Algebra Computazionale B

basato sull'omonimo corso
tenuto dal prof. Carlo Traverso

Anno Accademico 2012/13 - I semestre

Oscar Papini

Indice

Prefazione **vii**

Simboli e notazioni utilizzati **ix**

1 Reticoli **1**

1.1 Classificazione dei reticoli 1
1.2 Parallelepipedo fondamentale e volume 5
1.3 Minimi successivi 6
1.4 Basi ridotte e algoritmo di Gauss 9
1.5 L'algoritmo LLL 14
1.6 Usare LLL per il Closest Vector Problem 16
1.7 Un'applicazione crittografica: NTRU 17
1.8 Fattorizzare polinomi a coefficienti razionali 19
1.9 Il protocollo Goldreich-Goldwasser-Halevi (GGH) 22
1.10 Reticoli e ideali binomiali 23
1.11 Lattice Polly Cracker 24

2 Curve ellittiche **29**

2.1 Definizione e prime proprietà 29
2.2 Legge di gruppo 32
2.3 Una prima applicazione: la fattorizzazione 34
2.4 Endomorfismi di curve ellittiche 35
2.5 Punti di torsione 42
2.6 Curve ellittiche su campi finiti 49
2.7 Curve ellittiche su $\mathbb{C}$ 56
2.8 Divisori 74
2.9 Applicazioni delle curve ellittiche 85

3 Topologia delle curve e delle superfici **91**
3.1 La forma delle curve algebriche reali 92
3.2 Superfici algebriche reali orientabili 97

4 Geometria algebrica reale **113**
4.1 Contare le radici reali I: il metodo di Sturm 113
4.2 Il Teorema di Tarski-Seidenberg 118
4.3 Contare le radici reali II: il metodo di Hermite 122
4.4 Contare le radici reali III: coefficienti sottorisultanti principali . . . 128
4.5 Insiemi semialgebrici 130
4.6 Funzioni semialgebriche 134
4.7 *Cylindrical Algebraic Decomposition* 135

Bibliografia **141**

Indice degli algoritmi

Algoritmo di Gauss 11
Algoritmo δLLL 15
Test Fattore 20
Trova Fattore 21
Fattorizzazione LLL 21
Algoritmo di Schoof 55

Prefazione

Questo testo è basato sul corso di *Algebra Computazionale B* tenuto dal prof. Carlo Traverso durante il primo semestre dell'anno accademico 2012/2013. Esso ripercorre quanto svolto durante il corso, seguendo la traccia degli appunti presi in classe.

Tuttavia, è spesso impossibile approfondire gli argomenti in classe come si vorrebbe; pertanto ho integrato gli appunti con passaggi attinti dalle fonti riportate in bibliografia. In particolare, i testi consigliati sono:

Reticoli: Daniele Micciancio e Shafi Goldwasser. *Complexity of Lattice Problems: a Cryptographic Perspective*. Kluwer Academic Publishers.

Curve ellittiche: Lawrence C. Washinghton. *Elliptic Curves: Number Theory and Cryptography.* Chapman & Hall/CRC.

Topologia delle curve e delle superfici: Elisabetta Fortuna, Patrizia Gianni, Paola Parenti, e Carlo Traverso. Algorithms to Compute the Topology of Orientable Real Algebraic Surfaces. *J. Symb. Comput.*, 36:343–364, 2003.

Geometria algebrica reale: Michel Coste. An Introduction to Semialgebraic Geometry. Dip. Mat. Univ. Pisa, Dottorato di Ricerca in Matematica, 2000.

Mi assumo ogni responsabilità per gli eventuali errori presenti nel testo: invito chiunque ne trovi, sia di natura concettuale che ortografica, a segnalarmeli.

Oscar Papini
papini@mail.dm.unipi.it

Ultima revisione: 28 aprile 2014

Simboli e notazioni utilizzati

$\mathbb{K}, \mathbb{F}_q$	Campo, campo finito con q elementi
$\mathbb{A}^n(\mathbb{K}), \mathbb{P}^n(\mathbb{K})$	Spazio affine, proiettivo n-dimensionale su $\mathbb{K}$
$\mathcal{M}_{m\times n}(R)$	Spazio delle matrici $m \times n$ a coefficienti in R
$\det(A)$, $\mathrm{tr}(A)$	Determinante, traccia di A
A^T	Trasposta di A
$\sigma(A)$	Se A è una matrice simmetrica, segnatura di A
$r(A)$	Rango di A
$\mathrm{diag}(\lambda_1, \ldots, \lambda_m)$	Matrice diagonale i cui elementi sulla diagonale sono $\lambda_1, \ldots, \lambda_m$
$\mathcal{SA}_n$	Classe degli insiemi semialgebrici di $\mathbb{R}^n$
$\mathcal{V}_{\mathbb{L}}(\mathcal{P})$	Luogo di zeri di $\mathcal{P}$ su $\mathbb{L}$; precisamente, se $\mathcal{P} \subseteq \mathbb{K}[X_1, \ldots, X_n]$ e $\mathbb{K} \subseteq \mathbb{L}$, è definito come $\{\mathbf{x} \in \mathbb{L}^n \mid p(\mathbf{x}) = 0 \ \forall\ p \in \mathcal{P}\}$; $\mathcal{V}(\mathcal{P}) := \mathcal{V}_{\mathbb{K}}(\mathcal{P})$
$\#V$	Cardinalità dell'insieme V
$B(\mathbf{x}, r)$	Palla (aperta) di centro $\mathbf{x}$ e raggio r
$\langle V \rangle$	Sottospazio generato da V
$\langle \mathbf{a}, \mathbf{b} \rangle$	Prodotto scalare tra $\mathbf{a}$ e $\mathbf{b}$
$\mathrm{vol}(S)$	Volume di S
$\lfloor x \rfloor$, $\lceil x \rceil$	Parte intera di x, intero successivo ad x
$\lfloor x \rceil$	Arrotondamento all'intero più vicino ad x (definito come $\lfloor x + 0.5 \rfloor$)
$\mathrm{lc}(f)$, $\mathrm{lt}(f)$	Coefficiente, termine di testa (*leading coefficient, term*) di f
$\mathrm{Lt}(\mathcal{P})$	Insieme dei termini di testa dei polinomi in $\mathcal{P}$
$\mathrm{Ris}(f, g)$	Risultante di f e g
$\mathrm{ord}_w(f)$	Ordine di f in w
$\mathrm{Res}_w(f)$	Residuo di f in w

Nota. Le variabili indicate in corsivo (come x) indicano oggetti con una sola componente, quelle in grassetto (come $\mathbf{x}$) indicano oggetti con più componenti, come vettori o n-uple. Incognite o valori precisi sono generalmente indicati in minuscolo, mentre le indeterminate dei polinomi sono sempre indicate in maiuscolo.

Capitolo 1

Reticoli

Questo capitolo è dedicato ai reticoli e ai principali problemi legati ad essi. Lo studio dei reticoli trova applicazione pratica in ambito crittografico (protocollo di Goldreich-Goldwasser-Halevi), oppure per la fattorizzazione di polinomi a coefficienti razionali.

Definizione 1.1. Un *reticolo* su $\mathbb{R}^n$ è un sottogruppo L di $(\mathbb{R}^n, +)$ discreto.

Per le applicazioni, i problemi di maggiore rilevanza che coinvolgono i reticoli sono principalmente due:

- *Shortest Vector Problem* (SVP): dato un reticolo L, determinare l'elemento $\boldsymbol{v} \in L$ di minima norma;
- *Closest Vector Problem* (CVP): dati un reticolo L e un vettore $\mathbf{c} \in \mathbb{R}^n$, determinare $\boldsymbol{v} \in L$ a distanza minima da $\mathbf{c}$.

È possibile dimostrare che questi problemi sono NP-completi. In realtà esistono algoritmi che girano in tempo polinomiale, ma danno solo soluzioni approssimate di tali problemi.

1.1 Classificazione dei reticoli

Un reticolo è un sottogruppo discreto nell'usuale senso topologico del termine: fissata una norma $\|\cdot\|$ su $\mathbb{R}^n$, il reticolo L è tale che per ogni $\boldsymbol{v} \in L$ esiste una palla $B(\boldsymbol{v}, r) \subseteq \mathbb{R}^n$ tale che $B(\boldsymbol{v}, r) \cap L = \{\boldsymbol{v}\}$.

Esempio 1.1. Siano $\mathbf{b}_1, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ vettori linearmente indipendenti. Allora l'insieme

$$L := \left\{ \sum_{i=1}^{k} u_i \mathbf{b}_i \;\middle|\; u_i \in \mathbb{Z} \right\}$$

è un reticolo. Il numero n è detto *dimensione* del reticolo, mentre k è il *rango*. Se $n = k$, il reticolo è detto *di rango massimo*.

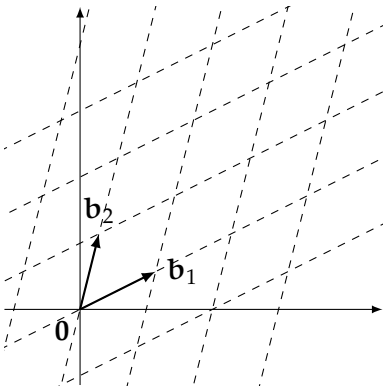


Figura 1.1: Esempio di reticolo in $\mathbb{R}^2$; i punti del reticolo sono le intersezioni delle linee tratteggiate.

Teorema 1.2. *Ogni reticolo su $\mathbb{R}^n$ è della forma presentata nell'esempio 1.1. In altre parole, se L è un reticolo su $\mathbb{R}^n$, allora esistono $\mathbf{b}_1, \dots, \mathbf{b}_k \in \mathbb{R}^n$ vettori linearmente indipendenti tali che*

$$L = \left\{ \sum_{i=1}^{k} u_i \mathbf{b}_i \;\middle|\; u_i \in \mathbb{Z} \right\}.$$

Dimostrazione. Consideriamo $\langle L \rangle$, il sottospazio generato da L (come sottospazio vettoriale di $\mathbb{R}^n$), e sia $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k)$ base per $\langle L \rangle$, con $\boldsymbol{v}_1, \dots, \boldsymbol{v}_k \in L$. Senza perdita di generalità, possiamo ricondurci a studiare L come sottoinsieme di $\mathbb{R}^k$, e quindi supponiamo già in partenza che $k = n$.

A questo punto cambiamo coordinate con un $\mathbb{R}$-isomorfismo lineare, mappando $\boldsymbol{v}_i \mapsto \boldsymbol{e}_i$ (dove con $\boldsymbol{e}_i$ è indicato l'i-esimo vettore della base canonica). In questo modo si ha $(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n) \subseteq L$, e quindi

$$\mathbb{Z}^n \subseteq L \subseteq \mathbb{R}^n.$$

Consideriamo ora l'azione $\mathbb{Z}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$ di traslazione, e il rispettivo spazio quoziente $\mathbb{R}^n/\mathbb{Z}^n$. Verifichiamo che $L/\mathbb{Z}^n$ è discreto in $\mathbb{R}^n/\mathbb{Z}^n$. Intanto notiamo che L è saturo rispetto alla proiezione al quoziente: infatti L è un sottogruppo e $\mathbb{Z}^n \subseteq L$, quindi per ogni $p \in L$ si ha $p + \mathbb{Z}^n \subseteq L$; In particolare L è invariante sotto l'azione di $\mathbb{Z}^n$. La restrizione della proiezione

$$\pi|_L : L \longrightarrow L/\mathbb{Z}^n$$

è allora un'applicazione continua, suriettiva e aperta (proiezione al quoziente per un'azione di gruppo), dunque è un'identificazione aperta. In particolare, ogni punto di $L/\mathbb{Z}^n$ è aperto (perché immagine di un punto di L, che è aperto perché L è discreto).

Verifichiamo che L è un chiuso in $\mathbb{R}^n$. Supponiamo che $\tilde{\mathbf{x}} \in \overline{L} \smallsetminus L$, e sia $(\mathbf{x}_n)_{n\in\mathbb{N}} \subseteq L$ una successione che converga a $\tilde{\mathbf{x}}$. In particolare $(\mathbf{x}_n)$ è di Cauchy, dunque per ogni $\varepsilon > 0$ esistono h, k tali che $0 < \|\mathbf{x}_h - \mathbf{x}_k\| < \varepsilon$. Ma $\mathbf{x}_h, \mathbf{x}_k \in L$, quindi $\mathbf{x}_h - \mathbf{x}_k \in L$: in altre parole, per ogni $\varepsilon > 0$ esiste $\mathbf{y} \in L \smallsetminus \{\mathbf{0}\}$ tale che $\|\mathbf{y}\| < \varepsilon$, contro la discretezza di L.

Quindi $L/\mathbb{Z}^n$ è chiuso e discreto in $\mathbb{R}^n/\mathbb{Z}^n$, che è compatto (è un toro n-dimensionale). Ne segue che $L/\mathbb{Z}^n$ è un insieme finito. È facile convincersi che i punti in questo quoziente devono avere coordinate razionali (altrimenti, le loro combinazioni lineari a coefficienti in $\mathbb{Z}$ genererebbero un denso nel toro). Possiamo dunque scegliere un rappresentante per ciascuna classe di equivalenza a coordinate razionali. Detto d il massimo comune divisore dei denominatori che compaiono in tutte queste coordinate (che sono in numero finito), abbiamo che

$$\mathbb{Z}^n \subseteq L \subseteq \left(\frac{1}{d}\mathbb{Z}\right)^n \simeq \mathbb{Z}^n$$

e quindi $L \simeq \mathbb{Z}^n$. In particolare, se $\varphi : \mathbb{Z}^n \xrightarrow{\sim} L$ è un isomorfismo, allora L è dato dalle combinazioni $\mathbb{Z}$-lineari di $\mathbf{b}_i := \varphi(\mathbf{e}_i)$. □

Chiameremo dunque *base* di un reticolo un insieme di vettori $\mathbf{b}_1, \dots, \mathbf{b}_k$ come nel teorema precedente. In questo modo possiamo associare a un reticolo una matrice[1]

$$B := \left(\begin{array}{c} \mathbf{b}_1 \\ \hline \vdots \\ \hline \mathbf{b}_k \end{array}\right) \in \mathcal{M}_{k\times n}(\mathbb{Q})$$

in modo che

$$L = \{B\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^k\}.$$

Supponiamo ora di avere un insieme di generatori $\boldsymbol{\nu}_1, \dots, \boldsymbol{\nu}_m$ per un reticolo L (non necessariamente una base).[2] Come possiamo fare per ottenere una base

[1] Possiamo supporre che i coefficienti della matrice siano in $\mathbb{Q}$ anziché in $\mathbb{R}$, come spiegato nella dimostrazione precedente.

[2] Per quanto visto prima, possiamo supporre che siano vettori di $\mathbb{Q}^n$, anzi di $\mathbb{Z}^n$ eventualmente moltiplicando per il massimo comune divisore dei denominatori.

per L? Se

$$V := \left(\begin{array}{c} \boldsymbol{v}_1 \\ \hline \vdots \\ \hline \boldsymbol{v}_m \end{array}\right),$$

ne possiamo calcolare la *forma di Hermite*. Vogliamo cioè ridurre V a una forma a scalini, effettuando operazioni che possono essere ricondotte a moltiplicazioni a sinistra per matrici unimodulari.[3] In particolare, è possibile

- scambiare tra loro due righe;
- cambiare il segno a una riga;
- sommare a una riga un multiplo intero di un'altra.

Con queste mosse, applicando l'algoritmo di Euclide alla prima colonna, si ottiene al primo passo una matrice della forma

$$\left(\begin{array}{c|c} d_1 & * \\ \hline 0 & \\ \vdots & V^{(1)} \\ 0 & \end{array}\right)$$

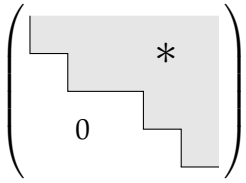
dove d_1 è il massimo comune divisore dei coefficienti della prima colonna.

A questo punto si ripete il procedimento sulla matrice $V^{(1)}$, ottenendo

$$\left(\begin{array}{c|c|c} d_1 & \sharp & * \\ \hline 0 & d_2 & * \\ \hline 0 & 0 & \\ \vdots & \vdots & V^{(2)} \\ 0 & 0 & \end{array}\right).$$

Si può fare in modo, sottraendo multipli della seconda riga, che in $(\sharp)$ ci sia un numero compreso fra 0 e $d_2 - 1$.

Alla fine si ottiene una matrice della forma



[3] Cioè invertibili a coefficienti in $\mathbb{Z}$.

dove

- il numero di righe non nulle è minore o uguale al numero delle colonne (che è la dimensione dello spazio ambiente);
- sulla colonna j-esima si ha che gli elementi prima di d_j sono tutti positivi e minori di d_j, mentre dopo d_j sono tutti nulli.

Le righe non nulle formano effettivamente una base per il reticolo L: infatti continuano a generare L (perché abbiamo applicato solo matrici unimodulari), e sono chiaramente linearmente indipendenti (perché la matrice ha una forma a scalini).

1.2 Parallelepipedo fondamentale e volume

Sia $\mathcal{B} := (\mathbf{b}_1, \ldots, \mathbf{b}_k) \subseteq \mathbb{R}^n$ una base per un reticolo L.

Definizione 1.3. Definiamo *parallelepipedo fondamentale* di L rispetto a $\mathcal{B}$ l'insieme

$$\left\{ \sum_{i=1}^{k} x_i \mathbf{b}_i \;\middle|\; 0 \leqslant x_i < 1 \right\}.$$

Definizione 1.4. Definiamo *determinante* di L, indicato con $\det(L)$, il volume k-dimensionale di un parallelepipedo fondamentale di L.

Detta M la matrice dei vettori di $\mathcal{B}$ (per righe o per colonne), se M è quadrata (cioè il reticolo è di rango massimo) si ha

$$\det(L) = |\det(M)|,$$

altrimenti

$$\det(L) = \sqrt{\det(M^T M)}.$$

È facile dunque mostrare che $\det(L)$ non dipende dalla base $\mathcal{B}$ scelta.

Esempio 1.2. Su $\mathbb{R}^2$, il reticolo generato da $\boldsymbol{e}_1 + \boldsymbol{e}_2$ ha determinante

$$\sqrt{\det\left(\begin{pmatrix} 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right)} = \sqrt{2}$$

che è proprio la lunghezza del vettore $\boldsymbol{e}_1 + \boldsymbol{e}_2$.

Un altro modo per calcolare il determinante di un reticolo è quello di ortogonalizzare (*non* normalizzare) la base $\mathcal{B}$ con Gram-Schmidt. Sia $\mathcal{B} = (\mathbf{b}_1, \dots, \mathbf{b}_k)$; poniamo

$$\begin{aligned} \mathbf{b}_1^* &= \mathbf{b}_1 \\ \mathbf{b}_i^* &= \mathbf{b}_i - \sum_{j=1}^{i-1} \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle} \mathbf{b}_j^*. \end{aligned}$$

A questo punto si ottiene

$$\det(L) = \prod_{i=1}^{k} \|\mathbf{b}_i^*\|.$$

A livello matriciale, detta M la matrice di cambiamento di base tra $\mathcal{B}$ e $\mathcal{B}^* := (\mathbf{b}_1^*, \dots, \mathbf{b}_k^*)$, si ha che M è triangolare con 1 sulla diagonale, quindi il suo determinante è 1 e questo non cambia $\det(L)$. Naturalmente $\mathcal{B}^*$ *non* è una base per L.

Notiamo infine che, anche supponendo $\mathcal{B} \subseteq \mathbb{Z}^n$, se il reticolo non è di rango massimo non è detto che il suo determinante sia intero.

1.3 Minimi successivi

In questa sezione arriveremo a un teorema che permette di stimare la minima lunghezza di un vettore non nullo di un reticolo L. Occorre prima premettere una definizione.

Definizione 1.5. Dato un reticolo L di rango k, per ogni $i = 1, \dots, k$ si definiscono *minimi successivi* i numeri

$$\lambda_i := \inf \{\rho \mid \dim \langle L \cap \overline{B}(\mathbf{0}, \rho) \rangle \geqslant i\}.$$

In altre parole, λ_i è il minimo raggio di una palla che contiene un numero i di vettori di L linearmente indipendenti.

Lemma 1.6. λ_i *in realtà è un minimo, cioè per ogni* $i = 1, \dots, k$ *esiste* $\boldsymbol{v}_i \in L$ *tale che* $\|\boldsymbol{v}_i\| = \lambda_i$.

Dimostrazione. Abbiamo visto nella dimostrazione del teorema 1.2 che L è chiuso, oltre che discreto. Quindi $L \cap \overline{B}(\mathbf{0}, \rho)$ è un insieme finito. Scegliendo come ρ, per esempio, $2\lambda_i$, segue dalla definizione di λ_i che uno dei vettori deve avere lunghezza λ_i. □

Notiamo che $\lambda_1 = \inf \{\|\boldsymbol{v}\| \mid \boldsymbol{v} \in L \setminus \{\mathbf{0}\}\}$. Dunque, il calcolo di λ_1 permette di stabilire qual è la minima lunghezza di un vettore non nullo del nostro reticolo.

Teorema 1.7. *Siano* $(\mathbf{b}_1, \ldots, \mathbf{b}_k)$ *base per un reticolo* L *e* $(\mathbf{b}_1^*, \ldots, \mathbf{b}_k^*)$ *il risultato dell'ortogonalizzazione di Gram-Schmidt. Allora*

$$\lambda_1 \geqslant \min \{\|\mathbf{b}_i^*\| \mid i = 1, \ldots, k\}.$$

Dimostrazione. Sia $\boldsymbol{v} = \sum x_i \mathbf{b}_i$, con $x_i \in \mathbb{Z}$, un elemento di $L \setminus \{\mathbf{0}\}$ e sia h il più grande indice tale che $x_h \neq 0$. Abbiamo la tesi se $\|\boldsymbol{v}\| \geqslant \|\mathbf{b}_h^*\|$. Calcoliamo il prodotto scalare di $\boldsymbol{v}$ con $\mathbf{b}_h^*$:

$$\langle \boldsymbol{v}, \mathbf{b}_h^* \rangle = \sum_{i=1}^{k} \langle x_i \mathbf{b}_i, \mathbf{b}_h^* \rangle = x_h \langle \mathbf{b}_h, \mathbf{b}_h^* \rangle = x_h \|\mathbf{b}_h^*\|^2$$

dove abbiamo usato l'ortogonalità di $\mathbf{b}_i$ e $\mathbf{b}_h^*$ per $i < h$, il fatto che $x_i = 0$ per $i > h$ e che $\langle \mathbf{b}_h, \mathbf{b}_h^* \rangle = \langle \mathbf{b}_h^*, \mathbf{b}_h^* \rangle$. D'altra parte, per la disuguaglianza di Cauchy-Schwarz

$$\|\boldsymbol{v}\| \, \|\mathbf{b}_h^*\| \geqslant |\langle \boldsymbol{v}, \mathbf{b}_h^* \rangle| = |x_h| \, \|\mathbf{b}_h^*\|^2$$

da cui, semplificando $\|\mathbf{b}_h^*\|$ e ricordando che $|x_h| \geqslant 1$, si ha

$$\|\boldsymbol{v}\| \geqslant \|\mathbf{b}_h^*\| \geqslant \min \{\|\mathbf{b}_i^*\| \mid i = 1, \ldots, k\}.$$

□

Teorema 1.8 (Blichfeldt)**.** *Siano* L *un reticolo di rango massimo, e* $S \subseteq \mathbb{R}^n$ *un insieme misurabile tale che* $\mathrm{vol}(S) > \det(L)$*. Allora esistono* $\boldsymbol{z}_1, \boldsymbol{z}_2 \in S$ *tali che* $\boldsymbol{z}_1 - \boldsymbol{z}_2 \in L$*.*

Dimostrazione. Sia $\mathcal{B}$ una base per L, e $\mathcal{P}$ il parallelepipedo fondamentale di L rispetto a $\mathcal{B}$. Definendo

$$\mathbf{x} + \mathcal{P} := \{\mathbf{x} + \mathbf{y} \mid \mathbf{y} \in \mathcal{P}\},$$

è facile vedere che $\{\mathbf{x} + \mathcal{P} \mid \mathbf{x} \in L\}$ è una partizione di $\mathbb{R}^n$. Definiamo $S_{\mathbf{x}} := S \cap (\mathbf{x} + \mathcal{P})$.

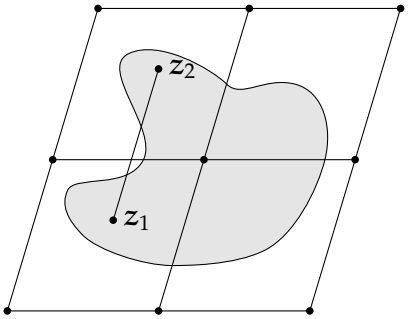


Figura 1.2: Il teorema di Blichfeldt.

Dato che $\{S_x \mid x \in L\}$ è una partizione di S, si ha

$$\mathrm{vol}(S) = \sum_{x \in L} \mathrm{vol}(S_x).$$

Trasliamo ora indietro ciascun S_x, riportandolo nel parallelepipedo fondamentale: se $\widehat{S_x} := S_x - x$, abbiamo $\widehat{S_x} \subseteq \mathcal{P}$ e $\mathrm{vol}(\widehat{S_x}) = \mathrm{vol}(S_x)$.

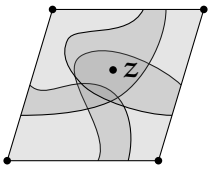


Figura 1.3: I pezzi S_x riportati in $\mathcal{P}$.

Ma ora

$$\sum_{x \in L} \mathrm{vol}(\widehat{S_x}) = \sum_{x \in L} \mathrm{vol}(S_x) = \mathrm{vol}(S) > \mathrm{vol}(\mathcal{P}),$$

dunque esistono $x, y \in L$, con $x \neq y$, tali che $\widehat{S_x} \cap \widehat{S_y} \neq \varnothing$. Sia $z \in \widehat{S_x} \cap \widehat{S_y}$; allora $z_1 := z + x$ sta in S_x (e quindi in S), $z_2 := z + y$ sta in S_y (e quindi in S), e $z_1 - z_2 = (z + x) - (z + y) = x - y \in L$, come richiesto. □

Corollario 1.9 (Teorema del corpo convesso di Minkowski)**.** *Siano* $L \subseteq \mathbb{R}^n$ *un reticolo di rango massimo, e* S *un insieme convesso, simmetrico rispetto all'origine, e tale che* $\mathrm{vol}(S) > 2^n \det(L)$*. Allora esiste* $v \neq \mathbf{0}$ *tale che* $v \in L \cap S$*.*

Dimostrazione. Dividiamo a metà (più o meno) il convesso: sia $\widetilde{S} := \{x \in \mathbb{R}^n \mid 2x \in S\}$. Si ha

$$\mathrm{vol}(\widetilde{S}) = 2^{-n} \mathrm{vol}(S) > \det(L),$$

quindi, per il teorema di Blichfeldt esistono due punti distinti $z_1, z_2 \in \widetilde{S}$ tali che $z_1 - z_2 \in L$. È sufficiente mostrare che $z_1 - z_2 \in S$: per definizione, abbiamo $2z_1, 2z_2 \in S$, e anche $-2z_2$ perché S è simmetrico rispetto all'origine; per convessità

$$\frac{2z_1 + (-2z_2)}{2} = z_1 - z_2 \in S$$

e questo conclude. □

Applicando il corollario 1.9 a $B(\mathbf{0}, \sqrt{n} \det(L)^{1/n})$, che ha volume maggiore di $2^n \det(L)$ perché contiene un ipercubo n-dimensionale di lato $2 \det(L)^{1/n}$, si ottiene che esiste $v \in L$ non nullo tale che $\|v\| < \sqrt{n} \det(L)^{1/n}$, e quindi

$$\lambda_1 < \sqrt{n} \det(L)^{1/n}.$$

Il risultato precedente è chiamato anche *primo teorema di Minkowski*. Il *secondo teorema di Minkowski* afferma che una stima analoga vale per la media geometrica dei minimi successivi, cioè

$$\left(\prod_{i=1}^{n} \lambda_i\right)^{1/n} < \sqrt{n}\det(L)^{1/n}.$$

1.4 Basi ridotte e algoritmo di Gauss

Se il reticolo ha rango 2, esiste un algoritmo (dovuto a Gauss) che calcola esattamente il vettore più corto non nullo del reticolo rispetto a una qualunque norma, e lo fa in tempo polinomiale (sempre che il calcolo della norma sia efficiente).

Definizione 1.10. Sia L un reticolo di rango 2, e sia $\mathcal{B} := (\mathbf{a}, \mathbf{b})$ una sua base. Diciamo che la base $\mathcal{B}$ è *ridotta* se

$$\|\mathbf{a}\|, \|\mathbf{b}\| \leqslant \|\mathbf{a} + \mathbf{b}\|, \|\mathbf{a} - \mathbf{b}\|,$$

cioè se le diagonali del parallelogramma fondamentale sono lunghe almeno quanto i lati.

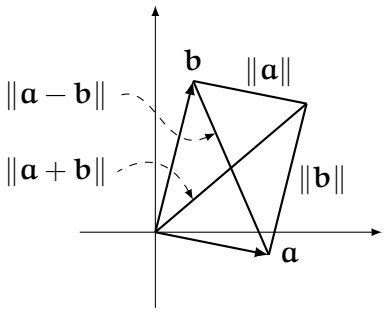


Figura 1.4: Base ridotta.

Questa definizione è giustificata dal fatto che i vettori di una base ridotta hanno effettivamente per lunghezze i minimi λ_1 e λ_2. Prima di provarlo, però, ci occorre un lemma.

Lemma 1.11. *Siano* $\mathbf{x}$, $\mathbf{x} + \mathbf{y}$ *e* $\mathbf{x} + \alpha\mathbf{y}$, *con* $\alpha \in (1, +\infty)$, *tre vettori allineati. Se* $\|\mathbf{x}\| \leqslant \|\mathbf{x} + \mathbf{y}\|$, *allora* $\|\mathbf{x} + \mathbf{y}\| \leqslant \|\mathbf{x} + \alpha\mathbf{y}\|$. *Analogamente, se* $\|\mathbf{x}\| < \|\mathbf{x} + \mathbf{y}\|$, *allora* $\|\mathbf{x} + \mathbf{y}\| < \|\mathbf{x} + \alpha\mathbf{y}\|$.

Dimostrazione. Dimostriamo solo il caso con le disuguaglianze strette, l'altro è identico sostituendo tutti i simboli di minore con simboli di minore o uguale.

Sia $\delta := \frac{1}{\alpha}$, e quindi $\delta \in (0,1)$. Si ha

$$\mathbf{x} + \mathbf{y} = (1-\delta)\mathbf{x} + \delta(\mathbf{x} + \alpha\mathbf{y})$$

da cui, per disuguaglianza triangolare

$$\|\mathbf{x} + \mathbf{y}\| < (1-\delta)\|\mathbf{x}\| + \delta\|\mathbf{x} + \alpha\mathbf{y}\|$$

Ora, per ipotesi,

$$\|\mathbf{x} + \mathbf{y}\| < (1-\delta)\|\mathbf{x} + \mathbf{y}\| + \delta\|\mathbf{x} + \alpha\mathbf{y}\|$$

da cui

$$\delta\|\mathbf{x} + \mathbf{y}\| < \delta\|\mathbf{x} + \alpha\mathbf{y}\|,$$

e quindi la tesi. □

Teorema 1.12. $(\mathbf{a}, \mathbf{b})$ *è una base ridotta per* L *se e solo se le lunghezze di* $\mathbf{a}$ *e* $\mathbf{b}$ *sono* λ_1 *e* λ_2.

Dimostrazione. Senza perdita di generalità, assumiamo $\|\mathbf{a}\| \leqslant \|\mathbf{b}\|$.
$\boxed{\Leftarrow}$ Per definizione, $\|\mathbf{a}\|$ è la lunghezza minima di un vettore nel reticolo, quindi (notando che $\mathbf{a} \pm \mathbf{b} \neq \mathbf{0}$ perché $\mathbf{a}$ e $\mathbf{b}$ sono una base)

$$\|\mathbf{a}\| \leqslant \|\mathbf{a} + \mathbf{b}\|,$$
$$\|\mathbf{a}\| \leqslant \|\mathbf{a} - \mathbf{b}\|.$$

Inoltre, $\mathbf{a} + \mathbf{b}$ e $\mathbf{a} - \mathbf{b}$ sono linearmente indipendenti da $\mathbf{a}$ (sempre perché $\mathbf{a}$ e $\mathbf{b}$ sono una base), quindi per definizione di λ_2

$$\lambda_2 \leqslant \max\{\|\mathbf{a}\|, \|\mathbf{a} + \mathbf{b}\|\} = \|\mathbf{a} + \mathbf{b}\|,$$
$$\lambda_2 \leqslant \max\{\|\mathbf{a}\|, \|\mathbf{a} - \mathbf{b}\|\} = \|\mathbf{a} - \mathbf{b}\|.$$

Da cui

$$\|\mathbf{a}\|, \|\mathbf{b}\| \leqslant \lambda_2 \leqslant \|\mathbf{a} + \mathbf{b}\|, \|\mathbf{a} - \mathbf{b}\|.$$

$\boxed{\Rightarrow}$ Siano $r, s \in \mathbb{Z}$, e consideriamo un generico vettore $r\mathbf{a} + s\mathbf{b} \in$ L. Mostreremo che

$$\|\mathbf{a}\| \leqslant \|r\mathbf{a} + s\mathbf{b}\| \qquad \forall (r,s) \neq (0,0), \tag{1.1a}$$
$$\|\mathbf{b}\| \leqslant \|r\mathbf{a} + s\mathbf{b}\| \qquad \forall s \neq 0. \tag{1.1b}$$

Infatti, in tal caso, si ha che $\mathbf{a}$ è il vettore non nullo di L più corto, quindi $\|\mathbf{a}\| = \lambda_1$, mentre $\mathbf{b}$ è il vettore più corto tra i vettori di L linearmente indipendenti da $\mathbf{a}$ e quindi $\|\mathbf{b}\| = \lambda_2$. Per dimostrare le relazioni precedenti, distinguiamo tre casi.

- Se $s = 0$, allora dobbiamo verificare (1.1a) per $r \neq 0$; ma $\|\mathbf{a}\| \leqslant \|r\mathbf{a}\| = \|r\mathbf{a} + s\mathbf{b}\|$ e questo prova (1.1a).
- Se $r = 0$, supponiamo $s \neq 0$; si ha $\|\mathbf{a}\| \leqslant \|\mathbf{b}\| \leqslant \|s\mathbf{b}\| = \|r\mathbf{a} + s\mathbf{b}\|$ e questo prova sia (1.1a) che (1.1b).
- Infine, se $(r, s) \neq (0, 0)$, supponiamo $r \geqslant s > 0$ (gli altri casi sono analoghi). Si ha $s \geqslant 1$, e quindi

$$\left\|\frac{r}{s}\mathbf{a} + \mathbf{b}\right\| = \left\|\frac{r\mathbf{a} + s\mathbf{b}}{s}\right\| \leqslant \|r\mathbf{a} + s\mathbf{b}\|.$$

  Applicando il lemma 1.11 ai vettori $\mathbf{b}$, $\mathbf{b} + \mathbf{a}$ e $\mathbf{b} + \frac{r}{s}\mathbf{a}$ si ottiene

$$\|\mathbf{a}\|, \|\mathbf{b}\| \leqslant \|\mathbf{a} + \mathbf{b}\| \leqslant \left\|\frac{r}{s}\mathbf{a} + \mathbf{b}\right\| \leqslant \|r\mathbf{a} + s\mathbf{b}\|$$

  che dimostra sia (1.1a) che (1.1b).

Questo conclude la dimostrazione. □

Data una base qualunque del reticolo, vorremmo un algoritmo che permetta di ricavare una base ridotta.

Definizione 1.13. Una base $(\mathbf{a}, \mathbf{b})$ è *ben ordinata* se $\|\mathbf{a}\| \leqslant \|\mathbf{a} - \mathbf{b}\| < \|\mathbf{b}\|$.

L'idea di base per l'algoritmo è la seguente: intanto viene ben ordinata la base data in input, dopodiché si itera riducendo progressivamente la base (e ottenendo sempre basi ben ordinate) finché non si arriva a una base ridotta. Il procedimento è simile all'algoritmo euclideo, generalizzato in due dimensioni.

Algoritmo ALGORITMO DI GAUSS

Input: $(\mathbf{a}, \mathbf{b})$ base per L

1: **if** $\|\mathbf{a}\| > \|\mathbf{b}\|$ **then**
2: Scambia $\mathbf{a}$ e $\mathbf{b}$
3: **end if**
4: **if** $\|\mathbf{a} - \mathbf{b}\| > \|\mathbf{a} + \mathbf{b}\|$ **then**
5: $\mathbf{b} := -\mathbf{b}$
6: **end if**
7: **if** $\|\mathbf{b}\| \leqslant \|\mathbf{a} - \mathbf{b}\|$ **then**
8: **return** $(\mathbf{a}, \mathbf{b})$
9: **end if**

▷ *Continua a pagina seguente*

▷ *Continua da pagina precedente*

10: **if** $\|\mathbf{a}\| \leqslant \|\mathbf{a} - \mathbf{b}\|$ **then**
11: **go to** 17
12: **end if**
13: **if** $\|\mathbf{a}\| = \|\mathbf{b}\|$ **then**
14: **return** $(\mathbf{a}, \mathbf{a} - \mathbf{b})$
15: **end if**
16: $(\mathbf{a}, \mathbf{b}) := (\mathbf{a} - \mathbf{b}, -\mathbf{b})$
17: **loop**
18: Trova $\mu \in \mathbb{Z}$ tale che $\|\mathbf{b} - \mu\mathbf{a}\|$ sia minima
19: $\mathbf{b} := \mathbf{b} - \mu\mathbf{a}$
20: **if** $\|\mathbf{a} - \mathbf{b}\| > \|\mathbf{a} + \mathbf{b}\|$ **then**
21: $\mathbf{b} := -\mathbf{b}$
22: **end if**
23: Scambia $\mathbf{a}$ e $\mathbf{b}$
24: **if** $(\mathbf{a}, \mathbf{b})$ è ridotta **then**
25: **return** $(\mathbf{a}, \mathbf{b})$
26: **end if**
27: **end loop**

Output: Una base ridotta di L

Vediamo più in dettaglio i passi dell'Algoritmo di Gauss. La prima parte (linee 1–16) ricava una base ben ordinata a partire da una base qualsiasi. Precisamente, dopo questa parte si avrà:

- $\|\mathbf{a}\| \leqslant \|\mathbf{b}\|$ (linee 1–3);
- $\|\mathbf{a} - \mathbf{b}\| \leqslant \|\mathbf{a} + \mathbf{b}\|$ (linee 4–6);
- $\|\mathbf{b}\| > \|\mathbf{a} - \mathbf{b}\|$, perché se $\|\mathbf{b}\| \leqslant \|\mathbf{a} - \mathbf{b}\|$, abbiamo una base ridotta, e l'algoritmo termina senza fare altro (linee 7–9);
- $\|\mathbf{a}\| > \|\mathbf{a} - \mathbf{b}\|$, perché se $\|\mathbf{a}\| \leqslant \|\mathbf{a} - \mathbf{b}\|$, abbiamo una base ben ordinata e l'algoritmo può entrare nella sua parte principale (linee 10–12);
- a questo punto restano due casi da analizzare:
  1. se $\|\mathbf{a}\| = \|\mathbf{b}\|$, è facile vedere che $(\mathbf{a}, \mathbf{a} - \mathbf{b})$ è una base ridotta, quindi si esce dall'algoritmo (linee 13–15);
  2. altrimenti ($\|\mathbf{a}\| < \|\mathbf{b}\|$), la base $(\mathbf{a} - \mathbf{b}, -\mathbf{b})$ è ben ordinata, e si può procedere (linea 16).

Quando entriamo nella parte principale (linee 17–27), possiamo supporre dunque che la base $(\mathbf{a}, \mathbf{b})$ sia ben ordinata. Il cuore dell'algoritmo è la linea 18, che sarà commentata in seguito.

Lemma 1.14. *Sia* $(\mathbf{a}, \mathbf{b})$ *la base (ben ordinata) in ingresso nel blocco di linee 18–23, e sia* $(\mathbf{a}', \mathbf{b}')$ *la base in uscita dallo stesso blocco. Allora* $(\mathbf{a}', \mathbf{b}')$ *è una base ridotta (e in tal caso l'algoritmo termina), oppure è una base ben ordinata.*

Dimostrazione. Abbiamo che $\mathbf{a}' = \pm(\mathbf{b} - \mu\mathbf{a})$, e $\mathbf{b}' = \mathbf{a}$. Dalle linee 20–22 si ha che $\|\mathbf{a}' - \mathbf{b}'\| \leqslant \|\mathbf{a}' + \mathbf{b}'\|$. Inoltre, $\|\mathbf{a}' - \mathbf{b}'\| = \|\pm(\mathbf{b} - \mu\mathbf{a}) - \mathbf{a}\| = \|\mathbf{b} - (\mu \pm 1)\mathbf{a}\|$, che per definizione di μ è maggiore o uguale di $\|\mathbf{b} - \mu\mathbf{a}\| = \|\mathbf{a}'\|$. Quindi

$$\|\mathbf{a}'\| \leqslant \|\mathbf{a}' - \mathbf{b}'\| \leqslant \|\mathbf{a}' + \mathbf{b}'\|.$$

Si presentano due casi:

- se $\|\mathbf{b}'\| \leqslant \|\mathbf{a}' - \mathbf{b}'\|$, allora la base $(\mathbf{a}', \mathbf{b}')$ è ridotta;
- se $\|\mathbf{b}'\| > \|\mathbf{a}' - \mathbf{b}'\|$, allora $\|\mathbf{a}'\| \leqslant \|\mathbf{a}' - \mathbf{b}'\| < \|\mathbf{b}'\|$ e la base $(\mathbf{a}', \mathbf{b}')$ è ben ordinata.

□

Proposizione 1.15. *L'*Algoritmo di Gauss *termina, e restituisce correttamente una base ridotta per* L.

Dimostrazione. Innanzitutto notiamo che su $(\mathbf{a}, \mathbf{b})$ sono eseguite solo operazioni elementari, quindi durante l'esecuzione dell'algoritmo $(\mathbf{a}, \mathbf{b})$ resta una base del reticolo. Inoltre, se l'algoritmo termina, $(\mathbf{a}, \mathbf{b})$ è effettivamente una base ridotta. Dobbiamo solo vedere che l'algoritmo termina. Per il lemma 1.14, all'inizio di ogni ciclo di linee 17–27 la base è ben ordinata, in particolare $\|\mathbf{b} - \mathbf{a}\| < \|\mathbf{b}\|$. Nel ciclo, $\mathbf{b}$ viene sostituito con $\mathbf{b} - \mu\mathbf{a}$, che è strettamente più corto di $\mathbf{b}$ (infatti, per definizione di μ, $\|\mathbf{b} - \mu\mathbf{a}\| \leqslant \|\mathbf{b} - \mathbf{a}\| < \|\mathbf{b}\|$). Quindi le lunghezze dei vettori della base ad ogni interazione calano (strettamente). Dato che c'è solo un numero finito di vettori di norma minore di $\|\mathbf{a}\| + \|\mathbf{b}\|$ nel reticolo, l'algoritmo deve terminare dopo un numero finito di iterazioni. □

L'Algoritmo di Gauss è polinomiale nella lunghezza dei vettori in input, e quindi SVP può essere risolto esattamente in dimensione 2, in tempo polinomiale; per una analisi più dettagliata, si rimanda a [12]. Vedremo nella prossima sezione un algoritmo in dimensione n, che trova una base ridotta (in senso generalizzato in dimensione n), il cui vettore più corto *non* realizza il minimo λ_1, ma solo un'approssimazione di esso.

1.5 L'algoritmo LLL

Vogliamo generalizzare l'Algoritmo di Gauss introdotto nella sezione precedente per dimensioni maggiori di 2. Questo algoritmo è stato descritto da Lenstra, Lenstra e Lovázs in [11]. Iniziamo con la nozione di base ridotta in dimensione n, limitandoci stavolta a considerare la norma euclidea su $\mathbb{R}^n$.

Siano $(\mathbf{b}_1, \dots, \mathbf{b}_k)$ una base di un reticolo $L \subseteq \mathbb{R}^n$, e $(\mathbf{b}_1^*, \dots, \mathbf{b}_k^*)$ il risultato dell'ortogonalizzazione di Gram-Schmidt. Definiamo per $i > j$

$$\mu_{i,j} := \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle},$$

cioè il coefficiente dell'ortogonalizzazione di Gram-Schmidt, e

$$\pi_i : \mathbf{x} \mapsto \sum_{j=i}^{k} \frac{\langle \mathbf{x}, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle} \mathbf{b}_j^*.$$

π_i è la proiezione su $\langle \mathbf{b}_i^*, \dots, \mathbf{b}_k^* \rangle$. In particolare, $\pi_i(\mathbf{b}_i) = \mathbf{b}_i^*$.

Definizione 1.16. Una base $(\mathbf{b}_1, \dots, \mathbf{b}_k)$ di un reticolo $L \subseteq \mathbb{R}^n$ è *LLL-ridotta* di parametro δ (in breve, *δLLL-ridotta*) se

1. $|\mu_{i,j}| < 1/2$ per ogni $i > j$;
2. per ogni coppia di vettori consecutivi $\mathbf{b}_i$, $\mathbf{b}_{i+1}$, si ha

$$\delta \|\pi_i(\mathbf{b}_i)\|^2 \leqslant \|\pi_i(\mathbf{b}_{i+1})\|^2.$$

Il parametro δ varia tra $1/4$ e 1, estremi esclusi; la situazione migliore si ha per $\delta = 1$, ma con questa scelta non si riesce a dimostrare che l'algoritmo converge. In effetti, si potrebbe scegliere $\delta = 1 - \varepsilon$: per $\varepsilon \longrightarrow 0$ il risultato è migliore, ma il costo dell'algoritmo cresce. Per $\delta = 1$, inoltre, si ha che la base 2-dimensionale $(\pi_i(\mathbf{b}_i), \pi_i(\mathbf{b}_{i+1}))$ è ridotta nel senso della definizione 1.10.

Si può dimostrare (per i dettagli, si veda [12]) che $\|\mathbf{b}_1\|$ non raggiunge il primo minimo successivo λ_1, ma si ha la stima

$$\|\mathbf{b}_1\| \leqslant \left(\frac{2}{\sqrt{4\delta - 1}} \right)^{n-1} \lambda_1.$$

L'idea di base per l'algoritmo è la stessa dell'Algoritmo di Gauss: si toglie a un vettore della base opportuni multipli degli altri, per ridurne la lunghezza. In particolare, supponiamo che $(\mathbf{b}_1, \dots, \mathbf{b}_{i-1})$ sia ridotta, mentre aggiungendo $\mathbf{b}_i$ no. Questo può succedere se $|\mu_{i,i-1}| > 1/2$, e in tal caso si riduce la lunghezza di

$\mathbf{b}_i$ levando multipli di $\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}$, oppure se $\mathbf{b}_i$ è troppo piccolo, e allora lo si scambia con un elemento precedente e si ricomincia.

Algoritmo ALGORITMO δLLL

Input: $(\mathbf{b}_1, \ldots, \mathbf{b}_k)$ base per L

1: **loop**
2: **for** $i := 1$ **to** k **do**
3: **for** $j := i - 1$ **downto** 1 **do**
4: $c_{i,j} := \lfloor \langle \mathbf{b}_i, \mathbf{b}_j \rangle / \langle \mathbf{b}_j, \mathbf{b}_j \rangle \rceil$
5: $\mathbf{b}_i := \mathbf{b}_i - c_{i,j}\mathbf{b}_j$
6: **end for**
7: **end for**
8: **if** $\delta \|\pi_i(\mathbf{b}_i)\|^2 > \|\pi_i(\mathbf{b}_{i+1})\|^2$ per qualche i **then**
9: Scambia $\mathbf{b}_i$ e $\mathbf{b}_{i+1}$
10: **else**
11: **return** $(\mathbf{b}_1, \ldots, \mathbf{b}_k)$
12: **end if**
13: **end loop**

Output: Una base δLLL-ridotta di L

Dopo il primo blocco di codice (linee 2–7), per gli elementi della base si ha effettivamente $|\mu_{i,j}| < 1/2$; a questo punto viene verificata la seconda condizione di δLLL-riduzione (linea 8), e in caso negativo vengono scambiate tra loro le due righe. Naturalmente questo comporta che la prima condizione possa non essere più verificata, quindi occorre rientrare nel ciclo che sistema i coefficienti $\mu_{i,j}$.

Diamo ora un'idea sulla stima della complessità dell'algoritmo. Per maggiori dettagli, si veda [12]. Mostreremo che il numero di iterazioni è polinomiale nella lunghezza dell'input, e che ogni iterazione richiede tempo polinomiale.

Il numero delle iterazioni è uguale al numero di scambi eseguiti nell'algoritmo. Detto Λ_i il reticolo generato dai primi i vettori della base, per $i = 1, \ldots, k$, sia $\Delta_i := \det(\Lambda_i)^2$, e $\Delta := \prod \Delta_i$. Per le proprietà del determinante di un reticolo, Δ_i e Δ sono numeri interi positivi. Notiamo che Δ non viene modificato dopo che la base è passata attraverso il blocco 2–7: infatti i vettori $\mathbf{b}_i^*$, calcolati usando la base prima della computazione oppure quella ottenuta dopo la computazione, sono gli stessi, e Δ dipende solo dalle lunghezze $\|\mathbf{b}_i^*\|$. Cosa succede invece se viene eseguito uno scambio? Supponiamo che vengano scambiati i vettori $\mathbf{b}_i$ e $\mathbf{b}_{i+1}$, e chiamiamo Δ_k' e Δ' quelli ottenuti dalla base dopo lo scambio. Si ha che $\Delta_k' = \Delta_k$ se $k \neq i$, perché

- se $k < i$, i vettori non vengono proprio modificati;
- se $k > i$, i reticoli Λ_k e Λ'_k sono generati dagli stessi vettori (solo in ordine diverso), quindi $\Lambda_k = \Lambda'_k$ e di conseguenza $\Delta_k = \Delta'_k$.

Di conseguenza, si ha

$$\frac{\Delta'}{\Delta} = \frac{\det(\Lambda'_i)^2}{\det(\Lambda_i)^2} = \frac{\left(\prod_{j=1}^{i-1} \|\mathbf{b}_j^*\|^2\right) \|\mathbf{b}_{i+1}^*\|^2}{\prod_{j=1}^{i} \|\mathbf{b}_j^*\|^2} = \frac{\|\pi_i(\mathbf{b}_{i+1})\|^2}{\|\pi_i(\mathbf{b}_i)\|^2} < \delta$$

dove l'ultima disuguaglianza è dovuta al fatto che lo scambio è stato eseguito, e quindi $\delta\|\pi_i(\mathbf{b}_i)\|^2 > \|\pi_i(\mathbf{b}_{i+1})\|^2$.

Per induzione, se $\Delta^{(0)}$ è associato alla base di partenza e $\Delta^{(k)}$ a quella dopo la k-esima iterazione, si ha $\Delta^{(k)} \leqslant \delta^k \Delta^{(0)}$. Dal fatto che $\Delta^{(k)}$ è un intero positivo segue che $\delta^k \Delta^{(0)} \geqslant 1$, e passando ai logaritmi

$$k \leqslant \frac{\ln(\Delta^{(0)})}{\ln(\delta^{-1})}.$$

Ora, $\Delta^{(0)}$ è calcolabile in tempo polinomiale dalla base di input, quindi chiaramente $\ln(\Delta^{(0)})$ è polinomiale nella dimensione dell'input. Fissato $\delta < 1$, $\ln(\delta^{-1})$ è un termine costante e non influenza il costo computazionale. Quindi il numero di iterazioni è polinomiale in termini di dimensione dell'input.

Per quanto riguarda il costo di ciascuna singola iterazione, il numero di operazioni svolte è polinomiale nella dimensione dell'input. Occorre fare attenzione all'eventuale crescita dei coefficienti (sia in termini di valore assoluto, che di numero di cifre per la loro rappresentazione), ma dopo qualche considerazione (si veda sempre [12] per un discorso più dettagliato) si può concludere che questa crescita resta polinomiale nella dimensione dell'input.

1.6 Usare LLL per il Closest Vector Problem

L'Algoritmo LLL può essere utilizzato anche per la risoluzione approssimata del CVP. Sia Λ un reticolo, e $\mathbf{p} \in \mathbb{R}^n$ un punto qualsiasi. Senza perdita di generalità, supponiamo che il reticolo sia di rango massimo (eventualmente possiamo proiettare su $\langle\Lambda\rangle$). Supponiamo inoltre di conoscere una base ridotta $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ di Λ.

L'idea in realtà è semplice: si lancia il passo di riduzione (che corrisponde alle linee 2–7 dell'Algoritmo LLL) sul reticolo che ha come base $(\mathbf{b}_1, \ldots, \mathbf{b}_n, \mathbf{p})$,

cioè si riduce $\mathbf{p}$ usando $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, dato che il resto della base è già ridotto. In questo modo, il vettore di output sarà della forma

$$\mathbf{p} - \sum_{j=1}^{n} c_j \mathbf{b}_j$$

dove $|c_j| \leqslant 1/2$ per ogni $j = 1, \ldots, n$.

L'algoritmo in questa forma è detto anche *Nearest Plane Algorithm*, perché ha un'interpretazione in termini geometrici: ogni iterazione del blocco di linee 3–6 applicato a $\mathbf{p}$ corrisponde alla scelta dell'iperpiano più vicino a $\mathbf{p}$. Più precisamente:

1. sia $\mathbf{s}$ la proiezione di $\mathbf{p}$ su $\langle \mathbf{b}_1, \ldots, \mathbf{b}_n \rangle$;
2. trova $c \in \mathbb{Z}$ tale che l'iperpiano $c\mathbf{b}_n + \langle \mathbf{b}_1, \ldots, \mathbf{b}_{n-1} \rangle$ sia il più vicino a $\mathbf{s}$;
3. sia $\mathbf{s}' := \mathbf{s} - c\mathbf{b}_n$, e riparti dal punto 1 applicato a $\mathbf{s}'$ e al reticolo generato da $\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}$; chiama $\boldsymbol{\nu}'$ il risultato;
4. restituisci $\boldsymbol{\nu} := \boldsymbol{\nu}' + c\mathbf{b}_n$.

La dimostrazione della correttezza di questo algoritmo si può trovare sempre in [12].

1.7 Un'applicazione crittografica: NTRU

Vediamo un protocollo crittografico la cui sicurezza si basa sulla difficoltà di risolvere il problema SVP. Questo crittosistema è stato introdotto da Hoffstein, Pipher e Silverman in [8] e prende il nome di NTRU.

L'ambiente di lavoro è l'anello

$$R := \mathbb{Z}[X]/(X^n - 1),$$

cioè si usano polinomi di grado al più $n - 1$. Il crittosistema ha tre parametri: n stesso; p, un intero piccolo (per esempio, 3); q, un intero di media grandezza (per esempio, 256). È richiesto che p e q siano coprimi.

1. Una volta fissati $n, p, q \in \mathbb{Z}$ come descritto sopra, Alice sceglie successivamente $f, g \in R$ con coefficienti identificabili modulo p (ad esempio in $\{-1, 0, 1\}$); f dev'essere invertibile modulo p e modulo q: denotiamo gli inversi rispettivamente con f_p e f_q. La chiave pubblica è costituita dal polinomio $h \equiv g f_q \pmod{q}$, quella privata dal polinomio f.

2. Bob codifica il messaggio m come un polinomio i cui coefficienti siano compresi (supponendo p dispari) tra $-\frac{p-1}{2}$ e $\frac{p-1}{2}$, e sceglie un polinomio r a coefficienti in $\{-1, 0, 1\}$. Il messaggio codificato inviato ad Alice è $c \equiv prh + m \pmod q$.

3. Per decifrare il messaggio, Alice calcola $a \equiv cf \equiv (prh + m)f \equiv prg + mf \pmod q$ e sceglie un rappresentante con i coefficienti compresi tra $-\frac{q}{2}$ e $\frac{q}{2}$. A questo punto Alice calcola $a \pmod p$, ottenendo fm, e quindi recupera m moltiplicando per f_p.

La decodifica funziona perché per opportune scelte dei parametri, il polinomio $prg + mf \in R$ ha coefficienti compresi tra $-\frac{q}{2}$ e $\frac{q}{2}$, quindi non cambia se ridotto modulo q. In altre parole, quando Alice calcola $cf \pmod q$ e sceglie il rappresentante con coefficienti tra $-\frac{q}{2}$ e $\frac{q}{2}$, recupera *esattamente* $prg + mf \in R$. A questo punto, il resto della decodifica è facile.

Su cosa si basa la sicurezza di questo sistema? In altre parole, come può un malintenzionato recuperare f conoscendo h? A parte metodi diretti di forza bruta, resi inefficaci dalle scelte dei parametri, si potrebbe tentare un SVP. Infatti, consideriamo il reticolo generato dalle righe della matrice $2n \times 2n$

$$\left(\begin{array}{cccc|cccc} \alpha & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{n-1} \\ 0 & \alpha & \cdots & 0 & h_{n-1} & h_0 & \cdots & h_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha & h_1 & h_2 & \cdots & h_0 \\ \hline 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{array}\right)$$

dove gli h_i sono i coefficienti della chiave pubblica e α un ulteriore parametro che sarà scelto opportunamente. Questo reticolo contiene il vettore $(\alpha f, g)$, cioè il vettore dei coefficienti di f moltiplicati per α e i coefficienti di g: si ottiene come combinazione lineare delle prime n righe, usando l'i-esimo coefficiente di f per la riga i-esima.

Un eventuale attaccante, allora, può scegliere α in modo che $(\alpha f, g)$ sia abbastanza vicino al vettore più corto del reticolo, e quindi possa essere trovato con un SVP. In risposta a questo tipo di attacco, gli sviluppatori di NTRU suggeriscono di scegliere f e g in modo da rendere il reticolo simile a un reticolo casuale (e quindi rendere la vita difficile agli algoritmi per SVP). Per ulteriori dettagli, si rimanda all'articolo originale di Hoffstein, Pipher e Silverman ([8]).

1.8 Fattorizzare polinomi a coefficienti razionali

Nel loro articolo originale ([11]), i fratelli Lenstra e Lovász mostravano un'applicazione dell'Algoritmo LLL al problema di fattorizzare polinomi a coefficienti razionali. Esponiamo qui brevemente il loro procedimento e i risultati su cui si basa, rimandando al loro articolo per i dettagli delle dimostrazioni.

L'idea di fondo consiste nel ricondurre la ricerca di fattori irriducibili alla ricerca di elementi piccoli di un opportuno reticolo. Supponiamo di voler cercare dei fattori irriducibili di un polinomio $f \in \mathbb{Z}[X]$ di grado n, e supponiamo di avere un polinomio $h \in \mathbb{Z}[X]$ tale che

(h1) $\mathrm{lc}(h) = 1$;

(h2) $[h]$ divide $[f]$ in $\mathbb{Z}/(p^k)[X]$;

(h3) $[h]$ è irriducibile in $\mathbb{Z}/(p)[X]$;

(h4) $[h]^2$ *non* divide $[f]$ in $\mathbb{Z}/(p)[X]$.

Proposizione 1.17. *Esiste un fattore irriducibile h_0 di f in $\mathbb{Z}[X]$ tale che $[h]$ divide $[h_0]$ in $\mathbb{Z}/(p)[X]$, e questo fattore è univocamente determinato (a meno di segno). Inoltre, se g divide f in $\mathbb{Z}[X]$, allora sono equivalenti*

1. *$[h]$ divide $[g]$ in $\mathbb{Z}/(p)[X]$;*
2. *$[h]$ divide $[g]$ in $\mathbb{Z}/(p^k)[X]$;*
3. *h_0 divide g in $\mathbb{Z}[X]$.*

In particolare $[h]$ divide $[h_0]$ in $\mathbb{Z}/(p^k)[X]$.

Sia $\ell := \deg(h)$, e sia $m \geqslant \ell$ un intero. Sia inoltre

$$L := \left\{ g \in \mathbb{Z}[X] \;\middle|\; \deg(g) \leqslant m,\ [h] \text{ divide } [g] \text{ in } \mathbb{Z}/(p^k)[X] \right\}.$$

Chiaramente $L \subseteq \mathbb{R}^{m+1}$, identificando un polinomio con la $(m+1)$-upla dei suoi coefficienti; di più L è un reticolo, una cui base è

$$\{p^k X^i \mid 0 \leqslant i < \ell\} \cup \{h(X)X^j \mid 0 \leqslant j \leqslant m - \ell\}.$$

Infatti in questo modo si ottengono tutti e soli i multipli di h di grado minore o uguale a m, a cui si può aggiungere qualsiasi polinomio (di grado minore di ℓ) con coefficienti multipli di p^k. Notiamo che $\det(L) = p^{k\ell}$.

Nel seguito, per $f \in \mathbb{Z}[X]$, indichiamo con $|f|$ la norma (euclidea) del vettore dei coefficienti di f.

Lemma 1.18. *Sia* $b \in L$ *tale che* $p^{k\ell} > |f|^m |b|^n$. *Allora* h_0 *(come nella proposizione 1.17) divide* b *in* $\mathbb{Z}[X]$*; in particolare* $\mathrm{MCD}(f, b) \neq 1$.

Da questo lemma si ottiene la proposizione seguente, che lega il grado di h_0 con la lunghezza di un vettore di una base ridotta.

Proposizione 1.19. *Utilizzando le stesse notazioni precedenti, sia* $(b_1, \dots, b_{m+1})$ *una base ridotta per* L. *Supponiamo che*

$$p^{k\ell} > 2^{\frac{mn}{2}} \binom{2m}{m}^{\frac{n}{2}} |f|^{m+n}. \tag{1.2}$$

Allora $\deg(h_0) \leqslant m$ *se e solo se*

$$|b_1| < \left(\frac{p^{k\ell}}{|f|^m}\right)^{\frac{1}{n}}.$$

Con un'ipotesi in più siamo anche in grado di trovare esplicitamente il fattore h_0.

Proposizione 1.20. *Nelle stesse ipotesi della proposizione 1.19, supponiamo inoltre che esista un indice* $j \in \{1, \dots, m+1\}$ *tale che*

$$|b_j| < \left(\frac{p^{k\ell}}{|f|^m}\right)^{\frac{1}{n}}. \tag{1.3}$$

Sia t *il massimo indice per cui valga* (1.3). *Allora si ha che* $\deg(h_0) = m + 1 - t$, $h_0 = \mathrm{MCD}(b_1, \dots, b_t)$, *e* (1.3) *vale per tutti gli indici* $j = 1, \dots, t$.

Grazie alle proposizioni precedenti possiamo scrivere in dettaglio l'algoritmo di fattorizzazione. Per prima cosa cerchiamo il fattore h_0 della proposizione 1.17.

Algoritmo TEST FATTORE

Input: $f \in \mathbb{Z}[X]$, $n := \deg(f)$, $p \in \mathbb{Z}$ primo, $k \in \mathbb{Z}$, $h \in \mathbb{Z}[X]$ con coefficienti ridotti modulo p^k per cui valgano (h1)–(h4), $\ell := \deg(h)$, $m \geqslant \ell$ per cui valga la relazione (1.2)

1: $L :=$ reticolo con base $\{p^k X^i \mid 0 \leqslant i < \ell\} \cup \{h(X)X^j \mid 0 \leqslant j \leqslant m - \ell\}$
2: Calcola una base ridotta $\mathcal{B} := (b_1, \dots, b_{m+1})$ di L con l'ALGORITMO LLL
3: **if** $|b_1| \geqslant (p^{k\ell}/|f|^m)^{1/n}$ **then**
4: **return** `FALLIMENTO`
5: **else**
6: $t := \max\{j \mid |b_j| < (p^{k\ell}/|f|^m)^{1/n}\}$
7: **return** $h_0 := \mathrm{MCD}(b_1, \dots, b_t)$
8: **end if**

Output: Se $\deg(h_0) \leqslant m$, h_0 come nella proposizione 1.17; `FALLIMENTO` in caso contrario

Algoritmo TROVA FATTORE

Input: $f \in \mathbb{Z}[X]$, $n := \deg(f)$, $p \in \mathbb{Z}$ primo, $h \in \mathbb{Z}[X]$ con coefficienti ridotti modulo p per cui valgano (h1)–(h4) con $k = 1$

1: $\ell := \deg(h)$
2: **if** $\ell = n$ **then**
3: **return** $h_0 := f$
4: **end if**
5: $k :=$ il minimo intero per cui valga (1.2) con $m = n - 1$
6: Cambia h in modo che valga (h2) con tale k senza cambiare $[h]$ in $\mathbb{Z}/(p)[X]$
▷ Questo può essere fatto, ad esempio, tramite Lemma di Hensel
7: $u :=$ il massimo intero per cui $\ell \leqslant (n-1)/2^u$
8: **for** $j := u$ **downto** 0 **do**
9: Lancia TEST FATTORE con $m = \lfloor (n-1)/2^j \rfloor$
10: **if not** `FALLIMENTO` **then**
11: **return** h_0
12: **end if**
13: **end for**
14: **return** $h_0 := f$ ▷ Se nessuno degli m precedenti funziona, $\deg(h_0) > n - 1$

Output: h_0 come nella proposizione 1.17

A questo punto è facile scrivere l'algoritmo completo. Per brevità di scrittura indicheremo con $[f]_p$ la classe di f in $\mathbb{Z}/(p)[X]$.

Algoritmo FATTORIZZAZIONE LLL

Input: $f \in \mathbb{Z}[X]$, $n := \deg(f)$

1: Calcola $\mathrm{Ris}(f, f')$
2: **if** $\mathrm{Ris}(f, f') = 0$ **then** ▷ f ha radici multiple
3: $g := \mathrm{MCD}(f, f')$
4: $f_0 := f/g$;
5: Lancia FATTORIZZAZIONE LLL su f_0
▷ A questo punto si completa la fattorizzazione di f per tentativi,
▷ dato che i fattori irriducibili di g dividono f_0
6: **else**
7: $p :=$ il più piccolo primo che non divide $\mathrm{Ris}(f, f')$
8: Fattorizza $[f]_p$
▷ Ad esempio con l'algoritmo di Berlekamp

▷ *Continua a pagina seguente*

▷ *Continua da pagina precedente*

```
    f_1 := 1; f_2 := f
            ▷ Ad ogni iterazione conosciamo la fattorizzazione di f_1 e di [f_2]_p
    while f_2 ≠ ±1 do
        for each [h]_p fattore irriducibile di [f_2]_p do
            Applica Trova Fattore a f_2 e h, trovando h_0
            f_1 := f_1 h_0; f_2 := f_2/h_0
            Rimuovi dalla lista dei fattori di [f_2]_p quelli che dividono [h_0]_p
        end for
    end while
end if
```

Output: La fattorizzazione di f in fattori irriducibili

Il costo totale dell'algoritmo Fattorizzazione LLL in termini di operazioni elementari è $\mathcal{O}(n^6 + n^5 \log |f|)$, e queste operazioni sono svolte su interi la cui rappresentazione binaria richiede $\mathcal{O}(n^3 + n^2 \log |f|)$ cifre. Per i dettagli, si veda [11].

1.9 Il protocollo Goldreich-Goldwasser-Halevi (GGH)

NTRU (vedi sezione 1.7) non è stato il primo protocollo crittografico la cui sicurezza si basa sulla difficoltà di risolvere SVP o CVP: un approccio più diretto era stato tentato qualche anno prima da Goldreich, Goldwasser ed Halevi.

L'idea da cui gli autori sono partiti è: CVP è difficile se la base $\mathcal{B}$ è qualsiasi, ma diventa facilmente risolvibile per alcune basi "belle" (ad esempio, formate da vettori quasi-ortogonali). Di conseguenza, possiamo utilizzare una base "bella" come chiave privata, e pubblichiamo una base qualsiasi come chiave pubblica.

Presentiamo qui una descrizione sommaria del protocollo GGH, rimandando all'articolo originale ([7]) per i dettagli.

1. Alice sceglie un reticolo Λ e una base "bella" $B \in \mathcal{M}_n(\mathbb{Z})$ (gli elementi della base sono le colonne della matrice B). Sceglie quindi una matrice di cambiamento di base $U \in \mathsf{GL}_n(\mathbb{Z})$, e pubblica $B' := UB$.

2. Bob vuole mandare ad Alice un messaggio $\mathbf{m} \in \mathbb{Z}^n$. Per fare ciò, sceglie un errore $\boldsymbol{e} \in \mathbb{Z}^n$ piccolo ed invia $\mathbf{c} = \mathbf{m}B' - \boldsymbol{e}$.

3. Per decifrare il messaggio, Alice usa la base B per risolvere il CVP e ottenere $\mathbf{m}B'$, da cui ricava facilmente $\mathbf{m}$.

In linea teorica, questo protocollo dovrebbe essere affidabile (B e B' sono scelte in modo che risolvere CVP sia facile con la prima e molto difficile con la seconda). In realtà, alcuni anni dopo la sua pubblicazione, si è mostrato che la particolare specifica del protocollo permette di risalire a informazioni del messaggio originale a partire dal messaggio cifrato, e tramite queste informazioni è possibile ricostruire il messaggio originale risolvendo un CVP più facile di quanto previsto. Per una descrizione più accurata delle falle del protocollo GGH, si veda l'articolo di Nguyen ([13]).

1.10 Reticoli e ideali binomiali

Introduciamo a questo punto un legame tra i reticoli e particolari ideali dell'anello $\mathbb{K}[X_1, \ldots, X_n]$. Questo legame ci permetterà di trasportare i problemi sui reticoli nell'ambiente degli anelli di polinomi, ed eventualmente viceversa.

Definizione 1.21. Un *binomio* è un polinomio di $\mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \ldots, X_n]$ della forma $a\mathbf{X}^{\boldsymbol{\alpha}} + b\mathbf{X}^{\boldsymbol{\beta}}$, con $a, b \in \mathbb{K}$ e $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^n$. Un *ideale binomiale* è un ideale per il quale esiste un insieme di generatori formato da binomi. Chiameremo *binomio di differenza pura* un binomio della forma $\mathbf{X}^{\boldsymbol{\alpha}} - \mathbf{X}^{\boldsymbol{\beta}}$.

È facile notare che un ideale è binomiale se e solo se una sua base di Gröbner ridotta (rispetto a qualsiasi ordinamento) è formata da binomi: infatti l's-polinomio tra due binomi è ancora un binomio, e analogamente il processo di riduzione coinvolge solo binomi. Inoltre le operazioni di s-polinomio e riduzione applicate a binomi di differenza pura restituiscono binomi di differenza pura.

Ora, un elemento $\boldsymbol{\gamma} \in \mathbb{Z}^n$ può essere rappresentato da una coppia $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{N}^n \times \mathbb{N}^n$ tale che $\boldsymbol{\alpha} - \boldsymbol{\beta} = \boldsymbol{\gamma}$. Questa rappresentazione è unica scegliendo $\boldsymbol{\alpha}$ e $\boldsymbol{\beta}$ minimali, ovvero tali che per ogni $i = 1, \ldots, n$ si abbia $\alpha_i \beta_i = 0$. Di conseguenza, a ogni $\boldsymbol{\gamma} \in \mathbb{Z}^n$ è possibile associare un binomio $p_{\boldsymbol{\gamma}} := \mathbf{X}^{\boldsymbol{\alpha}} - \mathbf{X}^{\boldsymbol{\beta}}$. Per L reticolo fissato, dunque, definiamo l'ideale

$$I_L := (p_{\boldsymbol{\gamma}} \mid \boldsymbol{\gamma} \in L).$$

Fissato un ordinamento, possiamo calcolare la base di Gröbner ridotta di I_L; per quanto visto sopra, tale base è formata da binomi di differenza pura, pertanto ad ogni binomio di essa è possibile associare un elemento del reticolo. Chiamiamo l'insieme di questi elementi *base di Gröbner* del reticolo.

Grazie a questa doppia lettura reticoli/ideali binomiali possiamo scegliere indifferentemente le tecniche proprie dell'una o dell'altra teoria per affrontare i problemi. Per esempio, supponiamo di voler calcolare una base di Gröbner Lex

di un ideale della forma I_L: possiamo farlo calcolando una forma di Hermite (vedi sezione 1.1). Infatti, supponiamo che L sia di rango massimo e che la forma di Hermite di L sia data dalla matrice

$$\begin{pmatrix} d_1 & c_{1,2} & \cdots & \cdots & c_{1,n} \\ 0 & d_2 & c_{2,3} & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & c_{n-1,n} \\ 0 & \cdots & \cdots & 0 & d_n \end{pmatrix}$$

in cui operiamo una piccola modifica: sottraendo opportunamente multipli della riga i-esima, possiamo fare in modo che per ogni $\ell = 1, \ldots, i-1$ si abbia $-d_i < c_{\ell,i} \leqslant 0$. I binomi corrispondenti alle righe sono

$$\begin{aligned} & X_1^{d_1} - X_2^{|c_{1,2}|} \cdots X_n^{|c_{1,n}|} \\ & X_2^{d_2} - X_3^{|c_{2,3}|} \cdots X_n^{|c_{2,n}|} \\ & \vdots \\ & X_n^{d_n} \end{aligned}$$

i quali effettivamente formano una base di Gröbner Lex (continuano a generare I_L per le proprietà della forma di Hermite, e sono una base di Gröbner ad esempio per il fatto che i *leading term* sono coprimi). Maggiori dettagli in [1].

Avendo il concetto di base di Gröbner per i reticoli, possiamo parlare di *forma normale* di un elemento di $\mathbb{Z}^n$. In realtà, se l'ordinamento scelto è compatibile con il grado, la forma normale di un vettore $\boldsymbol{v}$ è il più piccolo vettore (rispetto alla norma ℓ^1) equivalente a $\boldsymbol{v}$ tramite il reticolo; di conseguenza abbiamo che

- per risolvere CVP per $\boldsymbol{v}$ è sufficiente prendere il vettore $\boldsymbol{v} - \mathsf{NF}(\boldsymbol{v}) \in L$;
- per risolvere SVP basta calcolare una base di Gröbner per L e prendere il vettore più corto di tale base.

1.11 Lattice Polly Cracker

Alcuni anni fa era stato proposto uno schema di crittosistemi basato sulla difficoltà teorica del calcolo di una base di Gröbner. In effetti, se si riesce a tradurre un problema dimostrato difficile in termini polinomiali e la sua risoluzione nel trovare una base di Gröbner, allora si può essere certi che tale calcolo è impraticabile. Quindi, si è pensato di definire un crittosistema la cui *trapdoor*

information sia la conoscenza di una base di Gröbner. Tale crittosistema prende il nome di *Polly Cracker*.

1. Alice sceglie una base di Gröbner $\mathcal{G}$ di un ideale $I \subset \mathbb{K}[\mathbf{X}]$. La base $\mathcal{G}$ è mantenuta privata, mentre è pubblico l'insieme dei rappresentanti canonici di $\mathbb{K}[\mathbf{X}]/I$, che rappresenta lo spazio dei messaggi in chiaro.

2. Alice sceglie inoltre un insieme di polinomi $\{f_i\} \subseteq I$ in modo che il calcolo di una base di Gröbner di $J := (f_i) \subseteq I$ sia difficile. J rappresenta la chiave pubblica di Alice.

3. Bob, per mandare un messaggio $m \in \mathbb{K}[\mathbf{X}]/I$ ad Alice, sceglie $p \in J$ ed invia $c = m + p$.

4. Alice deve solo ridurre c con la base di Gröbner per recuperare il messaggio in chiaro.

Sfortunatamente, questo crittosistema così com'è non funziona. Vediamone un paio di motivi.

- Potrebbe non essere necessario calcolare l'intera base di Gröbner, ma limitarne il grado: i polinomi di grado elevato in $\mathcal{G}$ intervengono solo se c contiene elementi di grado elevato. Per evitare ciò, potremmo usare polinomi di grado elevato per mascherare il messaggio, ma questo alza notevolmente il costo della cifratura, che diventa paragonabile a quello della decifratura.

- Potremmo pensare di usare polinomi sparsi per non appesantire il calcolo, ma così facendo daremmo informazioni sul *pattern* dei monomi utilizzati. Infatti ci sono pochi polinomi in I sparsi; analizzando le differenze tra i monomi di c, è facile costruire un polinomio che sta in I, e utilizzarlo per eliminare una parte della maschera.

Il secondo problema potrebbe essere aggirato utilizzando ideali binomiali: se si usa un binomio per cancellare un monomio, rimane comunque un monomio ("come gli indiani che camminano uno nell'orma dell'altro"). Vista la corrispondenza tra gli ideali binomiali e i reticoli, questo porta a definire un crittosistema che combina le basi di Gröbner e i reticoli, chiamato *Lattice Polly Cracker*.

Come abbiamo visto, una base di Gröbner Lex di un reticolo si trova con un calcolo di forma normale di Hermite. Quindi non può essere usata come informazione segreta: è troppo facile da ottenere. D'altra parte, una base DegRevLex è ingestibile anche per chi definisce il crittosistema. L'idea allora è utilizzare un

reticolo a blocchi, e scegliendo l'ordinamento DegRevLex all'interno del singolo blocco e Lex tra i blocchi. Naturalmente è necessario nascondere la struttura a blocchi del reticolo.

Descriviamo ora brevemente il funzionamento di Lattice Polly Cracker, rimandando ancora una volta all'articolo originale ([1]) per i dettagli.

Una prima versione, che *non* fa uso di una struttura a blocchi (ed è insicura), ha le seguenti caratteristiche:

- l'insieme $M := [0, s]^n \subseteq \mathbb{Z}^n$ è lo spazio dei messaggi in chiaro (lo spazio è scelto simmetrico perché un suo eventuale adattamento all'*escalier* potrebbe portare a una conoscenza parziale dell'ordinamento fissato);
- la chiave pubblica è un reticolo L, scelto in modo che due elementi di M non siano equivalenti modulo L;
- per cifrare, si sostituisce un elemento $\mathbf{m} \in M$ con $\mathbf{c} = \mathbf{m} + \mathbf{l}$ per un certo $\mathbf{l} \in L$;
- la chiave privata consiste in un ordinamento e una corrispondente base di Gröbner $\mathcal{G}$ di L, tale che l'*escalier* associata contenga M;
- la decifratura avviene per mezzo del calcolo della forma normale di $\mathbf{c}$ tramite $\mathcal{G}$.

Nella scelta di un ordinamento opportuno entra in gioco la struttura a blocchi. Sia allora $\mathbf{b} := (b_1, \ldots, b_m)$ una m-upla di numeri naturali tali che $\sum b_i = n$, e sia a_j la somma parziale dei b_i fino a b_j. Diciamo che $\mathbf{b}$ è una struttura a blocchi su una matrice $L = (l_{r,s})$ se $l_{r,s} = 0$ per $s \leqslant a_i < r$ per ogni $i = 1, \ldots, m$. Il blocco con indici r, s compresi tra a_{i-1} (escluso) e a_i (incluso) è detto i-esimo blocco diagonale.

Ovviamente $\mathbf{b}$ induce una struttura a blocchi anche sui vettori $\boldsymbol{v} \in \mathbb{Z}^n$. Se $\boldsymbol{v} \neq \mathbf{0}$, sia i il primo blocco di $\boldsymbol{v}$ diverso da zero; la *testa* di $\boldsymbol{v}$ è il vettore $H(\boldsymbol{v})$ che ha lo stesso blocco i-esimo di $\boldsymbol{v}$ e zeri altrove, la *coda* di $\boldsymbol{v}$ è definita come $\boldsymbol{v} - H(\boldsymbol{v})$.

Una struttura a blocchi induce un ordinamento a blocchi: $\boldsymbol{v} < \boldsymbol{w}$ se, supponendo che i sia il blocco non nullo di $H(\boldsymbol{v})$ e j quello di $H(\boldsymbol{w})$, si ha $i < j$ o, nel caso in cui $i = j$, il confronto avviene tramite un altro ordinamento fissato.

Proposizione 1.22. *Sia* $\mathbf{b}$ *una struttura a blocchi su una matrice* L *e consideriamo l'ordinamento a blocchi associato. Sia* $\mathcal{G}_i$ *la base di Gröbner ridotta dell'*i*-esimo blocco diagonale. Allora la base di Gröbner ridotta di* L *è formata da vettori le cui teste*

corrispondono ai vettori dell'unione delle $\mathcal{G}_i$ e le cui code sono formate da elementi negativi o nulli.

Come possiamo nascondere questa struttura a blocchi? Il problema è che anche permutando le variabili si riesce a risalire ai blocchi di appartenenza, supponendo di conoscere i determinanti d_i dei blocchi diagonali (ricordiamo che $\det(L) = \prod d_i$ è un'informazione pubblica).

Lemma 1.23. *Sia L un reticolo a blocchi, e sia d_m il determinante del blocco più piccolo. Allora per ogni indeterminata X_i appartenente al blocco più piccolo si ha che il polinomio $X_i^{d_m} - 1$ appartiene a I_L.*

Di conseguenza, calcolando un polinomio univariato in I_L per ogni variabile (è possibile, per esempio, con una base di Gröbner Lex opportuna) si possono identificare i blocchi di appartenenza (una variabile dell'i-esimo blocco ha ordine che divide $d_i \cdot \ldots \cdot d_m$) e quindi risalire alla struttura a blocchi. Notiamo anche che l'ordine di tutte le variabili può essere calcolato in una volta adoperando la forma di Smith anziché quella di Hermite.

La soluzione che gli autori di [1] propongono è quella di mascherare la struttura a blocchi con un automorfismo di $\mathbb{Z}^n$ (*non* isometrico): infatti il concetto di struttura a blocchi non è invariante per automorfismo. Quindi questa nuova versione di Lattice Polly Cracker prevede due reticoli, uno privato per la decifratura e uno pubblico per la cifratura, collegati tra loro da un automorfismo non isometrico di $\mathbb{Z}^n$ (pertanto i due reticoli *non* sono isomorfi). Più in dettaglio:

- l'insieme $M := [0, s]^n \subseteq \mathbb{Z}^n$ è lo spazio dei messaggi in chiaro;
- la chiave pubblica è un reticolo L_{pub}, scelto in modo che due elementi di M non siano equivalenti modulo L_{pub};
- per cifrare, si sostituisce un elemento $\mathbf{m} \in M$ con $\mathbf{c} = \mathbf{m} + \mathbf{l}$ per un certo $\mathbf{l} \in L_{pub}$;
- la chiave privata consiste in
  - un automorfismo $\varphi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$, con $L = \varphi(L_{pub})$;
  - un ordinamento e una corrispondente base di Gröbner $\mathcal{G}$ di L;
  - un vettore di shift $\boldsymbol{\tau}$, tale che $\varphi(M) + \boldsymbol{\tau}$ sia contenuto nell'*escalier* associata;
- per la decifratura si calcola $\varphi^{-1}(-\boldsymbol{\tau} + \mathrm{NF}(\varphi(\mathbf{c}) + \boldsymbol{\tau}))$.

Rispetto al caso precedente, l'insieme M dei messaggi nelle coordinate private non è più un cubo n-dimensionale, anzi non è detto nemmeno che abbia coordinate positive (o nulle), a meno di applicare uno shift $\boldsymbol{\tau}$.

Rimandiamo ancora una volta alla descrizione originale del crittosistema ([1]) per un'analisi di eventuali attacchi e della scelta dei parametri che definiscono un'istanza di Lattice Polly Cracker.

Capitolo 2

Curve ellittiche

Recentemente hanno trovato importanza in algebra computazionale, e in particolar modo in crittografia, alcuni oggetti legati principalmente alla geometria algebrica e alla teoria dei numeri, le cosiddette *curve ellittiche*. Il motivo principale è che le curve ellittiche forniscono una notevole quantità di gruppi finiti su cui è particolarmente facile lavorare, perché molto ricchi di struttura.

Nella trattazione di questo argomento seguiremo principalmente il testo di Washington ([15]).

2.1 Definizione e prime proprietà

Iniziamo, naturalmente, definendo gli oggetti di cui parleremo.

Definizione 2.1. Sia $\mathbb{K}$ un campo. Un'equazione della forma

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

dove $a_1, \ldots, a_6 \in \mathbb{K}$ è detta *equazione di Weierstrass*.

Nel seguito indicheremo con $F(X, Y, Z) \in \mathbb{K}[X, Y, Z]$ il polinomio che definisce un'equazione di Weierstrass. In altre parole, scriviamo (2.1) come

$$F(X, Y, Z) = 0.$$

Definizione 2.2. Dato un campo $\mathbb{K}$, una *curva ellittica* definita su $\mathbb{K}$, indicata con $E/_{\mathbb{K}}$, è l'insieme delle soluzioni in $\mathbb{P}^2(\mathbb{K})$ di un'equazione di Weierstrass, cioè

$$E/_{\mathbb{K}} := \{[x : y : z] \in \mathbb{P}^2(\mathbb{K}) \mid F(x, y, z) = 0\}.$$

Osservazione. Un altro modo possibile per definire una curva ellittica è quello di *curva proiettiva di genere 1*. Tuttavia per fare ciò occorre dire cosa si intende per curva (e più in generale varietà) proiettiva e definirne il genere. Per i nostri scopi, l'equazione di Weierstrass è sufficiente; per chi fosse interessato all'altro punto di vista, rimandiamo ad esempio al testo di Silverman ([14]).

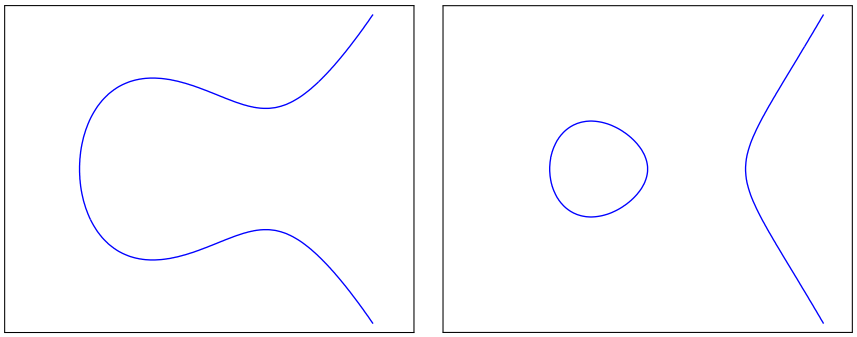


Figura 2.1: I due possibili grafici (a meno di trasformazioni affini) di una curva ellittica definita su $\mathbb{R}$.

Essendo F un polinomio omogeneo di terzo grado, una curva ellittica è ben definita. Nel seguito, quando non ci sono ambiguità, indicheremo una curva ellittica anche solo con E, senza esplicitare il campo $\mathbb{K}$ su cui è definita. Inoltre, se l'equazione di Weierstrass che definisce $E/_{\mathbb{K}}$ ha coefficienti in $\mathbb{K}$ e $\mathbb{L} \supseteq \mathbb{K}$ è un'estensione di campi, ha senso considerare i punti di $\mathbb{P}^2(\mathbb{L})$ che soddisfano l'equazione: tale curva ellittica sarà indicata con $E(\mathbb{L})$.

Mettiamoci adesso nella carta $U_z := \{z \neq 0\}$, che identificheremo con un piano affine $\mathbb{A}^2(\mathbb{K})$, e studiamo separatamente $E \cap U_z$ e $E \cap \{z = 0\}$.

Nella carta U_z, possiamo deomogeneizzare rispetto alla coordinata z, applicando

$$(x, y, z) \mapsto \left(\frac{x}{z}, \frac{y}{z}, 1\right)$$

che ci porta all'*equazione di Weierstrass non omogenea*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

dove abbiamo ribattezzato $x := x/z$ e $y := y/z$. Indicheremo con $f(X, Y) \in \mathbb{K}[X, Y]$ il polinomio che definisce l'equazione (2.2).

Quindi, in U_z possiamo mettere in corrispondenza biunivoca le soluzioni in $\mathbb{P}^2(\mathbb{K})$ di (2.1) con le soluzioni in $\mathbb{A}^2(\mathbb{K})$ di (2.2).

Cosa succede se $z = 0$? Sostituendo in (2.1), otteniamo $x^3 = 0$ e nessuna restrizione sulla y (se non la ovvia $y \neq 0$ affinché il punto del piano proiettivo

sia definito). In altre parole,

$$E/_{\mathbb{K}} \cap \{z = 0\} = \{[0 : 1 : 0]\}.$$

Il punto $O := [0 : 1 : 0]$ è detto *punto all'infinito* della curva ellittica. Da ora in avanti, se non esplicitamente specificato, supporremo che $E/_{\mathbb{K}}$ sia l'insieme dei punti di $\mathbb{A}^2(\mathbb{K})$ che verificano (2.2), unitamente a un punto all'infinito O.

Osservazione. Se $\mathrm{char}(\mathbb{K}) \neq 2$, l'equazione (2.2) si può semplificare completando il quadrato; in effetti, la sostituzione

$$y \longmapsto \frac{y - a_1 x - a_3}{2}$$

porta l'equazione nella forma

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6, \tag{2.3}$$

dove $b_2 := a_1^2 + 4a_4$, $b_4 := 2a_4 + a_1 a_3$ e $b_6 := a_3^2 + 4a_6$. Se inoltre $\mathrm{char}(\mathbb{K}) \neq 2, 3$ la (2.3) si può ulteriormente semplificare in

$$y^2 = x^3 - 27c_4 x - 54c_6,$$

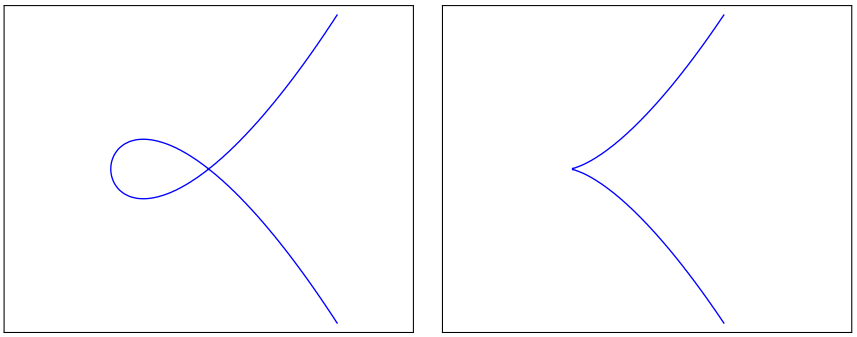
con $c_4 := b_2^2 - 24b_4$ e $c_6 := -b_2^3 + 36b_2 b_4 - 216b_6$, tramite il cambiamento di coordinate

$$(x, y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right).$$

Definizione 2.3. Sia $E/_{\mathbb{K}}$ una curva ellittica definita da un'equazione di Weierstrass $F(X, Y, Z) = 0$. Un punto $P \in \mathbb{P}^2(\mathbb{K})$ è detto *punto singolare* se

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

La curva si dice *singolare* se ha almeno un punto singolare, *non singolare* altrimenti.



(a) Nodo. (b) Cuspide.

Figura 2.2: I due tipi di punto singolare.

In un punto singolare, la curva non ha una tangente ben definita, e questo impedisce la buona definizione della legge di gruppo. Nel resto del capitolo, se non specificato, la curva ellittica si intende non singolare.

Un'ultima, importante osservazione. Se la curva ellittica è definita su un campo finito, logicamente avrà un numero finito di punti. Una stima di quanti siano effettivamente questi punti è data dal seguente teorema, di cui rimandiamo la dimostrazione: è necessario avere a disposizione qualche strumento in più.

Teorema 2.4 (Hasse)**.** *Sia* $E/_{\mathbb{F}_q}$ *una curva ellittica definita sul campo finito* $\mathbb{F}_q$*. Allora*

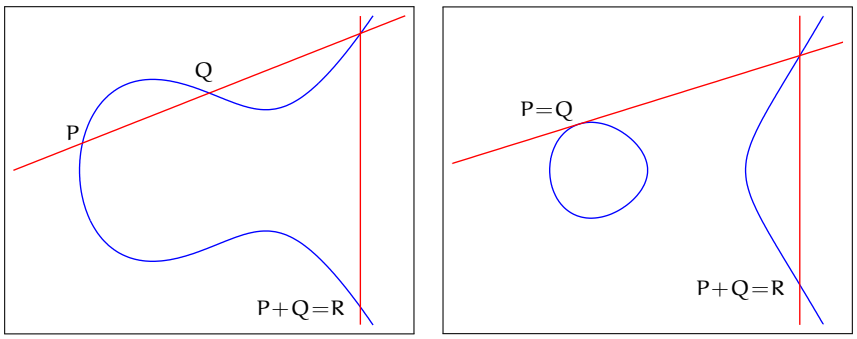
$$|\#E - (q+1)| \leqslant 2\sqrt{q}.$$

2.2 Legge di gruppo

Siano $E/_{\mathbb{K}}$ una curva ellittica e A un suo punto fissato. Siano P e Q due suoi punti; sia ℓ la retta che passa per P e Q, e sia R' il terzo punto di intersezione di ℓ con E. Sia ora ℓ' la retta passante per A e R', e sia R il terzo punto di intersezione di ℓ' con E. Definiamo

$$P + Q := R.$$

Si può dimostrare che la scelta del punto A è del tutto arbitraria. Normalmente viene scelto $A = O$: in questo modo i conti risultano notevolmente ridotti.



(a) Caso $P \neq Q$. (b) Caso $P = Q$.

Figura 2.3: Somma di punti.

Teorema 2.5. $(E, +)$ *è un gruppo abeliano, con* O *come elemento neutro.*

Dimostrazione. Mostriamo che $(E, +)$ soddisfa gli assiomi di gruppo.

Chiusura. Scrivendo esplicitamente le formule per il calcolo delle coordinate della somma di punti, si può notare che esse coinvolgono solo operazioni di campo. Quindi il punto risultante sta ancora in $E/_{\mathbb{K}}$.

Elemento neutro. Il punto all'infinito O è l'elemento neutro della somma. Dato un punto P, la retta passante per P e per O incontra la curva nell'unico altro punto P' che ha la stessa ascissa di P. La retta passante per P' e per O, chiaramente, incontra la curva in P. Quindi $P + O = P$.

Elemento inverso. Procedendo come per l'elemento neutro, si vede che l'inverso di un punto P è il punto P' con la stessa ascissa di P.

Commutatività. La retta che passa per P e per Q è la stessa che passa per Q e P.

Associatività. La dimostrazione dell'associatività richiede strumenti un po' più avanzati che saranno introdotti in seguito; è possibile trovarla nella sezione 2.8.

□

Nel caso in cui $P = Q$, si prende la retta tangente alla curva in P. Questa definizione di somma fa sì che per P, Q e R allineati si abbia

$$P + Q + R = O.$$

Naturalmente, avendo mostrato che i punti della curva ellittica formano un gruppo abeliano, possiamo descrivere la struttura di $\mathbb{Z}$-modulo: se $m \in \mathbb{Z}$

$$mP := \begin{cases} \underbrace{P + \cdots + P}_{m \text{ volte}} & \text{se } m > 0 \\ O & \text{se } m = 0 \\ \underbrace{-P - \cdots - P}_{-m \text{ volte}} & \text{se } m < 0. \end{cases}$$

Vediamo per curiosità le formule esplicite per calcolare $R = (x_3, y_3)$, somma di $P = (x_1, y_1)$ e $Q = (x_2, y_2)$; la loro scrittura è un semplice conto:

$$\begin{cases} x_3 = m^2 + a_1 m - a_2 - x_1 - x_2 \\ y_3 = -(m + a_1)x_3 - q - a_3, \end{cases}$$

dove $y = mx + q$ è la retta passante per P e Q (tangente se $P = Q$), con

$$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{se } P \neq Q \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{se } P = Q \end{cases}$$

$$q = y_1 - mx_1.$$

2.3 Una prima applicazione: la fattorizzazione

Come abbiamo visto, le formule per il calcolo della somma di due punti coinvolgono delle divisioni. Nel caso in cui l'anello di definizione della curva non sia un campo (e quindi, in realtà, non potremmo parlare propriamente di curva ellittica), queste divisioni potrebbero non essere possibili, a causa ad esempio della presenza di zero-divisori. Vediamo come usare questa impossibilità a nostro vantaggio.

Supponiamo di voler fattorizzare un numero n. Tra gli algoritmi a nostra disposizione, abbiamo l'*algoritmo* $p-1$ *di Pollard*, che si basa sul concetto di numero B-liscio.

Definizione 2.6. Sia B un intero positivo. Un intero n è detto B-*liscio* se tutti i suoi fattori primi sono minori o uguali a B.

L'idea dietro l'algoritmo è la seguente. Consideriamo un intero B e sia $Q := \text{mcm}\{q^t \mid q \text{ primo}, q \leqslant B,\ q^t \leqslant n\}$. Se $q^\ell \leqslant n$, si ha $\ell \leqslant \left\lfloor \frac{\ln n}{\ln q} \right\rfloor$, quindi

$$Q = \prod_{q \leqslant B} q^{\left\lfloor \frac{\ln n}{\ln q} \right\rfloor}$$

dove il prodotto è su tutti i primi $q \leqslant B$. Se p è un fattore primo di n tale che $p-1$ sia B-liscio, allora $p-1 \mid Q$ per definizione di Q; quindi, per ogni a tale che $\text{MCD}(a,p) = 1$, per il piccolo teorema di Fermat $a^Q \equiv 1 \pmod{p}$. Detto $d := \text{MCD}(a^Q - 1, n)$, si ha che $p \mid d$, e se $d \neq 1$ e $d \neq n$, abbiamo trovato un fattore non banale di n.

Il problema principale di quest'algoritmo è rappresentato dal fatto che è *one-shot*: se l'algoritmo fallisce, dobbiamo cercare altre soluzioni. L'adattamento alle curve ellittiche (che prende il nome di *algoritmo per fattorizzazione sulle curve ellittiche di Lenstra*) supera quest'ostacolo: in caso di fallimento, è sufficiente cambiare curva e/o punto di partenza.

Indichiamo per brevità con $\mathbb{Z}_n$ l'anello $\mathbb{Z}/(n)$. Considerando una *pseudo-curva ellittica*, cioè una curva ellittica definita su $\mathbb{Z}_n$, il calcolo di kP a un certo punto potrebbe fallire. Questo è un vantaggio per noi: il calcolo fallisce quando si è trovato uno zero-divisore in $\mathbb{Z}_n$, sostanzialmente un divisore di n.

Più in dettaglio, il calcolo di kP richiede la divisione tra classi di resto modulo n, che può essere compiuta tramite l'algoritmo euclideo esteso. In particolare, la divisione per un certo v modulo n richiede il calcolo di $\text{MCD}(v,n)$. Ora, se $\text{MCD}(v,n) = 1$, non ci sono problemi, perché v è invertibile. Anche se $v \equiv 0 \pmod{n}$ non ci sono problemi, perché il risultato della somma sarà il punto

all'infinito. Se invece $\mathrm{MCD}(v, n) \neq 1$ oppure n, la divisione non può essere svolta, e abbiamo trovato un fattore non banale di n.

1. Scegliamo un'equazione del tipo $y^2 = x^3 + ax + b$ in $\mathbb{Z}_n$, e un punto P.

2. Calcoliamo $eP \in E/_{\mathbb{Z}_n}$, dove e è prodotto di molti numeri piccoli, per esempio prodotto di potenze di primi piccoli, oppure $B!$ per qualche B non troppo grande: si può fare efficientemente calcolando $(2!)P$, $(3!)P = 3(2!)P$, e così via.

3. - Se siamo riusciti a compiere tutte le operazioni, proviamo qualche altra curva e/o qualche altro punto di partenza.
   - Se abbiamo trovato $kP = O$ in qualche fase, dato che O è elemento neutro, l'iterazione non ci sposta da O, quindi dobbiamo cambiare curva e/o punto di partenza.
   - Se a un certo punto abbiamo $\mathrm{MCD}(v, n) \neq 1$ oppure n, abbiamo trovato un fattore non banale di n.

2.4 Endomorfismi di curve ellittiche

Il nostro obiettivo è la dimostrazione del teorema di Hasse. Per fare ciò dobbiamo in primo luogo stabilire cosa si intende per endomorfismi di una curva ellittica.

Definizione 2.7. Sia $E/_{\mathbb{K}}$ una curva ellittica. Un *endomorfismo* di E è una mappa $\alpha : E(\overline{\mathbb{K}}) \longrightarrow E(\overline{\mathbb{K}})$ tale che

- sia un omomorfismo di gruppi: per ogni $P_1, P_2 \in E(\overline{\mathbb{K}})$ si ha $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$;

- sia definita da funzioni razionali: esistono $R_1, R_2 \in \overline{\mathbb{K}}(X, Y)$ funzioni razionali tali che per ogni $(x, y) \in E(\overline{\mathbb{K}})$ si abbia $\alpha(x, y) = (R_1(x, y), R_2(x, y))$.

Sistemeremo a breve i dettagli tecnici che sorgono qualora esistano punti di $E(\overline{\mathbb{K}})$ in cui le funzioni razionali non siano definite.

Osservazione. Sulla scia dell'osservazione in apertura di capitolo, potremmo definire endomorfismo di E come un morfismo di varietà proiettive da $E(\overline{\mathbb{K}})$ in sé che manda O in sé (si veda sempre [14]). Ancora una volta per i nostri scopi sarà sufficiente la definizione data.

Ad esempio, supponiamo che $E/_{\mathbb{K}}$ sia data dall'equazione $y^2 = x^3 + ax + b$. La mappa di moltiplicazione $\alpha(P) = 2P$ è un endomorfismo con

$$\begin{cases} R_1(X,Y) = \left(\dfrac{3X^2+a}{2Y}\right)^2 - 2X \\ R_2(X,Y) = \left(\dfrac{3X^2+a}{2Y}\right)\left(3X - \left(\dfrac{3X^2+a}{2Y}\right)^2\right) - Y. \end{cases}$$

Possiamo scrivere in una forma più comoda le funzioni razionali che definiscono un endomorfismo. Infatti, sia $R(X,Y) \in \overline{\mathbb{K}}(X,Y)$: sfruttando l'equazione di Weierstrass eliminiamo tutte le potenze di Y maggiori o uguali alla seconda, pertanto possiamo supporre

$$R(X,Y) = \frac{p_1(X) + p_2(X)Y}{p_3(X) + p_4(X)Y}$$

con $p_1, p_2, p_3, p_4 \in \overline{\mathbb{K}}[X]$. Inoltre, moltiplicando e dividendo per $p_3(X) - p_4(X)Y$ e utilizzando ancora l'equazione di Weierstrass possiamo ulteriormente assumere

$$R(X,Y) = \frac{q_1(X) + q_2(X)Y}{q_3(X)} \tag{2.4}$$

con $q_1, q_2, q_3 \in \overline{\mathbb{K}}[X]$. Ora, se α è un endomorfismo di E, abbiamo le funzioni razionali R_1, R_2 che lo definiscono; imponendo

$$\alpha(-P) = -\alpha(P)$$

per le proprietà di omomorfismo si ricava che, avendo scritto R_1 come in (2.4), il corrispondente q_2 dev'essere nullo, e analogamente dopo aver scritto R_2 come in (2.4), in quel caso q_1 dev'essere nullo. Alla fine otteniamo

$$\alpha(x,y) = (r_1(x), r_2(x)y)$$

con $r_1, r_2 \in \overline{\mathbb{K}}(X)$. A questo punto vediamo cosa capita quando una delle due funzioni razionali non è definita. Scriviamo $r_1 = p_1/q_1$, $r_2 = p_2/q_2$ con p_1, q_1 polinomi coprimi e p_2, q_2 idem. Se $q_1(x) = 0$ per qualche punto $P = (x,y)$, diciamo che $\alpha(P) = O$. Se invece $q_1(x) \neq 0$, allora anche $q_2(x) \neq 0$ in base al lemma seguente: di conseguenza $\alpha(P)$ è un punto ben definito.

Lemma 2.8. *Sia* $\alpha(x,y) = (p(x)/q(x), ys(x)/t(x))$ *un endomorfismo della curva* E *definita da* $y^2 = x^3 + ax + b$ *e supponiamo che* p *e* q *siano polinomi coprimi così come* s *e* t. *Se* $t(x_0) = 0$, *allora* $q(x_0) = 0$.

Dimostrazione. Dal fatto che $\alpha(x,y) \in E$ otteniamo

$$y^2 \frac{s(x)^2}{t(x)^2} = \frac{p(x)^3}{q(x)^3} + a\frac{p(x)}{q(x)} + b$$

e sostituendo $y^2 = x^3 + ax + b$ ricaviamo

$$\frac{(x^3 + ax + b)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3} \tag{2.5}$$

con $u(X) := p(X)^3 + ap(X)q(X)^2 + bq(X)^3$. Notiamo che u e q non hanno radici comuni (una loro eventuale radice comune sarebbe radice anche di p).

Sia ora x_0 tale che $t(x_0) = 0$. Il polinomio t^2 ha solo radici multiple, mentre $X^3 + aX + b$ non ne ha affatto; inoltre $X - x_0$ non divide $s(X)$ (per coprimalità di s e t). Quindi, dopo aver ridotto il membro di sinistra in (2.5) ai minimi termini, si ha che $X - x_0$ ne divide il denominatore ma non il numeratore. Di conseguenza, moltiplicando in croce l'equazione (2.5), otteniamo che $X - x_0$ divide il prodotto $(x^3 + ax + b)s(x)^2q(X)^3$ e quindi divide $q(X)$. □

Definizione 2.9. Sia $\alpha \neq 0$ un endomorfismo di E definito da

$$\alpha(x,y) = (r_1(x), yr_2(x))$$

con $r_1(X) = p(X)/q(X)$ ridotta ai minimi termini. Definiamo *grado* di α la quantità

$$\deg(\alpha) := \max\{\deg(p), \deg(q)\}.$$

Conveniamo che $\deg(0) = 0$.

Definizione 2.10. Sia $\alpha \neq 0$ come sopra. Diciamo che α è *separabile* se $r_1'(X) \neq 0$.

Osservazione. Se $\mathrm{char}(\mathbb{K}) = 0$, un endomorfismo (non nullo) è sempre separabile: vedremo a breve che un endomorfismo non nullo è suriettivo, mentre le uniche funzioni razionali su $\mathbb{K}$ con derivata nulla sono le costanti.

Definizione 2.11. Sia $E/_{\mathbb{F}_q}$ una curva ellittica definita su $\mathbb{F}_q$. La mappa

$$\begin{array}{rccc} \varphi_q : & E(\overline{\mathbb{F}_q}) & \longrightarrow & E(\overline{\mathbb{F}_q}) \\ & (x,y) & \longmapsto & (x^q, y^q) \end{array}$$

è detta *endomorfismo di Frobenius*.

Lemma 2.12. *L'endomorfismo di Frobenius è effettivamente un endomorfismo di* $E/_{\mathbb{F}_q}$*, non separabile, di grado* q.

Dimostrazione. È ovvio che la mappa sia definita da funzioni razionali (anzi, polinomi) ed abbia grado q. È altrettanto ovvio che non sia separabile, in quanto $(X^q)' = qX^{q-1} = 0$ in $\mathbb{F}_q$. Occorre solo mostrare che φ_q sia un omomorfismo di gruppi, ma questa è una semplice verifica a partire dalle formule esplicite di addizione tra punti. □

Proposizione 2.13. *Sia $\alpha \neq 0$ un endomorfismo di una curva ellittica $E/_{\mathbb{K}}$.*

- *Se α è separabile, allora* $\deg(\alpha) = \#\ker(\alpha)$*;*
- *Se α non è separabile, allora* $\deg(\alpha) > \#\ker(\alpha)$.

Dimostrazione. Per fissare le notazioni, sia $\alpha(x, y) = (r_1(x), yr_2(x))$ con $r_1(X) = p(X)/q(X)$. Inoltre notiamo che è sufficiente studiare la controimmagine di un punto qualsiasi, dato che le classi laterali del ker hanno la stessa cardinalità.

Supponiamo dapprima che α sia separabile, cosicché $p'q - pq'$ non sia il polinomio nullo. Definiamo

$$S := \{x \in \overline{\mathbb{K}} \mid (p'(x)q(x) - p(x)q'(x))q(x) = 0\}$$

e sia $(a, b) \in E(\overline{\mathbb{K}})$ tale che

1. $a \neq 0$, $b \neq 0$, $(a, b) \neq O$;
2. $\deg(p(X) - aq(X)) = \max\{\deg(p), \deg(q)\} = \deg(\alpha)$;
3. $a \notin r_1(S)$;
4. $(a, b) \in \alpha(E(\overline{\mathbb{K}}))$.

Un tale punto esiste sempre: infatti $\{r_1(x) \mid x \in \overline{\mathbb{K}}\}$ è un insieme infinito (per ogni t l'insieme $r_1^{-1}(t)$ è finito) e in corrispondenza di ogni x esiste un y tale che $(x, y) \in E(\overline{\mathbb{K}})$, quindi $\alpha(E(\overline{\mathbb{K}}))$ è un insieme infinito e abbiamo a disposizione infinite scelte per (a, b) che soddisfi 4. D'altra parte, S è un insieme finito, quindi gli a che non soddisfano 3. sono finiti; ovviamente sono finiti anche gli (a, b) che non soddisfano 1., e solo un a non soddisfa la 2. (quello che eventualmente cancellerebbe i termini di testa di p e q).

Abbiamo concluso se dimostriamo che esattamente $\deg(\alpha)$ punti (x, y) sono tali che $\alpha(x, y) = (a, b)$. Per tali punti si ha

$$\frac{p(x)}{q(x)} = a, \quad yr_2(x) = b.$$

Dal momento che $(a, b) \neq O$, $q(x) \neq 0$ e quindi $r_2(x)$ è definito per il lemma 2.8. Quindi (ricordando che $b \neq 0$) abbiamo $y = b/r_2(x)$: in altre parole il valore di x determina quello di y; perciò ci limiteremo a contare i possibili valori di x.

Per l'ipotesi 2., $p(X) - \alpha q(X)$ ha esattamente $\deg(\alpha)$ radici contate con molteplicità: dimostriamo allora che non ha radici multiple. Se per assurdo x_0 fosse una radice multipla, si avrebbe

$$p(x_0) - \alpha q(x_0) = 0, \quad p'(x_0) - \alpha q'(x_0) = 0,$$

da cui si deduce

$$\alpha p'(x_0)q(x_0) = \alpha p(x_0)q'(x_0).$$

Ma $\alpha \neq 0$, quindi x_0 è radice di $p'q - pq'$, pertanto $x_0 \in S$: in tal caso $\alpha = r_1(x_0) \in r_1(S)$ in contraddizione con l'ipotesi 3. Questo conclude la prima parte della proposizione.

Se α non è separabile, si possono ripetere tutti i passaggi precedenti (ad eccezione di quelli che riguardano S), con la differenza che stavolta $p' - \alpha q'$ è il polinomio nullo, quindi tutte le radici di $p - \alpha q$ sono multiple. Da ciò segue la tesi. □

Teorema 2.14. *Un endomorfismo di* E *non nullo è suriettivo.*

Dimostrazione. Sia α come nella proposizione precedente e sia $(z, w) \in E(\overline{\mathbb{K}})$. Dato che $\alpha(O) = O$, possiamo assumere $(z, w) \neq O$.

Se $p(X) - zq(X)$ non è una costante, sia x_0 una sua radice. I polinomi p e q non hanno radici comuni, quindi dev'essere $q(x_0) \neq 0$. Sia $y_0 \in \overline{\mathbb{K}}$ una qualunque delle due radici quadrate di $x_0^3 + ax_0 + b$. Per il lemma 2.8 è definito il punto $\alpha(x_0, y_0)$ e per costruzione esso è uguale a un punto $(z, \tilde{w})$ con $\tilde{w}^2 = z^3 + az + b = w^2$: quindi $\tilde{w} = \pm w$. Se $\tilde{w} = w$, abbiamo finito; altrimenti, $\alpha(x_0, -y_0) = (z, -\tilde{w}) = (z, w)$.

Ora mostriamo che esiste al più uno z per cui $p(X) - zq(X)$ sia costante. Innanzitutto non può capitare che $p(X)$ e $q(X)$ siano entrambi costanti, visto che in tal caso l'immagine di α consisterebbe in al più due punti e la controimmagine di un punto è un insieme finito (mentre il dominio $E(\overline{\mathbb{K}})$ è infinito). Se esistessero $z \neq \tilde{z}$ tali che $p(X) - zq(X)$ e $p(X) - \tilde{z}q(X)$ siano costanti, allora lo sarebbero anche sia $(\tilde{z} - z)q = (p - zq) - (p - \tilde{z}q)$ che $(\tilde{z} - z)p = \tilde{z}(p - zq) - z(p - \tilde{z}q)$, in contraddizione con quanto visto prima.

Di conseguenza, esistono al più due punti che non appartengono all'immagine di α, che sono (z, w) e $(z, -w)$ con z tale che $p - zq$ sia costante e w opportuno. Sia allora (z_1, w_1) un qualsiasi altro punto di $E(\overline{\mathbb{K}})$ e sia $P_1 \in E(\overline{\mathbb{K}})$ tale che

$\alpha(P_1) = (z_1, w_1)$. Possiamo scegliere (z_1, w_1) in modo che $(z_1, w_1) + (z, w) \neq (z, \pm w)$, dunque esiste P_2 tale che $\alpha(P_2) = (z_1, w_1) + (z, w)$. Ne segue che $\alpha(P_2 - P_1) = (z, w)$ e $\alpha(P_1 - P_2) = (z, -w)$. Possiamo concludere che α è suriettiva. □

Vediamo un criterio di separabilità che ci sarà utile per le future applicazioni. Se (x, y) è un punto variabile su una curva ellittica definita da $y^2 = x^3 + ax + b$, possiamo considerare la derivata di y rispetto a x e ottenere

$$2yy' = 3x^2 + a.$$

Analogamente, se $f(x, y)$ è una funzione razionale, possiamo considerare

$$\frac{d}{dx} f(x, y) = \frac{\partial f}{\partial x}(x, y) + \frac{\partial f}{\partial y}(x, y)y'.$$

Lemma 2.15. *Sia $(u, v) \in E$ un punto fissato e consideriamo la somma*

$$(x, y) + (u, v) = (f(x, y), g(x, y)).$$

Come abbiamo visto, le coordinate della somma sono funzioni razionali in x e y. Vale che

$$\frac{\frac{d}{dx} f(x, y)}{g(x, y)} = \frac{1}{y}.$$

Dimostrazione. La dimostrazione è un (lungo e noioso) conto a partire dalle formule di addizione dei punti, che sfrutta

$$\frac{dy}{dx} = \frac{3x^2 + a}{2y}$$

e il fatto che (x, y) e (u, v) siano punti di E. □

Lemma 2.16. *Siano $\alpha_1, \alpha_2, \alpha_3$ endomorfismi di E tali che $\alpha_1 + \alpha_2 = \alpha_3$. (Ovviamente la somma di endomorfismi è definita puntualmente.) Scriviamo*

$$\alpha_j(x, y) = (R_j(x), yS_j(x))$$

per $j = 1, 2, 3$, con R_j, S_j funzioni razionali. Supponiamo che esistano costanti c_1, c_2 tali che

$$\frac{R_1'(x)}{S_1(x)} = c_1, \quad \frac{R_2'(x)}{S_2(x)} = c_2.$$

Allora

$$\frac{R_3'(x)}{S_3(x)} = c_1 + c_2.$$

Dimostrazione. Sia

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$$

dove $(x_1, y_1) = \alpha_1(x, y)$ e $(x_2, y_2) = \alpha_2(x, y)$. Dal lemma 2.15 ricaviamo

$$\frac{\partial x_3}{\partial x_1} + \frac{\partial x_3}{\partial y_1}\frac{dy_1}{dx_1} = \frac{y_3}{y_1}, \quad \frac{\partial x_3}{\partial x_2} + \frac{\partial x_3}{\partial y_2}\frac{dy_2}{dx_2} = \frac{y_3}{y_2}.$$

Per ipotesi

$$\frac{dx_i}{dx} = R_j'(x) = c_j S_j(x) = c_j \frac{y_j}{y}$$

per $j = 1, 2$. A questo punto, secondo le regole di derivazione di funzioni composte

$$\begin{aligned}\frac{dx_3}{dx} &= \frac{\partial x_3}{\partial x_1}\frac{dx_1}{dx} + \frac{\partial x_3}{\partial y_1}\frac{dy_1}{dx_1}\frac{dx_1}{dx} + \frac{\partial x_3}{\partial x_2}\frac{dx_2}{dx} + \frac{\partial x_3}{\partial y_2}\frac{dy_2}{dx_2}\frac{dx_2}{dx} = \\ &= \frac{y_3}{y_1}\frac{y_1}{y}c_1 + \frac{y_3}{y_2}\frac{y_2}{y}c_2 = \\ &= (c_1 + c_2)\frac{y_3}{y}.\end{aligned}$$

Dividendo per y_3/y si ha la tesi. □

Proposizione 2.17. *Siano* E *una curva ellittica definita su un campo* $\mathbb{K}$ *e* $n \neq 0$ *un intero. Supponiamo che la moltiplicazione per* n *sia data da*

$$n(x, y) = (R_n(x), yS_n(x)).$$

Allora $R_n'(x)/S_n(x) = n$*; in particolare la moltiplicazione per* n *è separabile se e solo se* $\mathrm{char}(\mathbb{K})$ *non divide* n*.*

Dimostrazione. Innanzitutto osserviamo che è sufficiente dimostrare la proposizione per $n > 0$, in quanto $R_{-n} = R_n$ e $S_{-n} = -S_n$, quindi $R_{-n}'/S_{-n} = -R_n'/S_n$.

Ora, per $n = 1$ la proposizione è banalmente vera; supponiamo che sia vera per n: il lemma 2.16 garantisce che sia vera anche per $n + 1$, che è la somma di n e 1. Per induzione, la proposizione è vera per ogni n.

Per quanto riguarda la separabilità, abbiamo che la moltiplicazione per n è separabile se e solo se $R_n'(x) \neq 0$, o equivalentemente $R_n'(x)/S_n(x) = n \neq 0$, e questo accade se e solo se $\mathrm{char}(\mathbb{K})$ non divide n. □

Proposizione 2.18. *Sia* $E/_{\mathbb{F}_q}$ *una curva ellittica su* $\mathbb{F}_q$ *con* $\mathrm{char}(\mathbb{F}_q) = p$ *e siano* r, s *due interi non entrambi nulli. Sia inoltre* φ_q *l'endomorfismo di Frobenius. Allora* $r\varphi_q + s$ *è separabile se e solo se* p *non divide* s*.*

Dimostrazione. Scriviamo la moltiplicazione per r come $r(x,y) = (R_r(x), yS_r(x))$. Notiamo inoltre che tale endomorfismo commuta con φ_q (per definizione, un endomorfismo di moltiplicazione commuta con qualunque altro endomorfismo). Abbiamo allora

$$(R_{r\varphi_q}(x), yS_{r\varphi_q}(x)) = \varphi_q(r(x,y)) = (R_r(x)^q, y^q S_r(x)^q)$$

e quindi

$$\frac{R'_{r\varphi_q}(x)}{S_{r\varphi_q}(x)} = \frac{qR_r(x)^{q-1}R'_r(x)}{S_{r\varphi_q}(x)} = 0.$$

Segue dal lemma 2.16 che

$$\frac{R'_{r\varphi_q+s}(x)}{S_{r\varphi_q+s}(x)} = s$$

da cui si conclude che $r\varphi_q + s$ è separabile se e solo se p non divide s. □

2.5 Punti di torsione

Nello studio delle curve ellittiche rivestono un ruolo di grande importanza i *punti di torsione* della curva, cioè i punti che hanno ordine finito. In questa sezione supporremo sempre di poter scrivere l'equazione di Weierstrass nella forma $y^2 = x^3 + ax + b$.

Definizione 2.19. Sia $E/_{\mathbb{K}}$ una curva ellittica. Sia inoltre $n \in \mathbb{N} \setminus \{0\}$. Chiamiamo *punti di* n*-torsione* i punti della curva $E(\overline{\mathbb{K}})$ di ordine n. L'insieme dei punti di n-torsione è indicato con

$$E[n] := \{P \in E(\overline{\mathbb{K}}) \mid nP = O\}.$$

Ovviamente i punti di n-torsione formano un sottogruppo. Il teorema a cui vogliamo arrivare riguarda la determinazione della classe di isomorfismo di questo sottogruppo: ne presentiamo qui l'enunciato e giungeremo alla sua dimostrazione nel corso della sezione.

Teorema 2.20. *Sia* $E/_{\mathbb{K}}$ *una curva ellittica e sia* $n \in \mathbb{N} \setminus \{0\}$. *Se* $\mathrm{char}(\mathbb{K})$ *è zero oppure non divide* n, *allora*

$$E[n] \simeq {}^{\mathbb{Z}}/_{(n)} \oplus {}^{\mathbb{Z}}/_{(n)}.$$

Se invece $\mathrm{char}(\mathbb{K}) = p$ *e* $n = p^r m$ *con* $r \geqslant 1$ *e* $\mathrm{MCD}(p, m) = 1$, *allora*

$$E[n] \simeq {}^{\mathbb{Z}}/_{(m)} \oplus {}^{\mathbb{Z}}/_{(m)} \text{ oppure } E[n] \simeq {}^{\mathbb{Z}}/_{(n)} \oplus {}^{\mathbb{Z}}/_{(m)}.$$

Una curva $E/_{\mathbb{K}}$ con $\mathrm{char}(\mathbb{K}) = p$ è detta *ordinaria* se $E[p] \simeq \mathbb{Z}/_{(p)}$, *supersingolare* se $E[p] \simeq 0$. (Per le curve supersingolari vedi anche la sezione 2.9.)

Per studiare i punti di torsione, occorre dettagliare meglio la mappa di moltiplicazione per un intero. Iniziamo a definire i *polinomi di divisione* $\psi_m \in \mathbb{Z}[X, Y, A, B]$ come

$$\begin{aligned}
&\psi_0 && := 0\\
&\psi_1 && := 1\\
&\psi_2 && := 2Y\\
&\psi_3 && := 3X^4 + 6AX^2 + 12BX - A^2\\
&\psi_4 && := 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3)\\
\text{per } m \geqslant 2,\quad &\psi_{2m+1} && := \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3\\
\text{per } m \geqslant 3,\quad &\psi_{2m} && := (2Y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)
\end{aligned}$$

Lemma 2.21. *I polinomi ψ_n appartengono a $\mathbb{Z}[X, Y^2, A, B]$ per n dispari, mentre appartengono a $2Y\mathbb{Z}[X, Y^2, A, B]$ per n pari.*

Dimostrazione. Per $n \leqslant 4$ è evidente; procediamo per induzione. Supponiamo che la tesi sia vera per ogni $n < 2m$ e mostriamo che è vera anche per $n = 2m$ e $n = 2m + 1$. Possiamo assumere che $2m > 4$, quindi $2m > m + 2$, dunque tutti i polinomi che compaiono nella definizione di ψ_{2m} verificano l'ipotesi induttiva. Se m è pari, ψ_m, ψ_{m+2} e ψ_{m-2} stanno in $2Y\mathbb{Z}[X, Y^2, A, B]$, quindi anche ψ_{2m} vi appartiene. Se m è dispari, si giunge alla stessa conclusione notando che ψ_{m-1} e ψ_{m+1} sono in $2Y\mathbb{Z}[X, Y^2, A, B]$. Per $n = 2m + 1$ il ragionamento è analogo. □

A partire dai polinomi ψ_n definiamo

$$\begin{aligned}
\varphi_m &:= X\psi_m^2 - \psi_{m+1}\psi_{m-1}\\
\omega_m &:= (4Y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).
\end{aligned}$$

Lemma 2.22. *I polinomi φ_n appartengono a $\mathbb{Z}[X, Y^2, A, B]$ per ogni n. I polinomi ω_n appartengono a $Y\mathbb{Z}[X, Y^2, A, B]$ per n dispari, mentre appartengono a $\mathbb{Z}[X, Y^2, A, B]$ per n pari.*

Dimostrazione. Se n è dispari, ψ_{n-1} e ψ_{n+1} appartengono a $Y\mathbb{Z}[X, Y^2, A, B]$, quindi il loro prodotto sta in $\mathbb{Z}[X, Y^2, A, B]$. Segue che $\varphi_n \in \mathbb{Z}[X, Y^2, A, B]$ per n dispari. Per n pari il procedimento è analogo.

Ricalcando la dimostrazione del lemma 2.21 si ottiene facilmente che $Y^{-1}\omega_n \in \mathbb{Z}[X, Y^2, A, B]$ per n dispari e $\omega_n \in \frac{1}{2}\mathbb{Z}[X, Y^2, A, B]$ per n pari. La tesi discende facilmente con un conto: è possibile trovare la traccia in [15]. □

Ora aggiungiamo all'anello $\mathbb{Z}[X, Y^2, A, B]$ la relazione $Y^2 - X^3 - AX - B$, in modo da considerare i polinomi definiti sopra come appartenenti a $\mathbb{Z}[X, A, B]$.

Lemma 2.23. *Visti come polinomi in* X*, si ha che* $\mathrm{lt}(\varphi_n) = X^{n^2}$ *e* $\mathrm{lt}(\psi_n^2) = n^2 X^{n^2-1}$.

Dimostrazione. Si dimostra facilmente per induzione (vedi [15]) che

$$\psi_n(X) = \begin{cases} Y(nX^{(n^2-4)/2} + \dots) & \text{se } n \text{ è pari} \\ nX^{(n^2-1)/2} + \dots & \text{se } n \text{ è dispari.} \end{cases}$$

Da questo segue la tesi. □

Tutto questo ci permette infine di scrivere esplicitamente l'endomorfismo di moltiplicazione per n in termini di funzioni razionali. La dimostrazione del teorema seguente è omessa.

Teorema 2.24. *Sia* $P = (x, y)$ *un punto di una curva ellittica* $E/_{\mathbb{K}}$ *con* $\mathrm{char}(\mathbb{K}) \neq 2$*, data da* $y^2 = x^3 + ax + b$*. Sia* n *un intero. Allora*

$$nP = \left(\frac{\varphi_n(x)}{\psi_n(x)^2}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3} \right)$$

dove si è inoltre valutato A *con* a *e* B *con* b*.*

Corollario 2.25. *Il grado della mappa di moltiplicazione per* n *è* n^2*.*

Dimostrazione. Dal lemma 2.23, abbiamo che il massimo dei gradi di φ_n e ψ_n^2 è n^2. Abbiamo concluso se dimostriamo che tali polinomi non hanno radici comuni (cioè φ_n/ψ_n^2 è ridotta ai minimi termini).

Supponiamo che esista un indice per cui φ_n e ψ_n^2 abbiamo una radice in comune. Sia n il minimo indice per cui ciò accade. Distinguiamo i casi n pari ed n dispari.

Se $n = 2m$, un semplice conto mostra che

$$\varphi_2(X) = X^4 - 2AX^2 - 8BX + A^2, \quad \psi_2(X)^2 = 4Y^2 = 4(X^3 + AX + B).$$

Quindi, calcolando $n(x, y) = 2m(x, y) = 2(m(x, y))$ otteniamo

$$\begin{aligned} \frac{\varphi_{2m}}{\psi_{2m}^2} &= \frac{\varphi_2(\varphi_m/\psi_m^2)}{\psi_2(\varphi_m/\psi_m^2)^2} = \\ &= \frac{\varphi_m^4 - 2A\varphi_m^2\psi_m^4 - 8B\varphi_m\psi_m^6 + A^2\psi_m^8}{(4\psi_m^2)(\varphi_m^3 + A\varphi_m\psi_m^4 + B\psi_m^6)}. \end{aligned}$$

Chiamiamo U e V rispettivamente il numeratore e il denominatore dell'espressione precedente. Una semplice applicazione dell'algoritmo euclideo mostra che, detti

$$\begin{aligned}
\Delta &:= 4A^3 + 27B^2 \\
F(X,Z) &:= X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4 \\
G(X,Z) &:= 4Z(X^3 + AXZ^2 + BZ^3) \\
f_1(X,Z) &:= 12X^2Z + 16AZ^3 \\
g_1(X,Z) &:= 3X^3 - 5AXZ^2 - 27BZ^3 \\
f_2(X,Z) &:= 4\Delta X^3 - 4A^2BX^2Z + 4A(3A^3 + 22B^2)XZ^2 + 12B(A^3 + 8B^2)Z^3 \\
g_2(X,Z) &:= A^2BX^3 + A(5A^3 + 32B^2)X^2Z + 2B(13A^3 + 96B^2)XZ^2 \\
&\qquad \underline{-3A^2}(A^3 + 8B^2)Z^3,
\end{aligned}$$

si ha $Ff_1 - Gg_1 = 4\Delta Z^7$ e $Ff_2 + Gg_2 = 4\Delta X^7$. Dunque

$$\begin{aligned}
Uf_1(\varphi_m, \psi_m^2) - Vg_1(\varphi_m, \psi_m^2) &= 4\psi_m^{14}\Delta \\
Uf_2(\varphi_m, \psi_m^2) + Vg_2(\varphi_m, \psi_m^2) &= 4\psi_m^7\Delta.
\end{aligned}$$

Se U e V avessero una radice in comune, l'avrebbero anche φ_m e ψ_m^2, ma questo è impossibile perché il primo indice per cui capita è $n = 2m$.

Resta da dimostrare che in effetti $U = \varphi_{2m}$ e $V = \psi_{2m}^2$. Dato che $U/V = \varphi_{2m}/\psi_{2m}^2$, e dato che U e V non hanno radici comuni, abbiamo che φ_{2m} è multiplo di U e ψ_{2m}^2 è multiplo di V. Un rapido calcolo usando il lemma 2.23 mostra che $\mathrm{lt}(U) = X^{4m^2}$ da cui deduciamo che $U = \varphi_{2m}$ e quindi $V = \psi_{2m}^2$. Questo termina il caso in cui n è pari.

Ora supponiamo che $n = 2m + 1$ e sia r una radice comune a φ_n e ψ_n^2. Dalla definizione di φ_n valutata in r abbiamo che $(\psi_{n+1}\psi_{n-1})(r) = 0$. Di conseguenza si ha che almeno uno tra ψ_{n+1} e ψ_{n-1} si annulla in r, quindi $\psi_{n+\delta}(r)^2 = 0$ per almeno uno tra $\delta = 1$ e $\delta = -1$.

Dal momento che n è dispari, sia ψ_n che $\psi_{n+2\delta}$ sono polinomi in X; inoltre $(\psi_n\psi_{n+2\delta})^2 = \psi_n^2\psi_{n+2\delta}^2$ si annulla in r. Perciò $\psi_n\psi_{n+2\delta}$ pure si annulla in r. Dalla definizione segue che anche $\varphi_{n+\delta}$ si annulla in r: tale radice è comune a $\varphi_{n+\delta}$ e $\psi_{n+\delta}^2$. Notiamo che $n + \delta$ è pari: possiamo allora concludere dal caso precedente che esiste una radice comune anche per l'indice $(n + \delta)/2$, e per minimalità di n dev'essere

$$\frac{n + \delta}{2} \geqslant n$$

cioè $n = 1$. Ma chiaramente $\varphi_1 = X$ e $\psi_1^2 = 1$ non hanno radici comuni.

Questo dimostra che in nessun caso φ_n e ψ_n^2 hanno radici in comune. La dimostrazione è così conclusa. □

Siamo ora pronti per la dimostrazione del teorema di struttura per i punti di n-torsione della curva.

Dimostazione del teorema 2.20. Supponiamo dapprima che $\mathrm{char}(\mathbb{K}) = 0$ oppure che non divida n. Dalla proposizione 2.17 abbiamo che la moltiplicazione per n è un endomorfismo separabile. Dal corollario 2.25 e dalla proposizione 2.13 abbiamo che il nucleo di tale moltiplicazione, che è $E[n]$, ha ordine n^2.

Di conseguenza, il teorema di struttura per gruppi abeliani finiti ci assicura che esistono $n_1, \dots, n_k$ tali che n_i divida n_{i+1} e

$$E[n] \simeq \mathbb{Z}/(n_1) \oplus \cdots \oplus \mathbb{Z}/(n_k).$$

Ora, sia ℓ un primo che divida n_1. Questo significa che ℓ divide n_i per ogni i. Quindi $E[\ell] \subseteq E[n]$ ha ordine ℓ^k. Ma per quanto visto $E[\ell]$ ha ordine ℓ^2, quindi $k = 2$. A questo punto notiamo che la moltiplicazione per n manda a O tutti i punti di $E[n] \simeq \mathbb{Z}/(n_1) \oplus \mathbb{Z}/(n_2)$, quindi n_2 deve dividere n. D'altra parte $n^2 = \#E[n] = n_1 n_2$, quindi $n_1 = n_2 = n$ e

$$E[n] \simeq \mathbb{Z}/(n) \oplus \mathbb{Z}/(n).$$

Vediamo il caso in cui $\mathrm{char}(\mathbb{K}) = p$ divida n. Innanzitutto cerchiamo di capire com'è fatto il gruppo dei punti di p^k-torsione. Dai risultati precedenti sappiamo che la moltiplicazione per p non è separabile, quindi $\#\ker(p\cdot) < \deg(p\cdot) = p^2$. Ogni elemento di $E[p]$ ha ordine 1 oppure p, quindi l'ordine di $E[p]$ è una potenza di p, dunque può essere solo 1 oppure p. Se $E[p] = 0$, allora per induzione su k si dimostra che $E[p^k] = 0$ per ogni k. Se invece l'ordine di $E[p]$ è p, dimostriamo che per ogni k si ha $E[p^k] \simeq \mathbb{Z}/(p^k)$ mostrando che $E[p^k]$ è ciclico e che esistono elementi di ordine p^j per ogni j.

Vediamo intanto che $E[p^k]$ è ciclico: sappiamo che è un gruppo abeliano finito, quindi come abbiamo fatto sopra esistono $n_1, \dots, n_s$ tali che n_i divida n_{i+1} e

$$E[p^k] \simeq \mathbb{Z}/(n_1) \oplus \cdots \oplus \mathbb{Z}/(n_s).$$

Ogni elemento di $E[p^k]$ ha ordine che divide p^k, quindi possiamo specificare meglio la struttura: esistono interi $1 \leqslant i_1 \leqslant \dots \leqslant i_s$ tali che

$$E[p^k] \simeq \mathbb{Z}/(p^{i_1}) \oplus \cdots \oplus \mathbb{Z}/(p^{i_s}).$$

Dato che $E[p] \subseteq E[p^k]$, abbiamo che la copia di $E[p]$ in $E[p^k]$ ha ordine almeno p^s, ma sappiamo che $E[p] \simeq \mathbb{Z}/(p)$, quindi $s = 1$ e

$$E[p^k] \simeq \mathbb{Z}/(p^i)$$

per un qualche i. Terminiamo mostrando che esistono elementi di ordine p_j per ogni j, in particolare troviamo elementi di ordine esattamente p^k. Supponiamo per ipotesi induttiva che P abbia ordine p^j. Il teorema 2.14 ci dice che la moltiplicazione per p è suriettiva, quindi esiste Q tale che $pQ = P$. Ma ora $p^jQ = p^{j-1}P \neq O$ mentre $p^{j+1}Q = p^jP = O$: Q ha ordine p^{j+1}.

Ricomponiamo i risultati precedenti. Scriviamo $n = p^r m$, con $r \geqslant 1$ e $\text{MCD}(p, m) = 1$. Si ha

$$E[n] \simeq E[p^r] \oplus E[m].$$

Dalla prima parte si ha $E[m] \simeq \mathbb{Z}/(m) \oplus \mathbb{Z}/(m)$ mentre $E[p^r]$ è isomorfo a 0 oppure a $\mathbb{Z}/(p^r)$. Il Teorema Cinese del Resto ci dice inoltre

$$\mathbb{Z}/(m) \oplus \mathbb{Z}/(p^r) \simeq \mathbb{Z}/(n)$$

da cui si conclude facilmente. □

Introduciamo a questo punto uno tra gli strumenti più importanti nello studio delle curve ellittiche, l'*accoppiamento di Weil*. Siano $E/_{\mathbb{K}}$ una curva ellittica e n un intero tale che $\text{char}(\mathbb{K})$ non divida n. Definiamo

$$\mu_n := \{x \in \overline{\mathbb{K}} \mid x^n = 1\}$$

il gruppo delle radici n-esime dell'unità in $\overline{\mathbb{K}}$ (che è un gruppo ciclico di ordine n, dato che $\text{char}(\mathbb{K})$ non divide n). Esiste una mappa

$$e_n : E[n] \times E[n] \longrightarrow \mu_n,$$

detta *accoppiamento di Weil*, tale che

1. è lineare in ogni argomento: per ogni $S, S_1, S_2, T, T_1, T_2 \in E[n]$

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$
$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2);$$

2. è non degenere in ogni argomento:

$$e_n(S, T) = 1 \ \forall T \in E[n] \ \Rightarrow \ S = O$$
$$e_n(S, T) = 1 \ \forall S \in E[n] \ \Rightarrow \ T = O;$$

3. per ogni $T \in E[n]$ si ha $e_n(T, T) = 1$;

4. per ogni $S, T \in E[n]$ si ha $e_n(S, T) = e_n(T, S)^{-1}$;

5. per ogni $S, T \in E[n]$ e per ogni σ automorfismo di $\overline{\mathbb{K}}$ che lasci fisso $\mathbb{K}$ si ha $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$;

6. per ogni $S, T \in E[n]$ e per ogni α automorfismo di E si ha $e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}$.

L'esistenza dell'accoppiamento di Weil sarà affrontata in seguito; vediamo di derivarne qualche utile risultato.

Proposizione 2.26. *Se (T_1, T_2) è una base di $E[n]$ come $\mathbb{Z}/(n)$-modulo, allora $e_n(T_1, T_2)$ è una radice n-esima primitiva dell'unità.*

Dimostrazione. Ricordiamo che una radice primitiva n-esima dell'unità è un generatore del gruppo ciclico μ_n (o, equivalentemente, ζ è una radice primitiva n-esima dell'unità se $\zeta^k = 1$ se e solo se n divide k).

Supponiamo che $e_n(T_1, T_2) = \zeta$ con $\zeta^d = 1$. Per linearità $e_n(T_1, dT_2) = \zeta^d = 1$. Inoltre $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$. Sia ora $S \in E[n]$ un generico punto: esistono interi a, b tali che $S = aT_1 + bT_2$. Quindi

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1.$$

Da questo deduciamo che $dT_2 = O$, e questo capita se e solo se n divide d. Questo conclude la dimostrazione. □

Corollario 2.27. *Se i punti di $E[n]$ hanno coordinate in $\mathbb{K}$ (ricordiamo che per definizione le coordinate dei punti di $E[n]$ stanno* a priori *in $\overline{\mathbb{K}}$), allora $\mu_n \subset \mathbb{K}$.*

Dimostrazione. Sia σ un automorfismo di $\overline{\mathbb{K}}$ che lascia fisso $\mathbb{K}$ e sia (T_1, T_2) una base per $E[n]$. Per ipotesi, T_1 e T_2 hanno coordinate in $\mathbb{K}$, quindi $\sigma T_1 = T_1$ e $\sigma T_2 = T_2$. Allora

$$\zeta = e_n(T_1, T_2) = e_n(\sigma T_1, \sigma T_2) = \sigma(e_n(T_1, T_2)) = \sigma(\zeta).$$

In altre parole, ζ è fissato da ogni automorfismo di $\overline{\mathbb{K}}$ che lascia fisso $\mathbb{K}$. Per il teorema fondamentale della teoria di Galois, questo accade se e solo se $\zeta \in \mathbb{K}$. La proposizione precedente ci dice che ζ è una radice primitiva n-esima dell'unità, quindi l'intero gruppo $\mu_n \subset \mathbb{K}$. □

Se α è un endomorfismo di E, allora $\alpha|_{E[n]} : E[n] \longrightarrow E[n]$. Fissata una base di $E[n]$, dunque, possiamo rappresentare α con una matrice

$$\alpha_n := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2\left(\mathbb{Z}/(n)\right).$$

Proposizione 2.28. *Il determinante di* α_n *non dipende dalla base e* $\det(\alpha_n) \equiv \deg(\alpha) \pmod{n}$.

Dimostrazione. Sappiamo che $\zeta = e_n(T_1, T_2)$ è una radice primitiva n-esima dell'unità. Abbiamo

$$\begin{aligned}\zeta^{\deg(\alpha)} &= e_n(\alpha(T_1), \alpha(T_2)) = \\ &= e_n(aT_1 + bT_2, cT_1 + dT_2) = \\ &= e_n(T_1, T_1)^{ac} e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{bc} e_n(T_2, T_2)^{bd} = \\ &= e_n(T_1, T_2)^{ad-bc} = \zeta^{\det(\alpha_n)}\end{aligned}$$

da cui la tesi. □

Se α, β sono endomorfismi di E e a, b sono interi, ha senso definire l'endomorfismo $a\alpha + b\beta$ come

$$(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P).$$

Proposizione 2.29. *I gradi di* α, β *e* $a\alpha + b\beta$ *sono legati da*

$$\deg(a\alpha + b\beta) = a^2 \deg(\alpha) + b^2 \deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)).$$

Dimostrazione. Sia n un qualsiasi intero non divisibile da $\mathrm{char}(\mathbb{K})$. Rappresentiamo α e β con matrici α_n, β_n in modo che $a\alpha_n + b\beta_n$ rappresenti $(a\alpha + b\beta)|_{E[n]}$. Un conto mostra che la formula è vera per i determinanti di α_n e β_n. Quindi abbiamo

$$\deg(a\alpha + b\beta) \equiv a^2 \deg(\alpha) + b^2 \deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta))$$

e la congruenza è vera modulo n per infiniti n (tutti tranne i multipli di $\mathrm{char}(\mathbb{K})$). Di conseguenza tale congruenza dev'essere un'uguaglianza vera e propria. □

2.6 Curve ellittiche su campi finiti

In questa sezione applichiamo quanto visto nella sezione precedente per dimostrare il teorema di Hasse. Descriveremo anche un algoritmo dovuto a Schoof per calcolare il numero di punti di una curva ellittica definita su un campo finito.

Ricordiamo che l'endomorfismo di Frobenius è definito come

$$\begin{array}{rccc}\varphi_q : & E(\overline{\mathbb{F}_q}) & \longrightarrow & E(\overline{\mathbb{F}_q}) \\ & (x, y) & \longmapsto & (x^q, y^q).\end{array}$$

È facile mostrare che se E è definita su $\mathbb{F}_q$, gli unici punti lasciati fissi da φ_q sono quelli appartenenti a $E(\mathbb{F}_q)$, cioè quelli con coordinate in $\mathbb{F}_q$. Notiamo inoltre che $\varphi_q^n = \varphi_q \circ \cdots \circ \varphi_q$ composto n volte è l'endomorfismo di Frobenius associato al campo $\mathbb{F}_{q^n}$. Di conseguenza $\ker(\varphi_q^n - 1) = E(\mathbb{F}_{q^n})$.

Infine dalla proposizione 2.18 abbiamo che $\varphi_q^n - 1$ è separabile, quindi dalla proposizione 2.13 abbiamo che

$$\#E(\mathbb{F}_{q^n}) = \deg(\varphi_q^n - 1).$$

Dimostrazione del teorema di Hasse. Sia

$$a := q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\varphi_q - 1).$$

Dobbiamo mostrare che $|a| \leqslant 2\sqrt{q}$. Un conto diretto che segue dalla proposizione 2.29 ci dice

$$\deg(r\varphi_q - s) = r^2 q + s^2 - rsa.$$

Dato che $\deg(r\varphi_q - s) \geqslant 0$, otteniamo che

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geqslant 0$$

per tutti gli interi r, s, quindi

$$qx^2 - ax + 1 \geqslant 0$$

per ogni $x \in \mathbb{R}$ per densità. Imponendo il discriminante negativo o nullo si ottiene

$$a^2 - 4q \leqslant 0$$

cioè $|a| \leqslant 2\sqrt{q}$. Questo conclude la dimostrazione. □

Il numero a è chiamato *traccia* dell'endomorfismo di Frobenius. Il motivo di questa denominazione è contenuto nel seguente lemma.

Lemma 2.30. *Sia* $(\varphi_q)_m$ *la matrice che definisce l'azione di* φ_q *su* $E[m]$. *Allora* $\operatorname{tr}((\varphi_q)_m) \equiv a \pmod{m}$ *e* $\det((\varphi_q)_m) \equiv q \pmod{m}$.

Dimostrazione. Per il determinante è conseguenza immediata della proposizione 2.28, considerando che $\deg(\varphi_q) = q$. La traccia richiede qualche conto in più: intanto scriviamo esplicitamente

$$(\varphi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}.$$

Ora, da un lato abbiamo

$$\#\ker(\varphi_q - 1) = \deg(\varphi_q - 1) = q + 1 - a,$$

dall'altro

$$\#\ker(\varphi_q - 1) \equiv \det((\varphi_q)_m - I) = sv - tu - (s + v) + 1 \pmod{m}.$$

Tenendo conto che $\det((\varphi_q)_m) = sv - tu \equiv q \pmod{m}$, otteniamo

$$\mathrm{tr}((\varphi_q)_m) = s + v \equiv a \pmod{m}.$$

□

Proposizione 2.31. *Con le stesse notazioni precedenti, si ha che*

$$\varphi_q^2 - a\varphi_q + q = 0$$

come endomorfismo di $E/_{\mathbb{F}_q}$. *Inoltre* a *è l'unico intero* k *tale che*

$$\varphi_q^2 - k\varphi_q + q = 0.$$

Dimostrazione. Per la prima parte è sufficiente mostrare che il nucleo di $\varphi_q^2 - a\varphi_q + q$ è infinito. Sia m un intero primo con q e consideriamo la matrice $(\varphi_q)_m$. Per il lemma precedente, il polinomio caratteristico di $(\varphi_q)_m$ è $X^2 - aX + q$. Il teorema di Cayley-Hamilton ci dice

$$(\varphi_q)_m^2 - a(\varphi_q)_m + qI \equiv 0 \pmod{m},$$

cioè $(\varphi_q^2 - a\varphi_q + q)\big|_{E[m]} = 0$. Poiché ci sono infinite scelte per m, il nucleo di $\varphi_q^2 - a\varphi_q + q$ è infinito.

Supponiamo ora che esista $a_1 \neq a$ tale che $\varphi_q^2 - a_1\varphi_q + q = 0$. Quindi

$$(a - a_1)\varphi_q = (\varphi_q^2 - a_1\varphi_q + q) - (\varphi_q^2 - a\varphi_q + q) = 0.$$

D'altra parte φ_q, come ogni endomorfismo di E, è suriettivo: quindi $(a - a_1)$ annulla tutti i punti di $E(\overline{\mathbb{F}_q})$, in particolare annulla $E[m]$ per ogni $m \geqslant 1$. Visto che ci sono punti di ordine m in $E[m]$ quando $\mathrm{MCD}(m, q) = 1$, abbiamo che $a - a_1 \equiv 0 \pmod{m}$ per tali m, che sono infiniti. Concludiamo che $a - a_1 = 0$. □

Descriviamo ora l'algoritmo di Schoof. Sia S un insieme finito di primi tali che

$$\prod_{\ell \in S} \ell > 4\sqrt{q}.$$

Se riusciamo a calcolare a modulo ℓ per ogni $\ell \in S$, possiamo ricostruire a modulo $\prod \ell$ tramite il Teorema Cinese del Resto e quindi determinare univocamente a come l'unico rappresentante che giace nell'intervallo $[-2\sqrt{q}, 2\sqrt{q}]$.

Come calcoliamo a modulo ℓ? Per semplicità assumiamo che $\ell \neq \mathrm{char}(\mathbb{K})$ e che q sia dispari.

Per $\ell = 2$, il conto è facile. Se $X^3 + aX + b$ ha una radice $e \in \mathbb{F}_q$, allora $(e, 0) \in E[2] \cap E(\mathbb{F}_q)$, quindi $E(\mathbb{F}_q)$ ha ordine pari. In questo caso $q + 1 - a \equiv 0 \pmod 2$ e a è pari. Viceversa, se $X^3 + aX + b$ non ha radici in $\mathbb{F}_q$, allora $E(\mathbb{F}_q)$ non ha elementi di ordine 2 e a è dispari. Per trovare le radici di $X^3 + aX + b$ potremmo provare tutti gli elementi di $\mathbb{F}_q$, ma c'è una soluzione più rapida: ricordiamo che gli elementi di $\mathbb{F}_q$ sono tutte e sole le radici di $X^q - X$, quindi $X^3 + aX + b$ ha una radice in $\mathbb{F}_q$ se e solo se $\mathrm{MCD}(X^3 + aX + b, X^q - X) \neq 1$. Non è conveniente calcolare direttamente questo MCD, perché $X^q - X$ ha grado troppo elevato; allora si calcola $X_q \equiv X^q \pmod{X^3 + aX + b}$ (ad esempio, con i quadrati ripetuti e riducendo ad ogni passo) e poi si usa il risultato per calcolare

$$\mathrm{MCD}(X_q - X, X^3 + aX + b) = \mathrm{MCD}(X^q - X, X^3 + aX + b).$$

Vediamo ora cosa posiamo fare in generale. Nel seguito troveremo espressioni come x^q e x^{q^2}: si intende che si calcolano con metodi efficienti come quello appena descritto.

Richiamiamo i polinomi di divisione ψ_n introdotti nella sezione 2.5. Quando n è dispari, ψ_n è un polinomio in X (dopo aver aggiunto le relazioni $Y^2 - X^3 - aX - b$, $A - a$ e $B - b$) e per $(x, y) \in E(\overline{\mathbb{F}_q})$ abbiamo

$$(x, y) \in E[n] \iff \psi_n(x) = 0$$

(vedi anche il teorema 2.24).

Sia ora φ_q l'endomorfismo di Frobenius. Sappiamo dalla proposizione 2.31 che $\varphi_q^2 - a\varphi_q + q = 0$. Se $(x, y) \in E$, allora,

$$(x^{q^2}, y^{q^2}) + q(x, y) = a(x^q, y^q).$$

Supponiamo che (x, y) abbia ordine ℓ. Posto $q_\ell \equiv q \pmod \ell$ con $|q_\ell| < \ell/2$ abbiamo allora $q(x, y) = q_\ell(x, y)$, da cui

$$(x^{q^2}, y^{q^2}) + q_\ell(x, y) = a(x^q, y^q). \tag{2.6}$$

Notiamo che tutti i punti coinvolti nella relazione (2.6) hanno ordine ℓ e vediamo come da questa si può ricavare il valore di a modulo ℓ. Notiamo inoltre che non è importante il punto (x, y) da cui siamo partiti, in quanto il fatto che (2.6) valga

per un punto determina a modulo ℓ e di conseguenza (2.6) vale per ogni punto di ordine ℓ.

In primo luogo supponiamo che esista un punto $(x, y) \in E[\ell]$ tale che $(x^{q^2}, y^{q^2}) \neq \pm q_\ell(x, y)$. Chiamiamo

$$(\tilde{x}, \tilde{y}) := (x^{q^2}, y^{q^2}) + q_\ell(x, y) \neq O$$

(e quindi $a \not\equiv 0 \pmod{\ell}$). In questo caso la prima coordinata di (x^{q^2}, y^{q^2}) e di $q_\ell(x, y)$ è diversa, quindi per calcolarne la somma si usa la formula derivante dalla retta secante (e non dalla retta tangente o dalla retta verticale). Denoteremo con (x_s, y_s) le coordinate del punto $s(x, y)$, e in particolare $x_s = R_s(x)$ e $y_s = S_s(x)y$, come abbiamo visto precedentemente. Osserviamo che x_s e y_s possono essere calcolate con i polinomi di divisione.

Abbiamo dunque

$$\tilde{x} = \left(\frac{y^{q^2} - y_{q_\ell}}{x^{q^2} - x_{q_\ell}} \right)^2 - x^{q^2} - x_{q_\ell}.$$

Osservando che

$$\left(y^{q^2} - y_{q_\ell} \right)^2 = (x^3 + ax + b) \left((x^3 + ax + b)^{(q^2-1)/2} - S_{q_\ell}(x) \right)^2$$

e che x_{q_ℓ} è una funzione razionale di x, possiamo scrivere $\tilde{x}$ come funzione razionale di x.

Vogliamo trovare s tale che $(\tilde{x}, \tilde{y}) = (x_s^q, y_s^q)$. Intanto, se $\tilde{x} = x_s^q$, ricaviamo $(\tilde{x}, \tilde{y}) = \pm(x_s^q, y_s^q)$, quindi per ora limitiamoci a questa relazione. Prima abbiamo notato che (2.6) vale per ogni punto di $E[\ell]$: poiché le radici di ψ_ℓ corrispondono a tutte e sole le prime coordinate dei punti di $E[\ell]$, deduciamo

$$\tilde{x} - x_s^q \equiv 0 \pmod{\psi_\ell}.$$

Stiamo usando il fatto che ψ_ℓ ha solo radici semplici (è facile da vedere: ci sono $\ell^2 - 1$ punti di ordine ℓ, che hanno $(\ell^2 - 1)/2$ prime coordinate distinte, e ψ_ℓ ha grado $(\ell^2 - 1)/2$).

Una ricerca esaustiva (da 1 a $(\ell - 1)/2$) ci permette di trovare s tale che $(\tilde{x}, \tilde{y}) = \pm(x_s^q, y_s^q)$. Per determinare il segno, guardiamo la seconda coordinata. Dopo aver scritto $\tilde{y}/y$ e y_s^q/y come funzioni razionali di x, possiamo verificare se

$$(\tilde{y} - y_s^q)/y \equiv 0 \pmod{\psi_\ell};$$

in tal caso $a \equiv s$ modulo ℓ, altrimenti $a \equiv -s$.

Analizziamo adesso il caso in cui $(x^{q^2}, y^{q^2}) = \pm q_\ell(x, y)$ per ogni $(x, y) \in E[\ell]$. Distinguiamo ulteriormente due situazioni.

Supponiamo in primo luogo che esista un punto in $E[\ell]$ tale che $(x^{q^2}, y^{q^2}) = q_\ell(x, y)$; si ha allora $\varphi_q^2(x, y) = q_\ell(x, y)$, da cui

$$a\varphi_q(x, y) = \varphi_q^2(x, y) + q_\ell(x, y) = 2q_\ell(x, y)$$

e di conseguenza

$$a^2 q_\ell(x, y) = a^2\varphi_q^2(x, y) = (2q_\ell)^2(x, y).$$

Da ciò deduciamo che $a^2 q \equiv 4q^2 \pmod{\ell}$, dunque q è un quadrato modulo ℓ. (Notiamo che allora, se q non è un quadrato modulo ℓ, questo non può avvenire.) Sia $w^2 \equiv q \pmod{\ell}$. Abbiamo

$$(\varphi_q + w)(\varphi_q - w)(x, y) = (\varphi_q^2 - q)(x, y) = O,$$

e ciò può avvenire se, detto $P = (x, y)$, $(\varphi_q - w)P = O$ (cioè $\varphi_q(P) = wP$) oppure $(\varphi_q - w)P = Q$ con $(\varphi_q + w)Q = O$. In entrambi i casi abbiamo trovato un punto $(x, y) \in E[\ell]$ tale che $\varphi_q(x, y) = \pm w(x, y)$. Se $\varphi_q(x, y) = w(x, y)$, allora

$$O = (\varphi_q^2 - a\varphi_q + q)(x, y) = (q - aw + q)P,$$

da cui $aw \equiv 2q \equiv 2w^2 \pmod{\ell}$, e $a \equiv 2w \pmod{\ell}$. Similmente, se $\varphi_q(x, y) = -w(x, y)$, otteniamo $a \equiv -2w \pmod{\ell}$.

Come possiamo verificare di essere nel caso in cui $(x^{q^2}, y^{q^2}) = q_\ell(x, y)$? Abbiamo visto che in questa situazione si ha

$$(x^q, y^q) = \pm w(x, y) = \pm(x_w, y_w) = (x_w, \pm y_w)$$

con le stesse notazione già viste. Sarà sufficiente allora considerare $x^q - x_w$ come funzione razionale di x, considerarne il numeratore $\mathrm{num}(x)$ e calcolare

$$\mathrm{MCD}(\mathrm{num}(x), \psi_\ell).$$

Se esso è diverso da 1, allora esiste $(x, y) \in E[\ell]$ tale che $\varphi_q(x, y) = \pm w(x, y)$. Per decidere il segno è sufficiente controllare la seconda coordinata. Osserviamo che il massimo comun divisore verifica l'esistenza di un punto di $E[\ell]$ per cui si abbia $\varphi_q(x, y) = \pm w(x, y)$: verificare solamente che $x^q - x_w \equiv 0 \pmod{\psi_\ell}$ non ci avrebbe portati lontano, perché corrisponde alla verifica della relazione per tutti i punti di $E[\ell]$, cosa che non è garantita affatto.

Se $\mathrm{MCD}(\mathrm{num}(x), \psi_\ell) = 1$, risalendo nel ragionamento scopriamo che non possiamo essere nel caso $(x^{q^2}, y^{q^2}) = q_\ell(x, y)$, quindi resta l'ultima possibilità,

cioè che $(x^{q^2}, y^{q^2}) = -q_\ell(x, y)$ per ogni punto di $E[\ell]$. Ricaviamo facilmente che in tal caso

$$aP = (\varphi_q^2 + q)P = O$$

per ogni $P \in E[\ell]$, quindi $a \equiv 0 \pmod{\ell}$.

Riassumiamo l'algoritmo di Schoof, mettendo insieme quanto detto finora.

Algoritmo ALGORITMO DI SCHOOF

Input: Una curva ellittica $E/_{\mathbb{F}_q}$, con $\mathrm{char}(\mathbb{F}_q) = p$, definita da $y^2 = x^3 + ax + b$

Scegli $S = \{2, 3, 5, \dots\}$ insieme finito di primi tali che $p \notin S$ e $\prod_{\ell \in S} \ell > 4\sqrt{q}$
if $\mathrm{MCD}(X^q - X, X^3 + aX + b) \neq 1$ **then**
    $a_2 := 0$
else
    $a_2 := 1$
end if
for each $\ell \in S \setminus \{2\}$ **do**
    $q_\ell := q \mod \ell$
    $(\tilde{x}, \tilde{y}) := (x^{q^2}, y^{q^2}) + q_\ell(x, y) \pmod{\psi_\ell}$ ▷ Per ora basta $\tilde{x}$
    for $s := 1$ **to** $(\ell - 1)/2$ **do**
        $(x_s, y_s) = s(x, y)$ ▷ Per ora basta x_s
        if $\tilde{x} - x_s^q \equiv 0 \pmod{\psi_\ell}$ **then**
            Calcola $\tilde{y}$ e y_x ▷ Solo in questo caso servono $\tilde{y}$ e y_x
            if $(\tilde{y} - x_s^q)/y \equiv 0 \pmod{\psi_\ell}$ **then**
                $a_\ell := s$
            else
                $a_\ell := -s$
            end if
        end if
    end for ▷ Tutti i valori di s sono stati provati senza successo
    Calcola w tale che $w^2 \equiv q \pmod{\ell}$
    if w non esiste **then**
        $a_\ell := 0$
    end if
    if $\mathrm{MCD}(\mathrm{num}(x^q - x_w), \psi_\ell) = 1$ **then**
        $a_\ell := 0$

▷ *Continua a pagina seguente*

▷ *Continua da pagina precedente*

else if $\mathrm{MCD}(\mathrm{num}((y^q - y_w)/y), \psi_\ell) \neq 1$ **then**
  $a_\ell := 2w$
else
  $a_\ell := -2w$
end if
end for
Calcola a, sapendo $a \equiv a_\ell \pmod{\ell}$ e scegliendolo tale che $|a| < 2\sqrt{q}$
return $q + 1 - a$

Output: $\#E(\mathbb{F}_q)$

2.7 Curve ellittiche su $\mathbb{C}$

Vedremo in questa sezione che c'è una corrispondenza tra curve ellittiche definite sul piano complesso e tori complessi, cioè quozienti di $\mathbb{C}$ per reticoli di rango 2 su $\mathbb{R}$. Mostreremo come un toro dà origine a una curva ellittica e accenneremo soltanto al viceversa.

Sia $L \subset \mathbb{C}$ un reticolo di rango 2, cioè generato da due numeri complessi ω_1, ω_2 $\mathbb{R}$-linearmente indipendenti. Il quoziente (di gruppi abeliani) $\mathbb{C}/L$ è topologicamente un toro. Una funzione definita su $\mathbb{C}/L$ può essere vista come funzione definita su $\mathbb{C}$ tale che

$$f(z + \omega) = f(z)$$

per ogni $z \in \mathbb{C}$ e per ogni $\omega \in L$.

Definizione 2.32. Una funzione meromorfa $f : \mathbb{C} \dashrightarrow \mathbb{C} \cup \{\infty\}$ (dove si pone $f(z) = \infty$ se z è un polo) è detta *doppiamente periodica* di periodi (ω_1, ω_2) se

$$f(z + \omega) = f(z)$$

per ogni $z \in \mathbb{C}$ e per ogni $\omega \in L$, dove L è il reticolo generato da ω_1 e ω_2.

Definizione 2.33. Siano f una funzione meromorfa definita su $\mathbb{C}$ non identicamente nulla e $w \in \mathbb{C}$. Sappiamo che esiste lo sviluppo di Laurent

$$f(z) = a_r(z - w)^r + a_{r+1}(z - w)^{r+1} + \dots$$

con $a_r \neq 0$ e $r \in \mathbb{Z}$. Definiamo *ordine* di f in w il numero $\mathrm{ord}_w(f) := r \in \mathbb{Z}$. Definiamo *residuo* di f in w il numero $\mathrm{Res}_w(f) := a_{-1} \in \mathbb{C}$. (Notiamo che se f ha un polo in w, $\mathrm{ord}_w(f)$ è l'opposto dell'ordine del polo — l'ordine di un polo infatti è sempre un numero positivo.)

Indichiamo con $\mathcal{P}$ il parallelogramma fondamentale associato a L rispetto alla base (ω_1, ω_2).

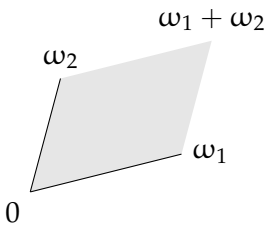


Figura 2.4: Parallelogramma fondamentale.

Definizione 2.34. Un *divisore* su $\mathcal{P}$ è una somma formale

$$D = \sum_{w \in \mathcal{P}} n_w [w]$$

con $n_w \in \mathbb{Z}$, $n_w \neq 0$ solo per un numero finito di $w \in \mathcal{P}$. In altre parole, per ogni $w \in \mathcal{P}$ abbiamo un simbolo $[w]$ e un divisore è una combinazione lineare finita di questi simboli a coefficienti in $\mathbb{Z}$. Il *grado* di un divisore è il numero

$$\deg(D) := \sum_{w \in \mathcal{P}} n_w.$$

Se f è una funzione meromorfa su $\mathbb{C}$ non identicamente nulla doppiamente periodica, definiamo il suo divisore come

$$\operatorname{div}(f) := \sum_{w \in \mathcal{P}} (\operatorname{ord}_w(f))[w].$$

Il seguente teorema ci garantisce, tra l'altro, che $\operatorname{div}(f)$ è ben definito.

Teorema 2.35. *Siano f una funzione doppiamente periodica di periodi (ω_1, ω_2), L il reticolo da loro generato e $\mathcal{P}$ il parallelogramma fondamentale associato. Allora*

1. *se f non ha poli, allora è costante;*
2. *la somma dei residui di f estesa a tutti i punti $w \in \mathcal{P}$ è nulla;*
3. *se f non è identicamente nulla,*

$$\deg(\operatorname{div}(f)) = \sum_{w \in \mathcal{P}} \operatorname{ord}_w(f) = 0;$$

4. *se* f *non è identicamente nulla,*

$$\sum_{w \in \mathcal{P}} (\mathrm{ord}_w(f))w \in L$$

dove $(\mathrm{ord}_w(f))w$ *è il prodotto tra numeri complessi;*

5. *se* f *non è costante, allora* $f : \mathbb{C} \longrightarrow \mathbb{C} \cup \{\infty\}$ *è suriettiva; inoltre, se* n *è la somma degli ordini dei poli di* f *in* $\mathcal{P}$ *e* $z_0 \in \mathbb{C}$*, allora l'equazione* $f(z) = z_0$ *ha esattamente* n *soluzioni (contate con molteplicità);*

6. *se* f *ha un solo polo in* $\mathcal{P}$*, esso non può essere un polo semplice (cioè di ordine 1).*

Tutte le somme estese a $w \in \mathcal{P}$ *coinvolgono solo un numero finito di addendi non nulli.*

Dimostrazione. Innanzitutto, f è meromorfa, quindi ha solo un numero finito di zeri e/o poli su un qualsiasi compatto, ad esempio su $\overline{\mathcal{P}}$. Di conseguenza tutte le somme coinvolte nel teorema sono in realtà finite.

1. Se f non ha poli, allora è limitata su $\overline{\mathcal{P}}$, quindi è limitata su tutto $\mathbb{C}$ per periodicità. Il Teorema di Liouville ci permette di concludere.

2. Il Teorema di Cauchy ci dice che

$$\int_{\partial \mathcal{P}} f(z)dz = 2\pi i \sum_{w \in \mathcal{P}} \mathrm{Res}_w(f)$$

dove l'integrale di linea lungo $\partial\mathcal{P}$ è percorso in senso antiorario. Supponendo che ω_1 e ω_2 siano orientati come in figura 2.4, possiamo scrivere

$$\int_{\partial \mathcal{P}} f(z)dz = \int_0^{\omega_1} f(z)dz + \int_{\omega_1}^{\omega_1+\omega_2} f(z)dz + \int_{\omega_1+\omega_2}^{\omega_2} f(z)dz + \int_{\omega_2}^{0} f(z)dz.$$

Per periodicità si ha

$$\int_{\omega_1}^{\omega_1+\omega_2} f(z)dz = \int_0^{\omega_2} f(z)dz = -\int_{\omega_2}^{0} f(z)dz$$

e analogamente

$$\int_{\omega_1+\omega_2}^{\omega_2} f(z)dz = -\int_0^{\omega_1} f(z)dz$$

quindi la somma dei quattro pezzi è nulla. In realtà c'è un piccolo particolare da sistemare: la formula non vale se ci sono poli lungo il percorso di integrazione. Nel caso in cui succeda, occorre sistemare il percorso in modo da escludere i poli (vedi figura 2.5).

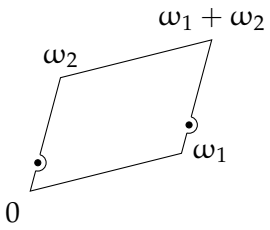


Figura 2.5: Parallelogramma fondamentale con poli.

3. Se $r = \mathrm{ord}_w(f)$, possiamo scrivere $f(z) = (z-w)^r g(z)$ con g tale che $g(w)$ sia un valore finito non nullo. Quindi
$$\frac{f'(z)}{f(z)} = \frac{r}{z-w} + \frac{g'(z)}{g(z)},$$
in particolare $\mathrm{Res}_w(f'/f) = r$. Tenendo conto del fatto che se f è doppiamente periodica lo è anche f'/f, applicando il punto precedente a f'/f si ottiene
$$2\pi i \sum_{w\in\mathcal{P}} \mathrm{ord}_w(f) = 2\pi i \sum_{w\in\mathcal{P}} \mathrm{Res}_w\left(\frac{f'}{f}\right) = 0.$$

4. Analogamente ai punti precedenti, possiamo scrivere
$$2\pi i \sum_{w\in\mathcal{P}} (\mathrm{ord}_w(f))w = 2\pi i \sum_{w\in\mathcal{P}} \mathrm{Res}_w\left(z\frac{f'}{f}\right) = \int_{\partial\mathcal{P}} z\frac{f'(z)}{f(z)}dz$$
ma stavolta non possiamo concludere, perché zf'/f non è doppiamente periodica. Scriviamo l'integrale come somma di quattro pezzi e osserviamo che
$$\begin{aligned}\int_{\omega_1+\omega_2}^{\omega_2} z\frac{f'(z)}{f(z)}dz &= \int_{\omega_1}^{0} (z+\omega_2)\frac{f'(z)}{f(z)}dz = \\ &= -\int_0^{\omega_1} z\frac{f'(z)}{f(z)}dz - \omega_2\int_0^{\omega_1}\frac{f'(z)}{f(z)}dz.\end{aligned}$$
A questo punto notiamo che
$$\frac{1}{2\pi i}\int_0^{\omega_1}\frac{f'(z)}{f(z)}dz$$
è l'indice del cammino $\{f(t\omega_1) \mid t \in [0,1]\}$ (che è chiuso in quanto $f(0) = f(\omega_1)$) intorno a zero, dunque è un intero. Concludiamo che
$$\int_0^{\omega_1} z\frac{f'(z)}{f(z)}dz + \int_{\omega_1+\omega_2}^{\omega_2} z\frac{f'(z)}{f(z)}dz = -\omega_2\int_0^{\omega_1}\frac{f'(z)}{f(z)}dz \in 2\pi i\mathbb{Z}\omega_2.$$

In maniera del tutto analoga

$$\int_{\omega_2}^{0} z\frac{f'(z)}{f(z)}dz + \int_{\omega_1}^{\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz \in 2\pi i\mathbb{Z}\omega_1,$$

da cui

$$2\pi i \sum_{w\in\mathcal{P}} (\mathrm{ord}_w(f))w \in 2\pi i L.$$

5. Sia $z_0 \in \mathbb{C}$. La funzione $h(z) := f(z) - z_0$ è doppiamente periodica ed ha gli stessi poli di f. Per il punto 3. il numero degli zeri di h (contati con molteplicità) è uguale al numero di poli di h (contati con molteplicità), che è n.

6. Supponiamo che f abbia un solo polo semplice in w. Allora $\mathrm{Res}_w(f) \neq 0$ e la somma del punto 2. ha un solo addendo non nullo, in contraddizione con il risultato precedente. Di conseguenza, w non può essere semplice, oppure esistono altri poli oltre w.

□

Ma esistono funzioni doppiamente periodiche? Sì, le costanti. Magari è meglio chiedersi se esistono funzioni doppiamente periodiche non costanti. Anche in questo caso, la risposta è sì, e un esempio cardine è fornito dalla $\wp$ di Weierstrass.

Definizione 2.36. Dato un reticolo L, si definisce *funzione $\wp$ di Weierstrass* associata a L la funzione

$$\wp(z) = \wp(z; L) := \frac{1}{z^2} + \sum_{\substack{\omega\in L\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

I termini aggiuntivi $1/\omega^2$ sono necessari per la convergenza della serie, come vedremo tra poco. In effetti, la loro presenza permette di confrontare la serie che definisce la $\wp$ con una serie convergente.

Lemma 2.37. *La serie* $\displaystyle\sum_{\substack{\omega\in L\\ \omega\neq 0}} \frac{1}{|\omega|^3}$ *è convergente.*

Dimostrazione. Sia $r > 0$ tale che il disco di centro 0 e raggio r non contenga punti di $L \setminus \{0\}$. Di conseguenza, per ogni $\omega \in L \setminus \{0\}$, si ha

$$\frac{1}{|\omega|} < \frac{1}{r}.$$

Ora, la serie $\sum |\omega|^{-3}$ è a termini positivi, quindi è possibile sommare riordinando i termini a piacere; in particolare, sommiamo per parallelogrammi concentrici. Nella cornice a livello n ci sono $8n$ punti del reticolo, ciascuno distante da 0 almeno nr. Di conseguenza

$$\sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{|\omega|^3} \leqslant \sum_{n=1}^{\infty} 8n \frac{1}{(nr)^3} = \frac{8}{r^3} \sum_{n=1}^{\infty} \frac{1}{n^2}$$

che converge. □

In realtà con un po' di fatica in più si può dimostrare che $\sum |\omega|^{-k}$ converge se e solo se $k > 2$.

Teorema 2.38. *Per la funzione $\wp$ valgono le seguenti proprietà.*

1. *La serie che definisce $\wp$ converge assolutamente e uniformemente sui compatti di $\mathbb{C}$ che non contengono punti di L.*

2. *$\wp(z)$ è una funzione meromorfa su $\mathbb{C}$ ed ha un polo doppio in ciascun punto di L.*

3. *$\wp$ è pari, cioè $\wp(-z) = \wp(z)$ per ogni $z \in \mathbb{C}$.*

4. *$\wp(z + \omega) = \wp(z)$ per ogni $\omega \in L$.*

5. *L'insieme delle funzioni doppiamente periodiche su L è $\mathbb{C}(\wp, \wp')$. In altre parole, ogni funzione doppiamente periodica su L è funzione razionale di $\wp$ e della sua derivata.*

Dimostrazione. 1. Sia K un compatto che non contiene punti di L e sia $M := \max\{|z| \mid z \in K\}$. Per $z \in K$ e $\omega \in L$ con $|\omega| > 2M$, abbiamo $|z - \omega| \geqslant |\omega| - |z| \geqslant |\omega|/2$ e $|2\omega - z| \leqslant 2|\omega| + |z| \leqslant 5|\omega|/2$, quindi

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{(z-\omega)^2 \omega^2} \right| \leqslant \frac{M(5|\omega|/2)}{|\omega|^4/4} = \frac{10M}{|\omega|^3}.$$

Grazie al lemma 2.37, per confronto possiamo concludere che la serie che definisce $\wp$ converge assolutamente e uniformemente per $z \in K$ con $|\omega| > 2M$. (Notiamo che senza i termini $1/\omega^2$ il confronto sarebbe avvenuto proprio con $1/|\omega|^2$ e non avremmo potuto concludere.) I termini della serie esclusi sono in numero finito, quindi si ha la convergenza della serie completa.

2. Dal punto precedente, $\wp$ è un limite uniforme di funzioni analitiche per $z \notin L$, quindi è anch'essa analitica negli stessi punti. Se $z \in L$, la somma dei termini per $\omega \neq z$ è analitica in un intorno di z, perciò il termine $1/(z-\omega)^2$ fa sì che $\wp$ abbia un polo doppio in z.

3. Per le proprietà di reticolo di L $\omega \in L$ se e solo se $-\omega \in L$. Scrivendo esplicitamente la serie per $\wp(-z)$, possiamo sommare su $-\omega \in L$ e ottenere
$$\frac{1}{(-z+\omega)^2} - \frac{1}{(-\omega)^2} = \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

4. I termini aggiuntivi $1/\omega^2$ che ci hanno permesso di mostrare la convergenza della serie rendono meno semplice la dimostrazione della doppia periodicità: senza di essi, infatti, si potrebbe dire che lo shift $z+\omega$ non cambia gli addendi della sommatoria.

   Differenziando termine a termine si vede che
   $$\wp'(z) = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3}$$
   che converge assolutamente per $z \notin L$. Cambiare z con $z+\omega$ porta a
   $$\wp'(z+\omega) = \wp'(z)$$
   cioè $\wp(z+\omega) - \wp(z) = c_\omega$, una costante che dipende da ω. Se ora si valuta in $z = \omega/2$ si ottiene
   $$c_\omega = \wp(-\omega/2) - \wp(\omega/2) = 0$$
   per parità di $\wp$.

5. Sia f una funzione doppiamente periodica. Possiamo scrivere
   $$f(z) = \frac{f(z)+f(-z)}{2} + \frac{f(z)-f(-z)}{2}$$
   che esprime f come somma di una funzione pari e di una funzione dispari. È sufficiente allora dimostrare la tesi per le funzioni pari e per le funzioni dispari. Dato che $\wp$ è pari, abbiamo che $\wp'$ è dispari. Inoltre, se $f(z)$ è dispari, $f(z)/\wp'(z)$ è pari. Di conseguenza basta dimostrare che le funzioni pari doppiamente periodiche sono funzioni razionali di $\wp$.

   Sia f pari doppiamente periodica e non identicamente nulla (altrimenti la tesi è banalmente verificata). Chiamiamo per comodità di scrittura $\omega_3 := \omega_1 + \omega_2$. A meno di una trasformazione invertibile della forma
   $$f \longmapsto \frac{af+b}{cf+d}$$

con $ad - bc \neq 0$, possiamo supporre che f non abbia zeri né poli in punti z tali che $2z \in L$ (cioè supponiamo che 0 non sia uno zero né un polo e che $\omega_i/2$ per $i = 1, 2, 3$ non siano zeri).

Dato che f è pari e doppiamente periodica, $f(\omega_3 - z) = f(z)$, quindi

$$\operatorname{ord}_w(f) = \operatorname{ord}_{\omega_3 - w}(f).$$

Possiamo allora sistemare gli zeri e i poli di f in $\mathcal{P}$ in coppie $(w, \omega_3 - w)$. Chiamiamo Z tale insieme. Notiamo che gli elementi che formano una coppia sono distinti, perché $w \neq \omega_3/2$. Occorre fare attenzione al caso in cui w stia sulla frontiera di $\mathcal{P}$: supponendo che $w = t\omega_1$ con $0 < t < 1$, infatti, $\omega_3 - w = (1 - t)\omega_1 + \omega_2 \notin \mathcal{P}$. In questo caso trasliamo di ω_2 ottenendo $(1-t)\omega_1 \in \mathcal{P}$ come secondo elemento della coppia. (Ancora una volta i due elementi della coppia sono distinti perché $w \neq \omega_1/2$.) Situazione analoga nel caso $w = t\omega_2$.

Fissato w, la funzione $\wp(z) - \wp(w)$ ha uno zero in w e uno zero in $\omega_3 - w$. Per il punto 5. del teorema 2.35 questi sono gli unici due zeri in $\mathcal{P}$ e sono zeri semplici. Ma allora la funzione

$$h(z) := \prod_{(w, \omega_3 - w) \in Z} (\wp(z) - \wp(w))^{\operatorname{ord}_w(f)}$$

ha uno zero di ordine $\operatorname{ord}_w(f)$ in w e in $\omega_3 - w$ quando $\operatorname{ord}_w(f) > 0$ e un polo dello stesso ordine di f quando $\operatorname{ord}_w(f) < 0$. Cosa succede ai poli in $z \in L$? Ciascun fattore ha un polo doppio nei punti di L, quindi il contributo totale ai poli è

$$2 \sum_{(w, \omega_3 - w) \in Z} \operatorname{ord}_w(f) = 0$$

sempre per il teorema 2.35. Quindi $h(z)$ ha zeri e poli negli stessi punti di f con lo stesso ordine. In particolare, $f(z)/h(z)$ non ha zeri né poli in $\mathcal{P}$, dunque è costante. Dato che $h(z)$ è una funzione razionale di $\wp$, anche f lo è.

□

Per costruire funzioni con proprietà assegnate, è utile a questo punto introdurre un'altra funzione speciale, che non è doppiamente periodica ma ha una descrizione semplice per la traslazione di elementi di L.

Definizione 2.39. Dato un reticolo L, si definisce *funzione* σ *di Weierstrass* associata a L la funzione

$$\sigma(z) = \sigma(z; L) := z \prod_{\substack{\omega \in L \\ \omega \neq 0}} \left(1 - \frac{z}{\omega}\right) e^{(z/\omega)+(z/\omega)^2/2}.$$

Teorema 2.40. *La funzione* σ *appena definita gode delle seguenti proprietà.*

1. *Il prodotto che definisce* σ *converge a una funzione analitica sull'intero piano complesso.*

2. $\sigma(z)$ *ha zeri semplici nei punti di* L *e nessun altro zero.*

3. *Vale che* $\dfrac{d^2}{dz^2} \log \sigma(z) = -\wp(z)$.

4. *Per ogni* $\omega \in L$ *esistono* a, b *(dipendenti da* ω*) tali che* $\sigma(z + \omega) = e^{az+b}\sigma(z)$ *per ogni* $z \in \mathbb{C}$.

Dimostrazione. 1. Il fattore esponenziale è introdotto appositamente per rendere il prodotto convergente. In effetti, sviluppando in serie,

$$(1-u)e^{u+u^2/2} = 1 + c_3u^3 + c_4u^4 + \dots$$

quindi esiste una costante C tale che

$$\left|(1-u)e^{u+u^2/2} - 1\right| \leqslant C|u|^3$$

per u in un intorno di 0. In particolare la disuguaglianza resta vera per $u = z/\omega$ con $|\omega|$ sufficientemente grande e z in un compatto. Ricordiamo che per le convergenze di prodotti infiniti vale che

- se $\sum |a_n|$ converge, allora $\prod(1 + a_n)$ converge;
- se $1 + a_n \neq 0$ per ogni n, allora anche il prodotto è diverso da 0.

Ora, $\sum |z/\omega|^3$ converge per il lemma 2.37, quindi il prodotto converge uniformemente sui compatti. Quindi $\sigma(z)$ è analitica.

2. Segue facilmente dal fatto che ogni fattore del prodotto, a parte uno, è non nullo per $z = \omega$.

3. È un semplice conto, differenziando termine a termine.

4. Sia $\omega \in L$. Dal punto precedente e dalla periodicità di $\wp$ abbiamo

$$\frac{d^2}{dz^2} \log \frac{\sigma(z+\omega)}{\sigma(z)} = 0$$

pertanto esistono a, b tali che

$$\log \frac{\sigma(z+\omega)}{\sigma(z)} = az + b.$$

L'esponenziale ci permette di concludere. In realtà dobbiamo supporre che z stia in una piccola regione del piano complesso per evitare complicazioni con le ramificazioni del logaritmo; tuttavia, una volta che abbiamo la tesi in questa regione, l'unicità del prolungamento analitico porta alla tesi per ogni $z \in \mathbb{C}$.

□

La σ di Weierstrass ci permette di dimostrare il seguente teorema, che identifica quali tra i divisori sono divisori di funzioni doppiamente periodiche.

Teorema 2.41 (Abel-Jacobi)**.** *Sia* $D = \sum n_w[w]$ *un divisore. Allora* $D = \operatorname{div}(f)$ *per qualche* f *se e solo se* $\deg(D) = 0$ *e* $\sum n_w w \in L$.

Dimostrazione. $\boxed{\Rightarrow}$ Discende immediatamente dal teorema 2.35.
$\boxed{\Leftarrow}$ Usiamo la σ per definire f: se $\deg(D) = 0$ e $\sum n_w w = \ell \in L$, costruiamo

$$f(z) := \frac{\sigma(z)}{\sigma(z-\ell)} \prod_w \sigma(z-w)^{n_w}$$

dove il prodotto è ovviamente esteso solamente ai w tali che $n_w \neq 0$. Occorre verificare che tutto torni.

Intanto vediamo che se $\omega \in L$,

$$\begin{aligned}\frac{f(z+\omega)}{f(z)} &= e^{az+b-a(z-\ell)-b} e^{\sum n_w (a(z-\ell)+b)} = \\ &= e^{a\ell} e^{az(\sum n_w)} e^{-a\sum (n_w w)} e^{b(\sum n_w)} = 1\end{aligned}$$

dal momento che $\sum n_w = 0$ e $\sum n_w w = \ell$. Guardiamo ora chi è $\operatorname{div}(f)$. $\sigma(z)$ e $\sigma(z-\ell)$ hanno zeri semplici esattamente nei punti di L, quindi il loro contributo a zeri e poli di f è nullo; le proprietà di σ fanno in modo che il prodotto abbia zeri e poli esattamente nei w tali che $n_w \neq 0$, e il loro ordine è proprio n_w. Questo prova che $\operatorname{div}(f) = D$. □

Siamo pronti per vedere come un toro complesso $\mathbb{C}/L$ sia isomorfo a una certa curva ellittica $E/\mathbb{C}$.

Definizione 2.42. Siano L un reticolo su $\mathbb{C}$ di rango 2 e $k \geqslant 3$ un intero. Definiamo *serie di Eisenstein* associata a L la serie

$$G_k = G_k(L) := \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^k}.$$

Per il lemma 2.37, la serie converge. Se k è dispari, i contributi di ω e $-\omega$ si cancellano e $G_k = 0$. Per k pari, invece, G_k ci permette di scrivere i coefficienti della serie di Laurent per $\wp$.

Proposizione 2.43. *Sia* $\lambda_1 = \min\{|\omega| \mid \omega \in L,\ \omega \neq 0\}$. *Per* $0 < |z| < \lambda_1$ *vale*

$$\wp(z) = \frac{1}{z^2} + \sum_{j=1}^{\infty} (2j+1) G_{2j+2} z^{2j}.$$

Dimostrazione. Quando $|z| < |\omega|$,

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \omega^{-2}\left(\frac{1}{(1-(z/\omega))^2} - 1\right) = \omega^{-2}\left(\sum_{n=1}^{\infty} (n+1)\frac{z^n}{\omega^n}\right).$$

Pertanto

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \sum_{n=1}^{\infty} (n+1)\frac{z^n}{\omega^{n+2}}.$$

Sommare prima su ω e poi su n porta al risultato cercato. □

Proposizione 2.44. *La funzione* $\wp$ *di Weierstrass verifica*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Dimostrazione. Scrivendo esplicitamente i primi termini degli sviluppi di $\wp$ e $\wp'$ abbiamo

$$\begin{aligned} \wp(z) &= z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \dots \\ \wp'(z) &= -2z^{-3} + 6G_4 z + 20G_6 z^3 + \dots \end{aligned}$$

Un rapido conto mostra che

$$\begin{aligned} f(z) := \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 = \\ = c_1 z + c_2 z^2 + \dots \end{aligned}$$

è una serie di potenze senza termine noto e senza potenze negative di z. Gli unici poli possibili per f sono quelli di $\wp$ e $\wp'$, cioè gli elementi di L. Ma 0 non è un polo, quindi f è doppiamente periodica senza poli: essa è costante per il teorema 2.35. Il fatto che $f(0) = 0$ permette di concludere che f è identicamente nulla, da cui segue la tesi. □

La proposizione appena scritta ci dice che il punto $(\wp(z), \wp'(z))$ giace sulla curva ellittica di equazione

$$y^2 = 4x^3 - g_2x - g_3 \tag{2.7}$$

dove per ragioni storiche si definiscono $g_2 := 60G_4$ e $g_3 := 140G_6$. In effetti, dovremmo verificare che l'equazione (2.7) definisca effettivamente una curva ellittica.

Proposizione 2.45. *L'equazione* (2.7) *definisce una curva non singolare.*

Dimostrazione. Siano ω_1, ω_2 i generatori di L e sia $\omega_3 := \omega_1 + \omega_2$. Dal fatto che $\wp'$ è dispari e doppiamente periodica segue che

$$\wp'(\omega_i/2) = 0 \text{ per } i = 1, 2, 3.$$

Dunque, ogni $\wp(\omega_i/2)$ è radice di $4X^3 - g_2X - g_3$ per l'equazione (2.7). È sufficiente mostrare che queste radici sono distinte.

Sia $h_i(z) := \wp(z) - \wp(\omega_i/2)$. Abbiamo che $h_i(\omega_i/2) = h_i'(\omega_i/2) = 0$, quindi $\omega_i/2$ è uno zero almeno doppio per h_i. D'altra parte h_i è una funzione doppiamente periodica il cui unico polo nel parallelogramma fondamentale è quello doppio nell'origine. Il teorema 2.35 ci assicura allora che $\omega_i/2$ è l'unico zero di h_i. In particolare $h_i(\omega_j/2) \neq 0$ per $j \neq i$, da cui deduciamo che i valori $\wp(\omega_i/2)$ sono distinti. □

Da quanto visto ha senso considerare la mappa

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{P}^2(\mathbb{C}) \\ z & \longmapsto & [\wp(z) : \wp'(z) : 1]. \end{array}$$

L'immagine di questa mappa nel piano affine $\mathbb{A}^2(\mathbb{C})$ è proprio $E(\mathbb{C})$ definita dall'equazione (2.7). Inoltre, essendo $\wp$ e $\wp'$ periodiche rispetto a L, risulta ben definita una mappa $\mathbb{C}/L \longrightarrow E(\mathbb{C})$.

Teorema 2.46. *La mappa*

$$\begin{array}{rccc} \Phi : & \mathbb{C}/L & \longrightarrow & E(\mathbb{C}) \\ & z & \longmapsto & (\wp(z), \wp'(z)) \quad \textit{se } z \neq 0 \\ & 0 & \longmapsto & O \end{array}$$

è un isomorfismo di gruppi, dove la struttura di gruppo su $\mathbb{C}/L$ è data dalla somma di numeri complessi modulo L.

Dimostrazione. La suriettività è facile. Sia $(x, y) \in E(\mathbb{C})$. La funzione $\wp(z) - x$ ha un polo doppio, quindi per il teorema 2.35 ha zeri: esiste $z \in \mathbb{C}$ tale che $\wp(z) = x$. Di conseguenza

$$\wp'(z)^2 = y^2$$

da cui $\wp'(z) = \pm y$. Se $\wp'(z) = y$, abbiamo finito, altrimenti basta considerare $-z$.

Per quanto riguarda l'iniettività, supponiamo che $\wp(z_1) = \wp(z_2)$ e $\wp'(z_1) = \wp'(z_2)$. Gli unici poli di $\wp$ sono in L, quindi se z_1 è un polo allora $z_1 \in L$ e $z_2 \in L$, quindi $z_1 \equiv z_2 \pmod{L}$. Supponiamo allora che z_1 non sia un polo, e consideriamo

$$h(z) := \wp(z) - \wp(z_1).$$

Tale funzione ha un polo doppio in 0 e non ha altri poli nel parallelogramma fondamentale $\mathcal{P}$. Per il teorema 2.35, ha esattamente due zeri in $\mathcal{P}$. Se $z_1 = \omega_i/2$, dalla dimostrazione della proposizione 2.45 sappiamo che $\wp'(\omega_i/2) = 0$, quindi z_1 è l'unico zero (doppio) di $h(z)$. Segue allora che $z_2 = z_1$. Supponiamo infine che z_1 non sia della forma $\omega_i/2$; in tal caso $h(-z_1) = h(z_1) = 0$ ma $-z_1 \not\equiv z_1 \pmod{L}$. Supponendo per assurdo allora che $z_1 \not\equiv z_2 \pmod{L}$, necessariamente $z_2 \equiv -z_1 \pmod{L}$. Ma questo porta a

$$y := \wp'(z_2) = \wp'(-z_1) = -\wp'(z_1) = -y$$

da cui $\wp'(z_1) = y = 0$. Questa è una contraddizione, in quanto l'unico polo di $\wp'$ è triplo nell'origine, quindi per il teorema 2.35 $\wp'$ ha esattamente tre zeri, che avevamo individuato in $\omega_i/2$ nel corso della dimostrazione della proposizione 2.45. Quindi $z_1 \equiv z_2 \pmod{L}$ e Φ è iniettiva.

Dobbiamo solo mostrare che Φ (o equivalentemente Φ^{-1}) è un omomorfismo di gruppi. Per fare ciò, studiamo l'intersezione di una retta $y = mx + q$ con la curva. La funzione

$$h(z) := \wp'(z) - (m\wp(z) + q)$$

ha un polo triplo in ciascun punto di L, quindi h ha tre zeri z_1, z_2 e z_3 in $\mathcal{P}$. In particolare $\operatorname{div}(h) = [z_1] + [z_2] + [z_3] - 3[0]$ e dal Teorema di Abel-Jacobi abbiamo $z_1 + z_2 + z_3 \in L$. In altre parole, i tre punti di intersezione di $y = mx + q$ con E, che sommano a O in E, vengono mappati tramite Φ^{-1} in tre punti che sommano a 0 in $\mathbb{C}/L$. Questo conclude la dimostrazione del teorema. □

Abbiamo visto che un reticolo su $\mathbb{C}$ definisce una curva ellittica. Quello che vogliamo dimostrare ora è il viceversa: data una curva ellittica, è possibile costruire un reticolo L tale che la curva ellittica sia isomorfa a $\mathbb{C}/L$. In realtà descriveremo a grandi linee i passi da compiere per giungere a questa dimostrazione: rimandiamo a [15] per i dettagli.

Per prima cosa occorre trovare un invariante che identifichi una curva ellittica a meno di cambiamento di coordinate. La conoscenza dell'equazione di Weierstrass non è sufficiente, in quanto due equazioni diverse possono dare origine alla stessa curva. L'unico cambiamento di coordinate che preserva la struttura dell'equazione di Weierstrass $y^2 = x^3 + ax + b$ (con $a, b \in \mathbb{K}$) è

$$\begin{cases} x_1 = u^2 x \\ y_1 = u^3 y \end{cases} \tag{2.8}$$

per qualche $u \in \overline{\mathbb{K}}^*$; i nuovi coefficienti dell'equazione di Weierstrass sono $a_1 = u^4 a$ e $b_1 = u^6 b$.

Definizione 2.47. Sia $E/_{\mathbb{K}}$ una curva ellittica data dall'equazione $y^2 = x^3 + ax + b$. Definiamo j-*invariante* la quantità

$$j = j(E) := 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Notiamo che il denominatore è non nullo sotto l'ipotesi di non singolarità della curva.

Teorema 2.48. *Siano* E_1 *ed* E_2 *due curve ellittiche definite su* $\mathbb{K}$ *date da equazioni di Weierstrass* $y_1^2 = x_1^3 + a_1 x_1 + b$ *e* $y_2^2 = x_2^3 + a_2 x_2 + b$ *e siano* j_1 *e* j_2 *i rispettivi* j-*invarianti. Allora* $j_1 = j_2$ *se e solo se esiste* $u \in \overline{\mathbb{K}}^*$ *tale che* $a_2 = u^4 a_1$ *e* $b_2 = u^6 b_1$. *In tal caso, la trasformazione* (2.8) *manda un'equazione di Weierstrass nell'altra.*

Dimostrazione. $\boxed{\Leftarrow}$ È un conto:

$$j_2 = 1728 \frac{4a_2^3}{4a_2^3 + 27b_2^2} = 1728 \frac{4a_1^3 u^{12}}{(4a_1^3 + 27b_1^2)u^{12}} = 1728 \frac{4a_1^3}{4a_1^3 + 27b_1^2} = j_1.$$

$\boxed{\Rightarrow}$ Supponiamo dapprima che $a_1 \neq 0$. Dato che questo è equivalente a $j_1 \neq 0$, abbiamo anche $a_2 \neq 0$. Scegliamo u tale che $a_2 = u^4 a_1$. Allora

$$\frac{4a_2^3}{4a_2^3 + 27b_2^2} = \frac{4a_1^3}{4a_1^3 + 27b_1^2} = \frac{4a_2^3 u^{-12}}{4u^{-12}a_2^3 + 27b_1^2} = \frac{4a_2^3}{4a_2^3 + 27u^{12}b_1^2},$$

che implica che $b_2^2 = (u^6 b_1)^2$, da cui $b_2 = \pm u^6 b_1$. Se $b_2 = u^6 b_1$, abbiamo finito; altrimenti, cambiamo u con iu: questo mantiene $a_2 = u^4 a_1$ e soddisfa $b_2 = u^6 b_1$.

Se invece $a_1 = 0$, allora anche $a_2 = 0$. Dal fatto che $4a_i^3 + 27b_i^2 \neq 0$ per $i = 1, 2$ possiamo dedurre che $b_1, b_2 \neq 0$. Basta allora scegliere u tale che $b_2 = u^6 b_1$. □

Il j-invariante si può ricavare a partire da considerazioni sui reticoli. In effetti, l'idea della costruzione del reticolo è proprio questa: data una curva ellittica, ne si calcola il j-invariante, quindi si trova un reticolo che abbia proprio quello come j-invariante.

Per prima cosa ci riconduciamo a reticoli parametrizzati da un singolo numero complesso. Sia (ω_1, ω_2) una base di un reticolo L, e definiamo

$$\tau := \frac{\omega_1}{\omega_2}.$$

Dato che ω_1 e ω_2 sono $\mathbb{R}$-linearmente indipendenti, τ non può essere reale. A meno di scambiare ω_1 e ω_2 possiamo supporre che la parte immaginaria di τ sia positiva, cioè che

$$\tau \in \mathcal{H} := \{z \in \mathbb{C} \mid \mathfrak{Im}(z) > 0\}.$$

Il reticolo L_τ che ha per base $(1, \tau)$ è omotetico a L, cioè esiste $\lambda \in \mathbb{C}$ non nullo tale che $\lambda L_\tau = L$. Nel nostro caso $\lambda = \omega_2$.

A partire da τ, possiamo definire le serie di Eisenstein esattamente come prima:

$$G_k(\tau) := G_k(L_\tau) = \sum_{(m,n)\in\mathbb{Z}^2\smallsetminus\{(0,0)\}} \frac{1}{(m\tau + n)^k},$$

e vale $G_k(\tau) = \omega_2^k G_k(L)$.

Una volta ottenute le serie di Eisenstein, possiamo calcolare anche

$$g_2 := g_2(\tau) = 60G_4(\tau)$$
$$g_3 := g_3(\tau) = 140G_6(\tau)$$

e di conseguenza

$$j(\tau) := 1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}.$$

Questo corrisponde al j-invariante associato alla curva definita dall'equazione (2.7)

$$y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

ottenuta a partire dal reticolo L_τ. Definiamo per comodità

$$q := e^{2\pi i\tau}$$

e notiamo che, poiché $\tau \in \mathcal{H}$, $|q| < 1$, quindi le serie di potenze in q convergono. In particolare, un calcolo diretto mostra che

$$j(\tau) = q^{-1} + 744 + 196844q + 21493760q^2 + \dots$$

anche se esistono altre espressioni di $j(\tau)$ più efficienti ai fini del calcolo.

Più in generale, per un reticolo L si può definire

$$j(L) := 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2}.$$

Osserviamo che per $\lambda \in \mathbb{C}^*$, le definizioni delle serie di Eisenstein implicano che

$$j(\lambda L) = j(L).$$

In particolare se L è il reticolo generato da (ω_1, ω_2), allora $j(L) = j(\tau)$ con $\tau = \omega_1/\omega_2$.

Ricordiamo ora che il gruppo

$$\mathsf{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

agisce su $\mathcal{H}$ con

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Lemma 2.49. *Siano $\tau \in \mathcal{H}$ e $A \in \mathsf{SL}_2(\mathbb{Z})$. Allora*

$$j(A \cdot \tau) = j(\tau).$$

Lemma 2.50. *L'insieme*

$$\mathcal{F} := \left\{ z \in \mathcal{H} \;\middle|\; |z| \geqslant 1,\ -\frac{1}{2} \leqslant \mathfrak{Re}(z) < \frac{1}{2},\ z \neq e^{i\theta} \text{ per } \frac{\pi}{3} < \theta < \frac{\pi}{2} \right\}$$

è un dominio fondamentale per l'azione di $\mathsf{SL}_2(\mathbb{Z})$ su $\mathcal{H}$. In altre parole, fissato $\tau \in \mathcal{H}$, esiste $A \in \mathsf{SL}_2(\mathbb{Z})$ tale che $z := A \cdot \tau \in \mathcal{F}$, e tale z è univocamente determinato da τ.

Nella figura 2.6 si è chiamato $\rho := e^{2\pi i/3}$ perché esso svolge un ruolo importante nel seguito. In effetti ciò è intuibile dal fatto che $j(\rho) = 0$.

Corollario 2.51. *Sia L un reticolo su $\mathbb{C}$. Esiste una base (ω_1, ω_2) di L tale che $\omega_1/\omega_2 \in \mathcal{F}$. In altre parole,*

$$L = \lambda(\mathbb{Z}\tau + \mathbb{Z})$$

per qualche $\lambda \in \mathbb{C}^*$ e qualche $\tau \in \mathcal{F}$ univocamente determinato.

Ricordiamo che per $z \in \mathbb{C}$ e f meromorfa è definito l'ordine $\mathrm{ord}_z(f)$ come l'intero per cui

$$f(\tau) = (\tau - z)^{\mathrm{ord}_z(f)} g(\tau)$$

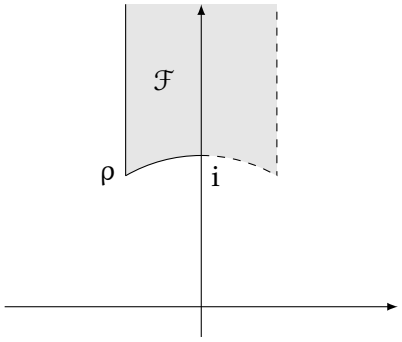


Figura 2.6: Dominio fondamentale per l'azione di $\mathsf{SL}_2(\mathbb{Z})$ su $\mathcal{H}$.

con $g(z) \neq 0$ e $g(z) \neq \infty$. Vorremmo definire l'ordine di f nel punto $i\infty$, cioè sapere cosa succede andando all'infinito in $\mathcal{F}$. Supponiamo di poter scrivere

$$f(\tau) = a_n q^n + a_{n+1} q^{n+1} + \dots$$

con $n \in \mathbb{Z}$, $a_n \neq 0$ (con q definito come sopra) e supponiamo inoltre che la serie converga in un intorno di $q = 0$. Allora poniamo

$$\operatorname{ord}_{i\infty}(f) = n.$$

In effetti per $\tau \longrightarrow i\infty$ si ha $q \longrightarrow 0$, quindi $\operatorname{ord}_{i\infty}(f)$ esprime il fatto che f si annulli ($n > 0$) o vada all'infinito ($n < 0$) per $\tau \longrightarrow i\infty$.

Proposizione 2.52. *Sia f una funzione meromorfa su $\mathcal{H}$ non identicamente nulla e tale che $f(A \cdot \tau) = f(\tau)$ per ogni $A \in \mathsf{SL}_2(\mathbb{Z})$. Allora*

$$\operatorname{ord}_{i\infty}(f) + \frac{1}{3}\operatorname{ord}_{\rho}(f) + \frac{1}{2}\operatorname{ord}_{i}(f) + \sum_{\substack{z \in \mathcal{H} \\ z \neq \rho, i}} \operatorname{ord}_z(f) = 0.$$

In parole povere, questa proposizione ci dice che il numero di zeri di f è uguale al numero di poli di f vista come funzione definita sulla superficie ottenuta identificando i lati sinistro e destro di $\mathcal{F}$, quindi ripiegando la parte con $|z| = 1$ su i e infine collassando l'estremità $i\infty$ a un punto. (Questa superficie è topologicamente una sfera.) Il punto i è speciale nel senso che un piccolo disco intorno a i è contenuto solo per metà in $\mathcal{F}$, mentre ρ è speciale perché $\mathcal{F}$ contiene solo un terzo di disco (un sesto intorno a ρ e un sesto intorno a $\rho + 1$, che è stato incollato a ρ). Questa spiegazione visiva giustifica i coefficienti $1/2$ e $1/3$ nella proposizione.

La proposizione precedente, unitamente a qualche altra considerazione, ci permette di dimostrare che la funzione $h(\tau) := j(\tau) - z$ per $z \in \mathbb{C}$ fissato ha un unico zero in $\mathcal{F}$. Racchiudiamo questo fatto in una proposizione.

Proposizione 2.53. *Se $z \in \mathbb{C}$, esiste un unico $\tau \in \mathcal{F}$ tale che $z = j(\tau)$.*

Corollario 2.54. *Siano $\tau_1, \tau_2 \in \mathcal{H}$. Allora $j(\tau_1) = j(\tau_2)$ se e solo se esiste $A \in \mathsf{SL}_2(\mathbb{Z})$ tale che $A \cdot \tau_1 = \tau_2$.*

Corollario 2.55. *Siano L_1, L_2 due reticoli. Allora $j(L_1) = j(L_2)$ se e solo se esiste $\lambda \in \mathbb{C}^*$ tale che $\lambda L_1 = L_2$.*

Possiamo finalmente enunciare il teorema principale.

Teorema 2.56. *Sia $E/_{\mathbb{C}}$ una curva ellittica definita dall'equazione $y^2 = 4x^3 - ax - b$. Allora esiste un reticolo L tale che $g_2(L) = a$ e $g_3(L) = b$. Di conseguenza, esiste un isomorfismo di gruppi tra $\mathbb{C}/_L$ e $E(\mathbb{C})$.*

Dimostrazione. Sia

$$j := 1728\frac{a^3}{a^3 - 27b^2}.$$

Dalla proposizione 2.53 esiste un reticolo $L := \mathbb{Z}\tau + \mathbb{Z}$ tale che $j(\tau) = j(L) = j$. Supponiamo dapprima che $a \neq 0$. In tal caso $j \neq 0$, quindi $g_2(L) \neq 0$. Scegliamo $\lambda \in \mathbb{C}^*$ tale che

$$g_2(\lambda L) = \lambda^{-4} g_2(L) = a.$$

Di conseguenza $g_3(\lambda L)^2 = b^2$, quindi $g_3(\lambda L) = \pm b$. Se $g_3(\lambda L) = b$, abbiamo finito, altrimenti $g_3(i\lambda L) = i^{-6} g_3(\lambda L) = b$ e $g_2(i\lambda L) = i^{-4} g_2(\lambda L) = a$. Dunque uno tra λL e $i\lambda L$ è il reticolo cercato.

Se invece $a = 0$ (e dunque anche $j = 0$ e $g_2(L) = 0$), dalla non singolarità abbiamo che $b \neq 0$ e $g_3(L) \neq 0$. Sia allora $\mu \in \mathbb{C}^*$ tale che

$$g_3(\mu L) = \mu^{-6} g_3(L) = b.$$

Allora $g_2(\mu L) = \mu^{-4} g_2(L) = 0 = a$, quindi μL è il reticolo cercato. □

L'identificazione delle curve ellittiche con i tori complessi rende particolarmente facile visualizzare i punti di n-torsione. Infatti, se L è generato da (ω_1, ω_2), i punti di n-torsione sono esattamente

$$\left\{ \frac{j}{n}\omega_1 + \frac{k}{n}\omega_2 \;\middle|\; 0 \leqslant j, k \leqslant n-1 \right\}$$

i quali in effetti sono proprio n^2.

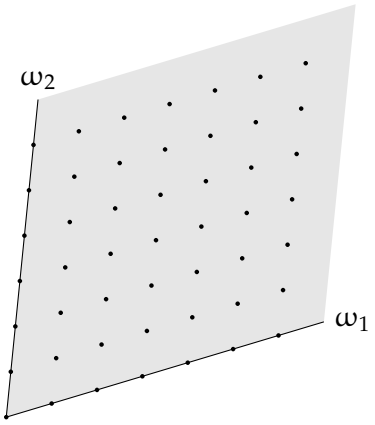


Figura 2.7: Punti di 7-torsione.

2.8 Divisori

Dopo aver visto una introduzione ai divisori nella sezione 2.7, generalizziamo questi oggetti per una curva ellittica qualsiasi. Questo ci permetterà di chiudere due questioni lasciate in sospeso: l'associatività della legge di gruppo (sezione 2.2) e l'esistenza dell'accoppiamento di Weil (sezione 2.5).

Definizione 2.57. Sia $E/_{\mathbb{K}}$ una curva ellittica. Per ogni punto $P \in E(\overline{\mathbb{K}})$ definiamo un simbolo formale $[P]$. Un *divisore* D su E è una combinazione lineare finita di tali simboli a coefficienti in $\mathbb{Z}$, cioè

$$D = \sum_{P \in E(\overline{\mathbb{K}})} a_P [P]$$

con $a_P \in \mathbb{Z}$, $a_P \neq 0$ solo per un numero finito di P. Il gruppo dei divisori su E è indicato con $\mathrm{Div}(E)$.

Possiamo definire *grado* di un divisore la quantità

$$\deg\left(\sum_{P \in E(\overline{\mathbb{K}})} a_P [P]\right) := \sum_{P \in E(\overline{\mathbb{K}})} a_P \in \mathbb{Z}$$

e *somma* di un divisore il punto

$$\mathrm{sum}\left(\sum_{P \in E(\overline{\mathbb{K}})} a_P [P]\right) := \sum_{P \in E(\overline{\mathbb{K}})} a_P P \in E(\overline{\mathbb{K}}).$$

I divisori di grado 0 formano un sottogruppo di $\mathrm{Div}(E)$, indicato con $\mathrm{Div}^0(E)$. La funzione somma ristretta a $\mathrm{Div}^0(E)$ dà un omomorfismo di gruppi suriettivo

$$\mathrm{sum} : \mathrm{Div}^0(E) \twoheadrightarrow E(\overline{\mathbb{K}}).$$

La suriettività discende dal fatto che $\mathrm{sum}([P] - [O]) = P$ per ogni $P \in E(\overline{\mathbb{K}})$.

Una funzione su E è una funzione razionale $f(x, y) \in \overline{\mathbb{K}}(x, y)$ definita su almeno un punto di E. In pratica, se E è data da $y^2 = x^3 + ax + b$, l'insieme delle funzioni su E (denotato con $\overline{\mathbb{K}}(E)$) corrisponde al campo dei quozienti di

$$\overline{\mathbb{K}}[E] := \overline{\mathbb{K}}[X, Y] \big/ (Y^2 - X^3 - aX - b) \cdot$$

Una funzione su E è a valori in $\overline{\mathbb{K}} \cup \{\infty\}$. Diciamo che P è uno *zero* per f se $f(P) = 0$, ed è un *polo* per f se $f(P) = \infty$. È possibile dimostrare in generale (si veda per esempio [14]) che fissato un punto P esiste una funzione u_P, detta *uniformizzante*, tale che $u_P(P) = 0$ e ogni funzione $f \in \overline{\mathbb{K}}(E)$ possa essere scritta come

$$f = u_P^r g$$

per qualche $r \in \mathbb{Z}$, per una qualche funzione g con $g(P) \neq 0, \infty$. Definiamo allora *ordine* di f in P

$$\mathrm{ord}_P(f) := r.$$

In particolare, se $r > 0$, f ha uno zero di ordine r in P, mentre se $r < 0$ f ha un polo di ordine $-r$ in P.

Anche a funzioni definite su E è possibile associare un divisore: se $f \in \overline{\mathbb{K}}(E)$ poniamo

$$\mathrm{div}(f) := \sum_{P \in E(\overline{\mathbb{K}})} \mathrm{ord}_P(f)[P].$$

Un divisore della forma $\mathrm{div}(f)$ per qualche f è detto *divisore principale*. La somma è finita in virtù della seguente proposizione, di cui omettiamo la dimostrazione.

Proposizione 2.58. *Siano* $E/_{\mathbb{K}}$ *una curva ellittica e* $f \in \overline{\mathbb{K}}(E)$ *non identicamente nulla.*

1. f *ha un numero finito di zeri e poli.*
2. $\deg(\mathrm{div}(f)) = 0$.
3. *Se* f *non ha zeri né poli (cioè* $\mathrm{div}(f) = 0$*), allora* f *è costante.*

Teorema 2.59. *Siano* E *una curva ellittica e* $D \in \mathrm{Div}(E)$ *con* $\deg(D) = 0$. *Allora esiste* $f \in \overline{\mathbb{K}}(E)$ *tale che* $D = \mathrm{div}(f)$ *se e solo se* $\mathrm{sum}(D) = O$.

Questo teorema ci dice sostanzialmente che

$$\ker\left(\text{sum}\big|_{\text{Div}^0(E)}\right) = \{\text{divisori principali}\},$$

e di conseguenza che $E(\overline{\mathbb{K}})$ è isomorfo a $\text{Div}^0(E)$ quozientato per il sottogruppo dei divisori principali.

Prima di dimostrare il teorema 2.59 ci occorrono diversi lemmi. Il primo è tecnico e ne omettiamo la dimostrazione, che si può comunque trovare in [15].

Lemma 2.60. *Siano $P_1, P_2 \in \overline{\mathbb{K}}[T]$ due polinomi senza radici comuni. Supponiamo che esistano quattro punti distinti $[a_i : b_i] \in \mathbb{P}^1(\overline{\mathbb{K}})$, $i = 1, \dots, 4$ tali che $a_i P_1 + b_i P_2$ sia un quadrato per ogni $i = 1, \dots, 4$. (Ovviamente questa condizione non dipende dalla scelta dei rappresentanti dei punti in $\mathbb{P}^1(\overline{\mathbb{K}})$.) Allora P_1 e P_2 sono costanti.*

Lemma 2.61. *Sia $E/_{\mathbb{K}}$ una curva ellittica definita da $y^2 = x^3 + ax + b$ e sia T un'indeterminata. Non esistono $x(T), y(T) \in \overline{\mathbb{K}}(T)$ non costanti tali che*

$$y(T)^2 = x(T)^3 + ax(T) + b.$$

Dimostrazione. Fattorizziamo

$$X^3 + aX + B = (X - e_1)(X - e_2)(X - e_3)$$

con $e_1, e_2, e_3 \in \overline{\mathbb{K}}$ distinti. Supponiamo che esistano $x(T), y(T)$ come nelle ipotesi. Scriviamo

$$x(T) = \frac{p_1(T)}{p_2(T)}, \qquad y(T) = \frac{q_1(T)}{q_2(T)}$$

con $p_1, p_2, q_1, q_2 \in \overline{\mathbb{K}}[T]$, p_1 e p_2 coprimi così come q_1 e q_2. Sostituendo otteniamo

$$q_1^2 p_2^3 = q_2^2(p_1^3 + a p_1 p_2^2 + b p_2^3). \tag{2.9}$$

Il membro di destra è un multiplo di q_2^2, quindi lo è anche quello di sinistra. Poiché q_1 e q_2 non hanno radici comuni, p_2^3 è un multiplo di q_2^2. D'altra parte p_2 e $p_1^3 + a p_1 p_2^2 + b p_2^3$ non possono avere radici comuni (una eventuale radice comune sarebbe radice anche di p_1, e ciò è impossibile per coprimalità di p_1 e p_2). Quindi q_2^2 è un multiplo di p_2^3.

Ne consegue che p_2^3 e q_2^2 sono multipli scalari l'uno dell'altro; aggiustando opportunamente con delle costanti p_1 e q_1 possiamo fare in modo che

$$p_2^3 = q_2^2.$$

Semplificando allora nell'equazione (2.9) abbiamo

$$q_1^2 = p_1^3 + a p_1 p_2^2 + b p_2^3 = (p_1 - e_1 p_2)(p_1 - e_2 p_2)(p_1 - e_3 p_2).$$

Supponiamo che $p_1 - e_i p_2$ e $p_1 - e_j p_2$ abbiano una radice comune r per $i \neq j$. Allora r è radice di

$$e_j(p_1 - e_i p_2) - e_i(p_1 - e_j p_2) = (e_j - e_i)p_1$$

e anche di

$$(p_1 - e_i p_2) - (p_1 - e_j p_2) = (e_j - e_i)p_2,$$

ma $e_i \neq e_j$ implica che r è radice comune di p_1 e p_2, in contraddizione con le ipotesi. Quindi $p_1 - e_i p_2$ e $p_1 - e_j p_2$ non hanno radici comuni per $i \neq j$. Da questo e dal fatto che

$$(p_1 - e_1 p_2)(p_1 - e_2 p_2)(p_1 - e_3 p_2)$$

è un quadrato segue che anche ciascuno dei fattori lo è. Inoltre abbiamo visto sopra che anche p_2 è un quadrato (discende dal fatto che $p_2^3 = q_2^2$). A questo punto applichiamo il lemma 2.60 ai polinomi p_1 e p_2 con i punti

$$[1 : -e_1],\ [1 : -e_2],\ [1 : -e_3],\ [0 : 1]$$

per concludere che p_1 e p_2 sono costanti. Ma $x = p_1/p_2$ non è costante per ipotesi, e questo porta alla dimostrazione del lemma. □

Lemma 2.62. *Siano* $P, Q \in E(\overline{\mathbb{K}})$ *per i quali esista* $h \in \overline{\mathbb{K}}(E)$ *tale che*

$$\operatorname{div}(h) = [P] - [Q].$$

Allora $P = Q$.

Dimostrazione. Supponiamo che $P \neq Q$. Per ogni costante c la funzione $h - c$ ha esattamente un polo semplice in Q, quindi deve avere esattamente uno zero semplice.

Sia ora $f \in \overline{\mathbb{K}}(E)$ e supponiamo dapprima che $\operatorname{ord}_Q(f) = 0$. Definiamo

$$g(x, y) := \prod_{R \in E(\overline{\mathbb{K}})} (h(x, y) - h(R))^{\operatorname{ord}_R(f)}.$$

Il fattore per $R = Q$ è 1 in quanto $\operatorname{ord}_Q(f) = 0$. Per costruzione $\operatorname{div}(g) = \operatorname{div}(f)$: ogni fattore ha uno zero o un polo nello stesso punto in cui ce l'ha f, e in più uno zero o un polo in Q di ordine $|\operatorname{ord}_R(f)|$. Dato che $\sum \operatorname{ord}_R(f) = 0$, il contributo dei fattori al punto Q si cancella, quindi Q non è zero né polo di g.

Da $\operatorname{div}(g) = \operatorname{div}(f)$ deduciamo che f/g non ha zeri né poli, quindi è costante. In altre parole, f è funzione razionale di h.

Il ragionamento non funziona se f ha uno zero o un polo in Q. Tuttavia possiamo applicarlo a $fh^{\mathrm{ord}_Q(f)}$, la quale non ha uno zero né un polo in Q, e ottenere ancora che f è funzione razionale di h.

Concludiamo dunque che ogni funzione $f \in E(\overline{\mathbb{K}})$ è funzione razionale di h, e in particolare anche le funzioni coordinate x e y lo sono, in contraddizione con il lemma 2.61. Questo conclude la dimostrazione. □

Dimostrazione del teorema 2.59. Consideriamo la retta di equazione $rx + sy + t = 0$ e supponiamo che essa intersechi E in tre punti distinti P_1, P_2, P_3. Quindi

$$\mathrm{div}(rx + sy + t) = [P_1] + [P_2] + [P_3] - 3[O].$$

La retta che passa per $P_3 = (x_3, y_3)$ e $-P_3$ è $x - x_3 = 0$, il cui divisore è

$$\mathrm{div}(x - x_3) = [P_3] + [-P_3] - 2[O].$$

Di conseguenza

$$\mathrm{div}\left(\frac{rx + sy + t}{x - x_3}\right) = \mathrm{div}(rx + sy + t) - \mathrm{div}(x - x_3) = [P_1] + [P_2] - [-P_3] - [O].$$

Dal momento che su E si ha $P_1 + P_2 = -P_3$, otteniamo

$$[P_1] + [P_2] = [P_1 + P_2] + [O] + \mathrm{div}\left(\frac{rx + sy + t}{x - x_3}\right). \tag{2.10}$$

Chiamiamo g la funzione $(rx + sy + t)/(x - x_3)$. Notiamo che

$$\mathrm{sum}(\mathrm{div}(g)) = P_1 + P_2 - (P_1 + P_2) - O = O.$$

Notiamo inoltre che se $P_1 + P_2 = O$, allora $[P_1] + [P_2] = 2[O] + \mathrm{div}(h)$ per qualche h.

Sia allora D il divisore come da ipotesi. Accorpando tutti i termini in D con coefficienti positivi e tutti quelli con coefficienti negativi, troviamo infine che esistono $P, Q \in E$, $n \in \mathbb{Z}$ e $g_1 \in \overline{\mathbb{K}}(E)$ tali che

$$D = [P] - [Q] + n[O] + \mathrm{div}(g_1)$$

ove g_1 è quoziente di prodotti di funzioni g tali che $\mathrm{sum}(\mathrm{div}(g)) = O$, quindi $\mathrm{sum}(\mathrm{div}(g_1)) = O$.

Dalla proposizione 2.58 abbiamo che $\deg(\mathrm{div}(g_1)) = 0$, quindi

$$0 = \deg(D) = 1 - 1 + n + 0 = n$$

da cui $n = 0$ e $D = [P] - [Q] + \mathrm{div}(g_1)$. In più

$$\mathrm{sum}(D) = P - Q + \mathrm{sum}(\mathrm{div}(g_1)) = P - Q.$$

$\boxed{\Leftarrow}$ Se $\mathrm{sum}(D) = O$, allora $P - Q = O$, da cui $P = Q$ e $D = \mathrm{div}(g_1)$.
$\boxed{\Rightarrow}$ Se $D = \mathrm{div}(f)$ per qualche f, allora $[P] - [Q] = \mathrm{div}(f/g_1)$. Per il lemma 2.62 allora $P = Q$ e quindi $\mathrm{sum}(D) = O$. □

Il teorema 2.59 ci permette di dimostrare finalmente l'associatività della legge di gruppo su una curva ellittica. Infatti la somma in $\mathrm{Div}(E)$ è associativa per definizione. Scriviamo dall'equazione (2.10)

$$[P_1] + [P_2] = [P_1 + P_2] + [O] + \mathrm{div}(g_1)$$
$$[P_2] + [P_3] = [P_2 + P_3] + [O] + \mathrm{div}(g_2).$$

Uguagliando $([P_1] + [P_2]) + [P_3]$ e $[P_1] + ([P_2] + [P_3])$ ricaviamo

$$[P_1 + P_2] + [P_3] - [P_1] - [P_2 + P_3] = \mathrm{div}(g_2/g_1)$$

e dal teorema 2.59 abbiamo allora

$$(P_1 + P_2) + P_3 - P_1 - (P_2 + P_3) = O$$

da cui $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

Nella sezione 2.5 avevamo lasciato in sospeso l'esistenza dell'accoppiamento di Weil. Vediamo ora come usare i divisori per costruirlo. Siano $E/_{\mathbb{K}}$ una curva ellittica, n un intero primo con $\mathrm{char}(\mathbb{K})$ e supponiamo che $E[n] \subset E(\mathbb{K})$. Vogliamo costruire una mappa

$$e_n : E[n] \times E[n] \longrightarrow \mu_n$$

dove μ_n è il gruppo delle radici n-esime dell'unità in $\overline{\mathbb{K}}$ (che per il corollario 2.27 è contenuto in $\mathbb{K}$).

Sia $T \in E[n]$. Dato che $\deg(n[T] - n[O]) = 0$ e $\mathrm{sum}(n[T] - n[O]) = O$, per il teorema 2.59 esiste $f \in \overline{\mathbb{K}}(E)$ tale che

$$\mathrm{div}(f) = n[T] - n[O].$$

Sia $T_1 \in E[n^2]$ (quindi non necessariamente in $E(\mathbb{K})$) tale che $nT_1 = T$. Consideriamo il divisore

$$D := \sum_{R \in E[n]} ([T_1 + R] - [R]).$$

Ovviamente $\deg(D) = 0$; chi è $\mathrm{sum}(D)$? Notando che ci sono n^2 punti in $E[n]$ e che i contributi di R si cancellano, abbiamo

$$\mathrm{sum}(D) = n^2 T_1 = nT = O,$$

quindi esiste g tale che $D = \mathrm{div}(g)$. Osserviamo che g non dipende dalla scelta di T_1, in quanto se T_2 è tale che $nT_2 = T$ allora $T_1 - T_2 \in E[n]$.

Indichiamo con $f \circ n$ la composizione di f con la mappa di moltiplicazione per n. La mappa f ha uno zero di ordine n in T, cioè in nP per ogni $P = T_1 + R$ al variare di $R \in E[n]$; inoltre ha un polo di ordine n in O, cioè in nR per ogni $R \in E[n]$. Quindi

$$\mathrm{div}(f \circ n) = n\left(\sum_{R \in E[n]} [T_1 + R]\right) - n\left(\sum_{R \in E[n]} [R]\right) = \mathrm{div}(g^n)$$

da cui segue che $f \circ n$ è un multiplo scalare di g^n, e possiamo assumere $f \circ n = g^n$ a meno di riscalare f. Ricordiamo che f e g dipendono da T.

Sia ora $S \in E[n]$ e $P \in E(\overline{\mathbb{K}})$. Allora

$$g(P + S)^n = f(n(P + S)) = f(nP) = g(P)^n$$

da cui $g(P + S)/g(P) \in \mu_n$. In effetti $g(P + S)/g(P)$ non dipende dal punto P. (Un'idea della dimostrazione di questo fatto è: la funzione $P \mapsto g(P + S)/g(P)$ è continua rispetto alla topologia di Zariski, E è connesso e μ_n è discreto e finito, quindi tale funzione dev'essere costante.) In più, poiché g è determinata a meno di un multiplo scalare, il rapporto è indipendente dalla scelta di g.

Definizione 2.63. Definiamo *accoppiamento di Weil* la mappa

$$\begin{aligned} e_n : \quad E[n] \times E[n] &\longrightarrow \mu_n \\ (S, T) &\longmapsto \frac{g(P + S)}{g(P)}. \end{aligned}$$

Teorema 2.64. *Come preannunciato nella sezione 2.5, l'accoppiamento di Weil gode delle seguenti proprietà:*

1. *è lineare in ogni argomento: per ogni* $S, S_1, S_2, T, T_1, T_2 \in E[n]$

$$\begin{aligned} e_n(S_1 + S_2, T) &= e_n(S_1, T) e_n(S_2, T) \\ e_n(S, T_1 + T_2) &= e_n(S, T_1) e_n(S, T_2); \end{aligned}$$

2. *è non degenere in ogni argomento:*

$$\begin{aligned} e_n(S, T) = 1 \ \forall T \in E[n] &\Rightarrow S = O \\ e_n(S, T) = 1 \ \forall S \in E[n] &\Rightarrow T = O; \end{aligned}$$

3. *per ogni* $T \in E[n]$ *si ha* $e_n(T,T) = 1$*;*

4. *per ogni* $S,T \in E[n]$ *si ha* $e_n(S,T) = e_n(T,S)^{-1}$*;*

5. *per ogni* $S,T \in E[n]$ *e per ogni* σ *automorfismo di* $\overline{\mathbb{K}}$ *che lasci fisso* $\mathbb{K}$ *si ha* $e_n(\sigma S, \sigma T) = \sigma(e_n(S,T))$*;*

6. *per ogni* $S,T \in E[n]$ *e per ogni* α *automorfismo di* E *si ha* $e_n(\alpha(S),\alpha(T)) = e_n(S,T)^{\deg(\alpha)}$.

Dimostrazione. 1. La linearità nel primo argomento è facile: dato che il punto P è arbitrario, possiamo usare P per valutare $e_n(S_1,T)$ e $P+S_1$ per valutare $e_n(S_2,T)$, ottenendo

$$\begin{aligned} e_n(S_1,T)e_n(S_2,T) &= \frac{g(P+S_1)}{g(P)}\frac{g(P+S_1+S_2)}{g(P+S_1)} = \\ &= \frac{g(P+S_1+S_2)}{g(P)} = e_n(S_1+S_2,T). \end{aligned}$$

Per la linearità nel secondo argomento c'è da fare un po' di lavoro in più. Siano $T_1,T_2,T_3 \in E[n]$ tali che $T_1+T_2=T_3$. Siano f_i,g_i le funzioni usate per definire $e_n(S,T_i)$. Sia h tale che

$$\operatorname{div}(h) = [T_3] - [T_1] - [T_2] + [O].$$

Allora

$$\operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) = n\operatorname{div}(h) = \operatorname{div}(h^n)$$

cioè $f_3 = c f_1 f_2 h^n$ per qualche $c \in \overline{\mathbb{K}}^*$. Questo implica

$$g_3^n = f_3 \circ n = c(f_1\circ n)(f_2\circ n)(h\circ n)^n = c g_1^n g_2^n (h\circ n)^n$$

da cui $g_3 = c^{1/n} g_1 g_2 (h\circ n)$. Di conseguenza

$$\begin{aligned} e_n(S,T_1+T_2) &= \frac{g_3(P+S)}{g_3(P)} = \frac{g_1(P+S)}{g_1(P)}\frac{g_2(P+S)}{g_2(P)}\frac{h(n(P+S))}{h(nP)} = \\ &= e_n(S,T_1)e_n(S,T_2) \end{aligned}$$

dove l'ultima uguaglianza è dovuta al fatto che $S \in E[n]$, quindi $h(n(P+S)) = h(nP)$.

2. Abbiamo bisogno di un risultato generale, la cui dimostrazione fa uso della teoria di Galois per estensioni di campi.

Proposizione. *Sia* $E/_{\mathbb{K}}$ *una curva ellittica. Siano* $f \in \overline{\mathbb{K}}(E)$ *e* $n \geqslant 1$ *un intero non divisibile da* $\mathrm{char}(\mathbb{K})$. *Supponiamo che* $f(P+T) = f(P)$ *per ogni* $P \in E(\overline{\mathbb{K}})$ *e per ogni* $T \in E[n]$. *Allora esiste* $h \in \overline{\mathbb{K}}(E)$ *tale che* $f = h \circ n$.

Sia $T \in E[n]$ tale che $e_n(S,T) = 1$ per ogni $S \in E[n]$. Questo significa che $g(P+S) = g(P)$ per ogni $P \in E(\overline{\mathbb{K}})$ e per ogni $S \in E[n]$, quindi dalla proposizione precedente $g = h \circ n$ per qualche h. Segue che $(h \circ n)^n = g^n = f \circ n$ e per suriettività della moltiplicazione per n si ha che $h^n = f$. Dunque

$$n \operatorname{div}(h) = \operatorname{div}(f) = n[T] - n[O]$$

cioè $\operatorname{div}(h) = [T] - [O]$. Dal teorema 2.59 deduciamo $T = O$. La dimostrazione per S segue dal punto 4. e da quanto appena visto per T.

3. Sia τ_{mT} la mappa di traslazione per mT, cosicché $f \circ \tau_{mT}$ rappresenti la mappa $P \longmapsto f(P+mT)$. Il divisore di $f \circ \tau_{mT}$ è $n[T-mT] - n[-mT]$, quindi

$$\operatorname{div}\left(\prod_{m=0}^{n-1} f \circ \tau_{mT}\right) = \sum_{m=0}^{n-1} (n[T-mT] - n[-mT]) = 0.$$

In altre parole, $\prod f \circ \tau_{mT}$ è costante. Ora,

$$\left(\prod_{m=0}^{n-1} g \circ \tau_{mT_1}\right)^n = \prod_{m=0}^{n-1} f \circ n \circ \tau_{mT_1} = \prod_{m=0}^{n-1} f \circ \tau_{mT} \circ n$$

da cui deduciamo che $\prod g \circ \tau_{mT_1}$ è costante. (In realtà stiamo usando il fatto che E è connessa nella topologia di Zariski: altrimenti avremmo potuto solo concludere che $\prod g \circ \tau_{mT_1}$ è costante su ogni componente connessa.) In particolare, la valutazione in P e in $P + T_1$ porta a

$$\prod_{m=0}^{n-1} g(P + T_1 + mT_1) = \prod_{m=0}^{n-1} g(P + mT_1).$$

Cancellando i fattori comuni (e assumendo di aver scelto P in modo che essi siano diversi da 0 e ∞) si ottiene

$$g(P + nT_1) = g(P)$$

ma $nT_1 = T$, dunque

$$e_n(T,T) = \frac{g(P+T)}{g(P)} = 1.$$

4. Dai punti 1. e 3. abbiamo

$$1 = e_n(S+T, S+T) = e_n(S,S)e_n(S,T)e_n(T,S)e_n(T,T) = e_n(S,T)e_n(T,S)$$

da cui la tesi.

5. Sia σ automorfismo di $\overline{\mathbb{K}}$ che lasci fisso $\mathbb{K}$. Applichiamo σ a tutti i passi della costruzione di e_n. Quindi ad esempio

$$\operatorname{div}(f^\sigma) = n[\sigma T] - n[O]$$

e analogamente per g^σ, dove questi simboli denotano le funzioni ottenute da f e g applicando σ ai coefficienti delle funzioni razionali che le definiscono. Di conseguenza

$$\sigma(e_n(S,T)) = \sigma\left(\frac{g(P+S)}{g(P)}\right) = \frac{g^\sigma(\sigma P + \sigma S)}{g^\sigma(\sigma P)} = e_n(\sigma S, \sigma T).$$

6. Dimostreremo questo punto solo nel caso di α endomorfismo separabile e nel caso α endomorfismo di Frobenius (che sono i casi che ci interessano).

Supponiamo α separabile e sia $\ker(\alpha) = \{Q_1, \ldots, Q_k\}$. Dato che α è separabile $\deg(\alpha) = k$. Siano

$$\operatorname{div}(f_T) = n[T] - n[O], \qquad \operatorname{div}(f_{\alpha(T)}) = n[\alpha(T)] - n[O]$$

e analogamente

$$g_T^n = f_T \circ n, \qquad g_{\alpha(T)}^n = f_{\alpha(T)} \circ n.$$

Sia τ_Q la traslazione per Q. Abbiamo

$$\operatorname{div}(f_T \circ \tau_{-Q_i}) = n[T+Q_i] - n[Q_i]$$

da cui ricaviamo che

$$\begin{aligned}\operatorname{div}(f_{\alpha(T)} \circ \alpha) &= n\left(\sum_{\{T_2 | \alpha(T_2) = \alpha(T)\}} [T_2]\right) - n\left(\sum_{\{Q|\alpha(Q)=O\}} [Q]\right) = \\ &= n\sum_{i=1}^{k}([T+Q_i] - [Q_i]) = \\ &= \operatorname{div}\left(\prod_{i=1}^{k}(f_T \circ \tau_{-Q_i})\right).\end{aligned}$$

Per ogni i sia Q'_i tale che $nQ'_i = Q_i$. Allora $g_T(P - Q'_i)^n = f_T(nP - Q_i)$. Ne consegue che

$$\begin{aligned}\operatorname{div}\left(\prod_{i=1}^{k}(g_T \circ \tau_{-Q'_i})^n\right) = \operatorname{div}\left(\prod_{i=1}^{k}(f_T \circ \tau_{-Q_i} \circ n)\right) = \\ = \operatorname{div}(f_{\alpha(T)} \circ \alpha \circ n) = \\ = \operatorname{div}(f_{\alpha(T)} \circ n \circ \alpha) = \\ = \operatorname{div}\left((g_{\alpha(T)} \circ \alpha)^n\right).\end{aligned}$$

Questo implica che $\prod(g_T \circ \tau_{-Q'_i})$ e $g_{\alpha(T)} \circ \alpha$ sono multipli scalari. Ma allora

$$\begin{aligned}e_n(\alpha(S), \alpha(T)) = \frac{g_{\alpha(T)}(\alpha(P+S))}{g_{\alpha(T)}(\alpha(P))} = \\ = \prod_{i=1}^{k}\frac{g_T(P+S-Q'_i)}{g_T(P-Q'_i)} = \\ = \prod_{i=1}^{k} e_n(S,T) = \\ = e_n(S,T)^k = e_n(S,T)^{\deg(\alpha)}.\end{aligned}$$

Se invece $\alpha = \varphi_q$, l'endomorfismo di Frobenius, il punto 5. implica che

$$e_n(\varphi_q(S), \varphi_q(T)) = \varphi_q(e_n(S,T)) = e_n(S,T)^q$$

(infatti φ_q è un automorfismo di $\overline{\mathbb{F}_q}$ che lascia fisso $\mathbb{F}_q$ e agisce come l'elevamento a potenza q-esima). La tesi è dimostrata ricordando che $\deg(\varphi_q) = q$ per il lemma 2.12.

□

Come si calcola effettivamente l'accoppiamento di Weil? Di solito non si trovano esplicitamente f e g usate per la sua costruzione; in effetti, il calcolo del divisore di g richiede una somma estesa a tutti i punti di n-torsione. Il teorema seguente (che non dimostriamo; si veda [15] per i dettagli) ci fornisce un metodo alternativo e più efficiente per calcolare e_n.

Teorema 2.65. *Siano* $S, T \in E[n]$. *Siano* D_S, D_T *due divisori di grado 0 tali che* $\operatorname{sum}(D_S) = S$ *e* $\operatorname{sum}(D_T) = T$ *e tali che i supporti siano disgiunti (cioè non abbiano punti in comune; ad esempio,* $D_S = [S] - [O]$ *e* $D_T = [T+R] - [R]$ *per qualche* R*). Siano poi* f_S, f_T *tali che* $\operatorname{div}(f_S) = nD_S$ *e* $\operatorname{div}(f_T) = nD_T$. *Allora*

$$e_n(S,T) = \frac{f_T(D_S)}{f_S(D_T)},$$

dove si intende che $f\left(\sum a_i[P_i]\right) = \prod f(P_i)^{a_i}$.

2.9 Applicazioni delle curve ellittiche

Tra i problemi computazionalmente difficili usati per definire protocolli crittografici rientra il *problema del logaritmo discreto* (in inglese *Discrete Logarithm Problem*, o DLP). In generale tale problema afferma che dato un gruppo G e due suoi elementi a, b, sapendo che esiste $k \in \mathbb{Z}$ tale che $a^k = b$ trovare k. Il DLP applicato al gruppo dei punti di una curva ellittica si chiama *problema del logaritmo discreto su curve ellittiche* (ECDLP — *Elliptic Curve Discrete Logarithm Problem*).

Ovviamente si può risolvere per forza bruta: se G è finito, si calcolano $a^2, a^3, \dots$ fino a quando uno dei valori funziona. Chiaramente questo metodo è infattibile all'atto pratico. Ci sono algoritmi efficienti per risolvere DLP su $(\mathbb{F}_q)^*$, il gruppo moltiplicativo di un campo finito.

L'*attacco MOV* (da Menezes, Okamoto e Vanstone che l'hanno definito) usa l'accoppiamento di Weil per ricondurre ECDLP su $E(\mathbb{F}_q)$ a un DLP su $(\mathbb{F}_{q^m})^*$, che è un problema trattabile (almeno finché $\mathbb{F}_{q^m}$ non è troppo grosso rispetto a $\mathbb{F}_q$). Per una classe di curve dette *supersingolari*, che introdurremo nel seguito, di solito $m = 2$ va bene; in effetti questo fa sì che le curve supersingolari non siano usate nella definizione di protocolli crittografici.

Sia $E/_{\mathbb{F}_q}$ una curva ellittica e siano $P, Q \in E(\mathbb{F}_q)$. Supponiamo che l'ordine di P sia n e supponiamo anche che $\mathrm{MCD}(n, q) = 1$. Vogliamo trovare k tale che $Q = kP$. Intanto vorremmo sapere se un tale k esiste.

Lemma 2.66. *Nelle ipotesi sopraelencate, esiste* k *tale che* $Q = kP$ *se e solo se* $Q \in E[n]$ *e* $e_n(P, Q) = 1$.

Dimostrazione. $\boxed{\Rightarrow}$ Sia $Q = kP$. Allora $nQ = k(nP) = O$. Inoltre

$$e_n(P, Q) = e_n(P, P)^k = 1.$$

$\boxed{\Leftarrow}$ Dal teorema 2.20 e dal fatto che $\mathrm{MCD}(n, q) = 1$ abbiamo

$$E[n] \simeq {}^{\mathbb{Z}}/_{(n)} \oplus {}^{\mathbb{Z}}/_{(n)}.$$

Sia $R \in E[n]$ tale che (P, R) sia una base per $E[n]$. Possiamo scrivere quindi $Q = aP + bR$ per qualche $a, b \in \mathbb{Z}$. Dalla proposizione 2.26 sappiamo che $e_n(P, R) = \zeta$ è una radice primitiva n-esima dell'unità. Quindi, da $e_n(P, Q) = 1$ ricaviamo

$$1 = e_n(P, Q) = e_n(P, P)^a e_n(P, R)^b = \zeta^b$$

da cui $b \equiv 0 \pmod{n}$. In particolare $bR = O$, quindi $Q = aP$. □

Siamo pronti per dettagliare i passi dell'attacco MOV. In primo luogo si sceglie m in modo che

$$E[n] \subset \mathbb{F}_{q^m}.$$

(Un tale m esiste, perché tutti i punti di $E[n]$ hanno coordinate in $\overline{\mathbb{F}_q} = \bigcup_{j=1}^{\infty} \mathbb{F}_{q^j}$.)
Di conseguenza $\mu_n \subset \mathbb{F}_{q^m}$ e tutti i calcoli saranno svolti in $\mathbb{F}_{q^m}$.

1. Si sceglie $T \in E(\mathbb{F}_{q^m})$ e si calcola il suo ordine r.
2. Sia $d := \text{MCD}(r, n)$ e sia $T_1 := (r/d)T$. In questo modo T_1 ha ordine d che divide n, quindi $T_1 \in E[n]$.
3. Si calcolano $\zeta_1 := e_n(P, T_1)$ e $\zeta_2 := e_n(Q, T_1)$. Entrambe queste radici sono contenute in $(\mathbb{F}_{q^m})^*$.
4. Si risolve il DLP $\zeta_2 = \zeta_1^k$ in $(\mathbb{F}_{q^m})^*$. Questo ci dà k modulo d.
5. Si ripete con altri punti T finché il minimo comune multiplo dei vari d usati sia n. Questo ci permette di ricostruire k modulo n, risolvendo ECDLP.

Potenzialmente l'intero m potrebbe essere grande: avremmo ricondotto il problema DLP da un gruppo di ordine circa q (per il Teorema di Hasse) a uno di ordine $q^m - 1$.

Definizione 2.67. Sia $E/_{\mathbb{F}_q}$ una curva ellittica con $p = \text{char}(\mathbb{F}_q)$. Sia a tale che

$$\#E(\mathbb{F}_q) = q + 1 - a.$$

La curva è detta *supersingolare* se $a \equiv 0 \pmod{p}$.

Equivalentemente, $E/_{\mathbb{F}_q}$ con $p = \text{char}(\mathbb{F}_q)$ è supersingolare se $E[p] = \{O\}$. (Per una dimostrazione di questa equivalenza, vedi [15].)

Vediamo alcuni esempi di curve supersingolari.

Proposizione 2.68. *Sia p primo maggiore o uguale a 5. Allora $E/_{\mathbb{F}_p}$ è supersingolare se e solo se $a = 0$.*

Dimostrazione. $\boxed{\Leftarrow}$ Per definizione.
$\boxed{\Rightarrow}$ Supponiamo che E sia supersingolare e $a \neq 0$. Allora $a \equiv 0 \pmod{p}$ implica $|a| \geqslant p$. D'altra parte il Teorema di Hasse ci dice $|a| \leqslant 2\sqrt{p}$. Quindi $p \leqslant 2\sqrt{p}$ e questo capita solo se $p \leqslant 4$. □

Proposizione 2.69. *Sia $q = p^m$ dispari e congruo a 2 modulo 3. Sia $b \in (\mathbb{F}_q)^*$. Allora la curva ellittica definita su $\mathbb{F}_q$ data da $y^2 = x^3 + b$ è supersingolare.*

Dimostrazione. Sia

$$\begin{array}{rccc} \psi: & (\mathbb{F}_q)^* & \longrightarrow & (\mathbb{F}_q)^* \\ & x & \longmapsto & x^3. \end{array}$$

Dato che $q-1$ non è multiplo di 3, non ci sono elementi di ordine 3 in $(\mathbb{F}_q)^*$, quindi il nucleo di ψ è banale. Questo prova che ψ è iniettiva e di conseguenza suriettiva in quanto $(\mathbb{F}_q)^*$ è un gruppo finito. In particolare, ogni elemento di $\mathbb{F}_q$ ha un'unica radice cubica in $\mathbb{F}_q$.

Fissato $y \in \mathbb{F}_q$, esiste un unico $x \in \mathbb{F}_q$ tale che $(x, y) \in E$, cioè la radice cubica di $y^2 - b$. I valori che può assumere y sono q e aggiungendo il punto all'infinito otteniamo

$$\#E(\mathbb{F}_q) = q + 1.$$

Questo prova che E è supersingolare. □

Vediamo quindi il comportamento delle curve supersingolari rispetto all'attacco MOV.

Proposizione 2.70. *Sia* $E/_{\mathbb{F}_q}$ *una curva supersingolare con* $\#E(\mathbb{F}_q) = q+1$, *cioè* $a = 0$. *Sia* n *un intero. Se esiste* $P \in E(\mathbb{F}_q)$ *di ordine* n, *allora* $E[n] \subset E(\mathbb{F}_{q^2})$.

Dimostrazione. L'endomorfismo di Frobenius in questo caso verifica

$$\varphi_q^2 = -q$$

(confronta la proposizione 2.31). Sia $S \in E[n]$. Dato che $\#E(\mathbb{F}_q) = q + 1$, abbiamo che n divide $q + 1$ o equivalentemente $-q \equiv 1 \pmod{n}$. Quindi

$$\varphi_q^2(S) = -qS = S.$$

Ricordando che $\varphi_q^2 = \varphi_{q^2}$ e che i punti fissi di φ_{q^2} sono esattamente i punti di $E(\mathbb{F}_{q^2})$ si ha la tesi. □

Curve supersingolari ottenute grazie alla proposizione 2.69 sono state usate per definire un protocollo crittografico simile a RSA da Koyama, Maurer, Okamoto e Vanstone ([10]). Anche in questo caso tratteremo pseudo-curve ellittiche, cioè curve definite da un'equazione di Weierstrass in $\mathbb{Z}/_{(n)}$ con n non primo.

Per comodità di scrittura useremo la notazione $\mathbb{Z}_n$ in luogo di $\mathbb{Z}/_{(n)}$. Supponiamo $n = pq$ con p, q primi. Il Teorema Cinese del Resto ci permette di spezzare

$$E(\mathbb{Z}_n) \simeq E(\mathbb{F}_p) \oplus E(\mathbb{F}_q).$$

Ogni punto di $E(\mathbb{Z}_n)$ può essere rappresentato come una coppia di punti (P_p, P_q), con O rappresentato da (O_p, O_q). L'operazione di gruppo su $E/_{\mathbb{Z}_n}$ non è definita

se e solo se coinvolge punti per i quali esattamente uno tra P_p e P_q è il punto all'infinito.

Lemma 2.71. *Sia* $E/_{\mathbb{Z}_n}$ *una pseudo-curva ellittica definita dall'equazione* $y^2 \equiv x^3 + ax + b \pmod{n}$*, in cui* $\text{MCD}(4a^3 + 27b^2, n) = 1$*. Sia* $n = pq$ *con* p *e* q *primi e sia* $\ell := \text{mcm}(\#E(\mathbb{F}_p), \#E(\mathbb{F}_q))$*. Allora per ogni* $P \in E/_{\mathbb{Z}_n}$ *e per ogni* $k \in \mathbb{Z}$

$$(k\ell + 1)P = P$$

in $E/_{\mathbb{Z}_n}$.

Dimostrazione. Segue facilmente dal Teorema Cinese del Resto. Osserviamo intanto che ℓ è multiplo di $\#E(\mathbb{F}_p)$ e $\#E(\mathbb{F}_q)$, quindi per ogni punto $P_p \in E(\mathbb{F}_p)$ e per ogni punto $P_q \in E(\mathbb{F}_q)$ vale

$$\ell P_p = O_p, \qquad \ell P_q = O_q.$$

Di conseguenza

$$(k\ell + 1)P \cong (k\ell + 1)(P_p, P_q) = ((k\ell + 1)P_p, (k\ell + 1)P_q) = (P_p, P_q) \cong P.$$

□

Ecco dunque come funziona lo schema crittografico.

1. Bob sceglie due numeri primi p e q con $p, q \equiv 2 \pmod 3$ e calcola $n = pq$. Dopodiché sceglie due interi e, d con $ed \equiv 1 \pmod{\text{mcm}(p+1, q+1)}$. La chiave pubblica è formata da n ed e, mentre quella privata da d, p e q.

2. Alice codifica il messaggio come una coppia di interi $M = (m_1, m_2) \in (\mathbb{Z}_n)^2$, visto come punto di una pseudo-curva ellittica $E/_{\mathbb{Z}_n}$ data da $y^2 \equiv x^3 + b \pmod n$ con $b = m_2^2 - m_1^3 \pmod n$. (Non è necessario calcolare esplicitamente b.)

3. Alice cifra M calcolando $C = (c_1, c_2) = eM$ su E. Manda quindi C a Bob.

4. Bob per decifrare calcola $M = dC$ su E.

Quali sono i punti di forza di questo protocollo? Vediamone alcuni.

- Non è necessario calcolare b, in quanto le formule di addizione non lo utilizzano. Un eventuale intercettatore anzi potrebbe ricavarlo come $b = c_2^2 - c_1^3$.

- Il calcolo di eM e dC richiede delle divisioni, in particolare occorre calcolare $(y_2 - y_1)/(x_2 - x_1)$ modulo n. È necessario che $\text{MCD}(x_2 - x_1, n) = 1$. Se non è 1, le possibilità sono p, q oppure n. Assumiamo implicitamente che fattorizzare n sia difficile, quindi escludiamo i casi p e q in quanto poco probabili. Se $\text{MCD}(x_2 - x_1, n) = n$, la somma dei punti è O e si usano le regole standard per il punto all'infinito.

- La decodifica funziona grazie al lemma 2.71: infatti $de = 1 + k\ell$ per costruzione, dove $\ell = \text{mcm}(p + 1, q + 1) = \text{mcm}(\#E(\mathbb{F}_p), \#E(\mathbb{F}_q))$.

- Tra i punti chiave della specifica c'è il fatto che l'ordine del gruppo della pseudo-curva ellittica non dipende dalla particolare curva scelta. Se infatti Bob avesse scelto arbitrariamente i coefficienti della curva, avrebbe dovuto calcolarne l'ordine (e p e q sono scelti in modo da rendere la fattorizzazione di n intrattabile, quindi il loro uso nel calcolo dell'ordine è pure intrattabile). Inoltre se la curva fosse fissata da Bob, Alice avrebbe difficoltà a trovare un punto M adatto: scegliere una coordinata m_1 e calcolare l'altra risolvendo $m_2^2 \equiv m_1^3 + am_1 + b \pmod{n}$ richiede l'estrazione di radici quadrate modulo n, che è computazionalmente equivalente alla fattorizzazione di n.

La sicurezza di questo crittosistema è basata sul fatto che la conoscenza di d, usato nella decodifica, è equivalente alla conoscenza della fattorizzazione di n; si veda [15] per un'analisi di questa situazione.

Capitolo 3

Topologia delle curve e delle superfici

Tutto ebbe inizio con il sedicesimo problema di Hilbert, il *problema della topologia delle curve e delle superfici algebriche*. La prima parte del problema, quella che ci interessa, recita:

> Il numero massimo di rami chiusi e disgiunti che può avere una curva algebrica piana di grado n è stato determinato da Harnack. Sorge spontanea l'ulteriore domanda di quale sia la posizione relativa di questi rami nel piano. Per quanto riguarda le curve di grado 6, io stesso sono riuscito a mostrare — con un argomento complicato, lo ammetto — che degli undici rami che esse possono avere in conseguenza del risultato di Harnack, in nessun modo essi possono essere esterni l'uno all'altro, ma deve esistere un ramo tale che al suo interno ci sia un altro ramo e al suo esterno i nove rimanenti, o viceversa. Credo che un'accurata indagine delle posizioni relative dei rami disgiunti quando il loro numero è il massimo possibile sia di grande interesse, e nondimeno sia interessante anche l'indagine corrispondente sul numero, la forma e la posizione relativa delle componenti di una superficie algebrica nello spazio. Al momento attuale, non si sa nemmeno quale sia il numero massimo di componenti che una superficie di grado 4 nello spazio tridimensionale possa avere.
>
> (David Hilbert)

In questo capitolo descriveremo, o meglio presenteremo le idee da cui sono stati sviluppati, due algoritmi che determinano la forma e la topologia rispettivamente di curve nel piano e di superfici nello spazio.

3.1 La forma delle curve algebriche reali

Siano $\mathcal{C}, \mathcal{C}' \subset \mathbb{P}^2(\mathbb{R})$ due curve algebriche non singolari.

Definizione 3.1. Diciamo che $\mathcal{C}$ e $\mathcal{C}'$ hanno *la stessa forma* se la coppia $(\mathbb{P}^2(\mathbb{R}), \mathcal{C})$ è omeomorfa alla coppia $(\mathbb{P}^2(\mathbb{R}), \mathcal{C}')$.

Cerchiamo allora degli invarianti che determinino univocamente la forma di una curva. Sappiamo che una curva non singolare $\mathcal{C}$ è omeomorfa all'unione disgiunta di un certo numero di S^1; ognuno di tali S^1 è detto *ramo* di $\mathcal{C}$. Un ramo è detto *pari* se una qualsiasi retta lo interseca in un numero pari di punti (contati con molteplicità), *dispari* altrimenti. Un ramo pari è detto anche *ovale*.

Una curva non singolare ha al massimo un ramo dispari (perché due rami dispari si incontrano in un numero dispari di punti, quindi almeno uno; tale punto tuttavia sarebbe singolare). Inoltre, un ramo dispari esiste se e solo se il grado di $\mathcal{C}$ è dispari.

Se R è un ramo dispari, $\mathbb{P}^2(\mathbb{R}) \setminus R$ è omeomorfo a $\mathbb{R}^2$; se invece è un ramo pari, allora $\mathbb{P}^2(\mathbb{R}) \setminus R$ è omeomorfo all'unione disgiunta di un nastro di Möbius (che chiameremo *esterno* di R) e un disco aperto (che chiameremo *interno* di R).

La forma di $\mathcal{C}$ è determinata se si conosce:

1. l'esistenza o meno di un ramo dispari;
2. il numero di ovali;
3. per ogni ovale, quali ovali sono contenuti nel suo interno.

Possiamo inserire le informazioni dei punti 2. e 3. in un grafo orientato, che risulterà un albero, tale che due curve non singolari di grado avente la stessa parità hanno la stessa forma se e solo se i rispettivi grafi sono isomorfi. Il grafo è definito come segue:

- i vertici sono le componenti connesse di $\mathbb{P}^2(\mathbb{R}) \setminus \mathcal{C}$;
- i lati sono gli ovali di $\mathcal{C}$;
- i vertici relativi al lato R sono le componenti connesse che hanno R sulla frontiera, e il primo vertice è quello esterno a R.

Questo grafo è un albero, e l'ordine parziale corrisponde alla relazione "essere interno a".

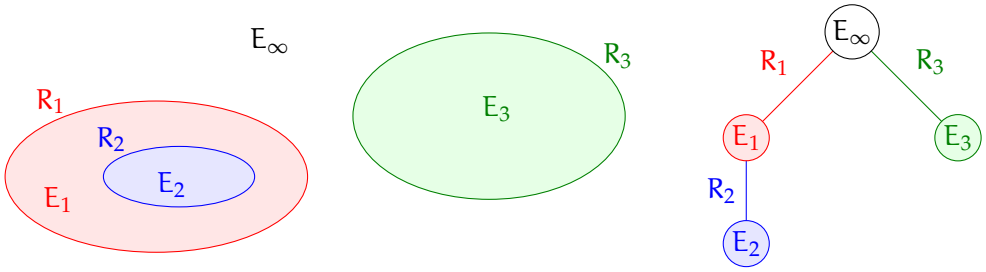


Figura 3.1: Un esempio di curva algebrica e il grafo associato. Qui $\mathbb{P}^2(\mathbb{R}) \setminus \mathcal{C}$ è l'unione di E_1, E_2, E_3 e E_∞, mentre i rami della curva sono R_1, R_2 e R_3.

L'idea dell'algoritmo è: si parte da una proiezione $\Pi : \mathbb{P}^2(\mathbb{R}) \longrightarrow \mathbb{P}^1(\mathbb{R})$ condotta da un punto esterno a $\mathcal{C}$ e si esaminano i punti e i valori critici della restrizione $\pi := \Pi|_{\mathcal{C}} : \mathcal{C} \longrightarrow \mathbb{P}^1(\mathbb{R})$. In particolare, si analizza la posizione di un punto critico rispetto agli altri punti della fibra del valore critico.

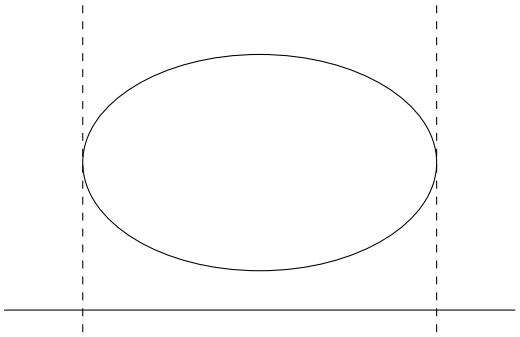


Figura 3.2: L'ovale è determinato dalla posizione dei punti critici di π; in particolare, leggendo da sinistra a destra, un ovale si "apre" su un minimo e si "chiude" su un massimo di π.

Per semplicità, supponiamo di scegliere coordinate omogenee $[x : y : z] \in \mathbb{P}^2(\mathbb{R})$ in modo che $\mathcal{C}$ non passi per $[0 : 1 : 0]$ e la retta $\{z = 0\}$ non sia tangente a $\mathcal{C}$; scegliamo la retta $\{z = 0\}$ come retta all'infinito e la proiezione Π di centro $[0 : 1 : 0]$. In questo modo, in coordinate non omogenee (x, y) la proiezione Π manda (x, y) in x e la retta all'infinito nel punto all'infinito di $\mathbb{P}^1(\mathbb{R})$; inoltre il punto all'infinito non è un valore critico per la restrizione $\pi = \Pi|_{\mathcal{C}}$.

Supponiamo inoltre che i valori critici di π siano semplici, cioè che i punti critici non siano degeneri e che ogni valore critico corrisponda a un solo punto critico.

Associamo a $\mathcal{C}$ i seguenti valori:

1. il numero r dei valori critici; per $i = 1, \dots, r$ indichiamo con $P_i \in \mathbb{R}$ tali valori (supponiamo che la successione sia crescente) e con $Q_i := (x_i, y_i)$ il rispettivo punto critico;
2. per ogni i, il numero n_i delle controimmagini non critiche di P_i;
3. per ogni i, il numero m_i delle controimmagini non critiche di P_i che hanno seconda coordinata minore di y_i;
4. il numero delle controimmagini di $P_0 := \infty$, ovvero il numero di intersezioni di $\mathcal{C}$ con la retta all'infinito; sia tale numero $n_0 + 1$.

Questi valori numerici determinano univocamente la forma di $\mathcal{C}$, nel senso che permettono di ricostruire il grafo associato a $\mathcal{C}$.

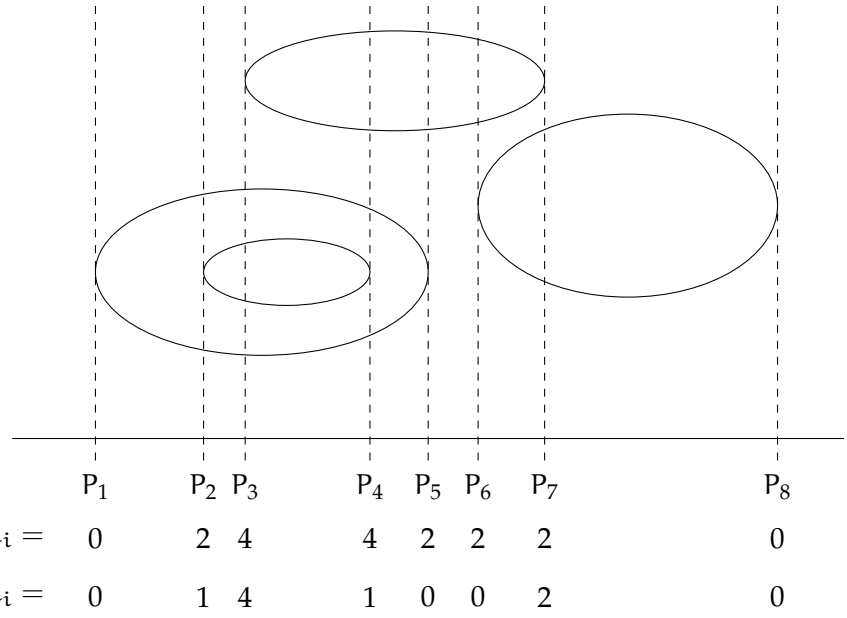


Figura 3.3: Esempio di sequenze n_i e m_i. Notiamo che un salto di 2 nella sequenza degli n_i determina l'apertura ($+2$) o la chiusura (-2) di un ovale. La sequenza degli m_i invece dà informazioni sulla posizione relativa degli ovali e sul loro annidamento.

Intanto iniziamo a vedere che possiamo determinare se Q_i è un massimo o un minimo relativo per π. Infatti

- se Q_i e Q_{i+1} sono un massimo e un minimo (in qualsiasi ordine), allora $n_{i+1} = n_i$;

- se Q_i e Q_{i+1} sono entrambi massimi, allora $n_{i+1} = n_i - 2$;
- se Q_i e Q_{i+1} sono entrambi minimi, allora $n_{i+1} = n_i + 2$;
- se Q_1 è un minimo, allora $n_1 = n_0 + 1$, altrimenti $n_1 = n_0 - 1$.

Per $i = 1, \dots, r$, consideriamo le controimmagini $P_{i,0}, \dots, P_{i,n_i}$ di P_i, ordinate secondo il valore crescente della seconda coordinata; per definizione $Q_i = P_{i,m_i}$.

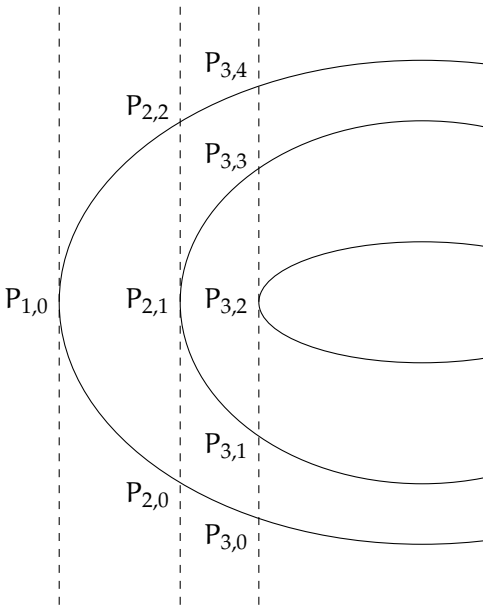


Figura 3.4: Notazione per le controimmagini di P_i.

Chiamiamo inoltre $P_{0,j}$ le controimmagini di P_0 ordinate ponendo $[x : y : 0]$ prima di $[x' : y' : 0]$ se $y/x > y'/x'$ (cioè considerando $\infty \in \mathbb{P}^1(\mathbb{R})$ come $-\infty$). Definiamo inoltre il punto $P_{r+1} := P_0$ e $P_{r+1,j} := P_{0,n_0-j}$ (invertendo cioè l'ordine; in altre parole, considerando P_{r+1} come $+\infty$).

I punti $P_{i,j}$ suddividono $\mathcal{C}$ in archi di curva. Da un punto $P_{i,j}$ si originano due segmenti di curva: i dati in nostro possesso ci permettono di identificare i due secondi estremi dei segmenti. La casistica è lunga ma non complicata.

1. Per $i = 1, \dots, r-1$, i punti $P_{i,j}$ e $P_{i+1,h}$ sono estremi di uno stesso segmento se $h = j + j_1 + j_2$, dove
   - $j_1 = 0$ se $j < m_i$;
   - $j_1 = 1$ se $j > m_i$ e Q_i è un minimo;

- $j_1 = -1$ se $j > m_i$ e Q_i è un massimo;
- $j_1 = 0$ oppure 1 se $j = m_i$ e Q_i è un minimo;

mentre

- $j_2 = 0$ se $j + j_1 < m_{i+1}$;
- $j_2 = 1$ se $j + j_1 > m_{i+1}$ e Q_{i+1} è un minimo;
- $j_2 = -1$ se $j + j_1 > m_{i+1}$ e Q_{i+1} è un massimo;
- $j_2 = 0$ se $j + j_1 = m_{i+1}$ e Q_{i+1} è un massimo.

2. I punti $P_{0,j}$ e $P_{1,h}$ sono estremi dello stesso segmento se
   - $h < m_1$ e $j = h$;
   - $h > m_1$, $j = h - 1$ e Q_1 è un minimo;
   - $h > m_1$, $j = h + 1$ e Q_1 è un massimo;
   - $h = m_1$, $j = h$ oppure $h + 1$ e Q_1 è un massimo.
3. I punti $P_{r,j}$ e $P_{r+1,h}$ sono estremi dello stesso segmento se
   - $j < m_r$ e $h = j$;
   - $j > m_r$, $h = j - 1$ e Q_r è un massimo;
   - $j > m_r$, $h = j + 1$ e Q_r è un minimo;
   - $j = m_r$, $h = j$ oppure $j + 1$ e Q_r è un minimo.
4. Non esistono altre coppie di punti che sono estremi dello stesso segmento.

Abbiamo visto che per determinare la forma di $\mathcal{C}$ è sufficiente conoscere il numero di ovali e la loro posizione relativa; osserviamo ora che la conoscenza dei punti $P_{i,j}$ e di quali di essi siano estremi dello stesso segmento basta per ricostruire quest'informazione.

Ogni ramo passa per l'infinito oppure contiene almeno un punto critico, quindi contiene qualche $P_{i,j}$. Definendo sull'insieme dei $P_{i,j}$ la relazione di equivalenza "essere estremi dello stesso segmento", cioè

$$P_{k,\ell} \sim P_{s,t} \iff \begin{array}{l} P_{k,\ell} = P_{s,t} \text{ oppure } \exists\, R_1, \dots, R_n \text{ tra i } P_{i,j} \text{ tali che} \\ P_{k,\ell} = R_1,\ P_{s,t} = R_n \text{ e } R_h, R_{h+1} \text{ sono estremi} \\ \text{dello stesso segmento per } h = 1, \dots, n-1, \end{array}$$

abbiamo che le classi di equivalenza sono in corrispondenza biunivoca con i rami. Di conseguenza è facile contare e identificare i rami. L'eventuale ramo dispari presente è rilevabile dal fatto che contiene un numero dispari di $P_{0,j}$.

Dobbiamo solo capire quali ovali sono contenuti in quali altri. Per questo è sufficiente osservare che se O è un ovale di $\mathcal{C}$, R è una curva omologa alla retta all'infinito che non incontri O e S un arco di curva trasversale a $\mathcal{C}$ con estremi rispettivamente su R e O, allora gli ovali che contengono O sono tutti e soli quelli che intersecano S un numero dispari di volte.

Se la curva ha un ramo dispari, possiamo prendere come R il ramo dispari e come S un segmento di retta: scegliamo un punto Q_i su O e un punto $P_{i,j}$ su R (questo è possibile perché ogni ovale ha punti critici e il ramo dispari incontra ogni retta verticale) e contiamo quanti punti compresi tra Q_i e $P_{i,j}$ stanno su un ovale. Contengono O esattamente quegli ovali per cui tale numero è dispari.

Se la curva non ha un ramo dispari, occorre costruire R. È possibile farlo a partire da considerazioni sui punti all'infinito, come descritto in [5].

Un'ultima considerazione di carattere pratico: come si trovano i valori critici? Se $f(X, Y)$ è il polinomio che descrive la curva $\mathcal{C}$, i valori critici sono le radici del discriminante di f visto come polinomio in Y, ovvero le radici di

$$\mathrm{Ris}_Y\left(f(X,Y), \frac{\partial f}{\partial Y}(X,Y)\right).$$

3.2 Superfici algebriche reali orientabili

Proviamo a generalizzare quanto visto nella sezione precedente al caso di una superficie. Un'idea che può venire è: studiamo le sezioni della superficie con un piano. Tali sezioni sono curve e possiamo usare quanto già visto.

Purtroppo possono sorgere dei problemi. Ad esempio, la sezione potrebbe essere una curva singolare. Possiamo aggirare il problema tagliando la superficie poco sopra e poco sotto la sezione singolare, in modo da evitare questo tipo di complicazioni, e analizzare i cambiamenti avvenuti tra le due sezioni.

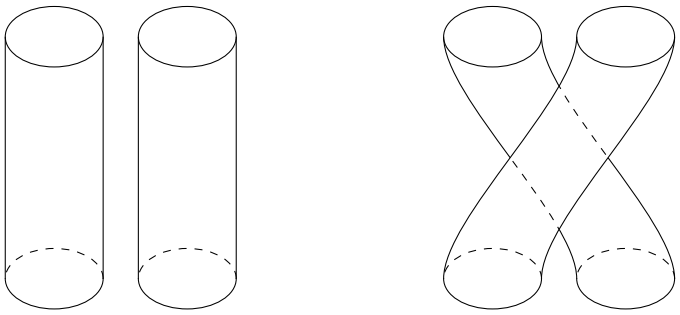


Figura 3.5: Problemi che si possono verificare nello spazio: come distinguiamo questi due casi?

Inoltre, nello spazio c'è un sacco di spazio: potrebbe capitare una situazione come in figura 3.5, in cui osservando solo le sezioni non si può distinguere se l'ovale di sinistra di una sezione era connesso all'ovale di sinistra o a quello di destra dell'altra.

Procediamo con ordine. Sappiamo che una superficie connessa, compatta, orientabile è omeomorfa a una sfera o a un toro con g buchi. Questo può essere determinato dal calcolo del primo gruppo di omologia H_1, che è un gruppo abeliano libero di rango $2g$. Di conseguenza, per conoscere il tipo topologico di una superficie compatta, basta calcolare il numero di componenti connesse e per ciascuna di esse il primo gruppo di omologia.

Richiamiamo un po' di definizioni. Sia $\mathcal{S}$ una superficie liscia e $f : \mathcal{S} \longrightarrow \mathbb{R}$ una funzione differenziabile. Un punto $P \in \mathcal{S}$ è detto *punto critico* per f se, dette u_1, u_2 coordinate locali per $\mathcal{S}$ in P, entrambe le derivate parziali $\partial f/\partial u_1$ e $\partial f/\partial u_2$ si annullano in P. Il corrispondente valore $f(P)$ è detto *valore critico*. Un punto critico è detto *non degenere* se la forma quadratica hessiana di f calcolata in P è non degenere; in tal caso, il numero di autovalori negativi è detto *indice* di P. Una funzione f per cui tutti i punti critici siano non degeneri è detta *funzione di Morse*.

Sia dunque $\varphi(X, Y, Z, T) \in \mathbb{R}[X, Y, Z, T]$ un polinomio omogeneo di grado d, che definisce una superficie algebrica reale non singolare ed orientabile $\mathcal{S}$. Per "non singolare" si intende che

$$\mathcal{V}_{\mathbb{R}}\left(\varphi, \frac{\partial\varphi}{\partial X}, \frac{\partial\varphi}{\partial Y}, \frac{\partial\varphi}{\partial Z}, \frac{\partial\varphi}{\partial T}\right) = \varnothing$$

in $\mathbb{P}^3(\mathbb{R})$; è ammessa l'esistenza di punti singolari non reali in $\mathbb{P}^3(\mathbb{C})$. In più, affinché $\mathcal{S}$ sia orientabile, d dev'essere pari.

Per questo algoritmo supporremo l'esistenza di una retta $L \subset \mathbb{P}^3(\mathbb{R})$ che non intersechi la superficie. L'esistenza di una tale retta è decidibile algoritmicamente; inoltre, ad esempio, si può dimostrare che questa retta esiste sempre per una superficie di grado 4. Per maggiori dettagli si veda [4].

Supporremo che nel nostro sistema di coordinate omogenee $[x : y : z : t]$ su $\mathbb{P}^3(\mathbb{R})$ si abbia che

1. $L = \{z = 0, t = 0\}$;

2. detto $Z := \{x = 0, y = 0\} \simeq \mathbb{P}^1(\mathbb{R})$, la funzione $\pi : \mathcal{S} \longrightarrow Z$, restrizione della proiezione $\Pi : \mathbb{P}^3(\mathbb{R}) \setminus L \longrightarrow Z$ di centro L, sia una funzione di Morse e $[0 : 0 : 1 : 0]$ non sia un valore critico per π;

3. se $P, Q \in \mathcal{S}$ sono punti critici per π, si abbia $\pi(P) \neq \pi(Q)$.

Più avanti ci occuperemo di come verificare che queste condizioni siano soddisfatte.

Identifichiamo $\mathbb{P}^3(\mathbb{R}) \setminus \{t = 0\}$ con lo spazio affine $\mathbb{R}^3$. L'equazione della parte affine di $\mathcal{S}$, dunque, è

$$F(x, y, z) = \varphi(x, y, z, 1) = 0.$$

Inoltre identifichiamo Z con la retta reale estesa $\mathbb{R} \cup \{\infty\}$ associando a un punto $[0 : 0 : z : t]$ la coordinata z/t se $t \neq 0$ e il punto ∞ se $t = 0$. Nella carta affine, dunque, π è la proiezione di $\mathcal{S}$ sull'asse z. I punti critici affini di π sono allora i punti di

$$\mathcal{V}_{\mathbb{R}}\left(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}\right).$$

Inoltre si dimostra che π può avere solo un numero finito di valori critici; dato che ∞ non lo è, esiste un intervallo $(-N, N) \subset \mathbb{R}$, con $N \in \mathbb{Q}_{>0}$, che contiene tutti i valori critici. (Conveniamo $N = 1$ se π non ha valori critici.)

Per ogni $a \in (-N, N]$, denotiamo con $S_a := \pi^{-1}([-N, a]) = \mathcal{S} \cap \Pi^{-1}([-N, a])$ la *superficie di livello*; denotiamo con $C_a := \pi^{-1}(a) = \mathcal{S} \cap \Pi^{-1}(a)$ la *curva di livello*. Con queste notazioni, la superficie di livello S_a ha come bordo $C_{-N} \cup C_a$. In più, C_a è la curva ottenuta sezionando $\mathcal{S}$ con il piano $\{z = a\}$, quindi ha equazione $F(x, y, a) = 0$.

Dalla teoria di Morse abbiamo che se l'intervallo $[a, b]$ non contiene valori critici per π, allora S_b è omotopicamente equivalente a S_a; invece, se $[a, b]$ contiene esattamente un valore critico c di indice k, con $a < c < b$, allora S_b è omotopicamente equivalente allo spazio ottenuto incollando una k-cella a S_a. Notiamo che però la conoscenza dei punti critici e del loro indice non è sufficiente per determinare la forma della superficie. Un esempio è riportato in figura 3.6

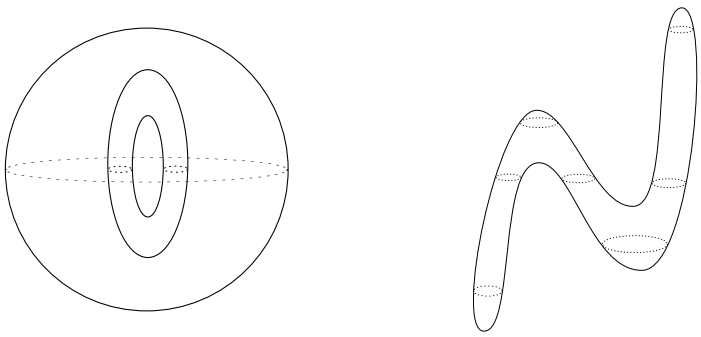


Figura 3.6: Entrambe le superfici hanno sei punti critici, di indice $0, 0, 1, 1, 2, 2$ (in ordine dal basso verso l'alto); tuttavia, non hanno nemmeno lo stesso numero di componenti connesse.

Definizione 3.2. Per un valore non critico a, un *data system* per S_a consiste in

1. una lista $\mathrm{Data}(C_a)$ di coppie (P_i, n_i) dove n_i è un nido della curva C_a (cioè una lista di ovali annidati uno nell'altro) e P_i è un punto interno all'ovale più interno del nido;

2. una lista $\mathrm{Hom}(S_a)$ di interi, dove la lunghezza della lista è il numero di componenti connesse di S_a e il k-esimo intero rappresenta il rango del gruppo H_1 della k-esima componente connessa;

3. una funzione $\mu_a : H_0(C_a) \longrightarrow H_0(S_a)$ che associa ogni ovale di C_a alla componente connessa di S_a che lo contiene nel bordo.

Vedremo tra poco che è possibile costruire un *data system* per S_b a partire da un *data system* per S_a se l'intervallo $[a, b]$ contiene al massimo un valore critico. A questo punto l'*outline* dell'algoritmo è chiara: si suddivide l'intervallo $[-N, N]$ in un numero finito di punti $-N = a_0 < a_1 < \cdots < a_m < a_{m+1} = N$ in modo che ciascun intervallo $[a_i, a_i + 1]$ contenga esattamente un valore critico e si ricostruiscono iterativamente i *data system* per S_{a_i} fino ad ottenere alla fine i gruppi di omologia di $\mathcal{S}$.

In particolare, dalla definizione di *data system* appare chiaro che sono necessari due passi principali: trovare la forma di C_{a_i} e sollevare le informazioni dal livello a_i al livello a_{i+1}.

Per il primo passo, possiamo usare l'algoritmo presentato nella sezione precedente, a cui vanno aggiunte due funzioni speciali, descritte in [4]:

- una funzione `findOvals` che, data una curva di livello C e un punto P nel piano della curva, restituisce la lista degli ovali di C che contengono P (ordinata per inclusione a partire dall'ovale più interno);

- una funzione `findPoint` che, dato un ovale ω di una curva C, restituisce un punto Q interno a ω, più precisamente restituisce un punto Q tale che ω sia il primo ovale della lista output di `findOvals`(Q).

Per dare un'idea del lavoro da svolgere nel secondo passo, torniamo alla figura 3.5. Supponiamo che C_a sia la curva a livello inferiore e C_b quella a livello superiore; entrambe sono formate da due ovali non contenuti l'uno nell'altro, che chiamiamo ω_1^a e ω_2^a (rispettivamente ω_1^b e ω_2^b). Non ci sono punti critici in $[a, b]$, quindi sappiamo che S_b è l'unione di S_a e due cilindri che collegano gli ovali ω_1^a e ω_2^a con ω_1^b e ω_2^b, ma non sappiamo quale ovale è collegato a quale. Al passo precedente abbiamo calcolato $\mathrm{Data}(C_a) = [(P_1, [\omega_1^a]), (P_2, [\omega_2^a])]$. Per distinguere

le due situazioni costruiamo un cammino che parta da P_1, non intersechi mai la superficie $\mathcal{S}$ e arrivi a un punto Q_1 nel piano $\Pi^{-1}(b)$. Necessariamente Q_1 è interno a uno tra ω_1^b e ω_2^b e possiamo decidere quale lanciando `findOvals`(Q_1).

Dall'esempio precedente sorgono spontanee due domande: detta W la componente connessa di $(\mathbb{R}^3 \setminus \mathcal{S}) \cap \{a \leqslant z \leqslant b\}$ che contiene P_1, esiste un cammino contenuto in W che unisca P_1 con un punto $Q_1 \in W \cap \Pi^{-1}(b)$? In caso affermativo, è possibile costruirlo? Fortunatamente sì, grazie all'esistenza di *roadmap*.

Definizione 3.3. Sia $W \subseteq \mathbb{R}^3$ una varietà algebrica. Una *roadmap* per W è un insieme semialgebrico (vedi definizione 4.27) 1-dimensionale $R \subseteq W$ tale che

1. per ogni componente connessa $U \subseteq W$, $U \cap R$ è connessa e non vuota;
2. per ogni $a \in \mathbb{R}$ e per ogni componente connessa V della sezione $W_a := W \cap \Pi^{-1}(a)$, $V \cap R \neq \varnothing$.

Per i nostri scopi, adotteremo le seguenti notazioni. Se $P \in \Pi^{-1}(a)$, $b > a$, sia $\alpha : [0,1] \longrightarrow \{a \leqslant z \leqslant b\}$ un cammino continuo semialgebrico tale che $\alpha(0) = P$, $\alpha(1) \in \Pi^{-1}(b)$ e $\alpha([0,1]) \cap \mathcal{S} = \varnothing$. Denoteremo con `RoadMap`$(P, b)$ il punto finale $\alpha(1)$. Analogamente, se $b < a$, denoteremo con `InvRoadMap`(P, b) il punto finale $\beta(1)$ di un cammino continuo semialgebrico $\beta : [0,1] \longrightarrow \{b \leqslant z \leqslant a\}$ che soddisfa le stesse condizioni di α.

Siamo pronti a descrivere il passo di sollevamento dell'informazione, cioè come ottenere un *data system* di S_b a partire da un *data system* di S_a. Supporremo noti, oltre al *data system* di S_a, anche l'indice del punto critico e la forma (cioè l'insieme degli ovali e il loro annidamento) della curva C_b. Distinguiamo quattro casi a seconda dell'indice del punto critico corrispondente al valore critico interno all'intervallo.

Caso 0. Il primo caso si ha quando $[a, b]$ non contiene valori critici. In questo caso S_a è un retratto di deformazione di S_b, quindi il numero di componenti connesse e i relativi gruppi di omologia non cambiano: $\mathrm{Hom}(S_b) = \mathrm{Hom}(S_a)$. Per completare la conoscenza del *data system* occorre calcolare un numero finito di *roadmap*. Nella fattispecie, per ogni $(P_i, n_i) \in \mathrm{Data}(C_a)$, sia $Q_i :=$ `RoadMap`(P_i, b); Q_i è interno a tutti gli ovali di un nido m_i che può essere trovato con `findOvals`(Q_i). La coppia (Q_i, m_i) è un elemento di $\mathrm{Data}(C_b)$. Ovviamente n_i e m_i contengono lo stesso numero di ovali e precisamente il k-esimo ovale di m_i appartiene al bordo della componente connessa di S_b che si retrae sulla componente connessa di S_a che ha nel bordo il k-esimo ovale di n_i. Quindi queste informazioni ci bastano per ricostruire sia $\mathrm{Data}(C_b)$ che μ_b.

Ora supponiamo che $[a, b]$ contenga un valore critico c, con $a < c < b$ e $c = \pi(P)$. Se $P = (x_0, y_0, z_0)$ sarà utile considerare i punti $P^+ := (x_0, y_0, z_0 + \varepsilon)$ e $P^- := (x_0, y_0, z_0 - \varepsilon)$ con ε sufficientemente piccolo in modo che il segmento che unisce P^+ e P^- intersechi $\mathcal{S}$ solo in P.

Caso 1. P ha indice zero, cioè è un minimo relativo. Siamo nel caso rappresentato in figura 3.7.

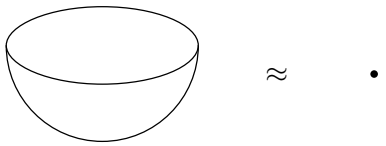


Figura 3.7: P è un minimo relativo. Le due figure sono omotopicamente equivalenti.

In questo caso S_b ha una componente connessa in più rispetto a S_a ed è omeomorfa all'unione disgiunta di S_a e un disco D. Di conseguenza per ottenere $\mathrm{Hom}(S_b)$ basta aggiungere a $\mathrm{Hom}(S_a)$ un numero intero 0, relativo all'omologia del disco D aggiuntivo. Per completare il *data system* dobbiamo capire la posizione di D rispetto ai cilindri in $S_b \setminus (S_a \cup D)$ e del suo bordo ω rispetto agli ovali in $C_b \setminus \omega$. Per fare ciò, ci abbassiamo di poco da P e consideriamo P^-. Possiamo costruire una *roadmap* tra P^- e il piano $\Pi^{-1}(a)$ arrivando a $P_a := \texttt{InvRoadMap}(P^-, a)$; dopodiché determiniamo la posizione di P_a rispetto agli ovali di C_a con `findOvals`.

1. Se P_a è esterno a tutti gli ovali di C_a, il disco D è esterno a tutti i cilindri di $S_b \setminus (S_a \cup D)$ e C_b contiene un nido in più (formato da un solo ovale, ω) rispetto a C_a. Di conseguenza creiamo un *data system* fittizio per S_a che contenga in $\mathrm{Data}(C_a)$ anche una coppia (P^+, n^+), dove n^+ rappresenta un nido con un ovale solo che contenga P^+.
2. Se P_a è interno a tutti gli ovali di un nido n_i di C_a, il disco D è interno a un annidamento di cilindri in $S_b \setminus (S_a \cup D)$ e C_b ha lo stesso numero di nidi di C_a, ma uno di essi contiene un ovale in più. Anche in questo caso creiamo un *data system* fittizio per S_a modificando $\mathrm{Data}(C_a)$ in modo che al posto della coppia (P_i, n_i) ci sia la coppia (P^+, n_i^+) dove n_i^+ è ottenuto da n_i aggiungendo un ovale fittizio nella posizione più interna del nido.
3. Altrimenti, il disco D è interno a qualche cilindro in $S_b \setminus (S_a \cup D)$ e il suo bordo ω dà origine a un nuovo nido in C_b (che condivide gli

ovali diversi da ω con un nido già esistente), di cui ω è l'ovale più interno. La lista $\mathrm{Data}(C_a)$ del *data system* fittizio conterrà una coppia aggiuntiva (P^+, n^+) dove n^+ è un nido che ha in posizione più interna ω ed è completato dagli ovali trovati con `findOvals`(P_a).

In ogni caso, abbiamo costruito un *data system* modificato che tenga conto di ciò che succede appena oltre il punto critico; possiamo completare la costruzione di un *data system* per S_b a partire da questo, procedendo come nel caso 0.

Caso 2. P ha indice 2, cioè è un massimo relativo. Siamo nel caso rappresentato in figura 3.8.

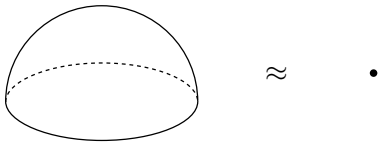


Figura 3.8: P è un massimo relativo. Le due figure sono omotopicamente equivalenti.

In questo caso otteniamo S_b da S_a attaccando una 2-cella D a un ovale ω di C_a che sia l'ovale più interno di un nido. È facile riconoscere ω: se $P_a :=$ `InvRoadMap`(P^-, a), ω è l'ovale più interno degli ovali che contengono P_a, trovati con `findOvals`(P_a). Poiché ω è l'ovale più interno di un nido (eventualmente singolo), esso compare in una sola coppia (P_i, n_i) che modifichiamo come segue: se ω è l'unico ovale di n_i, rimuoviamo la coppia (P_i, n_i) da $\mathrm{Data}(C_a)$; altrimenti, rimuoviamo ω da n_i e scegliamo P^+ come nuovo punto della coppia. Se, rimuovendo ω, tutti gli altri ovali di n_i compaiono in qualche altro nido n_j, possiamo in realtà rimuovere tranquillamente (P_i, n_i). Da questo *data system* fittizio possiamo ricavare $\mathrm{Data}(C_b)$ e μ_b come nel caso 1.

Per quanto riguarda $\mathrm{Hom}(S_b)$, la questione è un po' diversa. Dato che il numero di componenti connesse è lo stesso, $\mathrm{Hom}(S_b)$ ha lo stesso numero di elementi di $\mathrm{Hom}(S_a)$. Se W_ω è la componente connessa di S_a nel cui bordo è contenuto ω (e questa si può ricavare da μ_a), l'unico numero di $\mathrm{Hom}(S_a)$ che può cambiare è quello relativo alla componente W_ω e il modo in cui tale numero cambia dipende dalla posizione di ω. Siano $\nu : H_0(C_a) \longrightarrow H_1(S_a)$ l'omomorfismo ottenuto vedendo un ovale di C_a

come ciclo in S_a e $\widehat{W}_\omega$ la componente connessa di S_b ottenuta attaccando D a W_ω. Allora

1. se $\nu(\omega) = 0$, allora $H_1(\widehat{W}_\omega) \simeq H_1(W_\omega)$;
2. se $\nu(\omega) \neq 0$, allora $H_1(\widehat{W}_\omega) \simeq {}^{H_1(W_\omega)}/_{\langle \nu(\omega) \rangle}$.

Intuitivamente, questo risultato è dovuto al fatto che incollare una 2-cella a ω non cambia $H_1(W_\omega)$ se ω era già omologicamente banale in $H_1(S_a)$; altrimenti, se ω diventa nullo solo passando per la 2-cella appena incollata, un generatore di $H_1(W_\omega)$ scompare e il rango di questo gruppo cala di uno. Osserviamo infine che $\nu(\omega) = 0$ se e solo se ω è l'unica componente di bordo di W_ω, fatto che può essere stabilito conoscendo μ_a.

Caso 2. P ha indice 1, cioè è una sella. Questo può capitare nei due casi rappresentati in figura 3.9: due ovali si fondono oppure un ovale si divide in due.

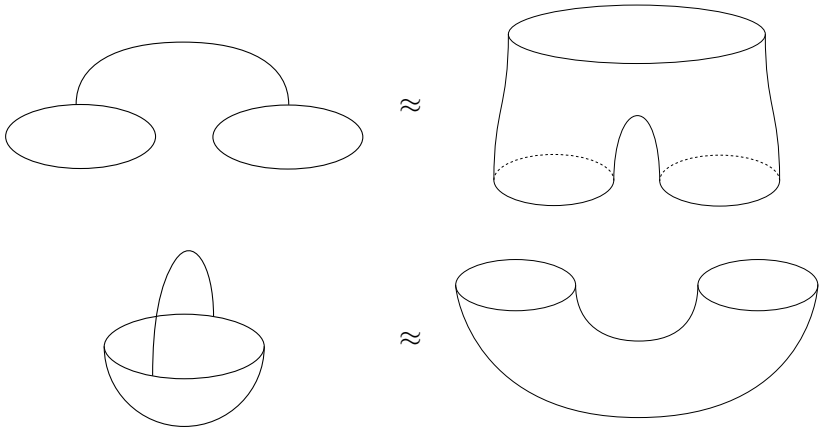


Figura 3.9: P è una sella. Le figure sulla stessa riga sono omotopicamente equivalenti.

In questo caso S_b si ottiene da S_a incollando una 1-cella a due ovali ω_1 e ω_2 di C_a, eventualmente coincidenti. Se $\omega_1 \neq \omega_2$, i due ovali sono incollati dalla 1-cella e danno origine a un ovale solo in C_b, che chiamiamo ω. Se invece $\omega_1 = \omega_2$, questo ovale si divide in due ovali distinti in C_b. Ovviamente è possibile distinguere le due situazioni contando il numero di ovali in C_a e C_b e confrontando tali numeri.

Iniziamo dal caso in cui $\omega_1 \neq \omega_2$. L'ovale ω nato dalla fusione di ω_1 e ω_2 si trova facilmente: basta calcolare $Q := \texttt{RoadMap}(P^+, b)$ e ω è l'ovale più

interno di $L := \texttt{findOvals}(Q)$. È possibile che L non sia un nido in C_b; in effetti, L è un nido se e solo se né ω_1 né ω_2 contengono altri ovali al loro interno. In tal caso il numero di nidi di C_b è diminuito di 1 rispetto al numero di nidi di C_a. Anche quando solo uno dei due ovali non ne contiene altri C_b ha un nido in meno rispetto a C_a (ma L non è un nido in C_b). Invece, quando sia ω_1 che ω_2 hanno altri ovali al loro interno, il numero di nidi resta invariato (e L non è un nido). Possiamo allora costruire $\text{Data}(C_b)$ come segue:

1. studiamo la curva C_b e calcoliamo Q, L e ω; inizializziamo $\text{Data}(C_b)$ come lista vuota;
2. se L è uno dei nidi di C_b, aggiungiamo (Q, L) in $\text{Data}(C_b)$, altrimenti la lasciamo vuota;
3. per ogni $(P_i, n_i) \in \text{Data}(C_a)$, calcoliamo $Q_i := \texttt{RoadMap}(P_i, b)$ e $m_i := \texttt{findOvals}(Q_i)$; se $m_i \neq L$, aggiungiamo (Q_i, m_i) a $\text{Data}(C_b)$, altrimenti scartiamo la coppia (Q_i, m_i).

È ora chiaro come ricostruire μ_b: per gli ovali di C_b che non compaiono in L, dato che appartengono a un nido ricostruito tramite *roadmap*, possiamo definire μ_b come abbiamo visto nel caso 0. Per quanto riguarda gli ovali in L, il più interno è ω, il quale quindi è nel bordo sia della componente connessa $\mu_a(\omega_1)$ che di $\mu_a(\omega_2)$. Bisogna fare attenzione al fatto che, quando $\mu_a(\omega_1) \neq \mu_a(\omega_2)$, stiamo incollando con una 1-cella due diverse componenti connesse di S_a.

Vediamo che succede invece nel caso in cui $\omega_1 = \omega_2$. Per ogni coppia $(P_i, n_i) \in \text{Data}(C_a)$, calcoliamo i punti $Q_i := \texttt{RoadMap}(P_i, b)$ e i nidi $m_i := \texttt{findOvals}(Q_i)$ e aggiungiamo (Q_i, m_i) in $\text{Data}(C_b)$. È possibile che esista un ovale in C_b che non compare nella lista dei nidi in $\text{Data}(C_b)$ così costruita; questo capita se e solo se, detti ω_1' e ω_2' i due ovali in cui si è diviso $\omega_1 = \omega_2$, tutti i punti Q_i costruiti a partire dai punti P_i interni a $\omega_1 = \omega_2$ stanno nello stesso ovale, per esempio ω_2'. In tal caso, calcoliamo un punto Q_1' interno all'ovale ω_1' con `findPoint` e aggiungiamo la coppia $(Q_1', \texttt{findOvals}(Q_1'))$ a $\text{Data}(C_b)$. Per quanto riguarda μ_b, possiamo seguire la solita procedura tramite *roadmap*; l'unico ovale che eventualmente resta fuori da quest'analisi è ω_1', per il quale sappiamo già che $\mu_b(\omega_1') = \mu_a(\omega_1)$.

Resta solo da vedere cosa succede ai gruppi di omologia. Ricordiamo che una superficie compatta con bordo non vuoto è omotopicamente equivalen-

te a un bouquet di n circonferenze, il cui H_1 ha rango n. Di conseguenza possiamo valutare cosa succede ai nostri H_1: se $\mu_a(\omega_1) = \mu_a(\omega_2)$ (cosa che in particolare accade quando $\omega_1 = \omega_2$), l'incollamento della 1-cella ha l'effetto di aggiungere una circonferenza al bouquet omotopicamente equivalente a $\mu_a(\omega_1)$, quindi il rango di $H_1(\mu_a(\omega_1))$ aumenta di uno; invece, se $\mu_a(\omega_1) \neq \mu_a(\omega_2)$, la 1-cella unisce le due componenti in una nuova omotopicamente equivalente a un bouquet che ha un numero di circonferenze pari alla somma dei ranghi di $H_1(\mu_a(\omega_1))$ e $H_1(\mu_a(\omega_2))$.

Vediamo l'algoritmo con un esempio: un toro. Supponiamo che la situazione sia come quella visualizzata nella figura 3.10. Non useremo numeri specifici ma etichetteremo le sezioni con le lettere riportate in figura. Inoltre ci limiteremo al calcolo dei gruppi di omologia, senza considerare la lista Data o la funzione μ.

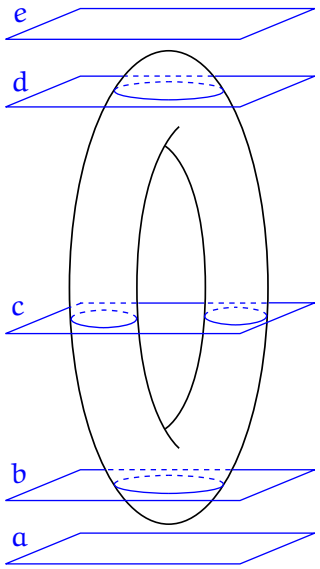


Figura 3.10: Sezioni di un toro.

Ovviamente a livello a sia S_a che C_a sono vuote, quindi $\mathrm{Hom}(S_a) = [\,]$.

Analizziamo ora il livello b. S_b e C_b sono disegnate in figura 3.11.

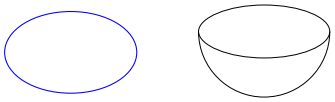


Figura 3.11: Le sezioni C_b e S_b.

A questo punto S_b è omeomorfa a un disco; in effetti, come nel caso 1., dobbiamo aggiungere uno 0 per la nuova componente connessa, quindi $\mathrm{Hom}(S_b) = [0]$.

A livello c abbiamo la situazione della figura 3.12.

Figura 3.12: Le sezioni C_c e S_c.

L'unico ovale presente in C_b si è diviso in due ovali; continua a esserci una sola componente connessa e il rango del suo H_1 aumenta di uno, pertanto ora abbiamo $\mathrm{Hom}(S_c) = [1]$.

Proseguiamo con il livello d. Le sezioni sono disegnate in figura 3.13.

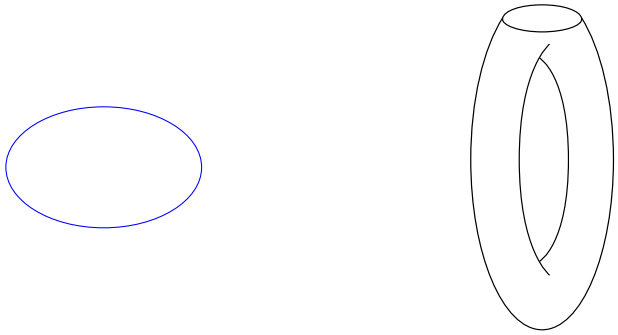


Figura 3.13: Le sezioni C_d e S_d.

Questa volta i due ovali del livello precedente si sono fusi. Continua ad esserci una sola componente connessa, quindi, in accordo con quanto visto, abbiamo $\mathrm{Hom}(S_d) = [2]$.

Terminiamo con il livello e. Ovviamente $C_e = \varnothing$ e S_e è l'intero toro. Abbiamo chiuso l'unica componente di bordo di S_d, dunque non si ha alterazione del gruppo di omologia. Concludiamo che $\mathrm{Hom}(S_e) = [2]$, cioè che la superficie è connessa con $H_1 \simeq \mathbb{Z}^2$: come ci aspettavamo, abbiamo trovato un toro.

Dobbiamo ora descrivere i controlli per il buon funzionamento dell'algoritmo. Un primo test consiste nel verificare che ∞ non sia una valore critico, controllando che la curva di livello C_∞ non sia singolare. Inoltre dobbiamo assicurarci che $\mathcal{S}$ non sia singolare e che i punti critici per π siano non degeneri.

Nota dell'autore. Da questo momento fino alla fine del capitolo non ho la certezza che i ragionamenti e le dimostrazioni siano del tutto corretti; anche se lo fossero, sicuramente non sono spiegati in modo chiaro. Sarò grato a chiunque riesca a trovare un modo per migliorare quest'ultima parte di capitolo.

Sia $\varphi \in \mathbb{R}[X, Y, Z, T]$ il polinomio omogeneo e libero da quadrati che descrive $\mathcal{S}$ in $\mathbb{P}^3(\mathbb{R})$. Definiamo gli ideali

$$J := \left(\varphi, \frac{\partial\varphi}{\partial X}, \frac{\partial\varphi}{\partial Y}, \frac{\partial\varphi}{\partial Z}, \frac{\partial\varphi}{\partial T}\right) \text{ e } K := \left(\varphi, \frac{\partial\varphi}{\partial X}, \frac{\partial\varphi}{\partial Y}\right).$$

In questo modo $\mathcal{V}_\mathbb{R}(J)$ è l'insieme dei punti singolari reali per $\mathcal{S}$, mentre $\mathcal{V}_\mathbb{R}(K)$ sarà l'insieme dei punti critici reali, una volta verificato che $\mathcal{V}_\mathbb{R}(J) = \varnothing$.

Il fatto che ∞ non sia un valore critico ci permette di poter investigare la natura di $\mathcal{V}_\mathbb{R}(J)$ e $\mathcal{V}_\mathbb{R}(K)$ nella carta affine $\{t \neq 0\}$, quindi consideriamo gli ideali non omogenei in tre variabili J_A e K_A ottenuti valutando i generatori di J e K per $t = 1$. Più precisamente, detto $F(X, Y, Z) := \varphi(X, Y, Z, 1)$, abbiamo

$$J_A = \left(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}\right) \text{ e } K_A = \left(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}\right).$$

Notiamo che possiamo supporre che F non sia divisibile per un polinomio univariato in Z. Infatti, sia f il prodotto di tutti i polinomi univariati in Z che dividono F. Se f ha una radice reale z_0, il piano $\{z = z_0\}$ è contenuto nella parte

affine di $\mathcal{S}$, la quale dunque avrebbe singolarità reali; se invece f non ha radici reali, possiamo considerare F/f e non alterare il luogo di zeri reali.

Dunque, il nostro primo problema è decidere se $\mathcal{V}_{\mathbb{R}}(J_A) = \varnothing$. Innanzitutto J_A non può avere dimensione 2: in tal caso (visto che $\mathbb{R}[X, Y, Z]$ ha dimensione 3) deve esistere $h \in J_A$ tale che $J_A = (h)$, in particolare h sarebbe un fattore comune a F e alle sue derivate parziali, contraddicendo il fatto che F è libero da quadrati. Possiamo inoltre assumere che J_A sia radicale, dato che il passaggio al radicale non cambia il luogo di zeri.

Di conseguenza, J_A può avere dimensione -1, 0 o 1. Nel primo caso $\mathcal{V}_{\mathbb{R}}(J_A) = \varnothing$. Nel secondo caso esistono algoritmi generali e facili per calcolare $\mathcal{V}_{\mathbb{R}}(J_A)$ (e quindi verificare se sia vuoto o meno).

La situazione è più delicata nel caso in cui $\dim(J_A) = 1$. Costruiremo un altro ideale D, con $\dim(D) \leqslant 0$, in modo che $\mathcal{V}_{\mathbb{R}}(J_A) = \varnothing$ se e solo se $\mathcal{V}_{\mathbb{R}}(D) = \varnothing$. L'ideale D è costruito scegliendo una "buona proiezione" della curva $C_A := \mathcal{V}(J_A)$ su un piano in modo che possiamo ricavare i punti reali di C_A a partire dallo studio dell'immagine proiettata di C_A.

Definizione 3.4. Siano $\pi : \mathbb{C}^n \dashrightarrow \mathbb{C}^2$ la proiezione sulle ultime due coordinate e $C = \mathcal{V}(I)$ una curva in $\mathbb{C}^n$, ove $I \subset \mathbb{C}[X_1, \ldots, X_n]$ è un ideale 1-dimensionale e radicale. Diciamo che $\pi|_C$ è una *buona proiezione* se è genericamente biiettiva (cioè il numero di $P \in \pi(C)$ tali che $\#\pi^{-1}(P) > 1$ è finito) e $A := {}^{\mathbb{C}[X_1,\ldots,X_n]}/_I$ è intero su $\mathbb{C}[X_n]$.[1]

Proposizione 3.5. *La proiezione $\pi|_C$ è buona se e solo se, detta $\mathcal{G}$ la base di Gröbner ridotta di I secondo l'ordinamento* Lex *con $X_1 > \cdots > X_n$, si ha che*

1. *per ogni $i = 1, \ldots, n-1$ esiste m_i tale che $X_i^{m_i} \in \mathrm{Lt}(\mathcal{G})$;*
2. *per ogni $i = 1, \ldots, n-2$ esiste ℓ_i tale che $X_i X_n^{\ell_i} \in \mathrm{Lt}(\mathcal{G})$, o equivalentemente esistono $q_i(X_n)$, $p_i(X_{n-1}, X_n)$ tali che $q_i(X_n)X_i - p_i(X_{n-1}, X_n) \in I$.*

Dimostrazione. $\boxed{\Rightarrow}$ Il fatto che A sia intero su $\mathbb{C}[X_n]$ implica il punto 1. Infatti le relazioni integrali per le variabili X_i (che sono moniche) appartengono a I e possiamo usarle per costruire $\mathcal{G}$.

Per il punto 2., costruiamo $g(X_n)$ che si annulli

- sulla componente zero-dimensionale di I, se esiste;
- su tutti i punti dove $\pi|_C$ non è biiettiva (che sono in numero finito);

[1] Sappiamo dal Lemma di Normalizzazione di Noether che una sola variabile di ${}^{\mathbb{C}[X_1,\ldots,X_n]}/_I$ è trascendente su $\mathbb{C}$; stiamo supponendo che essa sia X_n.

- su tutti i punti singolari.

Detto $B := {}^{\mathbb{C}[X_{n-1},X_n]}/_{I^c}$ (dove la contrazione è fatta rispetto alla mappa $\pi^* : \mathbb{C}[X_{n-1},X_n] \rightarrowtail \mathbb{C}[X_1,\dots,X_n]$), consideriamo gli anelli di frazioni A_g e B_g ottenuti invertendo le potenze di g.

Per costruzione $A_g \simeq B_g$; ma un isomorfismo mappa

$$X_i \longmapsto \frac{p_i(X_{n-1},X_n)}{q_i(X_n)}$$

dove q_i è un'opportuna potenza di g. Allora $q_i(X_n)X_i - p_i(X_{n-1},X_n) \in I$, da cui la tesi.

$\boxed{\Leftarrow}$ Le relazioni del punto 1. ancora una volta ci dicono che A è intero su $\mathbb{C}[X_n]$. Per verificare la biiettività a meno di un insieme finito, consideriamo i polinomi q_i del punto 2. e definiamo

$$q(X_n) := \prod_{i=1}^{n-2} q_i(X_n).$$

L'ideale (I,q) è zero-dimensionale (avendo aggiunto una relazione per l'ultima indeterminata), quindi $\mathcal{V}(I,q)$ è finito. Ma per tutti i punti di $C \setminus \mathcal{V}(I,q)$ la proiezione è biiettiva, perché possiamo ricavare le coordinate della controimmagine di (x_{n-1},x_n) come

$$x_i = \frac{p_i(x_{n-1},x_n)}{q_i(x_n)}.$$

□

In particolare, a meno di un cambio di coordinate generale, la base di Gröbner ridotta per I è della forma

$$(X_1 - p_1(X_{n-1},X_n), X_2 - p_2(X_{n-1},X_n), \dots, p_{n-1}(X_{n-1},X_n))$$

in cui i polinomi appartengono a $\mathbb{C}(X_n)[X_1,\dots,X_{n-1}]$. In effetti, estendendo I in $\mathbb{C}(X_n)[X_1,\dots,X_{n-1}]$, otteniamo un ideale zero-dimensionale e radicale: lo Shape Lemma ci garantisce l'esistenza di una base di Gröbner come scritta sopra, e levando i denominatori si ottiene una base di Gröbner come nella proposizione precedente.

Dunque, supponiamo di avere una buona proiezione π. Chiamiamo $I := J_A^c$ rispetto a π. Ovviamente vale che $\pi(\mathcal{V}(J_A)) = \mathcal{V}(I)$. A questo punto, dato che $\dim(I) = 1$, si ha che $I = I_0 \cap I_1$, con $\dim(I_0) = 0$ e $\dim(I_1) = 1$: precisamente, se $I = (h_1,\dots,h_t)$ e $g := \mathrm{MCD}(h_1,\dots,h_t)$, allora $I_1 = (g)$ e $I_0 = (h_1/g,\dots,h_t/g)$.

Possiamo supporre g libero da quadrati, in quanto questo non cambia il luogo di zeri.

Vogliamo mettere in relazione l'esistenza di zeri reali in $\mathcal{V}(J_A)$ e $\mathcal{V}(I)$. Notiamo che $\mathcal{V}(I) = \mathcal{V}(I_0) \cup \mathcal{V}(g)$, in cui $\mathcal{V}(I_0)$ ha un numero finito di punti e $\mathcal{V}(g)$ ha un numero finito di punti singolari. Inoltre $\pi(\mathcal{V}_{\mathbb{R}}(J_A)) \subseteq \mathcal{V}_{\mathbb{R}}(I)$, quindi se $\mathcal{V}_{\mathbb{R}}(I)$ è vuoto lo sarà anche $\mathcal{V}_{\mathbb{R}}(J_A)$. L'altra inclusione non è vera in generale, perché $\mathcal{V}_{\mathbb{R}}(I)$ potrebbe contenere punti reali che non sono immagine di alcun punto reale di $\mathcal{V}_{\mathbb{R}}(J_A)$, bensì sono immagine di punti con coordinate anche complesse di $\mathcal{V}(J_A)$. Il fatto che π sia una buona proiezione ci dice che questo può capitare solo un numero finito di volte. In particolare, $\mathcal{V}_{\mathbb{R}}(I) \setminus \pi(\mathcal{V}_{\mathbb{R}}(J_A))$ è formato da un numero finito di punti isolati.

Ne consegue che $\mathcal{V}_{\mathbb{R}}(I)$ (in particolare $\mathcal{V}_{\mathbb{R}}(g)$ che ne è la parte 1-dimensionale) non può contenere componenti connesse 1-dimensionali che intersecano la retta all'infinito: se Q è un eventuale punto di intersezione, la fibra $\pi^{-1}(Q) \cap \mathcal{V}(J_A)$ deve contenere punti di $\mathcal{V}_{\mathbb{R}}(J_A)$ (solo i punti isolati possono avere fibra disgiunta da $\mathcal{V}_{\mathbb{R}}(J_A)$), ma all'inizio avevamo escluso la possibilità che $\mathcal{V}_{\mathbb{R}}(J_A)$ contenesse punti all'infinito.

Da questo si deduce che, se $p(X_{n-1})$ è un fattore univariato di g, esso non può avere radici reali c, perché altrimenti la retta $\{x_{n-1} = c\}$ sarebbe contenuta in $\mathcal{V}_{\mathbb{R}}(g)$, contraddicendo quanto affermato nel paragrafo precedente. Possiamo allora dividere g per tutti i suoi fattori univariati in X_{n-1} senza cambiare il luogo di zeri reali.

Lemma 3.6. *Sia* K_1 *l'ideale generato da* g *e* $\partial g/\partial X_n$. *Allora* $\dim(K_1) \leqslant 0$.

Dimostrazione. $\mathcal{V}(K_1)$ contiene i punti di $\mathcal{V}(g)$ singolari oppure critici rispetto alla proiezione sull'asse x_{n-1}. Inoltre $\mathcal{V}(g)$ contiene un numero finito di punti singolari, perché g è libero da quadrati. In più, dal momento che g non ha fattori univariati in X_{n-1}, $\mathcal{V}(g)$ non può contenere componenti irriducibili 1-dimensionali di punti critici. Quindi $\mathcal{V}(K_1)$ è finito. □

Tenendo conto anche della parte zero-dimensionale I_0, possiamo concludere con la seguente proposizione.

Proposizione 3.7. *Sia* $D := (J_A, I_0K_1)$. *Allora* $\dim(D) \leqslant 0$ *e* $\mathcal{V}_{\mathbb{R}}(J_A) = \varnothing$ *se e solo se* $\mathcal{V}_{\mathbb{R}}(D) = \varnothing$.

Dimostrazione. Il fatto che $\dim(D) \leqslant 0$ segue da $\dim(I_0K_1) \leqslant 0$ e dal fatto che la proiezione sia buona. Inoltre è evidente che se $\mathcal{V}_{\mathbb{R}}(J_A) = \varnothing$, allora $\mathcal{V}_{\mathbb{R}}(D) = \varnothing$. Per il viceversa, supponiamo che $\mathcal{V}_{\mathbb{R}}(D) = \varnothing$. Ricordiamo che $\mathcal{V}_{\mathbb{R}}(g)$ non può

contenere componenti connesse 1-dimensionali che intersecano la retta all'infinito. D'altra parte, $\mathcal{V}_{\mathbb{R}}(g)$ non può nemmeno contenere componenti connesse 1-dimensionali compatte, perché una tale componente conterrebbe un punto singolare o critico non isolato $W \in \mathcal{V}_{\mathbb{R}}(K_1)$. Questo W non può appartenere a $\mathcal{V}_{\mathbb{R}}(I) \setminus \pi(\mathcal{V}_{\mathbb{R}}(J_A))$ per quanto visto prima, perciò la fibra $\pi^{-1}(W)$ contiene un punto di $\mathcal{V}_{\mathbb{R}}(J_A)$. A partire da questo si proverebbe l'esistenza di un punto in $\mathcal{V}_{\mathbb{R}}(D)$, contro l'ipotesi. Dunque $\mathcal{V}_{\mathbb{R}}(g)$ ha un numero finito di punti, i quali sono necessariamente singolari e quindi contenuti in $\mathcal{V}_{\mathbb{R}}(K_1)$. Dunque $\mathcal{V}_{\mathbb{R}}(I) = \mathcal{V}_{\mathbb{R}}(I_0) \cup \mathcal{V}_{\mathbb{R}}(K_1)$: per definizione di D e per ipotesi deduciamo che $\mathcal{V}_{\mathbb{R}}(J_A) = \varnothing$. □

Una volta accertato che la superficie non sia singolare, dobbiamo verificare che i punti critici per la proiezione sull'asse z non siano degeneri. Useremo un ragionamento analogo a quanto fatto nelle ultime pagine, stavolta applicato all'ideale K_A.

Anche l'ideale K_A non può avere dimensione 2. Infatti, se h è un polinomio che descrive una componente irriducibile di dimensione 2 di $\mathcal{V}(K_A)$, allora h deve dividere sia F che le sue derivate rispetto a X e Y, perciò h è un polinomio univariato in Z e sappiamo che F non può avere un tale fattore.

Ancora una volta, i casi in cui $\dim(K_A)$ sia -1 oppure 0 sono facili da trattare, pertanto supporremo $\dim(K_A) = 1$. Costruiremo un ideale G con $\dim(G) \leqslant 0$ tale che $\mathcal{V}_{\mathbb{R}}(G)$ contenga esattamente i punti critici non degeneri.

Per prima cosa escludiamo l'esistenza di punti critici degeneri: sono quelli che annullano il determinante della matrice hessiana

$$\mathcal{H}(F) := \begin{pmatrix} \partial^2 F/\partial X^2 & \partial^2 F/\partial X \partial Y \\ \partial^2 F/\partial Y \partial X & \partial^2 F/\partial Y^2 \end{pmatrix}.$$

Occorre dunque verificare che $\mathcal{V}_{\mathbb{R}}(K_A, \det(\mathcal{H}(F)))$ sia vuoto, cosa che può essere svolta in maniera analoga a quanto visto per $\mathcal{V}_{\mathbb{R}}(J_A)$. Una volta certi che tutti i punti critici siano non degeneri, dobbiamo calcolarli.

Proposizione 3.8. *Un qualsiasi punto P appartenente a una componente 1-dimensionale (complessa) di $\mathcal{V}(K_A)$ è necessariamente un punto singolare di S, oppure è degenere.*

Dimostrazione. Sia $\mathcal{J}$ la matrice jacobiana di K_A, ovvero

$$\mathcal{J} := \begin{pmatrix} \partial F/\partial X & \partial^2 F/\partial X^2 & \partial^2 F/\partial X \partial Y \\ \partial F/\partial Y & \partial^2 F/\partial Y \partial X & \partial^2 F/\partial Y^2 \\ \partial F/\partial Z & \partial^2 F/\partial X \partial X & \partial^2 F/\partial Z \partial Y \end{pmatrix}.$$

Per un punto critico P, il determinante di $\mathcal{J}$ è uguale al prodotto tra $(\partial F/\partial Z)(P)$ e $\det(\mathcal{H}(F))(P)$. Dato che P giace su una componente 1-dimensionale, $\det(\mathcal{J})(P) =$

0, quindi si deve avere che $(\partial F/\partial Z)(P) = 0$, e in tal caso P è singolare, oppure che $\det(\mathcal{H}(F))(P) = 0$, e in tal caso P è degenere. □

Sappiamo già che $\mathcal{S}$ non ha né punti singolari né punti critici degeneri, quindi non possono esistere componenti 1-dimensionali di punti critici; in altre parole, esiste solo un numero finito di punti critici. Inoltre, detto $\Phi := (\partial F/\partial Z)\det(\mathcal{H}(F))$, se rimuoviamo da $\mathcal{V}(K_A)$ i punti di $\mathcal{V}(\Phi)$ siamo sicuri che non eliminiamo alcun punto critico reale e per di più togliamo tutte le componenti 1-dimensionali di $\mathcal{V}(K_A)$. Dunque l'ideale G che definisce $\mathcal{V}(K_A) \setminus \mathcal{V}(\Phi)$, che altri non è che il saturato $K_A : (\Phi)^\infty$, è al più zero-dimensionale e $\mathcal{V}_{\mathbb{R}}(G)$ contiene esattamente i punti critici reali non degeneri. È noto in letteratura come calcolare G: pertanto sappiamo trovare esplicitamente i punti critici.

Capitolo 4

Geometria algebrica reale

In questo capitolo studieremo alcuni aspetti della geometria algebrica reale, cioè lo studio delle soluzioni reali di equazioni e disequazioni polinomiali. Inizieremo con le radici reali di polinomi (in un certo senso, la geometria reale zero-dimensionale) e continueremo con il Teorema di Tarski-Seidenberg. Definiremo gli insiemi semialgebrici e il loro legame con l'eliminazione dei quantificatori nella teoria dei campi reali. Infine introdurremo la CAD, *Cylindrical Algebraic Decomposition*, come strumento per lo studio degli insiemi semialgebrici.

4.1 Contare le radici reali I: il metodo di Sturm

Iniziamo dai casi semplici: supponiamo che $f(X)$ sia un polinomio in $\mathbb{R}[X]$ senza radici multiple, cioè $\mathrm{MCD}(f, f') = 1$.

Definizione 4.1. Definiamo *successione di Sturm* associata a f la successione definita da $f_0 := f$, $f_1 := f'$ e per $i \geqslant 2$ f_i è il negativo del resto della divisione euclidea di f_{i-1} per f_i, cioè $f_{i+1} = f_i g_i - f_{i-1}$ per un qualche g_i. La successione termina con f_k, l'ultimo polinomio non nullo.

Proprietà immediate della successione di Sturm sono le seguenti.

1. Il polinomio f_k è una costante reale non nulla.
2. Per ogni $j = 1, \ldots, k-1$ non esiste una radice comune a f_j e f_{j+1}: per costruzione essa sarebbe anche una radice di f_{j-1} e di conseguenza una radice per ogni polinomio della successione di Sturm. In particolare essa sarebbe una radice comune a f e f', fatto che abbiamo escluso.
3. Se $f_j(\alpha) = 0$, necessariamente $f_{i+1}(\alpha) f_{i-1}(\alpha) < 0$.

Per $\alpha \in \mathbb{R}$, consideriamo $\mathbf{s}_f(\alpha) := (f_0(\alpha), \dots, f_k(\alpha)) \in \mathbb{R}^{k+1}$ e sia $\nu_f(\alpha)$ il numero di cambiamenti di segno tra due elementi consecutivi in $\mathbf{s}_f(\alpha)$, senza tener conto di eventuali zeri presenti.

Teorema 4.2 (Sturm). *Sia f come sopra. Sia $(a, b) \subseteq \mathbb{R}$ tale che $f(a) \neq 0$ e $f(b) \neq 0$. Allora il numero di radici reali di f in (a, b) è pari a $\nu_f(a) - \nu_f(b)$.*

Dimostrazione. Supponiamo che l'insieme di tutte le radici reali di tutti i polinomi f_j, per $j = 0, \dots, k-1$, sia $\{\alpha_1, \dots, \alpha_r\}$, con $\alpha_1 < \cdots < \alpha_r$. In un intervallo (α_j, α_{j+1}) tutti i polinomi hanno segno costante. Quindi possiamo limitarci a studiare il caso in cui in (a, b) ci sia esattamente una sola radice $\alpha := \alpha_i$ e concludere per additività. In particolare, deve succedere che

1. $\nu_f(a) = \nu_f(b)$ se α è radice di f_j con $j \geqslant 1$;
2. $\nu_f(a) = \nu_f(b) + 1$ se α è radice di f.

Analizziamo i due casi. Nel primo, abbiamo che $f_{i+1}(\alpha) f_{i-1}(\alpha) < 0$. Ora, f_{j-1} e f_{j+1} hanno segno costante su (a, b); in particolare guardiamo in $\mathbf{s}_f(a)$ i termini

$$(f_{j-1}(a), f_j(a), f_{j+1}(a)).$$

Il primo e il terzo hanno segno discorde, e il secondo deve avere lo stesso segno di uno dei due: in totale una variazione di segno. Lo stesso discorso si può fare per $(f_{j-1}(b), f_j(b), f_{j+1}(b))$: quindi abbiamo $\nu_f(a) = \nu_f(b)$.

Nel secondo caso, abbiamo ovviamente $f'(\alpha) \neq 0$, perché f non ha radici multiple; dunque f' ha segno costante in (a, b) e precisamente si possono verificare le seguenti situazioni:

	a	α	b
f	$+$	0	$-$
f'	$-$	$-$	$-$

oppure

	a	α	b
f	$-$	0	$+$
f'	$+$	$+$	$+$

In ogni caso $\nu_f(a) = \nu_f(b) + 1$. Questo conclude la dimostrazione. □

Come possiamo trovare il numero totale di radici reali di f? Sappiamo che le radici reali sono limitate, cioè esiste $M \in \mathbb{R}_{\geqslant 0}$ tale che ogni radice reale di f è contenuta in $(-M, M)$. Di conseguenza $\nu_f(x)$ è costante su $(-\infty, -M)$ e su (M, ∞). Più precisamente, $\nu_f(-\infty)$ è il numero di cambiamenti di segno in

$$(\mathrm{lc}(f_0(-X)), \dots, \mathrm{lc}(f_k(-X)))$$

mentre $\nu_f(\infty)$ è il numero di cambiamenti di segno in

$$(\mathrm{lc}(f_0(X)), \dots, \mathrm{lc}(f_k(X))).$$

Quindi il numero di radici reali di f è $v_f(-\infty) - v_f(\infty)$. Dobbiamo solamente trovare M.

Proposizione 4.3. *Se* $f(X) = a_0X^d + \cdots + a_d$, *con* $a_0 \neq 0$, *allora ogni* $\alpha \in \mathbb{C}$ *tale che* $f(\alpha) = 0$ *soddisfa*

$$|\alpha| \leqslant M := \max_{i=1,\dots,d} \left(d \left| \frac{a_i}{a_0} \right| \right)^{1/i}.$$

Dimostrazione. Sia M come sopra e sia $\gamma \in \mathbb{C}$ con $|\gamma| > M$. Per definizione di M, per ogni i si ha

$$|a_i| < |a_0| \frac{|\gamma|^i}{d}.$$

Ma ora

$$|a_1\gamma^{d-1} + \cdots + a_d| \leqslant |a_1||\gamma|^{d-1} + \cdots + |a_d| < d \left(|a_0| \frac{|\gamma|^d}{d} \right) = |a_0\gamma^d|.$$

Quindi $f(\gamma) \neq 0$. □

Nel caso in cui f non sia libero da quadrati, la costruzione della successione di Sturm porta a $f_k = \mathrm{MCD}(f, f')$. In tal caso, possiamo considerare la sequenza

$$\left(\frac{f_0}{f_k}, \dots, \frac{f_{k-1}}{f_k}, 1 \right).$$

Per questa successione è possibile applicare il Teorema di Sturm e giungere allo stesso risultato. Purtroppo si perde l'informazione sulla molteplicità delle radici.

A questo punto affrontiamo il problema di contare le radici reali che soddisfano anche una disuguaglianza polinomiale. In altre parole, fissati $f, g \in \mathbb{R}[X]$, vogliamo

$$\#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g(\alpha) > 0\}.$$

Supponiamo intanto che $\mathrm{MCD}(f, f'g) = 1$, cioè che f non abbia radici multiple e non abbia radici comuni con g. Definiamo una sorta di successione di Sturm a partire da $f_0 := f$, $f_1 := f'g$ e f_i come nella successione di Sturm originale. A partire da questa, possiamo definire $\mathbf{s}_{f,g}$ e $v_{f,g}$ come sopra.

Teorema 4.4. *Siano* f, g *come sopra e* (a, b) *come nel Teorema di Sturm. Allora* $v_{f,g}(a) - v_{f,g}(b)$ *è uguale al numero di radici* α *di* f *in* (a, b) *tali che* $g(\alpha) > 0$ *meno il numero di radici* α *di* f *in* (a, b) *tali che* $g(\alpha) < 0$.

Dimostrazione. Analogamente a quanto abbiamo descritto nella dimostrazione del Teorema di Sturm, sia (a, b) un intervallo di $\mathbb{R}$ che contenga un'unica radice α di un f_j e nessun'altra radice di alcun f_i, $i \neq j$. Se $j \geqslant 1$, si ha la stessa situazione del Teorema di Sturm; se invece α è radice di f, abbiamo

se $g(\alpha) > 0$,

	a	α	b
f	$+$	0	$-$
f'	$-$	$-$	$-$

oppure

	a	α	b
f	$-$	0	$+$
f'	$+$	$+$	$+$

se $g(\alpha) < 0$,

	a	α	b
f	$+$	0	$-$
f'	$+$	$+$	$+$

oppure

	a	α	b
f	$-$	0	$+$
f'	$-$	$-$	$-$

Quindi, se $g(\alpha) > 0$ si ha $v_{f,g}(a) = v_{f,g}(b) + 1$, mentre se $g(\alpha) < 0$ si ha $v_{f,g}(a) = v_{f,g}(b) - 1$. Tirando le somme si ha la tesi. □

Corollario 4.5. *Il numero di radici α di f in (a, b) tali che $g(\alpha) > 0$ è*

$$\frac{1}{2}(v_{f,g}(a) - v_{f,g}(b) + v_{f,g^2}(a) - v_{f,g^2}(b)).$$

Dimostrazione. Il numero $v_{f,g^2}(a) - v_{f,g^2}(b)$ conta le radici di f in (a, b) che non sono radici reali di g. La tesi segue facilmente. □

Completiamo la generalizzazione al caso in cui le disuguaglianze sono più di una. Dati $f, g_1, \dots, g_\ell \in \mathbb{R}[X]$ vogliamo calcolare

$$\#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_1(\alpha) > 0, \dots, g_\ell(\alpha) > 0\}.$$

Supponiamo che $\mathrm{MCD}(f, g_i) = 1$ per ogni i. Sia $\varepsilon := (\varepsilon_1, \dots, \varepsilon_\ell) \in \{0,1\}^\ell$ e sia g^ε il polinomio $g_1^{\varepsilon_1} \cdots g_\ell^{\varepsilon_\ell}$. Definiamo $s_\varepsilon := v_{f,g^\varepsilon}(-\infty) - v_{f,g^\varepsilon}(\infty)$ che è il numero di radici distinte α di f tali che $g^\varepsilon(\alpha) > 0$ meno il numero di radici distinte α di f tali che $g^\varepsilon(\alpha) < 0$. Per $\boldsymbol{\varphi} := (\varphi_1, \dots, \varphi_\ell) \in \{0,1\}^\ell$ inoltre definiamo

$$c_{\boldsymbol{\varphi}} := \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0,\ \mathrm{sgn}(g_i(\alpha)) = (-1)^{\varphi_i}\}.$$

Che relazione c'è tra s_ε e $c_{\boldsymbol{\varphi}}$?

Lemma 4.6. *Detti $\mathbf{s}$ e $\mathbf{c}$ i vettori colonna di lunghezza 2^ℓ le cui coordinate sono tutti i possibili s_ε e $c_{\boldsymbol{\varphi}}$, esiste una matrice A_ℓ di dimensione $2^\ell \times 2^\ell$ invertibile tale che $\mathbf{s} = A_\ell \mathbf{c}$.*

Dimostrazione. Per induzione su ℓ. Nel caso $\ell = 0$ non c'è nulla da dimostrare. Per $\ell = 1$ abbiamo

$$s_0 = v_f(-\infty) - v_f(\infty)$$
$$s_1 = v_{f,g}(-\infty) - v_{f,g}(\infty).$$

In particolare, s_0 è il numero di radici reali di f mentre s_1 è la differenza tra il numero di radici α di f con $g(\alpha) > 0$ e quelle con $g(\alpha) < 0$. D'altra parte

$$c_0 = \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g(\alpha) > 0\}$$
$$c_1 = \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g(\alpha) < 0\}.$$

Dunque $s_0 = c_0 + c_1$ mentre $s_1 = c_0 - c_1$, in forma matriciale

$$\mathbf{s} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \mathbf{c}.$$

Vediamo anche il caso $\ell = 2$ per convincerci meglio. Le possibilità sono $(0,0)$, $(1,0)$, $(0,1)$ e $(1,1)$, che corrispondono a $g^{(0,0)} = 1$, $g^{(1,0)} = g_1$, $g^{(0,1)} = g_2$ e $g^{(1,1)} = g_1 g_2$. Nel dettaglio

$$s_{(0,0)} = \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0\}$$
$$s_{(1,0)} = \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_1(\alpha) > 0\} - \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_1(\alpha) < 0\}$$
$$s_{(0,1)} = \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_2(\alpha) > 0\} - \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_2(\alpha) < 0\}$$
$$s_{(1,1)} = \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_1 g_2(\alpha) > 0\} - \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_1 g_2(\alpha) < 0\}$$

mentre per $c_{\boldsymbol{\varphi}}$ abbiamo

$$c_{(0,0)} = \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_1(\alpha) > 0, g_2(\alpha) > 0\}$$
$$c_{(1,0)} = \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_1(\alpha) < 0, g_2(\alpha) > 0\}$$
$$c_{(0,1)} = \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_1(\alpha) > 0, g_2(\alpha) < 0\}$$
$$c_{(1,1)} = \#\{\alpha \in \mathbb{R} \mid f(\alpha) = 0, g_1(\alpha) < 0, g_2(\alpha) < 0\}.$$

Con un po' di attenzione notiamo che

$$A_2 = \begin{pmatrix} A_1 & A_1 \\ A_1 & -A_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Il passo induttivo è scontato: si verifica che

$$A_{\ell+1} = \begin{pmatrix} A_\ell & A_\ell \\ A_\ell & -A_\ell \end{pmatrix}.$$

Tutte queste matrici sono invertibili perché $\det(A_1) = -2$ (in effetti $A_1^{-1} = \frac{1}{2} A_1$) e per induzione

$$A_{\ell+1}^{-1} = \frac{1}{2} \begin{pmatrix} A_\ell^{-1} & A_\ell^{-1} \\ A_\ell^{-1} & -A_\ell^{-1} \end{pmatrix}.$$

□

Quindi abbiamo la soluzione al nostro problema: sappiamo calcolare $\mathbf{s}$ e quindi ottenere $\mathbf{c}$. In particolare il numero che ci interessa è c_0.

Occorre a questo punto generalizzare ulteriormente al caso in cui ci sia un numero arbitrario di equazioni e disequazioni, tra le quali possono comparire anche disuguaglianze non strette. In realtà non serve del lavoro aggiuntivo: quanto fatto finora basta. Infatti:

- se sono presenti $g < 0$ (o $g \leqslant 0$) si trasformano in $-g > 0$ (rispettivamente $-g \geqslant 0$);
- se sono presenti $g \geqslant 0$, si spezza il problema in due rami, uno con $g = 0$ e uno con $g > 0$;
- se sono presenti $f_1 = \cdots = f_m = 0$, le si rimpiazza con $f_1^2 + \cdots + f_m^2 = 0$;
- se non è presente un'uguaglianza, cioè abbiamo solo $g_1 > 0, \ldots, g_m > 0$, abbiamo che
  - su un intervallo illimitato (a, ∞) (rispettivamente $(-\infty, a)$) il sistema ammette soluzione se e solo se i coefficienti di testa di $g_1, \ldots, g_m$ (rispettivamente $g_1(-X), \ldots, g_m(-X)$) sono tutti positivi;
  - su un intervallo limitato (a, b), dove a e b sono radici di $g := \prod g_i$, il sistema ammette soluzione se e solo se il sistema $g' = 0, g_1 > 0, \ldots, g_m > 0$ ammette soluzione.

4.2 Il Teorema di Tarski-Seidenberg

Consideriamo un sistema di equazioni e disequazioni polinomiali

$$\mathcal{S}(\mathbf{T}, X) = \begin{cases} S_1(\mathbf{T}, X) \triangleright_1 0 \\ S_2(\mathbf{T}, X) \triangleright_2 0 \\ \cdots \\ S_r(\mathbf{T}, X) \triangleright_r 0 \end{cases}$$

dove i simboli $\triangleright_i$ possono indicare $=$, $\neq$, $>$ oppure $\geqslant$. I polinomi S_i appartengono a $\mathbb{R}[\mathbf{T}, X] = \mathbb{R}[T_1, \ldots, T_p, X]$. Considereremo $\mathbf{T}$ come parametri. La domanda a cui daremo risposta con il Teorema di Tarski-Seidenberg è la seguente: possiamo dare delle condizioni sui parametri affinché esista una soluzione (in X) del sistema $\mathcal{S}$?

Teorema 4.7 (Tarski-Seidenberg — Forma Algebrica)**.** *Esiste un algoritmo che accetta in ingresso un sistema $\mathcal{S}(\mathbf{T}, X)$ come sopra e restituisce una lista finita $\mathcal{C}_1(\mathbf{T}), \ldots, \mathcal{C}_k(\mathbf{T})$*

di sistemi di equazioni e disequazioni polinomiali in $\mathbf{T}$ *tale che, per ogni* $\mathbf{t} \in \mathbb{R}^p$*, il sistema* $\mathcal{S}(\mathbf{t}, X)$ *ha una soluzione reale se e solo se uno dei* $\mathcal{C}_j(\mathbf{t})$ *è soddisfatto.*

Esempio 4.1. Il "sistema"

$$\mathcal{S}(A, B, C, X) = \left\{ AX^2 + BX + C = 0 \right.$$

ammette soluzione reale se e solo se siamo in una delle tre situazioni

$$\begin{cases} A \neq 0 \\ B^2 - 4AC \geqslant 0, \end{cases} \qquad \begin{cases} A = 0 \\ B \neq 0, \end{cases} \qquad \begin{cases} A = 0 \\ B = 0 \\ C = 0. \end{cases}$$

Dal momento che calcoleremo successioni di Sturm, è opportuno che i gradi dei polinomi che compaiono nel sistema non possano calare improvvisamente. In altre parole, vogliamo fissare i gradi dei polinomi del sistema, visti come polinomi in X. Se $f \in \mathbb{R}[\mathbf{T}, X]$, indichiamo con $\mathrm{lc}(f) \in \mathbb{R}[\mathbf{T}]$ il *leading coefficient* di f visto come polinomio in X.

Definizione 4.8. Chiamiamo *sistema a gradi fissati* un sistema della forma

$$\begin{cases} \mathcal{S}(\mathbf{T}, X) \\ \mathcal{D}(\mathbf{T}) \end{cases}$$

tale che $\mathcal{D}(\mathbf{T})$ contenga le equazioni $\mathrm{lc}(S) \neq 0$ per ogni polinomio S che compare in $\mathcal{S}(\mathbf{T}, X)$.

Ogni sistema è equivalente a una disgiunzione di finiti sistemi a gradi fissati: ad esempio, se S è un polinomio del sistema $\mathcal{S}(\mathbf{T}, X)$, possiamo scrivere

$$\begin{cases} \mathcal{S}(\mathbf{T}, X) \\ \mathrm{lc}(S) \neq 0 \end{cases} \vee \begin{cases} \mathcal{S}(\mathbf{T}, X) \\ \mathrm{lc}(S) = 0, \end{cases}$$

in cui nel secondo sistema ovviamente si è provveduto a sostituire il valore di $\mathrm{lc}(S)$ ove possibile (ed eventualmente si è iterato il procedimento con i nuovi *leading coefficient*).

Lemma 4.9. *Sia* $\mathcal{S}(\mathbf{T}, X)$ *il sistema definito da*

$$\begin{cases} p(\mathbf{T}, X) = 0 \\ q_1(\mathbf{T}, X) > 0 \\ \dots \\ q_\ell(\mathbf{T}, X) > 0 \end{cases}$$

e sia $\mathcal{D}(\mathbf{T})$ *il sistema*

$$\begin{cases} \mathrm{lc}(P) \neq 0 \\ \mathrm{lc}(Q_1) \neq 0 \\ \dots \\ \mathrm{lc}(Q_\ell) \neq 0. \end{cases}$$

Esiste un algoritmo che, dati $(P, Q_1, \dots, Q_\ell)$*, restituisce una lista finita di polinomi* $R_1, \dots, R_m \in \mathbb{R}[\mathbf{T}]$ *e una funzione* $c : \{-1, 0, 1\}^m \longrightarrow \mathbb{N}$ *tale che per ogni coppia* $(\mathbf{t}, \boldsymbol{\varepsilon})$ *con* $\mathbf{t} \in \mathbb{R}^p$ *e* $\boldsymbol{\varepsilon} \in \{-1, 0, 1\}^m$ *che soddisfi*

$$\begin{cases} \mathcal{D}(\mathbf{t}) \\ \mathrm{sgn}(R_1(\mathbf{t})) = \varepsilon_1 \\ \dots \\ \mathrm{sgn}(R_m(\mathbf{t})) = \varepsilon_m \end{cases}$$

il sistema

$$\begin{cases} P(\mathbf{t}, X) = 0 \\ Q_1(\mathbf{t}, X) > 0 \\ \dots \\ Q_\ell(\mathbf{t}, X) > 0 \end{cases}$$

ha esattamente $c(\boldsymbol{\varepsilon})$ *soluzioni.*

Dimostrazione. Calcoliamo le successioni di Sturm come abbiamo descritto nella sezione precedente. Ogni volta che otteniamo un nuovo polinomio F, apriamo un nuovo ramo di calcolo distinguendo i due casi in cui il suo *leading coefficient* sia nullo o meno. Nel primo caso, il calcolo della successione di Sturm riprende con il polinomio $\tilde{F}$ ottenuto da F imponendo $\mathrm{lc}(F) = 0$; nel secondo si prosegue normalmente.

Alla fine si ottiene un albero di calcolo di successioni di Sturm, in cui i test nei punti di diramazione sono equazioni polinomiali o loro negazioni nei parametri $\mathbf{T}$. Percorrendo ogni ramo di questo albero si ottiene un sistema di equazioni e negazioni di equazioni $\mathcal{B}(\mathbf{T})$ e una successione di Sturm di polinomi parametrici in $\mathbb{R}[\mathbf{T}][X]$, che è la successione di Sturm associata ai polinomi di partenza corrispondente alla scelta di un $\mathbf{t} \in \mathbb{R}^p$ che renda vero $\mathcal{B}(\mathbf{t})$. I segni dei *leading coefficient* (che sono polinomi in $\mathbb{R}[\mathbf{T}]$) della successione di Sturm così ottenuta determina la differenza del numero di cambi di segno $v(-\infty) - v(\infty)$.

Ora, questi *leading coefficient* sono funzioni razionali del tipo $A(\mathbf{T})/B(\mathbf{T})$, dove B non può annullarsi nel ramo in cui compare. Il segno di $A(\mathbf{t})/B(\mathbf{t})$

è lo stesso di $A(\mathbf{t})B(\mathbf{t})$: prendiamo allora come $R_1, \dots, R_m$ tutti i polinomi di questo tipo presenti in tutti i rami di tutti gli alberi di calcolo delle successioni di Sturm associate al sistema. I risultati della sezione precedente ci dicono che, supponendo vera $\mathcal{D}(\mathbf{t})$ e fissando il segno di ogni $R_1(\mathbf{t}), \dots, R_m(\mathbf{t})$, possiamo calcolare il numero di soluzioni reali del sistema

$$\begin{cases} p(\mathbf{t}, X) = 0 \\ q_1(\mathbf{t}, X) > 0 \\ \dots \\ q_\ell(\mathbf{t}, X) > 0. \end{cases}$$

□

La dimostrazione del lemma 4.9 è abbastanza contorta; un esempio chiarificatore, in cui si stabilisce quando un polinomio di quarto grado ammette soluzioni reali, è presente in [2].

Dimostrazione del Teorema di Tarski-Seidemberg — Forma Algebrica. In primo luogo, procedendo come nella sezione precedente, possiamo supporre che il sistema $\mathcal{S}$ sia della forma

$$\begin{cases} p(\mathbf{T}, X) = 0 \\ q_1(\mathbf{T}, X) > 0 \\ \dots \\ q_\ell(\mathbf{T}, X) > 0. \end{cases}$$

Inoltre possiamo supporre che il sistema contenga al suo interno le equazioni $\mathcal{D}(\mathbf{T})$ che codificano il fatto che sia un sistema a gradi fissati.

Per $\boldsymbol{\varepsilon} \in \{-1, 0, 1\}^m$ definiamo $\mathcal{C}_\varepsilon(\mathbf{T})$ il sistema

$$\begin{cases} \operatorname{sgn}(R_1(\mathbf{T})) = \varepsilon_1 \\ \dots \\ \operatorname{sgn}(R_m(\mathbf{T})) = \varepsilon_m \\ c(\boldsymbol{\varepsilon}) > 0 \end{cases}$$

dove $R_1, \dots, R_m$ e c sono i polinomi e la funzione come definiti nel lemma 4.9. Notiamo che in effetti queste sono equazioni e/o disequazioni polinomiali. Mostriamo che i $\mathcal{C}_\varepsilon(\mathbf{T})$ soddisfano la tesi del problema. Sia $\mathbf{t} \in \mathbb{R}^p$ fissato.
$\boxed{\Leftarrow}$ Sia $\boldsymbol{\varepsilon}$ tale che $\mathcal{C}_\varepsilon(\mathbf{t})$ sia verificato. La coppia $(\mathbf{t}, \boldsymbol{\varepsilon})$ è tale che $\operatorname{sgn}(R_i(\mathbf{t})) = \varepsilon_i$ per ogni i, quindi il lemma 4.9 ci dice che $\mathcal{S}(\mathbf{t}, X)$ ha $c(\boldsymbol{\varepsilon}) > 0$ soluzioni.

$\boxed{\Rightarrow}$ Per assurdo supponiamo che $\mathcal{S}(\mathbf{t}, X)$ abbia soluzioni ma $\mathcal{C}_\varepsilon(\mathbf{t})$ non sia verificato per nessun ε. Osserviamo che, fissato $\mathbf{t} \in \mathbb{R}^p$, esiste un $\varepsilon \in \{-1, 0, 1\}^m$ tale che

$$\operatorname{sgn}(R_1(\mathbf{t})) = \varepsilon_1, \ \ldots, \ \operatorname{sgn}(R_m(\mathbf{t})) = \varepsilon_m.$$

Tuttavia, anche per tale ε, $\mathcal{C}_\varepsilon(\mathbf{t})$ non è verificato: l'unico modo affinché capiti ciò è che $c(\varepsilon) \not> 0$. D'altra parte alla coppia $(\mathbf{t}, \varepsilon)$ è possibile applicare il lemma 4.9 e concludere che $\mathcal{S}(\mathbf{t}, X)$ ha $c(\varepsilon) = 0$ soluzioni. Questo porta all'assurdo. □

Osservazione. La disequazione $c(\varepsilon) > 0$ nei sistemi $\mathcal{C}_\varepsilon$ è stata inserita solo per alleggerire la dimostrazione. In effetti, è una disequazione che non dipende da $\mathbf{T}$: all'atto pratico, possiamo eliminare i sistemi in cui essa è falsa e ignorarla nei sistemi in cui essa è vera.

4.3 Contare le radici reali II: il metodo di Hermite

Vediamo un altro metodo per contare le radici reali di un polinomio $f \in \mathbb{R}[X]$. Supponiamo che $\deg(f) = d$, $\operatorname{lc}(f) = 1$ e che le radici complesse di f siano $\alpha_1, \ldots, \alpha_m$ ciascuna di molteplicità $\mu(\alpha_i)$.

Definizione 4.10. Definiamo i-*esima somma di Newton* associata a f il numero

$$N_i := \sum_{j=1}^{m} \mu(\alpha_j)\alpha_j^i.$$

Le somme di Newton si possono ricavare dai coefficienti di f, anche senza conoscerne le radici.

Lemma 4.11. *Per la derivata logaritmica di* f *vale*

$$\frac{f'}{f} = \sum_{i=0}^{\infty} \frac{N_i}{X^{i+1}}.$$

Dimostrazione. È un semplice conto. Da

$$f'(X) = \sum_{j=1}^{m} \mu(\alpha_j)(X - \alpha_j)^{\mu(\alpha_j)-1} \prod_{\substack{i=1 \\ i \neq j}}^{m} (X - \alpha_i)^{\mu(\alpha_i)}$$

otteniamo

$$\begin{aligned}\frac{f'}{f} &= \sum_{j=1}^{m} \frac{\mu(\alpha_j)}{X-\alpha_j} = \\ &= \sum_{j=1}^{m} \frac{\mu(\alpha_j)}{X} \frac{1}{1-\alpha_j/X} = \\ &= \sum_{j=1}^{m} \frac{\mu(\alpha_j)}{X} \sum_{i=0}^{\infty} \frac{\alpha_j^i}{X^i} = \\ &= \sum_{i=0}^{\infty} \frac{1}{X^{i+1}} \sum_{j=1}^{m} \mu(\alpha_j)\alpha_j^i = \sum_{i=0}^{\infty} \frac{N_i}{X^{i+1}}.\end{aligned}$$

□

Dal lemma precedente allora

$$f' = f \sum_{i=0}^{\infty} \frac{N_i}{X^{i+1}}$$

e uguagliando termine a termine, se $f = X^d + a_{d-1}X^{d-1} + \cdots + a_0$, ricaviamo

$$\begin{aligned} & N_0 = d \\ & N_1 = -a_{d-1} \\ & N_2 = -(N_1 a_{d-1} + 2a_{d-2}) \\ & \dots \\ \text{per } i \leqslant d \quad & N_i = -(N_{i-1}a_{d-1} + N_{i-2}a_{d-2} + \cdots + i a_{d-i}) \\ \text{per } i > d \quad & N_i = -(N_{i-1}a_{d-1} + N_{i-2}a_{d-2} + \cdots + N_{i-d}a_0). \end{aligned}$$

Mettiamo le somme di Newton in una matrice: definiamo *matrice di Hermite* associata a f la matrice

$$H(f) := \begin{pmatrix} N_0 & N_1 & N_2 & \dots & N_{d-1} \\ N_1 & N_2 & \iddots & \iddots & \vdots \\ N_2 & \iddots & \iddots & & \vdots \\ \vdots & \iddots & & & \vdots \\ N_{d-1} & \dots & \dots & \dots & N_{2d-2} \end{pmatrix}.$$

Essendo una matrice simmetrica ha senso calcolarne la segnatura, qui intesa come differenza tra indice di positività e indice di negatività.

Teorema 4.12. *La segnatura* $\sigma(H(f))$ *è il numero di radici reali distinte di* f*; il rango* $r(H(f))$ *è il numero di radici (reali e complesse) distinte di* f*.*

Osservazione. Se le radici sono tutte distinte, ovvero $m = d$, si ha $H(f) = VV^T$, dove

$$V := \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \vdots & \vdots & & \vdots \\ \alpha_1^{d-1} & \alpha_2^{d-1} & \dots & \alpha_m^{d-1} \end{pmatrix}$$

è la matrice di Vandermonde associata a $\alpha_1, \dots, \alpha_m$.

Osservazione. Il Teorema di Sylvester ci dice che $H(f)$ è simile, tramite una matrice ortogonale, a una matrice

$$S := \begin{pmatrix} I_{i_+} & & \\ & -I_{i_-} & \\ & & 0 \end{pmatrix}$$

dove I_n sono matrici identità di ordine n e i_+, i_- sono gli indici di positività e negatività. In altre parole, esiste M ortogonale tale che $H(f) = M^T S M$. In particolare, la forma bilineare associata $\mathbf{x} \mapsto \mathbf{x}^T H(f)\mathbf{x}$ diventa

$$\begin{aligned} \mathbf{x}^T M^T S M \mathbf{x} = (M\mathbf{x})^T S (M\mathbf{x}) = \\ = \sum_{i=1}^{i_+} (M_i \mathbf{x})^2 - \sum_{i=i_+ + 1}^{i_+ + i_-} (M_i \mathbf{x})^2 \end{aligned}$$

dove M_i è la riga i-esima della matrice M.

Dimostrazione del teorema 4.12. Consideriamo la matrice di Vandermonde definita sopra, senza supporre $d = m$ (quindi $V \in \mathcal{M}_{d \times m}(\mathbb{C})$). Consideriamo inoltre la matrice

$$D := \begin{pmatrix} \mu(\alpha_1) & & \\ & \ddots & \\ & & \mu(\alpha_m) \end{pmatrix} \in \mathcal{M}_m(\mathbb{R}).$$

Il rango di V è m (infatti le radici α_j sono distinte e le prime m righe sono una matrice di Vandermonde propriamente detta).

Ora, il conto mostra che $H(f) = VDV^T$. Se chiamiamo $W \in \mathcal{M}_m(\mathbb{C})$ la matrice delle prime m righe di V, si ha

$$H(f) = \left(\begin{array}{c|c} WDW^T & * \\ \hline * & * \end{array}\right)$$

e in particolare $r(H(f)) \leqslant m$ (perché $r(AB) \leqslant \min\{r(A), r(B)\}$). D'altra parte $\det(WDW^T) \neq 0$ per il Teorema di Binet, quindi $r(H(f)) \geqslant m$. Da ciò segue che $r(H(f)) = m$, che è il numero di radici complesse distinte.

Per quanto riguarda la segnatura, esplicitando il fatto che $H(f) = VDV^T$ abbiamo

$$x^T H(f) x = \sum_{j=1}^{m} \mu(\alpha_j)(L_{\alpha_j}(x))^2$$

con $L_{\alpha_j} : x \longrightarrow \sum_{i=1}^{d} \alpha_j^{i-1} x_i$.

A meno di riordinare gli indici possiamo supporre che le radici siano

$$\alpha_1, \ldots, \alpha_t, \overline{\alpha_1}, \ldots, \overline{\alpha_t}, \alpha_{2t+1}, \ldots, \alpha_m$$

in cui le prime $2t$ sono in $\mathbb{C} \setminus \mathbb{R}$ e le ultime $m - 2t$ siano in $\mathbb{R}$. Spezziamo in parte reale e parte immaginaria:

$$L_{\alpha_j}(x) = u_{\alpha_j}(x) + i v_{\alpha_j}(x)$$

dove $u_{\alpha_j} : x \longrightarrow \sum_{i=1}^{d} \mathfrak{Re}(\alpha_j^{i-1}) x_i$ e così via. Le radici complesse coniugate contribuiscono con

$$(L_{\alpha_j}(x))^2 + (L_{\overline{\alpha_j}}(x))^2 = 2\left(u_{\alpha_j}(x)^2 - v_{\alpha_j}(x)^2\right)$$

e $\mu(\alpha_j) = \mu(\overline{\alpha_j})$. In definitiva

$$x^T H(f) x = \sum_{j=1}^{t} 2\mu(\alpha_j)\left(u_{\alpha_j}(x)^2 - v_{\alpha_j}(x)^2\right) + \sum_{j=2t+1}^{m} \mu(\alpha_j)(L_{\alpha_j}(x))^2.$$

In altre parole, le radici complesse coniugate non contribuiscono alla segnatura. Di conseguenza il teorema è dimostrato. □

Generalizziamo la costruzione delle somme di Newton in modo che ci diano informazioni sulle relazioni tra le radici di un polinomio f e un altro polinomio g. Più precisamente, sia $f \in \mathbb{R}[X]$ di grado d con $\alpha_1, \ldots, \alpha_m$ radici distinte in $\mathbb{C}$ di molteplicità $\mu(\alpha_j)$ e sia $g \in \mathbb{R}[X]$ fissato.

Definizione 4.13. Chiamiamo i-*esima somma di Newton generalizzata* associata a f e g il numero

$$\tilde{N}_i := \sum_{j=1}^{m} \mu(\alpha_j) g(\alpha_j) \alpha_j^i.$$

Osserviamo che, se g è il polinomio costante 1, $\tilde{N}_i = N_i$.

Anche in questo caso non è necessario conoscere le radici di f per calcolare $\tilde{N}_i$, infatti se $g(X) = \sum b_k X^k$ e $\deg(g) = n$ si ha

$$\begin{aligned}\tilde{N}_i &= \sum_{j=1}^{m} \mu(\alpha_j)\alpha_j^i \sum_{k=0}^{n} b_k \alpha_j^k = \\ &= \sum_{k=0}^{n} b_k \sum_{j=1}^{m} \mu(\alpha_j)\alpha_j^{i+k} = \\ &= \sum_{k=0}^{n} b_k N_{i+k}.\end{aligned}$$

Sistemiamo le somme generalizzate in una matrice

$$H(f,g) := \begin{pmatrix} \tilde{N}_0 & \tilde{N}_1 & \tilde{N}_2 & \dots & \tilde{N}_{d-1} \\ \tilde{N}_1 & \tilde{N}_2 & \iddots & \iddots & \vdots \\ \tilde{N}_2 & \iddots & \iddots & & \vdots \\ \vdots & \iddots & & & \vdots \\ \tilde{N}_{d-1} & \dots & \dots & \dots & \tilde{N}_{2d-2} \end{pmatrix}$$

Teorema 4.14. *Il rango* $r(H(f,g))$ *è il numero di radici distinte complesse di* f *che non annullano* g*; la segnatura* $\sigma(H(f,g))$ *è la differenza tra il numero di radici distinte* reali α *di* f *per cui* $g(\alpha) > 0$ *e quelle per cui* $g(\alpha) < 0$*.*

Dimostrazione. La dimostrazione è simile a quella già vista per il teorema 4.12. In effetti $H(f,g) = V\tilde{D}_g V^T$, dove V è la matrice di Vandermonde già vista e

$$\tilde{D}_g := \begin{pmatrix} \mu(\alpha_1)g(\alpha_1) & & \\ & \ddots & \\ & & \mu(\alpha_m)g(\alpha_m) \end{pmatrix}.$$

Conti analoghi a quelli svolti per la dimostrazione del teorema 4.12 portano a

$$r(H(f,g)) = r(\tilde{D}_g)$$

da cui la tesi per quanto riguarda il rango. Per la segnatura, ripetendo i conti dell'altra volta si ottiene

$$x^T H(f,g)x = \sum_{j=1}^{m} \mu(\alpha_j)g(\alpha_j)(L_{\alpha_j}(x))^2.$$

Ogni radice dà alla segnatura un contributo $+1$, -1 oppure 0 a seconda del segno di g valutato in quella radice. Questo ci permette di concludere. □

Corollario 4.15. *Il rango di* $H(f, f')$ *fornisce il numero di radici complesse semplici, mentre la segnatura di* $H(f, g^2)$ *fornisce il numero di radici reali di* f *che non annullano* g.

Le matrici appena definite sono legate alla struttura di $\mathbb{R}$-spazio vettoriale di $A := {}^{\mathbb{R}[X]}/_{(f)}$. Infatti esso è uno spazio vettoriale di dimensione $d = \deg(f)$ una cui base è $([X^i] \mid i = 0. . . . , d-1)$.

Sia $g \in \mathbb{R}[X]$. La mappa di moltiplicazione

$$\begin{array}{rccc} L_g : & A & \longrightarrow & A \\ & [h] & \longmapsto & [gh] \end{array}$$

è un endomorfismo lineare di A. È chiaro che $L_g = L_h$ se e solo se $g \equiv h \pmod f$. Inoltre

$$L_{g+h} = L_g + L_h, \qquad L_{gh} = L_g \circ L_h.$$

Proposizione 4.16. *Il polinomio caratteristico di* L_g *è*

$$p_g(T) = \prod_{j=1}^{m} (T - g(\alpha_j))^{\mu(\alpha_j)}.$$

In particolare, $g(\alpha_j)$ *sono autovalori per* L_g *di molteplicità* $\mu(\alpha_j)$*; di conseguenza*

$$\operatorname{tr}(L_g) = \sum_{j=1}^{m} \mu(\alpha_j) g(\alpha_j).$$

Idea di dimostrazione. Supponiamo $m = 1$, cioè che $f(X) = (X - \alpha)^d$. Se $h(X) := g(X) - g(\alpha)$, abbiamo ovviamente $h(\alpha) = 0$, quindi $h(X)^d \in (f)$, cioè $[h]$ è nilpotente in A. Questo implica che L_h è nilpotente e che $p_g(T) = (T - g(\alpha))^d$.

Supponiamo ora $m > 1$. Spezziamo $f = f_1 f_2$ con f_1, f_2 coprimi. Il Teorema Cinese del Resto ci permette di scrivere

$${}^{\mathbb{R}[X]}/_{(f)} \simeq {}^{\mathbb{R}[X]}/_{(f_1)} \oplus {}^{\mathbb{R}[X]}/_{(f_2)}$$

e procedere per induzione. □

Definizione 4.17. Per $g \in \mathbb{R}[X]$, definiamo g-*traccia* la forma bilineare su A

$$\begin{array}{rccc} B_g : & A \times A & \longrightarrow & \mathbb{R} \\ & (p, q) & \longmapsto & \operatorname{tr}(L_{pqg}). \end{array}$$

Proposizione 4.18. *La matrice associata a* B_g *rispetto alla base* $([X^i] \mid i = 0. . . . , d-1)$ *è proprio* $H(f, g)$.

Dimostrazione. Calcoliamo la componente (i,j)-esima della matrice M associata a B_g: se la tesi è vera dovremmo ottenere $\tilde{N}_{i+j-2}$.

$$\begin{aligned} M_{i,j} &= B_g(X^{i-1}, X^{j-1}) = \\ &= \operatorname{tr}(L_{X^{i+j-2}g}) = \\ &= \sum_{k=1}^{m} \mu(\alpha_k) g(\alpha_k) \alpha_k^{i+j-2} = \tilde{N}_{i+j-2}. \end{aligned}$$

□

4.4 Contare le radici reali III: coefficienti sottorisultanti principali

Vediamo (anche se non con tutti i dettagli) altri metodi per calcolare la segnatura di una matrice.

Teorema 4.19 (Jacobi)**.** *Sia V un $\mathbb{R}$-spazio vettoriale di dimensione d e sia $b : V \times V \longrightarrow \mathbb{R}$ una forma bilineare con matrice associata A rispetto a una qualche base $\mathcal{B}$. Siano $\delta_1, \dots, \delta_d$ i determinanti dei minori principali di testa di A (δ_i è il determinante della matrice ottenuta considerando le prime i righe e le prime i colonne di A). Supponiamo che $\delta_i \neq 0$ per ogni i. Allora esiste una matrice ortogonale B tale che $BAB^T = \operatorname{diag}(\delta_1, \delta_2/\delta_1, \dots, \delta_d/\delta_{d-1})$. Inoltre, detto ν il numero di cambiamenti di segno della sequenza $(\delta_1, \dots, \delta_d)$, si ha $\sigma(A) = d - 2\nu$.*

Quando almeno uno dei δ_i è nullo, non possiamo usare il teorema precedente. Ci viene in soccorso un altro risultato, dovuto a Frobenius, che però si applica solo a una classe particolare di matrici.

Definizione 4.20. Una matrice $A = (a_{i,j})$ è detta *matrice di Hankel* se tutti i coefficienti $a_{i,j}$ con $i + j$ costante sono uguali. In altre parole, una matrice di Hankel ha coefficienti uguali tra loro lungo le diagonali parallele alla diagonale secondaria.

Notiamo che $H(f)$ è una matrice di Hankel. Il metodo di Frobenius applicato a $H(f)$ unitamente al fatto che il rango di $H(f)$ è m se e solo se $\delta_m \neq 0$ e $\delta_{m+1} = \cdots = \delta_d = 0$ (fatto questo che dimostreremo tra poco) porta al seguente teorema.

Teorema 4.21. *Sia $f \in \mathbb{R}[X]$ con $\deg(f) = d$ e siano $\delta_1, \dots, \delta_d$ i determinanti dei minori principali di testa di $H(f)$. Sia m tale che $\delta_m \neq 0$ e $\delta_{m+1} = \cdots = \delta_d = 0$. (Notiamo che $m \geqslant 1$ perché $\delta_1 = d$.) Per $i = 1, \dots, m$ definiamo i "segni convenzionali" $\widetilde{\operatorname{sgn}}(\delta_i)$ come*

- *se* $\delta_i \neq 0$, $\widetilde{\operatorname{sgn}}(\delta_i) := \operatorname{sgn}(\delta_i)$;
- *se* $\delta_i = 0$ *e* δ_{i-j} *è l'ultimo determinante non nullo (cioè* $\delta_i = \delta_{i-1} = \cdots = \delta_{i-j+1} = 0$ *e* $\delta_{i-j} \neq 0$*),*

$$\widetilde{\operatorname{sgn}}(\delta_i) := (-1)^{j(j-1)/2} \operatorname{sgn}(\delta_{i-j}).$$

Allora, detto v *il numero di cambi di segno nella sequenza* $(\widetilde{\operatorname{sgn}}(\delta_1), \ldots, \widetilde{\operatorname{sgn}}(\delta_m))$*, il numero di radici reali distinte di* f *è pari a* $m - 2v$*.*

Come dimostriamo che se $r(H(f)) = m$ allora $\delta_m \neq 0$? A partire da due polinomi f e g è possibile definire una sequenza di altri polinomi che generalizzano il concetto di risultante. Questi polinomi sono detti *polinomi sottorisultanti*. I *leading coefficient* dei polinomi sottorisultanti sono detti *coefficienti sottorisultanti principali* (*Principal Subresultant Coefficients*, PSRC) e possono essere definiti anche autonomamente.

Definizione 4.22. Sappiamo cos'è la matrice di Sylvester $\operatorname{Syl}(f, g)$ associata ai polinomi f e g. In questo caso è meglio vederla in un'altra forma. Se $f(X) = a_d X^d + \cdots + a_0$ e $g(X) = b_n X^n + \cdots + b_0$, definiamo *matrice di Sylvester-Habicht* la matrice $\widetilde{\operatorname{Syl}}(f, g) \in \mathcal{M}_{d+n}(\mathbb{R})$ data da

$$\begin{pmatrix}
a_d & a_{d-1} & a_{d-2} & \ldots & \ldots & \ldots & \ldots & a_0 & 0 & \ldots & \ldots & 0 \\
0 & a_d & a_{d-1} & \ldots & \ldots & \ldots & \ldots & a_1 & a_0 & 0 & \ldots & 0 \\
\ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & \ldots & \ldots & \ldots & 0 & a_d & a_{d-1} & a_{d-2} & \ldots & \ldots & \ldots & a_0 \\
0 & \ldots & \ldots & \ldots & \ldots & 0 & b_n & b_{n-1} & \ldots & \ldots & \ldots & b_0 \\
\iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots & \iddots \\
0 & b_n & b_{n-1} & \ldots & \ldots & \ldots & b_1 & b_0 & 0 & \ldots & \ldots & 0 \\
b_n & b_{n-1} & b_{n-2} & \ldots & \ldots & \ldots & b_0 & 0 & \ldots & \ldots & \ldots & 0
\end{pmatrix}.$$

Definizione 4.23. Siano f, g polinomi di grado rispettivamente d e n. Per ogni $k = 0, \ldots, \min\{d, n\}$ (se $d \neq n$) o per ogni $k = 0, \ldots, d-1$ (se $d = n$) definiamo *coefficiente sottorisultante principale* di ordine k, indicato con $\operatorname{PSRC}_k(f, g)$, il determinante della matrice ottenuta da $\widetilde{\operatorname{Syl}}(f, g)$ eliminando le prime k righe, le ultime k righe, le prime k colonne e le ultime k colonne (tale matrice ha dunque ordine $d + n - 2k$). Osserviamo che $\operatorname{Ris}(f, g) = \operatorname{PSRC}_0(f, g)$.

Il seguente teorema generalizza il fatto che il massimo comun divisore fra f e g è diverso da 1 (cioè f e g hanno radici comuni) se e solo se $\operatorname{Ris}(f, g) = 0$. Una dimostrazione si può trovare in [2].

Teorema 4.24. *Sia ℓ un intero compreso tra 0 e $\min\{d, n\}$ (se $d \neq n$) oppure tra 0 e $d-1$ (se $d = n$). Allora* $\deg(\mathrm{MCD}(f, g)) > \ell$ *se e solo se* $\mathrm{PSRC}_0(f, g) = \cdots = \mathrm{PSRC}_\ell(f, g) = 0$.

È giunto il momento di legare i coefficienti sottorisultanti principali con la matrice di Hermite.

Proposizione 4.25. *Sia δ_j il determinante del minore principale di testa di ordine j di $H(f)$. Allora*

$$\mathrm{lc}(f)^{2j-1}\delta_j = \mathrm{PSRC}_{d-j}(f, f').$$

Corollario 4.26. *Sono equivalenti:*

1. *f ha m radici complesse distinte;*
2. *$r(H(f)) = m$;*
3. *$\delta_m \neq 0$ e $\delta_j = 0$ per $m < j \leqslant d$;*
4. *$\mathrm{PSRC}_{d-m}(f, f') \neq 0$ e $\mathrm{PSRC}_k(f, f') = 0$ per $0 \leqslant k < d - m$.*

4.5 Insiemi semialgebrici

Gli oggetti naturali con cui lavorare studiando la geometria algebrica reale non sono gli insiemi algebrici, bensì quelli *semialgebrici*: ammettiamo anche la presenza di disequazioni polinomiali. Ad esempio, tra i vantaggi che questa inclusione porta c'è il fatto che la proiezione di un insieme semialgebrico è ancora semialgebrica (invece non sempre la proiezione di un insieme algebrico è algebrica: la proiezione della circonferenza $x^2 + y^2 = 1$ su un asse è l'intervallo $-1 \leqslant x \leqslant 1$, che non è un insieme algebrico — in effetti è un insieme semialgebrico).

Definizione 4.27. Un *insieme semialgebrico* di $\mathbb{R}^n$ è l'insieme dei punti di $\mathbb{R}^n$ che soddisfano combinazioni booleane di equazioni e disequazioni polinomiali a coefficienti in $\mathbb{R}$. In altre parole, la classe degli insiemi semialgebrici di $\mathbb{R}^n$, indicata con $\mathcal{SA}_n$, è la più piccola classe di sottoinsiemi di $\mathbb{R}^n$ tale che

1. se $p \in \mathbb{R}[X_1, \ldots, X_n]$, allora $\{\mathbf{x} \in \mathbb{R}^n \mid p(\mathbf{x}) = 0\} \in \mathcal{SA}_n$ e $\{\mathbf{x} \in \mathbb{R}^n \mid p(\mathbf{x}) > 0\} \in \mathcal{SA}_n$;
2. se $A, B \in \mathcal{SA}_n$, allora anche $A \cup B$, $A \cap B$ e $\mathbb{R}^n \setminus A$ vi appartengono.

Proposizione 4.28. *Ogni insieme semialgebrico di $\mathbb{R}^n$ è unione finita di insiemi della forma*

$$\{\mathbf{x} \in \mathbb{R}^n \mid p(\mathbf{x}) = 0, q_1(\mathbf{x}) > 0, \dots, q_\ell(\mathbf{x}) > 0\}$$

al variare di $\ell \in \mathbb{N}$, $p, q_1, \dots, q_\ell \in \mathbb{R}[\mathbf{X}]$.

Dimostrazione. Se $\mathcal{F}_n$ è la classe delle unioni finite degli insiemi della forma suddetta, ovviamente $\mathcal{F}_n \subseteq \mathcal{SA}_n$; viceversa, $\mathcal{F}_n$ soddisfa le condizioni 1. e 2. della definizione 4.27, quindi $\mathcal{SA}_n \subseteq \mathcal{F}_n$. □

Esempi di insiemi semialgebrici sono:

- in $\mathbb{R}$, unioni finite di punti e intervalli aperti (limitati e illimitati);
- i sottoinsiemi algebrici, cioè definiti da equazioni polinomiali;
- se $f : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ è una mappa polinomiale, cioè $f(\mathbf{x}) = (f_1(\mathbf{x}), \dots, f_n(\mathbf{x}))$ con $f_i \in \mathbb{R}[X_1, \dots, X_m]$, allora per ogni $A \in \mathcal{SA}_n$ si ha $f^{-1}(A) \in \mathcal{SA}_m$ (perché composizioni di polinomi sono polinomi);
- se $A \in \mathcal{SA}_n$ e L è una retta in $\mathbb{R}^n$, allora $L \cap A \in \mathcal{SA}_1$;
- se $A \in \mathcal{SA}_m$ e $B \in \mathcal{SA}_n$, allora $A \times B \in \mathcal{SA}_{m+n}$.

Dunque la classe degli insiemi semialgebrici è chiusa per unione, intersezione, complementare, controimmagine rispetto a una mappa polinomiale, prodotto cartesiano. Il Teorema di Tarski-Seidenberg riletto in chiave di insiemi semialgebrici ci dice che tale classe è chiusa anche rispetto alla proiezione.

Teorema 4.29 (Tarski-Seidenberg — Forma Geometrica)**.** *Siano $A \in \mathcal{SA}_{n+1}$ e $\pi : \mathbb{R}^{n+1} \longrightarrow \mathbb{R}^n$ la proiezione sulle prime n coordinate. Allora $\pi(A) \in \mathcal{SA}_n$.*

Dimostrazione. A è l'unione di finiti insiemi della forma

$$\{\mathbf{x} \in \mathbb{R}^{n+1} \mid p(\mathbf{x}) = 0, q_1(\mathbf{x}) > 0, \dots, q_\ell(\mathbf{x}) > 0\},$$

quindi supponiamo che A stesso abbia questa forma. Ora,

$$\pi(A) = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid \exists\, x_{n+1} \in \mathbb{R} \text{ tale che } (x_1, \dots, x_{n+1}) \in A\}.$$

Il Teorema di Tarski-Seidenberg in forma algebrica ci dice che esiste una combinazione booleana $\mathcal{C}(X_1, \dots, X_n)$ di equazioni e disequazioni polinomiali tali che

$$\pi(A) = \{\mathbf{x} \in \mathbb{R}^n \mid \mathcal{C}(\mathbf{x})\},$$

che dunque è un insieme semialgebrico. □

Corollario 4.30. *Siano* $A \in \mathcal{SA}_{n+k}$ *e* $\pi_n : \mathbb{R}^{n+k} \longrightarrow \mathbb{R}^n$ *la proiezione sulle prime* n *coordinate. Allora* $\pi_n(A) \in \mathcal{SA}_n$.

Dimostrazione. Ovviamente, per induzione su k. □

Corollario 4.31. *Se* $A \in \mathcal{SA}_m$ *e* $f : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ *è una mappa polinomiale, allora* $f(A) \in \mathcal{SA}_n$.

Dimostrazione. Il grafico

$$\Gamma_f := \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^{m+n} \mid \mathbf{x} \in A, \mathbf{y} = f(\mathbf{x})\}$$

è un insieme semialgebrico di $\mathbb{R}^{m+n}$, e $f(A)$ è la sua proiezione sulle ultime n coordinate. □

Corollario 4.32. *Se* $A \in \mathcal{SA}_n$, *anche la sua chiusura topologica* $\overline{A}$ *(rispetto alla topologia euclidea di* $\mathbb{R}^n$*) è semialgebrica.*

Dimostrazione. La chiusura di A è

$$\overline{A} = \{\mathbf{x} \in \mathbb{R}^n \mid \forall\, \varepsilon > 0\ \exists\, \mathbf{y} \in A \text{ tale che } \|\mathbf{x} - \mathbf{y}\|^2 < \varepsilon^2\}$$

e può essere scritta come

$$\overline{A} = \mathbb{R}^n \setminus \Big(\pi_1\big(\{(\mathbf{x}, \varepsilon) \in \mathbb{R}^n \times \mathbb{R} \mid \varepsilon > 0\} \setminus \pi_2(B)\big)\Big)$$

dove $\pi_1 : (\mathbf{x}, \varepsilon) \mapsto \mathbf{x}$, $\pi_2 : (\mathbf{x}, \varepsilon, \mathbf{y}) \mapsto (\mathbf{x}, \varepsilon)$ e

$$B := \left\{ (\mathbf{x}, \varepsilon, \mathbf{y}) \in \mathbb{R}^n \times \mathbb{R} \times \mathbb{R}^n \;\middle|\; \mathbf{y} \in A, \sum_{i=1}^{n} (x_i - y_i)^2 < \varepsilon^2 \right\}.$$

Il fatto che B sia semialgebrico conclude la dimostrazione. □

Il Teorema di Tarski-Seidenberg ha delle conseguenze interessati anche dal punto di vista della logica matematica. In effetti, è più naturale descrivere gli insiemi in termine di formule piuttosto che di proiezioni (l'ultimo corollario ne è una prova pratica).

Definizione 4.33. Sia $\mathcal{V}$ un insieme (numerabile) di variabili, che possono assumere valori reali. Definiamo *formula del primo ordine* (nel linguaggio dei campi ordinati con parametri in $\mathbb{R}$) ricorsivamente:

1. se $n \in \mathbb{N}$, $p \in \mathbb{R}[X_1, \ldots, X_n]$ e $x_1, \ldots, x_n \in \mathcal{V}$, allora $p(x_1, \ldots, x_n) = 0$ e $p(x_1, \ldots, x_n) > 0$ sono formule;

2. se φ, ψ sono formule, allora $\varphi \vee \psi$, $\varphi \wedge \psi$ e $\neg\varphi$ sono formule;

3. se $n \in \mathbb{N}$, $\varphi(x_1, \ldots, x_{n+1})$ è una formula con $n+1$ variabili libere e $y \in \mathcal{V}$, allora $\exists\, y\ \varphi(x_1, \ldots, x_n, y)$ e $\forall\, y\ \varphi(x_1, \ldots, x_n, y)$ sono formule.

Le formule del tipo 1. sono dette *atomiche*; quelle del tipo 1. e 2. sono dette *libere da quantificatori*.

Per definizione, un insieme $A \subseteq \mathbb{R}^n$ è semialgebrico se e solo se esiste una formula libera da quantificatori $\varphi(x_1, \ldots, x_n)$ tale che

$$(x_1, \ldots, x_n) \in A \Leftrightarrow \varphi(x_1, \ldots, x_n).$$

Teorema 4.34 (Tarski-Seidenberg — Forma Logica)**.** *Se $\varphi(x_1, \ldots, x_n)$ è una formula del primo ordine qualsiasi, allora*

$$\{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid \varphi(x_1, \ldots, x_n)\}$$

è semialgebrico (e quindi può essere descritto da formule solo di tipo 1. e 2.).

Dimostrazione. Dimostriamo il teorema per induzione sulla complessità delle formule. Le formule di tipo 1. producono solo insiemi semialgebrici e le formule del tipo 2. producono insiemi semialgebrici a partire da insiemi semialgebrici. Resta da verificare il tipo 3. L'insieme

$$A = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid \exists\, y \text{ tale che } \varphi(x_1, \ldots, x_n, y)\}$$

è la proiezione di

$$\{(x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1} \mid \varphi(x_1, \ldots, x_{n+1})\},$$

che è semialgebrico per ipotesi induttiva; per il Teorema di Tarski-Seidenberg in forma geometrica anche A è semialgebrico. La dimostrazione per il quantificatore universale segue immediatamente ricordando che $\forall\, y\ \varphi(y)$ è equivalente a $\neg\exists\, y\ \neg\varphi(y)$. □

Il teorema precedente si traduce in: ogni formula del primo ordine è equivalente a una formula libera di quantificatori, o, in altre parole, $\mathbb{R}$ ammette l'eliminazione di quantificatori nel linguaggio dei campi ordinati.

4.6 Funzioni semialgebriche

Ora che abbiamo definito gli oggetti, occupiamoci delle funzioni tra di essi.

Definizione 4.35. Siano $A \subseteq \mathbb{R}^m$ e $B \subseteq \mathbb{R}^n$ due insiemi semialgebrici. Una mappa $f : A \longrightarrow B$ è *semialgebrica* se il grafico

$$\Gamma_f = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^m \times \mathbb{R}^n \mid \mathbf{y} = f(\mathbf{x})\}$$

è un insieme semialgebrico di $\mathbb{R}^m \times \mathbb{R}^n$.

Notiamo che *non* è richiesto che f sia continua.

Teorema 4.36. *Sia $f : (a, +\infty) \longrightarrow \mathbb{R}$ una mappa semialgebrica (non necessariamente continua). Allora esiste $b \geqslant a$ e $n \in \mathbb{N}$ tali che $|f(x)| \leqslant x^n$ per ogni $x \in (b, +\infty)$.*

Dimostrazione. Sia $\Gamma \subseteq \mathbb{R}^2$ il grafico di f, che per definizione è semialgebrico. Possiamo scrivere

$$\Gamma = \bigcup_{i=1}^{p} G_i$$

dove $G_i := \{(x, y) \in \mathbb{R}^2 \mid p_i(x, y) = 0, q_{i,1}(x, y) > 0, \ldots, q_{i,k_i}(x, y) > 0\}$. Ogni p_i deve avere grado strettamente positivo in Y, altrimenti se $(x_0, y_0) \in G_i$ si avrebbe che Γ contiene un intervallo aperto della retta verticale $\{x_0\} \times \mathbb{R}$, il che è impossibile perché Γ è grafico di una funzione. Sia p il prodotto di tutti i p_i; scriviamo

$$p(X, Y) = a_0(X)Y^d + \cdots + a_d(X)$$

con $d > 0$ e $a_0(X) \neq 0$. Sia $c \in \mathbb{R}$, $c \geqslant a$ tale che $a_0(x) \neq 0$ per ogni $x > c$.

Per definizione $(x, f(x))$ è una radice di p, quindi applicando la proposizione 4.3 a p visto come polinomio in Y si ha

$$|f(x)| \leqslant \max_{i=1,\ldots,d} \left(d \left| \frac{a_i(x)}{a_0(x)} \right| \right)^{1/i}.$$

Per $x \longrightarrow +\infty$ il membro di destra della disuguaglianza tende a λx^α per un opportuno $\lambda > 0$ e $\alpha \in \mathbb{Q}$; scegliendo opportunamente un intero $n > \alpha$ e $b \geqslant c$ si ottiene la tesi. □

Teorema 4.37 (Disuguaglianza di Łojasiewicz)**.** *Sia $K \subset \mathbb{R}^n$ un insieme semialgebrico compatto. Siano $f, g : K \longrightarrow \mathbb{R}$ funzioni semialgebriche continue tali che*

$$\forall\, \mathbf{x} \in K \; (f(\mathbf{x}) = 0 \Rightarrow g(\mathbf{x}) = 0).$$

Allora esistono un intero $n \in \mathbb{N}$ e una costante $c \geqslant 0$ tali che per ogni $\mathbf{x} \in K$

$$|g(\mathbf{x})|^n \leqslant c|f(\mathbf{x})|.$$

Dimostrazione. Per $t > 0$, definiamo

$$F_t := \{x \in K \mid t|g(x)| = 1\}.$$

Se $F_t \neq \varnothing$, è un compatto (è chiuso e sta in K). Per ipotesi f non si annulla in nessun punto di F_t, quindi su F_t è ben definita la funzione $x \longmapsto 1/|f(x)|$. Questa è continua, quindi per il Teorema di Weierstrass ammette massimo in F_t, che sarà indicato con $\theta(t)$. Se $F_t = \varnothing$, poniamo $\theta(t) = 0$. La funzione

$$\begin{array}{rccc} \theta: & (0,+\infty) & \longrightarrow & \mathbb{R} \\ & t & \longmapsto & \theta(t) \end{array}$$

è semialgebrica, quindi per il teorema 4.36 esistono $b > 0$ e $n \in \mathbb{N}$ tali che per ogni $t > b$ $|\theta(t)| \leqslant t^n$. Questo è equivalente a

$$\forall\, x \in K \left(0 < |g(x)| < \frac{1}{b} \Rightarrow \frac{1}{|f(x)|} \leqslant \frac{1}{|g(x)|^n}\right).$$

A questo punto consideriamo l'insieme

$$K_1 := \left\{x \in K \;\middle|\; |g(x)| \geqslant \frac{1}{b}\right\}.$$

K_1 è un compatto e f non si annulla in alcun suo punto; sia d il massimo assunto su K_1 dalla funzione continua

$$\frac{|g(x)|^n}{|f(x)|}$$

e sia $c := \max\{1, d\}$. Unendo i risultati precedenti si ha che

$$|g(x)|^n \leqslant c|f(x)|$$

per ogni $x \in K$. □

4.7 *Cylindrical Algebraic Decomposition*

Un sottoinsieme semialgebrico di $\mathbb{R}$ è unione finita di punti e/o intervalli aperti. In realtà ogni insieme semialgebrico di $\mathbb{R}^n$ può essere decomposto nell'unione disgiunta di un numero finito di componeni semialgebricamente omeomorfe a ipercubi aperti $(0,1)^d$ di dimensioni variabili.

Definizione 4.38. Una funzione f è un *omeomorfismo semialgebrico* se è semialgebrica, continua, biiettiva con inversa continua.

Osserviamo che l'inversa è automaticamente semialgebrica.

Definizione 4.39. Una *cylindrical algebraic decomposition* (in breve CAD) di $\mathbb{R}^n$ è una successione $(\mathcal{C}_1, \dots, \mathcal{C}_n)$ in cui ogni $\mathcal{C}_k$ è una partizione finita di $\mathbb{R}^k$ in insiemi semialgebrici (detti *celle*: vedremo tra poco il motivo di questa nomenclatura) tali che

1. ogni cella $C \in \mathcal{C}_1$ è un punto o un intervallo aperto, eventualmente illimitato;
2. per ogni $k = 1, \dots, n-1$ e per ogni $C \in \mathcal{C}_k$ esiste un insieme finito di funzioni continue semialgebriche

$$\xi_{C,1} < \cdots < \xi_{C,\ell_C} : C \longrightarrow \mathbb{R}$$

(in cui l'ordinamento è quello puntuale sulle immagini: $f < g$ se e solo se per ogni x nel dominio $f(x) < g(x)$) tali che il cilindro $C \times \mathbb{R} \subseteq \mathbb{R}^{k+1}$ è l'unione disgiunta di celle in $\mathcal{C}_{k+1}$ che sono di uno dei due tipi tra

   (a) grafico di una funzione $\xi_{C,j}$ per $j = 1, \dots, \ell_C$:

$$A_{C,j} := \{(\boldsymbol{x}, x_{k+1}) \in C \times \mathbb{R} \mid x_{k+1} = \xi_{C,j}(\boldsymbol{x})\};$$

   (b) banda del cilindro limitata dai due grafici di $\xi_{C,j}$ e $\xi_{C,j+1}$ per $j = 0, \dots, \ell_C$ (in cui per definizione $\xi_{C,0} := -\infty$ e $\xi_{C,\ell_C+1} := +\infty$):

$$B_{C,j} := \{(\boldsymbol{x}, x_{k+1}) \in C \times \mathbb{R} \mid \xi_{C,j}(\boldsymbol{x}) < x_{k+1} < \xi_{C,j+1}(\boldsymbol{x})\}.$$

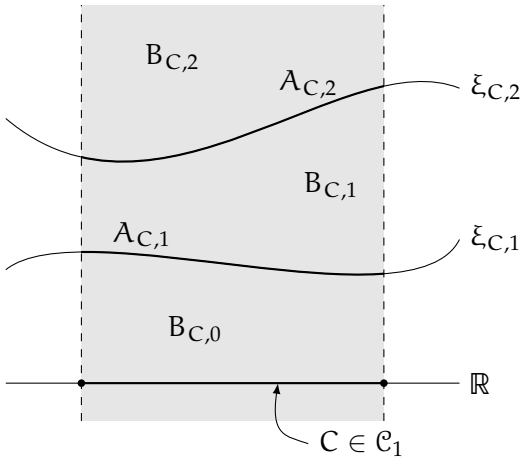


Figura 4.1: Esempio di decomposizione di un cilindro $C \times \mathbb{R} \subset \mathbb{R}^2$.

Proposizione 4.40. *Ogni cella di una CAD è omeomorfa semialgebricamente a un ipercubo aperto* $(0,1)^d$ *(per convenzione,* $(0,1)^0$ *è un punto).*

Dimostrazione. La dimostrazione procede per induzione su k, dimostrando la proprietà per le celle di $\mathcal{C}_k$. Se $k = 1$ la tesi è vera. Supponiamo che la tesi sia vera per le celle di $\mathcal{C}_k$. Per definizione, le celle di $\mathcal{C}_{k+1}$ sono della forma $A_{C,j}$ oppure $B_{C,j}$ per qualche cella $C \in \mathcal{C}_k$. Il punto chiave è mostrare che ogni insieme $A_{C,j}$ è semialgebricamente omeomorfo a C, mentre ogni insieme $B_{C,j}$ è semialgebricamente omeomorfo a $C \times (0,1)$.

Per $A_{C,j}$ è facile: la mappa

$$\begin{array}{ccc} C & \longrightarrow & A_{C,j} \\ x & \longmapsto & (x, \xi_{C,j}(x)) \end{array}$$

è un omeomorfismo semialgebrico. Per $B_{C,j}$ l'omeomorfismo è un po' più lungo da scrivere, ma è sostanzialmente una riparametrizzazione dei segmenti, distinguendo i casi limitati e quelli illimitati:

$$\begin{array}{ccc} C \times (0,1) & \longrightarrow & B_{C,j} \\ (x,t) & \longmapsto & \begin{cases} \big(x, (1-t)\xi_{C,j}(x) + t\xi_{C,j+1}(x)\big) & \text{se } 0 < j < \ell_C \\ \left(x, \dfrac{t-1}{t}\xi_{C,1}(x)\right) & \text{se } j = 0, \ell_C \neq 0 \\ \left(x, -\dfrac{1}{t} + \dfrac{1}{1-t}\right) & \text{se } j = \ell_C = 0 \\ \left(x, \dfrac{t}{1-t}\xi_{C,\ell_C}(x)\right) & \text{se } j = \ell_C \neq 0. \end{cases} \end{array}$$

□

Ma a cosa serve una CAD? Quello che in realtà ci serve è adattare la CAD ai dati polinomiali che abbiamo a disposizione.

Definizione 4.41. Dato un insieme finito di polinomi $p_1, \ldots, p_r \in \mathbb{R}[X_1, \ldots, X_n]$, diciamo che un sottoinsieme $C \subseteq \mathbb{R}^n$ è $(p_1, \ldots, p_r)$-*invariante* se ogni polinomio p_i ha segno costante in C. Una CAD è detta *adattata a* $(p_1, \ldots, p_r)$ se ogni sua cella $C \in \mathcal{C}_n$ è $(p_1, \ldots, p_r)$-invariante.

Se $(\mathcal{C}_1, \ldots, \mathcal{C}_n)$ è una CAD adattata a $(p_1, \ldots, p_r)$, un insieme semialgebrico di $\mathbb{R}^n$ descritto da equazioni e disequazioni che coinvolgono polinomi in $p_1, \ldots, p_r$ può essere decomposto nell'unione disgiunta di celle di $\mathcal{C}_n$. Se dimostriamo

l'esistenza di una CAD adattata a $(p_1, \dots, p_r)$, scelti $p_1, \dots, p_r \in \mathbb{R}[X_1, \dots, X_n]$, possiamo dedurre che ogni insieme semialgebrico può essere decomposto nell'unione disgiunta di un numero finito di pezzi, ciascuno semialgebricamente omeomorfo a un ipercubo aperto.

Cerchiamo di costruire dunque una CAD adattata. Dato che richiediamo che i polinomi $p_1, \dots, p_r$ abbiano segno costante nelle bande $B_{C,j}$, ci aspettiamo che le funzioni $\xi_{C,j}$ descrivano gli zeri dei polinomi $p_1, \dots, p_r$.

Proposizione 4.42. *Sia* $p(X_1, \dots, X_n) \in \mathbb{R}[X_1, \dots, X_n]$. *Sia* $C \subseteq \mathbb{R}^{n-1}$ *connesso, semialgebrico e siano* $k, d \in \mathbb{N}$ *con* $k \leqslant d$ *tali che per ogni punto* $\mathbf{x} = (x_1, \dots, x_{n-1}) \in C$ *il polinomio* $p(\mathbf{x}, X_n)$ *abbia grado* d *ed esattamente* k *radici distinte in* $\mathbb{C}$. *Allora esistono* $\ell \leqslant k$ *funzioni continue semialgebriche* $\xi_1 < \cdots < \xi_\ell : C \longrightarrow \mathbb{R}$ *tali che per ogni* $\mathbf{x} \in C$ *l'insieme delle radici reali di* $p(\mathbf{x}, X_n)$ *è* $\{\xi_1(\mathbf{x}), \dots, \xi_\ell(\mathbf{x})\}$. *Inoltre, per* $j = 1, \dots, \ell$ *la molteplicità di ogni radice* $\xi_j(\mathbf{x})$ *è costante al variare di* $\mathbf{x} \in C$.

Dimostrazione. La dimostrazione di questo fatto richiede il noto *principio di continuità delle radici*, che nel nostro caso può essere formulato come segue.

Proposizione (Continuità delle radici)**.** *Sia* $\boldsymbol{\alpha} \in C$ *e siano* $z_1, \dots, z_k \in \mathbb{C}$ *le radici complesse distinte di* $p(\boldsymbol{\alpha}, X_n)$ *con molteplicità rispettivamente* $m_1, \dots, m_k$. *Sia* $\varepsilon > 0$ *abbastanza piccolo in modo che i dischi aperti* $B(z_i, \varepsilon) \subseteq \mathbb{C}$ *siano disgiunti. Se* $\boldsymbol{\beta} \in C$ *è sufficientemente vicino ad* α, *allora il polinomio* $p(\boldsymbol{\beta}, X_n)$ *ha esattamente* m_i *radici, contate con molteplicità, nel disco* $B(z_i, \varepsilon)$ *per* $i = 1, \dots, k$.

Sia allora $\boldsymbol{\alpha} \in C$ come nelle ipotesi del principio di continuità delle radici. Sia $\boldsymbol{\beta} \in C$ sufficientemente vicino ad $\boldsymbol{\alpha}$. Per ipotesi, anche $p(\boldsymbol{\beta}, X_n)$ ha k radici complesse distinte. Dato che $p(\boldsymbol{\beta}, X_n)$ deve avere almeno una radice in ogni disco $B(z_i, \varepsilon)$ e ne deve avere m_i contate con molteplicità, deduciamo che in ogni disco $B(z_i, \varepsilon)$ il polinomio $p(\boldsymbol{\beta}, X_n)$ ha esattamente una radice ζ_i di molteplicità m_i. Ora, se z_i è reale, anche ζ_i dev'esserlo (altrimenti la coniugata $\overline{\zeta_i}$ sarebbe un'altra radice di $p(\boldsymbol{\beta}, X_n)$ in $B(z_i, \varepsilon)$); se z_i non è reale, nemmeno ζ_i lo è (il disco $B(z_i, \varepsilon)$ è disgiunto dalla sua immagine tramite coniugazione). Di conseguenza il numero di radici reali di $p(\boldsymbol{\alpha}, X_n)$ e $p(\boldsymbol{\beta}, X_n)$ è lo stesso per $\boldsymbol{\beta}$ sufficientemente vicino ad $\boldsymbol{\alpha}$. Poiché C è connesso (per archi), il numero di radici reali distinte di $p(\mathbf{x}, X_n)$ è costante al variare di $\mathbf{x} \in C$. Sia ℓ tale numero; per $i = 1, \dots, \ell$ sia $\xi_i : C \longrightarrow \mathbb{R}$ la funzione che manda $\mathbf{x}$ nell'i-esima radice (in ordine crescente) di $p(\mathbf{x}, X_n)$. Le funzioni ξ_i sono continue per costruzione (possiamo scegliere ε piccolo a piacere); la molteplicità delle radici $\xi_i(\mathbf{x})$ è costante sempre per connessione di C. Dobbiamo solo mostrare che le ξ_i sono semialgebriche. Sia $\Theta(\mathbf{x})$ la formula che

descrive C: il grafico di ξ_i è dato dai punti $(\mathbf{x}, x_n) \in \mathbb{R}^{n-1} \times \mathbb{R}$ tali che

$$\begin{cases} \Theta(\mathbf{x}) \\ \exists\, y_1, \ldots, y_\ell \text{ tali che } y_1 < \cdots < y_\ell, p(\mathbf{x}, y_1) = \cdots = p(\mathbf{x}, y_\ell) = 0, x_n = y_i \end{cases}$$

e questo prova che ξ_i è semialgebrica. □

Se abbiamo più di un polinomio, dobbiamo fare attenzione a non mescolare le radici di polinomi diversi.

Proposizione 4.43. *Siano* $p, q \in \mathbb{R}[X_1, \ldots, X_n]$ *e sia* $C \subseteq \mathbb{R}^{n-1}$ *semialgebrico e connesso. Supponiamo che il grado e il numero di radici distinte di* $p(\mathbf{x}, X_n)$*, di* $q(\mathbf{x}, X_n)$ *e il grado del massimo comun divisore tra* $p(\mathbf{x}, X_n)$ *e* $q(\mathbf{x}, X_n)$ *siano costanti al variare di* $\mathbf{x} \in C$*. Siano* $\xi, \zeta : C \longrightarrow \mathbb{R}$ *continue e semialgebriche tali che* $p(\mathbf{x}, \xi(\mathbf{x})) = 0$ *e* $q(\mathbf{x}, \zeta(\mathbf{x})) = 0$ *per ogni* $\mathbf{x} \in C$*. Se esiste* $\boldsymbol{\alpha} \in C$ *tale che* $\xi(\boldsymbol{\alpha}) = \zeta(\boldsymbol{\alpha})$*, allora* $\xi(\mathbf{x}) = \zeta(\mathbf{x})$ *per ogni* $\mathbf{x} \in C$*.*

Dimostrazione. Siano $z_1, \ldots, z_k$ le radici complesse distinte del polinomio prodotto $p(\boldsymbol{\alpha}, X_n)q(\boldsymbol{\alpha}, X_n)$ e supponiamo che $z_1 = \xi(\boldsymbol{\alpha}) = \zeta(\boldsymbol{\alpha})$. Sia m_i (rispettivamente n_i) la molteplicità di z_i come radice di $p(\boldsymbol{\alpha}, X_n)$ (rispettivamente $q(\boldsymbol{\alpha}, X_n)$), in cui si conviene $m_i = 0$ (rispettivamente $n_i = 0$) se z_i non è una radice di $p(\boldsymbol{\alpha}, X_n)$ (rispettivamente $q(\boldsymbol{\alpha}, X_n)$).

Il massimo comun divisore tra $p(\boldsymbol{\alpha}, X_n)$ e $q(\boldsymbol{\alpha}, X_n)$ ha z_i come radice di molteplicità $\min\{m_i, n_i\}$ ed ha grado $\sum_{i=1}^{k} \min\{m_i, n_i\}$. Osserviamo che questo grado è (strettamente) positivo in quanto sicuramente z_1 è una radice del massimo comun divisore. Sia $\varepsilon > 0$ tale che i dischi $B(z_i, \varepsilon)$ siano disgiunti. Per continuità delle radici, fissato $\mathbf{x}$ sufficientemente vicino ad $\boldsymbol{\alpha}$, ogni disco $B(z_i, \varepsilon)$ contiene una sola radice di molteplicità m_i di $p(\mathbf{x}, X_n)$, che è $\xi(\mathbf{x})$, e una sola radice di molteplicità n_i di $q(\mathbf{x}, X_n)$, che è $\zeta(\mathbf{x})$. Visto che il grado di $\mathrm{MCD}(p(\boldsymbol{\alpha}, X_n), q(\boldsymbol{\alpha}, X_n))$ è $\sum \min\{m_i, n_i\}$, questo massimo comun divisore deve avere una radice di molteplicità $\min\{m_i, n_i\}$ in ogni disco $B(z_i, \varepsilon)$ tale che $\min\{m_i, n_i\} > 0$. Tale radice è una radice comune a $p(\mathbf{x}, X_n)$ e $q(\mathbf{x}, X_n)$ e sappiamo chi sono le loro radici in $B(z_i, \varepsilon)$: ne segue necessariamente che $\xi(\mathbf{x}) = \zeta(\mathbf{x})$. Per connessione di C si ha che $\xi(\mathbf{x}) = \zeta(\mathbf{x})$ per ogni $\mathbf{x} \in C$. □

A questo punto costruiamo effettivamente una CAD: ci serviranno i coefficienti sottorisultanti principali introdotti nella sezione 4.4. Se $p \in \mathbb{R}[X_1, \ldots, X_n]$, lo vediamo come polinomio in $\mathbb{R}[X_1, \ldots, X_{n-1}][X_n]$ e di conseguenza chiameremo $\mathrm{lc}(p) \in \mathbb{R}[X_1, \ldots, X_{n-1}]$ il suo *leading coefficient*, $\mathrm{lt}(p)$ il suo *leading term*

e $\text{tail}(p) := p - \text{lt}(p)$. Analogamente $\deg(p)$ indicherà il grado di p rispetto all'indeterminata X_n.

Definizione 4.44. Siano $p_1, \ldots, p_r \in \mathbb{R}[X_1, \ldots, X_n]$ polinomi. Definiamo *proiezione* di $p_1, \ldots, p_r$, indicata con $\text{Proj}(p_1, \ldots, p_r)$, la più piccola famiglia di polinomi in $\mathbb{R}[X_1, \ldots, X_{n-1}]$ tale che

- se p_i è tale che $\deg(p_i) = d \geqslant 2$, $\text{Proj}(p_1, \ldots, p_r)$ contiene tutti i polinomi non costanti tra i $\text{PSRC}_j\left(p_i, \dfrac{\partial p_i}{\partial X_n}\right)$ per $j = 0, \ldots, d-1$;
- se p_i e p_k sono tali che $\min\{\deg(p_i), \deg(p_k)\} = d \geqslant 1$, $\text{Proj}(p_1, \ldots, p_r)$ contiene tutti i polinomi non costanti tra i $\text{PSRC}_j(p_i, p_k)$ per $j = 0, \ldots, d$;
- se p_i è tale che $\deg(p_i) \geqslant 1$ e $\text{lc}(p_i)$ non è costante, $\text{Proj}(p_1, \ldots, p_r)$ contiene $\text{lc}(p_i)$ e $\text{Proj}(p_1, \ldots, \text{tail}(p_i), \ldots, p_r)$;
- se p_i è tale che $\deg(p_i) = 0$ e p_i non è costante, $\text{Proj}(p_1, \ldots, p_r)$ contiene p_i.

Ricomponendo quanto visto finora, la conclusione è il seguente teorema.

Teorema 4.45. *Sia $(p_1, \ldots, p_r)$ una famiglia di polinomi in $\mathbb{R}[X_1, \ldots, X_n]$ e sia $C \subseteq \mathbb{R}^{n-1}$ connesso, semialgebrico e $\text{Proj}(p_1, \ldots, p_r)$-invariante. Allora esistono funzioni continue semialgebriche $\xi_1 < \cdots < \xi_\ell : C \to \mathbb{R}$ tali che per ogni $\mathbf{x} \in C$ l'insieme $\{\xi_1(\mathbf{x}), \ldots, \xi_\ell(\mathbf{x})\}$ è l'insieme delle radici reali di tutti i polinomi non nulli $p_1(\mathbf{x}, X_n), \ldots, p_r(\mathbf{x}, X_n)$. I grafici di ogni ξ_i e le bande del cilindro $C \times \mathbb{R}$ delimitate da tali grafici sono insiemi semialgebrici connessi, semialgebricamente omeomorfi rispettivamente a C e $C \times (0,1)$, e $(p_1, \ldots, p_r)$-invarianti.*

Se abbiamo una CAD di $\mathbb{R}^{n-1}$ adattata a $\text{Proj}(p_1, \ldots, p_r)$, il teorema 4.45 può essere usato per estenderla a una CAD di $\mathbb{R}^n$ adattata a $(p_1, \ldots, p_r)$. D'altra parte, iterando l'applicazione di Proj $n-1$ volte, arriviamo a una famiglia finita di polinomi nella variabile X_1, per i quali è facile costruire una CAD adattata di $\mathbb{R}$: i loro zeri reali tagliano la retta reale in un numero finito di punti e intervalli aperti.

Corollario 4.46. *Per ogni famiglia di polinomi $p_1, \ldots, p_r \in \mathbb{R}[X_1, \ldots, X_n]$ esiste una CAD di $\mathbb{R}^n$ adattata a $(p_1, \ldots, p_r)$.*

Bibliografia

[1] Massimo Caboara, Fabrizio Caruso, e Carlo Traverso. Lattice Polly Cracker Cryptosystems. *J. Symb. Comput.*, 46:534–549, 2011.

[2] Michel Coste. An Introduction to Semialgebraic Geometry. Dip. Mat. Univ. Pisa, Dottorato di Ricerca in Matematica, 2000.

[3] Elisabetta Fortuna, Patrizia Gianni, e Paola Parenti. Some Constructions for Real Algebraic Curves. *J. Symb. Comput.*, 40:1169–1179, 2005.

[4] Elisabetta Fortuna, Patrizia Gianni, Paola Parenti, e Carlo Traverso. Algorithms to Compute the Topology of Orientable Real Algebraic Surfaces. *J. Symb. Comput.*, 36:343–364, 2003.

[5] Patrizia Gianni e Carlo Traverso. La forma delle curve algebriche reali piane. Realizzazione di un algoritmo. In *Curve Algebriche — Atti del convegno di Geometria Algebrica tenuto a Firenze nell'ottobre '81*. CNR, Istituto di Analisi Globale e applicazioni, 1981.

[6] Patrizia Gianni e Carlo Traverso. On an Algorithm for the Shape of Real Curves. Dip. Mat. Univ. Pisa, vol. 31, 1983.

[7] Oded Goldreich, Shafi Goldwasser, e Shai Halevi. Public-Key Cryptosystems from Lattice Reduction Problems. In *Advances in Cryptology — Proc. of CRYPTO '97*, volume 1294 di *Lecture Notes in Computer Science*, pp. 112–131. Springer-Verlag, 1997.

[8] Jeffrey Hoffstein, Jill Pipher, e Joseph H. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. In *Algorithmic Number Theory — Proc. of ANTS-III*, volume 1423 di *Lecture Notes in Computer Science*, pp. 267–288. Springer-Verlag, 1998.

[9] Dale Husemöller. *Elliptic Curves*. Springer-Verlag, seconda edizione, 2004.

[10] Kenji Koyama, Ueli M. Maurer, Tatsuaki Okamoto, e Scott A. Vanstone. New Public-Key Schemes Based on Elliptic Curves over the Ring $\mathbb{Z}_n$. In *Advances in Cryptology — Proc. of CRYPTO '91*, volume 576 di *Lecture Notes in Computer Science*, pp. 252–266. Springer-Verlag, 1992.

[11] Arjen K. Lenstra, Hendrik W. Lenstra jr., e László Lovász. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[12] Daniele Micciancio e Shafi Goldwasser. *Complexity of Lattice Problems: a Cryptographic Perspective*. Kluwer Academic Publishers, 2002.

[13] Phong Nguyen. Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97. In *Advances in Cryptology — Proc. of CRYPTO '99*, volume 1666 di *Lecture Notes in Computer Science*, pp. 288–304. Springer-Verlag, 1999.

[14] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, seconda edizione, 2009.

[15] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC, seconda edizione, 2008.