Università di Pisa

Corso di Laurea in Matematica

Il teorema di Mordell-Weil e applicazione al problema dei quattro quadrati

Tesi di Laurea Triennale
in Matematica

Candidato
Francesca Rizzo

Relatore
Davide Lombardo
Università di Pisa

Anno Accademico 2019 - 2020

Indice

Introduzione

L'argomento di questa tesi è lo studio di alcune proprietà delle curve ellittiche, curve algebriche piane non singolari definite da un polinomio omogeneo di terzo grado in forma normale di Weierstrass.
Lo studio delle curve ellittiche è interessante sotto molti aspetti: ne presentiamo alcuni, focalizzandoci sulle proprietà aritmetiche. Ogni curva ellittica E ammette una struttura di gruppo abeliano, la cui legge di gruppo è espressa da funzioni razionali: se E è una curva ellittica definita su un campo K anche l'insieme dei suoi punti K-razionali $E(K)$ è un gruppo abeliano, e determinarne la struttura è una questione rilevante e molto studiata in letteratura.

Nel capitolo 1 presentiamo le curve ellittiche come particolari curve algebriche piane, ed alcuni risultati di geometria algebrica utili nel seguito.
Lo struttura complessa di una curva ellittica su $\mathbb{C}$ è studiata in dettaglio nel capitolo 2: utilizzando la teoria delle funzioni ellittiche e modulari dimostriamo l'equivalenza di categorie fra curve ellittiche su $\mathbb{C}$ con isogenie di curve ellittiche e tori complessi con isogenie di tori. Come conseguenza otteniamo che le isogenie di curve ellittiche sono omomorfismi di gruppi.

Il capitolo successivo è dedicato allo studio della struttura di gruppo di $E(\mathbb{Q})$, descritta dal famoso Teorema di Mordell-Weil. Nel 1922 Mordell dimostra che, data una curva ellittica E definita su $\mathbb{Q}$, il gruppo dei punti razionali $E(\mathbb{Q})$ è finitamente generato, mostrando che il processo di discesa infinita di Fermat funziona sempre.

> *"I shall now prove that if any of these equations have an infinite number of solutions, then the method of infinite descent applies, that is to say, all the solutions can be expressed rationally in terms of a finite number by means of the classical method"*
>
> L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees.*

Il Teorema di Mordell è stato generalizzato nel 1928 da Weil, per ogni varietà abeliana su un campo di numeri: in particolare per le curve ellittiche vale

Teorema (Teorema di Mordell-Weil)**.** *Sia E una curva ellittica definita su un campo di numeri K. Il gruppo dei punti K-razionali $E(K)$ è finitamente generato.*

Nel capitolo 3 presentiamo una dimostrazione completa di questo teorema per $K = \mathbb{Q}$. Tramite l'introduzione di una funzione *altezza* e un argomento di

discesa infinita, il teorema di Mordell-Weil si riduce a dimostrare che il sottogruppo $2E(\mathbb{Q})$ ha indice finito in $E(\mathbb{Q})$. Questo si deduce dalla seguente forma debole, dimostrata nella sezione 3.4:

Teorema. *Sia E una curva ellittica definita su un campo di numeri K, con un punto $P \in E(K)$ di ordine 2. Il sottogruppo $2E(K)$ ha indice finito in $E(K)$.*

La schema della dimostrazione della forma debole del Teorema di Mordell-Weil segue la linea presentata in [ST15] per curve ellittiche su $\mathbb{Q}$ con un punto razionale di ordine 2. L'idea principale è quella di spezzare la moltiplicazione per 2 come composto di due isogenie, e dimostrare che queste due isogenie hanno conucleo finito. Il nostro approccio è però più teorico e concettuale: sfruttiamo la corrispondenza fra curve ellittiche e tori complessi per mostrare come costruire le isogenie, e utilizziamo la teoria di Kummer per dimostrare la finitezza dei conuclei. Infine utilizzando alcuni risultati sui campi di numeri rimuoviamo l'ipotesi che il punto di ordine 2 sia razionale.

Per concludere, nel capitolo 4, mostriamo un'applicazione della teoria delle curve ellittiche al problema della non esistenza di 4 quadrati consecutivi in una progressione aritmetica non banale. Questo problema fu proposto da Fermat nel 1640, e risolto da lui per discesa infinita.
Nella tesi dimostriamo che le soluzioni al problema dei 4 quadrati sono in corrispondenza con i punti razionali di una particolare curva ellittica E. Ripercorrendo la dimostrazione del Teorema di Mordell-Weil, troviamo che in questo caso $E(\mathbb{Q})$ è un gruppo abeliano di rango 0, e quindi i punti razionali della curva ellittica sono tutti punti di torsione. Il teorema di Nagell-Lutz permette di determinare i punti di torsione di E, e quindi il gruppo $E(\mathbb{Q})$, e si verifica che questi punti corrispondono tutti a progressioni aritmetiche di ragione 0.
Infine mostriamo che esistono infiniti campi quadratici in cui il problema dei quattro quadrati ha soluzioni non banali.

Capitolo 1

Preliminari

In questo capitolo diamo la definizione e mostriamo le prime proprietà delle curve ellittiche, sfruttando alcuni risultati di geometria algebrica. Per ulteriori approfondimenti si veda [Sil09, Sezioni I, II, III].
Nel seguito indicheremo con K un campo perfetto (ovvero tale che ogni sua estensione algebrica è separabile) con $\mathrm{char}(K) > 3$ e $\overline{K}$ una fissata chiusura algebrica.

1.1 Curve algebriche

Definizione 1.1.1. Dato un campo K, definiamo:

- lo spazio *affine* n-dimensionale
$$\mathbb{A}^n(K) = \{P = (x_1, \dots, x_n) | x_i \in K \ \forall i\};$$
- lo spazio *proiettivo* n-dimensionale
$$\mathbb{P}^n(K) = \mathbb{A}^{n+1}(K) \setminus \{0\} / \sim$$
dove la relazione di equivalenza è data da
$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \iff \exists \lambda \in K^* \text{ tale che } x_i = \lambda y_i \ \forall i.$$

Si verifica che $\mathbb{P}^n(K) = \{[x_0, \dots, x_n] \in \mathbb{P}^n(\overline{K}) : x_i \in K \ \forall i\}$.

Per ogni estensione di Galois L/K, consideriamo l'azione del gruppo di Galois $G = \mathrm{Gal}\,(L/K)$ su $\mathbb{A}^n(L)$ definita nel modo seguente: per ogni $\sigma \in G$, e per ogni $P \in \mathbb{A}^n(L)$ poniamo
$$\sigma P = (\sigma(x_1), \dots, \sigma(x_n)).$$
È facile osservare che vale $\mathbb{A}^n(K) = \{P \in \mathbb{A}^n(L) : \sigma P = P \ \forall \sigma \in G\}$.
Poiché l'azione di G su $\mathbb{A}^n(L)$ rispetta la relazione di equivalenza che definisce $\mathbb{P}^n(L)$, G agisce in modo analogo su $\mathbb{P}^n(L)$ e vale
$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n(L) : \sigma P = P \ \forall \sigma \in G\}.$$
Per ogni $i = 0, \dots, n$ consideriamo la carta $U_i = \{[x_0, \dots, x_n] \in \mathbb{P}^n(K) | x_i \neq 0\}$ e le bigezioni
$$\begin{aligned} \phi_i : \mathbb{A}^n(K) &\longrightarrow U_i & (x_1, \dots, x_n) &\longmapsto [x_1, \dots, x_{i-1}, 1, x_i, \dots, x_n] \\ \phi_i^{-1} : U_i &\longrightarrow \mathbb{A}^n(K) & [x_0, \dots, x_n] &\mapsto \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}\right). \end{aligned}$$

Osserviamo che per ogni $P \in \mathbb{P}^n(K)$ esiste i tale che $P \in U_i$.

Definizione 1.1.2. Un polinomio $f \in K[X] = K[X_0, \ldots, X_n]$ si dice *omogeneo* di grado d se per ogni $\lambda \in \overline{K}$ vale

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n).$$

Dato un polinomio omogeneo f possiamo deomogenizzarlo rispetto alla variabile X_i trovando un polinomio

$$D_i(f)(y_1, \ldots, y_n) = f(y_1, \ldots, y_{i-1}, 1, y_i, \ldots, y_n) \in K[y_1, \ldots, y_n].$$

Analogamente, dato $f \in K[y_1, \ldots, y_n]$ possiamo associargli un polinomio omogeneo $H_i(f)$ omogeneizzando rispetto ad una variabile X_i: detto $d = \deg(f)$,

$$H_i(f)(X_0, \ldots, X_n) = X_i^d f\left(\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i}\right).$$

Indichiamo con $\overline{K}[X] = \overline{K}[X_0, \ldots, X_n]$ l'anello dei polinomi in $n+1$ variabili e con $\overline{K}(X) = \overline{K}(X_0, \ldots, X_n)$ il campo delle funzioni razionali.

Definizione 1.1.3. Dato un ideale primo $I = (f_0, \ldots, f_m) \subset \overline{K}[X]$, dove $f_0, \ldots, f_m$ sono polinomi omogenei a coefficienti in un campo K, si dice *varietà proiettiva* associata ad I il funtore $V : \{\text{estensioni } L/K\} \to \mathbf{Set}$ che associa ad ogni estensione L/K l'insieme

$$V(L) = \{P \in \mathbb{P}^n(L) \mid f_i(P) = 0 \ \forall i = 0, \ldots, m\}$$

e rispetta le inclusioni.

Poiché f è omogeneo, $f(\lambda X) = 0$ se e soltanto se $f(X) = 0$, quindi il luogo di zeri di polinomi omogenei è ben definito nello spazio proiettivo.

È ovvio dalla definizione che V non dipende dai particolari generatori scelti per l'ideale I.

Osserviamo che possiamo definire una varietà algebrica in maniera più astratta con il suo anello delle coordinate omogenee

$$A = \frac{\overline{K}[X_0, \ldots, X_n]}{I}$$

dove I è l'ideale che definisce V.
Poiché I è primo, e quindi radicale, il Nullstellensatz garantisce che su un campo algebricamente chiuso V e I sono in corrispondenza.

Se f è un polinomio a coefficienti in K, allora $f(\sigma P) = \sigma(f(P))$ per ogni $\sigma \in G = \mathrm{Gal}\,(L/K)$, quindi se V è definita su K:

$$V(K) = \{P \in V(L) \mid \sigma P = P \ \forall \sigma \in G\}.$$

Definizione 1.1.4. Data una varietà V definita su K dall'ideale I, possiamo definire il campo delle funzioni $K(V)$ come:

$$K(V) = \left\{ \frac{f(X)}{g(X)} \in K(X) \middle| f, g \text{ sono polinomi omogenei dello stesso grado}, g \notin I \right\} \Big/ \sim$$

dove $\frac{f}{g} \sim \frac{f'}{g'}$ se $fg' - gf' \in I$.

Si può dimostrare che se i è tale che $V(K) \cap U_i \neq \emptyset$, allora $I(V)_i = \{D_i(f) | f \in I\}$ è un ideale di $K[y] = K[y_1, \cdots, y_n]$ e vale

$$K(V) \simeq \text{Quot}\left(\frac{K[y]}{I(V)_i}\right)$$

Anche in questo caso, data $\phi \in L(V)$ abbiamo che $G = \text{Gal}\,(L/K)$ agisce su ϕ, agendo sui suoi coefficienti, e si dimostra che $K(V) = L(V)^G$. Indicata l'azione di σ su ϕ con $\phi \mapsto \sigma\phi$, osserviamo che

$$\sigma\phi(\sigma P) = \sigma(\phi(P)).$$

Definizione 1.1.5 (Dimensione)**.** Data una varietà V definita su K la *dimensione* di V è il grado di trascendenza di $\overline{K}(V)$ su $\overline{K}$, cioè

$$\dim(V) = \text{trdeg}_{\overline{K}}\overline{K}(V)$$

Definizione 1.1.6. Sia $P \in V(\overline{K})$, dove V è una varietà definita dall'ideale $I = (f_0, \ldots, f_m)$. Sia $0 \leq i \leq n$ tale che $P \in V \cap U_i$: allora P si dice *punto non singolare* di V se

$$\left(\frac{\partial D_i(f_j)}{\partial X_k}\right)_{\substack{0 \leq j \leq m \\ 1 \leq k \leq n}}(P)$$

ha rango $n - \dim(V)$. Altrimenti P si dice *punto singolare*.

Anche in questo caso si verifica che la definizione di punto singolare non dipende dai generatori scelti, né dalla scelta di i.

Definizione 1.1.7. Una varietà V si dice *non singolare* se non ha punti singolari.

Definizione 1.1.8 (Curva algebrica)**.** Una *curva algebrica* C è una varietà proiettiva di dimensione 1.

In particolare una curva algebrica piana $C(\overline{K}) \subset \mathbb{P}^2(\overline{K})$ è

$$C(\overline{K}) = \{[X, Y, Z] \in \mathbb{P}^2(\overline{K}) \mid F(X, Y, Z) = 0\}$$

dove $F \in \overline{K}[X, Y, Z]$ è un polinomio omogeneo e irriducibile.

Se F è tale che $C(\overline{K}) \cap \{Z \neq 0\} \neq 0$, si può verificare che

$$\overline{K}(C) = \overline{K}\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

1.1.1 Mappe fra curve

Definizione 1.1.9. Siano C_1 e C_2 due curve definite su K, con $C_2 \subset \mathbb{P}^n$: $\phi : C_1 \to C_2$ si dice *mappa razionale* se $\phi = [\phi_0, \ldots, \phi_n]$ e

- $\phi_i \in \overline{K}(C_1)$ per ogni $i = 0, \ldots, n$;
- per ogni P in cui ϕ è definita $\phi(P) = [\phi_0(P), \ldots, \phi_n(P)] \in C_2$.

La mappa ϕ si dice *regolare* in $P \in C_1(\overline{K})$ se esiste $g \in \overline{K}(C_1)$ tale che:

- $g\phi_i$ è definita in P per ogni P;

- esiste i tale che $g\phi_i(P) \neq 0$.

In questo caso poniamo $\phi(P) = [(g\phi_0)(P), \ldots, (g\phi_n)(P)]$.

Definizione 1.1.10. Date due curve C_1 e C_2, un *morfismo* fra C_1 e C_2 è una mappa razionale $\phi : C_1 \to C_2$ regolare in ogni punto.
Se C_1 e C_2 sono definite su K, $\phi = [\phi_0, \ldots, \phi_n] : C_1 \to C_2$ è un morfismo di curve ed esiste $\lambda \in \overline{K}^*$ tale che $\lambda\phi_i \in K(C_1)$, diciamo che ϕ è definita su K.

In particolare se $\phi : C_1 \to C_2$ è un morfismo definito su K, per ogni estensione L/K, ϕ induce una funzione $C_1(L) \to C_2(L)$, che indichiamo sempre con la stessa lettera.

Ancora una volta, se C_1 e C_2 sono definite su K, σ agisce su ϕ agendo sulle sue componenti

$$\sigma\phi = [\sigma\phi_0, \ldots, \sigma\phi_n]$$

e vale $\sigma(\phi(P)) = \sigma\phi(\sigma P)$.

Riportiamo il seguente teorema, la cui dimostrazione si trova in [Har77, II.6.8].

Teorema 1.1.11. *Per ogni morfismo di curve $\phi : C_1 \to C_2$, la funzione*

$$\phi : C_1(\overline{K}) \to C_2(\overline{K})$$

è costante o surgettiva.

Date due curve C_1 e C_2 definite su K e $\phi : C_1 \to C_2$ morfismo non costante definito su K, questo induce

$$\begin{aligned} \phi^* : K(C_2) &\longrightarrow K(C_1) \\ f &\longmapsto f \circ \phi \end{aligned}$$

e questa mappa è iniettiva per il teorema precedente.

Riportiamo il seguente risultato, di cui si può trovare la dimostrazione in [Har77, I.6.12].

Teorema 1.1.12. *Sia $K' \subset K(C)$ un sottocampo di indice finito che contiene K. Esiste un'unica curva non singolare C'/K, unica a meno di K-isomorfismi, e una mappa non costante $\phi : C \to C'$ tale che $\phi^*(K(C')) = K'$.*

1.2 Curve ellittiche

Definizione 1.2.1 (Curva ellittica)**.** Una *curva ellittica* definita su K è una curva algebrica piana non singolare definita da un polinomio $F(X, Y, Z)$ in *forma normale di Weierstrass*, cioè

$$F(X, Y, Z) = Y^2Z - X^3 - aX^2Z - bXZ^2 - cZ^3 \in K[X, Y, Z].$$

Nel seguito indicheremo con

$$E : Y^2Z = X^3 - aX^2Z - bXZ^2 - cZ^3$$

una curva ellittica.

Possiamo deomogenizzare un polinomio in forma di Weierstrass rispetto alla coordinata Z: detti $x = X/Z$, $y = Y/Z$, otteniamo

$$y^2 = x^3 + ax^2 + bx + c$$

e poiché l'unico punto sulla retta $Z = 0$ è $\mathcal{O} = [0 : 1 : 0]$ (che viene detto *punto all'infinito*), troviamo:

$$E(\overline{K}) = \{(x, y) \in \overline{K}^2 \mid y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathcal{O}\}.$$

Osserviamo che la condizione di non singolarità equivale a richiedere che per ogni $(x, y) \in E(K)$

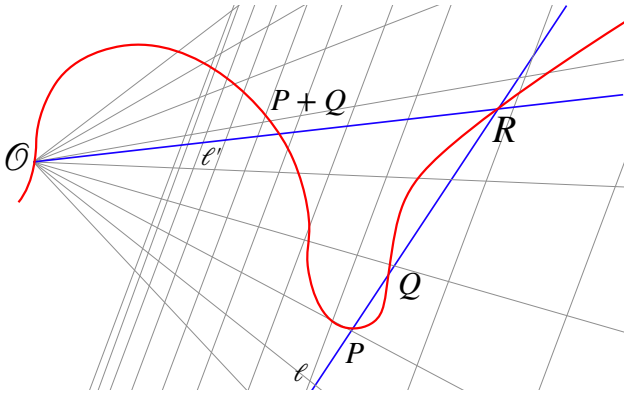
$$\big(2y, 3x^2 + 2ax + b\big) \neq (0, 0),$$

cioè che il polinomio $f(x) = x^3 + ax^2 + bx + c$ non abbia radici multiple.

1.2.1 Struttura di gruppo su $E(\overline{K})$

Sia E una curva ellittica, di equazione $Y^2Z = X^3 + aX^2Z^+bXZ^2 + cZ^3$, e sia inoltre $f(x) = x^3 + ax^2 + bx + c$.

Ogni retta $\ell \subset \mathbb{P}^2(\overline{K})$ interseca la curva ellittica E in 3 punti (non necessariamente distinti). Possiamo definire un'operazione $+$ su $E(\overline{K})$ nel modo seguente. Per ogni coppia di punti (non necessariamente distinti) $P, Q \in E(\overline{K})$, sia ℓ la retta per P e Q (eventualmente la tangente ad E in P se $P = Q$) e R la terza intersezione di ℓ con E. Sia inoltre ℓ' la retta per R e $\mathcal{O}$. Definiamo $P + Q$ come la terza intersezione di ℓ' con E.



Vediamo in coordinate sul piano affine come si comporta l'operazione $+$ appena definita: osserviamo che poiché deomogenizziamo rispetto alla variabile Z e l'unico punto all'infinito è $\mathcal{O} = [0 : 1 : 0]$, nel piano affine le rette per $\mathcal{O}$ sono rette parallele all'asse delle y.

Proposizione 1.2.2. *Siano $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(\overline{K}) \setminus \{\mathcal{O}\}$:*

- *se $Q \neq (x_1, -y_1)$ il punto $P + Q$ ha coordinate $(\tilde{x}, \tilde{y})$ con*

$$\tilde{x} = \lambda^2 - a - x_1 - x_2 \quad \tilde{y} = -(\lambda\tilde{x} + \nu)$$

con

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & P \neq Q \\ \frac{f'(x_1)}{2y_1} & P = Q \end{cases}, \quad \nu = y_1 - \lambda x_1$$

- *se* $Q = (x_1, -y_1)$, $P + Q = \mathcal{O}$.

Dimostrazione. Supponiamo che $Q \neq (x_1, -y_1)$: allora la retta per P e Q (o tangente a E in P se $P = Q$) ha equazione $y = \lambda x + \nu$ dove $\nu = y_1 - \lambda x_1$ e $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$ se $P \neq Q$ o $\lambda = \frac{f'(x_1)}{2y_1}$ se $P = Q$.
Osserviamo che λ è ben definito in entrambi i casi:

- se $P \neq Q$ e $Q \neq (x_1, -y_1)$ sicuramente $x_2 \neq x_1$;
- se $P = Q$ ma $Q = (x_1, y_1) \neq (x_1, -y_1)$ sicuramente $y_1 \neq 0$.

Allora detto $R = (x_3, y_3)$ l'ulteriore punto di intersezione di L con E vale:

$$\begin{cases} y = \lambda x + \nu \\ y^2 = x^3 + ax^2 + bx + c \end{cases}$$

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3) = 0$$

Allora: $x_1 + x_2 + x_3 = \lambda^2 - a$ da cui troviamo $x_3 = \lambda^2 - a - x_1 - x_2$ e $y_3 = \lambda x_3 + \nu$.
Adesso la retta per R e $\mathcal{O}$ è la retta verticale passante per R, quindi l'altro punto di intersezione fra la retta $x = x_3$ e E è proprio $P + Q = (x_3, -y_3)$.
Nel caso in cui $y_2 = -y_1$, la retta ℓ è $y = x_1$ e interseca E in $\mathcal{O}$: poiché $\mathcal{O}$ è un punto di flesso, è l'unica intersezione fra E e la tangente ad E in $\mathcal{O}$. □

La seguente proposizione mostra come + definisca una struttura di gruppo abeliano su $E(\overline{K})$.

Proposizione 1.2.3. *L'operazione + definita sopra soddisfa le seguenti proprietà:*

(a) ($\mathcal{O}$ *è l'elemento neutro)* $P + \mathcal{O} = P \ \forall P \in E(\overline{K})$.

(b) (Commutatività) $P + Q = Q + P \ \forall P, Q \in E(\overline{K})$.

(c) (Inverso) Per ogni P *esiste* $-P \in E(\overline{K})$ *tale che* $P + (-P) = \mathcal{O}$.

(d) (Associatività) Dati $P, Q, R \in E(\overline{K})$*:* $(P + Q) + R = P + (Q + R)$.

Quindi $(E(\overline{K}), +)$ *è un gruppo abeliano.*
Inoltre se E *è definita su* K*, per ogni estensione* L/K *si ha:* $E(L) < E(\overline{K})$

Dimostrazione. Osserviamo per prima cosa che dalla definizione segue che se ℓ è una retta che interseca E in P, Q, R (non necessariamente distinti), allora $(P + Q) + R = \mathcal{O}$: infatti per costruzione $\mathcal{O}$, $P + Q$ e R sono allineati.

(a) Osserviamo che nella definizione di + per P e $\mathcal{O}$ le rette ℓ e ℓ' coincidono, quindi $P + \mathcal{O} = P$.

(b) Poiché la definizione di + è simmetrica in P e Q, + è commutativo.

(c) Sia $-P$ il terzo punto d'intersezione della retta per P e $\mathcal{O}$ con E: allora

$$\mathcal{O} = (P + \mathcal{O}) + (-P) = P + (-P)$$

In particolare dalla Proposizione 1.2.2 si ha che se $P = (x, y)$, allora $-P = (x, -y)$.

(d) Se uno dei punti è $\mathcal{O}$ allora la tesi segue da (a).
Altrimenti si può verificare usando la Proposizione 1.2.2 che effettivamente la legge di gruppo è associativa.

Infine sempre dalla Proposizione 1.2.2 vediamo che la funzione che somma due punti è $K(P,Q)$-razionale, quindi se $P, Q \in E(L)$ anche $P+Q \in E(L)$. □

Diciamo che un punto $P \in E(K)$ ha ordine finito se esiste $m \in \mathbb{Z}$ per cui

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ volte}} = \mathcal{O}.$$

Indichiamo con

$$E[m] = \{P \in E(\overline{K}) : mP = \mathcal{O}\}$$

l'insieme dei punti di ordine che divide m: è facile verificare che $E[m] \cap E(K)$ è un sottogruppo di $E(K)$.

Un caso interessante sono i punti di ordine 2, che sappiamo caratterizzare completamente. Dato $P = (x, y) \in E(K)$, dalla proposizione 1.2.2 sappiamo che $2P = \mathcal{O}$ se e soltanto se $P = (x, 0)$, cioè $f(x) = 0$.

Quindi $E[2] = \{\mathcal{O}\} \cup \{(\alpha, 0) : f(\alpha) = 0\}$ e, poiché f è un polinomio di ordine 3 senza radici multiple, $E[2]$ è un gruppo di cardinalità 4 ed esponente 2, cioè

$$E[2] \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

1.2.2 Isogenie di curve ellittiche

Definizione 1.2.4 (Isogenie di curve ellittiche)**.** Siano E_1 e E_2 due curve ellittiche. Una *isogenia* fra E_1 e E_2 è un morfismo di curve

$$\phi : E_1 \longrightarrow E_2 \quad \text{tale che } \phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$$

Il Teorema 1.1.11 garantisce che ϕ è costante, e quindi $\phi \equiv \mathcal{O}$ (detta *zero-isogenia*), oppure $\phi(E_1(\overline{K})) = E_2(\overline{K})$. Ogni isogenia non banale (cioè diversa dalla zero-isogenia) induce

$$\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$$

iniettiva.

Nel paragrafo 2.3.1 dimostreremo, usando la teoria complessa, che ogni isogenia di curve ellittiche è anche un omomorfismo di gruppi.

La seguente proposizione, dimostrata in [Sil09, II.4.10], mette in relazione il nucleo di un'isogenia non banale ϕ e l'immagine di ϕ^*.

Proposizione 1.2.5. *Sia $\phi : E_1 \to E_2$ una isogenia non costante e consideriamo l'omomorfismo $\phi : E_1(\overline{K}) \to E_2(\overline{K})$. Valgono le seguenti proprietà:*

- $\ker\phi$ *è un sottogruppo finito di* $E_1(\overline{K})$*;*
- $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ *è una estensione di Galois finita con gruppo di Galois*

$$\mathrm{Gal}\left(\overline{K}(E_1)/\phi^*(\overline{K}(E_1))\right) = \{\tau_T^* | T \in \ker\phi\},$$

dove $\tau_T : E_1 \to E_1$ è la traslazione per T.

1.2.3 Discriminante e j-invariante

Sia E una curva ellittica definita su un campo K di equazione affine $y^2 = x^3 + ax^2 + bx + c$. A meno del cambio di coordinate $(x, y) \mapsto \left(2\left(x + \frac{a}{3}\right), 8y\right)$, possiamo supporre che l'equazione di E sia del tipo

$$y^2 = 4x^3 - c_2x - c_3, \tag{1.1}$$

ed indichiamo con $f(x)$ il polinomio $4x^3 - c_2x - c_3$.

Definizione 1.2.6. Il *discriminante* della curva ellittica E è

$$\Delta = 16 \cdot \mathrm{Ris}\left(f, f'\right).$$

Si può verificare che se E ha equazione (1.1), il discriminante è dato da

$$\Delta = -16 \cdot \left(4\left(\frac{-c_2}{4}\right)^3 + 27\left(\frac{-c_3}{4}\right)^2\right) = c_2^3 - 27c_3^2$$

Inoltre, per le proprietà del risultante, è facile verificare che E è non singolare se e solo se $\Delta \neq 0$.

Definizione 1.2.7. Data E con equazione (1.1), si dice *j-invariante* di E la quantità

$$j = 1728\frac{c_2^3}{\Delta}.$$

Nel paragrafo 2.3.1 dimostreremo che due curve ellittiche su $\mathbb{C}$ sono isomorfe se e soltanto se hanno lo stesso j-invariante.
In generale si può dimostrare (si veda ad esempio [Sil09, III.1.4]) che questa proprietà vale in ogni campo algebricamente chiuso.

1.3 Strumenti algebrici

In questa sezione riportiamo alcuni fatti di Teoria di Galois e Teoria dei Numeri che utilizzeremo nel capitolo 3, e nel seguito supporremo che K sia un campo di numeri.

Successione di Kummer

Presentiamo dei risultati di coomologia di Galois, che utilizzeremo su una opportuna successione esatta, alla sezione 3.4.2.

Definizione 1.3.1. Dato un anello commutativo con unità A e un gruppo G, possiamo definire l'*anello di gruppo*

$$A[G] = \left\{ \sum_{g \in G} a_g g \mid a_g \in A \right\}$$

che è un anello con le naturali operazioni di somma e prodotto.

È facile verificare che un gruppo abeliano M con un'azione di un gruppo G è uno $\mathbb{Z}[G]$-modulo. In particolare, data una curva ellittica E definita su K, per ogni estensione di Galois L/K, l'azione di $\mathrm{Gal}\left(L/K\right)$ definisce su $E(L)$ una struttura di $\mathbb{Z}[\mathrm{Gal}\left(L/K\right)]$-modulo.

Dati due $\mathbb{Z}[G]$-moduli M e N, diciamo che un omomorfismo $f : M \to N$ è uno $\mathbb{Z}[G]$-omomorfismo se

$$f(gm) = gf(m)\ \forall m \in M, g \in G,$$

ed indichiamo con $\mathrm{Hom}_{\mathbb{Z}[G]}(M, N)$ l'insieme degli $\mathbb{Z}[G]$-omomorfismi.

Si può verificare che $\mathcal{F} = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, \cdot)$ è un funtore covariante, ed esatto a sinistra, dalla categoria degli $\mathbb{Z}[G]$-moduli continui (dove supponiamo che G agisca banalmente su $\mathbb{Z}$) nella categoria dei gruppi abeliani. Possiamo quindi considerare il funtore derivato destro associato ed indicare con

$$H^i(G, M) = R^i(\mathcal{F}(I^{\cdot}))$$

dove $I^{\cdot}$ è una risoluzione iniettiva di uno $\mathbb{Z}[G]$-modulo M,.
Data una successione esatta corta $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ di $\mathbb{Z}[G]$-moduli, per le proprietà dei funtori derivati, otteniamo la successione esatta lunga in coomologia:

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to \cdots$$

Si verifica che

$$H^0(G, M) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \simeq \{m \in M | gm = m\ \forall g \in G\} = M^G$$

quindi otteniamo:

$$0 \to A^G \to B^G \to C^G \xrightarrow{\partial} H^1(G, A) \to H^1(G, B) \to \cdots \tag{1.2}$$

dove le prime due mappe sono la restrizione delle mappe α e β e la mappa di cobordo $\partial : C^G \to H^1(G, A)$ è definita nel modo seguente: per ogni $c \in C^G$, sia $b \in B$ tale che $\beta(b) = c$. Poiché c è G-invariante, per ogni $g \in G$, si ha

$$\beta(gb - b) = gc - c = 0 \implies gb - b \in \ker(\beta) = \mathrm{Im}(\alpha).$$

Quindi possiamo porre $\partial(c) := [\chi_b]$, dove $\chi_b(g) = \alpha^{-1}(gb - b)$.

In particolare si può dimostrare che, se l'azione di G su M è banale, vale

$$H^1(G, M) \simeq \mathrm{Hom}_{\mathrm{cont}}(G, M). \tag{1.3}$$

Consideriamo ora la successione esatta corta in notazione moltiplicativa

$$1 \longrightarrow \langle -1 \rangle \longrightarrow \overline{K}^* \xrightarrow{\hat{}2} \overline{K}^* \longrightarrow 1.$$

Sia $G = \mathrm{Gal}\left(\overline{K}/K\right)$: applicando il funtore $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, \cdot)$ come in (1.2), otteniamo:

$$1 \longrightarrow \langle -1 \rangle \longrightarrow K^* \xrightarrow{\hat{}2} K^* \longrightarrow \mathrm{Hom}_{\mathrm{cont}}(G, \langle -1 \rangle) \longrightarrow H^1(G, \overline{K}^*)$$

dove abbiamo usato che G agisce banalmente su $\langle -1 \rangle$ e quindi vale l'uguaglianza in (1.3).

D'altra parte per il Teorema 90 di Hilbert versione infinita (si veda [NSW08, 6.2.1]) si ha che

$$H^1(\mathrm{Gal}\left(\overline{K}/K\right), \overline{K}^*) = 1$$

quindi, data la descrizione di ∂, otteniamo:

Proposizione 1.3.2 (Kummer). $\frac{K^*}{K^{*2}} \xrightarrow{\sim} \mathrm{Hom}_{cont}(\mathrm{Gal}\left(\overline{K}/K\right), \mathbb{Z}/2\mathbb{Z})$ *dove l'isomorfismo è dato da*

$$\frac{K^*}{K^{*2}} \ni [a] \longrightarrow \chi : g \mapsto \frac{g(\sqrt{a})}{\sqrt{a}}.$$

È facile verificare che l'inversa dell'isomorfismo di Kummer è la mappa che manda

$$\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}\left(\overline{K}/K\right), \mathbb{Z}/2\mathbb{Z}) \ni \chi \mapsto [z]$$

dove z è tale che $\overline{K}^{\ker\chi} = K(\sqrt{z})$.

Anelli degli interi di campi di numeri

Nel caso in cui K è un campo di numeri, per la descrizione del gruppo $E(K)$ possiamo sfruttare le importanti proprietà del suo anello degli interi

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ è intero su } \mathbb{Z}\}.$$

Chiaramente $\mathcal{O}_K$ è integralmente chiuso.

Proposizione 1.3.3. *Per ogni campo di numeri K, $\mathcal{O}_K$ è un dominio di Dedekind, cioè un dominio noetheriano, integralmente chiuso e di dimensione di Krull 1 (ovvero tale che ogni ideale primo non nullo è massimale).*

Definizione 1.3.4. Sia R un dominio e sia K il suo campo dei quozienti. Un R-modulo $I \subset K$ si dice *ideale frazionario* se

$$\exists d \in R \text{ tale che } dI \subset R.$$

Per un dominio di Dedekind R, possiamo definire

$$\mathcal{F}(R) = \{I \text{ ideali frazionari di } R\}.$$

Chiaramente, se I, J sono ideali frazionari, anche IJ lo è. Per ogni ideale frazionario I di R, possiamo definire:

$$I^{-1} = \{x \in K \mid xI \subset R\}$$

e si dimostra che I^{-1} è un ideale frazionario di R. Diciamo che I è invertibile se $II^{-1} = R$.
Un risultato importante sui domini di Dedekind è il seguente Teorema di fattorizzazione unica, [Sam70, 3.4 Teorema 3]:

Teorema 1.3.5. *Sia R un dominio di Dedekind. Ogni ideale frazionario $I \neq (0)$ di R si scrive in modo unico come prodotto di ideali primi, cioè esistono P_i ideali primi e $e_i \in \mathbb{Z}$ tali che*

$$I = P_1^{e_1} \cdots P_r^{e_r}.$$

In particolare ogni ideale frazionario di $\mathcal{O}_K$ è invertibile.

Il teorema di fattorizzazione unica è molto importante perché permette di definire una nozione di divisibilità fra gli ideali frazionari. Dati due ideali $I, J \subset R$, diciamo che

$$I \mid J \text{ se esiste } L \subset R \text{ per cui J = IL.}$$

Si può dimostrare che $I \mid J$ se e soltanto se $J \subset I$.

Grazie alla nozione di divisibilità introdotta, possiamo quindi definire nel modo canonico

$$\text{mcd}(I, J) \quad \text{e mcm}(IJ).$$

Un'altra conseguenza del teorema di fattorizzazione unica è che, per ogni dominio di Dedekind R, $\mathcal{F}(R)$ è un gruppo abeliano generato dagli ideali primi.

Definizione 1.3.6. Dato un campo K definiamo *gruppo delle classi di ideali* il quoziente

$$\text{Cl}(K) = \frac{\mathcal{F}(\mathcal{O}_K)}{\mathcal{P}(\mathcal{O}_K)}$$

dove $\mathcal{P}(\mathcal{O}_K)$ è il sottogruppo degli ideali frazionari principali.

Nel caso dei campi di numeri vale il seguente teorema, [Sam70, 4.3 Teorema 2]

Teorema 1.3.7. *Dato un campo di numeri K, il gruppo delle classi* $\text{Cl}(K)$ *è finito.*

Ci sarà utile anche il seguente risultato, che segue dal Teorema delle unità di Dirichlet, [Sam70, 4.4 Teorema 1].

Teorema 1.3.8. *Il gruppo delle unità di $\mathcal{O}_K$ è un gruppo (abeliano) finitamente generato.*

Capitolo 2

Teoria Complessa

In questo capitolo presentiamo la teoria delle funzioni ellittiche e delle funzioni modulari, che useremo per dimostrare che ogni curva ellittica corrisponde ad un toro complesso $\mathbb{C}/\Lambda$, dove Λ è un sottogruppo discreto di $\mathbb{C}$ di rango 2 su $\mathbb{Z}$. Questo ci permetterà anche di caratterizzare le isogenie di curve ellittiche e dimostrare che ogni isogenia è un omomorfismo di gruppi.
Lo sviluppo di questa teoria segue l'approccio proposto in [Zan19].

2.1 Funzioni ellittiche

Sia $\Lambda \subset \mathbb{C}$ un reticolo, ovvero un sottogruppo discreto di $\mathbb{C}$ di rango 2 su $\mathbb{Z}$. I sottogruppi discreti di $\mathbb{R}^n$, [Sam70, 4.1 Teorema 1], sono tutti del tipo $\mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_n$ con $g_1, \ldots, g_n$ linearmente indipendenti su $\mathbb{R}$: quindi ogni reticolo è del tipo $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, dove ω_1, ω_2 sono elementi linearmente indipendenti su $\mathbb{R}$.

Definizione 2.1.1 (Varietà complesse)**.** Uno spazio topologico X è una *varietà complessa* di dimensione n se:

- X è connesso e di Hausdorff;
- $X = \bigcup_\alpha U_\alpha$ con U_α aperti, ed esistono omeomorfismi $\varphi_\alpha : U_\alpha \to \mathbb{C}$, detti *carte*, tali che $\forall \alpha, \beta$ la mappa

$$\varphi_\alpha \circ \varphi_\beta^{-1} : \varphi_\beta(U_\alpha \cap U_\beta) \to \varphi_\alpha(U_\alpha \cap U_\beta) \text{ è olomorfa.}$$

Una varietà complessa di dimensione 1 si chiama *superficie di Riemann.*

Chiaramente $\mathbb{C}/\Lambda$ con la topologia quoziente indotta da $\mathbb{C}$ è una superficie di Riemann, connessa e compatta, per cui le carte sono date dall'inversa della restrizione della proiezione $\mathbb{C} \to \mathbb{C}/\Lambda$ ad un intorno su cui è iniettiva.
Lo spazio proiettivo $\mathbb{P}^n(\mathbb{C})$ è una varietà complessa di dimensione n, con le carte costruite alla Sezione 1.1. Dal teorema della funzione implicita segue che per ogni curva algebrica piana non singolare C, lo spazio $C(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$ è una superficie di Riemann.

In questa sezione caratterizziamo l'insieme delle funzioni meromorfe su $\mathbb{C}/\Lambda$, dimostrando che è il campo delle funzioni di una certa curva ellittica E: vedremo inoltre che $\mathbb{C}/\Lambda \simeq E(\mathbb{C})$, sia come superfici di Riemann che come gruppi.

Definizione 2.1.2 (Funzione ellittica di periodo Λ)**.** Una funzione ellittica di periodo Λ è una funzione meromorfa $f : \mathbb{C} \to \mathbb{C}$ tale che

$$f(z + \omega) = f(z) \ \forall \omega \in \Lambda, z \in \mathbb{C}.$$

Indichiamo con $\mathbb{C}_\Lambda$ l'insieme delle funzioni ellittiche di periodo Λ. È facile verificare che questo è un campo.
Ogni funzione ellittica $f \in \mathbb{C}_\Lambda$ corrisponde per passaggio al quoziente ad una funzione meromorfa (che indichiamo con la stessa lettera)

$$f : \mathbb{C}/\Lambda \to \mathbb{C},$$

dove $\mathbb{C}/\Lambda = \mathbb{C}/\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \simeq S^1 \times S^1$, con la struttura naturale di gruppo quoziente, è un toro complesso. Inoltre f è determinata dalla sua restrizione al dominio fondamentale:

$$D = \{t\omega_1 + s\omega_2 | t, s \in [0, 1)\}.$$

Proposizione 2.1.3. *Una funzione ellittica senza poli (o zeri) è costante.*

Dimostrazione. Supponiamo che f sia una funzione ellittica di reticolo Λ senza poli, cioè una funzione olomorfa. Indicata con $\bar{D}$ la chiusura del dominio fondamentale D, dalla periodicità di f segue che

$$\sup_{\mathbb{C}} |f| = \sup_{\bar{D}} |f| \overset{(*)}{<} M,$$

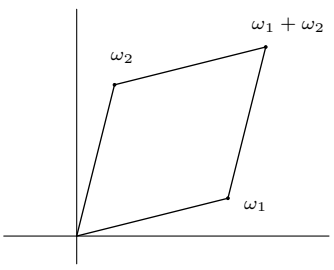
dove in $(*)$ usiamo il fatto che f è limitata per compattezza di $\bar{D}$.
Questo mostra che f è una funzione olomorfa e limitata su $\mathbb{C}$ e per il teorema di Liouville, [Car95, III.1.1], è costante.
Per il caso in cui f è senza zeri, basta applicare lo stesso argomento a $\frac{1}{f}$. □

Data una funzione meromorfa f indichiamo con $\mathrm{ord}_z(f)$ l'ordine di annullamento di f in z e con $\mathrm{Res}_z(f)$ il residuo di f in z.

Proposizione 2.1.4. *Sia f una funzione ellittica non costante di periodo Λ e D un suo dominio fondamentale. Valgono le seguenti uguaglianze:*

- $\sum_{\omega \in D} \mathrm{Res}_\omega(f) = 0$;
- $\sum_{\omega \in D} \mathrm{ord}_\omega(f) = 0$;
- $\sum_{\omega \in D} \omega \mathrm{ord}_\omega(f) \in \Lambda$.

Dimostrazione. Una funzione meromorfa non costante su un compatto ha un numero finito di zeri e di poli: per periodicità di f, a meno di traslare D, possiamo supporre che f non abbia zeri né poli su ∂D.



- Dal teorema dei Residui, [Car95, III.5.2], usando che f è periodica rispetto a Λ abbiamo:

$$\begin{aligned}2\pi i \sum_{\omega\in D} \mathrm{Res}_\omega(f) &= \int_{\partial D} f(z)dz \\ &= \int_0^{\omega_1} f(z)dz + \int_{\omega_1}^{\omega_1+\omega_2} f(z)dz + \int_{\omega_1+\omega_2}^{\omega_2} f(z)dz + \int_{\omega_2}^{0} f(z)dz \\ &= \int_0^{\omega_1} f(z) - f(z)dz + \int_0^{\omega_2} f(z) - f(z)dz = 0.\end{aligned}$$

- Sappiamo che la funzione $g(z) = \frac{f'(z)}{f(z)}$ è tale che $\mathrm{Res}_z(g) = \mathrm{ord}_z(f)$. Inoltre poiché f è ellittica, anche f', e quindi anche g, sono funzioni ellittiche, e la tesi segue applicando il punto 1 alla funzione g.

- Consideriamo la funzione $h(z) = z\frac{f'(z)}{f(z)}$: allora $\mathrm{Res}_z(h) = z\mathrm{ord}_z(f)$: dal teorema dei residui abbiamo

$$\begin{aligned}\sum_{\omega\in D} \omega\mathrm{ord}_\omega(f) &= \frac{1}{2\pi i}\int_{\partial D} h(z)dz \\ &= \frac{1}{2\pi i}\left[\int_0^{\omega_1} z\frac{f'(z)}{f(z)}dz + \int_{\omega_1}^{\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz + \int_{\omega_1+\omega_2}^{\omega_2} z\frac{f'(z)}{f(z)}dz + \int_{\omega_2}^{0} z\frac{f'(z)}{f(z)}dz\right] \\ &= \frac{1}{2\pi i}\left[\int_0^{\omega_1} z\frac{f'(z)}{f(z)} - (z+\omega_2)\frac{f'(z)}{f(z)}dz + \int_0^{\omega_2} (z+\omega_1)\frac{f'(z)}{f(z)} - z\frac{f'(z)}{f(z)}dz\right] \\ &= \omega_1\left(\frac{1}{2\pi i}\int_0^{\omega_2}\frac{f'(z)}{f(z)}dz\right) - \omega_2\left(\frac{1}{2\pi i}\int_0^{\omega_1}\frac{f'(z)}{f(z)}dz\right).\end{aligned}$$

  Adesso $\frac{1}{2\pi i}\int_0^x \frac{f'(z)}{f(z)}$ è l'indice del cammino $t \mapsto f(tx)$: ora per $x = \omega_i$ il cammino è chiuso per la periodicità di f, quindi $\frac{1}{2\pi i}\int_0^{\omega_1}\frac{f'(z)}{f(z)}dz$ e $\frac{1}{2\pi i}\int_0^{\omega_2}\frac{f'(z)}{f(z)}dz$ sono interi.

□

Proposizione 2.1.5. *Per ogni reticolo $\Lambda \subset \mathbb{C}$ definiamo la* funzione di Weierstrass *relativa a Λ come:*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{0\neq\omega\in\Lambda}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

Valgono i seguenti fatti:

- *La serie converge assolutamente su $\mathbb{C}\setminus\Lambda$ e uniformemente su ogni compatto di $\mathbb{C}\setminus\Lambda$;*
- *$\wp_\Lambda(z)$ è una funzione meromorfa su $\mathbb{C}$ con poli doppi su Λ;*
- *$\wp_\Lambda(z)$ è una funzione ellittica pari.*

Dimostrazione. Poiché Λ è un reticolo si può dimostrare che esiste una costante $c = c(\Lambda)$ tale che

$$\#\{\omega\in\Lambda | N \leq |\omega| < N+1\} < cN.$$

Nel seguito per semplicità di notazione indichiamo $\wp_\Lambda$ con $\wp$.

- Per ogni $R > 0$, si ha $\Lambda \setminus \{0\} = S \cup S'$ dove $S = \{\omega \in \Lambda : 0 \neq |\omega| \leq 2R\}$ è un insieme finito perché Λ è discreto, e S' il complementare.

  Sia z tale che $|z| \leq R$: allora $\wp(z) = \frac{1}{z^2} + t(z) + t'(z)$ dove:

  - $t(z) = \sum_{\omega \in S} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ è una somma finita, quindi ben definita per ogni $z \notin \Lambda$;
  - $t'(z) = \sum_{\omega \in S'} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$: poiché in S' vale $|\omega/2| > R \geq |z|$, abbiamo la seguente stima:

    $$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right| \leq \frac{5/2R|\omega|}{|\omega|^2 |\omega/2|^2} = \frac{10R}{|\omega^3|}$$

    da cui otteniamo

    $$\sum_{\omega \in S'} \left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| \leq 10R \sum_{\omega \in S'} \frac{1}{|\omega|^3} \leq 10R \sum_{N=1}^{\infty} \frac{cN}{N^3} < +\infty,$$

    ovvero la serie converge assolutamente per ogni $z \in \mathbb{C} \setminus \Lambda$ e uniformemente sui compatti di $\mathbb{C} \setminus \Lambda$.

- Per il punto precedente, la funzione $\wp$ è una funzione olomorfa su $\mathbb{C} \setminus \Lambda$ e come funzione $\mathbb{C} \to \mathbb{C}$ ha un polo doppio in ogni $\omega \in \Lambda$.

- Sostituendo ω con $-\omega$ nella serie che definisce $\wp$ si vede che è una funzione pari. Per verificare che $\wp$ è una funzione ellittica (ovvero che ha periodo Λ) calcoliamo la sua derivata: per uniforme convergenza della serie che definisce $\wp$ si ha:

  $$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3} \ \forall z \notin \Lambda.$$

  Quindi per ogni $\omega_0 \in \Lambda$ vale

  $$\wp'(z + \omega_0) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z + \omega_0 - \omega)^3} = -2 \sum_{\overline{\omega} \in \Lambda} \frac{1}{(z - \overline{\omega})^3} = \wp'(z),$$

  dove possiamo riordinare la serie per convergenza assoluta.

  Da questo si ottiene che $\wp(z + \omega_0) = \wp(z) + c(\omega_0)$ per ogni $z \notin \Lambda$. Valutando in $z = -\omega_0/2$ troviamo

  $$\wp\left(\frac{\omega_0}{2}\right) = \wp\left(-\frac{\omega_0}{2}\right) + c(\omega_0) \overset{\wp \text{ pari}}{\Longrightarrow} c(\omega_0) = 0$$

  e questo dimostra la periodicità di $\wp$.

Quanto dimostrato mostra anche che $\wp'(z)$ è una funzione ellittica dispari e come funzione $\wp' : \mathbb{C}/\Lambda \to \mathbb{C}$ ha un unico polo triplo in 0. Per la Proposizione 2.1.4, $\wp'$ ha quindi esattamente 3 zeri, ed è facile verificare che questi sono i punti $\omega_1/2$, $\omega_2/2$ e $(\omega_1+\omega_2)/2$, ovvero gli unici tre punti di ordine 2 di $\mathbb{C}/\Lambda$. □

Gli stessi argomenti della dimostrazione precedente possono essere usati per dimostrare che le serie di Eisenstein

$$G_n(\Lambda) = \sum_{0 \neq \omega \in \Lambda} \frac{1}{\omega^{2n}} \tag{2.1}$$

convergono assolutamente per $n > 1$.

Proposizione 2.1.6. $\mathbb{C}_\Lambda = \mathbb{C}(\wp(z), \wp'(z))$.

Dimostrazione. Abbiamo già dimostrato che $\wp(z), \wp'(z)$ sono funzioni ellittiche di periodo Λ quindi $\mathbb{C}(\wp(z), \wp'(z)) \subset \mathbb{C}_\Lambda$. Vediamo l'altro contenimento.

Ogni funzione ellittica è somma di una funzione ellittica pari e una dispari: infatti se f è una funzione ellittica anche $f(-\cdot)$ è una funzione ellittica, e vale

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}.$$

Quindi basta dimostrare $f \in \mathbb{C}(\wp(z), \wp'(z))$ per ogni funzione ellittica f pari o dispari.

Sia $f : \mathbb{C}/\Lambda \to \mathbb{C}$ una funzione meromorfa pari ed indichiamo con T il toro complesso $\mathbb{C}/\Lambda$: osserviamo che se $u \in T$ è tale che $u = -u$ allora $\mathrm{ord}_u(f)$ è pari. Infatti se f è pari, $f^{(2k)}$ è pari e $f^{(2k+1)}$ è dispari: quindi

$$f^{(2k+1)}(u) = -f^{(2k+1)}(-u) = -f^{(2k+1)}(u) \implies f^{(2k+1)}(u) = 0,$$

cioè $\mathrm{ord}_u(f) = \min\{k | f^{(k)}(u) \neq 0\}$ è pari.

Osserviamo che:

1. Ogni f è una funzione meromorfa su un compatto ha un numero finito di poli: indichiamo con $z_1, \ldots, z_n$ i poli di f diversi da 0.
   Detto $n_i = \mathrm{ord}_{z_i}(f) < 0$, poniamo
   $$g : \mathbb{C}/\Lambda \to \mathbb{C}$$
   $$g(z) = \left(\prod_{i=1}^{n} (\wp(z) - \wp(z_i))^{-n_i} \right) f(z).$$
   La funzione $\wp(z) - \wp(z_i)$ ha come unico polo 0 e come zeri z_i e $-z_i$, quindi $g(z)$ è una funzione ellittica pari, con al più un unico polo in 0.

2. Sia f una funzione ellittica pari con al più un unico polo in 0: sappiamo che $\mathrm{ord}_0(f) = -2m$. Dimostriamo per induzione su m che $f \in \mathbb{C}[\wp(z)]$.

   - Se $\mathrm{ord}_0(f) = 0$, allora f è una funzione ellittica senza poli, e per la Proposizione 2.1.3 è costante.
   - Sia $\mathrm{ord}_0(f) = -2m$: allora in serie di Laurent $f(z) = \frac{c}{z^{2m}} + \ldots$, cioè la funzione
     $$h(z) = f(z) - c(\wp(z))^m \text{ è tale che } \mathrm{ord}_0(h) > -2m.$$
     Per ipotesi induttiva $h(z) = A(\wp(z))$ con $A(x) \in \mathbb{C}[x]$, da cui otteniamo
     $$f(z) = c(\wp(z))^m + A(\wp(z)) \in \mathbb{C}[\wp(z)].$$

Per ogni funzione ellittica pari f, dal punto 1 troviamo un polinomio $B \in \mathbb{C}[z]$ tale che $B(\wp(z))f(z)$ ha come unico polo 0, e dal punto 2 un polinomio $A \in \mathbb{C}[z]$ tale che:

$$B(\wp(z))f(z) = A(\wp(z)) \implies f(z) = \frac{A(\wp(z))}{B(\wp(z))} \in \mathbb{C}(\wp(z)).$$

Infine per ogni funzione ellittica dispari f, la funzione $f(z)\wp'(z)$ è una funzione ellittica pari, quindi $f(z) \in \mathbb{C}(\wp(z), \wp'(z))$.

□

Corollario 2.1.7. *Per ogni $z \in \mathbb{C}$, $z \notin \Lambda$ vale*

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2\wp(z) - g_3$$

dove $g_2 = 60G_2$ e $g_3 = 140G_3$, e $G_n = G_n(\Lambda)$ sono le serie di Eisenstein associate al reticolo Λ definite dall'equazione (2.1).
Inoltre il polinomio $A(x) = 4x^3 - g_2x - g_3$ non ha radici multiple.

Dimostrazione. Nella dimostrazione del teorema precedente abbiamo visto che ogni funzione ellittica pari con un unico polo in 0 appartiene a $\mathbb{C}[\wp(z)]$: in particolare esiste un polinomio $A(x) \in \mathbb{C}[x]$ tale che

$$\left(\wp'(z)\right)^2 = A(\wp(z)).$$

Sappiamo che $\mathrm{ord}_0(\wp') = -3$ e $\mathrm{ord}_0(\wp) = -2$: quindi

$$-6 = \mathrm{ord}_0\left(\wp'^2\right) = \mathrm{ord}_0\left(A(\wp(\cdot))\right) = -2 \cdot \deg A,$$

cioè A è un polinomio di grado 3.
Inoltre il polinomio $A(x)$ non può avere radici multiple, infatti se esistesse c tale che $A(x) = (x-c)^2(ax+b)$ allora avremmo

$$\left(\frac{\wp'(z)}{\wp(z)-c}\right)^2 = a\wp(z) + b.$$

Contiamo i poli: la funzione $\wp(z) - c$ ha un unico polo doppio in 0, quindi per la Proposizione 2.1.4 ha esattamente due zeri, cioè $\left(\frac{\wp'(z)}{\wp(z)-c}\right)^2$ ha almeno 4 poli contati con molteplicità. D'altra parte $a\wp(z) + b$ è una funzione con un unico polo doppio in 0. Questo dà l'assurdo.

Vediamo ora la forma del polinomio $A(x)$, e per farlo scriviamo la serie di Laurent di $\wp(z)$ in 0. Se $|z| < |\omega|$, allora

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(\frac{z}{\omega}-1)^2} - 1\right) = \frac{1}{\omega^2}\sum_{n\geq 2} n\left(\frac{z}{\omega}\right)^{n-1},$$

da cui otteniamo

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n\left(\sum_{\Lambda\setminus\{0\}}\frac{1}{\omega^{n+2}}\right).$$

Osserviamo che se n è dispari, poiché Λ è simmetrico rispetto allo 0, $\sum_{\Lambda\setminus\{0\}}\frac{1}{\omega^{n+2}} = 0$. Otteniamo quindi che lo sviluppo di $\wp$ in serie di Laurent in 0 è:

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

Derivando otteniamo $\wp'(z) = -\frac{2}{z^3} + \sum_{n=1}^{\infty} 2n(2n+1)G_n z^{2n-1}$, e confrontando i coefficienti delle serie di Laurent per $\wp^3$, $\wp'^2$ e $\wp$ otteniamo che la relazione che lega $\wp'^2$ e $\wp$ è:

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_2\wp(z) + 140G_3.$$

□

Il corollario precedente mostra che il campo delle funzioni ellittiche su un reticolo Λ è

$$\mathbb{C}_\Lambda = \mathbb{C}(x, y),$$

dove $y^2 = 4x^3 - g_2x - g_3$ dove g_2 e g_3 sono determinati dal reticolo Λ, o analogamente $\mathbb{C}_\Lambda = \mathbb{C}(E)$ per la curva ellittica E di equazione affine $y^2 = 4x^3 - g_2x - g_3$.
Inoltre ad ogni $z \in \mathbb{C}$ possiamo associare un punto $(\wp(z), \wp'(z)) \in E(\mathbb{C})$.

Definizione 2.1.8. Date due varietà complesse X e Y e una funzione $f : X \to Y$, diciamo che f è olomorfa se è olomorfa in carte, cioè se per ogni carta di X $\varphi_X : U \to \mathbb{C}^n$ e ogni carta di Y $\varphi_Y : V \to \mathbb{C}^m$ di Y tali che $f(U) \subset V$, la funzione

$$\varphi_Y \circ f \circ \varphi_X^{-1} : \mathbb{C}^n \to \mathbb{C}^m \text{ è olomorfa.}$$

Se f è invertibile diciamo che è biolomorfa se è olomorfa con inversa olomorfa.

È facile verificare che in realtà basta che per ogni punto della varietà esista una coppia di carte per cui f letta in quelle carte è olomorfa.

Nella seguente proposizione mostriamo che $\mathbb{C}/\Lambda$ e $E(\mathbb{C})$ sono biolomorfe come superfici di Riemann e isomorfe come gruppi. In particolare questo dimostra che la struttura di gruppo definita sulla curva ellittica nella sezione 1.2.1 è isomorfa alla struttura indotta da $\mathbb{C}/\Lambda$.

Proposizione 2.1.9 (Curva ellittica associata a un toro complesso)**.** *Dato $T = \mathbb{C}/\Lambda$ siano g_2 e g_3 le costanti associate a T: allora*

$$E : y^2 = 4x^3 - g_2x - g_3$$

è una curva ellittica su $\mathbb{C}$. Inoltre la mappa

$$\begin{aligned} W : T &\longrightarrow E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}) \\ z &\longmapsto \begin{cases} [\wp(z), \wp'(z), 1] & [z] \neq 0 \\ [0:1:0] & [z] = 0 \end{cases} \end{aligned}$$

è un isomorfismo di gruppi, ed una mappa biolomorfa fra superfici di Riemann.

Dimostrazione. Dal Corollario 2.1.7 sappiamo che E è una curva ellittica. Consideriamo allora la mappa W descritta sopra.

- Per ogni punto $z \neq 0$, abbiamo $\wp(z), \wp'(z) \in \mathbb{C}$, quindi $W(z)$ è ben definito e dal Corollario 2.1.7 segue che $W(z) \in E(\mathbb{C})$.
  Consideriamo $z = 0$, sappiamo che $\operatorname{ord}_0(\wp(z)/\wp'(z)) = 1$, quindi in un intorno di 0 in cui $\wp'$ non si annulla

  $$W(z) = [\wp(z), \wp'(z), 1] = \left[\frac{\wp(z)}{\wp'(z)}, \frac{\wp'(z)}{\wp'(z)}, \frac{1}{\wp'(z)}\right] \tag{2.2}$$

  da cui troviamo che anche $W(0) = [0:1:0] = \mathcal{O} \in E(\mathbb{C})$.

- W è surgettiva. Sia $(x, y) \in E(\mathbb{C})$: la funzione $\wp(z) - x$ ha almeno uno zero $\bar{z}$. Allora $\wp'(\bar{z})^2 = A(\wp(\bar{z})) = A(x) = y^2$. Quindi $\wp'(\bar{z}) = \pm y$ e poiché $\wp'$ è dispari, uno fra $\bar{z}$ e $-\bar{z}$ è tale che $W(\bar{z}) = [x : y : 1]$.

- W è iniettiva. Supponiamo che esistano $z_1 \neq z_2$ tali che $W(z_1) = W(z_2)$. Se $2z_1 \neq 0$, allora uguagliando $\wp(z_1) = \wp(z_2)$ troviamo che la funzione $\wp(z) - \wp(z_1)$, che ha solo due zeri, e si annulla in $z_1, -z_1$ e z_2 quindi necessariamente $z_2 = -z_1$. D'altra parte

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

ovvero $\wp'(z_1) = 0$: sappiamo però che questo è possibile solo se $2z_1 = 0$. Se $2z_1 = 0$, allora $\wp(z) - \wp(z_1)$ ha almeno uno zero doppio in z_1 e uno zero in z_2, ma quindi troviamo $z_1 = z_2$.

- W è un omomorfismo di gruppi: si tratta di verificare che

$$W(z_1 + z_2) = W(z_1) + W(z_2)$$

dove sommiamo i punti di E con la struttura di gruppo data nella sezione precedente. Supponiamo che z_1 e z_2 siano diversi da 0 (il caso in cui uno dei due è 0 è banale). L'osservazione chiave è che il terzo punto d'intersezione della retta per $W(z_1)$ e $W(z_2)$ (o della tangente a E in $W(z_1)$ se i due punti coincidono) con E è, per surgettività di W, del tipo $W(z_3)$, per un qualche $z_3 \in T$. Inoltre osserviamo che se la retta considerata ha equazione $y = ax + b$, allora z_1, z_2 e z_3 sono zeri semplici della funzione ellittica $\wp'(z) - a\wp(z) - b$: applicando la proposizione 2.1.4 troviamo che i punti z_1, z_2, z_3 rispettano in T

$$z_1 + z_2 + z_3 = 0 \implies z_3 = -(z_1 + z_2).$$

Adesso $W(z_1) + W(z_2)$ è il simmetrico di $W(z_3)$ rispetto all'asse delle x, ovvero

$$W(z_1) + W(z_2) = (\wp(z_3), -\wp'(z_3)) = (\wp(-z_3), \wp'(-z_3)) = W(z_1 + z_2)$$

- $W : \mathbb{C}/\Lambda \to E(\mathbb{C})$ è un biolomorfismo, cioè è olomorfa con inversa olomorfa. Ricordiamo la seguente proposizione:

Proposizione 2.1.10. *Sia $f : U \to V$ una mappa olomorfa, con U, V aperti di $\mathbb{C}$. Se f è invertibile, allora è un biolomorfismo.*

Abbiamo già dimostrato che W è bigettiva: per la proposizione precedente basta dimostrare che è olomorfa. Infatti in carte otteniamo una funzione olomorfa e invertibile fra aperti di $\mathbb{C}$, quindi biolomorfa.

Osserviamo che $E(\mathbb{C})$ è una sottovarietà di $\mathbb{P}^2(\mathbb{C})$: per verificare che W è olomorfa, basta mostrare che $W : \mathbb{C}/\Lambda \to \mathbb{P}^2(\mathbb{C})$ lo è.
Per $z \neq 0$, $W(z) \in U_2 = \{[x : y : 1] \subset \mathbb{P}^2(\mathbb{C})\}$: consideriamo la carta $\phi_2 : U_2 \to \mathbb{C}$ tale che $\phi_2([x : y : 1]) = (x, y)$. Scelto $U(z) \subset \mathbb{C}$ intorno di z tale che $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ ristretta ad $U(z)$ sia iniettiva, ed indicata con i l'inversa, si ha che

$$\phi_2 \circ W \circ i : U(z) \to \mathbb{C}^2 \text{ tale che } z \mapsto (\wp(z), \wp'(z))$$

è una mappa olomorfa.
Su un intorno $U(0)$ di 0 la funzione W ha l'espressione calcolata in (2.2): in questo caso $W(z) \in U_1 = \{[x : 1 : z] \subset \mathbb{P}^2(\mathbb{C})\}$ e abbiamo:

$$\phi_1 \circ W \circ i : U(0) \to \mathbb{C}^2 \text{ tale che } z \mapsto (\wp(z)/\wp'(z), 1/\wp'(z))$$

che è una funzione olomorfa.

□

2.2 Isogenie di tori complessi

Siano $T_1 = \mathbb{C}/\Lambda_1$ e $T_2 = \mathbb{C}/\Lambda_2$ due tori complessi.

Definizione 2.2.1. Si dice *isogenia di tori complessi* una mappa olomorfa $\phi : T_1 \to T_2$ tale che $\phi(0) = 0$.

Proposizione 2.2.2. *Fissati T_1 e T_2 valgono i seguenti fatti:*

(a) Per ogni α tale che $\alpha\Lambda_1 \subset \Lambda_2$

$$\begin{aligned} \phi_\alpha : T_1 &\longrightarrow T_2 \\ [z] &\mapsto [\alpha z] \end{aligned}$$

è una isogenia.

(b) C'è una corrispondenza biunivoca

$$\begin{array}{ccc} \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} & \longrightarrow & \{\textit{isogenie } \phi : T_1 \to T_2\} \\ \alpha & \longmapsto & \phi_\alpha \end{array}$$

Dimostrazione. (a) Sia $\alpha : \mathbb{C} \to \mathbb{C}$ tale che $\alpha(z) = \alpha z$: questa è una mappa olomorfa. Inoltre, se $\alpha\Lambda_1 \subset \Lambda_2$, per ogni $z \equiv w \pmod{\Lambda_1}$, $\alpha(z - w) \in \alpha\Lambda_1 \subset \Lambda_2$, cioè $\alpha z \equiv \alpha w \pmod{\Lambda_2}$, ovvero ϕ_α è ben definita e olomorfa.
In particolare vale $\phi_\alpha([0]) = [0]$, cioè ϕ_α è una isogenia.

(b) Sappiamo dal punto (a) che la corrispondenza è ben definita: dobbiamo verificare che è iniettiva e surgettiva

- Siano α, β tali che $\phi_\alpha = \phi_\beta$, cioè per ogni $z \in T_1$, $(\alpha - \beta)z \in \Lambda_2$. Allora la mappa $\mathbb{C} \to \mathbb{C}$ definita da $z \mapsto (\alpha - \beta)z$ è una mappa olomorfa con immagine nell'insieme discreto Λ_2, quindi per connessione di $\mathbb{C}$ è costante: quindi $\alpha - \beta = 0$.

- Sia $\phi : T_1 \to T_2$ una isogenia di tori: poiché $\mathbb{C} \to \mathbb{C}/\Lambda_2$ è rivestimento universale, la mappa $f : \mathbb{C} \to \mathbb{C}/\Lambda_1 \xrightarrow{\phi} \mathbb{C}/\Lambda_2$ si solleva a una funzione olomorfa $\tilde{f} : \mathbb{C} \to \mathbb{C}$ tale che $\tilde{f}(0) = 0$.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{f}} & \mathbb{C} \\ \downarrow & \overset{f}{\searrow} & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\phi} & \mathbb{C}/\Lambda_2 \end{array}$$

  La mappa $\tilde{f}$ è tale che per ogni $\omega \in \Lambda_1$ e per ogni $z \in \mathbb{C}$, $\tilde{f}(z+\omega) - \tilde{f}(z) \in \Lambda_2$: sempre poiché Λ_2 è discreto, troviamo che $\tilde{f}(z+\omega) - \tilde{f}(z)$ non dipende da z. Quindi derivando otteniamo che per ogni $z \in \mathbb{C}$ e per ogni $\omega \in \Lambda_1$:

$$\tilde{f}'(z + \omega) = \tilde{f}'(z)$$

  ovvero $\tilde{f}'$ è una funzione ellittica olomorfa su $\mathbb{C}$, e per la Proposizione 2.1.3 è costante. Quindi $\tilde{f}(z) = \alpha z + b$ per qualche $\alpha, \beta \in \mathbb{C}$, cioè

$$\phi([z]) = [\alpha z + \beta].$$

  Poiché $\tilde{f}(0) = 0$, necessariamente $\beta = 0$, cioè $\phi([z]) = [\alpha z]$. In particolare inoltre $\tilde{f}(\Lambda_1) \subset \Lambda_2$ cioè $\alpha\Lambda_1 \subset \Lambda_2$ e $\phi = \phi_\alpha$.

□

Proposizione 2.2.3. *Siano E_1 e E_2 due curve ellittiche associate ai tori T_1 e T_2. Allora l'inclusione naturale*

$$\{\textit{isogenie } \varphi : E_1 \to E_2\} \longrightarrow \{\textit{isogenie di tori } \phi : T_1 \to T_2\}$$

è ben definita ed è una bigezione.
Questa corrispondenza è tale che $\mathrm{id}_{E_1} \mapsto \mathrm{id}_{T_1}$ *e date* $\varphi : E_1 \to E_2$ *e* $\varphi' : E_2 \to E_3$ *tali che* $\varphi \mapsto \phi$ *e* $\varphi' \mapsto \phi'$ *allora* $\varphi' \circ \varphi \mapsto \phi' \circ \phi$.

Dimostrazione. Fissiamo due reticoli Λ_1, Λ_2 tali che $T_i = \mathbb{C}/\Lambda_i$.
Dalla Proposizione 2.1.9 abbiamo le mappe biolomorfe $W_i : T_i \to E_i$: ogni isogenia ϕ di curve ellittiche è rappresentata localmente da funzioni razionali quindi induce $W_2^{-1} \circ \phi \circ W_1 : T_1 \to T_2$ olomorfa, che è in particolare un'isogenia perché $W_i(0) = \mathcal{O}$ e $\phi(\mathcal{O}) = \mathcal{O}$.

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ {\scriptstyle W_1}\uparrow & & \uparrow{\scriptstyle W_2} \\ T_1 & \longrightarrow & T_2 \end{array}$$

Quindi abbiamo un'inclusione naturale {isogenie $\varphi : E_1 \to E_2$} nell'insieme {isogenie di tori $\phi : T_1 \to T_2$}. Vediamo che questa mappa è surgettiva.

Sappiamo che ogni isogenia fra tori è del tipo ϕ_α, per qualche $\alpha \in \mathbb{C}$ tale che $\alpha\Lambda_1 \subset \Lambda_2$: la mappa indotta fra curve ellittiche è quindi del tipo $\phi : E_1 \to E_2$ tale che

$$\phi([\wp_1(z) : \wp_1'(z) : 1]) = [\wp_2(\alpha z) : \wp_2'(\alpha z) : 1],$$

dove $\wp_i$ è la mappa di Weierstrass relativa al reticolo Λ_i.

Osserviamo che, poiché $\alpha\Lambda_1 \subset \Lambda_2$,

$$\wp_2(\alpha(z+\omega)) = \wp_2(\alpha z + \alpha\omega) = \wp_2(\alpha z)\ \forall \omega \in \Lambda_1$$

e analogamente $\wp_2'(\alpha(z+\omega)) = \wp_2'(\alpha z)$.
Quindi $\wp_2(\alpha z), \wp_2'(\alpha z)$ sono funzioni in $\mathbb{C}_{\Lambda_1} = \mathbb{C}(\wp_1, \wp_1')$, e questo garantisce che ϕ è una mappa razionale.

Chiaramente questa corrispondenza manda id_{T_1} in id_{E_1}, inoltre il seguente diagramma è commutativo;

$$\begin{array}{ccccc} E_1 & \xrightarrow{\varphi} & E_2 & \xrightarrow{\varphi'} & E_3 \\ {\scriptstyle W_1}\uparrow & & \uparrow{\scriptstyle W_2} & & \uparrow{\scriptstyle W_3} \\ T_1 & \xrightarrow[\phi]{} & T_2 & \xrightarrow[\phi']{} & T_3 \end{array}$$

quindi $\varphi' \circ \varphi \mapsto W_3^{-1} \circ \varphi' \circ \varphi \circ W_1 = \phi' \circ \phi$. □

Inoltre, poiché le mappe ϕ_α sono chiaramente omomorfismi di tori complessi, ogni isogenia di curve ellittiche provenienti da tori è un omomorfismo di gruppo.

Corollario 2.2.4. *Siano E_1 ed E_2 due curve ellittiche associate ai tori $T_1 \simeq \mathbb{C}/\Lambda_1$ e $T_2 \simeq \mathbb{C}/\Lambda_2$: allora E_1 ed E_2 sono isomorfe se e soltanto se i reticoli Λ_1 e Λ_2 sono omotetici, cioè esiste $\alpha \in \mathbb{C}^*$ tale che $\alpha\Lambda_1 = \Lambda_2$.*

Dimostrazione. E_1 ed E_2 sono isomorfe se e soltanto se esistono due isogenie di curve ellittiche $\varphi : E_1 \to E_2$ e $\varphi^{-1} : E_2 \to E_1$ tali che $\mathrm{id}_{E_1} = \varphi^{-1} \circ \varphi$ e $\mathrm{id}_{E_2} = \varphi \circ \varphi^{-1}$.
Per la corrispondenza della proposizione precedente esistono due mappe $\phi : T_1 \to T_2$ e $\psi : T_2 \to T_1$ tali che $\psi \circ \phi = \mathrm{id}_{T_1}$ e $\phi \circ \psi = \mathrm{id}_{T_2}$ e dalla Proposizione 2.2.2 abbiamo $\phi = \phi_\alpha$ e $\psi = \phi_{\alpha^{-1}}$. In particolare questo è possibile se e soltanto se:

$$\alpha\Lambda_1 \subset \Lambda_2, \quad \alpha^{-1}\Lambda_2 \subset \Lambda_1 \text{ cioè } \alpha\Lambda_1 = \Lambda_2.$$

□

2.3 Funzioni modulari

Abbiamo dimostrato nelle sezioni precedenti che ad ogni reticolo Λ, e quindi ad ogni toro complesso $T = \mathbb{C}/\Lambda$, è associata una curva ellittica, e che a tori omotetici sono associate curve isomorfe. Per far vedere che questa corrispondenza è biunivoca, dimostreremo che ogni curva ellittica di equazione $y^2 = 4x^2 - c_2x - c_3$ proviene da un toro.
La chiave della dimostrazione è mostrare che l'invariante j definito nella sezione 1.2.3, visto come funzione che associa ad ogni toro complesso l'invariante j della curva associata, è una funzione surgettiva: per farlo introdurremo alcuni risultati della teoria delle funzioni modulari.

Vogliamo studiare lo spazio dei tori complessi modulo isomorfismo, ovvero lo spazio dei reticoli modulo omotetia.

Sia $\mathcal{H} = \{x + iy \in \mathbb{C} | y > 0\}$ il semipiano superiore di $\mathbb{C}$: osserviamo che dato un reticolo Λ esiste una base del tipo $[\omega_1, \omega_2]$, con $\tau = \frac{\omega_1}{\omega_2} \in \mathcal{H}$, quindi ogni reticolo è omotetico ad uno del tipo $\tau\mathbb{Z} + \mathbb{Z}$ con $\tau \in \mathcal{H}$.

Proposizione 2.3.1. *Due reticoli $\Lambda_1 = \tau_1\mathbb{Z}+\mathbb{Z}$ e $\Lambda_2 = \tau_2\mathbb{Z}+\mathbb{Z}$, con $\tau_1, \tau_2 \in \mathcal{H}$, sono omotetici se e soltanto se esiste $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tale che*

$$g\tau_1 = \frac{a\tau_1 + b}{c\tau_1 + d} = \tau_2,$$

dove $\mathrm{SL}_2(\mathbb{Z}) = \{A \in M(2, \mathbb{Z}) | \det(A) = 1\}$.

Dimostrazione. Osserviamo per prima cosa che se $\tau \in \mathcal{H}$ e $g \in \mathrm{GL}_2(\mathbb{Z})$ allora

$$\mathrm{Im}(g\tau_1) = \mathrm{Im}\left(\frac{a\tau_1 + b}{c\tau_1 + d}\right) = \frac{(ad - bc)\mathrm{Im}(\tau_1)}{|c\tau_1 + d|^2},$$

quindi $g\tau \in \mathcal{H}$ se e soltanto se $g \in \mathrm{SL}_2(\mathbb{Z})$.

Siano Λ_1 e Λ_2 reticoli omotetici e sia $\alpha \in \mathbb{C}^*$ tale che $\Lambda_2 = \alpha\Lambda_1$: allora

$$\begin{cases} \tau_2 = \alpha(a\tau_1 + b) \\ 1 = \alpha(c\tau_1 + d) \end{cases} \quad \text{e} \quad \begin{cases} \alpha\tau_1 = (A\tau_2 + B) \\ \alpha = (C\tau_2 + D) \end{cases}$$

con $a, b, c, d \in \mathbb{Z}$ e $A, B, C, D \in \mathbb{Z}$. Allora $\tau_2 = \frac{\tau_2}{1} = \frac{a\tau_1+b}{c\tau_1+d}$ e vale

$$\begin{pmatrix}\tau_2\\1\end{pmatrix} = \alpha \begin{pmatrix}a & b\\c & d\end{pmatrix}\begin{pmatrix}\tau_1\\1\end{pmatrix} \quad \text{e} \quad \begin{pmatrix}\tau_1\\1\end{pmatrix} = \alpha^{-1}\begin{pmatrix}A & B\\C & D\end{pmatrix}\begin{pmatrix}\tau_2\\1\end{pmatrix}.$$

Quindi la matrice

$$\begin{pmatrix}a & b\\c & d\end{pmatrix}\begin{pmatrix}A & B\\C & D\end{pmatrix}$$

fissa $\begin{pmatrix}\tau_2\\1\end{pmatrix}$ e $\begin{pmatrix}\bar{\tau_2}\\1\end{pmatrix}$, cioè è l'identità. Inoltre la matrice $g = \begin{pmatrix}a & b\\c & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ è tale che $\tau_2 = g\tau_1$, dove $\tau_1, \tau_2 \in \mathcal{H}$, quindi per l'osservazione fatta $g \in \mathrm{SL}_2(\mathbb{Z})$.

D'altra parte se $\tau_2 = g\tau_1$ per $g = \begin{pmatrix}a & b\\c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, allora

$$\tau_1\mathbb{Z} + \mathbb{Z} = (a\tau_1 + b)\mathbb{Z} + (c\tau_1 + d)\mathbb{Z} \sim \frac{(a\tau_1+b)}{(c\tau_1+d)}\mathbb{Z} + \mathbb{Z}$$

□

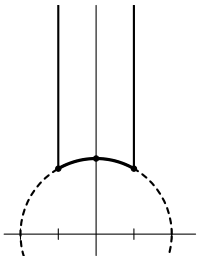
Abbiamo dimostrato che, detto $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, lo spazio dei reticoli modulo omotetia coincide con $\mathcal{H}/\Gamma$ dove l'azione è data da

$$g = \begin{pmatrix}a & b\\c & d\end{pmatrix} \in \Gamma : gz = \frac{az+b}{cz+d} \in \mathcal{H}.$$

Osserviamo che in realtà tutte le matrici scalari agiscono banalmente su $\mathcal{H}$, quindi $\mathcal{H}/\Gamma = \mathcal{H}/\Gamma'$, con $\Gamma' = \Gamma/\{\pm I\}$.

Si può dimostrare, si veda [Lan87, 3§1 Teorema 1], che un dominio fondamentale per l'azione di Γ' su $\mathcal{H}$ è dato da

$$D = \left\{ z \in \mathcal{H} \mid -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2} \text{ e } |z| \geq 1 \right\}.$$



Inoltre vale

$$\Gamma = \langle S, T \mid S^2 = I, (ST)^3 = I \rangle,$$

dove $S = \begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}$ e $T = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$.

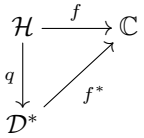
In particolare osserviamo che T è la traslazione di 1.

Definizione 2.3.2. Una funzione f meromorfa su $\mathcal{H}$ si dice *debolmente modulare* di peso $2k$, con $k \in \mathbb{N}$, se per ogni $g = \begin{pmatrix}a & b\\c & d\end{pmatrix} \in \Gamma$ vale

$$f(gz) = f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z).$$

Osserviamo che, poiché $Tz = z + 1$, necessariamente una funzione debolmente modulare è periodica di periodo 1.

Sia $\mathcal{D} = \{z : |z| < 1\}$ e $q : \mathcal{H} \to \mathcal{D}^*$ la funzione $q(z) = e^{2\pi i z}$: poiché f è periodica di periodo 1, induce una funzione meromorfa $f^* : \mathcal{D}^* \to \mathbb{C}$.



Definizione 2.3.3. Una funzione debolmente modulare f si dice *modulare* se f^* si estende ad una funzione meromorfa in 0 (ed in questo caso si dice che f è *meromorfa all'infinito*).
Se f^* è olomorfa su tutto $\mathcal{D}$, allora f si dice *forma modulare*.

Teorema 2.3.4. *Sia f una funzione modulare di peso $2k$, e per ogni $z \in \mathcal{H}$ sia $v_z(f) = \mathrm{ord}_z(f)$: posto $\rho = \frac{1+i\sqrt{3}}{2}$ vale*

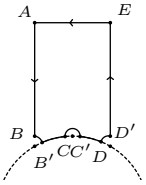
$$v_\infty(f) + \frac{1}{3}v_\rho(f) + \frac{1}{2}v_i(f) + \sum_{\substack{z \neq \rho, i \\ z \in D}} v_z(f) = \frac{k}{6}.$$

Dimostrazione. Osserviamo per prima cosa che ogni funzione modulare ha solo un numero finito di zeri e di poli. Infatti $f^* : \mathcal{D} \to \mathbb{C}$ è una funzione meromorfa, quindi esiste $r > 0$ tale che f^* non ha zeri né poli in $\{0 < |z| < r\}$, ovvero f non ha zeri né poli su $\{z | \mathrm{Im}(z) > \frac{1}{2\pi}\log(1/r)\}$. Restringendoci al dominio fondamentale D, zeri e poli di f appartengono a $D_r = D \cap \{z | \mathrm{Im}(z) \leq \frac{1}{2\pi}\log(1/r)\}$ che è un compatto: f ha solo un numero finito di zeri e poli in D_r, e quindi in D.

Sia $\gamma^{(\epsilon)}$ il cammino descritto in figura scelto in modo che contenga tutti gli zeri e i poli di f, dove i punti E e D' sono il traslato di 1 dei punti A e B rispettivamente, e gli archi BB', CC' e DD' sono archi di circonferenza di raggio ϵ centrati in $\rho, i, -\rho^2$ rispettivamente, con eventualmente ulteriori archi di circonferenza intorno ai possibili poli sul bordo di D.
Per semplicità trattiamo il caso in cui non ci sono poli sul bordo di D.

Per il teorema dei residui:

$$\frac{1}{2\pi i}\int_{\gamma^{(\epsilon)}} \frac{df}{f} = \sum_{\substack{z \neq \rho, i \\ z \in D}} v_z(f).$$



Analizziamo l'integrale sui vari tratti di $\gamma^{(\epsilon)}$, che per brevità indichiamo con γ.

* $\int_{\gamma_{AB}} \frac{df}{f} = -\int_{\gamma_{D'E}} \frac{df}{f}$ perché f periodica di periodo 1;
* $\int_{\gamma_{EA}} \frac{df}{f}$: osserviamo che la funzione q manda γ_{EA} in γ' parametrizzazione in senso orario di una circonferenza centrata nell'origine (che per come abbiamo scelto γ non contiene zeri né poli di f^* diversi da 0)

$$\int_{\gamma_{EA}} \frac{df}{f} = \int_{\gamma'} \frac{df^*}{f^*} = -2\pi i v_\infty(f).$$

* L'integrale sull'arco di circonferenza intorno a ρ è $\int_{\gamma_{BB'}} \frac{df}{f}$: detto $m = v_\rho(f)$, allora $f(z) = (z-\rho)^m g(z)$, con g olomorfa e non nulla su un intorno di ρ, da cui otteniamo

$$\int_{\gamma_{BB'}} \frac{df}{f} = m\int_{\gamma_{BC}} \frac{dz}{z-\rho} + \int_{\gamma_{BC}} \frac{dg}{g}.$$

Ora mandando il raggio della circonferenza a 0, l'integrale di $\frac{dg}{g}$ tende a 0 perché g è olomorfa in ρ, mentre $\int_{\gamma_{BC}} \frac{dz}{z-\rho}$ tende a $-\frac{2\pi i}{6}$.
Quindi

$$\int_{\gamma_{BB'}} \frac{df}{f} \xrightarrow[\epsilon\to 0]{} -\frac{2\pi i}{6} v_\rho(f).$$

Analogamente $\int_{\gamma_{CC'}} \frac{df}{f} \xrightarrow[\epsilon\to 0]{} -\frac{2\pi i}{2} v_i(f)$ e $\int_{\gamma_{DD'}} \frac{df}{f} \xrightarrow[\epsilon\to 0]{} -\frac{2\pi i}{6} v_{\bar\rho}(f)$.

* Infine osserviamo che S manda $z \mapsto -\frac{1}{z}$ quindi manda $\gamma_{B'C} \mapsto \gamma_{DC'}$. Inoltre vale $f(Sz) = z^{2k} f(z)$ quindi $\frac{df}{f}(Sz) = \frac{2kdz}{z} + \frac{df}{f}$, cioè:

$$\begin{aligned}\int_{\gamma_{B'C}} \frac{df}{f} + \int_{\gamma_{C'D}} \frac{df}{f} &= \int_{\gamma_{DC'}} \frac{df}{f}(Sz) + \int_{\gamma_{C'D}} \frac{df}{f} \\ &= \int_{\gamma_{DC'}} \frac{2kdz}{z} + \int_{\gamma_{DC'}} \frac{df}{f} + \int_{\gamma_{C'D}} \frac{df}{f} \\ &= 2k \int_{\gamma_{DC'}} \frac{dz}{z} \xrightarrow[\epsilon\to 0]{} 2k \cdot \frac{2\pi i}{6}.\end{aligned}$$

Unendo i risultati trovati e passando al limite per $\epsilon \to 0$ troviamo la tesi. □

2.3.1 La funzione modulare j

Sappiamo che ad ogni reticolo Λ è associata una curva ellittica E di equazione

$$E : y^2 = 4x^3 - g_2 x - g_3$$

dove $g_2 = 60G_2(\Lambda)$ e $g_3 = 140G_3(\Lambda)$.
Sia $\Lambda = z\mathbb{Z} + \mathbb{Z}$ con $z \in \mathcal{H}$: per ogni k, possiamo considerare le funzioni

$$G_k(z) = G_k(\Lambda) = \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^{2k}} \in \mathbb{C}.$$

Chiaramente $G_k(z) = G_k(z+1)$ e $G_k(-\frac{1}{z}) = z^{2k} G_k(z)$, quindi $G_k : \mathcal{H} \to \mathbb{C}$ è debolmente meromorfa. Inoltre, poiché abbiamo visto nella sezione 2.1 che la serie che definisce G_k è assolutamente convergente,

$$\lim_{z\to\infty} G_k(z) = \lim_{z\to\infty} \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^{2k}} = 2\sum_{n\neq 0} \frac{1}{n^{2k}} \in \mathbb{C}\setminus\{0\}$$

quindi G_k è un forma modulare di peso $2k$.
Analogamente possiamo considerare $\Delta(z) = g_2^3 - 27g_3^2$: è una forma modulare di peso 12, e poiché ogni reticolo definisce una curva non singolare, è diversa da 0 per ogni $z \in \mathbb{C}$. Inoltre dal Teorema 2.3.4 troviamo che $v_\infty(\Delta) = 1$.
Infine consideriamo la funzione $j(z) = 1728\frac{g_2^3}{\Delta}$: questa è una funzione modulare di peso 0 (quoziente di due forme modulari dello stesso peso), olomorfa su $\mathcal{H}$ e

$$v_\infty(j) = v_\infty(g_2^3) - v_\infty(\Delta) = -1.$$

Osserviamo inoltre che, poiché essere modulare di peso 0 equivale ad essere Γ-invariante, per ogni $c \in \mathbb{C}$, $j - c$ è ancora modulare di peso 0.

Proposizione 2.3.5. *$j : \mathcal{H}/\Gamma \to \mathbb{C}$ è una bigezione.*

Dimostrazione. Applicando il Teorema 2.3.4 con $2k = 0$ alla funzione modulare $j - c$:

$$\frac{1}{3}v_\rho + \frac{1}{2}v_i + \sum v_z = 1,$$

dove poiché f è olomorfa su $\mathcal{H}$, gli addendi del termine a sinistra sono tutti positivi: questo è possibile se e soltanto se esiste un unico $z \in \mathcal{H}/\Gamma$ tale che $v_z > 0$. □

Corollario 2.3.6. *Due reticoli Λ_1 e Λ_2 sono omotetici se e soltanto se le curve associate ai due reticoli hanno lo stesso invariante j.*

Dimostrazione. Dato un reticolo Λ possiamo considerare $j(\Lambda)$, l'invariante j della curva ellittica associata a Λ: osserviamo che poiché $j = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$ e $g_k(\alpha\Lambda) = \alpha^{-2k}g_k(\Lambda)$, se $\Lambda_2 = \alpha\Lambda_1$, allora $j(\Lambda_1) = j(\Lambda_2)$.
Viceversa siano $\tau_1, \tau_2 \in \mathcal{H}$ tali che $\Lambda_i \sim \tau_i\mathbb{Z} + \mathbb{Z}$ e supponiamo che i due reticoli abbiano lo stesso j-invariante: allora $j(\tau_1) = j(\tau_2)$ ma j è iniettiva su $\mathcal{H}/\Gamma$, ovvero i due reticoli sono omotetici. □

Corollario 2.3.7. *Dati $c_2, c_3 \in \mathbb{C}$ tali che $c_2^3 - 27c_3^2 \neq 0$, esiste Λ tale che $g_2(\Lambda) = c_2$, $g_3(\Lambda) = c_3$.*

Dimostrazione. Per la proposizione, esiste $\tau \in \mathcal{H}$ tale che $j(\tau) = 1728\frac{c_2^3}{c_2^3 - 27c_3^2}$: sia $\Lambda = \tau\mathbb{Z} + \mathbb{Z}$.
Se $c_2 = 0$, allora $j(\tau) = 0$ e $g_2(\Lambda) = 0$: necessariamente $c_3 \neq 0$, sia allora $\omega \in \mathbb{C}^*$ tale che $\frac{g_3}{c_3} = \omega^6$, allora $\tilde{\Lambda} = \omega\Lambda$ è tale che

$$g_2(\tilde{\Lambda}) = \omega^{-4}g_2(\Lambda) = 0,$$
$$g_3(\tilde{\Lambda}) = \omega^{-6}g_3(\Lambda) = c_3.$$

Altrimenti, $c_2 \neq 0$: sia $\omega \in \mathbb{C}^*$ tale che $\frac{g_2}{c_2} = \omega^4$, allora $\tilde{\Lambda} = \omega\Lambda$ è tale che $g_2(\tilde{\Lambda}) = c_2$. Inoltre, Λ e $\tilde{\Lambda}$ sono reticoli omotetici, quindi vale

$$1728\frac{c_2^3}{c_2^3 - 27c_3^2} = j(\Lambda) = j(\tilde{\Lambda}) = 1728\frac{c_2^3}{c_2^3 - 27g_3^2}$$

cioè $g_3^2(\tilde{\Lambda}) = c_3^2$, quindi uno fra $\tilde{\Lambda}$ e $i\tilde{\Lambda}$ è il reticolo cercato. □

Abbiamo visto alla sezione 1.2.3 che ogni curva ellittica su $\mathbb{C}$ è isomorfa, tramite un cambio di variabili, ad una curva ellittica di equazione $y^2 = 4x^3 - c_2x - c_3$, quindi dal corollario precedente abbiamo:

Corollario 2.3.8. *Sia $E/\mathbb{C}$ una curva ellittica: esiste $\Lambda \subset \mathbb{C}$ unico a meno di omotetia e una mappa biolomorfa, che è anche un omomorfismo di gruppo,*

$$W : \mathbb{C}/\Lambda \to E(\mathbb{C}).$$

In particolare abbiamo dimostrato che esiste una equivalenza di categorie

$$\left\{\begin{array}{l}\textit{Oggetti}\text{: Curve ellittiche su } \mathbb{C} \\ \textit{Mappe}\text{: Isogenie di curve ellittiche}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{Oggetti}\text{: Tori complessi} \\ \textit{Mappe}\text{: Isogenie di tori complessi}\end{array}\right\}$$

Otteniamo in particolare:

Corollario 2.3.9. *Ogni isogenia di curve ellittiche è un omomorfismo di gruppi.*

Capitolo 3

Curve ellittiche su $\mathbb{Q}$

In questa sezione ci occupiamo di studiare la struttura del gruppo dei punti razionali di una curva ellittica $E : y^2 = x^3 + ax^2 + bx + c$ definita su $\mathbb{Q}$.

Il risultato principale è il Teorema di Mordell-Weil su $\mathbb{Q}$, dimostrato nelle sezioni 3.2, 3.3, e 3.4, che afferma che il gruppo $E(\mathbb{Q})$ è finitamente generato, ovvero

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}.$$

Quindi, per descrivere la struttura del gruppo $E(\mathbb{Q})$, bisogna calcolare il *rango* r ed il sottogruppo di torsione (insieme dei punti di ordine finito) $E(\mathbb{Q})_{\text{tors}}$.
Determinare il rango di una curva ellittica è in generale difficile: nella sezione 3.5, ripercorrendo la dimostrazione del Teorema di Mordell-Weil per una curva ellittica E con un punto di 2-torsione, troviamo un'equazione, (3.10), che lega il rango r di $E(\mathbb{Q})$ ad altre quantità aritmetiche dipendenti dalla curva. Da questa equazione si ricava sempre una stima su r, ma trovare r in questo modo in generale è difficile, perché per calcolare le quantità aritmetiche coinvolte bisogna risolvere delle equazioni diofantee, per il cui studio non esiste un metodo sistematico.
Il gruppo di torsione è invece determinato completamente dal Teorema di Nagell-Lutz, presentato nella sezione 3.6: si può dimostrare che i punti di ordine finito hanno tutti coordinate intere ed in particolare la coordinata y ha solo un numero finito di possibilità.

Nel seguito indicheremo con K un campo di numeri e con $\bar{K}$ una fissata chiusura algebrica.

3.1 Punti razionali su $E(K)$

Prima di presentare la dimostrazione del teorema di Mordell-Weil dimostriamo alcune proprietà dei punti K-razionali di una curva ellittica.
Sia $E : y^2 = x^3 + ax^2 + bx + c$ una curva ellittica definita su K: osserviamo che esiste un cambio di variabili in K tale che la nuova equazione della curva è

$$y^2 = f(x) \text{ con } f(x) \in \mathcal{O}_K[x] \text{ monico.}$$

Infatti, poiché $a, b, c \in K$, esistono $a', b', c', d \in \mathcal{O}_K$ tali che $a = \frac{a'}{d}$, $b = \frac{b'}{d}$, $c = \frac{c'}{d}$ e quindi

$$y^2 = x^3 + \frac{a'}{d}x^2 + \frac{b'}{d}x + \frac{c'}{d} \implies (d^3y)^2 = (d^2x)^3 + (a'd)(d^2x)^2 + (b'd^3)(d^2x) + (c'd^5)$$

e il cambio di variabili cercato è $(x, y) \mapsto (d^2x, d^3y)$.

Proposizione 3.1.1. *Sia E una curva ellittica definita su K campo di numeri: allora per ogni $(x, y) \in E(K)$ esistono $m, n, e \in \mathcal{O}_K$ e C ideale di $\mathcal{O}_K$ tali che*

$$x = \frac{m}{e^2}, y = \frac{n}{e^3} \quad \textit{dove } (m, e^2) = C^2, (n, e^3) = C^3$$

Inoltre se $\mathcal{O}_K$ è un PID, si possono scegliere m, n, e in modo che $C = (1)$.

Dimostrazione. Per ogni primo P di $\mathcal{O}_K$, sia $v_P(z)$ l'esponente di P nella fattorizzazione dell'ideale frazionario (z). Dimostriamo che per ogni $(x, y) \in E(K)$ vale

$$v_P(x) < 0 \iff v_P(y) < 0 \iff v_P(x) = -2k, v_P(y) = -3k$$

per qualche $k \in \mathbb{N}$.

In forma normale di Weierstrass E avrà equazione $y^2 = x^3 + ax^2 + bx + c$ con $a, b, c \in \mathcal{O}_K$, quindi $v_P(a), v_P(b), v_P(c) \geq 0$.
Supponiamo $v_P(x) = -h$ con $h > 0$: $v_P(ax^2+bx+c) \geq \min(-2h+v_P(a), -h+v_P(b), v_P(c)) \geq -2h$ e $v_P(x^3) = -3h < -2h$. Quindi: $2v_P(y) = v_P(y^2) = v_P(x^3 + ax^2 + bx + c) = -3h$ da cui otteniamo che $v_P(x) = -h = -2k$ e $v_P(y) = -3k$ per qualche k intero positivo.
D'altra parte se $v_P(y) < 0$, allora $0 > v_P(y^2) = v_P(x^3 + ax^2 + bx + c)$: ora se $v_P(x) \geq 0$ anche $v_P(x^3 + ax^2 + bx + c) \geq 0$, che è assurdo.

Da questo segue che

$$(x) = P_1^{a_1} \cdots P_r^{a_r} Q_1^{-2k_1} \cdots Q_s^{-2k_s} \text{ e}$$
$$(y) = R_1^{c_1} \cdots R_t^{c_t} Q_1^{-3k_1} \cdots Q_s^{-3k_s}$$

con $a_i, k_i, c_i > 0$, ovvero $(x) = I_x/J^2$ e $(y) = I_y/J^3$ con I_x, I_y, J ideali di $\mathcal{O}_K$ tali che $(I_x, J) = (I_y, J) = (1)$.

Se $\mathcal{O}_K$ è un PID, $I_x = (m), I_y = (n), J = (e)$, quindi a meno di moltiplicare m ed n per una unità di $\mathcal{O}_K$ otteniamo $x = \frac{m}{e^2}$ e $y = \frac{n}{e^3}$ con $(m, e) = (n, e) = 1$.

In generale sia $e \in J$: allora $J \mid (e)$, cioè esiste un ideale intero C tale che $(e) = JC$. Quindi

$$(x) = I_x C^2 / J^2 C^2 = I_x C^2 / (e^2),$$

da cui ricaviamo che $I_x C^2$ è un ideale intero principale, e quindi esiste $m \in \mathcal{O}_K$ tale che $I_x C^2 = (m)$.
Ne segue che $(x) = (\frac{m}{e^2})$ e, a meno di moltiplicare m per un'unità di $\mathcal{O}_K$, vale $x = \frac{m}{e^2}$. In questo caso $(m, e^2) = (I_x C^2, JC^2) = (I_x, J)C^2 = C^2$.
Analogamente troviamo che $y = \frac{n}{e^3}$ con $(n) = I_y C^3$. □

3.2 Il teorema di Mordell-Weil

Nelle prossime sezioni dimostriamo il teorema di Mordell-Weil per $K = \mathbb{Q}$.

Teorema 3.2.1 (Mordell-Weil)**.** *Sia E una curva ellittica definita su K. Il gruppo $E(K)$ è un gruppo abeliano finitamente generato.*

Un passo fondamentale per la dimostrazione di questo teorema è la forma debole del teorema di Mordell-Weil che dimostreremo nel paragrafo 3.4:

Teorema 3.2.2 (Mordell-Weil debole)**.** *Sia E una curva ellittica definita su K. L'indice $[E(K) : 2E(K)]$ è finito.*

È chiaro che la forma debole del Teorema di Mordell-Weil non implica quella forte, perché anche gruppi non finitamente generati possono ammettere sottogruppi di indice finito (ad esempio $\mathbb{R}/2\mathbb{R} = 0$ ma $\mathbb{R}$ non è finitamente generato). Strumento fondamentale per arrivare alla dimostrazione del teorema di Mordell-Weil è la teoria delle altezze, che svilupperemo solo nel caso $K = \mathbb{Q}$. Vedremo che moltiplicare per 2 un punto di $E(\mathbb{Q})$ ne aumenta l'altezza: tramite una procedura di discesa, è possibile a stimare ogni punto di $E(\mathbb{Q})$ con rappresentanti di $E(\mathbb{Q})/2E(\mathbb{Q})$ più un punto di altezza "piccola". La conclusione segue dal fatto che esiste solo un numero finito di punti di altezza fissata.

Definizione 3.2.3 (Altezza)**.** Dato $x \in \mathbb{Q}$, sia $x = \frac{m}{n}$ una scrittura di x ridotta ai minimi termini. Definiamo l'*altezza* di x come

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

La funzione definita è interessante perché soddisfa la seguente proprietà di finitezza:

Proposizione 3.2.4 (Proprietà di finitezza dell'altezza)**.** *L'insieme dei punti $x \in \mathbb{Q}$ di altezza minore di una costante fissata è finito.*

Dimostrazione. Sia $M \in \mathbb{N}$: allora $H(x) = \max\{|m|, |n|\} \leq M$ se e soltanto se $|m|, |n| \leq M$. Quindi esistono solo finite possibilità per m e n e quindi per x. □

Data una curva ellittica E definita su $\mathbb{Q}$ possiamo definire l'altezza dei punti di $E(\mathbb{Q})$ nel modo seguente:

Definizione 3.2.5. Per ogni $P \in E(\mathbb{Q})$, l'*altezza* di P è

$$H(P) = H(x) \text{ se } P = (x, y) \text{ e } H(\mathcal{O}) = 1.$$

È facile osservare che $H : E(\mathbb{Q}) \to \mathbb{N}$ rispetta la proprietà di finitezza, ovvero per ogni $M \in \mathbb{N}$:

$$\{P \in \mathcal{O} | H(P) \leq M\} \text{ è finito.}$$

Infatti esiste solo un numero finito di $x \in \mathbb{Q}$ tali che $H(x) \leq N$ ed esistono al più due punti $(x, y) \in \mathbb{Q}$ con la stessa x.

In alcuni contesti si utilizza come altezza l'altezza logaritmica, cioè:

$$h : E(\mathbb{Q}) \to [0, +\infty) \text{ definita da } h(P) = \log(H(P))$$

Mostreremo che l'altezza h ha un buon comportamento rispetto alla legge di gruppo. Il seguente teorema ci permetterà quindi di dimostrare che la forma debole del teorema di Mordell-Weil implica quella forte.

Teorema 3.2.6. *Sia A un gruppo abeliano e supponiamo esista una funzione $h : A \to [0, +\infty)$ tale che*

(a) Per ogni reale M, l'insieme $\{P \in A | h(P) \leq M\}$ è finito.

(b) Per ogni $P \in A$ esiste una costante $k(P)$ tale che

$$h(Q+P) \leq 2h(Q) + k(P) \ \forall Q \in A.$$

(c) Esiste una costante c tale che

$$h(2P) \geq 4h(P) - c \ \forall P \in A.$$

Supponiamo inoltre che valga anche:

(d) Il sottogruppo $2A$ ha indice finito in A.

Allora A è finitamente generato.

Dimostrazione. Indichiamo con $Q_1, \ldots, Q_n$ dei rappresentanti delle classi laterali di $2A$ in A. Vogliamo dimostrare che per ogni punto $P \in A$ la differenza fra P e una combinazione lineari dei Q_i è multiplo di un punto di altezza minore di una costante M che *non dipende* da P: in questo modo $\{Q_1, \ldots, Q_n\} \cup \{R | h(R) < M\}$ è un insieme finito di generatori per A.
Sia $P \in A$ e sia i_1 tale che $P - Q_{i_1} \in 2A$: ovvero

$$P - Q_{i_1} = 2P_1 \text{ per qualche } P_1 \in A$$

Possiamo allora fare lo stesso ragionamento su P_1, e continuare in questo modo:

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\cdots \\ &\cdots \\ P_{m-1} - Q_{i_m} &= 2P_m \\ &\cdots \end{aligned}$$

Quindi per ogni m possiamo scrivere

$$P = Q_{i_1} + 2Q_{i_2} + 2^2 Q_{i_3} + \cdots + 2^{m-1} Q_{i_m} + 2^m P_m,$$

per certi indici i_j e un qualche punto $P_m \in A$.

Dimostriamo che esiste una costante M tale che per ogni $P \in A$ esiste m per cui $h(P_m) < M$. Studiamo come varia l'altezza di P_m rispetto a quella di P.

Sappiamo che $2P_m = P_{m-1} - Q_{i_m}$ quindi, per la proprietà (b), abbiamo che

$$h(2P_m) \leq 2h(P_{m-1}) + k(-Q_{i_m}) \leq 2h(P_{m-1}) + k,$$

dove $k = \max_{1 \leq i \leq n} k(-Q_i)$. Inoltre dalla proprietà (c) abbiamo che

$$h(2P_m) \geq 4h(P_m) - c$$

e quindi otteniamo:

$$\begin{aligned} h(P_m) &\leq \frac{1}{4}\left(h(2P_m) + c\right) \\ &\leq \frac{1}{4}\left(2h(P_{m-1}) + k + c\right) \\ &\leq \frac{h(P_{m-1})}{2} + \frac{k+c}{4}. \end{aligned}$$

Iterando questa disuguaglianza otteniamo

$$h(P_m) \leq \frac{h(P)}{2^m} + \left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^m}\right)\frac{k+c}{2} \leq \frac{h(P)}{2^m} + \frac{k+c}{2}. \tag{3.1}$$

Quindi esiste m per cui $h(P_m) \leq 1 + \frac{k+c}{2} = M$, dove la costante M non dipende da P. □

Grazie al teorema precedente, per dimostrare il teorema di Mordell-Weil su $\mathbb{Q}$ ci basta dimostrare che l'altezza verifica le proprietà (a), (b) e (c) – vedremo queste dimostrazioni nel paragrafo seguente – e la forma debole del teorema di Mordell-Weil (condizione (d) del teorema) – che dimostreremo, per ogni campo di numeri K, nel paragrafo 3.4.

Una volta nota la forma debole del Teorema di Mordell-Weil su K è possibile dimostrare che $E(K)$ è finitamente generato seguendo lo schema che qui applichiamo per $K = \mathbb{Q}$: possiamo costruire anche su $E(K)$ una funzione altezza, e dimostrare che anche questa soddisfa le ipotesi del teorema 3.2.6. Una costruzione può essere trovata in [Sil09, VIII.6].

3.3 Proprietà dell'altezza

In questa sezione verifichiamo che la funzione altezza

$$h : E(\mathbb{Q}) \to [0, +\infty) \text{ data da } h(P) = \log(H(P)) = \begin{cases} \log(1) = 0 & P = \mathcal{O} \\ \log(H(x)) & P = (x, y) \end{cases}$$

verifica le proprietà:

(a) Per ogni reale M, l'insieme $\{P \in E(\mathbb{Q}) | h(P) \leq M\}$ è finito.

(b) Per ogni $P \in E(\mathbb{Q})$ esiste una costante $k = k(P)$ tale che

$$h(Q + P) \leq 2h(Q) + k \ \forall Q \in E(\mathbb{Q}).$$

(c) Esiste una costante c tale che

$$h(2P) \geq 4h(P) - c \ \forall P \in E(\mathbb{Q}).$$

Nel paragrafo precedente abbiamo già visto che la funzione H ha la proprietà di finitezza, e quindi, poiché log è una funzione crescente e illimitata, anche $h = \log \circ H$ rispetta la proprietà di finitezza. Verifichiamo le altre due proprietà.

Per quanto dimostrato nella Sezione 3.1, poiché E è una curva ellittica definita su $\mathbb{Q}$ possiamo supporre che abbia equazione

$$E : y^2 = x^3 + ax^2 + bx + c \text{ con } a, b, c \in \mathbb{Z}.$$

Inoltre se $P = (x, y) \in E(\mathbb{Q})$ esistono $m, n, e \in \mathbb{Z}$ tali che $(m, e) = (n, e) = 1$ e

$$(x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right).$$

Allora $|m| \leq \max\{|m|, |e|^2\} = H(P)$ e $|e|^2 \leq H(P)$: vediamo che esiste una costante l, che dipende dalla curva ellittica E, tale che $|n| \leq \ell H(P)^{\frac{3}{2}}$. Dall'equazione di E otteniamo

$$\begin{aligned} |n|^2 &= |m^3 + ae^2m^2 + be^4m + ce^6| \\ &\leq |m|^3 + |a||e|^2|m|^2 + |b||e|^4|m| + |c||e^6| \quad \leq H(P)^3 \cdot (1 + |a| + |b| + |c|) \end{aligned}$$

cioè, per $\ell = \sqrt{1 + |a| + |b| + |c|}$, vale $|n| \leq \ell H(P)^{\frac{3}{2}}$.

Verifichiamo la proprietà (b).

Lemma 3.3.1. *Sia P un punto di $E(\mathbb{Q})$. Esiste una costante $k = k(E, P)$ tale che*

$$h(Q + P) \leq 2h(Q) + k \ \forall Q \in E(\mathbb{Q}).$$

Dimostrazione. Osserviamo che la tesi è banale per $P = \mathcal{O}$: supponiamo allora che $P = (p, q) \in E(\mathbb{Q})$. Vogliamo dimostrare che esiste una costante k, che dipende da P, tale che $k \geq h(Q + P) - 2h(Q)$: notiamo che basta dimostrare che k funziona per tutti i punti tranne un numero finito, e poi scegliere come costante il massimo fra k e le differenze $h(Q + P) - 2h(Q)$ per quei finiti punti Q che non soddisfano.

Dimostriamo quindi la tesi per tutti i $Q \neq \{P, -P, \mathcal{O}\}$: in questo caso sappiamo dalla Proposizone 1.2.2 che, se $Q = (x, y)$, allora $P + Q = (\xi, \eta)$, dove

$$\xi = \left(\frac{y - q}{x - p}\right)^2 - a - p - x = \frac{(y - q)^2 - (x - p)^2(a + p + x)}{(x - p)^2}$$

Usando $y^2 = x^3 + ax^2 + bx + c$, troviamo

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

dove $A, B, C, D, E, F, G \in \mathbb{Z}$ e dipendono solo dall'equazione della curva e dalle coordinate (p, q) di P. Adesso, sostituendo $x = m/e^2$, $y = n/e^3$ troviamo

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

Sapendo che $|n| \leq \ell H(Q)^{\frac{3}{2}}$, $|e| \leq H(Q)^{\frac{1}{2}}$ e $|m| \leq H(Q)$, otteniamo:

$$H(\xi) \leq \max\{(|A|\ell + |B| + |C| + |D|), (|E| + |F| + |G|)\}H(Q)^2$$

e passando ai logaritmi otteniamo

$$h(P + Q) \leq 2h(Q) + k$$

dove $k = \log(\max\{(|A|\ell + |B| + |C| + |D|), (|E| + |F| + |G|)\})$ dipende solo dall'equazione della curva e dalle coordinate di P. □

Per verificare anche la proprietà (c), dimostriamo prima la seguente proposizione:

Proposizione 3.3.2. *Siano $\phi, \psi \in \mathbb{Z}[x]$ due polinomi senza radici in comune e sia $d = \max\{\deg(\psi), \deg(\phi)\}$.*

- *Esiste* $R = R(\phi, \psi) \geq 1$ *tale che per ogni* $\frac{m}{n} \in \mathbb{Q}$,

$$\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) \text{ divide } R.$$

- *Esiste una costante* $k = k(\phi, \psi)$*, tale che per ogni* $\frac{m}{n} \in \mathbb{Q}$ *che non è una radice di* ψ*, vale*

$$h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \geq dh\left(\frac{m}{n}\right) - k.$$

Dimostrazione. (a) Osserviamo che, poiché ϕ e ψ hanno grado minore o uguale a d, i numeri $n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)$ sono entrambi interi. Possiamo inoltre supporre che ϕ abbia grado d:

$$n^d\phi\left(\frac{m}{n}\right) = a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d$$

Indichiamo con $\phi_1(m,n) = n^d\phi\left(\frac{m}{n}\right)$, $\psi_1(m,n) = n^d\psi\left(\frac{m}{n}\right)$ e sia

$$\gamma = \gcd(\phi_1(m,n), \psi_1(m,n))$$

Poiché ψ e ϕ non hanno radici in comune, sono relativamente primi in $\mathbb{Q}[x]$, quindi esistono due polinomi $f, g \in \mathbb{Q}[x]$ tali che $f\phi + g\psi = 1$. Sia $A \in \mathbb{Z}$ un intero tale che $Af, Ag \in \mathbb{Z}[x]$, allora, detto $D = \max\{\deg(f), \deg(g)\}$, otteniamo l'uguaglianza in $\mathbb{Z}$

$$n^DAf\left(\frac{m}{n}\right)\phi_1(m,n) + n^DAg\left(\frac{m}{n}\right)\psi_1(m,n) = An^{D+d}, \tag{3.2}$$

quindi $\gamma = \gcd(\phi_1(m,n), \psi_1(m,n))$ divide An^{D+d}.

Osserviamo che inoltre γ divide

$$An^{D+d-1}\phi_1(m,n) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + \cdots + Aa_dn^{D+2d-1}$$

e tutti i termini del membro a destra tranne il primo sono divisibili per An^{D+d} (e quindi per γ). Da questo otteniamo:

$$\gamma \mid Aa_0m^dn^{D+d-1} \implies \gamma \text{ divide } (Aa_0m^dn^{D+d-1}, An^{D+d}) \mid An^{D+d-1}a_0.$$

Iterando questo ragionamento, troviamo che $\gamma \mid Aa_0^{D+d} = R$.

(b) Come nel lemma precedente, basta trovare una costante k che soddisfi la tesi per tutti i numeri di $\mathbb{Q}$ tranne al più un numero finito, quindi possiamo supporre che $\frac{m}{n}$ non sia una radice di ϕ. Osserviamo ancora che $h(r) = h(1/r)$, quindi a meno di scambiare ϕ e ψ, possiamo supporre che ϕ abbia grado d. Sempre con le notazioni del punto (a), vogliamo stimare l'altezza di

$$\xi = \frac{\phi(m/n)}{\psi(m/n)} = \frac{n^d\phi(m/n)}{n^d\phi(m/n)} = \frac{\phi_1(m,n)}{\psi_1(m,n)}$$

e detto $\gamma = (\phi_1(m,n), \psi_1(m,n))$ sappiamo che $\gamma \mid R$ e

$$\begin{aligned} H(\xi) &= \max\{|\phi_1(m,n)|/\gamma, |\psi_1(m,n)|/\gamma\} = \frac{1}{\gamma}\max\{|\phi_1(m,n)|, |\psi_1(m,n)|\} \\ &\geq \frac{1}{R}\max\{|\phi_1(m,n)|, |\psi_1(m,n)|\} \geq \frac{1}{2R}\left(|\phi_1(m,n)| + |\psi_1(m,n)|\right). \end{aligned}$$

Allora

$$\frac{H(\xi)}{H(m/n)^d} \geq \frac{1}{2R}\frac{\left(|n^d\phi(m/n)| + |n^d\psi(m/n)|\right)}{\max\{|m|^d, |n|^d\}} = \frac{1}{2R}\frac{(|\phi(m/n)| + |\psi(m/n)|)}{\max\{|m/n|^d, 1\}}$$

e la tesi equivale a dimostrare che il membro a destra è limitato dal basso al variare di $m, n \in \mathbb{Z}$.
Consideriamo allora la funzione $p(t) = \frac{|\phi(t)|+|\psi(t)|}{\max\{|t|^d,1\}}$: poiché ϕ ha grado d e ψ ha grado minore o uguale a d, $\lim_{t\to\infty} p(t) \in \mathbb{Z}\setminus\{0\}$. Allora: fuori da un compatto $p(t) \geq \epsilon > 0$, e dentro il compatto p ha un minimo strettamente maggiore di 0, perché ϕ e ψ non hanno radici in comune. Quindi esiste $C > 0$ per cui $p(t) > 0$. Allora otteniamo

$$H(\xi) \geq \frac{C}{2R}H(m/n)^d \implies h(\xi) \geq dh\left(\frac{m}{n}\right) - k$$

dove $k = \log(2R/C)$. □

Per concludere dimostriamo la proprietà (c).

Lemma 3.3.3. *Esiste una costante k, che dipende solo dalla curva ellittica E, tale che*

$$h(2P) \geq 4h(P) - k \ \forall P \in E(\mathbb{Q}).$$

Dimostrazione. Anche in questo caso basta dimostrare che esiste una costante k che verifica la tesi per tutti i punti tranne un numero finito, quindi possiamo supporre che $2P \neq \mathcal{O}$. Dette $P = (x, y)$ le coordinate del punto P, sappiamo che il punto $2P$ ha coordinate (ξ, η) con

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

dove abbiamo usato che $y^2 = f(x)$. Adesso $f'(x)$ ha grado 2 e $f(x)$ ha grado 3, quindi $\xi = \frac{\phi(x)}{\psi(x)}$ dove $\phi(x) = (f'(x))^2 - 4f(x)(2x-a)$ ha grado 4 e $\psi(x) = 4f(x)$ ha grado 3.

Sappiamo inoltre che, poiché f è non singolare ψ e ϕ non hanno radici in comune, e $x \in \mathbb{Q}$, quindi dalla proposizione precedente otteniamo che esiste una costante $k = k(\psi, \phi) = k(E)$ tale che

$$h(2P) = h(\xi) \geq 4h(x) - k = h(P) - k.$$

□

3.4 Mordell-Weil forma debole

Per completare la dimostrazione del teorema di Mordell-Weil resta da dimostrare che $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ è finito. Come anticipato, dimostreremo più in generale che per ogni curva ellittica E definita su un campo di numeri K, il gruppo $2E(K)$ ha indice finito in $E(K)$.

Nel seguito indicheremo con E una curva ellittica definita su K: possiamo supporre che abbia equazione del tipo

$$E : y^2 = f(x) \text{ con } f \text{ polinomio monico in } \mathcal{O}_K[x].$$

Vale la seguente proposizione:

Proposizione 3.4.1. *Sia L un'estensione finita di K: se $[E(L) : 2E(L)]$ è finito, allora anche $[E(K) : 2E(K)]$ è finito.*

Dimostrazione. Consideriamo la mappa $E(K)/2E(K) \to E(L)/2E(L)$: questa ha kernel $I = (E(K) \cap 2E(L))/2E(K)$. Per il primo teorema di omomorfismo, poiché $[E(L) : 2E(L)]$ è finito, $E(K)/2E(K)$ è finito se e soltanto se I è finito. Sia $\tilde{L}$ la chiusura normale di L/K (sappiamo che $\tilde{L}/K$ è di Galois finita) e sia G il suo gruppo di Galois. Per ogni $[P] \in I$ fissiamo un elemento $Q_P \in E(L)$ tale che $P = 2Q_P$.
Osserviamo che per ogni $\sigma \in G$ vale

$$[2](\sigma(Q_P) - Q_P) = \sigma([2]Q) - [2]Q = \sigma(P) - P = 0$$

quindi possiamo associare ad ogni $[P] \in I$ la mappa $\lambda_{[P]} : G \to E[2]$ definita da $\lambda_{[P]}(\sigma) = \sigma(Q_P) - Q_P$.
Questo definisce una mappa $I \to \text{Mappe}(G, E[2])$: vediamo che è iniettiva.
Siano $[P], [P'] \in I$ tali che $\lambda_{[P]} = \lambda_{[P']}$, allora $\sigma(Q_P) - Q_P = \sigma(Q_{P'}) - Q_{P'}$ per ogni $\sigma \in G$, ma quindi $Q_P - Q_{P'}$ è fissato da G ovvero appartiene a $E(K)$. Da questo segue che $P - P' \in 2E(K)$, cioè $[P] = [P']$.
Infine, poiché G e $E[2]$ sono insiemi finiti, anche I è finito. □

Grazie alla proposizione precedente, a meno di sostituire K con una sua estensione che contiene una radice di $f(x)$, basta dimostrare che $[E(K) : 2E(K)]$ è finito nel caso in cui $E(K)$ contenga un punto di ordine 2. La forma debole del Teorema di Mordell-Weil segue quindi dal seguente teorema.

Teorema 3.4.2. *Sia E una curva ellittica non singolare definita su K campo di numeri e supponiamo che esista $T \in E(K)$ di ordine 2, allora $[E(K) : 2E(K)]$ è finito.*

Nei prossimi paragrafi introduciamo gli strumenti per la dimostrazione di questo teorema.

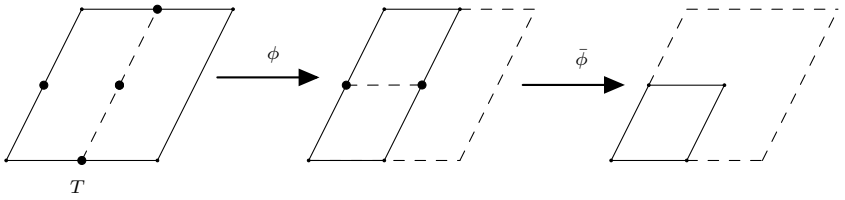
3.4.1 2-isogenie

Vogliamo studiare il cokernel dell'isogenia $[2] : E(K) \to E(K)$: il primo passo è mostrare che nel caso in cui la curva $E(K)$ è definita su K ed ha un punto K-razionale di ordine 2, è possibile trovare un'altra curva ellittica $\overline{E}$ e due mappe $\psi : E(K) \to \overline{E}(K)$ e $\varphi : \overline{E}(K) \to E(K)$ tali che $\varphi \circ \psi = [2]$

Sia $y^2 = f(x)$ l'equazione della curva ellittica E: poiché esiste un punto razionale di ordine 2, ovvero il polinomio $f(x)$ ha una radice in K, a meno di comporre con una traslazione possiamo supporre che il punto di ordine 2 sia $T = (0, 0)$, ovvero che la curva abbia equazione del tipo

$$y^2 = x(x^2 + ax + b) \text{ con } a, b \in \mathcal{O}_K$$

dove la condizione di non singolarità garantisce $a^2 - 4b \neq 0$, e $b \neq 0$.
Dal Corollario 2.3.8 sappiamo che esistono un reticolo Λ e una mappa W tali che $E \simeq \mathbb{C}/\Lambda$ e $W : \mathbb{C}/\Lambda \xrightarrow{\sim} E$. Osserviamo che possiamo sempre trovare $\{\omega_1, \omega_2\}$ base di Λ tale che $T = W\left(\frac{1}{2}\omega_1\right)$: infatti scelta una qualsiasi base $\{z_1, z_2\}$, poiché T è un punto di ordine 2, $T \in \{W(\frac{z_1}{2}), W(\frac{z_2}{2}), W(\frac{z_1+z_2}{2})\}$ e quindi una fra $\{z_1, z_2\}$, $\{z_2, z_1\}$ e $\{z_1 + z_2, z_2\}$ avrà la proprietà richiesta.



Costruiamo una isogenia di E di grado 2: detto $\bar{\Lambda} = \frac{1}{2}\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, consideriamo la mappa $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\bar{\Lambda}$ tale che $[z]_\Lambda \mapsto [z]_{\bar{\Lambda}}$.
È facile verificare che $\ker(\phi) = \{\mathcal{O}, \frac{1}{2}\omega_1\}$, ed in effetti $\deg(\phi) = 2$.
Possiamo costruire allora una mappa $\bar{\phi} : \mathbb{C}/\bar{\Lambda} \to \mathbb{C}/\bar{\bar{\Lambda}}$ dove questa volta $\bar{\bar{\Lambda}} = \frac{1}{2}\omega_1\mathbb{Z} + \frac{1}{2}\omega_2\mathbb{Z} = \frac{1}{2}\Lambda$: allora $\ker(\bar{\phi}) = \{\mathcal{O}, \frac{1}{2}\omega_2\}$. Abbiamo ottenuto:

$$\frac{\mathbb{C}}{\Lambda} \xrightarrow{\phi} \frac{\mathbb{C}}{\bar{\Lambda}} \xrightarrow{\bar{\phi}} \frac{\mathbb{C}}{\frac{1}{2}\Lambda} \overset{[2]}{\simeq} \frac{\mathbb{C}}{\Lambda}$$

Osserviamo inoltre che $[2] \circ \bar{\phi} \circ \phi(z) = [2z]_\Lambda \ \forall z \in \mathbb{C}/\Lambda$, quindi

$$[2] \circ \bar{\phi} \circ \phi = [2] : \frac{\mathbb{C}}{\Lambda} \to \frac{\mathbb{C}}{\Lambda}.$$

Per la Proposizione 2.2.3 sappiamo che ϕ corrisponde a $\psi : E \to \overline{E}$ omomorfismo, e in modo analogo $[2] \circ \bar{\phi}$ corrisponde a $\varphi : \overline{E} \to E$.

Vogliamo trovare una forma esplicita per $\overline{E}$ e per ψ e mostrare che tutto è definito su K.

Proposizione 3.4.3. *Detta τ la traslazione rispetto al punto T e $H = \langle \tau^* \rangle$ vale: $\overline{K}(E)^H = \overline{K}(\bar{x}, \bar{y})$ con $\bar{x} = x + a + \frac{b}{x}$ e $\bar{y} = y\left(1 - \frac{b}{x^2}\right)$.*

Dimostrazione. Dalla Proposizione 1.2.2 sappiamo che per ogni punto $P = (x, y) \in E$, $P \neq T$, il punto $P + T$ ha coordinate $(\tilde{x}, \tilde{y})$ date da:

$$(\tilde{x}, \tilde{y}) = \left(\lambda^2 - a - x, -\lambda\tilde{x} - \nu\right)$$

dove $\lambda = \frac{y}{x}, \nu = 0$, quindi:

$$\begin{cases} \tilde{x} = \lambda^2 - a - x = \frac{y^2}{x^2} - a - x = x + a + \frac{b}{x} - a - x = \frac{b}{x} \\ \tilde{y} = -\left(\lambda\tilde{x} + \nu\right) = -\frac{by}{x^2} \end{cases}$$

Quindi $\tau(x, y) = \left(\frac{b}{x}, -\frac{by}{x^2}\right)$. A questo punto è facile verificare che $\bar{x}$ e $\bar{y}$ appartengono a $\overline{K}(E)^H$, infatti:

- $\lambda = \frac{y}{x} \in \overline{K}(E)$ e $\tau^*(\lambda^2) = \left(-\frac{byx}{bx^2}\right)^2 = \lambda^2$, quindi $\lambda^2 \in \overline{K}(E)^H$: ed in particolare $\lambda^2 = \frac{y^2}{x^2} = x + a + \frac{b}{x} = \bar{x}$;
- $\bar{y} = y - \frac{by}{x^2} \in \overline{K}(E)$ e $\tau^*(y - \frac{by}{x^2}) = \left(-\frac{by}{x^2} + \frac{byx}{xb}\right) = y - \frac{by}{x^2}$.

Quindi $\overline{K}(\bar{x},\bar{y}) \subseteq \overline{K}(E)^H \subseteq \overline{K}(E)$: vediamo che in realtà $\overline{K}(\bar{x},\bar{y}) = \overline{K}(E)^H$ mostrando che $[\overline{K}(E) : \overline{K}(\bar{x},\bar{y})] = 2 = [\overline{K}(E) : \overline{K}(E)^H]$, dove l'ultima uguaglianza segue dalla teoria di Galois, poiché $H < \mathrm{Aut}(K(E))$ e $|H| = 2$.

Osserviamo infatti che $x \notin \overline{K}(\bar{x},\bar{y})$, perché $\tau^*(x) \neq x$, e si può verificare che soddisfa la seguente relazione

$$x^2 - x(\bar{x} - a) + \frac{1}{4}\left((\bar{x} - a)^2 - \frac{\bar{y}^2}{\bar{x}}\right) = 0$$

Inoltre poiché $y = \bar{y}/\left(1 - \frac{b}{x^2}\right)$, $y \in \overline{K}(\bar{x},\bar{y},x)$, cioè $\overline{K}(\bar{x},\bar{y},x) = \overline{K}(x,y)$. Quindi effettivamente $[\overline{K}(E) : \overline{K}(\bar{x},\bar{y})] = [\overline{K}(\bar{x},\bar{y},x) : \overline{K}(\bar{x},\bar{y})] = 2$. □

Dalla Proposizione 1.2.5 abbiamo quindi che $\psi^*(\overline{K}(\overline{E})) \simeq \overline{K}(\bar{x},\bar{y})$.
Una relazione di dipendenza fra $\bar{x}$ e $\bar{y}$ è data da:

$$\begin{aligned}\bar{y}^2 &= y^2(1 - b/x^2)^2 = (x + a + b/x)(x - b/x)^2 \\ &= \bar{x}((x + b/x)^2 - 4b) = \bar{x}((\bar{x} - a)^2 - 4b) = \bar{x}(\bar{x}^2 - 2a\bar{x} + a^2 - 4b).\end{aligned}$$

che è una cubica in forma di Weierstrass definita su K, ed in particolare è non singolare: infatti dalla non singolarità di E si ha che

$$a^2 - 4b \neq 0 \text{ e } (-2a)^2 - 4(a^2 - 4b) = 16b \neq 0.$$

Quindi dal teorema 1.1.12 segue che, a meno di isomorfismo, $\overline{E}$ ha equazione $y^2 = x(x^2 + \bar{a}x + \bar{b})$ dove $\bar{a} = -2a$ e $\bar{b} = a^2 - 4b$.

Possiamo quindi considerare la mappa $\psi : E \to \overline{E}$ data da $\psi(x,y) = (\bar{x},\bar{y})$: questa in forma proiettiva è data dalla mappa razionale

$$\psi([X : Y : Z]) = [Y^2Z : Y(X^2 - bZ^2) : X^2Z]$$

e si può verificare che in effetti è regolare anche in $\mathcal{O}$ e T, e $\psi(\mathcal{O}) = \psi(T) = \mathcal{O}$: quindi ψ è una isogenia di curve ellittiche con $\ker(\psi) = \{\mathcal{O}, T\}$.

Osserviamo inoltre che $\bar{T} = (0,0) \in \bar{E}(K)$ e vale:

$$\psi(x,y) = \left(x + a + \frac{b}{x}, y\left(1 - \frac{b}{x^2}\right)\right) = (0,0) \iff x^2 + ax + b = 0$$

quindi $(0,0)$ è immagine di uno degli altri due punti di ordine 2 di E, e in effetti di entrambi. Detto $i : \mathbb{C}/\bar{\Lambda} \xrightarrow{\sim} \bar{E}$, allora

$$(0,0) \in \{i(\phi(\omega_1/2)), i(\phi(\omega_2/2)), i(\phi((\omega_1 + \omega_2)/2))\} = \{\mathcal{O}, i(\omega_2/2)\},$$

cioè $(0,0) = i(\omega_2/2)$.

Quindi con lo stesso ragionamento troviamo una isogenia $\bar{\psi} : \overline{E} \to \overline{\overline{E}}$ della stessa forma di ψ e tale che $\ker\bar{\psi} = \{\mathcal{O}, \bar{T}\}$, dove $\overline{\overline{E}} \simeq \mathbb{C}/\frac{1}{2}\Lambda$.

In effetti la curva $\overline{\overline{E}}$ ha equazione

$$y^2 = x(x^2 - 2\bar{a}x + \bar{a}^2 - 4\bar{b}) = x(x^2 + 4ax + 16b) \qquad \left(\frac{y}{8}\right)^2 = \frac{x}{4}\left(\left(\frac{x}{4}\right)^2 + a\frac{x}{4} + b\right)$$

e quindi, a meno del cambio di coordinate $(x,y) \mapsto (x/4, y/8)$, coincide con E.

In particolare abbiamo costruito

$$E \xrightarrow{\psi} \overline{E} \xrightarrow{\bar{\psi}} \overline{\overline{E}} \xrightarrow{\sim} E$$

Proposizione 3.4.4. *Siano E e $\overline{E}$ le curve ellittiche su K definite rispettivamente dalle equazioni:*

$$y^2 = x(x^2 + ax + b) \quad e \quad y^2 = x(x^2 + \bar{a}x + \bar{b})$$

dove $a, b \in \mathcal{O}_K$ e $\bar{a} = -2a$, $\bar{b} = 4a^2 - 4b$.

Consideriamo le mappe $\psi : E \to \overline{E}$ e $\varphi = \overline{E} \to E$ definite da:

$$\psi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) & P = (x,y) \neq (0,0) \\ \mathcal{O} & P \in \{(0,0), \mathcal{O}\} \end{cases}$$

$$\varphi(P) = \begin{cases} \left(\frac{y^2}{4x^2}, \frac{y(x^2-\bar{b})}{8x^2}\right) & P = (x,y) \neq (0,0) \\ \mathcal{O} & P \in \{(0,0), \mathcal{O}\} \end{cases}$$

Allora ψ e φ sono omomorfismi,

$$\ker\psi = \{\mathcal{O}, T = (0,0)\},\ \ker\varphi = \{\mathcal{O}, \bar{T} = (0,0)\}$$

e vale $\varphi \circ \psi = [2]$.

Dimostrazione. Dalla Proposizione 2.3.9 sappiamo che le isogenie sono omomorfismi di curve ellittiche, e abbiamo già calcolato i nuclei delle mappe ψ e φ. Dobbiamo solo controllare che $\varphi \circ \psi = [2]$. Questo è chiaramente vero per $\mathcal{O}$ e per i punti di ordine 2, verifichiamolo per $P = (x,y)$ con $y \neq 0$. In questo caso, dalla Proposizione 1.2.2 sappiamo che il punto $2P$ ha coordinate $(\tilde{x}, \tilde{y})$ date da

$$\begin{cases} \tilde{x} = \left(\frac{f'(x)}{2y}\right)^2 - a - 2x = \frac{(x^2-b)^2}{4y^2} \\ \tilde{y} = \lambda x - y - \lambda\tilde{x} = \frac{(x^2-b)(4xy^2 - f'(x)(x^2-b))}{8y^3} \end{cases}$$

Calcolando $\varphi \circ \psi(x,y)$ troviamo

$$\begin{aligned} \varphi \circ \psi(x,y) &= \varphi\left(\frac{y^2(x^2-b)^2}{x^4}\frac{x^4}{4y^4}, \frac{y(x^2-b)}{x^2}\frac{y^4 - \bar{b}x^4}{8y^4}\right) \\ &= \varphi\left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)\frac{y^4-\bar{b}x^4}{x^2}}{8y^3}\right) \end{aligned}$$

e si verifica che $\frac{y^4-\bar{b}x^4}{x^2} = (x^2 + ax + b)^2 - (a^2 - 4b)x^2 = 4xy^2 - f'(x)(x^2 - b)$. Quindi vale $\varphi \circ \psi(x,y) = (\tilde{x}, \tilde{y})$.

□

Osserviamo che poiché le mappe ψ e φ sono K-razionali inducono

$$\psi : E(K) \to \overline{E}(K) \text{ e } \varphi : \overline{E}(K) \to E(K).$$

Abbiamo quindi effettivamente decomposto la mappa $[2] : E(K) \to E(K)$ come $[2] = \varphi \circ \psi$.

Ricordiamo il seguente fatto:

Proposizione 3.4.5. *Siano A, B due gruppi abeliani $\psi : A \to B, \varphi : B \to A$ due omomorfismi. Se $[A : \varphi(B)]$ e $[B : \psi(A)]$ sono finiti anche $[A : \varphi \circ \psi(A)]$ è finito.*

Dimostrazione. Siano $\{a_1, \dots, a_n\}$ e $\{b_1, \dots, b_m\}$ due insiemi di rappresentanti rispettivamente per le classi laterali di $\varphi(B)$ in A e $\psi(A)$ in B. Allora l'insieme $\{a_i + \varphi(b_j) | 1 \leq i \leq n, 1 \leq j \leq m\}$ contiene un insieme di rappresentanti delle classi laterali di $\varphi \circ \psi(A)$ in A.
Infatti dato $a \in A$ esiste i tale che $a - a_i = \varphi(b)$ con $b \in B$, ed esiste j tale che $b - b_j = \psi(a')$ con $a' \in A$: quindi

$$a = a_i + \varphi(b) = a_i + \varphi(b_j + \psi(a')) = a_i + \varphi(b_j) + \varphi \circ \psi(a')$$

□

Grazie alla proposizione precedente, per dimostrare che coker([2]) è finito, basta dimostrare che cokerψ e cokerφ sono finiti.
Inoltre poiché, a meno di un isomorfismo, le mappe ψ e φ sono costruite nello stesso modo, basta dimostrare che coker$\psi = E(K)/\psi(E(K))$ è finito.

3.4.2 Finitezza del cokernel di ψ

La mappa ψ costruita è K-razionale, quindi $\psi(E(\overline{K})) \subset \overline{E}(\overline{K})$. Verifichiamo allora che la seguente successione è esatta:

$$0 \longrightarrow \langle T \rangle \longrightarrow E(\overline{K}) \xrightarrow{\psi} \overline{E}(\overline{K}) \longrightarrow 0$$

La seguente proposizione caratterizza la preimmagini degli elementi dei punti di $\overline{E}$ tramite la mappa ψ.

Proposizione 3.4.6. *Per ogni $P \in \overline{E}(\overline{K})$ vale:*

- *$P = \mathcal{O}$ allora $\psi^{-1}(\mathcal{O}) = \{\mathcal{O}, T\}$;*
- *$P = T$, dette α_1, α_2 le radici di $x^2 + ax + b$, $\psi^{-1}(T) = \{(\alpha_1, 0), (\alpha_2, 0)\}$;*
- *altrimenti, $R = (\bar{x}, \bar{y})$ con $\bar{x} \neq 0$, e sia $\omega \in \overline{K}$ tale che $\bar{x} = \omega^2$: allora detti*

$$x_1 = \frac{1}{2}\left(\bar{x} - a + \frac{\bar{y}}{\omega}\right)$$
$$x_2 = \frac{1}{2}\left(\bar{x} - a - \frac{\bar{y}}{\omega}\right)$$

  vale $\psi^{-1}(P) = \{(x_1, \omega x_1), (x_2, \omega x_2)\}$.

Dimostrazione. Abbiamo già visto la tesi per $\mathcal{O}$ e T. Vediamo il caso $P = (\bar{x}, \bar{y})$ con $\bar{x} = \omega^2 \neq 0$. Un punto $(x, y) \in E(\overline{K})$ tale che $\psi(x, y) = (\bar{x}, \bar{y})$ deve soddisfare:

$$\begin{cases} \bar{x} = \omega^2 = \left(\frac{y}{x}\right)^2 \longrightarrow y^2 = (\omega x)^2 \\ \bar{y} = \frac{y(x^2 - b)}{x^2} \\ y^2 = x^3 + ax^2 + bx \longrightarrow x(x^2 + (a - \omega^2)x + b) = 0 \end{cases}$$

Osserviamo che $x^2 + (a - \omega^2)x + b$ ha discriminante

$$\Delta = (a - \omega^2)^2 - 4b = \omega^4 - 2a\omega^2 + a^2 - 4b \overset{(*)}{=} \left(\frac{\bar{y}}{\omega}\right)^2$$

(dove in $(*)$ usiamo che $(\omega^2, \bar{y}) \in \overline{E}(\overline{K})$): quindi il polinomio ha come radici $x_1, x_2 = \frac{1}{2}\left(\omega^2 - a \pm \frac{\bar{y}}{\omega}\right)$. Osserviamo che vale $x_1 x_2 = b$ e $\omega(x_1 - x_2) = \bar{y}$. Allora per costruzione $(x_i, \omega x_i) \in E(\overline{K})$ e si verifica che

$$\psi(x_i, \omega x_i) = \left(\omega^2, \frac{\omega(x_i^2 - x_1 x_2)}{x_i}\right) = (\bar{x}, \bar{y}).$$

Sappiamo inoltre che $|\ker\psi| = 2$, quindi tutte le fibre hanno cardinalità 2, cioè $\psi^{-1}(\bar{x}, \bar{y}) = \{(x_i, \omega x_i)\}$. □

In particolare per ogni $P \in E(\overline{K})$, $0 \neq \psi^{-1}(P) \subset E(\overline{K})$, cioè ψ è surgettiva.

Detto $G = \mathrm{Gal}\left(\overline{K}/K\right)$, osserviamo che $\langle T\rangle$, $E(\overline{K})$ e $\overline{E}(\overline{K})$ sono $\mathbb{Z}[G]$-moduli: come nell'equazione (1.2) otteniamo una successione esatta

$$0 \longrightarrow \langle T\rangle^G \longrightarrow E(\overline{K})^G \xrightarrow{\psi} \overline{E}(\overline{K})^G \xrightarrow{\partial} H^1(G, \langle T\rangle) \tag{3.3}$$

$$0 \longrightarrow \langle T\rangle \longrightarrow E(K) \xrightarrow{\psi} \overline{E}(K) \xrightarrow{\partial} H^1(G, \langle T\rangle) \tag{3.4}$$

dove $\langle T\rangle^G = \langle T\rangle$ perché $T \in E(K)$, e $E(\overline{K})^G = E(K)$, $\overline{E}(\overline{K})^G = \overline{E}(K)$ perché $\overline{K}^G = K$. Inoltre poiché l'azione di G su $\langle T\rangle$ è banale, vale:

$$H^1(G, \langle T\rangle) = \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}\left(\overline{K}/K\right), \langle T\rangle).$$

La mappa ∂ è costruita così: per ogni $Q \in \overline{E}(K)$ sia $P \in E(\overline{K})$ tale che $\psi(P) = Q$, allora

$$\partial(P) = \chi_P : G \to \langle T\rangle \text{ dove } \chi_P(\sigma) = \sigma P - P.$$

Osserviamo che $\psi(\sigma P) = \sigma\psi(P) = \sigma Q = Q$: quindi $\sigma P \in \psi^{-1}(Q)$, allora:

- $Q = \mathcal{O}$, abbiamo $P = \mathcal{O}$, e $\chi_{\mathcal{O}}(\sigma) = \mathcal{O}\ \forall\sigma \in G$;
- $Q = T$, abbiamo $P = (\alpha_1, 0)$, allora $\ker(\chi_P) = \{\sigma \in G | \sigma(\alpha_1) = \alpha_1\} = \mathrm{Gal}\left(\overline{K}, K(\alpha_1)\right)$. Inoltre $K(\alpha_1) = K(\sqrt{a^2 - 4b}) = K(\sqrt{b})$.
  Quindi $\ker(\chi_P) = \mathrm{Gal}\left(\overline{K}/K\left(\sqrt{b}\right)\right)$.
- $Q = (\bar{x}, \bar{y})$ con $\bar{x} \neq 0$, sia $\omega = \sqrt{\bar{x}}$: allora $P = (x_1, \omega x_1)$ con $x_1 = \frac{1}{2}(\bar{x} - a + \frac{\bar{y}}{\omega})$, quindi vale:

  $$\sigma P = (\sigma(x_1), \sigma(x_1\omega)) = \left(\sigma(x_1) = \frac{1}{2}\left(\bar{x} - a + \frac{\bar{y}}{\sigma(\omega)}\right), \sigma(x_1)\sigma(\omega)\right)$$

  quindi $\sigma P = P \iff \sigma(\omega) = \omega$, ovvero $\ker(\chi_P) = \mathrm{Gal}\left(\overline{K}/K(\omega)\right)$.

Inoltre poiché $\langle T\rangle \simeq \mathbb{Z}/2\mathbb{Z}$, dalla Proposizione 1.3.2 vale:

$$\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}\left(\overline{K}/K\right), T) \simeq \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}\left(\overline{K}/K\right), \mathbb{Z}/2\mathbb{Z}) \overset{i}{\simeq} \frac{K^*}{K^{*2}},$$

dove l'isomorfismo in i è dato da $i(f) = [z]$ tale che $K(\sqrt{z}) = \overline{K}^{\ker(f)}$.
Quindi la successione (3.4) diventa:

$$0 \longrightarrow \langle T\rangle \longrightarrow E(K) \xrightarrow{\psi} \overline{E}(K) \xrightarrow{\alpha} \frac{K^*}{K^{*2}} \tag{3.5}$$

dove $\alpha = i \circ \delta$ è definita da

$$\alpha(Q) = \begin{cases} 1 & (\text{mod } K^{*2}) \quad Q = \mathcal{O} \\ \bar{b} & (\text{mod } K^{*2}) \quad Q = \bar{T} \\ \bar{x} & (\text{mod } K^{*2}) \quad Q = (\bar{x}, \bar{y}), \bar{x} \neq 0 \end{cases}$$

Allora vale: $\text{coker}\psi = \overline{E}(K)/\text{Im}(\psi) = \overline{E}(K)/\ker(\delta) \simeq \text{Im}(\alpha)$: per mostrare che $\text{coker}\psi$ è finito, ci basta allora dimostrare che $\text{Im}(\alpha)$ è finita.

Proposizione 3.4.7. *Valgono i seguenti fatti:*

(a) Esiste un insieme finito $\Sigma \subset K^*/K^{*2}$ tale che $\forall (\bar{x}, \bar{y}) \in \overline{E}(K)$, $\bar{x} \equiv u\gamma \pmod{K^{*2}}$ con $u \in \mathcal{O}_K^*$ e $\gamma \in \Sigma$.

(b) $\text{Im}(\alpha)$ è finita.

Dimostrazione. (a) Dalla Proposizione 3.1.1, sappiamo che esistono $m, n, e \in \mathcal{O}_K$ e C ideale di $\mathcal{O}_K$ tali che $\bar{x} = \frac{m}{e^2}, \bar{y} = \frac{n}{e^3}$ e $(m, e^2) = C^2, (n, e^3) = C^3$. Sostituendo nell'equazione della curva e moltiplicando per e^6 troviamo:

$$n^2 = m(m^2 + \bar{a}me^2 + \bar{b}e^4). \tag{3.6}$$

Poiché $\bar{x} = \frac{m}{e^2} \equiv m \pmod{K^{*2}}$, possiamo limitarci a studiare m modulo K^{*2}. Dall'equazione (3.6) sappiamo che $(n)^2 = (m)(m^2 + \bar{a}me^2 + \bar{b}e^4)$: quindi ogni primo che divide (m) ma non $(m^2 + \bar{a}me^2 + \bar{b}e^4)$, necessariamente ha esponente pari nella fattorizzazione di (m).
Sia $(m) = C^2M$, $(e) = CJ$, sappiamo che $(J, M) = (1)$: allora

$$(m, m^2 + \bar{a}me^2 + \bar{b}e^4) = (m, \bar{b}e^4) = (C^2M, \bar{b}C^4J^4) = C^2(M, \bar{b}C^2J^4) = C^2(M, \bar{b}C^2)$$

e quindi, detto $I = (M, \bar{b}C^2)$, vale $(m) = ID^2$.

Dimostriamo che per ogni primo P che divide I: $v_P(I)$ è pari oppure $P \mid (\bar{b})$.

> Sia $P \mid I$ tale che $P \nmid (\bar{b})$: allora $P \mid (M, C^2)$ e, dette $\mu = v_P(M) > 0$ e $\gamma = v_P(C) > 0$, $v_P(I) = \min\{\mu, 2\gamma\}$. Passiamo alle valutazioni P-adiche nell'equazione (3.6): $v_P((m)) = v_P(C^2M) = 2\gamma + \mu$ e $v_P(e) = v_P(CJ) = \gamma$, infatti $(M, J) = 1$ e $P \mid M$ quindi $P \nmid J$, quindi abbiamo
>
> $$\begin{aligned} v_P((n)^2) &= v_P((m)(m^2 + \bar{a}me^2 + \bar{b}e^4)) \\ &= 2\gamma + \mu + \min\{4\gamma + 2\mu, 4\gamma + \mu + v_P(\bar{a}), v_P(\bar{b}) + 4\gamma\} \\ &\overset{P \nmid (\bar{b})}{=} 2\gamma + \mu + \min\{4\gamma + 2\mu, 4\gamma + \mu + v_P(\bar{a}), 4\gamma\} = 6\gamma + \mu. \end{aligned}$$
>
> Quindi $\mu = 2v_P((n)) - 6\gamma \equiv 0 \pmod 2$, ovvero $v_P(I) = \min\{\mu, 2\gamma\}$ è pari.

Allora, detta $(\bar{b}) = P_1^{a_1} \cdots P_t^{a_t}$ la fattorizzazione di $(\bar{b})$, vale

$$I = JD_1^2 \text{ con } J \in \mathcal{I} = \{P_1^{e_1} \cdots P_t^{e_t} | e_i = 0, 1\}.$$

Abbiamo che $(m) = ID^2 = JD'^2$ con $D' = DD_1$ e $J \in \mathcal{I}$: osserviamo che $\mathcal{I}$ è un insieme finito che dipende solo da $\bar{b}$.
Inoltre poiché K è un campo di numeri, il gruppo delle classi di ideali di K, $\text{Cl}(K)$, è finito: indichiamo con $M_1, \ldots, M_n$ un insieme di rappresentanti delle classi di ideali. Allora esiste i per cui $D' = (d)M_i$ per qualche $d \in K^*$, da cui:

$$(m) = JD'^2 = (d)^2 JM_i^2 \to JM_i^2 = \left(\frac{m}{d^2}\right) \in \mathcal{P}(K).$$

Per ogni $J \in \mathcal{I}$ e per ogni M_i tali che JM_i^2 è principale, fissiamo un elemento $\gamma_{J,i}$ tale che $JM_i^2 = (\gamma_{J,i})$: l'insieme $\Sigma = \{\gamma_{J,i}\}_{J,i}$ è finito. Allora

$$(m) = (d^2)JM_i = (d^2\gamma_{J,i}), \text{ cioè } m\mathcal{O}_K = d^2\gamma_{J,i}\mathcal{O}_K.$$

e quindi esiste $u \in \mathcal{O}_K^*$ tale che $m = u\gamma_{J,i}d^2 \equiv u\gamma_{J,i} \pmod{K^{*2}}$. Allora per ogni $(\bar{x}, \bar{y}) \in \overline{E}(K)$ vale $\bar{x} \equiv m \equiv u\gamma \pmod{K^{*2}}$ con $u \in \mathcal{O}_K^*$, $\gamma \in \Sigma$.
(b) Dal punto (a) sappiamo che $\bar{x} \equiv u\gamma \pmod{K^{*2}}$ con u unità e γ in un insieme finito. Poiché K è un campo di numeri $\mathcal{O}_K^*$ è finitamente generato e quindi $\mathcal{O}_K^*/\mathcal{O}_K^{*2}$ è un gruppo finito, ed in particolare u assume solo un numero finito di valori modulo K^{*2}. Otteniamo che $[\bar{x}]$ ha solo un numero finito di possibilità.
Quindi $\mathrm{Im}(\alpha) = \{1, [\bar{b}]\} \cup \{[\bar{x}] | (\bar{x}, \bar{y}) \in \overline{E}(K)\}$ è finita. □

3.5 Rango di $E(\mathbb{Q})$

Dal teorema di Mordell-Weil e dal teorema di struttura dei gruppi abeliani finitamente generati sappiamo che $E(\mathbb{Q})$ è un prodotto di un sottogruppo libero di rango r ed una parte di torsione T. In questa sezione siamo interessati a capire come determinare il *rango* di $\Gamma = E(\mathbb{Q})$.

Lemma 3.5.1. *Sia A un gruppo abeliano finitamente generato: allora*

$$\left|\frac{A}{2A}\right| = 2^r \cdot |A[2]|$$

dove r è il rango di A e $A[2]$ sottogruppo di 2-torsione di A.

Dimostrazione. Poiché A è un gruppo abeliano finitamente generato si ha $A \simeq \mathbb{Z}^r \times T$. Allora:

$$\frac{A}{2A} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^r \times \frac{T}{2T}.$$

Osserviamo che la mappa $f : T \to 2T$ data da $f(x) = 2x$ è un omomorfismo di gruppi surgettivo e tale che $\ker f = \{x \in T | 2x = 0\} = A[2]$, e dal teorema di omomorfismo otteniamo $2T \simeq T/A[2]$. Poiché A è finitamente generato, T è un gruppo finito, quindi passando alle cardinalità troviamo che $\frac{|T|}{|2T|} = |A[2]|$. □

In particolare quindi il rango r di Γ soddisfa l'equazione

$$[\Gamma : 2\Gamma] = 2^r \cdot |\Gamma[2]|. \tag{3.7}$$

Dall'equazione di $E(\mathbb{Q})$ sappiamo determinare $|\Gamma[2]|$, che è uguale al numero di zeri di $f(x)$ su $\mathbb{Q}$: dobbiamo quindi determinare l'indice di 2Γ in Γ.

Per il calcolo di $[\Gamma : 2\Gamma]$ ci limitiamo al caso in cui $E(\mathbb{Q})$ ha un punto di ordine 2, ovvero ha equazione del tipo

$$y^2 = x(x^2 + ax + b) \quad a, b \in \mathbb{Z}, b \neq 0, a^2 - 4b \neq 0$$

In questo caso dalla dimostrazione della forma debole del teorema di Mordell-Weil abbiamo due mappe

$$\psi : \Gamma \to \overline{\Gamma} \text{ e } \varphi : \overline{\Gamma} \to \Gamma \text{ tali che } \varphi \circ \psi = [2]$$

dove abbiamo indicato $\overline{\Gamma} = \overline{E}(\mathbb{Q})$.
Sappiamo che $\Gamma[2] \subset \varphi(\overline{\Gamma}) \subset \Gamma$, quindi usando i teoremi di omomorfismo troviamo:

$$\frac{\Gamma}{\varphi(\overline{\Gamma})} \simeq \frac{\Gamma/2\Gamma}{\varphi(\overline{\Gamma})/2\Gamma} \simeq \frac{\Gamma/2\Gamma}{\varphi(\overline{\Gamma})/\varphi(\psi(\Gamma))},$$

e passando alle cardinalità otteniamo

$$[\Gamma : 2\Gamma] = [\Gamma : \varphi(\overline{\Gamma})][\varphi(\overline{\Gamma}) : \varphi(\psi(\Gamma))]. \tag{3.8}$$

Inoltre per ogni omomorfismo di gruppi $\varphi : A \to A'$ dato $B < A$, vale:

$$\frac{\varphi(A)}{\varphi(B)} \simeq \frac{A}{(B + \ker(\varphi))} \simeq \frac{A/B}{(B + \ker(\varphi))/B} \simeq \frac{A/B}{\ker(\varphi)/\ker(\varphi) \cap B},$$

quindi per $A = \overline{\Gamma}$ e $B = \psi(\Gamma)$, usando anche (3.8), troviamo:

$$[\Gamma : 2\Gamma] = \frac{[\Gamma : \varphi(\overline{\Gamma})] \cdot [\overline{\Gamma} : \psi(\Gamma)]}{[\ker(\varphi) : \ker(\varphi) \cap \psi(\Gamma)]}. \tag{3.9}$$

Dall'equazione (3.7) otteniamo:

$$2^r = \frac{[\Gamma : \varphi(\overline{\Gamma})] \cdot [\overline{\Gamma} : \psi(\Gamma)]}{[\ker(\varphi) : \ker(\varphi) \cap \psi(\overline{\Gamma})] \cdot |\Gamma[2]|}$$

Osserviamo che $[\ker(\varphi) : \ker(\varphi) \cap \psi(\overline{\Gamma})] \cdot |\Gamma[2]| = 4$: infatti

- dalla Proposizione 3.4.6 sappiamo che $T \in \mathrm{Im}(\psi)$ se e soltanto se la curva ha 3 punti di ordine 2 definiti su $\mathbb{Q}$, ovvero ha $\Delta = a^2 - 4b \in \mathbb{Q}^{*2}$: quindi

$$[\ker(\varphi) : \ker(\varphi) \cap \psi(\overline{\Gamma})] = \begin{cases} 2 & a^2 - 4b \notin \mathbb{Q}^{*2} \\ 1 & a^2 - 4b \in \mathbb{Q}^{*2} \end{cases}$$

- $\{\mathcal{O}, T\} \subseteq \Gamma[2]$ quindi:

$$|\Gamma[2]| = \begin{cases} 2 & a^2 - 4b \notin \mathbb{Q}^{*2} \\ 4 & a^2 - 4b \in \mathbb{Q}^{*2} \end{cases}$$

Inoltre sempre nella dimostrazione del teorema di Mordell-Weil abbiamo costruito una mappa $\alpha : \overline{\Gamma} \to \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$ tale che $\psi(\Gamma) = \ker(\alpha)$, ed in modo analogo si può costruire $\bar{\alpha} : \Gamma \to \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$ tale che $\varphi(\Gamma) = \ker(\bar{\alpha})$. Quindi vale:

$$[\overline{\Gamma} : \psi(\Gamma)] = [\overline{\Gamma} : \ker(\alpha)] = |\alpha(\overline{\Gamma})| \text{ e } [\Gamma : \varphi(\overline{\Gamma})] = |\bar{\alpha}(\Gamma)|.$$

Ricaviamo una formula per il rango di una curva ellittica con un punto di ordine due:

$$2^{r+2} = |\alpha(\overline{\Gamma})| \cdot |\bar{\alpha}(\Gamma)| \tag{3.10}$$

Per definizione di α inoltre $\alpha(\overline{\Gamma}) = \{x \pmod{\mathbb{Q}^{*2}} | (x, y) \in \overline{E}(\mathbb{Q})\} \cup \{[1], [\bar{b}]\}$ e analogamente $\bar{\alpha}(\Gamma) = \{x \pmod{\mathbb{Q}^{*2}} | (x, y) \in E(\mathbb{Q})\} \cup \{[1], [b]\}$

Ricordiamo che per la Proposizione 3.1.1 nel caso $K = \mathbb{Q}$, i punti $(x, y) \in E(\mathbb{Q})$ sono del tipo

$$(x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right) \quad \text{con } (m, e) = 1,\ (n, e) = 1$$

quindi, come nella dimostrazione della forma debole del Teorema di Mordell-Weil, per determinare $\bar{\alpha}(\Gamma)$ dobbiamo trovare $m \pmod{\mathbb{Q}^{*2}}$ al variare delle coppie $(m,n) \in \mathbb{Z}^2$ che soddisfano

$$n^2 = m(m^2 + ame^2 + be^4).$$

Osserviamo che in questo caso necessariamente $m = dm_1^2$ con $d = (m, m^2 + ame^2 + be^4) = (m,b) \mid b$, quindi:

$$\bar{\alpha}(\Gamma) \subset \{1, [b]\} \cup \{[\pm d] : d \mid b\};$$

e d divisore di b appartiene a $\bar{\alpha}(\Gamma)$ se e soltanto se esistono $(m_1, n_1) \in \mathbb{Z}^2$ che soddisfano:

$$n_1^2 = m_1^2 \left(dm_1^4 + am_1^2 e^2 + \frac{b}{d} e^4 \right) \tag{3.11}$$

Ed in modo analogo si può caratterizzare $\alpha(\overline{\Gamma})$.

In generale il calcolo del rango di $E(\mathbb{Q})$ è un problema difficile, perché non esistono metodi generali per decidere se un'equazione come (3.11) ha soluzione. In alcuni casi più semplici, ad esempio quello che mostreremo nella sezione successiva, questo metodo funziona e si riesce a determinare il rango della curva ellittica.

3.6 Il teorema di Nagell-Lutz

In questa sezione riportiamo il teorema di Nagell-Lutz, che caratterizza il sottogruppo di torsione di $E(\mathbb{Q})$ per curve ellittiche definite su $\mathbb{Q}$.

Il punto chiave della dimostrazione del teorema di Nagell-Lutz è il seguente teorema, di cui si può trovare la dimostrazione in [ST15, II.4].

Teorema 3.6.1. *Per ogni primo p, l'insieme*

$$E_p = \{(x,y) \in E(\mathbb{Q}) : ord_p(x) < 0\}$$

non contiene punti di torsione.

Osserviamo che questo teorema, insieme alla Proposizione 3.1.1, garantisce che i punti di ordine finito hanno tutte le coordinate in $\mathbb{Z}$.
Infatti sia $P \in E(\mathbb{Q})$ un punto di torsione diverso da $\mathcal{O}$: sappiamo che esistono $m, n, e \in \mathbb{Z}$ con $(m,e) = (n,e) = 1$ tali che

$$P = \left(\frac{m}{e^2}, \frac{n}{e^3} \right)$$

e per ogni primo p, $P \notin E_p$ per il teorema precedente, cioè $p \nmid e$. Quindi $e = 1$ e $P = (m,n)$.

Teorema 3.6.2. *Sia E una curva ellittica definita su $\mathbb{Q}$ di equazione*

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

e sia $P \in E(\mathbb{Q})$ di ordine finito, $P \neq \mathcal{O}$: allora $P = (x,y)$ con $x, y \in \mathbb{Z}$ e vale uno dei seguenti fatti:

- $y = 0$ *(e quindi P è un punto di ordine 2);*
- $y \mid \mathrm{Ris}(f, f')$*, dove* $\mathrm{Ris}(f, f') = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ *è il discriminante del polinomio* $x^3 + ax^2 + bx + c$*.*

Dimostrazione. Abbiamo già visto che $P = (x, y)$ ha coordinate intere. Consideriamo adesso il punto $2P$:

- $2P = \mathcal{O}$ se e soltanto se $y = 0$;
- se $y \neq 0$, $2P$ è ancora un punto di ordine finito diverso da $\mathcal{O}$, quindi ha coordinate intere. Sia $2P = (X, Y)$: dalle formule in 1.2.2 abbiamo

$$\left(\frac{f'(x)}{2y}\right)^2 = 2x + X + a \in \mathbb{Z} \implies y \mid f'(x)$$

  inoltre chiaramente $y \mid f(x) = y^2$.
  Dalle proprietà del risultante sappiamo che $\mathrm{Ris}(f, f')$: per le proprietà del risultante esistono quindi due polinomi $r(x), s(x)$ tali che $r(x)f(x) + s(x)f'(x) = \mathrm{Ris}(f, f')$, quindi

$$y \mid r(x)f(x) + s(x)f'(x) = \mathrm{Ris}(f, f')$$

□

Capitolo 4

Quattro quadrati in progressione aritmetica

In questa sezione vogliamo dimostrare che non esistono 4 quadrati successivi in una progressione aritmetica non banale, ovvero che non esistono $x, y, z, w \in \mathbb{Z}$ tali che

$$w^2 - z^2 = z^2 - y^2 = y^2 - x^2 = d \neq 0.$$

Questo è uno dei problemi di Fermat, di cui esiste anche una dimostrazione elementare per discesa infinita [Dic66, Capitolo XIV, p.440].

In questa sezione dimostreremo questo risultato come applicazione della teoria sulle curve ellittiche. Infatti mostriamo che le soluzioni al problema di Fermat sono in corrispondenza con i punti razionali di una particolare curva ellittica: i teoremi di Mordell-Weil e di Nagell-Lutz ci permetteranno di dimostrare che i punti razionali di questa curva ellittica corrispondono alle sole progressioni aritmetiche di ragione 0, e quindi sono soluzioni banali.

Osserviamo per prima cosa che possiamo riscrivere il problema dei quattro quadrati in questa forma:

$$\begin{cases} x^2 + d = y^2 \\ y^2 + d = z^2 \\ z^2 + d = w^2 \end{cases} \iff \begin{cases} x^2 + w^2 = y^2 + z^2 \\ w^2 + y^2 = 2z^2 \end{cases}$$

dove possiamo equivalentemente supporre che $x, y, z, w, d \in \mathbb{Q}$ (detto D tale che $Dx, Dy, Dz, Dw \in \mathbb{Z}$, allora $(Dx)^2, (Dy)^2, (Dz)^2, (Dw)^2$ sono 4 quadrati consecutivi di una progressione aritmetica di ragione $D^2 d = (Dy)^2 - (Dx)^2 \in \mathbb{Z}$). Inoltre osserviamo che se $(x : y : w : z)$ è una soluzione al problema dei quattro quadrati, anche $(\lambda x : \lambda y : \lambda z : \lambda w)$ lo è, quindi possiamo cercare soluzioni in $\mathbb{P}^3(\mathbb{Q})$.

Consideriamo allora

$$\mathcal{S}(\overline{\mathbb{Q}}) = \left\{ [x : y : z : w] \in \mathbb{P}^3(\overline{\mathbb{Q}}) : \begin{array}{l} x^2 + w^2 = y^2 + z^2 \\ w^2 + y^2 = 2z^2 \end{array} \right\} \tag{4.1}$$

e dimostriamo che $\mathcal{S}$ è una curva. Per dimostrarlo dobbiamo verificare che $I = (x^2 - y^2 + w^2 - z^2, y^2 + w^2 - 2z^2)$ è un ideale primo di $\overline{\mathbb{Q}}[x, y, z, w]$ e che $\overline{\mathbb{Q}}(\mathcal{S})$ ha grado di trascendenza 1 su $\overline{\mathbb{Q}}$.

Lemma. *$I = (x^2-y^2+w^2-z^2, y^2+w^2-2z^2)$ è un ideale primo di $\overline{\mathbb{Q}}[x,y,z,w]$*

Dimostrazione. Sia $R = \overline{\mathbb{Q}}[y,z,w]$, e chiamiamo $p_1 = x^2 - y^2 + w^2 - z^2$ e $p_2 = y^2 + w^2 - 2z^2$, allora $(p_2) \subset I = (p_1, p_2) \subset R[x]$.
Gli ideali primi di $R[x]$ che contengono (p_2) sono in bigezione con gli ideali primi di $\frac{R[x]}{(p_2)} \simeq \frac{R}{(p_2)}[x]$: per verificare che I è un ideale primo di $R[x]$, basta verificare che $\bar{I} = \frac{(p_1,p_2)}{(p_2)} = (\overline{p_1}(x))$ è un ideale primo di $\frac{R}{(p_2)}[x]$.
Identifichiamo $p_1(x)$ con la sua classe $\overline{p_1}(x) \in \frac{R}{(p_2)}[x]$.

Osserviamo che $p_2 \in R$ è primo, perché R è UFD e p_2 è irriducibile, quindi $D = \frac{R}{(p_2)} = \overline{\mathbb{Q}}[\sqrt{2z^2 - y^2}][y,z]$ è un dominio.
Indichiamo con $F = \overline{\mathbb{Q}}(y,z)(\sqrt{2z^2 - y^2})$ il suo campo delle frazioni: si può verificare che, poiché p_1 è un polinomio monico in x a coefficienti in D, se (p_1) è un primo di $F[x]$, allora (p_1) è primo in $D[x]$.
Poiché F è un campo, e quindi $F[x]$ è UFD, ci basta dimostrare che p_1 è irriducibile in $F[x]$. Osserviamo che $p_1(x) = x^2 - \overline{y^2 - w^2 + z^2}$, quindi è irriducibile se e soltanto se $\alpha = \overline{y^2 - w^2 + z^2} = 2y^2 - z^2$ non è un quadrato in F.

Ora F è una estensione quadratica di $K = \overline{\mathbb{Q}}(y,z)$ e chiaramente α non è un quadrato in K: allora $\alpha \in F^{*2}$ se e soltanto se

$$K(\sqrt{\alpha}) = F = K(\sqrt{2z^2 - y^2})$$

cioè se e soltanto se $\alpha \cdot (2z^2 - y^2)$ è un quadrato in K. Ma è facile verificare che

$$\alpha(2z^2-y^2) = (2y^2-z^2)(2z^2-y^2) = \left(\sqrt{2}y - z\right)\left(\sqrt{2}y + z\right)\left(\sqrt{2}z - y\right)\left(\sqrt{2}z + y\right)$$

non è un quadrato in K, quindi $\bar{I}$ è un ideale primo di $D[x]$. □

Lemma. *$\overline{\mathbb{Q}}(\mathcal{S})$ ha grado di trascendenza 1.*

Dimostrazione. È facile osservare che

$$\overline{\mathbb{Q}}(\mathcal{S}) = \overline{\mathbb{Q}}\left(\frac{x}{w}, \frac{y}{w}, \frac{z}{w}\right),$$

infatti $\frac{x}{w}, \frac{y}{w}, \frac{z}{w}$ sono tre funzioni razionali omogenee di $\overline{\mathbb{Q}}(\mathcal{S})$ distinte e ogni funzione razionale omogenea si può scrivere come funzione razionale di $\frac{x}{w}, \frac{y}{w}, \frac{z}{w}$.
Osserviamo che $\frac{y}{w}$ è trascendente su $\overline{\mathbb{Q}}$ (perché $I \cap \overline{\mathbb{Q}}[y,w] = \{0\}$, quindi y e w non soddisfano nessuna relazione a coefficienti in $\overline{\mathbb{Q}}$), e

$$\left(\frac{z}{w}\right)^2 = \frac{1}{2} + \frac{1}{2}\left(\frac{y}{w}\right)^2 \quad \text{e} \quad \left(\frac{x}{w}\right)^2 = \left(\frac{z}{w}\right)^2 + \left(\frac{y}{w}\right)^2 - 1$$

quindi $\mathrm{trdeg}_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}(\mathcal{S})) = \mathrm{trdeg}_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}}(y/w)) = 1$. □

Ci siamo quindi ridotti a studiare l'insieme dei punti razionali della curva $\mathcal{S}$. Osserviamo che $\mathcal{S}(\mathbb{Q})$ contiene almeno 8 punti $\{[1 : \pm 1 : \pm 1 : \pm 1]\}$, che corrispondono alle progressioni aritmetiche di ragione 0. Quello che vogliamo dimostrare è che $\mathcal{S}(\mathbb{Q})$ ha cardinalità esattamente 8, ovvero che il problema dei quattro quadrati non ha soluzioni non banali.

Consideriamo il punto $P_0 = [1:1:1:1] \in \mathcal{S}(\mathbb{Q})$: possiamo proiettare la curva $\mathcal{S}$ su $\mathbb{P}^2$ dal punto P_0.

$$\begin{aligned} \pi_{P_0} : \mathcal{S} &\longrightarrow \mathbb{P}^2 \\ [x:y:z:w] &\mapsto [x-w : y-w : z-w] \end{aligned}$$

Osserviamo che questa mappa in effetti è definita anche in P_0. Infatti vale:

$$\frac{x-w}{w}\frac{x+w}{w} = \frac{x^2+w^2-2w^2}{w^2} = \frac{y^2+z^2-2w^2}{w^2} = 3\frac{z^2-w^2}{w^2} = 3\frac{z-w}{w}\frac{z+w}{w}$$

e allo stesso modo

$$\frac{y-w}{w}\frac{y+w}{w} = \frac{y^2+w^2-2w^2}{w^2} = \frac{2z^2-2w^2}{w^2} = 2\frac{z-w}{w}\frac{z+w}{w}$$

Quindi abbiamo

$$\begin{aligned} \left[\frac{x-w}{w} : \frac{y-w}{w} : \frac{z-w}{w}\right](P_0) &= \left[3\frac{z-w}{w}\frac{z+w}{x+w} : 2\frac{z-w}{w}\frac{z+w}{y+w} : \frac{z-w}{w}\right](P_0) \\ &= \left[3\frac{z+w}{x+w} : 2\frac{z+w}{y+w} : 1\right](P_0) = [3:2:1] \end{aligned}$$

Inoltre se $[X:Y:Z] = \pi_{P_0}(Q)$ per un punto $Q = [x:y:z:w] \neq P_0$ allora dall'equazione (4.1) otteniamo

$$\begin{cases} (X+w)^2 + w^2 = (Y+w)^2 + (Z+z)^2 \\ w^2 + (Y+w)^2 = 2(Z+w)^2 \end{cases} \implies \begin{cases} X^2 - Y^2 - Z^2 = 2w(Y+Z-X) \\ Y^2 - 2Z^2 = 2w(2Z-Y) \end{cases}$$

e moltiplicando la prima equazione per $2Z-Y$ e la seconda per $Y+Z-X$ otteniamo:

$$(X^2-Y^2-Z^2)(2Z-Y) = (Y^2-2Z^2)(Y+Z-X)$$

$$\mathcal{C} : X^2(2Z-Y) + X(Y^2-2Z^2) + 3ZY(Z-Y) = 0 \tag{4.2}$$

dove si verifica che $\mathcal{C}$ è una curva algebrica piana. Inoltre anche il punto $[3:2:1] \in \mathcal{C}$, cioè abbiamo un morfismo $\pi_{P_0} : \mathcal{S} \longrightarrow \mathcal{C}$.

Si verifica inoltre che

- $Y+Z-X = 0 \iff [X:Y:Z] \in \{[3:2:1], [1:0:1], [1:1:0]\}$
- $2Z-Y = 0 \iff [X:Y:Z] \in \{[3:2:1], [1:0:0]\}$

quindi per ogni $[X:Y:Z] \in \mathcal{C}(\mathbb{Q}) \setminus \{[3:2:1]\}$ è ben definita la funzione

$$w(X:Y:Z) = \begin{cases} \frac{Y^2-2Z^2}{2(2Z-Y)} & 2Z-Y \neq 0 \\ \frac{X^2-Y^2-Z^2}{2(Y+Z-X)} & Y+Z-X \neq 0 \end{cases}$$

e le due definizioni coincidono su $\{2Z-Y \neq 0\} \cap \{Y+Z-X \neq 0\}$ perché $[X:Y:Z] \in \mathcal{C}(\mathbb{Q})$.
Quindi la mappa $\pi_{P_0} : \mathcal{S}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q})$ è surgettiva: dato $Q \in \mathcal{C}(\mathbb{Q})$ se $Q = [3:2:1] = \pi_{P_0}(P_0)$, altrimenti

$$Q = \pi_{P_0}[X + w(Q) : Y + w(Q) : Z + w(Q) : w(Q)]$$

ed il punto $[X+w(Q) : Y+w(Q) : Z+w(Q) : w(Q)]$ appartiene a $\mathcal{S}(\mathbb{Q})$ perché i passaggi usati per trovare l'equazione di $\mathcal{C}$ sono tutti invertibili, e la funzione w è razionale.
Inoltre è facile verificare che la mappa π_{P_0} è iniettiva, quindi π_{P_0} è un isomorfismo di curve che induce una funzione bigettiva

$$\pi_{P_0} : \mathcal{S}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q}).$$

Osserviamo che la curva $\mathcal{C}$ ha un flesso nel punto $Q = [0 : 1 : 1]$: infatti la tangente in Q è la retta di equazione $X + 3Y - 3Z = 0$, e dall'equazione (4.2) sostituendo $3Z = X + 3Y$ e moltiplicando per 9 otteniamo:

$$3X^2(2X+3Y) - X(2X^2+12XY+9Y^2) + 3X(XY+3Y^2) = 0 \iff 4X^3 = 0$$

quindi l'unica intersezione di $3Z = X + 3Y$ con $\mathcal{C}$ è proprio il punto Q.
Consideriamo il cambio di coordinate (ben definito per ogni $[X : Y : Z]$):

$$[U : V : T] = \varphi([X : Y : Z]) = [X : Y : X + 3Y - 3Z]$$

questo manda il punto $Q \mapsto [0 : 1 : 0]$ e la retta $\{X+3Y-3Z = 0\} \mapsto \{T = 0\}$.
Inoltre φ è invertibile con inversa $\varphi^{-1}([U : V : T]) = [U : V : \frac{U-T}{3} + V]$.
Riordinando i termini, possiamo scrivere l'equazione di $\mathcal{C}$ come

$$Z^2(3Y - 2X) + Z(2X^2 - 3Y^2) + XY^2 - X^2Y = 0.$$

Moltiplicando l'equazione per 9 e scrivendo l'equazione di $\mathcal{C}$ nelle nuove coordinate U, V, T l'equazione diventa

$$\begin{gathered}(U+3V-T)^2(3V-2U) + 3(U+3V-T)(2U^2-3V^2) + 9UV^2 - 9U^2V = 0\\ (U+3V-T)(4U^2-3UV+2UT-3VT) + 9UV^2 - 9U^2V = 0\\ T^2(3V-2U) - T(2U^2+9V^2-6UV) + 4U^3 = 0\\ T(9V^2 - 3V(T+2U)) = 4U^3 - 2U^2T - 2UT^2.\end{gathered}$$

In particolare l'ultima equazione può essere riscritta come:

$$\begin{aligned}16T\left(3V - \frac{T+2U}{2}\right)^2 &= 64U^3 - 2\cdot 16U^2T - 8\cdot 4UT^2 + 4T^3 - 4\cdot 4UT^2 + 16U^2T\\ &= (4U)^3 - (4U)^2T - 4\cdot(4U)T^2 + 4T^3\end{aligned}$$

quindi l'ulteriore cambio di coordinate

$$[U : V : T] \mapsto [4U : 12V - 2T - 4U : T] = [X : Y : Z],$$

porta la curva $\mathcal{C}$ nella curva E definita da

$$E : Y^2Z = X^3 - X^2Z - 4XZ^2 + 4Z^3.$$

Inoltre osserviamo che anche quest'ultimo cambio di coordinate è ben definito per ogni $[U : V : T]$ e invertibile, infatti l'inverso di $[X : Y : Z]$ è $[\frac{X}{4} : \frac{Y+X+2Z}{12} : Z]$: la mappa che manda $\mathcal{C} \to E$ è un morfismo di curve su $\mathbb{Q}$ invertibile.
Infine osserviamo che il polinomio $x^3 - x^2 - 4x + 4 = (x-2)(x+2)(x-1)$ non ha radici multiple, quindi la curva E è non singolare: poiché è definita da un polinomio in forma normale di Weierstrass, è una curva ellittica.

Abbiamo costruito un morfismo di curve fra $\mathcal{S} \longrightarrow E$ che induce una funzione bigettiva

$$\mathcal{S}(\mathbb{Q}) \xrightarrow{\simeq} E(\mathbb{Q}).$$

Per dimostrare che la curva $\mathcal{S}$ non ha punti razionali oltre a quelli banali che abbiamo trovato ci basta dimostrare che la curva ellittica E ha esattamente 8 punti razionali.

4.1 $E(\mathbb{Q})$ ha rango 0

La curva ellittica E da studiare è data dalla chiusura proiettiva della curva affine:

$$y^2 = (x-2)(x+2)(x-1).$$

Osserviamo che tutti i punti di 2-torsione di E sono razionali, quindi a meno di comporre con la traslazione $(x, y) \mapsto (x-1, y)$, possiamo equivalentemente indicare con E la curva di equazione affine

$$y^2 = x(x+3)(x-1).$$

Dal Teorema di Mordell-Weil sappiamo che $\Gamma = E(\mathbb{Q})$ è finitamente generato: per quanto illustrato nella sezione 3.5, il rango r di $E(\mathbb{Q})$ rispetta l'equazione

$$2^{r+2} = |\alpha(\overline{\Gamma})| \cdot |\bar{\alpha}(\Gamma)|$$

dove $\overline{\Gamma} = \overline{E}(\mathbb{Q})$, $\overline{E}$, α e $\bar{\alpha}$ sono stati costruiti nella dimostrazione del teorema di Mordell-Weil.

Nota l'equazione di $E : y^2 = x(x^2 + ax + b)$ sappiamo che $\overline{E}$ ha equazione $x(x^2 + \bar{a}x + \bar{b})$ con $\bar{a} = -2a$ e $\bar{b} = b^2 - 4a$, quindi le due curve da considerare sono

$$E : y^2 = x(x^2 + 2x - 3) \quad \text{e} \quad \overline{E} : y^2 = x(x^2 - 4x + 16)$$

- Consideriamo la curva E: sicuramente $\bar{\alpha}(\mathcal{O}) = [1]$, $\bar{\alpha}(T) = [-3] \in \mathrm{Im}(\bar{\alpha})$. Dobbiamo capire per quali $m \pmod{\mathbb{Q}^{*2}}$ l'equazione

  $$n^2 = m(m + 3e^2)(m - e^2)$$

  ha soluzioni con $n, e, m \in \mathbb{Q}$ e $(m, e) = 1$.
  In questo caso $(m, (m - e^2)(m + 3e^2)) = (m, 3e^2) = (m, 3) \in \{\pm 1, \pm 3\}$: ed osserviamo che in effetti i punti $(3, 6)$ e $(-1, 2)$ appartengono a $E(\mathbb{Q})$, quindi $\mathrm{Im}(\bar{\alpha}) = \{[\pm 1], [\pm 3]\}$.

- Consideriamo la curva $\overline{E}$: sicuramente $\alpha(\mathcal{O}) = [1] = [16] = \alpha(T) \in \mathrm{Im}(\bar{\alpha})$. Dobbiamo capire per quali $m \pmod{\mathbb{Q}^{*2}}$ l'equazione

  $$n^2 = m(m^2 - 4me^2 + 16e^4)$$

  ha soluzioni con $n, e, m \in \mathbb{Q}$ e $(m, e) = 1$.
  In questo caso $(m, (m^2 - 4me^2 + 16e^4)) = (m, 16e^4) = (m, 16) = x \mid 16$: in particolare x può assumere i valori $\pm 1, \pm 2$ modulo $\mathbb{Q}^{*2}$. Vediamo che non possono esistere soluzioni se $x = q^2 y$ con $y \in \{-1, \pm 2\}$.

  Supponiamo $m = yq^2 m_1$ con $(m_1, 16) = 1$: necessariamente allora $m_1 \in \mathbb{Q}^{*2}$ e $m = yM^2$. L'equazione allora diventa

  $$n^2 = yM^2 \left(y^2 M^4 - 4M^2 e^2 y + y \frac{16}{y} e^4 \right) \implies y \mid n \implies n = yN.$$

$$N^2 = M^2\left(yM^4 - 4M^2e^2 + \frac{16}{y}e^4\right).$$

Quindi necessariamente $yM^4 - 4M^2e^2 + \frac{16}{y}e^4 \in \mathbb{Q}^{*2}$. Allora

- Se $y < 0$: $yM^4 - 4M^2e^2 + \frac{16}{y}e^4 = -1\left((-y)M^4 + 4M^2e^2 + \frac{16}{-y}e^4\right)$ che è sempre negativo, quindi non può essere un quadrato.
- Se $y = 2$: supponiamo che $2M^4 - 4M^2e^2 + 8e^4 = 2(M^4 - 2M^2e^2 + 4e^4)$ sia un quadrato e guardiamo la valutazione 2-adica: necessariamente $2 \mid (M^4 - 2M^2e^2 + 4e^4)$, cioè $v_2(M) \geq 1$, e quindi poiché $(m, e) = 1$, $v_2(e) = 0$

  $$\begin{aligned} v_2(2(M^4 - 2M^2e^2 + 4e^4)) &= 1 + v_2(M^4 - 2M^2e^2 + 4e^4) \\ &= 1 + \min\{4v_2(M), 1 + 2v_2(M), 2\} = 3. \end{aligned}$$

  Ma quindi $2(M^4 - 2M^2e^2 + 4e^4)$ non può essere un quadrato.

Abbiamo trovato che $\mathrm{Im}(\bar{\alpha}) = \{[1]\}$.

Quindi la formula del rango diventa:

$$2^{r+2} = 4 \cdot 1 \implies r = 0.$$

In particolare abbiamo dimostrato che $E(\mathbb{Q})$ è un gruppo finito.

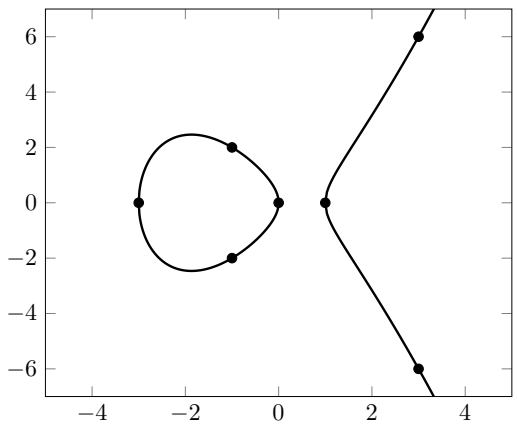
4.2 $E(\mathbb{Q})$ ha cardinalità 8

In questa sezione vogliamo calcolare $|E(\mathbb{Q})| = |E(\mathbb{Q})_{\mathrm{tors}}|$. Possiamo allora determinare i punti di ordine finito di E usando il teorema di Nagell-Lutz 3.6.2: se $P = (x, y) \in E(\mathbb{Q})$ allora $x, y \in \mathbb{Z}$ e:

- $y = 0$: allora x è una radice del polinomio $x(x + 3)(x - 1)$. I punti di questo tipo (che sono esattamente i punti di ordine 2) sono $(0, 0)$, $(1, 0)$ e $(-3, 0)$;
- $y \neq 0$: allora $y \mid \Delta$, dove Δ è il discriminante di $x(x + 3)(x - 1)$: poiché conosciamo le radici di questo polinomio, $\Delta = 3^2 \cdot 1 \cdot (3 - 1)^2 = 36$.
  Per ogni $d \mid 36$, allora $(x, \pm d) \in E(\mathbb{Q})$ se e soltanto se il polinomio

  $$x^3 + 2x^2 - 3x - d^2 \text{ ha radici intere.}$$

  Si può verificare che questo succede solo per $|d| \in \{2, 6\}$: otteniamo altri 4 punti in $E(\mathbb{Q})$, $(-1, \pm 2)$, $(3, \pm 6)$.



Quindi

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0,0), (1,0), (-3,0), (-1, \pm 2), (3, \pm 6)\}$$

poiché $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq E[2] \subset E(\mathbb{Q})$, vale

$$E(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

ed in particolare ha cardinalità 8.

Poiché l'insieme dei punti razionali di E è in bigezione con $\mathcal{S}(\mathbb{Q})$, abbiamo dimostrato che la curva $\mathcal{S}$ ha solo 8 punti razionali, ovvero gli 8 punti che abbiamo individuato a mano e che corrispondono alle soluzioni banali del problema dei 4 quadrati in progressione aritmetica.
Non esistono quindi 4 quadrati consecutivi in una progressione aritmetica non banale.

4.3 Problema dei quattro quadrati su $\mathbb{Q}(\sqrt{m})$

È facile osservare che invece esistono campi di numeri, ed in particolare estensioni quadratiche di $\mathbb{Q}$, in cui il problema dei quattro quadrati ha effettivamente soluzione.
Ad esempio i numeri

$$1, 25, 49, 73$$

sono 4 quadrati in una progressione aritmetica di ragione 24 su $\mathbb{Q}(\sqrt{73})$.

In particolare usando la mappa $\mathcal{S} \to E$ costruita si può dimostrare che esistono infiniti campi quadratici in cui il problema dei 4 quadrati ha soluzione. Infatti per ogni K abbiamo costruito una corrispondenza

$$\{ \text{ soluzioni in } \mathbb{P}^3(K) \text{ al problema dei 4 quadrati } \} \longrightarrow E(K)$$

e questa corrispondenza è tale che $\{$ soluzioni banali $\} \leftrightarrow E(\mathbb{Q})$: quindi ad ogni punto $(x, y) \in E(K) \setminus E(\mathbb{Q})$ corrisponde una soluzione non banale.
Osserviamo inoltre che i punti di $(x, y) \in E(\mathbb{Q})$ sono tutti tali che $|x| \leq 3$.

Costruiamo per induzione una famiglia infinita di estensioni quadratiche di $\mathbb{Q}$ in cui il problema dei quattro quadrati ha soluzione.

- Sia $x_1 = 4$ e $\omega_1 = x_1(x_1 + 3)(x_1 - 1)$: sicuramente $\omega_1 \notin \mathbb{Q}^{*2}$. Allora $K_1 = \mathbb{Q}(\sqrt{\omega_1})$ è un'estensione quadratica di $\mathbb{Q}$ e $(x_1, \sqrt{\omega_1}) \in E(K) \setminus E(\mathbb{Q})$.
- Supponiamo di aver costruito

  $$K_1 = \mathbb{Q}(\sqrt{\omega_1}), \cdots, K_n = \mathbb{Q}(\sqrt{\omega_n})$$

  estensioni quadratiche distinte di $\mathbb{Q}$ in cui il problema dei quattro quadrati ha soluzione. Dimostriamo che troviamo un'altra estensione quadratica in cui esiste una soluzione. Sia $p > 3$ un primo che non divide nessun ω_i, e poniamo $x_{n+1} = p + 1$: allora

  $$\omega_{n+1} = (p+1)(p+4)p \implies v_p(\omega - n + 1) = 1.$$

  Il campo $K_{n+1} = \mathbb{Q}(\sqrt{\omega_{n+1}})$ è un'estensione quadratica di $\mathbb{Q}$ in cui ho una soluzione non banale, ed è distinta da quelle già trovate perché $v_p(\omega_{n+1}\omega_j) = 1 \ \forall j \neq n+1$, quindi $\omega_{n+1}\omega_j \notin \mathbb{Q}^{*2}$.

In effetti in $K_1 = \mathbb{Q}(\sqrt{21})$ esistono *infinite* soluzioni distinte al problema dei quattro quadrati. Infatti il punto $Q = (4, 2\sqrt{21})$ non può essere un punto di torsione: per una generalizzazione del Teorema di Nagell-Lutz, [Sil09, Teorema VIII.7.1], i punti di $E(K_1)$ di ordine finito hanno tutti coordinate intere, mentre $2Q$ ha coordinata x uguale a $361/336$.
Quindi Q ha ordine infinito e di conseguenza $\mathcal{S}(K_1)$ ha infiniti punti: poiché la funzione da $\mathcal{S}$ nell'insieme delle progressioni aritmetiche di 4 quadrati non consecutivi (a meno di proporzionalità) è al massimo 8 a 1, in K_1 esistono infinite progressioni aritmetiche a due a due non proporzionali con 4 quattro quadrati consecutivi.

Bibliografia

[Car95] Henri Cartan. *Elementary theory of analytic functions of one or several complex variables*. Dover Publications, Inc., New York, 1995. Translated from the French, Reprint of the 1973 edition.

[Dic66] Leonard Eugene Dickson. *History of the theory of numbers. Vol. II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[Lan87] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Sam70] Pierre Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[ST15] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

[Zan19] Umberto Zannier. *Funzioni ellittiche e modulari*. Corso tenuto presso la Scuola Normale Superiore. 2019.