Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Specialistica in Matematica

IL GRUPPO DEI PUNTI RAZIONALI SULLE CURVE ELLITTICHE

Tesi in Geometria Superiore

Relatore: Chiar.mo Prof.
LUCA MIGLIORINI

Presentata da:
FRANCESCA CAMAGNI

Seconda Sessione
Anno Accademico 2009/2010

Introduzione

Questa tesi nasce dalla volontà di approfondire un settore particolare della matematica: la Teoria dei Numeri.
Durante la stesura e prima ancora nello studio, mi sono accorta in realtà di quanti siano i settori che si intersecano quando si parla di curve ellittiche. La particolarità di tali curve è questa: oltre alla intuitiva nozione geometrica di curve definite da cubiche nel piano proiettivo, le curve ellittiche possiedono anche una struttura algebrica di gruppo che rende l'addizione un'operazione chiusa su tale oggetto. Questo permette di studiarle davvero da punti di vista molto diversi.
Inoltre è molto interessante cercare anche soluzioni per tali curve ristrette ai numeri interi o razionali, scopo appunto della teoria dei numeri e della geometria diofantea. A questo proposito esistono risultati davvero notevoli per le curve ellittiche: le soluzioni a coordinate intere su un campo di numeri K sono finite (Teorema di Siegel, 1920); le soluzioni a coordinate in un campo finito sono finite e sono all'incirca tante quante il numero degli elementi del campo (Teorema di Hasse, 1930); le soluzioni a coordinate razionali costituiscono un gruppo finitamente generato (Teorema di Mordell-Weil, 1923). Ho deciso di approfondire l'ultimo di questi teoremi e di seguirne i passi della dimostrazione.
La tesi propone un primo capitolo con nozioni generali sulle varietà e sulle curve algebriche, sulle mappe fra di esse e su alcune proprietà geometriche importanti per caratterizzare poi le curve ellittiche.
Il secondo capitolo propone un'introduzione allo studio geometrico e algebrico di tali curve, approfondendo gli aspetti che le caratterizzano.
Il terzo e il quarto capitolo affrontano lo studio dei punti a coordinate razionali, per curve definite prima su campi locali e poi anche su campi globali: l'insieme di tali punti è un gruppo. Il risultato fondamentale, contenuto nel Teorema di Mordell-Weil, è che tale gruppo è finitamente generato. Tutto il quarto capitolo propone i risultati necessari per la dimostrazione di tale affermazione, che procede per passi lungo tutto il capitolo.

Riferimenti bibliografici
Per il Capitolo 1: [16], [7], [14], [6], [12], [1], [5], [4].
Per i Capitoli 2, 3, 4: [16], [17], [2], [8], [9], [11], [18], [15], [13], [3], [10].

Indice

Capitolo 1

Curve algebriche

Notazione. Siano: K un campo perfetto, i.e. ogni estensione algebrica di K è separabile;
$\bar{K}$ una chiusura algebrica fissata di K;
$G_{\bar{K}/K} = \{\sigma : \bar{K} \to \bar{K} \text{ automorfismo} : \sigma(x) = x \ \ \forall x \in K\}$ il gruppo di Galois di $\bar{K}/K$;
$A = \bar{K}[X_1, \dots, X_n]$ l'anello dei polinomi sul campo $\bar{K}$ in n variabili;
$B = \bar{K}[X_0, \dots, X_n]$ l'anello dei polinomi sul campo $\bar{K}$ in $n+1$ variabili;
A_K e B_K i corrispondenti anelli di polinomi sul campo K.

1.1 Varietà affini

Consideriamo lo *spazio affine* $\mathbb{A}^n = \{(x_1, \dots, x_n) = P : x_i \in \bar{K}\} = \mathbb{A}^n(\bar{K})$. Diciamo che P è un punto di $\mathbb{A}^n$ con coordinate x_i. Chiamiamo $\mathbb{A}^n(K)$ l'*insieme dei punti K-razionali di* $\mathbb{A}^n$ ovvero l'insieme dei punti $P \in \mathbb{A}^n$ tali che $x_i \in K$.
Notiamo che esiste un'azione del gruppo di Galois $G_{\bar{K}/K}$ su $\mathbb{A}^n$ tale che $P^\sigma = (x_1^\sigma, \dots, x_n^\sigma)$ per $\sigma \in G_{\bar{K}/K}$ e $P \in \mathbb{A}^n$. Possiamo quindi caratterizzare $\mathbb{A}^n(K)$ nel modo seguente: $\mathbb{A}^n(K) = \{P \in \mathbb{A}^n : P^\sigma = P \ \ \forall \sigma \in G_{\bar{K}/K}\}$.
Consideriamo ora l'anello A e guardiamo i suoi elementi f come funzioni dallo spazio affine in $\bar{K}$ definendo $f(P) = f(x_1, \dots, x_n)$ per $P \in \mathbb{A}^n$. Ha senso quindi considerare l'insieme degli zeri di f: $Z(f) = \{P \in \mathbb{A}^n : f(P) = 0\}$. Più in generale guardiamo l'*insieme degli zeri su* T con T sottoinsieme di A ovvero l'insieme degli zeri comuni a tutti gli elementi f di T: $Z(T) = \{P \in \mathbb{A}^n : f(P) = 0 \ \ \forall f \in T\}$.

Definizione 1.1.1. Un sottoinsieme V di $\mathbb{A}^n$ è un *insieme algebrico* se esiste un sottoinsieme $T \subset A$ tale che $V = Z(T)$. Se $\mathfrak{a}$ è l'ideale di A generato da T, allora $Z(T) = Z(\mathfrak{a})$. Si dice *ideale* di V in A l'insieme $I(V) = \{f \in A : f(P) = 0 \ \ \forall P \in V\}$.

Osservazione 1.1.2. Possiamo definire la *topologia di Zariski* su $\mathbb{A}^n$ prendendo come aperti i complementari degli insiemi algebrici. In particolare: l'unione di due insiemi algebrici, l'intersezione di una famiglia di insiemi algebrici e i due insiemi banali sono ancora insiemi algebrici.

Osservazione 1.1.3. L'ideale $I(V)$ coincide con il proprio radicale definito come $\sqrt{I(V)} = \{f \in A : f^r \in I(V) \text{ per qualche } r > 0\}$. Infatti $f^r \in I(V)$ significa $f^r(P) = 0 \ \forall P \in V$ quindi $f(P) = 0$, i.e. $f \in I(V)$.

Definizione 1.1.4. Un insieme algebrico V è *definito su* K se il suo ideale $I(V)$ può essere generato da polinomi in A_K. Lo denotiamo con V/K. Se V è definito su K, allora l'*insieme dei punti K-razionali di* V è l'insieme $V(K) = V \cap \mathbb{A}^n(K)$.

Esempio 1.1.5. L'insieme algebrico $V : X^n + Y^n = 1$ è definito su $\mathbb{Q}$. Dall'Ultimo Teorema di Fermat sappiamo che per $n \geq 3$

$$V(\mathbb{Q}) = \begin{cases} \{(1,0),(0,1)\} & \text{se } n \text{ è dispari} \\ \{(\pm 1,0),(0,\pm 1)\} & \text{se } n \text{ è pari.} \end{cases}$$

Osservazione 1.1.6. Se V è un insieme algebrico, l'ideale $I(V/K)$ è dato da $I(V/K) = \{f \in A_K : f(P) = 0 \ \forall P \in V\} = I(V) \cap A_K$. Quindi V è definito su K se e solo se $I(V) = I(V/K)A$.

Sia V definito su K. Notiamo che esiste un'azione del gruppo di Galois $G_{\bar{K}/K}$ su V indotta dall'azione su $\mathbb{A}^n$ tale che $f(P^\sigma) = (f(P))^\sigma$ per $\sigma \in G_{\bar{K}/K}$, $P \in \mathbb{A}^n$ e $f \in A_K$. Possiamo quindi caratterizzare $V(K)$ nel modo seguente: $V(K) = \{P \in V : P^\sigma = P \ \ \forall \sigma \in G_{\bar{K}/K}\}$.

Ritorniamo alla Definizione 1.1.1 e osserviamo che si hanno una mappa $Z : \mathfrak{a} \to Z(\mathfrak{a})$ che porta ideali di A in insiemi algebrici, e una mappa $I : V \to I(V)$ che porta insiemi algebrici in ideali. Valgono i seguenti fatti (che valgono più in generale per sottoinsiemi di A al posto di ideali, e per sottoinsiemi di $\mathbb{A}^n$ al posto di insiemi algebrici).

Proposizione 1.1.7.

1. $\mathfrak{a} \subseteq I(Z(\mathfrak{a}))$
2. $V \subseteq Z(I(V))$
3. $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \Rightarrow Z(\mathfrak{a}_1) \supseteq Z(\mathfrak{a}_2)$
4. $V_1 \subseteq V_2 \Rightarrow I(V_1) \supseteq I(V_2)$
5. $Z(\mathfrak{a}) = Z(I(Z(\mathfrak{a})))$
6. $I(V) = I(Z(I(V)))$
7. $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ *radicale di* $\mathfrak{a}$
8. $Z(I(V)) = \bar{V}$ *chiusura di* V.

Dimostrazione. **1.** $P \in Z(\mathfrak{a}) \Rightarrow f(P) = 0 \ \forall f \in \mathfrak{a}$, quindi $f \in \mathfrak{a} \Rightarrow f \in I(Z(\mathfrak{a}))$.
2. $f \in I(V) \Rightarrow f(P) = 0 \ \forall P \in V$, quindi $P \in V \Rightarrow P \in Z(I(V))$.
3. $f(P) = 0 \ \forall f \in \mathfrak{a}_2 \Rightarrow f(P) = 0 \ \forall f \in \mathfrak{a}_1$, quindi $P \in Z(\mathfrak{a}_2) \Rightarrow P \in Z(\mathfrak{a}_1)$.
4. $f(P) = 0 \ \forall P \in V_2 \Rightarrow f(P) = 0 \ \forall P \in V_1$, quindi $f \in I(V_2) \Rightarrow f \in I(V_1)$.
5. Si ottiene dalle proprietà 1.,2.,3. Infatti sostituendo $Z(\mathfrak{a})$ al posto di V in 2. si ottiene $Z(\mathfrak{a}) \subseteq Z(I(Z(\mathfrak{a})))$, mentre considerando insieme 1. e 3. si ottiene $Z(\mathfrak{a}) \supseteq Z(I(Z(\mathfrak{a})))$.
6. Analogamente dalle proprietà 1.,2.,4. sostituendo $I(V)$ al posto di $\mathfrak{a}$ in 1. e considerando insieme 2. e 4.
7. Si ottiene dal Nullstellensatz di Hilbert.

Teorema (Hilbert. Nullstellensatz. Versione forte)**.** *Sia $\mathfrak{a}$ un ideale in A e sia $f \in A$ un polinomio che si annulla in tutti i punti di $Z(\mathfrak{a})$. Allora $f^r \in \mathfrak{a}$ per qualche intero $r > 0$, i.e. $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*

Per una dimostrazione si veda [6] 1 §7, [5] 15.3 (Theorem 32), [4] 9.10 (Theorem 10.4).
Abbiamo precedentemente notato (vedi Osservazione 1.1.3) che l'ideale di un insieme algebrico coincide con il proprio radicale. Su un campo algebricamente chiuso, vale quindi qualcosa di più: ogni ideale uguale al proprio radicale è di questa forma.
8. Per 2. e poiché $Z(I(V))$ è un chiuso, vale $\bar{V} \subseteq Z(I(V))$.
Per vedere l'altra inclusione, consideriamo un chiuso W tale che $W \supseteq V$. Si ha $W = Z(\mathfrak{a})$ per qualche ideale $\mathfrak{a}$. Quindi $V \subseteq Z(\mathfrak{a})$ e per 4. si ha $I(V) \supseteq I(Z(\mathfrak{a}))$. Per 1. otteniamo $\mathfrak{a} \subseteq I(V)$ e per 3. si ha $W = Z(\mathfrak{a}) \supseteq Z(I(V))$. Quindi $Z(I(V)) = \bar{V}$.

□

Ricordiamo che un sottoinsieme V di $\mathbb{A}^n$ è detto *riducibile* se $V = \emptyset$ oppure $V = V_1 \cup V_2$ con V_1, V_2 sottoinsiemi propri chiusi di V. In caso contrario V è detto *irriducibile*.

Definizione 1.1.8. Un sottoinsieme V di $\mathbb{A}^n$ chiuso e irriducibile è una *varietà algebrica (affine)* o *varietà (affine)*. In particolare, gli insiemi algebrici irriducibili sono varietà affini.

Osservazione 1.1.9. Ogni sottoinsieme aperto non vuoto di uno spazio irriducibile è irriducibile e denso. Quindi un sottoinsieme aperto di una varietà è irriducibile e denso.

Proposizione 1.1.10. *Un insieme algebrico V è una varietà se e solo se $I(V)$ è un ideale primo in A.*

Dimostrazione. $\Rightarrow$**)** Siano f, g polinomi tali che $fg \in I(V)$, allora $V \subseteq Z(fg) = Z(f) \cup Z(g)$ ovvero $V = (V \cap Z(f)) \cup (V \cap Z(g)) = V_1 \cup V_2$, entrambi chiusi. Poiché V è irriducibile per ipotesi, V_1 e V_2 non possono essere propri. Quindi $V_1 = V$ oppure $V_2 = V$ che implicano rispettivamente $V \subseteq Z(f)$ oppure $V \subseteq Z(g)$. Quindi $f \in I(V)$ oppure $g \in I(V)$, i.e. $I(V)$ è primo.
$\Leftarrow$**)** Supponiamo $V = V_1 \cup V_2$, allora $I(V) = I(V_1) \cap I(V_2) \subseteq I(V_i)$ con $i = 1, 2$ quindi $I(V) = I(V_1)$ oppure $I(V) = I(V_2)$. Infatti se $I(V) \subsetneq I(V_i)$ esistono $f_1 \in I(V_1) \setminus$

$I(V)$ e $f_2 \in I(V_2) \setminus I(V)$ tali che $f_1 f_2 \in I(V_1 \cup V_2) = I(V)$, quindi $I(V)$ non è primo contrariamente all'ipotesi. Allora $V = V_1$ oppure $V = V_2$, i.e. V è irriducibile.

□

Esempio 1.1.11. Sia f un polinomio irriducibile in $\bar{K}[X, Y]$. f genera un ideale primo, quindi l'insieme $Z(f)$ degli zeri di (f) è irriducibile. Chiamiamo $Z(f) = C$ *curva affine* definita dall'equazione $f(X, Y) = 0$. Se f ha grado d, diciamo che C ha *grado d*.

Esempio 1.1.12. Un ideale massimale $\mathfrak{m}$ di A corrisponde a un insieme algebrico irriducibile minimo, ovvero un punto $P = (x_1, \ldots, x_n) \in \mathbb{A}^n$. Quindi ogni ideale massimale è del tipo $\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n)$ per qualche $x_i \in \bar{K}$. Questo risultato corrisponde alla versione debole del Nullstellensatz di Hilbert.

Teorema (Hilbert. Nullstellensatz. Versione debole)**.** *Ogni ideale massimale* $\mathfrak{m}$ *in* A *è del tipo*

$$\mathfrak{m} = (x_1 - \alpha_1, \ldots, x_n - \alpha_n) \qquad \text{con } \alpha_i \in \bar{K}.$$

Per una dimostrazione si veda [6] 1 §7, [5] 15.3 (Theorem 31), [4] 9.10 (Theorem 10.3).

Definizione 1.1.13. Sia V una varietà affine. L'*anello delle coordinate affini di* V è definito da $\bar{K}[V] = A/I(V)$. In particolare è un dominio di integrità (poichè $I(V)$ è primo). Il suo campo delle frazioni $\bar{K}(V)$ è detto *campo delle funzioni di* V.
Analoghe definizioni per V/K (i.e. V definita su K): $K[V] = A_K/I(V/K)$ è l'*anello delle coordinate affini di* V/K e $K(V)$ è il *campo delle funzioni di* V/K.

Notiamo che un elemento $f \in \bar{K}[V]$ è ben definito a meno di somma con un polinomio che si annulla su V, quindi questo induce una funzione ben definita $f : V \to \bar{K}$.
Sia V definita su K. Se $f \in A$, esiste un'azione del gruppo di Galois $G_{\bar{K}/K}$ su f o meglio sui coefficienti di f, che denotiamo con $f \to f^\sigma$: allora si ha $(f(P))^\sigma = f^\sigma(P^\sigma)$ $\forall P \in V$. Notiamo che $G_{\bar{K}/K}$ manda $I(V)$ in se stesso. Esiste allora un'azione di $G_{\bar{K}/K}$ su $\bar{K}[V]$ e $\bar{K}(V)$ che fissa rispettivamente i sottoinsiemi $K[V]$ e $K(V)$. Possiamo quindi caratterizzare $K[V]$ nel modo seguente: $K[V] = \{f \in \bar{K}[V] : f^\sigma = f \ \forall \sigma \in G_{\bar{K}/K}\}$. Analogamente per $K(V)$.

Definizione 1.1.14. Sia V una varietà. La *dimensione di* V, che denotiamo con $\dim(V)$, è il grado di trascendenza di $\bar{K}(V)$ su $\bar{K}$.

Esempio 1.1.15. $\dim(\mathbb{A}^n) = n$, infatti $\bar{K}(\mathbb{A}^n) = \bar{K}(X_1, \ldots, X_n)$.
Se $V \subset \mathbb{A}^n$ è data da una sola equazione non costante del tipo $f(X_1, \ldots, X_n) = 0$, allora $\dim(V) = n - 1$.

Definizione 1.1.16. Siano V una varietà, $P \in V$, $f_1, \ldots, f_m \in A$ un insieme di generatori per $I(V)$. V è *non singolare* o *liscia in* P se la matrice $S = \|\partial f_i/\partial X_j(P)\|$ ha rango $n - \dim(V)$, con $1 \le i \le m$ e $1 \le j \le n$.
V è *non singolare* o *liscia* se è non singolare in ogni punto.

Esempio 1.1.17. Sia V data dall'equazione $f(X_1, \ldots, X_n) = 0$. Dall'Esempio 1.1.15 sappiamo che $\dim(V) = n - 1$, quindi $P \in V$ è un punto singolare se e solo se $\partial f/\partial X_1(P) = \ldots = \partial f/\partial X_n(P) = 0$, i.e. il rango della matrice S è minore di $n - \dim(V) = 1$.

Sia $P \in V$ e definiamo in $\bar{K}[V]$ l'ideale $M_P = \{f \in \bar{K}[V] : f(P) = 0\}$. M_P è un ideale massimale poichè esiste un isomorfismo di campi $\bar{K}[V]/M_P \to \bar{K}$ dato da $f \to f(P)$. Il quoziente M_P/M_P^2 è un $\bar{K}$-spazio vettoriale a dimensione finita.
Vale un risultato molto importante: $P \in V$ è non singolare se e solo se $\dim_{\bar{K}}(M_P/M_P^2) = \dim(V)$. Si veda [7] I §5 (Theorem 5.1).

Definizione 1.1.18. Definiamo l'*anello locale di V in P* come la localizzazione di $\bar{K}[V]$ in M_P: $\bar{K}[V]_P = \{F \in \bar{K}(V) : F = f/g$ per qualche $f, g \in \bar{K}[V]$ con $g(P) \neq 0\}$.
Se $F \in \bar{K}[V]_P$, allora $F(P) = f(P)/g(P)$ è ben definita: si dice che F è *regolare* o *definita in P*. Ha quindi senso valutare F in P. $\bar{K}[V]_P$ è dunque l'insieme delle funzioni razionali su V definite in P.

1.2 Varietà proiettive

Consideriamo lo *spazio proiettivo* $\mathbb{P}^n = \{[x_0, \ldots, x_n] = P : (x_0, \ldots, x_n) \in \mathbb{A}^{n+1}\} = \mathbb{P}^n(\bar{K})$. P è un punto di $\mathbb{P}^n$ con coordinate omogenee x_i, ed è una classe di equivalenza data dalla relazione: $(y_0, \ldots, y_n) \sim (x_0, \ldots, x_n)$ se esiste $\lambda \in \bar{K}^*$ tale che $y_i = \lambda x_i \ \forall i$. L'*insieme dei punti K-razionali di $\mathbb{P}^n$*, denotato con $\mathbb{P}^n(K)$, è dato dai punti $P \in \mathbb{P}^n$ tali che $x_i \in K$.

Definizione 1.2.1. Sia $P \in \mathbb{P}^n$. Il *campo di definizione minimo di P su K* è il campo $K(P) = K(x_0/x_i, \ldots, x_n/x_i)$ con $x_i \neq 0 \ \forall i$.

Osservazione 1.2.2. Sia $P \in \mathbb{P}^n(K)$. Questo non implica in generale che ogni $x_i \in K$. Prendendo però i tale che $x_i \neq 0$, si ha $x_j/x_i \in K \ \forall j$.

Notiamo che esiste un'azione del gruppo di Galois $G_{\bar{K}/K}$ su $\mathbb{P}^n$ tale che $P^\sigma = [x_0^\sigma, \ldots, x_n^\sigma]$. Osserviamo che l'azione è ben definita in quanto indipendente dalla scelta delle coordinate omogenee: infatti $\lambda^\sigma = \lambda' \in \bar{K}^*$. Possiamo quindi caratterizzare $\mathbb{P}^n(K)$ nel modo seguente: $\mathbb{P}^n(K) = \{P \in \mathbb{P}^n : P^\sigma = P \ \forall \sigma \in G_{\bar{K}/K}\}$. In questo modo il campo di definizione minimo $K(P)$ è il campo fisso dell'azione di Galois $P^\sigma = P$.
Consideriamo ora l'anello B e prendiamo i polinomi f *omogenei di grado d* ovvero tali che $f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n) \ \forall \lambda \in \bar{K}$. Un ideale in B è detto *omogeneo* se è generato da polinomi omogenei. Analogamente al caso affine si hanno le seguenti definizioni.

Definizione 1.2.3. Un sottoinsieme V di $\mathbb{P}^n$ è un *insieme algebrico* se esiste un sottoinsieme $T \subset B$ di elementi omogenei tale che $V = Z(T)$. Se $\mathfrak{a}$ è l'ideale omogeneo di B

generato da T, allora $Z(T) = Z(\mathfrak{a})$.
Si dice *ideale* di V in B l'insieme $I(V) = \{f \in B \text{ omogeneo} : f(P) = 0 \ \forall P \in V\}$.
V è *definito su* K se il suo ideale $I(V)$ può essere generato da polinomi omogenei in B_K. Lo denotiamo con V/K. Se V è definito su K, allora l'*insieme dei punti K-razionali di* V è l'insieme $V(K) = V \cap \mathbb{P}^n(K)$. Possiamo inoltre caratterizzare $V(K)$ tramite l'azione di Galois nel modo seguente: $V(K) = \{P \in V : P^\sigma = P \ \forall \sigma \in G_{\bar{K}/K}\}$.

Esempio 1.2.4. Un punto in $\mathbb{P}^n(\mathbb{Q})$ è del tipo $[x_0, \ldots, x_n]$ con $x_i \in \mathbb{Q}$. Moltiplicando per un certo $\lambda \in \mathbb{Q}^*$ è possibile eliminare denominatori e fattori comuni dagli x_i. Questo implica che un punto in $\mathbb{P}^n(\mathbb{Q})$ può essere scritto nel modo seguente: $P = [x_0, \ldots, x_n]$ con $x_0, \ldots, x_n \in \mathbb{Z}$ e $MCD(|x|_0, \ldots, |x|_n) = 1$.

Definizione 1.2.5. Un insieme algebrico irriducibile è una *varietà algebrica (proiettiva)* o *varietà (proiettiva)*. Equivalentemente, un insieme algebrico V è una varietà se e solo se $I(V)$ è un ideale primo in B.

Per ottenere le ultime definizioni sulle varietà proiettive, mostriamo come è possibile ricoprire una varietà proiettiva con copie di una varietà affine.
Osserviamo che esiste una naturale inclusione $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$ tale che

$$\varphi_i(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = [x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n].$$

Siano H_i l'iperpiano in $\mathbb{P}^n$ dato da $X_i = 0$ e U_i il suo complementare in $\mathbb{P}^n$, quindi $H_i = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : x_i = 0\}$ e $U_i = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : x_i \neq 0\} = \mathbb{P}^n \setminus H_i$. Definiamo la mappa $\varphi_i^{-1} : U_i \to \mathbb{A}^n$ tale che

$$\varphi_i^{-1}([x_0, \ldots, x_n]) = \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

Infatti l'inversa di questa mappa agisce esattamente come φ_i e possiamo quindi identificare $\mathbb{A}^n$ con U_i.

Proposizione 1.2.6. *La mappa φ_i^{-1} è un omeomorfismo di U_i con la topologia indotta in $\mathbb{A}^n$ con la topologia di Zariski.*

Osservazione 1.2.7. Ricordiamo che, dato un polinomio $f \in A$, è possibile ottenere il polinomio omogeneo $f^* \in B$ tramite il processo di omogeneizzazione rispetto all'i-esima variabile:

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

dove $d = \deg f$ è il più piccolo intero per cui f^* è un polinomio.
Il processo inverso, detto deomogeneizzazione rispetto all'i-esima variabile, trasforma un polinomio omogeneo $g \in B$ nel polinomio $\widetilde{g} \in A$:

$$\widetilde{g}(X_1, \ldots, X_n) = g(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n).$$

Dimostrazione di 1.2.6. Sappiamo già che φ_i^{-1} è iniettiva, quindi basta vedere che chiusi di U_i sono mandati in chiusi di $\mathbb{A}^n$ da φ_i^{-1}. Per semplicità, fissiamo un certo i per esempio $i = 0$ e scriviamo U al posto di U_0 e $\phi^{-1} : U \to \mathbb{A}^n$ al posto di φ_0^{-1}. Siano $\alpha : A \to B$ e $\beta : B \to A$ rispettivamente l'omogeneizzazione e la deomogeneizzazione rispetto a X_0: $\alpha(f) = f^* = X_0^d f(X_1/X_0, \ldots, X_n/X_0)$ e $\beta(g) = \widetilde{g} = g(1, X_1, \ldots, X_n)$.
Sia ora $V \subseteq U$ un sottoinsieme chiuso e sia $\bar{V}$ la sua chiusura in $\mathbb{P}^n$. $\bar{V}$ è un insieme algebrico, quindi $\bar{V} = Z(T)$ per qualche $T \subseteq B$ sottoinsieme di polinomi omogenei con $\widetilde{T} = \beta(T)$. Allora si ha $\phi^{-1}(V) = Z(\widetilde{T})$, i.e. ϕ^{-1} è chiusa.
Sia ora $W \subseteq \mathbb{A}^n$ chiuso. Allora $W = Z(T)$ per qualche $T \in A$ con $T^* = \alpha(T)$. Allora $\phi(W) = Z(T^*) \cap U$, i.e. ϕ è chiusa.

□

Sia ora V un insieme algebrico proiettivo con ideale $I(V)$. Come gli insiemi $U_0, \ldots, U_n$ ricoprono $\mathbb{P}^n$, così V è ricoperto dai sottoinsiemi $V \cap U_0, \ldots, V \cap U_n$ e ciascuno di questi è anche un insieme algebrico affine tramite una certa φ_i^{-1}. Quindi $V \cap \mathbb{A}^n$, pensato come $\varphi_i^{-1}(V \cap U_i)$ per qualche i, è un insieme algebrico affine con ideale $I(V \cap \mathbb{A}^n)$ dato da $I(V \cap \mathbb{A}^n) = \{\widetilde{g} : g \in I(V)\}$.

Definizione 1.2.8. Sia V un insieme algebrico affine con ideale $I(V)$. Guardiamo V come un sottoinsieme di $\mathbb{P}^n$ tramite la mappa $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$. La *chiusura proiettiva di* V, che denotiamo con $\bar{V}$, è l'insieme algebrico proiettivo il cui ideale omogeneo $I(\bar{V})$ è generato da $\{f^* : f \in I(V)\}$.

Possiamo ampliare alle varietà il discorso appena fatto per gli insiemi algebrici (il seguente Corollario si ottiene dalla Proposizione 1.2.6).

Corollario 1.2.9. *Sia V una varietà proiettiva, allora V è ricoperta dagli insiemi aperti $V \cap U_0, \ldots, V \cap U_n$ omeomorfi a varietà affini tramite le rispettive mappe φ_i^{-1}.*

Proposizione 1.2.10.

1. *Sia V una varietà affine. Allora $\bar{V}$ è una varietà proiettiva con $V = \bar{V} \cap \mathbb{A}^n$.*
2. *Sia V una varietà proiettiva. Allora $V \cap \mathbb{A}^n$ è una varietà affine con $V = \overline{V \cap \mathbb{A}^n}$ se $V \cap \mathbb{A}^n \neq \emptyset$.*
3. *Se V è una varietà affine definita su K, allora $\bar{V}$ è definita su K.*
4. *Se V è una varietà proiettiva definita su K, allora $V \cap \mathbb{A}^n$ è definita su K.*

Dimostrazione. **1.** e **2.** Dal Corollario 1.2.9.
3. e **4.** Dalle definizioni.

□

Osservazione 1.2.11. Grazie alla Proposizione 1.2.10, ogni varietà affine può essere identificata con un'unica varietà proiettiva. Siano V la varietà affine e $\bar{V}$ la corrispondente varietà proiettiva, allora i punti di $\bar{V} \setminus V$ sono detti *punti all'infinito di* V.

Vediamo ora quindi le ultime proprietà di una varietà proiettiva V in termini della corrispondente varietà affine $V \cap \mathbb{A}^n$.

Definizione 1.2.12. Sia V una varietà proiettiva e sia $V \in P$. Scegliamo $\mathbb{A}^n \subset \mathbb{P}^n$ tale che $V \cap \mathbb{A}^n \neq \emptyset$ e $P \in \mathbb{A}^n$. La *dimensione di* V è la dimensione di $V \cap \mathbb{A}^n$. V è detta *non singolare* o *liscia in* P se lo è $V \cap \mathbb{A}^n$. E, analogamente, per il *campo delle funzioni di* V e *di* V/K e per l'*anello locale di* V *in* P si considera la varietà affine $V \cap \mathbb{A}^n$.

Osservazione 1.2.13. Notiamo che, per scelte differenti di $\mathbb{A}^n$, i diversi campi delle funzioni sono canonicamente isomorfi. Quindi possiamo identificarli.
Possiamo anche descrivere il campo delle funzioni di V direttamente in termini proiettivi come il campo delle funzioni razionali $F(X) = f(X)/g(X)$ tali che: f, g sono polinomi omogenei dello stesso grado; $g \notin I(V)$; $f_1/g_1 \sim f_2/g_2$ se $f_1 g_2 - f_2 g_1 \in I(V)$.

1.3 Mappe tra varietà

Definizione 1.3.1. Siano V_1 e V_2 varietà proiettive in $\mathbb{P}^n$. Una *mappa razionale da* V_1 *a* V_2 è una mappa del tipo $\varphi : V_1 \to V_2$ con $\varphi = [f_0, \ldots, f_n]$ e $f_i \in \bar{K}(V_1)$ tale che, per ogni $P \in V_1$ in cui le f_i sono definite, si ha $\varphi(P) = [f_0(P), \ldots, f_n(P)] \in V_2$.

Osservazione 1.3.2. Siano V_1 e V_2 definite su K. Diciamo che φ è *definita su* K se esiste $\lambda \in \bar{K}^*$ tale che $\lambda f_0, \ldots, \lambda f_n \in K(V_1)$. $[f_0, \ldots, f_n]$ e $[\lambda f_0, \ldots, \lambda f_n]$ danno la stessa mappa sui punti.
Notiamo che il gruppo di Galois $G_{\bar{K}/K}$ agisce su φ: $\varphi^\sigma(P) = [f_0^\sigma(P), \ldots, f_n^\sigma(P)]$. Si ha quindi $(\varphi(P))^\sigma = \varphi^\sigma(P^\sigma)$ con $P \in V_1$. Possiamo dire che φ è definita su K se e solo se $\varphi = \varphi^\sigma \ \forall \sigma \in G_{\bar{K}/K}$.

Osservazione 1.3.3. Una mappa razionale non è necessariamente sempre ben definita in ogni punto di V_1. É però possibile valutare $\varphi(P)$ anche nei punti $P \in V_1$ in cui qualche f_i non è regolare: si sostituisce gf_i a f_i per un'opportuna $g \in \bar{K}(V_1)$.

Definizione 1.3.4. Una mappa razionale $\varphi : V_1 \to V_2$ è *regolare* o *definita in* P se esiste una funzione $g \in \bar{K}(V_1)$ tale che:

- ogni gf_i è regolare in P, i.e. $gf_i \in \bar{K}[V_1]_P$
- $(gf_i)(P) \neq 0$ per qualche i.

In questo caso poniamo $\varphi(P) = [(gf_0)(P), \ldots, (gf_n)(P)]$.

Definizione 1.3.5. Un *morfismo* di varietà $\varphi : V_1 \to V_2$ è una mappa razionale regolare in ogni punto di V_1.

Ora estendiamo la nozione di morfismo a varietà qualsiasi.

Definizione 1.3.6. Sia V una varietà affine e siano $P \in V$ e $U \subset V$ aperto (i.e. U è una *varietà quasi affine*). Una funzione $f : U \to \bar{K}$ è *regolare in* P se esiste un intorno $W \subseteq U$ tale che $P \in W$ ed esistono $g, h \in A$ tali che $h \neq 0$ e $f = g/h$ in W.
Analogamente, sia V una varietà proiettiva e siano $P \in V$ e $U \subset V$ aperto (i.e. U è una *varietà quasi proiettiva*). Una funzione $f : U \to \bar{K}$ è *regolare in* P se esiste un intorno $W \subseteq U$ tale che $P \in W$ ed esistono $g, h \in B$ omogenei tali che $h \neq 0$ e $f = g/h$ in W.
Diciamo che f è *regolare* se è regolare in ogni punto di U.

Lemma 1.3.7. *Una funzione regolare è continua.*

Dimostrazione. Per ottenere la continuità basta vedere che le retroimmagini di chiusi sono chiusi.
Possiamo identificare $\bar{K}$ con $\mathbb{A}^1(\bar{K})$ nella topologia di Zariski. Un chiuso in $\mathbb{A}^1(\bar{K})$ è un insieme finito di punti, quindi basta vedere che $f^{-1}(x) = \{P \in U : f(P) = x\}$ è chiuso per ogni $x \in \bar{K}$. Localmente un sottoinsieme T di uno spazio topologico U è chiuso se e solo se U può essere ricoperto da aperti W_i tali che $T \cap W_i$ è chiuso in W_i per ogni i. Sia quindi W un aperto in cui f può essere scritta come g/h con $g, h \in A$ e $h \neq 0$ in W. Allora $f^{-1}(x) \cap W = \{P \in W : g(P)/h(P) = x\} = \{P \in W : (g - xh)(P) = 0\}$. Quindi $f^{-1}(x) \cap W = Z(g - xh) \cap W$ che è chiuso. Quindi $f^{-1}(x)$ è chiuso in U.

□

Definizione 1.3.8. Siano V_1 e V_2 varietà qualsiasi. Un *morfismo* $\varphi : V_1 \to V_2$ è una mappa continua tale che, per ogni aperto $U \subset V_2$ e per ogni $f : U \to \bar{K}$ regolare, la funzione $f \circ \varphi : \varphi^{-1}(U) \to \bar{K}$ è regolare.
Un *isomorfismo* $\varphi : V_1 \to V_2$ è un morfismo che ammette un morfismo inverso $\psi : V_2 \to V_1$ tale che $\psi \circ \varphi = id_{V_1}$ e $\varphi \circ \psi = id_{V_2}$.

Lemma 1.3.9. *Siano V_1 e V_2 varietà e $\varphi, \psi : V_1 \to V_2$ morfismi. Supponiamo che esista $U \subseteq V_1$ aperto non vuoto tale che $\varphi|_U = \psi|_U$. Allora $\varphi = \psi$.*

Dimostrazione. Supponiamo $V_2 \subseteq \mathbb{P}^n$ per qualche n e tramite il morfismo di inclusione $V_2 \to \mathbb{P}^n$ ci riduciamo al caso $V_2 = \mathbb{P}^n$.
Consideriamo il prodotto $\mathbb{P}^n \times \mathbb{P}^n$, che ha ancora una struttura di varietà proiettiva poiché esiste una naturale inclusione in $\mathbb{P}^{n^2+2n}$, e osserviamo che φ e ψ definiscono un morfismo $\varphi \times \psi : V_1 \to \mathbb{P}^n \times \mathbb{P}^n$. Sia ora $\Gamma = \{P \times P : P \in \mathbb{P}^n\}$ il sottoinsieme diagonale di $\mathbb{P}^n \times \mathbb{P}^n$, definito dalle equazioni $\{x_i y_j = x_j y_i \ \forall i, j\}$. Quindi Γ è chiuso. Per ipotesi abbiamo che $(\varphi \times \psi)(U) \subseteq \Gamma$. Per l'Osservazione 1.1.9 U è denso in V_1 e, poiché Γ è chiuso, si ha $(\varphi \times \psi)(V_1) \subseteq \Gamma$. Quindi $\varphi = \psi$.

□

Definizione 1.3.10. Una *mappa razionale* $\varphi : V_1 \to V_2$ è una classe di equivalenza di coppie $\{U, \varphi_U\}$ dove U è un sottoinsieme aperto non vuoto di V_1 e $\varphi_U : U \to V_2$ è un morfismo. La relazione di equivalenza è data da: $\{U, \varphi_U\} \sim \{W, \varphi_W\}$ se $\varphi_U = \varphi_W$ in $U \cap W$. Una mappa razionale è quindi un morfismo definito solo su qualche aperto.
φ è detta *dominante* se per qualche coppia $\{U, \varphi_U\}$ si ha che $\varphi_U(U)$ è densa in V_2.
Una *mappa birazionale* $\varphi : V_1 \to V_2$ è una mappa razionale che ammette un'inversa $\psi : V_2 \to V_1$ tale che $\psi \circ \varphi = id_{V_1}$ e $\varphi \circ \psi = id_{V_2}$ come mappe razionali.
Se esiste una mappa birazionale, allora V_1 e V_2 sono *birazionalmente equivalenti* o *birazionali*.

1.4 Curve

Definizione 1.4.1. Una *curva* è una varietà proiettiva di dimensione 1.

Osservazione 1.4.2. $\bar{K}(C)$ ha grado di trascendenza 1 su $\bar{K}$.
Riprendiamo infatti l'Esempio 1.1.15: se vogliamo che C sia data da una sola equazione affine non costante $f(X_1, \ldots, X_n) = 0$, allora $\dim(C) = 1$ implica $n = 2$ e C è data da $f(X, Y) = 0$. Supponiamo X trascendente su $\bar{K}$, allora Y è algebrico su $\bar{K}(X)$ grazie a f e si ha: $\bar{K}(C) = \bar{K}(X)[Y]/(f)$.

Definizione 1.4.3. Sia C una curva e P un punto liscio di C. É possibile definire una *valutazione discreta* sull'anello locale $\bar{K}[C]_P$ data da

$$\mathrm{ord}_P : \bar{K}[C]_P \to \{0, 1, 2, \ldots\} \cup \{\infty\},$$

$$\mathrm{ord}_P(f) = \sup\{d \in \mathbb{Z} : f \in M_P^d\}.$$

Valgono le seguenti proprietà:

- $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$
- $\mathrm{ord}_P(f + g) \geq \min\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\}$.

Ponendo $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$, estendiamo la valutazione al campo delle funzioni $\bar{K}(C)$:

$$\mathrm{ord}_P : \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}.$$

Sia quindi $f \in \bar{K}(C)$, allora $\mathrm{ord}_P(f)$ è detto *ordine di f in P*.
Quando $\mathrm{ord}_P(f) \geq 0$, f è regolare in P (i.e. $f \in \bar{K}[C]_P$) e possiamo calcolare $f(P)$.
Se $\mathrm{ord}_P(f) > 0$, diciamo che f ha uno *zero* in P e si ha $f(P) = 0$.
Se $\mathrm{ord}_P(f) < 0$, diciamo che f ha un *polo* in P e poniamo $f(P) = \infty$.

Osservazione 1.4.4. $\bar{K}[C]_P$ è un *anello a valutazione discreta* poiché per ogni suo elemento f vale $\mathrm{ord}_P(f) \geq 0$. M_P è il suo ideale massimale: infatti M_P contiene gli elementi f tali che $\mathrm{ord}_P(f) > 0$.
Un elemento $t \in \bar{K}(C)$ tale che $\mathrm{ord}_P(t) = 1$ è un *parametro uniformizzante di C in P*. In particolare t è un generatore per l'ideale M_P.

Esempio 1.4.5. Sia $C : Y^2 = X^3 + X$. Per l'Osservazione 1.2.11 possiamo guardare C dal punto di vista affine ricordando che esiste anche un punto all'infinito. C è non singolare poiché l'insieme dei punti singolari è dato da $C^{sing} : 3X^2 + 1 = 2Y = 0$ (vedi Esempio 1.1.17). In particolare $P = (0, 0)$ è liscio. Consideriamo $f = Y$, $g = X$, $h = 2Y^2 - X$ in $\bar{K}[C]_P$, osserviamo che $M_P = (X, Y)$ e $M_P^2 = (X^2, XY, Y^2)$, e guardiamo gli ordini:

$$\mathrm{ord}_P(f) = 1, \qquad \mathrm{ord}_P(g = Y^2 - X^3) = 2, \qquad \mathrm{ord}_P(h = Y^2 + X^3) = 2.$$

Vediamo che f è proprio un generatore di M_P e $\bar{K}[C]_P$ è un anello a valutazione discreta.

Proposizione 1.4.6. *Sia C/K una curva e sia $t \in K(C)$ un parametro uniformizzante in un certo punto $P \in C(K)$ non singolare. Allora $K(C)$ è un'estensione finita separabile di $K(t)$.*

Dimostrazione. Si veda [16] II.1 (Proposition 1.4).

□

1.5 Mappe tra curve

Proposizione 1.5.1. *Siano C una curva, $V \subset \mathbb{P}^n$ una varietà, $P \in C$ un punto liscio e $\varphi : C \to V$ una mappa razionale. Allora φ è regolare in P.*
In particolare, se C è liscia allora φ è un morfismo.

Dimostrazione. Sia $\varphi = [f_0, \ldots, f_n]$ con $f_i \in \bar{K}(C)$ e scegliamo un parametro uniformizzante $t \in \bar{K}(C)$ per C in P. Poniamo $k = \min_{0 \leq i \leq n}\{\mathrm{ord}_P(f_i)\}$, allora $\mathrm{ord}_P(t^{-k} f_i) \geq 0$ $\forall i$ e in particolare $\mathrm{ord}_P(t^{-k} f_j) = 0$ per qualche j, che implicano $t^{-k} f_i$ regolare in P per ogni i e $(t^{-k} f_j)(P) \neq 0$. Quindi φ è regolare in P.

□

Esempio 1.5.2. Sia C/K una curva liscia e sia $f \in K(C)$ una funzione. Allora f definisce una mappa razionale φ nel modo seguente:

$$\varphi : C \to \mathbb{P}^1, \qquad P \to [f(P), 1].$$

φ è un morfismo ed esplicitamente è dato da

$$\varphi(P) = \begin{cases} [f(P), 1] & \text{se } f \text{ è regolare in } P \\ [1, 0] & \text{se } f \text{ ha un polo in } P. \end{cases}$$

D'altra parte, sia

$$\varphi : C \to \mathbb{P}^1, \qquad \varphi = [g, h]$$

una mappa razionale definita su K. Allora per $h = 0$ si ha la mappa costante $\varphi = [1, 0]$, altrimenti si ha la mappa $\varphi = [f, 1]$ con $f = g/h \in K(C)$. Scrivendo ∞ al posto di $[1, 0]$ si ha una corrispondenza biunivoca tra le funzioni f e le mappe φ:

$$K(C) \cup \{\infty\} \leftrightarrow \{\text{mappe } C \to \mathbb{P}^1 \text{ definite su } K\}.$$

Teorema 1.5.3. *Sia $\varphi : C_1 \to C_2$ un morfismo di curve, con C_1 non singolare. Allora φ è costante oppure suriettiva.*

Dimostrazione. Osserviamo che $\varphi(C_1)$ è chiuso e irriducibile in C_2. Per la parte $\varphi(C_1)$ si rimanda a [7] II §6 (Proposition 6.8). Inoltre poiché C_2 è irriducibile, anche $\varphi(C_1)$ lo è. Ci sono quindi solo due possibilità: $\varphi(C_1)$ è un punto, i.e. φ è costante, oppure $\varphi(C_1) = C_2$, i.e. φ è suriettiva.

□

Osservazione 1.5.4. Siano ora C_1/K e C_2/K curve e sia $\varphi : C_1 \to C_2$ un morfismo non costante (i.e. suriettivo) definito su K. La composizione con φ induce quindi un'iniezione tra campi delle funzioni che fissa K:

$$\varphi^* : K(C_2) \to K(C_1), \qquad \varphi^*(f) = f \circ \varphi.$$

Infatti, riprendendo la Definizione 1.3.8, sappiamo che per φ morfismo vale che $f \circ \varphi$ è regolare per ogni f funzione regolare su $V \subseteq C_2$ aperto. f in particolare è una funzione razionale in $K(C_2)$ e, poiché $\varphi^{-1}(V)$ è aperto per continuità di φ, possiamo considerare la composizione $f \circ \varphi : \varphi^{-1}(V) \to K$. Questa è quindi ben definita su $\varphi^{-1}(V)$ e per definizione di morfismo è regolare. Quindi in particolare è una funzione razionale in $K(C_1)$.

Teorema 1.5.5. *Siano C_1/K e C_2/K curve.*

1. *Sia $\varphi : C_1 \to C_2$ una mappa razionale dominante non costante definita su K, allora $K(C_1)$ è un'estensione algebrica finita di $\varphi^*(K(C_2))$.*

2. *Sia $\alpha : K(C_2) \to K(C_1)$ un'iniezione tra campi delle funzioni che fissa K, allora esiste un'unica mappa non costante $\varphi : C_1 \to C_2$ definita su K tale che $\varphi^* = \alpha$.*

Dimostrazione. **1.** Il ragionamento è simile a quello esposto nell'Osservazione 1.5.4 perché consideriamo un morfismo φ_U suriettivo come rappresentante di φ secondo la Definizione 1.3.10. Inoltre per l'Osservazione 1.4.2 entrambe $K(C_1)$ e $K(C_2)$ sono estensioni finite con grado di trascendenza 1 su K, quindi $K(C_1)$ è un'estensione algebrica finita di $\varphi^*(K(C_2))$.

2. Supponiamo $C_1 \subset \mathbb{P}^n$. Sia $g_i \in K(C_2)$ la funzione su C_2 corrispondente a X_i/X_0 per ogni i (possiamo riordinare le X_j in modo tale che C_2 non contenga l'iperpiano $X_0 = 0$). Allora $\varphi = [1, \alpha(g_1), \ldots, \alpha(g_n)]$ dà la mappa φ tale che $\varphi^* = \alpha$. In particolare φ non è costante poiché le g_i non sono tutte costanti e inoltre α è iniettiva.
Sia poi $\psi = [f_0, \ldots, f_n]$ un'altra mappa tale che $\psi^* = \alpha$. Allora per ogni i si ha: $f_i/f_0 = \psi^*(g_i) = \varphi^*(g_i) = \alpha(g_i)$. Quindi $\psi = \varphi$.

□

Definizione 1.5.6. Sia $\varphi : C_1 \to C_2$ una mappa di curve definita su K. Se φ è costante, diciamo che il *grado di* φ è 0. Altrimenti φ è una *mappa finita* e il suo *grado* è dato da $\deg \varphi = [K(C_1) : \varphi^*(K(C_2))]$. La mappa φ si dice *separabile* o *non separabile* assumendo la corrispondente proprietà dell'estensione di campi (indichiamo il grado separabile e non separabile dell'estensione con $\deg_s \varphi$ e $\deg_i \varphi$).

Osservazione 1.5.7. Sia $\varphi : C_1 \to C_2$ una mappa di curve definita su K non costante. É possibile costruire una mappa di campi nel verso opposto rispetto a φ^* utilizzando la mappa norma:

$$\varphi_* : K(C_1) \to K(C_2), \qquad \varphi_* = (\varphi^*)^{-1} \circ N_{K(C_1)/\varphi^*(K(C_2))}.$$

Corollario 1.5.8. *Siano C_1 e C_2 curve non singolari e sia $\varphi : C_1 \to C_2$ una mappa di grado 1. Allora φ è un isomorfismo.*

Dimostrazione. Se $\deg \varphi = 1$, allora per definizione si ha che l'estensione di campi ha grado 1 ovvero $\bar{K}(C_1) = \varphi^*(\bar{K}(C_2))$ quindi φ^* è un isomorfismo tra campi delle funzioni. Possiamo considerare quindi la mappa inversa $(\varphi^*)^{-1} : \bar{K}(C_1) \xrightarrow{\sim} \bar{K}(C_2)$ e per la 2. del Teorema 1.5.5 esiste una mappa razionale $\psi : C_2 \to C_1$ tale che $\psi^* = (\varphi^*)^{-1}$. Poiché per ipotesi C_2 è liscia, allora la Proposizione 1.5.1 afferma che anche ψ è un morfismo. Inoltre sappiamo che $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$ è la mappa identità su $\bar{K}(C_2)$ e analogamente $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$ è la mappa identità su $\bar{K}(C_1)$. Quindi per l'unicità data dalla 2. del Teorema 1.5.5 si ha $\varphi \circ \psi$ e $\psi \circ \varphi$ sono rispettivamente le mappe identità su C_2 e C_1. Allora φ e ψ sono isomorfismi.

□

Osservazione 1.5.9. Si può riformulare il Corollario 1.5.8 nel modo seguente: C_1 e C_2 sono birazionalmente equivalenti se e solo se $\bar{K}(C_1)$ e $\bar{K}(C_2)$ sono isomorfi. Basta considerare i morfismi rappresentanti per le mappe razionali e farli agire su aperti.

Osservazione 1.5.10. Il risultato del Corollario 1.5.8 porta ad osservare una corrispondenza biunivoca tra curve non singolari definite su K ed estensioni di K finitamente generate con grado di trascendenza 1, tra mappe razionali non costanti dominanti definite su K (o equivalentemente morfismi suriettivi definiti su K) e omomorfismi iniettivi di campi che fissano K.

$$\begin{array}{c} C/K \\ \varphi : C_1 \to C_2 \end{array} \quad \Longleftrightarrow \quad \begin{array}{c} K(C) \\ \varphi^* : K(C_2) \to K(C_1) \end{array}$$

Osserviamo ora il comportamento di una mappa nell'intorno di un punto.

Definizione 1.5.11. Sia $\varphi : C_1 \to C_2$ una mappa non costante di curve non singolari e sia $P \in C_1$. L'*indice di ramificazione di φ in P*, denotato con $e_\varphi(P)$, è la quantità $e_\varphi(P) = \mathrm{ord}_P(\varphi^*(t_{\varphi(P)}))$ con $t_{\varphi(P)} \in K(C_2)$ parametro uniformizzante in $\varphi(P)$. In generale si ha che $e_\varphi(P) \geq 1$ e se $e_\varphi(P) = 1$ si dice che φ è *non ramificata in P*. Se questo vale per ogni P, allora φ è *non ramificata*.
Per ogni $Q \in C$, vale la seguente relazione:

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi. \tag{1.1}$$

Proposizione 1.5.12. *$\varphi : C_1 \to C_2$ è non ramificata se e solo se $\#\varphi^{-1}(Q) = \deg \varphi$, per ogni $Q \in C_2$.*

Dimostrazione. Si ottiene dalla relazione (1.1). Infatti $\#\varphi^{-1}(Q) = \deg \varphi$ se e solo se $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \#\varphi^{-1}(Q)$. Poiché $e_\varphi(P) \geq 1$, allora necessariamente $e_\varphi(P) = 1$. □

1.6 Divisori

Sia C una curva, il *gruppo dei divisori di C*, denotato con $\mathrm{Div}(C)$, è il gruppo abeliano libero generato dai punti di C. Quindi un divisore $D \in \mathrm{Div}(C)$ è una somma formale

$$D = \sum_{P \in C} n_P \{P\}$$

con $n_P \in \mathbb{Z}$ e $n_P = 0$ per ogni P tranne al più un numero finito. Il *grado di D* è dato dall'omomorfismo di gruppi

$$\deg : \mathrm{Div}(C) \to \mathbb{Z}, \qquad \deg D = \sum_{P \in C} n_P.$$

Sia $\mathrm{Div}_0(C) = \{D \in \mathrm{Div}(C) : \deg D = 0\}$ il sottogruppo dei divisori di grado 0: infatti $\mathrm{Div}_0(C) = \ker(\deg)$.
Se C è definita su K, $G_{\bar{K}/K}$ agisce su $\mathrm{Div}(C)$: $D^\sigma = \sum n_P \{P^\sigma\}$. Allora D si dice *definito su K* se $D^\sigma = D$ per ogni $\sigma \in G_{\bar{K}/K}$.

Sia ora C una curva liscia. Definiamo il divisore per $f \in \bar{K}(C)^*$:

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)\{P\} \ \in \mathrm{Div}(C).$$

Osservazione 1.6.1. Perché la definizione di $\mathrm{div}(f)$ abbia senso, osserviamo che f deve avere un numero finito di zeri e poli.

L'azione di $\sigma \in G_{\bar{K}/K}$ è tale che $\mathrm{div}(f^\sigma) = (\mathrm{div}(f))^\sigma$. Osserviamo inoltre che, poiché ord_P è una valutazione, la mappa $\mathrm{div} : \bar{K}(C)^* \to \mathrm{Div}(C)$ è un omomorfismo di gruppi abeliani.

Proposizione 1.6.2. *Sia C una curva liscia e $f \in \bar{K}(C)^*$. Allora*

1. $\mathrm{div}(f) = 0 \Leftrightarrow f \in \bar{K}^*$
2. $\deg \mathrm{div}(f) = 0$.

Dimostrazione. **1.** Se $\mathrm{div}(f) = 0$, allora f non ha zeri e poli, quindi in particolare f non è suriettiva. Allora il Teorema 1.5.3 implica che f è costante. Il viceversa vale per definizione di divisore.
2. Vedi Osservazione 1.6.9.

□

Osservazione 1.6.3. La 2. della Proposizione 1.6.2 è equivalente a $\sum \mathrm{ord}_P(f) = 0$. Poiché abbiamo visto che f ha un numero finito di zeri e poli (Osservazione 1.6.1), se f in particolare non ha poli (i.e. f è regolare), allora f è costante in $\bar{K}$.

Definizione 1.6.4. Un divisore D è *principale* se può essere scritto come $D = \mathrm{div}(f)$ per una certa $f \in \bar{K}(C)^*$. Si può definire una relazione di equivalenza su $\mathrm{Div}(C)$: D_1 e D_2 sono *linearmente equivalenti*, ovvero $D_1 \sim D_2$, se $D_1 - D_2$ è principale. Il quoziente di $\mathrm{Div}(C)$ con il sottogruppo dei divisori principali è detto *gruppo di Picard* o *gruppo delle classi di divisori di C*, denotato con $\mathrm{Pic}(C)$.
Dalla 2. della Proposizione 1.6.2 segue che i divisori principali formano un sottogruppo di $\mathrm{Div}_0(C)$. Definiamo quindi *parte di grado 0 del gruppo di Picard* il quoziente di $\mathrm{Div}_0(C)$ con il sottogruppo dei divisori principali e lo denotiamo con $\mathrm{Pic}_0(C)$.

Osservazione 1.6.5. La Definizione 1.6.4 e la Proposizione 1.6.2 possono essere riassunte nella seguente affermazione: esiste una successione esatta

$$1 \to \bar{K}^* \to \bar{K}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}_0(C) \to \mathrm{Pic}_0(C) \to 0.$$

Esempio 1.6.6. Su $\mathbb{P}^1$ vale che ogni divisore di grado 0 è principale.
Per vederlo supponiamo che $D = \sum n_P\{P\}$ abbia grado 0, i.e. $\sum n_P = 0$. Sia $P \in \mathbb{P}^1$ con $P = [\alpha, \beta]$, allora D è il divisore della funzione $\prod_{P \in \mathbb{P}^1} (\beta X - \alpha Y)^{n_P}$. Quindi l'ipotesi $\sum n_P = 0$ assicura che tale funzione sia in $\bar{K}(\mathbb{P}^1)$. Da questo segue che la mappa $\deg : \mathrm{Pic}(\mathbb{P}^1) \to \mathbb{Z}$ è un isomorfismo.
Vale anche il viceversa: se C è una curva liscia e $\mathrm{Pic}(C) \cong \mathbb{Z}$, allora C è isomorfo a $\mathbb{P}^1$.
In particolare si ha la successione esatta: $0 \to \mathrm{Pic}_0(C) \hookrightarrow \mathrm{Pic}(C) \xrightarrow{\sim} \mathbb{Z} \to 0$.

Sia ora $\varphi : C_1 \to C_2$ una mappa non costante di curve lisce. Sappiamo che φ induce le mappe φ^* e φ_* tra i campi delle funzioni di C_1 e C_2. In modo simile possiamo definire due mappe tra i gruppi dei divisori:

$$\begin{array}{rcl} \varphi_* : \mathrm{Div}(C_1) & \to & \mathrm{Div}(C_2), \\ \{P\} & \to & \{\varphi(P)\} \end{array} \qquad \begin{array}{rcl} \varphi^* : \mathrm{Div}(C_2) & \to & \mathrm{Div}(C_1), \\ \{Q\} & \to & \displaystyle\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)\{P\}. \end{array}$$

Esempio 1.6.7. Sia C una curva liscia e sia $f \in \bar{K}(C)$ una funzione non costante. Consideriamo la mappa $\varphi : C \to \mathbb{P}^1$ data da f (vedi Esempio 1.5.2). Allora si ha che $\mathrm{div}(f) = \varphi^*(\{0\} - \{\infty\})$.

Proposizione 1.6.8. *Sia $\varphi : C_1 \to C_2$ una mappa non costante di curve lisce. Allora:*

1. $\deg \varphi^*(D) = \deg \varphi \deg D$ *per ogni* $D \in \mathrm{Div}(C_2)$
2. $\varphi^*(\mathrm{div}(f)) = \mathrm{div}(\varphi^*(f))$ *per ogni* $f \in \bar{K}(C_2)^*$
3. $\deg \varphi_*(D) = \deg D$ *per ogni* $D \in \mathrm{Div}(C_1)$
4. $\varphi_*(\mathrm{div}(f)) = \mathrm{div}(\varphi_*(f))$ *per ogni* $f \in \bar{K}(C_1)^*$
5. $\varphi_* \circ \varphi^*$ *agisce come moltiplicazione per* $\deg \varphi$ *su* $\mathrm{Div}(C_2)$.

Dimostrazione. **1.** Osserviamo che, per linearità, basta verificare la formula per $D = \{P\}$. Si ottiene che $\sum e_\varphi(P) = \deg \varphi$, grazie alla relazione (1.1).
2. Dobbiamo vedere che $\mathrm{ord}_P(\varphi^*(f)) = e_\varphi(P)\ \mathrm{ord}_{\varphi(P)}(f)$. Osserviamo i seguenti fatti: sia $k = \mathrm{ord}_{\varphi(P)}(f) = \sup\{d \in \mathbb{Z} : f \in M^d_{\varphi(P)}\}$ quindi le funzioni f e $g = (t_{\varphi(P)})^k$ hanno lo stesso ordine in $\varphi(P)$. Applicando φ^* e guardando l'ordine in P, si ha: $\mathrm{ord}_P(\varphi^*(f)) = \mathrm{ord}_P(\varphi^*(g)) = e_\varphi(P)\ k$.
3. Ovvio dalla definizione di φ_*.
4. Si ottiene dalle definizioni di φ_* come mappa tra campi delle funzioni e come mappa tra gruppi dei divisori.
5. Si ottiene ancora dalla relazione (1.1).

□

Osservazione 1.6.9. La 1. e la 3. della Proposizione 1.6.8 mostrano che φ^* e φ_* portano divisori di grado 0 in divisori di grado 0, mentre la 2. e la 4. della stessa Proposizione mostrano che divisori principali vengono mandati in divisori principali. In particolare quindi si hanno le mappe

$$\varphi_* : \mathrm{Pic}_0(C_1) \to \mathrm{Pic}_0(C_2) \qquad \text{e} \qquad \varphi^* : \mathrm{Pic}_0(C_2) \to \mathrm{Pic}_0(C_1).$$

Riprendiamo l'Esempio 1.6.7 con $f \in \bar{K}(C_2)$ che definisce $\varphi : C \to \mathbb{P}^1$. Allora

$$\deg \mathrm{div}(f) = \deg \varphi^*(\{0\} - \{\infty\}) = \deg \varphi \deg(\{0\} - \{\infty\}) = 0$$

poiché $\{0\} - \{\infty\}$ è un divisore di grado 0 in $\mathbb{P}^1$.

1.7 Differenziali

Sia C una curva, lo *spazio delle forme differenziali (meromorfe) su* C, denotato con Ω_C, è il $\bar{K}$-spazio vettoriale generato dai simboli del tipo $d\alpha$ con $\alpha \in \bar{K}(C)$ tali che, per ogni $\alpha, \beta \in \bar{K}(C)$ e per ogni $k \in \bar{K}$, si ha:

1. $d(\alpha + \beta) = d\alpha + d\beta$
2. $d(\alpha\beta) = \alpha\, d\beta + \beta\, d\alpha$
3. $d(k\alpha) = k\, d\alpha$
4. $dk = 0$.

Osservazione 1.7.1. Sia $\varphi : C_1 \to C_2$ una mappa non costante di curve. La mappa dei campi delle funzioni associata $\varphi^* : \bar{K}(C_2) \to \bar{K}(C_1)$ induce una mappa sui differenziali:

$$\varphi^* : \Omega_{C_2} \to \Omega_{C_1}, \qquad \varphi^*\left(\sum f_i d\alpha_i\right) = \sum \varphi^*(f_i)\, d\varphi^*(\alpha_i).$$

Proposizione 1.7.2. *Sia C una curva e sia $P \in C$. Sia inoltre $t \in \bar{K}(C)$ un parametro uniformizzante in P. Valgono i seguenti fatti:*

1. *Ω_C è un $\bar{K}(C)$-spazio vettoriale 1-dimensionale.*
2. *Sia $\alpha \in \bar{K}(C)$, allora $d\alpha$ è una $\bar{K}(C)$-base per Ω_C se e solo se $\bar{K}(C)$ è un'estensione finita separabile di $\bar{K}(\alpha)$.*
3. *Per ogni $\omega \in \Omega_C$ esiste un'unica funzione $g \in \bar{K}(C)$ tale che $\omega = g\, dt$. Scriviamo anche $g = \omega/dt$.*
4. *Sia $\omega \in \Omega_C$ con $\omega \neq 0$. Il valore $\mathrm{ord}_P(\omega/dt)$ non dipende dalla scelta del parametro uniformizzante t ed è chiamato* ordine di ω in P, *denotato con $\mathrm{ord}_P(\omega)$.*
5. *Siano $\alpha, f \in \bar{K}(C)$ con $\alpha(P) = 0$. Sia $p = char(K)$, allora:*
   $ord_P(f\, d\alpha) = ord_P(f) + ord_P(\alpha) - 1$ se $p = 0$ o $p \nmid ord_P(\alpha)$,
   $ord_P(f\, d\alpha) \geq ord_P(f) + ord_P(\alpha)$ se $p > 0$ e $p \mid ord_P(\alpha)$.
6. *Sia $\omega \in \Omega_C$ con $\omega \neq 0$. Allora $ord_P(\omega) \neq 0$ solo per un numero finito di punti $P \in C$.*

Dimostrazione. Per **1.** e **2.** si rimanda a [14] III §5.4 (Theorem 3, Theorem 4).
3. Segue da 1. e 2. e dalla Proposizione 1.4.6.
4. Sia $t' \in \bar{K}(C)$ un altro parametro uniformizzante in P. Allora dt/dt' e dt'/dt sono entrambe regolari in P e $\mathrm{ord}_P(dt'/dt) = 0$. Scriviamo quindi $\omega = g\, dt' = g(dt'/dt)dt$ e otteniamo $\mathrm{ord}_P(\omega/dt) = \mathrm{ord}_P(g) = \mathrm{ord}(\omega/dt')$.

5. Possiamo scrivere $\alpha = ut^n$ con $n = \mathrm{ord}_P(\alpha) \geq 1$ e $\mathrm{ord}_P(u) = 0$. Allora $d\alpha = [nut^{n-1} + (du/dt)t^n]dt$. Osserviamo che du/dt è regolare, i.e. $\mathrm{ord}_P(du/dt) \geq 0$, quindi guardando l'ordine si ha che: $n > \mathrm{ord}_P(d\alpha) \geq \min\{n-1, n + \mathrm{ord}_P(du/dt)\} = n-1$. Si ottiene quindi che $\mathrm{ord}_P(fd\alpha) = \mathrm{ord}_P(f) + n - 1$.
Se $p > 0$ e $p \mid \mathrm{ord}_P(\alpha)$, allora il termine nut^{n-1} si annulla e si ha $\mathrm{ord}_P(d\alpha) = n + \mathrm{ord}_P(du/dt) \geq n$ da cui $\mathrm{ord}_P(fd\alpha) \geq \mathrm{ord}_P(f) + n$.
6. Sia $\alpha : C \to \mathbb{P}^1$ in $\bar{K}(C)$ tale che α è ramificata solo in un numero finito di punti di C con $\bar{K}(C)/\bar{K}(\alpha)$ separabile. Consideriamo quindi $\omega = fd\alpha$. Restringiamo il numero finito di punti ad un unico $P \in C$ tale che $\alpha(P) \neq \infty$ e supponiamo anche $f(P) \neq 0, \infty$ quindi $\mathrm{ord}_P(f) = 0$. Abbiamo allora $\alpha : C \to \mathbb{P}^1$ non ramificata in P. Dalle condizioni su α si ottiene che $\alpha - \alpha(P)$ è un parametro uniformizzante in P e si ha: $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(fd(\alpha - \alpha(P))) = 0$.

□

Definizione 1.7.3. Sia $\omega \in \Omega_C$. Il *divisore associato al differenziale* ω è dato da

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)\{P\} \ \in \mathrm{Div}(C).$$

Diciamo che ω è *regolare* (o *olomorfo*) se $\mathrm{ord}_P(\omega) \geq 0$ per ogni $P \in C$, e che ω è *non nullo* se $\mathrm{ord}_P(\omega) \leq 0$ per ogni $P \in C$.

Definizione 1.7.4. La *classe canonica di* C, denotata con K_C, è l'immagine di $\mathrm{div}(\omega)$ in $\mathrm{Pic}(C)$ per ogni differenziale $\omega \in \Omega_C$ non nullo. Ogni divisore in questa classe è detto *divisore canonico*.
Questa definizione ha senso perché per ogni coppia di divisori non nulli $\omega_1, \omega_2 \in \Omega_C$, esiste una funzione $f \in \bar{K}(C)^*$ tale che $\omega_1 = f\omega_2$ (per la 1. della Proposizione 1.7.2). Per questo vale: $\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$, i.e. $\mathrm{div}(\omega_1) \sim \mathrm{div}(\omega_2)$. Pertanto tutti i divisori canonici appartengono alla stessa classe di equivalenza in $\mathrm{Pic}(C)$.

1.8 Genere

Sia C una curva, è possibile dare un ordine parziale su $\mathrm{Div}(C)$ nel modo seguente.

Definizione 1.8.1. Diciamo che il divisore $D = \sum n_P\{P\}$ è *positivo* e lo indichiamo con $D \geq 0$ se $n_P \geq 0$ per ogni $P \in C$.
Dati due divisori D_1, D_2 scriviamo $D_1 \geq D_2$ quando $D_1 - D_2$ è positivo.

Esempio 1.8.2. Sia $f \in \bar{K}(C)^*$ una funzione regolare in ogni punto di C tranne un punto P. Supponiamo che f abbia un polo in P di ordine al più n. Possiamo scrivere quindi: $\mathrm{div}(f) \geq -n\{P\}$. Se scriviamo $\mathrm{div}(f) \geq \{Q\} - n\{P\}$, sappiamo inoltre che f ha uno zero in Q.

Osservazione 1.8.3. Riprendiamo la Proposizione 1.6.2 e consideriamo $f \in \bar{K}(C)^*$ tale che $\mathrm{div}(f) \geq 0$. Dalla 1. sappiamo che $\mathrm{div}(f) = 0$ implica $f \in \bar{K}^*$. Vediamo quindi il caso $\mathrm{div}(f) > 0$: dalla definizione si ha che $\mathrm{ord}_P(f) > 0$ per ogni P mentre per la 2. deve valere $\deg \mathrm{div}(f) = \sum \mathrm{ord}_P(f) = 0$. L'unica possibilità è che f sia costante.
Si ha quindi: $\mathrm{div}(f) \geq 0 \Leftrightarrow f \in \bar{K}$ (si veda anche l'Osservazione 1.6.3).

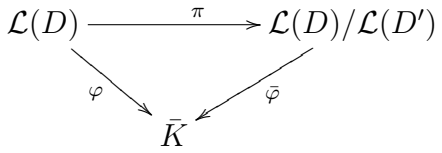
Sia D un divisore, associamo ad esso l'insieme $\mathcal{L}(D) = \{f \in \bar{K}(C)^* : \mathrm{div}(f) \geq -D\} \cup \{0\}$.

Proposizione 1.8.4. *Siano $D, D' \in Div(C)$.*

1. *$\mathcal{L}(D)$ è un $\bar{K}$-spazio vettoriale di dimensione finita. Sia quindi $\ell(D) = \dim_{\bar{K}} \mathcal{L}(D)$. Si hanno i seguenti casi:*
   (a) *$\mathcal{L}(0) = \bar{K}$ e $\ell(0) = 1$*
   (b) *se $\deg D < 0$, allora $\mathcal{L}(D) = \{0\}$ e $\ell(D) = 0$*
   (c) *se $\deg D \geq 0$, allora $\ell(D) \leq \deg D + 1$.*
2. *Se $D \sim D'$, allora $\mathcal{L}(D) \cong \mathcal{L}(D')$ e in particolare $\ell(D) = \ell(D')$.*

Dimostrazione. **1.** Poiché $D = \sum n_P\{P\}$ e $\mathrm{div}(f) = \sum \mathrm{ord}_P(f)\{P\}$, allora $f \in \mathcal{L}(D)$ equivale a $\mathrm{ord}_P(f) \geq -n_P$ per ogni P tale che $n_P \neq 0$ e $\mathrm{ord}_P(f) \geq 0$ se $n_P = 0$. Dalle proprietà della mappa ord_P dati $f, g \in \mathcal{L}(D)$ (i.e. $\mathrm{ord}_P(f) \geq -n_P$ e $\mathrm{ord}_P(g) \geq -m_P$) e $\alpha \in \bar{K}^*$ (i.e. $\mathrm{ord}_P(\alpha) = 0$) si ha che $f + g$ e αf sono ancora funzioni in $\mathcal{L}(D)$. Infatti $\mathrm{ord}_P(f+g) \geq \min\{\mathrm{ord}_P(f), \mathrm{ord}_P(g)\} \geq -\max\{n_P, m_P\}$ e $\mathrm{ord}_P(\alpha f) = \mathrm{ord}_P(f) \geq -n_P$.
1(a). Dall'Osservazione 1.8.3.
1(b). Sia $f \in \mathcal{L}(D)$. Per la 2. della Proposizione 1.6.2 si ha che $0 = \deg \mathrm{div}(f) \geq \deg(-D) = -\deg D$ da cui si ottiene $\deg D \geq 0$. Per ipotesi $\deg D < 0$ quindi l'assurdo implica $\ell(D) = 0$.
1(c). Consideriamo $D' < D$ allora è facile osservare che $\mathcal{L}(D') \subset \mathcal{L}(D)$. Infatti D sarà del tipo $D = D' + \sum\{P_i\}$ con i P_i non necessariamente distinti. Vogliamo dimostrare che $\dim_{\bar{K}}(\mathcal{L}(D)/\mathcal{L}(D')) \leq \deg(D - D')$.
Supponiamo per ora il risultato già dimostrato e prendiamo $D = D' + (n+1)\{P\}$ con $n = \deg D$. Osserviamo che $\mathcal{L}(D') = 0$ per 1(b). poiché $\deg D' = -1$. Allora $\dim_{\bar{K}}(\mathcal{L}(D)/\mathcal{L}(D')) \leq n + 1$ equivale a $\ell(D) \leq n + 1 = \deg D + 1$.
Resta da dimostrare l'affermazione precedente. Vediamo il caso più semplice, in cui $D = D' + \{P\}$. Vogliamo quindi dimostrare che $\dim(\mathcal{L}(D)/\mathcal{L}(D')) \leq 1$. Il risultato generale si ottiene per induzione.
Poiché gli spazi $\mathcal{L}(D)$ e $\mathcal{L}(D')$ sono $\bar{K}$-spazi vettoriali, allora sono anche $\bar{K}$-moduli. Costruiamo quindi una mappa lineare $\varphi : \mathcal{L}(D) \to \bar{K}$. Sia t un parametro uniformizzante in P e sia k il coefficiente di $\{P\}$ in D'. Allora definiamo φ come la mappa tale che $\varphi(f) = (t^{k+1}f)(P)$. φ è ben definita, infatti $\mathrm{ord}_P(f) \geq -k - 1$ poiché $f \in \mathcal{L}(D)$.
Osserviamo che $\ker(\varphi) = \mathcal{L}(D')$. Sia quindi $\pi : \mathcal{L}(D) \to \mathcal{L}(D)/\mathcal{L}(D')$ la proiezione sul

quoziente. Allora per le proprietà dei $\bar{K}$-moduli esiste una mappa $\bar{\varphi}$ tale che $\bar{\varphi} \circ \pi = \varphi$ costruita nel modo seguente:



Poiché $\mathcal{L}(D)/\mathcal{L}(D') = \mathcal{L}(D)/\ker(\varphi)$, allora $\bar{\varphi}$ è iniettiva. Si ottiene il risultato.
2. Possiamo scrivere $D = D' + \operatorname{div}(g)$ per qualche $g \in \bar{K}(C)^*$. Si ottiene quindi una mappa $\mathcal{L}(D) \to \mathcal{L}(D')$ tale che $f \to fg$ che è un isomorfismo di spazi vettoriali.

□

Osservazione 1.8.5. Nella dimostrazione di 1(c). della Proposizione 1.8.4, abbiamo osservato che: se $D' < D$ allora si ha $\mathcal{L}(D') \subset \mathcal{L}(D)$.

Osservazione 1.8.6. Sia K_C un divisore canonico di C, quindi $K_C = \operatorname{div}(\omega)$. Ogni funzione $f \in \mathcal{L}(K_C)$ soddisfa la proprietà $\operatorname{div}(f) \geq -\operatorname{div}(\omega)$ per cui $\operatorname{div}(f\omega) \geq 0$, i.e. $f\omega$ è olomorfa. Vale anche il viceversa: se il differenziale $f\omega$ è olomorfo, allora $f \in \mathcal{L}(K_C)$. Sappiamo che ogni differenziale su C è del tipo $f\omega$ per una certa f, quindi osserviamo che esiste un isomorfismo di $\bar{K}$-spazi vettoriali: $\mathcal{L}(K_C) \cong \{\omega \in \Omega_C : \omega \text{ è olomorfa}\}$.
La dimensione $\ell(K_C)$ di questo spazio è un invariante per la curva C.

Teorema 1.8.7 (Riemann-Roch)**.** *Sia C una curva liscia e sia K_C un divisore canonico su C. Allora esiste un intero $g \geq 0$, detto* genere di C*, tale che, per ogni divisore $D \in Div(C)$, si ha*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

Dimostrazione. Si veda [7] IV §1, [14] III §6.6, [6] 8 §6.

□

Corollario 1.8.8.

1. $\ell(K_C) = g$
2. $\deg K_C = 2g - 2$
3. *Se* $\deg D > 2g - 2$*, allora*

$$\ell(D) = \deg D - g + 1.$$

Dimostrazione. **1.** Dal Teorema 1.8.7 con $D = 0$, poiché $\ell(0) = 1$ per la 1(a). della Proposizione 1.8.4 e $\deg D = 0$.
2. Dal Teorema 1.8.7 con $D = K_C$ e dalla 1.
3. Dal Teorema 1.8.7 osservando che $\deg(K_C - D) < 0$ per la 2., quindi $\ell(K_C - D) = 0$ per la 1(b). della Proposizione 1.8.4.

□

Definizione 1.8.9. Riprendendo la notazione dell'Esempio 1.1.11, sia f un polinomio irriducibile di grado d in $\bar{K}[X,Y]$ e C la curva definita dall'equazione $f(X,Y)=0$. Il *genere di* C corrisponde anche alla quantità

$$g = \binom{d-1}{2} = \frac{(d-1)(d-2)}{2}.$$

Esempio 1.8.10. Vediamo ora che in $\mathbb{P}^1$ non esistono differenziali olomorfi e il genere di $\mathbb{P}^1$ vale 0.
Per la prima affermazione consideriamo la funzione coordinata t su $\mathbb{P}^1$ e mostriamo che

$$\operatorname{div}(dt) = -2\{\infty\}.$$

Sia infatti $k \in \bar{K}$, allora la funzione $t-k$ è un parametro uniformizzante in k. Per la 5. della Proposizione 1.7.2 si ha che

$$\operatorname{ord}_k(dt) = \operatorname{ord}_k(d(t-k)) = 0.$$

Resta da osservare il caso $\infty \in \mathbb{P}^1$ in cui consideriamo $1/t$ come parametro uniformizzante: si ha quindi che

$$\operatorname{ord}_\infty(-t^2 d(1/t)) = -2.$$

Vediamo quindi che $\deg \operatorname{div}(dt) = -2$ e dt non è olomorfa. La stessa cosa vale per ogni $\omega \in \Omega_{\mathbb{P}^1}$ poiché per la 3. della Proposizione 1.7.2 possiamo scrivere $\omega = f\,dt$. Allora

$$\deg \operatorname{div}(\omega) = \deg \operatorname{div}(dt)$$

poiché $\deg \operatorname{div}(f) = 0$ per la 2. della Proposizione 1.6.2.
Ora sappiamo che non esistono differenziali olomorfi in $\mathbb{P}^1$ quindi $\ell(K_{\mathbb{P}^1}) = 0$. Per la 1. del Corollario 1.8.8 e per l'Osservazione 1.8.6 abbiamo quindi che $g = 0$.
Il Teorema di Riemann-Roch 1.8.7 e il Corollario 1.8.8 applicati a $\mathbb{P}^1$ equivalgono a:

$$\ell(D) - \ell(-2\infty - D) = \deg D + 1 \qquad \text{e} \qquad \ell(D) = \deg D + 1 \quad \text{se } \deg D \geq -1.$$

Esempio 1.8.11. Consideriamo la curva $C:\ y^2 = (x-e_1)(x-e_2)(x-e_3)$ con e_1, e_2, e_3 distinti in $\bar{K}$. C è liscia e ha un solo punto all'infinito che denotiamo con P_∞.
Sia $P_i = (e_i, 0) \in C$ per $i = 1, 2, 3$. Allora si ha che

$$\operatorname{div}(x-e_i) = 2\{P_i\} - 2\{P_\infty\} \qquad \text{e} \qquad \operatorname{div}(y) = \{P_1\} + \{P_2\} + \{P_3\} - 3\{P_\infty\}.$$

Utilizzando ancora la 5. della Proposizione 1.7.2, calcoliamo ora il divisore di dx:

$$\operatorname{ord}_{P_i}(dx) = ord_{P_i}(d(x-e_1)) = ord_{P_i}(x-e_1) - 1 = 1,$$
$$\operatorname{ord}_{P_\infty}(dx) = \operatorname{ord}_{P_\infty}(d(x-e_i)) = \operatorname{ord}_{P_\infty}(x-e_i) - 1 = -3.$$

Concludiamo quindi che

$$\operatorname{div}(dx) = \operatorname{div}(y) \quad \text{ovvero} \quad \operatorname{div}(dx/y) = 0.$$

Allora il differenziale dx/y è olomorfo e non nullo contemporaneamente e la classe canonica su C è quella banale, i.e. $K_C = 0$. Usando la 1. del Corollario 1.8.8 e la 1(a). della Proposizione 1.8.4, otteniamo che il genere di C è 1: infatti $g = \ell(0) = 1$. Per la 3. del Corollario 1.8.8 su C abbiamo che:

$$\ell(D) = \deg D \quad \text{per } \deg D \geq 1.$$

Osservazione 1.8.12. C insieme al punto all'infinito P_∞ è una curva ellittica.

Capitolo 2

Geometria e aritmetica delle curve ellittiche

Definizione. Sia E una curva non singolare di genere 1 e sia $\mathcal{O} \in E$. La coppia $(E, \mathcal{O})$ è una *curva ellittica*.

2.1 Equazioni di Weierstrass

Iniziamo considerando il luogo proiettivo di un'equazione cubica in $\mathbb{P}^2(\bar{K})$ con un solo punto sulla retta all'infinito, il punto base $\mathcal{O}$. Vedremo poco oltre che ogni curva ellittica può essere descritta da una tale equazione (Proposizione 2.1.10). Date quindi X, Y, Z coordinate omogenee, una cubica ha un'equazione della forma

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

con punto base $\mathcal{O} = [0, 1, 0]$ e $a_1, a_2, a_3, a_4, a_6 \in \bar{K}$. Questa è la forma più generale di un'*equazione di Weierstrass*.
Se $a_1, a_2, a_3, a_4, a_6 \in K$ si dice che la curva è *definita su K*.

• In genere viene utilizzata l'equazione di Weierstrass affine con coordinate non omogenee $x = \frac{X}{Z}$ e $y = \frac{Y}{Z}$ della forma

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

considerando sempre anche il punto base $\mathcal{O} = [0, 1, 0]$.

Definizione 2.1.1. Il *differenziale invariante* associato all'equazione di Weierstrass è la quantità

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}. \tag{2.3}$$

b_2	$=$	$a_1^2 + 4a_2$
b_4	$=$	$2a_4 + a_1a_3$
b_6	$=$	$a_3^2 + 4a_6$
b_8	$=$	$a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 = (b_2b_6 - b_4^2)/4$
c_4	$=$	$b_2^2 - 24b_4$
c_6	$=$	$-b_2^3 + 36b_2b_4 - 216b_6$

Tabella 2.1: Coefficienti per equazioni di Weierstrass

• Se $\mathrm{char}(\bar{K}) \neq 2$ possiamo semplificare l'equazione tramite il completamento al quadrato dato dalla sostituzione

$$y \to \frac{1}{2}(y - a_1x - a_3)$$

ottenendo

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{2.4}$$

con i b_i definiti in Tabella 2.1.
• Se $\mathrm{char}(\bar{K}) \neq 2, 3$ possiamo semplificare ulteriormente l'equazione eliminando il termine in x^2 tramite la sostituzione

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

ottenendo

$$y^2 = x^3 - 27c_4x - 54c_6 \tag{2.5}$$

con i c_i definiti in Tabella 2.1.

Definizione 2.1.2. Il *discriminante* dell'equazione di Weierstrass è la quantità

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = \frac{c_4^3 - c_6^2}{1728}.$$

Definizione 2.1.3. Se Δ è invertibile, il *j-invariante* della curva è la quantità

$$j = \frac{c_4^3}{\Delta}.$$

Osservazione 2.1.4. L'indice i dei coefficienti a_i, b_i, c_i indica esattamente il *peso* della corrispondente quantità. Infatti valgono le seguenti due regole:
• quando due coefficienti sono moltiplicati tra loro, i loro pesi si sommano;
• combinazioni lineari di termini con lo stesso peso hanno ancora quel peso.
In particolare il discriminante Δ ha peso 12.

ua_1'	$=$	$a_1 + 2s$
u^2a_2'	$=$	$a_2 - sa_1 + 3r - s^2$
u^3a_3'	$=$	$a_3 + ra_1 + 2t$
u^4a_4'	$=$	$a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
u^6a_6'	$=$	$a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$
u^2b_2'	$=$	$b_2 + 12r$
u^4b_4'	$=$	$b_4 + rb_2 + 6r^2$
u^6b_6'	$=$	$b_6 + 2rb_4 + r^2b_2 + 4r^3$
u^8b_8'	$=$	$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$
u^4c_4'	$=$	c_4
u^6c_6'	$=$	c_6
$u^{12}\Delta'$	$=$	Δ
j'	$=$	j
$u^{-1}\omega$	$=$	ω

Tabella 2.2: Cambio di variabili per equazioni di Weierstrass

L'equazione di Weierstrass corrispondente ad una curva non è unica. Esiste però un cambio di variabili (unico, vedi 2. della Proposizione 2.1.10) che lega queste diverse equazioni di Weierstrass della stessa forma:

$$x = u^2x' + r \qquad \text{e} \qquad y = u^3y' + u^2sx' + t \tag{2.6}$$

con $u, r, s, t \in \bar{K}$ e $u \neq 0$. I coefficienti e le quantità associate alla nuova equazione compaiono in Tabella 2.2. Appare chiaro il motivo per cui il j-invariante è chiamato in tal modo: è un invariante per la classe di isomorfismi della curva e non dipende dalla particolare equazione scelta. In campi algebricamente chiusi, vale anche il viceversa (vedi 2. della Proposizione 2.1.6).

Osservazione 2.1.5. La restrizione a $\mathrm{char}(\bar{K}) \neq 2, 3$ permette di utilizzare la forma più breve dell'equazione che possiamo riscrivere nel modo seguente

$$y^2 = x^3 + Ax + B \tag{2.7}$$

con discriminante e j-invariante

$$\Delta = -16(4A^3 + 27B^2), \qquad j = -1728\frac{(4A)^3}{\Delta}.$$

Osserviamo anche che, in questo caso, l'unico cambio di variabili che conserva questa forma dell'equazione è

$$x = u^2x' \qquad \text{e} \qquad y = u^3y'$$

per qualche $u \in \bar{K}^*$. Quindi i nuovi coefficienti e il nuovo discriminante sono dati da

$$u^4A' = A, \qquad u^6B' = B, \qquad u^{12}\Delta' = \Delta.$$

Ritorniamo alla situazione generale. Sia $P = (x_0, y_0)$ un punto che soddisfa l'equazione $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$. Se P è un punto singolare, allora dall'Esempio 1.1.17 sappiamo che deve valere $\partial_x f(P) = 0 = \partial_y f(P)$. Esistono allora $\alpha, \beta \in \bar{K}$ tali che

$$f(x,y) - f(x_0,y_0) = ((y-y_0) - \alpha(x-x_0))((y-y_0) - \beta(x-x_0)) - (x-x_0)^3. \quad (2.8)$$

Diciamo che il punto singolare P è un *nodo* se $\alpha \neq \beta$. Le rette $y - y_0 = \alpha(x-x_0)$ e $y - y_0 = \beta(x-x_0)$ sono le *tangenti* in P. Diciamo invece che P è una *cuspide* se $\alpha = \beta$. In questo caso la tangente è data dalla retta $y - y_0 = \alpha(x-x_0)$.

Proposizione 2.1.6.

1. *Consideriamo una curva data da un'equazione di Weierstrass. Allora tale curva*
   - *(a) è singolare se e solo se $\Delta = 0$,*
   - *(b) ha un nodo se e solo se $\Delta = 0$ e $c_4 \neq 0$,*
   - *(c) ha una cuspide se e solo se $\Delta = 0 = c_4$.*

   In particolare, esiste al più un punto singolare.
2. *Due curve sono isomorfe su $\bar{K}$ se e solo se hanno lo stesso j-invariante.*
3. *$\forall j_0 \in \bar{K}$, esiste una curva definita su $K(j_0)$ il cui j-invariante è uguale a j_0.*

Dimostrazione. **1(a).** Osserviamo per prima cosa che il punto all'infinito $\mathcal{O}$ non è mai singolare. Sappiamo che il polinomio $F(X,Y,Z)$ dato dall'equazione (2.1) vale 0 in $\mathcal{O}$. Invece se guardiamo la derivata rispetto a Z abbiamo che $\partial_Z F(\mathcal{O}) = 1 \neq 0$, quindi $\mathcal{O}$ non è singolare.
Consideriamo ora l'equazione nella forma (2.4). La curva è non singolare se e solo se esiste un punto (x_0, y_0) che soddisfa $2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0$. In altre parole i punti singolari sono esattamente i punti del tipo $(x_0, 0)$ tali che x_0 è una radice doppia del polinomio cubico $4x^3 + b_2x^2 + 2b_4x + b_6$: questo si verifica se e solo se il suo discriminante è nullo. Poiché il discriminante di un polinomio di grado 3 del tipo $Ax^3 + Bx^2 + Cx + D$ è dato da $18ABCD - 4B^3D + B^2C^2 - 4AC^3 - 27A^2D^2$, sostituendo in esso i coefficienti dell'equazione di Weierstrass nei b_i, si ottiene che il discriminante del polinomio cubico vale 16Δ. Quindi la curva è singolare se e solo se $\Delta = 0$.
1(b). Consideriamo l'equazione (2.2) scritta come $f(x,y) = 0$. Senza perdere di generalità, possiamo supporre che il punto singolare sia $(0,0)$. Infatti una traslazione del tipo $x = x' + x_0$ e $y = y' + y_0$ lascia invariati Δ e c_4 (vedi Tabella 2.2 con $u = 1$). Osserviamo che $a_6 = f(0,0) = 0$, $a_4 = \partial_x f(0,0) = 0$ e $a_3 = \partial_y f(0,0) = 0$. Allora l'equazione si riduce alla forma $f(x,y) = y^2 + a_1xy - a_2x^2 - x^3 = 0$ per la quale $\Delta = 0$ e $c_4 = (a_1^2 + 4a_2)^2$. Per definizione, la curva ha un nodo in $(0,0)$ se la forma quadratica $y^2 + a_1xy - a_2x^2$ ha

fattori distinti, cosa che si verifica se e solo se il discriminante di tale forma non è nullo, i.e. se $a_1^2 + 4a_2 \neq 0$.
1(c). Si procede come per 1(b). ricordando che la curva ha una cuspide in $(0,0)$ se la forma quadratica ha fattori coincidenti, i.e. se $a_1^2 + 4a_2 = 0$.
1. Si conclude la prima parte osservando che un polinomio cubico non può avere due radici doppie. Allora E ha al più un punto singolare.
2. Per la formula (2.6), se due curve sono isomorfe allora hanno lo stesso j-invariante. Per il viceversa, consideriamo le due curve E e E' con equazioni della forma (2.7) e cerchiamo un isomorfismo del tipo $(x, y) = (u^2x', u^3y')$.
Per ipotesi $j(E) = j(E')$ quindi

$$\frac{A^3}{4A^3 + 27B^2} = \frac{A'^3}{4A'^3 + 27B'^2} \qquad \Rightarrow \qquad A^3B'^2 = A'^3B^2.$$

Si hanno tre casi osservando che $\Delta, \Delta' \neq 0$ per definizione di j-invariante:
$A = 0$ (i.e. $j = 0$) allora $B \neq 0$ poiché $\Delta \neq 0$. Quindi $A' = 0$ e per l'isomorfismo prendiamo u tale che $u^6 = B/B'$,
$B = 0$ (i.e. $j = 1728$) allora $A \neq 0$. Quindi $B' = 0$ e prendiamo u tale che $u^4 = A/A'$,
$AB \neq 0$ (i.e. $j \neq 0, 1728$) allora $A'B' \neq 0$ (in caso contrario, se anche solo uno dei due fosse 0, dovrebbero esserlo entrambi contro l'ipotesi di $\Delta' \neq 0$) e prendiamo u tale che $u^4 = A/A'$ e $u^6 = B/B'$.
3. Sia $j \neq 0, 1728$ e consideriamo la curva

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

Per essa $\Delta = j_0^2/(j_0 - 1728)^3$ e $j = j_0$. Per completare la lista aggiungiamo le equazioni $y^2 + y = x^3$ per $j = 0$ con $\Delta = -27$ e $y^2 = x^3 + x$ per $j = 1728$ con $\Delta = -64$.

□

Proposizione 2.1.7. *Se una curva data da un'equazione di Weierstrass è singolare, allora esiste una mappa razionale $\varphi : E \to \mathbb{P}^1$ di grado 1, i.e. la curva è birazionale a $\mathbb{P}^1$.*

Dimostrazione. Supponiamo che il punto singolare sia $(0,0)$ tramite un cambio di variabili e, come ottenuto nella dimostrazione di 1(b). della Proposizione 2.1.6, si ha che $y^2 + a_1xy = x^3 + a_2x^2$. Allora la mappa razionale (non regolare solo nel punto singolare) $E \to \mathbb{P}^1$ tale che $(x, y) \to [x, y]$ ha grado 1 poiché esiste l'inversa (regolare) $\mathbb{P}^1 \to E$ data da $[1, t] \to (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t)$. Essa si ottiene dividendo l'equazione per x^2 e ponendo $t = y/x$: allora $t^2 + a_1t = x + a_2$ e $y = tx$ da cui si osserva anche che x e y sono in $\bar{K}(t)$.

□

Forma di Legendre

Definizione 2.1.8. Un'equazione di Weierstrass è in *forma di Legendre* se può essere scritta come

$$y^2 = x(x-1)(x-\lambda), \tag{2.9}$$

con $\Delta = 16\lambda^2(\lambda-1)^2$ e $c_4 = 16(\lambda^2-\lambda+1)$.

Proposizione 2.1.9. *Sia char*$(K) \neq 2$.

1. *Ogni curva data da un'equazione di Weierstrass è isomorfa su* $\bar{K}$ *a una curva* E_λ *data in forma di Legendre (2.9) per qualche* $\lambda \in \bar{K}$ *tale che* $\lambda \neq 0, 1$.

2. *Il* j*-invariante di* E_λ *è*
$$j(E_\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}.$$

3. *La mappa* $\bar{K} \setminus \{0,1\} \to \bar{K}$ *tale che* $\lambda \to j(E_\lambda)$ *è suriettiva ed è esattamente* $6:1$ *tranne per* $j = 0$ *in cui è* $2:1$ *e per* $j = 1728$ *in cui è* $3:1$ *(eccetto il caso char*$(K) = 3$ *in cui la mappa è* $1:1$ *per* $j = 0 = 1728$*).*

Dimostrazione. **1.** Consideriamo l'equazione di Weierstrass (2.4). Applichiamo la sostituzione $(x, y) \to (x, 2y)$, dividiamo per 4 e fattorizziamo la cubica in x, ottenendo l'equazione $y^2 = (x-e_1)(x-e_2)(x-e_3)$ per qualche $e_1, e_2, e_3 \in \bar{K}$. Poiché il discriminante di un polinomio di grado 3 del tipo $x^3 + Bx^2 + Cx + D$ è dato da $18BCD - 4B^3D + B^2C^2 - 4C^3 - 27D^2$, sostituendo in esso i coefficienti dell'equazione di Weierstrass negli a_i, si ottiene $\Delta = 16(e_1-e_2)^2(e_1-e_3)^2(e_2-e_3)^2 \neq 0$. Allora gli e_i sono tutti distinti. Basta ora applicare la sostituzione $(x, y) = ((e_2-e_1)x' + e_1, (e_2-e_1)^{3/2}y')$ ottenendo l'equazione nella forma di Legendre con $\lambda = (e_3-e_1)/(e_2-e_1) \in \bar{K}$ e $\lambda \neq 0, 1$.
2. Si ottiene come c_4^3/Δ con le quantità date nella Definizione 2.1.8.
3. Usiamo il fatto che il j-invariante classifica una curva con equazione di Weierstrass a meno di isomorfismi (vedi 2. della Proposizione 2.1.6). Supponiamo quindi $j(E_\lambda) = j(E_\mu)$, per cui $E_\lambda \cong E_\mu$. Le rispettive equazioni di Weierstrass in forma di Legendre sono legate dal cambio di variabili $(x, y) = (u^2x' + r, u^3y')$. Poniamo quindi

$$x(x-1)(x-\mu) = \left(x + \frac{r}{u^2}\right)\left(x + \frac{r-1}{u^2}\right)\left(x + \frac{r-\lambda}{u^2}\right)$$

e abbiamo esattamente sei modi diversi per eguagliare i termini lineari. Si ottengono quindi sei possibili valori per μ: $\mu \in \{\lambda,\ 1/\lambda,\ 1-\lambda,\ 1/(1-\lambda),\ \lambda/(\lambda-1),\ (\lambda-1)/\lambda\}$. La mappa $\lambda \to j(E_\lambda)$ è esattamente $6:1$ a meno che due o più di questi valori per μ coincidano.
Eguagliandoli a due a due si vede che questo avviene se e solo se $\lambda \in \{-1, 1/2, 2\}$, i.e. la mappa è $3:1$, oppure se $\lambda^2 - \lambda + 1 = 0$, i.e. la mappa è $2:1$. Dalla 2. si ottiene $j = 1728$

e $j = 0$ rispettivamente.
Infine, se $\text{char}(K) = 3$, l'equazione $j(\lambda) = 0 = 1728$ ha l'unica soluzione $\lambda = -1$.

□

2.1.1 Equazioni di Weierstrass e curve ellittiche

Utilizziamo ora il Teorema di Riemann-Roch per mostrare che ogni curva ellittica può essere descritta da una cubica piana di Weierstrass e, viceversa, che ogni cubica piana di Weierstrass è una curva ellittica.

Proposizione 2.1.10. *Sia E una curva ellittica definita su K.*

1. *Esistono due funzioni $x, y \in K(E)$ tali che la mappa $\varphi : E \to \mathbb{P}^2$ con $\varphi = [x, y, 1]$ è un isomorfismo di E/K nella curva cubica data dall'equazione di Weierstrass $C : \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ con $a_1, a_2, a_3, a_4, a_6 \in K$ che soddisfa $\varphi(\mathcal{O}) = [0, 1, 0]$. Le funzioni x e y sono le* coordinate di Weierstrass *per la curva ellittica E.*

2. *Le equazioni di Weierstrass per la stessa curva ellittica E sono legate e due a due da un cambio lineare di variabili del tipo*

$$(X, Y) = (u^2X' + r, u^3Y' + u^2sX' + t) \qquad \text{con } u \in K^* \text{ e } r, s, t \in K.$$

3. *Viceversa, ogni curva cubica liscia C data da un'equazione di Weierstrass è una curva ellittica definita su K con punto base $\mathcal{O} = [0, 1, 0]$.*

Dimostrazione. **1.** Consideriamo gli spazi $\mathcal{L}(n\{\mathcal{O}\})$ per n intero positivo. Dalla 3. del Corollario 1.8.8 con $g = 1$ abbiamo $\ell(n\{\mathcal{O}\}) = n$ con $\deg(n\{\mathcal{O}\}) = n > 0$, quindi la dimensione di $\mathcal{L}(n\{\mathcal{O}\})$ è esattamente n e osserviamo che $K = \mathcal{L}(0) \subset \mathcal{L}(n\{\mathcal{O}\})$ per ogni n positivo (vedi Osservazione 1.8.5). Consideriamo le funzioni $x, y \in K(E)$ e tramite esse definiamo le basi per questi spazi. Infatti osserviamo che x non può avere in $\mathcal{O}$ un polo semplice perché altrimenti si avrebbe $x \in \mathcal{L}(\{\mathcal{O}\})$ e, poiché E ha genere 1 e $\deg\{\mathcal{O}\} = 1$, per il Corollario 1.8.8 allora $\ell(\{\mathcal{O}\}) = 1$ che implica $x \in K$: assurdo. Quindi x ha esattamente un polo di ordine 2 per cui $\{1, x\}$ è una base per $\mathcal{L}(2\{\mathcal{O}\})$. Analogamente y, scelto linearmente indipendente da $1, x$, non può avere un polo di ordine inferiore a 3 perché altrimenti si avrebbe $y \in \mathcal{L}(2\{\mathcal{O}\})$, per cui $\{1, x, y\}$ è una base per $\mathcal{L}(3\{\mathcal{O}\})$.
Guardiamo ora $\mathcal{L}(6\{\mathcal{O}\})$ che ha dimensione 6. Osserviamo che $1, x, y, x^2, xy, y^2, x^3 \in \mathcal{L}(6\{\mathcal{O}\})$ quindi deve esistere una combinazione lineare nulla con coefficienti $A_1, \ldots, A_7 \in K$ non tutti nulli: $A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$. Notiamo che $A_6A_7 \neq 0$ altrimenti ogni termine avrebbe un polo in $\mathcal{O}$ di ordine diverso e quindi ogni A_i dovrebbe essere nullo (per rispettare la proprietà di ordine di una somma di funzioni). Basta quindi sostituire x con $-A_6A_7x$ e y con $A_6A_7^2y$ e dividere per $A_6^3A_7^4$ per ottenere

un'equazione cubica in forma di Weierstrass. Quindi la mappa $\varphi = [x, y, 1] : E \to \mathbb{P}^2$ ha immagine $\varphi(E) = C$ dove C è una curva descritta da un'equazione di Weierstrass. In particolare φ è un morfismo per la Proposizione 1.5.1 ed è suriettivo per il Teorema 1.5.3. Si ha anche $\varphi(\mathcal{O}) = [0, 1, 0]$ poiché y ha in $\mathcal{O}$ un polo di ordine superiore rispetto a x.
Bisogna verificare ora che φ è un isomorfismo, i.e. una mappa di grado 1 tra curve lisce. Mostriamo che $K(E) = K(x, y)$ allora $\deg \varphi = 1$. Consideriamo la mappa $[x, 1] : \mathbb{P}^1 \to E$ tale che $\varphi^{-1}([1, 0]) = \mathcal{O}$ e utilizzando la relazione (1.1) otteniamo che la mappa ha grado 2, poiché $e_\varphi(\mathcal{O}) = \mathrm{ord}_{\mathcal{O}}(1/x) = 2$. Quindi $[K(E) : K(x)] = 2$ e analogamente, considerando la mappa $[y, 1] : \mathbb{P}^1 \to E$, si ha $[K(E) : K(y)] = 3$. Allora $k = [K(E) : K(x, y)] = 1$ è l'unica possibilità perché k deve dividere sia 2 che 3.
Vediamo ora che C è liscia. Supponiamo per assurdo C singolare, allora per la Proposizione 2.1.7 esiste una mappa razionale $\psi : C \to \mathbb{P}^1$ di grado 1. Allora la composizione $\psi \circ \varphi : E \to \mathbb{P}^1$ è una mappa di grado 1 tra curve lisce quindi per il Corollario 1.5.8 è un isomorfismo. Questo però contraddice il fatto che E ha genere 1 mentre $\mathbb{P}^1$ ha genere 0 (vedi Esempio 1.8.10). Quindi C è liscia e φ di grado 1 è un isomorfismo sempre per il Corollario 1.5.8.
2. Siano $\{x, y\}$ e $\{x', y'\}$ due insiemi di coordinate di Weierstrass su E. Allora in $\mathcal{O}$ sappiamo che x e x' hanno un polo di ordine 2 mentre y e y' hanno un polo di ordine 3. Sappiamo che $\{1, x\}$ e $\{1, x'\}$ sono basi per $\mathcal{L}(2\{\mathcal{O}\})$ e $\{1, x, y\}$ e $\{1, x', y'\}$ sono basi per $\mathcal{L}(3\{\mathcal{O}\})$. Allora esistono le costanti $u_1, u_2 \in K^*$ e $r, s, t \in K$ tali che $x = u_1 x' + r$ e $y = u_2 y' + s_2 x' + t$. Poiché (x, y) e (x', y') sono coordinate che soddisfano equazioni di Weierstrass con coefficiente 1 per Y^2 e X^3, allora $u_1^3 = u_2^2$. Poniamo $u = u_2/u_1$ quindi $u = u_1^{1/2} = u_2^{1/3}$ e sia anche $s = s_2/u^2$. Otteniamo così il cambio di variabili nella forma desiderata.
3. Sia C data da un'equazione di Weierstrass non singolare. Allora il differenziale $\omega \in \Omega_C$ non ha zeri e poli (vedi Proposizione 2.5.1) e $\mathrm{div}(\omega) = 0$. Per la 2. del Corollario 1.8.8 abbiamo $\deg K_C = 2g - 2$ quindi $\deg \mathrm{div}(\omega) = 2g - 2$ implica $g = 1$. Allora C ha genere 1 e, prendendo $[0, 1, 0]$ come punto base, si ottiene che C è una curva ellittica.

□

Corollario 2.1.11. *Sia E/K una curva ellittica con coordinate di Weierstrass x e y. Allora $K(E) = K(x, y)$ e $[K(E) : K(x)] = 2$.*

Dimostrazione. Vedi dimostrazione di 1. della Proposizione 2.1.10.

□

Osservazione 2.1.12. La 2. della Proposizione 2.1.10 non implica che, se due equazioni di Weierstrass hanno coefficienti in K, allora ogni cambio di variabili che porta l'una nell'altra ha coefficienti in K. Prendiamo ad esempio la curva $y^2 = x^3 - x$. Questa ha coefficienti in $\mathbb{Q}$ ed è mappata in se stessa dalla sostituzione $(x, y) \to (-x', iy')$.

2.2 La legge di gruppo "geometrica"

Sia $E \subset \mathbb{P}^2$ una curva ellittica data da un'equazione di Weierstrass. Abbiamo visto che E è composta dai punti (x, y) che soddisfano l'equazione insieme al punto all'infinito $\mathcal{O}$. Sia $L \subset \mathbb{P}^2$ una retta. Allora la retta interseca la curva in esattamente tre punti P, Q, R. Se L è tangente a E allora P, Q, R non sono distinti. La molteplicità di $L \cap E$ è data dal Teorema di Bézout. Si veda [7] I §7 (Corollary 7.8), [6] 5 §3. Definiamo la seguente legge su E.

Legge di composizione 2.2.1. *Siano $P, Q \in E$ e sia L la retta per P e Q. Se $P = Q$, allora L è la retta tangente in P a E.*
Sia R il terzo punto di intersezione di L con E e sia L' la retta passante per R e $\mathcal{O}$. Allora L' interseca E in $R, \mathcal{O}$ e in un terzo punto che denotiamo con $P \oplus Q$.

Proposizione 2.2.2. *La legge di composizione ha le seguenti proprietà, che rendono E un gruppo abeliano con elemento identità $\mathcal{O}$.*

1. *Sia L una retta che interseca E nei punti P, Q, R (non necessariamente distinti). Allora $(P \oplus Q) \oplus R = \mathcal{O}$.*
2. *$P \oplus \mathcal{O} = P$ per ogni $P \in E$.*
3. *$P \oplus Q = Q \oplus P$ per ogni $P, Q \in E$.*
4. *Sia $P \in E$, allora esiste in E un punto, denotato con $\ominus P$, tale che $P \oplus (\ominus P) = \mathcal{O}$.*
5. *$(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ per ogni $P, Q, R \in E$.*
6. *Se E è definita su K, $E(K) = \{(x, y) \in E : (x, y) \in K^2\} \cup \{\mathcal{O}\}$ è un sottogruppo di E.*

Dimostrazione. **1.** Dalla legge di composizione.
2. Se prendiamo $Q = \mathcal{O}$, dalla legge di composizione abbiamo che L e L' coincidono. L interseca E in $P, \mathcal{O}, R$ mentre L' interseca E in $R, \mathcal{O}, P \oplus \mathcal{O}$. Quindi deve essere $P \oplus \mathcal{O} = P$.
3. Ancora dalla legge di composizione si ottiene che la costruzione di $P \oplus Q$ è simmetrica in P e Q.
4. Siano P, Q, R i punti di intersezione tra E e L. Allora dalla 1. e dalla 2. otteniamo che $\mathcal{O} = (P \oplus \mathcal{O}) \oplus R = P \oplus R$. Denotiamo quindi R con $\ominus P$.
5. Sia $(P \oplus Q) \oplus S' = \mathcal{O} = S \oplus S'$ e sia $(S \oplus R) \oplus T' = \mathcal{O}$. Sia poi $(Q \oplus R) \oplus U' = \mathcal{O} = U \oplus U'$ e sia $(P \oplus U) \oplus T'' = \mathcal{O}$. Basta allora vedere che $T' = T''$. Si costruiscono due curve C_1 e C_2 tali che $E \cap C_1 = \{\mathcal{O}, P, Q, R, S, S', U, U', T'\}$ e $E \cap C_2 = \{\mathcal{O}, P, Q, R, S, S', U, U', T''\}$. La Proposizione seguente assicura che $T' = T''$.

Proposizione 2.2.3. *Sia C una cubica irriducibile e siano C_1 e C_2 cubiche. Supponiamo che $C \cap C_1 = \{P_1, \ldots, P_9\}$ e $C \cap C_2 = \{P_1, \ldots, P_8, Q\}$. Allora $Q = P_9$.*

Per una dimostrazione di questa Proposizione e per la costruzione di C_1 e C_2 si veda [6] 5 §6 (Proposition 3, Proposition 4).

6. Se P e Q hanno coordinate in K, allora l'equazione della retta passante per essi ha coefficienti in K. Se poi E è definita su K, allora il terzo punto di intersezione ha coordinate date da una combinazione di coordinate e coefficienti tutti razionali, quindi R è ancora in K. (La formula esplicita per il calcolo è data in 2.2.5).

□

Notazione 2.2.4. Per $m \in \mathbb{Z}$ e $P \in E$, poniamo

$$[m]P = \underbrace{P \oplus \ldots \oplus P}_{m \text{ volte}} \text{ se } m > 0, \qquad [m]P = [-m](-P) = \underbrace{\ominus P \ominus \ldots \ominus P}_{-m \text{ volte}} \text{ se } m < 0,$$

$[0]P = \mathcal{O}$. D'ora in poi, usiamo semplicemente i simboli $+$ e $-$ al posto di $\oplus$ e $\ominus$.

Deriviamo ora le formule esplicite per le operazioni di gruppo su E.
Per prima cosa cerchiamo una formula per la negazione. Sia quindi $P_0 = (x_0, y_0) \in E$, prendiamo la retta per P_0 e $\mathcal{O}$, e cerchiamo il terzo punto di intersezione con E, denotato con $-P_0$, come visto nella 4. della Proposizione 2.2.2. Consideriamo per E l'equazione (2.2) data da $f(x, y) = 0$. La retta L ha equazione $L : x - x_0 = 0$. Sostituiamo quindi x_0 in E al posto di x e il polinomio quadratico che otteniamo $f(x_0, y)$ ha due radici y_0 e y_0'. Allora $-P_0 = (x_0, y_0')$. Possiamo scrivere $f(x_0, y) = (y - y_0)(y - y_0')$ perché il coefficiente di y^2 è 1 ed eguagliamo i coefficienti del termine di grado 1 ottenendo $-y_0 - y_0' = a_1 x_0 + a_3$. Si ha quindi $-P_0 = (x_0, -y_0 - a_1 x_0 - a_3)$.
Cerchiamo ora una formula per l'addizione. Siano quindi $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$. Possiamo escludere il caso $P_2 = -P_1$ e prendiamo la retta per P_1 e P_2 (o la tangente se $P_1 = P_2$) che ha un'equazione del tipo $L : y = \lambda x + \nu$ con λ e ν in funzione delle coordinate di P_1 e P_2 e dei coefficienti a_i. Sostituiamo l'equazione di L in quella di E e otteniamo che $f(x, \lambda x + \nu)$ ha tre radici x_1, x_2, x_3. Allora $P_3 = (x_3, y_3)$ è il terzo punto di $L \cap E$. Sappiamo dalla 1. della Proposizione 2.2.2 che $P_1 + P_2 + P_3 = \mathcal{O}$. Analogamente a prima, scriviamo $f(x, \lambda x + \nu) = -(x - x_1)(x - x_2)(x - x_3)$ con il coefficiente di grado 3 pari a -1, ed eguagliamo i coefficienti di grado 2 ottenendo $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$. Abbiamo quindi una formula per x_3 che sostituiamo nell'equazione di L per ottenere $y_3 = \lambda x_3 + \nu$. Infine per trovare il punto $P_1 + P_2$ scriviamo $P_1 + P_2 = -P_3$ e applichiamo la formula di negazione.

Algoritmo per la legge di gruppo 2.2.5. *Sia E una curva ellittica data dall'equazione di Weierstrass (2.2). Sia $P_i = (x_i, y_i) \in E$ per $i = 0, 1, 2, 3$ e sia $P_1 + P_2 = P_3$.*

1. $-P_0 = (x_0, -y_0 - a_1 x_0 - a_3)$.

2. *Se* $x_1 = x_2$ *e* $y_1 = -y_2 - a_1x_2 - a_3$*, allora* $P_1 + P_2 = \mathcal{O}$.

3. *Sia* $y = \lambda x + \nu$ *la retta per* P_1 *e* P_2 *(o la tangente se* $P_1 = P_2$*), allora*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \qquad y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Se $x_1 \neq x_2$*, allora*

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$

Se invece $x_1 = x_2$*, allora*

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \qquad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

4. *Come caso speciale di 3. abbiamo la* formula di duplicazione *per* $P = (x, y) \in E$

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

con i b_i *dati in Tabella 2.1.*

Definizione 2.2.6. Sia E una curva ellittica singolare. Definiamo allora *parte non singolare di* E l'insieme dei punti non singolari di E, denotato con E_{ns}.

Proposizione 2.2.7. *Sia* E *una curva ellittica con* $\Delta = 0$*, quindi* E *ha un punto singolare che chiamiamo* S*. La legge di composizione 2.2.2 rende* E_{ns} *un gruppo abeliano.*

1. *Se* S *è un nodo, date le rette tangenti a* E *in* S $y = \alpha_1x + \beta_1$ *e* $y = \alpha_2x + \beta_2$*, abbiamo un isomorfismo di gruppi abeliani*

$$E_{ns} \to \bar{K}^*, \qquad (x, y) \to \frac{y - \alpha_1x - \beta_1}{y - \alpha_2x - \beta_2}.$$

2. *Se* S *è una cuspide, data la retta tangente a* E *in* S $y = \alpha x + \beta$*, abbiamo un isomorfismo di gruppi abeliani*

$$E_{ns} \to \bar{K}^+, \qquad (x, y) \to \frac{x - x(S)}{y - \alpha x - \beta}.$$

Dimostrazione. Vediamo che E_{ns} è chiuso rispetto alla legge di composizione. Se una retta L interseca E_{ns} in due punti (non necessariamente distinti), allora L non può contenere il punto S: infatti S ha molteplicità almeno 2 nell'intersezione $E \cap L$ e, se S stesse in L, ci dovrebbero essere almeno 4 punti in $E \cap L$. Ma questo è assurdo per il Teorema di Bézout: vedi [7] I §7 (Corollary 7.8).

Verifichiamo ora che le mappe in 1. e 2. sono biezioni tali che, se $L \cap E_{ns} = \{P_1, P_2, P_3\}$ non necessariamente distinti con $P_i \neq S$, il prodotto delle immagini dei P_i è 1 se S è un nodo oppure la somma delle immagini dei P_i è 0 se S è una cuspide.
Tramite un cambio di variabili supponiamo che il punto singolare sia $(0,0)$: vedi dimostrazione di 1(b). della Proposizione 2.1.6. Otteniamo quindi l'equazione $y^2 + a_1xy = x^3 + a_2x^2$. Sia $s \in \bar{K}$ una radice di $s^2 + a_1s - a_2 = 0$. Sostituiamo $y + sx$ al posto di y eliminando così il termine in x^2 e ottenendo l'equazione $y^2 + (2s + a_1)xy = x^3$. In coordinate omogenee abbiamo quindi $Y^2Z + AXYZ - X^3 = 0$ e $S = [0,0,1]$. E ha un nodo se $A \neq 0$ e una cuspide se $A = 0$.
1. Ricordando la relazione (2.8), vediamo che le rette tangenti in S sono $Y = 0$ e $Y + AX = 0$, quindi la mappa $E_{ns} \to \bar{K}^*$ è data da $[X,Y,Z] \to 1 + AX/Y$. Un altro cambio di variabili $X = A^2(X' - Y')$, $Y = A^3Y'$, $Z = Z'$, porta all'equazione $XYZ - (X - Y)^3 = 0$ che deomogeneizzata rispetto a Y diventa $xz - (x-1)^3 = 0$. In questo nuovo sistema di coordinate, il punto singolare diventa il punto all'infinito. La mappa $E_{ns} \to \bar{K}^*$ è quindi data da $(x,z) \to x$. Esiste la mappa inversa $\bar{K}^* \to E_{ns}$ tale che $t \to (t, (t-1)^3/t)$. Quindi abbiamo una biezione $E_{ns} \xrightarrow{\sim} \bar{K}^*$.
Vediamo ora che, se data una retta L non passante per S tale che L interseca E in tre punti $(x_1,z_1),(x_2,z_2),(x_3,z_3)$, allora $x_1x_2x_3 = 1$. L'equazione di L generica è del tipo $z = ax + b$ quindi le coordinate x_i dei tre punti saranno le radici del polinomio cubico $x(ax+b) - (x-1)^3 = -x^3 + (a+3)x^2 + (b-3)x + 1 = -(x - x_1)(x - x_2)(x - x_3)$. Eguagliando i termini costanti si ha $x_1x_2x_3 = 1$.
2. Se $A = 0$ allora la retta tangente in $S = [0,0,1]$ è $Y = 0$, quindi la mappa $E_{ns} \to \bar{K}^+$ è data da $[X,Y,Z] \to X/Y$. Deomogeneizzando rispetto a Y otteniamo $z - x^3 = 0$ e la mappa è quindi data da $(x,z) \to x$. La mappa inversa $\bar{K}^* \to E_{ns}$ è data da $t \to (t, t^3)$.
I tre punti di intersezione tra la retta L e E si ottengono come radici del polinomio $(ax+b) - x^3 = -(x - x_1)(x - x_2)(x - x_3)$. Eguagliando i coefficienti dei termini in x^2 otteniamo $x_1 + x_2 + x_3 = 0$.

□

2.3 La legge di gruppo "algebrica"

Vediamo ora che è possibile descrivere una legge di gruppo sui punti di una curva ellittica anche utilizzando il Teorema di Riemann-Roch. Ovviamente si ritrova la stessa legge descritta in 2.2.5.

Lemma 2.3.1. *Sia C una curva di genere 1 e siano $P, Q \in C$. Allora $\{P\} \sim \{Q\}$ se e solo se $P = Q$.*

Dimostrazione. Sia $f \in \bar{K}(C)$ tale che $\operatorname{div}(f) = \{P\} - \{Q\}$. Allora $f \in \mathcal{L}(\{Q\})$. Poiché $g = 1$ allora per la 3. del Corollario 1.8.8 sappiamo che $\dim \mathcal{L}(\{Q\}) = 1$. Quindi f è

costante perché $\mathcal{L}(\{Q\})$ contiene le funzioni costanti, allora $P = Q$.

□

Osservazione 2.3.2. Il Lemma 2.3.1 distingue $\mathbb{P}^1$ dalle curve di genere 1. Infatti in $\mathbb{P}^1$, o equivalentemente in una curva di genere 0, esistono due punti P, Q tali che $\{P\} \sim \{Q\}$. Basta sostituire $g = 0$ nella relazione della 3. del Corollario 1.8.8: in questo caso si ottiene che $\dim \mathcal{L}(\{Q\}) = 2$.

Proposizione 2.3.3. *Sia $(E, \mathcal{O})$ una curva ellittica.*

1. *Per ogni $D \in Div_0(E)$ esiste un unico punto $P \in E$ tale che $D \sim \{P\} - \{\mathcal{O}\}$. Definiamo*
$$\sigma : Div_0(E) \to E$$
la mappa che manda D nel suo punto P associato.

2. *σ è suriettiva.*

3. *Siano $D_1, D_2 \in Div_0(E)$. Allora $\sigma(D_1) = \sigma(D_2)$ se e solo se $D_1 \sim D_2$. Quindi σ induce una biezione di insiemi*
$$\sigma : Pic_0(E) \xrightarrow{\sim} E.$$

4. *Sia*
$$\gamma : E \xrightarrow{\sim} Pic_0(E)$$
l'inversa di σ definita da $P \to$ classe di $\{P\} - \{\mathcal{O}\} = [\{P\} - \{\mathcal{O}\}]$. Allora la legge di gruppo indotta da $Pic_0(E)$ usando σ è la legge definita in 2.2.5.

5. *Sia $D = \sum n_P\{P\} \in Div(E)$. Allora D è un divisore principale se e solo se*
$$\sum_{P \in E} n_P = 0 \quad e \quad \sum_{P \in E} [n_P]P = \mathcal{O}.$$
(La prima $\sum$ è l'addizione fra interi, la seconda è l'addizione su E).

Dimostrazione. **1.** Per ipotesi $\deg D = 0$, quindi per la 3. del Corollario 1.8.8 si ha $\dim \mathcal{L}(D + \{\mathcal{O}\}) = 1$. Sia $f \in \bar{K}(E)$ un elemento non nullo di $\mathcal{L}(D + \{\mathcal{O}\})$, allora f è una base. Per definizione, $\mathrm{div}(f) \geq -D - \{\mathcal{O}\}$ e per la 2. della Proposizione 1.6.2 $\deg \mathrm{div}(f) = 0$, allora $\mathrm{div}(f) = -D - \{\mathcal{O}\} + \{P\}$ per qualche $P \in E$. Si ha quindi $D \sim \{P\} - \{\mathcal{O}\}$ che mostra l'esistenza di tale punto. Supponiamo poi che P' sia un altro punto che soddisfa la stessa proprietà. Allora $\{P'\} \sim D + \{\mathcal{O}\} \sim \{P\}$ e si ha $P = P'$ per il Lemma 2.3.1 che mostra l'unicità.
2. Per ogni $P \in E$ si ha $\sigma(\{P\} - \{\mathcal{O}\}) = P$.
3. Poniamo $P_i = \sigma(D_i)$ con $i = 1, 2$. Dalla definizione di σ sappiamo che $\{P_1\} - \{P_2\} \sim$

$(D_1 + \{\mathcal{O}\}) - (D_2 + \{\mathcal{O}\}) = D_1 - D_2$. Se $P_1 = P_2$ allora $D_1 \sim D_2$. Se invece $D_1 \sim D_2$ allora $\{P_1\} \sim \{P_2\}$ e $P_1 = P_2$ per il Lemma 2.3.1.
4. Siano $P, Q \in E$. Basta verificare che $P \oplus Q = \gamma^{-1}(\gamma(P) + \gamma(Q))$.
Sia $f(X, Y, Z) = aX + bY + cZ = 0$ l'equazione della retta L di $\mathbb{P}^2$ che passa per P e Q, e sia R il terzo punto di intersezione di L con E. Sia poi $f'(X, Y, Z) = a'X + b'Y + c'Z = 0$ l'equazione della retta L' di $\mathbb{P}^2$ che passa per R e $\mathcal{O}$. Osserviamo inoltre che la retta $Z = 0$ interseca E nel punto $\mathcal{O}$ con molteplicità 3.
Si ha $\operatorname{div}(f/Z) = \{P\} + \{Q\} + \{R\} - 3\{\mathcal{O}\}$ e $\operatorname{div}(f'/Z) = \{R\} + \{P + Q\} - 2\{\mathcal{O}\} \Rightarrow \operatorname{div}(f'/f) = \{P+Q\} - \{P\} - \{Q\} + \{\mathcal{O}\} = (\{P+Q\} - \{\mathcal{O}\}) - (\{P\} - \{\mathcal{O}\}) - (\{Q\} - \{\mathcal{O}\})$, per cui passando al quoziente si ha $0 = [\{P + Q\} - \{\mathcal{O}\}] - [\{P\} - \{\mathcal{O}\}] - [\{Q\} - \{\mathcal{O}\}]$. Allora $\gamma(P + Q) = \gamma(P) + \gamma(Q)$ e $P \oplus Q = P + Q = \gamma^{-1}(\gamma(P) + \gamma(Q))$, per cui γ è un isomorfismo di gruppi.
5. Dalla 2. della Proposizione 1.6.2 sappiamo che ogni divisore principale ha grado 0, i.e. $\sum n_P = 0$. Sia quindi $D \in \operatorname{Div}_0(E)$, allora per 1. e 3. si ha che $D \sim 0$ se e solo se $\sigma(D) = \mathcal{O}$. Osserviamo che $D = \sum n_P\{P\} \sim 0 \sim \sum n_P(\{P\} - \{\mathcal{O}\})$ poiché $\sum n_P = 0$. Allora $\sigma(D) = \sigma(\sum n_P(\{P\} - \{\mathcal{O}\})) = \sum[n_P]\, \sigma(\{P\} - \{\mathcal{O}\})$ per la proprietà di gruppo in 4. considerando il quoziente. Poiché $\sigma(\{P\} - \{\mathcal{O}\}) = P$, si ottiene il risultato.

□

Osservazione 2.3.4. Riprendendo l'Osservazione 1.6.5 possiamo dire che ad ogni curva ellittica E/K è associata la successione esatta

$$1 \to \bar{K}^* \to \bar{K}(E)^* \xrightarrow{\text{div}} \operatorname{Div}_0(E) \xrightarrow{\sigma} E \to 0$$

dove σ è l'operazione di somma dei punti nel divisore tramite la legge di gruppo su E.

Teorema 2.3.5. *Sia E/K una curva ellittica. Allora la legge di gruppo 2.2.5 definisce due morfismi*

$$\begin{array}{rcl} \oplus : E \times E & \to & E, \\ (P_1, P_2) & \to & P_1 + P_2 \end{array} \qquad \begin{array}{rcl} \ominus : E & \to & E, \\ P & \to & -P. \end{array}$$

Dimostrazione. La mappa $\ominus$ è chiaramente una mappa razionale su E. Poiché E è liscia, per la Proposizione 1.5.1 $\ominus$ è un morfismo.
Consideriamo ora la mappa $\oplus$. Se escludiamo le coppie di punti del tipo (P, P), $(P, -P)$, $(P, \mathcal{O})$, $(\mathcal{O}, P)$, osserviamo che anch'essa è un morfismo: infatti, per tutte le coppie di punti che non presentano questa forma, le relazioni per λ e ν (vedi Legge 2.2.5) sono ben definite, quindi anche $\oplus$ è una mappa razionale ben definita su $E \times E$.
Vediamo cosa accade nelle quattro coppie escluse. Sia $Q \in E$ fissato con $Q \neq \mathcal{O}$. Consideriamo la mappa *traslazione rispetto a Q* $\tau_Q : E \to E$ tale che $\tau_Q(P) = P + Q$. Anch'essa è una mappa razionale su E e per la Proposizione 1.5.1 è un morfismo. Inoltre, poiché

esiste anche l'inversa τ_{-Q} tale che $\tau_{-Q}(P) = P - Q$, allora τ_Q è un isomorfismo. Siano quindi $Q_1, Q_2 \in E$ e siano τ_{Q_1}, τ_{Q_2} le relative traslazioni. Consideriamo la composizione di mappe

$$\phi : E \times E \xrightarrow{\tau_{Q_1} \times \tau_{Q_2}} E \times E \xrightarrow{+} E \xrightarrow{\tau_{-Q_1}} E \xrightarrow{\tau_{-Q_2}} E.$$

Poiché la legge di gruppo è associativa e commutativa (vedi Proposizione 2.2.2), la mappa ϕ agisce sulla coppia (P_1, P_2) nel modo seguente:

$$(P_1, P_2) \xrightarrow{\tau_{Q_1} \times \tau_{Q_2}} (P_1 + Q_1, P_2 + Q_2) \xrightarrow{+} P_1 + Q_1 + P_2 + Q_2 \xrightarrow{\tau_{-Q_1}} P_1 + P_2 + Q_2 \xrightarrow{\tau_{-Q_2}} P_1 + P_2.$$

ϕ è quindi una mappa razionale che agisce esattamente come la mappa $\oplus$ sulle coppie di punti in cui entrambe sono definite: infatti anche ϕ è un morfismo se escludiamo le coppie del tipo $(P - Q_1, P - Q_2)$, $(P - Q_1, -P - Q_2)$, $(P - Q_1, -Q_2)$, $(-Q_1, P - Q_2)$. I punti Q_1, Q_2 sono arbitrari, quindi al variare di essi otteniamo un insieme finito di mappe razionali $\phi_1, \ldots, \phi_n : E \times E \to E$ con le proprietà:
• ϕ_1 è la mappa di addizione definita nella 3. della Legge 2.2.5,
• per ogni $(P_1, P_2) \in E \times E$, qualche ϕ_i è definita in (P_1, P_2),
• se ϕ_i e ϕ_j sono entrambe definite in (P_1, P_2), allora $\phi_i(P_1, P_2) = \phi_j(P_1, P_2)$.
In tal modo la mappa $\oplus$ è definita su tutto $E \times E$ ed è un morfismo.

□

2.4 Isogenie

Definizione 2.4.1. Siano $(E_1, \mathcal{O})$, $(E_2, \mathcal{O})$ curve ellittiche. Un'*isogenia* tra E_1 a E_2 è un morfismo $\varphi : E_1 \to E_2$ tale che $\varphi(\mathcal{O}) = \mathcal{O}$. E_1 e E_2 sono *isogene* se esiste un'isogenia tra E_1 a E_2 con $\varphi(E_1) \neq \{\mathcal{O}\}$.

Osservazione 2.4.2. La traslazione τ_Q rispetto a un punto $Q \in E$ definita nella dimostrazione del Teorema 2.3.5 è un isomorfismo, come abbiamo visto, perché τ_{-Q} è un'inversa. Inoltre è un'isogenia solo quando $Q = \mathcal{O}$. Se consideriamo un morfismo arbitrario α tra E_1 e E_2 curve ellittiche, allora la composizione $\varphi = \tau_{-\alpha(\mathcal{O})} \circ \alpha$ è un'isogenia poiché $\varphi(\mathcal{O}) = \mathcal{O}$. Questo implica che ogni morfismo α tra curve ellittiche può essere scritto come $\alpha = \tau_{\alpha(\mathcal{O})} \circ \varphi$, composizione di un'isogenia e di una traslazione.

Osservazione 2.4.3. La definizione più generale di isogenia è data su due punti base distinti $\mathcal{O}, \mathcal{O}'$ per le due curve: si definisce quindi isogenia un morfismo tale che $\varphi(\mathcal{O}) = \mathcal{O}'$. Grazie all'Osservazione 2.4.2 è però possibile comporre con una traslazione per riportarsi al caso $\varphi(\mathcal{O}) = \mathcal{O}$.

Osservazione 2.4.4. Riprendiamo alcune informazioni dal Capitolo 1 riguardo alle mappe tra curve.
• Dal Teorema 1.5.3 segue che un'isogenia è tale che $\varphi(E_1) = \{\mathcal{O}\}$ oppure $\varphi(E_1) = E_2$.

• Escludendo l'isogenia nulla $\varphi(P) = \mathcal{O}\ \forall P \in E_1$, ogni altra isogenia è una mappa finita.
• Dall'Osservazione 1.5.4 si ottiene l'iniezione $\varphi^* : \bar{K}(E_2) \to \bar{K}(E_1)$ tra i campi delle funzioni.
• Analogamente alla Definizione 1.5.6, si ha $\deg \varphi = [\bar{K}(E_1) : \varphi^*(\bar{K}(E_2))]$. Sia poi per convenzione $\deg \varphi_0 = 0$, allora vale $\deg(\psi \circ \varphi) = \deg \psi \deg \varphi$ per ogni $\varphi : E_1 \to E_2$ e $\psi : E_2 \to E_3$.

Poiché le curve ellittiche sono gruppi abeliani, anche le mappe tra esse formano un gruppo. Denotiamo l'insieme delle isogenie tra E_1 a E_2 con $\mathrm{Hom}(E_1, E_2)$. La somma tra due isogenie φ, ψ è definita come $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$ e il Teorema 2.3.5 implica che $\varphi + \psi$ è un morfismo, quindi un'isogenia. Allora $\mathrm{Hom}(E_1, E_2)$ è un gruppo.
Se $E_1 = E_2$, possiamo ancora comporre le isogenie. Quindi definiamo, per una curva ellittica E, l'anello $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ detto *anello degli endomorfismi di* E, che è un invariante molto importante di E. L'addizione è definita come in $\mathrm{Hom}(E_1, E_2)$ e la moltiplicazione è data dalla composizione $(\varphi\psi)(P) = \varphi(\psi(P))$. Gli elementi invertibili di $\mathrm{End}(E)$ formano il *gruppo degli automorfismi*, denotato con $\mathrm{Aut}(E)$.
Il seguente Teorema motiva il nome dato al gruppo delle isogenie.

Teorema 2.4.5. *Sia $\varphi : E_1 \to E_2$ un'isogenia. Allora $\varphi(P+Q) = \varphi(P) + \varphi(Q)$ per ogni $P, Q \in E_1$.*

Dimostrazione. Se $\varphi(P) = \mathcal{O}$ per ogni $P \in E_1$, cioè φ è l'isogenia nulla, allora il risultato è già verificato. Supponiamo quindi che φ sia una mappa finita. Allora, come visto nell'Osservazione 1.6.9, φ induce un omomorfismo $\varphi_* : \mathrm{Pic}_0(E_1) \to \mathrm{Pic}_0(E_2)$. Abbiamo poi definito, nella 4. della Proposizione 2.3.3, un isomorfismo di gruppi $\gamma_i : E_i \xrightarrow{\sim} \mathrm{Pic}_0(E_i)$. Poiché $\varphi(\mathcal{O}) = \mathcal{O}$, allora il diagramma

$$\begin{array}{ccc} E_1 & \xrightarrow{\gamma_1} & \mathrm{Pic}_0(E_1) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi_*} \\ E_2 & \xrightarrow{\gamma_2} & \mathrm{Pic}_0(E_2) \end{array}$$

commuta. Poiché $\gamma_1, \gamma_2, \varphi_*$ sono omomorfismi di gruppo e i γ_i sono invertibili, allora anche $\varphi = \gamma_2^{-1} \circ \varphi_* \circ \gamma_1$ è un omomorfismo.

□

Corollario 2.4.6. *Sia $\varphi : E_1 \to E_2$ un'isogenia non nulla. Allora $\ker \varphi = \varphi^{-1}(\mathcal{O})$ è un gruppo finito.*

Dimostrazione. Per il Teorema 2.4.5 $\ker \varphi$ è un sottogruppo di E_1 e per la relazione (1.1) è finito, con ordine al più $\deg \varphi$.

□

Definizione 2.4.7. E_1 e E_2 sono *isomorfe* se esistono due isogenie $\varphi : E_1 \to E_2$ e $\psi : E_2 \to E_1$ tali che $\varphi \circ \psi = id_{E_2}$ e $\psi \circ \varphi = id_{E_1}$. Osserviamo che l'isomorfismo di curve ellittiche è un concetto più forte rispetto all'isomorfismo di curve algebriche: è infatti un isomorfismo di gruppi abeliani.

Riprendiamo ora in considerazione la mappa $[m] : E \to E$ definita nella Notazione 2.2.4, detta *moltiplicazione per m*. Per il Teorema 2.3.5 $[m]$ è un morfismo e anche un'isogenia perché fissa $\mathcal{O}$. Se E è definita su K, anche $[m]$ è definita su K.

Osservazione 2.4.8. Grazie alla definizione dell'operazione nel gruppo $\mathrm{Hom}(E_1, E_2)$, si ha che $\varphi + \varphi = [2] \circ \varphi$ e più in generale per m termini $\varphi + \ldots + \varphi = [m] \circ \varphi$. Denotiamo con $[0]$ l'isogenia nulla.

Proposizione 2.4.9.

1. *Sia E/K una curva ellittica e sia $m \in \mathbb{Z}$ con $m \neq 0$. Allora la mappa di moltiplicazione per m non è costante.*

2. *Siano E_1, E_2 curve ellittiche, allora il gruppo $Hom(E_1, E_2)$ è uno $\mathbb{Z}$-modulo (i.e. un gruppo abeliano) libero da torsione.*

3. *Sia E una curva ellittica, allora l'anello $End(E)$ è un dominio d'integrità con caratteristica 0 (non necessariamente commutativo).*

Dimostrazione. **1.** Per prima cosa vediamo che vale sempre $[2] \neq [0]$. Dalla formula di duplicazione data nella 4. di 2.2.5 osserviamo che, se un punto $P = (x, y) \in E$ ha ordine 2, allora $4x^3 + b_2x^2 + 2b_4x + b_6 = 0$. Se $\mathrm{char}(K) = 2$ allora l'unica possibilità per avere $[2] = [0]$ è che valga $b_2 = b_6 = 0$ che implica però $\Delta = 0$. Se invece $\mathrm{char}(K) \neq 2$ allora esiste solo un numero finito di tali punti. Possiamo ricondurci quindi al caso m dispari poiché vale $[mn] = [m] \circ [n]$.
Sia $\mathrm{char}(K) \neq 2$ allora si verifica che $h(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$ non divide $g(x) = x^4 - b_4x^2 - 2b_6x - b_8$ (rispettivamente denominatore e numeratore della formula di duplicazione). Se ciò accadesse, si avrebbe ancora $\Delta = 0$. Possiamo quindi trovare un $x_0 \in \bar{K}$ che sia uno zero per h di ordine superiore rispetto a g. Scegliamo poi $y_0 \in \bar{K}$ tale che $P_0 = (x_0, y_0) \in E$. Allora la formula di duplicazione implica $[2]P_0 = \mathcal{O}$ e quindi E ha un punto non banale P_0 di ordine 2. Per un intero dispari $m = 2k + 1$ si ha $[m]P_0 = [2k]P_0 + P_0 = P_0 \neq \mathcal{O}$, quindi $[m] \neq [0]$.
Per $\mathrm{char}(K) = 2$ si cerca un punto di ordine 3 ricavando la *formula di triplicazione* e si procede poi analogamente.
2. Basta verificare che l'unico elemento di torsione è dato dall'isogenia nulla. Supponiamo $\varphi \in \mathrm{Hom}(E_1, E_2)$ e $m \in \mathbb{Z}$ tale che $[m] \circ \varphi = [0]$. Passando ai gradi si ha $\deg[m] \deg \varphi = 0$ quindi $m = 0$ oppure $\deg[m] \geq 1$ per la 1. E in tal caso deve valere $\varphi = [0]$.

3. Per la 2. otteniamo subito che la caratteristica è 0. Vediamo ora che non esistono divisori dello zero. Siano $\varphi, \psi \in \mathrm{End}(E)$ tali che $\varphi \circ \psi = [0]$. Allora passando ai gradi si ha $\deg\varphi \deg\psi = 0$ da cui segue $\varphi = [0]$ oppure $\psi = [0]$.

□

Osservazione 2.4.10. Supponiamo $\mathrm{char}(K) = 0$. Allora la mappa $[\ ] : \mathbb{Z} \to \mathrm{End}(E)$ definisce l'isomorfismo $\mathrm{End}(E) \cong \mathbb{Z}$.

Definizione 2.4.11. Sia E una curva ellittica e sia $m \in \mathbb{Z}$ con $m > 0$. Il *sottogruppo di m-torsione di E*, denotato con $E[m]$, è l'insieme dei punti di E di ordine m:

$$E[m] = \{P \in E : [m]P = \mathcal{O}\}.$$

Il *sottogruppo di torsione di E*, denotato con E_{tors}, è l'insieme dei punti di ordine finito:

$$E_{\mathrm{tors}} = \bigcup_{m=1}^{\infty} E[m].$$

2.5 Differenziale invariante

Proposizione 2.5.1. *Sia E una curva ellittica. Allora il differenziale invariante ω definito in (2.3) associato all'equazione di Weierstrass di E è olomorfo e non nullo, i.e.* $\mathrm{div}(\omega) = 0$.

Dimostrazione. Basta dimostrare che ω non ha zeri e poli per alcun punto P di E. Consideriamo $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$. Sia $P = (x_0, y_0) \in E$, allora $\omega = d(x - x_0)/\partial_y f = -d(y - y_0)\partial_x f$. P non può essere un polo altrimenti si avrebbe $\partial_x f(P) = \partial_y f(P) = 0$, quindi P sarebbe un punto singolare di E. Consideriamo la mappa $E \to \mathbb{P}^1$ di grado 2 tale che $[x, y, 1] \to [x, 1]$. Allora $\mathrm{ord}_P(x - x_0) \leq 2$, per cui si hanno due casi: $\mathrm{ord}_P(x - x_0) = 1$ oppure $\mathrm{ord}_P(x - x_0) = 2$ che si ha se e solo se il polinomio quadratico $f(x_0, y)$ ha una radice doppia, i.e. $\partial_y f(P) = 0$. In entrambi i casi, utilizzando la 5. della Proposizione 1.7.2, si ottiene: $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(x - x_0) - \mathrm{ord}_P(\partial_y f) - 1 = 0$. Quindi $\mathrm{div}(\omega) = 0$.

□

La seguente Proposizione mostra perché il differenziale è invariante.

Proposizione 2.5.2. *Sia E una curva ellittica e sia ω il suo differenziale. Sia poi $Q \in E$ e sia τ_Q la mappa di traslazione rispetto a Q. Allora $\tau_Q^*\omega = \omega$.*
(Per la definizione di $\tau_Q^* : \Omega_E \to \Omega_E$ si veda 1.7.1).

Dimostrazione. Poiché sappiamo che Ω_E è un $\bar{K}(E)$-spazio vettoriale di dimensione 1 (vedi 1. della Proposizione 1.7.2), allora esiste una funzione $\alpha_Q \in \bar{K}(E)^*$ dipendente da Q tale che $\tau_Q^*\omega = \alpha_Q\omega$. Osserviamo che $\alpha_Q \neq 0$ poiché τ_Q è un isomorfismo. Guardiamo il divisore: $\mathrm{div}(\alpha_Q) = \mathrm{div}(\tau_Q^*\omega) - \mathrm{div}(\omega) = \tau_Q^*\mathrm{div}(\omega) - \mathrm{div}(\omega)$ per la 2. della Proposizione 1.6.8, e per la Proposizione 2.5.1 $\mathrm{div}(\alpha_Q) = 0$ poiché $\mathrm{div}(\omega) = 0$. Allora α_Q è costante per la 1. della Proposizione 1.6.2, i.e. $\alpha_Q \in \bar{K}^*$. Consideriamo ora la mappa $f : E \to \mathbb{P}^1$ tale che $Q \to [\alpha_Q, 1]$. Possiamo esprimere α_Q come una funzione razionale in $x(Q)$ e $y(Q)$ osservando il seguente fatto: la mappa τ_Q^* intuitivamente lega il differenziale ω_{P+Q} al differenziale ω_P in cui $x(Q)$ e $y(Q)$ sono considerate costanti. Per questo f è una mappa razionale e non è suriettiva perché $[1, 0], [0, 1] \notin f(E)$. Allora, per la Proposizione 1.5.1 e per il Teorema 1.5.3, f è costante. Per questo α_Q non dipende da Q, i.e. $\alpha_Q = \alpha_{\mathcal{O}} = 1$ per ogni $Q \in E$.

□

Vediamo ora una proprietà importante del differenziale di una curva ellittica che consiste nel rendere lineare la legge di addizione.

Teorema 2.5.3. *Siano E_1 e E_2 curve ellittiche e sia ω il differenziale invariante su E_2. Siano poi $\varphi, \psi : E_1 \to E_2$ isogenie. Allora $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$.*
Osserviamo che il primo segno + indica l'addizione in $Hom(E_1, E_2)$ data dalla legge di gruppo su E_2, il secondo invece indica l'addizione tra differenziali nello spazio Ω_{E_1}.

Dimostrazione. Si rimanda a [16] III.5 (Theorem 5.2).

□

Corollario 2.5.4. *Sia ω il differenziale invariante su una curva ellittica E. Sia $m \in \mathbb{Z}$. Allora $[m]^*\omega = m\omega$.*

Dimostrazione. La relazione vale per $m = 0$, poiché $[0]$ è la mappa costante, e vale per $m = 1$, poiché $[1]$ è la mappa identità. Usiamo la proprietà del Teorema 2.5.3 con $\varphi = [m]$ e $\psi = [1]$. Otteniamo $[m+1]^*\omega = [m^*]\omega + \omega$. Per induzione quindi si ottiene la formula.

□

2.6 Isogenia duale

Sia $\varphi : E_1 \to E_2$ un'isogenia non costante. Abbiamo visto nell'Osservazione 1.6.9 che φ induce una mappa $\varphi^* : \mathrm{Pic}_0(E_2) \to \mathrm{Pic}_0(E_1)$. Sappiamo inoltre dalla 4. della Proposizione 2.3.3 che esiste un isomorfismo di gruppi $\gamma_i : E_i \xrightarrow{\sim} \mathrm{Pic}_0(E_i)$ per $i = 1, 2$. Otteniamo quindi un omomorfismo tra E_2 e E_1 tramite la composizione

$$E_2 \xrightarrow{\gamma_2} \mathrm{Pic}_0(E_2) \xrightarrow{\varphi^*} \mathrm{Pic}_0(E_1) \xrightarrow{\gamma_1^{-1}} E_1. \tag{2.10}$$

Sia $Q \in E_2$ e sia $P \in E_1$ tale che $\varphi(P) = Q$. Allora posto $m = \deg \varphi$ si ha

$$(\gamma_1^{-1} \circ \varphi^* \circ \gamma_2)(Q) = [m](P). \tag{2.11}$$

Definizione 2.6.1. L'isogenia descritta nella relazione (2.11) con $\hat{\varphi} : E_2 \to E_1$ tale che $\hat{\varphi} \circ \varphi = [\deg \varphi]$ è detta *isogenia duale a* φ. Si pone $\hat{\varphi} = [0]$ se $\varphi = [0]$.

Vediamo ora le proprietà di questa nuova isogenia.

Teorema 2.6.2. *Sia $\varphi : E_1 \to E_2$ un'isogenia.*

1. *L'isogenia duale $\hat{\varphi}$ è unica.*
2. *Sia $m = \deg \varphi$. Allora $\hat{\varphi} \circ \varphi = [m]$ su E_1 e $\varphi \circ \hat{\varphi} = [m]$ su E_2.*
3. *Sia $\lambda : E_2 \to E_3$ un'altra isogenia. Allora $\widehat{\lambda \circ \varphi} = \hat{\varphi} \circ \hat{\lambda}$.*
4. *Sia $\psi : E_1 \to E_2$ un'altra isogenia. Allora $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$.*
5. *Per ogni $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ e $\deg[m] = m^2$.*
6. $\deg \hat{\varphi} = \deg \varphi$.
7. $\hat{\hat{\varphi}} = \varphi$.

Dimostrazione. Assumiamo che tutte le isogenie siano non costanti, altrimenti tutte le proprietà sono banali.
1. Supponiamo che esistano due isogenie $\hat{\varphi}$ e $\hat{\varphi}'$ che soddisfano la proprietà. Allora si ha che $(\hat{\varphi} - \hat{\varphi}') \circ \varphi = [m] - [m] = [0]$. Poiché φ non è costante, allora per il Teorema 1.5.3 $\hat{\varphi} - \hat{\varphi}'$ deve essere costante. Quindi $\hat{\varphi} = \hat{\varphi}'$.
2. La prima relazione è data dalla definizione di $\hat{\varphi}$. Per la seconda, consideriamo $(\varphi \circ \hat{\varphi}) \circ \varphi = \varphi \circ [m] = [m] \circ \varphi$. Poiché φ è non costante, si ha il risultato.
3. Sia $n = \deg \lambda$. Allora $(\hat{\varphi} \circ \hat{\lambda}) \circ (\lambda \circ \varphi) = \hat{\varphi} \circ [n] \circ \varphi = [n] \circ \hat{\varphi} \circ \varphi = [nm]$. Per la 2. si ha il risultato.
4. Consideriamo per $i = 1, 2$ le coordinate di Weierstrass $x_i, y_i \in K(E_i)$ ricordando che $K(E_i) = K(x_i, y_i)$ per il Corollario 2.1.11. Indichiamo per semplicità $K(E_i)$ con K_i. Consideriamo E_2 definita su K_1, allora l'isogenia φ è tale che $\varphi(x_1, y_1) \in E_2(K_1)$. Analogamente questo vale per $\psi(x_1, y_1)$ e $(\varphi + \psi)(x_1, y_1)$. Consideriamo ora il divisore

$$D = \operatorname{div}((\varphi + \psi)(x_1, y_1)) - \operatorname{div}(\varphi(x_1, y_1)) - \operatorname{div}(\psi(x_1, y_1)) + \{\mathcal{O}\}$$

con $D \in \operatorname{Div}_{K_1}(E_2)$. Per la definizione dell'operazione in $\operatorname{Hom}(E_1, E_2)$, si ha che $D = \{\mathcal{O}\}$. Quindi per la 5. della Proposizione 2.3.3 si ha che $D \sim 0$. Allora esiste $f \in K_1(E_2) = K(x_1, y_1, x_2, y_2)$ tale che $D = \operatorname{div}(f)$ se f è considerata come funzione in x_2, y_2.

Analogamente al ragionamento appena descritto, guardiamo ora f come una funzione in x_1, y_1, quindi guardiamo f come funzione in $K_2(E_1)$, considerando E_1 definita su K_2. Supponiamo che esista $P_1 \in E_1(\overline{K_2})$ tale che $\varphi(P_1) = (x_2, y_2)$. Guardando l'espressione di D e in particolare guardando il termine negativo $-\mathrm{div}(\varphi(x_1, y_1))$, notiamo che f ha un polo in P_1, i.e. f ha un polo se le coordinate di E_1 e E_2 sono tali che $(x_2, y_2) = \varphi(P_1)$. Analogamente osserviamo che f ha un polo in P_1 se $(x_2, y_2) = \psi(P_1)$ e f ha uno zero in P_1 se $(x_2, y_2) = (\varphi + \psi)(P_1)$. Guardiamo allora $D = \mathrm{div}(f)$ come funzione solo di x_1, y_1, poniamo $(x_2, y_2) = P_2$ e otteniamo la forma

$$D = (\varphi + \psi)^*(\{P_2\}) - \varphi^*(\{P_2\}) - \psi^*(\{P_2\}) + \sum n_i\{Q_i\}$$

con $D \in \mathrm{Div}_{\overline{K_2}}(E_1)$ e dove i Q_i sono in $E_1(\bar{K})$, i.e. $\sum n_i\{Q_i\} \in \mathrm{Div}_{\bar{K}}(E_1)$. Considerando la costruzione dell'isogenia duale vista in (2.10), vediamo che all'espressione per D è associato il punto

$$R = \widehat{(\varphi + \psi)}(P_2) - \hat{\varphi}(P_2) - \hat{\psi}(P_2)$$

che non può dipendere da P_2 poiché $D = \mathcal{O}$, quindi $R \in E_1(\bar{K})$. Poniamo $P_2 = \mathcal{O}$ e per le proprietà di isogenia abbiamo che $(\widehat{(\varphi + \psi)} - \hat{\varphi} - \hat{\psi})(P_2) = \mathcal{O} = [0](P_2)$. Allora $\widehat{(\varphi + \psi)} - \hat{\varphi} - \hat{\psi}$ deve essere costante cioè vale il risultato.

5. Per $m = 0, 1$ il risultato vale. Usiamo la 4. con $\varphi = [m]$ e $\psi = [1]$, quindi otteniamo $\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]}$. Per induzione si ottiene subito che $\widehat{[m]} = [m]$ per ogni m.
Sia ora $d = \deg[m]$, allora per definizione $[d] = \widehat{[m]} \circ [m] = [m^2]$ per la proprietà appena verificata. Poiché l'anello degli endomorfismi di una curva ellittica è uno $\mathbb{Z}$-modulo libero da torsione per la 2. e la 3. della Proposizione 2.4.9, allora $d = m^2$.

6. Per la 5. e la 2. si ha $m^2 = \deg[m] = \deg(\varphi \circ \hat{\varphi}) = \deg\varphi \deg\hat{\varphi} = m \deg\hat{\varphi}$. Allora $m = \deg\hat{\varphi}$.

7. Per la 2., la 5. e la 3. si ha $\hat{\varphi} \circ \varphi = [m] = \widehat{[m]} = \widehat{\hat{\varphi} \circ \varphi} = \hat{\varphi} \circ \hat{\hat{\varphi}}$. Si ottiene quindi il risultato.

□

Corollario 2.6.3. *Sia E una curva ellittica e sia $m \in \mathbb{Z}$ con $m \neq 0$ in K, i.e. $\mathrm{char}(K) = 0$ oppure $\mathrm{char}(K) = p > 0$ tale che $p \nmid m$. Allora*

$$E[m] = \ker[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Dimostrazione. Dalla 5. del Teorema 2.6.2 sappiamo che $\deg[m] = m^2$ quindi $[m]$ è una mappa finita separabile. Inoltre è anche non ramificata poiché $\#[m]^{-1}(Q) = \#[-m](Q)$ è costante per ogni $Q \in E$, in particolare $\#[-m](Q) = \deg[m]$. Se prendiamo $Q = \mathcal{O}$ abbiamo quindi $\#[-m](\mathcal{O}) = \#\ker[m] = \deg[m]$, cioè $\#E[m] = m^2$. Per ogni d che divide m analogamente si ha $\#E[d] = d^2$. Allora l'unica possibilità per scrivere $E[m]$ come prodotto di gruppi ciclici è $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

□

Osservazione 2.6.4. Il gruppo di Galois $G_{\bar{K}/K}$ agisce su $E[m]$: infatti, se $[m]P = \mathcal{O}$, allora $[m](P^\sigma) = ([m]P)^\sigma = \mathcal{O}^\sigma = \mathcal{O}$. Otteniamo quindi la rappresentazione

$$G_{\bar{K}/K} \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

scegliendo una base opportuna per $E[m]$.

2.7 Automorfismi

Mostriamo quanto sia piuttosto semplice ricavare la struttura del gruppo degli automorfismi di una curva ellittica. Al contrario, molto meno banale è la struttura dell'anello degli endomorfismi di E per la quale si rimanda a [16] III.9.

Teorema 2.7.1. *Sia E/K una curva ellittica, allora il gruppo $Aut(E)$ è finito con ordine che divide* 24*. Precisamente l'ordine è*

$$\begin{array}{cl} 2 & \text{se } j \neq 0, 1728 \\ 4 & \text{se } j = 1728 \text{ e } \mathrm{char}(K) \neq 2, 3 \\ 6 & \text{se } j = 0 \text{ e } \mathrm{char}(K) \neq 2, 3 \\ 12 & \text{se } j = 0 = 1728 \text{ e } \mathrm{char}(K) = 3. \end{array}$$

Dimostrazione. Consideriamo l'equazione di Weierstrass in forma di Legendre (2.9). Abbiamo visto nella 3. della Proposizione 2.1.9 che esiste una permutazione in Σ_3 che manda $\{0, 1, \lambda\}$ in $\{0, 1, \lambda\}$ in qualche ordine e abbiamo visto che l'orbita di λ è $\Lambda = \{\lambda,\ 1/\lambda,\ 1-\lambda,\ 1/(1-\lambda),\ \lambda/(\lambda-1),\ (\lambda-1)/\lambda\}$.
Sia $\mathrm{char}(K) \neq 3$. Sicuramente l'automorfismo *id* e l'automorfismo dato dal cambio di variabili $(x, y) = (x', -y')$ fissano le tre radici. In particolare questi sono gli unici due elementi in $\mathrm{Aut}(E)$ se $\lambda \neq \mu$ per ogni $\mu \in \Lambda \setminus \{\lambda\}$.
Supponiamo ora $\lambda = \mu$ per un certo μ come definito sopra. Abbiamo visto che λ coincide con un altro elemento della sua orbita se $\lambda \in \{-1, 1/2, 2\}$, i.e. $j = 1728$. Quindi gli automorfismi possibili, considerando le due possibilità $y = \pm y'$, sono 4.
Supponiamo invece che λ coincida con altri due elementi della sua orbita: abbiamo visto che questo accade per λ tale che $\lambda^2 - \lambda + 1 = 0$, i.e. $j = 0$. Gli automorfismi possibili allora sono 6.
Se $\mathrm{char}(K) = 3$ e $\lambda = -1$, allora tutti gli elementi dell'orbita coincidono, quindi gli automorfismi possibili sono 12.

□

Capitolo 3

Il gruppo dei punti razionali su campi locali

Notazione. Sia v una valutazione discreta su un campo K, vale a dire che v è una mappa $v : K^* \to \mathbb{Z}$ tale che $v(xy) = v(x) + v(y)$ (i.e. v è un omomorfismo di gruppi) e $v(x+y) \geq \min\{v(x), v(y)\}$ per ogni $x, y \in K^*$. Spesso si estende v a tutto K ponendo $v(0) = \infty$.
Sia K un campo locale, i.e. K è il completamento di un campo globale rispetto a una valutazione discreta v. Sono campi globali i campi di numeri algebrici, i.e. le estensioni algebriche finite su $\mathbb{Q}$, e i campi delle funzioni di curve algebriche su un campo finito, i.e. le estensioni finite di $\mathbb{F}_p(T)$.
Siano: R l'anello degli interi di K: $R = \{x \in K : v(x) \geq 0\}$;
R^* il gruppo delle unità di R: $R^* = \{x \in K : v(x) = 0\}$;
$\mathfrak{m}$ l'ideale massimale di R;
π un parametro uniformizzante per R, i.e. $\mathfrak{m} = \pi R$;
$k = R/\mathfrak{m}$ il campo dei residui di R.
Supponiamo che v sia normalizzata quindi $v(\pi) = 1$.
Assumiamo che K e k siano campi perfetti.

3.1 Equazioni di Weierstrass minime

Sia E/K una curva ellittica, consideriamo l'equazione di Weierstrass (2.2). La sostituzione $(x, y) \to (u^{-2}x', u^{-3}y')$ porta a una nuova equazione in cui i coefficienti sono del tipo $u^i a_i$. Se scegliamo quindi u divisibile per una potenza sufficientemente grande di π, otteniamo un'equazione di Weierstrass con tutti i coefficienti in R. Osserviamo che anche il discriminante è tale che $v(\Delta) \geq 0$. Poiché v è discreta, possiamo scegliere tra tutte le equazioni di Weierstrass a coefficienti in R quella che minimizza il valore di $v(\Delta)$.

Definizione 3.1.1. Si dice *equazione di Weierstrass minima per E rispetto a v* l'e-

quazione per cui $v(\Delta)$ è minimizzato rispettando la condizione $a_i \in R$. Questo valore minimo di $v(\Delta)$ è detto *valutazione minima del discriminante di E rispetto a v*.

Osservazione 3.1.2. Supponiamo di non sapere se una certa equazione è minima. Vale sicuramente che $\Delta \in R$ poiché $a_i \in R$ per ogni i. Allora tramite il cambio di coordinate descritto in Tabella 2.2, possiamo ottenere una nuova equazione. Per essa valgono: $\Delta' = u^{-12}\Delta,\ c_4' = u^{-4}c_4,\ c_6' = u^{-6}c_6$ con $\Delta', c_4', c_6' \in R$.
Osserviamo quindi che $v(\Delta)$ resta minimo se $v(\Delta) < 12$ perché in tal caso $v(\Delta') \notin R$. Lo stesso vale per c_4 e c_6. Quindi se $0 \leq v(\Delta) < 12$ oppure $0 \leq v(c_4) < 4$ oppure $0 \leq v(c_6) < 6$ allora l'equazione è minima.
Se $\mathrm{char}(K) \neq 2, 3$ vale anche il viceversa: l'equazione è minima se e solo se $0 \leq v(\Delta) < 12$.

Proposizione 3.1.3. *Sia E/K una curva ellittica.*

1. *E ha un'equazione di Weierstrass minima.*
2. *L'equazione di Weierstrass minima è unica a meno di cambi di coordinate del tipo $x = u^2x' + r$ e $y = u^3y' + u^2sx' + t$ con $u \in R^*$ e $r, s, t \in R$.*
3. *Il differenziale invariante ω associato all'equazione di Weierstrass minima è unico a meno di unità di R.*
4. *Data una generica equazione di Weierstrass a coefficienti in R, ogni cambio di coordinate del tipo $x = u^2x' + r$ e $y = u^3y' + u^2sx' + t$ che porta a un'equazione di Weierstrass minima è tale che $u, r, s, t \in R$.*

Dimostrazione. **1.** Tra tutte le equazioni a coefficienti in R, esiste sicuramente un'equazione che minimizza $v(\Delta)$ poiché v è discreta.
2. Sappiamo dalla 2. della Proposizione 2.1.10 che un'equazione di Weierstrass per E è unica a meno di cambi di coordinate come quello indicato. Supponiamo quindi che sia l'equazione data sia la nuova siano minime. Per la definizione di minimo, deve valere $v(\Delta') = v(\Delta)$. Sappiamo che $\Delta = u^{12}\Delta'$ come in Tabella 2.2, quindi l'unica possibilità è che $v(u) = 0$ cioè $v \in R^*$. Dalle altre espressioni per i nuovi coefficienti $u^6b_6', u^8b_8', u^2a_2', u^6a_6'$ si ottiene rispettivamente che $r, s, t \in R$.
3. Si procede in modo analogo a 2. poiché $\omega' = u\omega$.
4. Se la nuova equazione è minima, allora $v(\Delta') \leq v(\Delta) = v(u^{12}\Delta')$. Questo significa $v(u) \geq 0$ cioè $u \in R$. Si procede poi come in 2. per ottenere $r, s, t \in R$.

□

3.2 Riduzione modulo π

Sia $R \to k = R/\pi R$ la mappa di riduzione tale che $t \to \tilde{t}$. Data un'equazione di Weierstrass minima per E/K, è possibile ridurre i suoi coefficienti modulo π: in tal modo

si ottiene una curva su k, non necessariamente liscia. Questa nuova curva è descritta dall'equazione

$$\tilde{E}: \ y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6. \tag{3.1}$$

La curva $\tilde{E}/k$ è chiamata *riduzione di E modulo π*. Poiché per 2. della Proposizione 3.1.3 l'equazione di Weierstrass minima è unica a meno di cambi di coordinate, allora $\tilde{E}$ è unica a meno di cambi di coordinate del solito tipo. Sia $P = [x_0, y_0, z_0]$ con $x_0, y_0, z_0 \in R$ tali che almeno uno di essi è in R^*. Allora il punto ridotto $\tilde{P} = [\tilde{x}_0, \tilde{y}_0, \tilde{z}_0] \in \tilde{E}(k)$. Possiamo definire quindi una *mappa di riduzione* $E(K) \to \tilde{E}(k)$ tale che $P \to \tilde{P}$. In generale tale mappa di riduzione è definita tra $\mathbb{P}^n(K) \to \mathbb{P}^n(k)$. Quindi la mappa di riduzione definita su $E(K)$ è semplicemente la restrizione della mappa di riduzione su $\mathbb{P}^2(K)$.
Se la curva $\tilde{E}/k$ è singolare, indichiamo con $\tilde{E}_{ns}(k)$ l'insieme dei punti non singolari. Abbiamo visto che $\tilde{E}_{ns}(k)$ è un gruppo (vedi Proposizione 2.2.7). Definiamo quindi due nuovi sottoinsiemi per $E(K)$:

$$E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\},$$
$$E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{\mathcal{O}}\}.$$

L'insieme $E_0(K)$ contiene quindi tutti i punti con *riduzione non singolare* mentre $E_1(K)$ è il *nucleo di riduzione*. Poiché l'equazione minima è unica a meno di cambi di coordinate, allora questi insiemi non dipendono dalla scelta dell'equazione minima.

Proposizione 3.2.1. *Esiste una successione esatta di gruppi abeliani*

$$0 \to E_1(K) \xrightarrow{\phi} E_0(K) \xrightarrow{\tau} \tilde{E}_{ns}(k) \to 0.$$

Dimostrazione. Dividiamo la dimostrazione in tre parti: mostriamo prima che la mappa di riduzione τ è suriettiva, quindi vediamo che $E_0(K)$ è un sottogruppo di $E(K)$ per cui la mappa di riduzione τ è un omomorfismo. Infine proviamo l'iniettività di ϕ.
Parte I. Sia $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ un'equazione di Weierstrass minima e sia $\tilde{f}(x,y)$ il corrispondente polinomio con coefficienti ridotti modulo π. Sia poi $\tilde{P} = (\tilde{\alpha}, \tilde{\beta}) \in \tilde{E}_{ns}(k)$, allora si ha $\partial_x \tilde{f}(\tilde{P}) \neq 0$ oppure $\partial_y \tilde{f}(\tilde{P}) \neq 0$. Supponiamo che sia vera la seconda, l'altro caso si ottiene in modo del tutto analogo.
Prendiamo quindi $x_0 \in R$ tale che $\tilde{x}_0 = \tilde{\alpha}$ e consideriamo l'equazione $f(x_0, y) = 0$. Quando riduciamo modulo π, l'equazione $\tilde{f}$ ha una radice semplice in $\tilde{\beta}$ poiché stiamo supponendo $\partial_y \tilde{f}(x_0, \tilde{\beta}) \neq 0$. Allora la radice $\tilde{\beta}$ di $\tilde{f}$ può essere sollevata a una radice $y_0 \in R$ di f tale che $f(x_0, y_0) = 0$ e $\tilde{y}_0 = \tilde{\beta}$: questo è possibile grazie al Lemma di Hensel, vedi [13] 7 (Proposition 7.31, Proposition 7.33). Poiché il punto $P = (x_0, y_0) \in E_0(K)$ ha come riduzione $\tau(P) = \tilde{P}$, si ottiene che τ su $E_0(K)$ è suriettiva.
Parte II. Sappiamo che le leggi di gruppo su $E(K)$ e $E_{ns}(K)$ sono definite tramite intersezioni con le rette di $\mathbb{P}^2$. Per una retta L definita su K si ha un'equazione del tipo $Ax + By + Cz = 0$ con $A, B, C \in R$ tali che almeno uno di essi è in R^*, mentre la

riduzione di L è data dall'equazione $\tilde{L}: \tilde{A}x + \tilde{B}y + \tilde{C}z = 0$. Se $P \in \mathbb{P}^2(K)$ è un punto sulla retta L, allora il punto ridotto $\tilde{P}$ è sulla retta ridotta $\tilde{L}$.
Ciò che vogliamo mostrare è quanto segue: siano $P_1, P_2 \in E_0(K)$ e sia $P_3 \in E(K)$ tale che $P_1 + P_2 + P_3 = \mathcal{O}$. Quindi esiste una retta L che interseca E in tre punti P_1, P_2, P_3 non necessariamente distinti. Allora $\tilde{L}$ interseca $\tilde{E}$ esattamente in $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3$ da cui segue che $\tilde{P}_3 \in \tilde{E}_{ns}(k)$, $\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = \tilde{\mathcal{O}}$ e in particolare $P_3 \in E_0(K)$. Questo mostra che $E_0(K)$ è un sottogruppo di $E(K)$.
I casi da analizzare sono diversi:
a) P_1, P_2, P_3 distinti e $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3$ distinti
b) P_1, P_2, P_3 distinti e $\tilde{P}_1 = \tilde{P}_2 \neq \tilde{P}_3$
c) P_1, P_2, P_3 distinti e $\tilde{P}_1 = \tilde{P}_2 = \tilde{P}_3$
d) $P_1 = P_2 \neq P_3$ e $\tilde{P}_1 = \tilde{P}_2 \neq \tilde{P}_3$
e) $P_1 = P_2 \neq P_3$ e $\tilde{P}_1 = \tilde{P}_2 = \tilde{P}_3$
f) $P_1 = P_2 = P_3$ e $\tilde{P}_1 = \tilde{P}_2 = \tilde{P}_3$.
Ci concentriamo sui casi a) e b).
a) L'intersezione tra $\tilde{L}$ e $\tilde{E}$ consiste di tre punti distinti $\{\tilde{P}_1, \tilde{P}_2, \tilde{P}_3\}$ i primi due dei quali sono in $\tilde{E}_{ns}(k)$ poiché per ipotesi $P_1, P_2 \in E_0(K)$. Per la Proposizione 2.2.7 abbiamo che anche $\tilde{P}_3 \in \tilde{E}_{ns}(k)$. Per questo, $P_3 \in E_0(K)$ e $\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = \tilde{\mathcal{O}}$.
b) Prima di analizzare questo caso, enunciamo un Lemma che poi utilizziamo.

Lemma 3.2.2. *Siano $P, Q \in E_0(K)$ punti distinti le cui riduzioni coincidono $\tilde{P} = \tilde{Q}$ e sia L la retta che passa per P e Q. Allora $\tilde{L}$ è tangente a $\tilde{E}$ in $\tilde{P}$.*

Dimostrazione. Supponiamo $\tilde{P} \neq \tilde{\mathcal{O}}$. Scegliamo un'equazione minima per E data da $f(x, y) = 0$ e sia $\tilde{f}(x, y)$ il corrispondente polinomio ridotto modulo π. Scriviamo $P = (\alpha, \beta) \in E(K)$, allora $Q = (\alpha + \mu, \beta + \lambda) \in E(K)$ con $\alpha, \beta \in R$ e $\mu, \lambda \in \mathfrak{m}$ poiché per ipotesi $\tilde{P} = \tilde{Q}$. Ancora per ipotesi sappiamo che $P \in E_0(K)$ quindi $\tilde{P}$ è un punto non singolare per $\tilde{E}$: vale allora $\partial_x \tilde{f}(\tilde{P}) \neq 0$ oppure $\partial_y \tilde{f}(\tilde{P}) \neq 0$. Supponiamo vero il secondo caso e analogamente si ottiene l'altro.
Poiché $f(Q) = 0$ allora possiamo scrivere i primi termini dello sviluppo di Taylor di $f(x, y)$ attorno a Q. Si ha

$$0 = f(Q) = f(P) + \partial_x f(P)\mu + \partial_y f(P)\lambda + A\mu^2 + B\mu\lambda + C\lambda^2$$

per qualche $A, B, C \in R$ e con $f(P) = 0$. L'ipotesi $\partial_y \tilde{f}(\tilde{P}) \neq 0$ è equivalente a $\partial_y f(P) \in R^*$, i.e. $v(\partial_y f(P)) = 0$ poiché riducendo modulo π si ottiene qualcosa di non nullo. Calcoliamo ora

$$v(\lambda) = v(\partial_y f(P)\lambda) = v(\partial_x f(P)\mu + A\mu^2 + B\mu\lambda + C\lambda^2) \geq v(\partial_x f(P)\mu) = v(\mu)$$

poiché $v(A\mu^2 + B\mu\lambda + C\lambda^2) > 0$ per l'ipotesi $\mu, \lambda \in \mathfrak{m}$. Perciò $v(\lambda) \geq v(\mu)$ implica $\lambda/\mu \in R$. Allora, dividendo lo sviluppo di Taylor per μ, riducendo modulo π e ricordando $\mu, \lambda \in \mathfrak{m}$, otteniamo la congruenza $\partial_x f(P) + \partial_y f(P)(\lambda/\mu) \equiv 0 \pmod{\mathfrak{m}}$. Questo significa

che, dopo aver ridotto modulo π, la retta tangente a $\tilde{E}$ in $\tilde{P}$ ha pendenza $\widetilde{\lambda/\mu}$.
Poiché la retta che passa per P e Q ha equazione $L : \ y - \beta = (\lambda/\mu)(x - \alpha)$ con $\lambda/\mu \in R$, allora la riduzione di L è la retta passante per $\tilde{P}$ con pendenza $\widetilde{\lambda/\mu}$, ovvero $\tilde{L}$ è necessariamente la tangente in $\tilde{P}$ a $\tilde{E}$.
Il caso $\tilde{P} = \tilde{\mathcal{O}}$ si ottiene in modo analogo.

□

Per concludere la dimostrazione, consideriamo $P_1, P_2 \in E_0(K)$ e $P_3 \in E(K)$ distinti e tali che $P_1 + P_2 + P_3 = \mathcal{O}$. Supponiamo che le riduzioni siano tali che $\tilde{P}_1 = \tilde{P}_2 \neq \tilde{P}_3$. Sia L la retta passante per P_1, P_2, P_3. Applichiamo il Lemma 3.2.2 con $P = P_1$ e $Q = P_2$. Allora $\tilde{L}$ è tangente in $\tilde{P}_1$ a $\tilde{E}$ quindi $P_3 \in \tilde{L}$ e si ha $[2]\tilde{P}_1 + \tilde{P}_3 = \tilde{\mathcal{O}}$. In particolare poiché $\tilde{P}_1 = \tilde{P}_2$, allora $\tilde{P}_3 \in \tilde{E}_{ns}(k)$ e $\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = \tilde{\mathcal{O}}$. Quindi $P_3 \in E_0(K)$.
Parte III. Per definizione di $E_1(K)$ come nucleo di riduzione si ha direttamente che $E_1(K)$ è un sottogruppo di $E(K)$. In particolare $E_1(K)$ è il sottogruppo di $E_0(K)$ contenente i punti la cui riduzione è $\tilde{\mathcal{O}}$ poiché $\tilde{\mathcal{O}} \in \tilde{E}_{ns}(k)$. ϕ inoltre è necessariamente iniettiva.

□

Osservazione 3.2.3. L'esattezza della successione corta definita nella Proposizione 3.2.1 è equivalente a $E_1(K) = \ker\tau$ e $\tilde{E}_{ns}(k) = \mathrm{im}\tau$. Allora $\tilde{E}_{ns}(k) \cong E_0(K)/E_1(K)$.

Osservazione 3.2.4. Osserviamo che se $v(\Delta) = 0$ allora $\tilde{\Delta} \neq 0$, quindi $\tilde{E}$ è non singolare. Questo significa che $\tilde{E}_{ns} = \tilde{E}$ e $E_0(K) = E(K)$. Allora l'Osservazione 3.2.3 si traduce in $\tilde{E}(k) \cong E(K)/E_1(K)$, ovvero $E(K)$ è composto da due pezzi: $E_1(K)$ nucleo di riduzione e $\tilde{E}(k)$ insieme dei punti di una curva ellittica non singolare definita su un campo k più piccolo di K.

3.3 Punti di ordine finito e coordinate intere

Proposizione 3.3.1. *Sia E/K una curva ellittica e sia $m \geq 1$ un intero relativamente primo a char(k).*

1. *Il sottogruppo $E_1(K)$ non contiene punti non banali di ordine m.*

2. *Supponiamo inoltre che la curva ridotta $\tilde{E}$ sia non singolare. Allora la mappa di riduzione $E(K)[m] \to \tilde{E}(k)$ è iniettiva. $E(K)[m]$ denota l'insieme dei punti di ordine m in $E(K)$.*

Dimostrazione. **1.** Consideriamo $[m] : E_1(K) \to E_1(K)$ con m definito sopra. Allora la mappa $[m]$ è un isomorfismo: vedi [16] IV.2 (Proposition 2.3) e IV.3 (Proposition 3.2). Quindi $\ker[m] = \mathcal{O}$ e $E_1(K)$ non ha m-torsione.

2. Se $\tilde{E}$ è non singolare abbiamo la situazione descritta nell'Osservazione 3.2.4, ovvero la successione esatta diventa

$$0 \to E_1(K) \xrightarrow{\phi} E_0(K) = E(K) \xrightarrow{\tau} \tilde{E}_{ns}(k) = \tilde{E}(k) \to 0.$$

Quindi la parte di m-torsione $E(K)[m]$ di $E(K)$ si inietta in $\tilde{E}(k)$ poiché $E_1(K)$ per la 1. non ha m-torsione.

□

Osservazione 3.3.2 (**Applicazione**)**.** L'utilizzo ripetuto della Proposizione 3.3.1 fornisce un metodo molto veloce per calcolare il sottogruppo di torsione di una curva ellittica definita su un campo di numeri. Infatti sia K un campo di numeri e sia K_v il suo completamento rispetto alla valutazione discreta v. Ovviamente $E(K)$ si inietta in $E(K_v)$, quindi applicando la Proposizione 3.3.1 con diverse valutazioni v si possono ottenere informazioni sulla torsione di $E(K)$.

Vediamo alcuni esempi di questa applicazione su $\mathbb{Q}$.

Esempio 3.3.3. Sia $E/\mathbb{Q}$ la curva ellittica $y^2 + y = x^3 - x + 1$. Si calcola che $\Delta = -13 \cdot 47$ quindi modulo 2 $\tilde{E}$ è non singolare. Riduciamo l'equazione di E modulo 2 e otteniamo che l'unico punto di $\mathbb{F}_2$ che soddisfa $\tilde{E}$ è $\mathcal{O}$, quindi $\tilde{E}(\mathbb{F}_2) = \{\mathcal{O}\}$. Allora anche $E(\mathbb{Q})[2] = \{\mathcal{O}\}$ e in particolare questo implica che $E(\mathbb{Q})$ non ha punti di torsione non banali.

Esempio 3.3.4. Sia $E/\mathbb{Q}$ la curva ellittica $y^2 = x^3 + 3$. Si calcola che $\Delta = -2^4 \cdot 3^5$ quindi modulo $p \geq 5$ $\tilde{E}$ è non singolare. Riduciamo l'equazione di E modulo p per $p = 5, 7$ e cerchiamo i punti di $\mathbb{F}_p$ che soddisfano $\tilde{E}$: otteniamo che $\#E(\mathbb{F}_5) = 6$ e $\#E(\mathbb{F}_7) = 13$. Poiché $E(\mathbb{Q})[m] \to \tilde{E}(\mathbb{F}_p)$ è iniettiva per ogni m tale che $p \nmid m$, allora l'ordine di $E(\mathbb{Q})_{\text{tors}}$ dovrebbe dividere contemporaneamente 6 e 13, quindi l'unica possibilità è $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$. Allora $E(\mathbb{Q})$ non ha torsione non banale. In particolare scegliamo il punto $(1, 2) \in E(\mathbb{Q})$ che per quanto detto ha ordine infinito. Allora $E(\mathbb{Q})$ è un insieme infinito.

Esempio 3.3.5. Sia $E/\mathbb{Q}$ la curva ellittica $y^2 = x^3 + x$. Si calcola che $\Delta = -2^6$ quindi modulo $p \geq 3$ $\tilde{E}$ è non singolare. Riduciamo l'equazione di E modulo p per $p = 3, 5, 7$ e cerchiamo i punti di $\mathbb{F}_p$ che soddisfano $\tilde{E}$: otteniamo che $\#E(\mathbb{F}_3) = 4$, $\#E(\mathbb{F}_5) = 4$ e $\#E(\mathbb{F}_7) = 8$. Più in generale vale che $\#E(\mathbb{F}_p)$ è divisibile per 4 per ogni $p \geq 3$, quindi in questo caso esiste un sottogruppo di $E(\mathbb{F}_p)$ con ordine 4.
Osserviamo ora che il punto $P = (0, 0) \in E(\mathbb{Q})$ ha ordine 2 perché soddisfa $P = -P$ secondo la legge di gruppo su E. In particolare si calcolano

$$E(\mathbb{F}_3) = \{\mathcal{O}, (0, 0), (2, 1), (2, 2)\}, \qquad E(\mathbb{F}_5) = \{\mathcal{O}, (0, 0), (2, 0), (3, 0)\}.$$

Osserviamo che secondo la legge di gruppo su $\tilde{E}$ si ha $(2,1) = (2,-2) = -(2,2)$ e ogni punto del tipo $P_0 = (x_0, 0)$ ha ordine 2 perché soddisfa $P_0 = -P_0$. Allora $E(\mathbb{F}_3) \cong \mathbb{Z}/4\mathbb{Z}$ mentre $E(\mathbb{F}_5) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Poiché $E(\mathbb{Q})_{\text{tors}}$ si inietta in entrambi questi gruppi, allora $E(\mathbb{Q})_{\text{tors}}$ è banale oppure è ciclico di ordine 2 e in tal caso $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0,0)\}$. L'unico punto non banale è quindi $(0,0)$.

Il risultato seguente è molto importante perché permette di dare un limite preciso al denominatore di un punto di torsione.

Teorema 3.3.6 (Cassels)**.** *Siano $char(K) = 0$ e $char(k) = p > 0$. Sia E/K una curva ellittica data da un'equazione di Weierstrass non necessariamente minima del tipo (2.2) con i coefficienti $a_i \in R$. Sia $P \in E(K)$ un punto di ordine esattamente $m \geq 2$. Si hanno i seguenti fatti*

1. *se $p \nmid m$, allora $x(P), y(P) \in R$.*
2. *se $m = p^n$, allora $\pi^{2r}x(P), \pi^{3r}y(P) \in R$ con*

$$r = \left\lfloor \frac{v(p)}{p^n - p^{n-1}} \right\rfloor \qquad \textit{dove } \lfloor\ \rfloor \textit{ denota la parte intera.}$$

Dimostrazione. Se $x(P) \in R$ non dobbiamo provare nulla, quindi possiamo supporre $v(x(P)) < 0$.
Inoltre supponiamo che l'equazione data per E non sia minima e siano (x', y') le coordinate di un'equazione minima ottenuta tramite il cambio di coordinate. Allora dalla 4. della Proposizione 3.1.3, poiché i coefficienti del cambio di coordinate sono tutti in R, si ha $0 > v(x(P)) \geq v(x'(P))$ e $0 > v(y(P)) \geq v(y'(P))$. Quindi basta dimostrare il Teorema per un'equazione minima.
1. Dall'equazione di Weierstrass possiamo ricavare la seguente informazione: $3v(x(P)) = 2v(y(P))$. Poiché stiamo supponendo $v(x(P)) < 0$ possiamo anche scrivere $3v(x(P)) = 2v(y(P)) = -6s$ con $s \geq 1$ intero. Ovviamente anche $v(y(P)) < 0$ quindi il punto $P \in E_1(K)$ perché la riduzione lo manda necessariamente in $\mathcal{O}$. Dalla 1. della Proposizione 3.3.1 sappiamo che il gruppo $E_1(K)$ non ha m-torsione quando $p \nmid m$. Allora otteniamo per P un assurdo rispetto all'ipotesi del Teorema.
2. Poiché abbiamo visto $3v(x(P)) = 2v(y(P)) = -6s$, ciò significa che possiamo scrivere $x(P) = \pi^{-2s}\alpha$ e $y(P) = \pi^{-3s}\beta$ con $v(\alpha) = v(\beta) = 0$. Allora $v(-x(P)/y(P)) = v(x(P)/y(P)) = v(\pi^s\alpha/\beta) = s$. Utilizziamo il risultato

$$s \leq \frac{v(p)}{p^n - p^{n-1}} = \lambda$$

per la cui dimostrazione si rimanda a [16] IV.6 (Theorem 6.1). Poiché s deve essere intero, allora se poniamo $s = \lfloor\lambda\rfloor$ si ha il risultato.

□

Esempio 3.3.7 (**Applicazione**)**.** Sia $E/\mathbb{Q}$ una curva ellittica data da un'equazione di Weierstrass a coefficienti in $\mathbb{Z}$ e sia $P \in E(\mathbb{Q})$ un punto di ordine esattamente m. Immergiamo allora $E(\mathbb{Q})$ in $E(\mathbb{Q}_p)$ per vari primi p con $\mathbb{Q}_p$ completamento p-adico di $\mathbb{Q}$. Quindi, se m non è potenza di un primo, allora $x(P), y(P) \in \mathbb{Z}$. Se invece $m = p^n$ e se v è la valutazione normalizzata associata a p, si ha $v(p) = 1$ e la quantità r del Teorema 3.3.6 vale 0 tranne nel caso in cui $p = 2$ e $n = 1$. Concludiamo quindi che $x(P), y(P) \in \mathbb{Z}$ per ogni punto di torsione $P \in E(\mathbb{Q})$ con ordine $m \geq 3$. Ad esempio, il punto $P = (-1/4, 1/8) \in E(\mathbb{Q})[2]$ per la curva $E:\ y^2 + xy = x^3 + 4x + 1$.

3.4 Buona e cattiva riduzione

Sia E/K una curva ellittica e sia $\tilde{E}$ la riduzione modulo $\mathfrak{m}$ di un'equazione minima per E. Allora abbiamo tre possibilità.

Definizione 3.4.1. Si dice che E ha riduzione

1. *buona* (o *stabile*) se $\tilde{E}$ è non singolare,
2. *moltiplicativa* (o *semistabile*) se $\tilde{E}$ ha un nodo,
3. *additiva* (o *instabile*) se $\tilde{E}$ ha una cuspide.

In generale nei casi 2. e 3. si dice che E ha una *cattiva riduzione*. Nel caso 2 inoltre si dice che la riduzione *spezza* se le pendenze delle rette tangenti nel nodo sono in k, altrimenti la riduzione *non spezza*.

Proposizione 3.4.2. *Sia E/K una curva ellittica data da un'equazione di Weierstrass minima del tipo (2.2), con le quantità Δ e c_4 associate.*

1. *E ha buona riduzione se e solo se $v(\Delta) = 0$, i.e. $\Delta \in R^*$. Si ha che $\tilde{E}/k$ è una curva ellittica.*
2. *E ha riduzione moltiplicativa se e solo se $v(\Delta) > 0$ e $v(c_4) = 0$, i.e. $\Delta \in \mathfrak{m}$ e $c_4 \in R^*$. Si ha che $\tilde{E}_{ns}(\bar{k}) \cong \bar{k}^*$, gruppo moltiplicativo.*
3. *E ha riduzione additiva se e solo se $v(\Delta) > 0$ e $v(c_4) > 0$, i.e. $\Delta, c_4 \in \mathfrak{m}$. Si ha che $\tilde{E}_{ns}(\bar{k}) \cong \bar{k}^+$, gruppo additivo.*

Dimostrazione. Basta osservare i seguenti fatti:
1. $\Delta \in R^*$ implica $\tilde{\Delta} \neq 0$,
2. $\Delta \in \mathfrak{m}$ e $c_4 \in R^*$ implicano $\tilde{\Delta} = 0$ e $\tilde{c}_4 \neq 0$,
3. $\Delta, c_4 \in \mathfrak{m}$ implicano $\tilde{\Delta} = \tilde{c}_4 = 0$.
Basta allora applicare la Proposizione 2.1.6 alla curva $\tilde{E}/k$ e la Proposizione 2.2.7 al gruppo $\tilde{E}_{ns}(\bar{k})$.

□

Esempio 3.4.3. Sia $p \geq 5$.
La curva ellittica $E: \ y^2 = x^3 + px^2 + 1$ ha buona riduzione su $\mathbb{Q}_p$. Infatti $\Delta = -2^4(3^3 + 2^2p^2)$ che non è divisibile per $p \geq 5$, quindi $v(\Delta) = 0$.
La curva ellittica $E: \ y^2 = x^3 + x^2 + p$ ha riduzione moltiplicativa (che spezza) su $\mathbb{Q}_p$. Infatti $\Delta = -2^4p(2^2 + 3^3p)$ che è divisibile per p, quindi $v(\Delta) > 0$, mentre $c_4 = 2^4$ quindi $v(c_4) = 0$ per $p \geq 5$. Abbiamo un nodo in $(0, 0)$.
La curva ellittica $E: \ y^2 = x^3 + p$ ha riduzione additiva su $\mathbb{Q}_p$. Infatti $\Delta = -2^4 \cdot 3^3p^2$ quindi $v(\Delta) > 0$ e $c_4 = 0$ che implica direttamente $\tilde{c}_4 = 0$. Abbiamo una cuspide in $(0, 0)$ con tangenti $y = 0$ e $y = -2x$.
In quest'ultimo caso, se consideriamo l'estensione $\mathbb{Q}(\sqrt[6]{p})$, allora su questo campo la curva ha buona riduzione dal momento che la sostituzione $(x, y) \to (\sqrt[3]{p}x', \sqrt{p}y')$ porta a un'equazione $(y'^2 = x'^3 + 1)$ che ha buona riduzione: infatti $\Delta' = -2^4 \cdot 3^3$ quindi $v(\Delta') = 0$.

Osservazione 3.4.4. L'ultimo risultato vale anche più in generale: è possibile, estendendo il campo base, trasformare una riduzione additiva in una buona o anche in una moltiplicativa. Non esiste invece un'estensione di campi che modifichi una riduzione moltiplicativa o buona in qualsiasi altra.

Definizione 3.4.5. Si dice che E/K ha buona riduzione *potenziale* se esiste un'estensione finita K'/K tale che E ha buona riduzione su K'.

Proposizione 3.4.6. *La curva ellittica E/K ha buona riduzione potenziale se e solo se il suo j-invariante è intero, i.e. $j \in R$.*

Dimostrazione. Supponiamo $\mathrm{char}(k) \neq 2$ e consideriamo un'estensione finita di K in cui E è data da un'equazione di Legendre $y^2 = x(x-1)(x-\lambda)$ con $\lambda \neq 0, 1$.
$\Leftarrow$) Sia $j \in R$, allora sappiamo dalla 2. della Proposizione 2.1.9 che esiste tra j e λ la relazione

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

$j \in R$ implica $\lambda \not\equiv 0, 1 \pmod{\mathfrak{m}}$. Supponiamo inoltre che valga $v(\lambda) < 0$, allora dall'equazione otteniamo $v(j) = 6v(\lambda) - 4v(\lambda) < 0$ assurdo (possiamo guardare solo le potenze di λ più grandi per le proprietà di minimo). Segue che $v(\lambda) \geq 0$, i.e. $\lambda \in R$. Allora l'equazione ha coefficienti interi e buona riduzione poiché $\Delta = 16\lambda^2(\lambda - 1)^2$.
$\Rightarrow$) Supponiamo invece che E abbia buona riduzione e consideriamo un'estensione finita K'/K tale che E abbia buona riduzione anche su K'. Quindi R' è l'anello degli interi di R' e Δ', c_4', j' sono le quantità associate all'equazione minima di E su K'. Si ha $\Delta' \in R'^*$ e $c_4' \in R'$. Inoltre, per le proprietà del j-invariante, $j' = j = c_4'^3/\Delta' \in R'$. Sappiamo anche che $j \in K$ poiché E è definita su K, allora $j \in R$.

□

Concludiamo enunciando un Teorema importante per la cui dimostrazione si rimanda a [15] IV §5, IV §6, IV §8. Nelle Osservazioni 3.2.3 e 3.2.4 abbiamo visto come è possibile descrivere la struttura del gruppo $E_0(K)$. Resta ora da studiare la parte $E(K)/E_0(K)$.

Teorema 3.4.7 (Kodaira, Néron)**.** *Sia E/K una curva ellittica. Se E ha su K riduzione moltiplicativa che non spezza, allora $E(K)/E_0(K)$ è un gruppo ciclico di ordine $v(\Delta) = -v(j)$. In tutti gli altri casi, il gruppo $E(K)/E_0(K)$ è finito di ordine al più* 4.

Corollario 3.4.8. *Il sottogruppo $E_0(K)$ ha indice finito in $E(K)$.*

Capitolo 4

Il gruppo dei punti razionali su campi globali

Sia K un campo di numeri e sia E/K una curva ellittica. In questo capitolo mostriamo il Teorema di Mordell-Weil sull'insieme di punti $E(K)$.
Sappiamo già che $E(K)$ è un gruppo per la Legge di Composizione 2.2.2 su una curva ellittica. Il Teorema afferma che $E(K)$, detto anche *gruppo di Mordell-Weil*, è in realtà un gruppo finitamente generato, i.e.

$$E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^r \qquad \text{[Mordell-Weil]}$$

dove il *sottogruppo di torsione* $E(K)_{\text{tors}}$ è finito e il *rango* r di $E(K)$ è un intero non negativo. Mentre è relativamente semplice calcolare la parte di torsione, è molto più difficile calcolare il rango e in generale non esiste un procedimento che garantisca di ottenere una risposta.
La dimostrazione del Teorema di Mordell-Weil consiste di due parti distinte: il "Teorema di Mordell-Weil debole" e la "Discesa infinita". Nel caso $K = \mathbb{Q}$ quest'ultima parte si semplifica notevolmente.

Notazione. Siano: K un campo di numeri;
M_K un insieme completo di valori assoluti su K (i.e. $|x+y|_v \leq |x|_v + |y|_v$) non equivalenti, i.e. per due diversi valori assoluti v_1, v_2 non vale $|x|_{v_1} < 1 \Rightarrow |x|_{v_2} < 1$ o equivalentemente non esiste $\lambda > 0$ tale che $|x|_{v_1} = |x|_{v_2}^{\lambda}$;
M_K^0 l'insieme dei valori assoluti non archimedei in M_K, i.e. quelli per cui vale la disuguaglianza ultrametrica $|x + y|_v \leq \max\{|x|_v, |y|_v\}$ e tali che $|0|_v = 0$;
$M_K^\infty = M_K - M_K^0$ l'insieme dei valori assoluti archimedei in M_K, i.e. quelli per cui non vale la disuguaglianza ultrametrica e tali che $|0|_v = 0$;
$v(x)$ la quantità $-\log |x|_v$ per un valore assoluto $v \in M_K$;
ord_v una valutazione normalizzata per $v \in M_K^0$, i.e. tale che $\text{ord}_v(K^*) = \mathbb{Z}$ e $\text{ord}_v(0) = \infty$;
R l'anello degli interi di K: $R = \{x \in K : v(x) \geq 0 \text{ per ogni } v \in M_K^0\}$;

R^* il gruppo delle unità di R: $R^* = \{x \in K : v(x) = 0 \text{ per ogni } v \in M_K^0\}$;
K_v il completamento di K rispetto a $v \in M_K$;
R_v l'anello degli interi di K_v per $v \in M_K^0$;
$\mathfrak{m}_v$ l'ideale massimale di R_v;
k_v il campo dei residui di R_v.
Osserviamo che per $K = \mathbb{Q}$, il Teorema di Ostrowski assicura che:
se $v \in M_{\mathbb{Q}}^{\infty}$ allora $|\ |_v$ è equivalente al valore assoluto euclideo usuale $|\ |_{\infty}$;
se invece $v \in M_{\mathbb{Q}}^0$ allora $|\ |_v$ è equivalente al valore assoluto p-adico $|\ |_p$.
Si veda per questo risultato [13] 7 (Theorem 7.12).

4.1 La versione debole del Teorema di Mordell-Weil

Teorema 4.1.1 (Teorema di Mordell-Weil debole)**.** *Sia K un campo di numeri, sia E/K una curva ellittica e sia $m \geq 2$ un intero. Allora*

$$E(K)/mE(K)$$

è un gruppo finito.

Dimostriamo in più passi questo risultato. Per tutta la sezione $m \geq 2$ è un intero.

PASSO I. Lemma di Riduzione: ci si riduce a verificare l'enunciato per i punti a valore in un'estensione L di K finita e di Galois.

Lemma 4.1.2. *Sia L/K un'estensione finita di Galois. Se $E(L)/mE(L)$ è finito, allora anche $E(K)/mE(K)$ è finito.*

Dimostrazione. Dall'estensione $K \hookrightarrow L$ si ottiene l'inclusione $E(K) \hookrightarrow E(L)$ che induce una mappa naturale $E(K)/mE(K) \to E(L)/mE(L)$. Sia Φ il nucleo di questa mappa, allora

$$\Phi = E(K) \cap mE(L) \ / \ mE(K).$$

Quindi per ogni $P \in \Phi$ possiamo scegliere un punto $Q_P \in E(L)$ (non necessariamente unico) tale che $[m]Q_P = P$. Definiamo la mappa (che in generale non è un omomorfismo)

$$\lambda_P : G_{L/K} \to E[m], \qquad \lambda_P(\sigma) = Q_P^{\sigma} - Q_P.$$

La mappa ha senso, infatti $[m](Q_P^{\sigma} - Q_P) = ([m]Q_P)^{\sigma} - [m]Q_P = P^{\sigma} - P = \mathcal{O}$ poiché E è definita su K e $P \in E(K)$.
Supponiamo ora $P, P' \in E(K) \cap mE(L)$ tali che $\lambda_P = \lambda_{P'}$. Allora $Q_P^{\sigma} - Q_P = Q_{P'}^{\sigma} - Q_{P'}$ i.e. $(Q_P - Q_{P'})^{\sigma} = Q_P - Q_{P'}$ per ogni $\sigma \in G_{L/K}$, da cui si ha $Q_P - Q_{P'} \in E(K)$. Quindi

$P - P' = [m]Q_P - [m]Q_{P'} \in mE(K)$, da cui si ottiene $P \equiv P' \pmod{mE(K)}$. Quindi l'associazione

$$\Phi \to \{G_{L/K} \to E[m]\}, \qquad P \to \lambda_P$$

è una corrispondenza biunivoca. Poiché $G_{L/K}$ e $E[m]$ sono insiemi finiti, esiste solo un numero finito di mappe tra di essi e quindi anche Φ è finito. Allora la successione esatta

$$0 \to \Phi \to E(K)/mE(K) \to E(L)/mE(L) \to 0$$

implica $E(K)/mE(K)$ finito perché è inserito tra due gruppi finiti.

□

PASSO II. Associazione di Kummer: si crea una particolare estensione L di K di Galois per poter utilizzare il Lemma 4.1.2.
In particolare, grazie al Lemma 4.1.2 possiamo supporre $E[m] \subset E(K)$.

Definizione 4.1.3. L'*associazione di Kummer* è data da

$$\kappa : E(K) \times G_{\bar{K}/K} \to E[m], \qquad \kappa(P, \sigma) = Q^\sigma - Q$$

con $P \in E(K)$ e $Q \in E(\bar{K})$ tale che $[m]Q = P$.

Proposizione 4.1.4.

1. *κ è ben definita.*
2. *κ è bilineare, nel senso che:*

$$\kappa(P + P', \sigma) = \kappa(P, \sigma) + \kappa(P', \sigma) \qquad e \qquad \kappa(P, \sigma\tau) = \kappa(P, \sigma) + \kappa(P, \tau).$$

Dimostrazione. **1.** Per vedere che κ è ben definita, dobbiamo mostrare che $\kappa(P, \sigma) \in E[m]$ e che il suo valore non dipende dalla scelta di Q. Infatti $[m]\kappa(P, \sigma) = [m]Q^\sigma - [m]Q = P^\sigma - P = \mathcal{O}$ poiché $P \in E(K)$ e σ fissa K. Inoltre sia $T \in E[m]$, vediamo che ogni altra scelta è del tipo $Q+T$. Infatti $(Q+T)^\sigma - (Q+T) = Q^\sigma + T^\sigma - Q - T = Q^\sigma - Q$ poiché σ fissa T data l'ipotesi $E[m] \subset E(K)$.
2. Linearità in P: siano $P, P' \in E(K)$ allora $\kappa(P + P', \sigma) = (Q + Q')^\sigma - (Q + Q') = (Q^\sigma - Q) + (Q'^\sigma - Q') = \kappa(P, \sigma) + \kappa(P', \sigma)$.
Linearità in σ: siano $\sigma, \tau \in G_{\bar{K}/K}$ allora $\kappa(P, \sigma\tau) = Q^{\sigma\tau} - Q = Q^{\sigma\tau} - Q^\tau + Q^\tau - Q = (Q^\sigma - Q)^\tau - (Q^\tau - Q) = \kappa(P, \sigma)^\tau + \kappa(P, \tau)$. Ma $\kappa(P, \sigma) \in E[m] \subset E(K)$ è fissato da τ.

□

Proposizione 4.1.5. *Dalla bilinearità di κ segue che esistono due mappe:*

$$\kappa_1 : E(K) \to Hom(G_{\bar{K}/K}, E[m]) \qquad e \qquad \kappa_2 : G_{\bar{K}/K} \to Hom(E(K), E[m]).$$

Allora

1. $\ker \kappa_1 = mE(K)$.
2. $\ker \kappa_2 = G_{\bar{K}/L}$ *dove*
$$L = K([m]^{-1}E(K))$$
è il più piccolo sottocampo di $\bar{K}$ *che contiene tutti i punti* $Q \in E(\bar{K})$ *tali che* $[m]Q \in E(K)$.

Dimostrazione. **1.** Sia $P \in mE(K)$ allora $P = [m]Q$ con $Q \in E(K)$. Allora Q è fissato da ogni $\sigma \in G_{\bar{K}/K}$ quindi $\kappa(P, \sigma) = Q^\sigma - Q = \mathcal{O}$.
Viceversa, sia $\kappa(P, \sigma) = \mathcal{O}$ per ogni $\sigma \in G_{\bar{K}/K}$. Allora se $Q \in E(\bar{K})$ con $[m]Q = P$ si ha $Q^\sigma = Q$ per ogni σ, quindi $Q \in E(K)$ e $P = [m]Q \in mE(K)$.
2. Osserviamo che per definizione di Q si ha: $Q \in \{R \in E(\bar{K}) : [m]R \in E(K)\}$ quindi $Q \in \{[m]^{-1}S : S \in E(K)\}$, i.e. $Q \in E(L)$. Allora, se $\sigma \in G_{\bar{K}/L}$, σ fissa Q e si ha $\kappa(P, \sigma) = Q^\sigma - Q = \mathcal{O}$.
Viceversa, supponiamo $\sigma \in G_{\bar{K}/K}$ tale che $\kappa(P, \sigma) = \mathcal{O}$ per ogni $P \in E(K)$. Allora per ogni $Q \in E(\bar{K})$ tale che $[m]Q \in E(K)$ si ha $\mathcal{O} = \kappa([m]Q, \sigma) = Q^\sigma - Q$. Poiché L è il più piccolo sottocampo contenente tutti i punti Q tali che $[m]Q \in E(K)$, allora L deve contenere anche tutti i punti Q tali che $Q^\sigma = Q$. Quindi $\sigma \in G_{\bar{K}/L}$.

□

Corollario 4.1.6. *Sia* L *il campo dato in 2. della Proposizione 4.1.5.*
κ *induce un'associazione bilineare perfetta*

$$\tilde{\kappa} : E(K)/mE(K) \times G_{L/K} \to E[m],$$

cioè tale che le due mappe

$$\tilde{\kappa}_1 : E(K)/mE(K) \to Hom(G_{L/K}, E[m]) \quad e \quad \tilde{\kappa}_2 : G_{L/K} \to Hom(E(K)/mE(K), E[m])$$

sono iniettive.

Dimostrazione. Per la 2. della Proposizione 4.1.5 sappiamo che $G_{\bar{K}/L} = \ker \kappa_2$ con

$$\kappa_2 : G_{\bar{K}/K} \to \mathrm{Hom}(E(K), E[m]), \qquad \sigma \to \kappa(\cdot, \sigma).$$

Allora $G_{\bar{K}/L}$ è un sottogruppo normale di $G_{\bar{K}/K}$ e quindi l'estensione L/K è di Galois per il Teorema Fondamentale della Teoria di Galois. Allora l'associazione $\tilde{\kappa}$

$$\tilde{\kappa} : E(K)/\ker \kappa_1 \times G_{\bar{K}/K}/\ker \kappa_2 \cong E(K)/mE(K) \times G_{L/K} \longrightarrow E[m]$$

è perfetta poiché le mappe

$$\tilde{\kappa}_1 : E(K)/mE(K) \to \mathrm{Hom}(G_{L/K}, E[m]) \quad \text{e} \quad \tilde{\kappa}_2 : G_{L/K} \to \mathrm{Hom}(E(K)/mE(K), E[m])$$

sono entrambe suriettive ed iniettive per definizione.

□

PASSO III. Analisi e proprietà dell'estensione L/K: dal Corollario 4.1.6 sappiamo che $E(K)/mE(K)$ è finito se e solo se $G_{L/K}$ è finito, poiché il gruppo $E[m]$ è finito. Guardiamo allora l'estensione L/K.

Definizione 4.1.7. Sia K un campo di numeri e sia E/K una curva ellittica. Sia $v \in M_K^0$ una valutazione discreta. Allora E ha *buona* (rispettivamente *cattiva*) *riduzione in* v se E ha buona (rispettivamente cattiva) riduzione quando è considerata su un completamento K_v.
Se consideriamo per E un'equazione minima su K_v, denotiamo la curva ridotta $\tilde{E}_v/k_v$. In generale non è possibile scegliere una sola equazione di Weierstrass per E su K che sia minima contemporaneamente per tutti i K_v. Questo però è possibile quando $K = \mathbb{Q}$.

Osservazione 4.1.8. Data un'equazione di Weierstrass del tipo (2.2) per E/K, sappiamo che per ogni $v \in M_K^0$ tranne al più un numero finito si ha $v(a_i) \geq 0$ e $v(\Delta) = 0$. Per ogni v che soddisfa tali condizioni, l'equazione data è già minima e la curva ridotta $\tilde{E}_v/k_v$ è non singolare. Allora *E ha buona riduzione in v per ogni $v \in M_K^0$ tranne al più un numero finito.*

Proposizione 4.1.9 (Riformulazione di 2. della Proposizione 3.3.1)**.** *Sia $v \in M_K^0$ una valutazione discreta tale che $v(m) = 0$ e tale che E ha buona riduzione in v. Allora la mappa di riduzione $E(K)[m] \to \tilde{E}_v(k_v)$ è iniettiva.*

Definizione 4.1.10. É possibile reinterpretare l'iniettività della m-torsione in termini dell'azione del gruppo di Galois sui punti di torsione.
Sia K' un'estensione di K. Consideriamo l'insieme $\mathcal{V}$ delle classi di equivalenza delle valutazioni v' su K' dove $v' \in M_{K'}^0$ è l'estensione di $v \in M_K^0$ a K': una classe di equivalenza di questo tipo è detta *luogo*. Allora il gruppo di Galois $G_{K'/K}$ agisce su questo insieme nel modo seguente:

$$G_{K'/K} \times \mathcal{V} \to \mathcal{V}, \qquad (\sigma, [v']) \to \sigma([v']) = [v' \circ \sigma].$$

(La mappa è ben definita perché non dipende dalla scelta del rappresentante v'). Definiamo due gruppi:
• il *gruppo di decomposizione di v'* $G_{v'/v}$ è lo stabilizzatore di $[v']$ e quindi è il sottogruppo di $G_{K'/K}$ che contiene tutti gli elementi σ che fissano $[v']$;
• il *gruppo di inerzia di v'* $I_{v'/v}$ è il sottogruppo di $G_{v'/v}$ contenente gli elementi del gruppo di decomposizione che agiscono banalmente sul campo dei residui $k'_{v'}$, i.e. $\sigma \in I_{v'/v}$ se la mappa

$$G_{v'/v} \times R'_{v'} \to R'_{v'}, \qquad (\sigma, x) \to \sigma(x) \pmod{\mathfrak{m}}$$

è tale che $\sigma(x) \equiv x \pmod{\mathfrak{m}}$. Infatti $[v' \circ \sigma](x) = [v'](x)$.
Allora il gruppo di Galois $G_{K'/K}$ si decompone nel modo seguente:

$$1 \to I_{v'/v} \to G_{K'/K} \to G_{k'_{v'}/k_v} \to 1.$$

Sia ora Σ un insieme su cui agisce $G_{K'/K}$. Diciamo che Σ è *non ramificato in* v' se l'azione di $I_{v'/v}$ su Σ è banale.

Proposizione 4.1.11. *Sia* $L = K([m]^{-1}E(K))$ *il campo definito nella Proposizione 4.1.5.*

1. *L'estensione* L/K *è abeliana e ha esponente* m*, i.e. il gruppo di Galois* $G_{L/K}$ *è abeliano e l'ordine di ogni suo elemento divide* m*.*

2. *Sia* $S \subset M_K$ *tale che*

$$S = \{v \in M_K^0 : E \text{ ha cattiva riduzione in } v\} \cup \{v \in M_K^0 : v(m) \neq 0\} \cup M_K^\infty.$$

Allora L/K *è non ramificata al di fuori di* S*, i.e. se* $v \in M_K$ *e* $v \notin S$ *allora* L/K *è non ramificata in* v*.*

Dimostrazione. **1.** Si ottiene dal Corollario 4.1.6 poiché esiste un'iniezione $G_{L/K} \to \mathrm{Hom}(E(K)/mE(K), E[m])$.
2. Sia $v \in M_K$ con $v \notin S$. Sia poi $Q \in E(\bar{K})$ tale che $[m]Q \in E(K)$ e sia $K' = K(Q)$. Basta vedere che K'/K è non ramificata in v.
Sia $v' \in M_{K'}$ un luogo di K' su v e sia $k'_{v'}/k_v$ la corrispondente estensione di campi dei residui. Poiché $v \notin S$ allora E ha buona riduzione in v e anche in v' poiché consideriamo la stessa equazione di Weierstrass, vedi Osservazione 4.1.8.
Quindi guardiamo la mappa di riduzione sull'estensione: $E(K') \to \tilde{E}(k'_{v'})$. Consideriamo il sottogruppo di inerzia $I_{v'/v} \subset G_{\bar{K}/K}$ e $\sigma \in I_{v'/v}$.
Per definizione σ agisce banalmente su $\tilde{E}(k'_{v'})$, quindi si ha $\widetilde{Q^\sigma - Q} = \tilde{Q}^\sigma - \tilde{Q} = \tilde{\mathcal{O}}$. D'altra parte, poiché $[m]Q \in E(K)$, allora $[m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = \mathcal{O}$. Quindi il punto $Q^\sigma - Q$ ha ordine m per cui deve appartenere al nucleo della mappa di riduzione modulo v'. Ma per la Proposizione 4.1.9 tale mappa è iniettiva, per cui l'unica possibilità è $Q^\sigma - Q = \mathcal{O}$. Questo mostra che Q è fissato da ogni elemento di $I_{v'/v}$ e che quindi $K' = K(Q)$ è non ramificato in v' su K. Poiché questo vale per ogni v' su $v \notin S$, allora K'/K è non ramificato fuori da S.

□

PASSO IV. L/K è un'estensione finita: resta quindi da provare il fatto che un'estensione di K che soddisfa le condizioni della Proposizione 4.1.11 è necessariamente un'estensione finita.
Utilizziamo i seguenti risultati di teoria dei numeri algebrici.

Risultati sui numeri algebrici 4.1.12.
• Il numero di classi di K dove K è un campo di numeri è finito. Si veda [13] 3, 4. In particolare si definisce *numero di classi* l'ordine del gruppo di classi di ideali, dato dal quoziente tra il gruppo degli ideali frazionari di K (o meglio dell'anello degli interi R

di K) e il suo sottogruppo di ideali principali. Intuitivamente il numero di classi indica quanto l'anello è distante dall'essere un dominio a ideali principali e dall'avere quindi fattorizzazione unica.
• Se un campo di caratteristica 0 contiene le radici m-esime dell'unità ξ_m, allora la sua massima estensione abeliana di esponente m si ottiene aggiungendo le radici m-esime di tutti i suoi elementi. Si veda [5] 14.7, 17.3 (Kummer Theory) e [3] III §2.
• Il gruppo delle unità di K dove K è un campo di numeri è finitamente generato. Si veda [13] 5.

Proposizione 4.1.13. *Sia K un campo di numeri e sia $S \subset M_K$ un insieme finito di luoghi che contiene M_K^∞. Sia $m \geq 2$ un intero e sia L/K la massima estensione abeliana di K di esponente m non ramificata fuori da S. Allora L/K è un'estensione finita.*

Dimostrazione. Per prima cosa osserviamo che S è finito per quanto detto nell'Osservazione 4.1.8.
Supponiamo di sapere che la Proposizione è vera per qualche estensione finita K' di K, dove S' è il corrispondente insieme dei luoghi su S. Allora LK'/K', essendo un'estensione abeliana di esponente m non ramificata fuori da S', deve essere finita. E questo implica L/K finita. Basta dimostrare allora il risultato supponendo che K contenga le radici m-esime dell'unità ξ_m.
Come detto, aumentiamo l'insieme S in modo che L sia un'estensione più grande. Usando il primo risultato di teoria dei numeri algebrici 4.1.12, aggiungiamo un numero finito di elementi a S in modo tale che l'anello degli *S-interi*

$$R_S = \{a \in K : v(a) \geq 0 \text{ per ogni } v \in M_K \text{ con } v \notin S\}$$

sia un dominio a ideali principali. Questo significa scegliere $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ ideali interi che rappresentino le classi di ideali di K e poi aggiungere a S le valutazioni corrispondenti ai primi che dividono $\mathfrak{a}_1 \cdots \mathfrak{a}_h$. In tal modo siamo sicuri di ottenere $v(m) = 0$ per ogni $v \notin S$.
Applichiamo ora il secondo risultato di teoria dei numeri algebrici 4.1.12: per le nostre ipotesi si osserva che L è il più grande sottocampo di $K(\sqrt[m]{a} : a \in K)$ non ramificato fuori da S. Sia allora $v \in M_K$ con $v \notin S$ e si consideri l'equazione $X^m - a = 0$ sul campo locale K_v. Poiché $v(m) = 0$ e il discriminante di questo polinomio è $\pm m^m a^{m-1}$, l'estensione $K_v(\sqrt[m]{a})/K_v$ è non ramificata se e solo se $\mathrm{ord}_v(a) \equiv 0 \pmod m$, i.e. a è una m-potenza e il polinomio $X^m - a$ è irriducibile. Notiamo infine che quando si aggiungono le radici m-esime, è necessario considerare solo un rappresentante per ogni classe in $K^*/(K^*)^m$. Sia quindi

$$T_S = \{a \in K^*/(K^*)^m : \mathrm{ord}_v(a) \equiv 0 \pmod m \text{ per ogni } v \in M_K \text{ con } v \notin S\},$$

allora

$$L = K(\sqrt[m]{a} : a \in T_S)$$

e questa è un'estensione che soddisfa le ipotesi della Proposizione.
Per cui basta mostrare ora che T_S è finito. Consideriamo quindi la mappa naturale $R_S^* \to T_S$ e mostriamo che è suriettiva. Sia $a \in K^*$ un elemento in T_S, allora l'ideale aR_S è la potenza m-esima di un ideale in R_S. Poiché R_S è un dominio a ideali principali, esiste $b \in K^*$ tale che $aR_S = b^m R_S$ e quindi esiste $u \in R_S^*$ tale che $a = ub^m$. Ciò significa che in T_S a e u sono lo stesso elemento, quindi R_S^* è suriettivo su T_S. Il nucleo della mappa tra essi deve contenere $(R_S^*)^m$ quindi $R_S^*/(R_S^*)^m \to T_S$ è ancora suriettiva (ma in particolare è un isomorfismo). A questo punto si applica il terzo risultato di teoria dei numeri algebrici 4.1.12, ovvero il fatto che R_S^* è un gruppo finitamente generato. Segue subito che T_S è finito.

□

4.2 Il Teorema di discesa

Il risultato ottenuto nella sezione precedente non assicura che $E(K)$ sia finitamente generato (questo vale anche più in generale, ad esempio $\mathbb{R}/m\mathbb{R} = 0$ per ogni intero $m \geq 1$ ma $\mathbb{R}$ ovviamente non è finitamente generato). Occorre quindi definire una nuova proprietà: l'altezza.

Teorema 4.2.1 (Teorema di discesa)**.** *Sia A un gruppo abeliano. Supponiamo che esista una funzione, detta* altezza*, $h : A \to \mathbb{R}$ con le seguenti proprietà:*

1. *Sia $Q \in A$. Allora esiste una costante C_1 che dipende da A e Q tale che*

$$h(P + Q) \leq 2h(P) + C_1 \qquad \text{per ogni } P \in A.$$

2. *Esistono un intero $m \geq 2$ e una costante C_2 dipendente da A tali che*

$$h(mP) \geq m^2 h(P) - C_2 \qquad \text{per ogni } P \in A.$$

3. *Per ogni costante C_3, l'insieme*

$$\{P \in A : h(P) \leq C_3\}$$

è finito.

Supponiamo che per ogni intero m come in 2. il gruppo quoziente A/mA sia finito. Allora A è finitamente generato.

Dimostrazione. Siano $Q_1, \ldots, Q_r \in A$ i rappresentanti dell'insieme finito A/mA e sia $P \in A$. L'idea è quella di far vedere che la differenza tra P e una combinazione lineare dei Q_i è il multiplo di un punto con altezza minore di una certa costante indipendente

da P. Segue allora che i Q_i e tutti i punti con altezza minore di tale costante (che sono finiti) sono generatori per A.
Sia $P = mP_1 + Q_{i_1}$ per qualche $i_1 = 1, \ldots, r$ e analogamente ripetiamo il procedimento: $P_1 = mP_2 + Q_{i_2}, \ldots, P_{n-1} = mP_n + Q_{i_n}$. Applichiamo le proprietà della funzione h a un generico punto tra questi, allora

$$h(P_j) \leq \frac{1}{m^2}(h(mP_j) + C_2) = \frac{1}{m^2}(h(P_{j-1} - Q_{i_j}) + C_2) \leq \frac{1}{m^2}(2h(P_{j-1}) + C_1' + C_2)$$

dove C_1' è il valore massimo delle costanti per $Q = -Q_i$ e dove la prima e l'ultima relazione sono date rispettivamente da 2. e da 1. Si osserva che C_1' e C_2 non dipendono da P. Ora utilizziamo ripetutamente la relazione ottenuta per $h(P_j)$ partendo da P_n:

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^2} + \frac{4}{m^2} + \ldots + \frac{2^{n-1}}{m^2}\right)(C_1' + C_2) \\ &< \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1' + C_2}{m^2 - 2} \leq \frac{1}{2^n} h(P) + \frac{1}{2}(C_1' + C_2) \quad \text{con } m \geq 2. \end{aligned}$$

Per n abbastanza grande si ottiene $h(P_n) \leq 1 + (C_1' + C_2)/2$. Poiché abbiamo scritto P come combinazione lineare di P_n e dei Q_i per le relazioni scritte sopra, cioè

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j},$$

allora segue che ogni punto in A è una combinazione lineare dei punti dell'insieme

$$\{Q_1, \ldots, Q_r\} \cup \left\{ Q \in A : h(Q) \leq 1 + \frac{1}{2}(C_1' + C_2) = C_3 \right\}$$

che è finito per la 3. Allora A è finitamente generato.

□

4.3 Il Teorema di Mordell-Weil su $\mathbb{Q}$

Teorema 4.3.1. *Sia $E/\mathbb{Q}$ una curva ellittica. Allora $E(\mathbb{Q})$ è finitamente generato.*

Sappiamo dal Teorema 4.1.1 che $E(\mathbb{Q})/2E(\mathbb{Q})$ è finito. Dobbiamo trovare una funzione di altezza che soddisfi le proprietà del Teorema 4.2.1.

Definizione 4.3.2 (Altezza su $\mathbb{Q}$)**.** Sia $t \in \mathbb{Q}$ e scriviamo $t = p/q$ con la frazione ridotta ai minimi termini. L'*altezza di t* è definita da

$$H(t) = \max\{|p|, |q|\}.$$

Definizione 4.3.3 (Altezza logaritmica su $E(\mathbb{Q})$)**.** Sia $E(\mathbb{Q})$ data da un'equazione di Weierstrass, allora l'*altezza logaritmica* è definita da

$$h_x : E(\mathbb{Q}) \to \mathbb{R}, \qquad h_x(P) = \begin{cases} \log H(x(P)) & \text{se } P \neq \mathcal{O}, \\ 0 & \text{se } P = \mathcal{O}. \end{cases}$$

Per come è definita, $h_x(P)$ è sempre non negativa.

Il seguente Lemma ci permette di applicare il Teorema di discesa con h_x.

Lemma 4.3.4. *Sia $E/\mathbb{Q}$ una curva ellittica data dall'equazione di Weierstrass $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$.*

1. *Sia $P_0 \in E(\mathbb{Q})$, allora esiste una costante C_1 che dipende da P_0, A e B tale che*

$$h_x(P + P_0) \leq 2h_x(P) + C_1 \qquad \textit{per ogni } P \in E(\mathbb{Q}).$$

2. *Esiste una costante C_2 che dipende da A e B tale che*

$$h_x([2]P) \geq 4h_x(P) - C_2 \qquad \textit{per ogni } P \in E(\mathbb{Q}).$$

3. *Per ogni costante C_3, l'insieme $\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$ è finito.*

Dimostrazione. Esponiamo solo una traccia di dimostrazione, per i calcoli si rimanda a [16] VIII.4 (Lemma 4.2). Per una dimostrazione ancora più dettagliata si veda il procedimento seguito in [17] III §2, III §3.
1. Sia $C_1 > \max\{h_x(P_0), h_x([2]P_0)\}$. Allora la 1. vale per $P_0 = \mathcal{O}$ oppure se $P \in \{\mathcal{O}, \pm P_0\}$. In tutti gli altri casi poniamo

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \qquad \text{e} \qquad P_0 = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right)$$

con tutte le frazioni ridotte ai minimi termini. Sostituiamo P e P_0 nella formula per l'addizione di due punti su E, quindi otteniamo la stima $H(x(P+P_0)) \leq C_1' \max\{|a|^2, |d|^4, |bd|\}$ con C_1' espressione in funzione di A, B, a_0, b_0, d_0. Poiché $H(x(P)) = \max\{|a|^2, |d|^4\}$ è il termine che vogliamo ottenere a destra della relazione, utilizziamo il fatto che $P \in E$ per ottenere la stima $|b| \leq C_1'' \max\{|a|^{3/2}, |d|^3\}$ che sostituiamo in quella precedente:

$$H(x(P + P_0)) \leq C_1' \max\{|a|^2, |d|^4\}.$$

Poiché $H(x(P))^2 = \max\{|a|^2, |d|^4\}$ otteniamo per h_x la prima relazione passando al logaritmo.
2. Sia $C_2 \geq 4 \max\{h_x(T) : T \in E(\mathbb{Q})[2]\}$. Supponiamo $[2]P \neq \mathcal{O}$ e sostituiamo il punto $P = (x, y)$ tale che $x(P) = a/b$ nella formula di duplicazione di E. Otteniamo quindi

che $x([2]P)$ è dato da un rapporto di polinomi del tipo $F(a,b)/G(a,b)$ di cui possiamo calcolare il massimo comun divisore δ. Tramite alcune osservazioni (vedi Sublemma 4.3 in [16] VIII.4) si ottiene $|\delta| \leq |4\Delta|$ dove $\Delta = 4A^3 + 27B^2$ è il discriminante di E a meno di una costante (-16). Si ottiene infine la stima

$$H(x([2]P)) \geq \frac{\max\{|F(a,b)|, |G(a,b)|\}}{|4\Delta|} \geq (2C)^{-1} \max\{|a|^4, |b|^4\}$$

con C dipendente da A e B. Poiché $H(x(P)) = \max\{|a|, |b|\}$ allora passando al logaritmo si ottiene il risultato.
3. Per ogni costante C, l'insieme $\{t \in \mathbb{Q} : H(t) \leq C\}$ è finito: infatti ha al più $(2C+1)^2$ elementi poiché sia il numeratore sia il denominatore di t sono interi compresi tra $-C$ e C. Basta osservare che per ogni x ci sono al più due valori di y con $(x,y) \in E$, allora $\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$ è ancora un insieme finito.

□

Dimostrazione del Teorema 4.3.1. Sappiamo che $E(\mathbb{Q})/2E(\mathbb{Q})$ è finito e dal Lemma 4.3.4 si ha che la funzione di altezza h_x soddisfa le condizioni necessarie per applicare il Teorema di discesa con $m = 2$. Allora $E(\mathbb{Q})$ è finitamente generato.

□

4.4 Altezze su spazi proiettivi

Per poter utilizzare il Teorema di discesa anche nel caso più generale del Teorema di Mordell-Weil, dobbiamo definire una funzione di altezza sui punti K-razionali di una curva ellittica. Definiamo quindi prima l'altezza su uno spazio proiettivo e poi restringiamo ai punti di una curva ellittica.
Nel definire l'altezza in generale, bisogna prestare attenzione al fatto che l'anello degli interi di K non è necessariamente un dominio a ideali principali.
Sappiamo che su $\mathbb{Q}$ esistono due tipi di *valori assoluti standard* $M_{\mathbb{Q}}$, quelli archimedei definiti tramite il valore assoluto usuale

$$|x|_\infty = \max\{x, -x\},$$

e quelli non archimedei o p-adici definiti da

$$\left|p^n \frac{a}{b}\right|_p = p^{-n} \qquad \text{con } p \in \mathbb{Z} \text{ e } a, b \text{ tali che } p \nmid ab.$$

Su un generico campo K l'insieme dei valori assoluti standard M_K contiene tutti i valori assoluti la cui restrizione a $\mathbb{Q}$ coincide con uno dei due precedenti valori.

Definizione 4.4.1. Sia $v \in M_K$. Il *grado locale in* v è la quantità

$$n_v = [K_v : \mathbb{Q}_v]$$

dove K_v e $\mathbb{Q}_v$ sono i completamenti rispetto a v di K e $\mathbb{Q}$.

Riportiamo due risultati di teoria dei numeri algebrici.

Proposizione 4.4.2 (Formula di estensione)**.** *Sia $L/K/\mathbb{Q}$ una torre di campi di numeri e sia $v \in M_K$. Allora*

$$\sum_{\substack{w \in M_L \\ w|v}} n_w = [L : K] n_v,$$

dove $w \mid v$ significa che w ristretto a K è uguale a v.

Dimostrazione. Si veda [10] II §1 (Corollary 1).

□

Proposizione 4.4.3 (Formula di prodotto)**.** *Sia $x \in K^*$. Allora*

$$\prod_{v \in M_K} |x|_v^{n_v} = 1.$$

Dimostrazione. Si veda [10] V §1.

□

Definizione 4.4.4 (Altezza su $\mathbb{P}^N(K)$)**.** Sia $P \in \mathbb{P}^N(K)$ un punto con coordinate omogenee $P = [x_0, \ldots, x_N]$ con $x_0, \ldots, x_N \in K$. L'*altezza di* P relativa a K è

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v}.$$

Esempio 4.4.5 (Altezza su $\mathbb{P}^N(\mathbb{Q})$)**.** Sia $P \in \mathbb{P}^N(\mathbb{Q})$ un punto a coordinate razionali. Poiché $\mathbb{Z}$ è un dominio a ideali principali, possiamo trovare coordinate omogenee $P = [x_0, \ldots, x_N]$ tali che $x_0, \ldots, x_N \in \mathbb{Z}$ e $\mathrm{MCD}(x_0, \ldots, x_N) = 1$. L'*altezza di* P relativa a $\mathbb{Q}$ è la misura naturale

$$H_{\mathbb{Q}}(P) = \max\{|x_0|, \ldots, |x_N|\}.$$

Infatti, per ogni valore assoluto non archimedeo $v \in M_{\mathbb{Q}}$ si ha $|x_i|_v \leq 1$ per ogni i e $|x_i|_v = 1$ per almeno un i poiché gli x_i sono in $\mathbb{Z}$. Quindi al prodotto $H_{\mathbb{Q}}(P)$ contribuisce solo il fattore del valore assoluto archimedeo per cui

$$H_{\mathbb{Q}}(P) = \max\{|x_0|_\infty, \ldots, |x_N|_\infty\}.$$

Con tale definizione, si ottiene anche che per ogni costante C l'insieme $\{P \in \mathbb{P}^N(\mathbb{Q}) : H_{\mathbb{Q}}(P) \leq C\}$ è un insieme finito. Infatti ha al più $(2C+1)^N$ elementi, poiché gli $x_1, \ldots, x_N$ possono assumere tutti i valori tra $-C$ e C (fissiamo $x_0 = 1$).
Quest'ultimo risultato vale anche per K generico, vedi Teorema 4.4.12.

Proposizione 4.4.6. *Sia $P \in \mathbb{P}^N(K)$.*

1. *L'altezza $H_K(P)$ non dipende dalla scelta delle coordinate omogenee per P.*
2. *L'altezza soddisfa $H_K(P) \geq 1$.*
3. *Sia L/K un'estensione finita. Allora $H_L(P) = H_K(P)^{[L:K]}$.*

Dimostrazione. **1.** Consideriamo un'altra scelta di coordinate omogenee $[\lambda x_0, \ldots, \lambda x_N]$ per P con $\lambda \in K^*$. Usando la Formula di prodotto 4.4.3 si ha

$$\prod_{v \in M_K} \max\{|\lambda x_0|_v, \ldots, |\lambda x_N|_v\}^{n_v} = \prod_{v \in M_K} |\lambda|_v^{n_v} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v}.$$

2. Dato un qualsiasi punto P nello spazio proiettivo, è sempre possibile trovare coordinate omogenee tali che almeno una di esse valga 1.
3. Basta calcolare $H_L(P) =$

$$\prod_{w \in M_L} \max\{|x_i|_w\}^{n_w} = \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max\{|x_i|_v\}^{n_w} = \prod_{v \in M_K} \max\{|x_i|_v\}^{[L:K]n_v} = H_K(P)^{[L:K]}$$

poiché $x_i \in K$ e per la Formula 4.4.2.

□

Spesso è utile considerare una funzione di altezza che non sia collegata a un particolare campo di numeri. Utilizziamo quindi il punto 3. della Proposizione 4.4.6 per creare tale funzione.

Definizione 4.4.7 (Altezza assoluta su $\mathbb{P}^N(K)$)**.** Sia $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$. L'*altezza assoluta di* P è data da

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]}$$

con K campo di numeri scelto tale che $P \in \mathbb{P}^N(K)$. Consideriamo per $H(P)$ la radice positiva. Questa definizione è ben posta indipendentemente dalla scelta di K perché, se consideriamo due campi K, L tali che L/K è un'estensione finita, allora abbiamo

$$H_L(P)^{1/[L:\mathbb{Q}]} = (H_K(P)^{[L:K]})^{1/[L:\mathbb{Q}]} = H_K(P)^{1/[K:\mathbb{Q}]}$$

per la 3. della Proposizione 4.4.6. La 2. della stessa Proposizione mostra che $H(P) \geq 1$.

Enunciamo ora alcune importanti proprietà delle altezze, che utilizzeremo poi nella sezione seguente: per le relative dimostrazioni si rimanda a [16] VIII.5 (Theorem 5.6, Theorem 5.9, Theorem 5.10, Theorem 5.11).
I due seguenti risultati mostrano come si comporta l'altezza in presenza di mappe tra spazi proiettivi.

Teorema 4.4.8. *Sia $F : \mathbb{P}^N \to \mathbb{P}^M$ un morfismo di grado d, i.e. tale che $F(P) = [f_0(P), \ldots, f_M(P)]$ e gli f_i sono polinomi omogenei di grado d in $\bar{\mathbb{Q}}[X_0, \ldots, X_n]$ che non hanno zeri comuni in $\bar{\mathbb{Q}}^N$ tranne $X_0 = \ldots = X_N = 0$.*
Allora esistono due costanti positive C_1 e C_2 dipendenti da F tali che

$$C_1 H(P)^d \leq H(F(P)) \leq C_2 H(P)^d \qquad \text{per ogni } P \in \mathbb{P}^N(\mathbb{Q}).$$

Corollario 4.4.9. *Sia $A \in GL_{N+1}(\bar{\mathbb{Q}})$. Indichiamo ancora con A l'automorfismo $A : \mathbb{P}^N \to \mathbb{P}^N$ indotto dalla moltiplicazione per la matrice A. Esistono allora C_1 e C_2 costanti positive tali che*

$$C_1 H(P) \leq H(AP) \leq C_2 H(P) \qquad \text{per ogni } P \in \mathbb{P}^N(\mathbb{Q}).$$

Dimostrazione. Si ottiene direttamente dal Teorema 4.4.8 con A morfismo di grado 1. □

Vediamo ora la relazione tra i coefficienti di un polinomio e l'altezza delle sue radici.

Teorema 4.4.10. *Sia $f(T) = a_0 T^d + a_1 T^{d-1} + \ldots + a_d = a_0(T - \alpha_1) \cdots (T - \alpha_d) \in \bar{\mathbb{Q}}[T]$ un polinomio di grado d. Allora*

$$2^{-d} \prod_{j=1}^{d} H(\alpha_j) \leq H([a_0, \ldots, a_d]) \leq 2^{d-1} \prod_{j=1}^{d} H(\alpha_j)$$

dove $H(x) = H([x, 1])$ per ogni $P \in \bar{\mathbb{Q}}$.

Il seguente risultato mostra che l'azione del gruppo di Galois non modifica l'altezza di un punto.

Teorema 4.4.11. *Sia $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$ e sia $\sigma \in G_{\bar{\mathbb{Q}}/\mathbb{Q}}$. Allora $H(P^\sigma) = H(P)$.*

Infine si ottiene il risultato importante per cui il numero di punti ad altezza (proiettiva) limitata è finito.

Teorema 4.4.12. *Siano C e d costanti, allora l'insieme*

$$\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) : H(P) \leq C \text{ e } [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}$$

è un insieme finito di punti con $\mathbb{Q}(P) = \mathbb{Q}(x_0/x_i, \ldots, x_N/x_i)$ campo minimo di definizione di $P = [x_0, \ldots, x_n]$.
In particolare per ogni campo di numeri K vale che

$$\{P \in \mathbb{P}^N(K) : H_K(P) \leq C\}$$

è un insieme finito.

4.5 Altezze su curve ellittiche e il Teorema di Mordell-Weil

Vediamo ora come la teoria generale delle funzioni di altezza appena vista possa essere utilizzata per definire l'altezza sulle curve ellittiche. In particolare ciò che ancora manca per dimostrare il Teorema di Mordell-Weil per un campo di numeri arbitrario è il legame tra queste funzioni di altezza e la legge di addizione sulle curve ellittiche. Perché ciò sia possibile, abbiamo bisogno di una funzione di altezza che abbia un comportamento additivo e non moltiplicativo. Questo motiva la scelta del logaritmo nella definizione seguente.

Definizione 4.5.1 (Altezza logaritmica assoluta su $\mathbb{P}^N(K)$)**.** L'*altezza logaritmica assoluta* su uno spazio proiettivo è la funzione

$$h : \mathbb{P}^N(\bar{\mathbb{Q}}) \to \mathbb{R}, \qquad h(P) = \log H(P).$$

Poiché sappiamo che $H(P) \geq 1$ (Definizione 4.4.7), allora $h(P) \geq 0$ per ogni P.

Riprendendo l'Esempio 1.5.2, ricordiamo che una funzione $f \in \bar{K}(E)$ non costante definisce un morfismo suriettivo $f : E \to \mathbb{P}^1$ tale che $f(P) = [f(P), 1]$ tranne nel caso in cui P sia un polo per cui si ha $f(P) = [1, 0]$. Allora f manda un punto $P \in E(K)$ in $f(P) \in \mathbb{P}^1(K)$.

Definizione 4.5.2 (ALTEZZA SU UNA CURVA ELLITTICA)**.** Sia E/K una curva ellittica e sia $f \in \bar{K}(E)$ una funzione. L'*altezza su E* relativa a f è la funzione

$$h_f : E(\bar{K}) \to \mathbb{R}, \qquad h_f(P) = h(f(P)).$$

Possiamo ora proporre anche per questa nuova altezza il risultato ottenuto nel Teorema 4.4.12: l'insieme dei punti ad altezza limitata è finito.

Proposizione 4.5.3. *Sia E/K una curva ellittica e sia $f \in K(E)$ una funzione non costante. Allora per ogni costante C, l'insieme*

$$\{P \in E(K) : h_f(P) \leq C\}$$

è un insieme finito di punti.

Dimostrazione. Come detto poco fa, la funzione $f \in K(E)$ manda $P \in E(K)$ in $Q = f(P) \in \mathbb{P}^K$. Quindi f definisce una mappa finita tra l'insieme $\{P \in E(K) : h_f(P) = \log H(Q) \leq C\}$ nell'insieme $\{Q \in \mathbb{P}^1(K) : H(Q) \leq \exp^C\}$. Sappiamo dal Teorema 4.4.12 che questo insieme è finito, quindi si ottiene il risultato.

□

Mostriamo ora la proprietà fondamentale che lega le funzioni di altezza alla legge di addizione su una curva ellittica. Aggiungiamo prima un'osservazione sulle funzioni pari in $\bar{K}(E)$.

Osservazione 4.5.4. Sia f una funzione in $\bar{K}(E) = \bar{K}(x,y)$ (vedi Corollario 2.1.11). Allora f è pari, i.e. $f \circ [-1] = f$, se e solo se $f \in \bar{K}(x)$.

Dimostrazione. $\Leftarrow$) Sia $f \in \bar{K}(x)$. Dalla formula di negazione che dà le coordinate di $-P$ (vedi 2.2.5 punto 1.) si ottiene subito che f è pari.
$\Rightarrow$) Sia $f \in \bar{K}(x,y)$ pari. Consideriamo un'equazione di Weierstrass per E, quindi scriviamo f come $f(x,y) = g(x) + h(x)y$ per qualche $g, h \in \bar{K}(x)$. Poiché f è pari, si ha $f(x,y) = f(x, -y - a_1x - a_3) \Leftrightarrow g(x) + h(x)y = g(x) + h(x)(-y - a_1x - a_3)$ $\Leftrightarrow h(x)(2y + a_1x + a_3) = 0$. Poiché questo deve valere per ogni $x \in E$ allora l'unica possibilità è $h(x) = 0$, altrimenti si avrebbe $2 = a_1 = a_3$ che implica $\Delta = 0$. Quindi $f(x,y) = g(x) \in \bar{K}(x)$.

□

Teorema 4.5.5. *Sia E/K una curva ellittica e sia $f \in K(E)$ una funzione pari. Allora per ogni $P, Q \in E(\bar{K})$ si ha*

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1)$$

dove $O(1)$ contiene le costanti che dipendono da E e da f ma che sono indipendenti da P e Q.

Dimostrazione. Scegliamo un'equazione di Weierstrass della forma $y^2 = x^3 + Ax + B$ per E/K. Per essa la formula di negazione è semplicemente $-P = (x, -y)$ per ogni $P = (x,y) \in E$. Dimostriamo prima il Teorema per una funzione particolare $f = x$ proiezione su x. Poi il caso generale si ottiene grazie ad un Lemma.
Iniziamo osservando che $h_x(\mathcal{O}) = 0$ e $h_x(-P) = h_x(P)$, quindi il risultato è ovvio se $P = \mathcal{O}$ oppure $Q = \mathcal{O}$. Supponiamo quindi $P \neq \mathcal{O}$ e $Q \neq \mathcal{O}$ e scriviamo $x(P) = [x_1, 1]$, $x(Q) = [x_2, 1]$, $x(P+Q) = [x_3, 1]$, $x(P-Q) = [x_4, 1]$. Scriviamo quindi x_3 e x_4 in funzione di x_1 e x_2 utilizzando la formula di addizione e negazione per il particolare tipo di equazione:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 + x_2), \qquad x_4 = \left(\frac{-y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 + x_2).$$

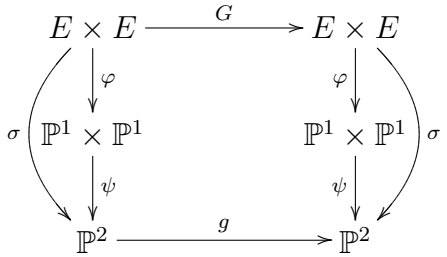
Tramite esse, scriviamo le espressioni di $x_3 + x_4$ e x_3x_4 sostituendo al posto di y_i^2 la quantità $x_i^3 + Ax_i + B$ dall'equazione di E per $i = 1, 2$. Otteniamo:

$$x_3 + x_4 = \frac{2(x_1+x_2)(A + x_1x_2) + 4B}{(x_1+x_2)^2 - 4x_1x_2}, \qquad x_3x_4 = \frac{(x_1x_2 - A)^2 - 4B(x_1+x_2)}{(x_1+x_2)^2 - 4x_1x_2}.$$

Definiamo ora una mappa $g : \mathbb{P}^2 \to \mathbb{P}^2$ tale che

$$g([t,u,v]) = [u^2 - 4tv, 2u(At+v) + 4Bt^2, (v-At)^2 - 4Btu].$$

Allora esiste una diagramma commutativo



con $G(P,Q) = (P+Q, P-Q)$ e σ data dalla composizione delle mappe φ e ψ tali che

$$\varphi(P,Q) = (x(P), x(Q)) \qquad \text{e} \qquad \psi([\alpha_1,\beta_1],[\alpha_2,\beta_2]) = [\beta_1\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1, \alpha_1\alpha_2].$$

Vogliamo mostrare che t, u, v nella mappa g rappresentano $1, x_1 + x_2, x_1x_2$ e quindi $g([t,u,v])$ diventa $[1, x_3 + x_4, x_3x_4]$. Poiché i tre polinomi omogenei che definiscono g non hanno zeri comuni diversi da $t = u = v = 0$, segue che g è un morfismo.
Sia allora $g([t,u,v]) = 0$. Se $t = 0$, allora da $u^2 - 4tv = 0$ e $(v-At)^2 - 4Btu = 0$ si ottiene $u = v = 0$. Supponiamo ora $t \neq 0$ e definiamo la quantità $x = u/2t$. L'equazione $u^2 - 4tv = 0$ si traduce in $x^2 = v/t$. Dividiamo le altre due equazioni $2u(At+v) + 4Bt^2 = 0$ e $(v-At)^2 - 4Btu = 0$ per t^2 e, riscrivendole in funzione di x otteniamo

$$\lambda(x) = 4x(A + x^2) + 4B = 4x^3 + 4Ax + 4B = 0,$$
$$\mu(x) = (x^2 - A)^2 - 8Bx = x^4 - 2Ax^2 - 8Bx + A^2 = 0.$$

Il rapporto μ/λ corrisponde esattamente alla formula di duplicazione corrispondente all'equazione di Weierstrass con coefficienti A e B. Per mostrare quindi che $\lambda(x)$ e $\mu(x)$ non hanno radici comuni è sufficiente verificare che esistono f_1, g_1 tali che $f_1(x)\lambda(x) - g_1(x)\mu(x)$ è una costante. In particolare si verifica (vedi già citato Sublemma 4.3 in [16] VIII.4)

$$(12x^2 + 16A)\lambda(x) - (3x^3 - 5Ax - 27B)\mu(x) = 4(4A^3 + 27B^2) \neq 0.$$

Qui gioca un ruolo fondamentale la non singolarità di E. Quindi g è un morfismo.
Ritornando al diagramma e guardando le altezze otteniamo

$$h(\sigma(P+Q, P-Q)) = h(\sigma \circ G(P,Q)) = h(g \circ \sigma(P,Q)) = 2h(\sigma(P,Q)) + O(1)$$

per il Teorema 4.4.8: infatti g è un morfismo di grado 2 per cui il Teorema assicura che $C_1 H(\sigma(P,Q))^2 \leq H(g \circ \sigma(P,Q)) \leq C_2 H(\sigma(P,Q))^2$ e passando all'altezza logaritmica si

ottiene il risultato.
Per finire la dimostrazione con $f = x$ basta mostrare che per ogni $R_1, R_2 \in E(\bar{K})$

$$h(\sigma(R_1, R_2)) = h_x(R_1) + h_x(R_2) + O(1). \tag{4.1}$$

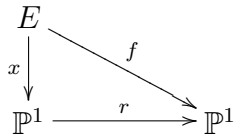
Supponiamo infatti che valga tale relazione, allora applicandola ad entrambi i membri di $h(\sigma(P+Q, P-Q)) = 2h(\sigma(P, Q)) + O(1)$ si ottiene l'affermazione del Teorema. Vediamo quindi che vale (4.1).
Se $R_1 = \mathcal{O}$ oppure $R_2 = \mathcal{O}$, si ottiene $h(\sigma(R_1, R_2)) = h([1, 0, 0]) = 0 = h_x(R_1) + h_x(R_2)$.
Siano quindi $R_1 \neq \mathcal{O}$ e $R_2 \neq \mathcal{O}$, allora $x(R_1) = [\alpha_1, 1]$ e $x(R_2) = [\alpha_2, 1]$ per cui si ha

$$h(\sigma(R_1, R_2)) = h([1, \alpha_1 + \alpha_2, \alpha_1\alpha_2]) \qquad \text{e} \qquad h_x(R_1) + h_x(R_2) = h(\alpha_1) + h(\alpha_2).$$

Applichiamo quindi il Teorema 4.4.10 al polinomio $(T + \alpha_1)(T + \alpha_2)$ e otteniamo il risultato. Infatti dal Teorema si ha $2^{-2}H(\alpha_1)H(\alpha_2) \leq H([1, \alpha_1 + \alpha_2, \alpha_1\alpha_2]) \leq 2H(\alpha_1)H(\alpha_2)$ e quindi passando ai logaritmi $h(\alpha_1) + h(\alpha_2) - \log 4 \leq h([1, \alpha_1 + \alpha_2, \alpha_1\alpha_2]) \leq h(\alpha_1) + h(\alpha_2) + \log 2$.
Infine, per provare il Teorema nel caso generale di $f \in K(E)$, utilizziamo un Lemma.

Lemma 4.5.6. *Siano $f, g \in K(E)$ funzioni pari. Allora* $\deg g \; h_f = \deg f \; h_g + O(1)$.

Dimostrazione. Siano $x, y \in K(E)$ coordinate di Weierstrass per E/K. Dall'Osservazione 4.5.4 sappiamo che una funzione in $K(E)$ è pari se e solo se sta in $K(x)$. Quindi esiste una funzione $r(x) \in K(x)$ tale che il seguente diagramma commuti:



Poiché r è un morfismo per la Proposizione 1.5.1, possiamo utilizzare il Teorema 4.4.8:

$$h_f = \deg r \; h_x + O(1)$$

poiché $C_1 H(x)^{\deg r} \leq H(r \circ x) \leq C_1 H(x)^{\deg r}$ e basta guardare i logaritmi. Osserviamo che $\deg x = 2$ poiché sappiamo che il grado dell'estensione $K(E)/K(x)$ è 2 (vedi Corollario 2.1.11), quindi $\deg f = \deg x \;\; \deg r = 2 \deg r$. Unendo questo risultato al precedente otteniamo $2h_f = \deg f \; h_x + O(1)$ e, ripetendo il procedimento in modo del tutto analogo per g, abbiamo $2h_g = \deg g \; h_x + O(1)$. Unendo questi due risultati si ottiene il Lemma. □

Poiché sappiamo che $\deg x = 2$, allora per il Lemma abbiamo

$$h_f = \frac{1}{2} \deg f \; h_x + O(1).$$

Basta quindi moltiplicare per $(\deg f)/2$ entrambi i membri della relazione del Teorema che già abbiamo ottenuto per h_x per ottenere la stessa espressione per h_f con f qualsiasi. □

Corollario 4.5.7. *Sia E/K una curva ellittica e sia $f \in K(E)$ una funzione pari.*

1. *Sia $Q \in E(\bar{K})$, allora $h_f(P+Q) \leq 2h_f(P) + O(1)$ per ogni $P \in E(\bar{K})$ con $O(1)$ che dipende da E, f e Q.*
2. *Sia $m \in \mathbb{Z}$, allora $h_f([m]P) = m^2 h_f(P) + O(1)$ per ogni $P \in E(\bar{K})$ con $O(1)$ che dipende da E, f e m.*

Dimostrazione. **1.** Si ottiene direttamente dal Teorema 4.5.5 poiché $h_f(P-Q) \geq 0$ e Q è fissato.
2. Sia f pari e consideriamo $m \geq 0$. Il risultato è banale per $m = 0, 1$. Usiamo l'induzione: supponiamo che il risultato valga per $m-1$ e per m e utilizziamo il Teorema 4.5.5 con $[m]P$ e P al posto rispettivamente di P e Q. Osservando che $[m+1]P = [m]P + P$ e $[m-1]P = [m]P - P$, otteniamo:

$$\begin{aligned} h_f([m+1]P) &= -h_f([m-1]P) + 2h_f([m]P) + 2h_f(P) + O(1) \\ &= (-(m-1)^2 + 2m^2 + 2)h_f(P) + O(1) \end{aligned}$$

dall'ipotesi induttiva. Si ha quindi $h_f([m+1]P) = (m+1)^2 h_f(P) + O(1)$.

□

Osservazione 4.5.8. I risultati 4.5.5, 4.5.6, 4.5.7 valgono anche se f è dispari poiché in tal caso f^2 è pari e vale che $h_{f^2} = 2h_f$. In realtà questi risultati valgono per una f qualsiasi in $K(E)$ a meno di un ε. In particolare riscriviamo la 2. del Corollario 4.5.7 per $\varepsilon > 0$

$$(1-\varepsilon)m^2 h_f + O(1) \leq h_f \circ [m] \leq (1+\varepsilon)m^2 h_f + O(1)$$

con $O(1)$ dipendente da E, f, m, ε.

Completiamo dunque ora la dimostrazione del nostro Teorema.

Teorema 4.5.9 (Mordell-Weil)**.** *Sia K un campo di numeri e sia E/K una curva ellittica. Allora il gruppo $E(K)$ è finitamente generato.*

Dimostrazione. Sia f una funzione non costante in $K(E)$, ad esempio anche la coordinata x di un'equazione di Weierstrass. Il Teorema segue direttamente dal Teorema debole 4.1.1 con $m = 2$ e dal Teorema di discesa 4.2.1 se mostriamo che una funzione di altezza $h_f : E(K) \to \mathbb{R}$ ha le tre proprietà:

(a) Sia $Q \in E(K)$, allora esiste una costante C_1 dipendente da E, f e Q tale che $h_f(P+Q) \leq 2h_f(P) + C_1$ per ogni $P \in E(K)$.

(b) Esiste una costante C_2 dipendente da E e da f tale che $h_f([2]P) \geq 4h_f(P) - C_2$ per ogni $P \in E(K)$.

(c) Per ogni costante C_3, l'insieme $\{P \in E(K) : h_f(P) \leq C_3\}$ è un insieme finito di punti.

Allora (a) è data dalla 1. del Corollario 4.5.7, (b) è data dalla 2. del Corollario 4.5.7 e (c) corrisponde alla Proposizione 4.5.3. La dimostrazione del Teorema di Mordell-Weil è completa.

□

Punti di torsione

Dire che il gruppo abeliano $E(K)$ è finitamente generato, equivale a dire $E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^r$, cioè $E(K)$ si decompone nella sua parte di torsione e in un gruppo (abeliano) libero di rango finito r, dove r dipende solo da $E(K)$. Questo risultato è dovuto al Teorema Fondamentale di Struttura dei gruppi abeliani finitamente generati: vedi [5] 5.2 (Theorem 3).
In generale il rango r risulta ancora "misterioso", ci sono più congetture che risultati provati che lo riguardano, e spesso non è semplice calcolare r o equivalentemente non è semplice trovare un insieme di generatori per $E(K)/E(K)_{\text{tors}}$. Per qualche informazione si veda [9] IV §6, IV §7 e [11] 16.
Per la parte di torsione invece le cose risultano meno complicate. Presentiamo solo alcuni dei risultati importanti (per approfondimenti si veda [8] 1 §3, 5 §5, 5 §6, [9] V §1, V §6, [11] 8).
Innanzitutto osserviamo che il Teorema di Mordell-Weil conferma il risultato già ottenuto attraverso lo studio dei campi locali: il gruppo dei punti di torsione razionali su una curva ellittica è finito. Riformuliamo il Teorema 3.3.6 per campi globali.

Teorema 4.5.10. *Sia E/K una curva ellittica con equazione di Weierstrass (2.2) con $a_i \in R$ anello degli interi di K. Sia $P \in E(K)$ un punto di torsione con ordine esattamente $m \geq 2$.*

1. *Se m non è potenza di un primo, allora $x(P), y(P) \in R$.*
2. *Se $m = p^n$ con p primo, allora per ogni $v \in M_K^0$ si ha $ord_v x(P) \geq -2r_v$ e $ord_v y(P) \geq -3r_v$ dove*

$$r_v = \left\lfloor \frac{ord_v(p)}{p^n - p^{n-1}} \right\rfloor \qquad \text{con } \lfloor\ \rfloor \text{ parte intera.}$$

In particolare, se $ord_v(p) = 0$, allora $x(P), y(P)$ sono v-interi.

Il seguente risultato mostra che su $\mathbb{Q}$ esistono condizioni anche meno forti rispetto a quelle date nel Teorema 4.5.10 (esiste anche una generalizzazione di tale risultato per un campo di numeri arbitrario).

Corollario 4.5.11 (Nagell, Lutz)**.** *Sia $E/\mathbb{Q}$ una curva ellittica con equazione di Weierstrass $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$. Supponiamo che $P \in E(\mathbb{Q})$ sia un punto di torsione non banale. Allora*

1. *$x(P), y(P) \in \mathbb{Z}$.*
2. *$[2]P = \mathcal{O}$ oppure $y(P)^2$ divide $4A^3 + 27B^2$.*

Dimostrazione. **1.** Sia P di ordine esattamente $m \geq 2$. Se $m = 2$ allora $y(P) = 0$, quindi $x(P) \in \mathbb{Z}$ poiché è radice di un polinomio monico a coefficienti interi. Se $m > 2$ allora il risultato si ottiene dal Teorema 4.5.10: in particolare per il punto 2. si ha necessariamente $r_v = 0$.
2. Assumiamo $[2]P \neq \mathcal{O}$ quindi $y(P) \neq 0$. Allora applicando 1. a P e $[2]P$ si ha in particolare $x(P), y(P), x([2]P) \in \mathbb{Z}$. Scriviamo

$$\psi(X) = X^4 - 2AX^2 - 8BX + A^2, \qquad \varphi(x) = X^3 + AX + B,$$

allora la formula di duplicazione su E diventa $x([2]P) = \varphi(x(P))/4\psi(x(P))$. Per il già citato Sublemma 4.3 in [16] VIII.4 sappiamo che vale l'identità

$$f(X)\varphi(X) - g(X)\psi(X) = 4A^3 + 27B^2$$

dove $f(X) = 3X^2 + 4A$ e $g(X) = 3X^3 - 5AX - 27B$. Poniamo $X = x(P)$ e, usando la formula di duplicazione e il fatto che $y(P)^2 = \psi(x(P))$, scriviamo

$$y(P)^2\Big(4f(x(P))x([2]P) - g(x(P))\Big) = 4A^3 + 27B^2.$$

Poiché le quantità che compaiono sono tutte intere, allora $y(P)^2$ deve dividere $4A^3+27B^2$. □

Concludiamo con un Teorema che mostra come in generale non sia vero che, dato un qualsiasi primo p, esiste una curva ellittica $E/\mathbb{Q}$ tale che $E(\mathbb{Q})$ contiene un punto di ordine p.

Teorema 4.5.12 (Mazur)**.** *Sia $E/\mathbb{Q}$ una curva ellittica. Allora il sottogruppo di torsione $E_{tors}(\mathbb{Q})$ di $E(\mathbb{Q})$ è isomorfo a uno dei seguenti 15 gruppi:*

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z} \quad & \text{con } 1 \leq N \leq 10 \text{ o } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad & \text{con } 1 \leq N \leq 4. \end{aligned}$$

Bibliografia

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*, chapter 1, 2, 5, 9. Addison-Wesley, Reading, MA, 1969.

[2] J. W. S. Cassels. *Lectures on Elliptic Curves*, volume 24 of *London Mathematical Society Student Texts*, chapter 6, 7, 8, 9, 10, 12, 13, 15, 17. Cambridge University Press, Cambridge, 1991.

[3] J. W. S. Cassels and A. Fröhlich. *Algebraic Number Theory*, chapter I, II, III. Academic Press, San Diego, CA, 1967.

[4] P. M. Cohn. *Algebra, Volume II*, chapter 9. John Wiley & Sons, London, second edition, 1989. (First edition, 1977).

[5] D. S. Dummit and R. M. Foote. *Abstract Algebra*, chapter 5, 14, 15, 16, 17. John Wiley & Sons, Hoboken, NJ, third edition, 2004. (First edition, 1990).

[6] W. Fulton. *Algebraic Curves. An Introduction to Algebraic Geometry*, chapter 1, 2, 4, 5, 6, 7, 8. Addison-Wesley, Redwood City, CA, 1989. (Reprint of 1969 original).

[7] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*, chapter I, II, IV. Springer-Verlag, New York, 1977.

[8] D. Husemöller. *Elliptic Curves*, volume 111 of *Graduate Texts in Mathematics*, chapter 1, 3, 4, 5, 6. Springer-Verlag, New York, second edition, 2004. (First edition, 1987).

[9] A. W. Knapp. *Elliptic Curves*, volume 40 of *Mathematical Notes*, chapter I, II, III, IV, V. Princeton University Press, Princeton, NJ, 1992.

[10] S. Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*, chapter I, II, V. Springer-Verlag, New York, 1984.

[11] J. S. Milne. Elliptic curves, 1996. Notes for Math 679, University of Michigan. (v1.01).

[12] J. S. Milne. Algebraic geometry, 2009. Available at www.jmilne.org/math/. (v5.20).

[13] J. S. Milne. Algebraic number theory, 2009. Available at www.jmilne.org/math/. (v3.02).

[14] I. R. Shafarevich. *Basic Algebraic Geometry 1*, chapter I, III. Study Edition. Springer-Verlag, Berlin, second edition, 1994. (First edition, 1977).

[15] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*, chapter III, IV. Springer-Verlag, New York, 1994.

[16] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*, chapter I, II, III, VII, VIII. Springer Science+Business Media, New York, second edition, 2009. (First edition, 1986).

[17] J. H. Silverman and J. T. Tate. *Rational Points on Elliptic Curves*, chapter I, II, III, IV. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[18] J. T. Tate. The arithmetic of elliptic curves. *Inventiones math.*, 23:179–206, 1974.