Minorazioni dell'altezza di numeri algebrici: qualche risultato recente

Francesco Amoroso

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen
France

Altezza: numeri razionali

Altezza = misura della complessità aritmetica.

Per $r = p/q \in \mathbb{Q}$ con $p \in \mathbb{Z}$, $q \in \mathbb{N}$, $\gcd(p, q) = 1$,

$$h(r) := \log \max(|p|, q).$$

Esempio : $h(2) = h(2/1) = \log 2$; $h(2,05) = h(41/20) = \log 41$.

Osservazione : $h(r) \geq 0$ e $h(r) = 0 \Leftrightarrow r \in \{-1, 0, 1\}$.

Altezza: interi algebrici

Per α intero algebrico di grado d e coniugati $\alpha_1, \ldots, \alpha_d$,

$$h(\alpha) := \frac{1}{d} \sum_{j=1}^{d} \log^+ |\alpha_j|$$

dove $\log^+(x) := \log \max(x, 1)$ per $x \geq 0$.

Osservazione : $h(\alpha) \geq 0$ e $h(\alpha) = 0 \Leftrightarrow \alpha = 0$ oppure radice di 1.

Osservazione : per $j = 1, \ldots, d$ si ha $h(\alpha_j) = h(\alpha)$.

Altezza: numeri algebrici

Per $\alpha \in \overline{\mathbb{Q}}$ di grado d e coniugati $\alpha_1, \ldots, \alpha_d$, equazione minima f (*i.e.* $f \in \mathbb{Z}[x]$ irriducibile, $f(\alpha) = 0$), coefficiente direttore $a > 0$,

$$h(\alpha) := \frac{1}{d}\left(\log a + \sum_{j=1}^{d} \log^+ |\alpha_j|\right).$$

Proprietà:

- h è invariante per l'azione del gruppo di Galois.
- $h(\alpha) \geq 0$ e $h(\alpha) = 0 \Leftrightarrow \alpha = 0$ o radice di 1.
- $h(\alpha\beta) \leq h(\alpha) + h(\beta)$.
- $h(\alpha\omega) = h(\alpha)$ per ω radice di 1.
- $h(\alpha^n) = nh(\alpha)$ $(n \in \mathbb{N})$.
- Un insieme di algebrici di grado e altezza limitata è finito.

Osservazione : Se α non è intero, $h(\alpha) \geq \frac{\log 2}{d}$.
La stessa cosa vale se α non è un'unità.

Esempi di altezze di interi algebrici

Formula: $h(\alpha) := \frac{1}{d} \sum_{j=1}^{d} \log^+ |\alpha_j|$.

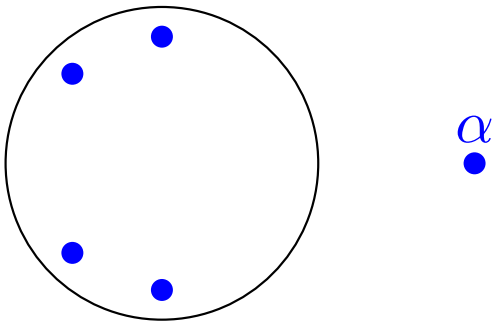
$h(\sqrt[d]{2}) = \frac{1}{d}\left(d \log \sqrt[d]{2}\right) = \frac{1}{d} \log 2.$

$h(\frac{1+\sqrt{5}}{2}) = \frac{1}{2} \log \frac{1+\sqrt{5}}{2}.$

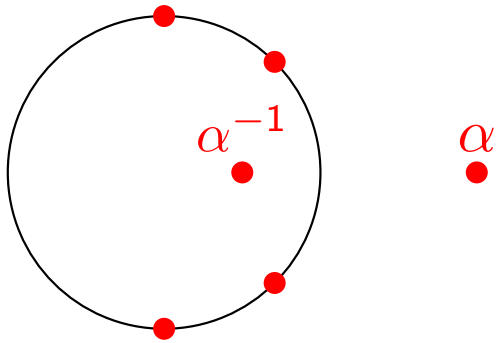
$$h(\tfrac{1+\sqrt{5}}{2} \cdot \sqrt[3]{2}) = \tfrac{1}{6} \times 3 \log(\tfrac{1+\sqrt{5}}{2} \cdot \sqrt[3]{2}) = \tfrac{1}{2} \log(\tfrac{1+\sqrt{5}}{2}) + \tfrac{1}{6} \log 2$$
$$= h(\tfrac{1+\sqrt{5}}{2}) + h(\sqrt[3]{2}).$$

Numeri di Pisot e Salem

Pisot



Salem



$$h(\alpha) = \tfrac{1}{d} \log \alpha$$

Più piccolo numero di Pisot: radice reale $\theta_0 \approx 1.324\ldots$
di $x^3 - x - 1$.

Più piccolo numero di Salem? Radice reale $\lambda_0 \approx 1.176\ldots$
di $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$?

Numeri e polinomi reciproci

I numeri di Salem sono particolari numeri algebrici *reciproci*. Un algebrico α è reciproco se α^{-1} è un suo coniugato.

Sia $P(x) = p_0 + p_1 x + \cdots + p_d x^d$. Il polinomio *reciproco* di P è

$$P^*(x) = x^d P(1/x) = p_0 x^d + p_1 x^{d-1} + \cdots + p_d.$$

Diciamo che P è reciproco se $P^* = P$.

Dunque α è reciproco se e solo se il suo polinomio minimo lo è (a meno di una costante moltiplicativa).

I numeri di Pisot *non sono* reciproci.

Congettura di Lehmer

Congettura (Lehmer 1933)

Esiste una costante $c > 0$ tale che per ogni intero algebrico α di grado d, diverso da 0 e da una radice dell'unità,

$$h(\alpha) \geq \frac{c}{d}.$$

Versione ancora più ottimista: $c = \log(\lambda_0)$.

Congettura di Lehmer: *state of the art*

La congettura è dimostrata per

- α *non reciproci* ($c = \log(\theta_0)$).

  [Breusch 1951; Smyth 1971]

- α tali che $\mathbb{Q}(\alpha)/\mathbb{Q}$ *galoisiana*.

  [A.-David 1999]

- α con *polinomio minimo a coefficienti dispari* ($c = \frac{1}{4}\log 5$).

  [Borwein - Dobrowolski - Mossinghoff 2007]

- $d \leq 55$ ($c = \log(\lambda_0)$).

  [Mossinghoff - Rhin - Qiang 2008]

Congettura di Lehmer: *state of the art*

Teorema (Dobrowolski 1979)

Esiste una costante $c > 0$ tale che per ogni intero algebrico α di grado d, diverso da 0 e da una radice dell'unità,

$$h(\alpha) \geq \frac{c}{d} \cdot \varepsilon(d)$$

dove

$$\varepsilon(d) = \left(\frac{\log(3d)}{\log\log(3d)} \right)^{-3}.$$

Un'idea della dimostrazione

Sia α un intero *razionale*, $\alpha \neq -1, 0, 1$. Ovviamente

$$h(\alpha) = \log|\alpha| \geq \log 2 \approx 0.693\ldots$$

Diamo una prova ... più complicata di un risultato più debole.

Sia p un primo. Per il piccolo teorema di Fermat, $\alpha^p \equiv \alpha \mod p$. Per ipotesi $\alpha^p \neq \alpha$. Dunque

$$p \leq |\alpha^p - \alpha| \leq 2|\alpha|^p$$

e

$$h(\alpha) = \log|\alpha| \geq \frac{\log(p/2)}{p}.$$

Scegliendo $p = 5$ si ottiene $h(\alpha) \geq \frac{\log(5/2)}{5} \approx 0.183\ldots$

Casa e congettura di Schinzel-Zassenhaus

Chiamiamo *casa (house)* $\overline{|\alpha|}$ di α il massimo modulo dei coniugati di α. Si noti che $h(\alpha) \leq \log \overline{|\alpha|}$ $(\star)$.

Congettura (Schinzel-Zassenhaus, 1965)

Esiste una costante $c > 0$ tale che per ogni intero algebrico α di grado d, diverso da 0 e da una radice dell'unità,

$$\overline{|\alpha|} \geq e^{c/d} \sim 1 + \frac{c}{d}, \qquad (d \to +\infty).$$

Per $(\star)$ la congettura di Lehmer implica la precedente.

D'altra parte, per un numero di Salem, $h(\alpha) = \frac{1}{d} \log \overline{|\alpha|}$ e in questo caso Schinzel-Zassenhaus non dà niente per Lehmer.

Osservazione: se α non è un unità, $\overline{|\alpha|} \geq 2^{1/d}$.

Teorema di Dimitrov

Teorema (Dimitrov, 2020)

La congettura di Schinzel-Zassenhaus è vera: per ogni intero algebrico α di grado d, diverso da 0 e da una radice dell'unità, si ha

$$\overline{|\alpha|} \geq 2^{1/4d}.$$

Idea della dimostrazione.

Sia P il polinomio minimo di un intero algebrico di grado d, diverso da 0 e da una radice dell'unità, di coniugati $\alpha_1, \ldots, \alpha_d$. Si dimostra, utilizzando congruenze, che

$$f(z) := \sqrt{\prod_{j=1}^{d}(1-\alpha_j^2/z)(1-\alpha_j^4/z)}$$

si sviluppa in serie a coefficienti *interi* in un intorno di ∞. Un criterio di razionalità di Polya, mostra poi che, se

$$\overline{|\alpha|} < 2^{1/4d},$$

allora f è una funzione razionale. Se si suppone

$$P_2(x) := \prod_{j=1}^{d}(x-\alpha_j^2)$$

irriducibile, questo forza α ad essere $= 0$ o $=$ radice di 1, contraddizione. Se P_2 è riducibile si procede per induzione.

Dimostrazione. I. Congruenze

Nel seguito: $P(x) = a\prod_{j=1}^{d}(x-\alpha_j)$ a coefficienti interi. Per $n \in \mathbb{N}$ poniamo: $P_n(x) := a^n \prod_{j=1}^{d}(x-\alpha_j^n) \in \mathbb{Z}[x]$.

Sia ℓ un primo. Allora[1]

$$P_\ell(x^\ell) = a^\ell \prod_{j=1}^{d}(x^\ell - \alpha_j^\ell) \equiv P(x)^\ell \equiv P(x^\ell) \mod \ell\mathbb{Z}[x]$$

e dunque

$$P_\ell \equiv P \mod \ell\mathbb{Z}[x].$$

Per $\ell = 2$, con un po' più di fatica:

Lemma

$$P_2 \equiv P_4 \mod 4\mathbb{Z}[x].$$

[1] usando $(x+y)^\ell \equiv x^\ell + y^\ell \mod \ell\mathbb{Z}[x,y]$ e il piccolo teorema di Fermat.

Dimostrazione. II. Una serie intera

Lemma

$$P_2 \equiv P_4 \mod 4\mathbb{Z}[x].$$

Utilizzando lo sviluppo in serie a coefficienti *interi* nell'intorno dell'origine

$$\sqrt{1+4z} = \sum_{k=0}^{\infty} \binom{1/2}{k} 4^k z^k$$

se ne deduce:

Corollario

Supponiamo $P(0) = 1$. *Allora*

$$\sqrt{P_2(z)P_4(z)}$$

si sviluppa in serie a coefficienti interi in un intorno dell'origine.

Dimostrazione. II. Una serie intera

- $P_2 \equiv P_4 \mod 4\mathbb{Z}[x]$.
- $\sqrt{1+4z}$ si sviluppa in serie a coefficienti *interi* nell'intorno dell'origine.

Corollario

Supponiamo $P(0) = 1$. Allora $\sqrt{P_2(z)P_4(z)}$ si sviluppa in serie a coefficienti interi in un intorno dell'origine.

Dim. Scriviamo $Q := P_2P_4 = U^2 + 4V$ con $U,\ V \in \mathbb{Z}[x]$. Allora $\sqrt{Q} = U\sqrt{1+4z}$ con $z := V/U^2$ che si sviluppa in serie intera nell'origine con termine costante 0 (infatti $Q(0) = 1$ e dunque $U(0) = 1$ e $V(0) = 0$).

□

Dimostrazione. III. Un criterio di razionalità

Teorema (Polya, anni '20)

Sia $\mathcal{K} \subset \mathbb{C}$ un compatto, simmetrico rispetto all'asse reale, con complementare $\mathbb{C}\backslash\mathcal{K}$ connesso. Sia $f(z)$ una funzione complessa, analitica in $\mathbb{C}\backslash\mathcal{K}$. Supponiamo:

- $\delta(K) < 1$.
- $f(z) = \sum_{k=0}^{\infty} a_k z^{-k}$ *in un intorno di* ∞, *con* $a_k \in \mathbb{Z}$.

Allora f è razionale.

Nel teorema, $\delta(K)$ è il *diametro transfinito* di $\mathcal{K}$,

$$\delta(K) = \lim_{n\to+\infty} \max_{z_1,\dots,z_n\in\mathcal{K}} \prod_{1\le i<j\le n} |z_i - z_j|^{\frac{2}{n(n-1)}}$$

Esempi: $\delta(|z| \le r) = \delta(|z| = r) = r$,

$$\delta([a,b]) = (b-a)/4.$$

Teorema di Polya: un esempio e un contro-esempio

Sia $r \in (0,1)$ e scegliamo $\mathcal{K} = \{|z| \leq r\}$, dunque $\delta(K) < 1$.

Sia f analitica nel complementare di $\mathcal{K}$ e supponiamo $f(z) = \sum_{k=0}^{\infty} a_k z^{-k}$ in un intorno di ∞, con coefficienti $a_k \in \mathbb{Z}$.

Osserviamo che $z = 1$ appartiene al complementare di $\mathcal{K}$, dunque la serie $\sum_{k=0}^{\infty} a_k$ converge, ed in particolare $\lim_{k\to\infty} a_k = 0$.
Ma gli a_k sono *interi*, dunque $a_k = 0$ definitivamente e f è un polinomio.

$\circ \bullet \circ \bullet \circ \bullet \circ$

Sia ora $f(z) = \sum_{n=0}^{\infty} z^{-2^n}$.

Allora f converge nel complementare del disco unitario (di diametro transfinito esattamente 1).

D'altra parte $f(z) \notin \mathbb{Q}(z)$, altrimenti $f(10) \in \mathbb{Q}$ avrebbe uno sviluppo decimale non definitivamente periodico.

Qualche proprietà del diametro transfinito

Il diametro transfinito è monotono rispetto all'inclusione di insiemi:

$$\mathcal{K}_1 \subseteq \mathcal{K}_2 \Rightarrow \delta(\mathcal{K}_1) \leq \delta(\mathcal{K}_2),$$

invariante per traslazioni, e rispetta le omotetie:

$$\delta(\lambda\mathcal{K} + w) = \lambda\delta(\mathcal{K}) \qquad (\lambda > 0, \quad w \in \mathbb{C}).$$

Se $F \in \mathbb{C}[z]$ è monico di grado n si ha $\delta(F^{-1}(\mathcal{K})) = \delta(\mathcal{K})^{1/n}$.
In particolare se $n > 1$ e $F^{-1}(\mathcal{K}) = \mathcal{K}$ allora $\delta(\mathcal{K}) = 1$.
Se ne deduce:

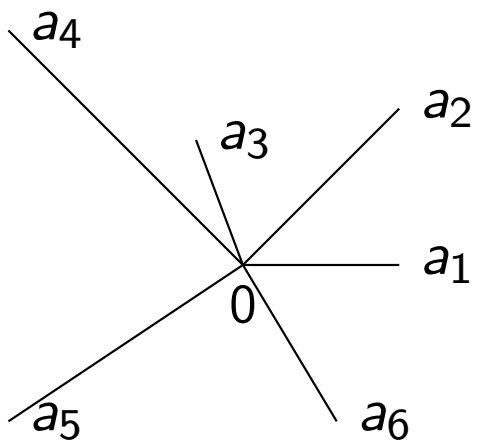
$\delta(|z| \leq 1) = \delta(|z| = 1) = 1$ (scegliere $F(z) = z^2$).

$\delta([-2, 2]) = 1$ (scegliere $F(z) = z^2 - 2$).

Dunque $\delta(|z| \leq r) = \delta(|z| = r) = r$ e $\delta([a, b]) = \frac{b-a}{4}$.

Dimostrazione. IV. Ricci e radici quadrate.

Chiamiamo *riccio (hedgehog)* di vertici $a_1, \ldots, a_n \in \mathbb{C}$ l'unione $\mathcal{K}(a_1, \ldots, a_n)$ dei segmenti $[0, a_j]$ che uniscono l'origine del piano complesso con i punti a_i.

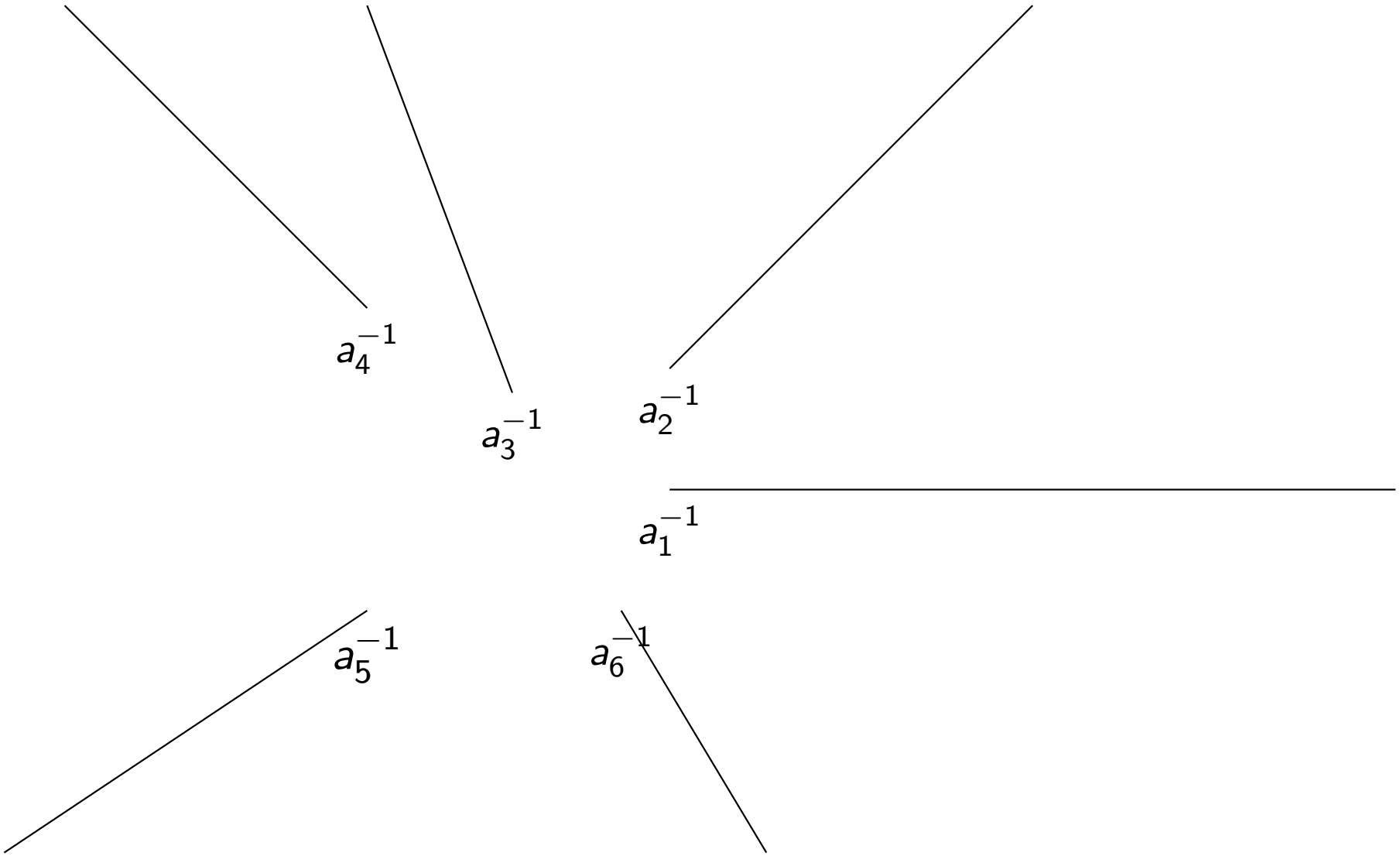


La funzione $F(z) = \prod_j (1 - a_j/z)$ è analitica e non nulla nel dominio semplicemente connesso $\mathbb{C} \cup \{\infty\} \backslash \mathcal{K}(a_1, \ldots, a_n)$.

Dunque $\sqrt{F}$ è analitica nel complementare del riccio $\mathcal{K}(a_1, \ldots, a_n)$.

Dimostrazione. IV. Perchè "riccio"?

Immagine di $\mathcal{K}(a_1, \ldots, a_n)$ per $z \to z^{-1}$.



Dimostrazione. IV. Ricci e diametro transfinito.

Sia $\omega_n = e^{\frac{2\pi i}{n}}$. Allora

$$\mathcal{K}(\omega_1, \ldots, \omega_n) = F^{-1}([0,1])$$

con $F(z) = z^n$, dunque $\delta(\mathcal{K}(\omega_1, \ldots, \omega_n)) = \delta([0,1])^{1/n} = 4^{-1/n}$.

Teorema (Dubinin, 1985)

Siano $a_1, \ldots, a_n$ di modulo 1. Il riccio $\mathcal{K}(a_1, \ldots, a_n)$ ha diametro transfinito $\leq 4^{-1/n}$ e l'eguaglianza vale se e solo se $a_1, \ldots, a_n$ sono i vertici di un n-agono regolare inscritto nel cerchio unitario.

Utilizzando monotonicità e omogenità per omotetie se ne deduce:

Corollario

Il riccio $\mathcal{K}(a_1, \ldots, a_n)$ ha diametro transfinito

$$\leq 4^{-1/n} \max_i |a_i|.$$

Dimostrazione. V. Riduzioni

Sia $P = \prod_{j=1}^{d}(x - \alpha_j)$ il polinomio minimo di un intero algebrico $\alpha \notin \{0, \text{radici di } 1\}$.

Possiamo supporre $P_2 = \prod_{j=1}^{d}(x - \alpha_j^2)$ irriducibile. Altrimenti α^2 ha grado $d/2$ e per ricorrenza

$$\overline{|\alpha|}^2 = \overline{|\alpha^2|} \geq 2^{1/2d}$$

da cui $\overline{|\alpha|} \geq 2^{1/4d}$.

Consideriamo il polinomio reciproco

$$P^*(x) = x^d P(1/x) = \prod_{j=1}^{d}(1 - \alpha_j x).$$

Osservazione: $P^*(0) = 1$ e $(P^*)_n = (P_n)^*$.

Dimostrazione. VI. Conclusione

- P pol. minimo di $\alpha \notin \{0, \text{radici di } 1\}$, di coniugati $\alpha_1, \ldots, \alpha_d$.
- $P_2 = \prod_{j=1}^{d}(x - \alpha_j^2)$ irriducibile.
- $P^*(x) = x^d P(1/x) = \prod_{j=1}^{d}(1 - \alpha_j x)$.

Sia

$$F(z) := P_2^*(1/z)P_4^*(1/z) = \prod_{j=1}^{d}(1 - \alpha_j^2/z)(1 - \alpha_j^4/z).$$

Per quanto visto (con P^* al posto di P), $f = \sqrt{F}$ si sviluppa in serie a coefficienti *interi* in un intorno di ∞. Inoltre f è analitica nel complementare del riccio

$$\mathcal{K}(\alpha_1^2, \ldots, \alpha_d^2, \alpha_1^4, \ldots, \alpha_d^4).$$

Dimostrazione. VI. Conclusione

- $\alpha \notin \{0, \text{radici di } 1\}$, di coniugati $\alpha_1, \ldots, \alpha_d$.
- $\prod_{j=1}^{d}(x - \alpha_j^2)$ irriducibile.
- $f(z) = \sqrt{\prod_{j=1}^{d}(1 - \alpha_j^2/z)(1 - \alpha_j^4/z)}$ si sviluppa in serie a coefficienti *interi* in un intorno di ∞ ed è analitica fuori dal riccio $\mathcal{K} := \mathcal{K}(\alpha_1^2, \ldots, \alpha_d^2, \alpha_1^4, \ldots, \alpha_d^4)$.

Il riccio $\mathcal{K}$ è simmetrico rispetto a $\mathbb{R}$ e ha diametro transfinito

$$\delta \leq 4^{-1/2d} \max_j\{|\alpha_j^2|, |\alpha_j^4|\} = 2^{-1/d}\ \overline{|\alpha|}^4$$

per il teorema di Dubinin. Supponiamo per assurdo $\overline{|\alpha|} < 2^{1/4d}$. Allora $\delta < 1$ e dunque f è razionale per il criterio di Polya.

Dimostrazione. VI. Conclusione

- $\alpha \notin \{0, \text{radici di } 1\}$, di coniugati $\alpha_1, \ldots, \alpha_d$.
- $\prod_{j=1}^{d}(x - \alpha_j^2)$ irriducibile.
- $f(z) = \sqrt{\prod_{j=1}^{d}(1 - \alpha_j^2/z)(1 - \alpha_j^4/z)}$ razionale.

Dunque $\prod_{j=1}^{d}(1 - \alpha_j^2/z)(1 - \alpha_j^4/z)$ è un quadrato.

Ma $\prod_{j=1}^{d}(x - \alpha_j^2)$ è irriducibile, quindi $\alpha_1^2, \ldots, \alpha_d^2$ sono a due a due distinti e dunque $\alpha^2 = \alpha_j^4$ per qualche i. Ma allora

$$2h(\alpha) = h(\alpha^2) = h(\alpha_j^4) = 4h(\alpha_j) = 4h(\alpha)$$

e $h(\alpha) = 0$, contro l'ipotesi $\alpha \neq 0$, $\alpha \neq$ radice di 1.

□

Referenze bibliografiche

- Problema di Lehmer e questioni connesse:

  Carmen Laura Basile, *Il problema di Lehmer*, Tesi di Laurea (relatore F. Amoroso), Torino, Marzo 1999.

- Articolo di Dimitrov:

  V. Dimitrov, *A proof of the Schinzel-Zassenhaus conjecture on polynomials*, `https://arxiv.org/abs/1912.12545`