UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

Curve ellittiche: La Famiglia di Legendre

Relatore:	**Prof. Matteo Longo**
Laureando:	**Leonardo Gagliardoni**
Matricola:	**1233841**

Anno Accademico 2022/2023

15/12/2023

Contenuti

CAPITOLO I

Introduzione

Lo studio delle curve ellittiche è uno dei settori di maggiore importanza della matematica moderna. Ad esempio la dimostrazione del famoso ultimo teorema di Fermat di Andrew Wiles ne fa utilizzo, sono usate alla base di crittosistemi e per la fattorizzazione di interi. Tuttavia questo non vuol dire che la conoscenza attuale sia esaustiva, esistono numerose congetture da provare che rendono questo settore fertile per la ricerca (ad esempio la congettura di Birch e Swinnerton-Dyer, uno dei problemi per il millennio).

Lo scopo di questa trattazione è di introdurre alle curve ellittiche il lettore e cercare di fargli coltivare un'intuizione delle loro proprietà andando ad approfondire una certa classe di curve: la così detta Famiglia di Legendre. Per la lettura sono richieste nozioni base di analisi, algebra e geometria.

Nel primo capitolo si riprendono gli spazi affini e proiettivi, si introducono le varietà e le proprietà fondamentali di queste e delle loro mappe. A seguire c'è una rapida esposizione dei principi di geometria algebrica che servono poi per andare a definire, nel capitolo tre, cosa sia una curva ellittica. Si enunciano quindi le proprietà di base delle curve ellittiche, fornendo un primo metodo per classificarle e definendo una legge di gruppo sui loro punti. Infine il capitolo cinque è dedicato interamente a presentare cosa succede se invece di parlare di curve ellittiche in generale ci si restringe a parlare di curve di Legendre.

1. Notazioni

Per il resto dell'elaborato si useranno le seguenti notazioni:

$\mathbb{N}$	insieme dei numeri naturali (0 compreso),
$\mathbb{Z}$	insieme dei numeri interi,
$\mathbb{Q}$	insieme dei numeri razionali,
$\mathbb{R}$	insieme dei numeri reali,
$\mathbb{C}$	insieme dei numeri complessi,
$\mathbb{K}$	un campo perfetto,
$\bar{\mathbb{K}}$	una chiusura algebrica fissata di $\mathbb{K}$,
$G_{\bar{\mathbb{K}}/\mathbb{K}}$	il gruppo di Galois di $\bar{\mathbb{K}}/\mathbb{K}$,
R^*	il gruppo degli elementi invertibili di un generico anello R.

Quando si dirà che una proprietà vale per quasi ogni $a \in A$ si intende che vale per ogni $a \in A$ a meno di un numero finito di elementi.

CAPITOLO II

Nozioni preliminari

1. Spazi affini e proiettivi

DEFINIZIONE II.1.1. Fissato $n \in \mathbb{Z}, n > 0$ si chiama *spazio affine su* $\mathbb{K}$ l'insieme

$$\mathbb{A}^n = \mathbb{A}^n(\bar{\mathbb{K}}) = \{(x_1, \ldots, x_n) \colon x_i \in \bar{\mathbb{K}},\ \forall i\}.$$

Gli elementi di $\mathbb{A}^n$ sono detti *punti*. Dato un punto $P = (x_1, \ldots, x_n) \in \mathbb{A}^n$, i valori $x_1, \ldots, x_n$ sono le *coordinate* di P. Si chiama *dimensione* di $\mathbb{A}^n$ la quantità

$$\dim(A^n) = n.$$

Il sottoinsieme di $\mathbb{A}^n(\bar{\mathbb{K}})$ dato dai punti a coordinate in $\mathbb{K}$ è detto *insieme dei punti* $\mathbb{K}$*-razionali di* $\mathbb{A}^n$ ed è indicato con

$$\mathbb{A}^n(\mathbb{K}) = \{(x_1, \ldots, x_n) \colon x_i \in \mathbb{K},\ \forall i\}.$$

OSSERVAZIONE II.1.2. Il gruppo di Galois $G_{\bar{\mathbb{K}}/\mathbb{K}}$ agisce in modo naturale su $\mathbb{A}^n$ coniugando le coordinate dei punti: dato $P = (x_1, \ldots, x_n) \in \mathbb{A}^n$ e $\sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}$ si ha

$$P^\sigma = (x_1^\sigma, \ldots, x_n^\sigma).$$

I punti $\mathbb{K}$-razionali di $\mathbb{A}^n$ si possono quindi caratterizzare come

$$\mathbb{A}^n(\mathbb{K}) = \{P \in \mathbb{A}^n \colon P^\sigma = P,\ \forall \sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}\}.$$

Si consideri ora lo spazio affine $\mathbb{A}^{n+1}$. Dati due punti $P, Q \in \mathbb{A}^{n+1}$ con coordinate

$$P = (p_0, p_1, \ldots, p_n), \quad Q = (q_0, q_1, \ldots, q_n),$$

si denota $P \sim Q$ l'esistenza di un $\lambda \in \bar{\mathbb{K}}^*$ tale che $p_i = \lambda q_i$, $\forall i$. La relazione tra punti $\sim$ è una relazione di equivalenza, infatti

(1) $P \sim P$ in quanto per $\lambda = 1 \in \bar{\mathbb{K}}^*$ vale $p_i = \lambda p_i$, $\forall i$.
(2) $P \sim Q$ implica l'esistenza di un $\lambda \in \bar{\mathbb{K}}^*$ tale che $p_i = \lambda q_i$, $\forall i$. Segue che $q_i = (1/\lambda)p_i$ e perciò $Q \sim P$.
(3) $P \sim Q, Q \sim R$ implica l'esistenza di $\lambda, \mu \in \bar{\mathbb{K}}^*$ tali che $p_i = \lambda q_i, q_i = \mu r_i$, $\forall i$. Segue che $p_i = (\lambda\mu) r_i$ e perciò $P \sim R$.

DEFINIZIONE II.1.3. Fissato $n \in \mathbb{Z}, n > 0$ si chiama *spazio proiettivo su* $\mathbb{K}$ l'insieme delle classi di equivalenza

$$\mathbb{P}^n = \mathbb{P}^n(\bar{\mathbb{K}}) = \left(\mathbb{A}^{n+1} \backslash \{0\}\right) / \sim .$$

Gli elementi di $\mathbb{P}^n$ sono detti *punti (proiettivi)*. Dato un punto $P = (x_0, \ldots, x_n) \in \mathbb{A}^{n+1} \backslash \{0\}$ la sua classe di equivalenza è denotata con $[x_0 : \cdots : x_n]$, i valori $x_0, \ldots, x_n$ sono detti *coordinate omogenee* del

rispettivo punto in $\mathbb{P}^n$. Il sottoinsieme di $\mathbb{P}^n(\bar{\mathbb{K}})$ dato dai punti a coordinate omogenee in $\mathbb{K}$ è detto *insieme dei punti* $\mathbb{K}$*-razionali di* $\mathbb{P}^n$ ed è indicato con

$$\mathbb{P}^n(\mathbb{K}) = \{[x_0 : \cdots : x_n] \colon x_i \in \mathbb{K},\ \forall i\}.$$

Osservazione II.1.4. Le coordinate omogenee di un punto $P \in \mathbb{P}^n$ non sono univoche, infatti se $P = [x_0 : \cdots : x_n]$ allora anche $[\lambda x_0 : \cdots : \lambda x_n]$ dove $\lambda \in \bar{\mathbb{K}}^*$ sono coordinate omogenee per P. Se P è in particolare un punto $\mathbb{K}$-razionale, non è perciò detto che $x_0, \ldots, x_n$ siano tutti in $\mathbb{K}$. È altresì vero che, preso un indice i tale che $x_i \neq 0$, si ha $x_j/x_i \in \mathbb{K}$, $\forall i$.

Osservazione II.1.5. Il gruppo di Galois $G_{\bar{\mathbb{K}}/\mathbb{K}}$ agisce su $\mathbb{P}^n$ coniugando le coordinate omogenee dei punti

$$[x_0 : \cdots : x_n]^\sigma = [x_0^\sigma : \cdots : x_n^\sigma].$$

L'azione è ben definita, infatti non dipende dalle coordinate omogenee scelte per rappresentare il punto: se $\lambda \in \bar{\mathbb{K}}^*$ si ha

$$[\lambda x_0 : \cdots : \lambda x_n]^\sigma = [\lambda^\sigma x_0^\sigma : \cdots : \lambda^\sigma x_n^\sigma] = [x_0^\sigma : \cdots : x_n^\sigma] = [x_0 : \cdots : x_n]^\sigma.$$

I punti $\mathbb{K}$-razionali di $\mathbb{P}^n$ possono quindi essere caratterizzati come

$$\mathbb{P}^n(\mathbb{K}) = \{P \in \mathbb{P}^n \colon P^\sigma = P,\ \forall \sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}\}.$$

Definizione II.1.6. Sia dato un punto $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n$. Si chiama *campo di definizione minimale su* $\mathbb{K}$ *per* P il campo dato da

$$\mathbb{K}(P) = \mathbb{K}\left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right),$$

dove l'indice i è tale che $x_i \neq 0$.

Osservazione II.1.7. Il campo di definizione minimale di P si può caratterizzare come il campo fisso dello stabilizzatore in $G = G_{\bar{\mathbb{K}}/\mathbb{K}}$ di P

$$\mathrm{St}_P(G) = \{\sigma \in G \colon P^\sigma = P\},$$
$$\mathbb{K}(P) = \{k \in \bar{\mathbb{K}} \colon \sigma(k) = k,\ \forall \sigma \in \mathrm{St}_P(G)\}.$$

2. Varietà affini e proiettive

Sia ora $\bar{\mathbb{K}}[X] = \bar{\mathbb{K}}[X_1 : \cdots : X_n]$ un anello di polinomi in n variabili.

Definizione II.2.1. Si chiama *insieme algebrico affine* un insieme del tipo

$$V_I = \{P \in \mathbb{A}^n \colon f(P) = 0,\ \forall f \in I\}$$

dove $I \subset \bar{\mathbb{K}}[X]$ è un ideale.

Osservazione II.2.2. Sia dato un insieme algebrico affine V. Si considerino $f, g, h \in \bar{\mathbb{K}}[X]$ tali che

$$f(P) = g(P) = 0,\ \forall P \in V.$$

I polinomi $(f+g), (fh) \in \bar{\mathbb{K}}[X]$ hanno la seguente proprietà

$$(f+g)(P) = f(P) + g(P) = 0,\ \forall P \in V,$$
$$(fh)(P) = f(P)h(P) = 0,\ \forall P \in V.$$

Segue che l'insieme dei polinomi che si azzera in ogni punto di V costituisce un ideale di $\bar{\mathbb{K}}[X]$.

Definizione II.2.3. Sia V un insieme algebrico affine. Si chiama *ideale di* V l'insieme dei polinomi che si azzerano in ogni punto di V

$$I(V) = \{f \in \bar{\mathbb{K}}[X] \colon f(P) = 0,\ \forall P \in V\}.$$

Dalla osservazione precedente si deduce come questo sia effettivamente un ideale. Si dice che V è *definito su* $\mathbb{K}$ e si scrive $V/\mathbb{K}$ se il suo ideale $I(V)$ può essere generato con polinomi in $\mathbb{K}[X]$. Se V è definito su $\mathbb{K}$, l'*insieme dei punti* $\mathbb{K}$*-razionali di* V è definito come

$$V(\mathbb{K}) = V \cap \mathbb{A}^n(\mathbb{K}).$$

Si definisce anche l'ideale $I(V/\mathbb{K})$ dato da

$$I(V/\mathbb{K}) = I(V) \cap \mathbb{K}[X].$$

Osservazione II.2.4. Dato un insieme algebrico affine V, $I(V/\mathbb{K})$ è l'ideale formato dai polinomi che si azzerano in V a coefficienti in $\mathbb{K}$. Si ha quindi che V è definito su $\mathbb{K}$ se e solo se $I(V) = I(V/\mathbb{K})\bar{\mathbb{K}}[X]$.

Osservazione II.2.5. Dati $f(X) \in \mathbb{K}[X]$, $P \in \mathbb{A}^n$ e $\sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}$ è immediato che

$$f(P^\sigma) = f(P)^\sigma.$$

Sia ora $V/\mathbb{K}$ un insieme algebrico affine definito su $\mathbb{K}$. L'azione di $G_{\bar{\mathbb{K}}/\mathbb{K}}$ sullo spazio affine induce un azione su V da cui

$$V(\mathbb{K}) = \{P \in V \colon P^\sigma = P,\ \forall \sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}\}.$$

Definizione II.2.6. Un polinomio $f \in \bar{\mathbb{K}}[X] = \bar{\mathbb{K}}[X_0 : \cdots : X_n]$ è detto *omogeneo di grado* d se rispetta

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n),\ \forall \lambda \in \bar{\mathbb{K}}.$$

Un ideale $I \in \bar{\mathbb{K}}[X]$ è detto *omogeneo* se è generato da polinomi omogenei.

Dato un polinomio omogeneo f ha senso parlare di $f(P), P \in \mathbb{P}^n$ poiché l'omogeneità garantisce che il valore di $f(P)$ non dipenda dalla scelta del rappresentante delle coordinate di P.

Definizione II.2.7. Si chiama *insieme algebrico proiettivo* un insieme del tipo

$$V_I = \{P \in \mathbb{P}^n \colon f(P) = 0,\ \forall f \text{ omogeneo} \in I\},$$

dove $I \subset \bar{\mathbb{K}}[X]$ è un ideale omogeneo. Se V è un insieme algebrico proiettivo, si chiama *ideale di* V e si scrive $I(V)$ l'ideale generato da

$$\{f \text{ omogeneo} \in \bar{\mathbb{K}}[X] \colon f(P) = 0,\ \forall P \in V\}.$$

Si dice che V è definito su $\mathbb{K}$ e si scrive $V/\mathbb{K}$ se il suo ideale $I(V)$ può essere generato con polinomi omogenei in $\mathbb{K}[X]$. Se V è definito su $\mathbb{K}$, l'*insieme dei punti* $\mathbb{K}$*-razionali di* V è definito come

$$V(\mathbb{K}) = V \cap \mathbb{P}^n(\mathbb{K}).$$

Osservazione II.2.8. Si noti come nel caso proiettivo $I(V)$, essendo generato da polinomi omogenei, è un ideale omogeneo.

Osservazione II.2.9. Analogamente al caso affine, è possibile caratterizzare i punti $\mathbb{K}$-razionali di un insieme algebrico proiettivo V definito su $\mathbb{K}$ come

$$V(\mathbb{K}) = \{P \in V \colon P^\sigma = P,\ \forall \sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}\}.$$

Definizione II.2.10. Un insieme algebrico affine V è chiamato *varietà affine* se $I(V)$ è un ideale primo in $\bar{\mathbb{K}}[X]$.

Osservazione II.2.11. Se V è definito su $\mathbb{K}$ non è sufficiente controllare che $I(V/\mathbb{K})$ sia primo in $\mathbb{K}[X]$ perché V sia effettivamente una varietà.

Definizione II.2.12. Un insieme algebrico proiettivo V è chiamato *varietà proiettiva* se $I(V)$ è un ideale (omogeneo) primo in $\bar{\mathbb{K}}[X]$.

Osservazione II.2.13. Lo spazio proiettivo $\mathbb{P}^n$ contiene varie copie di $\mathbb{A}^n$. Esistono n immersioni standard di $\mathbb{A}^n$ in $\mathbb{P}^n$ date da

$$\phi_i \colon \mathbb{A}^n \hookrightarrow \mathbb{P}^n, \quad (x_1, \ldots, x_n) \mapsto [x_1 : \cdots : x_{i-1} : 1 : x_i : \cdots : x_n],$$

con $i \in \{1, 2, \ldots, n\}$. Sia ora H_i l'iperpiano di $\mathbb{P}^n$ dato dall'equazione $X_i = 0$,

$$H_i = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n \colon x_i = 0\},$$

e sia U_i il complemento di H_i in $\mathbb{P}^n$,

$$U_i = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n \colon x_i \neq 0\} = \mathbb{P}^n \backslash H_i.$$

La restrizione di ϕ_i a U_i è una biezione, con inversa data da

$$\phi_i^{-1} \colon U_i \hookrightarrow \mathbb{A}^n, \quad [x_0 : \cdots : x_n] \mapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

Fissato i, si identificherà $\mathbb{A}^n$ con $\phi_i(\mathbb{A}^n) = U_i \subset \mathbb{P}^n$ e spesso si considererà $\mathbb{A}^n$ come sottoinsieme di $\mathbb{P}^n$ sottintendendo la naturale identificazione con U_i.

Osservazione II.2.14. Sia V una insieme algebrico proiettivo e sia $I(V) \subset \bar{\mathbb{K}}[X]$ il suo ideale omogeneo. Fissato un indice i si ha che $V \cap \mathbb{A}^n$ (inteso come $\phi_i^{-1}(V \cap U_i)$) è un insieme algebrico affine e il suo ideale è dato da

$$I(V \cap \mathbb{A}^n) = \{f(Y_1, \ldots, Y_{i-1}, 1, Y_{i+1}, \ldots, Y_n) \colon f(X_0, \ldots, X_n) \in I(V)\}.$$

Si noti come l'unione dei U_i da tutto lo spazio proiettivo $\mathbb{P}^n$ e perciò V è completamente coperto dai suoi sottoinsiemi $V \cap U_0, \ldots, V \cap U_n$. Il passaggio

$$f(X_0, \ldots, X_n) \to f(Y_0, \ldots, Y_{i-1}, 1, Y_{i+1}, \ldots, Y_n),$$

è chiamato *disomogeneizzazione rispetto a* X_i.

Viceversa, dato un polinomio generico $f(Y) \in \bar{\mathbb{K}}[Y]$ con $d = \deg(f)$ il polinomio omogeneo f^* dato da

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

è detto l'*omogeneizzazione di f rispetto a X_i*.

Definizione II.2.15. Sia $V \in \mathbb{A}^n$ un insieme algebrico affine, $I(V)$ il suo ideale e si consideri l'immagine di V in $\mathbb{P}^n$ data dall'inclusione

$$V \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n.$$

Si chiama *chiusura proiettiva di V* e si denota con $\bar{V}$ l'insieme algebrico proiettivo che ha ideale omogeneo associato $I(\bar{V})$ generato da

$$\{f^*(X) \colon f \in I(V)\}.$$

Proposizione II.2.16. (1) *Se V è una varietà affine e $\bar{V}$ è la sua chiusura proiettiva, vale*

$$V = \bar{V} \cap \mathbb{A}^n.$$

(2) *Sia V una varietà proiettiva. Allora $V \cap \mathbb{A}^n$ è una varietà affine e nel caso sia non vuota vale*

$$V = \overline{V \cap \mathbb{A}^n}.$$

Osservazione II.2.17. Dalla proposizione precedente è immediato:

(1) Se V è una varietà affine definita su $\mathbb{K}$, allora $\bar{V}$ è una varietà proiettiva definita su $\mathbb{K}$.
(2) Se V è una varietà proiettiva definita su $\mathbb{K}$, allora $V \cap \mathbb{A}^n$ è una varietà affine definita su $\mathbb{K}$.

Osservazione II.2.18. Ogni varietà affine si può quindi identificare con una varietà proiettiva. Spesso si parlerà di una varietà proiettiva V riferendosi a equazioni non omogenee, intendendo che V è la chiusura proiettiva della varietà affine associata alle equazioni. I punti di V che non appartengono alla varietà affine associata vengono chiamati *punti all'infinito* di V.

3. Proprietà di varietà

La maggior parte delle proprietà di una varietà proiettiva V possono essere definite a partire dalla varietà affine $V \cap \mathbb{A}^n$, quindi come fatto finora si procederà di pari passo tra la versione affine e la versione proiettiva.

Definizione II.3.1. Sia V una varietà affine definita su $\mathbb{K}$ (nel senso di insieme algebrico affine). Allora si chiama *anello delle coordinate affini di $V/\mathbb{K}$* il quoziente

$$\mathbb{K}[V] = \frac{\mathbb{K}[X]}{I(V/\mathbb{K})}.$$

Osservazione II.3.2. Dato che $I(V/\mathbb{K})$ è ideale primo, $\mathbb{K}[V]$ è dominio di integrità e perciò è ben definito il suo campo delle frazioni.

Definizione II.3.3. Il campo delle frazioni di $\mathbb{K}[V]$, denotato con $\mathbb{K}(V)$, è chiamato *campo delle funzioni di $V/\mathbb{K}$*. Allo stesso modo si definiscono $\bar{\mathbb{K}}[V]$ e $\bar{\mathbb{K}}(V)$.

Definizione II.3.4. Sia V una varietà proiettiva definita su $\mathbb{K}$. Il *campo delle funzioni di* V, denotato con $\mathbb{K}(V)$, è il campo delle funzioni di $V \cap \mathbb{A}^n$. Per diverse immersioni di $\mathbb{A}^n \subset \mathbb{P}^n$ i $\mathbb{K}(V)$ che si ottengono sono isomorfi canonicamente, così da permettere di identificarli.

Osservazione II.3.5. Se $f(X) \in \bar{\mathbb{K}}[X]$ è un polinomio il gruppo di Galois $G_{\bar{\mathbb{K}}/\mathbb{K}}$ coniuga f agendo sui suoi coefficienti. Gli elementi di $\bar{\mathbb{K}}[V]$ sono definiti a meno di sommare polinomi nulli in V. Segue che se V è definito su $\mathbb{K}$, l'azione di $G_{\bar{\mathbb{K}}/\mathbb{K}}$ manda $I(V)$ in se stesso e quindi $G_{\bar{\mathbb{K}}/\mathbb{K}}$ definisce un'azione su $\bar{\mathbb{K}}[V]$ e su $\bar{\mathbb{K}}(V)$. In questo modo $\mathbb{K}[V], \mathbb{K}(V)$ sono rispettivamente i sottoinsiemi di $\bar{K}[V], \bar{\mathbb{K}}(V)$ fissati da ogni $\sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}$. Indicando con f^σ il coniugato di f sotto l'azione di $G_{\bar{\mathbb{K}}/\mathbb{K}}$ allora è immediato che per ogni $P \in V$ vale

$$(f(P))^\sigma = f^\sigma(P^\sigma).$$

Definizione II.3.6. Sia V una varietà affine. Si chiama *dimensione di* V e si denota $\dim(V)$ il grado di trascendenza di $\bar{\mathbb{K}}(V)$ su $\bar{\mathbb{K}}$.

Osservazione II.3.7. Per uno spazio affine il campo delle funzioni è dato da $\bar{\mathbb{K}}(\mathbb{A}^n) = \bar{\mathbb{K}}(X_1, \ldots, X_n)$ e perciò quest'ultimo ha grado di trascendenza su $\bar{\mathbb{K}}$ pari a n, cioè $\dim(\mathbb{A}^n) = n$. Si noti come questa definizione di dimensione per uno spazio affine è in accordo con quella data precedentemente in II.1.1. Se si considera una varietà affine V è immediato che $\mathbb{K}(V) \subset \mathbb{K}(X_1, \ldots, X_n)$ e perciò il grado di trascendenza di $\mathbb{K}(V)$ su $\mathbb{K}$ è limitato superiormente dalla dimensione n dello spazio affine in cui vive V. Si noti come di conseguenza $\dim(V)$ è ben definita per ogni varietà V.

Definizione II.3.8. Sia V una varietà proiettiva definita su $\mathbb{K}$ e si scelga una immersione $\mathbb{A}^n \subset \mathbb{P}^n$ tale che $V \cap \mathbb{A}^n \neq 0$. Si chiama *dimensione di* V la dimensione di $V \cap \mathbb{A}^n$ come varietà affine.

Definizione II.3.9. Sia V una varietà affine e $f_1, \ldots, f_m \in \bar{\mathbb{K}}[X]$ un insieme di generatori di $I(V)$. Si dice che V è *liscia in* $P \in V$ se la matrice

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{1 \leq i \leq m, 1 \leq j \leq n},$$

ha rango $n - \dim(V)$. Se invece il rango è minore di $n - \dim(V)$ il punto P è detto punto *singolare* di V e si dice che V è singolare in P. Si dice che V è *liscia* se è liscia in ogni suo punto, altrimenti si dice che V è *singolare*.

Oltre all'approccio analitico per definire la liscezza di una curva, spesso è utile utilizzare il seguente. Sia quindi V una varietà affine e $P \in V$. Si definisce l'ideale $M_P \subset \bar{\mathbb{K}}[V]$ come

$$M_P = \{f \in \bar{\mathbb{K}}[V] \colon f(P) = 0\}.$$

La mappa data da

$$\bar{\mathbb{K}}[V]/M_P \to \bar{\mathbb{K}}, \quad f \mapsto f(P),$$

è chiaramente un isomorfismo e perciò M_P è un ideale massimale di $\bar{\mathbb{K}}[V]$. Vale inoltre che M_P/M_P^2 è uno spazio vettoriale su $\bar{\mathbb{K}}$ di dimensione finita (dove $M_P^2 = \{(fg) \in \bar{\mathbb{K}}[V] \colon f, g \in M_P\}$).

PROPOSIZIONE II.3.10. *Sia V una varietà affine e $P \in V$. Allora V è liscia in P se e solo se vale*

$$\dim_{\bar{\mathbb{K}}} M_P/M_P^2 = \dim(V).$$

DIMOSTRAZIONE. Vedi [Har77, I.5.1]. □

DEFINIZIONE II.3.11. Sia V una varietà proiettiva, $P \in V$ e si scelga una immersione $\mathbb{A}^n \subset \mathbb{P}^n$ tale che $P \in \mathbb{A}^n$. Allora si dice che V è *liscia in P* se $V \cap \mathbb{A}^n$ è liscia in P. Si dice che V è *liscia* se è liscia in ogni suo punto.

DEFINIZIONE II.3.12. Si chiama *anello locale in P di V* e si denota $\bar{\mathbb{K}}[V]_P$ l'insieme

$$\bar{\mathbb{K}}[V]_P = \{F \in \bar{\mathbb{K}}(V) \colon F = f/g \text{ con } f, g \in \bar{\mathbb{K}}[V] \text{ tali che } g(P) \neq 0\}.$$

Le funzioni contenute in $\bar{\mathbb{K}}[V]_P$ sono dette *regolari in P*.

DEFINIZIONE II.3.13. Sia V una varietà proiettiva, $P \in V \cap \mathbb{A}^n$. Si chiama *anello locale in P di V* e si denota $\bar{\mathbb{K}}[V]_P$ l'anello locale in P di $V \cap \mathbb{A}^n$. Una funzione di $\bar{K}(V)$ è detta *regolare in P* se appartiene a $\bar{\mathbb{K}}[V]_P$.

OSSERVAZIONE II.3.14. Per una funzione $F = f/g \in \bar{\mathbb{K}}[V]_P$ regolare in P, la valutazione in P data da $F(P) = f(P)/g(P)$ è ben definita.

OSSERVAZIONE II.3.15. Il campo delle funzioni di $\mathbb{P}^n$ è il sottocampo di $\bar{\mathbb{K}}(X)$ composto dalle funzioni razionali $F(X) = f(X)/g(X)$ dove f, g sono polinomi omogenei dello stesso grado. Si noti come $f(X)/g(X)$ è ben definita in tutti i punti $p \in \mathbb{P}^n$ tali che $g(P) \neq 0$. Allo stesso modo il campo delle funzioni di una varietà proiettiva V è composto dalle funzioni razionali $F(X) = f(X)/g(X)$ tali che:

(1) f, g sono polinomi omogenei dello stesso grado,
(2) $g \notin I(V)$,
(3) due funzioni $f_1(X)/g_1(X)$ e $f_2(X)/g_2(X)$ sono identificate se $f_1 g_2 - f_2 g_1 \in I(V)$.

4. Mappe tra varietà

DEFINIZIONE II.4.1. Siano $V_1, V_2 \subset \mathbb{P}^n$ due varietà proiettive. Si chiama *mappa razionale da V_1 a V_2* una funzione ϕ del tipo

$$\phi = [f_0 : \cdots : f_n] \colon U \subset V_1 \to V_2, \quad f_0, \ldots, f_n \in \bar{\mathbb{K}}(V_1),$$

che rispetti la condizione

$$\phi(P) = [f_0(P) : \cdots : f_n(P)] \in V_2, \ \forall P \in U,$$

dove U è l'intersezione dei domini delle f_i. Per indicare che una mappa razionale va da un sottoinsieme di V_1 a V_2 si scriverà

$$\phi \colon V_1 \dashrightarrow V_2.$$

Si dice che ϕ è *definita su* $\mathbb{K}$ se esiste $\lambda \in \bar{\mathbb{K}}^*$ tale che $\lambda f_0, \ldots, \lambda f_n \in \mathbb{K}(V_1)$.

Osservazione II.4.2. Si noti come, dati $P \in V_1$ e $\lambda \in \bar{\mathbb{K}}^*$, $[f_0(P) : \cdots : f_n(P)] = [\lambda f_0(P) : \cdots : \lambda f_n(P)]$ e quindi le mappe razionali corrispondenti combaciano.

Osservazione II.4.3. Se sia V_1 che V_2 sono definite su $\mathbb{K}$, il gruppo di Galois $G_{\bar{\mathbb{K}}/\mathbb{K}}$ agisce naturalmente su di ϕ nel seguente modo

$$\phi^\sigma(P) = [f_0^\sigma(P) : \cdots : f_n^\sigma(P)],$$

da cui vale la relazione

$$\phi(P)^\sigma = \phi^\sigma(P^\sigma),$$

con $\sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}$ e $P \in V_1$. Si ha quindi che ϕ è definita su $\mathbb{K}$ se e solo se $\phi = \phi^\sigma$, $\forall \sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}$.

Osservazione II.4.4. Le componenti $f_i \in \bar{\mathbb{K}}(V_1)$ non sono definite in ogni punto di V_1 in generale. Per un indice i e un punto P fissati tali che P non sia nel dominio di f_i a volte è possibile trovare una $g \in \bar{\mathbb{K}}(V_1)$ tale che il prodotto gf_i sia definito in P. In tal caso, moltiplicando tutte le f_i per g la mappa razionale in P resta la stessa, ma la componente i-esima stavolta è definita in P.

Definizione II.4.5. Una mappa razionale $\phi = [f_0 : \cdots : f_n] \colon V_1 \dashrightarrow V_2$ è detta *regolare in* $P \in V_1$ se esiste una funzione $g \in \bar{\mathbb{K}}(V_1)$ tale che:

(1) i prodotti gf_i sono regolari in P, cioè $gf_i \in \bar{\mathbb{K}}[V]_P$, $\forall i$,
(2) esiste un indice i tale che $(gf_i)(P) \neq 0$.

Se una tale g esiste si definisce quindi

$$\phi(P) = [(gf_0)(P) : \cdots : (gf_n)(P)].$$

Una mappa razionale che è regolare in ogni punto di V_1 è detta *morfismo*.

Osservazione II.4.6. Si possono definire le mappe razionali alternativamente anche nel seguente modo. Siano $V_1 \subset \mathbb{P}^m, V_2 \subset \mathbb{P}^n$ due varietà proiettive. Come visto in II.3.15 le funzioni di $\bar{\mathbb{K}}(V_1)$ sono date dal rapporto di polinomi omogenei in $\bar{\mathbb{K}}[X_0 : \cdots : X_m]$ dello stesso grado. Data una mappa razionale $\phi = [F_0 : \cdots : F_n]$ tale che $F_i(X) = f_i(X)/g_i(X)$, $\forall i$ si può quindi moltiplicare ogni F_i per ogni g_i senza alterare la mappa e ottenere così una rappresentazione di $\phi = [\phi_0 : \cdots : \phi_n]$ dove ϕ_i è un polinomio per ogni i. Si ottiene così la seguente definizione:

Una mappa razionale $\phi = [\phi_0 : \cdots : \phi_n] \colon V_1 \to V_2$ è una mappa tale che:

(1) $\phi_i(X) \in \bar{\mathbb{K}}[X_0 : \cdots : X_n]$ sono polinomi omogenei dello stesso grado,
(2) esiste un indice i tale che $\phi_i(X) \notin I(V_1)$,
(3) per ogni $f \in I(V_2)$ vale

$$f(\phi_0(X), \ldots, \phi_n(X)) \in I(V_1).$$

Osservazione II.4.7. Procedendo con la stessa filosofia si può andare a definire la regolarità nel seguente modo:

Una mappa razionale (come vista in II.4.6) $\phi = [\phi_0 : \cdots : \phi_n] \colon V_1 \to V_2$ è detta regolare in un punto $P \in V_1$ se esistono polinomi omogenei $\psi_0, \ldots, \psi_n \in \bar{\mathbb{K}}[X]$ dello stesso grado tali che:

(1) esiste un indice i per cui $\psi_i(P) \neq 0$,
(2) $\phi_i\psi_j - \phi_j\psi_i \in I(V_1)$ per ogni $0 \leq i, j \leq n$.

In tal caso allora si definisce

$$\phi(P) = [\psi_0(P) : \cdots : \psi_n(P)].$$

Se una mappa razionale è regolare in ogni suo punto è detta *morfismo*.

Definizione II.4.8. Due varietà proiettive $V_1, V_2 \subset \mathbb{P}^n$ sono dette *isomorfe* e si scrive $V_1 \cong V_2$ se esistono due morfismi $\phi \colon V_1 \to V_2$ e $\psi \colon V_2 \to V_1$ tali che $\phi \circ \psi = \mathrm{id}_{V_1}$ e $\psi \circ \phi = \mathrm{id}_{V_2}$. Si dice che $V_1/\mathbb{K}$ e $V_2/\mathbb{K}$ sono *definite su* $\mathbb{K}$ se ϕ, ψ sono entrambe definite su $\mathbb{K}$.

CAPITOLO III

Curve algebriche

In questa sezione si studieranno le proprietà delle varietà proiettive di dimensione 1, chiamate anche *curve algebriche*. Lo scopo è di dare abbastanza nozioni per permettere la definizione e la trattazione di una classe particolare di curve algebriche: le curve ellittiche, a cui è dedicata la prossima sezione.

PROPOSIZIONE III.0.1. *Sia C una curva e $P \in C$ un punto liscio. Allora l'anello locale $\bar{\mathbb{K}}[C]_P$ è un anello di valutazione discreta.*

DIMOSTRAZIONE. Da IV.1.9 il $\bar{\mathbb{K}}$-spazio vettoriale M_P/M_P^2 ha dimensione 1. Si conclude usando [AM69, Proposizione 9.2]. □

DEFINIZIONE III.0.2. Sia C una curva e $P \in C$ un punto liscio. Si chiama *valutazione su* $\bar{\mathbb{K}}[C]_P$ la funzione

$$\begin{aligned} \operatorname{ord}_P \colon \bar{\mathbb{K}}[C]_P &\to \mathbb{N} \cup \{\infty\} \\ f &\mapsto \sup\{d \in \mathbb{Z} \colon f \in M_P^d\}. \end{aligned}$$

La valutazione si estende poi su $\bar{\mathbb{K}}(C)$ nel seguente modo

$$\begin{aligned} \operatorname{ord}_P \colon \bar{\mathbb{K}}(C) &\to \mathbb{Z} \cup \{\infty\} \\ f/g &\mapsto \operatorname{ord}_P(f) - \operatorname{ord}_P(g). \end{aligned}$$

Si chiama *uniformatore per C in P* una funzione $t \in \bar{\mathbb{K}}(C)$ tale che $\operatorname{ord}_P(t) = 1$.

OSSERVAZIONE III.0.3. Un uniformatore per C in P non è altro che un generatore dell'ideale M_P.

Se in particolare la curva C è definita su $\mathbb{K}$ allora esistono uniformatori in P appartenenti a $\mathbb{K}(C)$.

DEFINIZIONE III.0.4. Sia C una curva, $P \in C$ liscio e $f \in \bar{\mathbb{K}}(C)$. Allora si chiama *ordine di f in P* la quantità $\operatorname{ord}_P(f)$.

(1) Se $\operatorname{ord}_P(f) > 0$ si dice che f ha uno *zero* in P,
(2) se $\operatorname{ord}_P(f) \geq 0$ si dice che f è *regolare* in P e di conseguenza si può valutare $f(P)$,
(3) se $\operatorname{ord}_P(f) < 0$ si dice che f ha un *polo* in P e si scrive $f(P) = \infty$.

PROPOSIZIONE III.0.5. *Sia C una curva e $f \in \bar{\mathbb{K}}(C)$ non nulla. Allora i punti in cui f ha zeri o poli sono in numero finito e se f non ha poli si ha $f \in \bar{\mathbb{K}}$.*

DIMOSTRAZIONE. [Har77, I.6.5] dice che i poli sono in numero finito. Gli zeri di f corrispondono ai poli di $1/f$, che sono in numero finito.

Inoltre se f non ha poli, la funzione $1/f$ non ha zeri e perciò è costante. Segue che anche $f \in \bar{\mathbb{K}}$. □

PROPOSIZIONE III.0.6. *Sia $C/\mathbb{K}$ una curva, $P \in C(K)$ liscio e $t \in \mathbb{K}(C)$ un uniformatore in P. Allora $\mathbb{K}(C)$ è estensione finita e separabile di $\mathbb{K}(t)$.*

DIMOSTRAZIONE. Vedi [Sil09, § II.1.4]. □

1. Mappe tra curve

PROPOSIZIONE III.1.1. *Sia C una curva, $P \in C$ liscio, $V \subset \mathbb{P}^N$ una varietà proiettiva e $\phi\colon C \dashrightarrow V$ una mappa razionale. Allora ϕ è regolare in P e quindi se C è liscia allora ϕ è morfismo.*

DIMOSTRAZIONE. Si scriva $\phi = [f_0 : \cdots : f_N]$ dove $f_i \in \bar{\mathbb{K}}(C)$, $\forall i$ e sia $t \in \bar{\mathbb{K}}(C)$ un uniformatore di C in P. Sia inoltre $n = \min \operatorname{ord}_P(f_i)$ al variare di $i \in \{0, \dots, N\}$. Si ha che

$$\operatorname{ord}_P(t^{-n} f_i) \geq 0,\ \forall i, \quad \operatorname{ord}_P(t^{-n} f_j) = 0,\ \exists j,$$

cioè ogni $t^{-n} f_i$ è regolare in P ed esiste un indice j per cui si abbia $(t^{-n} f_j)(P) \neq 0$. Segue che ϕ è regolare in P. □

ESEMPIO III.1.2. Sia $C/\mathbb{K}$ una curva e sia $f \in \mathbb{K}(C)$ una funzione. Allora f definisce una mappa razionale

$$f\colon C \to \mathbb{P}^1, \quad P \mapsto [f(P) : 1].$$

Da III.1.1 f è un morfismo, esplicitamente dato da

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

Viceversa, sia $\phi = [f : g]\colon C \to \mathbb{P}^1$ una mappa razionale definita su $\mathbb{K}$. Allora se $g = 0$ si ha che ϕ è la mappa costante $\phi = \infty = [1 : 0]$. Altrimenti ϕ corrisponde alla funzione $f/g \in \mathbb{K}(C)$. Si ha perciò una biezione

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

TEOREMA III.1.3. *Un morfismo di curve $\phi\colon C_1 \to C_2$ non costante è suriettivo.*

DIMOSTRAZIONE. Vedi [Har77, II.6.8]. □

Siano ora $C_1/\mathbb{K}, C_2/\mathbb{K}$ due curve e sia $\phi\colon C_1 \to C_2$ una mappa razionale non nulla definita su $\mathbb{K}$. Allora ϕ induce una mappa sui campi delle funzioni delle due curve che fissa $\mathbb{K}$ data da

$$\phi^*\colon \mathbb{K}(C_2) \to \mathbb{K}(C_1), \quad f \mapsto f \circ \phi.$$

TEOREMA III.1.4. *Siano $C_1/\mathbb{K}, C_2/\mathbb{K}$ curve.*

(1) *Sia $\phi\colon C_1 \to C_2$ una mappa non costante definita su $\mathbb{K}$. Allora si ha che $\mathbb{K}(C_1)$ è un'estensione finita di $\phi^*(\mathbb{K}(C_2))$.*

(2) *Sia* $\iota\colon \mathbb{K}(C_2) \hookrightarrow \mathbb{K}(C_1)$ *una immersione di campi di funzioni che tenga* $\mathbb{K}$ *fissato. Allora esiste una e una sola mappa non costante* $\phi\colon C_1 \to C_2$ *definita su* $\mathbb{K}$ *tale che* $\phi^* = \iota$.

(3) *Sia* $\mathbb{F} \subset \mathbb{K}(C_1)$ *un sottocampo con indice finito contenente* $\mathbb{K}$. *Allora a meno di isomorfismi su* $\mathbb{K}$ *esiste una unica curva liscia* $C'/\mathbb{K}$ *e una mappa non costante* $\phi\colon C_1 \to C'$ *definita su* $\mathbb{K}$ *tale che* $\phi^*\mathbb{K}(C') = \mathbb{F}$.

Dimostrazione. (1) Vedi [Har77, II.6.8].

(2) Sia $C_1 \in \mathbb{P}^N$. Senza perdere di generalità sia C_2 non contenuta in $X_0 = 0$ e siano $g_i \in \mathbb{K}(C_2)$ le funzioni su C_2 corrispondenti a X_i/X_0 al variare di i. Allora la mappa

$$\phi = [1 : \iota(g_1) : \cdots : \iota(g_N)]\colon C_1 \to C_2,$$

rispetta $\phi^* = \iota$. Si noti come ϕ non è costante, infatti le g_i non possono essere tutte costanti e l'inclusione ι è iniettiva.

Sia ora $\psi = [f_0 : \cdots : f_N]\colon C_1 \to C_2$ tale che $\psi^* = \iota$. Allora si ha che

$$f_i/f_0 = \psi^* g_i = \phi^* g_i = \iota(g_i),$$

per ogni i. Segue quindi che $\psi = \phi$ da cui l'unicità.

(3) Vedi [Har77, I.6.12] nel caso in cui $\mathbb{K} = \bar{\mathbb{K}}$. La dimostrazione per $\mathbb{K}$ non algebricamente chiuso è analoga. □

Definizione III.1.5. Sia $\phi\colon C_1 \to C_2$ una mappa di curve definite su $\mathbb{K}$. Si chiama *grado di* ϕ la quantità

$$\deg \phi = \begin{cases} 0, & \text{se } \phi \text{ è costante,} \\ [\mathbb{K}(C_1) : \phi^*\mathbb{K}(C_2)], & \text{altrimenti.} \end{cases}$$

Se $\deg \phi > 0$ allora ϕ è detta *mappa finita*. Si dice che ϕ è *separabile, inseparabile, puramente inseparabile* rispettivamente se lo è l'estensione $\mathbb{K}(C_1)/\phi^*\mathbb{K}(C_2)$. I gradi di separabilità e inseparabilità dell'estensione vengono rispettivamente denotati $\deg_s \phi, \deg_i \phi$.

Definizione III.1.6. Sia $\phi\colon C_1 \to C_2$ una mappa non costante di curve definite su $\mathbb{K}$. Allora si definisce la mappa

$$\phi_*\colon \mathbb{K}(C_2) \to \mathbb{K}(C_1), \quad \phi_* = (\phi^*)^{-1} \circ N,$$

dove $N = N_{\mathbb{K}(C_1)/\phi^*\mathbb{K}(C_2)}$ è la norma su C_1 associata a ϕ^*.

Proposizione III.1.7. *Siano* C_1, C_2 *curve lisce e sia* $\phi\colon C_1 \to C_2$ *una mappa di grado* 1. *Allora* ϕ *è un isomorfismo.*

Dimostrazione. Per definizione $\deg \phi = 1$ vuol dire che $\phi^*\mathbb{K}(C_2) = \mathbb{K}(C_1)$ e ϕ^* è un isomorfismo di campi di funzioni. Da III.1.4 quindi esiste un'unica mappa razionale $\psi\colon C_2 \to C_1$ corrispondente all'isomorfismo $(\phi^*)^{-1}\colon \mathbb{K}(C_1) \to \mathbb{K}(C_2)$, ovvero tale che $\psi^* = (\phi^*)^{-1}$. Inoltre dato che C_2 è liscia, da III.1.1 ψ è un morfismo. Infine si ha $(\phi\circ\psi)^* = \psi^*\circ\phi^* = \mathrm{id}_{\bar{\mathbb{K}}(C_2)}$ e $(\psi \circ \phi)^* = \phi^* \circ \psi^* = \mathrm{id}_{\bar{\mathbb{K}}(C_1)}$. Dall'unicità enunciata in III.1.4 quindi $\phi \circ \psi$ e $\psi \circ \phi$ sono le identità rispettivamente su C_2 e C_1. Segue quindi che ϕ, ψ sono isomorfismi. □

DEFINIZIONE III.1.8. Sia $\phi\colon C_1 \to C_2$ una mappa non costante tra curve lisce e sia $P \in C_1$. Si chiama *indice di ramificazione di ϕ in P* e si denota $e_\phi(P)$ la quantità

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)}),$$

dove $t_{\phi(P)}$ è un uniformatore in $\phi(P)$ di C_2. Si dice che ϕ è *ramificata in P* se $e_\phi(P) > 1$ e *non-ramificata in P* se $e_\phi(P) = 1$. Si dice che ϕ è *non-ramificata* se $e_\phi(P) = 1$ per ogni punto $P \in C_1$.

PROPOSIZIONE III.1.9. *Sia $\phi\colon C_1 \to C_2$ una mappa non costante tra curve lisce.*

(1) *Per ogni $Q \in C_2$ vale*

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

(2) *Per quasi ogni $Q \in C_2$ (ovvero a meno di un numero finito di punti) vale*

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

(3) *Sia $\psi\colon C_2 \to C_3$ un'altra mappa non costante di curve lisce. Allora per ogni $P \in C_1$ vale*

$$e_{\psi\circ\phi}(P) = e_\phi(P) e_\psi(\phi P).$$

DIMOSTRAZIONE.
(1) È sufficiente usare [Har77, II.6.9] con $Y = \mathbb{P}^1$ e $D = (O)$.
(2) Vedi [Har77, II.6.8].
(3) Sia $\phi P = Q \in C_2$ e siano t_2, t_3 degli uniformatori rispettivamente di Q su C_2 e di ψQ su C_3. Per definizione si ha che le funzioni

$$t_2^{e_\psi Q}, \quad \psi^* t_3,$$

hanno lo stesso ordine in Q. Applicando ϕ^* e valutando l'ordine in P di entrambe si ottiene quindi

$$e_\phi(P) e_\psi(\phi P) = \mathrm{ord}_P\left(\phi^* t_2^{e_\psi Q}\right) = \mathrm{ord}_P\left((\psi\circ\phi)^* t_3\right) = e_{\psi\circ\phi}(P). \qquad \square$$

COROLLARIO III.1.10. *Una mappa $\phi\colon C_1 \to C_2$ è non-ramificata se e solo se vale*

$$\#\phi^{-1}(Q) = \deg \phi,$$

per ogni $Q \in C_2$.

DIMOSTRAZIONE. Dalla proposizione precedente si ha che

$$\#\phi^{-1}(Q) = \deg\phi \iff \sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg\phi = \#\phi^{-1}(Q).$$

Dato che $e_\phi(P) \geq 1$ questo accade se e solo se $e_\phi(P) = 1$ per ogni $P \in C_1$. $\square$

2. Divisori

Definizione III.2.1. Si chiama *gruppo dei divisori di una curva* C e si denota $\mathrm{Div}(C)$ il gruppo abeliano libero generato dai punti di C. Un elemento di $\mathrm{Div}(C)$ è chiamato *divisore* di C ed è quindi una somma formale del tipo

$$\mathrm{Div}(C) \ni D = \sum_{P \in C} n_P(P)$$

dove i $n_P \in \mathbb{Z}$ sono quasi tutti nulli (cioè $n_P \neq 0$ per un numero finito di punti P). Si chiama *grado di* D la seguente quantità

$$\deg(D) = \sum_{P \in C} n_P \in \mathbb{Z}.$$

I divisori di grado 0 di C formano un sottogruppo di $\mathrm{Div}(C)$ denotato

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) \colon \deg(D) = 0\}.$$

Se la curva C è definita su $\mathbb{K}$ si può far agire il gruppo di Galois $G_{\bar{\mathbb{K}}/\mathbb{K}}$ su $\mathrm{Div}(C)$ coniugando i punti uno a uno:

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma), \quad \forall \sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}.$$

Definizione III.2.2. Un divisore $D \in \mathrm{Div}(C)$ si dice *definito su* $\mathbb{K}$ se è coniugato in se stesso da ogni elemento di $G_{\bar{\mathbb{K}}/\mathbb{K}}$,

$$D = D^\sigma, \quad \forall \sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}.$$

I divisori definiti su $\mathbb{K}$ formano un gruppo, denominato *gruppo dei divisori definiti su* $\mathbb{K}$ di C e denotato con $\mathrm{Div}_{\mathbb{K}}(C)$. Allo stesso modo, gli elementi di $\mathrm{Div}_{\mathbb{K}}(C)$ di grado 0 formano un sottogruppo denotato con $\mathrm{Div}^0_{\mathbb{K}}(C)$.

Osservazione III.2.3. Si noti come, preso un divisore $D = n_1(P_1) + \cdots + n_k(P_k) \in \mathrm{Div}(C)$ definito su $\mathbb{K}$, il fatto che $D = D^\sigma$ non implica che $P_1, \ldots, P_k \in C(\mathbb{K})$. Un elemento $\sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}$ infatti può permutare i $P_1, \ldots, P_k$ lasciando D invariato.

Definizione III.2.4. Sia C una curva liscia. Preso $f \in \bar{\mathbb{K}}(C)^*$ si definisce il *divisore associato ad* f nel seguente modo

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

Osservazione III.2.5. Dato che f ha un numero finito di zeri e di poli (III.0.5) segue che $\mathrm{div}(f) \in \mathrm{Div}(C)$. Inoltre data $\sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}$ è immediato

$$\mathrm{div}(f^\sigma) = (\mathrm{div}(f))^\sigma,$$

perciò se $f \in \mathbb{K}(C)$ si ha che $\mathrm{div}(f) \in \mathrm{Div}_{\mathbb{K}}(C)$.

Osservazione III.2.6.

$$\mathrm{div} \colon \bar{\mathbb{K}}(C)^* \to \mathrm{Div}(C)$$

è omomorfismo di gruppi abeliani.

Definizione III.2.7. Sia $f \in \bar{\mathbb{K}}(C)^*$. Il divisore $D = \mathrm{div}(f) \in \mathrm{Div}(C)$ associato a f è detto divisore *principale* di C. Due divisori D_1, D_2 sono detti *linearmente equivalenti* e si scrive $D_1 \sim D_2$ se la loro differenza $D_1 - D_2$ è principale.

Osservazione III.2.8. È immediato verificare che l'equivalenza lineare è una relazione di equivalenza su $\mathrm{Div}(C)$. Si ha infatti che, dati $D_1, D_2, D_3 \in \mathrm{Div}(C)$

(1) $D_1 \sim D_1$ in quanto $D_1 - D_1 = 0 = \mathrm{div}(k)$ dove $k \in \bar{\mathbb{K}}(C)^*$ è una funzione costante,
(2) $D_1 \sim D_2 \implies D_1 - D_2 = \mathrm{div}(f) \in \bar{\mathbb{K}}(C)^*$. Ma allora $\mathrm{div}(1/f) = D_2 - D_1 \implies D_2 \sim D_1$,
(3) $D_1 \sim D_2, D_2 \sim D_3 \implies D_1 - D_2 = \mathrm{div}(f), D_2 - D_3 = \mathrm{div}(g)$ per qualche $f, g \in \bar{\mathbb{K}}(C)^*$. Ma allora $\mathrm{div}(fg) = D_1 - D_3 \implies D_1 \sim D_3$.

Definizione III.2.9. Si chiama *gruppo di Picard di* C il quoziente di $\mathrm{Div}(C)$ rispetto alla relazione di equivalenza lineare

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\sim .$$

Il sottogruppo di $\mathrm{Pic}(C)$ fissato da $G_{\bar{\mathbb{K}}/\mathbb{K}}$ si denota con $\mathrm{Pic}_{\mathbb{K}}(C)$. (In generale questo non coincide con il quoziente del sottogruppo $\mathrm{Div}_{\mathbb{K}}(C)$.)

Proposizione III.2.10. *Sia C una curva liscia e sia $f \in \bar{\mathbb{K}}(C)^*$.*

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

Dimostrazione. (1) Se f è costante allora chiaramente il suo divisore è nullo. Viceversa, sia $\mathrm{div}(f) = 0$. Allora la mappa associata $f\colon C \to \mathbb{P}^1$ come in III.1.2 non ha poli e perciò non è suriettiva. Da III.1.3 allora la mappa è costante.
(2) Vedi osservazione III.2.18. □

Osservazione III.2.11. Sia C una curva liscia e siano $D_1, D_2 \in \mathrm{Div}(C)$ tali che $D_1 \sim D_2$. Allora esiste $f \in \bar{\mathbb{K}}(C)^*$ per cui vale $D_1 = D_2 + \mathrm{div}(f)$. Da III.2.10 segue quindi che

$$\deg D_1 = \deg(D_2 + \mathrm{div}(f)) = \deg D_2.$$

Esempio III.2.12. Su $\mathbb{P}^1$ ogni divisore di grado 0 è principale. Sia infatti $D = \sum n_P(P) \in \mathrm{Div}^0(\mathbb{P}^1)$. Scrivendo $P = [\alpha_P, \beta_P] \in \mathbb{P}^2$ è immediato che D è divisore della funzione

$$\prod_{P \in \mathbb{P}^2} (\beta_P X - \alpha_P Y)^{n_P}.$$

Il fatto che $\sum n_P = 0$ garantisce che la funzione sia in $\mathbb{K}(\mathbb{P}^1)$. Segue che la mappa $\deg\colon \mathrm{Pic}(\mathbb{P}^1) \to \mathbb{Z}$ è un isomorfismo.

Esempio III.2.13. Sia $\mathrm{char}\mathbb{K} \neq 2$ e sia C una curva data da

$$C\colon y^2 = (x - x_1)(x - x_2)(x - x_3),$$

dove $x_1, x_2, x_3 \in \bar{\mathbb{K}}$ sono distinti e perciò C è liscia. Sia inoltre P_∞ l'unico punto all'infinito di C. Siano $P_i = (x_i, 0) \in C$ per $i \in \{1, 2, 3, \}$. Allora si ha

$$\begin{aligned} \operatorname{div}(x - x_i) &= 2(P_i) - 2(P_\infty), \\ \operatorname{div}(y) &= (P_1) + (P_2) + (P_3) - 3(P_\infty). \end{aligned}$$

Definizione III.2.14. Dalla proposizione precedente si deduce che i divisori principali formano un sottogruppo di $\operatorname{Div}^0(C)$. Si chiama *parte di grado* 0 *del gruppo di Picard di* C e si denota $\operatorname{Pic}^0(C)$ il quoziente $\operatorname{Div}^0(C)/\sim$ dato dall'equivalenza lineare. Il sottogruppo di $\operatorname{Pic}^0(C)$ invariante sotto l'azione di $G_{\bar{\mathbb{K}}/\mathbb{K}}$ è denotato $\operatorname{Pic}^0_{\mathbb{K}}(C)$.

Definizione III.2.15. Data una mappa tra curve lisce $\phi\colon C_1 \to C_2$ non costante, si definiscono le mappe seguenti sui gruppi dei divisori

$$\begin{aligned} \phi_*\colon \operatorname{Div}(C_1) &\to \operatorname{Div}(C_2), & \phi^*\colon \operatorname{Div}(C_2) &\to \operatorname{Div}(C_1), \\ (P) &\mapsto (\phi P), & (Q) &\mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P). \end{aligned}$$

Esempio III.2.16. Sia C una curva liscia, $f \in \bar{\mathbb{K}}(C)$ una funzione non costante e $f\colon C \to \mathbb{P}^1$ la corrispondente mappa vista in III.1.2. Allora dalle definizioni precedenti è immediato che

$$\operatorname{div}(f) = f^*((0) - (\infty)).$$

Proposizione III.2.17. *Sia $\phi\colon C_1 \to C_2$ una mappa tra curve lisce non costante.*

(1) $\deg(\phi_* D) = \deg(D)$, $\quad \forall D \in \operatorname{Div}(C_1)$.
(2) $\phi_*(\operatorname{div} f) = \operatorname{div}(\phi_* f)$, $\quad \forall f \in \bar{\mathbb{K}}(C_1)^*$.
(3) $\deg(\phi^* D) = (\deg \phi)(\deg D)$, $\quad \forall D \in \operatorname{Div}(C_2)$.
(4) $\phi^*(\operatorname{div} f) = \operatorname{div}(\phi^* f)$, $\quad \forall f \in \bar{\mathbb{K}}(C_2)^*$.
(5) $\phi_* \circ \phi^* = (\deg \phi)\mathrm{id}_{\operatorname{Div}(C_2)}$.
(6) *Se $\psi\colon C_2 \to C_3$ è un'altra mappa del genere, valgono*

$$(\psi \circ \phi)_* = \psi_* \circ \phi_*, \quad (\psi \circ \phi)^* = \phi^* \circ \psi^*.$$

Dimostrazione. (1) Immediata dalla definizione di ϕ_*.
(2) Vedi [Ser79, I, Proposizione 14].
(3) Segue direttamente da III.1.9.
(4) Segue dalle definizioni e dal fatto che per ogni $P \in C_1$ vale

$$\operatorname{ord}_P(\phi^* f) = e_\phi(P)\operatorname{ord}_{\phi(P)}(f).$$

(5) Segue direttamente da III.1.9.
(6) La prima segue direttamente dalle definizioni, la seconda da III.1.9. □

Osservazione III.2.18. Dalla proposizione precedente si deduce che sia ϕ_* che ϕ^* mappano divisori di grado 0 in divisori di grado zero e divisori principali in divisori principali. Sono perciò ben definite le mappe indotte

$$\phi_*\colon \operatorname{Pic}^0(C_1) \to \operatorname{Pic}^0(C_2), \quad \phi^*\colon \operatorname{Pic}^0(C_2) \to \operatorname{Pic}^0(C_1).$$

In particolare è possibile così dimostrare III.2.10:

Sia C una curva liscia e sia $f \in \bar{\mathbb{K}}(C)$. La funzione f induce la mappa tra curve $f\colon C \to \mathbb{P}^1$ e si ottiene

$$\begin{aligned}\deg \operatorname{div} f = \deg f^*((0) - (\infty)) &= \deg f^*((0)) - \deg f^*((\infty)) \\ &= \deg f - \deg f = 0.\end{aligned}$$

3. Differenziali

Definizione III.3.1. Lo *spazio delle forme differenziali (meromorfe) su C* è il $\bar{\mathbb{K}}$-spazio vettoriale Ω_C generato dai simboli dx, con $x \in \bar{\mathbb{K}}(C)$, che rispettano le seguenti condizioni:

(1) $d(x+y) = dx + dy$,
(2) $d(xy) = x\,dy + y\,dx$,
(3) $dk = 0$,

per ogni $x, y \in \bar{\mathbb{K}}(C)$ e $k \in \bar{\mathbb{K}}$.

Osservazione III.3.2. Sia $\phi\colon C_1 \to C_2$ una mappa non costante di curve lisce. Allora la mappa associata $\phi^*\colon \bar{\mathbb{K}}(C_2) \to \bar{\mathbb{K}}(C_1)$ induce una mappa sui differenziali data da

$$\phi^*\colon \Omega_{C_2} \to \Omega_{C_1}, \quad \phi^*\left(\sum f_i dx_i\right) = \sum (\phi^* f_i) d(\phi^* x_i).$$

Proposizione III.3.3. *Sia C una curva.*

(1) *Ω_C è uno spazio vettoriale su $\bar{\mathbb{K}}(C)$ di dimensione 1.*
(2) *Sia $x \in \bar{\mathbb{K}}(C)$. Allora dx è una base per Ω_C se e solo se $\bar{\mathbb{K}}(C)/\bar{\mathbb{K}}(x)$ è un'estensione finita e separabile.*

Dimostrazione. [Sha77, III §4, Teorema 3]. □

Proposizione III.3.4. *Sia $\phi\colon C_1 \to C_2$ una mappa non costante di curve. Allora ϕ è separabile se e solo se la seguente mappa è iniettiva*

$$\phi^*\colon \Omega_{C_2} \to \Omega_{C_1}.$$

Dimostrazione. Da III.3.3 sia $y \in \bar{\mathbb{K}}(C_2)$ tale che $\Omega_{C_2} = \bar{\mathbb{K}}(C_2)dy$ e $\bar{\mathbb{K}}(C_2)/\bar{\mathbb{K}}(y)$ sia separabile. Segue che $\phi^*\bar{\mathbb{K}}(C_2)$ è separabile su $\phi^*\bar{\mathbb{K}}(y) = \bar{\mathbb{K}}(\phi^* y)$. Si ha quindi

$$\begin{aligned}\phi^* \text{ è iniettiva} &\iff d(\phi^* y) \neq 0 \\ &\iff d(\phi^* y) \text{ è una base di } \Omega_{C_2} \\ &\iff \bar{\mathbb{K}}(C_1)/\bar{\mathbb{K}}(\phi^* y) \text{ è separabile} \\ &\iff \bar{\mathbb{K}}(C_1)/\phi^*\bar{\mathbb{K}}(C_2) \text{ è separabile.}\end{aligned}$$ □

Proposizione III.3.5. *Siano C una curva, $P \in C$ e $t \in \bar{\mathbb{K}}(C)$ un uniformatore in P.*

(1) *Sia $\omega \in \Omega_C$. Allora esiste ed è unica una funzione $g \in \bar{\mathbb{K}}(C)$ (dipendente da ω, t) tale che $\omega = g\,dt$. Tale funzione viene denotata ω/dt.*
(2) *Sia $f \in \bar{\mathbb{K}}(C)$ regolare in P. Allora anche df/dt è regolare in P.*

(3) *Sia* $\omega \in \Omega_C$ *con* $\omega \neq 0$. *La quantità* $\mathrm{ord}_P(\omega/dt)$ *dipende solo da* ω, P *e* non *dalla scelta dell'uniformatore* t. *Questo valore è chiamato ordine di* ω *in* P *ed è denotato* $\mathrm{ord}_P(\omega)$.

(4) *Sia* $\mathrm{char}\mathbb{K} = p$. *Siano* $x, f \in \bar{\mathbb{K}}(C)$ *con* $x(P) = 0$ *e* $p = 0$ *oppure* $p \nmid \mathrm{ord}_P(x)$. *Allora vale*

$$\mathrm{ord}_P(f\,dx) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1.$$

(5) *Sia* $\omega \in \Omega_C$ *con* $\omega \neq 0$. *Allora per quasi ogni* $P \in C$ *vale* $\mathrm{ord}_P(\omega) = 0$.

Dimostrazione. (1) Segue da III.0.6 e III.3.3.

(2) Vedi [Har77, commento dopo IV.2.1].

(3) Sia t' un altro uniformatore in P. Da 2 si ha che sia dt/dt' sia dt'/dt sono regolari in P e perciò $\mathrm{ord}_P(dt'/dt) = 0$. Si conclude notando che

$$\omega = g\,dt' = g(dt'/dt)\,dt.$$

(4) Sia $x = ut^n$ con $n = \mathrm{ord}_P(x) > 0$ e quindi $\mathrm{ord}_P(u) = 0$. Si ha che

$$dx = [nut^{n-1} + (du/dt)t^n]\,dt.$$

Da 2 si ha che du/dt è regolare in P e perciò essendo $n \neq 0$ il primo termine ha ordine maggiore del secondo, da cui si ottiene

$$\mathrm{ord}_P(f\,dx) = \mathrm{ord}_P(fnut^{n-1}\,dt) = \mathrm{ord}_P(f) + n - 1.$$

(5) Sia $x \in \bar{\mathbb{K}}(C)$ tale che $\bar{\mathbb{K}}(C)/\bar{\mathbb{K}}(x)$ sia separabile e sia $f \in \bar{\mathbb{K}}(C)$ per cui $\omega = f\,dx$. Da [Har77, IV.2.2a] si ha che la mappa $x\colon C \to \mathbb{P}^1$ ramifica in un numero finito di punti di C. A meno di un numero finito di punti, si assuma quindi che $P \in C$ rispetti

$$f(P) \neq 0, \infty, \quad x(P) \neq \infty,$$

e la mappa $x\colon C \to \mathbb{P}^1$ non sia ramificata in P. Le condizioni su x implicano che $(x - x(P))$ sia un uniformatore in P e perciò vale

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P\left(f\,d(x - x(P))\right) = 0. \qquad \square$$

Definizione III.3.6. Sia $\omega \in \Omega_C$. Si chiama *divisore associato a* ω e si denota $\mathrm{div}(\omega)$ il divisore dato da

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

Il differenziale ω è detto *olomorfo* se

$$\mathrm{ord}_P(\omega) \geq 0, \quad \forall P \in C.$$

Il differenziale ω è detto *non-vanishing* se

$$\mathrm{ord}_P(\omega) \leq 0, \quad \forall P \in C.$$

Osservazione III.3.7. Se $\omega_1, \omega_2 \in \Omega_C$ sono differenziali non nulli da III.3.3 esiste una funzione $f \in \bar{\mathbb{K}}(C)^*$ tale che

$$\omega_1 = f\omega_2 \implies \mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(omega_2).$$

Definizione III.3.8. Si chiama *classe dei divisori canonici su C* l'immagine in $\mathrm{Pic}(C)$ di $\mathrm{div}(\omega)$ per un qualunque differenziale non nullo $\omega \in \Omega_C$. Un divisore in questa classe è detto *divisore canonico di C*.

Esempio III.3.9. Su $\mathbb{P}^1$ non esistono differenziali olomorfi. Sia infatti t una funzione coordinata di $\mathbb{P}^1$ e si calcoli $\mathrm{div}(dt)$. Dato $\alpha \in \bar{\mathbb{K}}$ allora $t - \alpha$ è un uniformatore in α e perciò

$$\mathrm{ord}_\alpha(dt) = \mathrm{ord}_\alpha(d(t-\alpha)) = 0.$$

Per il punto $\infty \in \mathbb{P}^1$ un possibile uniformatore è dato da $1/t$, si ha quindi

$$\mathrm{ord}_\infty(dt) = \mathrm{ord}_\infty\left(-t^2 d\left(\frac{1}{t}\right)\right) = -2.$$

Sia ora $\omega \in \Omega_{\mathbb{P}^1}$. Da III.3.5 si ha

$$\deg \mathrm{div}(\omega) = \deg \mathrm{div}(dt) = -2,$$

quindi ω non è olomorfa.

Esempio III.3.10. Sia C la curva data da

$$C\colon y^2 = (x-x_1)(x-x_2)(x-x_3),$$

(continuando l'esempio in III.2.13). Allora per calcolare $\mathrm{div}(dx)$ basta notare che $dx = d(x-x_i) = -x^2 d(1/x)$ e perciò usando III.3.5 si ha

$$\mathrm{div}(dx) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

Inoltre $\mathrm{div}(y) = \mathrm{div}(dx)$ (sempre da III.2.13) e quindi $\mathrm{div}(dx/y) = 0$. Si ha perciò che il differenziale dx/y è sia olomorfo sia non-vanishing.

4. Teorema di Riemann-Roch

Definizione III.4.1. Un divisore $D = \sum n_P(P)$ è detto *effettivo* e si scrive $D \geq 0$ se vale $n_P \geq 0$, $\forall P \in C$. Dati due divisori $D_1, D_2 \in \mathrm{Div}(C)$ si scrive $D_1 \geq D_2$ se $D_1 - D_2$ è effettivo.

Osservazione III.4.2. La relazione tra divisori $D_1 \geq D_2$ è una relazione di ordine parziale.

Definizione III.4.3. Dato $D \in \mathrm{Div}(C)$ si definisce l'insieme di funzioni

$$\mathcal{L}(D) = \{f \in \bar{\mathbb{K}}(C)^* \colon \mathrm{div}(f) + D \geq 0\} \cup \{0\},$$

È immediato che $\mathcal{L}(D)$ sia uno spazio vettoriale su $\bar{\mathbb{K}}$ e si definisce

$$\ell(D) = \dim_{\bar{\mathbb{K}}} \mathcal{L}(D).$$

Osservazione III.4.4. Nel caso in cui $D = 0$ si ha che $\mathcal{L}(D) = \mathcal{L}(0) = \bar{\mathbb{K}}$. Infatti se $f \in \bar{\mathbb{K}}(C) \in \mathcal{L}(0)$ allora $\mathrm{div}(f) \geq 0$, ovvero f non ha poli. Dalla proposizione III.0.5 segue quindi che $f \in \bar{\mathbb{K}}$. L'altra inclusione è banale.

Proposizione III.4.5. *Sia $D \in \mathrm{Div}(C)$.*

(1) *Se $\deg(D) < 0$ allora si ha $\mathcal{L} = \{0\}$ e quindi $\ell(D) = 0$.*
(2) *$\mathcal{L}(D)$ è uno spazio vettoriale su $\bar{\mathbb{K}}$ di dimensione finita (perciò $\ell(D)$ è sempre ben definita).*

(3) *Sia* $D' \in \mathrm{Div}(C)$ *linearmente equivalente a* D. *Allora vale* $\mathcal{L}(D') \cong \mathcal{L}(D)$ *e quindi* $\ell(D') = \ell(D)$.

DIMOSTRAZIONE. (1) Sia $f \in \mathcal{L}(D)$ non nulla. Da III.2.10 si ha che

$$0 = \deg \mathrm{div} f \implies \deg D = \deg(\mathrm{div} f + D) \geq 0.$$

(2) Che $\mathcal{L}(D)$ sia uno spazio vettoriale su $\bar{\mathbb{K}}$ è immediato. La finitezza segue dalla stima sulla dimensione data dalla proposizione III.4.6.

(3) Se $D' \sim D$ allora esiste $g \in \bar{\mathbb{K}}(C)^*$ tale che $\mathrm{div} g = D' - D$. La seguente mappa è l'isomorfismo cercato

$$\psi \colon \mathcal{L}(D) \to \mathcal{L}(D'), \quad f \mapsto fg. \qquad \square$$

PROPOSIZIONE III.4.6. *Siano* $D, D' \in \mathrm{Div}(C)$ *divisori con* D *divisore effettivo.*

(1) *Se* $D \leq D'$ *allora vale* $\mathcal{L}(D) \subset \mathcal{L}(D')$ *e si ha la seguente stima dimensionale*

$$\dim_{\bar{\mathbb{K}}} \frac{\mathcal{L}(D')}{\mathcal{L}(D)} \leq \deg(D' - D).$$

(2) $\ell(D) \leq \deg D + 1$.

DIMOSTRAZIONE. (1) L'inclusione tra spazi è immediata. Per provare la disuguaglianza si supponga senza perdere di generalità che $D' = D + P$ con $P \in C$. Allora si ha che D, D' si scrivono nella forma

$$D = a(P) + \sum_{Q \in C \setminus \{P\}} n_Q(Q), \quad D' = (a+1)(P) + \sum_{Q \in C \setminus \{P\}} n_Q(Q),$$

per qualche $a \in \mathbb{Z}$. In particolare se $f \in \mathcal{L}(D')$ si ha che $\mathrm{ord}_P(f) \geq -(a+1)$ e quindi preso un uniformatore $t \in \bar{\mathbb{K}}(C)$ in P si ha che la mappa

$$\phi \colon \mathcal{L}(D') \to \bar{\mathbb{K}}, \quad f \mapsto (t^{a+1} f)(P),$$

è ben definita (infatti $\mathrm{ord}_P(t^{a+1} f) \geq 0$) ed è lineare su $\bar{\mathbb{K}}$. Il nucleo di ϕ è dato da $\mathcal{L}(D)$ e l'immagine di ϕ ha al più dimensione 1, ovvero

$$\dim_{\bar{\mathbb{K}}} \frac{\mathcal{L}(D')}{\mathcal{L}(D)} \leq 1 = \deg(D' - D).$$

(2) Come visto in III.2.11 e III.4.5 i lati della disuguaglianza sono invarianti per divisori linearmente equivalenti. Se $\deg D = 0$ la stima è immediata da III.4.4. Se $\deg D > 0$ sia $f \in \mathcal{L}(D)$ non nulla. Sia $D' = D + \mathrm{div} f \geq 0$, allora dal punto precedente si ha

$$\ell(D') - 1 = \dim_{\bar{\mathbb{K}}} \frac{\mathcal{L}(D')}{\mathcal{L}(0)} \leq \deg(D' - 0) = \deg D'.$$

Dato che $D' \sim D$ si conclude. $\square$

Esempio III.4.7. Sia $K_C \in \mathrm{Div}(C)$ un divisore canonico, cioè $K_C = \mathrm{div}(\omega)$ per qualche $\omega \in \Omega_C$. Allora ogni funzione $f \in \mathcal{L}(K_C)$ rispetta

$$\mathrm{div}(f) + K_C \geq 0 \iff \mathrm{div}(f) + \mathrm{div}(\omega) \geq 0 \iff \mathrm{div}(f\omega) \geq 0,$$

ovvero $f\omega$ è olomorfa. Viceversa, se $f\omega$ è olomorfa allora $f \in \mathcal{L}(K_C)$. Dato che ogni differenziale su C può essere scritto come $f\omega$ per qualche f si ha un isomorfismo di spazi vettoriali su $\bar{\mathbb{K}}$

$$\mathcal{L}(K_C) \cong \{\omega \in \Omega_C : \omega \text{ è olomorfa}\}.$$

La dimensione $\ell(K_C)$ di questi spazi è quindi un'invariante di C, che si rivela di fondamentale importanza.

Teorema III.4.8 (Riemann-Roch). *Sia C una curva liscia e K_C un divisore canonico di C. Allora per ogni divisore $D \in \mathrm{Div}(C)$ vale*

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

dove g è una costante che non dipende dal divisore considerato ma solo dalla curva.

Definizione III.4.9. La costante g è detta *genere* della curva C.

Corollario III.4.10.
(1) *Usando III.4.8 con $D = 0$ si ottiene $1 - \ell(K_C) = 0 - g + 1$ da cui si deduce $\ell(K_C) = g$.*
(2) *Usando III.4.8 con $D = K_C$ si ottiene $g - 1 = \deg K_C - g + 1$ da cui si deduce $\deg K_C = 2g - 2$.*
(3) *Se $\deg D > 2g-2$ si ha $\deg(K_C - D) < 0$, da cui $\ell(K_C - D) = 0$ e quindi $\ell(D) = \deg D - g + 1$.*

Esempio III.4.11. Sia $C = \mathbb{P}^1$. Allora da III.3.9 non esistono differenziali olomorfi su C. Segue quindi da III.4.7 che $\ell(K_C) = 0$. Per III.4.10 quindi la retta proiettiva $\mathbb{P}^1$ ha genere 0. Il teorema di Riemann-Roch in questo caso diventa quindi

$$\ell(D) - \ell(-2(\infty) - D) = \deg D + 1.$$

In particolare se $\deg D \geq -1$ si ha

$$\ell(-2(\infty) - D) = 0 \implies \ell(D) = \deg D + 1.$$

Esempio III.4.12. Sia C la curva data da

$$C : y^2 = (x - x_1)(x - x_2)(x - x_3),$$

(continuando l'esempio in III.2.13 e III.3.10). Come visto $\mathrm{div}(dx/y) = 0$ e perciò $K_C = 0$. Da III.4.10 segue che

$$g = \ell(\mathbb{K}_C) = \ell(0) = 1,$$

cioè C ha genere 1. Dato un divisore D con $\deg D \geq 1$ allora Riemann-Roch diventa $\ell(D) = \deg D$. Si notino i seguenti casi particolari

(1) Sia $P \in C$, allora $\ell((P)) = 1$. Lo spazio $\mathcal{L}((P))$ contiene le funzioni costanti e perciò $\mathcal{L}((P)) = \bar{\mathbb{K}}(C)$. Segue che non esistono funzioni su C con poli di ordine 1.

(2) Sia $P_\infty \in C$ il punto all'infinito. Allora chiaramente $\ell(n(P)) = n$ per $n \in \mathbb{Z}, n > 0$. Si ha che

$$\{1, x\} \text{ è base di } \mathcal{L}(2(P_\infty)),$$
$$\{1, x, y\} \text{ è base di } \mathcal{L}(3(P_\infty)),$$
$$\{1, x, y, x^2\} \text{ è base di } \mathcal{L}(4(P_\infty)).$$

(3) Le sette funzioni $1, x, y, x^2, xy, x^3, y^2$ sono tutte in $\mathcal{L}(6(P_\infty))$, che ha dimensione 6. Queste funzioni sono perciò linearmente dipendenti su $\bar{\mathbb{K}}$ e un esempio di loro dipendenza è dato proprio da $y^2 = (x - x_1)(x - x_2)(x - x_3)$.

PROPOSIZIONE III.4.13. *Siano $C/\mathbb{K}$ una curva liscia e $D \in \mathrm{Div}_{\mathbb{K}}(C)$. Allora esiste una base di $\mathcal{L}(D)$ costituita di funzioni in $\mathbb{K}(C)$.*

DIMOSTRAZIONE. Vedi [Sil09, § II.5.8]. □

CAPITOLO IV

Curve ellittiche

DEFINIZIONE IV.0.1. Si chiama *curva ellittica* la coppia (E, O), con E una curva liscia di genere 1 e $O \in E$. (Di solito si indica semplicemente E, tenendo O sottinteso.) O viene detto punto base di E. Si dice che la curva ellittica E è *definita su* $\mathbb{K}$ e si indica $E/\mathbb{K}$ se E è definita su $\mathbb{K}$ come curva e $O \in E(\mathbb{K})$.

1. Forma di Weierstrass

PROPOSIZIONE IV.1.1. *Sia E una curva ellittica definita su $\mathbb{K}$.*

(1) *Esiste un isomorfismo $\phi\colon E \to \mathbb{P}^2$ della forma $\phi = [x : y : 1]$ con $x, y \in \mathbb{K}(E)$ che mappa E con la curva data dall'equazione di Weierstrass*

$$C\colon Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{1.1}$$

dove $a_i \in \mathbb{K}$, e che manda il punto base in $[0 : 1 : 0]$. Le funzioni x, y sono dette coordinate di Weierstrass di E.

(2) *Due equazioni di Weierstrass per la stessa curva E sono coniugate da un cambio di coordinate lineare della forma*

$$(X, Y) \mapsto (u^2X + r, u^3Y + su^2X + t), \tag{1.2}$$

con $u \in \mathbb{K}^*$ e $r, s, t \in \mathbb{K}$.

DIMOSTRAZIONE. (1) Si consideri lo spazio $\mathcal{L}(n(O))$ per $n \in \mathbb{Z}, n > 0$. Il genere di E è per definizione $g = 1$. Per il teorema di Riemann-Roch (III.4.10) si ha

$$\ell(n(O)) = \dim \mathcal{L}(n(O)) = \deg(n(O)) - g + 1 = n, \quad \forall n.$$

Come visto in III.4.13 si possono quindi scegliere $x, y \in \mathbb{K}(E)$ in modo che $\{1, x\}$ sia una base di $\mathcal{L}(2(O))$ e $\{1, x, y\}$ sia una base di $\mathcal{L}(3(O))$. In particolare x ha un polo di ordine 2 in O e y ha un polo di ordine 3 in O. Segue che le 7 funzioni $1, x, y, x^2, xy, y^2, x^3$ sono tutte contenute in $\mathcal{L}(6(O))$, che ha dimensione 6, e perciò esiste una combinazione lineare non banale

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0,$$

dove $A_1, \ldots, A_7 \in \mathbb{K}$ (ancora da III.4.13). In particolare si deve anche avere $A_6 \neq 0$ e $A_7 \neq 0$, gli altri termini hanno infatti tutti poli in O di ordine diverso e perciò se $A_6A_7 = 0$ l'unica combinazione lineare possibile sarebbe quella con $A_j = 0, \forall j$.

Si può quindi sostituire $(x, y) \mapsto (-A_6A_7x, A_6A_7^2y)$ e dividendo tutto per $A_6^3A_7^4$ si ottiene l'equazione di Weierstrass richiesta

$$y^2 - \frac{A_5}{A_6A_7}xy + \frac{A_3}{A_6^2A_7^2}y = x^3 - \frac{A_4}{A_6A_7^2}x^2 + \frac{A_2}{A_6^2A_7^3}x - \frac{A_1}{A_6^3A_7^4}.$$

Si ottiene così una mappa

$$\phi\colon E \to C \subset \mathbb{P}^2, \quad \phi = [x : y : 1],$$

che manda i punti di E nell'immagine C contenuta nel luogo dei punti che soddisfano l'equazione. Inoltre ϕ è un morfismo (III.1.1) suriettivo (III.1.3) e si ha $\phi(O) = [0 : 1 : 0]$ (infatti il polo in O di y è di ordine maggiore rispetto a x).

Si consideri ora la mappa $[x : 1]\colon E \to \mathbb{P}^1$. La funzione x ha un polo di ordine 2 in O e perciò da III.1.9 la mappa ha grado 2, cioè $[\mathbb{K}(E) : \mathbb{K}(x)] = 2$. Analogamente, si consideri la mappa $[y : 1]\colon E \to \mathbb{P}^1$. La funzione y ha un polo di ordine 3 in O e quindi si ha $[\mathbb{K}(E) : \mathbb{K}(y)] = 3$. Segue che $[\mathbb{K}(E) : \mathbb{K}(x, y)] = 1$ in quanto deve dividere sia 2 che 3. Ciò vuol dire che la mappa $\phi\colon E \to C$ ha grado 1.

Si supponga per assurdo che C sia singolare. Allora si vedrà in IV.1.11 che esiste una mappa razionale $\psi\colon C \to \mathbb{P}^1$ di grado 1. Ma allora la composizione $\psi \circ \phi\colon E \to \mathbb{P}^1$ è una mappa razionale di grado 1 tra curve lisce e perciò da III.1.7 è un isomorfismo. Si ha però che il genere di E è per definizione 1 mentre $\mathbb{P}^1$ ha genere 0 (III.4.11) $\lightning$. Segue quindi che C è liscia e quindi sempre da III.1.7 si ha che $\phi\colon E \to C$ è un isomorfismo.

(2) Siano ora $\{x, y\}$ e $\{x', y'\}$ funzioni coordinate di Weierstrass per E. Dato che x, x' hanno un polo di ordine 2 in O si ha che $\{1, x\}, \{1, x'\}$ sono due basi dello spazio $\mathcal{L}(2(O))$. Analogamente y, y' hanno un polo di ordine 3 in O e quindi $\{1, x, y\}, \{1, x', y'\}$ sono basi di $\mathcal{L}(3(O))$. Si ha allora che esistono $u_1, u_2 \in \mathbb{K}^*$ e $r, s_2, t \in \mathbb{K}$ tali che

$$x = u_1x' + r, \quad y = u_2y' + s_2x' + t.$$

Essendo inoltre $(x, y), (x', y')$ soluzioni di equazioni di Weierstrass in cui i termini X^3 e Y^2 hanno coefficiente 1 si deve avere $u_1^3 = u_2^2$. Posti $u = u_2/u_1$ e $s = s_2/u^2$ si ottiene infine

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t,$$

come richiesto. □

Proposizione IV.1.2. *Ogni cubica liscia C data da un'equazione di Weierstrass è una curva ellittica definita su K con punto base $O = [0 : 1 : 0]$.*

Dimostrazione. Si rimanda la dimostrazione a più avanti in IV.3.5. □

NOTAZIONE IV.1.3. Ai coefficienti a_i di (1.1) si associano le seguenti quantità, la cui utilità sarà chiara più avanti:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

OSSERVAZIONE IV.1.4. Se $\mathrm{char}(\mathbb{K}) \neq 2$ si può semplificare l'equazione (1.1) completando il quadrato con la sostituzione

$$(x, y) \mapsto \left(x, \frac{1}{2}(y - a_1x - a_3)\right).$$

L'equazione che si ottiene è

$$C\colon y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{1.3}$$

dove i b_i sono quelli definiti in IV.1.3.

OSSERVAZIONE IV.1.5. Se $\mathrm{char}(\mathbb{K}) \neq 2, 3$ l'equazione precedente si può semplificare ulteriormente con la sostituzione

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

cancellando il termine in x^2. L'equazione che si ottiene è

$$C\colon y^2 = x^3 - 27c_4x - 54c_6,$$

dove i c_i sono gli stessi definiti in IV.1.3.

OSSERVAZIONE IV.1.6. Dato che se $\mathrm{char}(\mathbb{K}) \neq 2, 3$ l'equazione di Weierstrass ha una forma relativamente semplice, nelle dimostrazioni dei teoremi a volte si escluderanno i casi con caratteristica $2, 3$ per rendere la dimostrazione più semplice e corta. Tuttavia nello studio delle curve ellittiche è importante studiare anche questi due casi, perciò le dimostrazioni per campi con caratteristica $2, 3$ si trovano nell'appendice alla fine dell'articolo.

DEFINIZIONE IV.1.7. Viene detto *discriminante* dell'equazione di Weierstrass la quantità

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

OSSERVAZIONE IV.1.8. Con un calcolo diretto si ottengono le relazioni

$$4b_8 = b_2b_6 - b_4^2, \quad 1728\Delta = c_4^3 - c_6^2.$$

PROPOSIZIONE IV.1.9. *Sia C una cubica in forma di Weierstrass. Allora C è liscia se e solo se il Δ associato è non-nullo.*

Dimostrazione. Sia C data dall'equazione

$$E\colon f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Per studiare il punto all'infinito $O = [0:1:0]$ si consideri la curva in $\mathbb{P}^2$ data dall'equazione omogenea

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

Si verifica direttamente che O non è punto singolare, infatti

$$\frac{\partial F}{\partial Z}(O) = 1 \neq 0.$$

Sia ora $P_0 = (x_0, y_0)$ un punto su C. Il cambio di coordinate

$$(x,y) \mapsto (x + x_0, y + y_0),$$

lascia il Δ invariato, quindi senza perdere di generalità si può supporre $P_0 = (0,0)$. Se P_0 è singolare si ha

$$a_6 = f(0,0) = 0, \quad a_4 = \frac{\partial f}{\partial x}(0,0) = 0, \quad a_3 = \frac{\partial f}{\partial y}(0,0) = 0,$$

da cui l'equazione di C diventa

$$C\colon y^2 + a_1xy - x^3 - a_2x^2 = 0.$$

Si verifica immediatamente che $\Delta = 0$.

Viceversa sia $\mathrm{char}(\mathbb{K}) \neq 2$ e si supponga che C sia liscia. L'equazione di Weierstrass si può scrivere nella forma

$$C\colon y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

come visto in (1.3). Un punto $P_0 = (x_0, y_0) \in E$ è singolare se e solo se soddisfa

$$2y_0 = 0, \quad 12x_0^2 + 2b_2x_0 + 2b_4 = 0,$$

cioè se e solo se $y_0 = 0$ e x_0 è una radice doppia del polinomio $4x^3 + b_2x^2 + 2b_4x + b_6$. Il discriminante di questo polinomio è uguale a 16Δ e perciò ha radici multiple se e solo se $16\Delta = 0$. Dato che C è liscia, $16\Delta \neq 0$ e perciò $\Delta \neq 0$. □

Osservazione IV.1.10. Se $\mathrm{char}(\mathbb{K}) \neq 2$, dalla dimostrazione precedente si nota come un punto singolare per una cubica di Weierstrass C è della forma $(x_0, 0)$, con x_0 radice del polinomio ben definito $4x^3 + b_2x^2 + 2b_4x + b_6$. Essendo questo di grado 3, non può avere più di una radice multipla (già 2 radici di molteplicità 2 richiederebbero un polinomio di grado ≥ 4) e quindi la curva ha al più un solo punto singolare.

Proposizione IV.1.11. *Se una curva C data da un'equazione di Weierstrass è singolare allora esiste una mappa razionale $\phi\colon C \to \mathbb{P}^1$ di grado* 1.

Dimostrazione. Con un cambio di coordinate si può assumere, senza perdere di generalità, che C sia singolare in $(0,0)$. L'equazione di Weierstrass deve perciò essere della forma

$$E\colon y^2 + a_1xy = x^3 + a_2x^2,$$

ponendo le derivate parziali nulle in $(0,0)$. Segue che la mappa razionale

$$\phi\colon C \to \mathbb{P}^1, \quad (x,y) \mapsto [x:y],$$

è di grado 1 dato che esiste l'inversa data da

$$\phi^{-1}\colon \mathbb{P}^1 \to C, \quad [1:t] \mapsto (t^2 + a_1 t - a_2, t^3 + a_1 t^2 - a_2 t). \qquad \square$$

2. j-invariante

Definizione IV.2.1. Sia C una cubica in forma di Weierstrass. Nel caso in cui $\Delta \neq 0$, cioè la curva associata sia liscia, si introduce la quantità

$$j(C) = \frac{c_4^3}{\Delta} = 12^3 \frac{c_4^3}{c_4^3 - c_6^2},$$

chiamata *j-invariante* di C.

Osservazione IV.2.2. Sotto il cambio di coordinate (1.2) c_4, c_6, j vengono mappati in

$$c_4 \mapsto u^4 c_4, \quad c_6 \mapsto u^6 c_6, \quad j \mapsto j.$$

Questo vuol dire quindi che j è invariante sotto cambi di coordinate. Segue che, a meno di isomorfismi su $\bar{\mathbb{K}}$, j dipende solo dalla curva ellittica E associata alla cubica, non a quale forma di Weierstrass si sceglie per rappresentarla. Se due curve E e E' sono isomorfe su $\bar{\mathbb{K}}$, allora si ha $j(E) = j(E')$.

Proposizione IV.2.3. *Due curve ellittiche sono isomorfe su $\bar{\mathbb{K}}$ se e solo se i loro j-invarianti sono uguali.*

Dimostrazione. Si è già visto nell'osservazione (IV.2.2) che se due curve sono isomorfe su $\bar{\mathbb{K}}$ allora hanno gli stessi j-invarianti.

Viceversa, sia $\mathrm{char}(\mathbb{K}) \neq 2, 3$ (le dimostrazioni per questi due casi si trovano nell'appendice). Siano date due curve ellittiche su $\mathbb{K}$ nella seguente forma

$$\begin{aligned} E\colon y^2 &= x^3 + Ax + B, & A, B &\in \mathbb{K}, \\ E'\colon y'^2 &= x'^3 + A'x' + B', & A', B' &\in \mathbb{K}, \end{aligned}$$

che abbiano lo stesso j-invariante. Segue che

$$\frac{(4A)^3}{4A^3 + 27B^2} = j(E) = j(E') = \frac{(4A')^3}{4A'^3 + 27B'^2},$$

da cui si ottiene che $A^3 B'^2 = A'^3 B^2$. L'obiettivo ora è di trovare un isomorfismo del tipo $(x,y) = (u^2 x', u^3 y')$ con $u \in \mathbb{K}^*$. Si distinguono tre casi:

(1) $A = 0$, che corrisponde a $j = 0$. Dato che $\Delta \neq 0$ si deve avere $B \neq 0$ e perciò $A' = 0$. L'isomorfismo cercato è dato da $u = (B/B')^{1/6}$.
(2) $B = 0$, che corrisponde a $j = 1728$. Dato che $\Delta \neq 0$ si deve avere $A \neq 0$ e perciò $B' = 0$. L'isomorfismo cercato è dato da $u = (A/A')^{1/4}$.

(3) $A \neq 0, B \neq 0$, cioè $j \neq 0, 1728$. Si ha quindi che $A' = 0 \iff B' = 0$ e se entrambi sono nulli si ha $\Delta' = 0$. Dato che $\Delta' \neq 0$ si deve per forza avere $A' \neq 0$, $B' \neq 0$. L'isomorfismo cercato è dato da $u = (A/A')^{1/4} = (B/B')^{1/6}$. □

PROPOSIZIONE IV.2.4. *Per ogni $j_0 \in \bar{\mathbb{K}}$ esiste una curva ellittica definita su $\mathbb{K}(j_0)$ il cui j-invariante è proprio j_0.*

DIMOSTRAZIONE. Si considerino i seguenti casi:

(1) $j_0 = 0$. Una possibile curva è data da
$$E\colon y^2 + y = x^3.$$
Si verifica direttamente che $\Delta = -27$ (quindi se $\mathrm{char}(\mathbb{K}) \neq 3, E$ è liscia) e $j(E) = 0$,

(2) $j_0 = 1728$. Una possibile curva è data da
$$E\colon y^2 = x^3 + x.$$
Si verifica direttamente che $\Delta = -64$ (quindi se $\mathrm{char}(\mathbb{K}) \neq 2, E$ è liscia) e $j(E) = 1728$,

(3) $j_0 \neq 0, 1728$. Si consideri la curva
$$E\colon y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$
Si verifica direttamente che $\Delta = \frac{j_0^3}{(j_0-1728)^3} \neq 0$ (quindi E è liscia) e $j(E) = j_0$.

Per concludere si noti come nei casi in cui $\mathrm{char}(\mathbb{K}) \in \{2, 3\}$ si ha $0 = 1728$. Perciò se $\mathrm{char}(\mathbb{K}) = 2$ il caso 1 fornisce una curva ellittica con $j_0 = 1728$; se $\mathrm{char}(\mathbb{K}) = 3$ il caso 2 fornisce una curva ellittica con $j_0 = 0$. □

3. Differenziale invariante

DEFINIZIONE IV.3.1. Si chiama *differenziale invariante* associato alla equazione di Weierstrass la forma differenziale
$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},$$
dove gli a_i sono i coefficienti dell'equazione (1.1).

OSSERVAZIONE IV.3.2. Scrivendo l'equazione della cubica di Weierstrass nel seguente modo
$$C\colon 0 = f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,$$
si nota come il differenziale invariante di C non è altri che
$$\omega = \frac{dx}{f_y(x, y)} = -\frac{dy}{f_x(x, y)}.$$

OSSERVAZIONE IV.3.3. Sotto il cambio di coordinate (1.2) la forma differenziale ω è mappata
$$\omega \mapsto u^{-1}\omega.$$

Proposizione IV.3.4. *Sia E una curva ellittica. Allora il differenziale invariante ω associato a un'equazione di Weierstrass per E è olomorfo e non-vanishing.*

Dimostrazione. Sia E data dall'equazione di Weierstrass

$$E\colon f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

e sia $P = (x_0, y_0) \in E$. Sia quindi ω data da

$$\omega = \frac{d(x - x_0)}{f_y(x,y)} = -\frac{d(y - y_0)}{f_x(x,y)}.$$

Il punto P non è polo di ω, infatti se lo fosse si avrebbe $f_y(x_0, y_0) = f_x(x_0, y_0) = 0$ e quindi E sarebbe singolare in P. Si consideri la mappa

$$\phi\colon E \to \mathbb{P}^1, \quad [x : y : 1] \mapsto [x : 1].$$

Dato che ϕ è di grado 2 si ha che $\mathrm{ord}_P(x - x_0) \leq 2$ con uguaglianza se e solo se il polinomio $f(x_0, y)$ ha una radice doppia. Se $\mathrm{ord}_P(x - x_0) = 1$ allora $f_y(x_0, y_0) \neq 0$ e se $\mathrm{ord}_p(x - x_0) = 2$ allora $f_y(x_0, y_0) = 0$. In entrambi i casi si ha quindi (da III.3.5)

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P(x - x_0) - \mathrm{ord}_P(f_y) - 1 = 0,$$

cioè il punto P non è zero né polo di ω.

Rimane da mostrare che anche O non è né polo né zero di ω. Sia quindi $t \in \bar{\mathbb{K}}(E)$ un uniformatore in O. Dato che $\mathrm{ord}_O(x) = -2$ e $\mathrm{ord}_O(y) = -3$ esistono funzioni $f, g \in \bar{K}(E)$ tali che $x = t^{-2}f, y = t^{-3}g$ e inoltre $f(O), g(O) \neq 0, \infty$. Sostituendo in ω si ottiene

$$\omega = \frac{dx}{f_y(x,y)} = \frac{-2f + tf'}{2g + a_1tf + a_3t^3}dt.$$

dove $f' = df/dt$. Da III.3.5 si ha che f' è regolare in O. Segue che se $\mathrm{char}(\mathbb{K}) \neq 2$ la funzione

$$\frac{-2f + tf'}{2g + a_1tf + a_3t^3},$$

è regolare e non nulla in O e perciò $\mathrm{ord}_O(\omega) = 0$. Nel caso in cui $\mathrm{char}(\mathbb{K}) = 2$ si può effettuare un calcolo analogo andando a sostituire in $\omega = -dy/f_x(x,y)$. □

Osservazione IV.3.5. Sia C una curva liscia data da un'equazione di Weierstrass. Da IV.3.4 si ha che il differenziale

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_C,$$

non ha né zeri né poli e perciò si ha $\mathrm{div}(\omega) = 0$. Dal teorema di Riemann-Roch (III.4.10) si ha che

$$2g - 2 = \deg \mathrm{div}(\omega) = 0,$$

dove g è il genere di C. La curva C ha quindi genere 1 e prendendo $[0 : 1 : 0]$ come punto base si ottiene una curva ellittica. Ciò fornisce una dimostrazione di IV.1.2.

4. Legge di gruppo

Sia ora $E \subset \mathbb{P}^2$ una curva ellittica data da un'equazione di Weierstrass, costituita quindi dai punti $P = (x, y)$ che soddisfano l'equazione e il punto all'infinito $O = [0 : 1 : 0]$. Presa una retta $L \subset \mathbb{P}^2$ il teorema di Bézout garantisce che L intersechi E in tre punti, contati con molteplicità (infatti i gradi della retta e della curva sono rispettivamente 1 e 3). Si può mostrare questo fatto anche senza l'uso di teoria generale mostrando i calcoli nel caso considerato (IV.4.10). A partire da ciò si può definire un'operazione binaria sui punti di E nel seguente modo:

Definizione IV.4.1. Si indicherà con $\oplus\colon E \times E \to E$ la funzione

$$\oplus\colon E \times E \to E, \quad (P, Q) \mapsto P \oplus Q = R,$$

dove R è costruito nel seguente modo: sia $L = P \vee Q$ la retta per i due punti (se $P = Q$, sia L la tangente a E in P), R è il terzo punto di intersezione di L con E.

Osservazione IV.4.2. La funzione $\oplus$ rispetta la proprietà commutativa

$$P \oplus Q = Q \oplus P, \quad \forall P, Q \in E,$$

ma non è legge di gruppo. Ad esempio non esiste un punto 0 che sia l'elemento neutro, ovvero tale che $0 \oplus P = P \oplus 0 = P$.

Anche se con l'operazione $\oplus$ i punti di E non formano un gruppo, è possibile definire un'operazione a partire da $\oplus$ che in effetti sia legge di gruppo. Per farlo, si sceglie un punto $O \in E$ che fungerà da elemento neutro per la legge, e poi si considera la somma $O \oplus (P \oplus Q)$. Si vedrà come, con questa accortezza, le proprietà di gruppo vengono effettivamente rispettate.

Definizione IV.4.3. Data una curva ellittica E con punto base O, si definisce la seguente operazione binaria

$$+\colon E \times E \to E, \quad (P, Q) \mapsto P + Q = O \oplus (P \oplus Q).$$

Proposizione IV.4.4. *Siano $P, Q, R \in E$ punti non necessariamente distinti. L'operazione definita in IV.4.3 gode delle seguenti proprietà:*

(1) $P + O = P$,
(2) $P + Q = Q + P$,
(3) $(P + Q) + R = P + (Q + R)$,
(4) *esiste un punto denotato $-P$ tale che $P + (-P) = O$.*
(5) *Sia $O' = O \oplus O$. Se P, Q, R sono allineati allora $P + Q + R = O'$.*

Dimostrazione. (1) Sia P' il terzo punto di intersezione di $P \vee O$ con E. Allora $P + O = O \oplus (P \oplus O) = O \oplus P' = P$.
(2) $P + Q = O \oplus (P \oplus Q) = O \oplus (Q \oplus P) = Q + P$.
(3) Si deduce da IV.4.12.
(4) Sia $O' = O \oplus O$ il terzo punto di intersezione della tangente a E in O con E stessa, sia poi $P'' = P \oplus O'$. Si ha quindi

$$P + P'' = O \oplus (P \oplus P'') = O \oplus O' = O.$$

Si ha quindi $-P = P''$.

(5) Si ha che $Q + R = O \oplus (Q \oplus R) = O \oplus P = P'$ e quindi $P + (Q + R) = P + P' = O \oplus (P \oplus P') = O \oplus O = O'$. □

Osservazione IV.4.5. La proposizione IV.4.4 dice che in effetti E con l'operazione $+\colon E \times E \to E$ forma un gruppo abeliano il cui elemento neutro è O.

Osservazione IV.4.6. Una curva ellittica E associata a una cubica in forma di Weierstrass ha un flesso nel punto base, cioè $O = [0 : 1 : 0]$ ha molteplicità 3 e perciò in tal caso $O' = O \oplus O = O$. La 5 diventa quindi $P + Q + R = O$.

Proposizione IV.4.7. *Sia E una curva ellittica definita su $\mathbb{K}$. Allora*

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\},$$

è un sottogruppo di E.

Dimostrazione. Siano $P, Q \in E(\mathbb{K})$. Dalle formule esplicite in IV.4.10 è immediato che anche $-P$ e $P + Q$ hanno coefficienti in $\mathbb{K}$ e quindi $-P, P + Q \in E(\mathbb{K})$. □

Notazione IV.4.8. Per semplicità si usano le seguenti notazioni

$$[m]P = \begin{cases} \underbrace{P + P + \cdots + P}_{m \text{ termini}}, & \text{se } m > 0, \\ \underbrace{-P - P - \cdots - P}_{-m \text{ termini}}, & \text{se } m < 0, \\ O, & \text{se } m = 0, \end{cases}$$

dove $m \in \mathbb{Z}$, $P \in E$.

Definizione IV.4.9. Un punto $P \in E$ si dice *di ordine $m > 0$* se $[m]P = O$ e $[j]P \neq O$ per $1 \leq j < m$.

Osservazione IV.4.10. Finora si è descritta la legge di gruppo sui punti di una curva ellittica teoricamente. Si mostra ora un modo per trovare le formule esplicite per effettuare calcoli sui punti di una curva ellittica. Sia quindi E una curva ellittica data da un'equazione di Weierstrass

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Sia $P_0 = (x_0, y_0) \in E$, per trovare $-P_0$ si può seguire lo stesso procedimento nella dimostrazione di IV.4.4. Nella osservazione IV.4.6 si è visto come $O' = O$, quindi si consideri la retta $L = P_0 \vee O$. Il punto $-P_0$ sarà dato dal terzo punto di intersezione di L con E. La retta L è data dall'equazione

$$L\colon x - x_0 = 0.$$

Sostituendo in E si ottiene un polinomio quadratico $f(x_0, y)$ nella sola variabile y, che quindi ha due radici y_0, y_0' corrispondenti ai punti $P_0 = (x_0, y_0)$ e $-P_0 = (x_0, y_0')$. Si ha quindi che per qualche $c \in \bar{\mathbb{K}}$ vale

$$f(x_0, y) = c(y - y_0)(y - y_0').$$

Eguagliando i coefficienti ai due lati dell'equazione si ottiene che $c = 1$ e $y_0' = -y_0 - a_1x_0 - a_3$. Si ottiene perciò

$$-P_0 = -(x_0, y_0) = (x_0, -y_0 - a_1x_0 - a_3).$$

Siano $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$ e si voglia ricavare una formula per $P_1 + P_2$. Se $P_2 = -P_1$ (in formule $x_1 = x_2, y_1 + y_2 + a_1x_2 + a_3 = 0$) si è già mostrato che $P_1 + P_2 = O$. Sia quindi $P_2 \neq -P_1$. La retta $L = P_1 \vee P_2$ è data dall'equazione

$$L\colon y = \lambda x + \nu,$$

dove $\lambda, \nu \in \bar{\mathbb{K}}$ sono così definiti:

(1) Se $x_1 \neq x_2$,

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

(2) Se $x_1 = x_2$,

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

Sostituendo in E si ottiene un polinomio cubico $f(x, \lambda x + \nu)$ che ha radici x_1, x_2, x_3 corrispondenti ai tre punti P_1, P_2 e $P_3 = (x_3, y_3)$. Tale polinomio si fattorizza quindi come

$$f(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3), \quad c \in \bar{\mathbb{K}}.$$

Uguagliando i coefficienti termine a termine si ottiene $c = -1$ e

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu.$$

Da IV.4.6 si ha

$$P_1 + P_2 + P_3 = O \implies P_1 + P_2 = -P_3,$$

perciò si ottiene la formula

$$\begin{aligned} P_1 + P_2 = (x_1, y_1) + (x_2, y_2) &= -(x_3, y_3) \\ &= (x_3, -y_3 - a_1x_3 - a_3) \\ &= (x_3, -(\lambda + a_1)x_3 - \nu - a_3), \\ \text{con } x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2. \end{aligned}$$

Proposizione IV.4.11. *Sia C una curva di genere 1 e siano $P, Q \in C$. Allora*

$$(P) \sim (Q) \iff P = Q.$$

Dimostrazione. Sia $(P) \sim (Q)$. Esiste una funzione $f \in \bar{\mathbb{K}}(C)$ tale che $\operatorname{div}(f) = (P) - (Q)$ e quindi $f \in \mathcal{L}((Q))$. Chiaramente le funzioni costanti sono contenute in $\mathcal{L}((Q))$, dal teorema di Riemann-Roch (III.4.10) si ha che $\ell((Q)) = \dim \mathcal{L}((Q)) = 1$ e perciò $\mathcal{L}((Q)) = \bar{\mathbb{K}}$. Segue che $f \in \bar{\mathbb{K}}$ e quindi $P = Q$. □

Proposizione IV.4.12. *Sia E una curva ellittica con punto base O.*

(1) *Dato un divisore* $D \in \mathrm{Div}^0(E)$ *di grado* 0 *esiste ed è unico un punto* $P \in E$ *tale che*

$$D \sim (P) - (O).$$

Sia σ *la mappa che manda* D *nel suo punto associato*

$$\sigma\colon \mathrm{Div}^0(E) \to E, \quad D \mapsto P.$$

Allora σ *è suriettiva.*

(2) *Siano* $D_1, D_2 \in \mathrm{Div}^0(E)$*. Allora si ha*

$$\sigma(D_1) = \sigma(D_2) \iff D_1 \sim D_2.$$

La mappa σ *induce perciò una biezione*

$$\sigma\colon \mathrm{Pic}^0(E) \to E$$

con inversa $\sigma^{-1} = \kappa$ *data da*

$$\kappa\colon E \to \mathrm{Pic}^0(E), \quad P \mapsto [(P) - (O)].$$

(3) *Data la legge di gruppo su* E *vista in IV.4.3, la mappa* κ *è omomorfismo di gruppi.*

Dimostrazione. (1) Dato che E ha genere 1 dal teorema di Riemann-Roch (III.4.10) si ha

$$\dim \mathcal{L}(D + (O)) = 1.$$

Presa quindi $f \in \mathcal{L}(D + (O))$ una funzione non nulla, questa forma una base dello spazio $\mathcal{L}(D + (O))$. Si ha perciò che

$$\mathrm{div}(f) + D + (O) \geq 0 \implies \mathrm{div}(f) \geq -D - (O), \quad \deg \mathrm{div}(f) = 0,$$

da III.2.10. Segue che esiste un punto $P \in E$ tale che

$$\mathrm{div}(f) = -D - (O) + (P) = ((P) - (O)) - D,$$

cioè $D \sim (P) - (O)$.

Per provare l'unicità, siano $P, P' \in E$ due punti che rispettino tale proprietà. È immediato che

$$(P) \sim D + (O) \sim (P'),$$

perciò da IV.4.11 si ha che $P = P'$.

Dato un punto $P \in E$ vale $\sigma((P) - (O)) = P$, da cui la suriettività.

(2) Siano $D_1, D_2 \in \mathrm{Div}^0(E)$ e siano $P_1, P_2 \in E$ tali che $\sigma(D_i) = P_i$.

Se $P_1 = P_2$ segue che

$$D_1 \sim (P_1) - (O) = (P_2) - (O) \sim D_2.$$

Viceversa, se $D_1 \sim D_2$ si ha che

$$(P_1) - (O) \sim (P_2) - (O) \implies (P_1) \sim (P_2),$$

quindi da IV.4.11 segue che $P_1 = P_2$.

(3) Sia E data da un'equazione di Weierstrass e siano $P, Q \in E$. Si vuole quindi mostrare che

$$\kappa(P+Q) = \kappa(P) + \kappa(Q).$$

Sia $L = P \vee Q \subset \mathbb{P}^2$ e sia R il terzo punto di intersezione di L con E. Sia $L' = R \vee O \subset \mathbb{P}^2$. Le due rette L, L' sono date da equazioni del tipo

$$L\colon f(X,Y,Z) = \alpha X + \beta Y + \gamma Z = 0$$
$$L'\colon f(X,Y,Z)' = \alpha' X + \beta' Y + \gamma' Z = 0.$$

Inoltre la retta data da $Z = 0$ interseca E in O con molteplicità 3. Segue che

$$\operatorname{div}(f) = (P) + (Q) + (R), \qquad \operatorname{div}(f/Z) = (P) + (Q) + (R) - 3(O),$$
$$\operatorname{div}(f') = (R) + (O) + (P+Q), \quad \operatorname{div}(f'/Z) = (R) + (P+Q) - 2(O).$$

Da ciò si deduce

$$0 \sim \operatorname{div}(f'/f) = (P+Q) - (P) - (Q) - (O),$$

ovvero $0 = \kappa(P+Q) - \kappa(P) - \kappa(Q)$ come si voleva. □

Definizione IV.4.13. Siano E, E' curve ellittiche. Si chiama *isogenia da E a E'* un morfismo $\phi\colon E \to E'$ che mandi il punto base di E nel punto base di E' (cioè $\phi(O) = O'$).

Osservazione IV.4.14. Un cambio di coordinate lineare come visto in 1.2 induce un'isogenia tra le curve ellittiche date dalle due equazioni di Weierstrass coniugate (infatti è immediato che i punti all'infinito, punti base delle curve ellittiche, sono coniugati dal cambio di coordinate).

Definizione IV.4.15. Le isogenie da E a E' formano un gruppo denotato $\operatorname{Hom}(E, E')$ dove

$$(\phi + \psi)(P) = \phi(P) + \psi(P), \quad \forall \phi, \psi \in \operatorname{Hom}(E, E').$$

(Il fatto che $\phi + \psi$ è isogenia discende direttamente da [Sil09, § III.6].)

Proposizione IV.4.16. *Siano E, E' curve ellittiche su $\mathbb{K}$ e sia data un'isogenia $\phi\colon E \to E'$. Allora ϕ è omomorfismo di gruppi abeliani.*

Dimostrazione. Il morfismo ϕ induce un omomorfismo di gruppi abeliani

$$h_*\colon \operatorname{Pic}^0(E) \to \operatorname{Pic}^0(E'), \quad \sum n_P(P) \mapsto \sum n_P(h(P)).$$

Da IV.4.12 si ha che

$$\sigma\colon E \to \operatorname{Pic}^0(E), \quad \sigma'\colon E' \to \operatorname{Pic}^0(E'),$$

sono isomorfismi di gruppi abeliani. È sufficiente quindi mostrare che il seguente diagramma commuti

$$\begin{array}{ccc} \operatorname{Pic}^0(E) & \xrightarrow{\sigma} & E \\ \downarrow{\scriptstyle h_*} & & \downarrow{\scriptstyle h} \\ \operatorname{Pic}^0(E') & \xrightarrow{\sigma'} & E' \end{array}$$

Ciò è immediato per i divisori del tipo $(P) - (O)$, infatti

$$h \circ \sigma((P) - (O)) = h(P) = \sigma'((h(P)) - (O')) = \sigma' \circ h_*((P) - (O)).$$

Sempre da IV.4.12 si ha che ogni divisore $D \in \mathrm{Div}^0(E)$ è linearmente equivalente a uno della forma $(P)-(O)$ e ciò permette di concludere. $\square$

CAPITOLO V

La Famiglia di Legendre

Si consideri una curva ellittica E su $\mathbb{K}(t)$ data dall'equazione

$$f(x,y,t) = y^2 + a_1(t)xy + a_3(t)y - x^3 - a_2(t)x^2 - a_4(t)x - a_6(t) = 0,$$

dove $a_i(t) \in \mathbb{K}[t]$. Si possono ora sostituire a t valori in $T = \bar{\mathbb{K}}$; per ogni t fissato si ottiene una curva E_t su $\bar{\mathbb{K}}$, se $\Delta(E_t) \neq 0$ inoltre è una curva ellittica il cui punto base è il punto all'infinito. Ogni punto di E si può quindi pensare come una mappa $t \to P(t)$ che al parametro t associa un punto di E_t.

Definizione V.0.1. Data una curva ellittica E su $\mathbb{K}(t)$ e un sottoinsieme $U \subset T$ si chiama *famiglia di curve ellittiche su* U e si denota E_U l'insieme di punti $(t,P) \in U \times \mathbb{P}^2$ che soddisfano l'equazione di Weierstrass associata ad E unito all'insieme dei punti base:

$$E_U = \{(t,[x:y:1])\colon f(x,y,t) = 0\} \cup \{(t,[0:1:0])\}.$$

L'insieme U è detto *spazio dei parametri*.

Notazione V.0.2. Per ogni $t \in U$ fissato c'è una biezione tra i punti $(t,P) \in E_U$ e i punti sulla curva ellittica E_t di equazione

$$E_t\colon y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t).$$

Per rappresentare una famiglia di curve ellittiche d'ora in poi quindi si espliciterà soltanto l'equazione di una generica E_t.

Per indicare i punti di E_U quando t sarà chiara dal contesto si scriverà solamente P (o $P(t)$) sottintendendo il punto $(t,P(t)) \in E_U$.

Definizione V.0.3. Dato un punto $P(t) \in E/\mathbb{K}(t)$ è detta *sezione* la mappa

$$p\colon U \to E_U, \quad t \mapsto (t,P(t)).$$

Usando la notazione precedente quindi $p(t) = P(t) \in E_t$. Spesso ci si riferirà a una sezione come a un punto di $E/\mathbb{K}(t)$, avendo chiara l'identificazione tra i due.

Osservazione V.0.4. Sia $\phi\colon E/\mathbb{K}(t) \to E/\mathbb{K}(t)$ un morfismo della curva ellittica E in sé stessa. Allora ϕ può essere vista come una mappa di sezioni sulla famiglia E_U, anche essa indicata con ϕ, data da

$$(\phi p)(t) = \phi(p(t)).$$

1. Proprietà delle curve di Legendre

DEFINIZIONE V.1.1. Sia $\mathbb{K}$ un campo di caratteristica diversa da 2 e sia $\lambda \in \Lambda = \mathbb{K}\backslash\{0,1\}$. La *Famiglia di Legendre* E_Λ è la famiglia di curve ellittiche su Λ data da:

$$E_\lambda \colon y^2 = x(x-1)(x-\lambda).$$

OSSERVAZIONE V.1.2. Se $\lambda \in \{0,1\}$, le curve date dall'equazione $y^2 = x(x-1)(x-\lambda)$ sono singolari e perciò non sono curve ellittiche.

PROPOSIZIONE V.1.3. *Sia* $\mathrm{char}(\mathbb{K}) \neq 2$. *Ogni curva ellittica* E *su* $\mathbb{K}$ *è isomorfa su* $\bar{\mathbb{K}}$ *a una curva* E_λ *per qualche* $\lambda \in \bar{\mathbb{K}}\backslash\{0,1\}$. *L'equazione*

$$y^2 = x(x-1)(x-\lambda),$$

è chiamata forma di Legendre di E.

DIMOSTRAZIONE. Dato che $\mathrm{char}(\mathbb{K}) \neq 2$, la curva E ha forma di Weierstrass del tipo

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

come mostrato in (1.3). Dopo aver fatto un cambio di variabile $(x,y) \mapsto (x,2y)$ è possibile fattorizzare la cubica per ottenere

$$y^2 = (x-x_1)(x-x_2)(x-x_3),$$

con $x_i \in \bar{\mathbb{K}}$, $\forall i$. Inoltre $\Delta \neq 0$, da cui gli x_i sono a due a due distinti. Si cambia di nuovo variabile $(x,y) \mapsto ((x_2-x_1)x + x_1, (x_2-x_1)^{3/2}y)$ e l'equazione diventa

$$y^2 = x(x-1)(x-\lambda), \quad \lambda = \frac{x_3-x_1}{x_2-x_1} \in \bar{\mathbb{K}}.$$

Si noti come essendo $x_2 \neq x_3 \neq x_1$ si ha $\lambda \neq 0,1$. □

OSSERVAZIONE V.1.4. Esempi di sezioni su E_Λ sono

$$0(\lambda) = O, \quad e_1(\lambda) = (0,0), \quad e_2(\lambda) = (1,0), \quad e_3(\lambda) = (\lambda,0).$$

I punti associati a queste sezioni su $E/\mathbb{K}(\lambda)$ sono i punti O, $P_1 = (0,0)$, $P_2 = (1,0)$, $P_3 = (\lambda,0)$. Si vuole mostrare che questi sono tutti e soli i punti P di E tali che $[2]P = 0$ (tali punti sono detti *punti di 2-torsione di* E).

Il punto base O rispetta chiaramente $[2]O = O$. Dalla legge di gruppo IV.4.3 si ha che

$$[2]P = O \iff O \oplus (P \oplus P) = O \iff P \oplus P = O \oplus O = O,$$

cioè P è punto di 2-torsione se e solo se la tangente a E in P interseca la curva nel punto base. In altre parole sono i punti che hanno tangente a E verticale e quindi se $P = (x_0, y_0)$ si deve avere che $f_y(x_0,y_0) = 2y_0 = 0$. I punti della forma $(x_0,0)$ che soddisfano $f(x_0,0) = 0$ sono proprio i punti che corrispondono a $x_0 \in \{0,1,\lambda\}$.

Si ha quindi che O, P_1, P_2, P_3 sono i 4 punti di 2-torsione di E ed è immediato che formino un gruppo chiamato *sottogruppo di 2-torsione di* E e denotato con $E[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Fissato $\lambda \in \mathbb{K}\backslash\{0,1\}$, un discorso analogo si può applicare ai punti O, $(0,0)$, $(1,0)$, $(\lambda,0)$ di una curva di Legendre E_λ.

Osservazione V.1.5. Il discriminante Δ_λ di una curva di Legendre E_λ vale

$$\Delta_\lambda = 2^4\lambda^2(\lambda-1)^2.$$

Osservazione V.1.6. Il j-invariante di E_λ vale

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

Per semplicità di notazione d'ora in avanti si considererà j come sola funzione di λ usando la notazione $j(\lambda)$ per indicare $j(E_\lambda)$.

È naturale chiedersi sotto quali condizioni due forme di Legendre corrispondono alla stessa curva, ovvero due curve di Legendre sono isomorfe tra loro. Si considerino i seguenti due esempi.

Esempio V.1.7. Le curve $E_\lambda, E_{\lambda'}$, con $\lambda' = 1-\lambda$, sono isomorfe. Un possibile isomorfismo è dato da

$$\phi_1 \colon E_\lambda \to E_{\lambda'}, \quad (x,y) \mapsto (1-x, iy).$$

Andando a sostituire nell'equazione di Legendre di E_λ si ottiene infatti

$$\begin{aligned}(iy)^2 &= (1-x)(1-x-1)(1-x-\lambda),\\ y^2 &= x(x-1)(x-(1-\lambda)).\end{aligned}$$

Dato inoltre che $\phi_1(O) = O$ si ha che ϕ_1 è un'isogenia e in quanto tale i punti di $E_\lambda[2]$ sono mandati in punti di $E_{\lambda'}[2]$. Esplicitamente:

$$(0,0) \mapsto (1,0), \quad (1,0) \mapsto (0,0), \quad (\lambda,0) \mapsto (\lambda',0) = (1-\lambda,0).$$

Il morfismo ϕ_1 induce quindi una mappa Φ_1 sulla famiglia di Legendre E_Λ data da

$$\Phi_1 \colon E_\Lambda \to E_\Lambda, \quad \Phi_1 \restriction_{E_\lambda} = \phi_1 \colon E_\lambda \to E_{\lambda'},$$

cioè la restrizione di Φ_1 a ogni sua fibra corrisponde al morfismo di curve di Legendre ϕ_1.

Esempio V.1.8. Le curve $E_\lambda, E_{\lambda'}$, con $\lambda' = 1/\lambda$, sono isomorfe. Un possibile isomorfismo è dato da

$$\phi_2 \colon E_\lambda \to E_{\lambda'}, \quad (x,y) \mapsto (\lambda x, \lambda^{3/2} y).$$

Sostituendo nell'equazione di E_λ si ottiene

$$\begin{aligned}(\lambda^{3/2}y)^2 &= (\lambda x)(\lambda x - 1)(\lambda x - \lambda),\\ y^2 &= x(x-1)\left(x - \frac{1}{\lambda}\right).\end{aligned}$$

Come nell'esempio precedente ϕ_2 è isogenia e i punti di ordine 2 sono mappati nel seguente modo

$$(0,0) \mapsto (0,0), \quad (1,0) \mapsto (\lambda',0) = \left(\frac{1}{\lambda}, 0\right), \quad (\lambda,0) \mapsto (1,0).$$

Il morfismo ϕ_2 induce su E_Λ la mappa

$$\Phi_2 \colon E_\Lambda \to E_\Lambda, \quad \Phi_2 \restriction_{E_\lambda} = \phi_2 \colon E_\lambda \to E_{\lambda'}.$$

Le mappe ottenute dalla composizione delle Φ_1, Φ_2 viste negli esempi precedenti formano un gruppo G. Sia ora $\Psi \in G$, chiaramente $\Psi \restriction_{E_\lambda}$ è un isomorfismo e sia $E_{\lambda'} = \Psi(E_\lambda)$. In particolare $\Phi_1(E_\lambda) = E_{1-\lambda}$ e $\Phi_2(E_\lambda) = E_{1/\lambda}$. Componendo le mappe $\lambda \overset{1}{\mapsto} 1-\lambda$ e $\lambda \overset{2}{\mapsto} 1/\lambda$ si ottengono così i possibili valori di λ', che sono:

$$\lambda \overset{1}{\mapsto} 1-\lambda \overset{2}{\mapsto} \frac{1}{1-\lambda} \overset{1}{\mapsto} \frac{\lambda}{\lambda-1} \overset{2}{\mapsto} \frac{\lambda-1}{\lambda} \overset{1}{\mapsto} \frac{1}{\lambda} \overset{2}{\mapsto} \lambda$$

Si consideri ora la restrizione delle mappe in G ai punti di ordine 2. Sia quindi $\Psi \in G$ e sia la sua restrizione $\psi = \Psi \restriction_{E_\lambda} \colon E_\lambda \to E_{\lambda'}$. Dato che ψ è isomorfismo e isogenia, è anche isomorfismo di gruppi. Segue che la restrizione di ψ data da

$$\psi \restriction_{E_\lambda[2]} = \psi' \colon E_\lambda[2] \to E_{\lambda'}[2], \quad \psi'(P) = \psi(P),$$

è a sua volta un isomorfismo di gruppi. Come già notato il gruppo di 2-torsione di una curva è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, perciò ψ' induce un automorfismo di $\mathbb{Z}_2 \times \mathbb{Z}_2$, dove i punti di 2-torsione sono identificati tramite le sezioni:

$$0(\lambda) \leftrightarrow 0(\lambda'), \quad e_1(\lambda) \leftrightarrow e_1(\lambda'), \quad e_2(\lambda) \leftrightarrow e_2(\lambda'), \quad e_3(\lambda) \leftrightarrow e_3(\lambda').$$

In virtù di ciò d'ora in poi si ometteranno λ, λ' e si considererà $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{0, e_1, e_2, e_3\}$.

Lemma V.1.9. *Il gruppo degli automorfismi di $\mathbb{Z}_2 \times \mathbb{Z}_2$ è isomorfo a S_3.*

Dimostrazione. Si noti come $\mathbb{Z}_2 \times \mathbb{Z}_2$ è generato da uno qualunque degli insiemi $B_1 = \{e_2, e_3\}, B_2 = \{e_3, e_1\}, B_3 = \{e_1, e_2\}$. Un automorfismo di $\mathbb{Z}_2 \times \mathbb{Z}_2$ quindi è univocamente definito dalle immagini degli elementi di uno dei B_i, ad esempio B_1. I possibili modi di mappare B_1 in B_i sono 6, e perciò $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ ha cardinalità 6.

Si consideri ora la mappa

$$l \colon \{1,2,3\} \to \{e_1, e_2, e_3\}, \quad i \mapsto e_i,$$

e si costruisca la mappa $\gamma \colon S_3 \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ che rende commutativo il diagramma

$$\begin{array}{ccc} \{1,2,3\} & \xrightarrow{\ l\ } & \{e_1,e_2,e_3\} \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \gamma(\sigma)} \\ \{1,2,3\} & \xrightarrow{\ l\ } & \{e_1,e_2,e_3\} \end{array}$$

ovvero $\gamma(\sigma)(e_i) = l \circ \sigma \circ l^{-1}(e_i) = e_{\sigma(i)}$. Si noti come γ è ben definita, infatti l, σ sono entrambe biezioni. Si vuole ora mostrare che γ è isomorfismo di gruppi.

Si ha che γ è omomorfismo, infatti date $\sigma_1, \sigma_2 \in S_3$ si ha

$$\gamma(\sigma_1\sigma_2)(e_i) = e_{(\sigma_1\sigma_2)(i)} = \gamma(\sigma_1)(e_{\sigma_2(i)}) = \gamma(\sigma_1) \circ \gamma(\sigma_2)(e_i).$$

Inoltre γ è iniettiva, siano infatti $\sigma_1, \sigma_2 \in S_3$. Allora si ha

$$\gamma(\sigma_1)(e_i) = \gamma(\sigma_2)(e_i),\ \forall i \iff \sigma_1(i) = \sigma_2(i),\ \forall i,$$

dove si è usata la biettività di l per mostrare la doppia implicazione.

Dato che S_3 e $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ hanno la stessa cardinalità, si conclude che ψ è isomorfismo. □

Dal lemma si ha quindi che ogni automorfismo ψ' è identificato con una permutazione $\sigma \in S_3$. Ad esempio le mappe Φ_1, Φ_2 degli esempi precedenti inducono gli isomorfismi ϕ_1', ϕ_2' che, tramite la mappa γ vista nella dimostrazione del lemma, soddisfano

$$\phi_1' = \gamma(1\ 2), \quad \phi_2' = \gamma(2\ 3).$$

Ricapitolando, si è dato un omomorfismo $\Gamma\colon G \to S_3$ tramite

$$G \xrightarrow{\restriction_{E_\lambda[2]}} \mathrm{Aut}(E_\lambda[2]) \xrightarrow{\cong} \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \xrightarrow{\gamma} S_3.$$
$$\Gamma$$

Dato che Φ_1, Φ_2 sono generatori di G e vengono mappati in generatori di S_3:

$$\Gamma(\Phi_1) = (1\ 2), \quad \Gamma(\Phi_2) = (2\ 3),$$

si ha che la mappa Γ è suriettiva. In altre parole, dato comunque un isomorfismo $\psi'\colon E_\lambda[2] \to E_{\lambda'}[2]$ esiste una $\Psi \in G$ che coincide con ψ' su $E_\lambda[2]$.

Si può quindi far agire G su $\mathbb{P}^1\backslash\{0, 1, \infty\}$ nel seguente modo:

Sia $\Psi \in G$ e sia $\Psi(E_\lambda) = E_{\lambda'}$. Allora Ψ agisce su $\lambda \in \mathbb{P}^1\backslash\{0, 1, \infty\}$ mandando $\lambda \mapsto \lambda'$.

Come si è visto l'orbita di λ sotto l'azione di G è perciò

$$G \cdot \lambda = \left\{\lambda,\ 1-\lambda,\ \frac{1}{\lambda},\ \frac{1}{1-\lambda},\ \frac{\lambda-1}{\lambda},\ \frac{\lambda}{\lambda-1}\right\}.$$

Proposizione V.1.10. *Siano $\lambda, \lambda' \in \mathbb{P}^1\backslash\{0, 1, \infty\}$. Allora le seguenti condizioni sono equivalenti:*

(1) *Le curve di Legendre $E_\lambda, E_{\lambda'}$ sono isomorfe su $\mathbb{K}$.*
(2) *$j(\lambda) = j(\lambda')$.*
(3) *λ e λ' appartengono alla stessa orbita sotto l'azione di G.*

Dimostrazione.

- (1) ⇒ (3) Sia $\phi\colon E_\lambda \to E_{\lambda'}$ un isomorfismo. Come si è visto ϕ induce un isomorfismo di gruppi $\phi'\colon E_\lambda[2] \to E_{\lambda'}[2]$. Si ha quindi che esiste un morfismo $\Phi \in G$ che coincide con ϕ' su $E_\lambda[2]$. Segue perciò che $\sigma \in G$ indotta da Φ manda $\sigma(\lambda) = \lambda'$.
- (3) ⇒ (2) Dato che ogni elemento di $G \cdot \lambda$ si può ottenere, a partire da λ, dalla composizione di $\lambda \overset{1}{\mapsto} 1 - \lambda$ e $\lambda \overset{2}{\mapsto} 1/\lambda$ basta

mostrare che j è invariante sotto queste due trasformazioni:

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

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

- (2) $\Rightarrow$ (1) Questa non è altri che la proposizione IV.2.3 nel caso particolare delle curve di Legendre.

□

Proposizione V.1.11. *Sia* $\mathrm{char}(\mathbb{K}) \neq 2$. *La mappa*

$$\mathbb{P}^1 \to \mathbb{P}^1, \quad \lambda \mapsto j(\lambda),$$

è suriettiva e le sue fibre hanno cardinalità 6*, meno che nei seguenti casi:*

(1) $j = 0$*, la cui fibra è* $j^{-1}(\{0\}) = \{-\xi, -\xi^2\}$ *dove* ξ *è una radice* 3*-primitiva dell'unità,*
(2) $j = 1728$*, la cui fibra è* $j^{-1}(\{1728\}) = \{-1, 1/2, 2\}$ *(a meno che* $\mathrm{char}(\mathbb{K}) = 3$*, da cui* $1728 = 0$ *e si riconduce al caso precedente),*
(3) $j = \infty$*, la cui fibra è* $j^{-1}(\{\infty\}) = \{0, 1, \infty\}$.

Dimostrazione. Il j-invariante identifica le curve ellittiche a meno di isomorfismi su $\bar{\mathbb{K}}$ come mostrato in (IV.2.3). Inoltre si è visto in IV.2.4 che per ogni $j_0 \in \bar{\mathbb{K}}$ esiste una curva E_{j_0} tale che $j(E_{j_0}) = j_0$. In virtù di V.1.3 esiste perciò un $\lambda \in \bar{\mathbb{K}}\backslash\{0,1\}$ tale che la curva di Legendre E_λ abbia j-invariante uguale a j_0. Per concludere la suriettività basta quindi notare che $j(0) = \infty$.

Siano quindi $\lambda, \lambda' \in \mathbb{P}^1$ tali che $j(\lambda) = j(\lambda')$, da cui $E_\lambda \cong E_{\lambda'}$. Le loro equazioni di Weierstrass sono coniugate da un cambio di variabile del tipo

$$(x, y) \mapsto (u^2x + r, u^3y).$$

Uguagliandole si ottiene

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

Imponendo l'uguaglianza tra i termini lineari delle due equazioni nei 6 modi possibili si ottiene, esplicitando i valori di λ' in funzione di λ,

$$\lambda' \in \left\{\lambda,\ 1-\lambda,\ \frac{1}{\lambda},\ \frac{1}{1-\lambda},\ \frac{\lambda-1}{\lambda},\ \frac{\lambda}{\lambda-1}\right\}.$$

A ognuno di questi valori di λ' corrisponde una curva $E_{\lambda'}$ isomorfa alle altre, e perciò $j(\lambda')$ assume lo stesso valore. Le fibre di j hanno cardinalità 6, a meno che due o più valori di λ' non coincidano. Uguagliandoli a coppie si ottengono tre casi possibili:

(1) $\lambda^2 - \lambda + 1 = 0$, corrispondente a $j = 0$, la cui fibra è composta dalle due radici seste dell'unità che risolvono l'equazione,
(2) $\lambda \in \{-1, 1/2, 2\}$, corrispondente a $j = 1728$,
(3) $\lambda \in \{0, 1, \infty\}$, corrispondente a $j = \infty$.

Se $\text{char}(\mathbb{K}) = 3$ si ha $1728 = 0$ e in tal caso la fibra di 1728 coincide con quella del caso 1. $\square$

APPENDICE A

Casi particolari in caratteristica 2, 3

PROPOSIZIONE I.0.1. *Sia $E/\mathbb{K}$ una curva ellittica definita da una equazione di Weierstrass. Allora per ognuno dei seguenti casi esiste un cambio di coordinate*

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t, \quad \textit{dove } u \in \mathbb{K}^* \textit{ e } r, s, t \in \mathbb{K},$$

che trasformi l'equazione in forma di Weierstrass nella rispettiva forma indicata.

(1) $\underline{\text{char}(\mathbb{K}) \neq 2, 3}$

$$y^2 = x^3 + a_4x + a_6, \quad \Delta = -16(4a_4^3 + 27a_6^2), \quad j = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}.$$

(2) $\underline{\text{char}(\mathbb{K}) = 3 \textit{ e } j(E) \neq 0}$

$$y^2 = x^3 + a_2x^2 + a_6, \quad \Delta = -a_2^3a_6, \quad j = -\frac{a_2^3}{a_6}.$$

(3) $\underline{\text{char}(\mathbb{K}) = 3 \textit{ e } j(E) = 0}$

$$y^2 = x^3 + a_4x + a_6, \quad \Delta = -a_4^3, \quad j = 0.$$

(4) $\underline{\text{char}(\mathbb{K}) = 2 \textit{ e } j(E) \neq 0}$

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad \Delta = a_6, \quad j = \frac{1}{a_6}.$$

(5) $\underline{\text{char}(\mathbb{K}) = 2 \textit{ e } j(E) = 0}$

$$y^2 + a_3y = x^3 + a_4x + a_6, \quad \Delta = a_4^3, \quad j = 0.$$

DIMOSTRAZIONE. (1) Visto nella sezione sulle curve ellittiche.

(2) Data l'equazione di Weierstrass è possibile ottenere, completando il quadrato, un'equazione del tipo

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

con invarianti

$$\Delta = a_2^2a_4^2 - a_2^3a_6 - a_4^3, \quad j = a_2^2/\Delta.$$

Dato che $j \neq 0$ si ha $a_2 \neq 0$ e la sostituzione $x \mapsto x + a_4/a_2$ da la forma cercata.

(3) Come nel caso precedente si ottiene

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

con invarianti

$$\Delta = a_2^2a_4^2 - a_2^3a_6 - a_4^3, \quad j = a_2^2/\Delta.$$

Da $j = 0$ si deduce $a_2 = 0$ e quindi la forma cercata.

(4) Dall'equazione in forma di Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

si ottiene $j = a_1^{12}/\Delta$. La sostituzione

$$(x, y) \mapsto \left(a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right)$$

fornisce un'equazione nella forma cercata.

(5) Come nel caso precedente si ha $j = a_1^{12}/\Delta$, da cui se $j = 0$ segue che $a_1 = 0$. La sostituzione

$$(x, y) \mapsto (x + a_2, y)$$

fornisce un'equazione nella forma cercata. □

PROPOSIZIONE I.0.2. (1) *Una curva definita da un'equazione di Weierstrass è singolare se e solo se il suo discriminante è nullo.*

(2) *Due curve ellittiche $E/\mathbb{K}, E'/\mathbb{K}$ sono isomorfe su $\bar{\mathbb{K}}$ se e solo se hanno la stessa j-invariante.*

DIMOSTRAZIONE. (1) L'unica parte rimanente da provare da IV.1.9 è il caso in cui $\mathrm{char}\mathbb{K} = 2$ e $\Delta = 0$ implicano che la curva sia singolare. Questo è immediato dalle forme delle equazioni nei casi in cui $\mathrm{char}\mathbb{K} = 2$ di I.0.1.

(2) Da IV.2.3 rimangono da provare i casi in cui $\mathrm{char}\mathbb{K} = 2, 3$. Per semplificare i calcoli si useranno le forme viste nella proposizione precedente.

(a) $\underline{\mathrm{char}(\mathbb{K}) = 3 \text{ e } j(E) \neq 0}$. In questo caso le curve E, E' sono date da equazioni di Weierstrass della forma

$$y^2 = x^3 + a_2x^2 + a_6.$$

Gli isomorfismi che preservano questa forma dell'equazione sono del tipo $(x, y) = (u^2x', u^3y')$. Da $j(E) = j(E')$ si ottiene $a_2^3a_6' = a_2'^3a_6 \neq 0$ e preso $u^2 = a_2/a_2'$ si ottiene l'isomorfismo cercato.

(b) $\underline{\mathrm{char}(\mathbb{K}) = 3 \text{ e } j(E) = 0}$. In questo caso le curve E, E' sono date da equazioni di Weierstrass della forma

$$y^2 = x^3 + a_4x + a_6.$$

Gli isomorfismi che preservano questa forma dell'equazione sono del tipo $(x, y) = (u^2x' + r, u^3y')$. Dato che $\Delta \neq 0$ si ha $a_4, a_4' \neq 0$. Si possono quindi scegliere u e r tali che valgano

$$u^4 = a_4'/a_4, \quad r^3 + a_4r + (1 - u^2)a_6 = 0,$$

e si ottiene l'isomorfismo cercato.

(c) $\underline{\mathrm{char}(\mathbb{K}) = 2 \text{ e } j(E) \neq 0}$. In questo caso le curve E, E' sono date da equazioni di Weierstrass della forma

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

Gli isomorfismi che preservano questa forma dell'equazione sono del tipo $(x, y) = (x', y' + sx')$. Da $j(E) = j(E')$ si ottiene $a_6 = a_6' \neq 0$ e preso s tale che

$$s^2 + s + a_2 + a_2' = 0,$$

si ottiene l'isomorfismo cercato.

(d) $\underline{\text{char}(\mathbb{K}) = 2 \text{ e } j(E) = 0}$. In questo caso le curve E, E' sono date da equazioni di Weierstrass della forma

$$y^2 + a_3 y = x^3 + a_4 x + a_6.$$

Gli isomorfismi che preservano questa forma dell'equazione sono del tipo $(x, y) = (u^2x' + s^2, u^3y' + su^2x' + t)$. Dall'ipotesi $a_3, a_3' \neq 0$ (altrimenti la dimostrazione è analoga al caso in cui $\text{char}(\mathbb{K}) \neq 2, 3$). Si possono scegliere u, s, t tali che valgano

$$\begin{aligned} u^3 - a_3/a_3' &= 0, \\ s^4 + a_3 s + a_4 - u^4 a_4' &= 0, \\ t^2 + a_3 t + s^6 + a_4 s^2 + a_6 - u^6 a_6' &= 0, \end{aligned}$$

e si ottiene l'isomorfismo cercato. □

Se $\text{char}(\mathbb{K}) = 2$ in generale non si può portare un'equazione di Weierstrass nella forma di Legendre, tuttavia esiste una forma simile valida in caratteristica 2.

Proposizione I.0.3 (Forma di Deuring). *Sia* $\text{char}(\mathbb{K}) \neq 3$ *e sia* $E/\mathbb{K}$ *una curva ellittica. Allora* E *ha equazione di Weierstrass della forma*

$$E_\alpha \colon y^2 + axy + y = x^3, \quad \alpha \in \bar{\mathbb{K}}, \alpha^3 \neq 27,$$

a cui sono associati gli invarianti

$$\Delta = \alpha^3 - 27, \quad j = \frac{\alpha^3(\alpha - 24)^3}{\alpha^3 - 27}.$$

Dimostrazione. I valori di Δ, j sono immediati dall'equazione in forma di Deuring. Sia $\alpha \in \bar{\mathbb{K}}$ tale che

$$\alpha^3(\alpha - 24)^3 - (\alpha^3 - 27)j(E) = 0.$$

Si noti come dato che $\text{char}(\mathbb{K}) \neq 3$ si ha $\alpha^3 \neq 27$ e perciò E_α è una curva ellittica tale che $j(E_\alpha) = j(E)$. In virtù di I.0.2 segue che E, E_α sono isomorfe su $\bar{\mathbb{K}}$. □

Bibliografia

[AM69] Michael F. Atiyah and Ian G. MacDonald. *Introduction to commutative algebra*. en. Reading, Mass.–London–Don Mills, Ont.: Addison-Wesley Publishing Co., 1969.

[Har77] Robin Hartshorne. *Algebraic Geometry*. en. Graduate Texts in Mathematics. New York, NY: Springer, 1977.

[Ser79] Jean-Pierre Serre. *Local Fields*. en, fr. Graduate Texts in Mathematics. New York, NY: Springer, 1979.

[Sha77] Igor R. Shafarevich. *Basic Algebraic Geometry*. en, ru. Berlin: Springer, 1977.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. en. 2nd ed. Graduate texts in mathematics. New York, NY: Springer, 2009.