Università degli Studi di Pisa
Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea in Matematica

Tesi di Laurea
29 settembre 2004

# Equazioni nell'anello di Hadamard


Candidato
**Andrea Ferretti**
a.ferretti@sns.it

Relatore
**Prof. Umberto Zannier**
Università IUAV, Venezia

Controrelatore
**Prof. Roberto Dvornicich**
Università di Pisa


Anno Accademico 2003/2004

# Introduzione

Le ricorrenze lineari sono state oggetto di studio in aritmetica per lungo tempo, dopo la definizione della famosa successione di Fibonacci

$$\begin{cases} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n. \end{cases}$$

La scrittura esplicita della soluzione di una generica ricorrenza lineare

$$c_0 x_{k+m} + \cdots + c_m x_k$$

su un campo qualsiasi è nota, e si determina facilmente con metodi algebra lineare. Ciò nonostante siamo ben lontani dal conoscere le proprietà più profonde legate a questi oggetti.

Un primo esempio di proprietà non banale delle ricorrenze lineari è la distribuzione degli zeri. A questo proposito abbiamo il teorema di Lech-Mahler-Skolem (valido in caratteristica 0), che afferma che se $(x_k)$ soddisfa un'equazione per ricorrenza l'insieme dei $k$ per cui $x_k = 0$ è unione di un insieme finito e di un numero finito i progressioni aritmetiche. Per quanto semplice, la dimostrazione di questo risultato richiede, come altri risultati in questo campo, tecniche di analisi $p$-adica.

Le altre proprietà di cui ci siamo interessati in questa tesi sono legate al cosiddetto anello di Hadamard di un campo $K$. L'osservazione fondamentale è che la somma e il prodotto di due successioni ricorrenti soddisfano ancora una ricorrenza lineare. Questo fatto si vede facilmente utilizzando la scrittura esplicita della soluzione di una ricorrenza lineare nella forma

$$x_k = \sum_{i=1}^{m} A_i(k)\alpha_i^k$$

per opportuni polinomi $A_i$ ed elementi $\alpha_i \in K$. Questo porta ad una struttura di anello sull'insieme delle successioni a coefficienti in $K$ che verificano definitivamente una ricorrenza lineare, l'anello di Hadamard di $K$.

Il problema affrontato è quello di determinare la risolubilità di equazioni nell'anello di Hadamard $\mathcal{H}(K)$, quando $K$ sia un campo di numeri, o più in generale un'estensione finitamente generata di $\mathbb{Q}$. Dapprima è necessario trovare una soluzione "formale" nell'anello di tutte le successioni di elementi di $K$: questo potrebbe essere già un ostacolo, a causa del fatto che $K$ è molto lontano dall'essere algebricamente chiuso. La filosofia è la seguente: garantire la risolubilità "formale" in $K$ è una condizione abbastanza forte, dunque basta molto poco (o niente) per avere il risultato più forte che esiste una soluzione in $\mathcal{H}(K)$.

Un primo risultato di questo tipo, nel caso di equazioni lineari, è stato ottenuto da Van der Poorten in [vdP88], dopo una dimostrazione non del tutto completa da parte di Pourchet in [Pou79]. Poiché le equazioni lineari hanno sempre soluzione nel campo, l'esistenza di una soluzione formale non basta a garantire una soluzione "vera". Il risultato richiede dunque un'ipotesi aggiuntiva: se $(c_k)$ e $(b_k)$ sono elementi di $\mathcal{H}(K)$ e abbiamo una successione $a_k$ *contenuta in un anello finitamente generato* che verifica $a_k b_k = c_k$, allora a sua volta $(a_k) \in \mathcal{H}(K)$.

Grazie al risultato di Van der Poorten è naturale ridursi, nello studio di equazioni di grado più alto, al caso monico. In questo ambito il primo risultato è dovuto a Zannier ([Zan00]): data una successione $(c_k) \in \mathcal{H}(K)$, se esiste una successione in $K$ che sia una radice $d$-esima, allora esiste una radice $d$-esima in $\mathcal{H}(K)$.

In questa tesi abbiamo cercato di ottenere un risultato analogo per la risolubilità in $\mathcal{H}(K)$ di un'equazione della forma

$$g(c_k, Y) = 0,$$

per un generico polinomio $g \in K[X, Y]$ monico in $Y$. Non siamo arrivati a dimostrare questo in generale, ma solo se il polinomio $g$ ha grado al più 3. Tuttavia la dimostrazione che proponiamo è un adattamento di [Zan00] che crediamo possa essere utilizzata con poche modifiche nel caso generale, e le restrizioni sulla natura di $g$ sono poste ad hoc per superare alcune difficoltà nella parte finale. Dopo aver concluso la dimostrazione nel caso particolare mostriamo una strada per superare queste difficoltà in generale, sotto forma di sketch, riproponendoci di fornire una dimostrazione completa in un prossimo lavoro.

L'organizzazione degli argomenti è la seguente. Nel primo capitolo sono rivisti i principali strumenti di teoria dei numeri utilizzati nel seguito. Dove possibile abbiamo cercato di dare le dimostrazioni dei fatti enunciati, anche se in una forma molto stringata, rimandando ad opportune fonti per esposizioni più complete. Nel secondo capitolo rivediamo invece le proprietà classiche delle successioni ricorrenti, incluso il teorema di Lech-Mahler-Skolem. Di queste proprietà faremo ampio uso nei capitoli successivi. I capitoli seguenti sono invece largamente indipendenti fra loro. Nel terzo esponiamo una dimostrazione del teorema del quoziente di Van der Poorten, facendo nuovamente uso di tecniche di analisi $p$-adica. Il quarto contiene il risultato originale della tesi, che è il Teorema 4.1.1. Come abbiamo detto questa è un'estensione del risultato di Zannier; le tecniche in questo capitolo sono più algebriche: si usano soprattutto l'aritmetica classica nei campi di numeri, le varietà su campi finiti e la teoria di Kummer. Infine il quinto capitolo mostra come usare tecniche di specializzazione per estendere i risultati aritmetici dei capitoli precedenti a campi più generali.

Ringrazio Umberto Zannier e Roberto Dvornicich per la disponibilità che hanno mostrato nei miei confronti e il tempo che mia hanno dedicato. La mia gratitudine va anche a Massimo Gobbino e a Paolo Tilli, senza i consigli dei quali non avrei intrapreso lo studio della matematica. Ringrazio di cuore la mia famiglia e tutti i miei amici, pisani e lucchesi, che non desidero ridurre ad un elenco. Infine un grazie a Maria Antonietta per il bel tempo passato insieme e per il continuo incoraggiamento.

# Indice

# Capitolo 1

# Alcuni strumenti di aritmetica

“Would you tell me, please, which way I ought to go from here?” “That depends a good deal on where you want to get to” said the Cat. “I don’t much care where” said Alice. “Then it doesn’t matter which way you go.” said the Cat.

*Lewis Carroll*
Alice adventures in Wonderland

## 1.1 Richiami sui campi di numeri

In questa sezione introduciamo brevemente gli anelli degli interi su campi di numeri e descriviamo, senza dimostrazioni, la loro struttura. Per maggiori dettagli vedano, ad esempio, [Mil98] o [Mar77].

**Definizione 1.1.1** *Un campo di numeri $k$ è un’estensione finita di $\mathbb{Q}$.*

Per fare aritmetica in un campo di numeri è necessario trovare un anello di cui $k$ sia il campo dei quozienti con buone proprietà di fattorizzazione.

**Definizione 1.1.2** *Siano $A \subset B$ due anelli. Diciamo che $x \in B$ è intero su $A$ se esiste un polinomio monico $f \in A[x]$ per cui $f(x) = 0$.*

Il prossimo è un risultato classico di algebra commutativa.

**Proposizione 1.1.1** *L’insieme degli elementi di $B$ interi su $A$ è chiuso per somma e prodotto, ed è dunque un sottoanello di $B$, che chiameremo chiusura integrale di $A$ in $B$. Diciamo che $A$ è integralmente chiuso in $B$ se coincide con la propria chiusura integrale.*

Il caso che ci interessa è $A = \mathbb{Z}$, $B = k$ campo di numeri. In questo caso la chiusura integrale $\mathcal{R}$ di $\mathbb{Z}$ in $k$ è detta l'anello degli interi di $k$. Sulla struttura di $\mathcal{R}$ si riesce a dire molto. Innanzitutto come gruppo additivo $\mathcal{R} \cong \mathbb{Z}^n$, dove $n = [k : \mathbb{Q}]$, e $k$ è il campo dei quozienti di $\mathcal{R}$.

**Esempio**
Prendiamo $k = \mathbb{Q}(\zeta_m)$. In questo caso si può dimostrare che $\mathcal{R} = \mathbb{Z}[\zeta_m]$, cioè una base di $\mathcal{R}$ su $\mathbb{Z}$ è data dalle potenze $1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}$. In generale, però, dato un campo di numeri $k$ e l'anello degli interi $\mathcal{R}$, non è detto che esista $\alpha \in \mathcal{R}$ per cui $\mathcal{R} = \mathbb{Z}[\alpha]$.

In generale $\mathcal{R}$ non è un anello a fattorizzazione unica, ma ciò è compensato da un altra proprietà.

**Definizione 1.1.3** *Sia $A$ un dominio d'integrità. Diciamo che $A$ è un dominio di Dedekind se verifica le seguenti proprietà*

*i) $A$ è noetheriano;*

*ii) ogni ideale primo di $A$ è massimale;*

*iii) $A$ è integralmente chiuso nel proprio campo dei quozienti.*

**Proposizione 1.1.2** *Sia $A$ un dominio di Dedekind, $K$ il suo campo dei quozienti. Sia $L$ un'estensione finita e separabile di $K$ e $B$ la chiusura integrale di $A$ in $L$. Allora $B$ è a sua volta di Dedekind.*

In particolare, visto che $\mathbb{Z}$ è banalmente un dominio di Dedekind, otteniamo che tutti gli anelli degli interi sono domini di Dedekind. Il vantaggio di questo fatto è la seguente proprietà di fattorizzazione.

**Teorema 1.1.3 (fattorizzazione unica per ideali)** *Sia $A$ un dominio di Dedekind. Allora ogni ideale $I$ di $A$ si scrive come prodotto di ideali primi*

$$I = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r},$$

*in modo unico a meno dell'ordine.*

Possiamo anche studiare cosa succede in un'estensione. Siano dunque $A$, $B$, $K$ ed $L$ come nella Proposizione 1.1.2. Se $I$ è un ideale primo di $A$ siamo interessati a capire come è fatto l'ideale esteso $I \cdot B$. Per il teorema di fattorizzazione unica ci possiamo limitare al caso $I = \mathcal{P}$ primo. In generale $\mathcal{P} \cdot B$ non sarà un ideale primo, ed avrà perciò una fattorizzazione

$$\mathcal{P} \cdot B = \mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_r^{e_r}.$$

Chiamiamo $e_i = e(\mathcal{Q}_i|\mathcal{P})$ l'indice di ramificazione di $\mathcal{Q}_i$ su $\mathcal{P}$. $\mathcal{P}$ si dice ramificato in $L$ se esiste almeno un $e_i > 1$. Gli ideali $\mathcal{Q}_i$ sono caratterizzati dalla seguente

**Proposizione 1.1.4** *Sia $\mathcal{Q}$ un ideale primo di $B$. Le seguenti condizioni sono equivalenti*

*i) Esiste un $i$ per cui $\mathcal{Q} = \mathcal{Q}_i$;*

*ii) $\mathcal{Q} \cap A = \mathcal{P}$;*

*iii)* $\mathcal{P} \subset \mathcal{Q}$.

*In questo caso diremo che $\mathcal{Q}$ divide $\mathcal{P}$, o che è sopra $\mathcal{P}$.*

Se $\mathcal{Q}$ è un primo sopra $\mathcal{P}$ abbiamo l'omomorfismo

$$A \overset{\iota}{\hookrightarrow} B \xrightarrow{\pi} B/\mathcal{Q}.$$

Poiché $\ker \pi \circ \iota = \mathcal{P}$, questo dà luogo all'estensione di campi $A/\mathcal{P} \hookrightarrow B/\mathcal{Q}$. Non è difficile dimostrare che questa è in realtà un'estensione finita.

**Definizione 1.1.4** *Il grado d'inerzia di $\mathcal{Q}$ su $\mathcal{P}$ è dato da*

$$f(\mathcal{Q}|\mathcal{P}) = [B/\mathcal{Q} : A/\mathcal{P}].$$

**Proposizione 1.1.5** *Grado d'inerzia e indice di ramificazione sono moltiplicativi, nel seguente senso. Sia $A$ un dominio di Dedekind con campo dei quozienti $K$. Siano $K \subset L \subset M$ estensioni finite separabili e $B$, $C$ le chiusure integrali di $A$ in $L$ e $M$ rispettivamente. Sia $\mathcal{Q}$ un primo di $B$ sopra $\mathcal{P}$ e $\mathcal{Q}'$ un primo di $C$ sopra $\mathcal{Q}$. Allora*

$$e(\mathcal{Q}'|\mathcal{P}) = e(\mathcal{Q}'|\mathcal{Q})e(\mathcal{Q}|\mathcal{P})$$
$$f(\mathcal{Q}'|\mathcal{P}) = f(\mathcal{Q}'|\mathcal{Q})f(\mathcal{Q}|\mathcal{P}).$$

Nel caso di un campo di numeri $k$ si dimostra che i campi residui $\mathcal{R}/I$ sono tutti campi finiti. In particolare per $I = \mathcal{P}$ primo sopra $p$ si ha

$$\mathcal{R}/\mathcal{P} \cong \mathbb{F}_q,$$

dove $q = p^{f(\mathcal{P}|p)}$.

**Definizione 1.1.5** *La norma dell'ideale $I$ è data da $N(I) = \#(\mathcal{R}/I)$.*

**Proposizione 1.1.6** *La norma è moltiplicativa, ovvero $N(IJ) = N(I)N(J)$.*

Il risultato fondamentale per le estensioni di domini di Dedekind è il seguente.

**Teorema 1.1.7 (Formula dimensionale)** *Con le notazioni precedenti, poniamo $n = [L : K]$ e $f_i = f(\mathcal{Q}_i|\mathcal{P})$. Allora*

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

Diremo che $\mathcal{P}$ si spezza totalmente in $B$ se $e_i = f_i = 1$ per ogni $i$, cioè $r = n$.

**Esempio**
Sia $k = \mathbb{Q}(\zeta_m)$ con anello degli interi $\mathbb{Z}[\zeta_m]$. Se $p \in \mathbb{Z}$ è un primo dispari, siamo interessati a vedere come si fattorizza $p\mathbb{Z}[\zeta_m]$. Si dimostra che $p$ è ramificato se e solo se divide $m$. Altrimenti la fattorizzazione è della forma

$$p\mathbb{Z}[\zeta_m] = \mathcal{P}_1 \cdots \mathcal{P}_r$$

dove $f = f(\mathcal{P}_i|p)$ è indipendente da $i$ (vedi la prossima sezione) ed è pari all'ordine di $p$ nel gruppo moltiplicativo $(\mathbb{Z}/m\mathbb{Z})^*$. In particolare $p$ si spezza completamente se e solo se $p \equiv 1 \pmod{m}$.

## 1.2 L'azione di Galois sui primi

Anche per questa sezione i riferimenti sono [Mil98] e [Mar77].

Siano $K \subset L$ campi di numeri, con anelli degli interi $\mathcal{R}$ ed $\mathcal{S}$, e supponiamo che $L/K$ sia normale. In questo caso l'azione di $G = G_{L,K}$ conserva gli elementi interi, e si restringe dunque ad un'azione su $\mathcal{S}$ che lascia fisso $\mathcal{R}$. Fissiamo un primo $\mathcal{P}$ di $\mathcal{R}$, e siano $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$ i primi di $\mathcal{S}$ sopra di lui. È evidente che $G$ agisce permutando $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_r\}$, e in effetti non è difficile vedere che

**Proposizione 1.2.1** *L'azione di $G$ su $\{\mathcal{Q}_1, \ldots, \mathcal{Q}_r\}$ è transitiva.*

**Dim.** Supponiamo che non esista $\sigma \in G$ con $\sigma(\mathcal{Q}_i) = \mathcal{Q}_j$. Per il teorema cinese del resto possiamo prendere $x \in \mathcal{S}$ con

$$x \equiv 0 \pmod{\mathcal{Q}_j}, \qquad x \equiv 1 \pmod{\sigma(\mathcal{Q}_i)} \quad \forall \sigma \in G.$$

Sia $y = N_{L/K}(x) \in K$. Poiché nessun fattore di $y$ appartiene a $\mathcal{Q}_i$, che è primo, $y \notin \mathcal{Q}_i$. Allo stesso tempo uno dei fattori è $x \in \mathcal{Q}_j$, dunque $y \in \mathcal{Q}_j \cap K = \mathcal{P}$, assurdo.

□

Da questo fatto segue facilmente che gli indici di ramificazione e i gradi d'inerzia dei vari primi sopra $\mathcal{P}$ coincidono. La fattorizzazione di $\mathcal{P}$ sarà allora

$$\mathcal{P}\mathcal{S} = (\mathcal{Q}_1 \cdots \mathcal{Q}_r)^e$$

e, se indichiamo con $f = f(\mathcal{Q}_i|P)$ il grado d'inerzia comune, la formula dimensionale ci dice che $[L : K] = ref$.

Indichiamo lo stabilizzatore di un primo $\mathcal{Q} = \mathcal{Q}_i$ come $D(\mathcal{Q}|\mathcal{P}) = \{\sigma \in G : \sigma(\mathcal{Q}) = \mathcal{Q}\}$. Se $\sigma \in D(\mathcal{Q}|\mathcal{P})$ l'azione di $\sigma$ su $\mathcal{S}$ passa al quoziente $\bmod \mathcal{Q}_i$, e pertanto otteniamo un omomorfismo

$$D(\mathcal{Q}|\mathcal{P}) \longmapsto G_{\mathcal{S}/\mathcal{Q}, \mathcal{R}/\mathcal{P}} = G_{\mathbb{F}_{q'}, \mathbb{F}_q},$$

dove $q' = q^f$ e $(q) = \mathcal{P} \cap \mathbb{Z}$.

**Definizione 1.2.1** *Definiamo gruppo di inerzia il nucleo*

$$E(\mathcal{Q}|\mathcal{P}) = \{\sigma \in G : \sigma(x) \equiv x \pmod{\mathcal{Q}} \, \forall x \in \mathcal{S}\}.$$

Dalle definizioni è chiaro che $E(\mathcal{Q}|\mathcal{P}) \lhd D(\mathcal{Q}|\mathcal{P})$. In generale $D(\mathcal{Q}|\mathcal{P}) \ntriangleleft G$, e se scegliamo $\sigma \in G$ con $\sigma(\mathcal{Q}_i) = \mathcal{Q}_j$ allora

$$D(\mathcal{Q}_j|\mathcal{P}) = \sigma D(\mathcal{Q}_i|\mathcal{P}) \sigma^{-1}.$$

In particolare se $L/K$ è abeliana il gruppo $D(\mathcal{Q}_i|\mathcal{P}) = D(\mathcal{P})$ dipende solo da $\mathcal{P}$ e non dal primo sopra di esso. Osserviamo che $|D(\mathcal{Q}_i|\mathcal{P})| = \frac{|G|}{r} = ef$. Poiché abbiamo un omomorfismo iniettivo

$$\frac{D(\mathcal{Q}|\mathcal{P})}{E(\mathcal{Q}|\mathcal{P})} \longmapsto G_{\mathbb{F}_{q'}, \mathbb{F}_q} \tag{1.2.1}$$

segue che $[D : E] \leq f$. In realtà si riesce a dire molto di più. La corrispondenza di Galois ci permette di associare a $D$, $E$, dei sottocampi $L_D$, $L_E$. Indichiamo con $\mathcal{S}_D$, $\mathcal{S}_E$ i rispettivi anelli degli interi, e con $\mathcal{Q}_D = \mathcal{Q} \cap L_D$, $\mathcal{Q}_E = \mathcal{Q} \cap L_E$. Poiché $L/L_D$ e $L/L_E$ sono estensioni di Galois, si applicano le stesse considerazioni che abbiamo visto per $L/K$. Mostriamo che

**Proposizione 1.2.2** $f(\mathcal{Q}|\mathcal{Q}_E) = 1$

**Dim.** Sia $\overline{\alpha} \in \mathcal{S}/\mathcal{Q}$ e consideriamo

$$g(x) = \prod_{\sigma \in E} (x - \sigma(\alpha)).$$

Chiaramente $g(x) \in \mathcal{S}_E[x]$, e dunque otteniamo $\overline{g}(x) \in \mathcal{S}_E/\mathcal{Q}_E[x]$. D'altra parte è chiaro che $\overline{g}(x) = (x - \overline{\alpha})^{|E|}$, mentre il polinomio minimo $\mu_{\overline{\alpha}}$ di $\overline{\alpha}$ su $\mathcal{S}_E/\mathcal{Q}_E$ è separabile, dunque $\mu_{\overline{\alpha}}(x) = x - \overline{\alpha}$ e $\overline{\alpha} \in \mathcal{S}_E/\mathcal{Q}_E$. Perciò $\mathcal{S}_E/\mathcal{Q}_E = \mathcal{S}/\mathcal{Q}$.

□

Da questo fatto si riescono a determinare tutte le altre informazioni, utilizzando la formula dimensionale e il fatto che $e$, $f$ ed il grado sono moltiplicativi nelle torri di estensioni. Ad esempio poiché $f(\mathcal{Q}|\mathcal{Q}_D) = f$ si trova che $[L_E : L_D] = [D : E] \geq f$. Visto che avevamo già l'altra disuguaglianza otteniamo $[D : E] = f$, e di nuovo per la formula dimensionale $e(\mathcal{Q}_E|\mathcal{Q}_D) = 1$, in modo che $\mathcal{Q}_D\mathcal{S}_E = \mathcal{Q}_E$. Possiamo riassumere tutto questo in un diagramma delle varie estensioni, dove rappresentiamo i campi, i corrispettivi sottogruppi di $G$ e anelli degli interi, i primi sotto $\mathcal{Q}$, i valori

$$\begin{array}{rcccl}
\{\mathrm{id}\} & L & \mathcal{S} & \mathcal{Q} & \\
e\Big| & \Big| & \Big| & \Big| & r = f = 1 \\
E & L_E & \mathcal{S}_E & \mathcal{Q}_E & \\
f\Big| & \Big| & \Big| & \Big| & r = e = 1 \\
D & L_D & \mathcal{S}_D & \mathcal{Q}_D & \\
r\Big| & \Big| & \Big| & \Big| & e = f = 1 \\
G & K & \mathcal{R} & \mathcal{P} &
\end{array}$$

di $e$, $f$ e il numero di primi.

Una semplice conseguenza di queste relazioni è la seguente

**Proposizione 1.2.3** *Nelle notazioni precedenti sia $F$ un campo intermedio tra $K$ e $L$, e poniamo $\mathcal{Q}_F = \mathcal{Q} \cap F$. Allora $e(\mathcal{Q}_F|\mathcal{P}) = f(\mathcal{Q}_F|\mathcal{P}) = 1$ se e solo se $F \subset L_D$. In particolare se $D \lhd G$ allora $L_D$ è il massimo campo in cui $\mathcal{P}$ si spezza completamente.*

**Corollario 1.2.4** *Siano $L, L'$ estensioni di $K$, $\mathcal{P}$ un primo di $K$. Allora $\mathcal{P}$ si spezza completamente in $LL'$ se e solo se si spezza completamente in $L$ e in $L'$.*

Dal diagramma deduciamo anche che $\mathcal{P}$ è non ramificato se e solo se $E(\mathcal{Q}|\mathcal{P}) = \{\mathrm{id}\}$ per ogni primo $\mathcal{Q}$ sopra $\mathcal{P}$. D'altra parte abbiamo il

**Teorema 1.2.5** *$\mathcal{P}$ è ramificato in $\mathcal{S}$ se e solo se $\mathcal{P} | \operatorname{disc}_{\mathcal{S}/\mathcal{R}}$.*

Pertanto solo per un numero finito di primi $E(\mathcal{Q}|\mathcal{P}) \neq \{\mathrm{id}\}$. Dal diagramma otteniamo anche che l'omomorfismo (1.2.1) è in realtà un isomorfismo. Sappiamo però che $G_{\mathbb{F}_{q'}, \mathbb{F}_q}$ è ciclico, generato dall'omomorfismo di Frobenius.

**Definizione 1.2.2** *L'elemento di Frobenius $\phi(\mathcal{Q}|\mathcal{P}) \in D/E$ è l'elemento che corrisponde all'omomorfismo di Frobenius tramite (1.2.1).*

Quando $E$ si riduce all'identità $\phi(\mathcal{Q}|\mathcal{P}) \in D < G$, cioè possiamo far agire il Frobenius su $\mathcal{S}$. In questo caso il Frobenius è determinato dalla condizione

$$\phi(\mathcal{Q}|\mathcal{P})(x) \equiv x^q \pmod{\mathcal{Q}} \quad \forall x \in \mathcal{S}.$$

Di nuovo è immediato verificare che se $\sigma(\mathcal{Q}_i) = \mathcal{Q}_j$ allora

$$\phi(\mathcal{Q}_j|\mathcal{P}) = \sigma\phi(\mathcal{Q}_i|\mathcal{P})\sigma^{-1}.$$

Di conseguenza se l'estensione è abeliana ogni primo $\mathcal{P}$ non ramificato individua un elemento di Frobenius $\phi(\mathcal{P}) \in G$. Nel caso generale, a $\mathcal{P}$ possiamo associare una classe di coniugio di $G$, composta dagli elementi $\phi(\mathcal{Q}|\mathcal{P})$ al variare di $\mathcal{Q}$ sopra $\mathcal{P}$. Indichiamo anche questa classe con $\phi(\mathcal{P})$.

In molte situazioni è importante trovare primi con Frobenius assegnato. A questo risponde il prossimo teorema. Introduciamo innanzitutto una definizione.

**Definizione 1.2.3** *Sia $X$ un insieme di primi di $\mathcal{R}$. La densità naturale di $X$ (quando esiste) è definita come*

$$\lim_{t\to+\infty} \frac{|\{\mathcal{P} \in X : N(\mathcal{P}) \leq t\}|}{|\{\mathcal{P} : N(\mathcal{P}) \leq t\}|},$$

*dove $N(\mathcal{P})$ indica la norma del primo $\mathcal{P}$.*

**Teorema 1.2.6 (Чеботарев[1])** *Sia $L/K$ un'estensione normale di campi di numeri con gruppo di Galois $G$. Siano $\{C_1, \ldots, C_k\}$ le classi di coniugio di $G$. Allora l'insieme*

$$P_j = \{\mathcal{P} \text{ primi non ramificati di } \mathcal{R} : \phi(\mathcal{P}) = C_j\}$$

*ha densità naturale $\frac{|C_j|}{G}$.*

Per una dimostrazione di questo si veda [Mil97, pag. 216].

**Esempio**
Il teorema di Чеботарев contiene come caso particolare quello di Dirichlet sui primi nelle progressioni aritmetiche. Consideriamo l'estensione $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Un primo $p$ è ramificato se e solo se divide $m$ (segue dal teorema (1.2.5)). Il gruppo di Galois è isomorfo a $(\mathbb{Z}/m\mathbb{Z})^*$, dove $\sigma$ corrisponde a $k$ se e solo se $\sigma(\zeta_m) = \zeta_m^k$. Poiché

$$\phi(p)(\zeta_m) \equiv \zeta_m^p \pmod{p\,\mathbb{Z}[\zeta_m]}$$

otteniamo che il Frobenius di $p$ è mandato nella classe di $p \bmod m$. Pertanto il teorema di Чеботарев ci dice che la densità naturale dell'insieme

$$P_k = \{p : p \equiv k \pmod{m}\}$$

è $1/\phi(m)$.

Talvolta può essere utile il seguente risultato analitico, utilizzato insieme al Teorema di Чеботарев.

**Teorema 1.2.7** *Sia $K$ un campo di numeri ed $\mathcal{R}$ il suo anello degli interi. Allora l'insieme dei primi $\mathcal{P}$ di $\mathcal{R}$ tali che $f(\mathcal{P}|p) > 1$, dove $(p) = \mathcal{P} \cap \mathbb{Z}$, ha densità naturale 0.*

[1] trasl. Chebotarev

## 1.3 Teoria di Kummer

Visto che ci tornerà utile in seguito, richiamiamo brevemente la teoria di Kummer. Il riferimento per questa sezione, e più in generale per la teoria di Galois, è [Lan02]. La teoria di Kummer mette in relazione le estensioni abeliane di un campo $K$ di esponente finito con certi sottogruppi di $K^*$, purché $K$ contenga abbastanza radici dell'unità. *Per semplicità in tutta la sezione lavoreremo con campi di caratteristica* 0. Iniziamo dal caso delle estensioni cicliche.

**Proposizione 1.3.1** *Supponiamo che $\zeta_n \in K$.*

*i) Se $L/K$ è ciclica di grado $n$ allora $\exists \alpha \in L$ per cui $L = K(\alpha)$ e il polinomio minimo di $\alpha$ è $\mu_\alpha(x) = x^n - c \in K[x]$.*

*ii) Sia $L = K(\alpha)$, dove $\alpha$ è radice di $f(x) = x^n - c \in K[x]$. Allora esiste $d|n$ e $b \in K$ per cui $\mu_\alpha(x) = x^d - b$; inoltre $L/K$ è ciclica.*

**Dim.**

i) Sia $\sigma$ un generatore di $G_{L,K}$. Poiché $N_{L/K}(\zeta_n) = 1$ per il teorema 90 di Hilbert esiste $\alpha \in L$ con $\frac{\sigma(\alpha)}{\alpha} = \zeta_n$. Dunque i coniugati di $\alpha$ sono $\alpha, \zeta_n\alpha, \ldots, \zeta_n^{n-1}\alpha$. In particolare $[K(\alpha) : K] = n$ e dunque $L = K(\alpha)$. Inoltre

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta_n\alpha)^n = \alpha^n,$$

per cui $c = \alpha^n \in K$ e si conclude.

ii) $L/K$ è normale in quanto $L$ è il campo di spezzamento di $f$. Sia

$$\phi : G_{L,K} \longmapsto U_n = \langle \zeta_n \rangle.$$

È immediato vedere che $\phi$ è un omomorfismo iniettivo, dunque $G_{L,K}$ è ciclico di grado $d|n$. Se $\sigma$ è un generatore, come sopra si verifica che $\sigma(\alpha^d) = \alpha^d$. Dunque $b = \alpha^d \in K$, da cui le tesi.

□

Continuiamo a supporre che $\zeta_n \in K$.

**Definizione 1.3.1** *Se $\Delta \subset K$ definiamo $K(\sqrt[n]{\Delta}) = \prod_{c\in\Delta} K(\sqrt[n]{c})$.*

**Lemma 1.3.2** *Sia $L = K(\sqrt[n]{\Delta})$. Allora $L/K$ è abeliana di esponente $n$.*

**Dim.** Sia $G = G_{K(\sqrt[n]{\Delta}),K}$. Per ogni $c \in \Delta$ abbiamo un'applicazione di restrizione

$$\rho_c : G \longmapsto G_{K(\sqrt[n]{c}),K}.$$

Il prodotto diretto di questi omomorfismi è iniettivo, perché $K(\sqrt[n]{\Delta})$ è il composto dei campi $K(\sqrt[n]{c})$, e la Proposizione (1.3.1) ci dice che ciascun gruppo $G_{K(\sqrt[n]{c})}$ è ciclico di ordine che divide $n$. Dunque realizziamo $G$ come sottogruppo di un gruppo abeliano di esponente $n$.

□

**Teorema 1.3.3 (Kummer)** *Supponiamo che $\zeta_n \in K$. Allora le estensioni abeliane di $K$ di esponente che divide $n$ sono in corrispondenza biunivoca con i sottogruppi $\Delta$ per cui $(K^*)^n < \Delta < K^*$, dove la corrispondenza è data da:*

$$\begin{array}{ccc} L & \longrightarrow & (L^*)^n \cap K^* \\ K(\sqrt[n]{\Delta}) & \longleftarrow & \Delta \end{array}$$

*Inoltre c'é un isomorfismo*

$$\begin{array}{rccc} \psi: & \Delta/(K^*)^n & \longrightarrow & \mathrm{Hom}_{cont.}(G_{L,K}, U_n) \\ & \overline{a} & \longrightarrow & \chi_a \end{array}$$

*dove* $\chi_a(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$.

**Dim.** Data $L/K$ come nelle ipotesi sia $\Delta = (L^*)^n \cap K^*$, e $L' = K(\sqrt[n]{\Delta})$. Per verificare che $L = L'$ basta vedere che $F \subset L'$ per ogni sottoestensione $F/K$ finita. In questo caso $G_{F,K}$ è abeliano finito, e possiamo scriverlo come prodotto diretto di gruppi ciclici. Usando la corrispondenza di Galois è immediato ottenere che $F$ è il composto di sottoestensioni cicliche. Dunque ci basta vedere il caso in cui $F/K$ è ciclica. Per la Proposizione (1.3.1) $F = K(\sqrt[n]{c})$, e poiché $F \subset L$ troviamo che $c \in \Delta$, cioè $F \subset L'$.

Indichiamo $G = G_{L,K}$. È una semplice verifica che $\psi$ è a valori in $U_n$ e che la sua definizione non dipende dalla scelta di $\sqrt[n]{a}$, visto che $\zeta_n \in K$. È del tutto immediato che $\psi$ è un omomorfismo. Inoltre

$$\ker \chi_a = \{\sigma \in G : \sigma(\sqrt[n]{a}) = \sqrt[n]{a}\} = G_{L,K(\sqrt[n]{a})},$$

che è un sottogruppo di indice finito, e perciò aperto nella topologia di Krull. Questo ci dice che $\psi$ è a valori in $\mathrm{Hom}_{cont.}(G, U_n)$.

$$\ker \psi = \{\overline{a} \in \Delta/K^* : \sigma(\sqrt[n]{a}) = \sqrt[n]{a} \quad \forall \sigma \in G\} = (K^*)^n/(K^*)^n,$$

perciò $\psi$ è iniettivo.

Per la surgettività supponiamo dapprima che $L/K$ sia finita. Se $\chi : G \longmapsto U_n$ è un omomorfismo, $\chi \in Z^1(G, U_n)$, perché l'azione di $G$ su $U_n$ è banale. Per il teorema 90 di Hilbert $\chi \in B^1(G, U_n)$, cioè esiste $b \in L^*$ per cui $\chi(\sigma) = \frac{\sigma(b)}{b}$ per tutti i $\sigma \in G$. Inoltre

$$\sigma(b^n) = \sigma(b)^n = (\chi(\sigma)b)^n = b^n \quad \forall \sigma \in G,$$

cioè $a = b^n \in K^*$. Quindi $a \in \Delta$ e $\chi = \chi_a$.

Sia ora $L/K$ qualunque, e $\chi : G \longmapsto U_n$ continuo. Allora $\ker(\chi)$ è aperto, cioè esiste $F/K$ finita con $\ker \chi = G_{L,F}$. Per il caso precedente troviamo $a \in (K^*) \cap (F^*)^n < \Delta$ per cui $\chi = \chi_a$.

Dato $\Delta$ sia $L = K(\sqrt[n]{\Delta})$ e $\Delta' = (L^*)^n \cap K^*$, in modo che $\Delta < \Delta'$. Posto $G = G_{L,K}$ osserviamo che, visto che $G$ ha esponente $n$, $\widehat{G} = \mathrm{Hom}_{cont.}(G, U_n)$. Abbiamo visto che $\Delta'/(K^*)^n \cong \widehat{G}$, e in questo isomorfismo $\Delta/(K^*)^n$ è mappato in $\{\chi_a : a \in \Delta\}$. Perciò l'annullatore di $\Delta/(K^*)^n$ è

$$\left(\frac{\Delta}{(K^*)^n}\right)^{\perp} = \{\sigma \in G : \sigma(\sqrt[n]{a}) = \sqrt[n]{a} \quad \forall a \in \Delta\} = \{\mathrm{id}\}.$$

Per dualità di Pontryagin si conclude che $\Delta = \Delta'$.

□

Per riferimenti sulla dualità di Pontryagin e più in generale sull'analisi armonica su gruppi localmente compatti abeliani si veda ad esempio [Fol95]. In realtà è possibile ricondursi al caso, più semplice, di gruppi finiti. Ci sarà utile anche qualche osservazione sul caso in cui non ci siano le radici dell'unità.

**Lemma 1.3.4** *Sia $c \in K$ e $u$ una sua radice $\ell$-esima, dove $\ell$ è primo. Se il polinomio $x^\ell - c$ è riducibile su $K$, allora esiste una radice dell'unità $\omega$ per cui $\omega u \in K^*$.*

**Dim.** Poniamo $g(x) = x^\ell - c \in K[x]$. Indichiamo la norma $N = N_{K(u)/K}$, e poniamo $a = N(u) \in K$. Osserviamo che

$$a^\ell = N(u)^\ell = N(c) = c^n.$$

Sia $b \in \overline{K}$ tale che $b^n = a$. Poiché $b^{n\ell} = a^\ell = c^n$, a meno di moltiplicare $b$ per una radice $n$-esima dell'unità, possiamo supporre che $b^\ell = c$. Poiché $\ell$ è primo, $(n, \ell) = 1$, dunque possiamo scrivere $sn + t\ell = 1$, con $s, t \in \mathbb{Z}$. Ma allora

$$b = b^{sn+t\ell} = a^s c^t \in K,$$

e $b$ è una radice di $g$, cioè differisce da $u$ per una radice dell'unità.

□

**Proposizione 1.3.5** *Sia $\ell$ un numero primo, e supponiamo che $\zeta_\ell \notin K$. Supponiamo che $u \in L$, dove $L/K$ è un'estensione abeliana, e che $u^\ell \in K^*$. Allora esiste una radice dell'unità $\omega$ per cui $\omega u \in K^*$.*

**Dim.** Sia $c = u^\ell \in K$, e $g(x) = x^\ell - c$. Supponiamo per assurdo che $g$ sia irriducibile; in questo caso $[K(u) : K] = \ell$. Essendo $L/K$ abeliana, la sottoestensione $K(u)/K$ è di Galois. Sia $\sigma \in G_{K(u),K}$ un elemento non banale, in modo che $\sigma(u) = \zeta_\ell^k u$ per un certo $k$ primo con $\ell$. A meno di prendere una potenza di $\sigma$ possiamo supporre $k = 1$. Ma allora $\zeta_\ell \in K(u)$, e $[K(\zeta_\ell) : K]$ divide sia $\ell$ che $[\mathbb{Q}(\zeta_\ell) : \mathbb{Q}] = \ell - 1$. Perciò $\zeta_\ell \in K$, assurdo.

Dunque $g$ è riducibile, e la tesi segue dal Lemma 1.3.4. □

## 1.4 Varietà su campi finiti

Nello studio delle equazioni sui campi finiti la geometria algebrica si è rivelata uno strumento naturale e potente.

**Definizione 1.4.1** *Sia $V$ una varietà algebrica (affine o proiettiva) sul campo $\overline{K}$. Diremo che $V$ è definita su $K$ se l'ideale $I(V)$ può essere generato da polinomi a coefficienti in $K$.*

In questa situazione possiamo considerare la $K$-varietà $V_K = V \cap \mathbb{A}^n(K)$ (risp. $\mathbb{P}^n(K)$). Il caso che ci interessa e $K = \mathbb{F}_q$. Essendo il campo finito, una cosa naturale da fare è contare il numero di punti sulla varietà. In particolare che supponiamo che $V$ sia definita da polinomi a coefficienti nell'anello degli interi $\mathcal{R}$

di un campo di numeri $K$. In questo caso possiamo ridurre le equazioni di $V$ mod $\mathcal{P}$ e contare il numero di punti al variare di $\mathcal{P}$. Quello che ci si aspetta è che almeno asintoticamente il numero di punti sia pari alla cardinalità di uno spazio proiettivo della stessa dimensione $d$, cioè $\frac{q^{(d+1)}-1}{q-1}$. Questo fatto è stato dimostrato nel 1936 da Hasse per le curve ellittiche.

**Definizione 1.4.2** *Una curva ellittica sul campo $K$ è una coppia $(E, O)$, dove $E$ è una curva algebrica proiettiva liscia di genere 1 definita su $K$ e $O \in E_K$.*

È noto che una curva ellittica ammette una struttura di gruppo che la rende una varietà abeliana, e la dimostrazione di Hasse fa uso di questa peculiarità.

**Teorema 1.4.1 (Hasse)** *Sia $E$ una curva ellittica definita su $\mathbb{F}_q$. Allora*

$$|\#(E_{\mathbb{F}_q}) - q - 1| \leq 2\sqrt{q}.$$

Per una dimostrazione si veda [Sil86, cap. 5]. La generalizzazione di questo risultato a curve lisce di genere qualsiasi è dovuta a Weil. Come conseguenza della disuguaglianza di Hasse è facile dimostrare che la funzione $Z$ associata ad una curva ellittica (per la definizione della funzione $Z$ di una varietà algebrica si veda [Sil86, cap. 5]) è una funzione razionale che verifica una certa equazione funzionale e l'ipotesi di Riemann. Nel 1940 Weil pubblica un lavoro ([]) nel quale estende questi risultati a curve di qualsiasi genere, supponendo però che si possa definire in termini algebrici la varietà Jacobiana associata ad una curva (che al tempo era definita solo per curve su $\mathbb{C}$), e che questa goda delle stesse proprietà di cui gode nel caso olomorfo. Nel 1948, al termine di un lavoro ([Wei46], [Wei48a], [Wei48b]) con il quale ha gettato le fondamenta della geometria algebrica astratta, Weil è in grado di dimostrare l'analogo dei teoremi di Hasse per curve qualsiasi. In particolare in ([Wei48a]) dimostra il

**Teorema 1.4.2 (Weil)** *Sia $C$ una curva liscia di genere $g$ definita su $\mathbb{F}_q$. allora*

$$|\#(C_{\mathbb{F}_q}) - q - 1| \leq 2g\sqrt{q}. \tag{1.4.1}$$

In realtà una disuguaglianza simile, con un'ulteriore costante, vale anche se la curva non è liscia, purché sia irriducibile (su $\overline{\mathbb{F}_q}$), e anche per curve affini.

**Definizione 1.4.3** *La $K$-varietà $V_K$ si dice assolutamente irriducibile se $V$ è irriducibile su $\overline{K}$.*

Dai risultati di Weil si deduce immediatamente

**Proposizione 1.4.3** *Sia $C$ una curva affine definita su $\mathbb{F}_q$ assolutamente irriducibile. Allora il numero di punti $N_k$ sulla curva in $\mathbb{F}_{q^k}$ verifica*

$$N_k = q^k + O(q^{k/2}).$$

Una dimostrazione elementare di questo risultato si trova in [Sch76, cap. 3]. In generale non possiamo aspettarci stime simili a (1.4.1) se la varietà non è assolutamente irriducibile.

**Esempio**
Prendiamo $p \equiv 3 \pmod 8$, e consideriamo la curva piana $C$ definita su $\mathbb{F}_p$ dall'equazione

$$y^2 = 2x^4 + 4x^2 + 2.$$

Su una chiusura algebrica possiamo fattorizzare l'equazione come

$$(y-\sqrt{2}(x^2+1))(y+\sqrt{2}(x^2+1))=0,$$

tuttavia questa non è una fattorizzazione su $\mathbb{F}_p$, per reciprocità quadratica. Se $(x,y)\in C_{\mathbb{F}_p}$ uno dei due fattori deve essere 0. Per l'indipendenza lineare di 1 e $\sqrt{2}$ troviamo $y=0$ e $x^2+1=0$, che non ha soluzioni $x\in\mathbb{F}_p$. Perciò $\#(C_{\mathbb{F}_p})=0$.

**Esempio**
Stavolta prendiamo $p\equiv 3 \pmod 4$ e sia $f\in\mathbb{F}_p[x]$. Sia $C$ la curva piana definita da

$$(y^2-f(x))(y^2+f(x))=0.$$

Essendo $-1$ un non-quadrato $\bmod p$, per ogni valore di $x$ troviamo almeno un valore di $y$ per cui $(x,y)\in C_{\mathbb{F}_p}$. Se poi $x$ non è una radice di $f$ troviamo esattamente 2 valori per $y$. Dunque $\#(C_{\mathbb{F}_p})\approx 2p$.

Sotto ipotesi di assoluta irriducibilità si riesce ad ottenere un risultato simile a (1.4.3) in ogni dimensione. Con un'induzione sulla dimensione (non banale) Lang e Weil ottengono la seguente generalizzazione ([LW54]).

**Teorema 1.4.4 (Lang-Weil)** *Sia $V$ una varietà affine definita su $\mathbb{F}_q$ assolutamente irriducibile. Allora il numero di punti $N_k$ sulla varietà in $\mathbb{F}_{q^k}$ verifica*

$$N_k=q^{dk}+O(q^{k(d-1/2)}).$$

Di nuovo, una dimostrazione elementare di questo risultato si può trovare in [Sch76, cap. 5]. Supponiamo di avere una varietà affine $V$ definita da equazioni a coefficienti in un anello di numeri $\mathcal{R}$. In questo caso possiamo effettuare la riduzione delle equazioni $\bmod \mathcal{P}$ per vari primi $\mathcal{P}$ dell'anello, ottenendo così diverse varietà su campi finiti. È importante osservare che in questo caso la costante moltiplicativa implicita nel termine $O(q^{k(d-1/2)})$ è indipendente dal primo $\mathcal{P}$ scelto. Per applicare il teorema di Lang-Weil in questa situazione dobbiamo prima garantirci che la varietà sia assolutamente irriducibile $\bmod \mathcal{P}$ per $N(\mathcal{P})$ abbastanza grande. In effetti abbiamo il

**Teorema 1.4.5** *Sia $V$ una $K$-varietà assolutamente irriducibile definita da equazioni a coefficienti in $\mathcal{R}$. Allora $V$ è assolutamente irriducibile* $\bmod \mathcal{P}$ *tranne che per un numero finito di primi $\mathcal{P}$.*

Nel caso di un'ipersuperficie abbiamo un enunciato lievemente più preciso. Diciamo che $f\in K[x_1,\dots,x_n]$ è assolutamente irriducibile se è irriducibile su $\overline{K}[x_1,\dots,x_n]$.

**Teorema 1.4.6 (Островски[2])** *Sia $f\in\mathcal{R}[x_1,\dots,x_n]$ assolutamente irriducibile. Allora $\overline{f}\in\mathcal{R}/\mathcal{P}[x_1,\dots,x_n]$ è assolutamente irriducibile tranne che per un numero finito di primi $\mathcal{P}$.*

**Dim. (sketch)** Consideriamo lo spazio vettoriale $P(k,n)$ dei polinomi di grado al più $k$ in $\overline{K}[x_1,\dots,x_n]$, e sia $\mathbb{P}_{k,n}$ lo spazio proiettivo associato. Osserviamo che

[2] trasl. Ostrowski

la condizione di irriducibilità è invariante per moltiplicazione per scalare, quindi possiamo considerare l'insieme $\Sigma_{k,n}$ dei polinomi riducibili in $\mathbb{P}_{k,n}$. Osserviamo che

$$\Sigma_{k,n} = \bigcup_{i=1}^{k-1} \mu(\mathbb{P}_{i,n} \times \mathbb{P}_{k-i,n}),$$

dove $\mu$ è l'applicazione di moltiplicazione tra polinomi. Essendo $\mu$ un morfismo, risulta che $\Sigma_{k,n}$ è un chiuso proiettivo. Con un po' più di lavoro (teoria dell'eliminazione) si possono costruire equazioni esplicite per $\Sigma_{k,n}$. In particolare si trova che queste equazioni sono universali, nel senso che sono date da polinomi a coefficienti in $\mathbb{Z}$ e non dipendono dal campo sul quale stiamo lavorando. Indichiamo con $g_1, \dots, g_t$ le equazioni di $\Sigma_{k,n}$.

Sia ora $f$ assolutamente irriducibile; questo vuol dire che almeno uno dei $g_i$ valutato nei coefficienti di $f$ assume un valore non nullo $x$. Se $x \notin \mathcal{P}$ otteniamo che

$$g_i(\text{coefficienti di } f) \not\equiv 0 \pmod{\mathcal{P}},$$

cioè $f$ è assolutamente irriducibile $\bmod \mathcal{P}$.

$\square$

Esplicitando questo metodo si ottengono anche delle stime per quanto grande deve essere $N(\mathcal{P})$ affinché la riduzione di $f$ sia ancora assolutamente irriducibile (vedi [Sch76]). In realtà il teorema di Островскии vale in situazioni più generali: si veda ad esempio [Zan97] in cui si dimostra il teorema per anelli di valutazione discreta con campo residuo di caratteristica positiva.

## 1.5 Valori assoluti

In alcune situazioni è utile avere una misura di quanto un numero algebrico sia 'complicato'. Se il numero è razionale possiamo prendere come misura di questo la sua altezza, definita da

$$H\left(\frac{a}{b}\right) = \max\{|a|, |b|\} \tag{1.5.1}$$

dove $a/b$ è una scrittura ridotta. Per estendere questo concetto a campi di numeri generali abbiamo bisogno del concetto di valore assoluto.

**Definizione 1.5.1** *Un valore assoluto su un campo $K$ è una funzione $|\cdot| : K \longmapsto \mathbb{R}$ tale che*

*(i)* $|x| \geq 0$ *per ogni* $x \in K$ *e* $|x| = 0$ *se e solo se* $x = 0$

*(ii)* $|xy| = |x||y|$ *per ogni* $x, y \in K$

*(iii)* $|x + y| \leq |x| + |y|$ *per ogni* $x, y \in K$.

*Se inoltre è verificata la*

*(iii)'* $|x + y| \leq \max\{|x|, |y|\}$ *per ogni* $x, y \in K$

*il valore assoluto si dice nonarchimedeo.*

Quando si ha a che fare con più valori assoluti contemporaneamente è tipograficamente utile indicare il generico valore assoluto con $v$ invece che con $|\cdot|$ e scrivere $|x|_v = v(x)$.

**Esempio**
Se $\sigma : K \longmapsto \mathbb{C}$ è un'immersione di campi la funzione definita da $|x|_\sigma = |\sigma(x)|$ è un valore assoluto su $K$ archimedeo. In particolare ogni campo di numeri possiede valori assoluti archimedei.

Un modo standard per ottenere valori assoluti è tramite le valutazioni.

**Definizione 1.5.2** *Una valutazione su un campo $K$ è una funzione $v : K \longmapsto \mathbb{R} \cup \{+\infty\}$ tale che*

*(i)* $v(x) = +\infty$ *se e solo se* $x = 0$

*(ii)* $v(xy) = v(x) + v(y)$ *per ogni* $x, y \in K$

*(iii)* $v(x + y) \geq \min\{v(x), v(y)\}$ *per ogni* $x, y \in K$.

*Se $v(K^*)$ è un sottogruppo discreto la valutazione si dirà discreta. In questo caso la possiamo normalizzare in modo che $v(K^*) = \mathbb{Z}$.*

Se $v$ è una valutazione possiamo definire un valore assoluto tramite $|x|_v = s^{-v(x)}$, dove $s > 0$. Quando, come sopra, si adotta la convenzione di indicare con $v$ il valore assoluto, se questo proviene da una valutazione ci può essere un'inconsistenza di notazione. In questi casi la valutazione normalizzata (cioè a valori in $\mathbb{Z}$) è generalmente indicata come $\mathrm{ord}_v$.

**Esempio**
Supponiamo che $K$ sia un campo di numeri con anello degli interi $\mathcal{R}$, e sia $\mathcal{P}$ un primo di $\mathcal{R}$. Consideriamo la valutazione $\mathcal{P}$-adica definita da

$$v_{\mathcal{P}}(x) = \max\{n \in \mathbb{N} : x \in \mathcal{P}^n\}$$

se $x \in \mathcal{R}$ ed estesa a $K$ ponendo $v_{\mathcal{P}}(x/y) = v_{\mathcal{P}}(x) - v_{\mathcal{P}}(y)$. È immediato verificare che la definizione è indipendente dalla scrittura di $x/y$ come frazione e che in questo modo si ottiene una valutazione. Il valore assoluto associato si dirà valore assoluto $\mathcal{P}$-adico.

Nei casi precedenti non ci siamo preoccupati troppo della scelta della base per definire un valore assoluto a partire da una valutazione. In effetti al variare della base si ottengono valori assoluti distinti, perciò diamo la

**Definizione 1.5.3** *Due valori assoluti $|\cdot|_1$ e $|\cdot|_2$ si dicono equivalenti se esiste una costante positiva $\lambda$ per cui $|\cdot|_2 = |\cdot|_1^\lambda$.*

Dato un valore assoluto su $K$ otteniamo una distanza ponendo $d(x, y) = |x - y|$. In particolare la topologia indotta è sufficiente a caratterizzare il valore assoluto.

**Proposizione 1.5.1** *Due valori assoluti $|\cdot|_1$ e $|\cdot|_2$ sono equivalenti se e solo se inducono la stessa topologia su $K$.*

**Dim.** Un'implicazione è ovvia. Supponiamo che $|\cdot|_1$ e $|\cdot|_2$ inducano la stessa topologia su $K$. Per $i = 1, 2$ poniamo $A_i = \{x \in K : |x|_i < 1\}$. Osserviamo che

$$A_i = \{x \in K : x^n \xrightarrow{|\cdot|_i} 0\},$$

e perciò $A_1 = A_2$. Escludiamo il caso banale in cui uno dei valori assoluti è identicamente 1. Allora possiamo prendere $y \in K$ con $|y|_1 > 1$; scegliamo $\lambda$ in modo che $|y|_2 = |y|_1^\lambda$. Sia ora $x \in K$ qualunque, e $a$ tale che $|x|_1 = |y|_1^a$; ci basta verificare che $|x|_2 = |y|_2^a$. Se $\frac{m}{n} > a$ allora $|x^n/y^m|_1 < 1$ e dunque $|x^n/y^m|_2 < 1$. Poiché questo vale per ogni razionale più grande di $a$ si trova $|x|_2 \leq |y|_1^a$. L'altra disuguaglianza è del tutto simile.

□

Siamo dunque interessati ai valori assoluti su campi di numeri a meno di equivalenza (d'ora in poi escluderemo sempre il valore assoluto banale). Su $\mathbb{Q}$ li conosciamo tutti grazie al seguente

**Teorema 1.5.2** (Островски) *Ogni valore assoluto su $\mathbb{Q}$ è equivalente al valore assoluto standard oppure ad un valore assoluto $p$-adico.*

**Dim.** Siano $m, n \in \mathbb{N}$. Se la scrittura di $m$ in base $n$ è

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

la disuguaglianza triangolare ci dà $m \leq \sum |a_i| N^r$, dove $N = \max\{1, |n|\}$. Per ottenere una disuguaglianza che coinvolga solo $m$ e $n$ osserviamo che $r \leq \frac{logm}{\log n}$ e $|a_i| \leq a_i \leq n$. Perciò otteniamo

$$|m| \leq (1 + r) n N^r \leq \left(1 + \frac{\log m}{\log n}\right) n N^{\frac{\log m}{\log n}}. \tag{1.5.2}$$

Sostituiamo in (1.5.2) $m$ con $m^t$. Se prendiamo la radice $t$-esima otteniamo, per $t \to \infty$

$$|m| \leq N^{\frac{\log m}{\log n}}. \tag{1.5.3}$$

Distinguiamo due casi.

- *Per ogni $n \in \mathbb{N}$ si ha* $|n| > 1$. In questo caso $N = |n|$ e dalla (1.5) troviamo

  $$|m|^{\frac{1}{\log m}} \leq |n|^{\frac{1}{\log n}}.$$

  Per simmetria si deve avere uguaglianza e quindi esiste una costante $c$ per cui $|n| = c^{\log n} = n^{\log c}$ per tutti gli $n$. Da questa è immediato ottenere $|x| = |x|_{st}^{\log c}$ per tutti i razionali.

- *Esiste un $n \in \mathbb{N}$ per cui* $|n| \leq 1$. In questo caso la (1.5) ci dice che $|m| \leq 1$ per ogni $m \in \mathbb{N}$. È una semplice verifica che allora l'insieme

  $$\{n \in \mathbb{Z} : |n| < 1\}$$

  è un ideale primo $(p)$ di $\mathbb{Z}$, non nullo perché il valore assoluto è non banale. Da questo si ottiene subito che $|\cdot| = |\cdot|_p^a$.

□

Se vogliamo trovare i valori assoluti su un campo di numeri possiamo intanto osservare che la loro restrizione a $\mathbb{Q}$ coincide con uno dei valori assoluti elencati sopra. Pertanto il problema diventa capire in quali modi si può estendere un valore assoluto dato da un campo ad una sua estensione finita. Lo strumento che si utilizza, importante anche per altri problemi, è quello del completamento. Un campo con un valore assoluto è in particolare uno spazio metrico. Come tale possiamo effettuare il suo completamento astratto; estendendo per continuità le operazioni si può dare al completamento la struttura di campo.

**Definizione 1.5.4** *Il completamento dei razionali rispetto al valore assoluto $|\cdot|_p$ si dice campo dei numeri $p$-adici, e si indica con $\mathbb{Q}_p$. Esso contiene il completamento di $\mathbb{Z}$, cioè*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\},$$

*detto anello degli interi $p$-adici.*

Uno dei vantaggi di lavorare con un campo completo è il seguente fatto, la cui dimostrazione è del tutto analoga a quella che su $\mathbb{R}^n$ tutte le norme sono equivalenti.

**Proposizione 1.5.3** *Sia $K$ un campo completo localmente compatto rispetto ad un valore assoluto $|\cdot|$. Se $E/K$ è un'estensione finita allora esiste al più un'estensione di $|\cdot|$ a $E$; inoltre $E$ risulta completo rispetto a questo valore assoluto.*

In realtà una tale estensione nel caso di $\mathbb{Q}_p$ esiste sempre. Infatti è chiaro dalle definizioni che

$$p\,\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\}$$

è l'unico ideale massimale di $\mathbb{Z}_p$, che risulta perciò locale. Se $\mathcal{R}$ è la chiusura integrale di $\mathbb{Z}_p$ in $E$ e $\mathcal{P}$ un primo sopra $p\mathbb{Z}_p$, il valore assoluto $\mathcal{P}$-adico estende quello $p$-adico.

Se $K$ è un campo di numeri e $v$ è un valore assoluto sopra $|\cdot|_p$ possiamo considerare l'estensione dei completamenti $K_v/\mathbb{Q}_p$. È facile vedere che questa è un'estensione finita; più precisamente se $K = \mathbb{Q}(\alpha)$ allora $K_v = \mathbb{Q}_p(\alpha)$. Sia $g(x) \in \mathbb{Q}[x]$ è il polinomio minimo di $\alpha$, e supponiamo che la fattorizzazione su $\mathbb{Q}_p[x]$ sia

$$g(x) = g_1(x) \cdots g_k(x).$$

Allora il polinomio minimo di $\alpha$ su $\mathbb{Q}_p$ è uno dei $g_i$.

Viceversa dato un fattore $g_i$ possiamo considerare il campo $E = \mathbb{Q}_p[x]/(g_i)$, che è un'estensione finita di $\mathbb{Q}_p$. Per quanto abbiamo visto c'è un unico valore assoluto su $E$ che estende quello $p$-adico. Abbiamo un'immersione $\sigma : K \longrightarrow E$ e possiamo dunque restringere questo valore assoluto su $K$.

In conclusione abbiamo stabilito una corrispondenza biunivoca tra i fattori irriducibili di $g$ in $\mathbb{Q}_p[x]$ e i valori assoluti su $K$ che estendono $|\cdot|_p$. Poiché ogni valore assoluto su $K$ si ottiene restringendo il valore assoluto di un'estensione $E/\mathbb{Q}_p$ finita, e questo a sua volta si ottiene da una valutazione $\mathcal{P}$-adica, si ricava il

**Teorema 1.5.4** *Sia $K$ un campo di numeri e $|\cdot|$ un valore assoluto che si restringe a $|\cdot|_p$. Allora esiste un primo $\mathcal{P}$ di $K$ per cui $|\cdot| = |\cdot|_{\mathcal{P}}$.*

In modo simile si ricava che ogni valore assoluto di $K$ che si restringa a $|\cdot|_{st}$ su $\mathbb{Q}$ è ottenuto da un'immersione $\sigma : K \longmapsto \mathbb{C}$. In questo modo abbiamo classificato i valori assoluti su un campo di numeri. Questo ci permette di ottenere l'importante formula del prodotto.

Prima di tutto abbiamo bisogno di normalizzare i valori assoluti scegliendone uno in ciascuna classe di equivalenza. Per ogni immersione $\sigma : K \longrightarrow \mathbb{C}$ abbiamo il valore assoluto archimedeo $|x|_\sigma = |\sigma(x)|$. Se invece $\mathcal{P}$ è un primo di $\mathcal{R}$ sopra $p$, sia $v_\mathcal{P}$ la valutazione normalizzata. Definiamo $|x|_\mathcal{P} = N(\mathcal{P})^{-v_\mathcal{P}(x)}$. In questo modo se $x \in \mathbb{Q}$

$$|x|_\mathcal{P} = |x|_p^{e(\mathcal{P}|p)f(\mathcal{P}|p)} \tag{1.5.4}$$

**Teorema 1.5.5 (Formula del prodotto)** *Sia $K$ un campo di numeri, $x \in K$ non nullo. Allora $|x|_v = 1$ per quasi ogni valore assoluto e*

$$\prod_v |x|_v^{\varepsilon(v)} = 1, \tag{1.5.5}$$

*dove $\varepsilon(v) = 1$, escluso il caso in cui $v$ sia nonarchimedeo e provenga da un'immersione $\sigma : K \longmapsto \mathbb{C}$ per la quale $\sigma(K) \not\subset \mathbb{R}$, nel qual caso $\varepsilon(v) = 2$.*

**Dim.** Nel caso $K = \mathbb{Q}$ la formula si ottiene per verifica diretta, utilizzando il teorema di Островскии. Nel caso generale osserviamo che

$$\prod_{v|_\mathbb{Q} \sim v_p} |x|_v = |N_{K/\mathbb{Q}}(x)|_p. \tag{1.5.6}$$

Questa relazione si ottiene facilmente osservando che se $\sigma \in \mathrm{Hom}_\mathbb{Q}(K, \mathbb{C})$, allora $\sigma$ dà un'identificazione tra i valori assoluti di $K$ e di $\sigma(K)$ che estendono $|\cdot|_p$. Dunque

$$\left(\prod_{v|_\mathbb{Q} \sim v_p} |x|_v\right)^{[K:\mathbb{Q}]} = \prod_{\substack{v|_\mathbb{Q} \sim v_p \\ \sigma \in \mathrm{Hom}_\mathbb{Q}(K,\mathbb{C})}} |\sigma(x)|_v = \prod_{v|_\mathbb{Q} \sim v_p} |N_{K/\mathbb{Q}}(x)|_v.$$

D'altra parte se $v$ è il valore assoluto $\mathcal{P}$-adico la (1.5.4) ci dà

$$|N_{K/\mathbb{Q}}(x)|_v = |N_{K/\mathbb{Q}}(x)|_p^{e(\mathcal{P}|p)f(\mathcal{P}|p)};$$

facendo il prodotto al variare di $\mathcal{P}$ e prendendo la radice $[K : \mathbb{Q}]$-esima si ottiene la (1.5.6), grazie alla formula dimensionale (1.1.7). Similmente

$$\prod_{v|_\mathbb{Q} \sim |\cdot|_{st}} |x|_v^{\varepsilon(v)} = |N_{K/\mathbb{Q}}(x)|_{st}. \tag{1.5.7}$$

Prendendo il prodotto di (1.5.6) al variare di $p$ e della (1.5.7) si ottiene la tesi.

□

## 1.6 Altezze

Adesso possiamo estendere la definizione (1.5.1) a campi di numeri qualunque. Per una generalizzazione a spazi proiettivi o curve ellittiche su campi di numeri si vedano [Sko99] oppure [Sil86, cap. 8]. [Ser89] contiene, tra le altre cose, applicazioni delle altezze al teorema di irriducibilità di Hilbert.

Indichiamo con $M_K$ l'insieme di tutti i valori assoluti su $K$ normalizzati come nella sezione precedente. Se $x \in K$ definiamo

$$H_K(x) = \prod_{|\cdot| \in M_K} \max\{|x|, 1\}. \tag{1.6.1}$$

Dalla (1.5.6) (che vale con la stessa dimostrazione per un'estensione di campi di numeri qualunque) segue che se $L$ è un'estensione finita di $K$ allora $H_L(x) = H_K(x)^{[L:K]}$. Possiamo allora definire l'altezza assoluta di un numero algebrico $x$ come

$$H(x) = H_K(x)^{\frac{1}{[K:\mathbb{Q}]}},$$

dove $K$ è un campo di numeri contenente $x$.

**Esempio**
Sia $a/b$ un numero razionale scritto in forma ridotta, in modo che $H(a/b) = H_{\mathbb{Q}}(a/b)$. Nel prodotto (1.6.1) possono essere diversi da 1 solo i termini relativi a $|\cdot|_{st}$ e a $|\cdot|_p$ con $p|b$. Per ciascuno di questi ultimi fattori se $p^k \| b$ abbiamo un fattore $p^k$, perciò il prodotto di questi termini è $|b|_{st}$. Se $|a| \leq |b|$ allora il termine $\max\{|a/b|_{st}, 1\}$ è 1 e dunque $H(a/b) = |b|_{st}$. Altrimenti

$$\max\{|a/b|_{st}, 1\} = |a/b|_{st}$$

e di conseguenza $H(a/b) = |a|_{st}$, in accordo con la (1.5.1).

Vediamo le prime proprietà delle altezze. Dalla formula del prodotto (1.5.5) è immediato ottenere che $H(x) = H(1/x)$. Inoltre è immediato che

$$H(x^k) = H(x)^k. \tag{1.6.2}$$

Direttamente dalle definizioni si ricava che $H(xy) \leq H(x)H(y)$. Inoltre abbiamo la

**Proposizione 1.6.1** $H(x+y) \leq 2H(x)H(y)$

**Dim.** Sia $K$ un campo contenente $x$ e $y$, sia $d = [K : \mathbb{Q}]$. Ci basta vedere che

$$H(x+y) \leq 2^d H(x)H(y).$$

Sia $v$ un valore assoluto non archimedeo, e supponiamo per simmetria $|x|_v \geq |y|_v$. Allora

$$\max\{1, |x+y|_v\} \leq \max\{1, |x|_v\} \leq \max\{1, |x|_v\} \max\{1, |y|_v\}.$$

Similmente se $v$ è archimedeo e $|x|_v \geq |y|_v$ troviamo

$$\max\{1, |x+y|_v\} \leq 2\max\{1, |x|_v\} \leq 2\max\{1, |x|_v\} \max\{1, |y|_v\}.$$

Prendendo il prodotto al variare di $v$ si ottiene la tesi.

$\square$

Avremo anche bisogno di due fatti leggermente più profondi.

**Proposizione 1.6.2 (Kronecker)** *$H(x) = 1$ se e solo se $x$ è una radice dell'unità, oppure $x = 0$.*

**Dim.** Se $x$ è una radice $n$-esima di 1 la (1.6.2) ci dice che $H(x)^n = 1$, da cui $H(x) = 1$. Viceversa supponiamo $H(x) = 1$, in modo che $H(x^n) = 1$ per ogni $n$. Allora il fatto che $x$ abbia ordine finito segue subito dal Teorema (1.6.3).

□

**Teorema 1.6.3 (Northcott)** *Per ogni scelta di costanti $A$ e $B$ l'insieme*

$$\{x : H(x) \leq A, [\mathbb{Q}(x) : \mathbb{Q}] \leq B\}$$

*è finito. In particolare ogni campo di numeri $K$ contiene solo un numero finito di elementi di altezza limitata.*

Se $f(x) = a_n x^n + \cdots + a_0$ definiamo la sua altezza come

$$H(f) = \left( \prod_{|\cdot| \in M_K} \max\{|a_n|, \ldots, |a_0|\} \right)^{1/d},$$

dove $d = [\mathbb{Q}(a_n, \ldots, a_0) : \mathbb{Q}]$. La formula del prodotto ci dice che $H(f)$ dipende da $f$ solo a meno di multipli.

**Lemma 1.6.4** *Sia $f(x) = a_n x^n + \cdots + a_0 = a_n(x - \alpha_1) \cdots (x - \alpha_n)$. Allora*

$$H(f) \leq 2^{n-1} \prod_{i=1}^{n} H(\alpha_i).$$

**Dim.** Per quanto osservato possiamo supporre $a_n = 1$. Fissato un valore assoluto $|\cdot|$ mostriamo che

$$\max_i\{|a_i|\} \leq \gamma^{n-1} \prod_{j=1}^{n} \max\{|\alpha_j|, 1\}, \tag{1.6.3}$$

dove $\gamma = 2$ se $|\cdot|$ è archimedeo e 1 altrimenti. Da questo si ottiene subito la tesi prendendo il prodotto al variare di $|\cdot|$.

Per ottenere (1.6.3) usiamo un'induzione su $n$, essendo il caso $n = 1$ ovvio. Sia $\alpha_k$ la radice di valore assoluto massimo. Poniamo

$$g(x) = x^{n-1} + b_{n-2}x^{n-2} \cdots + b_0 = (x - \alpha_1) \cdots \widehat{(x - \alpha_k)} \cdots (x - \alpha_n).$$

Poiché $f(x) = (x - \alpha_k)g(x)$ troviamo, confrontando i coefficienti,

$$a_i = b_{i-1} - \alpha_k b_i.$$

Perciò

$$|a_i| \leq \gamma \max\{|b_{i-1}|, |\alpha_k b_i|\} \leq \gamma \max_j\{|b_j|\} \max\{|\alpha_k|, 1\}$$

e si conclude per ipotesi induttiva.

□

**Dim. (teorema)** Dato $x \in \overline{\mathbb{Q}}$ sia $d = [\mathbb{Q}(x) : \mathbb{Q}]$, e siano $x = x_1, \ldots, x_d$ i suoi coniugati. È chiaro che $H(x_i) = H(x)$ per ogni $i$. Se $f$ è il polinomio minimo, il Lemma (1.6.4) ci dice che $H(f) \leq 2^{d-1} H(x)^d$. Se $H(x) \leq A$ e $d \leq B$ questo dà solo numero finito di scelte per il polinomio $f$, che è a coefficienti razionali, e dunque per $x$.

$\square$

Spesso è usata anche l'altezza logaritmica $h(x) = \log H(x)$. Chiaramente tutte le proprietà viste per $H$ si trasportano ad $h$. Così:

- $h(x) \geq 0$;
- $h(x) = 0$ se e solo se $x$ è una radice dell'unità oppure $x = 0$;
- $h(x^k) = kh(x)$;
- $h(xy) \leq h(x) + h(y)$;
- $h(x + y) \leq h(x) + h(y) + \log 2$;
- se $x \in K$ e $K/\mathbb{Q}$ è normale con gruppo di Galois $G$, allora $h(x) = h(\sigma(x))$ per ogni $\sigma \in G$;
- Date costanti $A$ e $B$ l'insieme $\{x : h(x) \leq A, [\mathbb{Q}(x) : \mathbb{Q}] \leq B\}$ è finito.

# Capitolo 2

# Ricorrenze lineari

Le idee chiare e precise sono le
più pericolose, perchè non si osa
più cambiarle.

*André Gide*

## 2.1 Soluzioni di ricorrenze lineari

**Definizione 2.1.1** *Sia $K$ un campo e $c_0, \dots, c_m \in K$, con $c_0 \neq 0$. L'equazione*

$$c_0 s_{m+k} + \cdots + c_m s_k = 0 \tag{2.1.1}$$

*è detta una ricorrenza lineare a coefficienti in $K$. Una soluzione della ricorrenza lineare è una successione $(s_k)_{k\in\mathbb{N}}$ che verifichi la (2.1.1) per ogni valore di $k$. L'intero $m$ è detto l'ordine della ricorrenza.*

Il primo scopo che ci prefiggiamo è quello di trovare la soluzione generale della (2.1.1). Osserviamo innanzitutto che le soluzioni di (2.1.1) formano uno spazio vettoriale. Poiché una soluzione è determinata induttivamente una volta che siano noti i primi $m$ termini e questi possono essere scelti arbitrariamente, la dimensione dello spazio delle soluzioni è $m$.

**Definizione 2.1.2** *Il polinomio caratteristico della ricorrenza lineare (2.1.1) è $q(x) = c_m x^m + \cdots + c_0 \in K[x]$. Le sue radici si dicono radici della ricorrenza lineare.*

Siano $\alpha_1, \dots, \alpha_k$ le radici del polinomio $q(x) = c_m x^m + \cdots + c_0$ in una chiusura algebrica, con molteplicità $d_1, \dots, d_r$. Allora $q^{(t)}(\alpha_i) = 0$ per $t < d_i$, e da questo segue per verifica diretta che le successioni

$$\{n^t \alpha_i^n\} \tag{2.1.2}$$

sono soluzione della (2.1.1) per $t < d_i$. Dunque abbiamo trovato $d_1 + \cdots + d_r = m$ soluzioni della ricorrenza. Se verifichiamo che sono linearmente indipendenti otteniamo una base dello spazio delle soluzioni su $\overline{K}$ . Per verificare l'indipendenza lineare mostriamo che il determinante della matrice

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & 2\alpha_1 & \cdots & 2^{d_k-1}\alpha_k \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{m-1} & (m-1)\alpha_1^{m-1} & \cdots & (m-1)^{d_k-1}\alpha_k^{m-1} \end{pmatrix} \tag{2.1.3}$$

è non nullo.

Consideriamo infatti lo spazio vettoriale $\overline{K}[x]_{<m}$ dei polinomi di grado minore di $m$ su $\overline{K}$. All'interno di questo spazio consideriamo i polinomi $p$ che verificano

$$p^{(i)}(\alpha_j) = 0 \tag{2.1.4}$$

per $j = 1, \ldots, k$ e $0 \leq i \leq d_j - 1$. Se $p$ verifica la (2.1.4) allora è divisibile per $(x-\alpha_1)^{d_1} \cdots (x-\alpha_k)^{d_k}$ e questo, insieme a $\deg(p) < m$, implica $p = 0$. Allo stesso tempo le soluzioni di (2.1.4) rispetto alla base standard $1, \ldots, x^{m-1}$ sono quelle nel nucleo della matrice (2.1.3), che pertanto risulta non singolare. In conclusione ogni soluzione della ricorrenza (2.1.1) è combinazione lineare delle (2.1.2), e pertanto ha la forma

$$s_n = \sum_{i=1}^{r} A_i(n)\alpha_i^n, \tag{2.1.5}$$

dove $\deg A_i < d_i$.

**Definizione 2.1.3** *Ogni funzione su $\mathbb{N}$ della forma (2.1.5) è detta polinomio esponenziale. Indichiamo con $K[x]_{esp}$ l'anello dei polinomi esponenziali a coefficienti in $K$.*

Con questa terminologia otteniamo la

**Proposizione 2.1.1** *Una successione $(s_n)$ verifica una ricorrenza lineare se e solo se è espressa da un polinomio esponenziale.*

**Dim.** Resta da verificare solamente che se $s_n$ è data dalla (2.1.5) allora è soluzione di una ricorrenza lineare. Posto $d_i = \deg(A_i)+1$ costruiamo un polinomio $q$ che si annulli esattamente nei punti $\alpha_i$ di ordine $d_i$, ad esempio

$$q(x) = \prod_{i=1}^{r}(x-\alpha_i)^{d_i}.$$

Allora $s_n$ è soluzione della ricorrenza lineare di polinomio caratteristico $q$, essendo combinazione lineare delle soluzioni standard date dalla (2.1.2).

□

**Proposizione 2.1.2** *I coefficienti di un polinomio esponenziale sono determinati dai suoi valori, cioè vale l'analogo del principio di identità dei polinomi.*

**Dim.** Siano

$$a(n) = \sum_{i=1}^{r} A_i(n)\alpha_i^n, \qquad b(n) = \sum_{i=1}^{s} B_i(n)\beta_i^n$$

due polinomi esponenziali, e supponiamo che $a(n) = b(n)$ per tutti gli $n$. A patto di prendere alcuni $A_i$ e $B_i$ nulli possiamo supporre che l'insieme delle radici sia lo stesso, cioè

$$a(n) = \sum_{i=1}^{t} A_i(n)\gamma_i^n, \qquad b(n) = \sum_{i=1}^{t} B_i(n)\gamma_i^n.$$

Sia $k$ maggiore o uguale del grado di tutti gli $A_i$ e i $B_i$. I coefficienti dei polinomi $A_i$ si ricavano dal sistema lineare

$$\begin{cases} A_1(0) \quad + \cdots + A_t(0) & = a(0) \\ A_1(1)\gamma_1 + \cdots + A_t(1)\gamma_t & = a(1) \\ \qquad\quad \vdots & \quad \vdots \\ A_1(k)\gamma_1^k + \cdots + A_t(k)\gamma_t^k & = a(k). \end{cases}$$

Come abbiamo visto sopra la matrice associata a questo sistema lineare è non singolare, perciò la soluzione è unica e $A_i = B_i$ per ogni $i$.

□

Data una successione siamo interessati a determinare se questa soddisfa una qualche ricorrenza lineare. Sappiamo che se questo è vero la successione è espressa da un polinomio esponenziale, ma questo non ci dà un criterio esplicito.

**Definizione 2.1.4** *Data una successione $s = \{s_i\}$ definiamo i suoi determinanti di Kronecker-Hankel come*

$$K_h(s) = \det(s_{i+j})_{\substack{i=0,\ldots,h \\ j=0,\ldots,h}}.$$

**Proposizione 2.1.3** *La successione $s$ verifica una ricorrenza lineare se e solo se $K_h(s) = 0$ per $h$ sufficientemente grande.*

**Dim.** Supponiamo che $s$ sia una soluzione di (2.1.1). Allora i vettori colonna della matrice $(s_{i+j})_{0\le i,j\le h}$ sono contenuti in un iperpiano se $h \ge m$, perciò sono linearmente dipendenti.

Viceversa supponiamo che per $h$ grande $K_h(s) = 0$ per $h \ge n$ mentre $K_{n-1}(s) \neq 0$. Allora possiamo trovare costanti $\lambda_0, \ldots, \lambda_n$ per cui, posto

$$t_h = \lambda_0 s_{h+n} + \cdots + \lambda_n s_n,$$

si abbia $t_h = 0$ per $h = 0, \ldots, n$. Con operazioni di riga e di colonna si trova che $K_{n+1}(s) = -t_{n+1}^2 K_{n-1}(s)$. Essendo $K_{n-1}(s) \neq 0$ si trova $t_{n+1} = 0$. Per induzione si ottiene la tesi.

□

In realtà per l'applicazione al teorema del quoziente di Hadamard avremo bisogno di una forma leggermente più precisa, che si ottiene con la stessa dimostrazione.

**Proposizione 2.1.4** *Supponiamo che $K_h(s) = 0$ per ogni $h$ con $H_0 \le h \le H$. Allora i termini $s_h$ soddisfano una ricorrenza lineare di ordine al più $H_0$ per $h \le H$.*

## 2.2 L'anello di Hadamard

Sia $K$ un campo di caratteristica 0 e $f \in K(x)$ una funzione razionale. Supponiamo che $f$ sia definita in 0, cioè se $f = p/q$ è una scrittura ridotta $q(0) \neq 0$. Allora $q$ è invertibile nell'anello delle serie di potenze $K[[x]]$, e possiamo scrivere $p/q = s \in K[[x]]$. Derivando più volte si trova che $s$ è la serie di Taylor formale di $f$, cioè

$$s = \sum_{i=0}^{\infty} \frac{f^{(i)}(0)x^i}{i!}. \tag{2.2.1}$$

Più precisamente le funzioni razionali $p/q$ definite in 0 formano un anello che è la localizzazione di $K[x]$ rispetto all'ideale del punto 0

$$I_0 = \{p(x) \in K[x] : p(0) = 0\}.$$

L'immersione $K[x] \hookrightarrow K[[x]]$ si estende ad un omomorfismo iniettivo

$$K[x]_{I_0} \longrightarrow K[[x]] \tag{2.2.2}$$

che è quello che abbiamo appena descritto. L'anello $K[[x]]$ è dotato di una $(K)$-derivazione standard $D : K[[x]] \longrightarrow K[[x]]$ data da

$$D\left(\sum_{i=0}^{\infty} a_n x^n\right) = \sum_{i=0}^{\infty} n a_n x^n, \tag{2.2.3}$$

che si restringe alla derivazione standard sul sottoanello dei polinomi. Allo stesso tempo la derivazione standard sui polinomi ha un'estensione su $K[x]_{I_0}$ data dalle usuali regole di derivazione

$$D\left(\frac{p(x)}{q(x)}\right) = \frac{D(p(x))q(x) - p(x)D(q(x))}{q(x)^2}. \tag{2.2.4}$$

Tuttavia è immediato vedere tramite le proprietà delle derivazioni che una derivazione su $K[x]_{I_0}$ è determinata dal suo valore su $K[x]$. Ne segue che le due derivazioni date dalla (2.2.3) e dalla (2.2.4) devono coincidere su $K[x]_{I_0}$ (stiamo considerando $K[x]_{I_0}$ come sottoanello di $K[[x]]$, tramite l'omomorfismo (2.2.2).) Ne segue che possiamo derivare l'uguaglianza $p/q = s$ utilizzando la derivazione (2.2.4) a sinistra e la (2.2.3) a destra. Valutando in 0 otteniamo infine $n!s_n = f^{(n)}(0)$, da cui la (2.2.1).

Viceversa ci chiediamo quando è che una serie di Taylor proviene da una funzione razionale. Se fissiamo un polinomio $q(x) = c_m x^m + \cdots + c_0$, allora $s \cdot q$ è un polinomio se e solo se $c_0 s_{m+k} + \cdots + c_m s_k = 0$ per $k$ grande, dove $s_n$ è la successione dei coefficienti di $s$. Dunque abbiamo la

**Proposizione 2.2.1** *Una serie $s = \sum s_i x^i \in K[[x]]$ è la serie di Taylor di una funzione razionale se e solo se la successione $s_n$ verifica definitivamente una ricorrenza lineare.*

D'altra parte i risultati della precedente sezione ci permettono di ottenere:

**Proposizione 2.2.2** *Una serie $s = \sum s_i x^i \in K[[x]]$ è la serie di Taylor di una funzione razionale se e solo se la successione $s_n$ è data definitivamente da un polinomio esponenziale.*

**Esempio**
L'esempio più familiare di ricorrenza lineare è dato dalla successione di Fibonacci

$$\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_{n+1} = F_n + F_{n-1} \text{ per } n \geq 1. \end{cases}$$

Il polinomio caratteristico della ricorrenza è $q(x) = x^2 - x - 1$ con radici

$$\alpha_{1,2} = \frac{1 \pm \sqrt{5}}{2}.$$

La scrittura di $F_n$ come combinazione lineare di $\alpha_1^n$ e $\alpha_2^n$ porta alla classica formula di Binet

$$F_n = \frac{1}{\sqrt{5}} \left( \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right).$$

Inoltre non è difficile ricavare la funzione razionale con coefficienti di Taylor $F_n$

$$\sum_{n=0}^{\infty} F_n x^n = \frac{x}{x^2 - x - 1}.$$

Sull'insieme $K[[x]]$ possiamo considerare operazioni diverse da quelle usuali, cioè la somma e la moltiplicazione componente per componente. In effetti la somma coincide con quella usuale, ma la moltiplicazione non è quella dell'anello $K[[x]]$. La somma e la moltiplicazione componente per componente sono dette operazioni di Hadamard. Per distinguere l'insieme delle serie formali con le operazioni di Hadamard dall'anello $K[[x]]$ lo indicheremo $K[[x]]_H$. Chiaramente queste operazioni non sono molto interessanti: semplicemente $K[[x]]_H \cong \prod_{i \in \mathbb{N}} K$. Indicheremo la somma con il simbolo usuale, mentre per la moltiplicazione useremo il simbolo $\star$, in modo che

$$\left( \sum s_i x^i \right) \star \left( \sum t_i x^i \right) = \sum s_i t_i x^i.$$

Dalla Proposizione (2.2.2) e dal fatto che $K[x]_{esp}$ è un anello segue subito che se $s$ e $t$ sono serie di Taylor di funzioni razionali anche $s \star t$ lo è. In questo modo otteniamo un sottoanello $\mathcal{H}(K)$ di $K[[x]]_H$ formato dalle serie di Taylor di funzioni razionali definite in 0. Mentre la struttura di $K[[x]]_H$ è molto semplice, quella di $\mathcal{H}(K)$ è piuttosto profonda, e questa tesi è proprio incentrata sulla struttura dell'anello $\mathcal{H}(K)$, in particolare sul problema di determinare quando una soluzione formale (cioè in $K[[x]]_H$) di un'equazione a coefficienti in $\mathcal{H}(K)$ sia ancora data da una funzione razionale.

## 2.3 Fattorizzazione di polinomi esponenziali

Gli anelli di polinomi esponenziali hanno anche buone proprietà di fattorizzazione, che sfrutteremo nel capitolo 5. Fissato un sottogruppo finitamente generato $W < K^*$ indichiamo con $K[h]_W$ l'anello dei polinomi esponenziali con radici in $W$. Vorremmo arrivare ad una ragionevole descrizione dell'anello $K[h]_W$. Innanzitutto osserviamo che essendo $W$ finitamente generato, $W \cong \mathbb{Z}^n \times T$, dove $T$ è la parte di torsione. Essendo $T$ un sottogruppo finito di $K^*$ è ciclico, ed arriviamo dunque a

$$W \cong \mathbb{Z}^n \times \mathbb{Z}/d\mathbb{Z}.$$

Indichiamo con $\zeta$ un generatore per $T$ e con $w_1, \ldots, w_n$ generatori liberi per $\mathbb{Z}^n < W$. Dal principio di identità per i polinomi esponenziali segue che

$$K[h]_W \cong K[H, Z, W_1, W_1^{-1}, \ldots, W_n, W_n^{-1}],$$

dove $H$ e le $W_i$ sono indeterminate algebricamente indipendenti e $Z$ ha ordine moltiplicativo $d$.

Vediamo in particolare la struttura dell'anello $K[Z] \cong K[X]/(X^d - 1)$. Visto che $K$ contiene la radice primitiva $d$-esima dell'unità $\zeta$, abbiamo la fattorizzazione su $K$

$$X^d - 1 = \prod_{i=1}^{d} (x - \zeta^i).$$

Il teorema cinese del resto ci permette di scrivere allora

$$K[Z] \cong K[X]/(X^d - 1) \cong \bigoplus_{i=1}^{d} K[X]/(x - \zeta^i) \cong \bigoplus_{i=1}^{d} K.$$

Questo corrisponde a restringere i polinomi esponenziali alle varie progressioni aritmetiche mod $d$.

In particolare l'anello $K[h]_W$ risulta una somma diretta di $d$ copie dell'anello $K[H, W_1, W_1^{-1}, \ldots, W_n, W_n^{-1}]$. Quest'ultimo è una localizzazione dell'anello di polinomi $K[H, W_1, \ldots, W_n]$, che è a fattorizzazione unica, e pertanto è a sua volta a fattorizzazione unica. In particolare se $W$ è un gruppo abeliano libero $K[h]_W$ è un anello a fattorizzazione unica.

## 2.4 Un po' di analisi $p$-adica

Nelle prossime sezioni avremo bisogno di un nuovo strumento: l'analisi in $\mathbb{Q}_p$ e nelle sue estensioni finite. Ci limitiamo ad alcuni cenni, rivolti ad ottenere i risultati di cui abbiamo bisogno. Per maggiori dettagli ed approfondimenti rimandiamo a [Kob84]. Poiché $\mathbb{Q}_p$ è un campo completo si può sperare di riprodurre in questo contesto le tecniche usuali dell'analisi reale o complessa. In effetti per molti scopi è così; in particolare possiamo riprodurre le usuali definizioni di funzioni differenziabili. Tuttavia l'approccio più conveniente è tramite lo studio delle funzioni analitiche.

Una prima osservazione è che, dato il carattere nonarchimedeo di $|\cdot|_p$ una serie $\sum a_n$ a coefficienti in $\mathbb{Q}_p$ converge se e solo se il termine generale tende a 0, il che semplifica molte cose rispetto all'analisi complessa. Data una serie di potenze possiamo definire il suo raggio di convergenza

**Definizione 2.4.1** *Il raggio di convergenza di $s(x) = \sum_{i=0}^{\infty} s_n x^n \in \mathbb{Q}_p[[x]]$ è $r = 1/L$, dove*

$$L = \limsup_{n \to \infty} |s_n|_p^{1/n}.$$

In modo molto simile al caso dell'analisi complessa si dimostra

**Teorema 2.4.1 (Cauchy-Hadamard)** *Se la serie di potenze $s(x)$ ha raggio di convergenza $r$, allora $s(t)$ converge per $|t|_p < r$ e diverge per $|t|_p > r$.*

**Esempio**
Tramite uno sviluppo in serie possiamo definire le funzioni esponenziale e logaritmo $p$-adiche. Poniamo

$$\log_p(1+x) = \sum_{n=1}^{\infty} \frac{1}{n} x^n$$
$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{1}{n!} x^n.$$

A differenza del caso complesso la funzione $\log_p(1+x)$ ha raggio di convergenza maggiore di $\exp_p(x)$. Questo è dovuto al fatto che i termini $n!$ al denominatore sono piccoli rispetto all'usuale valore assoluto, ma sono grandi $p$-adicamente. In effetti è facile calcolare che il raggio di convergenza di $\log_p(1+x)$ è 1, mentre quello di $\exp_p(x)$ è $p^{1/(p-1)}$. Inoltre se $x$ appartiene al disco

$$D = \left\{ t \in \mathbb{Q}_p : \operatorname{ord}_p(t) > -\frac{1}{p-1} \right\}$$

è facile ottenere direttamente dagli sviluppi in serie che

$$\exp_p(\log_p(1+x)) = 1+x; \qquad \log_p(1+(\exp_p(x)-1)) = x,$$

cioè le due funzioni $\exp_p$ e $\log_p$ sono inverse una dell'altra quando ristrette a $D$ e a $1+D$ rispettivamente.

Per ottenere risultati interessanti di analisi $p$-adica è necessario lavorare su un campo che sia non solo completo ma anche algebricamente chiuso. Dalla Proposizione 1.5.3 segue subito che il valore assoluto $|\cdot|_p$ su $\mathbb{Q}_p$ ha un'unica estensione sulla chiusura algebrica $\overline{\mathbb{Q}_p}$. Il completamento di $\overline{\mathbb{Q}_p}$ rispetto a questo valore assoluto è ancora algebricamente chiuso e viene indicato con $\mathbb{C}_p$.

Lo strumento fondamentale per lo studio delle funzioni analitiche su $\mathbb{C}_p$ è dato dai poligoni di Newton

**Definizione 2.4.2** *Sia $f(x) = \sum_{i=0}^{\infty} f_i x^i \in \mathbb{Q}_p[[x]]$ una serie di potenze tale che $\operatorname{ord}_p(f_0) = 0$, e supponiamo che $f$ non sia un polinomio . Il poligono di Newton di $f(x)$, se esiste, è il grafico della più grande funzione convessa lineare a tratti $g : [0, +\infty[ \longmapsto \mathbb{R}$ che verifica $g(i) \leq ord_p(i)$ per ogni $i \in \mathbb{N}$.*

È facile vedere che se esiste una funzione $g$ convessa lineare a tratti che verifica al disuguaglianza ne esiste anche una massima rispetto a queste proprietà. Escludiamo dal nostro studio il caso in cui il poligono di Newton non esista: in questo caso è facile vedere che la serie ha raggio di convergenza 0. Un esempio è dato dalla serie

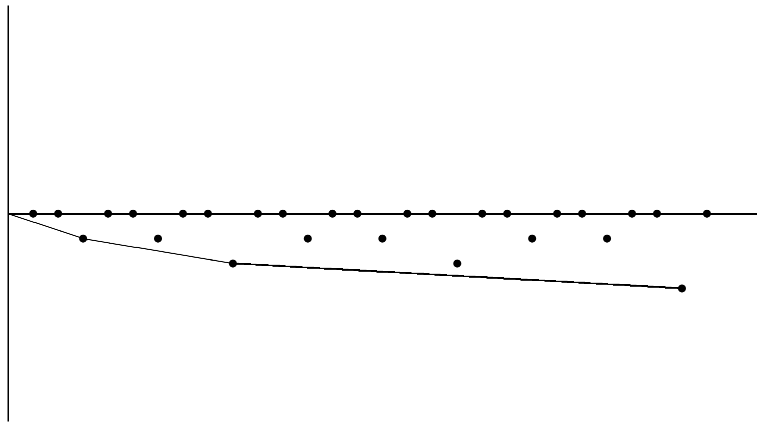
$$f(x) = \sum_{i=0}^{\infty} \frac{1}{p^{i^2}} x^i.$$

La definizione del poligono di Newton per un polinomio $f(x) = \sum_{i=0}^n f_i x^i$ è la stessa, con la sola differenza che si lavora con funzioni convesse lineari a tratti sull'intervallo $[0, n]$.

Nella figura riportiamo come esempio il poligono di Newton della serie

$$f(x) = \sum_{i=0}^{\infty} \frac{1}{i} x^i,$$

dove abbiamo preso $p = 3$.



Elenchiamo di seguito le proprietà principali dei poligoni di Newton ma, per non allontanarci troppo dal nostro oggetto di studio, rimandiamo a [Kob84, cap. IV] per le dimostrazioni, peraltro non difficili.

**Proposizione 2.4.2** *Sia $b$ l'estremo superiore delle pendenze dei tratti del poligono di Newton di $f(x)$. Allora il raggio di convergenza di $f$ è $p^b$.*

**Proposizione 2.4.3** *Sia $\lambda$ la prima pendenza del poligono di Newton di una serie di potenze $f$, e supponiamo che il poligono di Newton di $f$ non si riduca alla sola retta di pendenza $\lambda$. Allora esiste $x \in \mathbb{C}_p$ per cui $\mathrm{ord}_p(x) = -\lambda$ e $f(x) = 0$.*

**Teorema 2.4.4 (Preparazione di Weierstraß)** *Sia $f(x)$ una serie di potenze con $f_0 = 1$ e raggio di convergenza almeno $p^\lambda$. Chiamiamo $N$ il massimo intero per cui il punto $(N, \mathrm{ord}_p(N))$ si trova su un segmento di pendenza $\leq \lambda$ del poligono di Newton (è facile vedere che un tale $N$ esiste). Allora esiste un polinomio $p(x)$ di grado $N$ ed una serie $h(x)$ convergente e mai nulla sulla palla di raggio $p^\lambda$ per cui*

$$f(x) = p(x)h(x)$$

*sulla stessa palla.*

**Dim. (sketch)** Utilizziamo un'induzione su $N$. Nel caso $N = 0$ è sufficiente verificare che $f$ non si annulla sulla palla di raggio $p^\lambda$. Questo segue subito dalla disuguaglianza triangolare.

Per il passo induttivo supponiamo per semplicità che il poligono di Newton di $f$ non contenga una semiretta. Sia $\lambda_1 \leq \lambda$ la pendenza del primo tratto del poligono di Newton di $f$. Per la Proposizione 2.4.3 troviamo $\alpha$ con $\mathrm{ord}_p(\alpha) = -\lambda_1$ e $f(\alpha) = 0$. Poniamo

$$f_1(x) = f(x) \left( \sum_{i=0}^{\infty} \frac{1}{\alpha^i} x^i \right).$$

La serie per $f_1$ converge sulla palla di raggio $p^{\lambda_1}$, e per costruzione

$$f(x) = \left(1 - \frac{x}{\alpha}\right) f_1(x).$$

Una verifica che omettiamo è che il poligono di Newton di $f$ è ottenuto da quello di $f_1$ traslato a destra di 1 e in alto di $\lambda_1$, insieme al segmento che unisce $(0,0)$ a $(1, \lambda_1)$. Ne segue che $f_1$ verifica le ipotesi del teorema con $N$ rimpiazzato da $N-1$. Applicando l'ipotesi induttiva si conclude.

□

Tutto questo può essere applicato, nel caso che ci interessa, a funzioni analitiche che si ottengono come prolungamento di polinomi esponenziali. Uno studio dettagliato di questo caso particolare porta alla seguente proposizione, che ci sarà utile in un passo del teorema del quoziente di Hadamard. Per la dimostrazione, che si riconduce al teorema di preparazione, si veda [Rum87]; noi la omettiamo perché un po' tecnica.

**Proposizione 2.4.5** *Sia dato un polinomio esponenziale a coefficienti in $\mathbb{Q}_p$, prolungato ad una funzione analitica nella forma*

$$a(x) = \sum_{i=1}^{r} A_i(x) \exp_p(\alpha_i x),$$

*e poniamo*

$$V = \min_i(\mathrm{ord}_p(\alpha_i)).$$

*Allora l'espansione in serie di potenze di $a(x)$ converge sulla palla*

$$B = \left\{ x \in \mathbb{Q}_p : \mathrm{ord}_p(x) > -V + \frac{1}{p-1} \right\}.$$

*Inoltre $a(x)$ ha solo un numero finito di zeri su $B$ ed esiste una fattorizzazione*

$$a(x) = p(x)\lambda(x),$$

*dove $p$ è un polinomio con gli stessi zeri di $a(x)$ su $B$ e $\lambda(x)$ è una funzione analitica mai nulla su $B$, data dallo sviluppo in serie*

$$\lambda(x) = 1 + \sum_{i=1}^{\infty} \lambda_i x^i,$$

*dove*

$$\mathrm{ord}_p(\lambda_i) \geq i \left( V - \frac{1}{p-1} \right).$$

## 2.5 Il teorema di Lech-Mahler-Skolem

Vogliamo usare i risultati di analisi $p$-adica per studiare gli zeri delle soluzioni di ricorrenze lineari, o equivalentemente di polinomi esponenziali. L'insieme dove un polinomio esponenziale si annulla può essere anche infinito: ad esempio se $\gamma_1, \dots, \gamma_n$ sono radici dell'unità, il polinomio esponenziale

$$p(h) = \sum_{i=1}^{n} \lambda_i \gamma_i^h$$

è una funzione periodica di $k$ per ogni scelta di costanti $\lambda_i$. Se queste costanti sono scelte il modo che $p$ abbia uno zero, allora ce ne saranno infiniti. Abbastanza sorprendentemente l'insieme degli zeri di un polinomio esponenziale non può essere un sottoinsieme qualunque di $\mathbb{N}$.

**Teorema 2.5.1 (Lech-Mahler-Skolem)** *Sia $b(k)$ un polinomio esponenziale. Allora l'insieme*

$$\{h \in \mathbb{N} : b(h) = 0\}$$

*è unione di un insieme finito e di un numero finito di progressioni aritmetiche complete.*

Per progressione aritmetica completa intendiamo un insieme della forma

$$A_{r,k} = \{n \in \mathbb{N} : n \equiv r \pmod{k}\}.$$

Il risultato generale si deduce con un argomento di specializzazione dal caso particolare in cui $b(h)$ è a coefficienti in un campo di numeri $k$. Per un survey più completo sulle ricorrenze lineari e su altri aspetti legati al teorema di Lech-Mahler-Skolem si veda [vdP89], anche se la terminologia che usiamo qui è leggermente diversa da quella di Van der Poorten.

**Dim.** Scegliamo un primo $\mathcal{P}$ di $k$, con valore assoluto associato $v$. Sia dato

$$b(h) = \sum_{i=1}^{m} B_i(h) \beta_i^h.$$

Scartando un numero finito di primi $\mathcal{P}$ possiamo supporre che $|B_{i,j}|_v \leq 1$ per ogni coefficiente $B_{i,j}$ dei $B_i$, e che $|\beta_i|_v = 1$ per ogni $i$. In questo modo avremo $|b(h)|_v \leq 1$ per ogni $h$. Per il Teorema 1.2.7 possiamo scegliere $\mathcal{P}$ di grado 1 su $\mathbb{Q}$. Cerchiamo di estendere $b(h)$ ad una funzione analitica su un disco in $k_v$.

Indichiamo con $p$ il primo razionale sotto $\mathcal{P}$ e con $q = p - 1$. Scelto $r$ intero nell'intervallo $0 \leq r \leq q-1$ possiamo interpolare $b(h)$ sulla progressione aritmetica $h = r + t(p-1) = r + tq$. Sia $\mathcal{O}_v$ l'anello degli elementi di $k$ $v$-interi, cioè

$$\mathcal{O}_v = \{x \in k : |x|_v \leq 1\}.$$

Per come abbiamo scelto $\mathcal{P}$, ciascun $\beta_i$ è invertibile in $\mathcal{O}_v$, e di conseguenza

$$\beta_i^q \equiv 1 \pmod{\mathcal{P}}.$$

Questo fa sì che la serie del logaritmo $p$-adico converga in $\beta_i^q$ ad un elemento

$$\omega_i = \log_p \beta_i = \sum_{j=1}^{\infty} (-1)^j \frac{(\beta_i^q - 1)^j}{j},$$

e $\omega_i \in p\,\mathcal{O}_v$. Viceversa per $t$ intero la serie esponenziale converge in $\omega_i t$ e possiamo dunque ricostruire

$$\beta_i^{qt} = \exp_p(\omega_i t) = \sum_{j=0}^{\infty} \frac{\omega_i^j t^j}{t!}.$$

Perciò per $h = r + tq$ troviamo uno sviluppo in serie di potenze

$$b(h) = b_{v,r}(t) = \sum_i B_i(r + tq)\beta_i^r \exp_p(\omega_i t) = \sum_{j=0}^{\infty} b_{v,r,j} t^j.$$

Se $b(h)$ ha solo un numero finito di zeri non abbiamo niente da dimostrare. Altrimenti per alcune scelte di $r$ la funzione analitica $b_{v,r}$ dovrà avere infiniti zeri su $\mathcal{O}_v$, che è compatto. Come nel caso dell'analisi complessa si dimostra che una funzione analitica con infiniti zeri su un disco chiuso deve essere identicamente nulla. Questo significa che $b(h) = 0$ per tutti gli $h$ nella progressione aritmetica completa $h = r + tq$.

Questo vale per ciascun $r$ per cui $b_{v,r}$ ha infiniti zeri interi. Per le altre scelte di $r$ otteniamo un numero finito di zeri per $b(h)$, e il teorema è dimostrato.

$\square$

# Capitolo 3

# Il teorema del quoziente

L'opinione pubblica per molte persone è solo una scusa per non averne una propria.

*Anatole France*

## 3.1 Introduzione

Il primo problema che affrontiamo è quello di determinare quando sia possibile effettuare la divisione nell'anello $\mathcal{H}(K)$, dove $K$ è un campo di caratteristica 0. Siano quindi $f$ e $g$ due funzioni razionali con serie di Taylor $\sum b_k x^k$ e $\sum c_k x^k$ rispettivamente. Quello che cerchiamo è una funzione razionale con serie di Taylor $\sum a_k x^k$ per cui $a_k b_k = c_k$ per tutti i $k$. Per prima cosa possiamo utilizzare i risultati della Sezione 2.1 per ricondurci al caso in cui i termini $b_k$ e $c_k$ siano dati da polinomi esponenziali.

Il primo problema si presenta nel caso in cui uno o più termini $b_k$ si annullino. Vediamo come applicare il teorema di Lech-Mahler-Skolem al nostro problema. Scegliamo $N$ abbastanza grande, in modo che l'insieme dei $k$ per cui $b_k = 0$ sia unione di un insieme finito e di progressioni aritmetiche mod$N$. Dato $r < N$ le successioni $b_{r+kN}$ e $c_{r+kN}$ sono ancora date da polinomi esponenziali. Inoltre per ogni $r$ la successione $b_{r+kN}$ conterrà solo un numero finito di elementi nulli oppure solo un numero finito di elementi non nulli. Nel primo caso possiamo cercare di determinare se la successione $a_{r+kN} = \frac{c_{r+kN}}{b_{r+kN}}$, definita per $k$ abbastanza grande, provenga o meno da un polinomio esponenziale. Nel secondo caso non è possibile definire la successione dei quozienti.

Decidiamo allora di porre il problema in questi termini: cerchiamo una funzione razionale con serie di Taylor $\sum a_k x^k$ per cui $a_k b_k = c_k$ per tutti i $k$ per cui $b_k \neq 0$. In questo modo il teorema di Lech-Mahler-Skolem ci permette di ricondurci al caso in cui $b_k \neq 0$ per ogni $k$. Infatti come sopra ragioniamo su sottosuccessioni della forma $b_{r+kN}$. Se $r$ è tale che $b_{r+kN} = 0$ per tutti i $k$ tranne un numero finito possiamo scegliere $a_{r+kN}$ qualunque, purché sia generata da un polinomio esponenziale e l'uguaglianza $a_{r+kN} b_{r+kN} = c_{r+kN}$ sia valida per i valori piccoli di $k$ (ad esempio possiamo prendere $a_{k+r_N} = p(k)$ per un polinomio opportuno $p$). Dunque rimane il problema di capire cosa succede quando $b_{r+kN}$ assume solo numero finito di volte il valore 0. Se per un certo $r$ la successione $a_{r+k_N}$ non è data un polinomio esponenziale, lo stesso vale per la successione $a_n$ che si ottiene unendo le $a_{r+kN}$ al variare di $r < N$. Supponiamo invece che per ciascun $r$ la successione $a_{r+kN}$ sia generata dal polinomio esponenziale $p_r(k)$. Il polinomio esponenziale

$$\theta(n) = \frac{1}{N} \sum_{i=1}^{N} \zeta_N^n$$

assume valore 1 per $N|n$ e 0 altrimenti. Perciò

$$a_n = \sum_{r=0}^{N-1} \theta(n-r) p_r(n-r)$$

è una successione generata da un polinomio esponenziale.

In conclusione ci possiamo ricondurre a studiare il problema nel caso in cui $b_k = 0$ solo numero finito di volte. D'altra parte la Proposizione (2.2.2) ci dice che modificare un numero finito di coefficienti di una serie non modifica il fatto che questa sia razionale o meno. Perciò non è restrittivo studiare il caso in cui i $b_k$ non siano mai nulli. Scopo di questo capitolo è di dimostrare il seguente teorema, dovuto a Van der Poorten ([vdP88]).

**Teorema 3.1.1 (del quoziente di Hadamard)** *Sia $K$ un campo di caratteristica 0 e siano $\sum b_k x^k$ e $\sum c_k x^k$ le serie di Taylor di due funzioni razionali. Supponiamo che $b_k \neq 0$ per ogni $k$, e poniamo $a_k = c_k/b_k$. Allora $\sum a_k x^k$ è razionale se e solo se esiste un anello $A$ finitamente generato su $\mathbb{Z}$ contenente tutti gli $a_k$.*

**Corollario 3.1.2** *Sia $K$ un campo di caratteristica 0 e siano $\sum b_k x^k$ e $\sum c_k x^k$ le serie di Taylor di due funzioni razionali. Se $b_k \neq 0$ poniamo $a_k = c_k/b_k$. Allora esiste una serie $\sum \widetilde{a}_k x^k$ che è razionale ed è tale che $\widetilde{a}_k = a_k$ ogni volta che $b_k \neq 0$ se e solo se esiste un anello $A$ finitamente generato su $\mathbb{Z}$ contenente tutti gli $a_k$.*

In realtà la dimostrazione di Van der Poorten segue le linee di un argomento proposto da Pourchet in [Pou79]; noi seguiremo l'esposizione di Rumely in [Rum87]. Osserviamo che il fatto che tutti gli $a_k$ giacciano in un anello finitamente generato è banalmente necessaria per la razionalità. Infatti se per $k$ grande si ha

$$a_k = \sum_{i=1}^{n} A_i(k) \alpha_i^k,$$

allora gli $a_k$ appartengono all'anello generato dagli $\alpha_i$ e dai coefficienti degli $A_i$. D'altra parte questa condizione non è automaticamente verificata, come mostra il prossimo esempio.

**Esempio**

Prendiamo $b_k = k$ e $c_k = 1$. Queste scelte danno luogo alle serie

$$\sum_{k=1}^{\infty} k x^k = \frac{x}{(1-x)^2} \qquad \text{e} \qquad \sum_{k=1}^{\infty} x^k = \frac{x}{1-x}.$$

Tuttavia il quoziente di Hadamard è dato dalla serie

$$\sum_{k=1}^{\infty} \frac{1}{k} x^k = -\log(1-x),$$

che non è una funzione razionale.

## 3.2 Il teorema di Pólya-Cantor

Il primo passo per arrivare al teorema del quoziente è quello di trattare il caso in cui i valori $b_k$ sono espressi da un polinomio, invece di un polinomio esponenziale. Il risultato di questa sezione è stato dimostrato molto tempo prima del caso generale, dovuto a Pourchet e Van der Poorten, da parte di Cantor ([Can69]), dopo vari risultati parziali a partire dagli studi di Pólya.

**Teorema 3.2.1 (Pólya-Cantor)** *Sia $k$ un campo di numeri, $A \subset k$ un anello finitamente generato. Sia $\{a_k\}$ una successione di elementi di $A$ e $p(x) \in k[x]$. Se la serie $\sum_{j=0}^{\infty} p(j)a_j x^j$ è razionale, anche $\sum_{j=0}^{\infty} a_j x^j$ lo è.*

**Dim.** Un'induzione sul grado di $p$ ci permette di ricondurci al caso in cui $p(x) = x - \vartheta$, con $\vartheta$ algebrico. Per la proposizione (2.2.2), se $j$ è abbastanza grande, possiamo scrivere

$$p(j)a_j = \sum_{i=1}^{m} B_i(j)\alpha_i^j,$$

per opportuni polinomi $B_i \in \overline{k}[x]$ e $\alpha_i \in \overline{k}$. A meno di espandere $k$ possiamo supporre che i $B_i$ siano a coefficienti in $k$ e che $\alpha_i \in k$.

Il teorema di Чеботарев ci permette di trovare infiniti primi $p$ di $\mathbb{Z}$ che si spezzano totalmente in $k(\vartheta)$. Prendiamo uno di questi primi $p$, e sia $\mathcal{P}$ un primo di $k(\vartheta)$ sopra di esso. Per la scelta di $p$ troviamo $h \in \mathbb{Z}$, $h \equiv \vartheta \pmod{\mathcal{P}}$. Di conseguenza per ogni $j \in \mathbb{Z}$ si ha

$$h + jp \equiv \vartheta \pmod{\mathcal{P}}.$$

Sia $r \in k$ tale che $rA$ sia contenuto nell'anello degli interi di $k(\theta)$. Allora

$$r(h + jp - \vartheta)a_{h+jp} = r\sum_{i=1}^{m} B_i(h + jp)\alpha_i^{h+jp} \equiv r\sum_{i=1}^{m} B_i(\vartheta)\alpha_i^{h+j} \pmod{\mathcal{P}}.$$

Scartando un numero finito di primi $p$ possiamo supporre che $\mathcal{P}$ non divida $r$, gli $\alpha_i$ e le differenze $\alpha_i - \alpha_l$. Poiché gli elementi $ra_{h+jp}$ sono interi otteniamo, per ogni $j \in \mathbb{N}$

$$\sum_{i=1}^{m} rB_i(\vartheta)\alpha_i^{h+j} \equiv 0 \pmod{\mathcal{P}}.$$

Visto che il determinante di Vandermonde $\det(\alpha_i^j)1 \leq i, j \leq m$ non è nullo mod$\mathcal{P}$ ricaviamo

$$rB_i(\vartheta)\alpha_i^{h+j} \equiv 0 \pmod{\mathcal{P}},$$

cioè $B_i(\vartheta) \equiv 0 \pmod{\mathcal{P}}$. Poiché questo vale per infiniti primi $\mathcal{P}$ si deve avere $B_i(\vartheta) = 0$. Possiamo dunque scrivere $B_i(x) = (x - \vartheta)A_i(x)$ per opportuni polinomi $A_i$ e ricavare

$$a_j = \sum_{i=1}^{m} A_i(j)\alpha_i^j,$$

per $j$ grande.

□

## 3.3 La strategia

Lo scopo delle prossime sezioni è di arrivare ad una dimostrazione del Teorema (3.1.1). In realtà in questo capitolo ci limiteremo a considerare il caso di un campo di numeri $k$. Il teorema generale si può dedurre da questo caso tramite un argomento di specializzazione, che presenteremo nel capitolo 5.

A meno di ingrandire $k$ supponiamo innanzitutto che $k/\mathbb{Q}$ sia di Galois. Siano dunque $c_k$ e $b_k$ due successioni espresse da polinomi esponenziali, supponiamo $b_k \neq 0$ e poniamo $a_k = \frac{c_k}{b_k}$. Van der Poorten dimostra che esiste un polinomio $f \in \overline{\mathbb{Q}}$ tale che $f(k)a_k$ sia soluzione di una ricorrenza lineare, e da questo fatto si conclude per il teorema di Pólya-Cantor. L'idea è di mostrare che i determinanti $K_h(a)$ si annullano per $h$ sufficientemente grande, e per far questo si usa la formula del prodotto. Infatti sappiamo che se $K_h(a) \neq 0$

$$\prod_{v \in M_k} |K_h(a)|^{\varepsilon(v)} = 1.$$

Quindi quello di cui abbiamo bisogno è stimare $|K_h(a)|$ per diversi valori assoluti, in modo da trovare una contraddizione con la formula del prodotto.

Sfruttando il fatto che $b_h$ e $c_h$ sono espressi da polinomi esponenziali si ricava una disuguaglianza del tipo

$$|a_h| = |a_h|_v \leq M_v \rho_v^h,$$

per opportune costanti dipendenti dal valore assoluto. Da queste disuguaglianze otteniamo stime per i determinanti $|K_h(a)|$. Chiaramente ci sarà solo un numero finito di valori assoluti per cui $|a_h|$ può essere maggiore di 1.

Isoliamo allora un insieme finito di valori assoluti $T \subset M_k$ sui quali non riusciamo ad ottenere buone stime. Mettiamo in $T$ tutti i valori assoluti archimedei e tutti quelli per cui $|a_h| > 1$ per qualche $h$. Possiamo fare questo perché per ipotesi gli $a_h$ stanno dentro un anello finitamente generato. Scriviamo

$$b_h = \sum_{i=1}^{m} B_i(h)\beta_i^h, \qquad c_h = \sum_{i=1}^{n} C_i(h)\gamma_i^h.$$

Possiamo ingrandire $T$ in modo che per $|\cdot| \notin T$ si abbia $|\beta_i| = 1$, $|\gamma_j| = 1$ e i coefficienti dei $B_i$ e dei $C_j$ stiano nell'anello $\{x : |x| \leq 1\}$. Infine se $p$ è ramificato in $k$ aggiungiamo a $T$ il valore assoluto $\mathcal{P}$-adico per ogni primo $\mathcal{P}$ sopra $p$.

Per ottenere una contraddizione con la formula del prodotto abbiamo bisogno di compensare l'insieme $T$, sul quale le stime sono meno buone, con un altro insieme finito di valori assoluti per i quali otteniamo stime migliori. Scegliamo un primo $\mathcal{P}$ sopra $p$, con valore assoluto associato $v$, e sia $q = N(\mathcal{P}) - 1$. Preso $h$ sulla progressione aritmetica $h = r + tq$ i termini $b_h$ si possono ottenere come

$$b_h = b_{v,r}(t) = \sum_i B_i(r + tq)\beta_i^r \exp_p(t \log_p(\beta_i^q)), \tag{3.3.1}$$

e similmente per i termini $c_h$. Questo sviluppo in serie di potenze converge in un disco in $K_{\mathcal{P}}$ dato da

$$\mathrm{ord}_v(x) > -\left(1 - \frac{1}{p-1}\right).$$

Il vantaggio di questa interpolazione con una funzione analitica è dato dal fatto che per l'analisi $p$-adica vale l'analogo del teorema di Cauchy-Hadamard. In particolare se una serie di potenze $g(t) = \sum r_i t^i$ converge in un disco $\mathrm{ord}_v(t) > -\lambda$, allora

$$\liminf \left(\frac{1}{i} v(r_i)\right) \geq \lambda.$$

Per vedere come questo sia utile per stimare $|K_h(a)|$ introduciamo l'operatore differenza $\Delta$, dato da

$$(\Delta g)(t) = g(t+1) - g(t).$$

Possiamo vedere l'effetto di $\Delta$ sui singoli monomi:

$$\Delta^k t^j = \begin{cases} 0 & \text{se } j < k \\ k! & \text{se } j = k \\ k! p(t) & \text{se } j > k \end{cases}$$

dove $p(t) \in \mathbb{Z}[t]$. Di conseguenza se $g$ è a coefficienti $|\cdot|$ interi, cioè nell'anello $\{|x| \leq 1\}$, e $k$ è abbastanza grande, allora $(\Delta^k g)(t)$ sarà divisibile per una grande potenza di $\mathcal{P}$. Più precisamente

$$\mathrm{ord}_v((\Delta^k g)(t)) \approx k\left(\lambda + \frac{1}{p-1}\right).$$

Applichiamo tutto questo al problema di stimare $|K_h(a)|$. L'idea è di utilizzare operazioni di riga e colonna, che lasciano invariato il determinante. Se sapessimo che $a_h$ è dato da una funzione analitica simile a (3.3.1) per $h = r + tq$, potremmo ragionare come segue. Nel paragrafo precedente abbiamo visto che applicare l'operatore $\Delta$ ad una serie $g(t)$ permette di estrarre potenze di $\mathcal{P}$. Scegliamo $g(t) = a_{v,r}(t)$. Questo ci dice che prendere le differenze delle colonne della matrice

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_h \\ a_1 & a_2 & \cdots & a_{h+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_h & a_{h+1} & \cdots & a_{2h} \end{pmatrix}$$

ad intervalli di $q$ ci permette di mostrare che $K_h(a)$ è divisibile per una grande potenza di $\mathcal{P}$, e dunque avere una buona maggiorazione per $|K_h(a)|$.

Tutto questo non funziona direttamente perché siamo in grado di interpolare con funzioni analitiche solo i termini $b_h$ e $c_h$, ma non gli $a_h$. Poniamo allora

$$a_{v,r}(t) = \frac{c_{v,r}(t)}{b_{v,r}(t)}.$$

Non abbiamo un buon raggio di convergenza per $a_{v,r}(t)$, perché $b_{v,r}(t)$ potrebbe annullarsi. Tuttavia possiamo mostrare che $b_{v,r}(t)$ ha solo un numero finito di zeri, e dunque prendere un polinomio $Q_{v,r}(t)$ con gli stessi zeri. In questo modo possiamo interpolare $Q_{v,r}(t) a_{v,r}(t)$; se poi poniamo

$$Q_v(t) = \prod_{r=0}^{q-1} Q_{v,r}(t)$$

allora $Q_v(h)a_h$ può essere interpolato da una funzione analitica con un buon raggio di convergenza su ogni progressione aritmetica $h = r + tq$.

Questo ci dà buone stime per $|K_h(Q_v a)|$, ma il problema è che cambiando valore assoluto cambia il polinomio $Q_v(t)$. Noi vogliamo lavorare con un insieme finito di valori assoluti, per cui potremmo limitarci a prendere il prodotto di questi, ma l'ostacolo è che $Q_v(t) \in k_{\mathcal{P}}[t]$. Dobbiamo allora approssimare tutti i polinomi $Q_v(t)$ con un polinomio $Q(t) \in k[t]$.

Una difficoltà sorge con le stime per i valori assoluti in $T$. Infatti se i coefficienti di $Q$ sono troppo grandi le stime di $K_h(Qa)$ ai valori assoluti archimedei possono essere sensibilmente peggiori di quelle di $K_h(a)$. Quindi dobbiamo sostituire a $Q$ un suo multiplo $f$ i cui coefficienti siano abbastanza piccoli da non creare problemi.

Infine un'altra difficoltà è data dal fatto che $Q(t)$ è solo un'approssimazione dei $Q_v(t)$, perciò quello che si riesce a mostrare è che $K_h(fa) = 0$ non per ogni $h$ grande, ma solo in un intervallo $H_0 \leq h \leq H$. Tuttavia questo è sufficiente a vedere che la successione $f(h)a_h$ soddisfa una ricorrenza lineare. Infine il teorema di Pólya-Cantor permette di concludere.

## 3.4 I determinanti di Kronecker-Hankel

Come abbiamo visto nella sezione precedente, quello che dobbiamo fare è maggiorare $|K_h(a)|$ al variare del valore assoluto. In realtà, in vista delle modifiche che dovremo fare nella parte finale, è meglio considerare fin da subito $|K_h(fa)|$ per un certo polinomio $f$, che ancora dobbiamo scegliere. Abbiamo suddiviso $M_k$ in tre sottoinsiemi. C'è un primo sottoinsieme $T$ sul quale non otterremo buone stime. Per compensare considereremo un altro insieme finito $S$ sul quale otterremo disuguaglianze migliori di quelle generiche. Infine, per i restanti valori assoluti, avremo $|f(h)a_h| \leq 1$ e dunque semplicemente $K_h(fa) \leq 1$.

Per maggiorare la grandezza del determinante in termini delle entrate della matrice è utile la disuguaglianza di Hadamard. Dato un valore assoluto $|\cdot|$ su $k$ e un vettore $\mathbf{v} = (v_1, \ldots, v_n) \in k^n$ poniamo

$$|\mathbf{v}| = \sqrt{\sum_{i=1}^{n} |v_i|^2}.$$

**Proposizione 3.4.1 (Disuguaglianza di Hadamard)** *Sia $M$ una matrice $n \times n$ a coefficienti in $k$ e $|\cdot|$ un valore assoluto. Se indichiamo con $C_1, \ldots, C_n$ le colonne di $M$, allora*

$$|\det M| \leq \prod_{i=1}^{n} |C_i|.$$

**Dim.** Ci limitiamo a dimostrare la disuguaglianza per un valore assoluto archimedeo, che è poi il caso che useremo. Se $v$ è archimedeo sappiamo che esiste un'immersione

$$\sigma : k \longmapsto \mathbb{C}$$

tale che $|x|_v = |\sigma(x)|_{st}$ per ogni $x \in k$. Dunque ci basta dimostrare la disuguaglianza per il valore assoluto standard su $\mathbb{C}$.

Indichiamo con $(\cdot\,|\,\cdot)$ il prodotto hermitiano standard su $\mathbb{C}^n$. Applichiamo il procedimento di ortogonalizzazione di Gram-Schmidt alle colonne. Ad ogni passo il determinante della matrice resta invariato, poiché stiamo modificando una colonna aggiungendo un multiplo di un'altra. Invece il membro destro diminuisce. Infatti quando rimpiazziamo un vettore $\mathbf{v}$ con $\mathbf{v}' = \mathbf{v} - \frac{(\mathbf{v}|\mathbf{w})}{|\mathbf{w}|^2}\mathbf{w}$ otteniamo

$$|\mathbf{v}'|^2 = (\mathbf{v}'|\mathbf{v}) = |\mathbf{v}|^2 - \frac{|(\mathbf{v}|\mathbf{w})|^2}{|\mathbf{w}|^2} \leq |\mathbf{v}|^2.$$

Perciò possiamo limitarci a dimostrare la disuguaglianza nell'ipotesi che le colonne siano ortogonali. In questa ipotesi $MM^*$ è diagonale, con sulla diagonale gli elementi $(C_i|C_i)$, perciò

$$|\det M|^2 = |\det MM^*| = \prod_{i=1}^{n} |(C_i|C_i)| = \prod_{i=1}^{n} |C_i|^2.$$

□

Passiamo ora alle maggiorazioni vere e proprie, innanzitutto per $|a_h|_v$. Non è difficile stimare dall'alto i termini $|b_h|_v$ e $|c_h|_v$: essendo dati da polinomi esponenziali possiamo trovare costanti $I_v$, $J_v$, $\phi_v$ e $\psi_v$ per cui

$$|b_h|_v \leq I_v \phi_v^h; \qquad |c_h|_v \leq J_v \psi_v^h.$$

La stima per $|a_h|_v$ viene dalla formula del prodotto. Infatti possiamo prendere tutte le costanti uguali a 1 se $v \notin T$, e dunque

$$|b_h|_v^{\varepsilon(v)} = \prod_{w \neq v} |b_h|_w^{-\varepsilon(w)} \geq \prod_{\substack{w \neq v \\ w \in T}} (I_w \phi_w^h)^{-\varepsilon(w)}.$$

Di conseguenza

$$|a_h|_v \leq J_v \psi_v^h \prod_{\substack{w \neq v \\ w \in T}} (I_w \phi_w^h)^{\varepsilon(w)/\varepsilon(v)} = M_v \rho_v^h.$$

Sia $f \in \mathcal{R}[x]$, dove $\mathcal{R}$ è l'anello degli interi di $k$. Fissato un valore assoluto $v$, indichiamo $N = \deg f$ e supponiamo che $|f_i|_v \leq D_v$ per ogni coefficiente $f_i$ di $f(x)$. Sotto queste ipotesi

**Proposizione 3.4.2** *Se $v$ è un valore assoluto nonarchimedeo, allora*

$$|K_h(fa)|_v \leq M_v^{h+1} \rho_v^{\frac{3}{2}(h+1)^2}.$$

*Se invece $v$ è archimedeo, allora*

$$|K_h(fa)|_v \leq \left( \frac{D_v M_v (N+1)}{\sqrt{\rho_v^2 - 1}} \right)^{(h+1)} (2h)^{N(h+1)} \rho_v^{\frac{3}{2}(h+1)^2}.$$

**Dim.** Vediamo prima il caso in cui $v$ sia nonarchimedeo. Poiché il determinante è una somma alternata di prodotti di termini della matrice, ci basta verificare la disuguaglianza per ciascuno dei prodotti. Un'entrata nella colonna $C_i$ ha valore assoluto limitato da $M_v \rho_v^{(h+i)}$. Perciò il valore assoluto di ognuno dei prodotti si maggiora con

$$\prod_{i=0}^{h} M_v \rho_v^{(h+i)} = M_v^{h+1} \rho_v^{h(h+1)} \rho_v^{\frac{h(h+1)}{2}} \leq M_v^{h+1} \rho_v^{\frac{3}{2}(h+1)^2}.$$

Passiamo al caso archimedeo. Se $0 \leq k \leq 2h$ possiamo stimare il valore assoluto di $f(k)$:

$$|f(k)|_v \leq (N+1)D_v k^N \leq (N+1)D_v(2h)^N.$$

Indichiamo con $C_i$ l'$i$-esima colonna della matrice. Ricaviamo

$$|C_i|_v \leq (N+1)D_v(2h)^N \sqrt{\sum_{j=0}^{h}(M_v \rho_v^{i+j})^2} \leq \frac{(N+1)D_v(2h)^N M_v}{\sqrt{\rho_v^2 - 1}} \rho_v^{i+j+1}.$$

La tesi segue allora dalla disuguaglianza di Hadamard.

□

## 3.5 Stime migliori su un insieme finito di primi

Adesso sceglieremo un insieme finito $S$ di primi di $k$ che useremo per compensare le maggiorazioni fatte su $T$. Abbiamo bisogno di un risultato di teoria analitica dei numeri sulla distribuzione degli ideali primi in campi di numeri ([Nar90, cap. 7]).

**Teorema 3.5.1 (degli ideali primi)** *Sia $k$ un campo di numeri e indichiamo con $\pi_k(x)$ il numero di ideali primi di $k$ di norma al più $x$. Allora*

$$\pi_k(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

*La stessa stima asintotica vale se ci limitiamo a contare i primi di grado d'inerzia 1 su $\mathbb{Q}$.*

Vogliamo usare questo risultato per arrivare al

**Lemma 3.5.2** *Il prodotto*

$$\prod_{\mathcal{P} \text{ primo}} N(\mathcal{P})^{\frac{1}{N(\mathcal{P})-1}} \tag{3.5.1}$$

*è divergente, anche se limitiamo il prodotto ai primi $\mathcal{P}$ di grado 1 su $\mathbb{Q}$.*

**Dim.** Ci basta vedere che

$$\sum_{N(\mathcal{P}) \leq x} \frac{\log N(\mathcal{P})}{N(\mathcal{P}) - 1} = \log x + O(1). \tag{3.5.2}$$

A questo scopo definiamo

$$\Psi_k(x) = \sum_{\substack{I = \mathcal{P}^m \\ N(I) \leq x}} \log N(\mathcal{P}).$$

Il teorema degli ideali primi ci dice che $\Psi_k(x) = x + O(xe^{-c\sqrt{\log x}})$. Dunque se $x$ non è intero, integrando per parti troviamo

$$\sum_{\substack{I = \mathcal{P}^m \\ N(I) \leq x}} \frac{\log N(\mathcal{P})}{N(I)} = \int_1^x \frac{1}{t} d\Psi_k(t) = \left.\frac{\Psi_k(t)}{t}\right|_1^x + \int_1^x \frac{1}{t^2}\Psi_k(t)dt =$$

$$= O(1) + \int_1^x \frac{1}{t}\,dt + O\left(\int_1^x \frac{e^{-c\sqrt{\log t}}}{t}\,dt\right) = \log x + O(1).$$

D'altra parte la stessa somma fatta sulle potenze di primi con esponente maggiore di 1 converge:

$$\sum_{I=\mathcal{P}^m,\, m\geq 2} \frac{\log N(\mathcal{P})}{N(I)} \leq [k:\mathbb{Q}] \sum_p \frac{\log p}{p^2-1} < +\infty.$$

Perciò

$$\sum_{N(\mathcal{P})\leq x} \frac{\log N(\mathcal{P})}{N(\mathcal{P})} = \log x + O(1). \tag{3.5.3}$$

Similmente abbiamo

$$\begin{aligned}\sum_{\mathcal{P}\text{ primo}} \log N(\mathcal{P}) \left(\frac{1}{N(\mathcal{P})-1} - \frac{1}{N(\mathcal{P})}\right) &\leq \sum_{\mathcal{P}\text{ primo}} \frac{\log N(\mathcal{P})}{(N(\mathcal{P})-1)^2} \leq \\ &\leq [k:\mathbb{Q}] \sum_{n=2}^{\infty} \frac{\log n}{(n-1)^2} < +\infty.\end{aligned} \tag{3.5.4}$$

Per differenza tra la (3.5.4) e la (3.5.3) si trova la (3.5.2). Il risultato più forte che il prodotto diverge anche se ristretto ai primi $\mathcal{P}$ per cui $f(\mathcal{P}|p) = 1$, dove $(p) = P \cap \mathbb{Z}$, si ottiene allo stesso modo. È sufficiente restringere tutte le somme a questo insieme di primi ed utilizzare la seconda affermazione del teorema degli ideali primi.

$\square$

Scegliamo allora l'insieme $S$ nel seguente modo. Richiediamo che $S$ sia disgiunto da $T$ e che contenga solamente primi con grado d'inerzia 1 su $\mathbb{Q}$. per ogni primo $p$ scegliamo al più un primo $\mathcal{P}$ sopra $p$. Chiamiamo

$$r = \prod_{v\in T} \rho_v^{\frac{3}{2}\varepsilon(v)}.$$

Per il Lemma (3.5.2) possiamo prendere $S$ abbastanza grande, in modo che, posto

$$R = \prod_{v\in S} N(\mathcal{P}_v)^{\frac{1}{N(\mathcal{P}_v)-1}},$$

si abbia $R > r$. Chiaramente possiamo limitarci a scegliere al più un primo sopra ciascun primo razionale. Infatti sopra un primo $p$ troviamo al massimo $[k:\mathbb{Q}]$ primi $\mathcal{P}_i$di $k$ con $f(\mathcal{P}_i|p) = 1$, e per ciascuno di questi $N(\mathcal{P}_i) = p$. Pertanto il prodotto (3.5.1) diverge anche se prendiamo un solo primo sopra ciascun $p \in \mathbb{Z}$.

Sia $\mathcal{P}$ un primo con valore assoluto associato $v \in S$ e $p$ il primo razionale sotto di esso. Come per il teorema di Lech-Mahler-Skolem interpoliamo $b_h$ e $c_h$ sulla progressione aritmetica $h = r + t(p-1) = r + tq$. Sia $\mathcal{O}_v$ l'anello degli elementi di $k$ $v$-interi, cioè

$$\mathcal{O}_v = \{x \in k : |x|_v \leq 1\}.$$

Per ipotesi abbiamo un'espansione

$$b_h = \sum_{i=1}^{m} B_i(h)\beta_i^h, \qquad c_h = \sum_{i=1}^{n} C_i(h)\gamma_i^h.$$

Per la scelta che abbiamo fatto di $T$, che è disgiunto da $S$, ciascun $\beta_i$ è invertibile in $\mathcal{O}_v$, e i polinomi $B_i$ sono a coefficienti in $\mathcal{O}_v$. Poiché

$$\beta_i^q \equiv 1 \pmod{\mathcal{P}},$$

la serie del logaritmo $p$-adico converge in $\beta_i^q$ ad un elemento

$$\omega_i = \log_p \beta_i = \sum_{j=1}^{\infty} (-1)^j \frac{(\beta_i^q - 1)^j}{j},$$

e $\omega_i \in p\,\mathcal{O}_v$. Similmente per $t$ intero la serie esponenziale converge in $\omega_i t$ e possiamo dunque ricostruire

$$\beta_i^{qt} = \exp_p(\omega_i t) = \sum_{j=0}^{\infty} \frac{\omega_i^j t^j}{t!}.$$

Perciò per $h = r + tq$ troviamo uno sviluppo in serie di potenze

$$b_h = b_{v,r}(t) = \sum_i B_i(r+tq)\beta_i^r \exp_p(\omega_i t) = \sum_{j=0}^{\infty} b_{v,r,j} t^j,$$

e uno sviluppo analogo varrà anche per i termini $c_h$.

La Proposizione 2.4.5 ci permette di ottenere fattorizzazioni della forma

$$\begin{aligned} b_{v,r}(t) &= Q_{v,r}(t)\tau_{v,r}(t) \\ c_{v,r}(t) &= P_{v,r}(t)\kappa_{v,r}(t) \end{aligned}$$

per ciascun $r$ compreso tra 0 e $q-1$, valide per $t$ nel disco $\mathrm{ord}_v(t) > -1 + \frac{1}{q}$. Poiché $b_{v,r}$ e $c_{v,r}$ sono a coefficienti in $\mathcal{O}_v$, anche $Q_{v,r}$ e $P_{v,r}$ lo sono.

A questo punto otteniamo l'interpolazione cercata: poniamo

$$\begin{aligned} Q_v(h) &= \prod_{r=0}^{q-1} Q_{v,r}\left(\frac{h-r}{q}\right) \\ \lambda_{v,r}(t) &= \frac{\kappa_{v,r}(t)}{\tau_{v,r}(t)}. \end{aligned}$$

Poiché $q \equiv -1 \pmod{p}$ il polinomio $Q_v(h) \in \mathcal{O}_v[h]$. Inoltre abbiamo uno sviluppo in serie

$$\lambda_{v,r}(t) = \sum_{j=0}^{\infty} \lambda_{v,r,j} t^j$$

ottenuto per divisione dalle serie di $\kappa_{v,r}(t)$ e di $\tau_{v,r}(t)$. Effettuando la divisione si verifica che

$$\begin{aligned} \lambda_{v,r,0} &= 1 \\ \mathrm{ord}_v(\lambda_{v,r,j}) &\geq j\left(1 - \frac{1}{p-1}\right). \end{aligned} \tag{3.5.5}$$

Sulla progressione aritmetica $h = r + tq$ vale l'uguaglianza

$$Q_v(r+tq)a_{r+tq} = \prod_{s \neq r} Q_{v,s}\left(t + \frac{r-s}{q}\right) P_{v,r}(t)\lambda_{v,r}(t). \tag{3.5.6}$$

Vogliamo usare questa proprietà per ottenere una buona maggiorazione per i determinanti $|K_h(Q_v a)|_v$. Come abbiamo accennato nella sezione 3.3, poiché dobbiamo lavorare con più di un valore assoluto conviene sostituire il polinomio $Q_v(t)$ con un polinomio $f(t) \in \mathcal{R}[t]$ $v$-adicamente vicino ad un multiplo di $Q_v(t)$.

**Lemma 3.5.3** *Sia $f(t) \in \mathcal{R}[t]$, e supponiamo che esista $F_v(t) \in \mathcal{O}[t]$ tale che*

$$f(h) \equiv F_v(h)Q_v(h) \pmod{\mathcal{P}^{\lceil \frac{2H}{q} \rceil}\mathcal{O}_v}$$

*per un certo $H$. Sia $N = \deg f$ e $h \leq H$; allora esiste una costante $L_v$ dipendente da $v$ e dalla successione $(a_k)$ tale che*

$$\mathrm{ord}_v(K_h(fa)) \geq \frac{(h+1)^2}{q} - 2(h+1)(q+1)(N + L_v + 2 + \log H).$$

**Dim.** Usando l'uguaglianza (3.5.6) ricaviamo

$$f(r+tq)a_{r+tq} \equiv F_v(r+tq)Q_v(r+tq)a_{r+tq} \equiv G_{v,r}(t)\lambda_{v,r}(t) \pmod{\mathcal{P}^{\lceil \frac{2H}{q} \rceil}},$$

dove $G_{v,r}(t) \in \mathcal{O}[t]$. Poniamo

$$L_v = \max_r(\deg P_{v,r}).$$

Allora possiamo scegliere $G_{v,r}(t)$ in modo che $\deg G_{v,r} \leq N + L_v$. Infatti mod $\mathcal{P}^{\lceil \frac{2H}{q} \rceil}$ abbiamo

$$\deg F_v + \sum_{r=0}^{q-1} \deg Q_{v,r} = \deg(Q_v F_v) \leq N,$$

e $G_{v,r}$ è un prodotto di termini $Q_{v,s}$ per $s \neq r$ con $F_v$.

Indichiamo con $\Delta_q$ l'operatore differenza a passi di $q$, dato da

$$(\Delta_q g)(t) = g(t+q) - g(t).$$

Vogliamo arrivare innanzitutto alla disuguaglianza

$$\mathrm{ord}_v(\Delta_q^k f(h)a_h) \geq \max\{0, k - N - L_v - 2\log H\}, \tag{3.5.7}$$

valida per $k \leq \lceil \frac{2H}{q} \rceil$.

Sia $h = r+tq$; poiché la disuguaglianza a cui vogliamo arrivare coinvolge potenze di $p$ minori di $\lceil \frac{2H}{q} \rceil$ possiamo sostituire a $f(h)a_h$ il termine $G_{v,r}(t)\lambda_{v,r}(t)$. La stima

$$\mathrm{ord}_v((\Delta^k G_{v,r}\lambda_{v,r})(t)) \geq 0$$

è ovvia. Per quanto riguarda l'altra osserviamo che

$$(\Delta^k \lambda_{v,r})(t) = \sum_{j=k}^{\infty} \lambda_{v,r,j}(\Delta^k t^j).$$

Poiché $\Delta^k t^j$ è divisibile per $k!$, la (3.5.5) ci dà

$$\mathrm{ord}_v((\Delta^k \lambda_{v,r})(t)) \geq k\left(1 - \frac{1}{p-1}\right) + ord_v(k!).$$

D'altra parte l'operatore differenza soddisfa l'identità di Leibniz

$$(\Delta^k(fg))(t) = \sum_{i=0}^{k} \binom{k}{i} (\Delta^i f)(t+k-i)(\Delta^{k-i} g)(t).$$

Poiché $\deg G_{r,v} \leq N + L_v$, $\Delta^k G_{r,v} = 0$ se $k > N + L_v$. Di conseguenza

$$\mathrm{ord}_v((\Delta^k G_{v,r}\lambda_{v,r})(t)) \geq \min_{\substack{i+j=k \\ i \leq N+L_v}} \mathrm{ord}_v(i!) + j\left(1 - \frac{1}{q}\right) + \mathrm{ord}_v(j!)$$

Il termine $\mathrm{ord}_v(i!)$ si calcola esplicitamente: nel prodotto compaiono $\lfloor \frac{i}{p^\mu} \rfloor$ fattori che siano multipli di $p^\mu$, questo per ogni $\mu$, e dunque

$$\mathrm{ord}_v(i!) = \sum_{\mu=1}^{\infty} \left\lfloor \frac{i}{p^\mu} \right\rfloor = \sum_{\mu=1}^{\infty} \left( \frac{i}{p^\mu} - \frac{S_p(i)}{p^\mu} \right) = \frac{i - S_p(i)}{p-1},$$

dove $S_p(i)$ indica la somma delle cifre di $i$ in base $p$. Lo stesso vale per $j$, dunque riprendendo il conto troviamo

$$\begin{aligned}
&\mathrm{ord}_v((\Delta^k G_{v,r}\lambda_{v,r})(t)) \geq \\
&\quad \geq \min_{i \leq N+L_v} \frac{k}{q} + (k - N - L_v)\left(1 - \frac{1}{q}\right) - \frac{S_p(i)}{q} - \frac{S_p(k-i)}{q} \geq \\
&\quad \geq k - N - L_v + \frac{N + L_v}{q} - \frac{2}{\log p} \log\left(\frac{k}{2}\right) \geq \\
&\quad \geq k - N - L_v - 2\log H.
\end{aligned}$$

Finalmente possiamo passare ad eseguire le operazioni di riga e di colonna sulla matrice

$$\begin{pmatrix}
f(0)a_0 & f(1)a_1 & \cdots & f(h)a_h \\
f(1)a_1 & f(2)a_2 & \cdots & f(h+1)a_{h+1} \\
\vdots & \vdots & \ddots & \vdots \\
f(h)a_h & f(h+1)a_{h+1} & \cdots & f(2h)a_{2h}
\end{pmatrix}$$

per mostrare che $K_h(fa)$ è divisibile per una grande potenza di $\mathcal{P}$. Indichiamo con $C_i$ la colonna $i$-esima e con $R_i$ la riga $i$-esima. Teniamo ancora come parametro $H$ e supponiamo che $h < H$. Per $i = h, h-1, \ldots, q$ rimpiazziamo la colonna $C_i$ con la differenza $C_i - C_{i-q}$. Al secondo passo sostituiamo la colonna $C_i$ con $C_i - C_{i-q}$, ma soltanto per $i = h, h-1, \ldots, 2q$. Ripetiamo questo processo finché possibile, poi passiamo ad eseguire la stessa operazione sulle righe. Il risultato finale è che al posto $(i,j)$ della matrice troviamo l'elemento

$$\Delta_q^{\lfloor \frac{i}{q} \rfloor + \lfloor \frac{j}{q} \rfloor} f(r+s) a_{r+s},$$

dove $r$ ed $s$ sono quegli elementi $0 \leq r, s \leq q-1$ per cui $r \equiv i$, $s \equiv j \pmod q$. Grazie alla (3.5.7) possiamo estrarre da $C_j$ la potenza di $p$ con esponente

$$\max\{0, \lfloor \frac{j}{q} \rfloor - N - L_v - 2\log H\}$$

e poi da $R_i$ con esponente

$$\max\{0, \lfloor \frac{i}{q} \rfloor - N - L_v - 2\log H\}.$$

In conclusione

$$\begin{aligned}
\mathrm{ord}_v(K_h(fa)) &\geq 2q \sum_{k=0}^{\lfloor \frac{h}{q} \rfloor} \max\{0, k - N - L_v - 2\log H\} \geq \\
&\geq 2q \cdot \frac{1}{2} \left( \frac{h}{q} - 1 - N - L_v - 2\log H \right)^2 \geq \\
&\geq \frac{(h+1)^2}{q} - 2q(h+1) \left( N + L_v + 1 + \frac{1}{q} + 2\log H \right).
\end{aligned}$$

□

## 3.6 La scelta di $f$

A questo punto non resta che scegliere $f$ in modo che siano soddisfatte le ipotesi del Lemma 3.5.3. Allo stesso tempo dobbiamo tenere conto che le stime che abbiamo per i valori assoluti archimedei (Proposizione 3.4.2) dipendono dalla grandezza dei coefficienti di $f$. Pertanto vorremmo essere in grado di trovare $f$ con coefficienti relativamente piccoli. L'idea è la seguente: le ipotesi del Lemma 3.5.3 coinvolgono dei polinomi $F_v$ che siamo liberi di scegliere come vogliamo. Diverse scelte di questi polinomi porteranno a diversi $f$ che soddisfano le ipotesi. Facendo variare gli $F_v^{(i)}$ troveremo vari polinomi $f^{(i)}$; tra questi saremo in grado di trovarne due con coefficienti sufficientemente vicini per il principio dei cassetti. La differenza tra questi due sarà il polinomio cercato.

Per trovare un polinomio $f$ che approssimi gli $F_v Q_v$ utilizzeremo una generalizzazione del teorema cinese del resto (vedi [CF67, pag. 66]).

**Proposizione 3.6.1** *Dato un campo di numeri $k$ esiste una costante $C$ con la seguente proprietà. Supponiamo che per ogni valore assoluto $v$ sia dato un tetto $\xi_v > 0$ in modo che $\xi_v = 1$ per quasi ogni $v$ e*

$$\prod_{v \in M_k} \xi_v^{\varepsilon(v)} \geq C.$$

*Allora per ogni scelta di una successione $(x_v)_{v \in M_k}$ tale che $x_v \in \mathcal{O}_v$ per quasi ogni $v$ esiste $x \in k$ che verifica*

$$|x - x_v|_v \leq \xi_v$$

*per ogni valore assoluto $v$.*

Ricordiamo che abbiamo definito

$$R = \prod_{v \in S} N(\mathcal{P}_v)^{\frac{1}{N(\mathcal{P}_v) - 1}}.$$

Scegliamo la famiglia $(\xi_v)_{v \in M_k}$ nel seguente modo:

$$\xi_v = \begin{cases} N(\mathcal{P}_v)^{-1-\frac{2H}{N(\mathcal{P}_v)-1}} & \text{se } v \in S \\ \left(C \cdot \prod_{w \in S} N(\mathcal{P}_w) \cdot R^{2H}\right)^{\frac{1}{[k:\mathbb{Q}]}} & \text{se } v \text{ è archimedeo} \\ 1 & \text{altrimenti.} \end{cases}$$

La scelta di $(\xi_v)$ è fatta in modo che siano soddisfatte le ipotesi della Proposizione 3.6.1, come mostra un breve calcolo. Poniamo inoltre

$$L_S = \max_{v \in S}(\deg Q_v(h)).$$

Fissiamo un tetto $N_0$ per i gradi dei polinomi $F_v$ e scegliamo per ciascun $v \in S$ un polinomio $F_v(h) \in \mathcal{O}_v[h]$, di grado al più $N_0$. Sviluppiamo il prodotto

$$F_v(h)Q_v(h) = \sum_{k=0}^{N_0+L_S} x_{v,k}h^k.$$

Chiaramente $x_{v,k} \in \mathcal{O}_v$; possiamo anche porre $x_{v,k} = 0$ se $v \notin S$. La Proposizione 3.6.1 ci permette di trovare elementi $\overline{f}_k \in k$ per cui

$$|\overline{f}_k - x_{v,k}|_v \leq \xi_v$$

per ogni $v$. Inoltre, se $v$ è nonarchimedeo, $\overline{f}_k \in \mathcal{O}_v$, visto che $\xi_v \leq 1$ e $x_{v,k} \in \mathcal{O}_v$. Ne segue che $\overline{f}_k \in \mathcal{R}$. Poniamo allora

$$\overline{f}(h) = \sum_{k=0}^{N_0+L_S} \overline{f}_k h^k.$$

Con questa scelta $\overline{f} \in \mathcal{R}[h]$ e chiaramente $\deg \overline{f} \leq N_0 + L_S$. Inoltre se $v \in S$

$$\overline{f}(h) \equiv F_v(h)Q_v(h) \pmod{\mathcal{P}_v^{\left\lceil \frac{2H}{N(\mathcal{P}_v)-1} \right\rceil}\mathcal{O}_v}.$$

Invece la scelta di $\xi_v$ per $v$ archimedeo ci dà la stima

$$|\overline{f}_k|_v \leq C_1 \cdot R^{\frac{2H}{[k:\mathbb{Q}]}} \tag{3.6.1}$$

per un'opportuna costante $C_1$ (non terremmo traccia delle varie costanti che introdurremo).

Adesso vogliamo vedere cosa succede cambiando la scelta degli $F_v$. Supponiamo di effettuare due scelte distinte $F_v^{(i)}$ e $F_v^{(j)}$, e trovare di conseguenza due polinomi $\overline{f}^{(i)}$ e $\overline{f}^{(j)}$. È possibile che $\overline{f}^{(j)}$ coincida con $\overline{f}^{(j)}$, ma sicuramente non sarà così se troviamo un valore assoluto $v \in S$ per cui

$$F_v^{(i)}(h)Q_v(h) \not\equiv F_v^{(j)}(h)Q_v(h) \pmod{\mathcal{P}_v^{\left\lceil \frac{2H}{N(\mathcal{P}_v)-1} \right\rceil}\mathcal{O}_v} \tag{3.6.2}$$

Vogliamo riscrivere questa condizione in una forma più comoda. Dato un polinomio $g(h) = \sum g_h h^k$ definiamo il contenuto $v$-adico

$$c_v(g) = \min_k(\mathrm{ord}_v(g_k)).$$

La dimostrazione del lemma di Gauß ci dà la relazione $c_v(g_1g_2) = c_v(g_1) + c_v(g_2)$. In particolare

$$c_v\left((F_v^{(i)} - F_v^{(j)})Q_v\right) = c_v\left((F_v^{(i)} - F_v^{(j)})\right) + c_v(Q_v).$$

Dunque la (3.6.2) è equivalente a

$$F_v^{(i)}(h) \not\equiv F_v^{(j)}(h) \pmod{\mathcal{P}_v^{\lceil \frac{2H}{N(\mathcal{P}_v)-1} \rceil - c_v(Q_v)}\mathcal{O}_v}. \tag{3.6.3}$$

Pertanto il numero di polinomi $\overline{f}^{(i)}$ distinti che troviamo è almeno

$$\prod_{v \in S}\left(N(\mathcal{P}_v)^{\lceil \frac{2H}{N(\mathcal{P}_v)-1} \rceil - c_v(Q_v)}\right)^{N_0} \geq \frac{R^{2HN_0}}{C_2^{N_0}}.$$

Vogliamo vedere che una coppia di polinomi $\overline{f}^{(i)}$ e $\overline{f}^{(j)}$ ha i coefficienti $v$-adicamente vicini per ogni valore assoluto $v$ archimedeo. Indichiamo con $M_\infty$ l'insieme dei valori assoluti archimedei. Per ogni $t > 0$ possiamo considerare l'insieme

$$\{\mathbf{z} = (z_v)_{v \in M_\infty} : |z_v|_v \leq t\} \subset \prod_{v \in M_\infty} K_v$$

e indicare con vol$(t)$ il suo volume (ciascun completamento $K_v$ coincide con $\mathbb{R}$ o con $\mathbb{C}$ e il volume è preso rispetto all'usuale misura di Lebesgue). Per omogeneità avremo vol$(t) = C_3 t^{[k:\mathbb{Q}]}$. Se indichiamo con $\mathcal{R}[h]_D$ i polinomi a coefficienti in $\mathcal{R}$ di grado al più $D$ abbiamo una mappa

$$\begin{array}{rccc} \sigma: & \mathcal{R}[h]_{N_0+L_S} & \longrightarrow & \left(\prod_{v \in M_\infty} K_v\right)^{N_0+L_S+1} \\ & g(h) & \longrightarrow & (\underbrace{g_1, g_1, \ldots, g_1}_{[k:\mathbb{Q}] \text{ volte}}, g_2, \ldots, g_n) \end{array}$$

Sullo spazio $X = \left(\prod_{v \in M_\infty} K_v\right)^{N_0+L_S+1}$ utilizziamo la norma

$$\|\mathbf{z}\| = \max_{v \in M_\infty} |z_{v,j}|_v.$$

Vogliamo utilizzare il principio dei cassetti per trovare due polinomi $\overline{f}^{(i)}$ ed $\overline{f}^{(j)}$ sufficientemente vicini rispetto a tutti i valori assoluti archimedei.

**Lemma 3.6.2** *Sia* $D = \min \|\sigma(\overline{f}^{(i)}) - \sigma(\overline{f}^{(i)})\|$. *Allora*

$$D \leq C_4 R^{\frac{2H(L_S+1)}{[k:\mathbb{Q}](N_0+L_S+1)}}.$$

**Dim.** La (3.6.1) ci dice che tutti i $\sigma(\overline{f}^{(i)})$ si trovano dentro un insieme di volume

$$\mathrm{vol}\left(C_1 R^{\frac{2H}{[k:\mathbb{Q}]}}\right)^{N_0+L_S+1}.$$

Consideriamo i polidischi

$$B^{(i)} = \left\{\mathbf{z} \in X : \|\mathbf{z} - \sigma(\overline{f}^{(i)})\| \leq \frac{D}{2}\right\}.$$

Per definizione di $D$ questi sono disgiunti, e hanno volume $\mathrm{vol}(D/2)^{N_0+L_S+1}$. Inoltre sono contenuti nel polidisco

$$\left\{\mathbf{z} \in X : \|\mathbf{z}\| \le 2C_1 R^{\frac{2H}{[k:\mathbb{Q}]}}\right\}.$$

Poiché ci sono almeno $\frac{R^{2HN_0}}{C_2^{N_0}}$ polidischi $B^{(i)}$ il confronto tra i volumi dà la tesi.

□

Prendiamo allora una coppia di polinomi $\overline{f}^{(i)}$ ed $\overline{f}^{(j)}$ che realizzano la distanza $D$ e poniamo $f(h) = \overline{f}^{(i)}(h) - \overline{f}^{(j)}(h) \in \mathcal{R}[h]$. Per costruzione

$$f(h) \equiv \left(F_v^{(i)}(h) - F_v^{(j)}(h)\right) Q_v(h) \pmod{\mathcal{P}_v^{\left\lceil \frac{2H}{N(\mathcal{P}_v)-1} \right\rceil} \mathcal{O}_v}.$$

## 3.7 Mettere tutto insieme

Per concludere dobbiamo stimare il grado il valore assoluto dei coefficienti di $f$, e il risultato che otterremo dipenderà da $N_0$. Scegliamo

$$N_0 = \left\lceil \left(\frac{H}{\log H}\right)^{1/2} \right\rceil.$$

Per come è stato costruito $f$ abbiamo

$$N = \deg f \le N_0 + L_S + 1 \le C_5 \sqrt{\frac{H}{\log H}}.$$

Prendendo $C_5$ ed $H$ abbastanza grandi non è restrittivo supporre che

$$N + L_v + 2 + 2\log H \le C_5 \sqrt{\frac{H}{\log H}}$$

per ogni $v \in S$. Di conseguenza il Lemma 3.5.3 ci garantisce che per $v \in S$ e $h \le H$ vale

$$\mathrm{ord}_v(K_h(fa)) \ge \frac{(h+1)^2}{N(\mathcal{P}_v) - 1} - 2C_5(h+1)N(\mathcal{P}_v)\sqrt{\frac{H}{\log H}}.$$

Allo stesso tempo per $v$ archimedeo possiamo stimare i coefficienti di $f$ con

$$D_v = D \le C_4 R^{\frac{2H}{[k:\mathbb{Q}]} \frac{L_S+1}{\left(\frac{H}{\log H}\right)^{1/2} + L_S + 1}} \le C_6^{\sqrt{H \log H}}.$$

La Proposizione 3.4.2 ci permette di usare questa disuguaglianza per ottenere una stima di $|K_h(fa)|_v$ ai valori assoluti $v$ archimedei. Quello che troviamo è

$$|K_h(fa)|_v \le \left( \frac{C_6^{\sqrt{H\log H}} M_v \left(C_5 \sqrt{\frac{H}{\log H}}\right)}{\sqrt{\rho_v^2 - 1}} \right)^{(h+1)} (2h)^{C_5(h+1)\sqrt{\frac{H}{\log H}}} \rho_v^{\frac{3}{2}(h+1)^2}.$$

Per gli altri valori assoluti in $T$ la stima per $|K_h(fa)|_v$ è data dalla stessa Proposizione 3.4.2. Infine se $v \notin S \cup T$ ricordiamo che $|K_h(fa)|_v \le 1$.

Adesso abbiamo tutti gli ingredienti che servono. Poniamo $H_0 = H^{1/2} \log H$; se $H_0 \leq h \leq H$ diventa un calcolo, per quanto spiacevole, verificare che

$$\prod_{v \in M_k} |K_h(fa)|_v < 1,$$

e di conseguenza $K_h(fa) = 0$. La proposizione 2.1.4 ci dice allora che esiste una successione $(d_h)$ soluzione di una ricorrenza lineare di ordine al più $H_0$ tale che

$$d_h = f(h) a_h = f(h) \frac{c_h}{b_h}$$

per $h \leq H$. Possiamo riscrivere questa cosa come $x_h = b_h d_h - f(h) c_h = 0$. D'altra parte $x_h$ soddisfa anch'essa una ricorrenza lineare, e se indichiamo con $n$ l'ordine di $b_h$ e $m$ quello di $c_h$ l'ordine di $x_h$ è al più

$$n H^{1/2} \log H + m C_5 \sqrt{\frac{H}{\log H}} \leq H - H^{1/2} \log H$$

per $H$ grande. Poiché $x_h$ si annulla su un intervallo di lunghezza $H$, deve essere identicamente nulla, cioè $f(h) a_h = d_h$ soddisfa una ricorrenza lineare. Infine il teorema di Pólya-Cantor ci dice che la successione $(a_h)$ soddisfa anch'essa una ricorrenza lineare, che è la tesi del Teorema 3.1.1.

# Capitolo 4

# Equazioni moniche

For every problem, there is a solution which is simple, neat and wrong.

*Henry Louis Mencken*

## 4.1 Il problema

Il capitolo precedente è centrato sul problema del quoziente di Hadamard di funzioni razionali; in altri termini sono date funzioni razionali $f$ e $g$ ed è discussa la risolubilità dell'equazione $f \star x = g$ nell'anello $\mathcal{H}(k)$. Il nostro scopo è quello di arrivare a studiare la risolubilità di equazioni algebriche non lineari, e il teorema del quoziente ci permetterà di ricondurci al caso di equazioni moniche. Ovviamente affinché un'equazione sia risolubile in $\mathcal{H}(k)$ è necessario innanzitutto che vi sia una soluzione 'formale', cioè nell'anello $k[[X]]_H$. Nel caso di equazioni moniche questa condizione è probabilmente anche sufficiente (a meno di passare ad un'estensione finita del campo $k$). Studiando il problema è abbastanza naturale formulare la seguente congettura, proposta anche in [vdP96].

**Congettura 4.1.1** *Sia $k$ un campo di numeri e $g(X,Y) \in k[X,Y]$ un polinomio monico in $Y$. Sia $f \in \mathcal{H}(k)$ e supponiamo che l'equazione $g(f,Y) = 0$ abbia soluzione in $K_1[[t]]_H$, dove $K_1/k$ è un'estensione finita. Allora esiste un'estensione finita $K_2/k$ tale che $g(f,Y) = 0$ abbia soluzione in $\mathcal{H}(K_2)$.*

Chiaramente, allargando il campo $k$, possiamo supporre come ipotesi che l'equazione abbia soluzione in $k[[t]]_H$. Similmente possiamo passare alla chiusura normale su $\mathbb{Q}$ e supporre dunque che $k/\mathbb{Q}$ sia di Galois. Inoltre usando nuovamente la Proposizione 2.2.2 possiamo ricondurci alla seguente versione.

**Congettura 4.1.2** *Sia $k/\mathbb{Q}$ un'estensione di Galois finita e*

$$b(n) = \sum_{i=1}^{m} B_i(n)\beta_i^n$$

*un polinomio esponenziale, con $B_i \in k[X]$ e $\beta_i \in k$ per $i = 1, \dots m$. Sia $g \in k[X,Y]$ monico in $Y$, e supponiamo che per ogni $n \in \mathbb{N}$ l'equazione $g(b(n), y) = 0$ abbia soluzione $y_n \in k$. Allora esiste un polinomio esponenziale*

$$a(n) = \sum_{i=1}^{l} A_i(n)\alpha_i^n$$

*a coefficienti in un'estensione finita $K$ di $k$ tale che $g(b(n), a(n)) = 0$ per ogni $n \in \mathbb{N}$.*

Il caso in cui si sta cercando una radice $d$-esima di Hadamard di una funzione razionale, che corrisponde alla scelta

$$g(X,Y) = Y^d - X$$

è stato ottenuto in [Zan00]. Abbiamo cercato di generalizzare questi metodi per dimostrare la congettura in generale. Quello che abbiamo ottenuto è che la congettura 4.1.2 è vera nel caso di equazioni di grado minore o uguale a 3. Tuttavia crediamo che lo schema dimostrativo proposto si possa applicare nel caso generale; alcune difficoltà in paio di passaggi ci hanno costretto a limitare l'applicazione di questo metodo ad un caso particolare in cui queste difficoltà sono facilmente superate. Scopo del capitolo è perciò dimostrare il seguente

**Teorema 4.1.1** *La congettura 4.1.2 è vera almeno nei due casi:*

*i) se $g(X,Y)$ ha grado al più 3 in $Y$ oppure*

*ii) se $g(X,Y) = Y^d - X$.*

Una semplice induzione ci permetterà di limitarci a dimostrare il caso *ii*) del teorema sotto l'ipotesi che $d$ sia primo.

## 4.2 La strategia

Diamo un'idea di come procederà la dimostrazione prima di fare altre riduzioni:

- Scriviamo $b(n) = f(n, \beta_1^n, \dots, \beta_m^n)$ per un certo $f \in k[X_0, \dots, X_m]$ (in realtà, per un motivo tecnico, faremo prima un piccolo cambio di variabili). Se l'equazione $g(f(X_0, \dots, X_m), Y) = 0$ ha una soluzione nell'anello dei polinomi, riusciamo ad ottenere la conclusione. Più in generale tutto funziona se sostituiamo a $f$ il polinomio $f(X_0, X_1^D, \dots, X_m^D)$ per un certo $D$. Questa ulteriore libertà ci tornerà utile per riuscire ad applicare il teorema di Чеботарев nel terzo passo.

- Se l'equazione di sopra non ha soluzione per nessun $D$ cerchiamo di ottenere un assurdo. Scegliamo un $D$ opportuno ed un primo $\mathcal{P}$ di $k$ con $f(\mathcal{P}|p) = 1$, dove $(p) = \mathcal{P} \cap \mathbb{Z}$. Usando il teorema di Lang-Weil (applicato ad un'equazione ausiliaria) troveremo una $(m+1)$-upla $(x_0, \dots, x_m) \in \mathbb{F}_p^{m+1}$ per cui la congruenza
$$g(f(x_0, \dots, x_m), Y) \equiv 0$$
non ha soluzioni in $\mathbb{F}_p$.

- Solleviamo $(x_0, \ldots, x_m)$ a radici dell'unità $(z_0, \ldots, z_m)$ in un'estensione di $k$. In questo modo l'equazione
$$g(f(z_0, \ldots, z_m), Y) = 0$$
non avrà soluzioni in $k$. Applicando in teorema di Чеботарев saremo in grado di trovare un primo $\mathcal{Q}$ tale che la riduzione di queste radici mod $\mathcal{Q}$ sia la stessa della $(m+1)$-upla $(n, \beta_1^n, \ldots, \beta_m^n)$, e allo stesso tempo la congruenza
$$g(f(z_0, \ldots, z_m), Y) \equiv 0 \pmod{\mathcal{Q}}$$
continui a non avere soluzione.

- A questo punto abbiamo i due polinomi
$$g(f(z_0, \ldots, z_m), Y)$$
$$g(f(n, \beta_1^n \ldots, \beta_r^n), Y).$$
La loro riduzione mod $\mathcal{Q}$ è la stessa; tuttavia il primo non ha radici mod $\mathcal{Q}$, mentre il secondo ne ha per ipotesi almeno una. Questa contraddizione conclude la dimostrazione.

In realtà lo sketch di sopra è un po' impreciso, perché andando avanti con la dimostrazione avremo bisogno di sostituire a $k$ delle sue estensioni finite, e useremo una notazione lievemente diversa.

## 4.3 Il sottogruppo $\Gamma$

Il primo passo per dimostrare il Teorema 4.1.1 consiste in una piccola semplificazione, che ci tornerà utile nel seguito: vogliamo ricondurci al caso in cui il sottogruppo di $k^*$ generato da $\beta_1, \ldots, \beta_m$ sia libero da torsione. Se chiamiamo $\Gamma$ questo sottogruppo abbiamo allora il seguente

**Lemma 4.3.1** *Per dimostrare il Teorema (4.1.1) non è restrittivo supporre che $\Gamma$ sia libero da torsione.*

**Dim.** Sia $N$ l'ordine della parte di torsione di $\Gamma$. Consideriamo i polinomi esponenziali $b_r(n) = b(r + Nn)$, con $0 \leq r \leq N - 1$; le radici di questi polinomi esponenziali sono le $\beta_i^N$, e dunque generano un sottogruppo libero da torsione. Se il teorema vale sotto le ipotesi più forti otteniamo $a_r(n) \in K[x]_{esp}$ con $g(b_r(n), a_r(n)) = 0$. Scegliamo $c_r(n) \in K'[x]_{esp}$, dove $K'$ è un'estensione finita di $K$, in modo che $c_r(Nn) = a_r(n)$. Esplicitamente, se
$$a_r(n) = \sum_{i=1}^{l} C_i(n)\gamma_i^n$$
basta prendere
$$c_r(n) = \sum_{i=1}^{l} C_i(\frac{n}{N})\delta_i^n,$$

dove $\delta_i^N = \gamma_i$. Osserviamo ora che il polinomio esponenziale

$$\theta(n) = \frac{1}{N} \sum_{i=1}^{N} \zeta_N^n$$

assume valore 1 per $N|n$ e 0 altrimenti. Poniamo allora

$$a(n) = \sum_{r=0}^{N-1} \theta(n-r) c_r(n-r).$$

In questo modo se $n = s + Nm$, con $0 \leq r \leq N-1$, troviamo $a(n) = a(s+Nm) = c_s(Nm) = a_s(m)$, e $g(b(n), a(n)) = g(b_s(m), a_s(m)) = 0$.

$\square$

D'ora in poi lavoreremo dunque nell'ipotesi che $\Gamma$ sia privo di torsione; fissiamo una base (moltiplicativa) del gruppo, $\gamma_1, \ldots, \gamma_r$. Possiamo allora scrivere $b(n) = f(n, \gamma_1^n, \ldots, \gamma_r^n)$, dove $f(X_0, \ldots, X_r)$ è una funzione razionale in $X_1, \ldots X_r$ e polinomiale in $X_0$. Più precisamente $f$ è della forma

$$f(X_0, \ldots, X_r) = \frac{\widetilde{f}(X_0, \ldots, X_r)}{X_1^{a_1} \cdots X_r^{a_r}},$$

dove $\widetilde{f}$ è un polinomio. Perciò $f \in k_L[X_0, \ldots, X_r] = S^{-1}k[X_0, \ldots, X_r]$, dove $S$ è la parte moltiplicativa formata dai monomi in $X_1, \ldots, X_r$. Osserviamo che, essendo la localizzazione di un anello di polinomi su un campo, $k_L[X_0, \ldots, X_r]$ è un anello a fattorizzazione unica. Gli elementi di $k_L[X_0, \ldots, X_r]$ sono detti polinomi di Laurent su $k$.

## 4.4 Costruzione di alcuni polinomi

A questo punto è necessaria un'osservazione. Nella sezione precedente abbiamo scritto $b(n) = f(n, \gamma_1^n, \ldots, \gamma_r^n)$, dove $f(X_0, \ldots, X_r) \in k_L[X_0, \ldots, X_r]$. L'equazione che stiamo cercando di risolvere è

$$g(f(n, \gamma_1^n, \ldots, \gamma_r^n), Y) = 0.$$

Consideriamo invece l'equazione

$$g(f(X_0, \ldots, X_r), Y) = 0 \tag{4.4.1}$$

da risolvere nell'incognita $Y \in \overline{k}_L[X_0, \ldots, X_r]$. Se questa ha una soluzione $Y = y(X_0, \ldots, X_r)$, allora siamo a posto. Consideriamo infatti

$$a(n) = y(n, \gamma_1^n, \ldots, \gamma_r^n):$$

per costruzione $a(n)$ è un polinomio esponenziale e verifica $g(b(n), a(n)) = 0$. Allo stesso modo possiamo fissare un numero intero $D > 0$ e cercare di risolvere

$$g(f(X_0, X_1^D, \ldots, X_r^D), Y) = 0. \tag{4.4.2}$$

Se troviamo una soluzione $Y = y(X_0, \ldots, X_r)$, possiamo costruire il polinomio esponenziale

$$a(n) = y(n, \alpha_1^n, \ldots, \alpha_r^n),$$

dove gli $\alpha_i$ sono scelti in modo che $\alpha_i^D = \gamma_i$. Di nuovo troviamo che $g(b(n), a(n)) = 0$.

Per dimostrare il Teorema 4.1.1 possiamo allora supporre che per ogni $D \geq 1$ l'equazione (4.4.2) non abbia soluzione nell'anello $\overline{k}_L[X_0, \ldots, X_r]$. Il lemma di Gauß ci garantisce anche che l'equazione non abbia soluzioni in $\overline{k}(X_0, \ldots, X_r)$. Vogliamo vedere che tutto questo porta ad un assurdo, e il resto della dimostrazione consisterà nell'arrivare a questo assurdo. A questo scopo poniamo

$$S_D(X_0, X_1, \ldots, X_r, Y) = g(f(X_0, X_1^D, \ldots, X_r^D), Y);$$

la nostra ipotesi è che questi polinomi di Laurent non abbiano fattori lineari in $Y$. Quello che vorremmo fare è utilizzare il Teorema di Lang-Weil 1.4.4 applicato ad uno di questi polinomi ridotto modulo un opportuno primo. Non è possibile fare questo direttamente perché non sappiamo che questi polinomi sono assolutamente irriducibili, ma solo che non hanno radici nell'ultima variabile.

Nei casi che stiamo trattando, cioè che $g$ abbia grado al più 3 in $Y$ oppure sia binomiale, i polinomi $S_D$ sono effettivamente irriducibili su $\overline{k}_L[X_0, \ldots, X_r, Y]$. Questo segue immediatamente dal fatto di non avere radici se $g$ ha grado $\leq 3$. Se invece $g(X, Y) = Y^d - X$ la tesi segue subito dal Lemma 1.3.4 (ricordiamo che possiamo supporre che $d$ sia primo).

Anche se semplifica le cose questo passo non è veramente necessario, per cui possiamo portare avanti l'argomentazione nel caso generale. Fattorizziamo $S_1 = S_1^{(1)} \ldots S_1^{(\lambda)}$ su $\overline{k}_L[X_0, \ldots, X_r, Y]$; a meno di sostituire $k$ con una sua estensione finita possiamo supporre che la fattorizzazione sia a coefficienti in $k$. In realtà sarà conveniente ingrandire $k$ ancora un po'. Le radici (nella variabile $Y$) degli $S^{(j)}$ generano un'estensione finita $L$ di $k(X_0, \ldots, X_r)$; sia $\Xi$ un elemento primitivo per questa estensione, che possiamo prendere intero su $k[X_0, \ldots, X_r]$. Indichiamo con $T \in k[X_0, \ldots, X_r][Y]$ il polinomio minimo di $\Xi$. Consideriamo i polinomi

$$T_D = T(X_0, X_1^D, \ldots, X_r^D, Y).$$

Essendo un polinomio minimo $T_1 = T$ è irriducibile; in generale invece $T_2$ si fattorizzerà su $\overline{k}[X_0, \ldots, X_r, Y]$. Sia $T_2 = T_2^{(1)} \ldots T_2^{(\mu)}$ la fattorizzazione. Chiaramente

$$T_6(X_0, \ldots, X_r, Y) = T_2^{(1)}(X_0, X_1^3, \ldots, X_r^3, Y) \cdots T_2^{(\mu)}(X_0, X_1^3, \ldots, X_r^3, Y),$$

ma i fattori potrebbero non essere più irriducibili. Scomponiamo ulteriormente i fattori e ripetiamo l'operazione, sostituendo all'esponente 6 l'esponente $24 = 4!$. Di nuovo $T_{24}$ si potrà scrivere come prodotto dei fattori di $T_6$ in cui sostituiamo all'indeterminata $X_i$ la sua quarta potenza, per $i \geq 1$. Se questa non fosse ancora una fattorizzazione scomponiamo ulteriormente i termini, e procediamo considerando i polinomi $T_D$ al variare di $D \in \Lambda = \{n!,\, n \in \mathbb{N}\}$. A ciascun passo tutti i fattori sono monici in $Y$ e il grado in $Y$ dei fattori diminuisce. Pertanto dopo un numero finito di passi non otteniamo nuovi fattori; ingrandiamo $k$ in modo che tutti i fattori che troviamo siano a coefficienti in $k$.

Osserviamo che possiamo scrivere ogni radice di $S$ nella forma $P_i(\Xi)$, dove i $P_i$ sono polinomi a coefficienti in $k(X_0, \ldots, X_r)$. Di conseguenza avremo che le radici di $S_D$ sono $P_i(\Xi_D)$, dove $T_D(\Xi_D) = 0$. Visto che per ipotesi $S_D$ non ha radici in $\overline{k}(\underline{X})$, i fattori di $T_D$ avranno tutti grado almeno 2 in $Y$. In conclusione abbiamo ingrandito $k$ in modo che tutti i polinomi $T_D$ con $D \in \Lambda$ si fattorizzino in $k$ in termini assolutamente irriducibili. Inoltre ciascuno di questi fattori ha grado almeno 2 nella variabile $Y$.

## 4.5 La scelta di D

Per l'ultimo passo della dimostrazione avremo bisogno di controllare la riduzione dei $\gamma_i$ modulo un certo primo. Introduciamo un primo $\beta$ moltiplicativamente indipendente dai $\gamma_i$ e poniamo $\delta_i = \gamma_i \beta^{-h_i}$, dove gli $h_i$ sono interi che ancora dobbiamo scegliere. Troveremo che sarà più agevole controllare la riduzione di $\beta$ e dei $\delta_i$, ma per far questo avremo bisogno di un fatto un po' tecnico:

**Lemma 4.5.1** *[Zan00] Esiste un numero $L$ tale che se $M \geq 1$ e $\ell > L$ è un primo, allora $\beta^M$ non sta nel gruppo moltiplicativo generato dai $\delta_i$ e da $(k_c^*)^{\ell M}$. $L$ dipende solamente da $k$, $\beta$ e dai $\gamma_i$.*

**Oss.** Il fatto che $L$ non dipenda dagli $h_i$ ci permette di fissare adesso $L$ come nel Lemma 4.5.1 e di lasciare ancora in sospeso la scelta di questi interi. In particolare per scegliere gli $h_i$ dovremo usare i prossimi risultati, che presuppongono di aver fissato $L$, dunque questa indipendenza è fondamentale per non cadere in un circolo vizioso.

**Dim.** Se la conclusione non vale abbiamo una relazione del tipo

$$\beta^M \delta_1^{a_1} \cdots \delta_r^{a_r} = v^{\ell M}, \tag{4.5.1}$$

con $v \in k_c^*$, e possiamo prenderne una in cui $M$ sia minimo. Riscriviamo l'equazione in termini dei $\gamma_i$ come

$$\beta^{a_0} \gamma_1^{a_1} \cdots \gamma_r^{a_r} = v^{\ell M}. \tag{4.5.2}$$

Se $L$ (e dunque $\ell$) è grande rispetto a $k$ avremo che $\zeta_\ell \notin k$. Possiamo dunque applicare la Proposizione (1.3.5) e concludere che, posto $u = v^M$, esistono una radice dell'unità $\omega$ e $t \in k^*$ con $u = \omega t$.

Sia $Q$ un numero intero; per il Lemma 4.5.2 troviamo un intero positivo $b \leq Q^{r+1}$ e interi $p_i$ tali che $|b_i| \leq \ell/Q$, dove $b_i = ba_i - \ell p_i$. Eleviamo (4.5.2) alla $b$-esima potenza e riarrangiamo i termini in modo da avere

$$\beta^{b_0} \gamma_1^{b_1} \cdots \gamma_r^{b_r} = \omega^{\ell b} \rho^\ell$$

per un certo $\rho \in k^*$. Prendendo l'altezza otteniamo

$$\ell h(\rho) \leq \max(|b_i|) \left( h(\beta) + \sum_{i=1}^{r} h(\gamma_i) \right) \leq C \frac{\ell}{Q}$$

per una costante $C$ dipendente da $\beta$ e dai $\gamma_i$.

Tutto questo per ogni $Q$; scegliendo $Q = \lceil \ell^{\frac{1}{r+2}} \rceil$ troviamo

$$h(\rho) \leq C' \ell^{\frac{-1}{r+2}}$$

per $\ell$ grande. Esistono solo un numero finito di elementi di $k^*$ di altezza limitata, dunque se $\ell$ è abbastanza grande troviamo $h(\rho) = 0$, e per il teorema di Kronecker 1.6.2 concludiamo che $\rho$ è una radice dell'unità. Essendo $\beta, \gamma_1, \ldots, \gamma_r$ indipendenti ricaviamo che tutti i $b_i$ sono 0. Allo stesso tempo $b \leq Q^{r+1} < \ell$, perciò da $ba_i = \ell p_i$ segue che $\ell | a_i$ per ogni $i$. Poiché $a_0 = M - \sum a_i h_i$ segue anche che $\ell | M$; scriviamo $M = \ell M'$ e $a_i = \ell a'_i$. Sostituendo in (4.5.1) otteniamo

$$\beta^{M'} \delta_1^{a'_1} \cdots \delta_r^{a'_r} = (v\theta)^{\ell M'}$$

per una radice $\ell$-esima dell'unità $\theta$, contro la minimalità di $M$.

□

**Lemma 4.5.2 (Dirichlet)** *([Sch80, pag. 27]) Siano dati $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$, e fissiamo un tetto $Q$ per i denominatori. Allora possiamo trovare numeri razionali $p_i/b$ con $|b| \leq Q^r$ e*

$$\left| \lambda_i - \frac{p_i}{b} \right| < \frac{1}{bQ}$$

**Dim.** Suddividiamo il cubo $[0, 1[^r$ in $Q^r$ cubetti e consideriamo i punti $P(b) = (b\lambda_1, \ldots, b\lambda_r) \bmod 1$ al variare di $b \in \mathbb{N}$ con $1 \leq b \leq Q^r$. Se uno di questi punti si trova in $[0, 1/Q[^r$ abbiamo concluso. Infatti troviamo interi $p_i$ per cui $0 \leq b\lambda_i - p_i < 1/Q$, da cui la tesi. Altrimenti per il principio dei cassetti troviamo due punti $P(c)$ e $P(d)$ nello stesso cubetto, diciamo con $c < d$. Ma allora il punto $P(d - c) \in ]-1/Q, 1/Q[^r$, e concludiamo comunque.

□

Indichiamo con $\mathbb{Q}_c$ l'estensione ciclotomica massimale di $\mathbb{Q}$, e con $k_c = k\mathbb{Q}_c$ quella di $k$. Dato un numero naturale $L$ maggiore del grado in $Y$ di $g$ e abbastanza grande affinché siano soddisfatte le ipotesi del Lemma 4.5.1, prendiamo $D$ in modo che sia divisibile per ogni fattore primo $\leq L$. Supponiamo anche che $D$ sia abbastanza grande, in modo che $\mathbb{Q}_c \cap k \subset \mathbb{Q}(\zeta_D)$. Andiamo a costruire il primo di cui abbiamo bisogno per applicare il Teorema 1.4.4.

**Lemma 4.5.3** *Esistono infiniti primi $p = 1 + Dm$ che si spezzano totalmente in $k(\zeta_D)$, tali che ogni fattore primo di $m$ sia maggiore di $L$.*

**Dim.** Sia $\ell \leq L$ un primo. $k(\zeta_{\ell D})/k(\zeta_D)$ è un'estensione ciclica e, poiché $k(\zeta_D)$ e $\mathbb{Q}(\zeta_{\ell D})$ sono linearmente disgiunte su $\mathbb{Q}(\zeta_D)$, ha grado $\ell$. Sia $k'$ il composto dei campi $k(\zeta_{\ell D})$ al variare di $\ell \leq L$. Per questioni di grado tutti questi campi sono linearmente disgiunti su $k(\zeta_D)$, e pertanto l'estensione $k'/k(\zeta_D)$ è ciclica. Sia $\sigma$ un generatore del suo gruppo di Galois. Per il teorema di Чеботарев troviamo infiniti primi razionali $p$ che si spezzano completamente in $k(\zeta_D)$, e tali che il Frobenius $\phi(\mathcal{P})$ di un primo $\mathcal{P}|p$ in $k'/k(\zeta_D)$ sia proprio $\sigma$. Vediamo che possiamo scrivere $p = 1 + Dm$, dove ogni fattore primo di $m$ è maggiore di $L$. Infatti $p$ si spezza totalmente in $\mathbb{Q}(\zeta_D) \subset k(\zeta_D)$, ed è noto che il grado d'inerzia di $p$ in una tale estensione è pari all'ordine moltiplicativo di $p \bmod D$, da cui $p \equiv 1 \pmod{D}$. Allo stesso modo troviamo che $p \not\equiv 1 \pmod{\ell D}$ per $\ell \leq L$. Se così non fosse $p$ si spezzerebbe totalmente in $\mathbb{Q}(\zeta_{\ell D})$ e in $k(\zeta_D)$, e dunque nel composto $k(\zeta_{\ell D})$. Tuttavia questo è assurdo, perché il Frobenius di $\mathcal{P}$ in $k(\zeta_{\ell D})$ è la restrizione di $\sigma$, che non è l'identità.

□

## 4.6 Applicare Lang-Weil

Scegliamo $p$ come nel claim, e sia $\mathcal{P}|p$ un primo di $k(\zeta_D)$, in modo che, se $\mathcal{R}$ è l'anello degli interi, $\mathcal{R}/\mathcal{P} \cong \mathbb{F}_p$. Vorremmo trovare, almeno per $p$ abbastanza grande, una $(r+1)$-upla $(x_0, \dots, x_r)$ di elementi non nulli di $\mathbb{F}_p$ tali che la congruenza

$$g(f(x_0, \dots, x_r), Y) \equiv 0 \pmod{\mathcal{P}}$$

non abbia soluzione in $\mathbb{F}_p$. Tuttavia questo non è fattibile direttamente; il motivo è che il polinomio di Laurent $S_D$ potrebbe essere fattorizzabile su $\overline{k}$, e questo ci impedisce di utilizzare direttamente il teorema (1.4.4). Sia $S_D = S^{(1)} \dots S^{(\kappa)}$ la fattorizzazione di $S_D$ su $\overline{k}$; per le scelte che abbiamo fatto nella sezione 4.4 questa è in realtà una fattorizzazione a coefficienti in $k$. Fissiamo uno dei fattori irriducibili $\overline{S}_D = S^{(i)}$: dovremo applicare i risultati dei prossimi passi a ciascun fattore, ma sarà comodo non portarsi dietro troppi indici.

Allo stesso modo abbiamo la fattorizzazione (su $k$) $T_D = T^{(1)} \dots T^{(\nu)}$. Scegliamo un fattore $T^{(i)}$ e chiamiamo $N_i(p)$ il numero di soluzioni di $T^{(i)} \equiv 0$ in $\mathbb{F}_p^{r+2}$. Se $p$ è abbastanza grande il teorema di Островскии 1.4.6 ci garantisce che ogni fattore $T^{(i)}$ resta assolutamente irriducibile in $\mathbb{F}_p$. Possiamo allora applicare il teorema di Lang-Weil 1.4.4 e dedurre che

$$N_i(p) = p^{r+1} + O(p^{r+1/2}).$$

Ciascun fattore $T^{(i)}$ ha grado in $Y$ $d_i \geq 2$; inoltre se $(x_0, \dots, x_r) \in \mathbb{F}_p^{r+1}$ è tale che $T(x_0, \dots, x_r, Y)$ ha almeno una soluzione $Y \in \mathbb{F}_p$, allora $\overline{S}_D(x_0, \dots, x_r, Y)$ ha $d$ soluzioni, dove $d$ è il grado in $Y$ di $\overline{S}_D$. Il numero di tali $(r+1)$-uple è almeno

$$\frac{N_i(p)}{d_i} \geq \frac{p^{r+1}}{d_i} + O(p^{r+1/2}),$$

perciò otteniamo almeno $\frac{d}{d_i} p^{r+1} + O(p^{r+1/2})$ soluzioni di $\overline{S}_D$. Indichiamo con $M(p)$ il numero di soluzioni di $\overline{S}_D$ che non abbiamo ancora contato. Possiamo applicare il teorema di Lang-Weil anche al polinomio di Laurent $\overline{S}_D$, visto che il numero di zeri di $\overline{S}_D$ differisce da quello del suo numeratore per un $O(p^r)$. Quello che troviamo è

$$\frac{d}{d_i} p^{r+1} + M(p) = p^{r+1} + O(p^{r+1/2}),$$

cioè

$$M(p) \leq \left(1 - \frac{d}{d_i}\right) p^{r+1} + O(p^{r+1/2}).$$

Di conseguenza il numero di $(r+1)$-uple $(x_0, \dots, x_r)$ per cui $\overline{S}_D$ ha almeno una soluzione in $Y$ si stima con

$$\frac{p^{r+1}}{d_i} + M(p) + O(p^{r+1/2}) \leq p^{r+1} \left(1 - \frac{d-1}{d_i}\right) + O(p^{r+1/2}).$$

Perciò se $p$ è sufficientemente grande troviamo una $(r+1)$-upla di elementi non nulli $(x_0, \dots, x_r)$ mod $\mathcal{P}$ tale che la congruenza $\overline{S}_D(x_0, \dots, x_r, Y) \equiv 0 \pmod{\mathcal{P}}$ non abbia soluzioni in $\mathbb{F}_p$. La scelta di questa $(r+1)$-upla dipende dal fattore $\overline{S}_D = S^{(i)}$ considerato. Ripetiamo questa operazione per ogni fattore, scegliendo comunque lo stesso primo $\mathcal{P}$ per tutti i fattori, producendo diverse $(r+1)$-uple.

## 4.7 Scelta del primo $\mathcal{Q}$

A questo punto abbiamo fissato $L$ grande e di conseguenza $D$ ed un primo $p = 1 + Dm$, dove ogni fattore primo di $m$ è maggiore di $L$. $p$ si spezza completamente in $k$ e in $\mathbb{Q}(\zeta_{p-1})$, perciò anche in $\widetilde{k} = k(\zeta_{p-1})$. Come nella sezione precedente fissiamo un fattore $\overline{S}_D = S^{(i)}$ di $S_D$, e sia $(x_0, \ldots, x_r)$ la relativa $(r+1)$-upla costruita utilizzando Lang-Weil. Scegliamo un ideale primo $\mathcal{Q}|\mathcal{P}$ dell'anello degli interi $\mathcal{S}$ di $\widetilde{k}$ e osserviamo che le potenze di $\zeta_{p-1}$ sono un sistema di rappresentanti per le classi di elementi non nulle in $\mathcal{S}/\mathcal{Q}$. Possiamo determinare gli interi $h_i$ in modo che $\zeta_{p-1}^{h_i} \equiv x_i \pmod{\mathcal{Q}}$.

Dalla sezione precedente otteniamo che l'equazione

$$h(Y) = \overline{S}_D(\zeta_{p-1}^{h_0}, \zeta_{p-1}^{h_1}, \ldots, \zeta_{p-1}^{h_r}, Y) = 0$$

non ha soluzioni in $\widetilde{k}$. Infatti tale equazione è monica in $Y$, per cui un'eventuale soluzione starebbe in $\mathcal{S}$, ma questo non può essere perché non c'è soluzione in $\mathcal{S}/\mathcal{Q}$. Tuttavia in generale $h$ potrebbe non essere irriducibile su $\widetilde{k}$. Nell'ipotesi che $g$ abbia grado al più 3 in $Y$, dal fatto che $h$ non abbia radici segue la sua irriducibilità.

Vorremmo trovare un primo $\mathcal{Q}$ di $\mathcal{S}$ con le seguenti proprietà.

i) La congruenza $h(Y) \equiv 0 \pmod{\mathcal{Q}}$ non ha soluzioni;

ii) esistono infiniti $n$ tali che

$$\begin{cases} n \equiv \zeta_{p-1}^{h_0} & \pmod{\mathcal{Q}} \\ \gamma_j^n \equiv \zeta_m^{h_j} & \pmod{\mathcal{Q}} \quad j = 1, \ldots, r. \end{cases}$$

Introduciamo a questo scopo il campo $E = k(\zeta_{p-1}, \beta^{1/m}, \delta_1^{1/m}, \ldots, \delta_r^{1/m})$. Osserviamo che l'equazione $h(Y) = 0$ non ha soluzione nemmeno in $E$. Infatti sia $y$ una soluzione dell'equazione: allora $[\widetilde{k}(y) : \widetilde{k}] \leq d$, dove $d$ è il grado in $y$ di $g$, mentre $[E : \widetilde{k}]$ è un divisore di una potenza di $m$ per teoria di Kummer. Poiché ogni fattore primo di $m$ è $> L \geq d$ troviamo che $y \notin E$.

Osserviamo che

$$[E : k(\zeta_{p-1}, \delta_1^{1/m}, \ldots, \delta_r^{1/m})] = m. \tag{4.7.1}$$

Se infatti il grado fosse minore, visto che le radici $m$-esime dell'unità stanno nel campo base, sarebbe un divisore proprio di $m$ per la Proposizione (1.3.1). Sia $\ell$ un primo tale che il grado divida $m/\ell$. Applichiamo il Teorema di Kummer (1.3.3) al campo $\widetilde{k}$: i due gruppi

$$\begin{aligned} \Delta =& \langle (\widetilde{k}^*)^m, \beta, \delta_1, \ldots, \delta_r \rangle \\ \Delta' =& \langle (\widetilde{k}^*)^m, \beta^\ell, \delta_1, \ldots, \delta_r \rangle \end{aligned}$$

corrispondono alla stessa estensione $E/k$, perciò devono coincidere. In particolare

$$\beta = \alpha^m \beta^{\ell a_0} \delta_1^{a_1} \cdots \delta_r^{a_r}$$

per un certo $\alpha \in \widetilde{k}$. Ma questo è in contraddizione con il Lemma 4.5.1: infatti, essendo un divisore primo di $m$, $\ell > L$, e possiamo applicare il lemma con $M = 1$.

*A questo punto abbandoniamo la generalità in cui stiamo lavorando e ci restringiamo ai due casi in cui dimostreremo il teorema. Fattorizzando ulteriormente h sarebbe possibile proseguire ancora un po' nel caso generale, ma evitiamo di farlo per non appesantire la notazione.*

Poiché l'estensione $E/k(\zeta_{p-1}, \delta_1^{1/m}, \ldots, \delta_r^{1/m})$ è ciclica possiamo prendere un generatore $\tau$ del suo gruppo di Galois.

**Lemma 4.7.1** *Supponiamo che $h$ sia irriducibile. Sia $E'$ il campo di spezzamento di $h(Y)$ su $E$. Allora esiste $\xi \in G_{E'/\widetilde{k}}$ tale che ristretto a $E$ coincide con $\tau$, ma è esteso in modo che $\xi(y) \neq y$ per ogni radice $y$ di $h$.*

**Dim.** Per prima cosa cosa costruiamo $\sigma \in G = G_{E'/\widetilde{k}}$ con la proprietà che $\sigma(y) \neq y$ per ogni radice $y$ di $h$. Perché questo sia verificato è sufficiente che $\sigma$ non sia contenuto nell'unione degli stabilizzatori delle radici di $h$. Sia $H$ uno di questi stabilizzatori: essendo $h$ irriducibile $G$ agisce transitivamente sulle radici, e dunque gli altri stabilizzatori sono i coniugati di $H$ in $G$. Il numero di coniugati di $H$ è pari a

$$[G : N(H)] \leq [G : H].$$

Poiché la cardinalità di ciascuno stabilizzatore è pari a $|H|$, se $G$ fosse l'unione di essi, quest'unione dovrebbe essere disgiunta. Ma questo non è possibile perché gli stabilizzatori si intersecano almeno nell'identità. Questo ci permette di trovare $\sigma$.

Sia $\widetilde{\sigma} \in G_{E/\widetilde{k}}$ la restrizione di $\sigma$ a $E$, e $\varphi = \widetilde{\sigma}^{-1}\tau$. Ci basta vedere che è possibile estendere $\varphi$ a $E'$ in modo che $\varphi(y) = y$ per ogni radice $y$ di $h$. A questo punto prendiamo $\xi = \sigma\varphi$ e otteniamo la tesi. Se chiamiamo $F$ il campo di spezzamento di $h$ su $\widetilde{k}$, in modo che $E' = EF$, ci riconduciamo a verificare che $E$ e $F$ sono linearmente disgiunti, cioè $E \cap F = \widetilde{k}$. Quest'ultima conclusione segue per motivi di grado: infatti $[F : \widetilde{k}]$ è un divisore di $d!$, mentre $[E : \widetilde{k}]$ è un divisore di una potenza di $m$, e ogni fattore primo di $m$ è maggiore di $d$.

□

Per quanto osservato possiamo applicare il lemma se $g$ ha grado $\leq 3$, nel qual caso abbiamo visto che $h$ è irriducibile. La conclusione del lemma segue facilmente anche se $g$ è binomiale: in questo basta estendere $\tau$ in modo che $\tau(y) \neq y$ per una radice $y$ di $h$. Poiché le radici di $h$ differiscono tra loro per radici dall'unità in $\widetilde{k}$ dal fatto che $\tau$ ne sposti una segue che le sposta tutte.

Per il teorema di Чеботарев esiste un insieme di densità positiva di primi $\mathcal{Q}$ di $\widetilde{k}$ per cui $\phi(\mathcal{Q}'|\mathcal{Q}) = \xi$ in $E'$, per un opportuno primo $\mathcal{Q}'$ sopra $\mathcal{Q}$. Inoltre possiamo supporre che $f(\mathcal{Q}|q) = 1$ (dove $(q) = \mathcal{Q} \cap \mathbb{Z}$), per il Teorema 1.2.7. Scegliamo un primo $\mathcal{Q}$ fra questi di norma sufficientemente grande, e per il quale siano definite le riduzioni di $\beta$, dei $\gamma_j$ e di $f$.

Per un tale primo la congruenza $h(Y) \equiv 0 \pmod{\mathcal{Q}}$ non ha soluzione. Infatti $h$ ha radici distinte mod $\mathcal{Q}$ (se $q$ è abbastanza grande); se $y$ è una radice di $h$ allora sappiamo che $\xi(y) \neq y$. Perciò $\xi(y) - y$ è non nullo per ciascuna radice $y$; se $\mathcal{Q}'$ non fa parte dei divisori di nessuno di questi termini avremo anche $\xi(y) \not\equiv y \pmod{\mathcal{Q}'}$. Perciò il Frobenius di $\mathbb{F}_q$ non fissa $\overline{y} \in \overline{\mathbb{F}_q}$, e $h$ non ha radici mod $\mathcal{Q}$.

A questo punto non ci resta che controllare le riduzioni dei $\gamma_j$ e di $n$. Innanzitutto $q$ si spezza completamente in $\mathbb{Q}(\zeta_{p-1})$. Di conseguenza $q \equiv 1 \pmod{p-1}$, e in particolare $m|q-1$. Poiché $\xi$ fissa $\delta_j^{1/m}$ ciascun $\delta_j$ è una potenza $m$-esima mod $\mathcal{Q}$, cioè

$$\delta_j^{\frac{q-1}{m}} \equiv 1 \pmod{\mathcal{Q}}.$$

Similmente $\xi(\beta) = \zeta_m^a \beta$ per un certo $a$, che è coprimo con $m$ per la (4.7.1), e dunque

$$\beta^{\frac{q-1}{m}} \equiv \zeta_m^a \pmod{\mathcal{Q}}.$$

Mettendole insieme ricaviamo

$$\gamma_j^{\frac{q-1}{m}} \equiv \zeta_m^{ah_j} \pmod{\mathcal{Q}}.$$

Se $b$ è inverso di $a \bmod m$ troviamo allora

$$\gamma_j^{b\frac{q-1}{m}} \equiv \zeta_m^{h_j} \pmod{\mathcal{Q}}.$$

Inoltre possiamo prendere $c \in \mathbb{N}$ con $c \equiv \zeta_{p-1} \pmod{\mathcal{Q}}$. Per finire sia $n \in \mathbb{N}$ soluzione delle due congruenze

$$n \equiv c^{h_0} \pmod{q}, \qquad n \equiv b\frac{q-1}{m} \pmod{q-1}.$$

Con questa scelta valgono le condizioni i) e ii) enunciate all'inizio della sezione.

A questo punto possiamo trovare la contraddizione che stavamo cercando. Per ipotesi l'equazione

$$g(b(n), Y) = g(f(n, \gamma_1^n, \ldots, \gamma_r^n), Y) = S(n, \gamma_1^n, \ldots, \gamma_r^n, Y) = 0$$

ha soluzione in $k$. Allo stesso tempo abbiamo le due condizioni

$$\begin{aligned} n &\equiv \zeta_{p-1}^{h_0} \pmod{\mathcal{Q}} \\ \gamma_j^n &\equiv \zeta_m^{h_j} \pmod{\mathcal{Q}}, \end{aligned}$$

che ci garantiscono che

$$S(n, \gamma_1^n, \ldots, \gamma_r^n, Y) \equiv S(\zeta_{p-1}^{h_0}, \zeta_m^{h_1}, \ldots, \zeta_m^{h_r}, Y) \equiv h(Y) \pmod{\mathcal{Q}}.$$

Questo è assurdo perché $h$ non ha soluzioni $\bmod \mathcal{Q}$, e pertanto il Teorema 4.1.1 risulta provato

□

## 4.8 Come affrontare il caso generale

Vediamo quale potrebbe essere un approccio per il caso generale. Il punto difficoltoso è garantire in generale che il polinomio $h$ definito all'inizio della Sezione 4.7 sia irriducibile. Questo passo è fondamentale per ottenere il risultato del Lemma 4.7.1, che a sua volta permette l'applicazione del teorema di Чеботарев.

La tecnica che abbiamo usato, legata alle stime del teorema di Lang-Weil, non va molto lontano dall'obiettivo, garantendo che $h$ non abbia radici. In effetti mantenere l'irriducibilità di un polinomio tramite specializzazione è equivalente a garantire che la specializzazione di un certo numero di polinomi ausiliari non abbia radici. Infatti abbiamo la

**Proposizione 4.8.1** *Sia $a(X, Y) \in K[X, Y]$ un polinomio irriducibile monico in $Y$. Allora esistono dei polinomi irriducibili $h_J(X, Y) \in K[X, Y]$ con la seguente proprietà: se $t \in K$ è tale che nessuno dei polinomi $h_J(t, Y)$ abbia radici in $K$, allora $a(t, Y)$ è irriducibile su $K$.*

**Dim.** Vediamo $a$ come polinomio in $Y$ sul campo $K(X)$ e fattorizziamolo in una chiusura algebrica come

$$a(X,Y) = (Y-\alpha_1)\cdots(Y-\alpha_d).$$

Fissato un $t \in K$ consideriamo l'omomorfismo di specializzazione

$$\begin{array}{ccc} K[X] & \longrightarrow & K \\ X & \longrightarrow & t. \end{array}$$

Questo può essere esteso agli $\alpha_i$, che sono interi su $K[X]$, a valori in un'estensione finita di $K$ (per maggiori dettagli sulla costruzione di specializzazioni si veda il Capitolo 5). Dunque otteniamo

$$a(t,Y) = (Y-\alpha_1(t))\cdots(Y-\alpha_d(t)).$$

Supponiamo adesso che $a(t,Y)$ sia riducibile: questo significa che avremo un prodotto parziale non banale

$$\prod_{j\in J}(Y-\alpha_j(t))$$

a coefficienti in $K$, per un certo insieme di indici $J$. Consideriamo in corrispondenza il prodotto

$$\prod_{j\in J}(Y-\alpha_j):$$

questo per ipotesi non è a coefficienti in $K(X)$, dunque esiste almeno un coefficiente $\omega_J$ che non sta in $K(X)$. Indichiamo con $g_J \in K[X][Y]$ il polinomio minimo di $\omega_J$ su $K(X)$.

Per costruzione ciascun $g_J$ è irriducibile su $K(X)$. Inoltre abbiamo visto che se $a(t,X)$ si fattorizza almeno un termine $\omega_J(t)$ sta in $K$, e pertanto $g_J(t,X)$ ammette la radice $\omega_J(t)$.

□

Il fatto di lavorare con la sola variabile $X$ piuttosto che con $X_0,\dots,X_r$ non è realmente restrittivo. Consideriamo infatti il polinomio $\overline{S}_D(X_0,\dots,X_r,Y)$ (con le notazioni della dimostrazione) e fissiamo una costante $A$ grande rispetto al grado totale di $\overline{S}_D$. Non è difficile vedere che allora il polinomio

$$F(X,Y) = \overline{S}_D(X,X^A,\dots,X^{A^r},Y)$$

è a sua volta assolutamente irriducibile. La proposizione precedente, applicata a $F(X,Y)$ ci fornisce un numero finito di polinomi assolutamente irriducibili $g_J(X,Y)$.

A questo punto possiamo applicare il procedimento con Lang-Weil a ciascun termine $g_J(X,Y)$, utilizzando sempre lo stesso primo $p$. Otteniamo così il seguente risultato: per un'opportuna scelta di interi $h_J$ il polinomio $g_J(\zeta_{p-1}^{h_J},Y)$ non ha soluzioni. Se questi interi $h_J$ potessero essere scelti tutti uguali tra loro, $h_J = h$ (e sarebbe comodo averli indipendenti anche dal fattore $\overline{S}_D$ considerato), otterremmo l'irriducibilità del polinomio

$$F(\zeta_{p-1}^h,Y) = \overline{S}_D(\zeta_{p-1}^h,\zeta_{p-1}^{hA},\dots,\zeta_{p-1}^{hA^r},Y).$$

Questo è esattamente ciò di cui abbiamo bisogno per portare avanti il resto della dimostrazione.

Il problema è diventato perciò quello di applicare Lang-Weil a più di un polinomio $g_J(X,Y)$, ottenendo per ciascun polinomio la stessa radice dell'unità $\zeta_{p-1}^h$ con la proprietà che $g_J(\zeta_{p-1}^h, Y)$ non ha soluzioni in $\widetilde{k}$. Un'idea in questa direzione può essere la seguente: il polinomio $g_J(\zeta_{p-1}^{h_J}, Y)$ non ha radici in $\widetilde{k}$ e dunque lo stesso vale per i suoi coniugati su $k$, che sono della forma

$$g_J(\zeta_{p-1}^{ah_J}, Y) \tag{4.8.1}$$

per opportuni $a$ coprimi con $p-1$. La situazione migliore è quella in cui $k \cap \mathbb{Q}_c = \mathbb{Q}$, nel qual caso i coniugati di $g_J(\zeta_{p-1}^{h_J}, Y)$ sono dati dalla (4.8.1) *per ogni* $a$ coprimo con $p-1$.

Mettiamoci per semplicità in questo secondo caso (anche se in generale non cambia molto, grazie al fatto che $k \cap \mathbb{Q}_c \subset \mathbb{Q}(\zeta_D)$ e $D$ è fissato una volta per tutte prima della scelta di $p$). Quello che abbiamo visto è che se tutti gli $h_J$ possono essere scelti coprimi con $p-1$, coniugando su $k$ ci si può ricondurre al caso in cui siano tutti uguali, e quindi concludere. Vediamo come le stime legate a Lang-Weil ci potrebbero consentire di ottenere questa conclusione più forte, nonostante i termini $\zeta_{p-1}^a$ al variare di $a$ coprimo con $p-1$ rappresentino solo $\varphi(p-1)$ classi $\bmod\, p-1$.

Fissato uno dei polinomi $g_J$ poniamo

$$G_J(Z,Y) = g_J(Z^D, Y).$$

Quello che vogliamo fare è trovare una classe $z \bmod p$ che sia un generatore per $\mathbb{F}_p^*$ e tale che la congruenza

$$G_J(z,Y) \equiv 0 \pmod p \tag{4.8.2}$$

non abbia soluzioni in $\mathbb{F}_p$. Ciò fatto proseguiamo come abbiamo delineato sopra. Scelto $h_J$ in modo che $\zeta_{p-1}^{h_J} \equiv z \pmod p$, l'equazione

$$g_J(\zeta_{p-1}^{Dh_J}, Y) = 0$$

non ha soluzioni in $\widetilde{k}$, e coniugando ci riconduciamo al caso in cui tutti gli $h_J$ siano uguali.

Supponiamo dunque per assurdo che la (4.8.2) abbia soluzione per ogni generatore $z$ di $\mathbb{F}_p^*$. Sfruttando il fatto che $G_J$ dipende solo da $z^D$ e non da $z$, troviamo altri elementi che danno luogo a soluzioni per la (4.8.2). Precisamente la (4.8.2) avrà soluzione anche se $z^D = w^D$, dove $w$ è un generatore. Ricordando la scrittura $p-1 = dM$, dove possiamo prendere $D$ ed $m$ primi fra loro, otteniamo l'isomorfismo

$$\mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/D\mathbb{Z}.$$

Utilizzando questo isomorfismo troviamo che il numero di elementi $z$ per cui esiste un generatore $w$ tale che $z^D = w^D$ è $D\phi(m)$.

Nel caso in cui i polinomi $G_J$ siano a loro volta assolutamente irriducibili possiamo applicare il meccanismo della sezione 4.6; questo darà un assurdo se $\phi(m)$ non è molto più piccolo di $m$. Un metodo per ottenere questo è usare una forma effettiva del teorema di Чеботарев, che ci garantisca che $p$ può essere preso non troppo grande in termini di $k$. Una stima del genere, unita al fatto che ogni fattore primo di $m$ è maggiore o uguale a $L$, limita il numero di fattori primi che $m$ può avere. Poiché questi sono sufficientemente grandi otteniamo di conseguenza una stima dal basso per $\phi(m)$.

L'ostacolo a questo approccio è il fatto che, al contrario, $p$ deve essere abbastanza grande affinché il teorema di Lang-Weil dia informazioni utili. Non è del tutto chiaro al momento se $p$ possa essere scelto di un ordine di grandezza adatto per far funzionare entrambe le cose; verificare se questo sia possibile richiede di avere a disposizione versioni molto sharp sia del teorema di Lang-Weil che della forma effettiva di Чеботарев. Ad ogni modo ci riproponiamo di completare i dettagli di questo approccio per un prossimo articolo.

# Capitolo 5

# Specializzazione

I know the answer! The answer lies within the heart of all mankind! The answer is twelve? I think I'm in the wrong building.

*Lucy van Pelt* (The Peanuts)

## 5.1 Introduzione e strategia

Nei capitoli precedenti abbiamo ottenuto teoremi di razionalità per le serie di potenze che siano soluzioni di equazioni nell'anello di Hadamard. Il contesto in cui abbiamo lavorato è quello delle serie di potenze su un campo di numeri $k$. In questo capitolo, tramite argomenti di specializzazione, vogliamo estendere questi risultati al caso di un campo $K$ che sia finitamente generato su $\mathbb{Q}$, seguendo [Rum87] e [RvdP87a]. Precisamente vogliamo ottenere i seguenti risultati.

**Teorema 5.1.1** *Sia $K$ un campo di caratteristica $0$ e siano $\sum b_k x^k$ e $\sum c_k x^k$ le serie di Taylor di due funzioni razionali. Supponiamo che $b_k \neq 0$ per ogni $k$, e poniamo $a_k = c_k / b_k$. Allora $\sum a_k x^k$ è razionale se e solo se esiste un anello $A$ finitamente generato su $\mathbb{Z}$ contenente tutti gli $a_k$.*

**Teorema 5.1.2** *Sia $K$ un campo finitamente generato su $\mathbb{Q}$ e $g(X,Y) \in K[X,Y]$ un polinomio monico in $Y$. Sia $f \in \mathcal{H}(K)$ e supponiamo che l'equazione $g(f,Y) = 0$ abbia soluzione in $K_1[[t]]_H$, dove $K_1/K$ è un'estensione finita. Allora esiste un'estensione finita $K_2/K$ tale che $g(f,Y) = 0$ abbia soluzione in $\mathcal{H}(K_2)$.*

Nel Teorema 5.1.1 in effetti non è necessaria l'ipotesi che $K$ sia un campo finitamente generato. Abbiamo già osservato nella sezione 3.1 che una delle due implicazioni è banale: se $\sum a_k x^k$ è la serie di Taylor di una funzione razionale, allora il valore di $a_k$ è espresso da un polinomio esponenziale, per $k$ grande, e dunque gli $a_k$ stanno nell'anello generato dai coefficienti e dalle radici del polinomio esponenziale. Per dimostrare il viceversa abbiamo come ipotesi che tutti i termini coinvolti (gli $a_k$, i $b_k$ e i $c_k$) appartengano ad un sottoanello finitamente generato $A$ di $K$. Di conseguenza ci possiamo limitare a lavorare con il campo dei quozienti di

$A$, riconducendoci così a dimostrare il teorema nel caso di un campo $K$ finitamente generato.

La strategia per dimostrare i due teoremi è essenzialmente la stessa. Descriviamo il caso del quoziente. Poiché $K$ è finitamente generato, si può vedere come un'estensione finita di $\mathbb{Q}(X_1, \ldots, X_n)$. Scegliamo $n$ numeri algebrici $\alpha_1, \ldots, \alpha_n$ e chiamiamo $R(\alpha_1, \ldots, \alpha_n)$ l'anello delle funzioni razionali $f \in \mathbb{Q}(X_1, \ldots, X_n)$ che non hanno poli in $(\alpha_1, \ldots, \alpha_n)$. Abbiamo un naturale omomorfismo $\phi$ di valutazione definito su $R(\alpha_1, \ldots, \alpha_n)$:

$$f(X_1, \ldots, X_n) \xmapsto{\phi} f(\alpha_1, \ldots, \alpha_n).$$

Tale omomorfismo si può estendere alla chiusura integrale $S(\alpha_1, \ldots, \alpha_n)$ dell'anello $R(\alpha_1, \ldots, \alpha_n)$ in $K$.

Supponiamo ora di scegliere $\alpha_1, \ldots, \alpha_n$ in modo che $A \subset S(\alpha_1, \ldots, \alpha_n)$. Il teorema del quoziente per campi di numeri si applica alla successione $\phi(a_k)$, e di conseguenza $\phi(a_k)$ coincide con un polinomio esponenziale $q(k)$ per tutti i $k$ con $\phi(b_k) \neq 0$. Questo garantisce l'annullamento dei determinanti di Kronecker-Hankel

$$K_h(\phi(a)) = \phi(K_h(a)),$$

almeno finché $\phi(b_h) \neq 0$, e per $h$ più grande dell'ordine di $q$.

Per tornare indietro avremmo bisogno di garantirci che se $K_h(a) \neq 0$, allora $\phi(K_h(a)) \neq 0$, cioè abbiamo degli elementi non nulli e vorremmo che la loro specializzazione fosse non nulla. Questo è facile da fare, ma solo per un numero finito di elementi. Fissiamo allora una costante $\Lambda$ e costruiamo la specializzazione in modo che $\phi(b_k) \neq 0$ per $k \leq \Lambda$ e $\phi(K_h(a)) \neq 0$ per $k \leq \Lambda$ e $K_h(a) \neq 0$.

In questo modo otteniamo che $K_h(a) \neq 0$ per $h$ compreso tra l'ordine di $q$ e $\Lambda$. Dunque $a_k$ coincide con un polinomio esponenziale $p$ nello stesso intervallo. Su quell'intervallo abbiamo

$$p(h)b_k - c_k = 0.$$

Se l'intervallo è abbastanza grande rispetto all'ordine di $p$ (gli ordini di $c_h$ e $b_h$ sono fissati) quest'equazione vale identicamente.

Il problema diventa quindi di stimare a priori l'ordine di $p$ e di $q$. La stima a priori dell'ordine di $p$ è fattibile, e la stessa stima si porta anche a $q$, ma a condizione che la specializzazione abbia una proprietà ulteriore. C'è bisogno che l'omomorfismo di specializzazione conservi l'indipendenza moltiplicativa in un sottogruppo fissato di $K^*$, che risulta finitamente generato.

Di conseguenza il capitolo inizia con uno studio delle specializzazioni, che è indipendente dal resto e fornisce un teorema di esistenza per specializzazioni con buone proprietà. La prima cosa da studiare saranno le relazioni moltiplicative in un campo di numeri. Fatto questo introdurremo una funzione grado su $K^*$ e la useremo per dimostrare il teorema di specializzazione. A questo punto potremo passare alla stima a priori ed infine mettere tutto insieme nella successiva sezione. Il caso della radice è del tutto analogo ed è trattato nell'ultima sezione.

## 5.2 Relazioni moltiplicative

Passiamo dunque a studiare le relazioni moltiplicative tra elementi di un campo di numeri $k$. I teoremi di Northcott e di Kronecker (1.6.3, 1.6.2) ci garantiscono che fissato un intero $D$ esiste $\lambda(D) > 0$ con la proprietà che se $[k : \mathbb{Q}] \le D$ e $\alpha \in k^*$ con $h(\alpha) \le \lambda(D)$, allora $\alpha$ è una radice dell'unità. Inoltre indichiamo con $\omega(k)$ il numero di radici dell'unità nel campo $k$.

Il nostro scopo è quello di mostrare che se degli elementi di $k^*$ sono dipendenti, allora soddisfano una relazione con coefficienti che riusciamo a limitare in termini della loro altezza.

**Lemma 5.2.1 (Loxton, Van der Poorten)** *Sia $k$ un campo di numeri, con $[k : \mathbb{Q}] = D$, e $\alpha_1, \dots, \alpha_n \in k$. Se gli $\alpha_i$ sono moltiplicativamente dipendenti allora è possibile trovare una relazione*

$$\alpha_1^{q_1} \alpha_2^{q_2} \cdots \alpha_n^{q_n} = 1$$

*dove i $q_i$ sono interi non tutti nulli e*

$$|q_j| \le (n-1)!\, \omega(k) \prod_{i \ne j} \frac{h(\alpha_j)}{\lambda(D)}. \tag{5.2.1}$$

**Dim.** Innanzitutto non è restrittivo supporre che nessun sottoinsieme proprio di $\{\alpha_1, \dots, \alpha_n\}$ sia dipendente. Di conseguenza se $(b_1, \dots, b_n)$ è una relazione non banale avremo $b_j \ne 0$ per ogni $j$. In queste ipotesi esiste una relazione minima $(q_1, \dots, q_n) \in \mathbb{Z}^n$, tale che ogni relazione tra $\alpha_1, \dots, \alpha_n$ è multipla di questa. Infatti sia $\mathbf{q} = (q_1, \dots, q_n)$ una relazione con $|q_1|$ minimo. Poiché le relazioni formano un sottogruppo di $\mathbb{Z}^n$ se $\mathbf{b} = (b_1, \dots, b_n)$ è un'altra relazione si avrà $b_1 = cq_1$ per un certo $c \in \mathbb{Z}$. La relazione $\mathbf{b} - c\mathbf{q}$ ha il primo termine nullo, perciò è identicamente nulla, e $\mathbf{b} = c\mathbf{q}$.

Dobbiamo vedere che per ciascun termine $q_j$ vale la stima (5.2.1). Per la minimalità ci basta vedere che per ogni $j$ esiste una relazione $\mathbf{a} = (a_1, \dots, a_n)$ tale che

$$|a_j| \le (n-1)!\, \omega(k) \prod_{i \ne j} \frac{h(\alpha_j)}{\lambda(D)}.$$

Partiamo da una qualsiasi relazione $(b_1, \dots, b_n)$. Fissata una $n$-upla di numeri positivi $\mathbf{t} = (t_1, \dots, t_n)$ indichiamo

$$E(\mathbf{t}) = \left\{ (x_1, \dots, x_n) \in \mathbb{R}^n : \sum_{i \ne j} t_i \left| x_i - \frac{b_i}{b_j} x_j \right| < 1; \quad |x_j| \le t_j \right\}.$$

È immediato verificare che $E(\mathbf{t})$ è convesso e simmetrico rispetto all'origine. Il nostro scopo è applicare il teorema di Minkowksi ([Mil98, cap. 4]) al corpo convesso $E(\mathbf{t})$ e al reticolo $\mathbb{Z}^n \subset \mathbb{R}^n$. In questa direzione calcoliamo il volume di $E(\mathbf{t})$. Il cambio di variabile lineare

$$\begin{cases} y_i &= t_i(x_i - \frac{b_i}{b_j} x_j) \text{ se } i \ne j \\ y_j &= x_j \end{cases}$$

è espresso da una matrice di determinante $\prod_{i \ne j} t_i$. Il convesso $E(\mathbf{t})$ viene mandato nell'insieme

$$\left\{ (y_1, \dots, y_n) \in \mathbb{R}^n : \sum_{i \ne j} |y_i| < 1; \quad |y_j| \le t_j \right\},$$

il cui volume è

$$\frac{2^{n-1}}{(n-1)!} \cdot (2t_j);$$

pertanto

$$\mathrm{vol}(E(\mathbf{t})) = \frac{2^n t_j}{(n-1)! \prod_{i \neq j} t_i}.$$

Scegliamo allora

$$\begin{cases} t_i &= \frac{h(\alpha_i)}{\lambda(D)} \text{ se } i \neq j \\ t_j &= (n-1)! \prod_{i \neq j} t_i. \end{cases}$$

Il teorema di Minkowski ci garantisce l'esistenza di un punto $(a_1, \ldots, a_n) \in E(\mathbf{t})$ a coordinate intere diverso dall'origine. Poniamo $\alpha = \alpha_1^{a_1} \alpha_2^{a_2} \cdots \alpha_n^{a_n}$. Se $v$ è un valore assoluto troviamo

$$\log |\alpha|_v = \sum_{i=1}^{n} a_i \log |\alpha_i|_v.$$

Allo stesso tempo, essendo $\mathbf{b}$ una relazione, abbiamo

$$\sum_{i=1}^{n} b_i \log |\alpha_i|_v = 0.$$

Mettendole insieme si ricava

$$\log |\alpha|_v = \sum_{i \neq j} a_i - \frac{b_i}{b_j} a_j \log |\alpha_i|_v. \tag{5.2.2}$$

Poiché questo vale per ogni valore assoluto $v$, otteniamo una relazione tra le altezze. Se indichiamo $\log^+(x) = \max\{\log(x), 0\}$, la (5.2.2) ci dà

$$\log^+ |\alpha|_v + \log^+ |\alpha^{-1}|_v = |\log |\alpha|_v| \leq \sum_{i \neq j} \left| a_i - \frac{b_i}{b_j} a_j \log |\alpha_i|_v \right| =$$

$$= \sum_{i \neq j} \left| a_i - \frac{b_i}{b_j} a_j \right| (\log^+ |\alpha_i|_v + \log^+ |\alpha_i^{-1}|_v).$$

In termini di altezze otteniamo

$$h(\alpha) + h(\alpha^{-1}) \leq \sum_{i \neq j} \left| a_i - \frac{b_i}{b_j} a_j \right| \left( h(\alpha_i) + h(\alpha_i^{-1}) \right).$$

Usando il fatto che $h(x) = h(x^{-1})$ e che $(a_1, \ldots, a_n) \in E(\mathbf{t})$ ricaviamo

$$h(\alpha) \leq \sum_{i \neq j} \left| a_i - \frac{b_i}{b_j} a_j \right| h(\alpha_i) = \lambda(D) \left( \sum_{i \neq j} \left| a_i - \frac{b_i}{b_j} a_j \right| t_i \right) < \lambda(D).$$

Di conseguenza $\alpha$ è una radice dell'unità, perciò $\alpha^{\omega(k)} = 1$, da cui segue che $(\omega(k)a_1, \ldots, \omega(k)a_n)$ è una relazione. Il suo $j$-esimo termine soddisfa

$$|\omega(k) a_j| \leq |\omega(k) t_j| = (n-1)!\, \omega(k) \prod_{i \neq j} \frac{h(\alpha_j)}{\lambda(D)},$$

che è la nostra tesi.

□

Una forma più debole, ma più semplice, del lemma è il seguente

**Corollario 5.2.2** *Siano dati $D$ e $n$ interi positivi: allora possiamo trovare un numero $\Omega(D,n) = \Omega(D) > 0$ tale che se $k$ è un campo di numeri di grado al più $D$ su $\mathbb{Q}$ e $\alpha_1, \dots, \alpha_n \in k$ sono dipendenti e di altezza limitata da $H$, allora esiste una relazione non banale*

$$\alpha_1^{q_1}\alpha_2^{q_2}\cdots\alpha_n^{q_n} = 1$$

*dove*

$$|q_j| \leq \Omega(D)H^{n-1}.$$

## 5.3 Il teorema di specializzazione

Per proseguire introduciamo una funzione grado per gli elementi di $K$. Questa sarà una funzione

$$\deg : K \longmapsto \mathbb{N}$$

di cui saremo in grado di controllare il comportamento rispetto alle operazioni. Più precisamente troveremo due costanti $A, D \in \mathbb{N}$ per cui

$$\begin{aligned} \deg(-a) &= \deg(a) \\ \deg(a+b) &\leq \deg(a) + \deg(b) \\ \deg(ab) &\leq \deg(a) + \deg(b) + A \\ \deg(a^{-1}) &\leq D(\deg(a) + A) \end{aligned} \tag{5.3.1}$$

per ogni $a, b \in K^*$.

Per ipotesi $K/\mathbb{Q}$ è un'estensione finitamente generata, e dunque esiste una base di trascendenza finita $\{x_1, \dots, x_m\}$. Il teorema dell'elemento primitivo ci permette di scrivere

$$K = \mathbb{Q}(x_1, \dots, x_m)[y]$$

per un opportuno $y \in K$. Scriviamo esplicitamente il polinomio minimo di $y$ su $\mathbb{Q}(x_1, \dots, x_m)$ come

$$F(\mathbf{x}, y) = y^D + F_1(\mathbf{x})y^{D-1} + \cdots + F_D(\mathbf{x}),$$

dove $\mathbf{x} = (x_1, \dots, x_m)$. In realtà possiamo moltiplicare $y$ per un elemento di $\mathbb{Q}(x_1, \dots, x_m)$ e supporre così che $F_i(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_m]$ per ciascun $i$.

A questo punto scriviamo un elemento $a \in K^*$ nella forma

$$a = \frac{U_a(\mathbf{x}, y)}{V_a(\mathbf{x})}.$$

Per rendere unica la scrittura scegliamo $U_a$ di grado inferiore a $D$ e senza fattori comuni con $V_a$. In questo modo i due polinomi sono determinati a meno di cambiamento di segno. Chiamiamo $\deg(a)$ il massimo tra il grado totale nelle $\mathbf{x}$ di $U_a$ e $V_a$. Più esplicitamente scriviamo

$$U_a(\mathbf{x}, y) = \sum_{i=0}^{D-1} U_{a,i}(\mathbf{x})y^i,$$

di modo che

$$\deg(a) = \max\{\deg(V_a), \deg(U_{a,0}), \dots, \deg(U_{a,D-1})\}.$$

Passiamo dunque a dimostrare le relazioni 5.3.1. Per fare questo consideriamo $K$ come uno spazio vettoriale di dimensione $D$ su $\mathbb{Q}(x_1, \dots, x_m)$ e associamo all'elemento $a$ l'applicazione lineare data dalla moltiplicazione a sinistra per $a$. Rispetto alla base $\{1, y, \dots, y^{D-1}\}$ questa si rappresenta con una matrice

$$M(a) = \frac{1}{V_a(\mathbf{x})} \begin{pmatrix} U_{a,0\,0}(\mathbf{x}) & \cdots & U_{a,0\,D-1}(\mathbf{x}) \\ \vdots & \ddots & \vdots \\ U_{a,D-1\,0}(\mathbf{x}) & \cdots & U_{a,D-1\,D-1}(\mathbf{x}) \end{pmatrix}.$$

È immediato dalle definizioni che sulla prima colonna si trovano i termini $U_{a,i\,0}(\mathbf{x}) = U_{a,i}(\mathbf{x})$ definiti in precedenza. Per trovare le altre entrate scriviamo innanzitutto le potenze di $y$ nella forma

$$y^k = \sum_{i=0}^{D-1} F_{k,i}(\mathbf{x}) y^i.$$

Si calcola allora che

$$U_{a,i\,j}(\mathbf{x}) = \sum_{k=0}^{D-1} F_{k+j,i}(\mathbf{x}) U_{a,k}(\mathbf{x}).$$

Questo ci dà la stima

$$\deg(U_{a,i\,j}) \leq \deg(a) + A,$$

dove

$$A = \max_{\substack{0 \leq k \leq 2D-2 \\ 0 \leq i \leq D-1}} (\deg(F_{k,i})).$$

Dimostrare a questo punto le relazioni (5.3.1) è facile. Infatti il grado di $a$ è il massimo tra il grado di $V_a$ e i gradi dei polinomi sulla prima colonna di $M(a)$. Di conseguenza i gradi di $a + b$, $ab$ e $a^{-1}$ si stimano se maggioriamo i gradi dei polinomi sulle prime colonne delle matrici relative a questi elementi. Questo si fa facilmente esplicitando le operazioni di somma, prodotto e inverso di matrici. Ad esempio il generico elemento sulla prima colonna di $M(a + b)$ è

$$\frac{U_{a,i\,0} V_b + U_{b,i\,0} V_a}{V_a V_b},$$

da cui la prima disuguaglianza. Le altre si ottengono analogamente utilizzando la moltiplicazione riga per colonna e l'inversione di matrici con la regola di Cramer.

Veniamo adesso al vero e proprio argomento di specializzazione. Data una $m$-upla $\mathbf{c} = (c_1, \dots, c_m) \in \mathbb{Z}^m$ abbiamo l'omomorfismo di valutazione

$$\begin{aligned} \mathbb{Q}[x_1, \dots, x_m] &\longmapsto \mathbb{Q} \\ x_i &\longmapsto c_i. \end{aligned}$$

Questo si estende a $\mathbb{Q}[x_1, \dots, x_m, y]$ mandando $y$ in una radice $\gamma$ del polinomio $F(\mathbf{c}, y)$. Quello che otteniamo è un omomorfismo

$$\phi : \mathbb{Q}[x_1, \dots, x_m, y] \longmapsto k,$$

dove $k$ è un campo di numeri di grado al più $D$ su $\mathbb{Q}$. In realtà $\phi$ si può estendere all'anello degli elementi $a \in K$ per cui $V_a(\mathbf{c}) \neq 0$, ponendo

$$\phi(a) = \frac{U_a(\mathbf{c}, \gamma)}{V_a(\mathbf{c})}.$$

Siano ora $R \subset K$ un anello finitamente generato e $S \subset R^*$ un sottogruppo finitamente generato. Costruiamo un insieme finito $\Gamma$ contenente generatori per $R$ (come anello) ed $S$ (come gruppo). Inoltre scegliamo $\Gamma$ in modo che se $a \in \Gamma$, allora anche $a^{-1} \in \Gamma$. Poniamo

$$V_\Gamma(\mathbf{x}) = \prod_{a \in \Gamma} V_a(\mathbf{x}).$$

In questo modo se $V_\Gamma(\mathbf{c}) \neq 0$ l'omomorfismo $\phi$ risulta definito su $R$. Inoltre $\phi(S)$ è contenuto nel sottogruppo degli elementi invertibili di $\phi(R)$: infatti gli elementi di $\Gamma$ non si specializzano a 0, poiché $\phi$ è definito sui loro inversi, perciò le specializzazioni dei generatori di $S$ hanno i loro inversi in $(\phi(R))^*$.

Per costruire elementi $\mathbf{c} \in \mathbb{Z}^m$ per cui $V_\Gamma(\mathbf{c}) \neq 0$ utilizziamo il seguente

**Lemma 5.3.1** *Sia $P(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$ un polinomio non nullo, e sia $B \geq 1$. Allora i vettori $\mathbf{c} \in \mathbb{Z}^m$ che soddisfano $P(\mathbf{c}) = 0$ e $|c_i| \leq B$ sono al più $\deg(P) \cdot (2B+1)^{m-1}$.*

**Dim.** Utilizziamo un'induzione su $m$, il caso $m = 1$ essendo ovvio. Per il passo induttivo sviluppiamo $P$ in potenze di $x_m$:

$$P(x_1, \ldots, x_m) = P_0(x_1, \ldots, x_{m-1})x_m^n + \cdots + P_n(x_1, \ldots, x_{m-1}).$$

Se il grado di $P$ è $d$ allora $\deg(P_0) \leq d - n$, e l'ipotesi induttiva gi garantisce che ci sono al più $(d-n) \cdot (2B+1)^{m-2}$ vettori $(c_1, \ldots, c_{m-1})$ che soddisfano $|c_i| \leq B$ e $P_0(c_1, \ldots, c_{m-1}) = 0$. Per ciascuna $(m-1)$-upla abbiamo al più $2B+1$ scelte per $c_m$, dunque troviamo al più $(d-n) \cdot (2B+1)^{m-1}$ $m$-uple che soddisfano

$$P_0(c_1, \ldots, c_{m-1}) = P(c_1, \ldots, c_m) = 0.$$

Se invece supponiamo che $P_0(c_1, \ldots, c_{m-1}) \neq 0$ ci sono al più $n$ scelte per $c_m$ in modo che $P(c_1, \ldots, c_m) = 0$. Poiché le $(m-1)$-uple che soddisfano la stima sono $(2B+1)^{m-1}$ otteniamo al più $n \cdot (2B+1)^{m-1}$ $m$-uple che soddisfano la tesi e $P_0(c_1, \ldots, c_{m-1}) \neq 0$. In totale abbiamo al più $d \cdot (2B+1)^{m-1}$ scelte per la $m$-upla $\mathbf{c}$.

□

A questo punto possiamo mettere tutto insieme ed ottenere il seguente risultato generale sull'esistenza di buone specializzazioni.

**Teorema 5.3.2** *Sia $K/\mathbb{Q}$ un'estensione finitamente generata. Fissiamo un sottoanello finitamente generato $R \subset K$, un sottogruppo finitamente generato $S < R^*$ e infine un insieme finito $T \subset K$. Allora esiste una specializzazione di $K$ in un campo di numeri $k$ definita su $R$ e su $T$ e tale che:*

*i) gli elementi non nulli di $T$ sono mandati in elementi non nulli;*

*ii) sottoinsiemi moltiplicativamente indipendenti di $S$ restano indipendenti tramite la specializzazione.*

**Dim.** Prendiamo un insieme $\Gamma$ finito contenente $T$ e generatori per $R$ e per $S$. Come sopra richiediamo che se un elemento non nullo $a \in \Gamma$, anche $a^{-1} \in \Gamma$. Siano $s_1, \ldots, s_n$ generatori liberi della parte libera di $S$; supporremmo anche che $s_i \in \Gamma$. La specializzazione $\phi$ sarà indotta da un omomorfismo di valutazione $(x_1, \ldots, x_m) \longmapsto (c_1, \ldots, c_m)$ per un'opportuna $m$-upla $\mathbf{c} \in \mathbb{Z}^m$. Per quanto abbiamo visto sopra otteniamo la tesi (tranne il punto ii)) se ci garantiamo che $V_\Gamma(\mathbf{c}) \neq 0$.

Supponiamo dunque di avere scelto $B$ sufficientemente grande e $\mathbf{c} \in \mathbb{Z}^m$ tale che $|c_i| \leq B$ e $V_\Gamma(\mathbf{c}) \neq 0$. Vogliamo vedere che per $a \in \Gamma$ possiamo stimare

$$h(\phi(a)) \leq M \log B \tag{5.3.2}$$

per un'opportuna costante $M$ dipendente da $\Gamma$ ma non da $\mathbf{c}$. Innanzitutto poiché $\phi(y)$ è intero abbiamo $|\phi(y)|_v \leq 1$ per i valori assoluti non archimedei. Se invece $v$ è un valore assoluto archimedeo indotto da un embedding $\sigma$ di $\mathbb{Q}(\phi(y))$ in $\mathbb{C}$ abbiamo, utilizzando il fatto che i coniugati di $\phi(y)$ sono radici di $F(\mathbf{c}, \cdot)$,

$$|\phi(y)|_v = |\sigma(\phi(y))|_{st} \leq 1 + \sum_{i=1}^{D} |F_i(\mathbf{c})| \leq H \cdot B^K$$

per opportune costanti $H$, $K$ indipendenti da $\mathbf{c}$. Mettendo tutto insieme troviamo

$$h(\phi(y)) \leq L \log B. \tag{5.3.3}$$

Infine la (5.3.2) segue subito dalla (5.3.3) utilizzando le proprietà dall'altezza logaritmica elencate alla fine della sezione 1.6, visto che $\Gamma$ è costituito da un numero finito di funzioni razionali di $y$.

Vogliamo utilizzare tutto questo, insieme al Lemma 5.3.1, per ottenere anche la parte *ii)* della tesi. Sappiamo dal Corollario 5.2.2 che se $\phi(s_1), \ldots, \phi(s_n)$ sono dipendenti, allora esiste una relazione

$$\phi(s_1)^{b_1} \ldots \phi(s_n)^{b_n} = 1$$

per cui

$$|b_i| \leq \Omega(D) M^{n-1} (\log B)^{n-1}. \tag{5.3.4}$$

Sia $\Gamma(B)$ ottenuto da $\Gamma$ aggiungendo tutti gli elementi della forma

$$s_1^{b_1} \ldots s_n^{b_n} - 1,$$

al variare di $b_i$ tra gli interi che soddisfano la (5.3.4), e dei loro inversi.

Quello di cui abbiamo bisogno per concludere è una specializzazione indotta da una $m$-upla $\mathbf{c} \in \mathbb{Z}^m$ per cui $|c_i| \leq B$ e allo stesso tempo $V_{\Gamma B}(\mathbf{c}) \neq 0$. Chiaramente vogliamo usare il Lemma 5.3.1, ma l'ostacolo alla sua applicazione diretta è che il grado di $V_{\Gamma B}(\mathbf{x}$ cresce con $B$. Un'ultima stima su questo grado ci permetterà allora di applicare il lemma e di concludere. È qui che entra in ballo l'utilizzo della funzione deg su $K$.

Definiamo

$$C = \max\{\deg(s_1), \deg(s_1^{-1}), \ldots, \deg(s_n^{-1})\}.$$

In questo modo se abbiamo un elemento

$$s = s_1^{b_1} \dots s_n^{b_n} - 1, \tag{5.3.5}$$

dove i $b_i$ soddisfano la stima (5.3.4), ne limitiamo il grado usando le proprietà (5.3.1):

$$\deg(s) \leq \left( \sum_{i=1}^{n} |b_i| \right) (C+A) \leq n \cdot \Omega(D) \cdot (C+A) \cdot M^{n-1} (\log B)^{n-1} = C_1 (\log B)^{n-1}.$$

Similmente per $s^{-1}$ troviamo

$$\deg(s^{-1}) \leq D(\deg(s) + A) \leq C_2 (\log B)^{n-1}.$$

Il numero totale di elementi $s$ dati dalla (5.3.5) che aggiungiamo è maggiorato da $C_3(\log B)^{(n-1)n}$, avendo $C_3(\log B)^{n-1}$ scelte per ciascun $b_i$. Ne segue una maggiorazione per il grado di $V_{\Gamma(B)}$:

$$\deg(V_{\Gamma(B)}) \leq (C_3 (\log B)^{(n-1)n})(C_1 + C_2)(\log B)^{n-1} \leq C_4 + C_5 (\log B)^{n^2-1}.$$

Basta quindi prendere $B$ sufficientemente grande, in modo che

$$\deg(V_{\Gamma(B)}) \leq 2B + 1,$$

per poter applicare il Lemma 5.3.1. Infatti il numero totale di $m$-uple $\mathbf{c} \in \mathbb{Z}^m$ che soddisfano $|c_i| \leq B$ è $(2B+1)^m$, e questo è più grande di $\deg(V_{\Gamma(B)}) \cdot (2B+1)^{m-1}$. Il lemma ci garantisce allora l'esistenza di una $m$-upla per cui $V_{\Gamma(B)}(\mathbf{c}) \neq 0$, e come abbiamo osservato prima questo è sufficiente ad ottenere la tesi.

□

## 5.4 Il caso del quoziente: stima a priori

Supponiamo ora dati due polinomi esponenziali

$$b(h) = \sum_{i=1}^{l} B_i(h) \beta_i^h, \qquad c(h) = \sum_{i=1}^{m} C_i(h) \gamma_i^h.$$

Quello che vogliamo fare adesso è stimare l'ordine di un possibile polinomio quoziente. Sia dunque

$$a(h) = \sum_{i=1}^{k} A_i(h) \alpha_i^h$$

un polinomio esponenziale a coefficienti in $K$ e supponiamo che $a(h)b(h) = c(h)$ per tutti gli $h$. Indichiamo con $A$, $B$, $C$ i sottogruppi di $K^*$ generati rispettivamente dagli $\alpha_i$, dai $\beta_i$ e dai $\gamma_i$.

**Lemma 5.4.1** *Supponiamo che $a(h)b(h) = c(h)$. Allora, con le notazioni di sopra, $A < \langle B, C \rangle$.*

**Dim.** Supponiamo innanzitutto che $B$ sia libero. Indichiamo con $W$ un sottogruppo finitamente generato contenente $A$, $B$ e $C$, e con $T$ la sua parte di torsione. Fissati dei generatori $w_1, \ldots, w_n$ per la parte libera di $W$, otteniamo un ordine lessicografico sul quoziente $W/T$. Poiché $B$ è libero si proietta iniettivamente $\bmod T$; ne segue che fra le radici di $b(h)$ ce n'è una sola, diciamo $\beta_1$, massima rispetto all'ordine lessicografico. Supponiamo ora per assurdo che $A \not\subset \langle B, C \rangle$ e scegliamo una radice di $a(h)$, diciamo $\alpha_1$, massimale tra quelle non in $\langle B, C \rangle$. Visto che $\alpha_1 \notin \langle B, C \rangle$ il prodotto $\alpha_1 \beta_1$ non compare come radice di $c(h)$, perciò deve cancellarsi con un altro prodotto $\alpha_i \beta_j$. Tuttavia l'uguaglianza $\alpha_1 \beta_1 = \alpha_i \beta_j$ implica che $\alpha_i$ è maggiore di $\alpha_1$ nell'ordine lessicografico (dato che $\beta_1 > \beta_j$). Per massimalità di $\alpha_1$ troviamo che $\alpha_i \in \langle B, C \rangle$ e dunque anche

$$\alpha_1 = \beta_1^{-1} \alpha_i \beta_j \in \langle B, C \rangle,$$

in contrasto con la nostra ipotesi.

Nel caso generale avremo $B \cong \mathbb{Z}^r \times \mathbb{Z}/d\mathbb{Z}$, come abbiamo osservato all'inizio della sezione 2.3. Definiamo polinomi esponenziali ristretti alle progressioni aritmetiche $\bmod d$: $a_{r,d}(h) = a(r + hd)$, e similmente per $b(h)$ e $c(h)$. Le radici dei vari $b_{r,d}(h)$ sono in $B^d$, che è libero, perciò possiamo utilizzare la prima parte della dimostrazione per concludere che le radici dei vari $a_{r,d}(h)$ sono contenute in $\langle B^d, C^d \rangle$. Tuttavia non è difficile vedere che le radici dei vari $a_{r,d}(h)$ generano tutto $A^d$, pertanto otteniamo l'inclusione $A^d < \langle B^d, C^d \rangle$. Sia ora $\alpha$ una radice di $a(h)$: abbiamo ottenuto che $\alpha^d \in \langle B^d, C^d \rangle$, perciò $\alpha$ differisce da un elemento di $\langle B, C \rangle$ per moltiplicazione per una radice $d$-esima dell'unità. Poiché le radici $d$-esime dell'unità stanno in $B$ otteniamo la tesi.

□

La nostra stima è contenuta nella seguente

**Proposizione 5.4.2** *Sia $W$ un sottogruppo finitamente generato di $K^*$, e sia $d$ l'ordine della parte di torsione. Sia $c(h) \in K[h]_W$ e supponiamo che $c$ non si annulli identicamente sulle progressioni aritmetiche* $\bmod d$. *Allora l'ordine di un divisore di $c(h)$ in $K[h]_W$ è limitato da una costante $E$.*

*Inoltre questo bound vale anche per ogni specializzazione di $K$ in un altro campo $L$ purché:*

*i) la specializzazione sia definita su $c(h)$ e su $W$;*

*ii) la parte libera di $W$ sia mandata iniettivamente in $L$;*

*iii) l'immagine di $c(h)$ continui a non annullarsi identicamente sulle progressioni* $\bmod d$.

**Dim.** Supponiamo dapprima che $d = 1$, cioè $W$ sia libero. I risultati della sezione 2.3 ci dicono che

$$K[h]_W \cong K[H, W_1, W_1^{-1}, \ldots, W_n, W_n^{-1}]. \tag{5.4.1}$$

A meno di moltiplicare $c(h)$ per una potenza dei generatori $w_1, \ldots, w_n$ di $W$, che è un'operazione che non cambia l'ordine, possiamo considerare il caso in cui $c(h) \in K[H, W_1, \ldots, W_n]$ (usando l'identificazione (5.4.1)).

Supponiamo ora che $a(h)b(h) = c(h)$ per opportuni $a(h), b(h) \in K[h]_W$. Per il lemma di Gauß$a(h)$ e $b(h)$ sono associati ad elementi di $K[H, W_1, \ldots, W_n]$. Di nuovo non è restrittivo supporre che in effetti $a(h), b(h) \in K[H, W_1, \ldots, W_n]$. Se indichiamo con $N_0$ il grado di $c(h)$ nella variabile $H$ e con $N_i$ il grado nella variabile $W_i$ ($c(h)$ non è identicamente nullo) otteniamo che il numero di monomi di $a(h)$ è al più

$$(N_0 + 1) \cdots (N_n + 1).$$

Il numero di monomi corrisponde tramite l'isomorfismo (5.4.1) all'ordine di $a(h)$ e in questo caso la tesi è dimostrata.

Nel caso generale avremo $d > 1$ e di nuovo introduciamo i polinomi esponenziali $a_{r,d}(h) = a(r + hd)$ (similmente per $b(h)$ e $c(h)$). Nessuno dei polinomi $c_{r,d}(h)$ è nullo, dunque il caso precedente ci garantisce che troviamo dei bound $S_r$ per l'ordine di ciascun $a_{r,d}$. D'altra parte ricostruiamo $a(h)$ tramite

$$a(h) = \frac{1}{d} \sum_{j,k=1}^{d} a_{r,d} \left( \frac{h-k}{d} \right) \zeta_d^{j(h-k)},$$

il che ci permette di stimare l'ordine di $a(h)$ con

$$d(S_1 + \cdots S_d).$$

Infine la stabilità del bound sotto specializzazione è ovvia: è sufficiente ripetere lo stesso argomento sull'immagine di $c(h)$ tramite la specializzazione per trovare la stessa maggiorazione per l'ordine.

□

Supponiamo dunque che $a(h)b(h) = c(h)$ in $K[h]_{esp}$.Il Lemma 5.4.1 ci garantisce di poter trovare a priori un sottogruppo finitamente generato contenente le radici di $a(h)$, nella fattispecie $W = \langle B, C \rangle$. Possiamo allora usare la proposizione precedente per stimare l'ordine del polinomio esponenziale $a(h)$, che è l'obiettivo che ci eravamo prefissi all'inizio della sezione. Inoltre questa stima si può portare alle specializzazioni, purché queste siano scelte appropriatamente (useremo a questo scopo il Teorema 5.3.2).

## 5.5 Il caso del quoziente: conclusione

A questo punto possiamo dimostrare il Teorema del quoziente.

**Dim. del Teorema 5.1.1** Siano $c(h)$ e $b(h)$ due polinomi esponenziali a coefficienti in $K$, con $b(h) \neq 0$ per ogni $h$, e poniamo

$$a_h = \frac{c(h)}{b(h)}.$$

Come nelle sezioni precedenti indichiamo con $B$ e $C$ i sottogruppi di $K^*$ generati dalle radici di $b(h)$ e $c(h)$, e indichiamo con $F$ e $G$ l'ordine dei due polinomi esponenziali. Osserviamo innanzitutto che un'applicazione del teorema di Lech-Mahler-Skolem ci permette di ricondurci al caso in cui $c(h)$ non si annulli identicamente su alcuna progressione aritmetica.

Quello che vorremmo fare è trovare un polinomio esponenziale $p(h)$ per cui si abbia $p(h) = a_h$ per ogni $h$. Il Lemma 5.4.1 ci dice che un tale polinomio, se esiste, deve avere le sue radici in $W = \langle B, C \rangle$, e la Proposizione 5.4.2 ci permette di stimare il suo ordine con una costante $E$. Indichiamo infine con $d$ l'ordine della parte di torsione di $W$.

A questo punto costruiamo la specializzazione, usando il Teorema 5.3.2. Prendiamo come $R$ un anello finitamente generato contenente i quozienti $a_h$ e i termini $b(h)$, $c(h)$ e come $S$ il sottogruppo $W$ (eventualmente ingrandendo $A$ in modo che $W < A^*$). Infine l'insieme finito $T$ dovrà contenere:

i) i determinanti $K_h(a)$ non nulli per $0 \leq h \leq 2(EF + G)$;

ii) i termini $b(h)$ per $0 \leq h \leq 2(EF + G)$;

iii) per ogni progressione aritmetica $h = r + nd$ un termine $c(h) = c(r + nd) \neq 0$.

Il teorema ci garantisce l'esistenza di una specializzazione $\phi$ definita almeno su $R$, che preservi l'indipendenza in $S = W$ e non annulli gli elementi di $T$. In particolare siamo nelle ipotesi della seconda parte della Proposizione 5.4.2. Il teorema del quoziente nel caso algebrico ci permette di trovare un polinomio esponenziale $q(h)$ tale che

$$q(h) = \frac{\phi(c(h))}{\phi(b(h))} = \phi(a_h)$$

per tutti gli $h$ per cui $\phi(b(h)) \neq 0$, in particolare per $0 \leq h \leq 2(EF + G)$. D'altra parte l'ordine di $q(h)$ è al massimo $E$, per cui otteniamo l'annullamento di $K_h(q)$ per $h \geq E$. Quindi abbiamo

$$\phi(K_h(a)) = K_h(\phi(a)) = K_h(q) = 0$$

per $E \leq h \leq 2(EF + G)$.

Per la costruzione di $T$ questo significa che $K_h(a) = 0$ nello stesso intervallo. Dunque troviamo un polinomio esponenziale $p(h)$ di ordine al più $E$ con $p(h) = a_h$ per $h \leq 2(EF + G)$ (per la Proposizione 2.1.4). Riscriviamo questo come

$$p(h)b(h) - c(h) = 0$$

per $h$ nello stesso intervallo. Tuttavia il termine sulla sinistra è un polinomio esponenziale di ordine al più $EF + G$, e poiché si annulla per $0 \leq h \leq 2(EF + G)$ deve essere identicamente nullo, cioè $p(h) = a_h$ per ogni $h$.

□

## 5.6 Il caso della radice

La dimostrazione appena vista del teorema del quoziente si trasporta quasi uguale al caso della radice. Supponiamo quindi dato un polinomio esponenziale

$$c(h) = \sum_{i=1}^{m} C_i(h)\gamma_i^h$$

di cui stiamo cercando la radice $r$-esima. Il primo passo è ottenere una stima a priori sull'ordine della radice, e per questo abbiamo bisogno dell'analogo del Lemma 5.4.1. In [RvdP87b] Rumely e Van der Poorten usano le tecniche di fattorizzazione di Ritt ([Rit27]) per ottenere:

**Lemma 5.6.1** *Supponiamo che $a(h)^r = c(h)$ e indichiamo $C = \langle \gamma_i \rangle$. Indichiamo inoltre con $L$ il campo ottenuto aggiungendo a $K$ le radici $r$-esime dei coefficienti dei polinomi $C_i$ e dei $\gamma_i$. Allora esiste un polinomio esponenziale $\widetilde{a}(h) \in L[h]_{C^{1/r}}$ tale che $\widetilde{a}(h)^r = c(h)$ (con $C^{1/r}$ si intende il gruppo generato dalle radici $r$-esime degli elementi di $C$).*

Non riportiamo la dimostrazione, che richiede un'analisi assai più dettagliata del suo analogo per il teorema del quoziente. In quello che segue non è restrittivo supporre che $L = K$, a meno di aggiungere in partenza le radici $r$-esime dei coefficienti e delle radici di $c(h)$. Adesso che abbiamo a disposizione l'analogo di 5.4.1 per il caso della radice possiamo dimostrare il Teorema della radice di Hadamard nel caso generale.

**Dim. del Teorema 5.1.2** Non sorprendentemente la dimostrazione ricalca le linee del teorema del quoziente. Usiamo innanzitutto il teorema di Lech-Mahler-Skolem per ricondurci al caso in cui $c(h)$ non si annulla su alcuna progressione aritmetica. Sappiamo che se $a(h)$ è un polinomio esponenziale che soddisfa $a(h)^r = c(h)$, possiamo trovarne un altro che inoltre abbia le sue radici in un sottogruppo finitamente generato $W = C^{1/r}$; di conseguenza abbiamo una stima dall'alto $E$ per il suo ordine. Sia $d$ l'ordine della parte di torsione di $W$ e $F$ l'ordine di $c(h)$ .

Per ciascun termine $c(h)$ abbiamo a disposizione al più $r$ scelte per la radice $r$-esima. Questo dà luogo ad un numero finito di sequenze

$$(a_{h,\lambda}) \quad h = 0, \ldots, rE + F + 1$$

che verificano $a^r_{h,\lambda} = c(h)$.

Usiamo nuovamente il Teorema 5.3.2 per costruire una specializzazione $\phi$ definita sui termini $c(h)$ e $a_{h,\lambda}$, che mantenga l'indipendenza moltiplicativa in $W$. Richiediamo inoltre che $\phi$ non annulli i seguenti elementi:

i) per ciascun $\lambda$ i determinanti $K_h(a_\lambda)$ non nulli per $0 \le h \le rE + F + 1$;

ii) per ciascuna progressione $h = s + nd$ un termine $c(h) = c(s + nd) \neq 0$.

Per il teorema sulla radice su campi di numeri troviamo un polinomio esponenziale $q(h)$ tale che $q(h)^r = c(h)$ per tutti gli $h$, e possiamo stimare con $E$ l'ordine di $q$. Scegliamo $\lambda$ in modo che $a_{h,\lambda} = q(h)$ per $0 \le h \le rE + F + 1$. Questo ci dice che i determinanti di Kronecker-Hankel

$$\phi(K_h(a_\lambda)) = (K_h(\phi(a_\lambda)) = K_h(q)$$

si annullano per $E \le h \le rE + F + 1$. Per come è stata costruita $\phi$ questo ci dice che $K_h(a_\lambda) = 0$ nel'intervallo $E \le h \le rE + F + 1$.

Pertanto troviamo un polinomio esponenziale $p(h)$ di ordine al più $E$ che coincide con $a_{h,\lambda}$ per $h \le rE + F + 1$. In particolare

$$p(h)^r - c(h) = 0$$

per $h \le rE + F + 1$. D'altra parte $p(h)^r - c(h)$ è un polinomio esponenziale di ordine al più $rE + F$, perciò $p(h)^r - c(h) = 0$ identicamente.

□

# Bibliografia


[Can69] D. Cantor, *On arithemtic properties of the Taylor series of rational functions*, Canadian Journal of Mathematics **21** (1969), 378–382.

[CF67] A cura di John W. S. Cassels e Albrecht Fröhlich, *Algebraic number theory*, London New York, London Mathematical Society con il supporto della International Mathematical Union, Academic Press, 1967.

[Fol95] Gerald B. Folland, *A course in abstract harmonic analysis*, Studies in Advanced Mathematics, **18**, CRC Press, Boca Raton Ann Arbor London Tokio, 1995.

[Kob84] Neil Koblitz, *p-adic numbers, p-adic analysis and Zeta functions (second edition)*, Graduate Texts in Mathematics, **58**, Springer-Verlag, New York Berlin Heidelberg, 1984.

[Lan02] Serge Lang, *Algebra (third edition)*, Graduate Texts in Mathematics, **211**, Springer, New York Berlin Heidelberg, 2002.

[LW54] Serge Lang e André Weil, *Number of points on varieties in finite fields*, American Journal of Mathematics **76** (1954), 819–827.

[Mar77] Daniel A. Marcus, *Number fields*, Universitext, Springer-Verlag, New York Berlin Heidelberg, 1977.

[Mil97] James S. Milne, *Class field theory*, `www.math.lsa.umich.edu/~jmilne/`, 1997.

[Mil98] James S. Milne, *Algebraic number theory*, `www.math.lsa.umich.edu/~jmilne/`, 1998.

[Nar90] Władysław Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer Monographs in Mathematics, Springer-Verlag, New York Berlin Heidelberg, 1990.

[Pou79] Yves Pourchet, *Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sc. Paris **288** (1979), 1055–1057.

[Rit27] Joseph F. Ritt, *A factorisation theory for functions* $\sum_{i=1}^{n} a_i e^{\alpha_i z}$, Transactions of the American Mathematical Society **29** (1927), 584–596.

[Rum87] ROBERT RUMELY, *Notes on van der Poorten's proof of the Hadamard quotient theorem*, Séminaire de Théorie des Nombres (A cura di Catherine Goldstein), Progress in Mathematics, **75**, Birkhäuser, Boston Basel, 1986-87, pp. 349–409.

[RvdP87a] ROBERT RUMELY E ALFRED J. VAN DER POORTEN, *A note on the Hadamard $k^{th}$ root of a rational function*, Journal of the Australian Mathematical Society **43** (1987), 314–327.

[RvdP87b] ROBERT S. RUMELY E ALFRED J. VAN DER POORTEN, *Remarks on generalised powersums*, Bulletin of the Australian mathematical society **36** (1987), 311–329.

[Sch76] WOLFGANG M. SCHMIDT, *Equations over finite fields. an elementary approach*, Lecture Notes in Mathematics, **536**, Springer-Verlag, New York Berlin Heidelberg, 1976.

[Sch80] WOLFGANG M. SCHMIDT, *Diophantine approximation*, Lecture Notes in Mathematics, **785**, Springer-Verlag, New York Berlin Heidelberg, 1980.

[Ser89] JEAN-PIERRE SERRE, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, **E15**, Vieweg, Braunschweig, 1989.

[Sil86] JOSEPH H. SILVERMAN, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, **106**, Springer-Verlag, New York Berlin Heidelberg, 1986.

[Sko99] NILS-PETER SKORUPPA, *Heights*, `wotan.algebra.math.uni-siegen.de/~skoruppa/`, 1999.

[vdP88] ALFRED J. VAN DER POORTEN, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sc. Paris **306** (1988), 97–102.

[vdP89] ALFRED J. VAN DER POORTEN, *Some facts that should be better known, especially about rational functions*, Number Theory and Applications (A cura di Richard A. Mollin), Kluwer Academic Publishers, Dordrecht, 1989, pp. 497–528.

[vdP96] ALFRED J. VAN DER POORTEN, *A note on Hadamard roots of rational functions*, Rocky Mountain Journal of Mathematics **26** (1996), 1183–1197.

[Wei46] ANDRÉ WEIL, *Foundations of algebraic geometry*, Amer. Math. Soc. Colloquium Publications, **XXIX**, American Mathematical Society, 1946.

[Wei48a] ANDRÉ WEIL, *Sur les courbes algébriques et les variétés qui s'en deduisent*, Actualités scientifiques et industrielles, **1041**, Hermann & Cie., 1948.

[Wei48b] ANDRÉ WEIL, *Variétés abeliennes et courbes algébriques*, Actualités scientifiques et industrielles, **1064**, Hermann & Cie., 1948.

[Zan97] Umberto Zannier, *On the reduction modulo p of an absolutely irreducible polynomial* $f(x, y)$, Archiv der Mathematik **68** (1997), 129–138.

[Zan00] Umberto Zannier, *A proof of Pisot's* $d^{th}$ *root conjecture*, Annals of Mathematics **151** (2000), 375–383.