Università di Pisa

Facoltà di Matematica

Numeri p-adici e metodo di Skolem

Tesi di Laurea Triennale
in Matematica

Candidato
Riccardo Zanotto

Relatore
Davide Lombardo
Università di Pisa

Anno Accademico 2017 - 2018

Ai miei nonni

Indice

Introduzione

L'obiettivo di questa tesi è di introdurre i numeri p-adici e mostrarne alcune applicazioni aritmetiche, in particolare il cosiddetto "metodo di Skolem".
L'idea fondamentale dell'analisi p-adica è quella di completare $\mathbb{Q}$ con una distanza diversa dalla solita distanza euclidea: se $v_p(x)$ è il numero di fattori p contenuti in x, definiamo la distanza p-adica tramite $d_p(x,y) = p^{-v_p(x-y)}$.
Con questa norma due numeri sono "vicini" se la loro differenza è multipla di una grande potenza p, e quindi ad esempio la sequenza $1, p, p^2, \ldots, p^n, \ldots$ tende a 0.
Dato che $\mathbb{Q}$ con questa distanza non è completo, si considera il completamento metrico $\mathbb{Q}_p$ detto *campo dei numeri p-adici*.
Il metodo di Skolem si concentra sullo studio delle serie di potenze in $\mathbb{Q}_p$ e sue estensioni, arrivando a dimostrare un risultato di finitezza che fornisce anche un bound esplicito sul numero di zeri interi di una serie analitica.

Una volta introdotta tutta la strumentazione necessaria, la nostra tesi si occuperà principalmente di due problemi, entrambi risolti con un'applicazione del metodo di Skolem:

- Il teorema di Skolem-Mahler-Lech, che fornisce informazioni molto precise sugli zeri delle successioni per ricorrenza: l'insieme degli indici per cui la successione si annulla è l'unione di un insieme finito e di un numero finito di progressioni aritmetiche.
- La risoluzione della diofantea $x^3 + dy^3 = 1$, detta equazione di Skolem: dimostreremo che ci sono al più due soluzioni, di cui una è quella banale $(1, 0)$.

Il capitolo finale è dedicato alla caratterizzazione della soluzione non banale dell'equazione di Skolem, ridimostrando che è unica ed è l'unità fondamentale dell'anello $\mathbb{Z}[\sqrt[3]{d}]$, se il coefficiente di $\sqrt[3]{d^2}$ è 0.

1

Prerequisiti

1.1 Definizioni

Cominciamo ad introdurre gli oggetti standard della teoria algebrica dei numeri.

Definizione 1.1.1. Un *campo di numeri* K è un'estensione finita $K/\mathbb{Q}$.

Ricordiamo ora il seguente:

Teorema 1.1.2 (elemento primitivo)**.** *Data un'estensione di campi E/F finita e separabile, esiste un elemento $\alpha \in E$ tale che $E = F(\alpha)$*

Dunque ogni campo di numeri K è della forma $\mathbb{Q}(\alpha)$ con $\alpha \in K$ che soddisfa un polinomio f irriducibile a coefficienti in $\mathbb{Q}$.
Ma allora osserviamo che $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$, e quindi $K \cong \mathbb{Q}[x]/(f)$ con $\deg f = [K : \mathbb{Q}]$.
Ricordiamo poi che ogni polinomio di grado n irriducibile a coefficienti razionali ha esattamente n radici distinte in $\mathbb{C}$, poiché $\operatorname{char} \mathbb{Q} = 0$. Possiamo dunque arrivare alla seguente

Proposizione 1.1.3. *Dato un campo di numeri $K = \mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/(f)$ di grado n, esistono esattamente n embedding $\sigma_i : K \to \mathbb{C}$ tali che $\sigma_i(\alpha) = \alpha_i$ dove $\alpha_1, \ldots, \alpha_n$ sono le radici di f.*

Siamo pronti ora per definire due funzioni importanti, ovvero la traccia e la norma.

Definizione 1.1.4. Sia K un campo di numeri di grado n e siano $\sigma_1, \ldots, \sigma_n$ i corrispondenti embedding.
La *traccia* è la funzione $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ tale che $\mathrm{Tr}(x) = \sum_{i=1}^{n} \sigma_i(x)$.
La *norma* è la funzione $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ tale che $\mathrm{N}(x) = \prod_{i=1}^{n} \sigma_i(x)$.

Osservazione. A priori non è detto che traccia e norma abbiano immagine contenuta in $\mathbb{Q}$, però è facile vedere che $\mathrm{Tr}(x)$ e $\mathrm{N}(x)$ sono coefficienti del polinomio $\prod_{i=1}^{n}(t-\sigma_i(x))$ che è a coefficienti razionali.

Ricordiamo che un campo di numeri K è un $\mathbb{Q}$-spazio vettoriale di dimensione $n=[K:\mathbb{Q}]$, e osserviamo che $\mathrm{Tr}_{K/\mathbb{Q}}$ è un'applicazione lineare $K\to\mathbb{Q}$. Vale allora la seguente

Proposizione 1.1.5. *L'applicazione* $\mathrm{Tr}: K\to\mathbb{Q}$ *è non nulla, quindi è surgettiva. Inoltre, data una* $\mathbb{Q}$*-base* $\{\alpha_1,\dots,\alpha_n\}$ *di* K*, esiste un'altra base* $\{\beta_1,\dots,\beta_n\}$*, detta* base duale*, tale che* $\mathrm{Tr}(\alpha_i\beta_j)=\delta_{ij}$*.*

Anelli di interi

Passiamo ora allo studio della parte fondamentale della teoria algebrica dei numeri, ovvero gli anelli di interi dei campi di numeri.
Ricordiamo la ben nota

Definizione 1.1.6. Un numero $\alpha\in\mathbb{C}$ si dice *algebrico* se è radice di un polinomio $f\in\mathbb{Z}[x]$.
Un numero $\beta\in\mathbb{C}$ si dice *intero algebrico* se è radice di un polinomio monico $f\in\mathbb{Z}[x]$. Indichiamo con $\mathbb{A}$ l'insieme degli interi algebrici.

Abbiamo ora un'importantissima proprietà dell'insieme $\mathbb{A}$:

Proposizione 1.1.7. *Siano* $\alpha,\beta\in\mathbb{A}$*. Allora* $\alpha+\beta\in\mathbb{A}$ *e* $\alpha\beta\in\mathbb{A}$*.*
Ovvero, $\mathbb{A}$ *è un anello.*

Questa proprietà ci porta allora ad introdurre il concetto di anello degli interi.

Definizione 1.1.8. Sia K un campo di numeri. Il sotto-anello di K formato dagli interi algebrici, indicato con $\mathcal{O}_K=K\cap\mathbb{A}$, è detto *anello degli interi di* K*.*

L'esempio più banale è $K=\mathbb{Q}$, per cui vale $\mathcal{O}_{\mathbb{Q}}=\mathbb{Z}$: infatti ogni numero razionale α soddisfa un polinomio a coefficienti interi $px+q=0$, che può essere scelto monico se e solo se $\alpha\in\mathbb{Z}$.
Ricordiamo inoltre il

Lemma 1.1.9 (Gauss)**.** *Sia* $\alpha\in\mathbb{A}$ *e* $f_\alpha(x)$ *il suo polinomio minimo a coefficienti interi. Allora* f_α *è irriducibile in* $\mathbb{Q}[x]$*.*

che permette facilmente di arrivare alla seguente caratterizzazione:

Proposizione 1.1.10. *Sia* K *un campo di numeri con anello degli interi* $\mathcal{O}_K$*. Se* $\alpha\in\mathcal{O}_K$ *allora* $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)\in\mathbb{Z}$ *e* $\mathrm{N}_{K/\mathbb{Q}}(\alpha)\in\mathbb{Z}$*.*

Mostriamo ora un importante risultato sulla struttura additiva di $\mathcal{O}_K$.

Teorema 1.1.11. *Sia K un campo di numeri con $[K:\mathbb{Q}] = n$ e $\mathcal{O}_K$ il suo anello di interi.*
Allora $\mathcal{O}_K$ è uno $\mathbb{Z}$-modulo libero di rango n, o equivalentemente esiste una base $\{\alpha_1, \dots, \alpha_n\} \subset \mathcal{O}_K$ (detta base intera *di $\mathcal{O}_K$) tale che l'applicazione $\varphi : \mathbb{Z}^n \to \mathcal{O}_K$ data da $\varphi(m_1, \dots, m_n) = \sum_{i=1}^n m_i\alpha_i$ sia un isomorfismo.*

Dimostrazione. Vogliamo trovare due $\mathbb{Z}$-moduli liberi A, B di rango n tali che $A \subset \mathcal{O}_K \subset B$: in questo modo $\mathcal{O}_K$ è forzato ad essere uno $\mathbb{Z}$-modulo libero (perché contenuto in B) di rango massimo (poiché contiene A).
Per A la scelta è semplice: se $K = \mathbb{Q}(\alpha)$ con $\alpha \in \mathcal{O}_K$, basta scegliere $A = \mathbb{Z}[\alpha] = \langle 1, \alpha, \dots, \alpha^{n-1}\rangle_{\mathbb{Z}}$.
Per trovare B consideriamo invece una $\mathbb{Q}$-base di K $\{\alpha_1, \dots, \alpha_n\}$ con $\alpha_i \in \mathcal{O}_K$; consideriamo allora $\{\beta_1, \dots, \beta_n\}$ la base duale data dalla proposizione 1.1.5. Se $x \in \mathcal{O}_K$, possiamo scrivere $x = \sum_{i=1}^n \beta_i x_i$ con $x_i \in \mathbb{Q}$; moltiplicando entrambi i membri per α_j e prendendo la traccia otteniamo $\mathrm{Tr}(x\alpha_j) = \sum_{i=1}^n \mathrm{Tr}(\alpha_j\beta_i)x_i$. Osserviamo ora che $x\alpha_j \in \mathcal{O}_K$, quindi $\mathrm{Tr}(x\alpha_j) \in \mathbb{Z}$, e d'altra parte per definizione $\mathrm{Tr}(\alpha_j\beta_i) = \delta_{ij}$; perciò otteniamo $x_i \in \mathbb{Z}$, ovvero possiamo prendere $B = \langle \beta_1, \dots, \beta_n\rangle_{\mathbb{Z}} \supset \mathcal{O}_K$ □

Concludiamo questa parte sugli anelli di interi mostrando una fondamentale proprietà dei suoi ideali.

Lemma 1.1.12. *Sia $\mathcal{O}_K$ l'anello degli interi di un campo di numeri K. Sia I un ideale non nullo di $\mathcal{O}_K$. Allora $\mathcal{O}_K/I$ è finito.*

Dimostrazione. Sia $\alpha \in I$ non nullo. Consideriamo $\mathrm{N}(\alpha) = m \in \mathbb{Z}$, e scriviamo $m = \alpha\beta$ dove β è il prodotto dei coniugati di α con molteplicità. Osserviamo che $\beta = \frac{m}{\alpha}$, quindi $\beta \in K$.
Sia ora $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 = \prod_{i=1}^n (x - \sigma_i(\alpha)) \in \mathbb{Z}[x]$ il polinomio caratteristico di α; vale allora $f(\alpha) = 0$ e $m = c_0$. Dividendo ora la relazione $f(\alpha) = 0$ per α^n e moltiplicando per m^{n-1} otteniamo che

$$\frac{m^n}{\alpha^n} + c_1\frac{m^{n-1}}{\alpha^{n-1}} + \cdots + c_{n-1}m^{n-2}\frac{m}{\alpha} + m^{n-1} = 0$$

ovvero β è radice di un polinomio monico a coefficienti interi, e quindi anche $\beta \in \mathcal{O}_K$. Questo implica che $m \in I$.
Inoltre ricordiamo che $\mathcal{O}_K \cong \mathbb{Z}^n$ perciò $\mathcal{O}_K/m\mathcal{O}_K \cong \left(\mathbb{Z}/m\mathbb{Z}\right)^n$ che è finito.
Ma allora dato che $m\mathcal{O}_K \subset I$, otteniamo che anche $\mathcal{O}_K/I$ è finito. □

Discriminante

Un importante invariante di un campo di numeri è il cosiddetto *discriminante*, che definiremo in questo paragrafo.

Consideriamo un campo di numeri K di grado n, e siano $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$ i relativi embedding.

Definizione 1.1.13. Data una n-upla $(\alpha_1, \dots, \alpha_n) \in K^n$ si definisce il discriminante come

$$\mathrm{disc}_K(\alpha_1, \dots, \alpha_n) = \det([\sigma_i(\alpha_j)]_{ij})^2$$

Un modo alternativo per calcolare il discriminante di una n-upla è dato dal seguente:

Lemma 1.1.14. *Sia $(\alpha_1, \dots, \alpha_n) \in K^n$. Allora vale*

$$\mathrm{disc}_K(\alpha_1, \dots, \alpha_n) = \det[\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)]_{ij}$$

Spostiamo ora il nostro interesse sulle n-uple che sono basi intere di $\mathcal{O}_K$: siano $\alpha_1, \dots, \alpha_n$ e $\beta_1, \dots, \beta_n$ due basi intere. Esiste allora una matrice di cambio base $M \in \mathrm{GL}_n(\mathbb{Z})$ tale che $\beta_i = \sum m_{ij}\alpha_j$.
Sia ora $\Sigma(\alpha)$ la matrice $[\sigma_i(\alpha_j)]_{ij}$ e similmente $\Sigma(\beta)$; dato che i σ_i sono $\mathbb{Q}$-lineari, vale la relazione $\Sigma(\beta) = M\Sigma(\alpha)$.
Prendendo ora il determinante di entrambi i membri otteniamo che

$$\mathrm{disc}_K(\beta) = \det(M)^2 \,\mathrm{disc}_K(\alpha)$$

Ma $\det(M) = \pm 1$ perché M è una matrice invertibile a coefficienti interi, quindi abbiamo mostrato il

Teorema 1.1.15. *Siano $\mathcal{B}, \mathcal{B}'$ due basi intere di $\mathcal{O}_K$. Allora*

$$\mathrm{disc}_K \mathcal{B} = \mathrm{disc}_K \mathcal{B}'$$

Definiamo quindi il discriminante *di K come* $\mathrm{disc}(K) = \mathrm{disc}_K \mathcal{B}$*, dove $\mathcal{B}$ è una qualunque base intera di $\mathcal{O}_K$.*

Vediamo ora un'ultima proprietà del discriminante:

Proposizione 1.1.16. *Sia $\alpha \in \mathcal{O}_K$ e $\mu \in \mathbb{Z}[x]$ il suo polinomio caratteristico. Vale allora*

$$\mathrm{disc}_K(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = \mathrm{N}(\mu'(\alpha))$$

e si definisce $\mathrm{disc}_K(\alpha) = \mathrm{disc}_K(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$.

1.2 Basi intere di estensioni cubiche pure

Trovare una base intera è una parte importante dello studio di un campo di numeri, ed è un'operazione non completamente banale.
In generale, se $K = \mathbb{Q}(\alpha)$ con $\alpha \in \mathbb{A}$, non è vero che $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Ci sono però alcuni teoremi che ci permettono di trovare basi intere in estensioni di grado basso; a noi interesserà particolarmente il caso cubico.

Fissiamo K campo di numeri di grado n. Valgono i seguenti

Teorema 1.2.1. *Sia $\{\alpha_1, \dots, \alpha_n\}$ una $\mathbb{Q}$-base di K tale che $\alpha_i \in \mathcal{O}_K$ e sia $d = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$.*
Allora ogni $\alpha \in \mathcal{O}_K$ si può scrivere nella forma

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$$

dove $m_i \in \mathbb{Z}$ e $d \mid m_i^2$.

Teorema 1.2.2. *Sia $\alpha \in \mathcal{O}_K$ con polinomio minimo di grado n. Allora esiste una base intera di $\mathcal{O}_K$ della forma*

$$1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}}$$

dove $f_j \in \mathbb{Z}[x]$ sono polinomi monici con $\deg f_j = j$, i d_j sono interi univocamente determinati e vale $d_1 \mid d_2 \mid \dots \mid d_{n-1}$.
Infine se $i + j < n$ allora $d_i d_j \mid d_{i+j}$.

Possiamo ora usare questi teoremi per caratterizzare le basi intere di estensioni cubiche pure.

Sia $m \in \mathbb{Z}$ un intero libero da cubi, scritto nella forma $m = hk^2$ con $h, k \in \mathbb{Z}$ squarefree e coprimi.
Consideriamo $\alpha = \sqrt[3]{m}$ e sia $K = \mathbb{Q}(\alpha)$.

Proposizione 1.2.3. *Una base intera di $\mathcal{O}_K$ è formata da*

$$\begin{array}{llll} 1, & \alpha, & \alpha^2/k & \text{se } m \not\equiv \pm 1 \pmod 9 \\ 1, & \alpha, & \dfrac{\alpha^2 \pm k^2\alpha + k^2}{3k} & \text{se } m \equiv \pm 1 \pmod 9 \end{array}$$

Dimostrazione. Consideriamo una base intera fornita dal teorema precedente, ovvero con elementi della forma $1, \dfrac{f_1(\alpha)}{d_1}, \dfrac{f_2(\alpha)}{d_2}$. Dato che i polinomi f_i sono monici, vale un'uguaglianza

$$\begin{pmatrix} 1 \\ f_1(\alpha) \\ f_2(\alpha) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ * & * & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix}$$

da cui si ricava facilmente che $\operatorname{disc}_K(1,\alpha,\alpha^2) = \operatorname{disc}_K(1, f_1(\alpha), f_2(\alpha))$ e di conseguenza

$$\operatorname{disc}_K(\alpha) = (d_1 d_2)^2 \operatorname{disc} K \tag{1.1}$$

Nei seguenti step andremo allora a determinare d_1, d_2 e f_1, f_2.

1. Dimostriamo che $d_1 = 1$.
   Ricordiamo che, detto $\mu(x) = x^3 - m$ il polinomio minimo di α, vale $\operatorname{disc}_K(\alpha) = -\operatorname{N}(\mu'(\alpha))$. Dato che $\operatorname{N}(\alpha) = m$ si ottiene $\operatorname{disc}(\alpha) = -27m^2$.
   Dal teorema 1.2.2 ricaviamo $d_1^2 \mid d_2$, e quindi dalla (1.1) si ottiene $d_1^6 \mid \operatorname{disc}\alpha = -27m^2$. Essendo m libero da cubi, otteniamo $d_1 = 1$ a meno che $9 \mid m$.
   Supponiamo per assurdo $d_1 = 3$, che può accadere solo per $9 \mid m$, ovvero $3 \mid k$. Sia allora $\beta = \frac{f_1(\alpha)}{d_1} = \frac{\alpha + a}{3} \in \mathcal{O}_K$ con $a \in \mathbb{Z}$; consideriamo $\beta^3 = \dfrac{m + 3\alpha^2 a + 3\alpha a^2 + a^3}{3^3}$, che è intero è quindi avrà traccia $\in \mathbb{Z}$.
   Tuttavia $\operatorname{Tr}(\alpha) = \operatorname{Tr}(\alpha^2) = 0$, perciò $\operatorname{Tr}(\beta^3) = \frac{m + a^3}{3^2}$ e dato che $9 \mid m$ si ha $3 \mid a$.
   Avremmo perciò $\frac{\alpha}{3} \in \mathcal{O}_K$, che è assurdo considerando la norma: $\operatorname{N}\left(\frac{\alpha}{3}\right) = \frac{m}{3^3} \notin \mathbb{Z}$ perché m è libero da cubi.
   Avendo allora $d_1 = 1$, possiamo prendere $f_1(\alpha) = \alpha$.

2. Dimostriamo che $\frac{\alpha^2}{k} \in \mathcal{O}_K$ e se $m \equiv \pm 1 \pmod 9$, allora $\beta = \frac{(\alpha \mp 1)^2}{3} \in \mathcal{O}_K$.
   Osserviamo che $\left(\frac{\alpha^2}{k}\right)^3 = \frac{m^2}{k^3} = \frac{h^2 k^4}{k^3} = h^2 k$, quindi $\frac{\alpha^2}{k}$ è radice del polinomio monico a coefficienti interi $x^3 - h^2 k$ e pertanto sta in $\mathcal{O}_K$.
   Calcoliamo ora $\left(\beta - \frac{1}{3}\right)^3 = \beta^3 - \beta^2 + \frac{\beta}{3} - \frac{1}{27}$.
   D'altra parte $\left(\beta - \frac{1}{3}\right)^3 = \left(\frac{\alpha^2 \mp 2\alpha}{3}\right)^3 = \frac{m}{27}\left(\alpha^3 \mp 6\alpha^2 + 12\alpha \mp 8\right) = \frac{m}{27}(m \mp 2) \mp \frac{2m}{3}\beta$ e quindi otteniamo

   $$\beta^3 - \beta^2 + \frac{1 \pm 2m}{3}\beta - \frac{(m \mp 1)^2}{27} = 0$$

   dove i coefficienti sono interi dato che $m \equiv \pm 1 \pmod 9$.

3. Abbiamo appena ottenuto che $k \mid d_2$, e che se $m \equiv \pm 1 \pmod 9$ vale anche $3 \mid d_2$ e quindi $3k \mid d_2$.
   Inoltre usando la (1.1) si ha $d_2^2 \mid 27m^2$, da cui $d_2 \mid 3m$.

4. Poniamo ora $f_2(\alpha) = \alpha^2 + a\alpha + b$ con $a, b \in \mathbb{Z}$.

5. Sia $p \neq 3$ tale che $p \mid h$. Allora $p \nmid d_2$.
   Se per assurdo valesse $d_2 = cp$, allora avremmo $c \cdot \frac{f_2(\alpha)}{d_2} = \frac{\alpha^2 + a\alpha + b}{p} \in \mathcal{O}_K$; ma considerando la traccia varrebbe $\frac{3b}{p} \in \mathbb{Z}$, ovvero $p \mid b$ e quindi

anche $\frac{\alpha^2+a\alpha}{p} \in \mathcal{O}_K$.
Dovrebbe allora valere $\mathrm{Tr}\left(\left(\frac{\alpha^2+a\alpha}{p}\right)^3\right) = \frac{3m(m+a^3)}{p^3} \in \mathbb{Z}$. Dato che $\upsilon_p(m) = 1$, questo è però impossibile. Perciò $p \nmid d_2$.

6. Sia $p \neq 3$ tale che $p^2 \mid m$, ovvero $p \mid k$. Mostriamo che $p^2 \nmid d_2$.
Dal punto 2 sappiamo che $p \mid d_2$. Supponiamo per assurdo che $p^2 \mid d_2$. Allora come sopra $\frac{\alpha^2+a\alpha+b}{p^2} \in \mathcal{O}_K$ e considerando la traccia otteniamo $\frac{\alpha^2+a\alpha}{p^2} \in \mathcal{O}_K$. Elevando al cubo e prendendo la traccia abbiamo $\frac{3m(m+a^3)}{p^6} \in \mathbb{Z}$ che è impossibile in quanto $\upsilon_p(m) = 2$.

7. $a^2 + 2b, m + 2ab, b^2 + 2am$ sono tutti multipli di d_2.
Consideriamo $\beta = \left(\frac{\alpha^2+a\alpha+b}{d_2}\right)^2 = \frac{\alpha^2(a^2+2b)+\alpha(m+2ab)+(b^2+2ma)}{d_2^2}$. Dato che $\beta \in \mathcal{O}_K$, esistono interi r, s, t per cui $\beta = r + s\alpha + t\frac{\alpha^2+a\alpha+b}{d_2}$; moltiplicando per d_2^2 e raccogliendo le potenze di α, a destra abbiamo tutti coefficienti multipli di d_2, quindi devono esserlo anche a sinistra.

8. Se $3 \nmid m$, vale $d_2 = 3k$ per $m \equiv \pm 1 \pmod 9$ e $d_2 = k$ altrimenti.
Nel caso $m \equiv \pm 1 \pmod 9$ sappiamo per il punto 3 che $3k \mid d_2 \mid 3m$; ma m non è multiplo di 3 quindi $\upsilon_3(d_2) = 1$. Grazie ai punti $5, 6$ concludiamo che $d_2 = 3k$.
Se $m \equiv 2, 4, 5, 7 \pmod 9$, supponiamo per assurdo che $3 \mid d_2$. Allora per il punto 7 ricaviamo $b \equiv 1 \pmod 3$ e $a \equiv m \pmod 3$; perciò si ha $\frac{\alpha^2+m\alpha+1}{3} \in \mathcal{O}_K$.
Se $m \equiv 1 \pmod 3$ possiamo dire che anche $\frac{(\alpha-1)^2}{3} \in \mathcal{O}_K$. Considerandone la norma, otteniamo $\frac{(m-1)^2}{3^3} \in \mathbb{Z}$, che implica $m \equiv 1 \pmod 9$, assurdo.
Se invece $m \equiv 2 \pmod 3$ abbiamo $\frac{(\alpha+1)^2}{3} \in \mathcal{O}_K$. Di nuovo prendendone la norma si ottiene $\frac{(m+1)^2}{3^3} \in \mathbb{Z}$, da cui $m \equiv -1 \pmod 9$, assurdo.

9. Se $\upsilon_3(m) = 1$, allora $3 \nmid d_2$, ovvero $d_2 = k$.
Se per assurdo $3 \mid d_2$, dal punto 7 avremmo $a \equiv b \equiv 0 \pmod 3$. Ma allora possiamo dire che $\frac{\alpha^2}{3} \in \mathcal{O}_K$, e prendendo la norma avremmo $\frac{m^2}{3^3} \in \mathbb{Z}$, che è impossibile.

10. Se $\upsilon_3(m) = 2$, allora $\upsilon_3(d_2) = 1$, ovvero $d_2 = k$.
Se per assurdo $9 \mid d_2$, da 7 otterremmo che $9 \mid b$ e quindi $\frac{\alpha^2+a\alpha}{9} \in \mathcal{O}_K$. Elevando al cubo e considerando la traccia avremmo $3^6 \mid m(m + a^3)$ che è impossibile.

11. Osserviamo infine che dal punto 7 si ottiene $a \equiv b \equiv 0 \pmod k$, quindi nel caso $m \not\equiv \pm 1 \pmod 9$ una base intera è effettivamente

$1, \alpha, \frac{\alpha^2}{k}$.
Invece nel caso $m \equiv \pm 1 \pmod 9$ si vede che $\dfrac{\alpha^2 \pm k^2\alpha + k^2}{3k} \in \mathcal{O}_K$ quindi può essere usato come ultimo elemento di base.

□

1.3 Fattorizzazione di ideali

In questa sezione mostreremo che in ogni $\mathcal{O}_K$ c'è fattorizzazione unica degli ideali in ideali primi.
Cominciamo introducendo una nuova classe di anelli.

Definizione 1.3.1. Un dominio d'integrità R è detto *dominio di Dedekind* se valgono le tre seguenti proprietà:

1. R è Noetheriano, ovvero ogni ideale è finitamente generato.
2. Ogni ideale primo non nullo è massimale.
3. R è integralmente chiuso nel suo campo delle frazioni F (ovvero se $x \in F$ è radice di un polinomio monico a coefficienti in R, allora $x \in R$).

Per capire il motivo di questa definizione vediamo che vale

Teorema 1.3.2. *Sia K un campo di numeri con anello di interi $\mathcal{O}_K$. Allora $\mathcal{O}_K$ è un dominio di Dedekind.*

Studiamo ora la fattorizzazione degli ideali in domini di Dedekind, introducendo un nuovo concetto

Definizione 1.3.3. Dato un dominio A con campo delle frazioni K, diciamo che un A-modulo $I \subset K$ è un *ideale frazionario* se $\exists d \neq 0 \in A$ tale che $dI \subset A$.
Definiamo poi il prodotto di due ideali frazionari I, J come l'A-modulo generato dai prodotti xy con $x \in I, y \in J$.
Infine, dato un ideale frazionario I definiamo $I^{-1} = \{x \in K \mid xI \subset A\}$, che è ancora un ideale frazionario.
Se vale $II^{-1} = A$, diciamo che I è *invertibile*.

Vale allora l'importante

Proposizione 1.3.4. *Sia R un dominio di Dedekind. Allora ogni ideale massimale $\mathfrak{m} \subset R$ è invertibile.*

Da cui segue facilmente il risultato principale

Teorema 1.3.5. *Sia R un dominio di Dedekind e I un ideale frazionario non nullo. Allora esistono unici $\mathfrak{p}_i$ ideali primi di R e $e_i \in \mathbb{Z}$ tali che $I = \prod \mathfrak{p}_i^{e_i}$; inoltre $I \subset R$ se e solo se $e_i \geq 0$ $\forall i$.*

Grazie al teorema 1.3.2, possiamo riscrivere il risultato precedente specializzandoci ai campi di numeri, dove gli ideali frazionari sono $\mathcal{O}_K$-moduli finitamente generati da elementi di K.

Teorema 1.3.6. *Sia K un campo di numeri e I un ideale frazionario non nullo. Allora esistono unici $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideali primi di $\mathcal{O}_K$ e $v_1, \ldots, v_r \in \mathbb{Z}$ tali che*

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{v_i}$$

Diciamo allora che $v_i = v_{\mathfrak{p}_i}(I)$.

Ramificazione e inerzia

Ci occupiamo ora della fattorizzazione di ideali in estensioni di campi di numeri.
Fissiamo un'estensione di campi di numeri $L \supset K$, con rispettivi anelli di interi $\mathcal{O}_L, \mathcal{O}_K$.
Nelle proposizioni seguenti con "primo" intenderemo un ideale primo non nullo.

Teorema 1.3.7. *Siano $\mathfrak{p}$ un primo di $\mathcal{O}_K$ e $\mathfrak{q}$ un primo di $\mathcal{O}_L$. Allora le seguenti condizioni sono equivalenti*

1. $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$
2. $\mathfrak{q} \supset \mathfrak{p}\mathcal{O}_L$
3. $\mathfrak{q} \supset \mathfrak{p}$
4. $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$
5. $\mathfrak{q} \cap K = \mathfrak{p}$

e quando valgono si dice che $\mathfrak{q}$ sta sopra $\mathfrak{p}$ *e* $\mathfrak{p}$ sta sotto $\mathfrak{q}$.

Vale inoltre

Proposizione 1.3.8. *Ogni primo di $\mathcal{O}_L$ sta sopra un unico primo di $\mathcal{O}_K$; ogni primo di $\mathcal{O}_K$ sta sotto almeno un primo di $\mathcal{O}_L$.*

e quindi, dato $\mathfrak{p} \subset \mathcal{O}_K$ primo, possiamo scrivere in maniera unica

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$$

dove i $\mathfrak{q}_i$ sono tutti e soli i primi di $\mathcal{O}_L$ sopra $\mathfrak{p}$.

Definizione 1.3.9. Gli esponenti e_i si dicono *indici di ramificazione*, e si denotano come $e_i = e(\mathfrak{q}_i \mid \mathfrak{p})$.
Il primo $\mathfrak{p}$ si dice *ramificato* se $e_i > 1$ per almeno un indice.

Un'altra quantità importante è quella data dalla seguente

Proposizione 1.3.10. *Sia $\mathfrak{q}$ un primo di $\mathcal{O}_L$ sopra $\mathfrak{p}$ primo di $\mathcal{O}_K$. Allora $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{q}$ è un'estensione di campi finiti di grado $f = f(\mathfrak{q} \mid \mathfrak{p})$ detto* grado d'inerzia.

Inerzia e ramificazione sono legati dal fondamentale

Teorema 1.3.11. *Sia $L \supset K$ estensione di campi di numeri di grado n. Sia $\mathfrak{p} \subset \mathcal{O}_K$ un primo la cui fattorizzazione è*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$$

e siano $f_i = f(\mathfrak{q}_i \mid \mathfrak{p})$. Allora vale $\sum_{i=1}^{r} e_i f_i = n$.

Concludiamo la sezione con un risultato importante che ci sarà utile in seguito.

Teorema 1.3.12. *Sia $p \in \mathbb{Z}$ un numero primo e K un campo di numeri. Allora p ramifica in $\mathcal{O}_K$ se e solo se $p \mid \mathrm{disc}(K)$.*

1.4 Unità

Fissiamo un campo di numeri K con anello di interi $\mathcal{O}_K$; siamo interessati a studiare gli invertibili, o unità, di questo anello, indicati con $\mathcal{O}_K^\times$.

Osservazione. Le unità sono un gruppo abeliano moltiplicativo.

Abbiamo inoltre una caratterizzazione importante per le unità, ovvero

Proposizione 1.4.1. *Sia $\alpha \in \mathcal{O}_K$. Allora α è un'unità se e solo se* $\mathrm{N}(\alpha) = \pm 1$.

Abbiamo uno strumento potente per indagare la struttura delle unità. Ci serve intanto una notazione

Definizione 1.4.2. Siano $\sigma_1, \ldots, \sigma_n$ gli embedding di K in $\mathbb{C}$. Di questi ce ne saranno r la cui immagine è contenuta in $\mathbb{R}$ (gli embedding sono detti *reali*), e i rimanenti $2s$ sono coppie di mappe complesse coniugate; vale perciò $n = r + 2s$.
Si dice allora *segnatura* di K la coppia (r, s).

Possiamo allora enunciare il risultato di struttura del gruppo delle unità

Teorema 1.4.3 (Dirichlet)**.** *Sia K un campo di numeri con segnatura (r, s). Allora*

$$\mathcal{O}_K^\times \cong U \times \mathbb{Z}^{r+s-1}$$

dove U è un gruppo ciclico costituito dalle radici dell'unità in K.

Il teorema in realtà si può generalizzare anche ai cosiddetti ordini:

Definizione 1.4.4. Un sotto-anello $\mathcal{O}$ di $\mathcal{O}_K$ si dice un *ordine* se contiene una base intera. In particolare possiamo dire che $\mathcal{O} = \langle \alpha_1, \ldots, \alpha_n \rangle_\mathbb{Z}$ è un ordine se gli $\alpha_i \in \mathcal{O}_K$ sono una $\mathbb{Q}$-base di K.

Teorema 1.4.5. *Sia $\mathcal{O}$ un ordine di un campo di numeri K con segnatura (r, s). Allora il gruppo delle unità $\mathcal{O}^\times$ è finitamente generato di rango $r + s - 1$.*

Esempio 1.4.6.

- Se $K = \mathbb{Q}(\sqrt{m})$ con m positivo, allora $(r, s) = (2, 0)$, perciò il gruppo delle unità ha rango 1 (sono esattamente le soluzioni dell'equazione di Pell $x^2 - my^2 = 1$)
- Se $K = \mathbb{Q}(\sqrt{m})$ con m negativo, la segnatura è $(0, 1)$ quindi c'è un numero finito di unità.
- Se $K = \mathbb{Q}(\sqrt[3]{d})$ allora $(r, s) = (1, 1)$ e il gruppo delle unità ha rango 1; in virtù del teorema 1.4.5 anche $\mathbb{Z}[\sqrt[3]{d}]^\times$ ha rango 1, nonostante in generale non valga $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{d}]$ (si veda la proposizione 1.2.3). In entrambi i casi un generatore ε del gruppo delle unità si dice *unità fondamentale*; a seconda dei casi useremo una delle quattro normalizzazioni: $\pm\varepsilon, \pm 1/\varepsilon$.

Ci occupiamo infine di un caso specifico, nel quale sappiamo dare un bound sulle unità

Teorema 1.4.7 (Artin)**.** *Sia K un campo cubico reale e $u > 1$ un'unità. Allora*

$$|\mathrm{disc}(K)| \leq 4u^3 + 24$$

Dimostrazione. Sia $\mathcal{B} = \{b_1, b_2, b_3\}$ una base intera di K; sappiamo allora scrivere u come combinazione a coefficienti interi di elementi di $\mathcal{B}$; ovvero, esiste una matrice M a coefficienti interi tale che

$$\begin{pmatrix} 1 \\ u \\ u^2 \end{pmatrix} = M \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

Ma allora vale che $\mathrm{disc}_K(u) = \det M^2 \cdot \mathrm{disc}\, K$ e dato che $|\det M| \geq 1$, otteniamo $|\mathrm{disc}(K)| \leq |\mathrm{disc}_K(u)|$.
Ricordiamo che, detti σ_1 l'embedding reale di K e σ_2 uno dei due embedding complessi, vale $|\mathrm{disc}_K(u)| = |(\sigma_1(u)-\sigma_2(u))(\sigma_1(u)-\bar{\sigma}_2(u))(\sigma_2(u)-\bar{\sigma}_2(u))|^2$.
Detto $\sigma_2(u) = \rho e^{i\theta}$ con $\rho > 0$, poiché deve valere $\sigma_1(u)\sigma_2(u)\bar{\sigma}_2(u) = \pm 1$, otteniamo $\sigma_1(u) = \rho^{-2}$ e dunque $\rho < 1$.
Espandendo otteniamo

$$\begin{aligned} |\mathrm{disc}_K(u)| &= 4\rho^2 \sin^2\theta \left(\frac{1-\rho^3 e^{i\theta}}{\rho^2} \cdot \frac{1-\rho^3 e^{-i\theta}}{\rho^2} \right)^2 \\ &= 4\sin^2\theta \left(\rho^{-3} - 2\cos\theta + \rho^3\right)^2 \end{aligned}$$

Poniamo ora $t = \rho^{-3} + \rho^3$, $c = \cos\theta$ e otteniamo dunque una funzione $f(c,t) = 4(1-c^2)(t-2c)^2$. Fissato c, cerchiamo il massimo di $f(c,t) - 4t^2$, che è una parabola con coefficiente di testa negativo: il massimo perciò è nel vertice $t_0 = \frac{2(c^2-1)}{c}$ e $f(c,t_0) = 16(1-c^2) \leq 16$.
Identificando u e $\sigma_1(u)$ abbiamo allora $|\mathrm{disc}_K(u)| \leq 16 + 4(\rho^{-3}+\rho^3)^2 = 4(4 + u^3 + u^{-3} + 2)$ poiché $u = \rho^{-2}$.
Ricordando che $|\mathrm{disc}(K)| \leq |\mathrm{disc}_K(u)|$ e $u > 1$, otteniamo infine $|\mathrm{disc}(K)| < 4(u^3+7)$.
Per ottenere la disuguaglianza con il 6 invece del 7, vedere [FT93], proposizione $V.3.2$. □

Osservazione. La disuguaglianza di Artin vale in generale per ogni ordine di $\mathcal{O}_K$, sostituendo $\mathrm{disc}\, K$ con il discriminante di una base dell'ordine.
In particolare considerando $\mathcal{O} = \mathbb{Z}[\alpha]$, la disuguaglianza diventa $|\mathrm{disc}(\alpha)| \leq 4u^3 + 24$ con $u \in \mathcal{O}^\times$ e $u > 1$.

Esempio 1.4.8. Mostriamo ora con la disuguaglianza di Artin che $u = \sqrt[3]{9} - 2$ è un'unità fondamentale di $\mathbb{Z}[\sqrt[3]{9}]$. Osserviamo che $\sigma_1(u) < 1$, quindi $\sigma_1(1/u) > 1$.
Sia ε l'unità fondamentale tale che $\sigma_1(\varepsilon) > 1$; allora $1/u = \varepsilon^n$ con $n > 0$, ovvero $\varepsilon = (1/u)^{\frac{1}{n}}$.
Calcoliamo facilmente $|\mathrm{disc}(\sqrt[3]{9})| = \mathrm{N}(3\sqrt[3]{9^2}) = 3^7$.
Applicando la disuguaglianza di Artin su ε otteniamo $3^7 \leq 4(1/u)^{\frac{3}{n}} + 24$, da cui si ricava $\log(3^7 - 24) \leq \frac{3}{n}\log(4/u)$ ovvero $n \leq \dfrac{3\log(4/u)}{\log(3^7-24)} \approx 1.52$.
Essendo n intero, otteniamo che l'unico valore possibile è $n = 1$, ovvero u è un generatore del gruppo delle unità.

2

Numeri p-adici

Passiamo ora a studiare l'argomento principale della tesi, ovvero i campi p-adici e loro estensioni.

2.1 Campi p-adici

Dato un campo di numeri K e un ideale primo $\mathfrak{p} \subset \mathcal{O}_K$, ricordiamo che ad ogni ideale frazionario I possiamo associare $v_{\mathfrak{p}}(I) \in \mathbb{Z}$. Diamo allora la

Definizione 2.1.1. Sia $x \in K^{\times}$. Definiamo la mappa *valutazione* $\mathfrak{p}$*-adica* $v_{\mathfrak{p}} : K^{\times} \to \mathbb{Z}$ in modo che $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(x\mathcal{O}_K)$ dove la seconda è la valutazione di un ideale. Poniamo per convenzione $v_{\mathfrak{p}}(0) = +\infty$.
Possiamo anche definire la *norma* $\mathfrak{p}$*-adica* come $|x|_{\mathfrak{p}} = (\mathrm{N}(\mathfrak{p}))^{-v_{\mathfrak{p}}(x)}$ dove con $\mathrm{N}(\mathfrak{p})$ intendiamo la norma dell'ideale; poniamo inoltre $|0|_{\mathfrak{p}} = 0$.
Questa norma induce poi la *distanza* $\mathfrak{p}$*-adica* $d_{\mathfrak{p}}(x, y) = |x - y|_{\mathfrak{p}}$.

La norma appena definita soddisfa non solo la disuguaglianza triangolare, ma è addirittura *ultrametrica* nel senso della seguente:

Proposizione 2.1.2. *La norma* $|\ |_{\mathfrak{p}} : K \to \mathbb{R}$ *soddisfa la disuguaglianza*

$$|x + y|_{\mathfrak{p}} \leq \max(|x|_{\mathfrak{p}}, |y|_{\mathfrak{p}})$$

Possiamo ora introdurre il campo p-adico $K_{\mathfrak{p}}$ definito come il completamento di K rispetto alla distanza $d_{\mathfrak{p}}$.

Proposizione 2.1.3. *Il completamento metrico* $K_{\mathfrak{p}}$ *del campo* K *rispetto alla distanza* $d_{\mathfrak{p}}$ *è ancora un campo; esistono inoltre una mappa uniformemente continua* $i : K \to K_{\mathfrak{p}}$ *di immersione tale che* $i(K)$ *è denso in* $K_{\mathfrak{p}}$ *e una distanza* $\hat{d}_{\mathfrak{p}}$ *che estende* $d_{\mathfrak{p}}$ *ed è ancora ultrametrica.*

Esempio 2.1.4. Se si considera $K = \mathbb{Q}$ e come ideale si prende un qualunque primo non nullo (p), si ottiene il cosiddetto campo dei numeri p-adici che si indica con $\mathbb{Q}_p$.

Possiamo anche definire una norma indotta su $K_\mathfrak{p}$ nel seguente modo:

Proposizione 2.1.5. *Sia $x \in K_\mathfrak{p}^\times$, e $(x_n) \subset K$ una successione che tende a x; allora $|x|_\mathfrak{p} = \lim_{n\to\infty} |x_n|_\mathfrak{p}$ esiste ed è una buona definizione. Inoltre esiste un $k \in \mathbb{Z}$ tale che $|x|_\mathfrak{p} = \mathrm{N}(\mathfrak{p})^k$.*

Ovvero si può ancora definire una valutazione $\mathfrak{p}$-adica a valori interi su $K_\mathfrak{p}$ semplicemente tramite $\mathrm{N}(\mathfrak{p})^{-\upsilon_\mathfrak{p}(x)} = |x|_\mathfrak{p}$.

L'importanza di avere un campo completo è che ci si può fare dell'analisi; di questo parleremo meglio nella prossima sezione, ma anticipiamo una importante proprietà delle serie.

Proposizione 2.1.6. *Sia F un campo completo rispetto ad una norma ultrametrica $\|\ \|$. Allora una sequenza (a_n) converge se e solo se $\|a_{n+1} - a_n\|$ tende a 0; in particolare una serie $\sum_{n\geq 0} b_n$ converge se e solo se $\|b_n\| \to 0$.*

Dimostrazione. Essendo F completo, una successione converge se e solo se è di Cauchy, ovvero se $\forall \varepsilon > 0\ \exists N$ tale che se $m \geq n \geq N$ allora $\|a_m - a_n\| < \varepsilon$. Tuttavia possiamo osservare che $\|a_m - a_n\| = \left\|\sum_{m>j\geq n}(a_{j+1} - a_j)\right\|$, da cui, grazie alla proprietà ultrametrica, possiamo ricavare $\|a_m - a_n\| \leq \max_{m>j\geq n} \left\|a_{j+1} - a_j\right\|$; quindi se $\left\|a_{j+1} - a_j\right\| \to 0$, esiste un N per cui $\left\|a_{j+1} - a_j\right\| < \varepsilon$ per $j \geq N$, e dunque vale anche $\|a_m - a_n\| < \varepsilon$ per $m \geq n \geq N$.
Il risultato sulle serie segue banalmente, poiché $\sum_{n\geq 0} b_n$ converge se e solo se la successione delle somme parziali $a_n = \sum_{0\leq i<n} b_i$ converge, che per quanto appena visto accade se e solo se $\|a_{n+1} - a_n\| = \|b_n\| \to 0$ □

Abbiamo allora un immediato corollario specializzandoci ai $K_\mathfrak{p}$:

Corollario 2.1.7. *Una serie $\sum_{n\geq 0} a_n$ con $a_n \in K_\mathfrak{p}$ converge se e solo se $\upsilon_\mathfrak{p}(a_n) \to \infty$*

L'anello locale $\mathbb{Z}_\mathfrak{p}$

Passiamo ora a parlare dei cosiddetti interi $\mathfrak{p}$-adici, che hanno una struttura di anello locale.

Definizione 2.1.8. Dato $K_\mathfrak{p}$ campo p-adico, definiamo $\mathbb{Z}_\mathfrak{p}$ come il sottoinsieme degli $x \in K_\mathfrak{p}$ tali che $|x|_\mathfrak{p} \leq 1$, ovvero $\upsilon_\mathfrak{p}(x) \geq 0$.

Si osserva facilmente che $\mathbb{Z}_\mathfrak{p}$ è un anello, e viene perciò detto *anello degli interi $\mathfrak{p}$-adici*; vediamo ora una proprietà importante di questo anello.

Proposizione 2.1.9. *L'insieme $\mathbb{Z}_\mathfrak{p}$ è un* anello a valutazione discreta*, in particolare gli unici ideali non nulli sono della forma $\mathfrak{p}^k\mathbb{Z}_\mathfrak{p}$, l'unico ideale massimale è $\mathfrak{p}\mathbb{Z}_\mathfrak{p}$, e $x \in \mathbb{Z}_\mathfrak{p}$ è invertibile se e solo se $x \notin \mathfrak{p}\mathbb{Z}_\mathfrak{p}$ (ovvero $|x|_\mathfrak{p} = 1$).*

Vale inoltre una proprietà che lega i quozienti per gli ideali $\mathfrak{p}^k$ in $\mathcal{O}_K$ e in $\mathbb{Z}_\mathfrak{p}$:

Proposizione 2.1.10. *Per ogni $k \geq 1$ l'immersione $\mathcal{O}_K \hookrightarrow \mathbb{Z}_\mathfrak{p}$ induce un isomorfismo tra $\mathcal{O}_K/\mathfrak{p}^k$ e $\mathbb{Z}_\mathfrak{p}/\mathfrak{p}^k\mathbb{Z}_\mathfrak{p}$; dunque in particolare vale che $\mathbb{Z}_\mathfrak{p}/\mathfrak{p}\mathbb{Z}_\mathfrak{p} \cong \mathbb{F}_{p^f}$.*

Diamo ora una caratterizzazione importante degli elementi di $K_\mathfrak{p}$:

Proposizione 2.1.11. *Sia R un insieme di rappresentanti di $\mathcal{O}_K/\mathfrak{p}$ in $\mathcal{O}_K$, e per ogni $m \in \mathbb{Z}$ sia $\pi_m \in \mathfrak{p}^m \backslash \mathfrak{p}^{m+1}$ un elemento di valutazione esattamente m. Allora ogni $x \in K_\mathfrak{p}$ si scrive in modo unico come somma della serie*

$$x = \sum_{m \geq v_\mathfrak{p}(x)} a_m \pi_m \text{ con } a_m \in R, a_{v_\mathfrak{p}(x)} \notin \mathfrak{p}$$

Vediamo ora un risultato che permette di calcolare zeri di polinomi in $\mathbb{Z}_\mathfrak{p}$:

Lemma 2.1.12 (Hensel)**.** *Sia $f(X) \in \mathbb{Z}_\mathfrak{p}[X]$ e $\alpha \in \mathbb{Z}_\mathfrak{p}$ tale che $\left|f(\alpha)\right|_\mathfrak{p} < \left|f'(\alpha)\right|_\mathfrak{p}^2$. Allora esiste un'unica radice $\alpha^* \in \mathbb{Z}_\mathfrak{p}$ di $f(X) = 0$ tale che*

$$|\alpha^* - \alpha|_\mathfrak{p} \leq \frac{\left|f(\alpha)\right|_\mathfrak{p}}{\left|f'(\alpha)\right|_\mathfrak{p}}$$

La radice α^* è il limite della successione $\alpha_{k+1} = \alpha_k - \dfrac{f(\alpha_k)}{f'(\alpha_k)}$ con $\alpha_0 = \alpha$.

Spesso questo risultato viene usato nella seguente maniera, ovvero per sollevare radici di polinomi in $\mathbb{F}_p$ a radici in $\mathbb{Z}_p$

Corollario 2.1.13. *Sia $f(X) \in \mathbb{Z}[X]$ e $a \in \mathbb{Z}$ tale che $f(a) \equiv 0 \pmod p$ e $f'(a) \not\equiv 0 \pmod p$. Allora esiste $\alpha \in \mathbb{Z}_p$ tale che $f(\alpha) = 0$ in $\mathbb{Z}_p$ e $\alpha \equiv a \pmod{p\mathbb{Z}_p}$.*

Estensioni di campi p-adici

Concludiamo la sezione con un paio di teoremi sulle estensioni di campi p-adici

Teorema 2.1.14. *Sia $K \subset L$ estensione di campi di numeri, $\mathfrak{p}$ ideale primo di $\mathcal{O}_K$ e $\mathfrak{P}$ ideale primo di $\mathcal{O}_L$ sopra $\mathfrak{p}$; siano e, f indice di ramificazione e grado d'inerzia, ovvero $v_\mathfrak{P}(\mathfrak{p}\mathcal{O}_L) = e$, ed $f = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$.*
Allora $L_\mathfrak{P}$ è un'estensione finita di $K_\mathfrak{p}$, di grado $e \cdot f$.

Sia $L = K(\theta)$ un'estensione di campi di numeri, e consideriamo $T(X) \in K[X]$ il polinomio minimo di θ. Dato un primo $\mathfrak{p} \subset \mathcal{O}_K$, definiamo la $K_\mathfrak{p}$-algebra $K_\mathfrak{p}(\theta)$ tramite

$$K_\mathfrak{p}(\theta) = {}^{K_\mathfrak{p}[x]}\!\diagup_{T(x)K_\mathfrak{p}[x]}$$

Teorema 2.1.15. *Con le notazioni precedenti, supponiamo che valga la fattorizzazione* $\mathfrak{p}\mathcal{O}_L = \prod_{j=1}^{r} \mathfrak{P}_j^{e_j}$. *Allora*

1. *Gli unici valori assoluti su L che estendono $|\ |_\mathfrak{p}$ sono i $|\ |_{\mathfrak{P}_j}^{1/(e_j f_j)}$*
2. *Esiste un isomorfismo canonico $K_\mathfrak{p}(\theta) \cong K_\mathfrak{p} \otimes_K L \cong \bigoplus_{i=1}^{r} L_{\mathfrak{P}_j}$*

2.2 Analisi in campi p-adici

Quest'ultima sezione è dedicata a questioni di convergenza nei campi p-adici, che ricordiamo essere completi per costruzione.
Dato un campo p-adico $K_\mathfrak{p}$, sia $p \in \mathbb{Z}$ il primo sotto $\mathfrak{p}$; possiamo allora definire per ogni $x \in K_\mathfrak{p}$ la sua valutazione $\upsilon_p(x) = \frac{\upsilon_\mathfrak{p}(x)}{e}$ con e indice di ramificazione di $\mathfrak{p}$ sopra p, e la norma $|x|_p = |x|_\mathfrak{p}^{\frac{1}{ef}} = p^{-\upsilon_p(x)}$. Abbiamo già visto nella sezione precedente un importante criterio di convergenza delle serie, ovvero

Proposizione 2.2.1. *Una serie $\sum_{n\geq 0} a_n$ con $a_n \in K_\mathfrak{p}$ converge se e solo se $\upsilon_p(a_n) \to \infty$*

A noi interesserà principalmente studiare le serie esponenziali e logaritmiche; premettiamo alcuni lemmi sulle valutazioni di fattoriali e binomiali.

Definizione 2.2.2. Dato $x \in K_\mathfrak{p}$ e $n \in \mathbb{N}$, definiamo il *coefficiente binomiale*

$$\binom{x}{n} := \frac{x(x-1)\dots(x-n+1)}{n!}$$

Lemma 2.2.3. 1. *Dato $n \in \mathbb{N}$, vale*

$$\upsilon_p(n!) = \frac{n - s_p(n)}{p-1}$$

dove $s_p(n)$ è la somma delle cifre di n scritto in base p

2. *Se $x \in \mathbb{Z}_\mathfrak{p}$ e $n \in \mathbb{N}$ vale*

$$\upsilon_p\left(\binom{x}{n}\right) \geq 0$$

Proposizione 2.2.4. *La serie di potenze* $\exp_p(X) = \sum_{n\geq 0} \frac{X^n}{n!}$ *converge per* $|x|_p < r_p := p^{-1/(p-1)}$

Dimostrazione. Infatti $\upsilon_p\left(\frac{x^n}{n!}\right) = n\upsilon_p(x) - \upsilon_p(n!) = n\upsilon_p(x) - \frac{n-s_p(n)}{p-1} = n\left(\upsilon_p(x) - \frac{1}{p-1}\right) + \frac{s_p(n)}{p-1}$; affinché la serie converga è necessario e sufficiente che questa quantità tenda a ∞; ma $s_p(n)$ è frequentemente 1 (sulle potenze di p), quindi la condizione è equivalente a $\upsilon_p(x) > \frac{1}{p-1}$, che riscritto in norma è $|x|_p < r_p$. □

Del tutto analogamente si mostra anche la seguente

Proposizione 2.2.5. *La serie di potenze* $\log_p(1+X) = \sum_{n\geq 1}(-1)^{n+1}\frac{X^n}{n}$ *converge per* $|x|_p < 1$.

È inoltre possibile dare una condizione di convergenza della composizione di due serie:

Proposizione 2.2.6. *Siano* $f(X) = \sum_{n\geq 0} a_n X^n$ *e* $g(X) = \sum_{m\geq 1} b_m X^m$ *due serie di potenze (notare che quindi* $g(0) = 0$*), e consideriamo* $F(X) = f(g(X)) = \sum_{k\geq 0} X^k \sum_{0\leq n\leq k} c_{n,k}$ *la serie composta, ovvero con* $a_n g(X)^n = \sum_{k\geq n} c_{n,k} X^k$.
Detto R *il raggio di convergenza di* f*, se* x *è tale che* $g(x)$ *converge e inoltre* $|b_m x^m| < R$ *per* ogni $m \geq 1$*, allora anche la serie di potenze* $F(x)$ *converge e vale* $F(x) = f(g(x))$

Corollario 2.2.7. *Per* $|x|_p < r_p$ *e* $y \in \mathbb{Z}_p$ *la serie composta* $\varphi_x(y) = \exp_p(y\log_p(1+x))$ *converge. Inoltre per* $y \in \mathbb{Z}$*, si ha proprio* $\varphi_x(y) = (1+x)^y$

Dimostrazione. Osserviamo che se $|x|_p < r_p$, allora $\left|\log_p(1+x)\right|_p = |x|_p$: infatti vale $\left|\frac{x^{n-1}}{n!}\right|_p < r_p^{n-1} p^{\upsilon_p(n!)} \leq p^{-(n-1)/(p-1)} p^{(n-1)/(p-1)} = 1$ e dunque $\left|\frac{x^n}{n}\right|_p = \left|(n-1)!\, x\frac{x^{n-1}}{n!}\right|_p < |x|_p$ per $n > 1$. Dunque il termine dominante nella serie del logaritmo è il primo, e dunque per disuguaglianza ultrametrica si ha $\left|\log_p(1+x)\right|_p = |x|_p$.
Ma allora $\left|y\log_p(1+x)\right|_p = |y|_p\,|x|_p < 1 \cdot r_p$ e inoltre $\left|y\frac{x^n}{n}\right|_p < r_p$ (dato che $|y|_p \leq 1$), e dunque possiamo applicare la proposizione precedente e ottenere che la serie composta converge. □

Possiamo anche dare un significato ad una scrittura del tipo $(1+x)^y$ anche quando $y \notin \mathbb{Z}$. In particolare diamo la seguente

Definizione 2.2.8. Dati $x \in K_\mathfrak{p}$ e $y \in \mathbb{Z}_\mathfrak{p}$ definiamo $(1+x)^y$ tramite la serie di potenze $\sum_{n\geq 0} \binom{y}{n} x^n$, che converge per $\upsilon_\mathfrak{p}(x) > 0$.

Osservazione. Per $y \in \mathbb{Z}$ la serie coincide con il binomio di Newton, e quindi anche con la serie $\exp(y \log(1+x))$.

Possiamo poi stimare l'approssimazione di un troncamento di una serie, in maniera simile al teorema di Taylor.

Lemma 2.2.9. *Sia $f(x) = \sum_{n\geq 0} a_n \frac{x^n}{n!}$ e $p-1 \geq k \geq 1$. Supponiamo che $\upsilon_p(a_n) \geq z$ per $n \geq k$ e che $\upsilon_p(x) \geq \frac{1}{p-k}$. Allora vale*

$$\upsilon_p\left(f(x) - \sum_{0\leq n<k} a_n \frac{x^n}{n!}\right) \geq k\upsilon_p(x) + z$$

Come corollario otteniamo la seguente

Proposizione 2.2.10. *Sia $p \geq 3$, $x \in K_\mathfrak{p}$ e $y \in \mathbb{Z}_\mathfrak{p}$. Se $\upsilon_p(x) > 0$, esiste un $\beta \in \mathbb{Z}_\mathfrak{p}$ tale che*

$$(1+x)^y = 1 + yx + yx^2\beta$$

Vediamo ancora un lemma per una serie binomiale in un $K_\mathfrak{p}(\theta)$

Lemma 2.2.11. *Siano $n, k \in \mathbb{Z}$ con $(p,k) = 1$; sia θ un intero algebrico. Sia $t \in \mathbb{Q}_p(\theta)$ con $\upsilon_p(t) > 0$. Allora vale*

$$\left((1+t)^n\right)^{\frac{1}{k}} = (1+t)^{\frac{n}{k}}$$

Dimostrazione. Chiamiamo $\beta_1 = \left((1+t)^n\right)^{\frac{1}{k}}$ e $\beta_2 = (1+t)^{\frac{n}{k}}$. Osserviamo che $\beta_1^k = (1+t)^n = \beta_2^k$ per la proposizione 2.2.6.
Dato che $\upsilon_p(t) > 0$, per ogni $\mathfrak{p}$ ideale primo di $\mathbb{Q}(\theta)$ sopra p vale $\beta_1 \equiv \beta_2 \equiv 1 \pmod{\mathfrak{p}}$. Allora β_i, β_i^k sono invertibili in $\mathbb{Q}_p(\theta)$; perciò dividendo otteniamo $\left(\frac{\beta_1}{\beta_2}\right)^k = 1$.
Ma allora $\gamma = \frac{\beta_1}{\beta_2}$ è una radice dell'unità, e vale $\gamma \equiv 1 \pmod{\mathfrak{p}}$. Se per assurdo $\gamma \neq 1$, varrebbe $0 = \frac{\gamma^k - 1}{\gamma - 1} = 1 + \gamma + \cdots + \gamma^{k-1} \equiv k \pmod{\mathfrak{p}}$. Questo però implicherebbe $p \mid k$ che è contro l'ipotesi.
Abbiamo perciò $\frac{\beta_1}{\beta_2} = \gamma = 1$. □

Mostriamo infine il risultato più importante della sezione, che ci permetterà di trovare efficientemente gli zeri delle serie di potenze.

Teorema 2.2.12 (Strassmann)**.** *Sia $f(x) = \sum_{n\geq 0} f_n x^n$ una serie di potenze con coefficienti $f_n \in K_\mathfrak{p}$ non tutti nulli. Supponiamo che valga $|f_n|_\mathfrak{p} \to 0$ e prendiamo N il più grande intero per cui $|f_N|_\mathfrak{p} = \max |f_n|_\mathfrak{p}$.*
Allora l'equazione $f(x) = 0$ ha al più N soluzioni con $x \in \mathbb{Z}_\mathfrak{p}$

Dimostrazione. Si dimostra per induzione su N. Per $N = 0$ supponiamo che esista un $x_0 \in \mathbb{Z}_\mathfrak{p}$ per cui $f(x_0) = 0$, ovvero $f_0 = -\sum_{n\geq 1} f_n x_0^n$; dato che $|f_0|_\mathfrak{p} > |f_n|_\mathfrak{p}$ per $n > 0$ e $|x_0|_\mathfrak{p} \leq 1$, per disuguaglianza ultrametrica otteniamo $\left|\sum_{n\geq 1} f_n x_0^n\right|_\mathfrak{p} < |f_0|_\mathfrak{p}$, che è assurdo.
Sia ora $N > 0$ e prendiamo un $\bar{x} \in \mathbb{Z}_\mathfrak{p}$ tale che $f(\bar{x}) = 0$ (se non esiste, il teorema è verificato banalmente). Consideriamo poi $y \in \mathbb{Z}_\mathfrak{p}$ e scriviamo

$$f(y) = f(y) - f(\bar{x}) = \sum_{n\geq 1} f_n(y^n - \bar{x}^n) = (y - \bar{x}) \sum_{n\geq 1} \sum_{0\leq j<n} f_n y^j \bar{x}^{n-1-j}$$

Dato che $|f_n|_\mathfrak{p} \to 0$, $\left|y^j x^{n-1-j}\right|_\mathfrak{p} \leq 1$ e la seconda somma è finita, si può scambiare l'ordine delle due sommatorie e scrivere $f(y) = (y-\bar{x})g(y)$, dove $g(y) = \sum_{m\geq 0} g_m y^m$ con $g_m = \sum_{r\geq 0} f_{m+1+r} x^r$. Vediamo ora che $|g_m|_\mathfrak{p} \leq \max_{i\geq m+1} |f_i|_\mathfrak{p}$, quindi anche $|g_m|_\mathfrak{p} \to 0$ e $|f_N|_\mathfrak{p} = |g_{N-1}|_\mathfrak{p} > \left|g_j\right|_\mathfrak{p}$ per $j \geq N$; inoltre per $j < N$ vale $\left|g_j\right|_\mathfrak{p} \leq |f_N|_\mathfrak{p}$. Quindi $N-1$ è il più grande intero per cui si ha $|g_{N-1}|_\mathfrak{p} = \max \left|g_j\right|_\mathfrak{p}$, cioè g soddisfa le ipotesi induttive e quindi ha al più $N-1$ zeri in $\mathbb{Z}_\mathfrak{p}$.
Infine, $f(y) = 0$ se e solo se $y = \bar{x}$ oppure $g(y) = 0$, perciò ho al più N punti di $\mathbb{Z}_\mathfrak{p}$ (contati con molteplicità) in cui si annulla f. □

Osservazione. Sebbene il bound dato dal teorema sia spesso sharp, stiamo trovando zeri su tutto $\mathbb{Z}_\mathfrak{p}$, mentre a noi interesseranno gli zeri in $\mathbb{Z}$, e non ci sono modi per distinguere uno zero intero da uno $\mathfrak{p}$-adico.

3

Il metodo di Skolem

L'osservazione fondamentale del metodo di Skolem è che sotto opportune ipotesi di convergenza una potenza intera può essere trasformata in una serie di potenze in qualche campo p-adico, in cui la variabile è l'esponente. Questo permette di controllare efficacemente il comportamento di potenze con base fissata.
È questo il caso sia per le successioni di ricorrenza, in cui le soluzioni sono combinazioni lineari polinomiali di potenze di radici del polinomio caratteristico; sia per studiare le unità di un campo di numeri, quando queste hanno rango 1, scrivendo l'unità generica come potenza dell'unità fondamentale.

3.1 Il teorema di Skolem-Mahler

In questa sezione studieremo gli zeri di successioni per ricorrenza tramite gli strumenti dell'analisi p-adica, e in particolare il teorema di Strassmann. Il risultato che vogliamo mostrare è il seguente

Teorema 3.1.1 (Skolem-Mahler)**.** *Sia K un campo di numeri e siano $c_0, \dots, c_{s-1} \in K$ dei coefficienti fissati. Costruiamo la successione per ricorrenza $a_{n+s} = \sum_{i=0}^{s-1} c_i a_{n+i}$, a partire da $a_0, \dots, a_{s-1} \in K$. Definiamo l'insieme su cui la successione si annulla $A_0 = \{n \in \mathbb{N} \mid a_n = 0\}$.*
Allora A_0 è l'unione di un numero finito di progressioni aritmetiche (con la stessa ragione) e di un insieme finito.

Osservazione.

- Il teorema continua ad essere vero in qualunque campo di caratteristica 0 (dimostrato in [Lec53])
- Invece in caratteristica p è in generale falso: se si considera la successione $a_n = (1+t)^n - 1 - t^n$ in $\mathbb{F}_p(t)$, vale $A_0 = \{p^n \mid n \in \mathbb{N}\}$ che non è unione di progressioni aritmetiche. Infatti vale $a_n = \sum_{i=1}^{n-1} \binom{n}{i} t^i$, e per

$n = p^k q$ con $q \neq 1$ si ha $p \nmid \binom{p^k q}{p^k}$, mentre per $n = p^k$ tutti i binomiali sono multipli di p.

- Tuttavia anche in caratteristica p esiste un analogo teorema di struttura per A_0, enunciato e dimostrato in [Der07].

Utilizzando la teoria dei campi p-adici possiamo provare questo risultato senza troppa difficoltà.

Dimostrazione. Consideriamo $f(x) = x^s - \sum_{i=0}^{s-1} c_i x^i \in K[x]$ il polinomio associato alla successione, che ha radici $\alpha_1, \ldots, \alpha_s$ in una qualche estensione finita $L \supset K$. Osserviamo che esiste un intero d tale che $\beta_i = d\alpha_i \in \mathcal{O}_L$ per ogni i.
Grazie alla teoria generale delle successioni per ricorrenza sappiamo che esistono polinomi $g_i(t) \in L[t]$ per cui si ha

$$a_n = \sum_{i=1}^{s} g_i(n)\alpha_i^n$$

Cerchiamo ora un intero k e un ideale primo $\mathfrak{P} \in \mathcal{O}_L$ per cui si abbia $\beta_i^k = 1 + \pi_i$ con $\pi_i \in \mathcal{O}_L$ e $\upsilon_{\mathfrak{P}}(\pi_i) \geq 1$ per ogni i.
Sia S l'insieme dei divisori primi di un qualche $\mathrm{N}_{L/\mathbb{Q}}(\beta_i)$, e sia T l'insieme dei primi che dividono $\operatorname{disc} L$. Dato che entrambi gli insiemi sono finiti, esiste un primo $p \notin S \cup T \cup \{2\}$. Questo primo p non ramifica in L e nemmeno in K per il teorema 1.3.12; possiamo allora prendere un primo $\mathfrak{p} \subset \mathcal{O}_K$ sopra p e poi un $\mathfrak{P} \subset \mathcal{O}_L$ sopra $\mathfrak{p}$, entrambi con ramificazione 1, in modo che $\upsilon_p = \upsilon_{\mathfrak{p}} = \upsilon_{\mathfrak{P}}$.
Sappiamo inoltre che $\mathcal{O}_L/\mathfrak{P} = \mathbb{F}_{p^h}$ per un qualche h, e su questo campo vale che $x^{p^h-1} = 1$ per $x \neq 0$; sollevando questa relazione otteniamo quindi che $x^{p^h-1} - 1 \in \mathfrak{P}$ se $\mathfrak{P} \nmid (x)$.
Dato che abbiamo scelto $\mathfrak{P}$ in modo che non divida nessuno dei β_i, vale allora $\beta_i^{p^h-1} = 1 + \pi_i$ con $\pi_i \in \mathfrak{P}$ e quindi $\upsilon_{\mathfrak{P}}(\pi_i) \geq 1$.
Ponendo $k = p^h - 1$, possiamo allora scrivere $a_{kq+r} = \sum_{i=1}^{s} g_i(kq+r)d^{-r}\alpha_i^r(1+\pi_i)^q$ e quindi espandere ognuna delle potenze q-esime come serie di potenze $\mathfrak{P}$-adiche grazie al corollario 2.2.7.
In particolare, possiamo scrivere

$$a_{kq+r} = f_r(q) = \sum_{i=0}^{s} g_i(kq+r)d^{-r}\alpha_i^r \exp(q\log(1+\pi_i))$$

Otteniamo perciò k serie di potenze $f_r(x)$ (una per ciascun resto) in $L_{\mathfrak{P}}$: per il teorema di Strassmann ognuna di queste o è sempre nulla, oppure si annulla in un numero finito di punti (gli zeri sono in $\mathbb{Z}_{\mathfrak{P}}$, quindi a maggior

ragione ce n'è un numero finito $\in \mathbb{Z}$).
Poniamo quindi $X = \{r \in \{0, 1, \dots, k\} \mid f_r(x) \equiv 0\}$ e $Y = \{0, 1, \dots, k\} \backslash X$; vale allora che l'insieme $Z = \bigcup_{r \in Y} \{kq + r \mid q \in \mathbb{Z}, f_r(q) = 0\}$ è finito in quanto ogni elemento dell'unione è finito per Strassmann.
Ma quindi possiamo concludere che $A_0 = \bigcup_{r \in X} \{kt + r\}_{t \in \mathbb{N}} \bigcup Z$ □

Vediamo ora una dimostrazione alternativa, seguendo [Han85]

Dimostrazione. Invece di usare il polinomio caratteristico della successione, utilizziamo il formalismo dell'algebra lineare.
Scriviamo allora la relazione di ricorrenza tramite una matrice M:

$$\begin{pmatrix} a_{n+s} \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} c_{s-1} & c_{s-2} & \dots & c_0 \\ 1 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n+s-1} \\ \vdots \\ a_n \end{pmatrix}$$

Ponendo allora $v_n = \begin{pmatrix} a_{n+s-1} \\ \vdots \\ a_n \end{pmatrix}$, possiamo scrivere in modo compatto $v_{n+1} = Mv_n$ e quindi in generale $v_k = M^k v_0$. Se poniamo ora $w = \begin{pmatrix} 0 & \dots & 1 \end{pmatrix}$ possiamo scrivere $a_n = w \cdot v_n = w \cdot M^n v_0$.
Ricordiamo che la matrice M ha coefficienti in $\mathcal{O}_K$, quindi $\det M \in \mathcal{O}_K$; consideriamo ora un primo $\mathfrak{p}$ che non divida il determinante, che non ramifichi e tale che $\mathfrak{p} \nmid (2)\mathcal{O}_K$, e sia $\overline{M}$ la proiezione di M su $\mathrm{GL}_n(\mathcal{O}_K/\mathfrak{p})$. Dato che $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^s}$, $\overline{M}$ è una matrice con determinante non nullo a coefficienti in un campo finito, dunque è invertibile e allora esiste un intero h per cui $\overline{M}^h = I$ matrice identità. Risollevando in $\mathcal{O}_K$ otteniamo allora $M^h = I + B$ dove tutti i coefficienti di B sono in $\mathfrak{p}$.
A questo punto l'idea è uguale a quella della dimostrazione precedente, ovvero scrivere gli elementi della successione come serie di potenze in $K_\mathfrak{p}$: se facciamo la divisione con resto $n = qh + r$, possiamo scrivere

$$a_{hq+r} = w \cdot M^{qh} M^r v_0 = w \cdot (I + B)^q v_r = w \cdot \sum_{i=0}^{q} \binom{q}{i} B^i v_r$$

Ponendo $d_{r,i} = w \cdot B^i v_r$, dato che i coefficienti di B appartengono a $\mathfrak{p}$, ricaviamo che $d_{r,i} \in \mathfrak{p}^i$. Otteniamo allora $a_{qh+r} = \sum_{i=0}^{q} \binom{q}{i} d_{r,i}$, ed espandendo il binomiale possiamo riscriverla come serie di potenze in q:

$$a_{qh+r} = \sum_{l \geq 0} q^l \left(\sum_{k \geq l} \frac{d_{r,k} c_{l,k}}{k!} \right)$$

dove $c_{l,k}$ è il coefficiente di q^l nel numeratore di $\binom{q}{k}$. La serie tra parentesi converge $\mathfrak{p}$-adicamente per ogni $l \geq 0$ poiché $d_{r,k}c_{l,k} \in \mathfrak{p}^k$, mentre $v_\mathfrak{p}(k!) < k/2$ (ricordiamo infatti che $\mathfrak{p}$ non ramifica). Ma allora, fissato r, abbiamo una serie di potenze in q, che per Strassmann o è nulla oppure ha un numero finito di zeri. □

Osserviamo che shiftando la successione $a_n \mapsto a_n - c$ otteniamo una nuova successione per ricorrenza, alla quale applicare il teorema appena dimostrato, ovvero vale il seguente

Corollario 3.1.2. *La tesi del teorema non vale solo con A_0, ma anche con tutti gli $A_c = \{n \in \mathbb{N} \mid a_n = c\}$.*

Concludiamo la sezione con un'applicazione concreta, per far vedere che in svariati casi il metodo permette di determinare esplicitamente alcuni A_c.

Esempio 3.1.3. Prendiamo la successione $a_{n+2} = 2a_{n+1} - 3a_n$ con termini iniziali $a_0 = a_1 = 1$. La successione in forma chiusa è allora

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

Vogliamo ora mostrare che $|a_n| \to \infty$. Questo non è un esercizio banale, infatti i due termini hanno lo stesso modulo e non è ovvio che la sequenza non possa essere frequentemente vicino a 0.
Osserviamo innanzitutto che $(1+\sqrt{-2})^5 = 1-11\sqrt{-2}$ e che vale $\sqrt{-2} \in \mathbb{Z}_{11}$ poiché $x^2+2 \equiv x^2-9 \equiv (x-3)(x+3) \pmod{11}$ e quindi grazie al lemma di Hensel possiamo sollevare 3 ad una radice di x^2+2 in $\mathbb{Z}_{11}$.
Questo ci induce allora a prendere $\mathbb{Q}_{11}$ e ad espandere la formula per a_n come nella dimostrazione di Skolem-Mahler; possiamo farlo poiché $v_{11}(11\sqrt{-2}) = 1 > \frac{1}{11-1}$.
Otteniamo quindi 5 serie di potenze, corrispondenti a $r = 0, \ldots, 4$

$$\begin{aligned} f_r(q) = \frac{1}{2}\Big((1+\sqrt{-2})^r \exp_{11}(q\log_{11}(1-11\sqrt{-2})) \\ + (1-\sqrt{-2})^r \exp_{11}(q\log_{11}(1+11\sqrt{-2}))\Big) \end{aligned} \tag{3.1}$$

Per il corollario, ogni f_r o è costante, oppure assume un numero finito di volte ogni valore intero.
Basta allora scrivere i primi valori della successione:

0	1	2	3	4
1	1	−1	−5	−7
1	23	43	17	−95
−241				

per vedere che nessuna colonna è costante, dunque concludere che la successione $|a_n|$ tende davvero a ∞.

Possiamo inoltre mostrare che $A_1 = \{0, 1, 5\}$, ovvero le uniche volte che la successione assume il valore 1 sono quelle scritte in tabella.
Vogliamo quindi risolvere $f_r(q) = 1$. Osserviamo innanzitutto che $f_r(q) \equiv f_r(0) \pmod{11}$, quindi le soluzioni avranno tutte $r = 0, 1$. L'obiettivo è quello di espandere la serie di potenze con la precisione necessaria per poter trovare esplicitamente l'N del teorema di Strassmann.
Per fare ciò dobbiamo innanzitutto calcolare $\sqrt{-2}$; grazie al lemma di Hensel scopriamo che (uno dei due possibili valori di) $\sqrt{-2}$ è $3 + 9 \cdot 11 + 11^2 \cdot M$ con $M \in \mathbb{Z}_{11}$, ovvero

$$1 + 11\sqrt{-2} \equiv 1 + 3 \cdot 11 + 9 \cdot 11^2 \pmod{11^3\mathbb{Z}_{11}}$$

Ma allora, per il lemma 2.2.9 vale $\log(1 + 11t) \equiv 11t - 11^2 \frac{t^2}{2} \pmod{11^3\mathbb{Z}_{11}}$, da cui otteniamo

$$t_1 = \log(1 + 11\sqrt{-2}) \equiv 3 \cdot 11 + \frac{9}{2}11^2 \equiv 3 \cdot 11 + 10 \cdot 11^2 \pmod{11^3\mathbb{Z}_{11}}$$

Analogamente si ha

$$t_2 = \log(1 - 11\sqrt{-2}) \equiv 8 \cdot 11 + 2 \cdot 11^2 \pmod{11^3\mathbb{Z}_{11}}$$

Osserviamo ora che $f_0(q) = \frac{1}{2}\big(\exp(qt_1) + \exp(qt_2)\big)$, dove abbiamo

$$\exp(qt_i) = \sum_{n \geq 0} q^n \frac{t_i^n}{n!}$$

e vale $v_{11}\left(\frac{t_i^n}{n!}\right) \geq 3$ per $n \geq 3$ dunque si ha

$$f_0(q) = 1 + q\frac{t_1 + t_2}{2} + q^2\frac{t_1^2 + t_2^2}{4} + \sum_{n \geq 3} q^n c_n$$

con $c_n \equiv 0 \pmod{11^3\mathbb{Z}_{11}}$.
Con qualche conto possiamo ricavare che $\frac{t_1 + t_2}{2} \equiv 11^2 \pmod{11^3\mathbb{Z}_{11}}$ e $\frac{t_1^2 + t_2^2}{4} \equiv 10 \cdot 11^2 \pmod{11^3\mathbb{Z}_{11}}$, perciò applicando Strassmann alla serie $f_0(q) - 1$ otteniamo che ci sono al più $N = 2$ zeri interi, che sono esattamente $q = 0, 1$.

Invece per il caso $r = 1$ possiamo scrivere

$$\begin{aligned} f_1(q) = 1 &+ q\frac{(1 - \sqrt{-2})t_1 + (1 + \sqrt{-2})t_2}{2} \\ &+ q^2\frac{(1 - \sqrt{-2})t_1^2 + (1 + \sqrt{-2})t_2^2}{4} + \sum_{n \geq 3} q^n c_n \end{aligned} \tag{3.2}$$

e con un conto simile a sopra si ricava che il coefficiente di q ha valutazione 1, e tutti quelli dopo hanno valutazione almeno 2; perciò per il teorema di Strassmann esiste al più $N = 1$ zero, che noi conosciamo già essere $q = 0$.

3.2 L'equazione $x^3 + dy^3 = 1$

Fissato un $d \in \mathbb{Z}$, vogliamo trovare le coppie $(x, y) \in \mathbb{Z}^2$ che risolvono $x^3 + dy^3 = 1$, in certi casi detta "equazione di Skolem". Possiamo scrivere $d = ab^3$ con a libero da cubi, e riscrivere l'equazione come $x^3 + a(by)^3 = 1$; quindi le diofantee che ci interessano davvero sono quelle con d libero da cubi.
Inoltre se $d = \pm 1$, abbiamo semplicemente $x^3 \pm y^3 = 1$; assorbiamo il segno in y^3 e risolviamo $x^3 - y^3 = 1$.
Allora possiamo fattorizzare ottenendo $(x - y)(x^2 + xy + y^2) = 1$ da cui $x - y = \pm 1$ e $x^2 + xy + y^2 = \pm 1$; osserviamo che $x^2 + xy + y^2 = (x - y)^2 + 3xy$, perciò abbiamo $\pm 1 = 1 + 3xy$. Guardando modulo 3, il segno deve essere $+$ e ricaviamo $xy = 0$; unendo questa a $x - y = 1$ otteniamo infine che le uniche soluzioni sono $(0, -1)$ e $(1, 0)$.

In tutti gli altri casi possiamo fattorizzare la diofantea in $\mathbb{C}$ nel seguente modo: $(x + \theta y)(x + \theta\omega y)(x + \theta\omega^2 y) = 1$ dove $\theta = \sqrt[3]{d}$ e $\omega = \exp \frac{2\pi i}{3}$.
Se consideriamo $K = \mathbb{Q}(\theta)$, abbiamo la norma $N = N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ e la fattorizzazione precedente ci dice che (x, y) è soluzione se e solo se $N(x + \theta y) = 1$, che implica $x + \theta y \in \mathcal{O}_K^\times$.
Osserviamo che K ha segnatura $(1, 1)$ e quindi le unità di $\mathcal{O}_K$ hanno rango 1; esiste allora un unico ε tale che ogni unità di $\mathcal{O}_K$ sia della forma $\pm\varepsilon^n$ e valga $\varepsilon > 1$ rispetto all'unico embedding reale di K.
Per risolvere la diofantea occorre quindi trovare gli interi n per cui ε^n è della forma $x + \theta y$ (ci interessano infatti solo le unità di norma 1).
Dimostriamo che in realtà vale

Teorema 3.2.1 ([Del30], poi [Sko52])**.** *L'equazione $x^3 + dy^3 = 1$ ha al più 2 soluzioni intere, inclusa quella banale $(1, 0)$.*

Seguiamo la dimostrazione di [Coh07].

Dimostrazione. Supponiamo per assurdo che esistano due interi n_1, n_2 entrambi non nulli tali che $\varepsilon^{m_1} = x_1 + y_1\theta$ e $\varepsilon^{m_2} = x_2 + y_2\theta$; scriviamo $\frac{m_1}{m_2} = \frac{n_1}{n_2}$ con $(n_1, n_2) = 1$ e supponiamo per simmetria che $3 \nmid n_1$, e dunque possiamo scrivere che $(x_1 + y_1\theta)^{n_2} = (x_2 + y_2\theta)^{n_1}$.
Osserviamo che detto $z = x_i + y_i\theta$ vale $(z - 1)^3 = z^3 - 1 + 3K$ e anche $z^3 = x_i^3 + 3x_iy_i(x_i\theta + y_i\theta^2) + dy_i^3 = 1 + 3H$, quindi abbiamo $(z - 1)^3 = 3(H + K)$ ma allora $x_i - 1 + y_i\theta$ ha valutazione 3-adica positiva.
Dato che $3 \nmid n_1$, grazie al lemma 2.2.11 otteniamo che $(x_1 + y_1\theta)^{\frac{n_2}{n_1}} =$

$x_2 + y_2\theta$; possiamo vedere $N = \frac{n_2}{n_1}$ come un elemento di $\mathbb{Z}_3$ e perciò scrivere $N = 3M + r$ con $r \in \{0, 1, 2\}$ e $M \in \mathbb{Z}_3$. Studiamo l'uguaglianza $(x_1 + y_1\theta)^N = x_2 + y_2\theta$ in $\mathbb{Q}_3(\theta) = {}^{\mathbb{Q}_3[x]}\!/_{(x^3 - d)\mathbb{Q}_3[x]}$ che per il teorema 2.1.15 è una somma diretta di $K_\mathfrak{p}$ con $\mathfrak{p}$ primi sopra 3.
Espandendo la potenza usando $N = 3M + r$ e $(x_1 + y_1\theta)^3 = x_1^3 + 3x_1^2y_1\theta + 3x_1y_1^2\theta^2 + y_1^3\theta^3 = 1 + 3x_1y_1G$ con $G = x_1\theta + y_1\theta^2$, possiamo riscrivere l'uguaglianza come

$$x_2 + y_2\theta = (1 + 3x_1y_1G)^M(x_1 + y_1\theta)^r \tag{3.3}$$

Grazie alla proposizione 2.2.10 possiamo troncare la serie binomiale $(1 + 3x_1y_1G)^M$ e ottenere $(1 + 3x_1y_1G)^M = 1 + 3Mx_1y_1G + 9Mx_1^2y_1^2G^2\beta$ con $\beta \in \mathbb{Z}_3[\theta]$.
Scrivendo allora $G^2\beta = B_0 + B_1\theta + B_2\theta^2$ con $B_i \in \mathbb{Z}_3$, dato che $1, \theta, \theta^2$ sono ancora indipendenti in $\mathbb{Q}_3(\theta)$ come $\mathbb{Q}_3$-spazio vettoriale, possiamo confrontare il coefficiente di θ^2 nell'equazione 3.3 e a seconda di r otteniamo 3 equazioni, ovvero

$$0 = \begin{cases} 3Mx_1y_1^2(1 + 3x_1B_2) & r = 0 \\ 3Mx_1^2y_1^2(2 + 3y_1B_1 + 3x_1B_2) & r = 1 \\ y_1^2(1 + 9Mx_1^2(x_1 + B_2x_1^2 + 2B_1x_1y_1 + B_0y_1^2)) & r = 2 \end{cases} \tag{3.4}$$

Dato che $x_1, y_1 \neq 0$ e $N \neq 0, 1$ cioè $M \neq 0$ per $r = 0, 1$, possiamo dividere le tre equazioni rispettivamente per $3Mx_1y_1^2, 3Mx_1^2y_1^2, y_1^2$. Ma allora otteniamo subito un assurdo modulo 3, poiché $M, x_1, y_1, B_i \in \mathbb{Z}_3$. □

Mostriamo ora un altro approccio utile per risolvere diofantee specifiche.

Esempio 3.2.2. Risolviamo ora l'equazione $x^3 + 2y^3 = 1$. Naturalmente grazie al teorema appena fatto sappiamo che le uniche soluzioni sono $(1, 0)$ e $(-1, 1)$; tuttavia useremo un approccio leggermente diverso da quello della dimostrazione precedente.
Consideriamo allora $K = \mathbb{Q}[\theta] = {}^{\mathbb{Q}[t]}\!/_{(t^3 - 2)}$. Come già detto, ogni soluzione della diofantea è un'unità di $\mathcal{O}_K$ della forma $x + y\theta$; in particolare possiamo vedere che $\varepsilon = \theta - 1$ è un'unità fondamentale di norma 1, dunque dobbiamo trovare soluzioni di $x + y\theta = \varepsilon^n$.
Osserviamo ora che il polinomio $t^3 - 2$ spezza completamente in $\mathbb{F}_{31}$ e dunque anche in $\mathbb{Q}_{31}$. Dette c_1, c_2, c_3 le radici di $t^3 - 2$ in $\mathbb{Q}_{31}$ allora esistono tre embedding $\tau_i : K \to \mathbb{Q}_{31}$ tali che $\tau_i(\theta) = c_i$; definiamo inoltre $e_i = \tau_i(\varepsilon) = c_i - 1$.
Se allora consideriamo l'uguaglianza $x + y\theta = \varepsilon^n$ e applichiamo τ_i, otteniamo $x + yc_i = e_i^n$; moltiplicando per c_i e sommando otteniamo $x\sum c_i + y\sum c_i^2 = \sum c_ie_i^n$, ma dato che vale $t^3 - 2 = (x - c_1)(x - c_2)(x - c_3)$, otteniamo che

$\sum c_i = \sum c_i^2 = 0$, ovvero $c_1 e_1^n + c_2 e_2^n + c_3 e_3^n = 0$. Inoltre vale $e_1 e_2 e_3 = 1$ perché ε ha norma 1, quindi possiamo riscrivere l'equazione come

$$c_1 + c_2 e_2^{2n} e_3^n + c_3 e_2^n e_3^{2n} = 0 \tag{3.5}$$

Adesso occorre fare qualche conto esplicito; in particolare calcoliamo $c_1 \equiv 4 + 9 \cdot 31 \pmod{31^2\mathbb{Z}_{31}}$, $c_2 \equiv 7 + 13 \cdot 31 \pmod{31^2\mathbb{Z}_{31}}$, e $c_3 \equiv 20 + 8 \cdot 31 \pmod{31^2\mathbb{Z}_{31}}$, da cui si ricavano immediatamente anche gli e_i. Se ora guardiamo la 3.5 modulo 31, otteniamo $4 + 7 \cdot 2^n + 20 \cdot 27^n \equiv 0$ da cui si ricava $n \equiv 0, 1 \pmod{10}$.
Se $n = 10m$, possiamo riscrivere la 3.5 come $f(m) = c_1 + c_2 \left(e_2^{20} e_1^{10}\right)^m + c_3 \left(e_2^{10} e_1^{20}\right)^m = 0$, dove $e_2^{20} e_3^{10} \equiv 1 + 4 \cdot 31 \pmod{31^2\mathbb{Z}_{31}}$ e $e_2^{10} e_3^{20} \equiv 1 + 13 \cdot 31 \pmod{31^2\mathbb{Z}_{31}}$; ovvero possiamo vedere $f(m)$ come serie di potenze in m, in particolare

$$f(m) = c_1 + c_2 \exp(m \log(e_2^{20} e_3^{10})) + c_3 \exp(m \log(e_2^{10} e_3^{20}))$$

Ricordiamo che $\log(e_2^{20} e_3^{10})$ è multiplo di 31, quindi scrivendo $f(m) = d_0 + d_1 m + \sum_{k \geq 2} m^k d_k$ si ha $\upsilon_{31}(d_k) \geq k$.
Vediamo ora che $d_0 = f(0) = c_1 + c_2 + c_3 = 0$, mentre $d_1 = c_2 \log(e_2^{20} e_3^{10}) + c_3 \log(e_2^{10} e_3^{20}) \equiv 9 \cdot 31 \pmod{31^2\mathbb{Z}_{31}}$.
Possiamo allora applicare Strassmann con $N = 1$ e ottenere che $f(m) = 0$ ha al più una soluzione, data da $m = 0$, ovvero la soluzione banale $(1, 0)$ della diofantea.
Se $n = 10m + 1$, la serie di potenze cambia in minima parte:

$$f(m) = c_1 + c_2 e_2^2 e_3 \exp(m \log(e_2^{20} e_3^{10})) + c_3 e_2 e_3^2 \exp(m \log(e_2^{10} e_3^{20}))$$

e si ricava $d_0 = c_1 + c_2 e_2^2 e_3 + c_3 e_2 e_3^2 = 0$ (ricordiamo che $c_i = e_i + 1$ e $e_1 e_2 e_3 = 1$), mentre $d_1 = c_2 e_2^2 e_3 \log(e_2^{20} e_3^{10}) + c_3 e_2 e_3^2 \log(e_2^{10} e_3^{20}) \equiv 8 \cdot 31 \pmod{31^2\mathbb{Z}_{31}}$.
Come sopra applichiamo Strassmann con $N = 1$, che ci dà come unica soluzione $n = 1$ ovvero $x + y\theta = \varepsilon^1 = \theta - 1$.

4

Il teorema di Delone

Il teorema di Skolem afferma che la diofantea $x^3 + dy^3 = 1$ ha al più una soluzione non banale.
In questo capitolo ridimostriamo il teorema senza strumenti p-adici, e caratterizziamo la soluzione non banale: è l'unità fondamentale di $\mathbb{Z}[\theta]$, se questa non ha il termine in θ^2.
Per il teorema di Dirichlet, $\mathbb{Z}[\theta]^\times$ ha rango 1, quindi è generato da un elemento ε, e ci sono esattamente 4 candidati ad essere chiamati unità fondamentale: $\pm\varepsilon, \pm\frac{1}{\varepsilon}$; di questi ce n'è esattamente uno tale che $0 < \varepsilon_0 < 1$, e sarà questa la nostra unità fondamentale.
Siamo pronti ora ad enunciare il seguente:

Teorema (Delone)**.** *L'equazione $x^3 + dy^3 = 1$ (con d cubefree e diverso da ± 1) ha al più una soluzione non banale, data dall'unità fondamentale ε_0 di $\mathbb{Z}[\theta]$ se è della forma $a + b\theta$.*

4.1 Dimostrazione

Seguiremo la dimostrazione in [DF64], e iniziamo dando alcune notazioni.

Definizione 4.1.1. Le potenze positive di ε_0, cioè quelle con $\varepsilon_0^m < 1$ e $m > 0$, si dicono unità *dirette*.
Le potenze negative di ε_0, ovvero $\varepsilon = \varepsilon_0^m$ con $m < 0$ e $\varepsilon > 1$, si dicono unità *inverse*.

Definizione 4.1.2. Un'unità di $Z[\theta]$ con norma 1 si dice *binomiale* se è della forma $B\theta + C$ con $B, C \in \mathbb{Z}$.

Nella nostra ricerca di unità binomiali, ovvero soluzioni della diofantea, ci saranno utili alcuni lemmi.

Osservazione. Ricordiamo che abbiamo tre embedding $K \to \mathbb{C}$, di cui uno reale e una coppia di complessi coniugati. Sia $\sigma_1 : K \to \mathbb{R}$ quello reale,

ovvero $\sigma_1(\theta) = \sqrt[3]{d}$ e invece $\sigma_2 : K \to \mathbb{C}$ tale che $\sigma_2(\theta) = \sqrt[3]{d}\omega$; vale allora $N(z) = \sigma_1(z) \cdot |\sigma_2(z)|^2$.
Consideriamo d'ora in poi $\mathbb{Z}[\theta]$ come sotto-anello di $\mathbb{R}$, ovvero identificando z e $\sigma_1(z)$.

Osservazione. Si verifica che se $z = A\theta^2 + B\theta + C \in \mathbb{Z}[\theta]$, allora

$$N(z) = A^3d^2 + B^3d + C^3 - 3dABC \tag{4.1}$$

Si ricava anche facilmente che

$$\frac{1}{z} = (C^2 - dAB) + \theta(dA^2 - BC) + \theta^2(B^2 - AC) \tag{4.2}$$

Lemma 4.1.3. *Se $A\theta^2 + B\theta + C$ è un'unità inversa, allora A, B, C sono tutti non nulli.*

Dimostrazione. Sia z un'unità inversa con $N(z) = 1$, ovvero $z > 1$; allora $|\sigma_2(z)| < 1$ e in particolare $|\Re(\sigma_2(z))| < 1$. Ma $\sigma_2(A\theta^2 + B\theta + C) = A\theta^2\omega^2 + B\theta\omega + C$ e quindi, dato che $\omega^2 + \omega + 1 = 0$, vale $\Re(\sigma_2(z)) = \frac{3C-z}{2}$; otteniamo quindi la disuguaglianza $3C - z > -2$ da cui essendo $z > 1$, $3C > -1$ ed essendo $C \in \mathbb{Z}$, $C \geq 0$.
Se fosse $C = 0$, avremmo $1 = N(z) = A^3d^2 + B^3d$, da cui $d = \pm 1$ che non ci interessa. Quindi $C \geq 1$.
Vogliamo ora vedere che se $N(z) = 1$ e $z > 1$, allora $A \neq 0$ e $B \neq 0$; facciamo il cambio di variabili $X = A\theta^2, Y = B\theta, Z = C$.
Cerchiamo allora le soluzioni di $X^3 + Y^3 + Z^3 - 3XYZ = 1$ con $X + Y + Z > 1$ e $Z \geq 1$ intero.
Supponiamo per assurdo che ce ne sia una con $X = 0$ (oppure $Y = 0$, ma è completamente simmetrico). Allora abbiamo $(Y + Z)(Y^2 - YZ + Z^2) = Y^3 + Z^3 = 1$ e $Y + Z > 1$. Ma allora deve essere $Y^2 - YZ + Z^2 < 1$; riscrivendo abbiamo quindi $\frac{3}{4}Z^2 \leq \left(Y - \frac{Z}{2}\right)^2 + \frac{3}{4}Z^2 = Y^2 - YZ + Z^2 < 1$.
Quindi si deve avere $Z < \sqrt{\frac{4}{3}} < 2$ ed essendo Z intero, siamo costretti ad avere $Z = 1$. Da $Y^3 + Z^3 = 1$ si ricava allora facilmente $Y = 0$, cioè l'unità è banalmente 1, che non ha norma > 1, quindi assurdo. □

Osservazione. Con disuguaglianze più raffinate si può in realtà ottenere che i coefficienti di un'unità inversa sono in realtà positivi, e non solo non nulli.

Lemma 4.1.4. *Nessuna potenza positiva > 1 di un'unità del tipo $B\theta + C$ oppure $A\theta^2 + C$ può essere binomiale.*

Dimostrazione. Trattiamo prima il caso $|d| = 2$. È sufficiente vedere che l'equazione $x^3 + 2y^3 = 1$ ha come uniche soluzioni $(1, 0)$ e $(-1, 1)$; ma questo è esattamente l'esempio 3.2.2.
Se invece $|d| > 2$, facciamo separatamente i casi $B\theta + C$ e $A\theta^2 + C$.

- Caso $(B\theta + C)^m$

  Poniamo $E = (B\theta)^3 = B^3 d$; dato $B\theta + C$ che è un'unità, vale $B^3 d + C^3 = \pm 1$, ovvero $(E, C) = 1$, ed inoltre $|C| > 1$ per $|d| > 2$.

  Espandiamo la potenza $(B\theta + C)^m = \sum_{i=0}^{m} \binom{m}{i} (B\theta)^i C^{m-i}$; dato che vogliamo solo i θ^2, siamo interessati agli $i = 3j + 2$, ovvero il coefficiente di θ^2 è

  $$B^2 \sum_{j=0}^{\lfloor \frac{m-2}{3} \rfloor} \binom{m}{3j+2} (B\theta)^{3j} C^{m-3j-2} \tag{4.3}$$

  Dividiamo ora in tre casi, a seconda di m mod 3, in modo da riscrivere meglio la formula precedente.

  - $m = 3k + 2$
    Allora la (4.3) diventa $\sum_{j=0}^{k} \binom{m}{3j+2} E^j (C^3)^{k-j}$. Osserviamo che per tutti i termini $j \neq k$, ogni addendo è divisibile per C^3, mentre il termine con $j = k$ è esattamente E^k, che è coprimo con C: allora la somma non può fare 0.

  - $m = 3k + 1$
    Vogliamo risolvere $0 = \sum_{j=0}^{k-1} \binom{3k+1}{3j+2} E^j (C^3)^{k-j}$; facendo il cambio di variabile $j \to k - 1 - j$ e dividendo per C^3 otteniamo $0 = \sum_{j=0}^{k-1} \binom{3k+1}{3j+2} E^{k-1-j} (C^3)^j$. Osserviamo che $\binom{3k+1}{3j+2} = \binom{3k+1}{2} \cdot \binom{3k-1}{3j} \cdot \frac{2}{(3j+2)(3j+1)}$. Se sostituiamo nella sommatoria e dividiamo per le costanti abbiamo $0 = \sum_{j=0}^{k-1} \binom{3k-1}{3j} E^{k-1-j} (C^3)^j \frac{2}{(3j+2)(3j+1)}$
    Il termine in $j = 0$ è E^{k-1}, mentre tutti gli altri addendi sono multipli di qualche primo p tale che $p \mid C$: infatti il binomiale è intero, e $\upsilon_p\left(C^{3j}\right) + \upsilon_p(2) > \upsilon_p\left((3j+2)(3j+1)\right)$. Abbiamo infatti $LHS \geq 3j > \log_2(3j+2) \geq RHS$ che è vera per $j \geq 1$.
    Quindi la somma non può essere 0 perché tutti gli addendi tranne uno sono multipli di p.

  - $m = 3k$
    Vogliamo risolvere $\sum_{j=0}^{k-1} \binom{3k}{3j+2} E^j (C^3)^{k-1-j} = 0$.
    Come sopra scriviamo $\binom{3k}{3j+2} = \frac{3k}{3k-3j-2} \binom{3k-1}{3j+2}$ e dividiamo per $3k$: otteniamo $\sum_{j=0}^{k-1} \binom{3k-1}{3j+2} \frac{1}{3k-3j-2} E^j (C^3)^{k-1-j} = 0$.
    Consideriamo come prima p un primo tale che $p \mid C$; dato che vale $\upsilon_p\left(C^{3(k-1-j)}\right) > \upsilon_p(3k - 3j - 2)$ per $j < k - 1$, otteniamo che p divide tutti i termini della sommatoria tranne quello in $j = k - 1$ che è E^{k-1}.

- Caso $(A\theta^2 + C)^m$
  Allora vale $A^3 d^2 + C^3 = \pm 1$; poniamo $E = (A\theta^2)^3 = A^3 d^2$ e osserviamo

che come nel caso precedente $(E, C) = 1$ e $|C| > 1$. Espandiamo con il binomio di Newton e otteniamo che il coefficiente di θ^2 è

$$A \sum_{j=0}^{\lfloor \frac{m-1}{3} \rfloor} \binom{m}{3j+1} E^j C^{m-3j-1}$$

- $m = 3k + 2$
  Dopo aver semplificato, otteniamo $0 = \sum_{j=0}^{k} \binom{3k+2}{3j+1} E^j (C^3)^{k-j}$. Come nei casi precedenti, riscriviamo $\binom{3k+2}{3j+1} = \binom{3k+2}{3(k-j)+1} = \frac{3k+2}{3(k-j)+1}\binom{3k+1}{3(k-j)}$ e sostituendo nella sommatoria precedente si ha $0 = \sum_{j=0}^{k} \binom{3k+1}{3(k-j)} \frac{1}{3(k-j)+1} E^j (C^3)^{k-j}$. Di nuovo, il termine in $j = k$ è E^k, mentre tutti i rimanenti termini sono divisibili per uno stesso primo $p \mid C$; quindi non ci sono soluzioni.

- $m = 3k + 1$
  L'equazione da risolvere è $\sum_{j=0}^{k} \binom{3k+1}{3j+1} E^j (C^3)^{k-j} = 0$, ma in questa somma tutti i termini tranne $j = k$ sono multipli di C, il che è impossibile.

- $m = 3k$
  Riscrivendo otteniamo che a meno di costanti il coefficiente è $\sum_{j=0}^{k-1} \binom{3k}{3j+1} E^j (C^3)^{k-j-1}$. Espandiamo come sopra i binomiali $\binom{3k}{3j+1} = \binom{3k}{3(k-j-1)+2} = \frac{(3k)(3k-1)}{(3(k-j-1)+2)(3(k-j-1)+1)}\binom{3k-2}{3(k-j-1)}$.
  Dividendo per il numeratore otteniamo dunque l'equazione $0 = \sum_{j=0}^{k-1} \frac{1}{(3(k-j-1)+2)(3(k-j-1)+1)}\binom{3k-2}{3(k-j-1)} E^j (C^3)^{k-j-1}$ il cui termine in $j = k - 1$ è $E^{k-1}/2$, mentre tutti termini con $j < k - 1$ sono multipli di un primo $p \mid C$ (vedi caso $(B\theta + C)^{3k+1}$); perciò non esistono soluzioni neanche in questo sottocaso.

□

Lemma 4.1.5. *Il quadrato di un'unità irrazionale non è binomiale.*

Dimostrazione. Sia $z = M\theta^2 + P\theta + Q$ un'unità con M, P, non entrambi nulli e supponiamo per assurdo che $z^2 = B\theta + C$. Si ha allora il sistema di due equazioni:

$$M^3 d^2 + P^3 d + Q^3 - 3dMPQ = 1 \tag{4.4}$$

$$P^2 + 2MQ = 0 \tag{4.5}$$

Osserviamo che $(M, Q) = 1$: se δ è un fattore comune, allora anche $\delta \mid P$ e sostituendo nella prima si ha $\delta \mid 1$.

Quindi dalla (4.5) vale una delle seguenti, con $P = \pm 2\alpha\gamma$:

$$\begin{aligned} M &= -2\alpha^2 & Q &= \gamma^2 \\ M &= 2\alpha^2 & Q &= -\gamma^2 \\ M &= -\alpha^2 & Q &= 2\gamma^2 \\ M &= \alpha^2 & Q &= -2\gamma^2 \end{aligned}$$

e sostituendo nella (4.4) otteniamo rispettivamente

$$-8\alpha^6 d^2 \pm 20d\alpha^3\gamma^3 + \gamma^6 = 1 \tag{4.6}$$

$$8\alpha^6 d^2 \pm 20d\alpha^3\gamma^3 - \gamma^6 = 1 \tag{4.7}$$

$$-\alpha^6 d^2 \pm 20d\alpha^3\gamma^3 + 8\gamma^6 = 1 \tag{4.8}$$

$$\alpha^6 d^2 \pm 20d\alpha^3\gamma^3 - 8\gamma^6 = 1 \tag{4.9}$$

Tuttavia nessuna di queste ha soluzioni, per vari motivi:

- la (4.6) si può riscrivere come equazione di secondo grado in $t = \alpha^3 d$: $-8t^2 \pm 20t\gamma^3 + \gamma^6 - 1 = 0$; il discriminante è $\Delta/4 = 100\gamma^6 + 8\gamma^6 - 8 = 4 \cdot ((3\gamma^2)^3 - 2)$. Affinché la 4.6 abbia soluzioni intere, serve che $(3\gamma^2)^3 - 2$ sia un quadrato perfetto; dobbiamo cioè risolvere l'equazione di Mordell $\mu^3 - 2 = \nu^2$.
  Fattorizzando in $\mathbb{Z}[\sqrt{-2}]$, che è un UFD, otteniamo $\mu^3 = (\nu + \sqrt{-2}) \cdot (\nu - \sqrt{-2})$. Osserviamo che μ, ν sono dispari, quindi $\gcd(\nu + \sqrt{-2}, \nu - \sqrt{-2}) = 1$ e allora per fattorizzazione unica deve valere $\nu + \sqrt{-2} = (a + b\sqrt{-2})^3$ (le uniche unità sono ± 1, che posso assorbire in un cubo). Uguagliando allora le parti immaginarie si ottiene $1 = b(3a^2 - 2b^2)$, che ha come uniche soluzioni $a = \pm 1, b = 1$, che porta a $(\mu, \nu) = (3, \pm 5)$. Da $\mu = 3$ ricaviamo $\gamma = 1$ e quindi $\alpha^3 d = t = 0$. Questo implica $M = P = 0$, cosa che avevamo supposto non accadere.

- la (4.7) e la (4.8) ridotte modulo 4 sono della forma $t^2 \equiv -1 \pmod 4$, che è impossibile.

- nella (4.9) si fa la sostituzione $u = \alpha^3 d \pm 10\gamma^3$ e si riscrive come $u^2 - 4 \cdot (3\gamma^2)^3 = 1$ con u dispari, ovvero $\frac{u-1}{2}\frac{u+1}{2} = (3\gamma^2)^3$; questo implica che $\frac{u \pm 1}{2}$ sono due cubi consecutivi, e l'unica possibilità è $u = 1, \gamma = 0$, da cui si ottiene $P = Q = 0$, impossibile.

□

Lemma 4.1.6. *Il cubo di un'unità irrazionale non è binomiale*

Dimostrazione. Sia $M\theta^2 + P\theta + Q$ un'unità con M, P non entrambi nulli e tale che il suo cubo abbia coefficiente di θ^2 nullo. Abbiamo allora il seguente sistema

$$M^3 d^2 + P^3 d + Q^3 - 3dMPQ = 1 \tag{4.10}$$

$$MQ^2 + P^2 Q + dM^2 P = 0 \tag{4.11}$$

Sia $\delta = (M, P)$; dalla 4.10 ricaviamo $(Q, d) = (Q, \delta) = 1$.
Dalla 4.11 otteniamo $\delta^2 \mid M$; scriviamo allora

$$M = \delta^2 m, P = \delta p, \quad \text{con } (m, p) = 1$$

e sostituiamo ottenendo $mQ^2 + p^2 Q + d\delta^3 m^2 p = 0$.
Dato che $(m, p) = 1$ ricaviamo che $m^2 \mid Q$, e quindi scriviamo $Q = m^2 q$; sostituendo si ha $q(p^2 + m^3 q) = -d\delta^3 p$, da cui $q \mid p$ poiché $(q, d) = (q, \delta) = 1$ e dunque $p = qs$.
Sostituendo ancora otteniamo $q^2 s^2 + m^3 q = -d\delta^3 s$, da cui ancora $q \mid s$ ovvero $s = qe$; infine otteniamo $q^3 e^2 + m^3 = -d\delta^3 e$ e dato che $(e, m) = 1$ possiamo dire $e = \pm 1$, cioè ricapitolando

$$M = \delta^2 m, \quad P = \pm \delta q^2, \quad Q = m^2 q, \quad \delta^3 d = \mp (q^3 + m^3) \tag{4.12}$$

Sostituendo nella 4.10 otteniamo

$$\delta^6 m^3 d^2 \pm \delta^3 q^6 d + m^6 q^3 \mp 3 d m^3 \delta^3 q^3 = 1 \tag{4.13}$$

$$m^3 (q^3 + m^3)^2 - q^6 (q^3 + m^3) + m^6 q^3 + 3 m^3 q^3 (m^3 + q^3) = 1 \tag{4.14}$$

Espandendo e facendo il cambio di variabili $m^2 q = \lambda, m^3 - q^3 = \mu$ si ottiene l'equazione

$$9\lambda^3 + \mu^3 = 1$$

Questa diofantea può essere risolta grazie ai lemmi precedenti: infatti con la disuguaglianza di Artin possiamo dire che $\varepsilon_0 = \sqrt[3]{9} - 2$ è l'unità fondamentale diretta (vedere esempio 1.4.8) e grazie al lemma 4.1.4 sappiamo che nessuna potenza positiva di ε_0 è ancora binomiale, mentre grazie al lemma 4.1.3 si escludono anche le potenze negative.
Perciò le uniche soluzioni sono $(\lambda, \mu) = (0, 1), (1, -2)$.
La soluzione con $\lambda = 0$ implica una tra $M = Q = 0$ e $P = Q = 0$, che sono escluse perché implicano $d = 1$.
La soluzione con $m^3 - q^3 = \mu = -2$ implica $m = -1, q = 1$ da cui $\delta = 0$ ovvero $M = P = 0$, anche questa esclusa. □

Ora abbiamo tutti gli strumenti per

Dimostrazione del teorema di Delone. Sia $\varepsilon_0 = A\theta^2 + B\theta + C$ l'unità fondamentale di $\mathbb{Z}[\theta]$. Vogliamo cercare degli m per cui $\varepsilon_0^m = P\theta + Q$.
Per il lemma 4.1.3, dobbiamo cercare tra gli $m > 0$.
Osserviamo che ε_0 è irrazionale; allora per il lemma 4.1.5 cerchiamo gli m dispari, mentre per il lemma 4.1.6 cerchiamo solo gli $m = 3k + 1, 3k + 2$.

Usando il filtro delle radici dell'unità abbiamo

$$0 = (A\theta^2 + B\theta + C)^m + \omega(A\theta^2\omega^2 + B\theta\omega + C)^m + \omega^2(A\theta^2\omega + B\theta\omega^2 + C)^m$$

- Caso $m = 3k + 2$
  Allora $\omega = \omega^4 = (\omega^2)^{3k+2}$ e quindi vale $-(A\theta^2 + B\theta + C)^m = (A\theta^2\omega + B\theta + C\omega^2)^m + (A\theta^2\omega^2 + B\theta + C\omega)^m$.
  Dato che m è dispari, abbiamo che $(A\theta^2\omega + B\theta + C\omega^2) + (A\theta^2\omega^2 + B\theta + C\omega) \mid (A\theta^2\omega + B\theta + C\omega^2)^m + (A\theta^2\omega^2 + B\theta + C\omega)^m$, ovvero $-A\theta^2 + 2B\theta - C$ è ancora un'unità; prendendone allora la norma si ottiene $-A^3d^2 + 8B^3d - C^3 - 6dABC = \pm 1$. Vale inoltre $1 = \mathrm{N}(\varepsilon_0) = A^3d^2 + B^3d + C^3 - 3dABC$ per la (4.1) e sommando questa all'equazione precedente otteniamo $9B^3d - 9dABC = 0$ (non può essere 2 perché LHS è multiplo di 3) cioè $B(B^2 - AC) = 0$. Ma $B^2 - AC$ è un coefficiente di ε_0^{-1} come si vede dalla (4.2), quindi è non nullo per il lemma 4.1.3; perciò si ha $B = 0$ e allora per il lemma 4.1.4 nessuna potenza di ε_0 può essere binomiale.

- Caso $m = 3k + 1$
  Come sopra, scopriamo che $2A\theta^2 - B\theta - C$ è un'unità, quindi vale $8A^3d^2 - B^3d - C^3 - 6dABC = \pm 1$; sommando quest'ultima a $A^3d^2 + B^3d + C^3 - 3dABC = 1$ abbiamo $9A^3d^2 - 9dABC = 0$, ovvero $A(A^2d - BC) = 0$. Dato che $A^2d - BC$ è ancora un coefficiente di ε_0^{-1}, abbiamo $A = 0$, quindi ε_0 è binomiale ed è una soluzione; di nuovo per il lemma 4.1.4 l'unico m possibile è 1.

□

4.2 Osservazioni finali

Il teorema di Delone ci permette di dire che la soluzione non banale di $x^3 + dy^3 = 1$ è l'unità fondamentale di $\mathbb{Z}[\sqrt[3]{d}]$. In generale, detto $K = \mathbb{Q}(\sqrt[3]{d})$, si ha che $\mathbb{Z}[\sqrt[3]{d}]^\times$ è un sottogruppo di $\mathcal{O}_K^\times$, quindi non è detto che i generatori coincidano.
Tuttavia vale il seguente, dimostrato in [Nag25]

Teorema 4.2.1. *Se (x, y) è una soluzione non banale di $x^3 + dy^3 = 1$, allora $x + y\sqrt[3]{d}$ è l'unità fondamentale di $\mathcal{O}_K$, oppure il suo quadrato nei casi $d = 19, 20, 28$.*

Verifichiamo allora cosa succede con $d = 20$; chiamiamo $\theta = \sqrt[3]{20}$.
Si vede con la disuguaglianza di Artin che $u = 1 + \theta - \theta^2/2 < 1$ è l'unità fondamentale di $\mathcal{O}_{\mathbb{Q}(\theta)}$.
Tuttavia vale $u^2 = 7\theta - 19$, che è un generatore di $\mathbb{Z}[\theta]^\times$. Inoltre $(-19, 7)$ è l'unica soluzione non banale dell'equazione $x^3 + 20y^3 = 1$.

Grazie a questi teoremi è inoltre relativamente facile trovare la soluzione non banale, o verificare che non esiste.

d	(x, y)
2	$(-1, 1)$
7	$(2, -1)$
9	$(-2, 1)$
17	$(18, -7)$
19	$(-8, 3)$
20	$(-19, 7)$
26	$(3, -1)$
28	$(-3, 1)$
37	$(10, -3)$
43	$(-7, 2)$
63	$(4, -1)$
65	$(-4, 1)$
91	$(9, -2)$

Tabella 4.1: $2 \leq d \leq 100$

d	(x, y)
124	$(5, -1)$
126	$(-5, 1)$
182	$(-17, 3)$
215	$(6, -1)$
217	$(-6, 1)$
254	$(19, -3)$
342	$(7, -1)$
422	$(-15, 2)$
511	$(8, -1)$
614	$(17, -2)$
635	$(361, -42)$
651	$(-26, 3)$
730	$(-9, 1)$
813	$(28, -3)$

Tabella 4.2: $100 \leq d \leq 1000$

Per completezza, concludiamo la tesi con un elenco di tutti e soli i valori di $1 < d < 1000$ liberi da cubi per i quali la soluzione esiste.

Ringraziamenti

Ringrazio di cuore tutte le persone con cui ho condiviso alcuni momenti di questi ultimi tre anni; dato che siete tantissimi, sappiate che anche se non siete nominati esplicitamente voglio comunque dirvi grazie.
Il ringraziamento maggiore va alla mia famiglia, a mia sorella Federica, a nonni, zii e cugini; ma in particolare ai miei genitori, che mi hanno sempre seguito e supportato in questi 22 anni. Grazie davvero di tutto.
Desidero poi ringraziare tutti gli insegnanti che ho avuto nel tempo, per avermi anche trasmesso curiosità e passione.
Un ringraziamento speciale al mondo delle Olimpiadi di Matematica, a tutti i professori e ragazzi che si impegnano per renderlo così fantastico; grazie per avermi fatto scoprire già al liceo cosa volesse dire "far matematica". Grazie a tutti quelli che ho conosciuto agli stage, a Ballo, Alberto, Nikita, Dario, Giona, Luca e molti altri.
Un ulteriore enorme grazie al mio relatore Davide, senza il quale questa tesi non esisterebbe; grazie per tutti gli insegnamenti, la disponibilità e la cordialità.
Ringrazio poi tutti gli amici e compagni di Pisa, per aver reso lo studio più leggero con molteplici passatempi. Grazie ai miei compagni d'anno per questi tre bellissimi anni, per tutti gli esami superati insieme; grazie a Fabio, Giona, Gimmy, Igor, Caraz, Nico, Cola e Francesco per tutte le pizzate e le partite ad Age of Empires; grazie a Francesco per le camminate.
Grazie a tutti i Faediani, a Gori ed Enrico per le risate e il biliardino, a Lorenzo e Dario per le partite a LoL, a Cusu e Flavio per gli insulti collettivi ai computer che non funzionano.
Grazie ai Carducciani e al Carducci per le serate passate giocando a subotto o ai giochi da tavolo. Grazie a tutti quelli che hanno partecipato alla 24ore (un po' meno i fisici), e soprattutto ai Guardiani della Notte. Grazie al team del puzzle da 32000 pezzi, è davvero bellissimo. Un grazie speciale a Tess, perché rientra in tutte le categorie precedenti ed è sempre disponibile a spiegare argomenti poco chiari.

Un altro grandissimo ringraziamento va agli amici volpianesi, che mi fanno sentire a casa ogni volta che torno al Nord. Grazie a Davide, Noe, Marty, Benny, Vezze, Fede, David, Lorenzo e Roby; grazie per le innumerevoli avventure vissute insieme, per tutte le vacanze e perché ci siete sempre.
Infine ringrazio alcune persone che probabilmente non leggeranno mai questi ringraziamenti: Carl Barks e Don Rosa, per i loro splendidi paperi; Linus Torvalds per il kernel del sistema operativo più bello del mondo; Netflix, per tutto il tempo perso guardando serie TV; George Lucas, J. R. R. Tolkien e G. R. R. Martin per i meravigliosi universi che hanno creato.

Bibliografia

[Coh07] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[Del30] Boris Delone. Bemerkung über die Abhandlung von Herrn Trygve Nagell: "Darstellung ganzer Zahlen durch binäre kubische Formen mit negativen Diskriminanten". *Math. Z.*, 31(1):27–28, 1930.

[Der07] Harm Derksen. A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Invent. Math.*, 168(1):175–224, 2007.

[DF64] B. N. Delone and D. K. Faddeev. *The theory of irrationalities of the third degree*. Translations of Mathematical Monographs, Vol. 10. American Mathematical Society, Providence, R.I., 1964.

[FT93] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[Han85] G. Hansel. A simple proof of the Skolem-Mahler-Lech theorem. In *Automata, languages and programming (Nafplion, 1985)*, volume 194 of *Lecture Notes in Comput. Sci.*, pages 244–249. Springer, Berlin, 1985.

[Lec53] C. Lech. A note on recurring series. *Arkiv för Matematik*, 2:417–421, August 1953.

[Mar77] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York-Heidelberg, 1977. Universitext.

[Nag25] Trygve Nagell. Solution complète de quelques équations cubiques à deux indeterminées. *Journal de Mathématiques Pures et Appliquées*, 4:209–270, 1925.

[Sko52] Th. Skolem. Application of 3-adic analysis and "cofields" to the proof of some theorems concerning certain cubic equations. *Norsk Mat. Tidsskr.*, 34:45–51, 1952.