogli zaključiti da je $\mathrm{H}(U^*) \leq \mathrm{H}(W)$ i $\mathrm{H}(V^*) \leq \mathrm{H}(W)$, npr. $(x^2+2x+1)(x-1) = x^3+x^2-x-1$.

Time je lema 2.12 dokazana. ■

Nastavak dokaza teorema 2.11. Neka θ označava indeks od P s obzirom na $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}; r_1, \ldots, r_m\right)$. Tada je

$$\begin{aligned}
\operatorname{Ind} P_{i_1 \ldots i_{m-1} j-1} &\geq \theta - \frac{i_1}{r_1} - \cdots - \frac{i_{m-1}}{r_{m-1}} - \frac{j-1}{r_m} && \text{prema lemi 2.7} \\
&\geq \theta - \frac{i_1 + \cdots + i_{m-1}}{r_{m-1}} - \frac{j-1}{r_m} && \text{jer je } r_1 \geq \cdots \geq r_{m-1} \\
&\geq \theta - \frac{r_m}{r_{m-1}} - \frac{j-1}{r_m} && \text{prema (2.40)} \\
&\geq \theta - \omega - \frac{j-1}{r_m} && \text{prema (2.33)} \\
&\geq \theta - \frac{\varepsilon^2}{24} - \frac{j-1}{r_m} && \text{prema (2.32) jer je } m \geq 2.
\end{aligned}$$

Kao što smo prije spomenuli, svaki element u j-tom stupcu determinante koja određuje W je oblika $P_{i_1 \ldots i_{m-1} j-1}$. Prisjetimo se identiteta

$$\operatorname{Ind} P^{(1)} P^{(2)} = \operatorname{Ind} P^{(1)} + \operatorname{Ind} P^{(2)}$$

i nejednakosti

$$\operatorname{Ind}\left(P^{(1)} + P^{(2)}\right) \geq \min\left\{ \operatorname{Ind} P^{(1)}, \operatorname{Ind} P^{(2)} \right\}$$

iz leme 2.7. Budući da je W zbroj umnožaka od po k faktora, po jedan iz svakog stupca, vidimo da je

$$\Theta = \operatorname{Ind} W \geq \sum_{j=1}^{k} \max\left\{\theta - \frac{\varepsilon^2}{24} - \frac{j-1}{r_m}, 0\right\} \geq -\frac{k\varepsilon^2}{24} + \sum_{i=0}^{k-1} \max\left\{\theta - \frac{i}{r_m}, 0\right\}.$$

Zato je

$$\sum_{i=0}^{k-1} \max\left\{\theta - \frac{i}{r_m}, 0\right\} \leq \Theta + \frac{k\varepsilon^2}{24} \overset{\text{lema 2.12}}{\leq} \frac{k\varepsilon^2}{6} + \frac{k\varepsilon^2}{24} < \frac{k\varepsilon^2}{4}. \tag{2.42}$$

Postoje dva slučaja:

Slučaj I. $\theta > \frac{k-1}{r_m}$. Tada (2.42) postaje

$$\frac{1}{2} k \left(\theta + \theta - \frac{k-1}{r_m}\right) < \frac{k\varepsilon^2}{4},$$

što je ekvivalentno

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

No, $\theta - \frac{k-1}{r_m} > 0$, pa je $\theta < \frac{\varepsilon^2}{2} < \varepsilon$.

Slučaj II. $\theta \le \frac{k-1}{r_m}$. Tada (2.42) postaje

$$\sum_{i=0}^{\lfloor \theta r_m \rfloor} \Big(\theta - \frac{i}{r_m}\Big) < \frac{k\varepsilon^2}{4},$$

što daje

$$\frac{1}{2}\theta\big(\lfloor \theta r_m \rfloor + 1\big) < \frac{k\varepsilon^2}{4},$$

a odatle je

$$\frac{1}{2}\theta^2 r_m < \frac{k\varepsilon^2}{4}.$$

Ali, $k \overset{(2.39)}{\le} r_m + 1 \le 2r_m$, pa je $\frac{1}{2}\theta^2 r_m < \frac{1}{2}\varepsilon^2 r_m$ i zato $\theta < \varepsilon$.

U oba slučaja dobivamo da indeks θ od P s obzirom na $\big(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}; r_1, \dots, r_m\big)$ mora biti $< \varepsilon$. Ovim je završen dokaz teorema 2.11. ■

2.8 Završetak dokaza Rothovog teorema

Kao što smo napomenuli u §2.2, možemo se ograničiti na algebarske cijele brojeve. Pretpostavimo da postoji $\delta > 0$ tako da jednadžba

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}} \tag{2.43}$$

ima beskonačno mnogo racionalnih rješenja, gdje je α algebarski cijeli broj stupnja $d \ge 2$. Nastavljamo nizom koraka.

(i) Bez smanjenja općenitosti možemo pretpostaviti da je $0 < \delta < 1$.

(ii) Uzmimo ε takav da je $0 < \varepsilon < \frac{\delta}{36}$. Ovo je nejednakost (2.23) koja povlači $0 < \varepsilon < \frac{1}{12}$, a to je nejednakost (2.31).

(iii) Uzmimo prirodan broj $m > 16\varepsilon^{-2}\log 4d$. Dakle, (2.19) vrijedi. Definiramo $\omega = \omega(m, \varepsilon)$ prema (2.32).

(iv) Neka je $\frac{p_1}{q_1}$ rješenje od (2.43) u kojem je $(p_1, q_1) = 1$, $q_1 > 0$, $q_1^{\omega} > B^m$, gdje je $B = B(\alpha)$ veličina iz teorema 2.8, te vrijede (2.25) i (2.35) za $h = 1$.

(v) Uzastopce izaberimo $\frac{p_2}{q_2}, \dots, \frac{p_m}{q_m}$ tako da vrijedi (2.43), $(p_h, q_h) = 1$, $q_h > 0$ $(2 \le h \le m)$ i

$$\omega \log q_{h+1} \ge 2 \log q_h \qquad (1 \le h \le m-1).$$

Ovo povlači $q_1 < q_2 < \cdots < q_m$, pa su (2.25) i (2.35) ispunjene za $h = 1, 2, \dots, m$.

(vi) Neka je r_1 dovoljno velik cijeli broj tako da je $\varepsilon r_1 \log q_1 \ge \log q_m$.

(vii) Za $2 \le h \le m$ stavimo

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

Tada za $2 \le h \le m$ imamo

$$r_1 \log q_1 \overset{\text{(vii)}}{<} r_h \log q_h \overset{\text{(vii)}}{\le} r_1 \log q_1 + \log q_h \overset{\text{(vi)}}{\le} (1+\varepsilon) r_1 \log q_1.$$

Ovo daje (2.26) i (2.34). Iz ovog niza nejednakosti slijedi

$$r_{h+1} \log q_{h+1} \le (1+\varepsilon) r_h \log q_h \qquad (1 \le h \le m-1).$$

Posljedica je

$$\omega r_h \ge \omega \frac{r_{h+1} \log q_{h+1}}{(1+\varepsilon) \log q_h} \overset{\text{(v)}}{\ge} \frac{2}{1+\varepsilon} r_{h+1} \qquad (1 \le h \le m-1),$$

pa je zbog (ii)

$$\omega r_h \ge r_{h+1} \qquad (1 \le h \le m-1),$$

što je (2.33). Primjetimo da zbog $\omega \le 1$ vrijedi i $r_1 \ge \cdots \ge r_m$.

Uvjeti teorema 2.8 (teorem o indeksu) su ispunjeni jer je (2.19) prema (iii) istinito. Neka je $P(X_1, \ldots, X_m)$ polinom koji zadovoljava zaključke teorema o indeksu. Uvjeti teorema 2.9 (tj. (2.23),(2.24),(2.25),(2.26)) vrijede. Zato je indeks od P s obzirom na $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}; r_1, \ldots, r_m\right)$ nužno

$$\ge \varepsilon m. \tag{2.44}$$

S druge strane, vrijede i uvjeti teorema 2.11 (tj. (2.31),(2.32),(2.33),(2.34), (2.35),(2.36)). Nejednakost (2.36) je ispunjena jer je

$$\mathrm{H}(P) \overset{\text{teorem 2.8}}{\le} B^{r_1 + \cdots + r_m} \le B^{m r_1} \overset{\text{(iv)}}{\le} q_1^{\omega r_1}.$$

Iz teorema 2.11 zaključujemo da indeks od P s obzirom na $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}; r_1, \ldots, r_m\right)$ mora biti $\le \varepsilon$. Ali ovo proturječi (2.44). Dobili smo traženu kontradikciju i Rothov teorem je dokazan.

3 Primjene, poboljšanja i hipoteze vezane uz Rothov teorem

Budući da ćemo se često pozivati na Rothov teorem 1.15, radi praktičnosti ćemo ga ovdje ponovno iskazati.

Neka su algebarski broj α i realan broj $\delta > 0$ izabrani po volji. Promatramo nejednakosti

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}} \quad (1.10) \qquad \text{i} \qquad \left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha,\delta)}{q^{2+\delta}} \quad (1.11).$$

Rothov teorem govori da nejednadžba (1.10) ima konačno rješenja p/q u $\mathbb{Q}$, odnosno da postoji $c(\alpha,\delta) > 0$ tako da nejednakost (1.11) vrijedi za sve $p/q \in \mathbb{Q}\backslash\{\alpha\}$.

3.1 Alternativni dokaz Rothovog teorema

Umjesto korištenja Rothove leme, Rothov teorem može se dokazati i pomoću teorema 3.1 koji je Bombieri (nakon dokazivanja specijalnog slučaja) nazvao Dysonova lema. Kako bismo mogli izreći taj teorem, moramo najprije uvesti neke oznake.

Za dane m-torke $R = (r_1, \ldots, r_m)$ i $E = (e_1, \ldots, e_m)$ prirodnih brojeva, neka je $\mathfrak{S}\left(t, \frac{R}{E}\right)$ skup svih m-torki $(\xi_1, \ldots, \xi_m)$ realnih brojeva koje zadovoljavaju

$$0 \le \xi_i \le 1 \quad (i = 1, \ldots, m) \qquad \text{i} \qquad \xi_1 \frac{r_1}{e_1} + \cdots + \xi_m \frac{r_m}{e_m} \le t.$$

Sa $W\left(t, \frac{R}{E}\right)$ označavamo volumen od $\mathfrak{S}\left(t, \frac{R}{E}\right)$.

Teorem* 3.1 (Esnault i Viehweg, 1984.). *Neka je $r_1 \ge r_2 \ge \cdots \ge r_m$ i neka su $\underline{\alpha}_1, \ldots, \underline{\alpha}_k \in \mathbb{C}^m$ takvi da uz $\underline{\alpha}_i = (\alpha_{i1}, \ldots, \alpha_{im})$ vrijedi*

$$\alpha_{il} \ne \alpha_{jl} \quad za \quad i \ne j \qquad (1 \le l \le m).$$

Neka je $P \in \mathbb{C}[X_1, \ldots, X_m]$ polinom stupnja $\le r_i$ u X_i $(1 \le i \le m)$, $P \ne 0$ i indeks od P u $\underline{\alpha}_h$ s obzirom na $E = (e_1, \ldots, e_m)$ je $\ge t_h$ $(h = 1, \ldots, m)$. Tada je

$$\sum_{h=1}^{k} W\left(t_h, \frac{R}{E}\right) \le \prod_{j=1}^{m-1} \left(1 + (k' - 2) \sum_{i=j+1}^{m} \frac{r_i}{r_j}\right),$$

gdje je $k' = \max\{2, k\}$.

Teorem 3.1 je algebarske prirode, njegov dokaz koristi puno algebarske geometrije, a smjernice za dokaz i upotrebu nalaze se u [Sch 91].

3.2 Nekoliko primjera i jedno poopćenje

Ridout je 1957. dokazao važno proširenje Rothovog teorema.

Teorem* 3.2. *Neka je $\alpha \neq 0$ algebarski broj i neka su $p_1 \ldots, p_r, q_1, \ldots, q_s$ različiti prosti brojevi. Neka su μ, ν i c realni brojevi takvi da je $0 \leq \mu \leq 1$, $0 \leq \nu \leq 1$ i $c > 0$. Ograničimo p i q na cijele brojeve oblika $p = p^* p_1^{a_1} \cdots p_r^{a_r}$, $q = q^* q_1^{b_1} \cdots q_s^{b_s}$, gdje su $a_1, \ldots, a_r, b_1, \ldots, b_s$ nenegativni cijeli brojevi, a p^* i q^* su cijeli brojevi različiti od 0 koji zadovoljavaju $|p^*| \leq cp^\mu$ i $|q^*| \leq cq^\nu$. Ako je $\kappa > \mu + \nu$, onda postoji najviše konačno mnogo rješenja nejednadžbe*

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\kappa}.$$

Primjetimo da uzimanjem $\mu = \nu = c = 1$ iz prethodnog teorema dobivamo Rothov teorem.

Rothov teorem ima i generalizacije vezane uz aproksimaciju algebarskim brojevima. Iako su mnoge od tih generalizacija posljedice teorema o potprostorima 4.11 kojim ćemo se baviti u posljednjem poglavlju ovog rada, mi ih nećemo navoditi, a zainteresiranog čitatelja upućujemo na tri naše uobičajene reference [Sch 80, Sch 91, Bu 04].

Vratimo se sada standardnom Rothovom teoremu. Njegovom primjenom Davenport i Roth su dobili kriterij kojim se dokazuje da realan broj s "prevelikim" parcijalnim kvocijentima ne može biti algebarski. Ovaj je kriterij poboljšanje rezultata u primjeru 1.1 kojeg smo dobili korištenjem Liouvilleovog teorema 1.13.

Teorem* 3.3. *Neka je α realan broj. Za svaki prirodni broj n označimo s q_n nazivnik n-te konvergente u razvoju od α u verižni razlomak. Ako je*

$$\limsup_{n\to\infty} \frac{(\log\log q_n)(\log n)^{1/2}}{n} = +\infty,$$

onda je α transcendentan.

Pogledajmo još nekoliko primjera korištenja Rothovog teorema.

Primjer 3.1. [St 05] *Neka je $\varepsilon > 0$ i pretpostavimo da je $\alpha = [a_0, a_1, \ldots]$ iracionalan broj kojemu beskonačno parcijalnih kvocijenata zadovoljava $a_{n+1} \geq q_n^\varepsilon$, gdje je q_n nazivnik n-te konvergente od α. Tada je α transcendentan broj.*

Rješenje. Iz identiteta u teoremu 1.7 zaključujemo da za beskonačno prirodnih brojeva n vrijedi $q_{n+1} = a_{n+1}q_n + q_{n-1} > q_n^{1+\varepsilon}$. Za takve n zbog (1.6) vrijedi

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_{n+1}q_n} < \frac{1}{q_n^{2+\varepsilon}},$$

pa nam Rothov teorem pokazuje da α ne može biti algebarski broj. ♣

Primjer 3.2. [St 05] *Za prirodan broj $g \geq 2$ i rastuću funkciju $h : \mathbb{N} \to \mathbb{N}$ definiramo $\alpha = \sum_{n=1}^{\infty} a_n g^{-h(n)}$, gdje je $a_n \in \{1, \ldots, g-1\}$, $n \in \mathbb{N}$.*

i) Dokazati da je α transcendentan ako vrijedi

$$\limsup_{n\to\infty} \frac{h(n+1)}{h(n)} > 2.$$

ii) Iz i) zaključiti da je $\sum_{n=1}^{\infty} 2^{-3^n}$ transcendentan broj.

Uočimo da korištenjem rezultata iz ovog primjera ne možemo pokazati da je $\sum_{n=1}^{\infty} 2^{-2^n}$ transcendentan broj, iako on to zaista jest (v. [St 05]).

Rješenje.

i) Neka je $\limsup_{n\to\infty} \frac{h(n+1)}{h(n)} = 2 + \varepsilon$, gdje je $\varepsilon > 0$. Uzmimo podniz $(n_k)_{k\in\mathbb{N}}$ od $\mathbb{N}$ tako da vrijedi

$$\frac{h(n_k+1)}{h(n_k)} > 2 + \frac{\varepsilon}{2}. \tag{3.1}$$

Ako za $k \in \mathbb{N}$ stavimo $q_k = g^{h(n_k)}$, $p_k = q_k \sum_{n=1}^{n_k} a_n g^{-h(n)}$, onda je

$$\left|\alpha - \frac{p_k}{q_k}\right| = \sum_{n=n_k+1}^{\infty} a_n g^{-h(n)} \leq (g-1) g^{-h(n_k+1)} \sum_{i=0}^{\infty} g^{-i} = g^{1-h(n_k+1)}$$
$$\overset{(3.1)}{<} \frac{g}{g^{(2+\frac{\varepsilon}{2})h(n_k)}} = \frac{g}{q_k^{2+\frac{\varepsilon}{2}}}.$$

Pogledamo li sada Rothov teorem, tj. nejednakost (1.10) za $\delta = \frac{\varepsilon}{4}$, vidimo da α ne može biti algebarski broj.

ii) Tvrdnja slijedi iz prvog dijela primjera ako stavimo $g = 2$, $h(n) = 3^n$, $a_n = 1$ $(n \in \mathbb{N})$. ♣

Primjer 3.3. *Broj*[1] $\mathcal{M} = 0.12345678910111213141516171819202 1\ldots$ *je transcendentan.*

Rješenje. Potpuniji dokaz zajedno sa svom motivacijom može se naći u [BT 04]. Mi ćemo ovdje izložiti samo skicu rješenja.

Da bismo dobili dobre racionalne aproksimacije od $\mathcal{M}$, nećemo raditi direktno s $\mathcal{M}$, nego ćemo koristiti racionalne brojeve

$$\mathcal{M}_1 = 0.123456789,$$
$$\mathcal{M}_2 = 0.10111213\ldots979899,$$
$$\mathcal{M}_3 = 0.100101102\ldots997998999,$$
$$\vdots$$

[1] Ovaj broj naziva se *Champernowneova konstanta* po engleskom matematičaru D.W. Champernowneu.

i tako dalje – svaki od brojeva $\mathcal{M}_i$ nastao je od niza uzastopnih znamenki u decimalnom razvoju od $\mathcal{M}$. Ovi racionalni brojevi su dobre aproksimacije razlomljenom dijelu od, respektivno, $\mathcal{M}$, $10^9\mathcal{M}$, $10^{189}\mathcal{M}$, itd. Dakle, nakon dijeljenja $\mathcal{M}_n$ s prikladnom potencijom od 10 i dodavanja prikladnog cijelog dijela, dolazimo do dobrih aproksimacija od $\mathcal{M}$. Nažalost, te aproksimacije još nisu dovoljno blizu $\mathcal{M}$.

Nova ideja za pronalaženje boljih racionalnih aproksimacija od $\mathcal{M}$ je da najprije aproksimiramo $\mathcal{M}_1$ s racionalnim brojem koji ima vrlo mali nazivnik, ali je toliko blizu $\mathcal{M}_1$ da predstavlja jednako dobru aproksimaciju od $\mathcal{M}$ kakva je bila i $\mathcal{M}_1$.

Uočimo da je svaka znamenka u $\mathcal{M}_1$ dobivena dodavanjem 1 prethodnoj znamenci. Tako vidimo da je

$$10\mathcal{M}_1 - \mathcal{M}_1 = 1.111111101,$$

a ovaj se broj podudara s $1.111\cdots = 10/9$ u prvih sedam decimala. Dakle, $9\mathcal{M}_1$ je relativno dobro aproksimiran s $10/9$. Točnije

$$\left|9\mathcal{M}_1 - \frac{10}{9}\right| = 0.000000010111\ldots,$$

a dijeljenjem s 9 dobivamo

$$\left|\mathcal{M}_1 - \frac{10}{81}\right| < \frac{0.000000011}{9}.$$

Naravno, $\mathcal{M}$ i $\mathcal{M}_1$ se podudaraju u prvih deset znamenki, pa prethodna nejednakost vrijedi i kad $\mathcal{M}_1$ zamijenimo s $\mathcal{M}$. Nakon malo sređivanja oko gornje ograde, dobivamo

$$\left|\mathcal{M}_1 - \frac{10}{81}\right| < \frac{1}{81^4}.$$

Prva aproksimacija je zato $p_1/q_1 = 10/81$.

Sada nastavljamo na isti način. Primjećujemo da se

$$100\mathcal{M}_2 - \mathcal{M}_2 = 10.010101\ldots010001$$

podudara sa $991/99$ u 177 decimala. Ovo nam pokazuje da je $99\mathcal{M}_2$ dobro aproksimiran s $991/99$ iz čega slijedi da je $\mathcal{M}_2$ jednako dobro aproksimiran s $991/99^2$. Ali, $991/99^2$ implicira i dobru aproksimaciju od $\mathcal{M}$, iako s nešto većim nazivnikom. Kako bismo našli ovu racionalnu aproksimaciju, dovoljno je opaziti da se $10^9\mathcal{M}$ i $123456789 + \mathcal{M}_2$ podudaraju u prvih 180 decimalnih znamenki. Ovo zapažanje, zajedno s izvrsnom aproksimacijom od $\mathcal{M}_2$ povlači da je

$$\left|10^9\mathcal{M} - \left(123456789 + \frac{991}{99^2}\right)\right| < \frac{1}{10^{176}}.$$

Dijeljenjem s 10^9 dobivamo da vrijedi

$$\left|\mathcal{M} - \frac{p}{10^9 99^2}\right| < \frac{1}{10^{185}}$$

za neki veliki prirodni broj p. Ako sada postavimo $p_2/q_2 = p/(10^9 99^2)$, onda je

$$\left|\mathcal{M} - \frac{p_2}{q_2}\right| < \frac{1}{q_2^{13}} < \frac{1}{q_2^4}.$$

Daljna strategija je sada jasna. Sukcesivno aproksimiramo $\mathcal{M}$ racionalnim brojevima s nazivnicima 9^2,$10^9 99^2$,...,$10^{n_k}(10^k-1)^2$, pri čemu je n_k ukupan broj znamenki koji dobivamo ispisujući redom sve k-znamenkaste brojeve. Tako dolazimo do beskonačno mnogo racionalnih brojeva p_n/q_n koji zadovoljavaju

$$\left|\mathcal{M} - \frac{p_n}{q_n}\right| < \frac{1}{q_n^4}.$$

Broj $\mathcal{M}$ je očito iracionalan jer sadrži po volji dugačke nizove nula, pa nam Rothov teorem konačno osigurava da je $\mathcal{M}$ transcendentan broj. ♣

Još neke primjene Rothovog teorema dajemo u §§3.6, 3.7, 3.8.

3.3 Hipoteze

3.3.1 Efektivnost

Jedan od glavnih otvorenih problema (v. [Wa 04]) u diofantskim aproksimacijama je dokazati efektivnu verziju Rothovog teorema. U vezi s negativnim odgovorom Ju. Matijaseviča na Hilbertov deseti problem koji je tražio algoritam za rješavanje diofantskih jednadžbi, M. Mignotte je primjetio da efektivna verzija Schmidtovog teorema o potprostorima 4.11 možda nije moguća. Ako se pokaže da je tako i za sam Rothov teorem, koji je specijalni slučaj teorema o potprostorima, tada bi prema E. Bombieriju bila izvan dohvata i poznata *abc* hipoteza.

Za prirodan broj n označavamo s

$$R(n) := \prod_{\substack{p|n \\ p \text{ prost}}} p$$

radikal ili kvadratno slobodni dio od n.

***abc* hipoteza.** *Za svaki $\varepsilon > 0$ postoji realan broj $\kappa(\varepsilon) > 0$ sa sljedećim svojstvom: ako su a, b i c tri prirodna broja koji su relativno prosti i zadovoljavaju $a+b=c$, tada je*

$$c < \kappa(\varepsilon) R(abc)^{1+\varepsilon}.$$

M. Langevin je zapazio da *abc* hipoteza povlači jaču nejednakost od Rothove (1.11),

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha,\delta)}{R(pq)q^\delta}.$$

Kao što je prije rečeno, za sada su efektivna poboljšanja poznata samo za Liouvilleovu ogradu, a već je i njihovo unapređenje veliki izazov.

3.3.2 Ocjena u Rothovom teoremu

Drugi smjer bio bi poboljšati ocjenu u Rothovom teoremu.

Pretpostavlja se da se za nijedan realan algebarski broj stupnja ≥ 3 član $\frac{1}{q^{2+\delta}}$ u nejednakosti (1.11) ne može zamijeniti s $\frac{1}{q^2}$, ali je skup brojeva α za koje je odgovor na to pitanje poznat – prazan! O tome smo već govorili na kraju §1.2.

Izgleda da je vrlo teška i Langova hipoteza koja tvrdi da se član $\frac{1}{q^{2+\delta}}$ u (1.10), odnosno (1.11) može zamijeniti s $\frac{1}{q^2(\log q)^{1+\delta}}$.

Heurističke temelje za prethodne dvije hipoteze daje nam teorem koji je jedan od prvih rezultata u metričkoj teoriji diofantskih aproksimacija.

Teorem* 3.4 (Hinčin, 1929.). *Neka je ψ pozitivna nerastuća realna funkcija definirana na skupu prirodnih brojeva. Promotrimo nejednadžbu*

$$\left|\alpha - \frac{p}{q}\right| < \frac{\psi(q)}{q}. \tag{3.2}$$

Ako je

(i) $\sum_{q=1}^{\infty} \psi(q) < \infty$, *onda* (3.2) *ima najviše konačno mnogo rješenja za skoro sve* $\alpha \in \mathbb{R}$.

(ii) $\sum_{q=1}^{\infty} \psi(q) = \infty$, *onda* (3.2) *ima beskonačno mnogo rješenja za skoro sve* $\alpha \in \mathbb{R}$.

Napomena.
Za $\psi(q) = \frac{1}{q(\log q)^{1+\delta}}$, $\delta > 0$, slučaj (i) u Hinčinovom teoremu pokazuje da

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

ima konačno rješenja za skoro sve α. Uzmemo li $\psi(q) = \frac{1}{q(\log q)}$, slučaj (ii) u Hinčinovom teoremu povlači da

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

ima beskonačno rješenja za skoro sve α.

Mi ćemo dokazati samo lakši, dio (i), Hinčinovog teorema. Znatno je teže dokazati dio (ii), tj. divergencijski dio tog teorema. Ovdje dokaz tog dijela ne navodimo, nego samo upućujemo na [Hi 64, Sch 80, Bu 04].

Dokaz dijela (i) teorema 3.4. Nejednakost (3.2) definira interval za α duljine $2\psi(q)/q$. Unija ovih intervala za $p = 1, 2, \ldots, q$ ima mjeru $\leq 2\psi(q)$. Unija intervala određenih s (3.2) za $p \in \mathbb{Z}$ je skup koji je invarijantan na translaciju za cijeli broj, a presjek ovog skupa sa intervalom $[0, 1\rangle$ ima mjeru $\leq 2\psi(q)$. Dakle, ako sa $S(q)$ označimo skup svih $\alpha \in [0, 1\rangle$ za koje (3.2) vrijedi za neki p, onda $S(q)$ ima mjeru $\mu\big(S(q)\big) \leq 2\psi(q)$. Nadalje, ako je

$$S_N = \bigcup_{q=N}^{\infty} S(q),$$

onda $\mu(S_N) \to \infty$ jer je niz $\left(\sum_{q=1}^{N} \psi(q)\right)_{N\in\mathbb{N}}$ konvergentan. Za $\alpha \in [0,1\rangle$ postoji beskonačno mnogo rješenja od (3.2) ako i samo ako α leži u

$$\bigcap_{N=1}^{\infty} S_N,$$

a ovaj skup ima mjeru 0. ■

3.4 Waringov problem

Ilustrirajmo na Waringovom problemu (v. [Wa 04]) važnost dokazivanja efektivnih nejednakosti Rothovog tipa za iracionalne algebarske brojeve.

Godine 1770., nekoliko mjeseci prije nego što je J.L. Lagrange dokazao da je svaki prirodan broj suma najviše četiri potpuna kvadrata, E. Waring je napisao:

> "Svaki prirodan broj je kub ili suma dva, tri, ..., devet kubova; svaki prirodan broj je također kvadrat kvadrata ili suma do devetnaest takvih; i tako dalje.
>
> Slični zakoni mogu se potvrditi za prikladan broj veličina kojima je stupanj kakav god želimo."

Za $k \geq 2$ definirajmo $g(k)$ kao najmanji prirodan broj g takav da je svaki prirodan broj suma g pribrojnika oblika x^k, $x \geq 0$.[2] Drugim riječima, za svaki prirodan broj n jednadžba

$$n = x_1^k + \cdots + x_m^k$$

ima rješenje ako je $m = g(k)$, ali postoji n koji nije suma $g(k) - 1$ k-tih potencija.

Lagrangeov teorem, koji je riješio hipotezu Bacheta i Fermata, je $g(2) = 4$. Navodimo vrijednosti od $g(k)$ za prvih nekoliko brojeva k zajedno s imenima autora i godinama kad su te vrijednosti dokazane.

$g(2) = 4$	$g(3) = 9$	$g(4) = 19$	$g(5) = 37$	$g(6) = 73$	$g(7) = 143$
J.L. Lagrange	A. Wieferich	R. Balasubramanian J-M. Deshouillers F. Dress	J. Chen	S.S. Pillai	L.E. Dickson
1770.	1909.	1986.	1964.	1940.	1936.

Za svaki cijeli broj $k \geq 2$, definiramo

$$I(k) = 2^k + \lfloor (3/2)^k \rfloor - 2.$$

[2] D. Hilbert je 1909. dokazao egzistenciju takvog $g(k)$.

Lako se pokazuje da je $g(k) \geq I(k)$. Zaista, napišimo

$$3^k = 2^k q + r, \quad \text{gdje je} \quad 0 < r < 2^k,\ q = \lfloor (3/2)^k \rfloor$$

i promotrimo cijeli broj

$$N = 2^k q - 1 = (q-1)2^k + (2^k - 1)1^k.$$

Budući je $N < 3^k$, zapis od N kao sume k-tih potencija ne može sadržavati član 3^k, a kako je $N < 2^k q$, taj zapis sadrži najviše $q-1$ pribrojnika 2^k, dok su ostali pribrojnici 1^k. Takav zapis, dakle, mora imati barem $(q-1) + (2^k - 1) = I(k)$ pribrojnika.

L.E. Dickson i S.S. Pillai su neovisno jedan od drugog, 1936. dokazali da je $g(k) = I(k)$ za $k > 6$ uz uvjet da $r = 3^k - 2^k q$ zadovoljava

$$r \leq 2^k - q - 2.$$

U protivnom, postoji druga formula za $g(k)$.

Pokazano je da uvjet $r \leq 2^k - q - 2$ vrijedi za $3 \leq k \leq 471\ 600\ 000$, a K. Mahler je dokazao da taj uvjet vrijedi i za dovoljno velike k. Zato je $g(k) = I(k)$ za te vrijednosti od k. Problem je u tome što se Mahlerov dokaz oslanja na p-adsku verziju Rothovog teorema (usp. §4.4) i zbog toga nije efektivan. Postoji jaz kojemu ne znamo čak ni veličinu.

Jedna hipoteza još iz 1853. tvrdi da je $g(k) = I(k)$ za sve $k \geq 2$, a ovo vrijedi čim je

$$\left\| \left(\frac{3}{2}\right)^k \right\| \geq \left(\frac{3}{4}\right)^k,$$

($\|\cdot\|$ je udaljenost od najbližeg cijelog broja). Kao što je S. David napomenuo, takva ocjena (za dovoljno velike k) slijedi ne samo iz Mahlerove ocjene, nego i iz *abc* hipoteze (v. str. 43).

3.5 Ocjene broja rješenja

Iako je metoda Thuea, Siegela i Rotha neefektivna, tj. nije moguće odrediti sva rješenja nejednadžbe (1.10), ona ipak dopušta ocjenu *broja* rješenja te nejednadžbe. Donosimo rezultate Schmidta iz [Sch 91, Sch 95].

Objasnimo najprije neke oznake.
Za $x \in \mathbb{R}$ definiramo:

$$\log^+ x := \begin{cases} \log x & \text{za} \quad x \geq e, \\ 1 & \text{za} \quad x < e. \end{cases}$$

Za algebarski broj α sa $h(\alpha)$ ćemo označavati jednu od nekoliko mogućih *visina* od α. U sljedećim teoremima $h(\alpha)$ može biti bilo koja od visina $H_1(\alpha)$, $H_2(\alpha)$, $h_1(\alpha)$, $h_2(\alpha)$ koje ćemo sad definirati. Neka je $P(X) = a_d X^d + \cdots + a_1 X + a_0 = a_d(X - \alpha_1)\ldots(X - \alpha_d)$ minimalni polinom od α nad $\mathbb{Z}$, tj. polinom s cjelobrojnim koeficijentima najmanjeg

pozitivnog stupnja, s relativno prostim koeficijentima i pozitivnim vodećim članom, koji se poništava u α.
$H_1(\alpha)$ je najuobičajenija visina od α, tj.

$$H_1(\alpha) = \max\{|a_i| : 0 \le i \le d\}.$$

$H_2(\alpha)$ je tzv. *Mahlerova mjera* od α, tj.

$$H_2(\alpha) = a_d \prod_{i=1}^{d} \max\{1, |\alpha_d|\}.$$

Nadalje, $h_1(\alpha) = H_1(\alpha)^{1/d}$ i $h_2(\alpha) = H_2(\alpha)^{1/d}$. Mahlerova mjera i neke druge visine koje nismo spominjali vezane su uz apsolutne vrijednosti u polju $\mathbb{Q}(\alpha)$. Više o tome vidi u [La 02, §XII] i [Sch 91, str. 22].

Teorem* 3.5. *Neka je α algebarski broj stupnja $d \ge 3$ i $2 < \rho < 3$. Neka je $h(\alpha)$ visina od α. Tada je broj skraćenih razlomaka $p/q \in \mathbb{Q}$ (sa $q > 0$) za koje vrijedi*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\rho} \tag{3.3}$$

najviše

$$\frac{\log^+ \log h(\alpha)}{\log(\rho - 1)} + \mathcal{O}\Big((\rho-2)^{-5}(\log d)^2\big(-\log(\rho-2) + \log\log d\big)\Big). \tag{3.4}$$

Teorem* 3.6. *Neka je $\rho \ge 3$ i neka je α algebarski broj stupnja $d \ge \rho$. Neka je $h(\alpha)$ visina od α. Tada je broj skraćenih razlomaka $p/q \in \mathbb{Q}$ (sa $q > 0$) za koje vrijedi* (3.3) *najviše*

$$\frac{\log^+ \log h(\alpha)}{\log(\rho - 1)} + \mathcal{O}\left(\left(\frac{\log d}{\log \rho}\right)^2\left(1 + \frac{\log\log d}{\log \rho}\right)\right). \tag{3.5}$$

U prethodna dva teorema konstante koje se implicitno pojavljuju u velikom $\mathcal{O}$ su apsolutne.[3] Prvi pribrojnik u ocjenama (3.4) i (3.5) je najbolji mogući. Naime, te bi ocjene postale netočne kad bismo $\log(\rho - 1)$ zamijenili s nekom većom veličinom. To nam pokazuje sljedeći teorem.

Teorem* 3.7. *Neka je K realno algebarsko brojevno polje stupnja $d \ge 2$ i neka je dan $\rho > 2$. Tada postoji beskonačno mnogo $\alpha \in K$, takvih da je $K = \mathbb{Q}(\alpha)$ i da skraćenih racionalnih aproksimacija p/q od α koje zadovoljavaju* (3.3) *ima više od*

$$\frac{\log^+ \log h(\alpha)}{\log(\rho - 1)} - c_0(K, \rho). \tag{3.6}$$

[3] $\mathcal{O}$ je simbol Landaua. Izraz $f(x) = \mathcal{O}\big(g(x)\big)$ znači da postoji konstanta c takva da je $|f(x)| \le c|g(x)|$ za sve x iz domene od f i g (ili u okolini neke točke iz domene). Usp. fusnotu na str. 57.

3.6 Thueova jednadžba

Teorem 3.8 (Thue, 1908.). *Neka je $F(X,Y)$ binarna forma[4] s racionalnim koeficijentima i s barem tri različita linearna faktora (s algebarskim koeficijentima). Ako je m različit od nule, diofantska jednadžba*

$$F(x,y) = m \tag{3.7}$$

ima samo konačno mnogo rješenja u cijelim brojevima x, y.

Definicija. Jednadžbe tipa (3.7) nazivaju se *Thueove jednadžbe.*

Dokaz. Neka je d stupanj forme F. Uzimajući u obzir da je $F(X,Y) = Y^d F\big(\frac{X}{Y}, 1\big)$ i da je $F(Z,1)$ polinom u jednoj varijabli, vidimo da $F(X,Y)$ možemo ovako faktorizirati

$$F(X,Y) = a(\gamma_1 X + \delta_1 Y)^{e_1} \cdots (\gamma_s X + \delta_s Y)^{e_s} \tag{3.8}$$

Pri tome su $\gamma_1, \delta_1, \ldots, \gamma_s, \delta_s$ algebarski brojevi takvi da su za sve $i \neq j$ forme $\gamma_i X + \delta_i Y$ i $\gamma_j X + \delta_j Y$ linearno nezavisne, a iz uvjeta teorema je $s \geq 3$. Nadalje, možemo uzeti da je svaki γ_i ili 1 ili 0, a $\delta_i = 1$ ako je $\gamma_i = 0$.

Reindeksiranjem faktora bez smanjenja općenitosti možemo pretpostaviti da vrijedi

$$0 < |\gamma_1 x + \delta_1 y| \leq \cdots \leq |\gamma_s x + \delta_s y|.$$

Budući da su $\gamma_1 X + \delta_1 Y$ i $\gamma_2 X + \delta_2 Y$ linearno nezavisne, uz oznaku $\underline{\underline{x}} = (x,y)$ imamo:

$$|\gamma_s x + \delta_s y| \geq \cdots \geq |\gamma_2 x + \delta_2 y| \geq \frac{1}{2}\big(|\gamma_1 x + \delta_1 y| + |\gamma_2 x + \delta_2 y|\big) \geq^{5} c_1 \max\{|x|, |y|\} = c_1 \boxed{\underline{\underline{x}}},$$

$$|F(x,y)| \geq c_2 |\gamma_1 x + \delta_1 y|^{e_1} \boxed{\underline{\underline{x}}}^{d-e_1}, \tag{3.9}$$

gdje su c_1 i c_2 pozitivne konstante koje ovise samo o F.

Ako $\gamma_1 X + \delta_1 Y$ ima racionalne koeficijente, onda je $|\gamma_1 x + \delta_1 y| \geq c_3$, pa iz $d > e_1$ slijedi da $|F(x,y)|$ teži prema beskonačnosti kad $\boxed{\underline{\underline{x}}}$ neograničeno raste.

Ako je $\gamma_1 = 1$ i δ_1 algebarski broj stupnja $l \geq 2$, onda iz Thueovog rezultata na strani 13 u §1.4 (pa pogotovo iz Rothovog teorema) slijedi da za $\delta > 0$ imamo

$$|\gamma_1 x + \delta_1 y| \geq c_4(\delta_1, \delta) \boxed{\underline{\underline{x}}}^{-\frac{l}{2}-\delta},$$

što sa (3.9) daje

$$|F(x,y)| \geq c_5 \boxed{\underline{\underline{x}}}^{d-e_1(\frac{l}{2}+1+\delta)}.$$

[4] *Binarna forma* je homogeni polinom u dvije varijable.

[5] Linearni operator $A : \mathbb{R}^2 \to \mathbb{R}^2$ s matricom $\left(\begin{smallmatrix} \gamma_1 & \delta_1 \\ \gamma_2 & \delta_2 \end{smallmatrix}\right)$ u standardnoj bazi, nužno je regularan, pa i odozdo ograničen, tj. postoji $\widetilde{c} > 0$ takav da je $\boxed{A\underline{\underline{x}}} \geq \widetilde{c}\boxed{\underline{\underline{x}}}$ za sve $\underline{\underline{x}} \in \mathbb{R}^2$. Sada tražena nejednakost slijedi iz definicije norme $\boxed{\cdot}$, tj. $\boxed{\underline{\underline{x}}} = \boxed{(x,y)} = \max\{|x|, |y|\}$.

Uz faktor $\gamma_1 X + \delta_1 Y = X + \delta_1 Y$ forma F mora imati i konjugirane faktore, svaki s kratnošću e_1. Stoga je $d \geq le_1$, a za $l = 2$ imamo čak $d \geq 2e_1 + 1$ jer F ima barem 3 različita faktora. Kako $\delta > 0$ možemo uzeti po volji mali, to je $d > e_1(\frac{l}{2} + 1 + \delta)$ te ponovno $|F(x, y)|$ teži prema beskonačnosti kad i $\boxed{\underline{\underline{x}}}$. ■

Upotrebom pune snage Rothovog teorema u prethodnom dokazu, dobiva se sljedeći teorem.

Teorem 3.9. *Neka je $F(X, Y)$ binarna forma stupnja $d \geq 3$ s racionalnim koeficijentima i bez višestrukih faktora. Tada za $\nu < d - 2$ najviše konačno cjelobrojnih točaka $\underline{\underline{x}} = (x, y)$ zadovoljava*

$$0 < |F(x, y)| \leq \boxed{\underline{\underline{x}}}^{\nu}.$$

Posebice, ako je $G(X, Y)$ forma stupnja $< d - 2$, onda diofantska jednadžba

$$F(x, y) = G(x, y)$$

ima najviše konačno mnogo rješenja koja zadovoljavaju[6] $F(x, y) \neq 0$.

Dokazi prethodnih teorema Thueovom metodom su neefektivni, tj. ne daju ogradu na veličinu rješenja. Baker je 1967. dao ogradu

$$\boxed{\underline{\underline{x}}} < \exp\left((dH)^{(10d)^5}\right)$$

za rješenja $\underline{\underline{x}} = (x, y)$ Thueove jednadžbe (3.7), gdje je d stupanj od F, a F ima različite linearne faktore. Još se traži da m i koeficijenti od F budu cijeli brojevi čija je apsolutna vrijednost najviše H.

Može se dobiti i ocjena broja rješenja jednadžbe (3.7). Primjerice, Bombieri i Schmidt su 1987. dokazali idući teorem.

Teorem* 3.10. *Neka je F binarna forma stupnja d s cjelobrojnim koeficijentima, a m prirodan broj. Broj primitivnih rješenja diofantske jednadžbe $F(x, y) = m$ nije veći od $c_0 d^{1+\nu}$, gdje je c_0 apsolutna konstanta, a ν je broj različitih prostih faktora od m.*

3.7 O velikom Fermatovom teoremu

Veliki Fermatov teorem povlači da za $v \in \mathbb{N}$ i prost broj $p \geq 3$ jednadžba

$$x^p + (x + v)^p = z^p \tag{3.10}$$

nema rješenja u prirodnim brojevima x i z. Korištenjem Rothovog teorema C.J. Everett je dokazao (v. [E 73]) da ova jednadžba za fiksirane v i p može imati najviše konačno mnogo rješenja.

[6] $F(x, y) = G(x, y)$ ima beskonačno rješenja točno tada kad F i G imaju zajednički linearni faktor s racionalnim koeficijentima.

Dovoljno je pokazati da (3.10) ima najviše konačno mnogo rješenja u kojima su x i z relativno prosti. Naime, djelitelji od x i z dijele i v, a takvih je konačno mnogo, pa u općem slučaju, kada ne tražimo da su x i z relativno prosti, zapravo trebamo riješiti konačno jednadžbi istog oblika kao i (3.10).

Definirajmo $b = \frac{v}{2} \in \{\frac{1}{2}, 1, \frac{3}{2}, 2, \dots\}$ i neka je (x, z) jedan par relativno prostih prirodnih brojeva koji zadovoljavaju jednadžbu (3.10). Stavimo li $a = x + b$, možemo pisati

$$\begin{aligned} z^p &= (a-b)^p + (a+b)^p = \\ &= \sum_{i=0}^{p} \binom{p}{i} a^i (-b)^{p-i} + \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = \\ &= 2a\Bigg(\sum_{\substack{0 \le i \le p \\ i \in 2\mathbb{N}-1}} \binom{p}{i} a^{i-1} b^{p-i} \Bigg) > 2a \binom{p}{p} a^{p-1} = 2a^p, \end{aligned}$$

iz čega slijedi nejednakost

$$\begin{aligned} 0 &< (z - 2^{1/p}a)p(2^{1/p}a)^{p-1} \\ &< (z - 2^{1/p}a)\Big(\sum_{i=0}^{p-1} z^i (2^{1/p}a)^{p-1-i} \Big) = z^p - 2a^p \\ &= 2a\Bigg(\sum_{\substack{0 \le i \le p-2 \\ i \in 2\mathbb{N}-1}} \binom{p}{i} a^{i-1} b^{p-i} \Bigg) < Ka^{p-2}, \quad \text{tj.} \end{aligned}$$

$$0 < \frac{z}{a} - 2^{1/p} < \frac{K'}{a^2}, \tag{3.11}$$

gdje K i K' ovise samo o v i p. Budući da je svaki iracionalan broj aproksimabilan do reda 2 (v. korolar 1.2), ovo nam trenutno ne može pomoći. No, pokazuje se da razlomak $\frac{z}{a}$ nije skraćen i da nakon skraćivanja dobivamo $\frac{z}{a} = \frac{z'}{a'}$, gdje je $a^2 \ge K''(a')^{2+\varepsilon}$, $\varepsilon = \frac{2}{p-1}$ (K'' je fiksirano za fiksne v i p), pri čemu je $\frac{z'}{a'}$ različit za razne točke (x, z). Sada iz (3.11) korištenjem prethodne tvrdnje dobivamo

$$0 < \frac{z'}{a'} - 2^{1/p} < \frac{K'/K''}{(a')^{2+\varepsilon}} = \frac{K'''}{(a')^{2+\varepsilon}}.$$

Konstanta K''' također ovisi samo o v i p, pa primjenom Rothovog teorema završava dokaz konačnosti broja rješenja jednadžbe (3.10).

Dokaz nejednakosti $a^2 \ge K''(a')^{2+\varepsilon}$ provodi se za četiri slučaja, ovisno o tome je li v paran ili neparan i da li p dijeli ili ne dijeli z. Taj dio dokaza ne navodimo jer je više tehničke prirode, a može ga se naći u prije spomenutom članku [E 73].

Spomenimo još da se u slučaju $p = 2$ korištenjem teorije pellovskih jednadžbi pokazuje da jednadžba (3.10) ima beskonačno mnogo ili nijedno rješenje.

3.8 Donje ograde za udaljenost između 1 i produkta potencija cijelih brojeva

Neka su $a_1, \ldots, a_m$ prirodni brojevi koji su ≥ 2 i $b_1, \ldots, b_m$ cijeli brojevi. Pretpostavljamo da je

$$a_1^{b_1} \cdots a_m^{b_m} \neq 1$$

i tražimo donju ogradu za udaljenost ovih dvaju brojeva [Wa 93].

Postoji trivijalna ocjena: pozitivni racionalni broj je velik barem kao inverz njegovog nazivnika.

$$\begin{aligned} \left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| &\geq \prod_{b_i<0} a_i^{b_i} \\ &\geq \exp\Big(- \sum_{i=1}^{m} |b_i| \log a_i \Big) \\ &\geq \exp(-mB \log A), \end{aligned}$$

gdje je $B = \max\{|b_1|, \ldots, |b_m|\}$ i $A = \max\{a_1, \ldots, a_m\}$. Ovisnost o m i A u ovoj nejednakosti je oštra, ali glavni interes u primjenama je ovisnost o B.

Godine 1935. Geljfand je, koristeći svoje metode dokaza transcendentnosti, dao ovakvu ogradu:

Teorem* 3.11. *Za multiplikativno nezavisne*[7] *prirodne brojeve a_1, a_2 i za $\varepsilon > 0$, postoji konstanta $C_1 = C_1(a_1, a_2, \varepsilon)$ koju je moguće eksplicitno izračunati, tako da za sve $(b_1, b_2) \in \mathbb{Z}^2 \backslash \{(0,0)\}$, uz oznaku $B = max\{|b_1|, |b_2|, 2\}$, vrijedi*

$$\left|a_1^{b_1} a_2^{b_2} - 1\right| \geq C_1 \exp\big(- (\log B)^{5+\varepsilon}\big).$$

Geljfand je 1939. poboljšao ovu ocjenu i zamijenio eksponent $5+\varepsilon$ sa $3+\varepsilon$, a 1949. je došao i do eksponenta $2+\varepsilon$. U isto vrijeme dao je i ocjenu koja vrijedi za sve $m \geq 2$, ali je nažalost neefektivna.

Teorem 3.12 (Geljfandova neefektivna ocjena). *Za svaku m-torku $(a_1, \ldots, a_m)$ multiplikativno nezavisnih prirodnih brojeva i za svaki $\delta > 0$ postoji pozitivna konstanta $C_2 = C_2(a_1, \ldots, a_m, \delta)$ takva da vrijedi: ako su $b_1, \ldots, b_m$ cijeli brojevi koji nisu svi jednaki 0 i ako definiramo $B = \max\{|b_1|, \ldots, |b_m|, 2\}$, onda je*

$$\left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| \geq C_2 \exp(-\delta B).$$

[7] Drugim riječima $\log a_1$ i $\log a_2$ su linearno nezavisni nad $\mathbb{Q}$.

Dokaz. Geljfand je u dokazu ovog teorema koristio svoj rezultat (v. str. 13), ali mi ćemo radi jednostavnosti koristiti Rothov teorem, tj. slučaj izražen u nejednakosti (1.11) (i to za δ u toj nejednakosti jednak 1). Dakle,

$$\left|\alpha - \frac{p}{q}\right| > \frac{C_0(\alpha,1)}{q^3}, \qquad \frac{p}{q} \in \mathbb{Q}\backslash\{\alpha\}. \tag{3.12}$$

Neka je $\delta > 0$. Pretpostavimo da C_2 ne postoji, odnosno da za svaki realni broj $C > 0$ postoji $\underline{\underline{b}} = (b_1, \ldots, b_m) \in \mathbb{Z}^m$ takav da je

$$0 < \left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| \leq C \exp(-\delta B),$$

gdje je kao i obično $B = \max\{2, |b_1|, \ldots, |b_m|\}$. Zato je beskonačan skup E_1 svih $\underline{\underline{b}} \in \mathbb{Z}^m$ za koje je

$$0 < \left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| \leq \exp(-\delta B).$$

Neka je N prirodan broj koji zadovoljava $N > (6m/\delta)\log A$, pri čemu je $A = \max\{a_i : 1 \leq i \leq m\}$. Budući da je skup $(\mathbb{Z}/N\mathbb{Z})^m$ konačan, postoji beskonačan podskup E_2 od E_1 koji ima sve elemente u istoj klasi modulo N. To znači da postoji $\underline{\underline{r}} = (r_1, \ldots, r_m) \in \mathbb{N}_0^m$, $0 \leq r_i < N$ $(1 \leq i \leq m)$ takav da je za sve $\underline{\underline{b}} \in E_2$

$$b_i \equiv r_i \pmod{N} \qquad (1 \leq i \leq m).$$

Neka je E_3 skup svih $\underline{\underline{b}} \in E_2$ kojima je $B \geq N$. To je također beskonačan skup. Za svaki $\underline{\underline{b}} \in E_3$ postoji $\underline{\underline{x}} \in \mathbb{Z}^m$ takav da vrijedi

$$b_i = r_i + Nx_i \qquad (1 \leq i \leq m).$$

Imamo $|x_i| \leq 1 + B/N \leq 2B/N$, $(1 \leq i \leq m)$. Definirajmo dva racionalna broja $s = a_1^{r_1} \cdots a_m^{r_m}$ i $t = a_1^{x_1} \cdots a_m^{x_m}$. Primjetimo da s ne ovisi o $\underline{\underline{b}} \in E_3$, dok t ovisi o $\underline{\underline{b}} \in E_3$. Iz konstrukcije skupa E_3 zaključujemo da je

$$0 < \left|st^N - 1\right| \leq e^{-\delta B}.$$

Sada upotrebom ocjene $|x-1| \leq |x^N - 1|$ koja vrijedi za sve $x > 0$ dobivamo

$$0 < \left|s^{1/N}t - 1\right| \leq e^{-\delta B}.$$

Prethodna nejednakost pokazuje da je racionalan broj t blizu algebarskom broju $\alpha = s^{-1/N}$ koji je realni N-ti korijen iz $1/s$:

$$0 < |t - \alpha| \leq \alpha e^{-\delta B}.$$

Kako je nazivnik od t najviše $A^{2mB/N}$, Rothov teorem, tj. nejednakost (3.12), povlači

$$|t - \alpha| \geq C_0(\alpha,1) A^{-6mB/N}.$$

Kombiniranjem gornje i donje ograde izvodimo

$$B\Big(\delta - \frac{6m\log A}{N}\Big) \leq -\log C_0(\alpha,1) - \frac{1}{N}\log s$$

što pokazuje da je broj B odozgo omeđen (brojevi $\delta, A, N, C_0(\alpha,1), s$ ne ovise o $\underline{b} \in E_3$), a to proturječi činjenici da je E_3 beskonačan skup. ■

Geljfand je upotrijebio svoj teorem 3.12 u nekim diofantskim problemima, posebice u Gaussovom problemu određivanja svih imaginarnih kvadratnih brojevnih polja kojima je broj klasa jednak 1 (v. npr. [Ma 77] za razjašnjenje terminologije). Koristio ga je i u proučavanju nekih tipova diofantskih jednadžbi.

N.I. Feljdman je 1968. dao poboljšanje Geljfandove ocjene:

$$\left|a_1^{b_1}\cdots a_m^{b_m} - 1\right| \geq B^{-C_3},$$

gdje je $C_3 = C_3(a_1,\ldots,a_m)$ pozitivan efektivno izračunljiv broj [Fe 81, str. 163].

Više o teoriji linearnih formi u logaritmima iz koje dolaze prethodni rezultati može se naći u [Ba 90, Wa 93, Wa 04] i ondje navedenoj literaturi.

4 Teorem o potprostorima

4.1 Dirichletov teorem o simultanim aproksimacijama

Dirichletov teorem 1.1 može se poopćiti. Najprije ćemo dati dva parcijalna poopćenja i njihove korolare, a zatim ćemo dokazati i generalnu tvrdnju iz koje slijede.

Teorem 4.1. *Neka su $\alpha_1, \ldots, \alpha_n$ realni brojevi i neka je $Q > 1$ prirodan broj. Tada postoje cijeli brojevi $q, p_1, \ldots, p_n$ takvi da je*

$$1 \leq q < Q^n \qquad i \qquad |\alpha_i q - p_i| \leq \frac{1}{Q} \qquad (1 \leq i \leq n). \tag{4.1}$$

Korolar 4.2. *Ako je barem jedan od brojeva $\alpha_1, \ldots, \alpha_n$ iracionalan, onda postoji beskonačno n-torki $\left(\frac{p_1}{q}, \ldots, \frac{p_n}{q}\right)$ takvih da je*

$$\left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+\frac{1}{n}}} \qquad (1 \leq i \leq n). \tag{4.2}$$

Dokaz korolara. U teoremu 4.1 možemo dodatno zahtijevati da bude $M(q, p_1, \ldots, p_n) = 1$. Iz nejednakosti u teoremu očito slijede nejednakosti (4.2). Ako je sada, primjerice, α_1 iracionalan, onda je $|\alpha_1 q - p_1| \neq 0$. Zato za *fiksirane* $q, p_1, \ldots, p_n$, (4.1) može vrijediti samo za $Q \leq Q_0$. Kad $Q \to \infty$ dobivamo beskonačno mnogo rješenja od (4.2). ■

Teorem 4.3. *Neka su $\alpha_1, \ldots, \alpha_n$ realni brojevi i neka je $Q > 1$ prirodan broj. Tada postoje cijeli brojevi $q_1, \ldots, q_n, p$ takvi da je*

$$1 \leq \max\{|q_1|, \ldots, |q_n|\} < Q^{\frac{1}{n}} \qquad i \qquad |\alpha_1 q_1 + \cdots + \alpha_n q_n - p| \leq \frac{1}{Q}. \tag{4.3}$$

Korolar 4.4. *Ako su $1, \alpha_1, \ldots, \alpha_n$ linearno nezavisni nad $\mathbb{Q}$, onda postoji beskonačno mnogo relativno prostih $(n+1)$-torki $(q_1, \ldots, q_n, p)$ takvih da je*

$$q = \max\{|q_1|, \ldots, |q_n|\} > 0 \qquad i \qquad |\alpha_1 q_1 + \cdots + \alpha_n q_n - p| < \frac{1}{q^n}. \tag{4.4}$$

Dokaz korolara. Jasno je da iz (4.3) slijedi (4.4). Zbog linearne nezavisnosti je uvijek $|\alpha_1 q_1 + \cdots + \alpha_n q_n - p| \neq 0$. Zato za *fiksirane* $q_1, \ldots, q_n, p$, (4.3) može vrijediti samo za $Q \leq Q_0$. Kad $Q \to \infty$ dobivamo beskonačno mnogo rješenja od (4.4). ■

Teorem 4.5 (Dirichlet, 1842.). *Neka je α_{ij} $(1 \le i \le n,\ 1 \le j \le m)$ nm realnih brojeva i neka je $Q > 1$ prirodan broj. Tada postoje cijeli brojevi $q_1, \dots, q_m, p_1, \dots, p_n$ takvi da je*

$$\begin{aligned} 1 \le \max\{|q_1|, \dots, |q_m|\} &< Q^{\frac{n}{m}}, \\ |\alpha_{i1}q_1 + \cdots + \alpha_{im}q_m - p_i| &\le \frac{1}{Q} \qquad (1 \le i \le n). \end{aligned} \tag{4.5}$$

Napomena.
Pretpostavka da je Q prirodan broj je nepotrebna, ali dokaz teorema 4.5 koji ćemo izložiti ne može se direktno prilagoditi ovoj generalizaciji. Za općenitu tvrdnju trebalo bi koristiti teoreme Blichfeldta ili Minkowskog iz geometrije brojeva (v. npr. [Sch 80]).

Očito je da su teoremi 4.1 i 4.3 specijalni slučajevi teorema 4.5.

Dokaz. Promotrimo točke

$$\big(\{\alpha_{11}x_1 + \cdots + \alpha_{1m}x_m\}, \dots, \{\alpha_{n1}x_1 + \cdots + \alpha_{nm}x_m\}\big),$$

gdje je svaki x_j cijeli broj koji zadovoljava

$$0 \le x_j < Q^{\frac{n}{m}} \qquad (1 \le j \le m).$$

Ima barem Q^n takvih točaka, a ako im dodamo i točku $(1, 1, \dots, 1)$ dobivamo barem $Q^n + 1$ točaka koje leže u zatvorenoj kocki $[0, 1]^n$.

Podijelimo $[0, 1]^n$ na Q^n u parovima disjunktnih kockica kojima je brid duljine $\frac{1}{Q}$. (Neke će od tih kockica sadržavati pojedine svoje strane, a druge neće.) Neke dvije od prije spomenutih točaka moraju ležati u istoj kockici. Neka su to točke

$$\begin{aligned} &(\alpha_{11}x_1 + \cdots + \alpha_{1m}x_m - y_1, \dots, \alpha_{n1}x_1 + \cdots + \alpha_{nm}x_m - y_n) \qquad \text{i} \\ &(\alpha_{11}x'_1 + \cdots + \alpha_{1m}x'_m - y'_1, \dots, \alpha_{n1}x'_1 + \cdots + \alpha_{nm}x'_m - y'_n). \end{aligned}$$

Ovdje je $(x_1, \dots, x_m) \ne (x'_1, \dots, x'_m)$. Lako se vidi da je za $q_i = x_i - x'_i$ $(1 \le i \le m)$ i $p_j = y_j - y'_j$ $(1 \le j \le n)$ ispunjeno (4.5), pa je dokaz završen. ■

4.2 Simultane aproksimacije algebarskih brojeva

Koristeći svojstva norme u brojevnim poljima (v. [Ma 77]) nije teško dokazati (v. [Sch 80]) sljedeću propoziciju.

Propozicija* 4.6. *Neka su $1, \alpha_1, \dots, \alpha_v$ linearno nezavisni nad $\mathbb{Q}$ i neka oni generiraju brojevno polje stupnja d. Tada vrijedi*[1]

$$|\alpha_1 q_1 + \cdots + \alpha_v q_v - p| > \frac{c_1}{q^{d-1}} \tag{4.6}$$

za proizvoljne cijele brojeve $q_1, \dots, q_v, p$ kojima je $q = \max\{|q_1|, \dots, |q_v|\} > 0$.

[1] Konstanta c_1 eksplicitno ovisi o $\alpha_1, \dots, \alpha_v$.

Za $v = 1$ dobivamo Liouvilleov teorem 1.13. Eksponent u (4.6) je za $d = v + 1$ zbog korolara 4.4 očito najbolji mogući, no poboljšat ćemo ga u korolaru 4.10 za $d > v + 1$.

Pogledajmo sad teže rezultate Rothovog tipa. Prisjetimo se da za realni broj α sa $\|\alpha\|$ označavamo udaljenost od α do najbližeg cijelog broja, tj. $\|\alpha\| = \min\big\{\{\alpha\}, 1 - \{\alpha\}\big\}$.

Teorem 4.7. *Neka su $\alpha_1, \ldots, \alpha_u$ realni algebarski brojevi tako da su $1, \alpha_1, \ldots, \alpha_u$ linearno nezavisni nad skupom racionalnih brojeva. Usto, neka je $\delta > 0$. Tada postoji samo konačno mnogo prirodnih brojeva q koji zadovoljavaju*

$$q^{1+\delta} \|\alpha_1 q\| \cdots \|\alpha_u q\| < 1. \tag{4.7}$$

Neposredno iz prethodnog teorema dobivamo

Korolar 4.8. *Ako su $\alpha_1, \ldots, \alpha_u$ i δ kao u teoremu 4.7, onda postoji samo konačno u-torki $\left(\frac{p_1}{q}, \ldots, \frac{p_u}{q}\right)$ racionalnih brojeva takvih da je*

$$\left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+\frac{1}{u}+\delta}} \qquad (1 \le i \le u). \tag{4.8}$$

Teorem 4.9. *Neka su $\alpha_1, \ldots, \alpha_v$ realni algebarski brojevi tako da su $1, \alpha_1, \ldots, \alpha_v$ linearno nezavisni nad skupom $\mathbb{Q}$, te neka je $\delta > 0$. Tada postoji samo konačno mnogo v-torki $(q_1, \ldots, q_v)$ cijelih brojeva različitih od nule koje zadovoljavaju*

$$|q_1 q_2 \cdots q_v|^{1+\delta} \|\alpha_1 q_1 + \cdots + \alpha_v q_v\| < 1. \tag{4.9}$$

Primjenimo li teorem 4.9 na sve neprazne podskupove od $\{\alpha_1, \ldots, \alpha_v\}$ dobivamo

Korolar 4.10. *Ako su $\alpha_1, \ldots, \alpha_v$ i δ kao u teoremu 4.9, onda postoji najviše konačno mnogo $v+1$-torki $(q_1, \ldots, q_v, p)$ cijelih brojeva takvih da je $q = \max\{|q_1|, \ldots, |q_v|\} > 0$ i vrijedi*

$$|\alpha_1 q_1 + \cdots + \alpha_v q_v - p| < \frac{1}{q^{v+\delta}}. \tag{4.10}$$

Zbog Dirichletovog teorema o simultanim aproksimacijama, tj. korolara 4.2 i 4.4, eksponenti u korolarima 4.8 i 4.10 su najbolji mogući.

Teoreme 4.7 i 4.9 dokazao je W.M. Schmidt 1970., a kasnije se pokazalo da su ti teoremi ekvivalentni. Jasno je da u prethodnim teoremima za $u = 1$, odnosno $v = 1$, dobivamo Rothov teorem. Baker, Feljdman i Osgood su dokazali slabije, ali efektivne verzije korolara 4.10 za neke specijalne algebarske brojeve.

Schmidt je 1972. dokazao važnu višedimenzionalnu generalizaciju Rothovog teorema koja obuhvaća teoreme 4.7 i 4.9. Ova se tvrdnja, koja je postala jedan od temeljnih alata diofantske analize, naziva Schmidtov teorem o potprostorima (Schmidt's subspace theorem).

Teorem* 4.11 (Teorem o potprostorima). *Neka su $L_1, \ldots, L_n$ linearno nezavisne linearne forme u n varijabli s realnim ili kompleksnim algebarskim koeficijentima. Za*

$\delta > 0$ postoji konačno mnogo pravih potprostora $T_1, \ldots, T_w$ od $\mathbb{Q}^n$ tako da svaka cjelobrojna točka $\underline{\underline{x}} \neq \underline{\underline{0}}$ za koju vrijedi

$$\left|L_1(\underline{\underline{x}}) \cdots L_n(\underline{\underline{x}})\right| < \left|\underline{\underline{x}}\right|^{-\delta} \tag{4.11}$$

leži u jednom od tih potprostora.

U nastavku ćemo pokazati da su teoremi 4.7 i 4.9 posljedice teorema o potprostorima.

Izvod teorema 4.7 iz teorema 4.11. Za dani q koji zadovoljava (4.7) uzmimo $p_1, \ldots, p_u$ takve da je $\|\alpha_i q\| = |\alpha_i q - p_i|$ $(i = 1, \ldots, u)$. Tada je uz $n = u + 1$ i

$$\underline{\underline{x}} = (x_1, \ldots, x_n) = (p_1, \ldots, p_u, q)$$

jasno da vrijedi $\left|\underline{\underline{x}}\right| \ll q$.[2] Uvedimo linearne forme

$$\begin{aligned} L_i(\underline{\underline{X}}) &= \alpha_i X_n - X_i \qquad (1 \leq i \leq u), \\ L_n(\underline{\underline{X}}) &= X_n. \end{aligned} \tag{4.12}$$

Nejednakost (4.7) povlači

$$\left|L_1(\underline{\underline{x}}) \cdots L_n(\underline{\underline{x}})\right| < \left|\underline{\underline{x}}\right|^{-\frac{\delta}{2}}, \tag{4.13}$$

za dovoljno veliki q. Prema teoremu o potprostorima, rješenja od (4.13) leže u konačno mnogo pravih racionalnih potprostora. Tipičan takav potprostor T je definiran sa

$$c_1 x_1 + \cdots + c_u x_u + c_n x_n = 0. \tag{4.14}$$

Za $\underline{\underline{x}}$ iz T vrijedi

$$c_1(\alpha_1 q - p_1) + \cdots + c_u(\alpha_u q - p_u) = (c_1\alpha_1 + \cdots + c_u\alpha_u + c_n)q,$$

pa je

$$\frac{1}{2}\big(|c_1| + \cdots + |c_u|\big) \geq |c_1|\,\|\alpha_1 q\| + \cdots + |c_u|\,\|\alpha_u q\| \geq \gamma q, \tag{4.15}$$

gdje je $\gamma = |c_1\alpha_1 + \cdots + c_u\alpha_u + c_n| > 0$ zbog pretpostavke o linearnoj nezavisnosti. No, (4.15) pokazuje da je q omeđen. ■

Izvod teorema 4.9 iz teorema 4.11 Neka su dani $q_1, \ldots, q_v$ koji zadovoljavaju (4.9). Uzmimo p takav da je $\|\alpha_1 q_1 + \cdots + \alpha_v q_v\| = |\alpha_1 q_1 + \cdots + \alpha_v q_v - p|$. Tada je uz $n = v+1$ i

$$\underline{\underline{x}} = (x_1, \ldots, x_n) = (q_1, \ldots, q_v, p)$$

[2] $\ll$ je simbol Vinogradova. Tako primjerice $f(\underline{\underline{x}}) \ll g(\underline{\underline{x}})$ znači da je $|f(\underline{\underline{x}})| \leq c|g(\underline{\underline{x}})|$ za neku konstantu c. Ova implicitna konstanta c može ovisiti o nekim parametrima. U primjeru $\left|\underline{\underline{x}}\right| \ll q$ koji ova fusnota objašnjava, implicitna konstanta ovisi o $\alpha_1, \ldots, \alpha_u$. Usp. fusnotu na str. 47.

očito da vrijedi $\boxed{\underline{\underline{x}}} \ll q$. Uvedimo linearne forme

$$\begin{aligned} L_i(\underline{\underline{X}}) &= X_i \qquad (1 \le i \le v), \\ L_n(\underline{\underline{X}}) &= \alpha_1 X_1 + \cdots + \alpha_v X_v - X_n. \end{aligned} \tag{4.16}$$

Iz (4.9) dobivamo da, za dovoljno veliki q, vrijedi (4.13). U skladu s teoremom o potprostorima, rješenja leže u konačnom broju racionalnih potprostora i neka je jedan takav potprostor dan sa

$$c_1 x_1 + \cdots + c_v x_v + c_n x_n = 0. \tag{4.17}$$

Ako je $c_v \neq 0$, bez smanjenja općenitosti možemo uzeti $c_v > 0$, pa za $\underline{\underline{x}}$ koji zadovoljava jednadžbu (4.17) imamo

$$\begin{aligned} c_v \left\|\alpha_1 q_1 + \cdots + \alpha_v q_v\right\| &= c_v \left|\alpha_1 q_1 + \cdots + \alpha_v q_v - p\right| \\ &= \left|(c_v\alpha_1 - c_1\alpha_v)q_1 + \cdots + (c_v\alpha_{v-1} - c_{v-1}\alpha_v)q_{v-1} - (c_v + c_n\alpha_v)p\right| \\ &= \left|c_v + c_n\alpha_v\right| \left|\alpha_1' q_1 + \cdots + \alpha_{v-1}' q_{v-1} - p\right|, \end{aligned} \tag{4.18}$$

gdje je $\alpha_i' = \frac{c_v\alpha_i - c_i\alpha_v}{c_v + c_n\alpha_v}$ $(i = 1, \ldots, v)$.

Za $v = 1$ dobivamo $c_1 \left\|\alpha_1 q_1\right\| \gg |p| \geq 1$ ako je q velik, pa iz (4.9), tj. $|q_1|^{1+\delta} \left\|\alpha_1 q_1\right\| < 1$ slijedi $\frac{1}{c_1}|q_1|^{1+\delta} \ll 1$. Dakle, u ovom slučaju je q ograničen, pa (4.9) ima samo konačno mnogo rješenja.

Za $v > 1$ vrijedi

$$\left|q_1 q_2 \cdots q_{v-1}\right|^{1+\frac{\delta}{2}} \left\|\alpha_1' q_1 + \cdots + \alpha_{v-1}' q_{v-1}\right\| \overset{(4.18)}{\ll} \left|q_1 q_2 \cdots q_{v-1} q_v\right|^{1+\frac{\delta}{2}} c_v \left\|\alpha_1 q_1 + \cdots + \alpha_v q_v\right\|,$$

pa za dovoljno velik q, iz (4.9) zaključujemo da je

$$\left|q_1 q_2 \cdots q_{v-1}\right|^{1+\frac{\delta}{2}} \left\|\alpha_1' q_1 + \cdots + \alpha_{v-1}' q_{v-1}\right\| < 1. \tag{4.19}$$

Kako su $1, \alpha_1', \ldots, \alpha_{v-1}'$ linearno nezavisni nad $\mathbb{Q}$, indukcijom se pokazuje da (4.19), pa i (4.9) ima konačno rješenja.

Isti je dokaz ako je $c_j \neq 0$ za $j \in \{1, 2, \ldots, v-1\}$, a slično se rješava i slučaj $c_1 = \cdots = c_v = 0$, $c_n \neq 0$. ■

Prisjetimo se da je Rothov teorem bio neefektivan u smislu da nije davao ograde za p i q u nejednadžbi (1.10), no mogu se dobiti ocjene za broj rješenja te nejednadžbe i takve rezultate smo predstavili u §3.5. Slični zaključci vrijede i kod teorema o potprostorima. Ne možemo ocijeniti koeficijente definirajućih jednadžbi za potprostore (usp. (4.14)), ali se mogu dati ograde za *broj* potprostora.

Teorem* 4.12 (Schmidt, 1989.). *Neka su $L_1, \ldots, L_n$ linearno nezavisne forme s koeficijentima iz brojevnog polja stupnja d. Promotrimo nejednadžbu*

$$\left|L_1(\underline{\underline{x}}) \cdots L_n(\underline{\underline{x}})\right| < \left|\det(L_1, \ldots, L_n)\right| \left|\underline{\underline{x}}\right|^{-\delta},$$

gdje je $0 < \delta < 1$. *Tada postoje pravi potprostori* $S_1, \ldots, S_t$ *od* $\mathbb{Q}^n$, *gdje je*

$$t = \left\lfloor (2d)^{2^{26n\delta^{-2}}} \right\rfloor$$

takvi da sva cjelobrojna rješenja $\underline{\underline{x}} \neq \underline{\underline{0}}$ *leže u uniji* $S_1, \ldots, S_t$ *i kugle*

$$\left|\underline{\underline{x}}\right| \leq \max\left\{(n!)^{\frac{8}{\delta}}, \mathrm{H}(L_1), \ldots, \mathrm{H}(L_n)\right\}$$

Prema [Fu 04] do sad je najbolji kvantitativni rezultat dobio J.-H. Evertse.

Schmidtov teorem o potprostorima generaliziran je u raznim smjerovima, više o tome u [Sch 91, Ev 00, Fu 04] i drugdje.

Prikažimo u nastavku jedno područje gdje teorem o potprostorima igra važnu ulogu (v. [Ev 00]).

4.3 Linearni rekurzivni nizovi

Najpoznatiji primjer linearnog rekurzivnog niza je Fibonaccijev niz $(F_n)_{n\in\mathbb{N}_0}$ zadan sa $F_0 = 0$, $F_1 = 1$ i $F_n = F_{n-1} + F_{n-2}$ za $n \geq 2$. Općenito, *linearni rekurzivni niz* je niz $U = (U_n)_{n\in\mathbb{N}_0}$ kompleksnih brojeva kojemu su dane početne vrijednosti $U_0, \ldots, U_{k-1}$ i vrijedi linearna rekurzivna relacija

$$U_n = c_1 U_{n-1} + c_2 U_{n-2} + \cdots + c_k U_{n-k} \qquad \text{za} \quad n \geq k, \tag{4.20}$$

gdje su $c_1, \ldots, c_k$ fiksirani kompleksni brojevi.

Može se pokazati da U zadovoljava samo jednu rekurzivnu relaciju za koju je k minimalan. Ako je u relaciji (4.20) broj k minimalan, onda k zovemo *red*, a

$$F_U(X) = X^k - c_1 X^{k-1} - \cdots - c_k$$

karakteristični polinom od U. Napišimo $F_U(X) = (X - \alpha_1)^{e_1} \cdots (X - \alpha_t)^{e_t}$, pri čemu su $\alpha_1, \ldots, \alpha_t$ različiti korijeni od F_U, a $e_1, \ldots, e_t$ su prirodni brojevi. Osnovni teorem za linearne rekurzivne relacije (v. [Ve 01, str. 125]) kaže da postoje polinomi $f_i \in \mathbb{C}[X]$, stupnja $< e_i$ $(i = 1, \ldots, t)$ takvi da je

$$U_n = f_1(n)\alpha_1^n + \cdots + f_t(n)\alpha_t^n \qquad \text{za} \quad n \in \mathbb{N}_0. \tag{4.21}$$

Za niz U kažemo da je *jednostavan* ako su sve kratnosti e_i jednake 1, a U zovemo *nedegeneriran* ako nijedan od kvocijenata α_i/α_j $(1 \leq i < j \leq t)$ nije korijen od 1. Nedegeneriranost povlači da je za svaki prirodan broj k, broj korijena karakterističnog polinoma od $U^{(k)} = (U_{nk})_{n\in\mathbb{N}_0}$ jednak broju korijena karakterističnog polinoma od U.

Zanima nas diofantska jednadžba $U_n = 0$, tj.

$$f_1(n)\alpha_1^n + \cdots + f_t(n)\alpha_t^n = 0 \qquad \text{u} \quad n \in \mathbb{N}_0. \tag{4.22}$$

Klasični Skolem-Mahler-Lechov teorem govori da je broj rješenja od (4.22) konačan ako je U nedegeneriran. Dokaz te tvrdnje koristio je p-adsku analizu. Označimo broj rješenja od (4.22) s N_U. Jedna hipoteza pripisana Wardu tvrdi da se N_U može ograditi odozgo veličinom koja ovisi samo o redu od U. Kroz protekla desetljeća, dobivena su neka djelomična rješenja ovog problema (Beukers, Tijdeman, Schlickewei, Schmidt). Konačno je Schmidt 1999. godine potpuno riješio Wardovu hipotezu.

Teorem* 4.13 (Schmidt). *Pretpostavimo da je U nedegenerirani linearni rekurzivni niz reda k. Tada je*

$$N_U \leq \exp\exp\exp(3k\log k).$$

U svom dokazu Schmidt koristi kvantitativnu verziju teorema o potprostorima koju su dokazali Evertse i Schlickewei.

Više o upotrebi teorema o potprostorima u diofantskim problemima s linearnim rekurzijama može se naći u članku C. Fuchsa [Fu 04].

4.4 p-adska verzija teorema o potprostorima

Godine 1977. Schlickewei je dokazao tzv. p-adsku verziju teorema o potprostorima koja uključuje osim uobičajene apsolutne vrijednosti i konačan broj p-adskih apsolutnih vrijednosti. Za racionalni broj $\alpha \in \mathbb{Q}$ i prost broj p , definiramo $|\alpha|_p = p^{-w}$, gdje je $w \in \mathbb{Z}$ eksponent takav da je $\alpha = p^w \frac{a}{b}$, pri čemu cijeli brojevi a i b nisu djeljivi s p. Primjerice $|9/8|_2 = 8$ i $|9/8|_3 = 1/9$. Svaka p-adska apsolutna vrijednost $|\cdot|_p$ definira metriku na $\mathbb{Q}$. Uzmemo li metričko upotpunjenje, dobivamo polje $\mathbb{Q}_p$. Neka $\mathbb{C}_p$ označava algebarski zatvarač od $\mathbb{Q}_p$. Na jedinstven način možemo p-adsku apsolutnu vrijednost proširiti na $\mathbb{C}_p$. Detaljniji prikaz prethodnih definicija i tvrdnji može se naći npr. u [La 02, str. 231,469].

Radi uniformnosti oznaka pišemo $|\cdot|_\infty$ za uobičajenu apsolutnu vrijednost $|\cdot|$ i $\mathbb{C}_\infty$ za $\mathbb{C}$. Upotrebljavat ćemo p kao oznaku za ∞ (tzv. beskonačni prosti broj od $\mathbb{Q}$) ili za prost broj. Navedimo sada spomenuti teorem u verziji u kojoj ćemo ga koristiti.

Teorem* 4.14 (p-adski teorem o potprostorima). *Neka $S = \{\infty, p_1, \ldots, p_t\}$ sadrži beskonačni prosti broj i konačno mnogo prostih brojeva iz $\mathbb{N}$. Neka su za $p \in S$*

$$\begin{aligned} L_{1p} &= \alpha_{11p}X_1 + \cdots + \alpha_{1np}X_n, \\ &\vdots \\ L_{np} &= \alpha_{n1p}X_1 + \cdots + \alpha_{nnp}X_n \end{aligned}$$

linearno nezavisne linearne forme s koeficijentima $\alpha_{ijp} \in \mathbb{C}_p$ koji su algebarski nad $\mathbb{Q}$. Nadalje, neka su c_{ip} $(i = 1, \ldots, n,\ p \in S)$ realni brojevi koji zadovoljavaju

$$\sum_{p\in S}\sum_{i=1}^{n} c_{ip} < 0.$$

Promotrimo sustav nejednadžbi

$$\left|L_{ip}(\underline{\underline{x}})\right|_p \leq \left|\underline{\underline{x}}\right|^{c_{ip}} \qquad (p \in S,\ i = 1, \ldots, n) \tag{4.23}$$

koji treba riješiti u $\underline{\underline{x}} \in \mathbb{Z}^n$. *Tada postoje pravi linearni potprostori* $T_1, \ldots, T_t$ *od* $\mathbb{Q}^n$ *takvi da je skup rješenja od* (4.23) *sadržan u* $T_1 \cup \cdots \cup T_t$.

Kao ilustraciju primjene ovog teorema pogledajmo jednadžbu (v. [Ev 00])

$$2^{z_1} + 2^{z_2} - 11^{z_3} = 1 \tag{4.24}$$

koju treba riješiti u $z_1, z_2, z_3 \in \mathbb{Z}$.
Lako je vidjeti da (4.24) ima rješenja samo s nenegativnim z_1, z_2, z_3. Stavimo $x_1 = 2^{z_1}$, $x_2 = 2^{z_2}$, $x_3 = 11^{z_3}$, $\xi = \log x_1 / \log x_3$, $\eta = \log x_2 / \log x_3$, $\underline{\underline{x}} = (x_1, x_2, x_3)$. Tada je $\left|\underline{\underline{x}}\right| = x_3$ i $0 \leq \xi, \eta \leq 1$. Zato postoje $k, l \in \{0, 1, 2\}$ za koje je $\frac{k}{3} \leq \xi \leq \frac{k+1}{3}$ i $\frac{l}{3} \leq \eta \leq \frac{l+1}{3}$. Promatramo rješenja dane jednadžbe za fiksirane vrijednosti od k, l. Ta rješenja zadovoljavaju nejednakosti

$$\begin{array}{lll}
|x_1|_\infty \leq \left|\underline{\underline{x}}\right|^{\frac{k+1}{3}}, & |x_2|_\infty \leq \left|\underline{\underline{x}}\right|^{\frac{l+1}{3}}, & |x_1 + x_2 - x_3|_\infty \leq \left|\underline{\underline{x}}\right|^0 \\
|x_1|_2 \leq \left|\underline{\underline{x}}\right|^{-\frac{k}{3}}, & |x_2|_2 \leq \left|\underline{\underline{x}}\right|^{-\frac{l}{3}}, & |x_3|_2 \leq \left|\underline{\underline{x}}\right|^0 \\
|x_1|_{11} \leq \left|\underline{\underline{x}}\right|^0, & |x_2|_{11} \leq \left|\underline{\underline{x}}\right|^0, & |x_3|_{11} \leq \left|\underline{\underline{x}}\right|^{-1}.
\end{array}$$

Ovaj sustav je poseban slučaj od (4.23) i budući da je suma eksponenata jednaka $-1/3 < 0$, možemo upotrijebiti p-adski teorem o potprostorima za $n = 3$. Uzimajući u obzir mogućnosti za k i l, vidimo da $\underline{\underline{x}} = (x_1, x_2, x_3) = (2^{z_1}, 2^{z_2}, 11^{z_3})$ leži u uniji konačno mnogo pravih linearnih potprostora od $\mathbb{Q}^3$. Promatrajući rješenja u jednom potprostoru, zaključujemo da možemo eliminirati jednu od varijabli x_1, x_2, x_3 i dobiti jednadžbu istog tipa kao i (4.24), ali u samo dvije varijable. Ponovno primjenjujući p-adski teorem o potprostorima, ali sada za $n = 2$, dobivamo da rješenja leže u konačno mnogo jednodimenzionalnih potprostora. Na kraju dobivamo da (4.24) ima samo konačno mnogo rješenja.

Zahvale

Najljepše zahvaljujem svojem mentoru, prof. dr. sc. Andreju Dujelli, za odabir teme i korisne savjete. Hvala svim učiteljima i profesorima u mojem dosadašnjem školovanju, ponajprije Vladi Stošiću i Petru Mladiniću.

Hvala mojim prijateljima i prijateljicama na podršci. Hvala svima koji su me upozorili na pogreške, ne samo u ovom radu.

Posebno hvala mojoj tetki Ruži koja se potrudila detaljno pročitati rad. Hvala i bratićima, Petru i Stjepanu, što su joj to dopustili. Hvala Jasni na jednom upozorenju.

Hvala svima koji su čitajući ili listajući moj diplomski rad došli do ovih zahvala. Hvala onima koje nisam poimence naveo u zahvalama iako su to zaslužili. Oprostite mi.

Mojoj braći, Branimiru i Marku, i mojim roditeljima – hvala. Više od toga bilo bi premalo.

Literatura

[Ba 90] Baker, A. – *Transcendental number theory.* Second edition. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1990.

[Bu 04] Bugeaud, Y. – *Approximation by algebraic numbers.* Cambridge Tracts in Mathematics, **160.** Cambridge University Press, Cambridge, 2004.
Dodatak bibliografiji s najnovijim radovima:
`http://www-irma.u-strasbg.fr/~bugeaud/travaux/UpdatesRef.pdf`

[BT 04] Burger, E. B.; Tubbs, R. – *Making transcendence transparent. An intuitive approach to classical transcendental number theory.* Springer-Verlag, New York, 2004.

[Co 04] Cosgrave, J. B. – *An Introduction to the History of Transcendental Numbers.*
`http://www.spd.dcu.ie/johnbcos/transcendental_numbers.htm`

[Du 99] Dujella, A. – *Skripta iz uvoda u teoriju brojeva.*
`http://www.math.hr/~duje/utb/utblink.pdf`

[Dy 96] Dyson, F. – *Selected papers of Freeman Dyson with commentary.* With a foreword by Elliott H. Lieb. Collected Works, **5.** American Mathematical Society, Providence, RI; International Press, Cambridge, MA, 1996.

[E 73] Everett, C. J. – *Fermat's conjecture, Roth's theorem, Pythagorean triangles, and Pell's equation.* Duke Math. J. **40** (1973), 801–804.

[Ev 00] Evertse, J.-H. – *Diophantine equations and Diophantine approximation.* Biennial report 2000&2001 of the Thomas Stieltjes Institute for Mathematics.
`http://www.math.leidenuniv.nl/~evertse/02-stieltjes.pdf`

[Fe 81] Fel'dman, N. I. – *Приближения алгебраических чисел.* Moskov. Gos. Univ., Moskva, 1981.

[Fu 04] Fuchs, C. – *Diophantine problems with linear recurrences via the Subspace Theorem.* Integers: Electronic Journal of Combinatorial Number Theory **5(3)** (2005), #A08.
`http://finanz.math.tu-graz.ac.at/~fuchs/publ/dplrss2.pdf`

[Hi 64] Khinchin, A. Ya. – *Continued fractions.* Reprint of the 1964 translation. Dover Publications, Inc., Mineola, NY, 1997.

[La 02] Lang, S. – *Algebra.* Revised third edition. Graduate Texts in Mathematics, **211.** Springer-Verlag, New York, 2002.

[Ma 77] Marcus, D. A. – *Number fields.* Universitext. Springer-Verlag, New York-Heidelberg, 1977.

[Sch 80] Schmidt, W. M. – *Diophantine approximation.* Lecture Notes in Mathematics, **785.** Springer-Verlag, Berlin, 1980.

[Sch 91] Schmidt, W. M. – *Diophantine approximations and Diophantine equations.* Lecture Notes in Mathematics, **1467.** Springer-Verlag, Berlin, 1991.

[Sch 95] Schmidt, W. M. – *The number of exceptional approximations in Roth's theorem.* J. Austral. Math. Soc. Ser. A **59** (1995), no. 3, 375–383.

[St 05] Steuding, J. – *Diophantine analysis.* Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2005.

[Un 94] Ungar, Š. – *Matematička analiza 3.* Prirodoslovno-matematički fakultet–Matematički odjel, Zagreb, 1994.
`http://www.math.hr/~ungar/Analiza3_internet.pdf`

[Ve 01] Veljan, D. – *Kombinatorna i diskretna matematika.* Algoritam, Zagreb, 2001.

[Wa 93] Waldschmidt, M. – *Introduction to Recent Results in Transcendental Number Theory.* Workshop and conference in number theory, Hong-Kong, 1993.
`http://www.institut.math.jussieu.fr/~miw/articles/ps/irrtnt.ps`

[Wa 04] Waldschmidt, M. – *Open Diophantine problems.* Mosc. Math. J. **4** (2004), no. 1, 245–305.
`http://www.institut.math.jussieu.fr/~miw/articles/pdf/odp.pdf`