
UNIVERSITÀ DI PISA

DIPARTIMENTO DI MATEMATICA

Laurea Triennale in Matematica

# Minorazione dell'altezza di numeri algebrici in estensioni abeliane

Relatrice:

**Prof.ssa Ilaria Del Corso**

Candidato:

**Federico Allegri**

ANNO ACCADEMICO 2023/2024

*A Babuška.*

*Vivo e intero,*
*non più in me,*
*ma in ogni cosa fuori.*

# Indice

**Introduzione** **iii**

**1 Preliminari di teoria algebrica dei numeri** **1**
1.1 Campi di numeri . . . . . 1
1.1.1 Fattorizzazione degli ideali . . . . . 1
1.2 Valori assoluti e valutazioni . . . . . 3
1.3 Valori assoluti su $\mathbb{Q}$ . . . . . 4
1.4 Valori assoluti su campi di numeri . . . . . 4
1.5 Completamenti . . . . . 6
1.6 Appendice di teoria analitica dei numeri . . . . . 8

**2 La Misura di Mahler e l'altezza di Weil** **9**
2.1 Misura di Mahler di un polinomio . . . . . 9
2.1.1 Minorazione della misura di Mahler in funzione delle norme indotte . . . . . 11
2.1.2 Il teorema di finitezza di Northcott e il teorema di Kronecker . . . . . 13
2.2 Altezza di Weil di un numero algebrico . . . . . 14
2.2.1 Altezza normalizzata di un polinomio . . . . . 16

**3 Minorazione dell'altezza in un'estensione abeliana** **20**
3.0.1 Lemmi preliminari . . . . . 21
3.0.2 Dimostrazione del risultato principale . . . . . 24
3.1 Applicazioni e Corollarî . . . . . 29
3.1.1 Minorazione della norma in un'estensione abeliana . . . . . 29
3.1.2 Campi ciclotomici . . . . . 30
3.2 Conclusioni e Sviluppi . . . . . 31

**Ringraziamenti** **34**

# Introduzione

La congettura di Lehmer prevede l'esistenza di una costante assoluta $c$ tale che per ogni numero algebrico $\alpha$ non nullo e diverso da una radice dell'unità, di grado $d$, si abbia $h(\alpha) > cd^{-1}$, dove $h$ indica l'altezza di Weil. Questo problema, formulato dal matematico americano Henry Derrick Lehmer nel 1933 è per lo più tuttora aperto.
Sicuramente non è possibile trovare una costante assoluta che minori l'altezza di Weil di un qualunque numero algebrico; basta infatti considerare, per ogni intero $D$, l'intero algebrico $\alpha^{1/D}$, la cui altezza vale $h(\alpha) = \log 2/D$ e che può diventare arbitrariamente piccola all'aumentare di $D$.
Il miglior risultato a oggi conosciuto del problema sopra esposto è dovuto a Dobrowolski, ed è conosciuto come "lower bound di Dobrowolski": questo afferma che per ogni $\epsilon > 0$ esiste una costante $c(\epsilon) > 0$, dipendente da $\epsilon$, tale che $h(\alpha) \geq c(\epsilon)d^{-1-\epsilon}$.
Esiste inoltre un aneddoto molto interessante che concerne la risoluzione di Dobrowolski di questo problema: egli era uno studente del matematico Narkiewicz, al quale chiese un problema da risolvere. Costui gli propose di cimentarsi nella risoluzione di alcuni problemi del suo libro "Elementary and analytic theory of algebraic numbers" [10], sottolineando che fossero tutti problemi aperti. Dobrowolski tentò per lungo tempo di risolvere il primo problema. Dopo molto tempo senza aver ricevuto notizie, Narkiewicz chiese allo studente a che punto fosse nel suo studio e il motivo per il quale egli non si fosse più fatto sentire. Dobrowolski, affranto, rispose che, non essendo ancora riuscito a risolvere il problema, aveva evitato di contattare il docente, al quale presentò poi la sua risoluzione parziale, non sapendo che i problemi aperti sopravvivono al tempo per lunghe decadi e non trovano soluzione nell'arco di pochi giorni. Tale risoluzione parziale è esattamente il lower bound di Dobrowolski citato sopra.

L'obiettivo di questa tesi è quello di analizzare un lavoro svolto dai professori Francesco Amoroso e Roberto Dvornicich, pubblicato in un articolo del 2000, in cui viene trattato il problema di Lehmer nel caso particolare delle estensioni abeliane di $\mathbb{Q}$, cioè limitatamente a numeri algebrici $\alpha$ generatori di un'estensione abeliana dei razionali. Il caso interessante è quello in cui $\alpha$ abbia valore assoluto (ordinario) uguale a 1; il caso complementare, e più semplice, era già stato affrontato dal matematico polacco Andrzej Schinzel nel 1973.

Nel primo capitolo di questa tesi definiremo le nozioni algebriche necessarie alla presentazione del risultato e ricorderemo alcuni risultati della teoria algebrica dei numeri, con un focus sulla definizione dei valori assoluti su campi di numeri e la loro classificazione.

Nel secondo capitolo introdurremo e studieremo la misura di Mahler di un polinomio a coefficienti interi e le sue proprietà. Definiremo poi l'altezza logaritmica di Weil di un numero algebrico $\alpha$ per mezzo dei valori assoluti dei campi di numeri che contengono $\alpha$, mostrando in seguito che essa è indipendente dal campo. Daremo prova infine di come questi due oggetti siano strettamente legati.

Nel terzo capitolo affronteremo il problema di Lehmer per estensioni abeliane di $\mathbb{Q}$, dimostrando il risultato principale del lavoro di Amoroso e Dvornicich. Per farlo daremo alcuni lemmi preliminari: faremo vedere che, sotto determinate ipotesi, si può affermare l'esistenza di un particolare elemento del gruppo di Galois di $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, dove $m$ è un numero naturale, con certe proprietà e che, fissato un valore assoluto non archimedeo su un campo di numeri, esiste sempre un "denominatore locale" di valore assoluto fissato. Utilizzeremo poi questi risultati per dare un bound inferiore all'altezza di Weil rispetto ai numeri primi dispari, per poi focalizzarci sul caso speciale $p = 2$, che porterà, attraverso il teorema di Kronecker-Weber, alla minorazione voluta.
Concludiamo questa tesi mostrando alcune applicazioni del teorema principale: daremo una minorazione della norma di un numero algebrico in un'estensione abeliana e dimostreremo che esiste solo un numero finito di campi ciclotomici il cui anello degli interi è un dominio a ideali principali.
Infine, nell'ultima sezione di conclusioni e sviluppi, sulla base di alcuni lavori di Francesco Amoroso, parleremo di alcuni problemi che generalizzano la congettura di Lehmer, introducendo le proprietà di Bogomolov e Northcott.

Capitolo 1

# Preliminari di teoria algebrica dei numeri

In questo primo capitolo d'introduzione presentiamo in maniera sintetica i concetti fondamentali e alcuni dei risultati della teoria algebrica dei numeri che useremo nel seguito con un focus sulla ramificazione e sui valori assoluti su campi di numeri.

## 1.1 Campi di numeri

Tutti i risultati presentati in questa sezione possono essere trovati dettagliatamente esposti in [6]. Un campo di numeri è un'estensione finita di $\mathbb{Q}$. Dal teorema dell'elemento primitivo sappiamo che ogni campo di numeri $K$ è un'estensione semplice di $\mathbb{Q}$, cioè esiste $\alpha \in K$ tale per cui $K = \mathbb{Q}(\alpha)$. Indichiamo con $\overline{\mathbb{Q}}$ la chiusura algebrica di $\mathbb{Q}$ contenuta in $\mathbb{C}$.

**Definizione 1.1 - Intero algebrico**
Sia $\alpha \in \overline{\mathbb{Q}}$. Diciamo che $\alpha$ è un **intero algebrico** se esiste un polinomio monico, non nullo, a coefficienti in $\mathbb{Z}$ di cui $\alpha$ è radice.

Indichiamo con $\mathbb{A} = \{\alpha \in \overline{\mathbb{Q}} : \alpha \text{ è un intero algebrico}\}$ l'insieme degli interi algebrici. $\mathbb{A}$ è un sottoanello di $\overline{\mathbb{Q}}$.
Dato un campo di numeri $K$, definiamo **l'anello degli interi** di $K$ come il sottoanello $\mathcal{O}_K := \mathbb{A} \cap K$ degli interi algebrici contenuti in $K$.

### 1.1.1 Fattorizzazione degli ideali

In questo paragrafo parliamo di fattorizzazione di ideali in dominî di Dedekind. Per fare ciò occorre dare definizione dei concetti di chiusura integrale e di anello integralmente chiuso.

**Definizione 1.2**
Sia $R$ un dominio con campo dei quozienti $K$. Un elemento $\alpha \in K$ è **intero** su $R$ se è radice di un polinomio monico a coefficienti in $R$. $R$ è detto **integralmente chiuso** se per ogni $\alpha \in K$ con $\alpha$ intero su $R$, $\alpha \in R$.

Definiamo adesso un'importante classe di dominî di integrità, alla quale appartengono anche gli anelli degli interi dei campi di numeri.

**Definizione 1.3 - Dominio di Dedekind**
Un dominio $R$ è un **dominio di Dedekind** se verifica le seguenti proprietà:
1. È noetheriano;
2. Ogni ideale primo non nullo è massimale;
3. È integralmente chiuso.

I dominî di Dedekind godono della proprietà di fattorizzazione unica degli ideali.

**Teorema 1.4**
*In un dominio di Dedekind $R$ ogni ideale proprio non nullo $I$ di $R$ si scrive in modo unico, a meno dell'ordine dei fattori, come prodotto di ideali primi, ovvero*

$$I = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i},$$

*con $\mathfrak{p}_i \in Spec(R)$ e $e_i \geq 0$ per ogni $i = 1, ..., n$.*

Sia $L/K$ è un'estensione di campi di numeri e sia $\mathcal{O}_L/\mathcal{O}_K$ la rispettiva estensione degli anelli degli interi. Consideriamo $\mathfrak{p} \subset \mathcal{O}_K$ un ideale primo e sia $\mathfrak{p}\mathcal{O}_L$ la sua estensione, che, in generale, non è un ideale primo. Per il Teorema 1.4, $\mathfrak{p}$ si fattorizza in $\mathcal{O}_L$ come prodotto di ideali primi:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{n} \mathfrak{P}_i^{e_i}.$$

**Definizione 1.5 - Indice di ramificazione**
Chiamiamo **indice di ramificazione** di $\mathfrak{P}$ sopra $\mathfrak{p}$, e lo indichiamo con $e(\mathfrak{P}|\mathfrak{p})$, l'esponente di $\mathfrak{P}$ che compare nella fattorizzazione di $\mathfrak{p}\mathcal{O}_L$.

**Definizione 1.6 - Grado di inerzia**
Chiamiamo **grado di inerzia** di $\mathfrak{P}$ sopra $\mathfrak{p}$, e lo indichiamo con $f(\mathfrak{P}|\mathfrak{p})$, il grado dell'estensione di campi finiti $\mathcal{O}_L/\mathfrak{P}$ su $\mathcal{O}_K/\mathfrak{p}$.

L'indice di ramificazione e il grado d'inerzia sopra definiti godono della seguente proprietà.

**Proposizione 1.7**
*L'indice di ramificazione e il grado d'inerzia sono moltiplicativi in una torre di estensioni, cioè se $K \subset L \subset F$ sono tre campi di numeri e $\mathfrak{p}, \mathfrak{q}$ e $\mathfrak{f}$ sono tre ideali primi rispettivamente di $K, L$ e $F$ tali che $\mathfrak{f}|\mathfrak{q}|\mathfrak{p}$, allora*

$$e(\mathfrak{f}|\mathfrak{p}) = e(\mathfrak{f}|\mathfrak{q}) \cdot e(\mathfrak{q}|\mathfrak{p})$$

*e*

$$f(\mathfrak{f}|\mathfrak{p}) = f(\mathfrak{f}|\mathfrak{q}) \cdot f(\mathfrak{q}|\mathfrak{p}).$$

Vale inoltre il seguente teorema:

**Teorema 1.8**
*Sia $L/K$ un'estensione di campi di numeri di grado $n$ e sia $\mathfrak{p}$ un ideale primo di $\mathcal{O}_K$. Siano $\mathfrak{P}_1, ..., \mathfrak{P}_r$ gli ideali primi di $\mathcal{O}_L$ che compaiono nella fattorizzazione di $\mathfrak{p}\mathcal{O}_L$. Allora, posto*

*$e_i = e(\mathfrak{P}_i|\mathfrak{p})$ e $f_i = f(\mathfrak{P}_i|\mathfrak{p})$, si ha che*

$$n = \sum_{i=1}^{r} e_i f_i$$

## 1.2 Valori assoluti e valutazioni

Ci occupiamo ora di definire il concetto di valore assoluto e di valutazione su un generico campo $K$. Le dimostrazioni di tutti i teoremi e di tutte le proposizioni da qui in poi riportati possono essere trovati in [2], [6] e [10].

**Definizione 1.9 - Valori assoluti su un campo**
Sia $K$ un campo. Un **valore assoluto** su $K$ è una funzione $|\cdot| : K \to \mathbb{R}_{\geq 0}$ che rispetta le seguenti proprietà:
1. $|x| = 0$ se e solo se $x = 0$,
2. Per ogni coppia di elementi $x, y \in K$ vale che $|x||y| = |xy|$,
3. Esiste una costante $C' > 0$ tale che per ogni coppia di elementi $\forall x, y \in K$ vale

$$|x + y| \leq C'(|x| + |y|).$$

Diciamo che il valore assoluto $|\cdot|$ è **non archimedeo** se inoltre vale che per ogni coppia di elementi $x, y \in K$,

$$|x + y| \leq \max\{|x|, |y|\},$$

altrimenti diciamo che è **archimedeo**.

La mappa che manda ogni elemento invertibile $x \in K^*$ in 1 e 0 in 0 è un valore assoluto su $K$, che chiamiamo valore assoluto banale.
È possibile definire una relazione d'equivalenza sull'insieme dei valori assoluti su un certo campo $K$, che risulta particolarmente utile nel loro studio e nella loro classificazione.

**Definizione 1.10 - Valori assoluti equivalenti**
Due valori assoluti $|\cdot|_1$ e $|\cdot|_2$ su un campo $K$ si dicono equivalenti, e scriviamo $|\cdot|_1 \sim |\cdot|_2$, se esiste un numero reale positivo $\lambda \in \mathbb{R}^+$ tale che $|\cdot|_1 = |\cdot|_2^{\lambda}$.
Indichiamo l'insieme quoziente $\{\text{valori assoluti non banali su } K\}/\sim$ con il simbolo $\mathcal{M}_K$. Generalmente gli elementi di $\mathcal{M}_K$ sono indicati con delle lettere.

Strettamente collegate ai valori assoluti sono le valutazioni su un campo $K$.

**Definizione 1.11**
Una **valutazione** (reale) su un campo $K$ è una funzione $v : K \to R \cup \{\infty\}$ che rispetta le seguenti proprietà:
1. $v(x) = \infty$ se e solo se $x = 0$,
2. Per ogni coppia di elementi $x, y \in K$ vale che $v(xy) = v(x) + v(y)$,
3. Per ogni coppia di elementi $x, y \in K$ vale che $v(x + y) \geq \min\{v(x), v(y)\}$.
Diciamo che la valutazione $v$ è **discreta** se l'immagine $v(K^*)$ è un sottogruppo di $\mathbb{R}$ isomorfo a $\mathbb{Z}$.

Osserviamo che ogni valutazione discreta può essere normalizzata in modo che l'immagine $v(K^*)$ sia esattamente $\mathbb{Z}$.

Anche sulle valutazioni è possibile definire una relazione di equivalenza, analoga a quella per i valori assoluti.

**Definizione 1.12**
Siano $v_1$ e $v_2$ due valutazioni su un campo $K$. Diciamo che $v_1$ è equivalente a $v_2$, e scriviamo $v_1 \sim v_2$ se esiste un numero reale positivo $\gamma \in \mathbb{R}^+$ tale che $v_1(\cdot) = \gamma v_2(\cdot)$.

Sussiste una relazione molto stretta tra valutazioni e valori assoluti non archimedei su un campo $K$: esiste infatti una bigezione esplicita tra i due seguenti insiemi

$$\{\text{valori assoluti non archimedei su } K\}/\sim \longleftrightarrow \{\text{valutazioni su } K\}/\sim .$$

## 1.3 Valori assoluti su $\mathbb{Q}$

Lo scopo di questa sezione è quello di classificare tutti i valori assoluti su $\mathbb{Q}$ a meno di equivalenza. Oltre al valore assoluto banale e a quello usuale, denotato con $|\cdot|_\infty$, è possibile associare a ogni numero primo razionale un valore assoluto non archimedeo su $\mathbb{Q}$.

**Definizione 1.13**
Per ogni numero primo $p$, definiamo la valutazione $p$-adica di un numero $x \in \mathbb{Q}^*$ come quel numero intero $v_p(x)$ tale che

$$x = p^{v_p(x)}\frac{a}{b},$$

con $(ab, p) = 1$. Definiamo inoltre il valore assoluto $p$-adico, e lo indichiamo con $|\cdot|_p$, il valore assoluto che a un generico numero razionale $x \in \mathbb{Q}$ associa

$$|x|_p = p^{-v_p(x)}.$$

I valori assoluti $p$-adici, il valore assoluto banale e quello ordinario sono a due a due non equivalenti. Il seguente risultato afferma che questi sono tutti e soli i valori assoluti su $\mathbb{Q}$ a meno di equivalenza ([6], pagina 45).

**Teorema 1.14 - Ostrowski**
*Ogni valore assoluto non banale su $\mathbb{Q}$ è equivalente a un valore assoluto $p$-adico $|\cdot|_p$ o all'ordinario valore assoluto $|\cdot|_\infty$.*

Terminiamo il paragrafo con la formula del prodotto su $\mathbb{Q}$.

**Proposizione 1.15**
*Per ogni $x \in \mathbb{Q}^*$, abbiamo che*

$$|x|_\infty \prod_{p\in\mathbb{P}} |x|_p = 1,$$

*dove con $\mathbb{P}$ indichiamo l'insieme dei numeri primi di $\mathbb{Z}$.*

## 1.4 Valori assoluti su campi di numeri

In questo paragrafo rendiamo specifica la nozione di valore assoluto su un campo ai campi di numeri $K$. Anche in questo caso è possibile classificare tutti i valori assoluti a meno di equivalenza.

Sia $K$ un campo di numeri e sia $\sigma$ un'immersione di $K$ in $\mathbb{C}$. Possiamo associare a $\sigma$ un valore assoluto normalizzato definendo, per ogni $x \in K$,

$$|x|_\sigma = |\sigma(x)|_\infty$$

dove $|\cdot|_\infty$ designa il valore assoluto archimedeo usuale su $\mathbb{C}$. Osserviamo che se $\sigma$ è un'immersione complessa e $\tau$ è l'immersione coniugata a $\sigma$, ovvero $\tau(x) = \overline{\sigma(x)}$, allora $|\cdot|_\sigma = |\cdot|_\tau$.
Enunciamo il seguente teorema che classifica i valori assoluti archimedei di un campo di numeri ([8], pagina 89).

**Teorema 1.16**
*Sia $K$ un campo di numeri.*
*1. Siano $\sigma$ e $\tau$ due immersioni di $K$ in $\mathbb{C}$. Allora, i valori assoluti $|\cdot|_\sigma$ e $|\cdot|_\tau$ sono equivalenti se e soltanto se $\tau = \sigma$ o $\tau = \overline{\sigma}$.*
*2. Ogni valore assoluto archimedeo su $K$ è equivalente a un valore assoluto $|\cdot|_\sigma$, per una certa immersione $\sigma$ di $K$ in $\mathbb{C}$.*

Segue da questo teorema che, detto $r$ il numero di immersioni reali di $K$ in $\mathbb{C}$ e $s$ il numero di coppie di immersioni complesse, su $K$ ci sono $r + s$ valori assoluti archimedei a meno di equivalenza.

Occupiamoci ora dei valori assoluti non archimedei su un campo di numeri $K$. In modo analogo a come abbiamo fatto su $\mathbb{Q}$, definiamo i valori assoluti $\mathfrak{p}$-adici su $K$, dove $\mathfrak{p}$ è un ideale primo non nullo di $\mathcal{O}_K$.

**Definizione 1.17**
Sia $K$ un campo di numeri e sia $\mathfrak{p}$ un ideale primo non nullo di $\mathcal{O}_K$. Indichiamo con $p$ il primo razionale che sta sotto $\mathfrak{p}$, cioè $p = \mathbb{Z} \cap \mathfrak{p}$.
1. Chiamiamo **valutazione $\mathfrak{p}$-adica** su $K$, e la indichiamo con $v_\mathfrak{p}$, l'applicazione che a ogni $x \in K^*$ associa

$$v_\mathfrak{p}(x) = \frac{\lambda}{e(\mathfrak{p}|p)},$$

dove $\lambda \in \mathbb{Z}$ è l'esponente di $\mathfrak{p}$ nella fattorizzazione in ideali primi dell'ideale $(x)\mathcal{O}_K$.
2. Chiamiamo **valore assoluto $\mathfrak{p}$-adico** su $K$ l'applicazione $|\cdot|_\mathfrak{p} : K \to \mathbb{R}$, che a ogni $x$ in $K$ associa:

$$|x|_\mathfrak{p} = p^{-v_\mathfrak{p}(x)}.$$

Terminiamo la classificazione dei valori assoluti di un generico campo di numero $K$ a meno di equivalenza ([8], pagina 89):

**Teorema 1.18**
*Sia $K$ un campo di numeri.*
*1. I valori assoluti $\mathfrak{p}$-adici, con $\mathfrak{p}$ ideale primo non nullo di $\mathcal{O}_K$, sono a due a due non equivalenti.*
*2. Ogni valore assoluto non archimedeo, che non sia il valore assoluto banale, su $K$ è equivalente a un valore assoluto $\mathfrak{p}$-adico $|\cdot|_\mathfrak{p}$, per un certo ideale primo non nullo $\mathfrak{p}$ di $\mathcal{O}_K$.*

Concludiamo la sezione con la seguente definizione.

**Definizione 1.19**
Sia $K$ un campo di numeri. Definiamo **primo** di $K$ una classe di equivalenza di valori assoluti non banali su $K$.

Generalmente un primo di $K$ è quindi un $v \in \mathcal{M}_K$. Utilizzando quanto detto in questa sezione, d'ora in poi quando ci riferiremo a un primo di $K$, andremo sempre a scegliere un rappresentante normalizzato $|\cdot|_v$ del primo $v$. In particolare se $v$ è un primo archimedeo (scriviamo $v|\infty$), allora con $|\cdot|_v$ indicheremo il valore assoluto indotto dall'immersione $\sigma$ di $K$ in $\mathbb{C}$ che classifica $v$. Se invece $v$ è un primo non archimedeo (scriviamo $v \nmid \infty$), ogni valore assoluto appartenente a $v$ è equivalente al valore assoluto $|\cdot|_\mathfrak{p}$, dove $\mathfrak{p}$ è un ideale primo di $\mathcal{O}_K$, e quindi con $|\cdot|_v$ indicheremo $|\cdot|_\mathfrak{p}$.

## 1.5 Completamenti

Nella sezione 1.2 abbiamo definito i valori assoluti su campi arbitrari. Osserviamo ora che ogni valore assoluto induce una metrica $d$ su $K$ definita da

$$d(x, y) = |x - y|,$$

dove $x$ e $y$ sono due elementi di $K$. Con ciò siamo in grado di dare la seguente

**Definizione 1.20 - Campo completo**
Sia $K$ un campo. $K$ è detto **completo** rispetto a un valore assoluto $|\cdot|$ se è uno spazio metrico completo rispetto alla distanza $d$ indotta, cioè se ogni successione di Cauchy di elementi di $K$ ha limite in $K$ rispetto a $d$.

Il seguente teorema ci assicura che è sempre possibile completare un campo $K$ rispetto a un suo valore assoluto ([6], pagina 47).

**Teorema 1.21**
*Sia $K$ un campo e sia $|\cdot|$ un valore assoluto ivi definito. Allora esistono un campo $\overline{K}$ e un valore assoluto $|\cdot|^*$ su $\overline{K}$ tali che:*
*1. $\overline{K}$ è completo rispetto a $|\cdot|^*$,*
*2. $K$ si immerge in modo denso in $\overline{K}$,*
*3. Per ogni $x \in K$ si ha che $|x| = |x|^*$.*
*Inoltre la coppia $(\overline{K}, |\cdot|^*)$ è unica a meno di isomorfismo algebrico e topologico.*

Poniamo ora l'attenzione ai campi di numeri.
Sia $K$ un campo di numeri. Per ogni primo $v \in \mathcal{M}_K$, indichiamo con $K_v$ il completamento di $K$ rispetto al valore assoluto $|\cdot|_v$ e con $\mathbb{Q}_v$ il completamento di $\mathbb{Q}$ rispetto alla restrizione di $|\cdot|_v$. Definiamo inoltre il grado dell'estensione dei completati

$$n_v = [K_v : \mathbb{Q}_v].$$

Valgono le seguenti ([2], pagina 21)

**Proposizione 1.22**
*Sia $K$ un campo di numeri e sia $v \in \mathcal{M}_K$ un primo. Se $v$ è archimedeo, allora $n_v = 1$ se $v$ è associato a un'immersione reale, mentre $n_v = 2$ se $v$ è associato a un'immersione complessa. Se invece $v$ è non archimedeo, vale che*

$$n_v = e(\mathfrak{p}|p\mathbb{Z}) f(\mathfrak{p}|p\mathbb{Z})$$

*dove $\mathfrak{p}$ è l'ideale primo di $\mathcal{O}_K$ associato a $v$ e $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.*

**Proposizione 1.23 - Formula del prodotto**
*Sia $K$ un campo di numeri. Per ogni $\alpha \in K^*$ vale*

$$\prod_{v \in \mathcal{M}_K} |\alpha|_v^{n_v} = 1.$$

Diamo la seguente definizione.

**Definizione 1.24**
Siano $K$ e $L$ due campi di numeri con $K \subset L$ e siano $v \in \mathcal{M}_K$ e $w \in \mathcal{M}_L$. Diciamo che $w$ divide $v$, e scriviamo $w|v$, se per ogni $\alpha \in K$ si ha che $|\alpha|_v = |\alpha|_w$.

Il senso della definizione di sopra è chiarificato dalla prossima proposizione.

**Proposizione 1.25**
*Siano $K$ e $L$ due campi di numeri tali che $K \subset L$.*
*1. Siano $\sigma : K \to \mathbb{C}$ e $\tau : L \to \mathbb{C}$ due immersioni e denotiamo con $v$ e $w$ i primi archimedei di $K$ e $L$ associati rispettivamente a $\sigma$ e $\tau$. Allora, $w$ divide $v$ se e soltanto se la restrizione di $\tau$ a $K$ coincide con $\sigma$ o con $\overline{\sigma}$.*
*2. Siano $\mathfrak{p}$ e $\mathfrak{q}$ due ideali primi non nulli rispettivamente di $\mathcal{O}_K$ e $\mathcal{O}_L$. Denotiamo con $v$ e $w$ i primi non archimedei di $K$ e $L$ associati a $\mathfrak{p}$ e $\mathfrak{q}$ rispettivamente. Allora, $w$ divide $v$ se e solo se $\mathfrak{q}$ divide $\mathfrak{p}$.*

*Dimostrazione.* 1. Discende direttamente dal Teorema 1.16.
2. Supponiamo che $\mathfrak{q} \nmid \mathfrak{p}$, esiste allora $\alpha \in \mathfrak{p} \setminus \mathfrak{q}$ e dunque $|\alpha|_v < 1$ e $|\alpha|_w = 1$, ovvero $w \nmid v$. Supponiamo ora che $\mathfrak{q}|\mathfrak{p}$ e sia $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$. Denotiamo con $a$ il più grande intero tale che $\mathfrak{p}^a|(\alpha)$. Si ha allora che

$$v_{\mathfrak{q}}(\alpha) = \frac{a\, e(\mathfrak{q}|\mathfrak{p})}{e(\mathfrak{q}|\mathfrak{p} \cap \mathbb{Z})} = \frac{a}{e(\mathfrak{p}|\mathfrak{p} \cap \mathbb{Z})} = v_{\mathfrak{p}}(\alpha),$$

ovvero $w|v$. □

Concludiamo la sezione e il capitolo con una formula di cui avremo bisogno per mostrare che l'altezza assoluta di Weil di un numero algebrico è indipendente dal campo di numeri che lo contiene.

**Proposizione 1.26**
*Siano $K$ e $L$ due campi di numeri tali che $\mathbb{Q} \subset K \subset L$. Allora, per ogni primo $v$ di $K$, abbiamo*

$$\sum_{\substack{v \in \mathcal{M}_L \\ w|v}} \frac{n_w}{n_v} = [L : K].$$

*Dimostrazione.* Sia $v$ un primo archimedeo. Grazie alle Proposizioni 1.22 e 1.25 è sufficiente verificare che il numero di immersioni di $L$ in $\mathbb{C}$ la cui restrizione a $K$ coincide con l'immersione $\sigma$ associata a $v$ è uguale a $[L : K]$, ma questo è un fatto noto dalla teoria dei campi.
Sia invece $v$ un primo non archimedeo e sia $\mathfrak{p} \subset \mathcal{O}_K$ l'ideale primo non nullo di $\mathcal{O}_K$ associato a $v$. Sia inoltre

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e(\mathfrak{q}_1|\mathfrak{p})}\mathfrak{q}_2^{e(\mathfrak{q}_2|\mathfrak{p})} \dots \mathfrak{q}_k^{e(\mathfrak{q}_k|\mathfrak{p})}$$

la fattorizzazione in ideali primi di $\mathfrak{p}\mathcal{O}_L$. Utilizzando anche in questo caso le Proposizioni 1.22 e 1.25 abbiamo che:

$$\sum_{\substack{w \in \mathcal{M}_l \\ w|v}} \frac{n_w}{n_v} = \sum_{j=1}^{k} \frac{e(\mathfrak{q}_j|\mathfrak{p} \cap \mathbb{Z}) f(\mathfrak{q}_j|\mathfrak{p} \cap \mathbb{Z})}{e(\mathfrak{p}|\mathfrak{p} \cap \mathbb{Z}) f(\mathfrak{p}|\mathfrak{p} \cap \mathbb{Z})} = \sum_{j=1}^{k} e(\mathfrak{q}_j|\mathfrak{p}) f(\mathfrak{q}_j|\mathfrak{p}) = [L : K],$$

dove la seconda uguaglianza è dovuta a 1.7 e l'ultima è il Teorema 1.8. □

Osserviamo quindi che per ogni campo di numeri $K$ e per ogni primo razionale $p \in \mathbb{Z}$ abbiamo

$$\sum_{\substack{v \in \mathcal{M}_K \\ v|\infty}} n_v = \sum_{\substack{v \in \mathcal{M}_K \\ v|p}} n_v = [K : \mathbb{Q}].$$

## 1.6 Appendice di teoria analitica dei numeri

Presentiamo qui due risultati della teoria analitica dei numeri, che ci serviranno per le applicazioni del teorema principale della tesi, che svilupperemo nella sezione 3.1.

**Teorema 1.27 - Mertens**
*Sia $\mathbb{P} \subset \mathbb{N}$ l'insieme dei numeri primi. Per $x \to +\infty$ si ha la stima asintotica*

$$\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x},$$

*dove $\gamma = 0,5772...$ è la costante di Eulero-Mascheroni.*

Una dimostrazione del precedente Teorema può essere trovata in [7],Teorema 429, pagina 466.

**Teorema 1.28 - Linnik**
*Siano $a$ e $d$ due numeri interi coprimi, con $1 \leq a \leq d$. Esiste una costante assoluta $1 < L \leq 5$ tale che, detto $p(a,d)$ il più piccolo numero primo $p \equiv a \mod d$, si ha*

$$p(a,d) \ll d^L.$$

Osserviamo che, con le notazioni di sopra, l'esistenza di un tale $p(a,d)$ è accertata dal Teorema di Dirichlet:

**Teorema 1.29 - Dirichlet**
*Siano $a$ e $d$ due numeri interi coprimi, con $1 \leq a \leq d$. Esistono infiniti primi $p \equiv a \mod d$.*

Una trattazione completa del Teorema di Linnik può essere trovata in [8].

Capitolo 2

# La Misura di Mahler e l'altezza di Weil

Il seguente capitolo è diviso in due sezioni principali. Nella prima sarà data definizione del concetto di Misura di Mahler di un polinomio e saranno trattate alcune delle proprietà di maggior rilievo di quest'ultima, tra cui il Teorema di finitezza di Northcott e il Teorema di Kronecker. Nella seconda parte invece verrà presentato quello che può essere considerato l'oggetto chiave della tesi: l'altezza logaritmica di Weil per numeri algebrici. Successivamente sarà studiato il legame che questa ha con la misura di Mahler.

## 2.1 Misura di Mahler di un polinomio

Per misurare la complessità di un polinomio

$$F(x) = a_n x^n + ... + a_0$$

a coefficienti in $\mathbb{Z}$ un approccio standard è quello di considerare le norme indotte da $\mathbb{C}$ su $\mathbb{C}[x]$. Le più famose sono:

$$||F||_1 = |a_0| + ... + |a_n|, \tag{2.1}$$

$$||F||_2 = \sqrt{|a_0|^2 + ... + |a_n|^2}, \tag{2.2}$$

$$||F||_\infty = max\{|a_0|, ..., |a_n|\}, \tag{2.3}$$

$$|F|_1 = max_{|z|=1}|F(z)|, \tag{2.4}$$

dette rispettivamente **lunghezza, norma quadratica, altezza naïve** e **norma della convergenza uniforme sulla sfera unitaria**.
Le relazioni tra queste norme di polinomi sono riassumibili nella proposizione seguente, che è un'immediata conseguenza delle relazioni che sussistono tra le norme definite su $\mathbb{C}$:

**Proposizione 2.1**
*Per ogni polinomio $F \in \mathbb{C}[x]$ di grado al più $n$ vale la seguente catena di disuguaglianze*

$$||F||_\infty \leq ||F||_2 \leq |F|_1 \leq ||F||_1 \leq (n+1)||F||_\infty.$$

Ognuna delle norme sopra introdotte misura in un qualche modo specifico la complessità del polinomio $F$ (per esempio la lunghezza dà un'idea del numero di cifre necessarie alla scrittura di $F$) dipendente però dai suoi coefficienti e non direttamente dalle sue radici. Definiamo allora un'altra misura polinomiale, la misura di Mahler, che risponde a questa esigenza.

**Definizione 2.2 - Misura di Mahler**
Sia $F(x) \in \mathbb{C}[x]$ un polinomio non nullo di grado $n$ e sia

$$F(x) = a(x-\alpha_1)...(x-\alpha_n)$$

la sua fattorizzazione in $\mathbb{C}$, con $\alpha_i$ non necessariamente distinto da $\alpha_j$ per $i \neq j$. Chiamiamo **misura di Mahler** di $F$, e la denotiamo con $M(F)$, la quantità

$$M(F) = |a| \prod_{i=1}^{n} \max\{1, |\alpha_i|\}. \tag{2.5}$$

Per completezza, definiamo la misura di Mahler del polinomio nullo $M(0) = 1$.

La misura di Mahler di $F$ è quindi il prodotto tra il valore assoluto ordinario del suo coefficiente direttore e quello delle sue radici al di fuori del disco unitario, contate con la loro molteplicità. Estendiamo in maniera naturale la definizione di misura di Mahler anche ai numeri algebrici:

**Definizione 2.3**
Sia $\alpha$ un numero algebrico. Chiamiamo misura di Mahler di $\alpha$, e scriviamo $M(\alpha)$, la misura di Mahler del suo polinomio minimo su $\mathbb{Z}$.

Dalla definizione di misura di Mahler si deducono le seguenti semplici proprietà:
1. Per ogni coppia di polinomi $F, G \in \mathbb{C}[x]$ si ha che $M(FG) = M(F)M(G)$.
2. Se $F \in \mathbb{C}[x]$ è un polinomio di grado $n$, indicando con $F^*$ il polinomio reciproco (ovvero quel polinomio definito come $F^*(x) = x^n F(x^{-1})$) si ha che $M(F) = M(F^*)$.
3. Per ogni polinomio $F(x) \in \mathbb{C}[x]$ e per ogni intero $n \geq 1$, $M(F(x)) = M(F(x^n))$.
4. $M(F)$ è minorata dal valore assoluto del coefficiente direttivo di $F$.

Concludiamo il paragrafo con un importante risultato di Kurt Mahler che lega la definizione algebrica di misura di Mahler con un'espressione analitica equivalente:

**Teorema 2.4**
*Sia $F \in \mathbb{C}[x]$ un polinomio di grado $n \geq 1$. Allora*

$$M(F) = \exp\Big(\frac{1}{2\pi}\int_0^{2\pi} \log(|F(e^{it})|)\, dt\Big)$$

*Dimostrazione.* Poniamo

$$\tilde{M}(F) = \exp\Big(\frac{1}{2\pi}\int_0^{2\pi} \log(|F(e^{it})|) dt\Big).$$

Abbiamo già osservato che la misura di Mahler è moltiplicativa ed è immediato verificare che lo stesso vale per la funzione $\tilde{M}$. Inoltre $M(a) = |a| = \tilde{M}(a)$ per ogni $a \in \mathbb{C}^*$. Per dimostrare il teorema è dunque sufficiente far vedere che per ogni $\alpha \in \mathbb{C}$ si ha che $\tilde{M}(X-\alpha) = M(X-\alpha)$. In realtà, è sufficiente trattare il caso $\alpha \in \mathbb{R}^+$, infatti, se $\alpha = re^{i\theta} \in \mathbb{C}$, con $r \in \mathbb{R}^+$ e $\theta \in [0, 2\pi]$, da una parte abbiamo che $M(X-\alpha) = \max(1, |\alpha|) = \max(1, r) = M(X-r)$ e dall'altra

$$\log(\tilde{M}(X-\alpha)) = \frac{1}{2\pi}\int_0^{2\pi} \log|e^{it}-\alpha| dt = \frac{1}{2\pi}\int_0^{2\pi} \log|e^{i(t-\theta)}-r| dt =$$

$$= \frac{1}{2\pi}\int_\theta^{2\pi+\theta} \log|e^{it}-r| dt = \log(\tilde{M}(X-r)).$$

Poniamo adesso

$$I(r) = \frac{1}{2\pi}\int_0^{2\pi} \log|e^{it} - r|dt,$$

ci basta allora mostrare che $I(r) = \log\max(1, r)$.
Proviamo che per ogni $r \in \mathbb{R}^+$ vale $I(r^2) = 2I(r)$ :

$$I(r^2) = \frac{1}{2\pi}\int_0^{2\pi} \log|e^{it} - r^2|dt = \frac{1}{4\pi}\int_0^{4\pi} \log|e^{it} - r^2|dt =$$

$$= \frac{1}{4\pi}\int_0^{2\pi} 2\log|e^{2is} - r^2|ds = \frac{1}{2\pi}\int_0^{2\pi} \log|e^{is} - r|ds + \frac{1}{2\pi}\int_0^{2\pi} \log|e^{is} + r|ds =$$

$$= I(r) + I(-r) = 2I(r),$$

dove l'ultima uguaglianza è dovuta al fatto che $-r = re^{i\pi}$. In particolare, per $r = 1$ si ha che $I(1) = 2I(1)$, ovvero $I(1) = 0 = \log\max(1, 1)$. Ricorsivamente deduciamo dalla relazione di sopra che $I(r^{2^n}) = 2^n I(r)$. Inoltre

$$|r^{2^n} - 1| \leq |e^i t - r^{2^n}| \leq r^{2^n} + 1$$

e integrando questa disuguaglianza otteniamo

$$\frac{1}{2^n}\log|r^{2^n} - 1| \leq \frac{I(r^{2^n})}{2^n} \leq \frac{1}{2^n}\log|r^{2^n} + 1|$$

ovvero

$$\frac{1}{2^n}\log|r^{2^n} - 1| \leq I(r) \leq \frac{1}{2^n}\log|r^{2^n} + 1|.$$

Facendo tendere $n$ a $+\infty$, troviamo per $r < 1$

$$I(r) = 0 = \log 1 = \log\max(1, r),$$

e per $r > 1$

$$I(r) = \log r = \log\max(1, r).$$

□

### 2.1.1 Minorazione della misura di Mahler in funzione delle norme indotte

Lo scopo di questo paragrafo è quello di trovare una minorazione di $M(F)$ in funzione delle norme introdotte all'inizio del paragrafo precedente. Introduciamo un lemma preliminare:

**Lemma 2.5**
*Sia $F(x) = a_n x^n + ... + a_0 \in \mathbb{C}[x]$ un polinomio di grado $n$. Indicando con $\alpha_1, ..., \alpha_n$ le sue radici (contate con molteplicità), vale che per ogni $j = 1, ..., n$*

$$|a_j| \leq \binom{n}{j} M(F).$$

*Dimostrazione.* Scriviamo la fattorizzazione di $F$ in $\mathbb{C}[x]$:

$$a_n \prod_{j=1}^{n}(x - \alpha_j).$$

Sfruttando il fatto che i coefficienti di un generico polinomio sono funzioni simmetriche nelle radici, moltiplicate per il coefficiente direttore, otteniamo

$$\begin{cases} a_{n-1} & = -a_n \sum_{j=1}^{n} \alpha_j \\ a_{n-2} & = a_n \sum_{1\le j<k\le n} \alpha_j\alpha_i \\ \vdots & \\ a_0 & = (-1)^n a_n \prod_{j=1}^{n} \alpha_j \end{cases}$$

Da cui, per $j = 1, .., n$, si ha che

$$|a_j| = |a_n| \left| \sum_{1\le i_1<\ldots<i_j\le n} \alpha_{i_1}\ldots\alpha_{i_j} \right| \le |a_n| \sum_{1\le i_1<\ldots<i_j\le n} |\alpha_{i_1}|\ldots|\alpha_{i_j}|$$

$$\le |a_n| \prod_{k=1}^{n} \max(1, |\alpha_k|) \sum_{1\le i_1<\ldots<i_j\le n} 1 = |a_n| \binom{n}{j} \prod_{k=1}^{n} \max(1, |\alpha_k|) = \binom{n}{j} M(F).$$

□

Utilizzando questo lemma deduciamo il seguente

**Teorema 2.6**
*Per ogni polinomio $F \in \mathbb{C}[x]$ di grado al più $n$ valgono le seguenti disuguaglianze*

$$||F||_2 \le \binom{2n}{n}^{1/2} M(F), \tag{2.6}$$

$$|F|_1 \le 2^n M(F), \tag{2.7}$$

$$||F||_1 \le 2^n M(F), \tag{2.8}$$

$$||F||_\infty \le \binom{n}{[n/2]} M(F), \tag{2.9}$$

*dove con $[x]$ indichiamo la parte intera di $x$.*

*Dimostrazione.* Per mostrare le disuguaglianze (2.6), (2.8) e (2.9) basta applicare il lemma precedente combinato con le seguenti formule

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n},$$

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n,$$

$$\max_{i=0,\ldots,n} \binom{n}{i} \le \binom{n}{[n/2]}$$

rispettivamente. La disuguaglianza (2.7) è invece conseguenza immediata del fatto che $|F|_1 \le ||F||_1$, come mostrato in 2.1, unita a (2.8). □

Tutte le disuguaglianze del teorema precedente sono ottimali, come è possibile verificare considerando il polinomio $F(x) = (x+1)^n$.

Terminiamo il paragrafo con un'interessante curiosità che lega la misura di Mahler a ogni altra norma sullo spazio vettoriale $\mathbb{C}[x]_n$ dei polinomi di grado minore di $n$. Enunciamo un lemma preliminare che servirà nella trattazione:

**Lemma 2.7 - Landau**
*Per ogni polinomio $F \in \mathbb{C}[x]$ si ha*

$$M(F) \leq ||F||_2.$$

In particolare, grazie a 2.1, vale anche la disuguaglianza $M(F) \leq ||F||_1$.

Sia ora

$$F(x) = a_n \prod_{i=1}^{n} (x - \alpha_i)$$

un polinomio a coefficienti complessi di grado $n$ e, per ogni intero $m \in \mathbb{N}^*$, poniamo

$$F_m(x) = a_n^m \prod_{i=1}^{n} (x - \alpha_i^m).$$

Osserviamo che per ogni $m \in \mathbb{N}^*$, $F_m(x)$ è un polinomio di grado $n$. Come conseguenza dei teoremi 2.6, 2.7 e dalla Definizione 2.2, otteniamo che per ogni $m \in \mathbb{N}^*$

$$M(F) = M(F_m)^{1/m} \leq ||F_m||_1^{1/m} \leq (2^n)^{1/m} M(F_m)^{1/m} = 2^{n/m} M(F)$$

e facendo tendere $n$ all'infinito

$$\lim_{n \to +\infty} ||F_n||_1^{1/n} = M(F).$$

Dato però che l'insieme $\mathbb{C}[x]_n$ dei polinomi di $\mathbb{C}[x]$ di grado minore di $n$ è un $\mathbb{C}$-spazio vettoriale di dimensione finita, tutte le norme ivi definite sono equivalenti: abbiamo così dimostrato il seguente

**Teorema 2.8**
*Sia $F \in \mathbb{C}[x]$ un polinomio di grado $n$ e sia $|| \cdot ||$ una norma definita su $\mathbb{C}[x]_n$. Allora*

$$\lim_{n \to +\infty} ||F_n||^{1/n} = M(F).$$

### 2.1.2 Il teorema di finitezza di Northcott e il teorema di Kronecker

Grazie alle stime viste nel paragrafo precedente è ora possibile enunciare e dimostrare con tecniche elementari un teorema di grande rilevanza teorica.

**Teorema 2.9 - di finitezza di Northcott**
*Sia $n \in \mathbb{N}^*$ un intero non nullo e sia $M_0 \in \mathbb{R}^+$ un numero reale positivo. L'insieme dei numeri algebrici di grado limitato da $n$ e con misura di Mahler limitata da $M_0$ è finito.*

*Dimostrazione.* Grazie a (2.9) sappiamo che per ogni polinomio $F$ di grado minore di $n$

$$||F||_\infty \leq \binom{n}{[n/2]} M(F),$$

da cui deduciamo che ogni numero algebrico di grado limitato da $n$ e con misura di Mahler limitata da $M_0$ è radice di un polinomio irriducibile $F$ a coefficienti interi, la cui altezza naïve è limitata da

$$\binom{n}{[n/2]} M_0.$$

Ricordando la Definizione (2.3) di altezza naïve, il numero di polinomi con la proprietà sopra esposta è inferiore o uguale a

$$\Big[2\binom{n}{[n/2]} M_0 + 1\Big]^{n+1}$$

e quindi il numero di numeri algebrici che rispettano le limitazioni imposte è inferiore uguale a

$$n\Big[2\binom{n}{[n/2]} M_0 + 1\Big]^{n+1}$$

in quanto ogni polinomio $F$ ha al più $\deg(F) \leq n$ radici distinte. Da questo segue la tesi. □

Concludiamo il capitolo con il seguente risultato, che è un corollario al teorema 2.9 e che fu messo in evidenza per la prima volta da Leopold Kronecker nel 1859, matematico polacco dal quale questo teorema eredita il nome:

**Teorema 2.10 - Kronecker**
*Sia $\alpha \in \overline{\mathbb{Q}}^*$. $M(\alpha) = 1$ se e soltanto se $\alpha$ è una radice dell'unità.*

*Dimostrazione.* Supponiamo che $\alpha$ sia una radice $n$-esima primitiva dell'unità, allora il suo polinomio minimo su $\mathbb{Z}$ è un polinomio ciclotomico, in particolare monico, di grado $\phi(n)$, le cui radici sono tutte e sole le radici $n$-esime primitive dell'unità. Chiamando $\alpha = \alpha_1, ..., \alpha_{\phi(n)}$ i coniugati di $\alpha$, si ha che per ogni $j = 1, ..., \phi(n)$

$$|\alpha_j| = 1$$

ed essendo il polinomio minimo monico si ha di conseguenza che $M(\alpha) = 1$.

Viceversa, sia $\alpha$ un numero algebrico non nullo tale che $M(\alpha) = 1$, allora $\alpha$ è un intero algebrico, in quanto il polinomio minimo su $\mathbb{Z}$ deve avere coefficiente direttore uguale a 1. Mostriamo che, per ogni $n \in \mathbb{N}^*$, $M(\alpha^n) = 1$: è chiaro che $\mathbb{Q}(\alpha^n) \subset \mathbb{Q}(\alpha)$, quindi ogni immersione di $\mathbb{Q}(\alpha^n)$ in $\overline{\mathbb{Q}}$ è la restrizione di $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)]$ immersioni di $\mathbb{Q}(\alpha)$ in $\overline{\mathbb{Q}}$. Segue da ciò che i coniugati di $\alpha^n$ sono potenze $n$-esime dei coniugati di $\alpha$. Si conclude osservando che, per l'ipotesi, ogni coniugato di $\alpha$ deve avere modulo minore o uguale a 1 e lo stesso vale per le loro potenze $n$-esime.
Chiamando ora $D$ il grado di $\alpha$ su $\mathbb{Q}$, segue che, per ogni intero $n \in \mathbb{N}^*$, $[\mathbb{Q}(\alpha^n) : \mathbb{Q}] \leq D$ e per il teorema 2.9 devono esistere due interi positivi $m$ e $n$, con $m \neq n$, tali per cui

$$\alpha^m = \alpha^n.$$

Questo implica che $\alpha$ è una radice dell'unità. □

## 2.2 Altezza di Weil di un numero algebrico

Sia $\alpha \in \overline{\mathbb{Q}}$ un numero algebrico e sia $K$ un campo che contiene $\alpha$. Poniamo provvisoriamente

$$h_K(\alpha) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log^+(|\alpha|_v),$$

dove definiamo $\log^+(x) = \log(\max\{1, x\})$, per $x$ reale non negativo. Vogliamo dimostrare che la definizione presentata poc'anzi non dipende dal campo $K$.

**Proposizione 2.11**
*La definizione precedente non dipende dal campo $K$. Più precisamente, siano $K \subset L$ due campi e sia $\alpha \in \overline{\mathbb{Q}}$ un numero algebrico tale che $\alpha \in K$, allora*

$$h_K(\alpha) = h_L(\alpha).$$

*Dimostrazione.* Sia $\alpha \in K$, dalla definizione di sopra si ha che

$$h_L(\alpha) = \frac{1}{[L:\mathbb{Q}]} \sum_{v \in \mathcal{M}_L} n_v \log^+ |\alpha|_v$$

$$= \frac{1}{[L:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} \sum_{\substack{w \in M_L \\ w|v}} n_w \log^+ |\alpha|_w$$

$$= \frac{1}{[L:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} \Big( \sum_{\substack{w \in M_L \\ w|v}} n_w \Big) \log^+ |\alpha|_v.$$

Per la Proposizione 1.26, per ogni $v \in \mathcal{M}_K$ abbiamo che

$$\sum_{\substack{v \in M_L \\ w|v}} n_w = [L:K] n_v$$

e dunque:

$$h_L(\alpha) = \frac{[L:K]}{[L:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log^+ |\alpha|_v$$

$$= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log^+(|\alpha|_v) = h_K(\alpha).$$

□

Questa proposizione giustifica la seguente definizione.

**Definizione 2.12 - Altezza logaritmica di Weil**
Sia $\alpha \in \overline{\mathbb{Q}}$ e sia $K$ un campo di numeri che contiene $\alpha$. Chiamiamo **altezza logaritmica di Weil** di $\alpha$ il numero reale definito da

$$h(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log^+ |\alpha|_v.$$

In certe situazioni è utile considerare l'altezza non logaritmica definita da $H(\alpha) = \exp h(\alpha)$.

Presentiamo alcune proprietà di cui gode l'altezza di Weil.

**Proposizione 2.13**
*La funzione altezza $h : \overline{\mathbb{Q}} \to \mathbb{R}^{\geq 0}$ verifica, per $\alpha, \beta \in \overline{\mathbb{Q}}$, le proprietà seguenti.*
*1) $h(\alpha) \geq 0$ e inoltre $h(\alpha) = 0$ se e solo se $\alpha$ è una radice dell'unità o $\alpha = 0$.*
*2) $h(\alpha\beta) \leq h(\alpha) + h(\beta)$. Se poi $\beta$ è una radice dell'unità allora $h(\alpha\beta) = h(\alpha)$.*
*3) Per ogni $n \in \mathbb{Z}$ si ha che $h(\alpha^n) = |n| h(\alpha)$.*

*Dimostrazione.* Sia $K$ un campo di numeri contenente $\alpha$ e $\beta$:
1) La prima asserzione è ovvia dalla definizione. Per mostrare la seconda osserviamo che

$$h(\alpha) = 0 \iff |\alpha|_v \leq 1 \text{ per ogni primo } v \in \mathcal{M}_K.$$

Deduciamo quindi che $h(\alpha) = 0$ se e soltanto se $\alpha$ è un intero algebrico (segue considerando i primi non archimedei di $K$) e se $|\sigma(\alpha)| \leq 1$ per ogni immersione $\sigma$ di $K$ in $\mathbb{C}$ (segue considerando i primi archimedei di $K$). Ma allora la misura di Mahler di $\alpha$ è $M(\alpha) = 1$. Il Teorema 2.10 implica quindi che o $\alpha = 0$ o $\alpha$ è una radice dell'unità.
2) Per ogni primo $v \in \mathcal{M}_K$ abbiamo

$$\max(1, |\alpha\beta|_v) = \max(1, |\alpha|_v|\beta|_v) \leq \max(1, |\alpha|_v)\max(1, |\beta|_v)$$

e quindi $h(\alpha\beta) \leq h(\alpha)+h(\beta)$. Inoltre, se $\beta$ è una radice dell'unità, si ha che $h(\alpha\beta) \leq h(\alpha)+h(\beta) = h(\alpha)$ e $h(\alpha) \leq h(\alpha\beta) + h(\beta^{-1}) = h(\alpha\beta)$, dunque $h(\alpha\beta) = h(\alpha)$.
3) Il caso $n = 0$ è ovvio.
Supponiamo ora $n \neq 0$ e mostriamo innanzitutto che $h(\alpha^{-1}) = h(\alpha)$. Per ogni $v \in \mathcal{M}_K$ abbiamo

$$\frac{\max(1, |\alpha|_v)}{\max(1, |\alpha^{-1}|_v)} = |\alpha|_v$$

e

$$\log^+ |\alpha|_v - \log^+ |\alpha^{-1}|_v = \log |\alpha|_v.$$

Dalla formula del prodotto 1.23 otteniamo

$$h(\alpha) - h(\alpha^{-1}) = \frac{1}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log |\alpha|_v = 0.$$

Sia ora $n \in \mathbb{Z}$. Per ogni $v \in \mathcal{M}_K$ si ha

$$\log^+ |\alpha^n|_v = \begin{cases} n \log^+ |\alpha|_v & \text{se } n \geq 1 \\ |n| \log^+ |\alpha^{-1}|_v & \text{se } n < 0. \end{cases}$$

La prima uguaglianza dà la tesi nel caso in cui $n$ sia positivo, mentre la seconda (combinata col fatto che $h(\alpha) = h(\alpha^{-1})$) dà la tesi quando $n$ è negativo. □

### 2.2.1 Altezza normalizzata di un polinomio

Ci proponiamo di introdurre un'altezza normalizzata su $\overline{\mathbb{Q}}[x]$ che prolunga la nozione di misura di Mahler di un polinomio a coefficienti interi. Cominciamo col dare una definizione.

**Definizione 2.14**
Sia $K$ un campo di numeri e siano $P = \sum_{i=0}^{n} a_i x^i \in K[x]$ un polinomio e $v \in \mathcal{M}_K$ un primo di $K$. Se $v$ è un primo archimedeo associato all'immersione $\sigma$ di $K$ in $\overline{\mathbb{Q}}$, poniamo $M_v(P) = M(\sigma P)$. Se invece $v$ è un primo non archimedeo, definiamo $M_v(P)$ come $M_v(P) = \max\{|a_0|_v, \ldots, |a_n|_v\}$.

Fissato $v \in \mathcal{M}_K$ un primo di $K$, la funzione $M_v$ appena definita definita è completamente moltiplicativa:

**Lemma 2.15**
*Sia $K$ un campo di numeri e siano $P, Q \in K[x]$ due polinomi e $v \in \mathcal{M}_K$ un primo di $K$. Allora $M_v(PQ) = M_v(P)M_v(Q)$.*

*Dimostrazione.* Il caso in cui $v$ sia un primo archimedeo è ovvio. Supponiamo allora $v$ non archimedeo. Siano $P = \sum_i a_i x^i$ e $Q = \sum_j b_j x^j$ e sia $PQ = \sum_l c_l x^l$. Allora

$$|c_l|_v = \big| \sum_{i+j=l} a_i b_j \big|_v \leq \max_{i+j=l} |a_i b_j|_v \leq M_v(P) M_v(Q)$$

e dunque $M_v(PQ) \leq M_v(P)M_v(Q)$. Mostriamo l'altra disuguaglianza. Siano ora

$$r = \min\{i \text{ t.c. } |a_i|_v = M_v(P)\}$$

e

$$s = \min\{j \text{ t.c. } |b_j|_v = M_v(Q)\}.$$

Si ha allora che $|a_r b_s|_v = M_v(P)M_v(Q)$ e che $|a_i b_j|_v < M_v(P)M_v(Q)$ con $i + j = r + s$ ma $(i, j) \neq (r, s)$. Segue allora che

$$|c_{r+s}|_v = |a_r b_s + \sum_{\substack{i+j=r+s \\ (i,j)\neq(r,s)}} a_i b_j|_v = M_v(P)M_v(Q)$$

da cui segue che $M_v(PQ) \geq M_v(P)M_v(Q)$. □

Definiamo adesso un'altezza polinomiale su $\overline{\mathbb{Q}}$, che dimostreremo essere fortemente legata all'altezza di Weil.

**Definizione 2.16**
Sia $P \in \overline{\mathbb{Q}}[x]$ un polinomio e sia $K$ un campo di numeri contenente i coefficienti di $P$. Definiamo

$$\hat{h}(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log M_v(P).$$

Anche in questo caso la definizione non dipende dal campo $K$ e la dimostrazione è analoga a quella della Proposizione 2.11.
Le proprietà della funzione $\hat{h}$ che più ci risulteranno utili sono riassunte nel seguente lemma:

**Lemma 2.17**
*La funzione $\hat{h}$ verifica le seguenti proprietà.*
*1) Per ogni numero $\lambda \in \overline{\mathbb{Q}}^*$ e per ogni polinomio $P \in \overline{\mathbb{Q}}[x]$ si ha che $\hat{h}(\lambda P) = \hat{h}(P)$.*
*2) Per ogni coppia di polinomi $P, Q \in \overline{\mathbb{Q}}[x]$ si ha che $\hat{h}(PQ) = \hat{h}(P) + \hat{h}(Q)$.*
*3) Sia $\alpha \in \overline{\mathbb{Q}}^*$ un numero algebrico non nullo, allora $\hat{h}(x - \alpha) = h(\alpha)$.*

*Dimostrazione.* 1) Vale che

$$\hat{h}(\lambda P) - \hat{h}(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v (\log M_v(\lambda P) - \log M_v(P)) =$$

$$= \frac{1}{[K : \mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log |\lambda|_v = 0$$

per la formula del prodotto.
2) Segue direttamente dal Lemma 2.15.
3) Sia $\sigma$ un'immersione di $K$ in $\overline{\mathbb{Q}}$, allora la misura di Mahler del polinomio $x - \sigma(\alpha)$ è

$$M(x - \sigma(\alpha)) = \max(1, |\alpha|)$$

e quindi

$$\hat{h}(x-\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log M_v(x-\alpha) =$$

$$= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} n_v \log^+ |\alpha|_v = h(\alpha)$$

□

Il teorema seguente è una conseguenza immediata del precedente lemma.

**Teorema 2.18**
*Sia $P \in \overline{\mathbb{Q}}[x]$ un polinomio e denotiamo con $\alpha_1, ..., \alpha_n$ le sue radici, contate con la loro molteplicità. Si ha allora che*

$$\hat{h}(P) = \sum_{j=1}^{n} h(\alpha_j)$$

*Dimostrazione.* Dal punto 1) del Lemma 2.17 possiamo supporre $P$ unitario. Considerando allora la fattorizzazione di $P$ in $\overline{\mathbb{Q}}$

$$P(x) = \prod_{i=1}^{n} (x - \alpha_i)$$

sempre grazie ai punti 2) e 3) del Lemma 2.17 si ha che

$$\hat{h}(P) = \sum_{j=1}^{n} \hat{h}(x-\alpha_j) = \sum_{j=1}^{n} h(\alpha_j).$$

□

Dal teorema precedente segue un importantissimo corollario, che ci permette di esprimere in un modo semplice l'altezza di Weil di un numero algebrico, dipendentemente dalla misura di Mahler di quest'ultimo.

**Corollario 2.19**
*Per ogni numero algebrico $\alpha$, si ha che*

$$h(\alpha) = \frac{\log M(\alpha)}{[\mathbb{Q}(\alpha):\mathbb{Q}]}.$$

*Dimostrazione.* Usiamo il Teorema 2.18 e la Definizione 2.16 scegliendo come polinomio $P$ il polinomio minimo di $\alpha$ su $\mathbb{Z}$ e come campo $K = \mathbb{Q}$. Dal Teorema di Ostrowski 1.14 sappiamo che i valori assoluti su $\mathbb{Q}$ a meno di equivalenza sono il valore assoluto ordinario e quelli $p$-adici; possiamo quindi calcolare i valori di $M_v(P)$ al variare di $v \in \mathcal{M}_{\mathbb{Q}}$. Dato che $P$ è un polinomio primitivo, otteniamo che

$$M_p(P) = 1$$

per ogni primo razionale $p$, mentre

$$M_\infty(P) = M(P)$$

in quanto l'unica immersione di $\mathbb{Q}$ in $\overline{\mathbb{Q}}$ è l'identità. Segue che per la Definizione 2.16

$$\hat{h}(P) = \sum_{v \in \mathcal{M}_{\mathbb{Q}}} \log M_v(P) = \log M(P).$$

Denotando ora con $\alpha_1, ..., \alpha_n$ i coniugati di $\alpha$, dal Teorema 2.18 segue che

$$\hat{h}(P) = \sum_{j=1}^{n} h(\alpha_j) = nh(\alpha),$$

dove l'ultima uguaglianza segue direttamente dal fatto che

$$\sum_{\substack{v \in \mathcal{M}_K \\ v \nmid \infty}} n_v \log^+ |\alpha|_v = \log(a)$$

con $a$ coefficiente direttore di $P$. Per mostrare questa uguaglianza possiamo supporre, a meno di localizzare alla parte moltiplicativa data dal complementare dei primi che compaiono nella fattorizzazione di $\alpha$, che $\mathcal{O}_{\mathbb{Q}(\alpha)}$ sia un PID. Allora $\alpha = \beta/\gamma$ per certi $\beta, \gamma \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ ridotti ai minimi termini, in questo modo

$$\log^+ |\alpha|_v = \max(\log \left|\frac{\beta}{\gamma}\right|_v, 0) = \begin{cases} \log |\beta|_v - \log |\gamma|_v & \text{se } |\beta|_v > |\gamma|_v, \\ 0 & \text{se } |\beta|_v \leq |\gamma|_v. \end{cases}$$

Possiamo allora limitarci a considerare i primi che dividono $\gamma$ e da qua la conclusione segue considerando il polinomio minimo di $\alpha$ che in $\mathbb{Z}$ ha coefficiente direttore $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\gamma)$. Uguagliando i risultati otteniamo la tesi. □

Concludiamo la sezione e il capitolo con due semplici ma importanti corollari.

**Corollario 2.20**
*Per ogni polinomio $P \in \overline{\mathbb{Q}}[x]$ si ha che $\hat{h}(P) = 0$ se e soltanto se ogni radice di $P$ è una radice dell'unità.*

**Corollario 2.21**
*Se $\alpha$ e $\beta$ sono coniugati allora $h(\alpha) = h(\beta)$.*

Capitolo 3

# Minorazione dell'altezza in un'estensione abeliana

Questo capitolo è incentrato su una risoluzione parziale del problema di Lehmer, già presentato nell'introduzione a questo elaborato di tesi, nel particolare caso in cui il numero algebrico $\alpha$ (diverso da zero e da una radice dell'unità) sia generatore di un'estensione abeliana dei razionali. In particolare verrà prodotto un estremo inferiore ai possibili valori che l'altezza logaritmica può assumere per numeri algebrici con la proprietà sopra citata.

Un primo risultato parziale fu trovato da Schinzel [11], che è riuscito a mostrare che in campi totalmente reali o CM (ovvero estensioni quadratiche immaginarie di campi totalmente reali) esiste una minorazione assoluta dell'altezza logaritmica che non dipende dal grado dell'estensione per certi numeri algebrici. Il risultato è presentato nel seguente

**Teorema 3.1 - Schinzel**
*Sia $K$ un campo di numeri totalmente reale o CM e sia $\alpha \in K^*$ un numero algebrico tale che $|\alpha| \neq 1$; allora*

$$H(\alpha) \geq \sqrt{\frac{1+\sqrt{5}}{2}} = 1.272... \, .$$

Per una dimostrazione si veda [11].

Nel caso in cui $\alpha$ sia un intero algebrico, la condizione $|\alpha| \neq 1$ non è restrittiva, in quanto sotto l'ipotesi in cui $K$ sia un campo CM o totalmente reale, se $|\alpha| = 1$, allora tutti i coniugati di $\alpha$ hanno modulo 1 e di conseguenza $\alpha$ è una radice dell'unità. Infatti, nel caso in cui $K$ sia totalmente reale si ha che se $|\alpha| = 1$ allora $\alpha = \pm 1$ e quindi anche $\sigma(\alpha) = \pm 1$ per ogni $\sigma : K \to \mathbb{C}$, mentre se $K$ è CM allora o $\alpha$ sta nella sottoestensione reale (e si cade nel caso precedente) oppure $\alpha \in K \cap \mathbb{C}$ e dato che $K$ è un'estensione di grado due di un campo totalmente reale, l'unico coniugato di $\alpha$ è $\overline{\alpha}$ e quindi $|\alpha| = 1 \Rightarrow |\overline{\alpha}| = 1$.
La condizione $|\alpha| \neq 1$ diventa però rilevante nel momento in cui si vuole cercare di minorare l'altezza di numeri che non sono interi algebrici e si vuole dunque capire se, sotto determinate ipotesi, possa essere omessa. Il seguente teorema, che è il risultato principale di questo lavoro di tesi, dà una risposta affermativa, seppur parziale, al problema appena esposto, nel particolare caso di estensioni abeliane dei razionali.

**Teorema 3.2**
*Sia $L/\mathbb{Q}$ un'estensione abeliana e sia $\alpha \in L^*$ diverso da una radice dell'unità. Allora*

$$h(\alpha) \geq \frac{\log 5}{12} = 0.1341... .$$

Non sappiamo se questo sia un estremo inferiore ottimale o se possa essere ulteriormente raffinato, ma è possibile mostrare che la costante $\log 5/12$ non può essere sostituita con nessun numero maggiore di $\log 7/12 = 0.162...$ (la dimostrazione di questo fatto si trova alla fine di questa sezione). Presentiamo adesso tutti gli strumenti necessari alla dimostrazione del Teorema 3.2.

### 3.0.1 Lemmi preliminari

Nella trattazione che segue useremo la seguente notazione: indicheremo con $K_m$ il campo ciclotomico $\mathbb{Q}(\zeta_m)$, dove $m$ è un intero naturale $m \not\equiv 2 \mod 4$ e $\zeta_m$ è una radice primitiva $m$-esima dell'unità. Utilizzeremo inoltre la seguente proposizione, la cui dimostrazione può essere trovata in [9]:

**Proposizione 3.3**
*Sia $\zeta_m$ una radice primitiva $m$-esima dell'unità, con $m \not\equiv 2 \mod 4$. Allora l'anello degli interi dell'estensione ciclotomica $K_m = \mathbb{Q}(\zeta_m)$ è $\mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$.*

Introduciamo dei lemmi preliminari che risulteranno cruciali nella dimostrazione della disuguaglianza presentata nel Teorema 3.2.

**Lemma 3.4**
*Sia $p$ un primo razionale. Esiste un omomorfismo $\sigma_p \in Gal(K_m/\mathbb{Q})$ con le seguenti proprietà:*
*1) Se $p$ non divide $m$, allora per ogni $\gamma \in \mathcal{O}_{K_m}$ si ha che $\gamma^p \equiv \sigma_p(\gamma) \mod p\mathcal{O}_{K_m}$.*
*2) Se $p$ divide $m$, allora per ogni $\gamma \in \mathcal{O}_{K_m}$ si ha che $\gamma^p \equiv \sigma_p(\gamma^p) \mod p\mathcal{O}_{K_m}$. Inoltre, per ogni $\alpha \in \mathcal{O}_{K_m}$ che verifica $\sigma_p(\alpha^p) = \alpha^p$, esiste una radice dell'unità $\zeta \in K_m$ tale che $\zeta\alpha \in K'$, dove $K'$ è un'estensione ciclotomica di $\mathbb{Q}$ strettamente contenuta in $K_m$.*

*Dimostrazione.* 1. Supponiamo che $p$ non divida $m$ e sia $\sigma_p \in Gal(K_m/\mathbb{Q})$ l'unico omomorfismo che verifica $\sigma(\zeta_m) = \zeta_m^p$. Sia $\gamma \in \mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$, esiste allora un polinomio $F \in \mathbb{Z}[x]$ tale che $\gamma = F(\zeta_m)$. Per il Piccolo Teorema di Fermat, esiste un polinomio $G \in \mathbb{Z}[x]$ tale che $F(x)^p = F(x^p) + pG(x)$, dunque abbiamo che

$$\gamma^p = F(\zeta_m)^p = F(\zeta_m^p) + pG(\zeta_m) \equiv \sigma_p(\gamma) \mod p\mathcal{O}_{K_m}.$$

2. Supponiamo che $p$ divida $m$ e consideriamo in questo caso $\sigma_p$ un generatore del gruppo $Gal(K_m/K_{m/p})$, che è ciclico di ordine $p$ nel caso in cui $p^2$ divide $m$, di ordine $p-1$ altrimenti. Sia ora $\gamma \in \mathcal{O}_{K_m}$, come nel caso precedente esistono un polinomio $F \in \mathbb{Z}[x]$ e un polinomio $G \in \mathbb{Z}[x]$ tali che $\gamma = F(\zeta_m)$ e $F(x)^p = F(x^p) + pG(x)$. Si ha allora che

$$\gamma^p = F(\zeta_m)^p = F(\zeta_m^p) + pG(\zeta_m) \equiv F(\zeta_m^p) \mod p\mathcal{O}_{K_m}$$

e

$$\sigma_p(\gamma^p) = \sigma_p(F(\zeta_m)^p) \equiv \sigma_p(F(\zeta_m^p)) \mod p\mathcal{O}_{K_m}. \tag{3.1}$$

Inoltre $\zeta_m^p \in K_{m/p}$ e dunque, dato che $\langle\sigma_p\rangle = Gal(K_m/K_{m/p})$, si ha che $\sigma_p(\zeta_m^p) = \zeta_m^p$ e di conseguenza $F(\zeta_m^p) = \sigma_p(F(\zeta_m^p))$. Sostituendo nella (3.1) si ottiene $\gamma^p = \sigma_p(\gamma^p) \mod p\mathcal{O}_{K_m}$.
Per dimostrare la seconda affermazione, supponiamo che esista un elemento $\alpha \in K_m$ tale che $\sigma_p(\alpha^p) = \alpha^p$. Dal momento che $\sigma_p(\zeta_m^p) = \zeta_m^p$ e che $\sigma_p$ è un generatore di $Gal(K_m/K_{m/p})$, si ha che

$$\sigma_p(\zeta_m) = \zeta_p\zeta_m$$

dove $\zeta_p$ è una radice $p$-esima primitiva dell'unità. Con le stesse argomentazioni, esiste un intero $u \in \mathbb{Z}$ tale che $\sigma_p(\alpha) = \zeta_p^u \alpha$. Deduciamo da ciò che

$$\sigma_p\Big(\frac{\alpha}{\zeta_m^u}\Big) = \frac{\zeta_p^u \alpha}{\zeta_m^u \zeta_p^u} = \frac{\alpha}{\zeta_m^u},$$

ma allora $\alpha/\zeta_m^u$ è un elemento fissato da $\sigma_p$, che è un generatore di $Gal(K_m/K_{m/p})$: dalla teoria di Galois classica segue che $\alpha/\zeta_m^u \in K_{m/p}$ e ciò conclude la dimostrazione del lemma. □

**Lemma 3.5**
*Siano $K$ un campo di numeri e $\alpha \in K^*$ un elemento non nullo. Sia inoltre $v \in \mathcal{M}_K$ un primo non archimedeo. Esiste allora un intero algebrico $\beta \in \mathcal{O}_K$ tale che $\beta\alpha \in \mathcal{O}_K$ e $|\beta|_v = \max(1, |\alpha|_v)^{-1}$.*

*Dimostrazione.* Sia

$$\alpha\mathcal{O}_K = \prod_{i=1}^{n} \mathfrak{p}_i^{a_i}$$

la fattorizzazione di $(\alpha)$ come ideale frazionario di $K$, garantita dal Teorema 1.4, dove $a_i \in \mathbb{Z} - \{0\}$ per ogni $i \in \{1, ..., n\}$. Separiamo la dimostrazione in due casi:
1) Supponiamo che esista un $i \in \{1, ..., n\}$ tale che $|\cdot|_v = |\cdot|_{\mathfrak{p}_i}$. Allora, un $\beta$ che rispetti le condizioni della tesi deve essere soluzione del sistema

$$\begin{cases} \beta \equiv 0 \mod \mathfrak{p}_j^{-a_j} & \text{se } a_j < 0, \text{ con } j \in \{1, ..., n\}, \\ \beta \in \mathfrak{p}_{\mathfrak{i}}{}^{-a_i} \smallsetminus \mathfrak{p}_{\mathfrak{i}}{}^{-(a_i+1)} \end{cases}$$

e, dato che ci sono solo un numero finito di condizioni da soddisfare, una soluzione a questo sistema esiste per il Teorema cinese del resto.
2) Supponiamo ora invece che $|\cdot|_v = |\cdot|_{\mathfrak{p}}$ per un certo ideale primo $\mathfrak{p} \in \mathcal{O}_K$ diverso da ognuno dei $\mathfrak{p}_i$. Allora, un $\beta$ che rispetti le condizioni della tesi deve essere soluzione del sistema

$$\begin{cases} \beta \equiv 0 \mod \mathfrak{p}_i^{-a_i} & \text{se } a_i < 0, \\ \beta \equiv 1 \mod \mathfrak{p} \end{cases}$$

e anche in questo caso una soluzione a questo sistema esiste per il Teorema cinese del resto. □

Il precedente lemma è particolarmente importante perché mostra l'esistenza di un denominatore locale all'interno di un campo di numeri.

**Lemma 3.6**
*Sia $\alpha \in \overline{\mathbb{Q}}$ un numero algebrico non nullo, appartenente a un certo campo ciclotomico $K_m$ e sia $p \geq 3$ un primo razionale. Supponiamo che $\alpha$ non sia una radice dell'unità.*
*1) Se $p$ non divide $m$, allora*

$$h(\alpha) \geq \frac{\log(p/2)}{p+1}.$$

*2) Supponiamo ora che per ogni radice dell'unità $\zeta$, il campo $\mathbb{Q}(\zeta\alpha)$ non sia contenuto in nessun campo ciclotomico $K_n \subsetneq K_m$ (con $n < m$, $n|m$). Allora, per ogni primo razionale $p$ che divide $m$, si ha che*

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

*Dimostrazione.* 1) Supponiamo che $p \nmid m$ e cerchiamo di maggiorare $|\alpha^p - \sigma_p(\alpha)|_v$ per ogni primo $v \in \mathcal{M}_{K_m}$ di $K_m$, così da ottenere la disuguaglianza voluta utilizzando la formula del prodotto 1.23. Sia allora $v \in \mathcal{M}_{K_m}$ tale che $v|p$. Dal Lemma 3.5, sappiamo che esiste $\beta \in \mathcal{O}_{K_m}$, tale che $\beta\alpha \in \mathcal{O}_{K_m}$ e $|\beta|_v = \max(1, |\alpha|_v)^{-1}$, mentre grazie al Lemma 3.4, possiamo affermare che esiste un omomorfismo $\sigma_p \in Gal(K_m/\mathbb{Q})$ tale che $(\alpha\beta)^p - \sigma_p(\alpha\beta), \beta^p - \sigma_p(\beta) \in p\mathcal{O}_{K_m}$. Otteniamo dunque che

$$|(\alpha\beta)^p - \sigma_p(\alpha\beta)|_v \leq \frac{1}{p}$$

e che

$$|\beta^p - \sigma_p(\beta)|_v \leq \frac{1}{p}.$$

Combinando i risultati ottenuti e utilizzando la disuguaglianza ultrametrica

$$\begin{aligned} |\alpha^p - \sigma_p(\alpha)|_v &= |\beta|_v^{-p} |(\alpha\beta)^p - \sigma_p(\alpha\beta) + (\sigma_p(\beta) - \beta^p)\sigma_p(\alpha)|_v \\ &\leq |\beta|_v^{-p} \max(|(\alpha\beta)^p - \sigma_p(\alpha\beta)|_v, |\sigma_p(\beta) - \beta^p|_v |\sigma_p(\alpha)|_v) \\ &\leq \frac{1}{p} \max(1, |\alpha|_v)^p \max(1, |\sigma_p(\alpha)|_v). \end{aligned}$$

Per quanto riguarda i restanti valori assoluti non archimedei, cioè quelli tali che $w \in \mathcal{M}_{K_m}$ con $w \nmid p$ e $m \nmid \infty$, utilizzando la disuguaglianza ultrametrica otteniamo:

$$|\alpha^p - \sigma_p(\alpha)|_w \leq \max(1, |\alpha|_w)^p \max(1, |\sigma_p(\alpha)|_w).$$

E infine, per i valori assoluti archimedei, grazie alla disuguaglianza triangolare si ha

$$\begin{aligned} |\alpha^p - \sigma_p(\alpha)|_v \leq |\alpha|_v^p + |\sigma_p(\alpha)|_v \leq \max(1, |\alpha|_v)^p \max(1, |\sigma_p(\alpha)|_v) + \max(1, |\alpha|_v)^p \max(1, |\sigma_p(\alpha)|_v) = \\ = 2 \max(1, |\alpha|_v)^p \max(1, |\sigma_p(\alpha)|_v). \end{aligned}$$

Dall'ipotesi che $\alpha$ non sia né nullo né una radice dell'unità, segue che $\alpha^p - \sigma_p(\alpha) \neq 0$, se infatti così fosse, avremmo che $ph(\alpha) = h(\alpha^p) = h(\sigma_p(\alpha)) = h(\alpha)$, da cui $h(\alpha) = 0$, in contraddizione con la Proposizione 2.13. Possiamo allora applicare la formula del prodotto 1.23 all'elemento $\alpha^p - \sigma_p(\alpha)$, insieme alla Proposizione 1.26 e alle disuguaglianze trovate di sopra, ottenendo:

$$\begin{aligned} 0 = \sum_{v \in \mathcal{M}_{K_m}} n_v \log |\alpha^p - \sigma_p(\alpha)|_v \leq \sum_{\substack{v \in M_{K_m} \\ v|p}} n_v \log \frac{1}{p} + \sum_{\substack{v \in M_{K_m} \\ v|\infty}} n_v \log 2 \\ + p \sum_{v \in \mathcal{M}_{K_m}} n_v \log^+(|\alpha|_v) + \sum_{v \in \mathcal{M}_{K_m}} n_v \log^+(|\sigma_p(\alpha)|_v) \\ = [K_m : \mathbb{Q}]\Big( \log \frac{2}{p} + ph(\alpha) + h(\sigma_p(\alpha))\Big) = [K_m : \mathbb{Q}]\Big( - \log \frac{p}{2} + (p+1)h(\alpha)\Big), \end{aligned}$$

che dà la disuguaglianza cercata.
2) Il caso in cui $p$ divide $m$ si tratta come il precedente, andando però a sostituire l'elemento $\sigma_p(\alpha)$ con $\sigma_p(\alpha^p)$, in accordo con il Lemma 3.4, ottenendo le seguenti disuguaglianze:

$$|\alpha^p - \sigma_p(\alpha^p)|_v \leq \begin{cases} \frac{1}{p} \max(1, |\alpha|_v)^p \max(1, |\sigma_p(\alpha)|_v)^p & \text{se } v|p \\ \max(1, |\alpha|_v)^p \max(1, |\sigma_p(\alpha)|_v)^p & \text{se } v \nmid p \text{ e } v \nmid \infty \\ 2 \max(1, |\alpha|_v)^p \max(1, |\sigma_p(\alpha)|_v)^p & \text{se } v|\infty \end{cases}.$$

Grazie a queste, applicando ancora una volta la formula del prodotto 1.23 all'elemento $\alpha^p - \sigma_p(\alpha)^p$, che è diverso da 0 per le ipotesi fatte sul campo e per il punto 2 del Lemma 3.4, deduciamo

$$0 \leq [K_m : \mathbb{Q}]\Big( -\log \frac{p}{2} + 2ph(\alpha)\Big).$$

da cui segue la tesi. □

Osserviamo che il lemma precedente offre una stima dal basso dell'altezza di Weil leggermente più piccola della costante presentata nel Teorema 3.2; vale infatti la prossima proposizione, la cui dimostrazione passa attraverso il seguente teorema di importanza capitale nella teoria dei numeri:

**Teorema 3.7 - Kronecker-Weber**
*Ogni estensione abeliana di $\mathbb{Q}$ è contenuta in un'estensione ciclotomica.*

**Proposizione 3.8**
*Sia $L/\mathbb{Q}$ un'estensione abeliana e sia $\alpha \in L^*$ diverso da una radice dell'unità. Allora*

$$h(\alpha) \geq \frac{\log(5/2)}{10} = 0.0916... \ .$$

*Dimostrazione.* Denotiamo con $K_m$ il più piccolo campo ciclotomico tale per cui esiste una radice dell'unità $\zeta$ con la proprietà che $\zeta\alpha \in K_m$: tale campo esiste per il teorema di Kronecker-Weber 3.7. Consideriamo il risultato della Proposizione 3.6, nel caso specifico in cui $p = 5$. Allora, otteniamo la disuguaglianza

$$h(\alpha) = h(\zeta_m\alpha) \geq \min\Big(\frac{\log(5/2)}{6}, \frac{\log(5/2)}{10}\Big) = \frac{\log(5/2)}{10}.$$

Il caso $p = 5$ è ottimale, in quanto per $p \geq 7$ o $p = 3$

$$\min\Big(\frac{\log(p/2)}{2p}, \frac{\log(p/2)}{p+1}\Big) = \frac{\log(p/2)}{2p} < \frac{\log(5/2)}{10},$$

dato che la funzione $f(x) = \frac{\log(x/2)}{2x}$ ha un massimo in $x = 2e = 5,436... \ .$ □

Per raggiungere la stima annunciata nel Teorema 3.2, studiamo il caso speciale $p = 2$.

### 3.0.2 Dimostrazione del risultato principale

Come preannunciato alla fine dello scorso paragrafo, studiamo il caso $p = 2$ e vediamo come i lemmi sopra presentati possano essere opportunamente ampliati.

**Lemma 3.9**
*Esiste un omomorfismo $\sigma = \sigma_2 \in Gal(K_m/\mathbb{Q})$ con le seguenti proprietà:*
*1) Se 4 non divide $m$, allora per ogni $\gamma \in \mathcal{O}_{K_m}$ si ha che $\gamma^4 \equiv \sigma(\gamma^2) \mod 4\mathcal{O}_{K_m}$.*
*2) Se 4 divide $m$, allora per ogni $\gamma \in \mathcal{O}_{K_m}$ si ha che $\gamma^2 \equiv \sigma(\gamma^2) \mod 4\mathcal{O}_{K_m}$.*

Ricordiamo che nel Lemma 3.4 si avevano le condizioni più deboli $\sigma(\gamma) \equiv \gamma^2 \mod 2\mathcal{O}_{K_m}$ quando $m$ è dispari e $\sigma(\gamma^2) \equiv \gamma^2 \mod 2\mathcal{O}_{K_m}$ quando $m$ è pari.

*Dimostrazione.* 1) È una diretta conseguenza del Lemma 3.4, in quanto vale la fattorizzazione

$$\gamma^4 - \sigma(\gamma^2) = (\gamma^2 - \sigma(\gamma))((-\gamma)^2 - \sigma(-\gamma)).$$

2) Sia $\gamma \in \mathcal{O}_{K_m}$, allora esistono coefficienti $a_0, ..., a_s \in \mathbb{Z}$ tali che $\gamma = \sum_{i=0}^{n} a_i \zeta_m^i$. Si ha che

$$\sigma(\gamma) = \sum_{i=0}^{n} a_i \sigma(\zeta_m)^i = \sum_{i=0}^{n} (-1)^i a_i \zeta_m^i,$$

da cui seguono $\sigma(\gamma) - \gamma \equiv 0 \mod 2\mathcal{O}_{K_m}$ e $\sigma(\gamma) + \gamma \equiv 0 \mod 2\mathcal{O}_{K_m}$ e quindi

$$\sigma(\gamma^2) - \gamma^2 \equiv 0 \mod 4\mathcal{O}_{K_m}.$$

□

**Lemma 3.10**
*Siano $x_1, ..., x_k \in (-1, 1)$ $k$ numeri reali di modulo minore di 1 e consideriamo le seguenti due funzioni reali:*

$$f(x) = 4\log 2 - 2\log^+ \sqrt{2 - 2x}; \qquad g(x) = 3\log 2 - \log^+ \sqrt{4 - 4x^2}.$$

*Allora*

$$\frac{1}{k} \max\Big\{ \sum_{j=1}^{k} f(x_j), \sum_{j=1}^{k} g(x_j) \Big\} \geq \log 5.$$

*Dimostrazione.* Consideriamo i seguenti tre insiemi:

$$I_1 = \Big\{ x \mid -1 < x \leq -\frac{\sqrt{3}}{2} \Big\},$$

$$I_2 = \Big\{ x \mid -\frac{\sqrt{3}}{2} < x \leq \frac{1}{2} \Big\},$$

$$I_3 = \Big\{ x \mid \frac{1}{2} < x \leq 1 \Big\}.$$

Si ha che

$$\begin{cases} f(x) \geq 2\log 2, & \text{se } x \in I_1; \\ f(x) = 4\log 2, & \text{se } x \in I_3; \end{cases}$$

$$\begin{cases} g(x) = 3\log 2, & \text{se } x \in I_1; \\ g(x) \geq 3\log 2 - \log\sqrt{3}, & \text{se } x \in I_3. \end{cases}$$

Inoltre, per $x \in I_2$, si verifica facilmente che $f$ e $g$ sono funzioni convesse, quindi, denotando con $k_l$ il numero di $j$ per cui $x_j \in I_l$, si hanno le disuguaglianze:

$$\frac{1}{k} \sum_j f(x_j) \geq \frac{k_1}{k} \cdot 2\log 2 + \frac{k_2}{k} \cdot f\Big( \frac{1}{k_2} \sum_{x_j \in I_2} x_j \Big) + \frac{k_3}{k} \cdot 4\log 2;$$

$$\frac{1}{k} \sum_j g(x_j) \geq \frac{k_1}{k} \cdot 3\log 2 + \frac{k_2}{k} \cdot g\Big( \frac{1}{k_2} \sum_{x_j \in I_2} x_j \Big) + \frac{k_3}{k} \cdot (3\log 2 - \log\sqrt{3}).$$

Siano poi

$$F(x_0, ; y_1, y_2, y_3) = y_1 \cdot 2\log 2 + y_2 \cdot f(x_0) + y_3 \cdot 4\log 2,$$

$$G(x_0,;y_1,y_2,y_3) = y_1 \cdot 3\log 2 + y_2 \cdot g(x_0) + y_3 \cdot (3\log 2 - \log\sqrt{3}).$$

Inferiamo dalle disuguaglianze presentate sopra che

$$\frac{1}{k}\max\Big\{\sum_{j=1}^{k} f(x_j), \sum_{j=1}^{k} g(x_j)\Big\} \geq \min_{\substack{x_0\in I_2 \\ y_1+y_2+y_3=1}} \max\{F(x_0;y_1,y_2,y_3), G(x_0,;y_1,y_2,y_3)\} = \log 5.$$

□

**Teorema 3.11**
*Sia $\alpha \in K_m^*$. Valgono i seguenti fatti:*
*1) Se $4|m$ e non esiste nessuna radice dell'unità $\zeta \in K_m$ tale che $\alpha\zeta$ sia contenuto in una sottoestensione ciclotomica propria di $K_m$, allora*

$$h(\alpha) \geq \frac{\log 2}{4} = 0.1732...;$$

*2) Se $4 \nmid m$ e $\alpha$ non è una radice dell'unità, allora*

$$h(\alpha) \geq \frac{\log 5}{12} = 0.1341... .$$

*Dimostrazione.* 1) Assumiamo che $4|m$ e che $\alpha\zeta$ non sia contenuto in nessuna sottoestensione ciclotomica propria di $K_m$ per ogni radice dell'unità $\zeta \in K_m$. Allora la dimostrazione della disuguaglianza

$$h(\alpha) \geq \frac{\log 2}{4}$$

può essere ottenuta come la dimostrazione della disuguaglianza

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

nella dimostrazione del Lemma 3.6, sostituendo la relazione $\gamma^p \equiv \sigma_p(\gamma^p) \mod p\mathcal{O}_{K_m}$ con la relazione più forte $\gamma^2 \equiv \sigma(\gamma^2) \mod 4\mathcal{O}_{K_m}$.
Fissiamo $v \in \mathcal{M}_{K_m}$ un primo di $K_m$ tale che $v|2$. Dal Lemma 3.5, sappiamo che esiste $\beta \in \mathcal{O}_{K_m}$, tale che $\beta\alpha \in \mathcal{O}_{K_m}$ e $|\beta|_v = \max(1,|\alpha|_v)^{-1}$, mentre grazie al Lemma 3.9, possiamo affermare che esiste un omomorfismo $\sigma \in Gal(K_m/\mathbb{Q})$ tale che $(\alpha\beta)^2 - \sigma((\alpha\beta)^2), \beta^2 - \sigma(\beta^2) \in 4\mathcal{O}_{K_m}$. Allora

$$|(\alpha\beta)^2 - \sigma((\alpha\beta)^2)|_v \leq \frac{1}{4}$$

e

$$|\beta^2 - \sigma(\beta^2)|_v \leq \frac{1}{4}.$$

Combinando allora i risultati e utilizzando la disuguaglianza ultrametrica si ottiene che

$$\begin{aligned}|\alpha^2 - \sigma(\alpha^2)|_v &= |\beta|_v^{-2}|(\alpha\beta)^2 - \sigma((\alpha\beta)^2) + (\sigma(\beta^2) - \beta^2)\sigma(\alpha^2)|_v \\ &\leq |\beta|_v^{-2}\max(|(\alpha\beta)^2 - \sigma((\alpha\beta)^2)|_v, |\sigma(\beta^2) - \beta^2|_v|\sigma(\alpha^2)|_v) \\ &\leq \frac{1}{4}\max(1,|\alpha|_v)^2\max(1,|\sigma(\alpha^2)|_v).\end{aligned}$$

Per quanto riguarda i restanti valori assoluti non archimedei, cioè quelli tali che $w \in \mathcal{M}_{K_m}$ con $w \nmid 2$ e $m \nmid \infty$, utilizzando la disuguaglianza ultrametrica otteniamo:

$$|\alpha^2 - \sigma(\alpha^2)|_w \leq \max(1,|\alpha|_w)^2\max(1,|\sigma(\alpha^2)|_w).$$

E infine, per i valori assoluti archimedei, grazie alla disuguaglianza triangolare si ha

$$|\alpha^2-\sigma(\alpha^2)|_v \le |\alpha|_v^2+|\sigma(\alpha^2)|_v \le \max(1,|\alpha|_v)^2\max(1,|\sigma(\alpha^2)|_v)+\max(1,|\alpha|_v)^2\max(1,|\sigma(\alpha^2)|_v)=$$
$$=2\max(1,|\alpha|_v)^2\max(1,|\sigma(\alpha^2)|_v).$$

Adesso, dato che $\alpha^2-\sigma(\alpha^2)\neq 0$ per quanto detto in 3.6 applicando la formula del prodotto 1.23 all'elemento $\alpha^2-\sigma(\alpha^2)$, insieme alla Proposizione 1.26 e alle disuguaglianze trovate di sopra, otteniamo:

$$0=\sum_{v\in\mathcal{M}_{K_m}} n_v\log|\alpha^2-\sigma(\alpha^2)|_v \le \sum_{\substack{v\in M_{K_m}\\ v|2}} n_v\log\frac{1}{4}+\sum_{\substack{v\in M_{K_m}\\ v|\infty}} n_v\log 2$$
$$+2\sum_{v\in\mathcal{M}_{K_m}} n_v\log^+(|\alpha|_v)+2\sum_{v\in\mathcal{M}_{K_m}} n_v\log^+(|\sigma(\alpha)|_v)$$
$$=[K_m:\mathbb{Q}]\Big(\log\frac{2}{4}+2h(\alpha)+2h(\sigma(\alpha))\Big)=[K_m:\mathbb{Q}]\Big(-\log 2+4h(\alpha)\Big),$$

che dà la disuguaglianza cercata.
2) Supponiamo ora che $4\nmid m$ e che $\gamma$ non sia una radice dell'unità. Sostituendo la relazione $\gamma^p\equiv\sigma(\gamma)^p \mod p\mathcal{O}_{K_m}$ con la relazione più forte $\gamma^4\equiv\sigma(\gamma^2) \mod 4\mathcal{O}_{K_m}$ nel Lemma 3.6, otteniamo

$$h(\alpha)\ge\frac{2\log 2+\frac{2}{\varphi(m)}\sum_{v|\infty}\log^+|\alpha^4-\sigma(\alpha^2)|_v}{6},$$

dove con $\varphi$ indichiamo la funzione $\varphi$ di Eulero. Similmente, considerando $\alpha^8-\sigma(\alpha^4)$, otteniamo un'espressione analoga

$$h(\alpha)\ge\frac{3\log 2+\frac{2}{\varphi(m)}\sum_{v|\infty}\log^+|\alpha^8-\sigma(\alpha^4)|_v}{12}.$$

Se $|\alpha|\neq 1$, dal Teorema 3.1 abbiamo il bound inferiore

$$h(\alpha)\ge\frac{1}{2}\log\frac{1+\sqrt{5}}{2}=0.2406...\,,$$

possiamo allora supporre che $|\alpha|=1$ e che quindi $|\alpha|_v=1$ per ogni primo archimedeo $v\in\mathcal{M}_{K_m}$ di $K_m$. Poniamo allora $\sigma(\alpha^2)=\alpha^4e^{it}$ e per ogni primo archimedeo $v\in\mathcal{M}_{K_m}$ di $K_m$ definiamo $|1-e^{it}|_v=|1-e^{it_v}|$. Con tali notazioni si ottiene che

$$|\alpha^4-\sigma(\alpha)^2|_v=|\alpha^4-\alpha^4e^{it}|_v=|\alpha^4|_v|1-cos(t_v)+i\,sin(t_v)|$$
$$=\sqrt{1+cos^2(t_v)-2cos(t_v)+sin^2(t_v)}=\sqrt{2-2cos(t_v)}$$

e analogamente

$$|\alpha^8-\sigma(\alpha)^4|_v=\sqrt{4-4cos^2(t_v)}.$$

Sostituendo nelle disuguaglianze di sopra si ha

$$h(\alpha)\ge\frac{1}{12}\max\Big\{\frac{2}{\varphi(m)}\sum_{v|\infty}(4\log 2-2\log^+\sqrt{2-2cos(t_v)}),\frac{2}{\varphi(m)}\sum_{v|\infty}(3\log 2-\log^+\sqrt{4-4cos^2(t_v)})\Big\}.$$

Ma allora, ponendo $x_v=cos(t_v)$ possiamo applicare il Lemma 3.10, infatti il numero di valori assoluti archimedei a meno di equivalenza coincide con il numero di coppie di immersioni complesse di $K_m$ in $\overline{\mathbb{Q}}$ (in quanto $K_m$ è un'estensione puramente immaginaria di $\mathbb{Q}$ e non ci sono immersioni reali nella chiusura algebrica), che sono proprio $\varphi(m)/2$. Si ottiene così che

$$h(\alpha)\ge\frac{\log 5}{12},$$

che è la tesi. □

Combiniamo ora il Lemma 3.6 e il Teorema 3.11 e osserviamo che per i primi $p \geq 13$ abbiamo

$$\frac{\log(p/2)}{p+1} < \frac{\log 5}{12} < \frac{\log(11/2)}{12} < \frac{\log(5/2)}{6} < \frac{\log(7/2)}{8} < \frac{\log(2)}{4}.$$

Definiamo allora il simbolo

$$c(m) = \begin{cases} \frac{\log(7/2)}{8}, & \text{se } 7 \nmid m; \\ \frac{\log(5/2)}{6}, & \text{se } 7|m \text{ e } 5 \nmid m; \\ \frac{\log(11/2)}{12}, & \text{se } 35|m \text{ e } 11 \nmid m; \\ \frac{\log(5)}{12}, & \text{se } 385|m. \end{cases}$$

Abbiamo così provato il seguente teorema:

**Teorema 3.12**
*Sia $\alpha \in K_m^*$. Allora*
*1) Se $\alpha$ non è una radice dell'unità,*

$$h(\alpha) \geq c(m);$$

*2) Se $4|m$ e non esiste nessuna radice dell'unità $\zeta \in K_m$ tale che $\alpha\zeta$ sia contenuto in una sottoestensione ciclotomica propria di $K_m$,*

$$h(\alpha) \geq \frac{\log 2}{4}.$$

In particolare, combinando il precedente teorema con il Teorema di Kronecker-Weber 3.7, otteniamo una dimostrazione del Teorema 3.2.

*Dimostrazione.* (del Teorema 3.2) Denotiamo con $K_m$ il più piccolo campo ciclotomico tale per cui esiste una radice dell'unità $\zeta$ con la proprietà che $\zeta\alpha \in K_m$: tale campo esiste per il teorema di Kronecker-Weber 3.7. Dal Teorema 3.12 segue

$$h(\alpha) = h(\zeta\alpha) \geq \min\Big(\frac{\log(7/2)}{8}, \frac{\log(5/2)}{6}, \frac{\log(11/2)}{12}, \frac{\log 5}{12}, \frac{\log 2}{4}\Big) = \frac{\log 5}{12}.$$

□

Come era stato anticipato all'inizio del capitolo, non sappiamo se la costante $\log 5/12$ sia ottimale, ma possiamo affermare che essa non può essere sostituita da nessun numero maggiore di $\log 7/12$.

**Esempio 3.1**
Sia $K = K_{21}$. Consideriamo la fattorizzazione di $(7)$ in $\mathcal{O}_{K_{21}} = \mathbb{Z}[\zeta_{21}]$, data dal teorema di Kummer. Dal momento che $\Phi_{21}(x) \equiv (x+5)^6(x+3)^6 \mod 7$ si ha che

$$(7)\mathbb{Z}[\zeta_{21}] = (7, \zeta_{21}+5)^6(7, \zeta_{21}+3)^6,$$

ovvero $(7)$ si fattorizza come prodotto di due primi con indice di ramificazione 6 e grado d'inerzia 1. Visto che $\mathbb{Z}[\zeta_{21}]$ è un PID (si veda la sezione successiva per un dettaglio completo sull'argomento, Teorema 3.16) i due ideali $(7, \zeta_{21}+5)$ e $(7, \zeta_{21}+3)$ possono essere riscritti in termini di un generatore, in particolare, facendo uso di un calcolatore, otteniamo che: $(7, \zeta_{21}+5) = (\gamma)$ con

$$\gamma = \zeta_{21}^{11} - \zeta_{21}^{9} + \zeta_{21}^{8} - \zeta_{21}^{7} + \zeta_{21}^{5} - 1.$$

Consideriamo ora $\alpha = \gamma/\overline{\gamma}$, il cui polinomio minimo è

$$\mu_\alpha(x) = x^{12} - 5x^{11} + 13x^{10} - 23x^9 + 32x^8 - 38x^7 + \frac{281}{7}x^6 - 38x^5 + 32x^4 - 23x^3 + 13x^2 - 5x + 1;$$

è possibile verificare computazionalmente che la misura di Mahler di $\alpha$ è 7, da cui, usando il Corollario 2.19, otteniamo che

$$h(\alpha) = \frac{\log 7}{12}.$$

L'elemento $\alpha$ produce il migliore esempio che conosciamo di un numero algebrico di altezza "piccola" contenuto in un'estensione abeliana di $\mathbb{Q}$.

## 3.1 Applicazioni e Corollarî

In questa sezione presentiamo le principali conseguenze e applicazioni del Teorema 3.2. Daremo prima una minorazione della norma in estensioni abeliane e successivamente mostreremo che esiste solo un numero finito di campi ciclotomici il cui anello degli interi è un dominio a ideali principali.

### 3.1.1 Minorazione della norma in un'estensione abeliana

Fissata un'estensione abeliana $L/\mathbb{Q}$, presentiamo un lemma che lega la norma di un intero algebrico $\gamma \in \mathcal{O}_L$ all'altezza logaritmica di $\overline{\gamma}/\gamma$.

**Lemma 3.13**
*Sia $L$ un'estensione abeliana di $\mathbb{Q}$ e sia $\gamma \in \mathcal{O}_L - \{0\}$. Allora*

$$\log|N_{L/\mathbb{Q}}(\gamma)| \geq [L:\mathbb{Q}]h(\overline{\gamma}/\gamma).$$

*Dimostrazione.* Sia $\gamma \in \mathcal{O}_L - \{0\}$ e definiamo $\alpha = \overline{\gamma}/\gamma$. Per ogni valore assoluto archimedeo $v$ di $L$ si ha che $|\alpha|_v = 1$, infatti associato a $v$ esiste un elemento $\sigma \in Gal(L/\mathbb{Q})$ tale che $|\alpha|_v = |\sigma(\alpha)|_\infty$, da cui

$$|\alpha|_v^2 = \sigma(\alpha)\overline{\sigma(\alpha)} = \sigma(\alpha)\sigma(\overline{\alpha}) = \sigma(|\alpha|^2) = 1,$$

in quanto, essendo $Gal(L/\mathbb{Q})$ abeliano, la coniugazione complessa commuta con $\sigma$.
Dalla definizione di altezza 2.12 e applicando la formula del prodotto 1.23 a $\gamma$, otteniamo:

$$[L:\mathbb{Q}]h(\alpha) = \sum_{\substack{v\in\mathcal{M}_L \\ v\nmid\infty}} n_v \log^+|\alpha|_v = \sum_{\substack{v\in\mathcal{M}_L \\ v\nmid\infty}} n_v \log^+|\alpha|_v + \sum_{v\in\mathcal{M}_L} n_v \log|\gamma|_v =$$

$$= \sum_{\substack{v\in\mathcal{M}_L \\ v\nmid\infty}} n_v \log\max(|\gamma|_v, |\overline{\gamma}|_v) + \sum_{\substack{v\in\mathcal{M}_L \\ v|\infty}} n_v \log|\gamma|_v \leq \sum_{\substack{v\in\mathcal{M}_L \\ v|\infty}} n_v \log|\gamma|_v$$

dove la disuguaglianza è dovuta al fatto che $\gamma$ e $\overline{\gamma}$ sono interi algebrici e quindi $|\gamma|_v \leq 1$ e $|\overline{\gamma}|_v \leq 1$ per ogni valore assoluto non archimedeo $|\cdot|_v$. Adesso, dalla definizione di norma

$$N_{L/\mathbb{Q}} = \prod_{\substack{v\in\mathcal{M}_L \\ v|\infty}} |\gamma|_v^{n_v},$$

otteniamo la disuguaglianza annunciata nella tesi

$$\log|N_{L/\mathbb{Q}}(\gamma)| \geq [L:\mathbb{Q}]h(\overline{\gamma}/\gamma).$$

□

**Corollario 3.14**
*Sia $L$ un'estensione abeliana di $\mathbb{Q}$ e sia $\gamma \in \mathcal{O}_L - \{0\}$ tale che $\overline{\gamma}/\gamma$ non è una radice dell'unità. Allora*

$$\frac{\log |N_{L/\mathbb{Q}}(\gamma)|}{[L:\mathbb{Q}]} \geq \frac{\log 5}{12}.$$

*Dimostrazione.* Basta applicare il Teorema 3.2 e il lemma precedente. □

### 3.1.2 Campi ciclotomici

Utilizzando le tecniche precedenti, dimostreremo in questa sezione che esistono solo un numero finito di campi ciclotomici il cui anello degli interi è un dominio a ideali principali.

Con le stesse notazioni usate in precedenza, presentiamo un lemma che ci servirà nel seguito.

**Lemma 3.15**
*Supponiamo che l'anello degli interi del campo ciclotomico $K_m$ sia a ideali principali. Allora per ogni primo $p \equiv 1 \mod m$, esiste un intero algebrico $\gamma \in \mathcal{O}_{K_m}$ tale che $N_{K_m/\mathbb{Q}}(\gamma) = p$ e tale che $\gamma/\overline{\gamma}$ non sia una radice dell'unità.*

*Dimostrazione.* L'ipotesi fatta su $p$ ci assicura che questo si spezza completamente in $\mathcal{O}_{K_m}$, ovvero esistono $\mathfrak{p}_1, ..., \mathfrak{p}_{\varphi(m)}$ ideali primi di $\mathcal{O}_{K_m}$ tali che

$$p\mathcal{O}_{K_m} = \prod_{i=1}^{\varphi(m)} \mathfrak{p}_i.$$

Dall'ipotesi che $\mathcal{O}_{K_m}$ sia a ideali principali discende che per ogni $i = 1, ..., \varphi(m)$ esiste $\gamma_i \in \mathcal{O}_{K_m}$ tale che $(\gamma_i) = \mathfrak{p}_i$. Segue allora che $N_{K_m/\mathbb{Q}}(\gamma_i) = N(\mathfrak{p}_i) = p$ per ogni $i = 1, ..., \varphi(m)$; inoltre, dato che $p$ spezza completamente in $\mathcal{O}_{K_m}$, per ogni $i = 1, ..., \varphi(m)$, $\mathfrak{p}_i \neq \overline{\mathfrak{p}_i}$, e quindi $\gamma_i/\overline{\gamma}_i$ non è una radice dell'unità. □

Dimostriamo adesso il risultato principale della sezione.

**Teorema 3.16**
*Esistono solo un numero finito di campi ciclotomici il cui anello degli interi è un dominio a ideali principali.*

*Dimostrazione.* Dal Teorema di Linnik 1.28, sappiamo che esiste una costante $L > 1$ tale che, per ogni intero $m \geq 2$, esiste un numero primo $p \equiv 1 \mod m$ che verifica $p < m^L$. Sia allora $m \geq 2$ un intero e supponiamo che l'anello degli interi di $K_m$ sia principale. Utilizzando il Lemma 3.15, possiamo affermare che esiste un intero algebrico $\gamma \in \mathcal{O}_{K_m}$ tale che $N_{K_m/\mathbb{Q}}(\gamma) = p < m^L$ e tale che $\gamma/\overline{\gamma}$ non è una radice dell'unità. Applicando il logaritmo ad ambo i membri e il Corollario 3.14 si ottiene

$$[K_m : \mathbb{Q}]\frac{\log 5}{12} \leq L \log m$$

e quindi possiamo affermare che esiste una costante assoluta $c_1 > 0$ tale che

$$L \log m \geq c_1 \varphi(m).$$

Dal Teorema di Mertens 1.27, esiste una costante $c_2 > 0$ indipendente da $m$ tale che

$$L \log m \geq c_1 c_2 \frac{m}{\log m}$$

o equivalentemente

$$\frac{m}{\log^2 m} \leq \frac{L}{c_1 c_2}$$

e questo è vero solo per un numero finito di $m$, in quanto

$$\lim_{m\to+\infty} \frac{m}{\log^2 m} = +\infty.$$

Questo conclude la dimostrazione. □

Le costanti $c_1, c_2$ e $L$ del precedente Teorema sono effettivamente calcolabili e da questo si può dimostrare che ci sono esattamente 29 campi ciclotomici con anello degli interi a ideali principali, che sono $K_m$ con $m$=3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84 (si veda [12] per una trattazione completa).

## 3.2 Conclusioni e Sviluppi

In questa sezione conclusiva presentiamo gli sviluppi di questioni legati alla congettura di Lehmer, successivi al lavoro analizzato in questa tesi. Riferimenti per questa sezione sono gli articoli [3] e [4].

In [3] viene proposta una versione relativa della congettura di Lehmer, dove il campo base è stato sostituito con la massima estensione abeliana di $\mathbb{Q}$.

**Congettura 3.17**
*Esiste una costante reale $c > 0$ tale che per ogni $\alpha \in \overline{\mathbb{Q}}^*$ diverso da una radice dell'unità si ha che*

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}^{ab}(\alpha) : \mathbb{Q}^{ab}]}.$$

Nello stesso articolo si è anche cercato di comprendere quale possa essere un buon candidato per il campo base nella formulazione del problema di Lehmer. Con il punto di vista sopra presentato, per qualificare un campo $K$ come un buon candidato a essere il campo base, bisogna che l'altezza di Weil sia almeno limitata inferiormente al di fuori dell'insieme delle radici dell'unità (la congettura 3.17 implica che $\mathbb{Q}^{ab}$ soddisfa questa proprietà). Introduciamo allora le seguenti nozioni, seguendo il lavoro di Bombieri e Zannier [4]:

**Definizione 3.18**
Sia $\mathcal{A} \subset \overline{\mathbb{Q}}$ un sottoinsieme di numeri algebrici.
1) Diciamo che $\mathcal{A}$ ha la proprietà (B) di Bogomolov se esiste un numero reale $T_0 = T_0(\mathcal{A}) > 0$ tale che l'insieme degli elementi di $\mathcal{A}$ con altezza più piccola di $T_0$ consiste di tutte le radici dell'unità contenute in $\mathcal{A}$
2) Diciamo che $\mathcal{A}$ ha la proprietà (N) di Northcott se per ogni numero reale $T > 0$, l'insieme degli elementi di $\mathcal{A}$ con altezza più piccola di $T$ è finito.

Sicuramente ogni campo di numeri ha sia la proprietà (B) che la proprietà (N), per questo motivo, l'unica prospettiva nella quale ha senso porsi la domanda di sopra è quella di considerare estensioni infinite di $\mathbb{Q}$.

Una prima e interessante classe di campi con la proprietà (B) è data dai campi $K$ con grado locale limitato a un certo primo di $K$.
Fissiamo un primo non archimedeo $v \in \mathcal{M}_K$ e sia $L/K$ un'estensione infinita. Diciamo che $L/K$

ha grado locale limitato al primo $v$, se esiste un intero $d_0$ tale che per ogni estensione $w$ di $v$ in $L$ abbiamo che $[L_w : K_v] \leq d_0$.
Un risultato di Bombieri e Zannier ([4], Teorema 2) afferma che ogni estensione di Galois $L/\mathbb{Q}$ con grado locale limitato a un certo primo razionale soddisfa la proprietà (B). Grazie al Teorema 3.1, un altro esempio che può essere aggiunto alla classe dei campi che rispettano la proprietà (B) è $\mathbb{Q}^{tr}$, ovvero l'insieme di tutti i numeri algebrici totalmente reali.
In secondo luogo, la chiusura abeliana $\mathbb{Q}^{ab}$ di $\mathbb{Q}$ soddisfa la proprietà (B) (si veda [1]) e questo risolve il caso $[\mathbb{Q}^{ab}(\alpha) : \mathbb{Q}^{ab}] = 1$ della congettura 3.17. Più in generale, se $K$ è un campo di numeri, allora la sua chiusura abeliana $K^{ab}$ soddisfa la proprietà (B) ([3]).
Uno degli scopi attuali della ricerca è quello di trovare una certa proprietà (Π) tale che se $G$ è un gruppo di Galois per cui la proprietà (Π) è vera, allora ogni estensione di Galois $L/\mathbb{Q}$ con gruppo di Galois $G$ soddisfa la proprietà di Bogomolov. Purtroppo, al momento non si è ancora trovata una proprietà con queste caratteristiche.

Concludiamo la sezione con una serie di problemi concernenti la proprietà (B), enunciati in [3].

**Problema 3.19**
*Sia $K/\mathbb{Q}$ un'estensione con grado locale limitato a un certo primo razionale. È vero che $K^{ab}$ ha la proprietà (B)?*

**Problema 3.20**
*Siano $N$ un gruppo abeliano e $H$ un gruppo di esponente finito. Supponiamo che $G$ sia un'estensione di $H$ mediante $N$, cioè esiste una successione esatta corta*

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1.$$

*È vero che se $K$ è un campo di numeri e $L/K$ è un'estensione normale con gruppo di Galois $G$, allora $L$ ha la proprietà (B)?*

Concentrandosi poi sulla stabilità della proprietà (B) in estensioni finite, sorge naturale il seguente quesito.

**Problema 3.21**
*Sia $L$ un campo con la proprietà (B)/(N) e sia $F/L$ un'estensione finita. È vero che $F$ ha necessariamente la proprietà (B)/(N)?*

A questa domanda è stata data una risposta completa. Nel caso della proprietà (B) la risposta è negativa, mentre si può dimostrare che se $L/\mathbb{Q}$ soddisfa la proprietà (N), allora ogni estensione finita $F/L$ soddisfa la proprietà (N): questo mostra che le due proprietà si comportano in modi molto diversi in estensioni finite (si veda [3] per una trattazione completa dell'argomento).

# Bibliografia


[1] Francesco Amoroso and Roberto Dvornicich. A lower bound for the height in abelian extensions. *J. Number Theory*, 80(2):260–272, 2000.

[2] Francesco Amoroso and Damien Vergnaud. *Minorations de la hauteur d'un nombre algébrique*. Plus - Università di Pisa, 2004.

[3] Francesco Amoroso and Umberto Zannier. On fields with property (B). *Proc. Amer. Math. Soc.*, 142(6):1893–1910, 2014.

[4] Enrico Bombieri and Umberto Zannier. A note on heights in certain infinite extensions of $\mathbb{Q}$. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, 12:5–14, 2001.

[5] Siegfried Bosch. *Algebra—from the viewpoint of Galois theory*. Birkhäuser Advanced Texts: Basler Lehrbücher. [Birkhäuser Advanced Texts: Basel Textbooks]. Birkhäuser/Springer, Cham, german edition, 2018.

[6] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*. London Mathematical Society, London, 2010. Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965, Including a list of errata.

[7] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[8] U. V. Linnik. On the least prime in an arithmetic progression. I. The basic theorem. *Rec. Math. [Mat. Sbornik] N.S.*, 15/57:139–178, 1944.

[9] Daniel A. Marcus. *Number fields*. Universitext. Springer, Cham, second edition, 2018. With a foreword by Barry Mazur.

[10] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[11] A. Schinzel. On the product of the conjugates outside the unit circle of an algebraic number. *Acta Arith.*, 24:385–399, 1973.

[12] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

# Ringraziamenti

Ringraziare è un verbo particolare, significa essere grati a qualcuno per qualcosa che ha fatto. Per questo motivo, non penso che questa pagina meriti di essere riempita asetticamente di nomi, uno dietro l'altro, come una fila di piccole formiche nere: non sarebbe in linea col significato del termine. D'altra parte, cercare di dare una spiegazione, seppur minima, a ogni cosa e a ogni persona che voglio ringraziare per i motivi più variegati implicherebbe terminare la stesura di queste pagine in un tempo e in uno spazio infiniti. Quindi, tenterò di essere conciso, anche se non mi è mai venuto troppo bene.

Per primo, ringrazio quel pezzo di me che meno di due anni fa mi ha inaspettatamente salutato per l'ultima volta, per ogni cosa che ha significato nella mia vita e per ogni granello di amore incondizionato che ha saputo darmi.

Ringrazio la mia famiglia: mia mamma, mio babbo e Giulia, per ogni cosa che ogni giorno, ininterrottamente, fate per rendere tutto migliore. Non penso di dirvi mai a parole che vi voglio bene, anche se spero di mostrarvelo in ogni cosa che faccio.

Ringrazio mio zio, perché è sempre stato un grande amico, ancor prima di un parente.

Ringrazio Lucre, perché la tua presenza è indispensabile nella mia vita di tutti i giorni.

Ringrazio Linda, perché il tuo emanare gioia è una medicina per chiunque ti stia intorno, per me soprattutto.

Ringrazio Kira, perché oltre alla calma che trasmetti con la tua sola presenza, mi hai fatto crescere più di quanto immagini su tantissimi aspetti.

Ringrazio Lia, perché quando siamo insieme, anche se non sempre, riesci a rendere tutto più leggero.

Ringrazio Ele, perché il tuo amore smisurato per la nostra città è una delle cose più belle che condividiamo.

Ringrazio Fabio, per averci dato la sicurezza di un luogo sempre confortevole e accogliente.

Ringrazio Cecilia, per aver reso la biblioteca un posto che sa meno di serio e più di scherzoso.

Ringrazio Chiara, per questi lunghissimi anni insieme e per i viaggi insieme.

Ringrazio Slavik, perché abbiamo aperto tanti orizzonti, non solo cosmologici.

Ringrazio Mati, perché il tuo emozionarti facilmente con le piccole cose che vedi ti rende incredibilmente fanciulla.

Ringrazio Rache, per tutti gli splendidi pomeriggi passati insieme.

Ringrazio Vio e Ari, perché nonostante la scuola sia finita, il nostro rapporto è rimasto quello che era.

Ringrazio Nora, per tutto ciò che hai significato in quest'anno insieme.

Ringrazio Irma ed Eva, perché senza dubbio sarete il più bel ricordo di questi anni di università quando saremo lontani.

Ringrazio i miei compagni del terzo anno: Ale, Andre, Carlo, Davide, Diego, Gabriel, Giulia, Leo, Lisa, Matte, Matti, Pietro, Tommy, Vale per aver creato memorie e rapporti, non solo incentrati sulla matematica.

Ringrazio i ragazzi del primo anno, per aver riempito l'aula 2 di un'allegria smisurata.

Ringrazio i ragazzi più grandi del dipartimento: Ale, Andre, Chiara, Fau, France, Matti, Sofi per aver rappresentato dei fratelli maggiori in questo bellissimo percorso.

Ringrazio Brunella, Daniele e Niccolò, perché ormai siete una seconda famiglia.

Ringrazio Gino e Artin, perché i gatti sanno darti un affetto indescrivibile.

Ringrazio la copisteria Sprint, perché senza il vostro servizio impeccabile, non avrei avuto pagine su cui studiare.

Ringrazio il Dipartimento, perché è riuscito a essere una seconda casa per tutti noi.

Ringrazio la Matematica, per aver reso migliore ogni parte delle mie giornate e per avermi fatto incredibilmente innamorare del mondo meraviglioso che questa rappresenta.

Ringrazio la musica, perché ovunque la vita mi porterà, il violino sarà sempre al mio fianco.

Ringrazio la letteratura, in particolare Leopardi, perché è e rimarrà sempre una parte profonda e fondamentale dei miei studi e della mia formazione.

Ringrazio il mare, perché sono nato sulla costa e non riesco a stare senza il salmastro addosso.

Infine, ringrazio Ilaria del Corso, non solo come relatrice, ma anche e soprattutto per ciò che è riuscita a trasmettermi: grazie per avermi fatto amare l'algebra, è stato il dono più bello che potesse farmi.