View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by AMS Tesi di Laurea

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

SCUOLA DI SCIENZE

Corso di Laurea Magistrale in Matematica

Il gruppo dei punti razionali di una curva ellittica

Tesi di Laurea in Teoria dei Numeri

Relatore:

Chiar.mo Prof.

MONICA IDÀ

Presentata da:

IRENE UDASSI

III Sessione

Anno Accademico 2014/2015

Indice

Introduzione **I**

1 Premesse **1**

1.1 Curve algebriche proiettive 1

1.2 Cubiche liscie piane e parametrizzabilità 8

1.3 Forma normale di Weierstrass 13

2 La legge di gruppo su una cubica liscia **19**

2.1 Costruzione geometrica della somma di due punti 19

2.2 La legge di gruppo su $\mathscr{C}$ in forma normale 26

2.2.1 Proprietà 26

2.2.2 Formule di addizione su $\mathscr{C}$ 27

2.3 Punti di ordine finito m: i casi $m = 2$ e $m = 3$ 30

2.3.1 Proprietà geometriche dei punti di ordine 3 36

3 Il gruppo dei punti razionali **39**

3.1 Cubiche razionali in forma normale 40

3.2 Il discriminante di $x^3 + ax^2 + bx + c$ 43

3.3 Le coordinate dei punti di $\mathscr{C}(\mathbb{Q})$ 45

3.4 Punti di ordine finito 47

3.4.1 I sottogruppi $\mathscr{C}(p^\nu)$ 47

3.4.2 I teoremi di Nagell-Lutz e di Mazur 56

3.4.3 Esempi di calcolo del sottogruppo dei punti di ordine finito: $\mathbb{Z}_6$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\{0\}$, $\mathbb{Z}_8$ 59

3.5 Una cubica $\mathscr{C}$ con $|\mathscr{C}(\mathbb{Q})| < \infty$ 63

4 Il teorema di Mordell **69**

4.1 Altezza di un punto e proprietà 70

4.2 La mappa di duplicazione 79

4.3 L'indice di $2\mathscr{C}(\mathbb{Q})$ in $\mathscr{C}(\mathbb{Q})$ 90

4.4 Il teorema di Mordell 97

4.5 Il rango di $\mathscr{C}(\mathbb{Q})$ 99

4.5.1 Esempi di calcolo del rango 104

Appendice A **108**

Bibliografia **113**

Introduzione

Nel presente lavoro, ci occupiamo dello studio dell'insieme dei punti di una curva ellittica (cioè una cubica liscia di $\mathbb{P}^2$) $\mathscr{C}$, visto come gruppo abeliano, concentrandoci in particolare sul caso dei punti a coordinate in $\mathbb{Q}$ quando $\mathscr{C}$ è data da un'equazione razionale. Si osservi che nel seguito, scrivendo "$\mathscr{C}$ curva razionale" non intenderemo che il genere della curva è zero, ma che è possibile dare un'equazione per $\mathscr{C}$ a coefficienti razionali.

La ricerca e lo studio dei punti razionali di una cubica razionale è un problema che ha origine nella matematica del periodo tardo-antico: una cubica infatti è descritta da un'equazione di grado 3, e fu Diofanto che per primo si occupò delle soluzioni razionali di equazioni di terzo grado a coefficienti interi. Egli trovò che da una soluzione se ne può ottenere una seconda: anche se non fu sviluppato in questi termini, il suo metodo sfruttava il fatto che la tangente alla cubica in un punto razionale deve incontrare la curva in un terzo punto, e anch'esso deve essere razionale.
Fermat vide che, talvolta, con questo metodo si ottengono infinite soluzioni razionali; potremmo dire allora che il lavoro che segue risponde alla domanda: "perché succede questo?"

Nei primi due capitoli, dopo aver richiamato alcuni elementi della teoria sulle curve algebriche, ci concentreremo sulle cubiche lisce do $\mathbb{P}^2$, ovvero curve piane di grado 3 senza punti singolari. Vedremo che, da una parte, possiamo sempre trovare un'equazione affine per $\mathscr{C}$ che sia in forma normale, ovvero del tipo

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx + c \,, \quad a, b, c \in \mathbb{C} \,,$$

e dall'altra che, fissato un punto $O \in \mathscr{C}$, si può sempre dotare l'insieme dei punti di $\mathscr{C}$ della struttura di gruppo abeliano in modo che O sia l'elemento neutro.
Questa forma, oltre ad avere interessanti proprietà (ad esempio, $\mathscr{C}$ è liscia $\Leftrightarrow$ $f(x) = x^3 + ax^2 + bx + c$ ha tre radici distinte), è assai maneggevole; studieremo quindi il gruppo $(\mathscr{C}, +, O)$ con $\mathscr{C}$ in forma normale e $O = [0, 0, 1]$ (cioè O è l'unico punto all'infinito di $\mathscr{C}$, ed è un flesso).
Così sarà possibile ottenere per via analitica delle formule per la somma di due punti, che torneranno utili in più occasioni; prima fra queste, lo studio dei punti di ordine 2 e 3, affrontato alla fine del secondo capitolo. Qui ricaveremo alcune proprietà dei flessi di una cubica liscia e inizieremo a guardare meglio la struttura dei sottogruppi costituiti da questi punti, e cosa succede quando si considera la cubica su $\mathbb{R}$ o su $\mathbb{Q}$.

Nei capitoli seguenti ci concentriamo sui punti razionali della cubica, seguendo essenzialmente la trattazione di J.H. Silverman e J. Tate ([ST]): anzitutto mostreremo che se $\mathscr{C}$ è data da un'equazione a coefficienti in $\mathbb{Q}$, fissato un punto $O \in \mathscr{C}$ razionale, l'insieme $\mathscr{C}(\mathbb{Q})$ dei punti di $\mathscr{C}$ a coordinate in $\mathbb{Q}$ è un sottogruppo di $(\mathscr{C}, +, O)$.
Non è sempre detto però che una cubica razionale abbia punti razionali (ad esempio, la cubica liscia $3x_0^3 + 4x_1^3 + 5x_2^3 = 0$ individuata da Ernst Selmer non ne possiede), e non si conosce un metodo che permetta di stabilirlo sempre.
Dovremo quindi supporre che $\mathscr{C}$ abbia almeno un punto razionale; così riusciremo a ricavare un'equazione della forma

$$y^2 = x^3 + ax^2 + bx + c\ , \quad a, b, c \in \mathbb{Z}\ , \tag{$*$}$$

che ci permetterà di lavorare su $(\mathscr{C}, +, O)$ sfruttando da un lato le proprietà viste nei primi due capitoli, e dall'altro il fatto che i punti di $\mathscr{C}(\mathbb{Q})$ si possono scrivere come

$$(x, y) = \left(\frac{m}{d^2}, \frac{n}{d^3}\right)\ , \quad m, n, d \in \mathbb{Z}\ ,\ d > 0\ ,\ (m, d) = (n, d) = 1\ .$$

Questo, come vedremo, ci consentirà di ragionare sui punti di $\mathscr{C}(\mathbb{Q})$ usando gli strumenti datici dalla teoria dei numeri.
Trygve Nagell ed Elisabeth Lutz, nel 1935 e nel 1937 rispettivamente, pubblicaro-

no un risultato ancora più notevole: se $\mathscr{C}$ ha un'equazione della forma $(*)$, i punti di $\mathscr{C}(\mathbb{Q})$ di ordine finito hanno coordinate intere, e per di più la loro ordinata affine y è zero oppure divide il discriminante D del polinomio $f(x) = x^3+ax^2+bx+c$. Questo teorema non solo ci dice che i punti razionali di ordine finito costituiscono quindi un gruppo Λ finito (dato che sono possibili solo finiti valori di y), ma dà anche un algoritmo, facilmente implementabile su calcolatore per valori di D non troppo grandi, che stili una lista (finita) dei possibili punti di ordine finito di $\mathscr{C}(\mathbb{Q})$.
La dimostrazione del teorema di Nagell-Lutz non richiede strumenti sofisticati, ma per lo più fatti ben noti sui morfismi fra gruppi, sulla divisibilità in $\mathbb{Z}$ e sui polinomi di $\mathbb{Z}[x]$: partendo da questi, studieremo le proprietà del discriminante di $f(x)$ e degli insiemi

$$\mathscr{C}(p^\nu) = \left\{ (x,y) \in \mathscr{C}(\mathbb{Q}) \;\middle|\; \begin{array}{l} x = \dfrac{m}{n}p^{-2\nu}\ ,\ y = \dfrac{u}{w}p^{-3\nu}\ ,\ (m,n) = (u,w) = 1\ , \\ (m,p) = (n,p) = (u,p) = (w,p) = 1 \end{array} \right\}$$

definiti per ogni p primo, $\nu \in \mathbb{Z}$ fissati, $\nu > 0$. Vedremo che questi sono tutti sottogruppi di $\mathscr{C}(\mathbb{Q})$, e non contengono mai punti di $\mathscr{C}(\mathbb{Q})$ di ordine finito.
Purtroppo non è altrettanto facile mostrare che sono solo 15 le forme possibili per il sottogruppo Λ: di questo splendido risultato di classificazione, provato da Barry Mazur negli anni '70, daremo solo l'enunciato, e vedremo nel dettaglio alcuni esempi di sottogruppi Λ.

Il quarto capitolo è dedicato alla dimostrazione di un fatto fondamentale sulla struttura di $\mathscr{C}(\mathbb{Q})$, e cioè che $\mathscr{C}(\mathbb{Q})$ è finitamente generato, per cui esistono univocamente determinati r, t, p_i, $\nu_i \in \mathbb{Z}$, r, $t \geq 0$, p_i primi, $\nu_i > 0$ per $i = 1, ..., t$, tali che

$$\mathscr{C}(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ volte}} \oplus \mathbb{Z}_{p_1^{\nu_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\nu_t}}\ .$$

La prova di questo teorema, pubblicata da Louis Mordell nel 1922 e generalizzato al caso delle varietà abeliane da André Weil, fa uso del metodo della discesa infinita di Fermat, e del fatto che $\mathscr{C}(\mathbb{Q}) \Big/ 2\mathscr{C}(\mathbb{Q})$ è finito.
Per utilizzare il metodo della discesa, introdurremo una funzione definita sui punti di $\mathscr{C}(\mathbb{Q})$ e a valori in $\mathbb{R}^+$, che chiamiamo altezza, e ne studieremo le proprietà; in particolare vedremo che l'insieme dei punti di $\mathscr{C}(\mathbb{Q})$ con altezza minore di un

valore fissato è sempre finito, e daremo una stima della somma di due punti.
Per mostrare che $[\mathscr{C}(\mathbb{Q}) : 2\mathscr{C}(\mathbb{Q})] < \infty$, lavoreremo sull'applicazione $P \mapsto 2P$, vista come composizione di due morfismi:

$$\begin{array}{ccccc} & & \widehat{\mathscr{C}}\,(\mathbb{Q}) & & \\ & \overset{\Phi}{\nearrow} & & \overset{\Psi}{\searrow} & \\ \mathscr{C}(\mathbb{Q}) & & \xrightarrow{\Psi \circ \Phi} & & \mathscr{C}(\mathbb{Q}) \\ P & & \longmapsto & & 2P \end{array}$$

dove $\widehat{\mathscr{C}}$ è una curva ellittica definita a partire da $\mathscr{C}$, e ad essa profondamente legata.
Infine, la dimostrazione del teorema di Mordell ci permetterà di ricavare una formula per il rango r di $\mathscr{C}(\mathbb{Q})$, infatti vedremo che

$$2^r = \frac{[\mathscr{C}(\mathbb{Q}) : \Psi(\widehat{\mathscr{C}}\,(\mathbb{Q}))] \cdot [\widehat{\mathscr{C}}\,(\mathbb{Q}) : \Phi(\mathscr{C}(\mathbb{Q}))]}{4}\,.$$

Purtroppo però, per il momento si è in grado di calcolare i due indici al numeratore solo in casi particolari, ed anche in questi casi non è detto che si riesca a trovare esplicitamente un insieme di generatori per $\mathscr{C}(\mathbb{Q})$.
In effetti, la questione del rango è un problema ancora aperto e assai rilevante: la congettura di Birch e Swinnerton-Dyer, uno dei *millennium prize problem*, mette in relazione il rango r di $\mathscr{C}$ con le soluzioni modulo p dell'equazione di $\mathscr{C}$, dove p è un primo che divide il doppio del discriminante dell'equazione; nella sua forma più forte, darebbe anche un metodo per determinare un insieme di generatori per $\mathscr{C}(\mathbb{Q})$, che risulterebbe così completamente descritto.

Capitolo 1

Premesse

1.1 Curve algebriche proiettive

In questa sezione introduciamo rapidamente le definizioni, le notazioni e i risultati necessari per poter affrontare il nostro discorso sulle cubiche del piano proiettivo complesso. Per ulteriori approfondimenti, si rimanda in generale a [Se, § 24-28].

Definizione 1.1.1. Com'è consueto, indicheremo con $\mathbb{P}^2(\mathbb{C})$ l'insieme delle rette vettoriali di $\mathbb{C}^3$; sappiamo che $\mathbb{P}^2(\mathbb{C})$ può essere identificato con lo spazio $\mathbb{C}^3 \setminus \{\mathbf{0}\}/_\sim$, dove $\sim$ è la relazione di proporzionalità su $\mathbb{C}^3 \setminus \{\mathbf{0}\}$:

$$(a,b,c) \sim (a',b',c') \quad \Leftrightarrow \quad \exists \lambda \in \mathbb{C}, \lambda \neq 0 \text{ tale che } (a',b',c') = \lambda(a,b,c)\ .$$

Fissata una base $\mathcal{B} = \{v_0, v_1, v_2\}$ di $\mathbb{C}^3$, quindi un riferimento proiettivo $\mathcal{P} = \{\lambda v_0, \lambda v_1, \lambda v_2\}_{\lambda \in \mathbb{C}^*}$ di $\mathbb{P}^2(\mathbb{C})$, un punto $P \in \mathbb{P}^2(\mathbb{C})$ è identificato da una terna di scalari non tutti nulli $[x_0, x_1, x_2]$ determinata a meno di proporzionalità; x_0, x_1, x_2 si dicono *coordinate omogenee* di P rispetto a $\mathcal{P}$.

Osservazione 1.1.a. Ricordiamo che è possibile definire una corrispondenza biunivoca fra le rette vettoriali di $\mathbb{C}^3$ che non giacciono sul piano $H_0 : x_0 = 0$ e i punti del piano affine $x_0 = 1$, che identifichiamo con $\mathbb{A}^2(\mathbb{C})$ tramite l'applicazione $(1, x_1, x_2) \mapsto (x_1, x_2)$. Infatti se s è una retta per l'origine non contenuta in H_0, allora s interseca il piano $x_0 = 1$ in un unico punto $(1, x_1, x_2)$; viceversa $(1, x_1, x_2)$ appartiene alla retta vettoriale costituita dai punti della forma $(\lambda, \lambda x_1, \lambda x_2)$, che in $\mathbb{P}^2(\mathbb{C})$ è il punto di coordinate omogenee $[1, x_1, x_2]$.

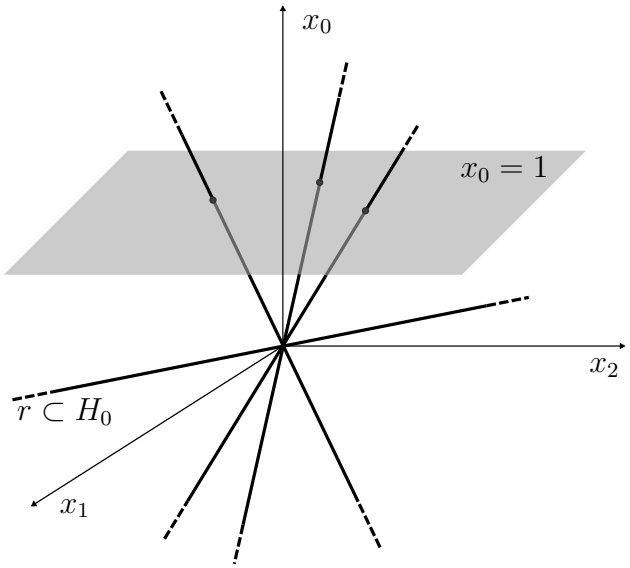
In definitiva, è possibile definire un'applicazione biunivoca

$$\begin{aligned} j_0 : \mathbb{A}^2(\mathbb{C}) &\longrightarrow \mathbb{P}^2(\mathbb{C}) \smallsetminus H_0 \\ (x_1, x_2) &\longmapsto [1, x_1, x_2] \end{aligned}$$

detta *applicazione di passaggio a coordinate omogenee* rispetto a x_0, la cui inversa è

$$\begin{aligned} j_0^{-1} : \mathbb{P}^2(\mathbb{C}) \smallsetminus H_0 &\longrightarrow \mathbb{A}^2(\mathbb{C}) \\ [x_0, x_1, x_2] &\longmapsto \left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right) \\ \| & \\ \left[1, \tfrac{x_1}{x_0}, \tfrac{x_2}{x_0}\right] & \end{aligned}$$

(*passaggio a coordinate non omogenee* rispetto ad x_0). Le rette su H_0 invece si possono associare alle direzioni del piano affine $x_0 = 0$, cioè ai punti della retta impropria di quel piano, che identifichiamo con $\mathbb{P}^1(\mathbb{C})$.



Ovviamente, il ragionamento appena fatto si può ripetere considerando x_1 o x_2 al posto di x_0.

Nella nostra trattazione, sarà spesso utile vedere $\mathbb{P}^2(\mathbb{C})$ come $\mathbb{A}^2(\mathbb{C}) \cup \mathbb{P}^1(\mathbb{C})$.

Definizione 1.1.2. Sia $F(x_0, x_1, x_2) \in \mathbb{C}[x_0, x_1, x_2]$ un polinomio omogeneo di grado $d > 0$; si dice *curva algebrica* di $\mathbb{P}^2(\mathbb{C})$ di grado d la classe di proporzionalità di F.

Se $\mathscr{C}$ è una curva algebrica e F è un suo rappresentante, scriveremo

$$\mathscr{C} : F(x_0, x_1, x_2) = 0$$

e diremo che $F(x_0, x_1, x_2) = 0$ è un'equazione per $\mathscr{C}$.
Poiché

$$\mu F(\lambda x_0, \lambda x_1, \lambda x_2) = \lambda^d \mu F(x_0, x_1, x_2)$$

è ben definito l'insieme

$$\breve{\mathscr{C}} = \{[x_0, x_1, x_2] \in \mathbb{P}^2(\mathbb{C}) \mid F(x_0, x_1, x_2) = 0\}$$

detto *supporto* di $\mathscr{C}$.
Con un abuso di notazione, diremo che P appartiene a $\mathscr{C}$, e scriveremo $P \in \mathscr{C}$, se P è un punto del supporto di $\mathscr{C}$.

Definizione 1.1.3. Sia $\mathscr{C}$ una curva algebrica di $\mathbb{P}^2(\mathbb{C})$ di grado d,

$$\mathscr{C} : F(x_0, x_1, x_2) = 0$$

e definiamo

$$f(x, y) = F(1, x, y) \ ;$$

allora f è un polinomio non omogeneo in $\mathbb{C}[x, y]$, detto *deomogeneizzato di* F rispetto ad x_0. Se $F \neq ax_0^d$, la sua classe di proporzionalità definisce una curva $\mathscr{C}^*$ di $\mathbb{A}^2(\mathbb{C})$ di equazione $f(x, y) = 0$; $\mathscr{C}^*$ si dice *carta affine* di $\mathscr{C}$ rispetto a x_0. Osserviamo che $P = (x, y) \in \mathscr{C}^* \Leftrightarrow P' = [1, x, y] \in \mathscr{C}$; così i punti di $\mathscr{C}$ di coordinate $[x_0, x_1, x_2]$ con $x_0 \neq 0$ si dicono *punti propri* di $\mathscr{C}$ rispetto a x_0; i punti con $x_0 = 0$ si dicono *punti impropri* di $\mathscr{C}$ rispetto a x_0.
È facile verificare che $\mathscr{C}^*$ ha lo stesso grado d di $\mathscr{C}$ se e solo se $x_0 \nmid F$ in $\mathbb{C}[x_0, x_1, x_2]$; in tal caso

$$x_0^d \cdot f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right) = F(x_0, x_1, x_2)$$

e si dice che F è l'*omogeneizzato di* f rispetto a x_0, $\mathscr{C}$ è la *chiusura proiettiva* di $\mathscr{C}^*$ rispetto a x_0.

Notazione 1. Poiché considereremo carte affini di cubiche lisce di $\mathbb{P}^2(\mathbb{C})$, varrà

sempre, come vedremo, $x_0 \nmid F$; pertanto useremo lo stesso simbolo per $\mathscr{C}$ e $\mathscr{C}^*$, e diremo che $F(x_0, x_1, x_2) = 0$ è un'*equazione omogenea* per $\mathscr{C}$, $f(x, y) = 0$ è un'*equazione non omogenea* (o *affine*) per $\mathscr{C}$ nelle coordinate $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$.

Definizione 1.1.4. Sia $\mathscr{C}$ una curva algebrica di $\mathbb{P}^2(\mathbb{C})$, $\mathscr{C} : F(x_0, x_1, x_2) = 0$ con F polinomio omogeneo di grado d, e sia

$$F(x_0, x_1, x_2) = F_1(x_0, x_1, x_2)^{d_1} \cdot ... \cdot F_k(x_0, x_1, x_2)^{d_k} \ , \qquad (\star)$$

con $F_i \neq F_j$ se $i \neq j$, la sua decomposizione in fattori irriducibili. Se $k = 1$, diremo che la curva è *irriducibile*; se $d_1 = ... = d_k = 1$, diremo che la curva è *ridotta*. Quindi chiedere $\mathscr{C}$ ridotta e irriducibile equivale a chiedere F polinomio irriducibile.

Per il teorema degli zeri di Hilbert [H, cap.I sez.1], una curva ridotta e irriducibile $\mathscr{C}$ di $\mathbb{P}^2(\mathbb{C})$ si può identificare con il suo supporto $\breve{\mathscr{C}}$.
Se $\mathscr{C}$ è come sopra la curva $F(x_0, x_1, x_2)$, e vale $(\star)$, poste

$$\begin{aligned} \mathscr{C}_1 &: F_1(x_0, x_1, x_2) = 0 \ , \\ &\vdots \\ \mathscr{C}_k &: F_k(x_0, x_1, x_2) = 0 \ , \end{aligned}$$

le $\mathscr{C}_i$ si dicono *componenti irriducibili* di $\mathscr{C}$, e fra i supporti delle curve sussiste la relazione

$$\breve{\mathscr{C}} = \breve{\mathscr{C}}_1 \cup ... \cup \breve{\mathscr{C}}_k \ .$$

Definizione 1.1.5. Sia $\mathscr{C}$ una curva algebrica di $\mathbb{P}^2(\mathbb{C})$, $\mathscr{C} : F(x_0, x_1, x_2) = 0$ con F polinomio omogeneo di grado d, e sia $\phi \in PGL_2(\mathbb{C})$ la proiettività rappresentata dalla matrice

$$\phi = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix} \ .$$

Posto $G(x_0, x_1, x_2) = F(\phi(x_0, x_1, x_2))$, G è certo un polinomio omogeneo di grado d, quindi è ben definita la curva $\mathscr{D} : G(x_0, x_1, x_2) = 0$.

Poiché ϕ è invertibile, valgono

$$[y_0, y_1, y_2] \in \mathscr{C} \iff \phi^{-1}[y_0, y_1, y_2] \in \mathscr{D} \ ,$$
$$[x_0, x_1, x_2] \in \mathscr{D} \iff \phi(x_0, x_1, x_2) \in \mathscr{C} \ ,$$

quindi per i supporti si ha

$$\phi^{-1}(\breve{\mathscr{C}}) = \breve{\mathscr{D}} \quad , \quad \phi(\breve{\mathscr{D}}) = \breve{\mathscr{C}} \ .$$

Diremo allora che $\mathscr{D}$ è la *trasformata di* $\mathscr{C}$ *tramite* ϕ^{-1}, $\mathscr{C}$ è la trasformata di $\mathscr{D}$ tramite ϕ, e scriveremo $\phi^{-1}(\mathscr{C}) = \mathscr{D}$, $\phi(\mathscr{D}) = \mathscr{C}$.

Definizione 1.1.6. Se $\mathscr{C}$ e $\mathscr{D}$ sono due curve algebriche di $\mathbb{P}^2(\mathbb{C})$, si dice che $\mathscr{C}$ e $\mathscr{D}$ sono *proiettivamente equivalenti* se esiste $\phi \in PGL_2(\mathbb{C})$ tale che $\phi(\mathscr{D}) = \mathscr{C}$ (equivalentemente $\phi^{-1}(\mathscr{C}) = \mathscr{D}$). La definizione è ben posta giacché non dipende dai rappresentanti scelti per $\mathscr{C}$, $\mathscr{D}$, ϕ, e dà una relazione di equivalenza sull'insieme delle curve di $\mathbb{P}^2(\mathbb{C})$.

Osservazione 1.1.b. Si può dimostrare [Se, pp.455-457] che una curva $\mathscr{C} \in \mathbb{P}^2(\mathbb{C})$ è irriducibile $\iff$ ogni curva proiettivamente equivalente a $\mathscr{C}$ è irriducibile; per questo si dice che l'irriducibilità è una *proprietà proiettiva* della curva.
Inoltre, si verifica che grado, numero e molteplicità delle componenti irriducibili di una curva sono proprietà proiettive.

Ricorreremo più volte a curve proiettivamente equivalenti ad una cubica $\mathscr{C}$ data; poiché il nostro lavoro si concentrerà anche sull'insieme numerico a cui appartengono le coordinate dei punti di $\mathscr{C}$, è utile notare che se $\phi \in PGL_2(\mathbb{C})$, allora sono equivalenti

(i) $\phi(\mathbb{P}^2(\mathbb{R})) = \mathbb{P}^2(\mathbb{R})$ (rispettivamente $\phi(\mathbb{P}^2(\mathbb{Q})) = \mathbb{P}^2(\mathbb{Q})$)

(ii) esiste una matrice $A \in GL_3(\mathbb{R})$ (rispettivamente $A \in GL_3(\mathbb{Q})$) che rappresenta ϕ.

(Si osservi che se $A \in GL_3(\mathbb{Q})$ rappresenta ϕ, anche $\sqrt{2}A$ o iA rappresentano ϕ come proiettività di $\mathbb{P}^2(\mathbb{C})$).

Definizione 1.1.7. Siano $\mathscr{C} \subseteq \mathbb{P}^2(\mathbb{C})$ una curva, $\mathscr{C} : F(x_0, x_1, x_2) = 0$, $P \in \mathbb{P}^2(\mathbb{C})$ un punto; se

$$r : \begin{cases} x_0 = \alpha_0\lambda + \beta_0\mu \\ x_1 = \alpha_1\lambda + \beta_1\mu \\ x_2 = \alpha_2\lambda + \beta_2\mu \end{cases} \quad , \quad rank \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_0 & \beta_1 & \beta_2 \end{pmatrix} = 2 \quad , \quad [\lambda, \mu] \in \mathbb{P}^1$$

è una retta passante per P, $P = (\alpha_0\bar{\lambda} + \beta_0\bar{\mu}\,,\, \alpha_1\bar{\lambda} + \beta_1\bar{\mu}\,,\, \alpha_2\bar{\lambda} + \beta_2\bar{\mu})$, si definisce la *molteplicità di intersezione* di r e $\mathscr{C}$ in P nel modo seguente:

$$i(\mathscr{C}, r, P) = \begin{cases} 0 & \text{se } P \notin \mathscr{C} \\ \infty & \text{se } r \subseteq \mathscr{C} \\ m & \begin{array}{l} \text{se } [\bar{\lambda}, \bar{\mu}] \text{ è radice di molteplicità } m \text{ di} \\ F(\alpha_0\lambda + \beta_0\mu\,,\, \alpha_1\lambda + \beta_1\mu\,,\, \alpha_2\lambda + \beta_2\mu)\,. \end{array} \end{cases}$$

Questa definizione non dipende dalla parametrizzazione scelta per r.

Useremo spesso il seguente risultato, che è un caso particolare del teorema di Bézout [BCGB, teorema 4.2.1]:

Teorema 1.1.8. *Sia $\mathscr{C} \in \mathbb{P}^2(\mathbb{C})$ una curva di grado d, e sia r una retta, $r \nsubseteq \mathscr{C}$ come supporto. Allora*

$$\sum_{P \in r} i(\mathscr{C}, r, P) = d. \tag{1.1}$$

Dimostrazione. Nella sommatoria al primo membro di (1.1), solo un numero finito di termini sono non nulli, perché $r \nsubseteq \mathscr{C}$, e questi corrispondono ai punti di $\mathscr{C} \cap r$. Se scriviamo

$$r : \begin{cases} x_0 = \alpha_0\lambda + \beta_0\mu \\ x_1 = \alpha_1\lambda + \beta_1\mu \\ x_2 = \alpha_2\lambda + \beta_2\mu \end{cases} \quad \text{e} \quad \mathscr{C} : F(x_0, x_1, x_2) = 0$$

con $rank \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_0 & \beta_1 & \beta_2 \end{pmatrix} = 2$ e $[\lambda, \mu] \in \mathbb{P}^1$, la risolvente di $\mathscr{C} \cap r$ è un'equazione omogenea di grado d nelle indeterminate λ, μ, e poiché $\mathbb{C}$ è algebricamente chiuso, questo ha, a meno di proporzionalità, d radici contate con molteplicità, che sono d punti su $\mathscr{C} \cap r$ contati con le loro molteplicità di intersezione. □

Definizione 1.1.9. Sia $\mathscr{C}$ una curva di $\mathbb{P}^2(\mathbb{C})$, e sia $P \in \mathbb{P}^2(\mathbb{C})$ un punto. Si definisce la *molteplicità di $\mathscr{C}$ in P*:

$$\mu_P(\mathscr{C}) = \min_{r \ni P} i(\mathscr{C}, r, P) \ .$$

Vale $\mu_P(\mathscr{C}) = 0 \Leftrightarrow P \notin \mathscr{C}$; se $\mu_P(\mathscr{C}) = 1$, P si dice *punto semplice* per $\mathscr{C}$; se $\mu_P(\mathscr{C}) > 1$, P si dice *punto singolare* (o *multiplo*) di molteplicità $\mu_P(\mathscr{C})$ per $\mathscr{C}$. Se una curva $\mathscr{C}$ non ha punti singolari, diremo che $\mathscr{C}$ è *liscia* (o *non singolare*).

C'è moltissimo da dire sui punti singolari di una curva, ma poiché lavoreremo solo con cubiche lisce, ci limitiamo ad enunciare questo risultato fondamentale:

Teorema 1.1.10. *Sia $\mathscr{C}$ una curva di $\mathbb{P}^2(\mathbb{C})$, $\mathscr{C} : F(x_0, x_1, x_2) = 0$.*

(*a*) *Un punto $P \in \mathbb{P}^2(\mathbb{C})$ è un punto di molteplicità $m \geq 1$ per $\mathscr{C}$ se e solo se*

- $\left.\dfrac{\partial^{m-1} F}{\partial x_0^h \, \partial x_1^k \, \partial x_2^\ell}\right|_P = 0 \quad \forall h, k, \ell \in \mathbb{N}$ *tali che* $h + k + \ell = m - 1$
- *esistono $h, k, \ell \in \mathbb{N}$ tali che $h + k + \ell = m$ e* $\left.\dfrac{\partial^m F}{\partial x_0^h \, \partial x_1^k \, \partial x_2^\ell}\right|_P \neq 0$

(*b*) *Se P è un punto semplice per $\mathscr{C}$, esiste un'unica retta $t \subseteq \mathbb{P}^2(\mathbb{C})$ tale che $i(\mathscr{C}, t, P) \geq 2$, di equazione*

$$t : \left.\frac{\partial F}{\partial x_0}\right|_P x_0 + \left.\frac{\partial F}{\partial x_1}\right|_P x_1 + \left.\frac{\partial F}{\partial x_2}\right|_P x_2 = 0 \ .$$

La retta t si dice tangente a $\mathscr{C}$ in P*; se $i(\mathscr{C}, r, P) = 3$, P si dice punto di* flesso ordinario *per $\mathscr{C}$; se $i(\mathscr{C}, r, P) = k + 2$, $k \geq 1$, P si dice* flesso di specie k *per $\mathscr{C}$.*

Di conseguenza, per una cubica liscia $\mathscr{C} : F(x_0, x_1, x_2) = 0$, le derivate parziali di F non sono mai tutte e tre nulle in un punto, e poiché $\deg F = 3$, ogni retta interseca $\mathscr{C}$ in 3 punti contati con molteplicità; in particolare, $\mathscr{C}$ può avere al più flessi ordinari.
Infine, se $\mathscr{D}$ è una cubica riducibile, $\mathscr{D} : G = 0$, notiamo che si verifica solo uno dei seguenti casi:

- $G = F_1 \cdot F_2$, con $\deg F_1 = 1$, $\deg F_2 = 2$, F_2 irriducibile
- $G = G_1 \cdot G_2 \cdot G_3$, con $\deg G_i = 1$ per $i = 1, 2, 3$.

Allora, posti $r : F_1 = 0$, $\mathscr{C} : F_2 = 0$, $r_i : G_i = 0$ per $i = 1, 2, 3$, si hanno 6 configurazioni possibili per i supporti delle curve:

(a) $\breve{r} \cap \breve{\mathscr{C}} = \{P_1, P_2\}$, $P_1 \neq P_2$

(b) $\breve{r} \cap \breve{\mathscr{C}} = \{P\}$

(c) $\breve{r}_1 \cap \breve{r}_2 = P$, $\breve{r}_1 \cap \breve{r}_3 = Q$, $\breve{r}_2 \cap \breve{r}_3 = R$ P, Q, R distinti

(d) $\breve{r}_1 \cap \breve{r}_2 \cap \breve{r}_3 = \{P\}$

(e) $\breve{r}_1 = \breve{r}_2 \neq \breve{r}_3$

(f) $\breve{r}_1 = \breve{r}_2 = \breve{r}_3$.

In ogni caso, si verifica subito che esiste almeno un punto multiplo per $\mathscr{D}$.

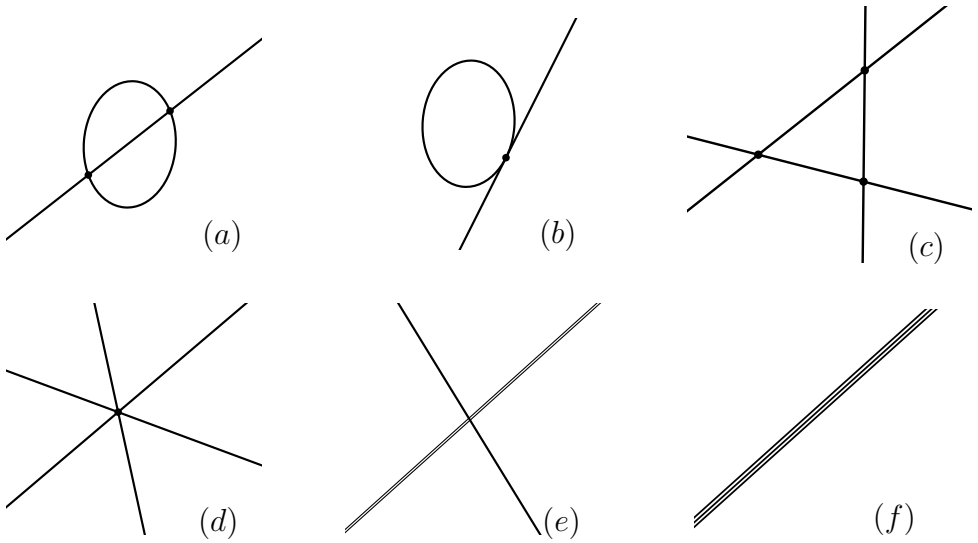


Figura 1.1. Esempi nel piano reale di possibili configurazioni del supporto di una cubica $\mathscr{D}$ riducibile.

In particolare, una cubica liscia è irriducibile.

1.2 Cubiche liscie piane e parametrizzabilità

L'obiettivo principale del lavoro presentato è descrivere l'insieme dei punti a coordinate razionali di una cubica $\mathscr{C}$ liscia razionale (cioè una cubica per cui esiste un'equazione a coefficienti razionali).
Ricordiamo che $\mathbb{K}(x)$ denota il campo delle funzioni razionali a coefficienti in $\mathbb{K}$, cioè il campo dei quozienti di $\mathbb{K}[x]$.
Se avessimo una parametrizzazione razionale per $\mathscr{C}$, ovvero se valesse (nel piano

affine)

$$\mathscr{C} : \begin{cases} x = h(t) \\ y = g(t) \end{cases} \quad \text{con } t \in \mathbb{C} \ , \ h, g \in \mathbb{C}(x)$$

o addirittura $h, g \in \mathbb{Q}(x)$ (dato che $\mathscr{C}$ è razionale), avremmo anche un modo per ottenere tutti punti a coordinate in $\mathbb{Q}$ di $\mathscr{C}$; purtroppo però una parametrizzazione siffatta non può esistere. Per mostrarlo, ci occorrerà il seguente risultato:

Lemma 1.2.1. *Siano $p, q \in \mathbb{C}[x]$ primi fra loro, e supponiamo che*

$$\begin{gathered} \exists [\lambda_i, \mu_i] \in \mathbb{P}^1(\mathbb{C}), i = 1, ..., 4, \ \textit{a due a due distinti} \\ \textit{tali che } \lambda_1 p + \mu_1 q \, , ..., \lambda_4 p + \mu_4 q \textit{ sono quadrati in } \mathbb{C}[x] \ . \end{gathered} \tag{$*$}$$

Allora p, q sono costanti.

Dimostrazione. Osserviamo preliminarmente che se $p, q \in \mathbb{C}[x]$ sono coprimi e tali che vale $(*)$, allora esistono $\bar{p}, \bar{q} \in \mathbb{C}[x]$ primi fra loro, tali che

$$\bar{p} \ , \ \bar{p} - \bar{q} \ , \ \bar{p} - \lambda \bar{q} \ , \ \bar{q} \quad \text{con } \lambda \neq 0, 1 \tag{1.2}$$

sono quadrati in $\mathbb{C}[x]$ e

$$\max\{\deg \bar{p} \, , \, \deg \bar{q}\} = \max\{\deg p \, , \, \deg q\} \ .$$

Infatti $[\lambda_i, \mu_i]$, $i = 1, ..., 4$, sono punti in posizione generale, quindi esiste un'unica proiettività ϕ della retta proiettiva tale che

$$\phi(\lambda_1, \mu_1) = [1, 0] \ , \ \phi(\lambda_2, \mu_2) = [0, 1] \ , \ \phi(\lambda_3, \mu_3) = [1, -1] \ ;$$

varrà poi $\phi(\lambda_4, \mu_4) = [1, -\lambda]$ per qualche $\lambda \neq 0, 1$. Quindi se ϕ^{-1} è rappresentata dalla matrice $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ con $ad - bc \neq 0$, i polinomi

$$\bar{p} = ap + bq \ , \ \bar{q} = cp + dq$$

sono tali che i (1.2), che sono ordinatamente uguali a multipli non nulli di $\lambda_1 p + \mu_1 q, ..., \lambda_4 p + \mu_4 q$, sono quadrati; inoltre $\bar{p}, \bar{q}$ non hanno fattori in comune,

altrimenti li avrebbero

$$d\bar{p} - b\bar{q} = (ad - cb)p \ , \ c\bar{p} - a\bar{q} = (bc - ad)q \ .$$

Infine si ha $\max\{\deg \bar{p}\, , \deg \bar{q}\} = \max\{\deg p\, , \deg q\}$: anzitutto, vale certamente $\max\{\deg \bar{p}\, , \deg \bar{q}\} \leq \max\{\deg p\, , \deg q\}$. Supponiamo valga la disuguaglianza stretta; chiamiamo α e β i coefficienti direttori rispettivamente di p e q, e sia per esempio $\deg p \leq \deg q$. Se $\deg p < \deg q$, deve essere $b\beta = d\beta = 0$, cioè $b = d = 0$, il che contraddice $ad - bc \neq 0$; se $\deg p = \deg q$, allora deve essere

$$\begin{aligned} a\alpha + b\beta &= 0 \\ c\alpha + d\beta &= 0 \end{aligned} \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

contraddicendo di nuovo $ad - bc \neq 0$.
Procediamo ora alla dimostrazione. Per assurdo, l'insieme

$$S = \{(p, q) \mid p, q \in \mathbb{C}[x] \ , \ p, q \text{ non costanti, coprimi e tali che vale } (*)\}$$

è non vuoto, quindi

$$\{m \in \mathbb{N} \mid m = \max\{\deg p\, , \deg q\} \ , \ (p, q) \in S\}$$

ha minimo $\bar{m}$, e per quanto detto prima, esiste una coppia $(\bar{p}, \bar{q}) \in S$ tale che $\bar{m} = \max\{\deg \bar{p}\, , \deg \bar{q}\}$ e $\bar{p}$, $\bar{p} - \bar{q}$, $\bar{p} - \lambda\bar{q}$, $\bar{q}$ con $\lambda \neq 0, 1$ sono quadrati.
Scriviamo

$$\bar{p} = u^2 \ , \ \bar{q} = v^2 \tag{1.3}$$

$$\implies \begin{aligned} \bar{p} - \bar{q} &= u^2 - v^2 = (u + v)(u - v) \\ \bar{p} - \lambda\bar{q} &= u^2 - \lambda v^2 = (u + \sqrt{\lambda}v)(u - \sqrt{\lambda}v) \end{aligned} \tag{1.4}$$

dove $\sqrt{\lambda}$ è una radice fissata di λ.
Poiché $\bar{p}$, $\bar{q}$ sono primi fra loro, lo sono anche $(u + v)$, $(u - v)$ (altrimenti $2u$, $2v$, e quindi u^2, v^2 avrebbero fattori in comune in $\mathbb{C}[x]$) e $(u + \sqrt{\lambda}v)$, $(u - \sqrt{\lambda}v)$ (per lo stesso motivo).
D'altra parte, i loro prodotti $u^2 - v^2$, $u^2 - \lambda v^2$ sono quadrati in $\mathbb{C}[x]$ per la (1.4),

quindi ogni loro fattore compare con una potenza pari, ovvero

$$u+v\ ,\ u-v\ ,\ u+\sqrt{\lambda}v\ ,\ u-\sqrt{\lambda}v$$

sono quadrati in $\mathbb{C}[x]$. In definitiva $(u,v)\in S$, e per (1.3) vale $\max\{\deg u\,,\,\deg v\}<\bar{m}$, assurdo. □

Si ha:

Proposizione 1.2.2. *Una cubica liscia di $\mathbb{P}^2(\mathbb{C})$ non è parametrizzabile tramite funzioni razionali.*

Dimostrazione. Anticipiamo ora alcuni risultati che vedremo a breve: una cubica liscia $\mathscr{C}$ si può sempre immergere in nel piano proiettivo complesso in modo che una sua equazione affine sia

$$\mathscr{C}: y^2=x^3+ax^2+bx+c\quad,\quad a,b,c\in\mathbb{C}\ ;$$

possiamo traslare $\mathscr{C}$ in modo da avere

$$\mathscr{C}: y^2=x(x-\alpha)(x-\beta)\ ,\ \text{ con }\alpha,\beta\neq 0\,,\,\alpha\neq\beta$$

(vedi osservazione 1.3.a). Infine, se $\sqrt{\alpha^3}$ è una radice fissata di α^3, usando la trasformazione

$$\begin{cases} x=\alpha X \\ y=\sqrt{\alpha^3}Y \end{cases}$$

e dividendo tutto per α^3, troviamo

$$\mathscr{C}: Y^2=X(X-1)(X-\lambda)\ ,\ \text{ con }\lambda\neq 0,1\ .$$

Se $\mathscr{C}$ avesse una parametrizzazione razionale:

$$\mathscr{C}:\begin{cases} X=h(t) \\ Y=g(t) \end{cases}\quad,\quad h,g\in\mathbb{C}(t)$$

allora per h e g varrebbe la relazione

$$h^2=g(g-1)(g-\lambda)\ . \qquad (\bullet)$$

Poiché $\mathbb{C}(t)$ è un dominio a fattorizzazione unica, si può scrivere

$$h = \frac{r}{s}\ , \quad r, s \text{ coprimi in } \mathbb{C}[t]$$
$$g = \frac{p}{q}\ , \quad p, q \text{ coprimi in } \mathbb{C}[t]\ .$$

Vogliamo mostrare che h e g sono costanti sfruttando il lemma appena visto; proviamo allora che esistono quattro combinazioni lineari distinte di p, q che sono quadrati in $\mathbb{C}[t]$. Sostituendo $\frac{r}{s}$ e $\frac{p}{q}$ in $(\bullet)$ e moltiplicando ambo i membri per q^3s^2 si trova

$$r^2q^3 = s^2p(p-q)(p-\lambda q)$$

da cui

$$s^2 \mid r^2q^3 \implies s^2 \mid q^3$$

e

$$q^3 \mid s^2p(p-q)(p-\lambda q) \implies q^3 \mid s^2\ .$$

Pertanto $s^2 = \gamma q^3$, $\gamma \in \mathbb{C}$, e in particolare $\gamma q = \left(\frac{s}{q}\right)^2$ è un quadrato in $\mathbb{C}(t)$; ma poiché $\gamma q \in \mathbb{C}[t]$, è un quadrato in $\mathbb{C}[t]$. Inoltre $r^2 = \gamma p(p-q)(p-\lambda q)$, dove p, $(p-q)$, $(p-\lambda q)$ non hanno fattori in comune (altrimenti li avrebbero p e q), quindi $\exists\, \delta, \varepsilon, \kappa \in \mathbb{C}$ tali che

$$\delta p\ ,\ \varepsilon(p-q)\ ,\ \kappa(p-\lambda q)$$

sono quadrati in $\mathbb{C}[t]$. Per il lemma, p e q sono costanti, quindi lo sono anche r ed s per le relazioni dette sopra, e h, $g \in \mathbb{C}$; pertanto non possono costituire una parametrizzazione per $\mathscr{C}$. □

Osservazione 1.2.a. Abbiamo visto nella dimostrazione precedente che se $\mathscr{C}$ è una cubica liscia, si può sempre trovare un'equazione affine per $\mathscr{C}$ della forma

$$\mathscr{C} : y^2 = x(x-1)(x-\lambda)\ , \quad \lambda \in \mathbb{C} \smallsetminus \{0,1\}\ . \qquad (\star)$$

Per il teorema di Salmon [Se, 36.3], se P è un flesso di $\mathscr{C}$ allora esistono 4 tangenti a $\mathscr{C}$ a due a due distinte passanti per P, compresa la tangente in P.
Inoltre, identificando il fascio di rette per P con la retta proiettiva $\mathbb{P}^1$, le 4 tan-

genti si possono vedere come punti $[\lambda_1, \mu_1], ..., [\lambda_4, \mu_4]$ di $\mathbb{P}^1$, e si dimostra che il loro modulo (definito come $j(\beta)$, dove j è la funzione $j(x) = \frac{(x^2-x+1)^3}{x^2(x-1)^2}$ e β è il birapporto [Se, pp.343-344] di $[\lambda_1, \mu_1], ..., [\lambda_4, \mu_4]$) non dipende dalla scelta del flesso P.
Pertanto è ben definito il modulo della cubica $j(\mathscr{C}) := j(\beta)$; tale modulo è un invariante proiettivo [Se, corollario 36.4], e se $\mathscr{C} = \mathscr{C}_\lambda$ è la cubica data da $(\star)$, vale $j(\mathscr{C}_\lambda) = j(\lambda)$.
D'altra parte, $\forall \lambda, \lambda' \in \mathbb{C} \setminus \{0, 1\}$, risulta

$$j(\lambda) = j(\lambda') \iff \lambda' \in \left\{ \lambda\,,\, \frac{1}{\lambda}\,,\, 1-\lambda\,,\, \frac{1}{1-\lambda}\,,\, \frac{\lambda-1}{\lambda}\,,\, \frac{\lambda}{\lambda-1} \right\}$$

quindi posto

$$\mathcal{M} = \{\text{classi di equivalenza proiettiva di cubiche liscie piane}\}$$

si ha

$$|\mathcal{M}| = \left| \{ j(\lambda)\,,\ \lambda \in \mathbb{C} \setminus \{0,1\} \} \right|$$

dove l'ultimo insieme indicato ha la stessa cardinalità di $\mathbb{C}$.

1.3 Forma normale di Weierstrass

Pur dovendo rinunciare ad una parametrizzazione razionale, possiamo comunque ottenere un'equazione per $\mathscr{C}$ che ci permetterà di studiare la curva in maniera efficace.

Teorema 1.3.1. *Sia $\mathscr{C}$ una cubica liscia di $\mathbb{P}^2(\mathbb{C})$. Allora $\mathscr{C}$ è proiettivamente equivalente ad una cubica di equazione affine*

$$\widetilde{\mathscr{C}} : y^2 = x^3 + ax^2 + bx + c$$

ovvero esiste $\Phi \in PGL_2(\mathbb{C})$ tale che $\mathscr{C} = \Phi(\widetilde{\mathscr{C}})$.

Dimostrazione. Poiché $\mathscr{C}$ è non singolare, possiede almeno un flesso P [Se, proposizione 34.8, corollario 34.9]. Con una proiettività Φ trasformiamo P nel punto $[0, 0, 1] = P'$, in modo che la tangente di flesso sia $r : x_0 = 0$ (Φ siffatta esiste: imporre condizioni su P e sulla sua tangente equivale a imporle su P e un altro punto $\neq P$ sulla tangente; una proiettività è determinata, come sappiamo, dalle immagi-

ni di 4 punti in posizione generale). Questo significa che, se $\mathscr{C}' : F(x_0, x_1, x_2) = 0$ è l'equazione della trasformata nel nuovo sistema di riferimento, con

$$\begin{aligned} F(x_0, x_1, x_2) =& a_0x_0^3 + a_1x_1^3 + a_2x_2^3 + a_3x_0^2x_1 + a_4x_0^2x_2 + a_5x_0x_1^2 + \\ &+ a_6x_0x_2^2 + a_7x_1^2x_2 + a_8x_1x_2^2 + a_9x_0x_1x_2, \end{aligned} \tag{1.5}$$

poiché $P' \in \mathscr{C}'$ e $F(0,0,1) = a_2$, dovrà essere $a_2 = 0$.
Scriviamo poi

$$\begin{aligned} \frac{\partial F}{\partial x_0} &= 3a_0x_0^2 + 2a_3x_0x_1 + 2a_4x_0x_2 + a_5x_1^2 + a_6x_2^2 + a_9x_1x_2 \ , \\ \frac{\partial F}{\partial x_1} &= 3a_1x_1^2 + a_3x_0^2 + 2a_5x_0x_1 + 2a_7x_1x_2 + a_8x_2^2 + a_9x_0x_2 \ , \\ \frac{\partial F}{\partial x_2} &= 3a_2x_2^2 + a_4x_0^2 + 2a_6x_0x_2 + a_7x_1^2 + 2a_8x_1x_2 + a_9x_0x_1 \ ; \end{aligned}$$

l'equazione della retta tangente a $\mathscr{C}$ in P è $\frac{\partial F}{\partial x_0}\big|_P x_0 + \frac{\partial F}{\partial x_1}\big|_P x_1 + \frac{\partial F}{\partial x_2}\big|_P x_2 = 0$, cioè $a_6x_0 + a_8x_1 + 3a_2x_2 = 0$, e nel nostro caso deve essere $r : x_0 = 0$, per cui $a_6 \neq 0$ e $a_8 = 0$. Rimane quindi

$$\mathscr{C}' : a_0x_0^3 + \underset{\not\equiv 0}{a_1x_1^3} + a_3x_0^2x_1 + a_4x_0^2x_2 + a_5x_0x_1^2 + \underset{\not\equiv 0}{a_6x_0x_2^2} + a_7x_1^2x_2 + a_9x_0x_1x_2 = 0 \ .$$

Infine, deve valere $i(\mathscr{C}', r, P') = 3$, dunque la risolvente di $\mathscr{C}' \cap r$, che è $a_1x_1^3 + a_7x_1^2x_2 = 0$, deve avere $[0,0,1]$ come radice di molteplicità 3, da cui $a_7 = 0$ e $a_1 \neq 0$.
Deomogeneizzando rispetto ad x_0, con $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$, a meno di dividere per $a_6 \neq 0$, posso scrivere $\mathscr{C}'$ come

$$\mathscr{C}' : y^2 + \beta xy + \gamma y = \alpha x^3 + \delta x^2 + \varepsilon x + \zeta$$

dove $\alpha = \frac{a_1}{a_6} \neq 0$.
Considero poi la trasformazione affine Ψ^{-1}

$$\begin{cases} x = X \\ y = Y - \dfrac{\beta}{2}X - \dfrac{\gamma}{2} \end{cases}$$

per cui l'equazione della trasformata $\mathscr{C}''$ di $\mathscr{C}'$ risulta

$$Y^2 - \frac{\beta^2}{4}X^2 - \frac{\beta\gamma}{2}X - \frac{\gamma^2}{4} = \alpha X^3 + \delta X^2 + \varepsilon X + \zeta$$

cioè $\mathscr{C}'' : Y^2 = f_1(X)$ con f_1 polinomio di grado 3. Se $\alpha \neq 1$, utilizzando l'affinità

$$\begin{cases} X = \alpha x \\ Y = \alpha^2 y \end{cases}$$

e dividendo tutto per α^4, otteniamo una curva $\widetilde{\mathscr{C}}$, proiettivamente equivalente a $\mathscr{C}$, con l'equazione della forma cercata. □

Notazione 2. Possiamo riformulare il teorema precedente in questo modo: data una cubica liscia $\mathscr{C}$ di $\mathbb{P}^2(\mathbb{C})$, è possibile determinare un riferimento proiettivo $\mathcal{P}$ tale che $\mathscr{C}$ abbia equazione rispetto a $\mathcal{P}$ data da

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx + c \qquad a,\, b,\, c \in \mathbb{C}\ .$$

In tal caso diremo che $\mathscr{C}$ è in *forma normale*. Scriveremo anche

$$\mathscr{C} : y^2 = f(x) \quad \text{con} \quad f(x) = x^3 + ax^2 + bx + c\ .$$

***Esempio* 1.1.** Cerchiamo un'equazione in forma normale per la cubica:

$$\mathscr{C} : x_0^2x_1 + x_0^2x_2 + x_0x_1^2 + x_0x_2^2 + x_1^2x_2 + x_1x_2^2 + x_0x_1x_2 = 0\ .$$

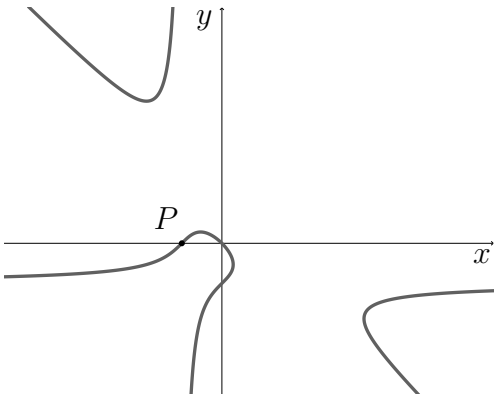


Figura 1.2. Rappresentazione dei punti reali di $\mathscr{C}$ in coordinate non omogenee $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$, $\mathscr{C} : x + y + x^2 + y^2 + xy + x^2y + xy^2 = 0$. Vedi appendice A.

Osserviamo che $\mathscr{C}$ è non singolare, infatti posto

$$F(x_0, x_1, x_2) = x_0^2x_1 + x_0^2x_2 + x_0x_1^2 + x_0x_2^2 + x_1^2x_2 + x_1x_2^2 + x_0x_1x_2$$

il sistema

$$\begin{cases} \dfrac{\partial F}{\partial x_0}(x_0, x_1, x_2) = 0 \\ \dfrac{\partial F}{\partial x_1}(x_0, x_1, x_2) = 0 \\ \dfrac{\partial F}{\partial x_2}(x_0, x_1, x_2) = 0 \end{cases}$$

ha solo la soluzione banale $(0, 0, 0)$.
$\mathscr{C}$ ha un flesso in $P = [1, -1, 0]$, con tangente $r : x_0 + x_1 - x_2 = 0$; scegliamo dunque $\Phi \in PGL_2$ tale che $\Phi(P) = [0, 0, 1]$ e $\Phi(r) = r'$ con $r' : x_0 = 0$; ad esempio la proiettività rappresentata dalla matrice

$$\Phi = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

$\Phi(\mathscr{C}) = \mathscr{C}'$ avrà equazione data da $F(\Phi^{-1}(x_0, x_1, x_2)) = 0$; facendo i conti risulta

$$\mathscr{C}' : -x_0^3 + 4x_0^2x_1 - 2x_0^2x_2 - 5x_0x_1^2 - x_0x_2^2 + 2x_1^3 + 3x_0x_1x_2 = 0$$

e deomogeneizzando rispetto ad x_0 rimane

$$\mathscr{C}' : y^2 - 3xy + 2y = 2x^3 - 5x^2 + 4x - 1.$$

Applicando la proiettività Ψ rappresentata dalla matrice

$$\Psi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & -\dfrac{3}{2} & 1 \end{pmatrix}$$

trovo $\Psi(\mathscr{C}') = \mathscr{C}''$ di equazione $F(\Phi^{-1}(\Psi^{-1}(1, x, y))) = 0$, ovvero

$$\mathscr{C}'' : y^2 = 2x^3 - \frac{11}{4}x^2 + x\ ;$$

ancora ponendo $y = 4Y$, $x = 2X$, ossia utilizzando l'affinità

$$\Theta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{4} \end{pmatrix}$$

e dividendo tutto per 16, si ottiene $\widetilde{\mathscr{C}} : \frac{1}{16} F(\Phi^{-1}(\Psi^{-1}(\Theta^{-1}(1, x, y)))) = 0$, cioè

$$\tilde{\mathscr{C}} : Y^2 = X^3 - \frac{11}{16}X^2 + \frac{1}{8}X$$

proiettivamente equivalente a $\mathscr{C}$ tramite

$$\Theta \circ \Psi \circ \Phi = \begin{pmatrix} 1 & 1 & -1 \\ \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{8} & -\frac{1}{8} & 0 \end{pmatrix}.$$

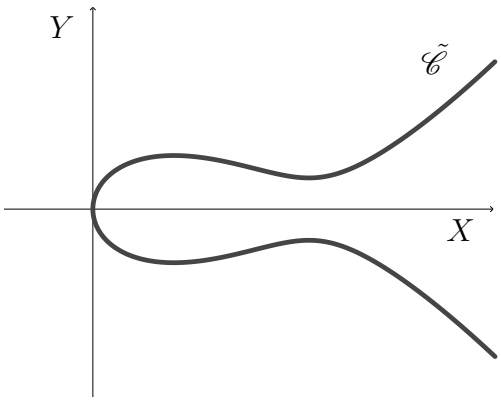


Figura 1.3. Rappresentazione di $\widetilde{\mathscr{C}}$ in coordinate non omogenee X, Y.

Osservazione 1.3.a. È bene notare alcune proprietà di una cubica liscia scritta in forma normale, che torneranno utili in seguito. Anzitutto, il suo grafico in coordinate non omogenee $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$, è simmetrico rispetto all'asse delle x (quindi $(a, b) \in \mathscr{C} \Leftrightarrow (a, -b) \in \mathscr{C}$). Inoltre $\mathscr{C}$ ha $[0, 0, 1]$ come unico punto all'infinito, e questo è sempre un punto di flesso; le rette che passano per $[0, 0, 1]$ sono le rette aventi equazione affine del tipo $x = \alpha$, $\alpha \in \mathbb{C}$, più la tangente inflessionale, che è la retta all'infinito $x_0 = 0$; tenendo conto di questo, possiamo lavorare su $\mathscr{C}$ considerando per lo più la parte affine.
Infine, scrivendo $\mathscr{C} : y^2 = f(x)$, osserviamo che sono possibili 2 casi: il polinomio $f(x)$ ha una sola radice reale (figura 1.4), oppure ha 3 radici reali distinte (figura

1.5).

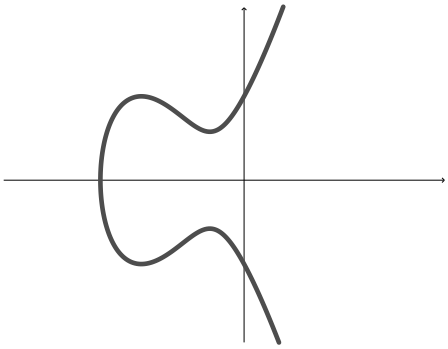


Figura 1.4

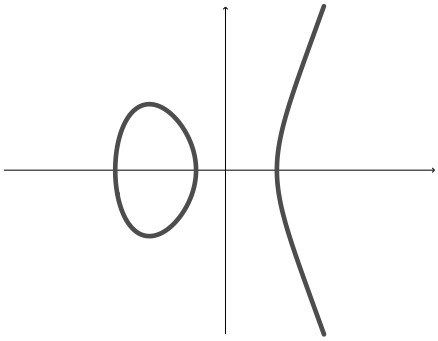


Figura 1.5

Non può succedere che $f(x)$ abbia una radice reale $\bar{x}$ doppia o tripla: infatti in tal caso $\bar{x}$ sarebbe radice di f e di f'; d'altra parte, posto $F(x,y) = y^2 - f(x)$, vale $\mathscr{C} : F(x,y) = 0$ e $\frac{\partial F}{\partial x} = -f'(x)$, $\frac{\partial F}{\partial y} = 2y$, quindi il punto $(\bar{x}, 0) \in \mathscr{C}$ azzera entrambe le derivate parziali, ovvero è singolare, contro l'ipotesi che $\mathscr{C}$ sia liscia.

Capitolo 2

La legge di gruppo su una cubica liscia

2.1 Costruzione geometrica della somma di due punti

È possibile dare all'insieme dei punti di una cubica non singolare del piano proiettivo complesso la struttura di gruppo; questo ci permetterà di ricavare molte informazioni, non più di carattere solo geometrico, sui punti di una cubica liscia.

Definizione 2.1.1. Sia $\mathscr{C} \subseteq \mathbb{P}^2(\mathbb{C})$ una cubica liscia e sia $O \in \mathscr{C}$ fissato. Per ogni P, $Q \in \mathscr{C}$, definiamo $P + Q$ nel modo seguente:

> sia $\langle P, Q\rangle$ la retta passante per P e Q; questa interseca $\mathscr{C}$ in un terzo punto per il teorema (1.1.8), che indichiamo con $P * Q$. Chiamiamo allora $P + Q$ il terzo punto di intersezione fra $\mathscr{C}$ e la retta $\langle O, P * Q\rangle$, ovvero $P + Q = O * (P * Q)$.

La definizione è ben posta; in particolare è bene notare che le intersezioni con $\mathscr{C}$ delle rette vanno considerate con le loro molteplicità, ovvero

- se $P = Q$, allora $\langle P, P\rangle$ è la retta tangente a $\mathscr{C}$ in P (che è sempre ben definita perché $\mathscr{C}$ è liscia)
- se $P \neq Q$ e $\langle P, Q\rangle$ è tangente a $\mathscr{C}$ in Q, allora $P * Q = Q$
- se P è un punto di flesso, allora $P * P = P$.

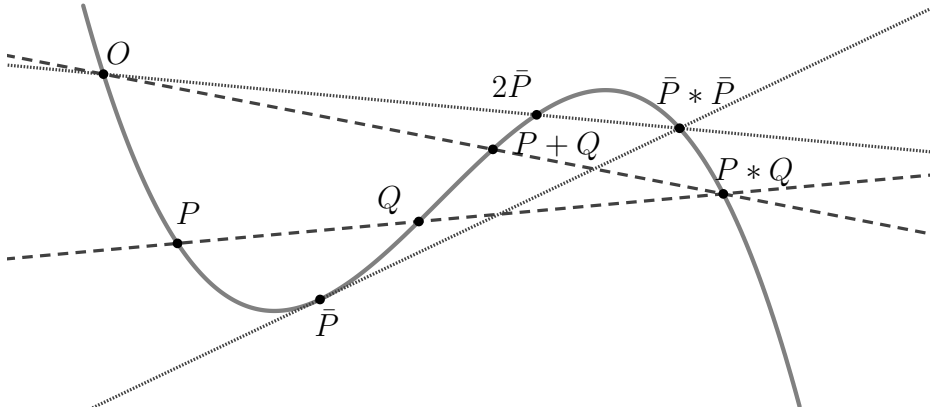


Figura 2.1. Due esempi su una cubica liscia: $P + Q$ e $\bar{P} + \bar{P} = 2\bar{P}$

Vorremmo ora provare che quella definita sopra è un'operazione che dà all'insieme dei punti di $\mathscr{C}$ la struttura di gruppo abeliano. La dimostrazione completa di questo fatto richiede alcuni risultati sui sistemi lineari di curve, che vedremo a breve, e vari risultati legati al concetto di varietà algebrica, di cui daremo solo alcuni cenni.

Nel seguito indicheremo con S_d il $\mathbb{C}$-spazio vettoriale dato dall'insieme dei polinomi omogenei di grado d in 3 indeterminate a coefficienti in $\mathbb{C}$, più il polinomio nullo, cioè $S_d = \mathbb{C}[x_0, x_1, x_2]_d$, e con $\mathbb{P}(S_d)$ l'insieme delle classi di proporzionalità degli elementi di $S_d \setminus \{0\}$, che si identifica con l'insieme delle curve di $\mathbb{P}^2(\mathbb{C})$ di grado d. Ricordiamo che una base per S_d è data dai monomi

$$x_0^{d_0} x_1^{d_1} x_2^{d_2} \quad , \quad \text{con} \quad d_0 + d_1 + d_2 = d \quad , \quad 0 \leq d_i \leq d$$

dunque $\dim S_d = \binom{d+2}{d} = \binom{d+2}{2} := N$ e $\dim \mathbb{P}(S_d) = N - 1$.
Inoltre se $F \in \mathbb{P}(S_d)$, $P_1, ..., P_n \in \mathbb{P}^2(\mathbb{C})$, denoteremo con $\Delta_d(P_1, ..., P_n)$ l'insieme $\{F \in \mathbb{P}(S_d) \mid F(P_i) = 0 \quad i = 1, ..., n\}$, che risulta essere un sottospazio di $\mathbb{P}(S_d)$ di dimensione $\geq N - n$.

Lemma 2.1.2. *Siano $r : g(x_0, x_1, x_2) = 0$ con $\deg g = 1$ e $\mathscr{C} : h(x_0, x_1, x_2) = 0$ con $\deg h = 2$ rispettivamente una retta e una conica non degenere di $\mathbb{P}^2(\mathbb{C})$. Siano poi $P_1, ..., P_n \in \mathbb{P}^2(\mathbb{C})$, e si consideri $\Delta_d(P_1, ..., P_n)$ con d fissato. Allora*

(i) se $P_1, ..., P_k \in r$, $P_{k+1}, ..., P_n \notin r$ e $k > d$, vale

$$\Delta_d(P_1, ..., P_n) = g \cdot \Delta_{d-1}(P_{k+1}, ..., P_n)$$

(*ii*) *se* $P_1, ..., P_k \in \mathscr{C}$, $P_{k+1}, ..., P_n \notin \mathscr{C}$ *e* $k > 2d$, *vale*

$$\Delta_d(P_1, ..., P_n) = h \cdot \Delta_{d-2}(P_{k+1}, ..., P_n)$$

Dimostrazione. Se $F \in \Delta_d(P_1, ...P_n)$, la curva $\mathscr{D} : F = 0$ interseca r nei punti $P_1, ..., P_k$, con $k > d$; per il teorema 1.1.8 deve essere $r \subseteq \mathscr{D}$. Come conseguenza del teorema degli zeri di Hilbert (si veda [H, par.1.1]) si ha $F = gF_1$ per qualche $F_1 \in \mathbb{P}(S_{d-1})$. Inoltre, poiché $P_{k+1}, ..., P_n \in \mathscr{D}$ ma $\notin r$, tali punti dovranno appartenere alla curva $\mathscr{D}_1 : F_1 = 0$, cioè $F_1 \in \Delta_{d-1}(P_{k+1}, ..., P_n)$. Questo mostra l'inclusione

$$\Delta_d(P_1, ..., P_n) \subseteq g \cdot \Delta_{d-1}(P_{k+1}, ..., P_n);$$

l'altra inclusione segue subito dalla definizione di Δ_d. Quindi vale (*i*); per (*ii*) si ragiona in maniera del tutto analoga: si usa un altro caso particolare del teorema di Bézout, che si dimostra analogamente al teorema 1.1.8. □

Proposizione 2.1.3. *Siano* $P_1, ..., P_8 \in \mathbb{P}^2(\mathbb{C})$ *punti distinti. Supponiamo che*

(∗) *comunque presi* 4 *dei* P_i, *questi non sono allineati*

(∗∗) *comunque presi* 7 *dei* P_i, *questi non giacciono sulla stessa conica non degenere*

Allora le cubiche di $\mathbb{P}^2(\mathbb{C})$ *passanti per* $P_1, ..., P_8$ *formano uno spazio proiettivo di dimensione 1, cioè* $\dim \Delta_3(P_1, ..., P_8) = 1$

Dimostrazione. Si ha anzitutto $\dim \Delta_3(P_1, ..., P_8) \geq 1$, perché i P_i impongono 8 condizioni lineari sui punti di $\mathbb{P}(S_3)$, che ha dimensione 9.

Caso (a) I punti sono a 3 a 3 non allineati e a 6 a 6 non giacciono sulla stessa conica non degenere. Per assurdo, $\dim \Delta_3(P_1, ..., P_8) \geq 2$; considero allora P_9 e P_{10} punti distinti scelti su $r = \langle P_1, P_2 \rangle$. Il passaggio per P_9, P_{10} impone alle cubiche di $\mathbb{P}^2$ due condizioni lineari, indipendenti o meno da quelle imposte da $P_1, ..., P_8$, ovvero

$$\dim \Delta_3(P_1, ..., P_{10}) \geq \dim \Delta_3(P_1, ..., P_8) - 2 \geq 0.$$

In particolare $\exists F \in \Delta_3(P_1, ..., P_{10})$. Ora, poiché $r : g = 0$ contiene i 4 punti P_1, P_2, P_9, P_{10}, per il lemma 2.1.2 deve essere $F = gF_1$, con $F_1 \in \Delta_2(P_3, ..., P_8)$.

Ma questo va contro l'ipotesi: infatti se $F_1 = 0$ è l'equazione di una conica degenere, almeno 3 punti fra $P_3, ..., P_8$ devono essere allineati su una delle rette del supporto della conica; se non degenere, ho 6 punti fra $P_1, ..., P_8$ che vi giacciono.

Caso (b) Tre punti sono allineati, ad esempio $P_1, P_2, P_3 \in r : g = 0$. Sia $P_9 \in r$ diverso da P_1, P_2, P_3; per il lemma 2.1.2 vale $\Delta_3(P_1, ..., P_9) = g\Delta_2(P_4, ..., P_8)$, dove $\Delta_2(P_4, ..., P_8)$ contiene almeno un punto, e anzi ne contiene esattamente 1 [R, cap.1, corollario 1.10] per l'ipotesi $(*)$.
Quindi $\dim \Delta_3(P_1, ..., P_9) = \dim \Delta_2(P_4, ..., P_8) = 0$, da cui $\dim \Delta_3(P_1, ..., P_8) \leq 1$.

Caso (c) Sei punti giacciono sulla stessa conica con degenere, ad esempio $P_1, ..., P_6$ su $\mathscr{C} : h = 0$. Sia $P_9 \in \mathscr{C}$ diverso da $P_1, ..., P_6$; ancora per il lemma 2.1.2 vale $\Delta_3(P_1, ..., P_9) = h\Delta_1(P_7, P_8)$.
Ma $\Delta_1(P_7, P_8) = \{\langle P_7, P_8 \rangle\}$, quindi di nuovo $\dim \Delta_3(P_1, ..., P_9) = 0$, e si ragiona come nel caso (b).

□

Corollario 2.1.4. *Siano $\mathscr{C}_1$, $\mathscr{C}_2 \subseteq \mathbb{P}^2(\mathbb{C})$ due cubiche tali che*

$$\mathscr{C}_1 \cap \mathscr{C}_2 = \{P_1, ..., P_9\} \ , \quad P_i \neq P_j \text{ se } i \neq j.$$

Allora una cubica $\mathscr{D} \subseteq \mathbb{P}^2(\mathbb{C})$ passante per 8 di questi punti passa anche per il nono.

Dimostrazione. Per i P_i, $i = 1, ..., 8$ valgono le condizioni $(*)$ e $(**)$ della proposizione 2.1.3: infatti se 4 punti fossero allineati su una retta r, questa dovrebbe essere contenuta in $\mathscr{C}_1$ e in $\mathscr{C}_2$, contro l'ipotesi $\mathscr{C}_1 \cap \mathscr{C}_2 = \{P_1, ..., P_9\}$; allo stesso modo, se 7 punti fossero sulla stessa conica non degenere, questa dovrebbe essere contenuta in $\mathscr{C}_1 \cap \mathscr{C}_2$.
Quindi $\dim \Delta_3(P_1, ..., P_8) = 1$, e se $\mathscr{C}_1 : F_1 = 0$, $\mathscr{C}_2 : F_2 = 0$, con F_1, $F_2 \in \Delta_3(P_1, ..., P_8)$, $F_1 \neq F_2$, queste costituiscono una base di $\Delta_3(P_1, ..., P_8)$; pertanto una cubica $\mathscr{D}$ passante per i P_i, $i = 1, ..., 8$, avrà equazione del tipo $\mathscr{D} : \lambda F_1 + \mu F_2 = 0$, $[\lambda, \mu] \in \mathbb{P}^1$, quindi passerà anche per P_9. □

Con questo risultato, siamo in grado di dimostrare la prima parte del seguente:

Teorema 2.1.5. *Siano $\mathscr{C} \subseteq \mathbb{P}^2(\mathbb{C})$ una cubica liscia, $O \in \mathscr{C}$ fissato, e*

$$\begin{aligned} \zeta : \mathscr{C} \times \mathscr{C} &\longrightarrow \mathscr{C} \\ (A, B) &\longrightarrow \zeta(A, B) = A + B \end{aligned}$$

l'operazione definita in 2.1.1. Allora $(\mathscr{C}, +, O)$ è un gruppo abeliano.

Dimostrazione. Siano A, B, $C \in \mathscr{C}$; vale certamente $A + B = B + A$ dato che $A * B = B * A$.
Proviamo che O è l'elemento neutro, cioè $A + O = O * (A * O) = A$. La retta per A e O interseca $\mathscr{C}$ la terza volta in $A * O$; quindi la retta per $A * O$ e O, che è la stessa, interseca $\mathscr{C}$ la terza volta in A.
Per trovare gli elementi opposti, si considera il punto $\bar{O} = O * O$ e si definisce il punto $A' = A * \bar{O}$; vale quindi $A * A' = \bar{O}$. Allora

$$A + A' = O * (A * A') = O * \bar{O} = O$$

dato che $\langle O, \bar{O} \rangle$ è tangente in O. Questo prova $A' = -A$.
Per mostrare l'associatività, poiché

$$\begin{aligned} (A + B) + C &= O * ((A + B) * C) \\ A + (B + C) &= O * (A * (B + C)) \end{aligned}$$

basterà mostrare $(A + B) * C = A * (B + C)$.
Consideriamo le rette $r = \langle A + B, C \rangle$ e $t = \langle A, B + C \rangle$, e supponiamo che i punti

$$O,\ A,\ B,\ C,\ A * B,\ B * C,\ A + B,\ B + C,\ r \cap t =: E \tag{2.1}$$

siano tutti distinti (quindi E è ben definito perché r e t sono rette distinte); è sufficiente mostrare che E appartiene a $\mathscr{C}$. Infatti, poiché r e t intersecano già $\mathscr{C}$ ciascuna in due punti diversi da E, se anche $E \in \mathscr{C}$, questo dovrà coincidere con $(A + B) * C$ e $A * (B + C)$.
Ora, nella costruzione di $(A + B) * C$ e $A * (B + C)$ sono tracciate 6 rette:

$$\begin{aligned} r_1 = \langle A, B \rangle,\ r_2 = \langle O, A * B \rangle,\ r = \langle A + B, C \rangle \\ t_1 = \langle B, C \rangle,\ t_2 = \langle O, B * C \rangle,\ t = \langle A, B + C \rangle \end{aligned} .$$

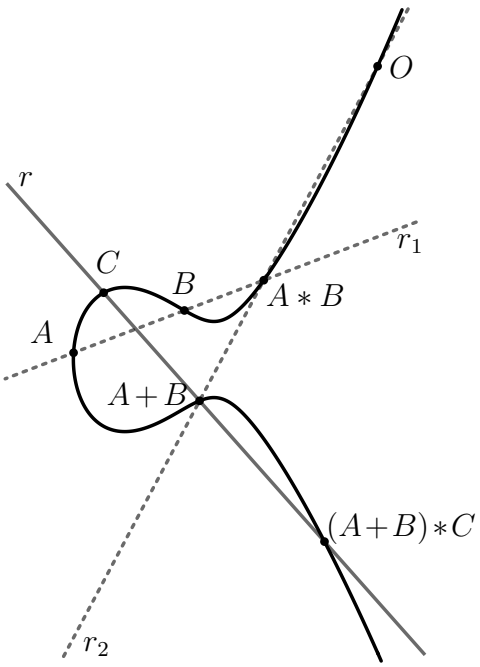


Figura 2.2

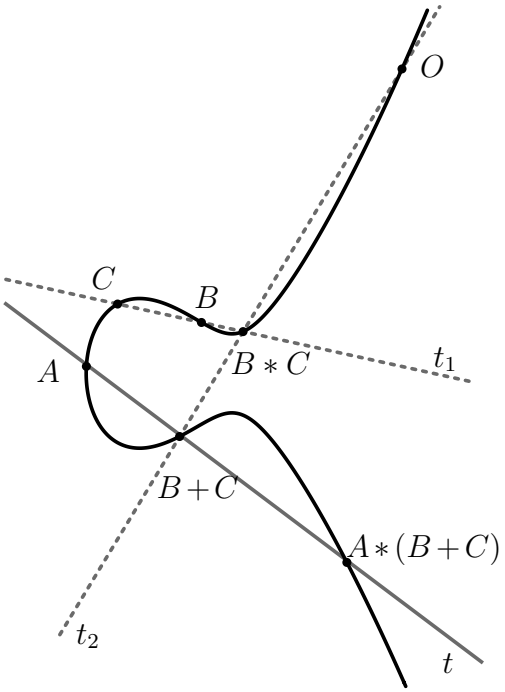


Figura 2.3

Considero le cubiche degeneri $\mathscr{C}_1$ e $\mathscr{C}_2$ che hanno come supporto rispettivamente $r_1 \cup t_2 \cup r$ e $t_1 \cup r_2 \cup t$; queste passano per i nove punti (2.1), e $\mathscr{C}$ passa per 8 di questi. Per il corollario 2.1.4, $\mathscr{C}$ deve passare anche per il nono, cioè E; questo prova l'associatività nel caso che i punti (2.1) siano distinti. □

Osservazione 2.1.a. Diamo un'idea di come si può dimostrare l'associatività nel caso in cui due o più punti in (2.1) coincidano. Per una dimostrazione alternativa si veda [K, pp.67-74].
Anzitutto, una cubica liscia $\mathscr{C} \subseteq \mathbb{P}^2(\mathbb{C})$ è una varietà proiettiva, su cui possiamo mettere la topologia indotta dalla topologia di Zariski in $\mathbb{P}^2(\mathbb{C})$, cioè la topologia in cui un chiuso è il luogo degli zeri di un numero finito di polinomi omogenei $\in \mathbb{C}[x_0, x_1, x_2]$.
In questo ambito, si può dimostrare che valgono i seguenti fatti:

(**I**) la funzione $* : \begin{array}{ccc} \mathscr{C} \times \mathscr{C} & \longrightarrow & \mathscr{C} \\ (A, B) & \longmapsto & A * B \end{array}$ è una funzione continua

(**II**) l'insieme $U = \{(A, B, C) \in \mathscr{C} \times \mathscr{C} \times \mathscr{C} \mid \text{i punti (2.1) sono distinti}\}$ è un sottoinsieme denso di $\mathscr{C} \times \mathscr{C} \times \mathscr{C}$.

La (**I**) ci dice che la funzione $A \longmapsto A * O$ è pure continua (perché restrizione di $*$ a $\mathscr{C} \times \{O\}$), quindi lo sono anche $\zeta : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$, $\zeta(A, B) = A + B$, e la funzione opposto $A \mapsto A * (O * O)$, perché composizioni di funzioni continue. Allora anche le funzioni

$$\begin{array}{rccccc} \Sigma_1 = \zeta \circ (\zeta \times id_{\mathbb{C}}) : & (\mathscr{C} \times \mathscr{C}) \times \mathscr{C} & \longrightarrow & \mathscr{C} \times \mathscr{C} & \longrightarrow & \mathscr{C} \\ & (A, B, C) & \longmapsto & (A + B, C) & \longmapsto & (A + B) + C \end{array}$$

$$\begin{array}{rccccc} \Sigma_2 = \zeta \circ (id_{\mathbb{C}} \times \zeta) : & \mathscr{C} \times (\mathscr{C} \times \mathscr{C}) & \longrightarrow & \mathscr{C} \times \mathscr{C} & \longrightarrow & \mathscr{C} \\ & (A, B, C) & \longmapsto & (A, B + C) & \longmapsto & A + (B + C) \end{array}$$

definite su $\mathscr{C} \times \mathscr{C} \times \mathscr{C}$ sono continue e coincidono su U per (**II**).
Inoltre, la funzione

$$\begin{array}{rcl} \mathscr{C} \times \mathscr{C} \times \mathscr{C} & \longrightarrow & \mathscr{C} \\ (A, B, C) & \longmapsto & \Sigma_1(A, B, C) - \Sigma_2(A, B, C) \end{array}$$

è continua perché composizione di funzioni continue.
Di conseguenza, l'insieme

$$\{(A, B, C) \in \mathscr{C} \times \mathscr{C} \times \mathscr{C} \mid \Sigma_1(A, B, C) = \Sigma_2(A, B, C)\}$$

è un chiuso, in quanto controimmagine di $\{O\}$ tramite la funzione continua $\Sigma_1 - \Sigma_2$, e contiene U; pertanto contiene anche la sua chiusura, che è appunto $\mathscr{C} \times \mathscr{C} \times \mathscr{C}$.
In altre parole

$$\forall A, B, C \in \mathscr{C} \ , \ A + (B + C) = (A + B) + C$$

quindi vale l'associatività e $(\mathscr{C}, +, O)$ è un gruppo abeliano.

2.2 La legge di gruppo su $\mathscr{C}$ in forma normale

2.2.1 Proprietà

Osservazione 2.2.a. La legge di gruppo su una cubica dipende dal punto scelto come elemento neutro, infatti certamente $O * (P * Q) \neq O' * (P * Q)$ se $O \neq O'$. Vale comunque la seguente proposizione.

Proposizione 2.2.1. *Siano O, O' due punti di $\mathscr{C}$, e siano $+$, rispettivamente $\oplus$ le leggi di gruppo su $\mathscr{C}$ con elemento neutro O, rispettivamente O'.*
I gruppi $(\mathscr{C}, +, O)$, $(\mathscr{C}, \oplus, O')$ sono isomorfi tramite l'applicazione

$$\phi : P \longmapsto P \ominus O \ .$$

Dimostrazione. Si ha

$$\phi(P+Q) = (P+Q) \ominus O = (\bullet)$$
$$\phi(P) \oplus \phi(Q) = (P \ominus O) \oplus (Q \ominus O) = P \oplus Q \ominus 2O = (\bullet\bullet).$$

Dunque $(\bullet) = (\bullet\bullet)$ se e solo se $P+Q = P \oplus Q \ominus O \Leftrightarrow (P+Q) \oplus O = P \oplus Q$. Ma

$$(P+Q) \oplus O = (O * (P * Q)) \oplus O = O' * (O * (O * (P * Q))) = (\circ)$$
$$P \oplus Q = O' * (P * Q) = (\circ\circ)$$

Quindi $(\circ) = (\circ\circ)$ se e solo se $O * (O * (P * Q)) = P * Q$, che è vero. □

È bene notare che questo non significa $\phi(A * B) = \phi(A) * \phi(B)$; infatti ad esempio se O è un flesso ma non lo è O', risulta $\phi(O * O) = \phi(O) = O'$ e $\phi(O) * \phi(O) = O' * O' \neq O'$.

Osservazione 2.2.b. La legge di gruppo su una cubica non dipende dal riferimento proiettivo scelto: infatti la definizione 2.1.1 è basata su una costruzione puramente geometrica, valida a prescindere dalla scelta della coordinate.

Alla luce di queste osservazioni, da ora studieremo $(\mathscr{C}, +, O)$ considerando $\mathscr{C}$ in forma normale e prendendo come elemento neutro O il punto all'infinito di $\mathscr{C}$, che è un punto di flesso; il gruppo così ottenuto è particolarmente maneggevole, ed è caratterizzato completamente da alcune sue proprietà:

Teorema 2.2.2. *Sia $\mathscr{C}$ una cubica liscia di $\mathbb{P}^2(\mathbb{C})$ in forma normale*

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx + c\,;$$

esiste un'unica legge di gruppo su $\mathscr{C}$ tale che

(i) *l'elemento neutro sia $O = [0, 0, 1]$*

(ii) *l'opposto di $A = (x_A, y_A) \in \mathscr{C}$ sia $-A = (x_A, -y_A)$*

(iii) *$\forall A, B, C \in \mathscr{C}$ valga $A + B + C = O \Leftrightarrow A, B, C$ sono allineati.*

Dimostrazione. Nel teorema 2.1.5 abbiamo già mostrato che $(\mathscr{C}, +, O)$, con l'operazione definita in 2.1.1, è un gruppo, per cui vale (i). Inoltre, $\forall A \in \mathscr{C}$, $-A$ è dato da

$$-A = A * (O * O) = A * O$$

perché O è un punto di flesso; ma $\langle A, O\rangle$ è la retta $x = x_A$, che interseca $\mathscr{C}$ la terza volta in $(x_A, -y_A) = -A$, cioè (ii). Infine, A, B, C sono allineati $\Leftrightarrow A * B = C$ $\Leftrightarrow O * (A * B) = O * C$, cioè $A + B = -C$, da cui (iii).
Mostriamo l'unicità: se $(\mathscr{C}, \oplus, O)$ è un gruppo che soddisfa (i) - (iii), allora $A \oplus B = \ominus C$ con $\ominus C = \ominus(x_C, y_C) = (x_C, -y_C) = -C$; quindi $A + B = A \oplus B$. $\square$

2.2.2 Formule di addizione su $\mathscr{C}$

Diamo ora delle formule per calcolare le coordinate di $A + B$ in $(\mathscr{C}, +, O)$, che torneranno utili per ricavare proprietà algebriche e numeriche degli elementi del gruppo.

Proposizione 2.2.3. *Consideriamo la cubica $\mathscr{C} \subseteq \mathbb{P}^2(\mathbb{C})$,*

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx + c\,,$$

e siano $f(x) = x^3 + ax^2 + bx + c$, $A, B \in \mathscr{C}$ diversi da $O = [0, 0, 1]$, con $A = (x_A, y_A)$, $B = (x_B, y_B)$. Allora

$$A + B = (\lambda^2 - a - x_A - x_B, -(\lambda(\lambda^2 - a - x_A - x_B) + \mu)) \tag{2.2}$$

con

$$\lambda = \frac{y_B - y_A}{x_B - x_A}\ ,\ \mu = y_A - \lambda x_A = y_B - \lambda x_B \qquad \text{se } B \neq \pm A$$
$$\lambda = \frac{f'(x_A)}{2y_A}\ ,\ \mu = y_A - \lambda x_A \qquad \text{se } B = A \text{ e } y_A \neq 0$$

In particolare se $A = B$ vale la cosiddetta formula di duplicazione*:*

$$x_{2A} = \frac{x_A^4 - 2bx_A^2 - 8cx_A + b^2 - 4ac}{4(x_A^3 + ax_A^2 + bx_A + c)} \tag{2.3}$$

Dimostrazione. Sia $B \neq -A$ (quindi in particolare $B \neq A$ con $y_A = 0$); allora la retta $\langle A, B\rangle$ non è del tipo $x = k$.
Scriviamo $A * B = (x_C, -y_C)$, $A + B = O * (A * B) = (x_C, y_C)$, e cerchiamo $(x_C, -y_C)$ come terzo punto di intersezione fra $\mathscr{C}$ e $\langle A, B\rangle$; se $B \neq \pm A$ e quindi $x_B - x_A \neq 0$, $\langle A, B\rangle$ ha equazione:

$$y = \lambda x + \mu \quad \text{con} \quad \lambda = \frac{y_B - y_A}{x_B - x_A}\ ,\ \mu = y_A - \lambda x_A = y_B - \lambda x_B.$$

La risolvente di $\mathscr{C} \cap \langle A, B\rangle$ è quindi

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\mu)x + (c - \mu^2) = 0\ ,$$

dove il polinomio al primo membro ha come radici x_A, x_B, x_C, quindi si può scrivere come

$$x^3 - (x_A + x_B + x_C)x^2 + (x_Ax_B + x_Ax_C + x_Bx_C)x - x_Ax_Bx_C\ .$$

Pertanto $a - \lambda^2 = -(x_A + x_B + x_C)$, da cui

$$x_C = \lambda^2 - a - x_A - x_B \quad , \quad y_C = -(\lambda x_C + \mu).$$

Se $B = A$ con $y_A \neq 0$, le coordinate per $2A$ si ottengono considerando la tangente in A a $\mathscr{C}$: posto $F = y^2 - f(x)$, questa ha equazione

$$\left.\frac{\partial F}{\partial x}\right|_A (x - x_A) + \left.\frac{\partial F}{\partial y}\right|_A (y - y_A) = 0$$

ovvero

$$-f'(x_A)(x - x_A) + 2y_A(y - y_A) = 0$$

che riscriviamo come

$$y = \frac{f'(x_A)}{2y_A}(x - x_A) + y_A \ .$$

Ponendo $\lambda = \dfrac{f'(x_A)}{2y_A}$, $\mu = y_A - \lambda x_A$ e intersecando con $\mathscr{C}$ risulta come prima $x_{2A} = \lambda^2 - a - 2x_A$, cioè

$$\begin{aligned} x_{2A} &= \frac{(3x_A^2 + 2ax_A + b)^2}{(2y_A)^2} - a - 2x_A = \\ &= \frac{(3x_A^2 + 2ax_A + b)^2}{4(x_A^3 + ax_A^2 + bx_A + c)} - a - 2x_A = \\ &= \frac{x_A^4 - 2bx_A^2 - 8cx_A + b^2 - 4ac}{4(x_A^3 + ax_A^2 + bx_A + c)}. \end{aligned}$$

□

Osservazione 2.2.c. Le formule trovate ci permettono di sommare quasi tutte le possibili coppie di punti di $\mathscr{C}$; sono escluse le coppie del tipo (A, O), $(A, -A)$ e (A, A) con $y_A = 0$. I primi due casi sono banali, e il terzo è un caso particolare del secondo, infatti $y_A = 0$ equivale a $A = -A$, quindi $2A = A - A = O$.

***Esempio* 2.1.** È estremamente facile implementare le formule (2.2) su un calcolatore; per un esempio di codice per Matlab/Octave si rimanda all'appendice A (vedi `somma`).
Dato $A = (3, 8)$ su $\mathscr{C} : y^2 = x^3 - 43x + 166$, proviamo a calcolare $2A$, $4A$, $8A$; usando `somma`, basta dare i comandi

```
A=[3,8] ; a=0 ; b=-43 ;
dA=somma(A,A,a,b);
qA=somma(dA,dA,a,b);
oA=somma(qA,qA,a,b);
```

e si trovano i punti

$$2A = (-5, -16) \quad , \quad 4A = (11, 32) \quad , \quad 8A = (3, 8) = A \ .$$

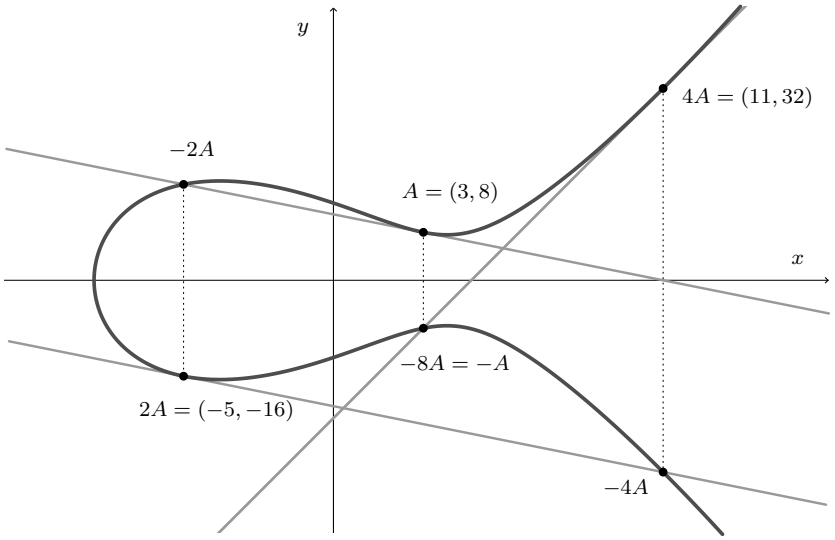


Figura 2.4. Rappresentazione della cubica nel piano reale affine (la scala usata per gli assi è $x : y = 1 : 5$).

2.3 Punti di ordine finito m: i casi $m = 2$ e $m = 3$

Notazione 3. Nel seguito, se $a \in \mathbb{R}$, $a > 0$, la scrittura $\sqrt{a}$ indicherà, com'è consueto, la radice quadrata positiva di a; se $a \in \mathbb{R}$, $a < 0$ oppure $a \in \mathbb{C} \setminus \mathbb{R}$, $\sqrt{a}$ denoterà una (fissata) radice quadrata complessa di a, e l'altra verrà indicata con $-\sqrt{a}$.

Ricordiamo che dato un gruppo $(G, +, 0)$, un elemento $a \in G$ ha ordine finito m se $\exists k \geq 0$ intero tale che $ka = 0$ e m è il più piccolo naturale con questa proprietà; se $ka \neq 0 \ \forall k \in \mathbb{N} \setminus \{0\}$, si dice che a ha ordine infinito.
Abbiamo già incontrato elementi di ordine finito in $(\mathscr{C}, +, O)$: nella cubica dell'esempio precedente, $A = (3, 8)$ era tale che $8A = A$, quindi $7A = O$; in una cubica liscia qualsiasi in forma normale, se $A = (x_A, 0)$, allora $A = -A$, quindi $2A = O$.
Sappiamo anche che, dato un gruppo abeliano G e fissato $m > 0$ intero, l'insieme $\{a \in G \mid ma = 0\}$ è un sottogruppo di G (il nucleo dell'applicazione $a \mapsto ma$). Iniziamo allora a guardare come sono fatti questi sottogruppi nel caso di $(\mathscr{C}, +, O)$; per $m = 2$ e 3 si ha il seguente:

Teorema 2.3.1. *In $\mathbb{P}^2(\mathbb{C})$, sia $\mathscr{C} : y^2 = f(x)$ con $f(x) = x^3 + ax^2 + bx + c$ una cubica non singolare in forma normale, e si consideri il gruppo $(\mathscr{C}, +, O)$ con $O = [0, 0, 1]$. Allora*

(i) *un punto $A = (x_A, y_A) \in \mathscr{C}$, $A \neq O$, ha ordine 2 $\Leftrightarrow$ $y_A = 0$*

(ii) *$\mathscr{C}$ contiene esattamente 4 punti di ordine k, con $k|2$, e questi costituiscono un sottogruppo Γ_2 di $\mathscr{C}$ isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$*

(iii) *un punto $A = (x_A, y_A) \in \mathscr{C}$, $A \neq O$, ha ordine 3 $\Leftrightarrow$ x_A è radice del polinomio*

$$p(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) \tag{2.4}$$

(iv) *$\mathscr{C}$ contiene esattamente 9 punti di ordine k, con $k|3$, e questi costituiscono un sottogruppo Γ_3 di $\mathscr{C}$ isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_3$.*

Dimostrazione.

(i) Abbiamo già visto che, se $A \neq O$, $2A = O \Leftrightarrow A = -A \Leftrightarrow y_A = -y_A \Leftrightarrow y_A = 0$.

(ii) I punti $A = (x_A, y_A)$ tali che $y_A = 0$ sono tutti e soli quelli per cui x_A è radice di $f(x)$. Nell'osservazione 1.3.a abbiamo visto che le radici α_1, α_2, α_3 di questo polinomio sono distinte, altrimenti $\mathscr{C}$ sarebbe singolare; per (i) si hanno quindi tre punti di ordine 2, dati da

$$A_1 = (\alpha_1, 0)\ ,\ A_2 = (\alpha_2, 0)\ ,\ A_3 = (\alpha_3, 0).$$

Dunque l'insieme $\Gamma_2 = \{O, A_1, A_2, A_3\}$ (dove abbiamo aggiunto O che ha ovviamente ordine $1|2$) contiene tutti e soli i punti A tali che $2A = O$, quindi è sottogruppo di $(\mathscr{C}, +, O)$; poiché ha ordine 4 e contiene solo elementi di ordine al più 2, è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ [J, teorema 3.13].

(iii) Mostriamo anzitutto che, se $A \neq O$, vale $3A = O \Leftrightarrow x_{2A} = x_A$. Infatti $3A = O \Rightarrow 2A = -A \Rightarrow x_{2A} = x_{-A} = x_A$; viceversa se $x_{2A} = x_A$, allora $2A = \pm A$, e poiché $A \neq O$ deve essere $2A = -A$, quindi $3A = O$.
Ricordando che x_{2A} è dato dalla formula (2.3), x_A sarà soluzione dell'equazione

$$x = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)} \tag{2.5}$$

ovvero, moltiplicando ambo i membri per il denominatore (che sarà $\neq 0$ in

x_A dato che A non ha ordine 2) e svolgendo i calcoli:

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0 \tag{2.6}$$

Quindi $3A = O \Leftrightarrow p(x_A) = 0$, dove p è il polinomio al primo membro di (2.6).

(iv) Per prima cosa, occorre mostrare che p ha quattro radici distinte $\alpha_1, ..., \alpha_4 \in \mathbb{C}$; queste corrisponderanno ai punti

$$\begin{gathered}\{(\alpha_1, \pm\beta_1),\ (\alpha_2, \pm\beta_2),\ (\alpha_3, \pm\beta_3),\ (\alpha_4, \pm\beta_4)\} \\ \beta_i = \sqrt{f(\alpha_i)} \quad i = 1, ..., 4\end{gathered} \tag{2.7}$$

che per (iii) sono tutti e soli i punti di ordine 3.
Per mostrare che gli α_i sono distinti, facciamo vedere che p e p' non hanno radici in comune; scrivendo la formula di duplicazione come

$$x_{2A} = \frac{f'(x_A)^2}{4f(x_A)} - a - 2x_A$$

l'equazione (2.5) diventa

$$x = \frac{f'(x)^2}{4f(x)} - a - 2x$$

cioè, essendo $f(x) \neq 0$ perché A non ha ordine 2,

$$4f(x)x + 4f(x)(a + 2x) - f'(x)^2 = 0$$

da cui

$$\begin{aligned} p(x) &= 4f(x)(3x + a) - f'(x)^2 \\ &= 2f(x)f''(x) - f'(x)^2. \end{aligned} \tag{2.8}$$

Se p ha una radice α di molteplicità ≥ 2, questa deve essere anche radice di

$$\begin{aligned} p'(x) &= 2f(x)f'''(x) + 2f'(x)f''(x) - 2f'(x)f''(x) \\ &= 2f(x)f'''(x) = 12f(x) \end{aligned} \tag{2.9}$$

Pertanto se α è una radice di $p(x)$ e $p'(x)$, per la (2.8), α deve essere

necessariamente anche radice di $f(x)$ e di $f'(x)$, ma sappiamo che questo non è possibile perché $\mathscr{C}$ è liscia.
Poiché non può essere $\beta_i = 0$ per qualche i, i punti (2.7) sono tutti distinti, e l'insieme

$$\Gamma_3 = \{O, (\alpha_1, \pm\beta_1),\ (\alpha_2, \pm\beta_2),\ (\alpha_3, \pm\beta_3),\ (\alpha_4, \pm\beta_4)\}\ ,$$

dato da tutti e soli i punti tali che $3A = O$, contiene esattamente 9 elementi. Infine, dato che Γ_3 contiene solo punti di ordine 1 o 3, non è ciclico e deve quindi essere isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_3$ (si veda [J, teorema 3.13]). □

Vediamo cosa succede se anziché studiare i punti di ordine finito su $\mathbb{C}$ li studiamo su $\mathbb{R}$ o su $\mathbb{Q}$.

Corollario 2.3.2. *Nelle notazioni precedenti*

(a) • *se a, b, $c \in \mathbb{R}$, l'insieme*

$$\{A = (x_A, y_A) \in \mathscr{C} \mid x_A, y_A \in \mathbb{R}\ ,\ 2A = O\} \cup \{O\}$$

è un sottogruppo di Γ_2 isomorfo a $\mathbb{Z}_2$ oppure a $\mathbb{Z}_2 \times \mathbb{Z}_2$;

• *se a, b, $c \in \mathbb{Q}$, l'insieme*

$$\{A = (x_A, y_A) \in \mathscr{C} \mid x_A, y_A \in \mathbb{Q}\ ,\ 2A = O\} \cup \{O\}$$

è il gruppo nullo, oppure è un sottogruppo di Γ_2 isomorfo a $\mathbb{Z}_2$ o a $\mathbb{Z}_2 \times \mathbb{Z}_2$

(b) • *se $a, b, c \in \mathbb{R}$, l'insieme*

$$\{A = (x_A, y_A) \in \mathscr{C} \mid x_A, y_A \in \mathbb{R}\ ,\ 3A = O\} \cup \{O\}$$

è un sottogruppo di Γ_3 isomorfo a $\mathbb{Z}_3$;

• *se $a, b, c \in \mathbb{Q}$, l'insieme*

$$\{A = (x_A, y_A) \in \mathscr{C} \mid x_A, y_A \in \mathbb{Q}\ ,\ 3A = O\} \cup \{O\}$$

è il gruppo nullo, oppure è isomorfo a $\mathbb{Z}_3$.

Dimostrazione. La prima affermazione di (a) segue immediatamente dal punto (ii) del teorema precedente e dal fatto che $f(x)$, polinomio a coefficienti reali, può avere una o tre radici reali; analogamente la seconda segue da (ii), osservando che f (a coefficienti razionali) può avere zero, una oppure 3 radici razionali.
Mostriamo ora la (b); abbiamo visto che i punti di ordine 3 hanno come ascissa le radici del polinomio $p(x)$ dato da (2.4): cerchiamo quindi di capire quali di queste radici sono reali studiando l'andamento di $p(x)$ come funzione di una variabile reale. I punti estremanti di $p(x)$ si trovano cercando le radici di (vedi (2.9))

$$p'(x) = 12f(x)$$

quindi se $\bar{x}$ è una sua radice reale, questa è certamente punto estremante per $p(x)$, perché non può essere radice anche di $p''(x) = 12f'(x)$ (vedi osservazione 1.3.a). Se ho solo una radice reale (figura 2.5), questa corrisponde necessariamente ad un minimo assoluto, perché $p(x) \xrightarrow[x\to\pm\infty]{} +\infty$. Se tutte e 3 le radici sono reali (figura 2.6), sempre perché $p(x) \xrightarrow[x\to\pm\infty]{} +\infty$, queste corrisponderanno a due minimi e un massimo relativi per p. Inoltre, se $\bar{x}$ è una radice reale di p' (quindi $p'(\bar{x}) = 12f(\bar{x}) = 0$), si ha per (2.8)

$$p(\bar{x}) = 2f(\bar{x})f''(\bar{x}) - f'(\bar{x})^2 = -f'(\bar{x})^2 < 0\ .$$

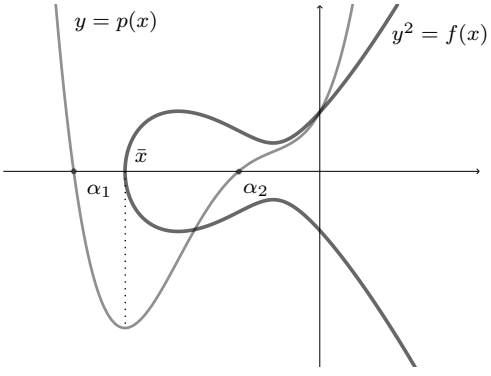


Figura 2.5

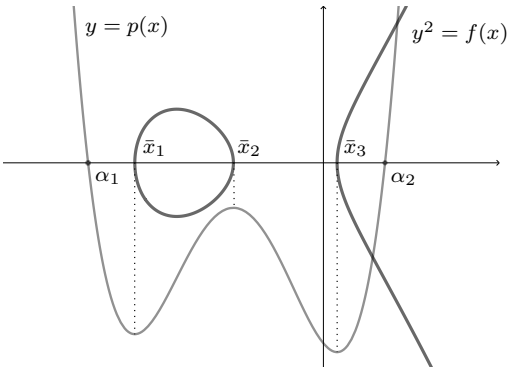


Figura 2.6

In definitiva, per le proprietà dei punti estremanti e per il teorema di Bolzano, p ha esattamente due radici reali α_1, α_2 con $\alpha_1 < \alpha_2$. Infine, in un intorno di α_1, p è decrescente (perché $p(x) \xrightarrow[x\to-\infty]{} +\infty$), quindi $f(\alpha_1) = \frac{p'(\alpha_1)}{12} < 0$; analogamente, in un intorno di α_2, p è crescente, dunque $f(\alpha_2) = \frac{p'(\alpha_2)}{12} > 0$.

Quindi solo $\pm\sqrt{f(\alpha_2)} \in \mathbb{R}$, ovvero su $\mathscr{C}$ ho esattamente due punti reali di ordine 3

$$A = (\alpha_2, \sqrt{f(\alpha_2)}) \quad , \quad B = (\alpha_2, -\sqrt{f(\alpha_2)})$$

e questi costituiscono, insieme a O, un sottogruppo ciclico di ordine 3 di Γ_3.
Infine se a, b, c sono razionali, si può ripetere lo stesso ragionamento fatto sopra, osservando che se $\alpha_2 \in \mathbb{R} \setminus \mathbb{Q}$ o $f(\alpha_2)$ non è un quadrato in $\mathbb{Q}$, l'insieme indicato conterrà solo O. □

***Esempio* 2.2.** Determiniamo i sottogruppi

$$\Gamma_2 = \{A \in \mathscr{C} \mid 2A = O\} \quad , \quad \Gamma_3 = \{A \in \mathscr{C} \mid 3A = O\}$$

in $\mathscr{C} : y^2 = x^3 + 4x$.
Gli elementi di Γ_2 diversi da O sono i punti (x_A, y_A) con $y_A = 0$ o, equivalentemente, x_A radice di $x^3 + 4x$, ovvero

$$A_1 = (0, 0) \ , \quad A_2 = (2i, 0) \ , \quad A_3 = (-2i, 0).$$

Un isomorfismo fra $\mathbb{Z}_2 \times \mathbb{Z}_2$ e Γ_2 potrebbe essere

$$\begin{array}{ll} (0,0) \longleftrightarrow O & (0,1) \longleftrightarrow A_2 \\ (1,1) \longleftrightarrow A_1 & (1,0) \longleftrightarrow A_3. \end{array}$$

Gli elementi di Γ_3 diversi da O hanno come ascisse le radici di

$$p(x) = 3x^4 + 24x^2 - 16 \ ,$$

e sono i punti (nella notazione 3):

$$A = \left(\sqrt{-4 + \frac{8\sqrt{3}}{3}} \ , \ \frac{4\sqrt{3}}{3} \sqrt[4]{-3 + 2\sqrt{3}} \right) \qquad B = -A$$

$$C = \left(\sqrt{-4 - \frac{8\sqrt{3}}{3}} \ , \ \frac{4\sqrt{-3i}}{3} \sqrt[4]{3 + 2\sqrt{3}} \right) \qquad D = -C$$

$$E = \left(-\sqrt{-4 + \frac{8\sqrt{3}}{3}} \ , \ \frac{4i\sqrt{3}}{3} \sqrt[4]{-3 + 2\sqrt{3}} \right) \qquad F = -E$$

$$G = \left(-\sqrt{-4 - \frac{8\sqrt{3}}{3}}\ ,\ \frac{4\sqrt{3i}}{3}\sqrt[4]{3+2\sqrt{3}} \right) \qquad H = -G$$

Si verifica poi che l'applicazione definita da:

$$\begin{array}{llll} A \longmapsto (1,0) & C \longmapsto (0,1) & E \longmapsto (1,2) & G \longmapsto (2,2) \\ B \longmapsto (2,0) & D \longmapsto (0,2) & F \longmapsto (2,1) & H \longmapsto (1,1) \\ O \longmapsto (0,0) & & & \end{array}$$

è un isomorfismo fra Γ_3 e $\mathbb{Z}_3 \times \mathbb{Z}_3$.
Osserviamo infine che solo A e B sono punti a coordinate reali, e insieme a O costituiscono un sottogruppo ciclico di Γ_3 di ordine 3.

2.3.1 Proprietà geometriche dei punti di ordine 3

Osservazione 2.3.a. Ricordiamo che un punto di flesso per una cubica piana $\mathscr{D}$ è un punto non singolare P tale che, se t è la tangente alla curva in P, si ha

$$i(\mathscr{D}, t, P) \geq 3\ .$$

Se $\mathscr{D}$ è una cubica, questa condizione diventa quindi $i(\mathscr{D}, t, P) = 3$.
Pertanto in $(\mathscr{C}, +, O)$ vale $3A = O \Leftrightarrow A$ è punto di flesso per $\mathscr{C}$, infatti

$$3A = O \quad \Leftrightarrow \quad 2A = -A \quad \Leftrightarrow \quad -(A * A) = -A \quad \Leftrightarrow \quad A * A = A.$$

Analiticamente, si può vedere così: i punti di flesso della cubica liscia $\mathscr{C}$: $F(x_0, x_1, x_2) = 0$ sono i punti che questa ha in comune con la curva di equazione $\det H(x_0, x_1, x_2) = 0$ (vedi [Se, pp.416-418]), dove $F(x_0, x_1, x_2)$ è l'omogeneizzato di $f(x) - y^2$ (vedi notazione 2) e H è la matrice hessiana:

$$H = \begin{pmatrix} \frac{\partial^2 F}{\partial x_0^2} & \frac{\partial^2 F}{\partial x_0 \partial x_1} & \frac{\partial^2 F}{\partial x_0 \partial x_2} \\ \frac{\partial^2 F}{\partial x_1 \partial x_0} & \frac{\partial^2 F}{\partial x_1^2} & \frac{\partial^2 F}{\partial x_1 \partial x_2} \\ \frac{\partial^2 F}{\partial x_2 \partial x_0} & \frac{\partial^2 F}{\partial x_2 \partial x_1} & \frac{\partial^2 F}{\partial x_2^2} \end{pmatrix} = \begin{pmatrix} 2bx_1 + 6cx_0 & 2ax_1 + 2bx_0 & -2x_2 \\ 2ax_1 + 2bx_0 & 6x_1 + 2ax_0 & 0 \\ -2x_2 & 0 & -2x_0 \end{pmatrix} ;$$

nel nostro caso è

$$\begin{aligned}\det H(x_0, x_1, x_2) =& 4((2a^2 - 6b)x_0x_1^2 + (2ab - 18c)x_0^2x_1 + \\ &+ (2b^2 - 6ac)x_0^3 - 6x_1x_2^2 - 2ax_0x_2^2).\end{aligned}$$

Una soluzione al sistema

$$\begin{cases} \det H(x_0, x_1, x_2) = 0 \\ F(x_0, x_1, x_2) = 0 \end{cases}$$

la conosciamo già, ed è $[0, 0, 1]$, l'unico punto di $\mathscr{C}$ sulla retta $x_0 = 0$. Lavoriamo allora sul sistema deomogeneizzato

$$\begin{cases} (2a^2 - 6b)x^2 + (2ab - 18c)x + (2b^2 - 6ac) - 6xy^2 - 2ay^2 = 0 \\ y^2 = x^3 + ax^2 + bx + c \end{cases};$$

sostituendo y^2 nella prima equazione e svolgendo i calcoli si trova

$$-12bx^2 - 24cx + 2b^2 - 8ac - 6x^4 - 8ax^3 = 0\ ,$$

dove al primo membro ho proprio il polinomio p definito in (2.4) moltiplicato per una costante; poiché le sue radici corrispondono a tutti e soli i punti di ordine 3, vale l'asserto.

L'osservazione appena fatta e il punto (iv) del teorema 2.3.1 provano quindi il seguente

Teorema 2.3.3. *Una cubica liscia di $\mathbb{P}^2(\mathbb{C})$ ha esattamente 9 flessi.*

La configurazione dei 9 flessi di una cubica liscia è molto particolare:

Teorema 2.3.4. *Se una retta contiene due dei nove flessi di cubica liscia di $\mathbb{P}^2(\mathbb{C})$, allora ne contiene anche un terzo.*

Dimostrazione. Consideriamo $(\mathscr{C}, +, O)$, e siano $A \neq O$, $B \neq O$, $B \neq A, 2A$ due flessi; allora $|A| = |B| = 3$ per l'osservazione 2.3.a, e A e B sono generatori per

$$\Gamma_3 = \{O\ ,\ A\ ,\ B\ ,\ 2A\ ,\ 2B\ ,\ A + B\ ,\ 2A + B\ ,\ A + 2B\ ,\ 2A + 2B\}\ .$$

Presi quindi due flessi distinti, questi si possono scrivere come

$$\begin{matrix} mA+nB \\ sA+tB \end{matrix} \qquad \text{con } \ 0 \leq m,n,s,t \leq 2 \ , \ (m,n) \neq (s,t) \ ;$$

si ha

$$(mA+nB)+(sA+tB)+(3-m-s)A+(3-n-t)B = O$$

pertanto i 3 punti distinti

$$mA+nB \quad , \quad sA+tB \quad , \quad (3-m-s)A+(3-n-t)B$$

sono allineati. □

Capitolo 3

Il gruppo dei punti razionali

Definizione 3.0.5. Diremo che una curva $\mathscr{D}$ di $\mathbb{P}^2(\mathbb{C})$ è razionale se è possibile scrivere un'equazione $F(x_0, x_1, x_2) = 0$ per $\mathscr{D}$ con F polinomio omogeneo a coefficienti in $\mathbb{Q}$. Diremo anche che un punto $A = [a_0, a_1, a_2]$ è razionale se le sue coordinate sono proporzionali ad una terna di numeri razionali (anzi, interi).

Osservazione 3.0.b. Se una retta è razionale, possiede certamente infiniti punti razionali, infatti $r : ax_0 + bx_1 + cx_2 = 0$ con $a, b, c \in \mathbb{Q}$ contiene i punti del tipo $[qb, -qa - cd, d]$, con $q, d \in \mathbb{Q}$. Questo non vale già più nel caso delle coniche, ad esempio $x_0^2 + x_1^2 + x_2^2 = 0$ ha solo punti non reali se vista in $\mathbb{P}^2(\mathbb{C})$, nessun punto in $\mathbb{P}^2(\mathbb{R})$ o $\mathbb{P}^2(\mathbb{Q})$. Tuttavia è sempre possibile [ST, pp.14-15] stabilire se una conica proiettiva razionale ha punti razionali.
Il caso delle cubiche è più complicato; si può dimostrare che esistono cubiche razionali senza, con un numero finito o con un numero infinito di punti razionali (vedi sezione 3.5), ma ancora non si è trovato un metodo che permetta di determinare se una cubica qualsiasi ne possiede almeno uno.
Nel seguito quindi, quando considereremo una cubica non singolare, supporremo sempre che abbia almeno un punto razionale.

Proposizione 3.0.6. *Sia $\mathscr{C}$ una cubica liscia razionale di $\mathbb{P}^2(\mathbb{C})$, e supponiamo che $\mathscr{C}$ abbia un punto razionale O. Sia poi*

$$\mathscr{C}(\mathbb{Q}) = \{A = [a_0, a_1, a_2] \in \mathscr{C} \mid a_i \in \mathbb{Q}\}$$

l'insieme dei punti razionali di $\mathscr{C}$; allora $\mathscr{C}(\mathbb{Q})$ è un sottogruppo di $(\mathscr{C}, +, O)$.

Dimostrazione. Siano $A, B \in \mathscr{C}(\mathbb{Q})$; mostriamo che $A+B = O*(A*B) \in \mathscr{C}(\mathbb{Q})$. Anzitutto, $\langle A, B\rangle$ è una retta razionale perché passa per A, B razionali; inoltre, poiché la risolvente di $\mathscr{C} \cap \langle A, B\rangle$ è un'equazione di terzo grado a coefficienti in $\mathbb{Q}$ e ha 2 soluzioni razionali, anche la terza deve essere tale. Quindi $(A*B) \in \mathscr{C}(\mathbb{Q})$, e per un ragionamento analogo anche $O*(A*B) \in \mathscr{C}$. □

3.1 Cubiche razionali in forma normale

Osservazione 3.1.a. Vorremmo ora studiare il sottogruppo $\mathscr{C}(\mathbb{Q})$ in $(\mathscr{C}, +, O)$ usando le formule per la somma descritte nella proposizione 2.2.3, le quali erano definite a partire da un'equazione in forma normale della cubica.
Si può provare che se $\mathscr{C}$ è una cubica liscia razionale, studiare il gruppo $(\mathscr{C}, +, O)$ equivale a studiare $(\mathscr{C}', +, O')$, dove $\mathscr{C}'$ è un'opportuna cubica razionale in forma normale, ovvero

$$\mathscr{C}' : y^2 = x^3 + ax^2 + bx + c \quad , \quad a, b, c \in \mathbb{Q} \, ,$$

e O' è un opportuno punto razionale di $\mathscr{C}'$. Non diamo la dimostrazione completa di questo fatto ma mostriamo come si può determinare $\mathscr{C}'$, accennando ai risultati teorici che giustificano il nostro ragionamento.
Osserviamo intanto che se O è punto di flesso, si può procedere come nella dimostrazione al teorema 1.3.1: come prima proiettività scegliamo una Φ che porti O in $[0, 0, 1]$, la sua tangente (che sarà una retta razionale) in $x_0 = 0$ e un punto razionale non sulla tangente in un altro punto razionale $\notin x_0 = 0$. Risulta $\Phi \in PGL_2(\mathbb{Q})$, così $\Phi(\mathscr{C})$ è ancora razionale. Tutte le altre trasformazioni usate nella dimostrazione suddetta si possono scrivere come proiettività a coefficienti in $\mathbb{Q}$, e danno in effetti un'equazione per $\mathscr{C}$ in forma normale e a coefficienti in $\mathbb{Q}$.
Supponiamo ora che O non sia un flesso, e sia P il terzo punto di intersezione della tangente di O con $\mathscr{C}$; scriviamo l'equazione di $\mathscr{C} : F(x_0, x_1, x_2) = 0$, con

$$\begin{aligned} F(x_0, x_1, x_2) =& a_0x_0^3 + a_1x_1^3 + a_2x_2^3 + a_3x_0^2x_1 + a_4x_0^2x_2 + a_5x_0x_1^2 + \\ &+ a_6x_0x_2^2 + a_7x_1^2x_2 + a_8x_1x_2^2 + a_9x_0x_1x_2 \end{aligned} \tag{3.1}$$

e derivate parziali non tutte nulle in un punto, nel sistema di riferimento in cui $O = [0, 1, 0]$, $x_0 = 0$ è la tangente a $\mathscr{C}$ in O, P=[0,0,1], $x_1 = 0$ è la tangente a $\mathscr{C}$ in P.
Vale $F(0, 1, 0) = a_1$, $F(0, 0, 1) = a_2$, quindi deve essere $a_1 = a_2 = 0$ dato che O e P appartengono a $\mathscr{C}$.
Le tangenti a $\mathscr{C}$ in O e P hanno equazione rispettivamente

$$r : a_5x_0 + 3a_1x_1 + a_7x_2 = 0$$
$$t : a_6x_0 + a_8x_1 + 3a_2x_2 = 0$$

e devono coincidere con le rette $x_0 = 0$ e $x_1 = 0$, quindi $a_6 = a_7 = 0$, $a_5 \neq 0$, $a_8 \neq 0$. L'equazione (3.1) diventa quindi

$$\mathscr{C} : a_0x_0^3 + a_3x_0^2x_1 + a_4x_0^2x_2 + \underset{\neq 0}{a_5x_0x_1^2} + \underset{\neq 0}{a_8x_1x_2^2} + a_9x_0x_1x_2 = 0 \ .$$

Deomogeneizzando rispetto ad x_0, con $x = \frac{x_1}{x_0}$ e $y = \frac{x_2}{x_0}$, e dividendo tutto per $a_8 \neq 0$ si trova

$$\mathscr{C} : xy^2 + (\beta x + \gamma)y = \alpha x^2 + \delta x + \varepsilon \ ,$$

dove $\beta = \frac{a_9}{a_8}$, $\gamma = \frac{a_4}{a_8}$, $\alpha = -\frac{a_5}{a_8} \neq 0$, $\delta = -\frac{a_3}{a_8}$, $\varepsilon = -\frac{a_0}{a_8}$.
Consideriamo ora la trasformazione (definita su $\{X \neq 0\}$):

$$\begin{cases} x = & X \\ y = & \dfrac{Y}{X} \end{cases} ;$$

tramite questa si può definire una corrispondenza (definita quasi dappertutto), che è una *mappa birazionale* (vedi [R, 5.6, 5.8]) fra $\mathscr{C}$ e la cubica

$$Y^2 + (\beta X + \gamma)Y = \alpha X^3 + \delta X^2 + \varepsilon X \qquad (**)$$

la quale si dirà appunto *birazionalmente equivalente* a $\mathscr{C}$. Da qui possiamo procedere usando l'affinità

$$\begin{cases} X = X' \\ Y = Y' - \dfrac{\beta}{2}X' - \dfrac{\gamma}{2} \end{cases}$$

che ci dà

$$(Y')^2 = -\frac{1}{4}(\beta X' + \gamma)^2 + \alpha(X')^3 + \delta(X')^2 + \varepsilon X' \ ;$$

poi, essendo $\alpha \neq 0$, usiamo ancora l'affinità

$$\begin{cases} X' = \alpha x \\ Y' = \alpha^2 y \end{cases}$$

e dividiamo tutto per α^4: si ottiene così l'equazione in forma normale di una cubica $\mathscr{C}''$ birazionalmente equivalente a $\mathscr{C}$,

$$\mathscr{C}'' : y^2 = x^3 + ax^2 + bx + c \ .$$

Certo $\mathscr{C}''$ è razionale, infatti tutti i coefficienti di ogni equazione ricavata sono funzioni razionali dei coefficienti della cubica $\mathscr{C}$ di partenza, che era razionale.
Per le proprietà delle mappe birazionali, sappiamo che $\mathscr{C}''$ deve essere una cubica irriducibile; inoltre $\mathscr{C}''$ è liscia: questo si vede considerando il genere geometrico della curva, che è un invariante birazionale e vale 1 per le cubiche lisce (mentre è zero per le cubiche singolari irriducibili).
Infine, i gruppi $(\mathscr{C}, +, O)$ e $(\mathscr{C}'', +, O'')$, dove O'' è il punto all'infinito di $\mathscr{C}''$, sono isomorfi; infatti è possibile dimostrare che la mappa birazionale fra $\mathscr{C}$ e $\mathscr{C}''$ si può estendere in modo unico ad un isomorfismo di varietà proiettive [H, I.6.8]; d'altra parte $\mathscr{C}$ e $\mathscr{C}''$ sono curve ellittiche, su cui possiamo dare la legge di gruppo senza che questa dipenda dall'immersione delle curve in $\mathbb{P}^2(\mathbb{C})$; così un isomorfismo di varietà è anche isomorfismo di gruppi [H, IV.4.9].

Tenendo conto di questo, da ora studieremo la legge di gruppo su una cubica razionale $\mathscr{C}$ con almeno un punto razionale e in forma normale.

Osservazione 3.1.b. Se $\mathscr{C}$ è una cubica liscia razionale,

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx + c \quad , \qquad a,\, b,\, c \in \mathbb{Q} \ ,$$

e $d \in \mathbb{Z}$ è non nullo, usando l'affinità

$$\begin{cases} x = \frac{X}{d^2} \\ y = \frac{Y}{d^3} \end{cases}$$

e moltiplicando tutto per d^6 si trova un'equazione per $\mathscr{C}$

$$\mathscr{C} : Y^2 = X^3 + d^2aX^2 + d^4bX + d^6c$$

che sarà a coefficienti interi se d è abbastanza grande (ad esempio, si può prendere il minimo comune multiplo dei denominatori di a, b, c).

Nel seguito considereremo quindi

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx + c \quad , \quad a, b, c \in \mathbb{Z} \, . \tag{3.2}$$

3.2 Il discriminante di $x^3 + ax^2 + bx + c$

Il primo risultato notevole che vorremmo mostrare su $\mathscr{C}(\mathbb{Q})$, con $\mathscr{C}$ data da (3.2), è il teorema di Nagell-Lutz (vedi 3.4.6), il quale afferma che in questo gruppo gli elementi di ordine finito hanno coordinate affini intere; per questo introduciamo anzitutto il concetto di *discriminante* di $f(x) = x^3 + ax^2 + bx + c$ e studiamo la sua relazione con la curva $\mathscr{C} : y^2 = f(x)$.

Definizione 3.2.1. Sia $f \in \mathbb{Z}[x]$, $f(x) = x^3 + ax^2 + bx + c$; si definisce il *discriminante* di f la quantità:

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \ \in \mathbb{Z}.$$

Proposizione 3.2.2. *Sia $f \in \mathbb{Z}[x]$, $f(x) = x^3 + ax^2 + bx + c$, e siano α_1, α_2, $\alpha_3 \in \mathbb{C}$ le sue radici; sono equivalenti*

(a) *D è il discriminante di f*

(b) $D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$

(c) $D = r(x)f(x) + s(x)f'(x)$ *con*

$$r(x) = (18b - 6a^2)x - (4a^3 - 15ab + 27c) \ \in \mathbb{Z}[x]$$
$$s(x) = (2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2) \ \in \mathbb{Z}[x]$$

Dimostrazione. Mostriamo $(a) \Leftrightarrow (b)$; vale

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

$$= x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3$$

così $a = -(\alpha_1 + \alpha_2 + \alpha_3)$, $b = (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)$, $c = -\alpha_1\alpha_2\alpha_3$. Ora si tratta di svolgere alcuni calcoli; si ha

$$\begin{aligned}
&(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = \\
&\quad =(\alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2)(\alpha_1^2 - 2\alpha_1\alpha_3 + \alpha_3^2)(\alpha_2^2 - 2\alpha_2\alpha_3 + \alpha_3^2) \\
&\quad =\alpha_1^4\alpha_2^2 + \alpha_1^4\alpha_3^2 + \alpha_1^2\alpha_2^4 + \alpha_1^2\alpha_3^4 + \alpha_2^4\alpha_3^2 + \alpha_2^2\alpha_3^4 - \\
&\qquad - 2(\alpha_1^4\alpha_2\alpha_3 + \alpha_1\alpha_2^4\alpha_3 + \alpha_1\alpha_2\alpha_3^4) - 2(\alpha_1^3\alpha_2^3 + \alpha_1^3\alpha_3^3 + \alpha_2^3\alpha_3^3) + \\
&\qquad + 2(\alpha_1^3\alpha_2^2\alpha_3 + \alpha_1^3\alpha_2\alpha_3^2 + \alpha_1^2\alpha_2^3\alpha_3 + \alpha_1^2\alpha_2\alpha_3^3 + \alpha_1\alpha_2^3\alpha_3^2 + \alpha_1\alpha_2^2\alpha_3^3) - 6\alpha_1^2\alpha_2^2\alpha_3^2 \\
&\quad =(*)
\end{aligned}$$

ed anche

$$\begin{aligned}
D &= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \\
&= -4(\alpha_1 + \alpha_2 + \alpha_3)^3\alpha_1\alpha_2\alpha_3 + (\alpha_1 + \alpha_2 + \alpha_3)^2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^2 + \\
&\quad + 18(\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)\alpha_1\alpha_2\alpha_3 - \\
&\quad - 4(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^3 - 27(\alpha_1\alpha_2\alpha_3)^2 = (*)\ ,
\end{aligned}$$

come volevamo.
Mostriamo ora $(a) \Leftrightarrow (c)$. Nel prodotto

$$\begin{aligned}
&r(x)f(x) + s(x)f'(x) = \\
&\quad =\big((18b - 6a^2)x - (4a^3 - 15ab + 27c)\big)(x^3 + ax^2 + bx + c) + \\
&\qquad + \big((2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2)\big)(3x^2 + 2ax + b)
\end{aligned}$$

tutti gli addendi in cui compare una potenza di x si elidono fra loro, e rimane

$$r(x)f(x) + s(x)f'(x) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = D. \qquad \square$$

Osservazione 3.2.a. La proprietà (b) ci dice che il discriminante è non nullo se e solo se f non ha radici multiple, cioè se e solo se la cubica $\mathscr{C} : y^2 = f(x)$ è liscia. La proprietà (c) invece può anche essere letta così: D appartiene all'ideale in $\mathbb{Z}[x]$ generato da $f(x)$ e $f'(x)$.

Proposizione 3.2.3. *Sia $\mathscr{C} : y^2 = f(x)$ una cubica liscia razionale, con*

$$f(x) = x^3 + ax^2 + bx + c \quad , \quad a, b, c \in \mathbb{Z} \, ,$$

sia D il discriminante di f, e sia $A = (x_A, y_A) \in \mathscr{C}$ tale che $A \neq O$ e $2A \neq O$ hanno coordinate intere. Allora $y_A \mid D$.

Dimostrazione. Poiché per ipotesi $A \neq O$ e $2A \neq O$, il che equivale a $y_A \neq 0$ (vedi teorema 2.3.1), ha senso scrivere $2A = (x_{2A}, y_{2A})$. Per la proposizione 2.2.3, vale la formula

$$x_{2A} = \lambda^2 - a - 2x_A \quad , \quad \text{con} \;\; \lambda = \frac{f'(x_A)}{2y_A}$$

dove a, x_A, x_{2A} sono interi, quindi anche λ^2 lo è; questo significa che $\lambda = \frac{f'(x_A)}{2y_A}$ (che certo è razionale), è pure intero $\implies y_A \mid f'(x_A)$. Poiché $y_A^2 = f(x_A)$, vale anche $y_A \mid f(x_A)$. Per la (c) della proposizione 3.2.2, y_A divide anche

$$D = r(x_A)f(x_A) + s(x_A)f'(x_A) \, ,$$

da cui l'asserto (si osservi che $r(x_A)$, $s(x_A)$, $f(x_A)$, $f'(x_A) \in \mathbb{Z}$). □

3.3 Le coordinate dei punti di $\mathscr{C}(\mathbb{Q})$

Mettendo una cubica razionale in forma normale, si scopre una proprietà cruciale dei punti di $\mathscr{C}(\mathbb{Q})$; per parlarne introduciamo il concetto di *ordine rispetto ad un primo p* di un numero razionale.

Definizione 3.3.1. Sia $p > 0$ un primo fissato, e sia $a \in \mathbb{Q} \setminus \{0\}$,

$$a = \frac{m}{n} p^\nu \, , \; \text{con } m, n, \nu \in \mathbb{Z} \, , \; n > 0 \;\; \text{e} \;\; (m, n) = (m, p) = (n, p) = 1 \, .$$

L'intero ν si dice *ordine di a rispetto a p* (lo indicheremo con $\mathrm{ord}_p(a)$ o semplicemente $\mathrm{ord}(a)$), ed è ben definito $\forall a \in \mathbb{Q}$ non nullo. Infatti, se $a \neq 0$ è un razionale qualsiasi, sono uniche le scritture

$$a = \frac{m'}{n'} \;\; \text{con } (m', n') = 1 \, , \; n' > 0$$
$$m' = \mathrm{sign}(a) \cdot p_{i_1}^{\alpha_1} \cdot \ldots \cdot p_{i_t}^{\alpha_t}$$

$$n' = p_{j_1}^{\beta_1} \cdot ... \cdot p_{j_s}^{\beta_s}$$

con p_{i_k}, p_{j_h} primi, $a_k, \beta_h > 0$ per $k = 1, ..., t$, $h = 1, ..., s$. Quindi se $p \mid m'$, p coincide con uno dei p_{i_k}, ad esempio p_{i_1}, e posto $m = \text{sign}(a) \cdot p_{i_2}^{\alpha_2} \cdot ... \cdot p_{i_t}^{\alpha_t}$, $n = n'$, $\nu = \alpha_1$, si ha $a = \frac{m}{n} p^{\nu}$; se $p \mid n'$, $p = p_{j_1}$, allora si pone $m = m'$, $n = p_{j_2}^{\beta_2} \cdot ... \cdot p_{j_s}^{\beta_s}$, $\nu = -\beta_1$; se $p \nmid m'$, $p \nmid n'$, allora $m = m'$, $n = n'$, $\nu = 0$. In ogni caso, m, n, ν sono interi univocamente determinati e sono tali che $(m, n) = (m, p) = (n, p) = 1$, $n > 0$.
Osserviamo inoltre che $\forall r_1, r_2 \in \mathbb{Q} \setminus \{0\}$, valgono

$$\text{ord}(r_1 r_2) = \text{ord}(r_1) + \text{ord}(r_2) \ , \ \text{ord}\left(\frac{1}{r_1}\right) = -\text{ord}(r_1) \ .$$

Proposizione 3.3.2. *Sia $\mathscr{C}$ la cubica di equazione*

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx + c \quad , \quad a, b, c \in \mathbb{Z} \ ,$$

$O = [0, 0, 1]$, e siano $P = (x, y)$ un punto razionale di $\mathscr{C}$, p un primo fissato. Vale

$$\text{ord}_p(x) < 0 \Leftrightarrow \text{ord}_p(y) < 0$$

cioè p divide il denominatore di $x \Leftrightarrow$ divide il denominatore di y, e in tal caso esiste $\nu > 0$ tale che

$$\text{ord}_p(x) = -2\nu \ , \ \text{ord}_p(y) = -3\nu \ . \tag{3.3}$$

Dimostrazione. Scriviamo anzitutto

$$x = \frac{m}{np^{\mu}} \quad , \quad y = \frac{u}{wp^{\sigma}}$$

dove p non divide m, n, u, w.
Sostituendo x e y nell'equazione di $\mathscr{C}$ si trova

$$\begin{aligned} \frac{u^2}{w^2 p^{2\sigma}} &= \frac{m^3}{n^3 p^{3\mu}} + a\frac{m^2}{n^2 p^{2\mu}} + b\frac{m}{np^{\mu}} + c \\ &= \frac{m^3 + am^2 np^{\mu} + bmn^2 p^{2\mu} + cn^3 p^{3\mu}}{n^3 p^{3\mu}} \ . \end{aligned}$$

Proviamo che $\mathrm{ord}_p(x) < 0 \implies \mathrm{ord}_p(y) < 0$, e che in queste ipotesi valgono le (3.3).
Sia dunque $\mu > 0$; si ha

$$\begin{aligned} & p \mid (am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}) \quad , \quad p \nmid m^3 \\ \implies & \quad p \nmid (m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}) \\ \implies & \mathrm{ord}\left(\frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}\right) = -3\mu \ . \end{aligned}$$

Inoltre

$$p \nmid u^2 \ , \ p \nmid w^2 \implies \mathrm{ord}\left(\frac{u^2}{w^2p^{2\sigma}}\right) = -2\sigma$$

pertanto $3\mu = 2\sigma$; in particolare, anche $\sigma > 0$.
Infine $2 \mid 3\mu \Rightarrow 2 \mid \mu$, cioè $\exists \nu > 0$ intero tale che $\mu = 2\nu$, da cui si ha anche $\sigma = 3\nu$.
Proviamo ora che $\mathrm{ord}_p(y) < 0$ implica $\mathrm{ord}_p(x) < 0$. Sia quindi $\sigma > 0$; siccome $p \nmid n^3$ e

$$\mathrm{ord}\left(\frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}\right) = \mathrm{ord}\left(\frac{u^2}{w^2p^{2\sigma}}\right) = -2\sigma < 0 \ ,$$

deve essere $\mu > 0$ perché se fosse $\mu \leq 0$, si avrebbe $p^{-3\mu}$, $p^{-2\mu}$, $p^{-\mu} \in \mathbb{Z}$, e

$$\frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}} = \frac{m^3p^{-3\mu} + am^2np^{-2\mu} + bmn^2p^{-\mu} + cn^3}{n^3} \ ,$$

che ha ordine rispetto a p certamente ≥ 0. Ragionando come sopra, sarà anche $3\mu = 2\sigma$. □

3.4 Punti di ordine finito

3.4.1 I sottogruppi $\mathscr{C}(p^\nu)$

La proposizione 3.3.2 ci dice che se $P = (x, y)$ è un punto razionale di $\mathscr{C}$ (ma non a coordinate intere), possiamo sempre trovare p primo e $\nu > 0$ intero tali che

$$x = \frac{m}{np^{2\nu}} \ , \ y = \frac{u}{wp^{3\nu}} \ .$$

Allora, l'idea per mostrare il teorema di Nagell-Lutz consiste nel far vedere che non esistono p e ν siffatti per i punti razionali di ordine finito; introduciamo dunque la seguente notazione.

Definizione 3.4.1. Siano p primo, $\nu > 0$ intero, $\mathscr{C} : y^2 = x^3 + ax^2 + bx + c$, $a, b, c \in \mathbb{Z}$. Poniamo

$$\mathscr{C}(p^\nu) \coloneqq \{(x, y) \in \mathscr{C}(\mathbb{Q}) \mid \mathrm{ord}_p(x) \leq -2\nu \ , \ \mathrm{ord}_p(y) \leq -3\nu\} \cup \{O\}$$

ovvero l'insieme dei punti di $\mathscr{C}(\mathbb{Q})$ della forma

$$(x, y) = \left(\frac{m}{np^{2\nu+h}}, \frac{u}{wp^{3\nu+k}}\right) \qquad h, k \geq 0$$

più l'elemento neutro O; per la proposizione precedente gli elementi di $\mathscr{C}(p^\nu)$ possono essere scritti come

$$(x, y) = \left(\frac{m}{np^{2(\nu+i)}}, \frac{u}{wp^{3(\nu+i)}}\right)$$

per qualche $i \in \mathbb{N}$. Valgono poi le inclusioni:

$$\mathscr{C}(\mathbb{Q}) \supseteq \mathscr{C}(p) \supseteq \mathscr{C}(p^2) \supseteq ... \supseteq \mathscr{C}(p^\nu) \supseteq ...$$

È bene osservare che $\mathscr{C}(p^\nu)$ dipende dal rifermento scelto.
Inoltre, indicheremo con R_p (o semplicemente R) l'insieme

$$R_p \coloneqq \{x \in \mathbb{Q} \mid \mathrm{ord}_p(x) \geq 0\} \cup \{0\}$$

cioè l'insieme dei numeri razionali, scritti come in 3.3.1, tali che p non compare al loro denominatore; si vede subito che R_p è un sottoanello di $\mathbb{Q}$, e gli elementi invertibili rispetto al prodotto sono della forma $x = \frac{m}{n}$ con $(m, p) = (n, p) = 1$.
Se ν è un intero > 0, scriviamo

$$p^\nu R = \{x \in \mathbb{Q} \mid \mathrm{ord}_p(x) \geq \nu\} \ .$$

Proposizione 3.4.2. *Nelle notazioni precedenti, per ogni primo p e per ogni intero $\nu > 0$, $\mathscr{C}(p^\nu)$ è sottogruppo di $(\mathscr{C}(\mathbb{Q}), +, O)$.*

Dimostrazione. Siano p un primo fissato, ν un intero fissato, $\nu > 0$.
Vogliamo mostrare che dati due punti di $\mathscr{C}(p^\nu)$, la somma appartiene ancora a $\mathscr{C}(p^\nu)$; occorrerà quindi studiare le coordinate dei punti.
Anzitutto, effettuiamo un cambiamento di coordinate affini: passiamo prima a coordinate omogenee, con $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$, per cui

$$\mathscr{C} : x_0 x_2^2 = x_1^3 + a x_0 x_1^2 + b x_0^2 x_1 + c x_0^3 \tag{3.4}$$

e deomogeneizziamo poi rispetto a x_2, ponendo

$$t = \frac{x_1}{x_2} \ , \ s = \frac{x_0}{x_2} \ ;$$

si ottiene così l'equazione affine

$$\mathscr{C} : s = t^3 + a t^2 s + b t s^2 + c s^3 \ . \tag{3.5}$$

Quindi stiamo considerando su $\mathbb{P}^2(\mathbb{C}) \setminus (\{x_0 = 0\} \cup \{x_2 = 0\})$ il cambiamento di coordinate

$$\begin{cases} x = \frac{t}{s} \\ y = \frac{1}{s} \end{cases} \quad \text{ovvero} \quad \begin{cases} t = \frac{x}{y} \\ s = \frac{1}{y} \end{cases} \ .$$

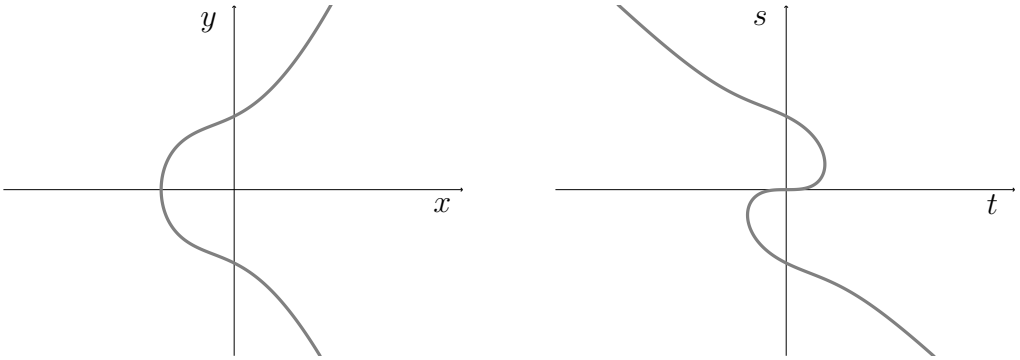


Figura 3.1. Rappresentazione della cubica $\mathscr{C} : x_0 x_2^2 = x_1^3 + a x_0 x_1^2 + b x_0^2 x_1 + c x_0^3$ nei piani affini xy e ts (qua $a = b = c = 1$; osserviamo che $\mathscr{C}$ è non singolare, infatti $y^2 = x^3 + x^2 + x + 1$ è tale che $x^3 + x^2 + x + 1 = (x+1)(x^2+1)$, che ha tre radici distinte in $\mathbb{C}$). Vedi appendice A.

Nel piano ts, O è l'origine, e i punti all'infinito di $\mathscr{C}$ sono quelli che giacciono sulla retta $x_2 = 0$ del piano proiettivo (la retta $y = 0$ nel piano xy), cioè i punti di ordine 2 per quanto detto nella proposizione 2.3.1. Questi non appartengono a $\mathscr{C}(p^\nu)$ (se stanno in $\mathscr{C}(\mathbb{Q})$, le loro ascisse nel piano xy sono le radici razionali di $f(x)$, quindi sono della forma $\frac{m}{n}$, con $m \mid c$, $n \mid 1$, ovvero sono intere). Pertanto nel piano ts troviamo in effetti tutti i punti che ci interessano.

Ovviamente, la legge di gruppo rimane la stessa (il riferimento proiettivo è lo stesso), e se A ha coordinate (x_A, y_A) rispetto al piano xy, (t_A, s_A) rispetto al piano ts (quindi ha coordinate omogenee $[1, x_A, y_A]$), risulta

$$A = (t_A, s_A) = \left(\frac{x_A}{y_A}, \frac{1}{y_A}\right) \implies -A = \left(\frac{x_A}{-y_A}, \frac{1}{-y_A}\right) = (-t_A, -s_A)\ . \tag{3.6}$$

Sia ora $A \in \mathscr{C}(p^\nu)$; per qualche $i \geq 0$, si ha

$$(x_A, y_A) = \left(\frac{m}{np^{2(\nu+i)}}, \frac{u}{wp^{3(\nu+i)}}\right) \implies (t_A, s_A) = \left(\frac{mw}{nu}p^{\nu+i}, \frac{w}{u}p^{3(\nu+i)}\right)$$

Inoltre m, n, u, w sono tutti primi con p, quindi

$$\mathrm{ord}(t_A) = \nu + i > 0\ ,\ \mathrm{ord}(s_A) = 3(\nu+i) > 0 \implies t_A \in p^\nu R\ ,\ s_A \in p^{3\nu}R\ .$$

Viceversa, se un punto $A \in \mathscr{C}$ ha coordinate (t_A, s_A) nel piano affine ts date da

$$t_A = \frac{m'}{n'}p^{\nu+h} \in p^\nu R\ ,\ s_A = \frac{u'}{w'}p^{3\nu+k} \in p^{3\nu}R \qquad h, k \geq 0$$

nel piano xy avrà coordinate

$$x_A = \frac{t_A}{s_A} = \frac{m'w'}{n'u'p^{2\nu+k-h}}\ ,\ y_A = \frac{1}{s_A} = \frac{w'}{u'p^{3\nu+k}}\ ;$$

in particolare $\mathrm{ord}(y_A) < 0$, quindi per la proposizione 3.3.2 anche $\mathrm{ord}(x_A) < 0$, ed esistono m, n, u, $w \in \mathbb{Z}$ primi con p, $\exists \nu' \geq \nu > 0$ intero tali che $n > 0$, $w > 0$ e

$$(x_A, y_A) = \left(\frac{m}{np^{2\nu'}}, \frac{u}{wp^{3\nu'}}\right) \in \mathscr{C}(p^{\nu'}) \subseteq \mathscr{C}(p^\nu)\ .$$

Quindi vale:

$$A = (x_A, y_A) \in \mathscr{C}(p^\nu) \iff t_A \in p^\nu R\ ,\ s_A \in p^{3\nu}R\ .$$

Siano ora $A = (x_A, y_A)$, $B = (x_B, y_B) \in \mathscr{C}(p^\nu)$, $A+B = (x_C, y_C)$, e indichiamo con (t_A, s_A), (t_B, s_B), (t_C, s_C) le rispettive coordinate nel piano ts; per quanto detto sopra, sarà

$$A + B = (x_C, y_C) \in \mathscr{C}(p^\nu) \quad \iff \quad t_C \in p^\nu R\ ,\ s_C \in p^{3\nu}R\ .$$

Calcoliamo allora t_C, s_C tenendo presente che, per (3.6), vale

$$A + B = O * (A * B) = -(A * B) = -(-t_C, -s_C) = (t_C, s_C) \ .$$

Osserviamo prima che se $A \neq B$ sono due punti di $\mathscr{C}$ tali che $t_A = t_B$, allora vale $\frac{x_A}{y_A} = \frac{x_B}{y_B} =$ costante, e A e B appartengono alla retta $y = kx$, dove $\frac{1}{k} = \frac{x_A}{y_A} = \frac{x_B}{y_B}$, oppure alla retta $x = 0$. Nel secondo caso $\mathscr{C} \cap \{x = 0\}$ è dato da $\{(0, \sqrt{c}) \, , \, (0, -\sqrt{c})\}$; se $c \geq 0$ e $\sqrt{c} \in \mathbb{Q}$, allora $\sqrt{c} \in \mathbb{Z}$ dato che c è intero, e i due punti non appartengono a $\mathscr{C}(p^\nu)$; se $c < 0$, i punti non sono neanche razionali. Altrimenti, $\mathscr{C} \cap \{y = kx\}$ dà

$$k^2x^2 = x^3 + ax^2 + bx + c \implies x^3 + (a - k^2)x^2 + bx + c = 0 \ ;$$

questa equazione può avere zero, una o tre soluzioni in $\mathbb{Q}$ (non può averne solo due). Mostriamo che in quest'ultimo caso due soluzioni non danno punti nello stesso $\mathscr{C}(p^\nu)$ per qualche p fissato. Infatti, se fosse

$$\begin{gathered} x_A = \frac{m}{n} p^{-2(\nu+i)} \ , \ x_B = \frac{m'}{n'} p^{-2(\nu+j)} \\ m, n, m', n' \in \mathbb{Z} \ , \ (m, n) = (m', n') = 1 \ , \\ (m, p) = (n, p) = (m', p) = (n', p) = 1 \ , \end{gathered}$$

cioè $A, B \in \mathscr{C}(p^\nu)$, posto $x_C = \frac{h}{u}$, con $(h, u) = 1$, si avrebbe

$$-c = x_A x_B x_C = \frac{mm'}{nn'} p^{-4\nu-2i-2j} \frac{h}{u} \ \in \mathbb{Z}$$

quindi $p^{4\nu+2i+2j} \mid h$.
D'altro canto

$$\begin{aligned} b &= x_A x_B + x_A x_C + x_B x_C \\ &= \frac{mm'}{nn'} p^{-4\nu-2i-2j} + \frac{m}{n} p^{-2(\nu+i)} \frac{h}{u} + \frac{m'}{n'} p^{-2(\nu+j)} \frac{h}{u} \\ &= \frac{mm'u + mn'hp^{2(\nu+j)} + m'nhp^{2(\nu+i)}}{nn'up^{4\nu+2i+2j}} \in \mathbb{Z} \ ; \end{aligned}$$

dunque $p^{4\nu+2i+2j} \mid (mm'u + mn'hp^{2(\nu+j)} + m'nhp^{2(\nu+i)})$, e siccome divide gli ultimi due addendi, deve dividere anche $mm'u$. Ma $(m, p) = (m', p) = 1$, quindi

$p^{4\nu+2i+2j} \mid u$, contro l'ipotesi $(h,u)=1$.
In definitiva, in $\mathscr{C}(p^\nu)$ non si hanno mai due elementi distinti A, B tali che $t_A = t_B$.

Questo ci lascia con due sole possibilità:
Caso 1: $A \neq B$, $t_A \neq t_B$.
La retta per A, B nel piano ts ha equazione

$$\langle A,B\rangle : s = \alpha t + \beta \qquad \text{con } \alpha = \frac{s_B - s_A}{t_B - t_A}\ ,\ \beta = s_A - \alpha t_A$$

Usando la (3.5) possiamo scrivere

$$\begin{aligned} s_B - s_A &= (t_B^3 - t_A^3) + a(t_B^2 s_B - t_A^2 s_A) + b(t_B s_B^2 - t_A s_A^2) + c(s_B^3 - s_A^3) \\ &= (t_B^3 - t_A^3) + a\big((t_B^2 - t_A^2)s_B + t_A^2(s_B - s_A)\big) + \\ &\quad + b\big((t_B - t_A)s_B^2 + t_A(s_B^2 - s_A^2)\big) + c(s_B^3 - s_A^3) \\ &= (t_B - t_A)\big((t_A^2 + t_A t_B + t_B^2) + a(t_A + t_B)s_B + b s_B^2\big) + \\ &\quad + (s_B - s_A)\big(a t_A^2 + b t_A(s_A + s_B) + c(s_A^2 + s_A s_B + s_B^2)\big) \\ &= (t_B - t_A)\alpha_1 + (s_B - s_A)\alpha_2 \end{aligned}$$

con

$$\begin{aligned} \alpha_1 &= (t_A^2 + t_A t_B + t_B^2) + a(t_A + t_B)s_B + b s_B^2 \\ \alpha_2 &= a t_A^2 + b t_A(s_A + s_B) + c(s_A^2 + s_A s_B + s_B^2) \end{aligned}$$

da cui

$$\frac{s_B - s_A}{t_B - t_A} = \frac{\alpha_1}{1 - \alpha_2}$$

cioè

$$\alpha = \frac{\alpha_1}{1-\alpha_2} = \frac{(t_A^2 + t_A t_B + t_B^2) + a(t_A + t_B)s_B + b s_B^2}{1 - (a t_A^2 + b t_A(s_A + s_B) + c(s_A^2 + s_A s_B + s_B^2))}\ . \tag{3.7}$$

Caso 2: $A = B$.
Considero l'equazione omogenea per $\mathscr{C}$ data da (3.4); la tangente per $A = (t_A, s_A)$ ha equazione

$$\left.\frac{\partial F}{\partial x_0}\right|_A x_0 + \left.\frac{\partial F}{\partial x_1}\right|_A x_1 + \left.\frac{\partial F}{\partial x_2}\right|_A x_2 = 0\ .$$

Svolgendo i calcoli, nel piano affine ts risulta

$$s = \frac{(3t_A^2 + 2at_As_A + bs_A^2)t - 2s_A}{(1 - at_A^2 - 2bt_As_A - 3cs_A^2)} \ ;$$

osserviamo che il coefficiente angolare di questa retta coincide con la quantità all'ultimo membro di (3.7) quando $t_A = t_B$, $s_A = s_B$, quindi possiamo usare sempre la (3.7).
Calcoliamo le coordinate di $A * B = (-t_C, -s_C)$ in questi due casi; sostituendo $s = \alpha t + \beta$ nell'equazione (3.5) si trova

$$\begin{aligned} \alpha t + \beta &= t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3 \\ &= t^3 + a\alpha t^3 + a\beta t^2 + b\alpha^2 t^3 + 2b\alpha\beta t^2 + b\beta^2 t + c\alpha^3 t^3 + 3c\alpha^2\beta t^2 + \\ &\quad + 3c\alpha t\beta^2 + c\beta^3 \\ \implies \qquad 0 &= (1 + a\alpha + b\alpha^2 + c\alpha^3)t^3 + (a\beta + 2b\alpha\beta + 3c\alpha^2\beta)t^2 + \\ &\quad + (b\beta^2 + 3c\alpha\beta^2 - \alpha)t + c\beta^3 - \beta \ . \end{aligned}$$

Per un ragionamento già visto, vale

$$t_A + t_B - t_C = -\frac{\overbrace{(a\beta + 2b\alpha\beta + 3c\alpha^2\beta)}^{K_1}}{\underbrace{1 + a\alpha + b\alpha^2 + c\alpha^3}_{K_2}} =: K \ .$$

Per quanto detto sopra, vale $t_A, t_B \in p^\nu R$, $s_A, s_B \in p^{3\nu} R$; cerchiamo allora di capire com'è fatto K.
Dalla (3.7) sappiamo che $1 - \alpha_2$ ha ordine rispetto a p pari a zero (cioè è un'unità in R), mentre α_1 ha ordine $\geq 2\nu \implies \alpha \in p^{2\nu} R$. Vale poi $\beta = s_A - \alpha t_A \in p^{3\nu} R$. Pertanto K_2 è anch'esso un'unità in R, e K_1 è un elemento di $p^{3\nu} R$, da cui si conclude $K \in p^{3\nu} R$

$$\implies \qquad \begin{aligned} t_C &= \ t_A + t_B - K \ \in p^\nu R \\ s_C &= \ \alpha t_C - \beta \ \in p^{3\nu} R \end{aligned}$$

$\implies (A + B) \in \mathscr{C}(p^\nu)$. □

Dall'ultima parte della dimostrazione appena vista segue anche la:

Proposizione 3.4.3. *Nelle notazioni precedenti, l'applicazione*

$$\begin{aligned} \mathcal{T} : \mathscr{C}(p^\nu) &\longrightarrow {p^\nu R}/{p^{3\nu} R} \\ A &\longmapsto t_A + p^{3\nu} R \end{aligned}$$

è un omomorfismo di gruppo, il cui nucleo è $\mathscr{C}(p^{3\nu})$.

Dimostrazione. Si osservi che $O \mapsto [t_O] = [0]$, e se $A \neq O$, $t_A = \frac{x_A}{y_A}$.
Sopra abbiamo provato che $\forall A, B \in \mathscr{C}(p^\nu)$ vale

$$\begin{aligned} & t_A + t_B - t_{A+B} = K \ \in p^{3\nu} R \\ \Longrightarrow \quad & t_{A+B} \equiv t_A + t_B \mod p^{3\nu} R \,, \end{aligned} \tag{3.8}$$

dunque $\mathcal{T}$ è un omomorfismo. Il nucleo di $\mathcal{T}$ è

$$\ker(\mathcal{T}) = \{A \in \mathscr{C}(p^\nu) \mid t_A \in p^{3\nu} R\} \,;$$

d'altra parte si ha $t_A = \frac{x_A}{y_A} \in p^{3\nu} R \iff \mathrm{ord}_p(x_A) - \mathrm{ord}_p(y_A) \geq 3\nu$; poiché x_A e y_A sono della forma $x_A = \frac{m}{n} p^{-2(\nu+i)}$, $y_A = \frac{m'}{n'} p^{-3(\nu+i)}$, deve essere $-2\nu - 2i + 3\nu + 3i \geq 3\nu$, cioè $i \geq 2\nu$, da cui

$$\mathrm{ord}_p(x_A) \geq -2(\nu + 2\nu) = -2(3\nu) \implies A \in \mathscr{C}(p^{3\nu}) \,. \qquad \square$$

Vediamo ora un'altra proprietà dei sottogruppi $\mathscr{C}(p^\nu)$, che segue dalla proposizione precedente e dalla

Proposizione 3.4.4. *Sia p un primo fissato, $R = R_p$ l'anello definito in 3.4.1, siano $\sigma \geq \nu > 0$ degli interi. Allora* ${p^\nu R}/{p^\sigma R}$ *è ciclico di ordine* $p^{\sigma-\nu}$.

Dimostrazione. Nel seguito indichiamo con $\overline{p^\nu}$ la classe $p^\nu + p^\sigma R$; se $k \in \mathbb{Z}$, vale $\overline{kp^\nu} = k\overline{p^\nu}$. Anzitutto, $\overline{p^\nu}$ ha ordine $p^{\sigma-\nu}$, infatti

$$\begin{aligned} \langle \overline{p^\nu} \rangle &= \{k\overline{p^\nu} \ , \ k \in \mathbb{Z}\} \\ &= \Big\{ \overbrace{\underbrace{0, \ \overline{p^\nu}, \ \overline{2p^\nu}, \ldots}_{p}, \underbrace{\overline{p \cdot p^\nu}, \ \overline{(p+1)p^\nu}, \ldots}_{p}, \overline{(p+p)p^\nu}, \ldots, \overline{(p \cdot p)p^\nu}}^{p \cdot p}, \ldots \\ &\qquad \ldots, \overline{p^{\sigma-\nu-1} p^\nu}, \ldots, \overline{(p^{\sigma-\nu} - 1)p^\nu} \Big\} \end{aligned}$$

è costituito da $p^{\sigma-\nu}$ elementi distinti.
Mostriamo che ogni elemento di ${}^{p^\nu R}\!/_{p^\sigma R}$ si può scrivere come $k\overline{p^\nu}$ per qualche $k \in \mathbb{Z}$.
Prima osserviamo questo: in generale, se per due elementi vale la congruenza

$$\frac{m}{n}p^{\nu+h} \equiv \frac{m'}{n'}p^{\nu+\ell} \mod (p^\sigma R) \tag{3.9}$$

con $(m,p) = (n,p) = (m',p) = (n',p) = 1$ e $0 \leq \ell \leq h < \sigma - \nu$, allora

$$\frac{m}{n}p^{\nu+h} - \frac{m'}{n'}p^{\nu+\ell} = \frac{n'mp^{\nu+h} - nm'p^{\nu+\ell}}{nn'} = p^{\nu+\ell}\left(\frac{n'mp^{h-\ell} - nm'}{nn'}\right) \in p^\sigma R\,;$$

se fosse $h > \ell$, avrei $(n'mp^{h-\ell} - nm', p) = 1$, dunque

$$\operatorname{ord}_p\left(\frac{m}{n}p^{\nu+h} - \frac{m'}{n'}p^{\nu+\ell}\right) = \nu + \ell < \sigma$$

contro l'ipotesi. Quindi $h = \ell$, e poiché deve valere

$$\operatorname{ord}_p\left(\frac{m}{n}p^{\nu+h} - \frac{m'}{n'}p^{\nu+h}\right) \geq \sigma$$

sarà anche $n'm - nm' = qp^{\sigma-\nu-h}$ per qualche $q \in \mathbb{Z}$.
Viceversa, dati $\frac{m}{n}p^{\nu+h}$, $\frac{m'}{n'}p^{\nu+\ell} \in p^\nu R$ con $(m,p) = (n,p) = (m',p) = (n',p) = 1$, se

$$h = \ell \quad \text{e} \quad p^{\sigma-\nu-h} \mid (n'm - nm')\,,$$

si verifica subito che vale (3.9).
Sia dunque $b = \overline{\frac{m}{n}p^{\nu+h}} \in {}^{p^\nu R}\!/_{p^\sigma R}$, con $0 \leq h < \sigma - \nu$. Cerchiamo $k \in \mathbb{Z}$ tale che

$$\begin{aligned} &\frac{m}{n}p^{\nu+h} \equiv kp^\nu \mod p^\sigma R \iff \\ \iff \quad &\exists k' \in \mathbb{Z} \,:\, k = k'p^h,\ (k',p) = 1 \\ &\text{ed } \exists q \in \mathbb{Z} \,:\, m - k'n = qp^{\sigma-\nu-h} \end{aligned}$$

per quanto detto sopra.

Si tratta allora di risolvere l'equazione

$$k'n + qp^{\sigma-\nu-h} = m \qquad (*)$$

nelle incognite k' e q; vale $(n, p^{\sigma-\nu-h}) = 1$, quindi esistono soluzioni per $(*)$. Possiamo concludere pertanto che $\overline{p^\nu}$ genera ${}^{p^\nu R}\!/_{p^\sigma R}$, che è dunque ciclico di ordine $p^{\sigma-\nu}$. □

Corollario 3.4.5. *Sia p primo, $\nu > 0$ intero; allora ${}^{\mathscr{C}(p^\nu)}\!/_{\mathscr{C}(p^{3\nu})}$, con l'operazione indotta da quella su $\mathscr{C}$, è un gruppo ciclico di ordine p^σ per qualche $\sigma \in \mathbb{Z}$, $0 \leq \sigma \leq 2\nu$.*

Dimostrazione. Per la proposizione 3.4.3, l'applicazione

$$\begin{aligned} {}^{\mathscr{C}(p^\nu)}\!/_{\mathscr{C}(p^{3\nu})} &\longrightarrow {}^{p^\nu R}\!/_{p^{3\nu} R} \\ A + \mathscr{C}(p^{3\nu}) &\longmapsto t_A + p^{3\nu} R \end{aligned}$$

è un morfismo iniettivo di gruppi, cioè ${}^{\mathscr{C}(p^\nu)}\!/_{\mathscr{C}(p^{3\nu})}$ è isomorfo ad un sottogruppo di ${}^{p^\nu R}\!/_{p^{3\nu} R}$; per la proposizione 3.4.4, questo è ciclico di ordine $p^{2\nu}$, pertanto anche ${}^{\mathscr{C}(p^\nu)}\!/_{\mathscr{C}(p^{3\nu})}$ è ciclico, e di ordine che divide $p^{2\nu}$. □

3.4.2 I teoremi di Nagell-Lutz e di Mazur

Come già accennato, la costruzione dei sottogruppi $\mathscr{C}(p^\nu)$, ma anche la congruenza (3.8), costituiscono la chiave per dimostrare il seguente:

Teorema 3.4.6 (di Nagell-Lutz). *Sia $\mathscr{C} : y^2 = f(x)$ una cubica liscia razionale, con $f(x) = x^3 + ax^2 + bx + c$ e $a, b, c \in \mathbb{Z}$, e sia D il discriminante di $f(x)$. Se $A = (x_A, y_A)$ è un punto razionale di ordine finito di $(\mathscr{C}, +, O)$ diverso da O, allora ha coordinate intere; in tal caso vale $y_A = 0$ (che equivale ad $|A| = 2$) oppure $y_A \mid D$.*

Dimostrazione. Sia $A \in \mathscr{C}$ di ordine m, e supponiamo per assurdo che abbia coordinate razionali ma non intere, ovvero esiste p primo tale che $A \in \mathscr{C}(p)$. Sono possibili due casi:
Caso 1: $(m, p) = 1$. Anzitutto osserviamo che esiste $\nu > 0$ intero tale che $A \in$

$\mathscr{C}(p^\nu) \setminus \mathscr{C}(p^{\nu+1})$.
Applicando m volte la congruenza (3.8) con $t_A = t_B$, si trova

$$t_{mA} \equiv mt_A \mod p^{3\nu}R\,;$$

poiché $mA = O$, vale anche $t_{mA} = t_O = 0$. Quindi $mt_A \equiv 0 \mod p^{3\nu}R$, cioè $mt_A \in p^{3\nu}R$; ma m è un'unità in R, dunque $t_A \in p^{3\nu}R$, da cui segue, per la proposizione 3.4.3, $A \in \mathscr{C}(p^{3\nu})$. Però $3\nu > \nu + 1$, quindi $A \in \mathscr{C}(p^{\nu+1})$, contro l'ipotesi.
Caso 2: $p \mid m$. Scriviamo $m = pm'$, e consideriamo il punto $A' = m'A \neq O$. In $(\mathscr{C}, +, O)$, A' ha ordine p, e poiché $A \in \mathscr{C}(p)$ e $\mathscr{C}(p)$ è un gruppo, anche $A' \in \mathscr{C}(p)$.
Ragionando come sopra, esisterà $\nu > 0$ intero tale che $A' \in \mathscr{C}(p^\nu)$ e $A' \notin \mathscr{C}(p^{\nu+1})$; inoltre, sempre per la (3.8), vale

$$0 = t_O = t_{pA'} \equiv pt_{A'} \mod p^{3\nu}R\,,$$

cioè $\mathrm{ord}_p(pt_{A'}) = \mathrm{ord}_p(p) + \mathrm{ord}_p(t_{A'}) \geq 3\nu$, da cui $\mathrm{ord}_p(t_{A'}) \geq 3\nu - 1$. Per un ragionamento già visto, se $t_{A'} = \frac{x_{A'}}{y_{A'}}$ con $x_{A'} = \frac{m}{n}p^{-2(\nu+i)}$, $y_{A'} = \frac{m'}{n'}p^{-3(\nu+i)}$, m, n, m', n' primi con p, si ha

$$-2\nu - 2i + 3\nu + 3i \geq 3\nu - 1 \iff 2\nu - i - 1 \leq 0 \iff i \geq 2\nu - 1$$

quindi $\mathrm{ord}_p(x_{A'}) \geq -2(\nu + 2\nu - 1)$, cioè $A' \in \mathscr{C}(p^{3\nu-1})$. Ma $\nu \geq 1$, per cui $3\nu - 1 \geq \nu + 1$, assurdo.
In definitiva, se $A \in \mathscr{C}(\mathbb{Q})$ ha ordine finito, allora ha coordinate intere.
Più precisamente, se A ha ordine 2, cioè $2A = O$, $A \neq O$, allora per il teorema 2.3.1 si ha $y_A = 0$; se A ha ordine > 2, allora anche $2A \neq O$ ha ordine finito e coordinate intere per quanto appena provato; vale quindi la proposizione 3.2.3, ovvero $y_A \mid D$. □

Il teorema di Nagell-Lutz è particolarmente interessante perché ora, dati $f \in \mathbb{Z}[x]$, $f(x) = x^3 + ax^2 + bx + c$, e $\mathscr{C} : y^2 = f(x)$ una cubica liscia razionale, possiamo stilare una lista che comprenda tutti i punti razionali di ordine finito di $(\mathscr{C}, +, O)$.
Per i punti di ordine 2, come abbiamo visto, si calcolano le soluzioni intere al-

l'equazione $f(x) = 0$; per gli altri punti di ordine finito, basterà sostituire ad y i divisori del discriminante D nell'equazione di $\mathscr{C}$, e cercare le soluzioni intere dell'equazione così ottenuta.
Nota: Possono esistere punti $P \in \mathscr{C}$ a coordinate intere con $y \mid D$ e che non hanno ordine finito; questi si possono distinguere dai punti di ordine finito se si trova $k \in \mathbb{Z}$, $k > 0$, tale che kP è un punto razionale ma non intero. In tal caso infatti kP non può avere ordine finito per il teorema di Nagell-Lutz, dunque neanche P.

Osserviamo che i punti di ordine finito di $\mathscr{C}(\mathbb{Q})$ costituiscono un gruppo; questo vale in generale, infatti se G è un gruppo abeliano e $g, h \in G$ sono due elementi di ordine finito, allora $|-g| = |g| < \infty$, e se $m = \text{mcm}(|g|, |h|)$, vale $m(g+h) = 0$; pertanto $H = \{g \in G \mid |g| < \infty\}$ è sottogruppo di G.
In particolare quindi data $\mathscr{C} : y^2 = x^3 + ax^2 + bx + c$, si ha che

$$\Lambda(\mathscr{C}) \coloneqq \{P \in \mathscr{C}(\mathbb{Q}) \mid |P| < \infty\}$$

è sottogruppo di $(\mathscr{C}(\mathbb{Q}), +, O)$.
Il caso delle cubiche lisce è molto peculiare: anche se non saremo in grado di dare un cenno della dimostrazione, enunciamo ora un risultato significativo sulla struttura di $\Lambda(\mathscr{C})$.

Teorema 3.4.7 (di Mazur). *Sia $\mathscr{C}$ una cubica liscia razionale con almeno un punto razionale. Allora il sottogruppo $\Lambda(\mathscr{C})$ dei punti razionali di ordine finito è isomorfo a uno dei seguenti gruppi:*

(I) $\mathbb{Z}_n$, *con* $1 \leq n \leq 10$ *o* $n = 12$

(II) $\mathbb{Z}_2 \times \mathbb{Z}_{2n}$, *con* $1 \leq n \leq 4$.

Nota: In particolare, un punto razionale di ordine finito di $\mathscr{C}$ può avere al massimo ordine 12; questo può essere utile per dire quali punti, fra quelli determinati tramite il teorema di Nagell-Lutz, hanno ordine infinito: infatti se $P \in \mathscr{C}(\mathbb{Q})$ è tale che kP, pur essendo a coordinate intere, è $\neq O$ per ogni $k = 1, ..., 12$, possiamo concludere che P ha ordine infinito.

3.4.3 Esempi di calcolo del sottogruppo $\Lambda(\mathscr{C})$

Vediamo ora alcuni esempi in cui applichiamo il metodo dato dal teorema di Nagell-Lutz per la ricerca dei possibili punti razionali di ordine finito; a tal scopo sono stati realizzati alcuni codici Matlab/Octave riportati nell'appendice A (si veda in particolare `ord_fin` e `ordine`). Per ogni cubica considerata, riconosceremo poi la struttura di $\Lambda(\mathscr{C})$, che sarà una delle forme descritte dal teorema di Mazur. Per una lista di esempi di tutte le possibili forme di $\Lambda(\mathscr{C})$, si veda [K, p.133].

***Esempio* 3.1:** $\Lambda(\mathscr{C}) \cong \mathbb{Z}_6$.
Consideriamo la cubica liscia

$$\mathscr{C} : y^2 = x^3 + 1 \ ;$$

anzitutto, risolvendo $x^3 + 1 = 0$ troviamo come unico punto razionale di ordine 2 il punto $A = (-1, 0)$.
Il discriminante di $f(x) = x^3 + 1$ è $D = -27$, pertanto i valori possibili per y sono

$$\{\pm 1, \pm 3, \pm 9, \pm 27\} \ ;$$

si tratta allora di cercare le soluzioni intere alle equazioni:

$$\begin{aligned} x^3 = 0 \qquad & \text{per } y = \pm 1 \\ x^3 - 8 = 0 \qquad & \text{per } y = \pm 3 \\ x^3 - 80 = 0 \qquad & \text{per } y = \pm 9 \\ x^3 - 728 = 0 \qquad & \text{per } y = \pm 27 \ . \end{aligned}$$

Si trovano così i punti

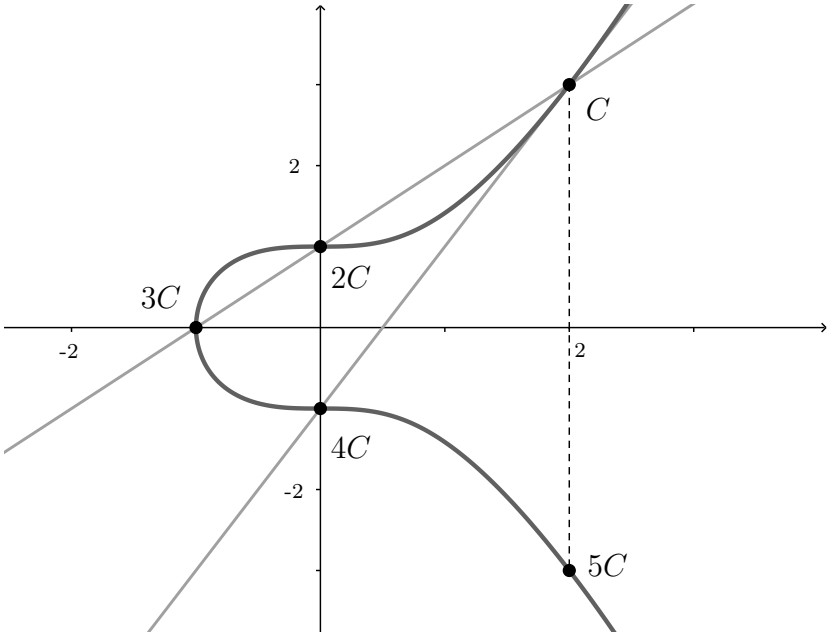
$$B = (0, 1) \ , \ C = (2, 3) \ , \ -B \ , \ -C \ ;$$

B e C hanno rispettivamente ordine 3 e 6, infatti

$$2C = (0, 1) = B \ , \ 3C = (-1, 0) = A \ , \ 4C = (0, -1) \ , \ 5C = (2, -3) \ , \ 6C = O \ .$$

Questi sono tutti e soli i punti razionali di ordine finito in $\mathscr{C}$, e costituiscono un

gruppo ciclico di ordine 6.



***Esempio* 3.2:** $\Lambda(\mathscr{C}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.
Per la cubica

$$\mathscr{C} : y^2 = x^3 + 2x^2 - 3x$$

vale $f(x) = x(x+3)(x-1)$, quindi $\mathscr{C}$ ha 3 punti razionali di ordine 2:

$$A = (0,0)\ ,\ B = (1,0)\ ,\ C = (-3,0)\ .$$

Il discriminante di f è $D = 144$, quindi questa volta non faremo un elenco di tutte le equazioni che occorre risolvere; però col calcolatore è facile verificare che solo per $y = \pm 2$ e $y = \pm 6$ si trovano soluzioni intere, che danno i punti

$$D = (-1,2)\ ,\ E = (3,6)\ ,\ -D\ ,\ -E.$$

Vale

$$2D = (1,0) = B \qquad 3D = (-1,-2) = -D$$
$$2E = (1,0) = B \qquad 3E = (3,-6) = -E$$

quindi D ed E hanno ordine 4. Abbiamo trovato che i punti razionali di ordine

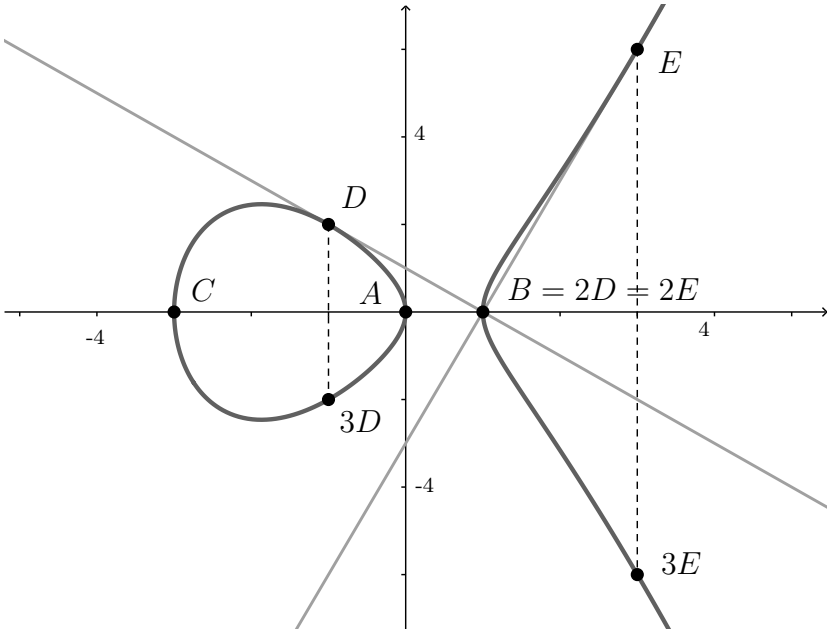
finito di $\mathscr{C}$ sono

$$\Lambda = \{A,\ B,\ C,\ D,\ E,\ -D,\ -E,\ O\}$$

e questi costituiscono un gruppo abeliano con 8 elementi, fra cui elementi di ordine 2 e di ordine 4, ma non di ordine 8: quindi il gruppo è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$. Si può verificare che

$$\begin{aligned} O &\longmapsto (0,0) & D &\longmapsto (0,1) \\ A &\longmapsto (1,0) & E &\longmapsto (1,1) \\ B &\longmapsto (0,2) & -D &\longmapsto (0,3) \\ C &\longmapsto (1,2) & -E &\longmapsto (1,3) \end{aligned}$$

è un isomorfismo di gruppi fra Γ e $\mathbb{Z}_2 \times \mathbb{Z}_4$.



***Esempio* 3.3:** $\Lambda(\mathscr{C}) \cong \{0\}$.

Consideriamo ora la cubica

$$\mathscr{C} : y^2 = x^3 + 5x^2 + 2x + 1\ ;$$

si verifica che $\mathscr{C}$ non ha punti razionali di ordine 2, e che ha discriminante $D =$

-279; per $y = \pm 1$ e $y = \pm 3$ si ottengono valori interi della x, e si trovano i punti:

$$A = (0,1)\ ,\ B = (1,3)\ ,\ C = (-2,3)\ ,\ D = (-4,3)\ ,\ -A\ ,\ -B\ ,\ -C\ ,\ -D\ .$$

Vale

$$\begin{aligned} 2A &= (-4,3) = D \\ 3A &= \left(-\frac{3}{4}, -\frac{11}{8}\right) \\ 4A &= 2D = \left(\frac{52}{9}, -\frac{521}{27}\right) \end{aligned}$$

così nè A nè $D = 2A$ possono avere ordine finito, perché se così fosse, anche $3A$ e $2D$ dovrebbero avere ordine finito, ma non hanno coordinate intere, contro il teorema di Nagell-Lutz.
Per i punti B e C si ha

$$2B = \left(-\frac{3}{4}, \frac{11}{8}\right)\ ,\ 2C = (0,-1) = -A$$

quindi, per lo stesso ragionamento sopra, anche B e C hanno ordine infinito. Osserviamo che, se avessimo iniziato da C, avremmo trovato

$$\begin{gathered} 2C = (0,-1) = -A\ ,\ 3C = (1,3) = B\ , \\ 4C = (-4,-3) = -D\ ,\ 5C = (10,-39)\ ,\ 6C = \left(-\frac{3}{4}, \frac{11}{8}\right) \end{gathered}$$

e sarebbe bastato questo per concludere che nessuno dei punti trovati ha ordine finito.

***Esempio* 3.4:** $\Lambda(\mathscr{C}) \cong \mathbb{Z}_8$.
La cubica

$$y^2 = x^3 + 49x^2 + 256x$$

ha come unico punto razionale di ordine 2 il punto $A = (0,0)$.
Il discriminante di f risulta

$$D = 90243072$$

e si trova che gli unici punti a coordinate intere che soddisfano $y \mid D$ sono

$$B = (-8, 24)\ ,\ C = (-32, 96)\ ,\ D = (16, 144)\ ,\ -B\ ,\ -C\ ,\ -D\ .$$

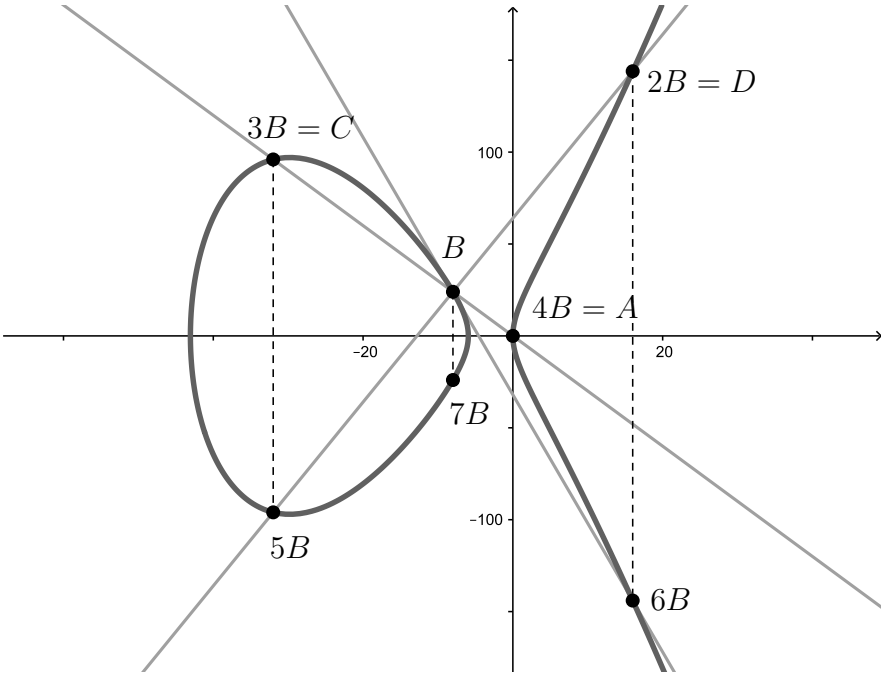
Cerchiamo l'ordine di B:

$$2B = (16, 144) = D\ ,\ 3B = (-32, 96) = C\ ,\ 4B = (0, 0) = A$$
$$5B = (-32, -96) = -C\ ,\ 6B = (16, -144) = -D\ ,\ 7B = (-8, -24) = -B\ .$$

Così B e C hanno ordine 8, D ha ordine 4, e i punti razionali di ordine finito di $\mathscr{C}$

$$\{O\ ,\ A\ ,\ B\ ,\ C\ ,\ D\ ,\ -B\ ,\ -C\ ,\ -D\}$$

costituiscono un gruppo ciclico isomorfo a $\mathbb{Z}_8$.



3.5 Una cubica $\mathscr{C}$ con $|\mathscr{C}(\mathbb{Q})| < \infty$

All'inizio di questo capitolo, abbiamo affermato che esistono cubiche lisce razionali tali che il loro insieme dei punti razionali è vuoto, oppure contiene un numero finito o infinito di elementi.

Ad esempio, si può provare che la cubica $\mathscr{D} \subseteq \mathbb{P}^2(\mathbb{C})$ data da

$$\mathscr{D} : 3x_0^3 + 4x_1^3 + 5x_2^3 = 0$$

non ha punti razionali (una dimostrazione di questo fatto si trova in [Sl]).
Poi, la cubica $\mathscr{C}$ dell'esempio 3.3 possiede sicuramente infiniti punti razionali, dato che abbiamo trovato degli elementi di ordine infinito in $\mathscr{C}(\mathbb{Q})$.
Prima di presentare un esempio di cubica con un numero finito di punti razionali, diamo un risultato che tornerà subito utile, ed è particolarmente interessante perché nella dimostrazione si usa un metodo simile a quello usato da Fermat per provare che

$$x^n + y^n = z^n$$

non ha soluzioni intere non banali per $n = 4$.

Proposizione 3.5.1. *L'equazione*

$$x^4 - y^4 = z^2 \qquad (*)$$

non ha soluzioni intere (M, N, L) *con* $MNL \neq 0$.

Dimostrazione. Supponiamo che esista una soluzione siffatta; possiamo assumere $M, N, L > 0$ (se esiste una soluzione (M, N, L) con ad esempio $M < 0$, allora anche $(-M, N, L)$ è una soluzione di $(*)$), così $M > N$. Inoltre possiamo assumere M, N, L a due a due primi fra loro: infatti si vede facilmente che se p primo divide due fra M, N, L, allora deve dividere anche il terzo, quindi

$$\exists M_1, N_1, L_1 \in \mathbb{Z} \text{ tali che } M = pM_1 \ , \ N = pN_1 \ , \ L = pL_1$$
$$\implies p^4(M_1^4 - N_1^4) = p^2 L_1 \implies \exists L_2 \text{ tale che } L_1 = p^2 L_2$$

$\implies (M_1, N_1, L_2)$ è una soluzione di $(*)$.
Il nostro scopo è provare che esiste sempre un'altra soluzione $(\widetilde{M}, \widetilde{N}, \widetilde{L})$ di $(*)$ con $0 < \widetilde{M} < M$; poiché questo ragionamento si potrà ripetere infinite volte, per il principio del minimo avremo un assurdo.

Caso (a) N pari, $N = 2\overline{N}$ (quindi M, L sono dispari per quanto detto sopra).
Vale

$$N^4 = 2^4\overline{N}^4 = M^4 - L^2 \implies 2^4 \mid (M^2 + L)(M^2 - L)$$

dove $(M^2 + L)$, $(M^2 - L)$ sono entrambi pari; notiamo che non si può avere $4 \mid (M^2 + L)$ e $4 \mid (M^2 - L)$, altrimenti 4 dovrebbe dividere anche $2M^2$, ma M^2 è dispari. Dunque

$$2 \mid (M^2 + \varepsilon L) \quad , \quad 8 \mid (M^2 - \varepsilon L) \, ,$$

dove si è posto $\varepsilon = \pm 1$.
Mostriamo ora che

$$\exists M_1, N_1 \in \mathbb{Z} \text{ tali che } \begin{cases} M^2 + \varepsilon L = 2M_1^4 \\ M^2 - \varepsilon L = 8N_1^4 \end{cases} ; \tag{3.10}$$

scriviamo

$$\overline{N}^4 = \frac{N^4}{2^4} = \frac{M^2 + \varepsilon L}{2} \cdot \frac{M^2 - \varepsilon L}{8}$$

dove $\text{MCD}\left(\frac{M^2+\varepsilon L}{2}, \frac{M^2-\varepsilon L}{8}\right) = 1$, altrimenti troveremmo $\text{MCD}(M, L) > 1$. Da questa relazione si vede che se p è un primo e p^r è la massima potenza di p che divide $\frac{M^2+\varepsilon L}{2}$, allora è anche la massima potenza di p che divide $\overline{N}^4$; quindi r è un multiplo di 4, e ragionando analogamente con $\frac{M^2-\varepsilon L}{8}$ si trova (3.10).
Da qui seguono

$$N^4 = 2^4 M_1^4 N_1^4 \implies N = 2M_1 N_1 \tag{3.11}$$

e

$$\begin{gathered} 2M^2 = 2M_1^4 + 8N_1^4 \\ \implies M^2 = M_1^4 + 4N_1 \\ \implies M^2 - M_1^4 = (M - M_1^2)(M + M_1^2) = 4N_1^4 \, . \end{gathered}$$

Ancora una volta, se p primo divide $(M - M_1^2)$ e $(M + M_1^2)$ allora $p \mid 2M$, dunque $p = 2$ oppure $p \mid M$, ma in quest'ultimo caso p dividerebbe anche M_1 e N_1, quindi anche N, contro l'ipotesi $(M, N) = 1$; similmente, neanche 4 divide contemporaneamente $(M - M_1^2)$ e $(M + M_1^2)$, ovvero

$$\text{MCD}(M - M_1^2 \, , \, M + M_1^2) = 2 \, .$$

Poiché il loro prodotto è $4N_1^4$, e non hanno fattori in comune a parte 2, esistono

$M_2, N_2 \in \mathbb{Z}$ tali che

$$M + M_1^2 = 2M_2^4 \quad , \quad M - M_1^2 = 2N_2^4 \tag{3.12}$$
$$\implies 4N_1^4 = 4M_2^4 N_2^4$$
$$\implies N_1 = M_2 N_2 \, . \tag{3.13}$$

Ora, sottraendo membro a membro le relazioni in (3.12) si trova

$$2M_2^4 - 2N_2^4 = M + M_1^2 - M + M_1^2 = 2M_1^2 \, ,$$

così (M_2, N_2, M_1) è una soluzione di $(*)$.
D'altra parte, per (3.11) e (3.13), poiché M_2, N_2, M_1, N_1 sono interi positivi, vale

$$M_2 < 2M_2 \leq 2M_2 N_2 M_1 = 2N_1 M_1 = N < M \, ;$$

per quanto detto all'inizio della dimostrazione, il caso N pari è provato.

Caso (b) N dispari, $N = 2\overline{N} + 1$; allora

$$N^2 = 4(\overline{N}^2 + \overline{N}) + 1 \implies N^2 \equiv 1 \mod 4$$
$$\implies N^4 = M^4 - L^2 \equiv 1 \mod 4 \, ;$$

siccome un quadrato è congruo a 0 oppure 1 mod 4, deve essere $M^4 \equiv 1 \mod 4$ e $L^2 \equiv 0 \mod 4$.
In particolare L è pari e

$$L^2 = (M^2 - N^2)(M^2 + N^2) \implies 4 \mid (M^2 - N^2)(M^2 + N^2) \, .$$

Poiché $(M, N) = 1$, ragionando come prima si trova

$$M^2 - N^2 = 2M_1^2 \quad , \quad M^2 + N^2 = 2N_1^2$$

per qualche $M_1, N_1 \in \mathbb{Z}$, per cui

$$M^2 = M_1^2 + N_1^2 \quad , \quad N^2 = N_1^2 - M_1^2$$
$$\implies N_1^4 - M_1^4 = M^2 N^2 \, .$$

Pertanto (M_1, N_1, MN) soddisfa $(*)$, e si ha

$$M_1 < \sqrt{M_1^2 + N_1^2} = M \ ;$$

questo conclude la prova del fatto che l'equazione $(*)$ non ha soluzioni intere (M, N, L) con $MNL \neq 0$. □

Proposizione 3.5.2. *La cubica*

$$\mathscr{C} : y^2 = x^3 - x$$

possiede come unici punti razionali i punti

$$\{(0,0)\,,\,(-1,0)\,,\,(1,0)\,,\,O\}$$

dove $O = [0,0,1]$ *è il punto all'infinito di* $\mathscr{C}$.

Dimostrazione. Anzitutto, ponendo $y = 0$ si trova $0 = x(x+1)(x-1)$, quindi $(0,0), (-1,0), (1,0) \in \mathscr{C}$; questi tre sono gli unici punti di $\mathscr{C}$ con ascissa o ordinata nulla.
Supponiamo allora che esista un punto razionale $A = (x_A, y_A) \in \mathscr{C}$ con $x_A y_A \neq 0$; possiamo assumere $y_A > 0$ (già sappiamo che $(x_A, y_A) \in \mathscr{C} \Leftrightarrow (x_A, -y_A) \in \mathscr{C}$) ed anche $x_A > 0$, infatti se $x_A < 0$, si vede facilmente che il punto razionale $\left(-\frac{1}{x_A}, \frac{y_A}{x_A^2}\right)$ appartiene ancora a $\mathscr{C}$.
Scriviamo quindi $(x_A, y_A) = \left(\frac{m}{n}, \frac{u}{w}\right)$, con $(m,n) = (u,w) = 1$.
Per la proposizione 3.3.2, se $p_1, ..., p_k$ sono i fattori primi di n, allora esistono degli interi $\nu_1, ..., \nu_k > 0$ tali che

$$(x_A, y_A) = \left(\frac{m}{p_1^{2\nu_1} ... p_k^{2\nu_k}}, \frac{u}{p_1^{3\nu_1} ... p_k^{3\nu_k}}\right)$$

quindi, posto $d = p_1^{\nu_1} ... p_k^{\nu_k}$, possiamo scrivere

$$(x_A, y_A) = \left(\frac{m}{d^2}, \frac{u}{d^3}\right) \ .$$

Questo vale ovviamente anche per i punti di $\mathscr{C}(\mathbb{Q})$ a coordinate intere, con $d = 1$.

In ogni caso n è un quadrato, e vale $n^3 = d^6 = w^2$, quindi

$$\left(\frac{u}{w}\right)^2 = \left(\frac{m}{n}\right)^3 - \frac{m}{n} \implies u^2 n^3 = w^2(m^3 - n^2 m)$$
$$\implies u^2 = m(m-n)(m+n)\ . \tag{3.14}$$

Mostriamo che anche m deve essere un quadrato; prima notiamo che

$$\mathrm{MCD}(m, m+n) = \mathrm{MCD}(m, m-n) = 1 \quad \text{e} \quad \mathrm{MCD}(m+n, m-n) \leq 2$$

altrimenti troverei dei fattori comuni a m e n, contro l'ipotesi $(m, n) = 1$.
Ora, se $p \mid m$, per la (3.14) p divide anche u^2, quindi (poiché non può essere anche fattore di $m \pm n$) compare fra i fattori di m con una potenza pari, cioè m è un quadrato.
In definitiva, abbiamo scoperto che se esiste un punto razionale $(x_A, y_A) = \left(\frac{m}{n}, \frac{u}{w}\right)$ $\in \mathscr{C}$ con x_A, $y_A > 0$, deve valere

$$n = N^2 \quad , \quad m = M^2$$

e da (3.14) segue

$$M^4 - N^4 = (m+n)(m-n) = \frac{u^2}{m} =: L^2\ ,$$

dove $M, N, L \in \mathbb{Z}$, e sono tutti non nulli; in altre parole, (M, N, L) è una soluzione intera all'equazione $x^4 - y^4 = z^2$ con $MNL \neq 0$, contro la proposizione precedente.

□

Capitolo 4

Il teorema di Mordell

In questo capitolo riprendiamo a parlare in generale del gruppo $\mathscr{C}(\mathbb{Q})$, e affrontiamo la dimostrazione del teorema di Mordell (teorema 4.4.2), il quale afferma che, se $\mathscr{C}$ è una cubica liscia razionale, $\mathscr{C}(\mathbb{Q})$ è finitamente generato. Noi proveremo questo teorema solo per una classe (seppure molto ampia) di cubiche lisce, ovvero per quelle che hanno almeno un punto razionale di ordine 2.
Ovviamente, l'idea sarà quella di cercare $Q_1, ..., Q_m \in \mathscr{C}(\mathbb{Q})$ tali che ogni punto $P \in \mathscr{C}(\mathbb{Q})$ si può scrivere come somma

$$P = k_1 Q_1 + ... + k_m Q_m \qquad k_i \in \mathbb{Z}\ ,\ i = 1, ..., m\ .$$

Per poter dimostrare questo, abbiamo bisogno di una serie di risultati preliminari, raccolti nelle sezioni da 4.1 a 4.3.
Introduciamo anzitutto il concetto di *altezza* di un punto.

In questo capitolo $\mathscr{C}$ denoterà sempre una cubica liscia razionale data da

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx + c \quad , \quad a, b, c \in \mathbb{Z} \tag{4.1}$$

e denoteremo sempre con $f(x)$ il polinomio

$$f(x) = x^3 + ax^2 + bx + c\ .$$

4.1 Altezza di un punto e proprietà

Definizione 4.1.1. Sia $x = \frac{m}{n} \in \mathbb{Q} \setminus \{0\}$, $(m,n) = 1$, $n > 0$. Si dice *altezza di* x, e si indica con $H(x)$, la quantità

$$H(x) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\} \ \in \mathbb{N} \, .$$

Sia $P \in \mathscr{C}(\mathbb{Q})$, $P \neq O$, $P = (x_P, y_P)$; si definisce l'*altezza di* P come

$$H(P) = H(x_P) \, ;$$

si pone inoltre $H(O) = 1$.
Talvolta sarà utile considerare, al posto di H, il suo logaritmo naturale:

$$\begin{aligned} &\forall x \in \mathbb{Q} \, , \ h(x) \coloneqq \ln H(x) \\ &\forall P \in \mathscr{C}(\mathbb{Q}) \, , \ h(P) \coloneqq \ln H(P). \end{aligned}$$

Vale così $h(O) = 0$, $h : \mathscr{C}(\mathbb{Q}) \longrightarrow [0, +\infty[$.

Proposizione 4.1.2. *Sia $M \in \mathbb{R}$, $M > 0$. Allora*

(*i*) *l'insieme $\{x \in \mathbb{Q} \mid h(x) \leq M\}$ è finito*

(*ii*) *l'insieme $\{P \in \mathscr{C}(\mathbb{Q}) \mid h(P) \leq M\}$ è finito*

Dimostrazione. Supponiamo M intero (altrimenti possiamo considerare la parte intera di M), e sia $x = \frac{m}{n} \in \mathbb{Q}$, $(m,n) = 1$.
Se vale $H(x) \leq M$, vuol dire che $|m| \leq M$, $|n| \leq M$; sappiamo che di razionali positivi fatti così ce ne sono meno di $M(M-1)$, quindi

$$\#\{x \in \mathbb{Q} \mid H(x) \leq M\} \ \leq \ 2M(M-1) + 1 \, .$$

Ripetendo il ragionamento con e^M al posto di M, poiché il logaritmo è una funzione crescente e vale $h(x) \leq M \Leftrightarrow H(x) \leq e^M$, si trova proprio (*i*).
Per mostrare (*ii*) basta osservare che se $P = (x_P, y_P)$ e $H(P) \leq M$, allora per quanto detto sopra x_P può assumere valori solo in un insieme finito, e che ad ogni x_P corrispondono al più 2 valori di y_P. □

Oltre questa importantissima proprietà di finitezza, ci occorreranno altri due risultati sull'altezza di un punto, per capire come questa si comporta nella somma. Per prima cosa vorremmo mostrare che se A e Q sono punti di $\mathscr{C}(\mathbb{Q})$, allora esiste una relazione fra $h(A+Q)$ e $h(A)$.

Ricordiamo preliminarmente che, per la proposizione 3.3.2 e come osservato nella dimostrazione di 3.5.2, se $A = (x_A, y_A) \in \mathscr{C}(\mathbb{Q})$ allora esistono $m, n, d \in \mathbb{Z}$, $d > 0$, con $(m,d) = (n,d) = 1$, tali che $(x_A, y_A) = \left(\frac{m}{d^2}, \frac{n}{d^3}\right)$; ne segue

$$|m| \ , \ d^2 \leq H(A) \ . \tag{4.2}$$

Lemma 4.1.3. *Sia $A \in \mathscr{C}(\mathbb{Q})$, $A = \left(\frac{m}{d^2}, \frac{n}{d^3}\right)$, $(m,d) = (n,d) = 1$, $d > 0$; allora esiste $K = K(a,b,c) \in \mathbb{R}$, $K > 0$, tale che*

$$|n| \leq K \cdot H(A)^{3/2} \ .$$

Dimostrazione. Sostituendo $x_A = \dfrac{m}{d^2}$ e $y_A = \dfrac{n}{d^3}$ nell'equazione di $\mathscr{C}$ e moltiplicando per d^6 si trova

$$\begin{aligned} n^2 &= m^3 + ad^2m^2 + bd^4m + cd^6 \\ \Longrightarrow |n^2| &\leq |m^3| + |ad^2m^2| + |bd^4m| + |cd^6| \ . \end{aligned}$$

Per (4.2) vale

$$|n^2| \leq H(A)^3 + |a|H(A)^3 + |b|H(A)^3 + |c|H(A)^3$$

quindi con $K = \sqrt{1 + |a| + |b| + |c|}$ si ha l'asserto. □

Teorema 4.1.4. *Fissato un punto $Q \in \mathscr{C}(\mathbb{Q})$, esiste una costante κ che dipende solo da Q, a, b, c, tale che per ogni $A \in \mathscr{C}(\mathbb{Q})$ vale*

$$h(A+Q) \leq 2h(A) + \kappa \ . \tag{4.3}$$

Dimostrazione. Se $Q = O$, la disuguaglianza (4.3) vale banalmente con $\kappa = 0$, perché $h(A) \geq 0$. Sia dunque $Q \neq O$; basta provare che esiste $\tilde{\kappa}$ che soddisfa la disuguaglianza (4.3) per $A \notin \{Q, -Q, O\}$. Infatti, se questo è vero, siccome

$h(Q) = h(-Q) > 0$ e $h(O) = 0$, la costante

$$\kappa = \max\left\{\tilde{\kappa}\ ,\ h(2Q) - 2h(Q)\ ,\ h(Q)\right\}$$

soddisfa (4.3) $\forall A \in \mathscr{C}(\mathbb{Q})$.
Prendiamo quindi $A \in \mathscr{C}(\mathbb{Q}) \smallsetminus \{Q, -Q, O\}$ e scriviamo

$$A + Q = (X, Y)\ .$$

Ci interessa calcolare $H(A+Q) = H(X)$; per la formula (2.2), vale:

$$\begin{aligned}
X &= \frac{(y_Q - y_A)^2}{(x_Q - x_A)^2} - a - x_A - x_Q \\
&= \frac{y_Q^2 + y_A^2 - 2y_Q y_A - (x_Q - x_A)^2(a + x_A + x_Q)}{(x_Q - x_A)^2} \\
&= \frac{y_Q^2 + \boxed{y_A^2} - 2y_Q y_A - (a + x_Q)(x_Q - x_A)^2 - (x_A x_Q^2 + \boxed{x_A^3} - 2x_Q x_A^2)}{(x_Q - x_A)^2} \\
&= \frac{y_Q^2 + \boxed{ax_A^2 + bx_A + c} - 2y_Q y_A - (a + x_Q)(x_Q - x_A)^2 - x_A x_Q^2 - 2x_Q x_A^2}{(x_Q - x_A)^2} \\
&= \frac{(-2y_Q)y_A + (b + x_Q)x_A^2 + (x_Q^2 + 2ax_Q)x_A + (y_Q^2 - x_Q^3 - ax_Q^2 + c)}{x_Q^2 + x_A^2 - 2x_Q x_A}\ .
\end{aligned}$$

Quindi esistono $\alpha_1, ..., \alpha_7 \in \mathbb{Q}$ dipendenti da a, b, c, x_Q, y_Q tali che

$$X = \frac{\alpha_1 y_A + \alpha_2 x_A^2 + \alpha_3 x_A + \alpha_4}{\alpha_5 x_A^2 + \alpha_6 x_A + \alpha_7}\ ; \tag{4.4}$$

a meno di moltiplicare e dividere X per il minimo comune multiplo dei denominatori degli α_i, possiamo supporre che questi siano interi.
Sostituiamo ora $(x_A, y_A) = \left(\frac{m}{d^2}, \frac{n}{d^3}\right)$ nella (4.4); moltiplicando e dividendo tutto per d^4, troviamo

$$X = \frac{\alpha_1 nd + \alpha_2 m^2 + \alpha_3 md^2 + \alpha_4 d^4}{\alpha_5 m^2 + \alpha_6 md^2 + \alpha_7 d^4}\ . \tag{4.5}$$

Nella (4.5), numeratore e denominatore sono interi, anche se non necessariamente primi fra loro; poiché semplificando il loro modulo diventa più piccolo, per

definizione di altezza vale

$$H(X) \leq \max\{|\alpha_1 nd + \alpha_2 m^2 + \alpha_3 md^2 + \alpha_4 d^4|, |\alpha_5 m^2 + \alpha_6 md^2 + \alpha_7 d^4|\} .$$

D'altra parte, per la (4.2), per il lemma 4.1.3 e per la disuguaglianza triangolare si ha

$$\begin{aligned} |\alpha_1 nd + \alpha_2 m^2 + \alpha_3 md^2 + \alpha_4 d^4| \ &\leq \ |\alpha_1 K| H(A)^{\frac{3}{2}} \sqrt{H(A)} + \\ &\quad + (|\alpha_2| + |\alpha_3| + |\alpha_4|) H(A)^2 \\ |\alpha_5 m^2 + \alpha_6 md^2 + \alpha_7 d^4| \ &\leq \ (|\alpha_5| + |\alpha_6| + |\alpha_7|) H(A)^2 , \end{aligned}$$

dove K dipende solo da a, b, c; pertanto

$$H(A+Q) = H(X) \leq \max\left\{|\alpha_1 K| + |\alpha_2| + |\alpha_3| + |\alpha_4|, |\alpha_5| + |\alpha_6| + |\alpha_7|\right\} H(A)^2 .$$

Da qui, ponendo

$$\tilde{\kappa} = \ln(\max\left\{|\alpha_1 K| + |\alpha_2| + |\alpha_3| + |\alpha_4|, |\alpha_5| + |\alpha_6| + |\alpha_7|\right\})$$

si ricava

$$h(A+Q) \leq 2h(A) + \tilde{\kappa} ;$$

per come è stato definito, $\tilde{\kappa}$ dipende solo da a, b, c, x_Q, y_Q, quindi si ha la tesi. □

Il secondo risultato che vorremmo mostrare mette in relazione l'altezza di A con quella di $2A$; ricordiamo che se A ha ordine diverso da 2 in $(\mathscr{C}, +, O)$, per la formula di duplicazione data da (2.3), x_{2A} si può scrivere come funzione razionale di x_A, ovvero come quoziente di due polinomi (nel nostro caso a coefficienti interi) valutati in x_A.
Tenendo questo a mente, diamo prima due risultati validi in generale per polinomi in $\mathbb{Z}[x]$.

Proposizione 4.1.5. *Siano g_1, $g_2 \in \mathbb{Z}[x]$,*

$$\begin{aligned} g_1 &= a_0 + a_1 x + ... + a_{d_1} x^{d_1} \\ g_2 &= b_0 + b_1 x + ... + b_{d_2} x^{d_2} \end{aligned}$$

e supponiamo che g_1 e g_2 non abbiano radici complesse in comune; poniamo inoltre

$$d = \max\{d_1, d_2\} \ .$$

Allora esiste $R \in \mathbb{Z}$, $R > 0$, che dipende da g_1 e g_2, tale che $\forall x = \dfrac{m}{n} \in \mathbb{Q}$ si ha

$$MCD\left(n^d g_1\left(\frac{m}{n}\right), n^d g_2\left(\frac{m}{n}\right) \right) \Bigg| R \ .$$

Dimostrazione. Supponiamo $d = d_1$ e $\forall x \in \mathbb{Q}$ scriviamo $x = \frac{m}{n}$, $(m,n) = 1$, $n > 0$; certamente $n^d g_1\left(\frac{m}{n}\right)$ e $n^d g_2\left(\frac{m}{n}\right)$ sono interi, quindi ha senso parlare di massimo comune divisore. Poniamo dunque

$$M = \mathrm{MCD}\left(n^d g_1\left(\frac{m}{n}\right), n^d g_2\left(\frac{m}{n}\right) \right)$$

e cerchiamo un multiplo di M che non dipenda da $\dfrac{m}{n}$ ma solo dai coefficienti di g_1, g_2.
Anzitutto, poiché g_1 e g_2 non hanno radici complesse in comune, vale

$$\mathrm{MCD}(g_1(x), g_2(x)) = 1 \quad \text{in } \mathbb{Q}[x]$$

quindi esistono due polinomi ϕ_1, $\phi_2 \in \mathbb{Q}[x]$ tali che

$$\phi_1 g_1 + \phi_2 g_2 \equiv 1 \quad \text{in } \mathbb{Q}[x] \tag{4.6}$$

(vedi [J, teoremi 2.13-2.15; sezione 2.15]).
Fissiamo ora $K \in \mathbb{Z}$ in modo che $K\phi_1$, $K\phi_2$ siano polinomi in $\mathbb{Z}[x]$, e poniamo $D = \max\{\deg \phi_1, \deg \phi_2\}$; allora

$$\begin{aligned} & \phi_1\left(\tfrac{m}{n}\right) g_1\left(\tfrac{m}{n}\right) + \phi_2\left(\tfrac{m}{n}\right) g_2\left(\tfrac{m}{n}\right) = 1 \\ \Longrightarrow \ & K n^{d+D}\left(\phi_1\left(\tfrac{m}{n}\right) g_1\left(\tfrac{m}{n}\right) + \phi_2\left(\tfrac{m}{n}\right) g_2\left(\tfrac{m}{n}\right)\right) = K n^{d+D} \\ \Longrightarrow \ & \underbrace{K n^D \phi_1\left(\tfrac{m}{n}\right)}_{\in\mathbb{Z}} \cdot \underbrace{n^d g_1\left(\tfrac{m}{n}\right)}_{\in\mathbb{Z}} + \underbrace{K n^D \phi_2\left(\tfrac{m}{n}\right)}_{\in\mathbb{Z}} \cdot \underbrace{n^d g_2\left(\tfrac{m}{n}\right)}_{\in\mathbb{Z}} = K n^{d+D} \ . \end{aligned}$$

Per come lo abbiamo definito, vale certamente

$$M \ \Big| \ K n^{d+D} \ ; \tag{4.7}$$

d'altra parte

$$M \mid n^d g_1\left(\frac{m}{n}\right)$$

quindi

$$\begin{aligned} M \mid Kn^{2d+D-1} g_1\left(\frac{m}{n}\right) =& Kn^{d+D-1}(a_0 n^d + ... + a_d m^d) \\ =& Kn^{2d+D-1}a_0 + ... + Kn^{d+D}m^{d-1}a_{d-1} + Kn^{d+D-1}m^d a_d \,. \end{aligned} \tag{4.8}$$

Nella sommatoria all'ultimo membro compare Kn^{d+D} in ogni addendo tranne l'ultimo; quindi per (4.7) e (4.8) deve valere anche

$$M \mid Kn^{d+D-1}m^d a_d \,.$$

Così

$$\begin{aligned} M \mid \mathrm{MCD}\left(Kn^{d+D-1}m^d a_d \,,\; Kn^{d+D}\right) &= Kn^{d+D-1} \cdot \mathrm{MCD}(m^d a_d \,,\; n) \\ &= Kn^{d+D-1} \cdot \mathrm{MCD}(a_d \,,\; n) \end{aligned}$$

e in particolare $M \mid Kn^{d+D-1}a_d$.
Riassumendo, abbiamo mostrato che

$$M \mid Kn^{d+D} \implies M \mid Kn^{d+D-1}a_d \,.$$

Ripetiamo il ragionamento: partendo ora dal fatto che

$$\begin{aligned} M \mid Ka_d n^{2d+D-2} g_1\left(\frac{m}{n}\right) = Kn^{2d+D-2}a_d a_0 + ... + Kn^{d+D-1}m^{d-1}a_d a_{d-1} + \\ + Kn^{d+D-2}m^d a_d^2 \end{aligned}$$

e sapendo che M divide i primi d termini della sommatoria all'ultimo membro, troviamo

$$\begin{aligned} M \mid \mathrm{MCD}\left(Kn^{d+D-2}m^d a_d^2 \,,\; Kn^{d+D}\right) \\ \implies M \mid Kn^{d+D-2}a_d^2 \,. \end{aligned}$$

In definitiva

$$M \mid Kn^{d+D} \implies M \mid Kn^{d+D-2}a_d^2 \implies ... \implies M \mid Ka_d^{d+D} \,,$$

dove $Ka_d^{d+D} =: R$ è una costante che dipende solo da g_1 e g_2, come si voleva.

□

Lemma 4.1.6. *Siano g_1, $g_2 \in \mathbb{Z}[x]$ come nell'enunciato del lemma 4.1.5, senza radici complesse in comune, sia d il massimo dei loro gradi, e $\forall x \in \mathbb{Q}$ sia $h(x)$ la sua altezza logaritmica. Allora esistono κ_1, $\kappa_2 \in \mathbb{R}$, che dipendono solo da g_1 e g_2, tali che*

$$d \cdot h(x) - \kappa_1 \ \leq \ h\left(\frac{g_1(x)}{g_2(x)}\right) \ \leq \ d \cdot h(x) + \kappa_2 \tag{4.9}$$
$$\forall x \in \mathbb{Q} \smallsetminus \{y \mid g_2(y) = 0\} \ .$$

Dimostrazione. Sia $x \in \mathbb{Q} \smallsetminus \{y \mid g_2(y) = 0\}$, $x = \frac{m}{n}$, $(m, n) = 1$; mostriamo prima che esiste κ_1 tale che

$$dh(x) - \kappa_1 \ \leq \ h\left(\frac{g_1(x)}{g_2(x)}\right) \ . \tag{4.10}$$

Possiamo supporre anche che x non sia radice di g_1: infatti se $g_1(x)=0$ e $g_2(x)\neq 0$, vale $h\left(\frac{g_1(x)}{g_2(x)}\right)=0$, e quindi se $\widetilde{\kappa_1}$ soddisfa (4.10) per ogni $x \in \mathbb{Q} \smallsetminus \{y \mid g_1(y) = 0 \ , \ g_2(y) = 0\}$, allora

$$\kappa_1 = \max\left\{\widetilde{\kappa_1}\,, \max\{d \cdot h(x) \mid x \in \mathbb{Q}\,, g_1(x) = 0\}\right\}$$

soddisfa (4.10) per ogni $x \in \mathbb{Q} \smallsetminus \{y \mid g_2(y) = 0\}$.
Poiché $g_1(x) \neq 0$ e $g_2(x) \neq 0$, per come abbiamo definito l'altezza di un razionale risulta $h\left(\frac{g_1(x)}{g_2(x)}\right) = h\left(\frac{g_2(x)}{g_1(x)}\right)$; quindi possiamo supporre anche, come prima, $d = d_1$.
Anzitutto, poniamo

$$X = \frac{g_1(x)}{g_2(x)} = \frac{n^d g_1(x)}{n^d g_2(x)}$$
$$M = \mathrm{MCD}\left(n^d g_1\left(\frac{m}{n}\right), n^d g_2\left(\frac{m}{n}\right)\right) ;$$

per il lemma 4.1.5 esiste $R > 0$ intero, dipendente solo da g_1 e g_2, tale che $M \mid R$; pertanto

$$H(X) = \max\left\{\left|\frac{n^d g_1(x)}{M}\right|, \left|\frac{n^d g_2(x)}{M}\right|\right\}$$

$$\geq \frac{1}{R}\max\left\{|n^d g_1(x)|\,,|n^d g_2(x)|\right\}$$
$$\geq \frac{1}{2R}\left(|n^d g_1(x)| + |n^d g_2(x)|\right)\,.$$

Ricordiamo che il nostro scopo è trovare κ_1 tale che valga la (4.10), o, equivalentemente,

$$\frac{1}{e^{\kappa_1}} \leq \frac{H(X)}{H(x)^d}\,;$$

ma, per quanto detto sopra

$$\frac{H(X)}{H(x)^d} = \frac{H\left(\dfrac{g_1(x)}{g_2(x)}\right)}{H(x)^d} \geq \frac{1}{2R}\cdot\frac{|n^d g_1(x)| + |n^d g_2(x)|}{\max\{|m|^d\,,|n|^d\}} = \frac{1}{2R}\cdot\frac{|g_1(x)| + |g_2(x)|}{\max\{|x|^d\,,1\}}\,.$$

Quindi, per dare una stima di $\frac{H(X)}{H(x)^d}$ che non dipenda da x, potremmo studiare la funzione $\xi : \mathbb{R} \to \mathbb{R}$ definita da

$$\xi(t) = \frac{|g_1(t)| + |g_2(t)|}{\max\{|t|^d\,,1\}}\,.$$

ξ è una funzione continua e non negativa; inoltre

$$\xi(t) \xrightarrow[t\to\pm\infty]{} \begin{cases} |a_d| & \text{se } d_2 < d \\ |a_d| + |b_d| & \text{se } d_2 = d \end{cases}$$

quindi il limite all'infinito è strettamente positivo; dall'analisi sappiamo che è possibile trovare ℓ, $L_1 > 0$ tali che

$$\xi(t) > L_1 \quad \forall t \in \mathbb{R} \setminus [-\ell, \ell]\,.$$

In aggiunta, poiché g_1 e g_2 non hanno radici in comune, allora $\xi(t) \neq 0\ \forall t \in \mathbb{R}$, e dato che ξ è continua, essa ha minimo $L_2 > 0$ su $[-\ell, \ell]$; così

$$\xi(t) \geq L = \min\left\{L_1, L_2\right\} > 0 \quad \forall t \in \mathbb{R}\,.$$

Osserviamo che, per come è stato definito, L dipende solo da g_1 e g_2.

In definitiva abbiamo mostrato che

$$\exists L > 0 \text{ tale che } \frac{H\left(\frac{g_1(x)}{g_2(x)}\right)}{H(x)^d} \geq \frac{L}{2R} ;$$

pertanto $\kappa_1 \coloneqq \ln\left(\frac{2R}{L}\right)$ è la costante cercata, e per quanto detto all'inizio della dimostrazione, vale la prima disuguaglianza.
Mostriamo ora che esiste κ_2 tale che $h(X) \leq dh(x) + \kappa_2$, ovvero

$$H\left(\frac{g_1(x)}{g_2(x)}\right) \leq H(x)^d e^{\kappa_2} .$$

Vale

$$\begin{aligned} H\left(\frac{g_1(x)}{g_2(x)}\right) &= H\left(\frac{n^d g_1(x)}{n^d g_2(x)}\right) = H\left(\frac{a_0 n^d + ... + a_d m^d}{b_0 n^d + ... + b_{d_2} m^{d_2} n^{d-d_2}}\right) \\ &= \max\{|a_0 n^d + ... + a_d m^d| , |b_0 n^d + ... + b_{d_2} m^{d_2} n^{d-d_2}|\} \\ &\leq \max\{|a_0|\cdot|n^d| + ... + |a_d|\cdot|m^d| , \ |b_0|\cdot|n^d| + ... + |b_{d_2}|\cdot|m^{d_2}|\cdot|n^{d-d_2}|\} \\ &\leq \max\{(|a_0| + ... + |a_d|)H(x)^d , (|b_0| + ... + |b_{d_2}|)H(x)^d\} ; \end{aligned}$$

così

$$\kappa_2 \coloneqq \ln \max\{|a_0| + ... + |a_d| \ , |b_0| + ... + |b_{d_2}|\}$$

soddisfa la seconda disuguaglianza in (4.9), e questo conclude la prova del lemma.

□

Ora possiamo tornare a $\mathscr{C}(\mathbb{Q})$ e dimostrare il seguente

Teorema 4.1.7. *Esiste $\kappa \in \mathbb{R}$, dipendente solo da a, b, c, tale che*

$$h(2A) \geq 4h(A) - \kappa \quad \forall A \in \mathscr{C}(\mathbb{Q})$$

Dimostrazione. Analogamente a quanto fatto nella dimostrazione di 4.1.4, possiamo dimostrare la tesi per tutti i punti di $\mathscr{C}(\mathbb{Q})$ eccetto un numero finito; sia dunque $A = (x, y) \in \mathscr{C}(\mathbb{Q}) \setminus \{P \mid 2P = O\}$, e scriviamo $2A = (X, Y)$.
Dalla proposizione 2.2.3 sappiamo che

$$X = \lambda^2 - a - 2x , \ \text{ con } \lambda = \frac{f'(x)}{2y}$$

(abbiamo supposto $A \neq -A$, quindi $y \neq 0$), cioè si ha

$$X = \frac{f'(x)^2 - (a+2x)4y^2}{4y^2} = \frac{f'(x)^2 - 4(a+2x)f(x)}{4f(x)} \ .$$

Così abbiamo espresso X come quoziente di due polinomi g_1, g_2 a coefficienti interi in x; inoltre g_1 e g_2 non hanno radici in comune (altrimenti le avrebbero f e f', ma sappiamo dall'osservazione 1.3.a che non è possibile), e il massimo tra i gradi di g_1 e g_2 è 4.
Dunque vale il lemma 4.1.6, in particolare esiste una costante κ_1 che dipende da g_1 e g_2 (i quali hanno coefficienti in funzione di a, b, c) tale che

$$h(2A) = h(X) = h\left(\frac{g_1(x)}{g_2(x)}\right) \geq 4h(x) - \kappa_1 = 4h(A) - \kappa_1$$
$$\forall A \in \mathscr{C}(\mathbb{Q}) \smallsetminus \{P \mid 2P = O\}$$

quindi ponendo

$$\kappa = \max\left\{\kappa_1 \, , \max\{4h(P) \mid P \in \mathscr{C}(\mathbb{Q}) \, , 2P = O\}\right\}$$

si ha l'asserto.

□

4.2 La mappa di duplicazione

Ricordiamo che il nostro scopo è provare che esistono $Q_1, ..., Q_m \in \mathscr{C}(\mathbb{Q})$ tali che ogni $A \in \mathscr{C}(\mathbb{Q})$ si può scrivere come

$$P = k_1 Q_1 + ... + k_m Q_m \qquad k_i \in \mathbb{Z} \ , \ i = 1, ..., m \ .$$

Il nostro obiettivo in questa e nella sezione seguente sarà mostrare che

$$[\mathscr{C}(\mathbb{Q}) : 2\mathscr{C}(\mathbb{Q})] < \infty$$

e che ogni $A \in \mathscr{C}(\mathbb{Q})$ si può scrivere come somma di multipli interi di elementi di altezza limitata e rappresentanti (fissati) delle classi in $\mathscr{C}(\mathbb{Q})\Big/2\mathscr{C}(\mathbb{Q})$.

Notazione 4. Se $(G, +)$ è un gruppo, denotiamo con $2G$ il sottogruppo $\operatorname{Im}\phi$, dove ϕ è il morfismo

$$\begin{aligned} \phi : G &\longrightarrow G \\ g &\longmapsto 2g \ . \end{aligned}$$

Quindi se $G = \mathscr{C}(\mathbb{Q})$, si ha $2\mathscr{C}(\mathbb{Q}) = \{2P \ , \ P \in \mathscr{C}(\mathbb{Q})\}$.

Per provare che l'indice di $2\mathscr{C}(\mathbb{Q})$ in $\mathscr{C}(\mathbb{Q})$ è finito, studieremo l'applicazione

$$\begin{aligned}\mathscr{C}(\mathbb{Q}) &\longrightarrow \mathscr{C}(\mathbb{Q})\\ A &\longmapsto 2A\end{aligned}$$

come composizione di altre mappe che definiremo a breve.
Nel seguito, sarà utile poter scrivere $\mathscr{C}$ nella forma

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx\ , \quad a, b \in \mathbb{Z};$$

per questo motivo, come già detto , supporremo che $\mathscr{C}$ abbia almeno un punto razionale di ordine 2, infatti:

Osservazione 4.2.a. Supponiamo che $f(x)$ abbia una radice in $\mathbb{Q}$, cioè che esista $T = (x_T, 0) \in \mathscr{C}(\mathbb{Q})$. Si osservi che $x_T \in \mathbb{Z}$ poiché $a, b, c \in \mathbb{Z}$ e il coefficiente direttore di f è 1. Allora l'affinità

$$\begin{cases} X = x - x_T \\ Y = y \end{cases}$$

porta T in $(0, 0)$, e l'equazione di $\mathscr{C}$ diventa

$$\begin{aligned}&\mathscr{C} : Y^2 = (X + x_T)^3 + a(X + x_T)^2 + b(X + x_T) + c\\ \implies &\mathscr{C} : Y^2 = X^3 + (3x_T + a)X^2 + (3x_T^2 + 2ax_T + b)X\ ,\end{aligned}$$

dato che $x_T^3 + ax_T^2 + bx_T + c = 0$. Inoltre, poiché $x_T \in \mathbb{Z}$, la nuova equazione per $\mathscr{C}$ è ancora a coefficienti interi.

Nel seguito supponiamo quindi sempre $c = 0$, cioè

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx\ , \quad a, b \in \mathbb{Z}\ ; \tag{4.11}$$

e $f(x) = x^3 + ax^2 + bx$. Il punto $T = (0, 0)$ è un punto di ordine 2 su $\mathscr{C}$.

Definizione 4.2.1. Indichiamo con $\widehat{\mathscr{C}}$ la curva di $\mathbb{P}^2(\mathbb{C})$ di equazione affine

$$\widehat{\mathscr{C}} : y^2 = x^3 + \widehat{a}\,x^2 + \widehat{b}\,x\ , \qquad \begin{aligned}\widehat{a} &= -2a\\ \widehat{b} &= a^2 - 4b\ .\end{aligned} \tag{4.12}$$

Scriveremo anche $\widehat{\mathscr{C}} : y^2 = \widehat{f}\,(x)$.

Osservazione 4.2.b. Poiché $\mathscr{C}$ è liscia, anche $\widehat{\mathscr{C}}$ lo è. Infatti, ricordando quanto detto nell'osservazione 3.2.a, il discriminante di $\mathscr{C}$ è

$$D_{\mathscr{C}} = a^2b^2 - 4b^3 = b^2(a^2 - 4b) \neq 0\ ,$$

e in particolare $b \neq 0$, $(a^2 - 4b) \neq 0$; pertanto il discriminante di $\widehat{\mathscr{C}}$, che è

$$D_{\widehat{\mathscr{C}}} = \widehat{b}^{\,2}(\widehat{a}^{\,2} - 4\widehat{b}) = (a^2 - 4b)^2(4a^2 - 4a^2 + 16b) = 16b(a^2 - 4b)^2\ ,$$

sarà ancora non nullo.
Inoltre, ponendo

$$\widehat{\widehat{\mathscr{C}}} : y^2 = x^3 + \widehat{\widehat{a}}\,x^2 + \widehat{\widehat{b}}\,x\ , \qquad \begin{aligned} \widehat{\widehat{a}} &= -2\widehat{a} \\ \widehat{\widehat{b}} &= \widehat{a}^{\,2} - 4\widehat{b} \end{aligned}$$

risulta

$$\widehat{\widehat{\mathscr{C}}} : y^2 = x^3 + 4ax^2 + 16bx\ . \tag{4.13}$$

Si verifica facilmente che $\widehat{\widehat{\mathscr{C}}}$ è affinemente equivalente a $\mathscr{C}$ tramite l'affinità

$$\alpha : (x, y) \longmapsto \left(\frac{x}{4}, \frac{y}{8}\right)\ ;$$

dall'osservazione 2.2.b, sappiamo che $\mathscr{C}$ e $\widehat{\widehat{\mathscr{C}}}$ sono gruppi isomorfi.

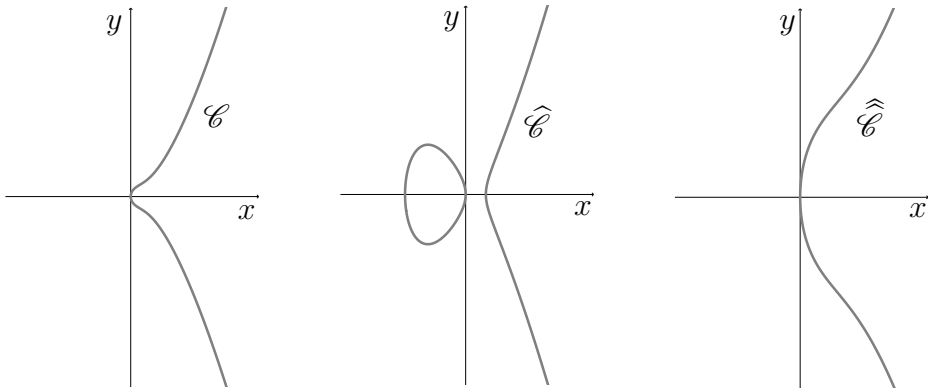


Figura 4.1. Rappresentazione dei punti reali delle cubiche date dalle equazioni (4.11), (4.12), (4.13) con $a = -1$, $b = 1$.

Proposizione 4.2.2. *Siano $\mathscr{C}$ e $\widehat{\mathscr{C}}$ le cubiche di equazioni rispettivamente* (4.11) *e* (4.12)*, e si considerino i gruppi $(\mathscr{C},+,O)$, $(\widehat{\mathscr{C}},+,O)$; allora è ben definita l'applicazione*

$$\begin{aligned}
\Phi: \qquad & \mathscr{C} \longrightarrow \widehat{\mathscr{C}} \\
& (x,y) \longmapsto (\widehat{x}\,,\widehat{y}\,) = \left(\frac{y^2}{x^2}\,,\, y\frac{x^2-b}{x^2}\right) \qquad \textit{se } x \neq 0 \\
& T=(0,0) \longmapsto O \\
& O \longmapsto O
\end{aligned} \tag{4.14}$$

e risulta Φ omomorfismo di gruppi.

Dimostrazione. Mostriamo che Φ è ben definita: sia $A \in \mathscr{C}$, $A \neq O, T$; vale certo $x_A \neq 0$, e $\Phi(A) = (\widehat{x}_A, \widehat{y}_A)$ soddisfa l'equazione di $\widehat{\mathscr{C}}$, infatti

$$\begin{aligned}
\widehat{x}_A^3 + \widehat{a}\,\widehat{x}_A^2 + \widehat{b}\,\widehat{x}_A &= \left(\frac{y_A^2}{x_A^2}\right)^3 - 2a\left(\frac{y_A^2}{x_A^2}\right)^2 + (a^2-4b)\left(\frac{y_A^2}{x_A^2}\right) \\
&= \left(\frac{y_A^2}{x_A^2}\right)\left(\frac{y_A^4 - 2ax_A^2y_A^2 + a^2x_A^4 - 4bx_A^4}{x_A^4}\right) \\
&= \left(\frac{y_A^2}{x_A^2}\right)\frac{(y_A^2 - ax_A^2)^2 - 4bx_A^4}{x_A^4} \\
&= \left(\frac{y_A^2}{x_A^2}\right)\frac{(x_A^3 + bx_A)^2 - 4bx_A^4}{x_A^4} \\
&= y_A^2\frac{(x_A^2+b)^2 - 4bx_A^2}{x_A^4} = y_A^2\left(\frac{x_A^2-b}{x_A^2}\right)^2 = \widehat{y}_A^2\,.
\end{aligned}$$

Mostriamo ora che Φ è un omomorfismo, ovvero che $\forall A, B \in \mathscr{C}$ vale

$$\Phi(A+B) = \Phi(A) + \Phi(B)\,.$$

Procediamo per gradi: se A o B coincidono con O, è banale; se $A = T \neq B$, allora per (2.2) e per (4.14), usando la relazione $y_B^2 - x_B^3 - ax_B^2 = bx_B$, si ha

$$T + B = \left(\left(\frac{y_B}{x_B}\right)^2 - a - x_B\,,\, -\left(\frac{y_B}{x_B}\right)\left(\left(\frac{y_B}{x_B}\right)^2 - a - x_B\right)\right) = \left(\frac{b}{x_B}, -\frac{by_B}{x_B^2}\right)$$

$$\begin{aligned}\implies \Phi(T+B) &= \left(\left(\frac{-by_B/x_B^2}{b/x_B}\right)^2, -\frac{by_B}{x_B^2}\left(\frac{(b/x_B)^2-b}{(b/x_B)^2}\right)\right)\\ &= \left(\frac{y_B^2}{x_B^2}, -\frac{y_B}{x_B^2}(b-x_B^2)\right)\\ &= \Phi(B) = \Phi(B)+O = \Phi(B)+\Phi(T)\end{aligned} \tag{4.15}$$

Se $A = B = T$, poiché T ha ordine 2,

$$\Phi(T+T) = \Phi(O) = O = O+O = \Phi(T)+\Phi(T)\ .$$

Supponiamo ora $A, B \neq O, T$; per il teorema 2.2.2 valgono

- $\forall A, B, C \in \mathscr{C}\ , \quad A+B=C \iff A+B-C=O$
  $\iff A, B, -C$ sono allineati
- $\forall \widehat{A}\,, \widehat{B}\,, \widehat{C} \in \widehat{\mathscr{C}}\ , \quad \widehat{A}+\widehat{B}=\widehat{C} \iff \widehat{A}+\widehat{B}-\widehat{C}=O$
  $\iff \widehat{A}\,, \widehat{B}\,, -\widehat{C}$ sono allineati .

Quindi, se proviamo

$$(i) \quad \forall C \in \mathscr{C}\ , \Phi(-C) = -\Phi(C)$$

$$(ii) \quad \forall A, B, C \in \mathscr{C}\ ,\ A, B, C \text{ allineati} \implies \Phi(A), \Phi(B), \Phi(C) \text{ allineati,}$$

avremo anche $\Phi(A+B) = \Phi(C) = \Phi(A)+\Phi(B)$.
Anzitutto, $\forall C \in \mathscr{C}$ vale

$$\begin{aligned}\Phi(-C) = \Phi(x_C, -y_C) &= \left(\left(\frac{-y_C}{x_C}\right)^2, \frac{-y_C(x_C^2-b)}{x_C^2}\right)\\ &= \left(\left(\frac{y_C}{x_C}\right)^2, \frac{-y_C(x_C^2-b)}{x_C^2}\right) = -\Phi(C)\end{aligned} \tag{4.16}$$

cioè (i). Proviamo ora (ii); per quanto detto sopra, possiamo supporre $A, B \neq O, T$. Per prima cosa osserviamo che se $A = -B$, allora A, B, C sono allineati $\Leftrightarrow$ $C = O$, quindi per (i)

$$\begin{aligned}\Phi(A+B+C) = \Phi(O) = O = O+O &= \Phi(A)-\Phi(A)+\Phi(O)\\ &= \Phi(A)+\Phi(B)+\Phi(C)\ .\end{aligned}$$

Supponiamo ora che A, B, C, con $A \neq -B$, siano sulla retta

$$y = \lambda x + \mu;$$

se $\mu = 0$, uno dei tre punti è T, necessariamente C. Allora

$$A + B + T = O \implies A + B = -T = T \implies B = T - A$$

quindi per (4.15) e (4.16) si ha

$$\Phi(B) = \Phi(T - A) = \Phi(-A) \implies \Phi(B) = -\Phi(A) \tag{4.17}$$

pertanto $\Phi(A), \Phi(B), \Phi(C) = \Phi(T) = O$ sono allineati (per la precisione, sulla retta $x = \frac{y_A^2}{x_A^2}$).

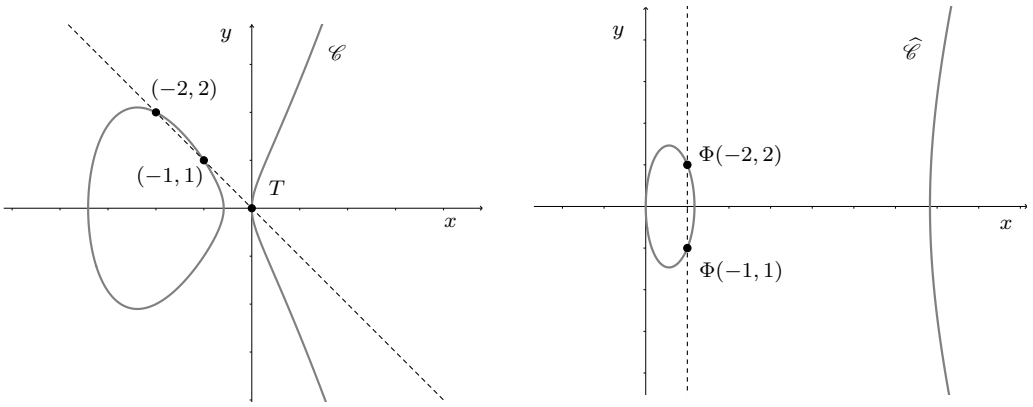


Figura 4.2. Esempio sulle cubiche date da (4.11) e (4.12) con $a = 4$, $b = 2$.

Sia dunque $\mu \neq 0$; mostriamo che $\Phi(A)$, $\Phi(B)$, $\Phi(C)$ giacciono sulla retta

$$y = \widehat{\lambda}\, x + \widehat{\mu} \qquad \text{con } \widehat{\lambda} = \frac{\lambda\mu - b}{\mu}\ ,\ \widehat{\mu} = \frac{\mu^2 - a\lambda\mu + b\lambda^2}{\mu}$$

o meglio che $\widehat{x}_A = \frac{y_A^2}{x_A^2}$, $\widehat{x}_B = \frac{y_B^2}{x_B^2}$, $\widehat{x}_C = \frac{y_C^2}{x_C^2}$ sono tutte e sole le soluzioni dell'equazione

$$(\widehat{\lambda}\, x + \widehat{\mu}\,)^2 = \widehat{f}\,(x)\ .$$

Facciamo vedere che se un punto $A \in \mathscr{C}$ sta sulla retta $y = \lambda x + \mu$, allora $\Phi(A) \in \widehat{\mathscr{C}}$ sta sulla retta $y = \widehat{\lambda}\, x + \widehat{\mu}$. Infatti:

$$\widehat{\lambda}\, \widehat{x}_A + \widehat{\mu} = \frac{(\lambda\mu - b)y_A^2 + x_A^2(\mu^2 - a\lambda\mu + b\lambda^2)}{\mu x_A^2}$$

$$= \frac{\lambda\mu(y_A^2 - ax_A^2) - b(y_A - \lambda x_A)(y_A + \lambda x_A) + \mu^2 x_A^2}{\mu x_A^2}$$
$$= \frac{\lambda\mu(x_A^3 + bx_A) - b\mu(y_A + \lambda x_A) + \mu^2 x_A^2}{\mu x_A^2}$$
$$= \frac{x_A^2(\lambda x_A + \mu) - by_A}{x_A^2} = y_A\left(\frac{x_A^2 - b}{x_A^2}\right) = \widehat{y}_A\ ,$$

dove abbiamo usato le relazioni $y_A^2 - ax_A^2 = x_A^3 + bx_A$, $y_A - \lambda x_A = \mu$.
I conti visti però non dicono niente sulla molteplicità di $\widehat{x}_A$,$\widehat{x}_B$, $\widehat{x}_C$ come radici complesse di $(\widehat{\lambda}\,x + \widehat{\mu}\,)^2 = \widehat{f}\,(x)$: ci stiamo chiedendo cioè se esistono altre radici nel caso in cui due o più fra $\widehat{x}_A$, $\widehat{x}_B$, $\widehat{x}_C$ coincidano. Questo è possibile, come si vede nell'esempio qui sotto:

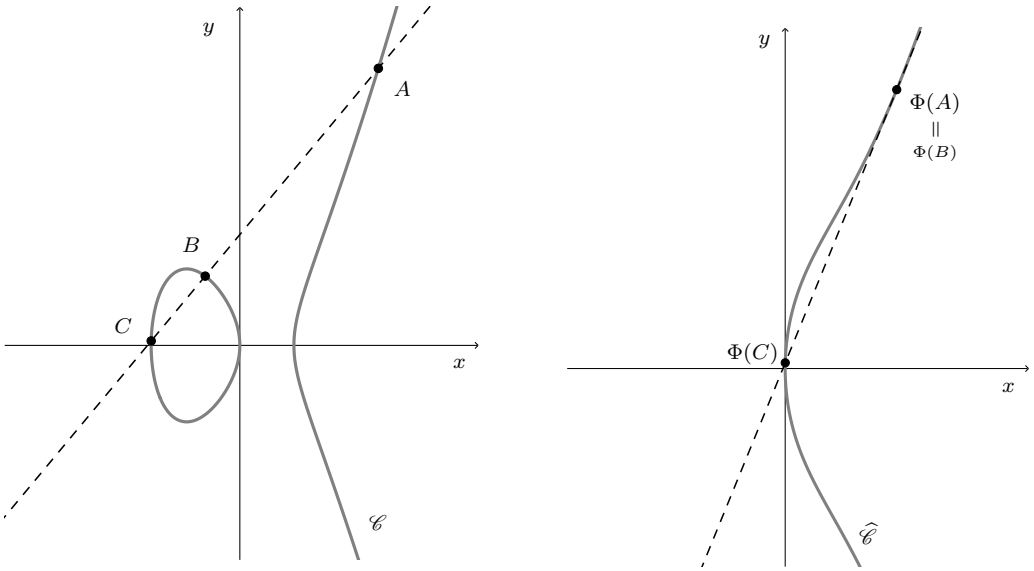


Figura 4.3. Esempio sulle cubiche date da (4.11) e (4.12) con $a = 1$, $b = -4$, $A = (4, 8)$, $B = (-1, 2)$.

Osserviamo allora che x_A,x_B, x_C sono le radici di $(\lambda x + \mu)^2 = f(x)$ se e solo se

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\mu)x - \mu^2 = x^3 - (x_A + x_B + x_C)x^2 + \\ + (x_Ax_B + x_Ax_C + x_Bx_C)x - (x_Ax_Bx_C)$$

cioè se e solo se valgono le relazioni

$$(a) \quad \lambda^2 - a = x_A + x_B + x_C$$

$$(b) \quad b - 2\lambda\mu = x_A x_B + x_A x_C + x_B x_C$$
$$(c) \quad \mu^2 = x_A x_B x_C \ .$$

Usando queste, con un po' di pazienza si verifica che

$$\widehat{\lambda}^2 - \widehat{a} = \left(\frac{y_A}{x_A}\right)^2 + \left(\frac{y_B}{x_B}\right)^2 + \left(\frac{y_C}{x_C}\right)^2$$
$$\widehat{b} - 2\widehat{\lambda}\widehat{\mu} = \frac{(y_A y_B x_C)^2 + (y_A x_B y_C)^2 + (x_A y_B y_C)^2}{(x_A x_B x_C)^2}$$
$$\widehat{\mu}^2 = \left(\frac{y_A y_B y_C}{x_A x_B x_C}\right)^2$$

dunque il polinomio $(\widehat{\lambda}\,x + \widehat{\mu}\,)^2 - \widehat{f}\,(x)$ si scompone in effetti come $(x - \widehat{x}_A)(x - \widehat{x}_B)(x - \widehat{x}_C)$. Per quanto detto sopra, la tesi è provata. □

Corollario 4.2.3. *Siano $\mathscr{C}$, $\widehat{\mathscr{C}}$ le cubiche razionali lisce di equazione rispettivamente* (4.11) *e* (4.12)*; allora*

$$\begin{aligned} \Psi : \qquad \widehat{\mathscr{C}} &\longrightarrow \mathscr{C} \\ (\widehat{x}\,, \widehat{y}\,) &\longmapsto \left(\frac{\widehat{y}^{\,2}}{4\widehat{x}^{\,2}}\,,\ \widehat{y}\,\frac{\widehat{x}^{\,2} - \widehat{b}}{8\widehat{x}^{\,2}}\right) \qquad \textit{se } \widehat{x} \neq 0 \\ T = (0,0) &\longmapsto O \\ O &\longmapsto O \end{aligned} \tag{4.18}$$

è un morfismo di gruppi. Inoltre, se Φ è l'applicazione definita in (4.14)*, si ha*

$$\begin{aligned} \Psi \circ \Phi : \mathscr{C} &\longrightarrow \mathscr{C} \\ A &\longmapsto 2A \ . \end{aligned}$$

Dimostrazione. Per la proposizione precedente, l'applicazione

$$\begin{aligned} \Psi_1 : \qquad \widehat{\mathscr{C}} &\longrightarrow \widehat{\widehat{\mathscr{C}}} \\ (\widehat{x}\,, \widehat{y}\,) &\longmapsto \left(\frac{\widehat{y}^{\,2}}{\widehat{x}^{\,2}}\,,\ \widehat{y}\,\frac{\widehat{x}^{\,2} - \widehat{b}}{\widehat{x}^{\,2}}\right) \qquad \text{se } \widehat{x} \neq 0 \\ T = (0,0) &\longmapsto O \\ O &\longmapsto O \end{aligned}$$

è un morfismo di gruppo fra $\widehat{\mathscr{C}}$ e $\widehat{\widehat{\mathscr{C}}}$; d'altra parte, per quanto detto nell'osservazione 4.2.b, $\widehat{\widehat{\mathscr{C}}}$ è affinemente equivalente a $\mathscr{C}$ tramite l'affinità α, che induce un isomorfismo di gruppi:

$$\begin{aligned} \Psi_2 : \quad \widehat{\widehat{\mathscr{C}}} &\longrightarrow \mathscr{C} \\ (x,y) &\longmapsto \left(\frac{x}{4}, \frac{y}{8}\right) . \end{aligned}$$

Pertanto l'applicazione $\Psi = \Psi_2 \circ \Psi_1$ è ben definita ed è morfismo di gruppi da $\widehat{\mathscr{C}}$ a $\mathscr{C}$.
Consideriamo ora il morfismo $\Psi \circ \Phi = \Psi_2 \circ \Psi_1 \circ \Phi : \mathscr{C} \longrightarrow \mathscr{C}$; proviamo che vale $\Psi \circ \Phi(A) = 2A$ per ogni $A \in \mathscr{C}$.
Poiché $\ker \Psi = \{O, T\}$, risulta

$$\begin{gathered} \Psi \circ \Phi(A) = O \iff \Phi(A) = O \text{ oppure } \Phi(A) = T \\ \iff A = O \text{ oppure } A = T \text{ oppure } \left(\frac{y_A^2}{x_A^2}\,,\, y_A \frac{x_A^2 - b}{x_A^2}\right) = (0,0) \\ \iff y_A = 0 \end{gathered}$$

dunque per gli elementi di ordine ≤ 2 vale $\Psi \circ \Phi(A) = 2A$.
Se $2A \neq O$, nè x_A nè y_A sono nulli, quindi possiamo scrivere

$$\Phi(x_A, y_A) = \left(\frac{y_A^2}{x_A^2}\,,\, y_A \frac{x_A^2 - b}{x_A^2}\right) \,,\; \Psi(\widehat{x}_A, \widehat{y}_A) = \left(\frac{\widehat{y}_A^{\,2}}{\widehat{x}_A^{\,2}}\,,\, \widehat{y}_A \frac{\widehat{x}_A^{\,2} - b}{\widehat{x}_A^{\,2}}\right)$$

e componendo si trova

$$\begin{aligned} \Psi \circ \Phi(A) &= \Psi\left(\frac{y_A^2}{x_A^2}\,,\, y_A \frac{x_A^2 - b}{x_A^2}\right) \\ &= \left(\frac{\left(y_A \frac{x_A^2 - b}{x_A^2}\right)^2}{4\left(\frac{y_A^2}{x_A^2}\right)^2}\,,\, y_A \frac{x_A^2 - b}{x_A^2}\left(\frac{\left(\frac{y_A^2}{x_A^2}\right)^2 - a^2 - 4b}{8\left(\frac{y_A^2}{x_A^2}\right)^2}\right)\right) \\ &= \left(\left(\frac{x_A^2 - b}{2y_A}\right)^2\,,\, y_A \frac{x_A^2 - b}{x_A}\left(\frac{y_A^4 - a^2 x_A^4 + 4b x_A^4}{8 y_A^4}\right)\right) \\ &= \left(\left(\frac{x_A^2 - b}{2y_A}\right)^2\,,\, \frac{x_A^2(x_A^2 - b)((x_A^2 + a x_A + b)^2 - a^2 x_A^2 + 4b x_A^2)}{8 y_A^3 x_A^2}\right) \end{aligned}$$

$$= \left(\left(\frac{x_A^2 - b}{2y_A} \right)^2 \, , \, \frac{x_A^6 + 2ax_A^5 + 5bx_A^4 - 5b^2x_A^2 - 2ab^2x_A - b^3}{8y_A^3} \right) .$$

D'altra parte, dalle formule (2.2) e (2.3) con $c = 0$, si ha

$$\begin{aligned} 2A &= \left(\frac{x_A^4 - 2bx_A^2 + b^2}{4y_A^2} \, , \, -\left(\frac{f'(x_A)}{2y_A} \left(\frac{x_A^2 - b}{2y_A} \right)^2 + y_A - \frac{f'(x_A)}{2y_A} x_A \right) \right) \\ &= \left(\left(\frac{x_A^2 - b}{2y_A} \right)^2 \, , \, -\frac{f'(x_A)(x_A^2 - b)^2 + 8y_A^4 - 4x_A y_A^2 f'(x_A)}{8y_A^3} \right) \\ &= \left(\left(\frac{x_A^2 - b}{2y_A} \right)^2 \, , \, -\frac{-x_A^6 - 2ax_A^5 - 5bx_A^4 + 5b^2x_A^2 + 2ab^2x_A + b^3}{8y_A^3} \right) = \Psi \circ \Phi(A) \, , \end{aligned}$$

come volevamo. □

Osservazione 4.2.c. Si noti che tutti i morfismi di questa sezione sono visti sui punti di $\mathscr{C}$ come curva su $\mathbb{C}$. Quindi la mappa Φ definita in (4.14) è suriettiva, infatti se $\widehat{A} = (\widehat{x}, \widehat{y}) \in \widehat{\mathscr{C}}$, $\widehat{A} \neq O$, T, e ω è una fissata radice di $\widehat{x}$, i punti $A_1 = (x_1, y_1)$, $A_2 = (x_2, y_2)$ definiti da

$$\begin{aligned} x_1 &= \frac{1}{2}\left(\omega^2 - a + \frac{\widehat{y}}{\omega} \right) \quad , \quad y_1 = x_1\omega \\ x_2 &= \frac{1}{2}\left(\omega^2 - a - \frac{\widehat{y}}{\omega} \right) \quad , \quad y_1 = -x_2\omega \end{aligned} \tag{4.19}$$

appartengono a $\mathscr{C}$ e sono tali che $\Phi(A_1) = \Phi(A_2) = \widehat{A}$. Prima di mostrare questi fatti, osserviamo che, siccome valgono

$$\widehat{y}^2 = \widehat{x}^3 - 2a\widehat{x}^2 + (a^2 - 4b)\widehat{x} \quad , \quad \omega^2 = \widehat{x}$$

allora

$$\begin{aligned} x_1x_2 &= \frac{1}{4}\left((\omega^2 - a)^2 - \left(\frac{\widehat{y}}{\omega} \right)^2 \right) = \frac{1}{4}\left((\widehat{x} - a)^2 - \frac{\widehat{y}^2}{\widehat{x}} \right) \\ &= \frac{1}{4}\left(\frac{\widehat{x}^3 - 2a\widehat{x}^2 + a^2\widehat{x} - \widehat{y}^2}{\widehat{x}} \right) \\ &= \frac{1}{4}\left(\frac{4b\widehat{x}}{\widehat{x}} \right) = b \, . \end{aligned}$$

Essendo $\mathscr{C}$ non singolare, deve essere $b \neq 0$, cioè $x_1x_2 \neq 0$. Quindi, per come sono stati definiti y_1, y_2, vale $\frac{y_1}{x_1} = \omega$, $\frac{y_2}{x_2} = -\omega$. Usando le relazioni appena trovate,

per $i = 1, 2$ risulta

$$A_i = (x_i, y_i) \in \mathscr{C} \iff y_i^2 = x_i^3 + ax_i^2 + bx_i$$
$$\iff \frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i} \iff \omega^2 = x_1 + x_2 + a \ .$$

D'altra parte, per la (4.19) si ha

$$x_1 + x_2 = \frac{1}{2}\left(\omega^2 - a + \frac{\widehat{y}}{\omega}\right) + \frac{1}{2}\left(\omega^2 - a - \frac{\widehat{y}}{\omega}\right) = \omega^2 - a$$

dunque A_1, $A_2 \in \mathscr{C}$.
Mostriamo ora $\Phi(A_i) = \widehat{A}$; sempre per le relazioni trovate prima e per (4.19), abbiamo

$$\frac{y_i^2}{x_i^2} = \omega^2 = \widehat{x} \ , \ i = 1, 2$$
$$y_1\left(\frac{x_1^2 - b}{x_1^2}\right) = \frac{y_1}{x_1}\left(\frac{x_1^2 - x_1x_2}{x_1}\right) = \omega(x_1 - x_2)$$
$$y_2\left(\frac{x_2^2 - b}{x_2^2}\right) = \frac{y_2}{x_2}\left(\frac{x_2^2 - x_1x_2}{x_2}\right) = -\omega(x_2 - x_1)$$

ed anche

$$\omega(x_1 - x_2) = \frac{\omega}{2}\left(\frac{2\widehat{y}}{\omega}\right) = \widehat{y}$$

da cui $\Phi(A_1) = \Phi(A_2) = \widehat{A}$.

Notiamo che anche la mappa Ψ, definita in (4.18), che è composizione di un morfismo suriettivo e uno biettivo, è suriettivo.

Osservazione 4.2.d. Poiché Φ è suriettiva, $\forall \widehat{A} \in \widehat{\mathscr{C}}$ esiste $A \in \mathscr{C}$ tale che $\Phi(A) = \widehat{A}$. Consideriamo il morfismo $\Phi \circ \Psi : \widehat{\mathscr{C}} \longrightarrow \widehat{\mathscr{C}}$; si ha

$$\Phi \circ \Psi(\widehat{A}) = \Phi(\Psi \circ \Phi(A)) = \Phi(2A) = 2\Phi(A) = 2\widehat{A}$$

ovvero $\Phi \circ \Psi$ è la mappa di duplicazione su $\widehat{\mathscr{C}}$.

4.3 L'indice di $2\mathscr{C}(\mathbb{Q})$ in $\mathscr{C}(\mathbb{Q})$

Nel seguito utilizziamo le notazioni di sezione 4.2, e se $\mathscr{C}$, $\widehat{\mathscr{C}}$ sono le cubiche di equazione rispettivamente (4.11), (4.12), indichiamo con Γ il gruppo $\mathscr{C}(\mathbb{Q})$, con $\widehat{\Gamma}$ il gruppo $\widehat{\mathscr{C}}\,(\mathbb{Q})$.
Il nostro scopo ora è provare

$$[\Gamma : 2\Gamma] < \infty \; ; \qquad (\bigstar)$$

sappiamo che $2\Gamma = \Psi \circ \Phi(\Gamma)$, dove Φ e Ψ sono le mappe definite in (4.14) e (4.18) rispettivamente; notiamo inoltre che valgono le inclusioni (di gruppi)

$$\Phi(\Gamma) \subseteq \widehat{\Gamma} \quad , \quad \Psi(\widehat{\Gamma}\,) \subseteq \Gamma \; .$$

Allora, se mostriamo

$$(\mathbf{a}) \qquad [\Gamma : \Psi(\widehat{\Gamma}\,)] \; , \; [\widehat{\Gamma} : \Phi(\Gamma)] < \infty$$
$$(\mathbf{b}) \qquad [\Gamma : 2\Gamma] \leq [\Gamma : \Psi(\widehat{\Gamma}\,)] \cdot [\widehat{\Gamma} : \Phi(\Gamma)]$$

avremo anche $(\bigstar)$ e potremo procedere alla dimostrazione del teorema di Mordell. Iniziamo con (**a**), e studiamo le immagini $\Phi(\Gamma)$, $\Psi(\widehat{\Gamma}\,)$.

Proposizione 4.3.1. *Nelle notazioni precedenti si ha:*

(i) $O \in \Phi(\Gamma)$

(ii) $T \in \Phi(\Gamma) \;\Leftrightarrow\; \widehat{b} = a^2 - 4b$ *è il quadrato di un numero intero*

(iii) *se* $\widehat{A} \in \widehat{\Gamma}$, $\widehat{A} = (\widehat{x}_{\,A}, \widehat{y}_{\,A})$ *con* $\widehat{x}_{\,A} \neq 0$, *vale* $\widehat{A} \in \Phi(\Gamma)$ *se e solo se* $\widehat{x}_{\,A}$ *è il quadrato di un numero razionale.*

Dimostrazione. (i) È ovvio perché $O \in \Gamma$ e $\Phi(O) = O$

(ii) Anzitutto, $T \in \Phi(\Gamma) \;\Leftrightarrow\; \exists A = (x_A, y_A) \in \Gamma$, $A \neq T$, tale che

$$\left(\frac{y_A^2}{x_A^2} \, , \, y_A \frac{x_A^2 - b}{x_A^2} \right) = (0, 0) \; ,$$

cioè se e solo se $y_A = 0$ e $x_A \neq 0$.
Ora, affinché $A = (x_A, 0)$ sia un elemento di Γ diverso da $(0, 0)$, occorre e basta che x_A sia una radice razionale del polinomio

$$q(x) = x^2 + ax + b$$

(ricordiamo che $b \neq 0$ perché $\mathscr{C}$ è liscia, quindi 0 non è una radice); ma $q(x)$ ha soluzioni razionali $\Leftrightarrow$ il discriminante $\Delta = a^2 - 4b$ è un quadrato in $\mathbb{Z}$.

(*iii*) Sia $\widehat{A} = (\widehat{x}_A, \widehat{y}_A) \in \Phi(\Gamma)$; allora $\exists A = (x_A, y_A) \in \Gamma$ tale che $\widehat{x}_A = \frac{y_A^2}{x_A^2}$, quindi certamente $\widehat{x}_A$ è il quadrato di un numero razionale.
Viceversa, se $\widehat{x}_A = \omega^2$, $\omega \in \mathbb{Q}$, sappiamo per l'osservazione 4.2.c che esistono due punti A_1, A_2 mappati da Φ in A (e solo due); A_1 e A_2 hanno coordinate rispettivamente (x_1, y_1), (x_2, y_2) date dalla (4.19), dunque appartengono a Γ, e $\widehat{A} \in \Phi(\Gamma)$. □

È bene notare che la proposizione appena vista vale ancora scambiando $\mathscr{C}$ con $\widehat{\mathscr{C}}$, Γ con $\widehat{\Gamma}$, e sostituendo Ψ a Φ, b a $\widehat{b}$.

Per mostrare l'affermazione (**a**) di pagina 90, o equivalentemente

$$\left|\Gamma \Big/ \Psi(\widehat{\Gamma})\right| \ , \ \left|\widehat{\Gamma} \Big/ \Phi(\Gamma)\right| < \infty$$

faremo vedere che questi due insiemi sono in corrispondenza biunivoca con un insieme finito; a tal scopo introduciamo la seguente

Notazione 5. Sia $(\mathbb{Q}^*, \cdot)$ il gruppo moltiplicativo dei numeri razionali non nulli; indichiamo con $\mathbb{Q}^{*2}$ il sottogruppo

$$\mathbb{Q}^{*2} = \{u^2 \mid u \in \mathbb{Q}\} \ .$$

Inoltre, se Γ è il gruppo dei punti razionali della cubica liscia $\mathscr{C}$ data da (4.11), definiamo l'applicazione

$$\begin{aligned} \xi : \qquad \Gamma &\longrightarrow \mathbb{Q}^* \big/ \mathbb{Q}^{*2} \\ O &\longmapsto [1] \\ T = (0,0) &\longmapsto [b] \\ (x,y) &\longmapsto [x] \quad \text{se } x \neq 0 \ . \end{aligned} \tag{4.20}$$

Si ha:

Proposizione 4.3.2. *Nelle notazioni precedenti si ha:*

(I) *l'applicazione* $\xi : \Gamma \to \mathbb{Q}^* \big/ \mathbb{Q}^{*2}$ *definita sopra è un omomorfismo di gruppi;*

(II) $\ker \xi = \Psi(\widehat{\Gamma})$*; in particolare abbiamo un morfismo iniettivo di gruppi*

$$\Gamma \Big/ \Psi(\widehat{\Gamma}) \lhook\joinrel\longrightarrow \mathbb{Q}^* \big/ \mathbb{Q}^{*2} \ ;$$

(III) *se il coefficiente b si fattorizza come $b = p_1^{k_1} \cdot ... \cdot p_t^{k_t}$, p_i primi, $k_i > 0$ per $i = 1, ..., t$, allora*

$$\operatorname{Im} \xi \subseteq \{\pm[p_1^{\varepsilon_1} \cdot ... \cdot p_t^{\varepsilon_t}] \mid \varepsilon_i = 0, 1 \ , \ i = 1, ..., t\} \ ;$$

(IV) $[\Gamma : \Psi(\widehat{\Gamma})] \leq 2^{t+1}$.

Dimostrazione. (I) Occorre mostrare che $\forall A, B \in \Gamma$ vale $\xi(A+B) = \xi(A)\xi(B)$. Se uno fra A o B coincide con O, è banale; se invece $A = T \neq B = (x_B, y_B)$, come abbiamo visto nella dimostrazione della proposizione 4.2.2 (si veda (4.15))

$$T + B = \left(\frac{b}{x_B}, -\frac{by_B}{x_B^2} \right) \implies \xi(T + B) = \left[\frac{b}{x_B} \right]$$

dove $\left[\frac{1}{x_B} \right] = [x_B]$, giacché $[x_B] \cdot [x_B] = [x_B^2] = [1]$ in $\mathbb{Q}^* \big/ \mathbb{Q}^{*2}$, quindi

$$\xi(T + B) = [b] \cdot [x_B] = \xi(T)\xi(B) \ .$$

Se $A = B = T$, allora $\xi(T + T) = \xi(O) = [1] = [b] \cdot [b] = \xi(T)\xi(T)$.
Se $A = -B$, $A, B \neq O, T$, allora $x_A = x_B$, quindi

$$\xi(A + B) = \xi(O) = [1] = [x_A] \cdot [x_A] = \xi(A)\xi(B) \ .$$

Ora procediamo in maniera simile alla dimostrazione della proposizione 4.2.2: mostriamo che $\forall A, B, C \in \mathscr{C}$, se A, B, C sono allineati ($\Leftrightarrow A + B + C = O$), allora

$$\xi(A)\xi(B)\xi(C) = [1] \ . \tag{4.21}$$

Da qui, poiché $\forall C \in \mathscr{C}$, $C \neq O, T$, vale

$$\xi(-C) = \xi(x_C, -y_C) = [x_C] = \left[\frac{1}{x_C} \right] = \xi(C)^{-1} \ ,$$

avremo $\xi(A + B) = \xi(-C) = \xi(C)^{-1} = \xi(A)\xi(B)$.

Per quanto detto sopra, possiamo supporre $A, B \neq O, T$, $A \neq -B$.
Ora, abbiamo visto tante volte che se A, B, C sono allineati sulla retta $y = \lambda x + \mu$, allora le loro ascisse x_A, x_B, x_C sono radici del polinomio

$$(\lambda x + \mu)^2 - x^3 - ax^2 - bx$$

e valgono le relazioni

$$\begin{aligned} &x_A + x_B + x_C = \lambda^2 - a \ , \\ &x_A x_B + x_A x_C + x_B x_C = b - 2\lambda\mu \ , \\ &x_A x_B x_C = \mu^2 \ . \end{aligned} \tag{4.22}$$

Se $\mu = 0$, poiché abbiamo supposto $A, B \neq T$, dovrà essere $C = T$, quindi

$$\begin{aligned} A + B + T = O \implies A = -(B + T) \\ \implies \xi(A) = \xi(B + T)^{-1} = (\xi(B)\xi(T))^{-1} \end{aligned}$$

e quindi (4.21).
Se $\mu \neq 0$, dall'ultima delle relazioni (4.22) si ha

$$\xi(A)\xi(B)\xi(C) = [x_A x_B x_C] = [\mu^2] = [1] \ .$$

(II) Nel nucleo di ξ c'è ovviamente O, ci sono tutti gli $A = (x_A, y_A) \in \Gamma$ tali che x_A è un quadrato in $\mathbb{Q}$, e c'è anche T se b è un quadrato; dalla proposizione 4.3.1 sappiamo che questi sono proprio tutti e soli i punti di $\Psi(\widehat{\Gamma}\,)$.

(III) Sia $A = (x_A, y_A) \in \Gamma$, $A \neq T$; ricordiamo che possiamo scrivere $A = (\frac{m}{d^2}, \frac{n}{d^3})$ con $(m, d) = (n, d) = 1$. Supponiamo anche $m > 0$ (per $m < 0$ il ragionamento è identico). Siano poi $p_1, ..., p_t$ i fattori primi distinti di b; vogliamo provare che esistono $\varepsilon_1, ..., \varepsilon_t$ con $\varepsilon_i = 0, 1$ per $i = 1, ..., t$, tali che

$$\xi(A) = [x_A] = [m] = [p_1^{\varepsilon_1} \cdot ... \cdot p_t^{\varepsilon_t}] \tag{4.23}$$

ovvero che m si può scrivere come

$$m = k^2 p_1^{\varepsilon_1} \cdot ... \cdot p_t^{\varepsilon_t} \ , \ k \in \mathbb{Q} \ .$$

Al solito, sostituendo le coordinate di A nell'equazione di $\mathscr{C}$ e moltiplicando

tutto per d^6 si trova

$$n^2 = m^3 + am^2d^2 + bmd^4 = m(m^2 + amd^2 + bd^4) \; ; \qquad (4.24)$$

se $D = \mathrm{MCD}(m, m^2 + amd^2 + bd^4)$, allora D deve dividere bd^4, e non può dividere d^4 dato che $(m, d) = 1$. Quindi $D \mid b$; poiché $b = p_1^{k_1} \cdot ... \cdot p_t^{k_t}$, i possibili fattori primi di D sono solo $p_1, ..., p_t$, quindi esistono $\bar{D} \in \mathbb{Z}$, $\varepsilon_1, ..., \varepsilon_t$, $\varepsilon_i = 0$ o $\varepsilon_i = 1$ per $i = 1, ..., t$, tali che

$$D = \bar{D}^2 p_1^{\varepsilon_1} \cdot ... \cdot p_t^{\varepsilon_t} \; .$$

D'altra parte, se p è un primo che divide m e non D, allora non divide neanche $m^2 + amd^2 + bd^4$; poiché per (4.24) p è un fattore anche di n^2, sarà fattore di m secondo una potenza pari. In definitiva, posto $m = \bar{m}D$, $\bar{m}$ deve essere un quadrato, e

$$m = \bar{m}D = \bar{m}\bar{D}^2 p_1^{\varepsilon_1} \cdot ... \cdot p_t^{\varepsilon_t} = k^2 p_1^{\varepsilon_1} \cdot ... \cdot p_t^{\varepsilon_t} \; , \; k \in \mathbb{Z}$$

da cui si ha (4.23).
Se $A = T$, vale $\xi(A) = [b]$, che ovviamente si può scrivere come $\pm[p_1^{\varepsilon_1} \cdot ... \cdot p_t^{\varepsilon_t}]$, $\varepsilon_i = 0, 1$ per $i = 1, ..., t$.

(IV) L'insieme

$$\Lambda = \{\pm[p_1^{\varepsilon_1} \cdot ... \cdot p_t^{\varepsilon_t}] \mid p_i \text{ primi } \; , \; p_i \text{ divide } b \; , \; \varepsilon_i = 0, 1 \; , \; i = 1, ..., t\}$$

è un sottogruppo di $\mathbb{Q}^* \big/ \mathbb{Q}^{*2}$ (la verifica è immediata), e l'inclusione (III) è un'inclusione di gruppi; Λ contiene $2 \cdot 2^t$ elementi (tutti i prodotti dei primi $p_1, ..., p_t$ presi con esponente zero o uno, con il segno $+$ o $-$); per i punti (II) e (III) e per il teorema fondamentale di omomorfismo fra gruppi vale

$$\Gamma \big/ \ker \xi \cong \mathrm{Im}\, \xi \subseteq \Lambda \quad , \quad \Gamma \big/ \ker \xi = \Gamma \Big/ \Psi(\widehat{\Gamma}\,)$$

pertanto

$$[\Gamma : \Psi(\widehat{\Gamma}\,)] = \Big| \Gamma \Big/ \Psi(\widehat{\Gamma}\,) \Big| \leq |\Lambda| = 2^{t+1}. \qquad \square$$

Questo risultato vale ovviamente anche per $\widehat{\Gamma}\Big/\Phi(\Gamma)$, infatti posto

$$\begin{aligned} \widehat{\xi}: \quad \widehat{\Gamma} &\longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2} \\ \widehat{O} &\longmapsto [1] \\ (0,0) &\longmapsto [\,\widehat{b}\,] \\ (x,y) &\longmapsto [x] \quad \text{se } x \neq 0\ . \end{aligned} \tag{4.25}$$

e ragionando esattamente come sopra, si trova

$$[\widehat{\Gamma} : \Phi(\Gamma)] \leq 2^{s+1}\ ,$$

dove s è il numero di fattori primi distinti di $\widehat{b}$. Questo conclude la prova dell'affermazione (**a**).
La (**b**) segue subito dalla seguente

Proposizione 4.3.3. *Siano G, H gruppi abeliani, e supponiamo che esistano due omomorfismi $\Phi : G \to H$, $\Psi : H \to G$ tali che*

(i) $\forall g \in G$, $\forall h \in H$, si abbia

$$\Psi \circ \Phi(g) = 2g \quad , \quad \Phi \circ \Psi(h) = 2h$$

(ii) $[G : \Psi(H)]$, $[H : \Phi(G)] < \infty$;

allora vale

$$[G : 2G] \leq [G : \Psi(H)] \cdot [H : \Phi(G)]\ .$$

Dimostrazione. Per l'ipotesi (ii), esistono $g_1, ..., g_s \in G$, $h_1, ..., h_t \in H$, $s, t \in \mathbb{N}$, tali che

$$\begin{aligned} G\Big/\Psi(H) &= \{[g_1], ..., [g_s]\} \\ H\Big/\Phi(G) &= \{[h_1], ..., [h_t]\}\ . \end{aligned}$$

Mostriamo che vale

$$G/2G = \{[g_i + \Psi(h_j)]\ ,\ i = 1, ..., s\ ,\ j = 1, ..., t\} \tag{$\blacklozenge$}$$

o equivalentemente

$$\forall g \in G \quad \exists\, g' \in G\ ,\ i \in \{1,..,s\}\ ,\ j \in \{1,...,t\} \text{ tali che}$$
$$g = 2g' + g_i + \Psi(h_j)\ .$$

Sia dunque $g \in G$; g è contenuto in una della classi di $G\Big/\Psi(H)$, sia $[g_i]$, quindi esiste $h \in H$ tale che

$$g - g_i = \Psi(h)\ .$$

A sua volta, h appartiene ad una delle classi di $H\Big/\Phi(G)$, sia $[h_j]$, quindi esiste $g' \in G$ tale che

$$h - h_j = \Phi(g')\ .$$

Così

$$g = g_i + \Psi(h) = g_i + \Psi(h_j + \Phi(g')) = g_i + \Psi(h_j) + 2g'\ ;$$

quindi (⧫) è vera.
La (⧫) significa che $\left|G/2G\right| \leq \left|G\Big/\Psi(H)\right| \cdot \left|H\Big/\Phi(G)\right|$, da cui l'asserto. □

Corollario 4.3.4. *Sia $\mathscr{C}$ una cubica liscia razionale di equazione*

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx\ ,\ a, b \in \mathbb{Z}$$

e sia $\mathscr{C}(\mathbb{Q})$ l'insieme dei punti razionali di $\mathscr{C}$. Allora l'indice di $2\mathscr{C}(\mathbb{Q})$ in $\mathscr{C}(\mathbb{Q})$ è finito, per la precisione

$$[\mathscr{C}(\mathbb{Q}) : 2\mathscr{C}(\mathbb{Q})] \leq 2^{t+s+2}$$

dove t è il numero di fattori primi distinti di b ed s è il numero di fattori primi distinti di $a^2 - 4b$.

Dimostrazione. Le applicazioni Φ e Ψ definite in (4.14) e (4.18) sono morfismi fra $\mathscr{C}(\mathbb{Q})$ e $\widehat{\mathscr{C}}\,(\mathbb{Q})$, e per la proposizione 4.2.2, il corollario 4.2.3 e l'osservazione 4.2.d, Φ e Ψ soddisfano l'ipotesi (i) della proposizione precedente. Inoltre, per la proposizione 4.3.2, soddisfano anche la (ii); dunque

$$[\mathscr{C}(\mathbb{Q}) : 2\mathscr{C}(\mathbb{Q})] \leq [\mathscr{C}(\mathbb{Q}) : \Psi(\widehat{\mathscr{C}}\,(\mathbb{Q}))] \cdot [\widehat{\mathscr{C}}\,(\mathbb{Q}) : \Phi(\mathscr{C}(\mathbb{Q}))] = 2^{t+s+2}\ .$$ □

4.4 Il teorema di Mordell

Riassumiamo quanto visto finora in questo quarto capitolo: data una cubica $\mathscr{C}$ liscia razionale, abbiamo definito una funzione da $\mathscr{C}(\mathbb{Q})$ a $\mathbb{R}^+$, chiamandola altezza, con la proprietà che, fissandone un valore, si trova solo un numero finito di punti di $\mathscr{C}(\mathbb{Q})$ con altezza minore; in più conosciamo una stima dell'altezza della somma di due punti e del doppio di un punto.
Poi, supponendo che $\mathscr{C}$ avesse almeno un punto razionale, abbiamo scritto un'equazione per $\mathscr{C}$ in forma normale "ridotta" (cioè senza termine noto) con i coefficienti interi; così abbiamo potuto studiare $2\mathscr{C}(\mathbb{Q})$ come immagine della composizione di due particolari morfismi, ricavando $[\mathscr{C}(\mathbb{Q}) : 2\mathscr{C}(\mathbb{Q})] < \infty$.
Come si legano tutti questi elementi sarà chiaro nel prossimo teorema, che è valido per tutti i gruppi abeliani con certe proprietà. La dimostrazione di tale teorema fa uso del metodo della "discesa infinita" di Fermat.

Teorema 4.4.1. *Sia $(G, +)$ un gruppo abeliano, e sia definita una funzione $\eta : G \longrightarrow [0, \infty[$ tale che:*

(a) $\forall M \in \mathbb{R}$, *l'insieme* $\{A \in G \mid \eta(A) < M\}$ *è finito*

(b) $\forall Q \in G$, *esiste* $\kappa \in \mathbb{R}$, $\kappa = \kappa(Q)$, *tale che* $\eta(A + Q) \leq 2\eta(A) + \kappa \quad \forall A \in G$

(c) $\exists \tilde{\kappa} \in \mathbb{R}$ *tale che* $\eta(2A) \geq 4\eta(A) - \tilde{\kappa} \quad \forall A \in G$.

Supponiamo inoltre che

(d) *l'indice di $2G$ in G è finito.*

Allora G è finitamente generato.

Dimostrazione. Se A è un elemento di G, indichiamo con $\overline{A}$ la sua classe in ${}^{G}\!/_{2G}$. Per l'ipotesi (d), vale ${}^{G}\!/_{2G} = \{\overline{Q}_1, ..., \overline{Q}_n\}$ dove Q_i, $i = 1, ..., n$ sono rappresentanti fissati.
Sia $A \in G$; A appartiene ad una sola della classi in ${}^{G}\!/_{2G}$, sia $\overline{Q}_{i_1}$, $i_1 \in \{1, ..., n\}$, e si ha

$$A - Q_{i_1} = 2A_1$$

per qualche $A_1 \in G$. Lo stesso vale certamente per A_1, ovvero esiste $i_2 \in \{1, ..., n\}$ tale che

$$A_1 - Q_{i_2} = 2A_2 \ , \ A_2 \in G \ ;$$

dopo m passi troviamo quindi le relazioni

$$\begin{aligned} &A - Q_{i_1} = 2A_1 \\ &A_1 - Q_{i_2} = 2A_2 \qquad\qquad \text{con } \ i_j \in \{1, ..., n\} \\ &... \qquad\qquad\qquad\qquad \text{e } \ A_j \in G \\ &A_{m-1} - Q_{i_m} = 2A_m \qquad\quad \text{per } \ j = 1, ..., m, ... \\ &... \end{aligned} \tag{4.26}$$

da cui si ricava

$$\begin{aligned} A &= Q_{i_1} + 2A_1 = Q_{i_1} + 2Q_{i_2} + 4A_2 = ... \\ &= Q_{i_1} + 2Q_{i_2} + ... + 2^{m-1}Q_{i_m} + 2^m A_m \ . \end{aligned} \tag{4.27}$$

Si osservi che $\forall m \in \mathbb{N}$, $m \geq 1$, è possibile la scrittura (4.27); in particolare A appartiene al sottogruppo di G generato da $Q_1, ..., Q_n, A_m$.
Vogliamo stimare $\eta(A_m)$; anzitutto poniamo $A = A_0$ e osserviamo che, per (b)

$$\forall i = 1, ..., n \quad \exists \kappa_i \in \mathbb{R} \ \text{ tale che } \ \eta(B - Q_i) \leq 2\eta(B) + \kappa_i \quad \forall B \in G$$

quindi posto $\kappa = \max\{\kappa_i \ , \ i = 1, ..., n\}$ si ha

$$\eta(B - Q_i) \leq 2\eta(B) + \kappa \quad \forall B \in G \ , \ \forall i = 1, ..., n. \tag{4.28}$$

Inoltre, per (c) esiste $\tilde{\kappa}$ tale che $\forall j = 0, ..., m$ vale

$$4\eta(A_j) \leq \eta(2A_j) + \tilde{\kappa} \ ;$$

si osservi che κ e $\tilde{\kappa}$ sono costanti che non dipendono dagli A_j.
Quindi per (4.26) e (4.28)

$$\begin{aligned} &\eta(A_j) \leq \eta(A_{j-1} - Q_{i_j}) + \tilde{\kappa} \leq 2\eta(A_{j-1}) + \kappa + \tilde{\kappa} \\ \implies \ &\eta(A_j) \leq \frac{1}{2}\eta(A_{j-1}) + \frac{\kappa + \tilde{\kappa}}{4} \\ &\qquad = \frac{3}{4}\eta(A_{j-1}) - \frac{1}{4}(\eta(A_{j-1}) - (\kappa + \tilde{\kappa})) \qquad\quad \forall j = 1, ..., m \ . \end{aligned}$$

In particolare, se $\eta(A_{j-1}) \geq \kappa + \tilde{\kappa}$ allora $\eta(A_j) \leq \frac{3}{4}\eta(A_{j-1})$.
Poniamo $\ell := \min\{j \geq 0 \mid \eta(A_j) < \kappa + \tilde{\kappa}\}$; tale minimo esiste perché se $\eta(A_j) \geq \kappa + \tilde{\kappa}$ per ogni j in $\mathbb{N}$, siccome la successione $\left\{ \left(\frac{3}{4}\right)^s \eta(A_0) \right\}_{s \in \mathbb{N}}$ tende a zero, anche

la successione $\{\eta(A_j)\}_{j\in\mathbb{N}}$ tende a zero, il che ovviamente non è possibile. Pertanto, esiste $\ell \in \mathbb{N}$ tale che, in (4.26), $\eta(A_\ell) < \kappa + \tilde{\kappa}$ e

$$A = Q_{i_1} + 2Q_{i_2} + ... + 2^{\ell-1}Q_{i_\ell} + 2^\ell A_\ell \ , \quad i_1, ..., i_\ell \in \{1, ..., n\} \ . \tag{4.29}$$

Questo significa che

$$\{Q_1, ..., Q_n\} \cup \{B \in G \mid \eta(B) < \kappa + \tilde{\kappa}\}$$

è un insieme di generatori per G (si osservi che se in (4.29) è $\ell = 0$, A sta in questo insieme di generatori), ed è finito per (a), da cui la tesi. □

Concludiamo presentando finalmente il teorema di Mordell, che enunciamo con l'ipotesi aggiuntiva con cui è stato dimostrato qui, cioè l'esistenza di un punto razionale di ordine 2.

Teorema 4.4.2 (di Mordell). *Sia $\mathscr{C}$ una cubica liscia razionale, e supponiamo che $\mathscr{C}$ abbia almeno un punto razionale di ordine 2. Allora il gruppo $\mathscr{C}(\mathbb{Q})$ dei punti razionali di $\mathscr{C}$ è finitamente generato.*

Dimostrazione. La funzione $h : \mathscr{C}(\mathbb{Q}) \to [0, \infty[$ definita in 4.1.1 soddisfa le ipotesi (a), (b), (c) del teorema 4.4.1, come abbiamo provato nella proposizione 4.1.2 e nei teoremi 4.1.4 e 4.1.7 rispettivamente. Inoltre, come abbiamo ricordato all'inizio della sezione, poiché $\mathscr{C}$ ha un punto razionale di ordine 2, possiamo scriverla come

$$\mathscr{C} : y^2 = x^3 + ax^2 + bx \ , \quad a, b \in \mathbb{Z} \ ,$$

e vale il corollario 4.3.4. Quindi $\Gamma = \mathscr{C}(\mathbb{Q})$ soddisfa anche la condizione (d) del teorema precedente, da cui concludiamo che $\mathscr{C}(\mathbb{Q})$ è finitamente generato. □

4.5 Il rango di $\mathscr{C}(\mathbb{Q})$

Il teorema di Mordell ha una conseguenza immediata: per il teorema fondamentale sui gruppi abeliani finitamente generati [J, teorema 3.13], esistono r, p_j, $\nu_j \in \mathbb{N}$, p_j primi, $\nu_j > 0$, $j = 1, ..., s$, tali che

$$\mathscr{C}(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ volte}} \oplus \mathbb{Z}_{p_1^{\nu_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}} \tag{♠}$$

dove l'intero r si dice *rango* di $\mathscr{C}(\mathbb{Q})$.
Il teorema di Mazur ci dice quali valori di p_j, ν_j sono possibili per il sottogruppo isomorfo a $\mathbb{Z}_{p_1^{\nu_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}}$ degli elementi di ordine finito, e il teorema di Nagell-Lutz ci dà uno strumento per calcolare tali elementi direttamente.
Il passo successivo allora sarebbe studiare gli elementi di ordine infinito, in particolare determinare r; dagli esempi visti nel corso della trattazione possiamo dire che r può essere sia 0 (la cubica dell'esempio 3.5 era tale che $\mathscr{C}(\mathbb{Q})$ conteneva solo 4 punti razionali di ordine ≤ 2, quindi $r = 0$) che > 0 (la cubica dell'esempio 3.3 aveva un punto razionale di ordine infinito, quindi $r \geq 1$). È possibile dire qualcosa di più sul rango?
A breve determineremo un metodo, basato sulla dimostrazione del teorema di Mordell, che permette di calcolare r, ma solo in casi molto particolari; una formula generale, che permetterebbe di dare anche un insieme di generatori di $\mathscr{C}(\mathbb{Q})$, è data dalla congettura di Birch e Swinnerton-Dyer, uno dei *millennium problem*.

Nel seguito usiamo ancora le notazioni della sezione precedente; in particolare $\mathscr{C}$ e $\widehat{\mathscr{C}}$ sono le cubiche definite dalle equazioni rispettivamente (4.11) e (4.12), O denota ancora il punto improprio $[0, 0, 1]$, T denota il punto $(0, 0)$ e $\mathscr{C}(\mathbb{Q}) = \Gamma$, $\widehat{\mathscr{C}}\,(\mathbb{Q}) = \widehat{\Gamma}$.

Proposizione 4.5.1. *Siano ξ, $\widehat{\xi}$ le mappe definite in* (4.20) *e* (4.25)*, e sia r il rango di Γ; allora*

$$2^r = \frac{|\xi(\Gamma)| \cdot |\widehat{\xi}\,(\widehat{\Gamma}\,)|}{4}\ .$$

Dimostrazione. Anzitutto, la relazione (♠) ci dice che

$$\Gamma/2\Gamma \cong \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}_{p_1^{\nu_1}}\Big/2\mathbb{Z}_{p_1^{\nu_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}}\Big/2\mathbb{Z}_{p_s^{\nu_s}}$$

dove $\left|\, \mathbb{Z}/2\mathbb{Z} \,\right| = 2$ e

$$\mathbb{Z}_{p_j^{\nu_j}}\Big/2\mathbb{Z}_{p_j^{\nu_j}} \cong \begin{cases} \mathbb{Z}_2 \text{ se } p_j = 2 \\ \{0\} \text{ altrimenti} \end{cases}\ , \qquad j = 1, ..., s\ .$$

Dunque, posto $k := \#\big\{j \in \{1, ..., s\} \mid p_j = 2\big\}$, si ha

$$\left|\, \Gamma/2\Gamma \,\right| = 2^{r+k}\ . \tag{4.30}$$

Mostriamo che vale $2^k = |\Lambda_2|$, dove con Λ_2 indichiamo il sottogruppo di Γ degli elementi razionali di ordine ≤ 2.
Sempre da (♠) sappiamo che esistono $P_1, ..., P_r, Q_1, ..., Q_s \in \Gamma$, ed esistono $n_\ell \in \mathbb{Z}$, $\ell = 1, ..., r$, $m_j \in \mathbb{Z}$, $0 \leq m_j < p_j^{\nu_j}$, $j = 1, ..., s$, tali che un elemento $P \in \Gamma$ si può scrivere in modo unico come

$$P = n_1 P_1 + \cdots + n_r P_r + m_1 Q_1 + \ldots m_s Q_s$$

(ricordiamo che si pone $0A = O$ per ogni $A \in \Gamma$); se P ha ordine ≤ 2 vale quindi

$$\begin{aligned} 2P = 2(n_1 P_1 + \cdots + n_r P_r + m_1 Q_1 + \ldots m_s Q_s) = O \\ \iff \quad \begin{array}{ll} 2n_\ell = 0 & \text{per } \ell = 1, ..., r \ , \\ 2m_j \equiv 0 \mod p_j^{\nu_j} & \text{per } j = 1, ..., s \ . \end{array} \end{aligned}$$

Ora, se p_j è dispari, si ha $2m_j \equiv 0 \mod p_j^{\nu_j} \Leftrightarrow m_j \equiv 0 \mod p_j^{\nu_j}$, mentre se $p_j = 2$, $2m_j \equiv 0 \mod 2^{\nu_j}$ implica $m_j \equiv 0 \mod 2^{\nu_j - 1}$.
Quindi ogni elemento di ordine ≤ 2 si scrive come $P = m_{j_1} Q_{j_1} + \cdots + m_{j_t} Q_{j_t}$, dove $p_{j_1} = \cdots = p_{j_t} = 2$ e m_{j_i} può assumere solo due valori in $\mathbb{Z}$, cioè 0 o $2^{\nu_{j_i} - 1}$, per $i = 1, ..., t$; in particolare $t = k$ e $|\Lambda_2| = 2^k$.
D'altra parte, sappiamo già dal teorema 2.3.1 e dal corollario 2.3.2 che in generale Λ_2 può avere 1, 2 o 4 elementi; nel nostro caso ci sono sicuramente O e T, quindi

$$|\Lambda_2| = \begin{cases} 2 & \text{se } a^2 - 4b \text{ non è un quadrato in } \mathbb{Q} \\ 4 & \text{se } a^2 - 4b \text{ è un quadrato in } \mathbb{Q} \end{cases}$$

Quindi la (4.30) diventa

$$\left| \Gamma / 2\Gamma \right| = 2^r 2^k \quad \text{con } k = \begin{cases} 1 & \text{se } a^2 - 4b \text{ non è un quadrato in } \mathbb{Q} \\ 2 & \text{altrimenti.} \end{cases}$$

Adesso consideriamo $\left| \Gamma / 2\Gamma \right|$: ricordando che $2\Gamma = (\Psi \circ \Phi)(\Gamma)$, con Φ, Ψ date da (4.14), (4.18) rispettivamente, e che valgono quindi le inclusioni di gruppi $2\Gamma \subseteq \Psi(\widehat{\Gamma}) \subseteq \Gamma$, possiamo scrivere

$$[\Gamma : 2\Gamma] = [\Gamma : (\Psi \circ \Phi)(\Gamma)] = [\Gamma : \Psi(\widehat{\Gamma})] \cdot [\Psi(\widehat{\Gamma}) : (\Psi \circ \Phi)(\Gamma)] \ .$$

Guardiamo il fattore $[\Psi(\widehat{\Gamma}) : (\Psi\circ\Phi)(\Gamma)]$; tenendo presente che, in generale, se $(G,+)$ è un gruppo abeliano, $H \subseteq G$ è un sottogruppo, ψ è un morfismo da G ad un certo gruppo, valgono

$$\begin{aligned}\psi(G)\Big/\psi(H) &\cong \frac{G\big/\ker\psi}{H\Big/(\ker\psi\cap H)} \cong \frac{G\big/\ker\psi}{(H+\ker\psi)\Big/\ker\psi} \cong G\Big/(H+\ker\psi)\\ &\cong \frac{G\big/H}{(H+\ker\psi)\Big/H} \cong \frac{G\big/H}{\ker\psi\Big/(H\cap\ker\psi)}\ ,\end{aligned}$$

e ricordando che $\Phi(\Gamma) \subseteq \widehat{\Gamma}$ come gruppi, risulta, dato che $[\Gamma : 2\Gamma]$ è finito e quindi lo sono anche gli indici dei gruppi che compaiono qui:

$$[\Psi(\widehat{\Gamma}) : \Psi\circ\Phi(\Gamma)] = \frac{[\widehat{\Gamma} : \Phi(\Gamma)]}{[\ker\Psi : (\ker\Psi\cap\Phi(\Gamma))]}$$

dove, dato che $\ker\Psi = \{O,T\}$, si ha (si veda 4.3.1):

$$[\ker\Psi : (\ker\Psi\cap\Phi(\Gamma))] = \begin{cases} 1 \ \text{ se } T\in\Phi(\Gamma)\ (\Leftrightarrow\ a^2-4b \text{ è un quadrato in } \mathbb{Q})\\ 2 \ \text{ se } T\notin\Phi(\Gamma)\ .\end{cases}$$

In definitiva

$$2^r = \frac{[\Gamma : 2\Gamma]}{2^k} = \frac{[\Gamma : \Psi(\widehat{\Gamma})]\cdot[\widehat{\Gamma} : \Phi(\Gamma)]}{2^k[\ker\Psi : (\ker\Psi\cap\Phi(\Gamma))]} = \frac{[\Gamma : \Psi(\widehat{\Gamma})]\cdot[\widehat{\Gamma} : \Phi(\Gamma)]}{4}\ .$$

Infine, dalla (II) della proposizione 4.3.2, abbiamo $[\Gamma : \Psi(\widehat{\Gamma})] = |\xi(\Gamma)|$, $[\widehat{\Gamma} : \Phi(\Gamma)] = |\widehat{\xi}\,(\widehat{\Gamma})|$, da cui l'asserto. □

Osservazione 4.5.a. Vediamo ora come si può calcolare $|\xi(\Gamma)|$ (si ragionerà allo stesso modo per $|\widehat{\xi}\,(\widehat{\Gamma})|$); dalla (III) della proposizione 4.3.2 sappiamo che

$$\xi(\Gamma) \subseteq \Big\{ \pm[p_1^{\varepsilon_1}\cdot\dots\cdot p_t^{\varepsilon_t}] \ \Big|\ \varepsilon_i = 0,1\ ,\ p_i \text{ primo}\ ,\ p_i|b\ ,\ i=1,...,t\Big\}\ ;$$

cerchiamo di determinare più precisamente i valori possibili per $\xi(P)$ con $P\neq O$, $P=(x,y)\in\Gamma$.
Scriviamo $(x,y) = \big(\frac{m}{d^2},\frac{n}{d^3}\big)$, $(m,d) = (n,d) = 1$. Se $m=0$, allora $P=T$ e $\xi(P)=[b]$; se a^2-4b è il quadrato di un razionale e, allora i punti $\big(\frac{-a+e}{2},0\big)$, $\big(\frac{-a-e}{2},0\big)$ sono gli unici altri punti di Γ con $n=0$, e $\big[\frac{-a+e}{2}\big]$, $\big[\frac{-a-e}{2}\big] \in \xi(\Gamma)$.

Supponiamo ora $mn \neq 0$; al solito, sostituendo $\left(\frac{m}{d^2}, \frac{n}{d^3}\right)$ nell'equazione di $\mathscr{C}$ e moltiplicando tutto per d^6, troviamo

$$n^2 = m(m^2 + amd^2 + bd^4) \ .$$

Se $b_1 = \text{sign}(m) \cdot \text{MCD}(b, m)$, allora esistono $b_2, m_1 \in \mathbb{Z}$ tali che $b = b_1 b_2$, $m = m_1 b_1$, con $(m_1, b_2) = 1$ e $m_1 > 0$, e si ha

$$n^2 = m_1 b_1^2 (m_1^2 b_1 + a m_1 d^2 + b_2 d^4)$$

quindi $b_1^2 \mid n^2$, cioè $n = b_1 n_1$. Sostituendo nell'equazione sopra e semplificando b_1^2, troviamo

$$n_1^2 = m_1(m_1^2 b_1 + a m_1 d^2 + b_2 d^4)$$

dove $\text{MCD}(m_1, m_1^2 b_1 + a m_1 d^2 + b_2 d^4) = 1$ e il loro prodotto è un quadrato. Pertanto esistono M, $N \in \mathbb{Z}$, $(M, N) = 1$, tali che $M^2 = m_1$, $N^2 = m_1^2 b_1 + a m_1 d^2 + b_2 d^4$, e vale $n_1 = MN$; sostituendo N, M nell'ultima equazione e semplificando $M \neq 0$ si trova

$$N^2 = M^4 b_1 + a M^2 d^2 + b_2 d^4 \ . \qquad (\blacktriangledown)$$

In definitiva, se $P = (x, y) \in \Gamma$, $x \neq 0$, allora

$$x = \frac{b_1 M^2}{d^2} \ , \ y = \frac{b_1 MN}{d^3} \qquad (4.31)$$

dove (M, d, N) è soluzione intera dell'equazione $(\blacktriangledown)$, b_1, b_2 sono tali che $b_1 b_2 = b$, e M, d, N soddisfano le condizioni

- $M \neq 0$
- $(M, d) = (N, d) = (b_1, d) = 1$ (perché $(m, d) = (n, d) = 1$) $\qquad (\triangledown)$
- $(M, b_2) = (M, N) = 1$ (perché $(m_1, b_2) = 1$)

(notiamo che così si trovano anche i punti con $y = 0$ quando $a^2 - 4b = e^2$, $e \in \mathbb{Q}$: infatti in tal caso $b = \frac{-a+e}{2} \cdot \frac{-a-e}{2}$, e scelto b_1 fra questi due fattori, $(1, 1, 0)$ è soluzione di $(\blacktriangledown)$ che soddisfa $(\triangledown)$).
Viceversa, sia b_1 un divisore di b fissato, e si ponga $b_2 = \frac{b}{b_1}$; allora se (M, d, N) è una soluzione intera di $(\blacktriangledown)$ per cui valgono $(\triangledown)$, tramite la formula (4.31) si

ottiene sempre un punto di Γ.

Ne segue che $\xi(\Gamma)$ è data dagli elementi del tipo $[b_1]$ con $b_1 \mid b$ e tale che esiste una soluzione intera (M, d, N) all'equazione $(\blacktriangledown)$ che verifica le condizioni $(\triangledown)$; quindi, se siamo in grado per ogni divisore b_1 di b di decidere se esiste almeno una soluzione di $(\blacktriangledown)$+$(\triangledown)$ oppure che non ne esistono, allora conosciamo $\xi(\Gamma)$. Si osservi che è sempre vero che $[1] = \xi(0)$ e $[b] = \xi(T)$ per come è stata definita ξ in (4.20); quindi per $b_1 = 1$ e $b_1 = b$ non è necessario cercare soluzioni di $(\blacktriangledown)$. È bene sottolineare che per adesso non si conosce un metodo generale per sapere se un'equazione del tipo $(\blacktriangledown)$ ha soluzioni intere.

4.5.1 Esempi di calcolo del rango

Esempio* 4.1*: una cubica con* Γ *di rango* 1*.
Proviamo a calcolare il rango di

$$\mathscr{C} : y^2 = x^3 - 5x$$

usando la formula $2^r = \frac{|\xi(\Gamma)| \cdot |\widehat{\xi}(\widehat{\Gamma})|}{4}$. Per quanto detto sopra, per determinare quali elementi sono contenuti in $\xi(\Gamma)$ si cercano le soluzioni intere all'equazione

$$N^2 = M^4 b_1 + aM^2 d^2 + b_2 d^4 \ . \qquad (\blacktriangledown)$$

dove $a = 0$ e $b = b_1 \cdot b_2 = -5$. I valori possibili per b_1 sono dunque $1, -1, 5, -5$, e le equazioni corrispondenti sono

$$\begin{aligned} (i) \ \ & N^2 = M^4 - 5d^4 \ , \\ (ii) \ \ & N^2 = -M^4 + 5d^4 \ , \\ (iii) \ \ & N^2 = 5M^4 - d^4 \ , \\ (iv) \ \ & N^2 = -5M^4 + d^4 \ . \end{aligned}$$

Procedendo per tentativi, si trova che $(M, d, N) = (3, 2, 1)$ è soluzione di (i), da cui $(2, 3, 1)$ è soluzione di (iv), e che $(1, 1, 2)$ è soluzione di (ii) e (iii). Queste soddisfano anche le condizioni $(\triangledown)$; pertanto tutte le scelte possibili di b_1 danno equazioni con soluzioni intere ammissibili, e $\xi(\Gamma) = \{[1] \ , \ [-1], \ [5], \ [-5]\}$.

Ora dobbiamo calcolare $|\widehat{\xi}\,(\widehat{\Gamma}\,)|$, dove

$$\widehat{\mathscr{C}}\ : y^2 = x^3 + 20x\ ;$$

i valori possibili per b_1 stavolta sono ±1, ±2, ±4, ±5, ±10, ±20, quindi $\widehat{\xi}\,(\widehat{\Gamma}\,)$ sarà contenuto in $\{[\pm1], ..., [\pm20]\}$; ma poiché stiamo lavorando modulo $\mathbb{Q}^{*2}$, abbiamo $[20] = [5]$ e $[4] = [1]$, quindi $\widehat{\xi}\,(\widehat{\Gamma}\,)$ sarà contenuto in

$$\{[1]\,,\ [-1]\,,\ [2]\,,\ [-2]\,,\ [5]\,,\ [-5]\,,\ [10]\,,\ [-10]\}\ .$$

Deve essere poi $b_1 b_2 = 20$, quindi b_1, b_2 sono entrambi positivi o negativi; nel secondo caso, l'equazione (▼) non ha soluzioni reali non banali, quindi possiamo escludere tutte le scelte con $b_1 < 0$, ovvero $\widehat{\xi}\,(\widehat{\Gamma}\,) \subseteq \{[1]\,,\ [2]\,,\ [5]\,,\ [10]\}$. Notiamo poi che $\widehat{\xi}\,(O) = [1]$ e $\widehat{\xi}\,(T) = [20] = [5]$; resta solo da capire se $[2]$ e $[10]$ appartengono a $\widehat{\xi}\,(\widehat{\Gamma}\,)$.
Consideriamo l'equazione $N^2 = 2M^4 + 10d^4$; mostriamo che questa non ha soluzioni intere con $(M, 10) = 1$. Supponiamo che esista una soluzione siffatta; poiché $(M, 10) = 1$, anche $(M, 5) = 1$, dunque per il piccolo teorema di Fermat è $M^4 \equiv 1 \mod 5$. Riducendo $N^2 = 2M^4 + 10d^4$ modulo 5 si trova pertanto $N^2 \equiv 2 \mod 5$, per la quale però non esistono soluzioni perché, nel campo $\mathbb{Z}_5$, $[2]_5$ non è un quadrato; dunque $[2] \notin \widehat{\xi}\,(\widehat{\Gamma}\,)$.
Infine, neanche $[10]$ può appartenere a $\widehat{\xi}\,(\widehat{\Gamma}\,)$, altrimenti troveremmo $[10] \cdot [5]^{-1} = [2] \in \widehat{\xi}\,(\widehat{\Gamma}\,)$, contro quanto appena detto.
Così $\widehat{\xi}\,(\widehat{\Gamma}\,) = \{[1]\,,\ [5]\}$ e $2^r = \dfrac{4 \cdot 2}{4} = 2$, ovvero $r = 1$.
Possiamo trovare un insieme di generatori per Γ: anzitutto si può verificare (ad esempio con il programma Matlab `ord_fin`) che O, T sono gli unici punti di ordine finito; inoltre la soluzione $(3, 2, 1)$ dell'equazione (i) ci dà, tramite la formula (4.31) con $b_1 = 1$, il punto $\left(\frac{9}{4}, \frac{3}{8}\right) \in \Gamma$. Pertanto

$$\Gamma = \left\langle \left(\frac{9}{4}, \frac{3}{8}\right) \right\rangle \oplus \langle (0,0) \rangle \cong \mathbb{Z} \oplus \mathbb{Z}_2$$

***Esempio* 4.2*: una cubica con* Γ *di rango* 2.**
Cerchiamo il rango di

$$\mathscr{C} : y^2 = x^3 + 73x \ .$$

Qua $b = 73$, quindi $b_1 = \pm 1, \pm 73$ e $b_1 \cdot b_2 = 73$; le equazioni che dobbiamo considerare per calcolare $|\xi(\Gamma)|$ sono dunque

$$\begin{aligned} (i) \quad & N^2 = M^4 + 73d^4 \ , \\ (ii) \quad & N^2 = -M^4 - 73d^4 \ , \\ (iii) \quad & N^2 = 73M^4 + d^4 \ , \\ (iv) \quad & N^2 = -73M^4 - d^4 \ . \end{aligned}$$

Vediamo subito che (ii) e (iv) non possono avere soluzioni intere non banali perché $N^2 \geq 0$; d'altra parte (i) e (iii) sono relative a $b_1 = 1$ e $b_1 = b$ rispettivamente, quindi non è necessario calcolare le soluzioni perché sappiamo già che $\xi(0) = [1]$ e $\xi(T) = [b] \in \xi(\Gamma)$.
Pertanto $\xi(\Gamma) = \{[1]\,, [73]\}$ e $|\xi(\Gamma)| = 2$.
Consideriamo ora

$$\widehat{\mathscr{C}} : y^2 = x^3 - 292x \ .$$

Stavolta b_1 può assumere valori in

$$\{\pm 1\,, \pm 2\,, \pm 4\,, \pm 73\,, \pm 146\,, \pm 292\}$$

dunque, dato che $[4] = [1]$, $[-4] = [-1]$, $[292] = [73]$, $[-292] = [-73]$, si ha

$$\widehat{\xi}\,(\widehat{\Gamma}\,) \subseteq \{[1]\,, [-1]\,, [2]\,, [-2]\,, [73]\,, [-73]\,, [146]\,, [-146]\} \ .$$

Come prima $\widehat{\xi}\,(O) = [1]$, $\widehat{\xi}\,(T) = [292] = [73] \in \widehat{\xi}\,(\widehat{\Gamma}\,)$.
Per gli altri valori di b_1 occorre cercare delle soluzioni intere alle equazioni $(\blacktriangledown)$ per cui valga $(\triangledown)$; usando Matlab e facendo variare M e d in un range piccolo, ad esempio da 1 a 20, se si è fortunati si trovano soluzioni intere per N. Così, nel nostro caso, si trova che per $b_1 = 2$, $b_2 = -146$, l'equazione $N^2 = 2M^4 - 146d^4$ ha la soluzione $(3, 1, 4)$, che soddisfa le $(\triangledown)$; ancora, per $b_1 = 146$, $b_2 = -2$, si trova che $N^2 = 146M^4 - 2d^4$ ha la soluzione $(1, 1, 2)$.

Quindi [1], [2], [73], [146] $\in \widehat{\xi}\,(\Gamma)$.
Vediamo ora i casi $b_1 < 0$. Per $b_1 = -1$, si trova l'equazione $N^2 = -M^4 + 292d^4$, che non ha soluzioni accettabili; infatti se esistesse una soluzione (M, d, N) con $(M, b_2) = (M, 292) = 1$, allora M sarebbe dispari e $M^4 \equiv 1 \mod 4$. Riducendo modulo 4 l'equazione considerata avremmo $N^2 \equiv -1 \mod 4$, ma un quadrato è congruo a 0 oppure ad 1 modulo 4.
Questo però non significa che $[-1] \notin \widehat{\xi}\,(\widehat{\Gamma}\,)$; infatti per $b_1 = -4$ l'equazione $N^2 = -4M^4 + 73d^4$ ha la soluzione accettabile $(2, 1, 3)$, quindi $[-4] = [-1] \in \widehat{\xi}\,(\widehat{\Gamma}\,)$.
Poiché $\widehat{\xi}\,(\widehat{\Gamma}\,)$ è un sottogruppo, deduciamo che anche $[-2] = [-1] \cdot [2]$, $[-73] = [-1] \cdot [73]$, $[-146] = [-1] \cdot [146]$ devono appartenere a $\widehat{\xi}\,(\widehat{\Gamma}\,)$; pertanto vale la relazione

$$2^r = \frac{2 \cdot 8}{4} = 4\ ,$$

ovvero il rango di Γ è $r = 2$.
Si verifica infine che l'unico punto $\neq O$ di ordine finito di $\mathscr{C}$ è $T = (0, 0)$, pertanto

$$\Gamma \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}_2\ .$$

Appendice A

Nota sugli esempi

Nel seguito sono riportati i codici Matlab/Octave utilizzati negli esempi dei capitoli 2 e 3; a parte `divisor`[1], sono stati tutti realizzati al puro scopo di mettere in pratica i risultati teorici visti, quindi non sono ottimizzati dal punto di vista computazionale, pur restando stabili in molti casi testati, e in tutti gli esempi presentati.

```
function C = somma(A,B,a,b)
%% Calcola la somma di due punti A, B, (A~=-B), sulla cubica
%% C:y^2=x^3+ax^2+bx+c
% A,B = coordinate dei punti
% a,b = coefficienti a,b della cubica in FN
% C = coordinate di A+B
% Calcola la somma di A e B sulla cubica
if A(1)~=B(1)
    l=(B(2)-A(2))/(B(1)-A(1));
else
    l=polyval([3,2*a,b],A(1))/(2*A(2));
end
m=A(2)-l*A(1);
xC=l^2-a-A(1)-B(1);
yC=-(l*xC+m);
C=[xC,yC];
end


function D = discr( a,b,c )
%% Calcola il discriminante del polinomio f(x)=x^3+ax^2+bx+c
D= -4*a^3*c+a^2*b^2+18*a*b*c-4*b^3-27*c^2;
end
```

[1] Si trova al link `www.mathworks.com/matlabcentral/fileexchange/24500-divisor-n-`.

```
function ord_fin(a,b,c)
%% Cerca i possibili punti di ordine finito
%% (con ordinata y>0) di una cubica razionale in FN,
%% secondo il criterio dato dal teorema di Nagell - Lutz.
% a,b,c= coefficienti interi dell'equazione della cubica in FN
D=discr(a,b,c)
Y=divisor((abs(D))) % se D=0, la cubica è singolare;
                    % l'esecuzione si arresta
                    % quando si cercano i divisori di D
for i=1:length(Y)
   p=[1 ,a ,b ,c-Y(i)^2];
   %Y(i)
   X=roots(p);
    for k=1:length(X)
        if  abs(round(X(k))-X(k))<1e-12 % x è intero
            fprintf('(X,Y)=(%3.0f,%d)\n',X(k),Y(i))
        end
    end
end
p=[1 ,a ,b ,c];
X=roots(p);
for k=1:length(X)
    if  abs(round(X(k))-X(k))<1e-12 % x è intero
        fprintf('ordine 2: (X,Y)=(%3.0f,%d)\n',X(k),0)
    end
end


function ordine(A,a,b)
%% Calcola l'ordine di un punto a coordinate intere sulla cubica C
% A = coordinate del punto
% a,b = coefficienti interi dell'eqne della cubica in FN
B=A; m=2;
while (abs(B(2)+A(2))>1e-12 || abs(B(1)-A(1))>1e-12)
                            % B non è l'opposto di A
    if norm(round(B)-B)<1e-12
        B=somma(A,B,a,b);
    else
        fprintf(...
            ['A=(%d,%d) ha ordine infinito perché ', ...
            'B=%dA ha coordinate ( %s,%s)\n'],...
            A(1),A(2),m-1,strtrim(rats(B(1))),strtrim(rats(B(2))))
       return
   end
   m=m+1;
end
fprintf('A=(%d,%d) ha ordine %d\n',  A(1),A(2),m)
```

Nota sulle figure

Tutte le figure sono state realizzate tramite il software GeoGebra. È bene notare comunque che si può dare una rappresentazione dei punti reali delle cubiche considerate anche senza l'uso di un software; questo vale certamente per le cubiche in forma normale, per le proprietà viste nell'osservazione 1.3.a.
Per la cubica liscia della figura 3.1 di pagina 49, che ha equazione

$$\mathscr{C} : s = t^3 + t^2 s + t s^2 + s^3 \ ,$$

si può ragionare così: anzitutto, se $u = 0$ è la retta impropria del piano ts, allora i punti impropri di $\mathscr{C}$ sono dati dalle soluzioni di

$$\begin{cases} t^3 + t^2 s + t s^2 + s^3 = 0 \\ u = 0 \end{cases} \implies \begin{cases} (t+s)(t+is)(t-is) = 0 \\ u = 0 \end{cases}$$

cioè $[0,1,-1]$, $[0,1,-i]$, $[0,1,i]$; il punto reale $[0,1,-1]$ dà la direzione dell'unico asintoto, che è quindi del tipo $t + s = h$, $h \in \mathbb{R}$.
Inoltre vale $P = (t,s) \in \mathscr{C} \Leftrightarrow (-t,-s) \in \mathscr{C}$; dunque $\mathscr{C}$ è simmetrica rispetto ad $O = (0,0)$, e l'asintoto è $t + s = 0$.
Guardando le intersezioni con gli assi, si trova

$$\mathscr{C} \cap \{s = 0\} : \begin{cases} t^3 = 0 \\ s = 0 \end{cases} \implies \quad O \in \mathscr{C} \text{ è un punto di flesso}$$

e

$$\mathscr{C} \cap \{t = 0\} : \begin{cases} s^3 - s = 0 \\ t = 0 \end{cases} \implies \begin{cases} s(s+1)(s-1) = 0 \\ t = 0 \end{cases}$$

$\implies (0,1)\ ,\ (0,0)\ ,\ (0,-1) \in \mathscr{C}$.
Questi dati sono sufficienti per dare una rappresentazione grafica approssimativa di $\mathscr{C}$ nel piano reale affine.

Si può fare un ragionamento analogo anche per la cubica della figura 1.2 di pagina 15, la cui equazione è

$$\mathscr{C} : x + y + x^2 + y^2 + xy + x^2 y + x y^2 = 0 \ ;$$

in primo luogo, se $x_0 = 0$ è l'equazione della retta impropria del piano affine xy, i punti all'infinito di $\mathscr{C}$ sono dati dalle soluzioni di

$$\begin{cases} x^2y + xy^2 = 0 \\ x_0 = 0 \end{cases} \implies \begin{cases} xy(x+y) = 0 \\ x_0 = 0 \end{cases}$$

ovvero $[0,1,0]$, $[0,0,1]$, $[0,1,-1]$; così $\mathscr{C}$ ha tre asintoti, di equazioni rispettivamente $x = k$, $y = h$, $x + y = \ell$, con $k, h, \ell \in \mathbb{R}$.
Poi, vale $(x,y) \in \mathscr{C} \Leftrightarrow (y,x) \in \mathscr{C}$, quindi $\mathscr{C}$ è simmetrica rispetto alla retta $x = y$ e vale $k = h$.
Guardando le intersezioni con l'asse x, si trova

$$\mathscr{C} \cap \{y = 0\} : \begin{cases} x + x^2 = 0 \\ y = 0 \end{cases} \implies (0,0), (-1,0) \in \mathscr{C}$$

quindi $(0,-1) \in \mathscr{C}$ e non ho altre intersezioni con gli assi.
Consideriamo ora le tangenti in questi punti:

- in $(0,0)$ è $x + y = 0$, dove $\mathscr{C} \cap \{x + y = 0\} : \begin{cases} x^2 = 0 \\ x + y = 0 \end{cases}$
- in $(-1,0)$ è $y = x + 1$, dove $\mathscr{C} \cap \{y = x + 1\} : \begin{cases} 2(x+1)^3 = 0 \\ y = x + 1 \end{cases}$, quindi $(-1,0)$ è un punto di flesso
- analogamente, $(0,-1)$ è flesso per $\mathscr{C}$ con tangente $x = y + 1$.

Allora, anche $[0,1,-1]$, che è allineato a $(-1,0)$ e $(0,-1)$ (vedi teorema 2.3.4), è un flesso per $\mathscr{C}$, quindi l'asintoto $x + y = \ell$ interseca $\mathscr{C}$ solo in $[0,1,-1]$ e in nessun punto proprio. D'altra parte

$$\mathscr{C} \cap \{x + y = l\} : \begin{cases} (1-\ell)x^2 - \ell(1-\ell)x + \ell + \ell^2 = 0 \\ x + y = \ell \end{cases}$$

è vuoto quando $\ell = 1$, quindi $x + y = 1$ è l'asintoto cercato.
Non ci sono altri flessi reali (vedi corollario 2.3.2); in particolare gli altri due punti all'infinito non sono flessi, e gli asintoti corrispondenti intersecano $\mathscr{C}$ in un suo punto proprio con molteplicità 1.

Poiché

$$\mathscr{C} \cap \{x = k\} : \begin{cases} (1+k)y^2 + (k^2+k+1)y + k + k^2 \\ x = k \end{cases}, \qquad (\circ)$$

si ha un'unica soluzione (contando con molteplicità) quando $k = -1$; quindi $x = -1$, $y = -1$ sono gli altri due asintoti di $\mathscr{C}$. Studiando l'andamento del discriminante $\Delta = k^4 - 2k^3 - 5k^2 - 2k + 1$ di $(\circ)$ al variare di k possiamo vedere quando la retta $x = k$ non ha intersezioni reali con $\mathscr{C}$; vale inoltre $\mathscr{C} \cap \{x > 0, y > 0\} = \varnothing$.

Si osservi poi che, poiché la chiusura proiettiva $\overline{\mathscr{C}}$ è compatta, per ogni asintoto $\mathscr{C}$ ha due rami che vi tendono, uno verso $+\infty$ e l'altro verso $-\infty$.

Tenendo conto di tutte le informazioni ricavate, siamo in grado di avere un'idea di come può essere fatto il grafico di $\mathscr{C}$.

Bibliografia

[BCGB] Mauro C. Beltrametti, Ettore Carletti, Dionisio Gallarati, Giacomo Monti Bragadin, *Letture su curve, superfici e varietà proiettive speciali*, Bollati Boringhieri, Torino, 2002.

[H] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1997

[J] Nathan Jacobson, *Basic Algebra I*, Seconda edizione, W. H. Freeman and Company, New York, 1985

[K] Anthony W. Knapp, *Elliptic Curves*, Mathematical Notes 40, Princeton University Press, Princeton, 1992

[MM] Henry McKean, Victor Moll, *Elliptic Curves: Function Theory, Geometry, Arithmetic*, Cambridge University Press, Cambridge, 1999

[R] Miles Reid, *Undergraduate Algebraic Geometry*, Cambridge University Press, Cambridge, 1988

[Se] Edoardo Sernesi, *Geometria 1*, Seconda edizione, Bollati Boringhieri, Torino, 2000

[Si] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986

[Sl] Ernst Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Mathematica 85, Institut Mittag-Leffler, Djursholm, 1951

[ST] Joseph H. Silverman, John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992

[Sw] John Stillwell, *Mathematics and Its History*, Springer-Verlag, New York, 1989

[W] Andrew Wiles, *The Birch and Swinnerton-Dyer conjecture*,
`http://www.claymath.org/millennium-problems/birch-and-swinnerton-dyer-conjecture`