Alma Mater Studiorum · Università di Bologna

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

ESEMPI DI CALCOLO DELLA FUNZIONE ZETA DI HASSE-WEIL

Tesi di Laurea in Geometria

Relatore:
Chiar.mo Prof.
LUCA MIGLIORINI

Presentata da:
LEONARDO MALTONI

♯ Sessione di Luglio
Anno Accademico 2015-2016

Introduzione

La funzione zeta di Hasse-Weil è un oggetto estremamente importante della geometria algebrica. Attraverso di essa sono formulate infatti le congetture di Weil, le quali costituiscono un capitolo fondamentale nello sviluppo di questa disciplina. La loro formulazione moderna, attraverso la funzione zeta, fu fatta da André Weil nel 1949 ed esse furono dimostrate da Dwork (1960), Grothendieck (1965) e Deligne (1974).
Questi risultati vanno ben oltre gli scopi di questa tesi. Ci limiteremo a dare la definizione formale e alcune proprietà elementari della funzione zeta, e a calcolarla in alcuni esempi. In particolare esauriremo il caso delle coniche affini.

Indice

Capitolo 1

Nozioni preliminari sulle varietà

1.1 Varietà algebriche

Uno schema[1] $(X, \mathscr{O}_X)$ si dice *ridotto* quando $\mathscr{O}(U)$ è un anello ridotto, per ogni aperto $U \subset X$.
Sia k un campo: uno schema su k (o un k-schema) è un morfismo di schemi

$$\begin{array}{c} X \\ \downarrow \\ \text{Spec } k \end{array}$$

Ovvero, equivalentemente, uno schema $(X, \mathscr{O}_X)$, tale che $\mathscr{O}(U)$ sia una k-algebra, per ogni aperto $U \subset X$. X si dice inoltre *localmente di tipo finito* se ammette un ricoprimento di sottoschemi aperti affini del tipo Spec B_i, dove B_i è una k-algebra finitamente generata e, infine, si dice *di tipo finito* se è localmente di tipo finito ed è quasi compatto (dunque ammette un ricoprimento *finito* di sottoschemi aperti affini come sopra).

Definizione 1.1.1 (Varietà algebrica)**.** Sia k un campo. Diremo varietà algebrica uno schema ridotto e di tipo finito su k. Indicheremo una varietà su

[1] Per le nozioni di base sugli schemi, vedere [**Vak**] o [**Mum**].

k con X/k (nel caso non siano possibili ambiguità, scriveremo semplicemente X).

Osservazione 1.1.2. Spec A è una varietà algebrica in questo senso se e solo se A è una k-algebra ridotta e finitamente generata (ovvero $A \cong k[x_1, \ldots, x_N]/I$ con I un ideale radicale).

Esempio 1.1.3 (Spazio affine)**.** Diciamo *spazio affine N-dimensionale su* k la varietà $\mathbb{A}_k^N = \text{Spec}(k[x_1, \ldots, x_N])$. Tra i suoi punti, in particolare ci sono quelli del tipo $[(x_1 - a_1, \ldots, x_N - a_N)]$, che possiamo pensare come i punti *tradizionali* dello spazio affine N-dimensionale su k.

Esempio 1.1.4 (Luogo degli zeri di polinomi)**.** La varietà

$$\text{Spec}(k[x_1, \ldots, x_N]/(p_1, \ldots, p_r))$$

che corrisponde al chiuso $V(I)$ di $\mathbb{A}_k^N$, dove $I = (p_1, \ldots, p_r)$ è un ideale radicale, si può pensare come il luogo degli zeri dei polinomi $p_1, \ldots, p_r \in k[x_1, \ldots, x_N]$: esso contiene in particolare i punti $[(x_1 - a_1, \ldots, x_N - a_N)/I]$ dove $(x_1 - a_1, \ldots, x_N - a_N) \supset I$, o, equivalentemente, $p_1(a_1, \ldots, a_N) = \cdots = p_r(a_1, \ldots, a_N) = 0$. Poiché, per il teorema della base di Hilbert, $k[x_1, \ldots, x_N]$ è Nötheriano, ogni ideale $I \subset k[x_1, \ldots, x_N]$ è di questo tipo.

Osservazione 1.1.5. Sia X una varietà su k e sia k' un sottocampo di k tale che k ne risulti un'estensione finitamente generata, allora X si può considerare, in modo naturale, una varietà su k'. Infatti, come mostra il seguente diagramma,

$$\begin{array}{c} X \\ \big\downarrow \\ \text{Spec } k \\ \big\downarrow \\ \text{Spec } k' \end{array}$$

preso U un aperto di X, $\mathscr{O}_X(U)$ è una k-algebra e dunque una k'-algebra. Inoltre, nella scrittura

$$X = \bigcup_{i=1}^{n} \text{Spec } B_i$$

ogni B_i è una k'-algebra finitamente generata, in quanto è, per definizione, una k-algebra finitamente generata, e k è finitamente generato su k'.

Si può procedere in direzione opposta dell'osservazione 1.1.5? Ovvero: si può costruire una varietà su un'estensione di k a partire da una varietà su k? Supponiamo k perfetto e k' una sua estensione, e consideriamo

$$X' = X \times_{\text{Spec } k} \text{Spec } k'$$

Questo risulta prima di tutto uno schema su k', in quanto per definizione di prodotto fibrato si ha il diagramma seguente

$$\begin{array}{ccc} X' & \longrightarrow & X \\ \downarrow & & \downarrow \\ \text{Spec } k' & \longrightarrow & \text{Spec } k \end{array}$$

Mostriamo inoltre che esso è una varietà su k'. Trattiamo dapprima il caso affine: sia $X = \text{Spec } A$, con A una k-algebra ridotta e finitamente generata, allora

$$X' = \text{ Spec } A \times_{\text{Spec } k} \text{ Spec } k' = \text{ Spec}(A \otimes_k k')$$

e dunque si conclude osservando che $A \otimes_k k'$ è una k'-algebra finitamente generata e che è ridotta in quanto k è perfetto.
Nel caso generale, se $X = \bigcup_{i=1}^{n} \text{Spec } A_i$, allora

$$X' = \bigcup_{i=1}^{n} (\text{Spec } A_i \times_{\text{Spec } k} \text{Spec } k')$$

Esempio 1.1.6. Si ha $\mathbb{A}^N_k \times_{\text{Spec } k} \text{Spec } k' \cong \mathbb{A}^N_{k'}$. Questo deriva direttamente dal fatto che $k[x_1, \ldots, x_N] \otimes_k k' \cong k'[x_1, \ldots, x_N]$. Allo stesso modo si ha $\text{Spec}(k[x_1, \ldots, x_N]/I) \times_{\text{Spec } k} \text{ Spec } k' \cong \text{Spec}(k'[x_1, \ldots, x_N]/I)$.

Esempio 1.1.7. Poiché non abbiamo fatto ipotesi sull'estensione, data una varietà X su un campo perfetto k, possiamo sempre considerare $\overline{X} \stackrel{def}{=} X \times_{\text{Spec } k} \text{Spec } \overline{k}$, dove $\overline{k}$ è una chiusura algebrica di k.

1.2 Punti di una varietà

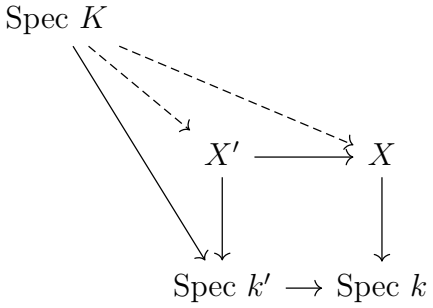
Sia $(X, \mathscr{O}_X)$ una varietà su un campo k. La spiga $\mathscr{O}_{X,p}$ di ogni punto $p \in X$, è un anello locale, ovvero ha un unico ideale massimale $\mathfrak{m}_p$: chiamiamo $\kappa(p)$ il campo dei residui $\mathscr{O}_{X,p}/\mathfrak{m}_p$. Indichiamo poi con X_{cl} l'insieme dei punti chiusi di X: questi saranno gli unici che considereremo. Se $p \in X_{\text{cl}}$, $\kappa(p)$ è un'estensione finita di k, infatti se p sta nel sottoschema affine Spec A e corrisponde all'ideale massimale $\mathfrak{m}$ allora $\mathscr{O}_{X,p} = A_{\mathfrak{m}}$ e il suo (unico) ideale massimale è ${}^e\mathfrak{m}$ (ovvero l'estensione di $\mathfrak{m}$ nella localizzazione). Dunque $\kappa(p) = A_{\mathfrak{m}}/{}^e\mathfrak{m} = A/\mathfrak{m}$ che per il Teorema degli zeri di Hilbert, è un'estensione finita di k. Allora poniamo $\deg(p) = [\kappa(p) : k]$.
Vi è inoltre una seconda nozione di punti che è la seguente:

Definizione 1.2.1 (K-punti di una varietà)**.** Sia X una varietà su k, e sia K un'estensione di k. Un K-punto (o un punto K-razionale) è un morfismo di schemi su k:

$$\text{Spec } K \longrightarrow X$$

Dove Spec K è inteso come k-schema per mezzo dell'inclusione $k \hookrightarrow K$. Quando in particolare $K = k$ si parla semplicemente di punto razionale.
L'insieme dei K-punti di X si indica con $X(K)$.

Osservazione 1.2.2. Se k' è un sottocampo di k e K un'estensione di k, un K-punto di X/k risulta immediatamente un K-punto di X/k'.
Sia invece $X' = X \times_{\text{Spec } k} \text{Spec } k'$, con k' un'estensione di k (che supponiamo perfetto). Se K è un'estensione di k', allora abbiamo un'identificazione $X'(K) = X(K)$. Infatti nel diagramma seguente



ciascuno dei due morfismi tratteggiati determina univocamente l'altro.
Dunque, per esempio, l'immagine di un K-punto di X è lo stesso che l'immagine (nel morfismo $X' \longrightarrow X$) di un K-punto di X'.

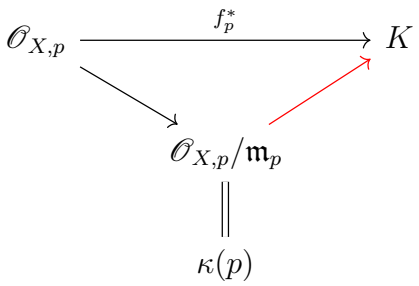
Proposizione 1.2.3. *Si ha una biiezione:*

$$X(K) \leftrightarrows \{(p, \phi) \,|\, p \in X,\ \phi : \kappa(p) \to K \ \textit{morfismo di } k\textit{-algebre}\}$$

Dimostrazione. Sia $f : \operatorname{Spec} K \longrightarrow X$ un K-punto. Per ogni aperto $U \subset X$, f dà un morfismo di k-algebre $f(U) : \mathscr{O}_X(U) \longrightarrow K$: al livello delle spighe si ottiene $f_p^* : \mathscr{O}_{X,p} \longrightarrow K$

$$\begin{array}{ccc} \mathscr{O}_X(U) & \xrightarrow{f(U)} & K \\ \downarrow & & \| \\ \mathscr{O}_{X,p} & \xrightarrow{f_p^*} & K \end{array}$$

Per definizione di morfismo di schemi, questo deve essere un morfismo di anelli locali, dunque l'ideale massimale di $\mathscr{O}_{X,p}$ è contenuto nel nucleo e, pertanto, questo morfismo fattorizza e induce il morfismo $\kappa(p) \longrightarrow K$.



Associamo allora ad f il punto $p = f([(0)])$ e il morfismo di k-algebre così ottenuto.
Viceversa, dati $p \in X$ e $\kappa(p) \longrightarrow K$, possiamo ricostruire facilmente il morfismo di schemi, ricomponendo ciascuna delle precedenti fattorizzazioni. □

Osservazione 1.2.4. Un morfismo di k-algebre $\sigma : K \longrightarrow K'$ induce una mappa $\varphi_\sigma : X(K) \longrightarrow X(K')$, così come un morfismo di schemi $f : X \longrightarrow Y$

induce una mappa $\psi_f : X(K) \longrightarrow Y(K)$:

$$\begin{array}{ccc} \operatorname{Spec} K' & \longrightarrow & \operatorname{Spec} K \\ & \searrow \quad \swarrow & \\ & X & \end{array} \qquad \begin{array}{ccc} & \operatorname{Spec} K & \\ & \swarrow \quad \searrow & \\ X & \longrightarrow & Y \end{array}$$

Le due mappe φ_σ e ψ_f si possono leggere attraverso la biiezione della proposizione 1.2.3. Abbiamo cioè:

$$\begin{array}{ccc} P & \overset{\varphi_\sigma}{\longmapsto} & P' \\ \downarrow\uparrow & & \downarrow\uparrow \\ (p,\phi) & \longmapsto & (p, \sigma \circ \phi) \end{array} \qquad \begin{array}{ccc} P & \overset{\psi_f}{\longmapsto} & Q \\ \downarrow\uparrow & & \downarrow\uparrow \\ (p,\phi) & \longmapsto & (f(p), \phi \circ f_p^*) \end{array}$$

Dove f_p^* è il morfismo indotto da f sui campi di residui. In particolare:

(a) Se $K \hookrightarrow K'$ è un'estensione di campi, si ha un'inclusione $X(K) \hookrightarrow X(K')$.

(b) Se $K \to K$ è un k-automorfismo, si ha una biiezione $X(K) \to X(K)$: dunque abbiamo un'azione del gruppo $\operatorname{Aut}(K/k)$ su $X(K)$.

(c) Se $X \to X$ è l'identità al livello degli spazi topologici, questo dà ancora una biiezione $X(K) \to X(K)$ (infatti f_p^* risulta un k-automorfismo).

Osservazione 1.2.5. Se K è un'estensione algebrica allora l'immagine p dell'unico punto di Spec K è un punto chiuso, infatti dalla dimostrazione di 1.2.3 risulta $\kappa(p) \hookrightarrow K$ e quindi $\dim\overline{\{p\}} = \operatorname{tr.deg}(\kappa(p)/k) \leq \operatorname{tr.deg}(K/k) = 0$. Dunque la biiezione di 1.2.3 si trasforma in:

$$X(K) \leftrightarrows \bigsqcup_{p \in X_{\mathrm{cl}}} \{\psi \mid \psi : \kappa(p) \to K, \text{ morfismo di } k\text{-algebre}\} \tag{1.1}$$

Cerchiamo ora di esplicitare la relazione tra i K-punti di una varietà e i suoi punti chiusi.

Osservazione 1.2.6. Supponiamo $X = \operatorname{Spec}(k[x_1, \ldots, x_N]/I)$. I K-punti di X ammettono un'interessante interpretazione geometrica. Infatti, un K-punto è determinato da un morfismo

$$k[x_1, \ldots, x_N]/I \longrightarrow K$$

il quale non è altro che un'assegnazione di valori in K alle variabili $x_1, \ldots, x_N$, tale che $\forall p \in I, \quad p(x_1, \ldots, x_N) = 0$. Equivalentemente, se $I = (p_1, \ldots, p_r)$, un K-punto è dato da una soluzione in K^N delle equazioni

$$\begin{cases} p_1(x_1, \ldots, x_N) = 0 \\ \qquad \vdots \\ p_r(x_1, \ldots, x_N) = 0 \end{cases}$$

In particolare, i punti razionali saranno le soluzioni in k^N di queste equazioni. D'altra parte anche un punto di X del tipo

$$[(x_1 - a_1, \ldots, x_N - a_N)/I]$$

si può pensare come il punto di coordinate $(a_1, \ldots, a_N)$ (vedere l'esempio 1.1.4). In effetti esso non è altro che l'immagine del corrispondente punto razionale:

$$\text{Spec } k \longrightarrow X$$

dato da

$$\begin{array}{rcl} k[x_1, \ldots, x_N]/I & \longrightarrow & k \\ x_1 & \longmapsto & a_1 \\ & \vdots & \\ x_N & \longmapsto & a_N \end{array}$$

Se k è un campo algebricamente chiuso, per il Teorema (debole) degli zeri di Hilbert, i suoi ideali massimali sono tutti e soli quelli del tipo

$$(x_1 - a_1, \ldots, x_N - a_N)$$

dunque i punti chiusi sono soltanto quelli del tipo illustrato nell'osservazione 1.2.6.
Tuttavia, se k non è algebricamente chiuso, ve ne sono altri.

Esempio 1.2.7. Prendiamo il piano affine razionale $\mathbb{A}^2_{\mathbb{Q}}$.
$(xy-2, x-y)$ è un ideale massimale di $\mathbb{Q}[x,y]$, infatti

$$\mathbb{Q}[x,y]/(xy-2, x-y) \cong \mathbb{Q}[\sqrt{2}] \tag{1.2}$$

Dunque $p = [(xy-2, x-y)]$ è un punto chiuso: come possiamo interpretarlo? Proprio la 1.2 fornisce una risposta. Consideriamo l'estensione trovata: in $\mathbb{Q}[\sqrt{2}][X,Y]$ l'ideale $(XY-2, X-Y)$ non è massimale, infatti esso è contenuto sia in $(X-\sqrt{2}, Y-\sqrt{2})$ sia in $(X+\sqrt{2}, Y+\sqrt{2})$.
Ma abbiamo un morfismo naturale di inclusione

$$\mathbb{Q}[x,y] \longrightarrow \mathbb{Q}[\sqrt{2}][X,Y]$$

che induce sugli schemi corrispondenti il morfismo

$$\mathbb{A}^2_{\mathbb{Q}[\sqrt{2}]} \longrightarrow \mathbb{A}^2_{\mathbb{Q}}$$

Per quanto detto, in questo morfismo i due punti trovati in $\mathbb{A}^2_{\mathbb{Q}[\sqrt{2}]}$ hanno la stessa immagine: il punto p.
Quindi il punto p rivela di fatto la carenza algebrica del campo $\mathbb{Q}$ che non *vede* le due soluzioni delle equazioni $xy = 2$, $x = y$ e dunque non le distingue. In altre parole p non è (l'immagine di) un punto razionale, ma è immagine di due $\mathbb{Q}[\sqrt{2}]$-punti, o, equivalentemente, è immagine di due punti razionali di $\mathbb{A}^2_{\mathbb{Q}[\sqrt{2}]}$.

Questo ragionamento si può generalizzare. Sia p un punto chiuso di una varietà X, $\kappa(p)$ è un'estensione (finita) di k: sia $K = \kappa(p)$. Nella corrispondenza della proposizione 1.2.3 il punto p è associato ad alcuni K-punti, uno per ogni k-automorfismo di K. L'insieme di questi punti è dunque un'orbita del gruppo $\mathrm{Aut}(K/k)$ nell'azione descritta in 1.2.4. In particolare il loro numero divide $\#\mathrm{Aut}(K/k)$ (se K/k è di Galois, allora quest'ultimo è uguale a $[K:k]$).
Per l'osservazione 1.2.2, possiamo considerare i K-punti in $X' = X \times_{\mathrm{Spec}\ k} \mathrm{Spec}\ K$ e qui l'azione del gruppo $\mathrm{Aut}(K/k)$ diventa *osservabile* sui punti veri e propri dello schema.

Notiamo infine che se $\overline{k}$ è una chiusura algebrica di k, ogni punto chiuso risulta un $\overline{k}$-punto.

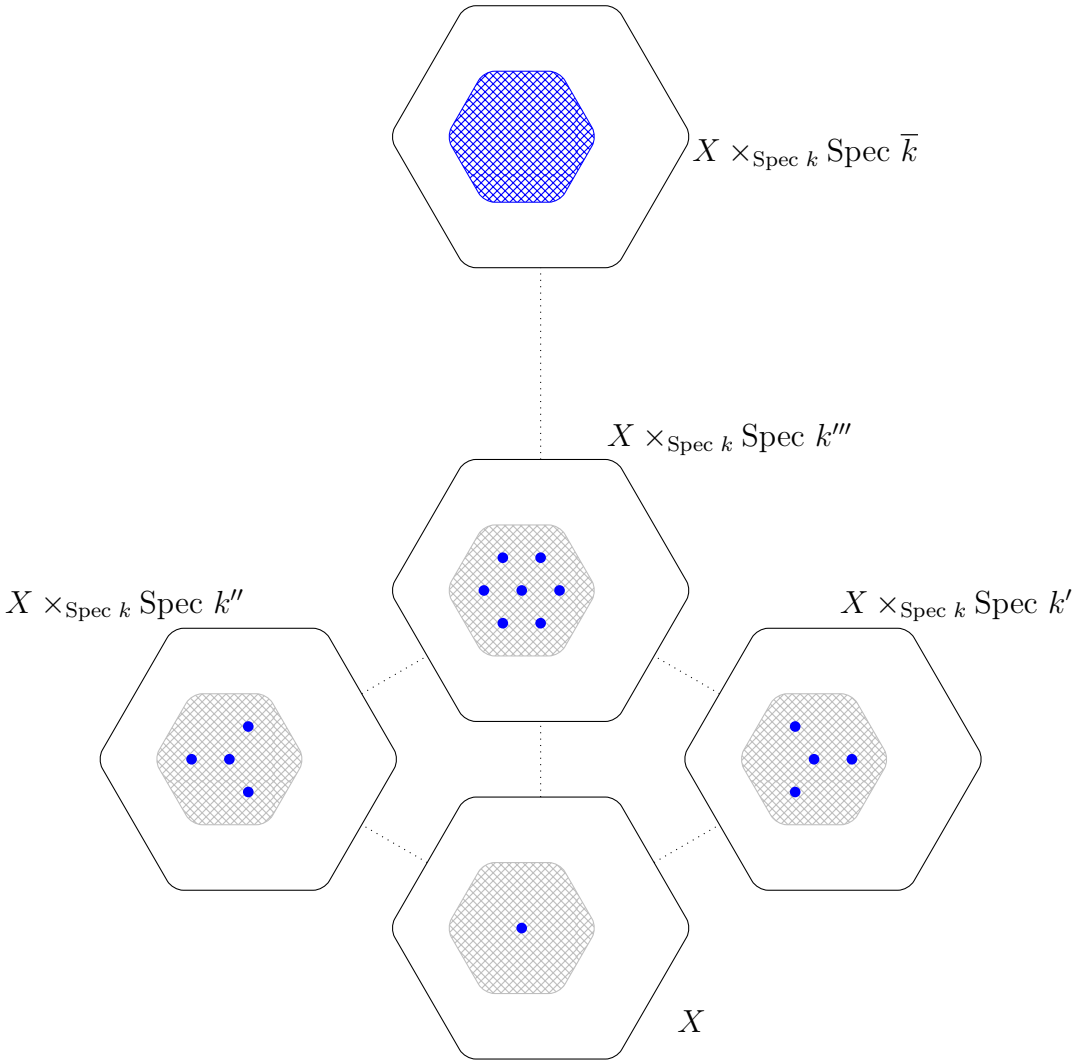


Figura 1.1: Man mano che si amplia algebricamente il campo base, si distinguono sempre più punti.

Esempio 1.2.8. $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$, ma l'estensione non è di Galois e

$$\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = \{\mathrm{id}\}$$

Infatti, per esempio, il punto $[(x^3-2, y^3-2)]$ in $\mathbb{A}^2_{\mathbb{Q}}$ è immagine del solo punto $(\sqrt[3]{2}, \sqrt[3]{2})$. Gli altri punti di cui è immagine sono $\mathbb{Q}[\eta\sqrt[3]{2}]$-punti, dove η è una radice terza dell'unità diversa da 1. Qui vediamo che un'iniziale insufficienza dell'estensione presa (non è un'estensione normale) viene colmata prendendo una sovraestensione. Diverso sarebbe il caso di un'estensione non separabile, ma tutti i campi che considereremo (in particolare quelli finiti) sono perfetti.

Esempio 1.2.9. $[\mathbb{C} : \mathbb{R}] = 2$ e

$$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, z \mapsto \overline{z}\}$$

I due $\mathbb{C}$-punti $(a + \alpha i, b + \beta i)$ e $(a - \alpha i, b - \beta i)$ di $\mathbb{A}^2_{\mathbb{R}}$ hanno per immagine $[((x-a)(y-b) - \alpha\beta, \beta(x-a) - \alpha(y-b))]$. Poichè $\mathbb{C}$ è la chiusura algebrica di $\mathbb{R}$, tutti gli ideali massimali di $\mathbb{R}[x, y]$ sono di questa forma.

1.3 Varietà su campi finiti

D'ora in avanti considereremo soltanto varietà su campi finiti. Ricordiamo alcune proprietà:

(a) se k e k' sono campi finiti dello stesso ordine allora sono isomorfi;

(b) se k è un campo finito, per ogni $m \geq 1$ esiste un'estensione di k di grado m, inoltre se K è una tale estensione ($k \cong \mathbb{F}_q$ e $K \cong \mathbb{F}_{q^m}$), allora $\mathrm{Gal}(K/k) \cong \mathbb{Z}/(m)$ con generatore $\mathscr{F} : a \mapsto a^q$ (automorfismo di Frobenius);

(c) se E e F sono estensioni di k di gradi m e n rispettivamente, allora esistono morfismi di k-algebre $K \longrightarrow K'$ se e solo se $m|n$;

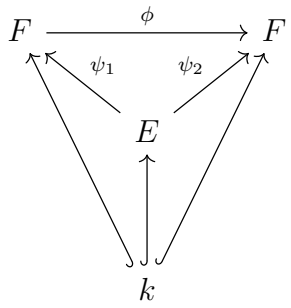
(d) se K è un'estensione di k di grado m e $n \mid m$ allora esiste un'unica sottoestensione di k in K di grado n.

(e) se $\overline{k}$ è una chiusura algebrica di k, $\mathrm{Gal}(\overline{k}/k)$ è generato come gruppo topologico da $\mathscr{F}$, mentre il suo sottogruppo $\mathrm{Gal}(\overline{k}/K)$ (con K l'unica sottoestensione di k in $\overline{k}$ di grado n) è generato da $\mathscr{F}^n$.

Della proprietà (c) si può dire di più:

Lemma 1.3.1. *Sia k un campo finito, E una sua estensione di grado d e F un'altra sua estensione di grado m, con $d|m$: allora ci sono esattamente d morfismi di k-algebre $E \longrightarrow F$.*

Dimostrazione. $\mathrm{Gal}(F/k) \cong \mathbb{Z}/(m)$ agisce transitivamente sull'insieme dei morfismi di k-algebre $E \to F$, infatti, se ψ è un tale morfismo e $\phi \in \mathrm{Gal}(F/k)$, allora anche $\phi \circ \psi$ è un morfismo di k-algebre, e, dati ψ_1 e ψ_2, esiste un k-automorfismo ϕ di K tale che commuti il diagramma



Infatti, esiste un'estensione del morfismo $\psi_2 \circ (\psi_1)^{-1} : \psi(E) \longrightarrow F$ e tale estensione risulta un k-automorfismo di F. Inoltre, in questa azione, lo stabilizzatore di ogni morfismo ψ è isomorfo al gruppo $\mathbb{Z}/(\frac{m}{d})$, infatti i k-automorfismi che, nell'azione del gruppo, non modificano ψ, sono quelli che lasciano invariata la sua immagine $\psi(E)$ la quale è un sottocampo di F isomorfo a E e dunque $[F : \psi(E)] = \frac{m}{d}$. □

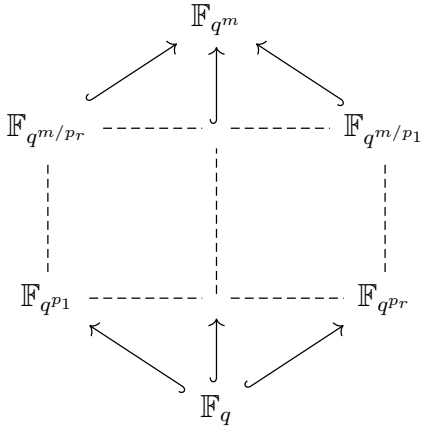
Sia allora X una varietà su un campo finito $k \cong \mathbb{F}_q$, consideriamo i K-punti di X.

Proposizione 1.3.2. *Sia $m = [K : k]$, allora*

$$\#X(K) = \sum_{d|m} d \cdot \#\left\{x \in X_{cl} | \deg(x) = d\right\}$$

Dimostrazione. Per la (1.1), dobbiamo contare, per ogni $x \in X_{\mathrm{cl}}$, i morfismi di k-algebre $\kappa(x) \longrightarrow K$: sia allora $d = \deg(x) = [\kappa(x) : k]$ e $m = [K : k]$. Se $d \nmid m$ non vi sono morfismi, se invece $d \mid m$, per il lemma, ve ne sono esattamente d. □

Sia dunque K un'estensione di k di grado m: $\mathrm{Gal}(K/k) \cong \mathbb{Z}/(m)$. Chiamiamo $\mathbb{F}_{q^d}$ l'unica sottoestensione di k in K di grado d. Se $m = p_1^{h_1} \dots p_r^{h_r}$, i K-punti di X si raggruppano, per quanto visto nella sezione precedente, in orbite del gruppo $\mathrm{Gal}(K/k)$. Ci saranno: orbite costituite da punti singoli (punti razionali), orbite di p_1 elementi ($\mathbb{F}_{q^{p_1}}$-punti che non sono razionali), orbite di p_2 elementi ($\mathbb{F}_{q^{p_2}}$- punti che non sono razionali) e così via, per tutti i divisori di m, fino a orbite di m elementi ($\mathbb{F}_{q^m}$-punti diversi dai precedenti).



Se, anziché K, prendiamo una chiusura algebrica $\overline{k}$ di k, e chiamiamo $\mathbb{F}_{q^r}$ l'unica sottoestensione di k in $\overline{k}$, allora si raggruppano via via tutti gli $\mathbb{F}_{q^r}$-punti di X.

Osservazione 1.3.3. In questo modo, se prendiamo $X = \mathbb{A}_{\mathbb{F}_q}$, si enumerano, al crescere del grado dei generatori, tutti gli ideali massimali di $\mathbb{F}_q[x_1, \dots, x_N]$.

Esempio 1.3.4. Sia $q = 2$ e $N = 2$, abbiamo $\mathbb{F}_2 = \{0, 1\}$, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha{+}1\}$ con la regola che $\alpha^2 = \alpha + 1$. Ci sono dunque 4 punti razionali di $\mathbb{A}^2_{\mathbb{F}_2}$ e altri 12 $\mathbb{F}_4$-punti oltre a questi. $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) = \{\mathrm{id}, \mathscr{F}\}$, dove $\mathscr{F}$ scambia α con $\alpha + 1$ (è l'automorfismo di Frobenius: $x \mapsto x^2$). Questo divide i 12 punti non razionali in coppie di punti coniugati ($(0, \alpha)$ con $(0, \alpha+1)$ ecc.). Le immagini di questi punti danno gli ideali massimali di $\mathbb{F}_2[x, y]$ della tabella 1.1.
E in questo modo, prendendo le estensioni $\mathbb{F}_8$, $\mathbb{F}_{16}$, ecc. si possono enumerare tutti gli ideali massimali di $\mathbb{F}_2[x, y]$.

Punti razionali		**$\mathbb{F}_4$-punti non razionali**	
$(0,0)$	$[(x,y)]$	$(0,\alpha)$ $(0,\alpha+1)$	$[(x,y^2+y+1)]$
$(0,1)$	$[(x,y+1)]$	$(1,\alpha)$ $(1,\alpha+1)$	$[(x+1,y^2+y+1)]$
$(1,0)$	$[(x+1,y)]$	$(\alpha,0)$ $(\alpha+1,0)$	$[(x^2+x+1,y)]$
$(1,1)$	$[(x+1,y+1)]$	$(\alpha,1)$ $(\alpha+1,1)$	$[(x^2+x+1,y+1)]$
		(α,α) $(\alpha+1,\alpha+1)$	$[(xy+x+1,x+y)]$
		$(\alpha,\alpha+1)$ $(\alpha+1,\alpha)$	$[(xy+1,x+y+1)]$

Tabella 1.1: I primi ideali massimali di $\mathbb{F}_2[x,y]$

Abbiamo visto (sempre nell'osservazione 1.2.4) che anche un morfismo di schemi induce una mappa sui K-punti. Vediamo che nel caso dei campi finiti l'azione degli automorfismi sui punti di X si rispecchia in un morfismo di X. Definiamo infatti il *morfismo di Frobenius*

$$\mathrm{Frob}_{X,q} : X \longrightarrow X$$

nel modo seguente. Esso è costituito dall'identità sullo spazio topologico X mentre, per ogni $U \subset X$ aperto, il morfismo di anelli $\mathscr{O}_X(U) \longrightarrow \mathscr{O}_X(U)$ è dato da $u \mapsto u^q$, dove $\mathscr{O}_X(U) \cong k[x_1,\ldots,x_n]/I$ (con I un ideale radicale). Osserviamo che questo risulta un morfismo di k-algebre, infatti $\forall a \in k, a^q = a$. Al livello dei campi di residui, $\mathrm{Frob}_{X,q}$ dà:

$$\begin{aligned} \mathrm{Frob}^*_{X,q}(p) : \kappa(p) &\longrightarrow \kappa(p) \\ v &\longmapsto v^q \end{aligned}$$

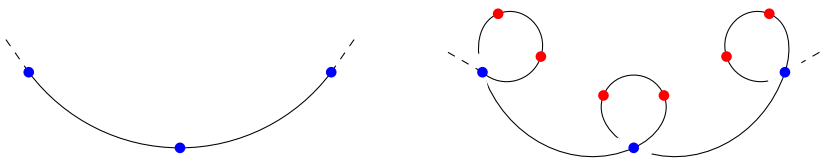
e questo non è altro che l'automorfismo di Frobenius di $\kappa(p)$.
Sia ora K un'estensione di k e chiamiamo $\mathscr{F}_K$ l'automorfismo di Frobenius di K. Abbiamo che per ogni $i \geq 1$,

$$\mathscr{F}_K^i \circ \phi = \phi \circ \mathrm{Frob}^*_{X,q}(p)^i$$

Dunque, come dicevamo, il morfismo di Frobenius e le sue potenze agiscono sui punti di X proprio come gli automorfismi di K.
In particolare, fissato $p \in X_{\mathrm{cl}}$, le potenze di $\mathrm{Frob}_{X,q}$ hanno un'azione transitiva sui K-punti aventi per immagine p (dalla dimostrazione del lemma 1.2.4

infatti segue che ciò accade per i k-automorfismi di K). Inoltre a potenze diverse corrispondono K-punti diversi. In altre parole, iterando successivamente il morfismo $\mathrm{Frob}_{X,q}$ si permutano ciclicamente gli insiemi di K-punti aventi la stessa immagine.

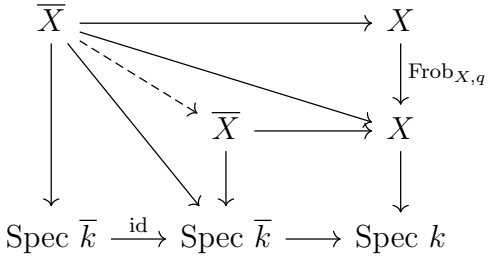
Osservazione 1.3.5. Sia k' un sottocampo di k, tale che $[k : k'] = s$ ($k' \cong \mathbb{F}_{q'}$ con $q = (q')^s$). Chiamiamo allora $f = \mathrm{Frob}_{X/k,q}$ e $f' = \mathrm{Frob}_{X/k',q'}$. Sia p un punto chiuso: consideriamo i K-punti di immagine p. La permutazione ciclica data dalle potenze di f' risulta più fine di quella data dalle potenze di f: se da un lato abbiamo soltanto $\mathrm{id}, f, f^2, \ldots, f^{\deg(p)}$, dall'altro abbiamo $\mathrm{id}, f', (f')^2, \ldots (f')^s, (f')^{s+1}, \ldots, (f')^{2s}, \ldots, \ldots, (f')^{\deg(p)\, s}$. Dunque abbiamo



moltiplicato per s il numero dei K-punti. In particolare, un punto razionale diventa un insieme di s k-punti permutati da f'.
Invece, se $s \nmid [K : k']$, non vi sono K-punti, in quanto ogni $\kappa(p)$ è un'estensione di k e dunque un'estensione di k' di grado multiplo di s.

Prendiamo ora $\overline{k}$ una chiusura algebrica di k. I K-punti saranno un sottoinsieme dei $\overline{k}$-punti, e possiamo dire di più: poiché $\mathrm{Gal}(\overline{k}/K)$ è il sottogruppo di $\mathrm{Gal}(\overline{k}/k)$ generato da $\mathscr{F}^m$, allora i K-punti saranno precisamente quelli lasciati fissi da $\mathrm{Frob}^m_{X,q}$.
Sappiamo che i K-punti si possono considerare punti razionali dello spazio $\overline{X} = X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k})$. Come si esprime l'azione descritta in questo spazio? Poniamo $\mathrm{Frob}_{\overline{X},q} = \mathrm{Frob}_{X,q} \times \mathrm{id} : \overline{X} \longrightarrow \overline{X}$. Questa costruzione ci è consentita dalla struttura di prodotto fibrato come mostra il diagramma

seguente



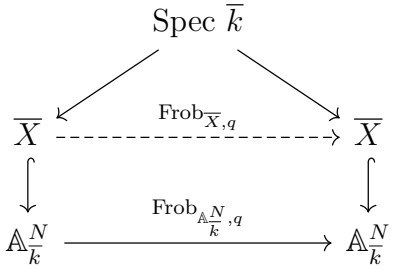
Questo nuovo morfismo non risulta più l'identità su $\overline{X}$.
Nel caso particolare $X = \mathbb{A}^N_k$ si ha $\overline{X} = \mathbb{A}^N_k \times_{\mathrm{Spec}\ k} \mathrm{Spec}\ \overline{k} \cong \mathbb{A}^N_{\overline{k}}$ e $\mathrm{Frob}_{\mathbb{A}^N_{\overline{k}},q}$ è dato dal morfismo di $\overline{k}$-algebre

$$\phi : \overline{k}[x_1, \ldots, x_N] \longrightarrow \overline{k}[x_1, \ldots, x_N]$$
$$x_i \longmapsto x_i^q$$

Questo infatti soddisfa la proprietà universale che caratterizza $\mathrm{Frob}_{X,q} \times \mathrm{id}$. Ovvero, siano $\iota^* : \mathbb{A}^N_{\overline{k}} \longrightarrow \mathbb{A}^N_k$ e $\lambda^* : \mathbb{A}^N_{\overline{k}} \longrightarrow \mathrm{Spec}\ \overline{k}$ i morfismi naturali, risulta

$$\mathrm{Frob}_{\mathbb{A}^N_k,q} \circ \iota^* = \iota^* \circ \mathrm{Frob}_{\mathbb{A}^N_{\overline{k}},q}$$
$$\mathrm{id} \circ \lambda^* = \lambda^* \circ \mathrm{Frob}_{\mathbb{A}^N_{\overline{k}},q}$$

L'azione di questo morfismo sui $\overline{k}$-punti è data da $(\alpha_1, \ldots, \alpha_N) \longmapsto (\alpha_1^q, \ldots, \alpha_N^q)$. Se $X = \mathrm{Spec}(k[x_1, \ldots, x_N]/I)$, allora $\overline{X} = \mathrm{Spec}(\overline{k}[x_1, \ldots, x_N]/I)$ e si ha $\overline{X} \hookrightarrow \mathbb{A}^N_{\overline{k}}$, quindi il punto $(\alpha_1, \ldots, \alpha_N)$ si può considerare immerso nello spazio affine, e l'azione di $\mathrm{Frob}_{\overline{X},q}$ è la medesima, come illustra il diagramma seguente:



Infine, per X generico, è sufficiente considerare ogni suo sottoschema aperto affine e ricondursi al caso precedente.

Abbiamo dunque che l'azione sui K-punti che avevamo individuato diventa *visibile* su $\overline{X}$: i K-punti di X diventano $\overline{k}$-punti (punti razionali) di $\overline{X}$ fissati da $\mathrm{Frob}^r_{\overline{X},q}$.

Capitolo 2

La funzione zeta di Hasse-Weil

2.1 Definizione e proprietà elementari

Definiremo ora la funzione zeta di Hasse-Weil e daremo alcune proprietà elementari [1]. Sia X una varietà algebrica (nel senso specificato in 1.1) su un campo finito k di ordine q.

Osservazione 2.1.1. Il numero di K-punti di X non dipende dalla particolare estensione K/k, ma soltanto dal suo grado $[K : k]$, infatti se K e K' sono due estensioni di grado uguale di k, l'isomorfismo di k-algebre tra essi induce una biiezione tra $X(K)$ e $X(K')$ (vedere l'osservazione 1.2.4). Dunque è ben definito il numero $N_m = |X(\mathbb{F}_{q^m})|$.

Diamo allora la seguente definizione:

Definizione 2.1.2 (Funzione zeta di Hasse-Weil)**.**

$$Z(X,t) \stackrel{def}{=} \exp\left(\sum_{m\geq 1} \frac{N_m}{m} t^m\right) \tag{2.1}$$

Mostriamo subito un'importante proprietà della funzione zeta, che ne fornisce una forma più compatta

[1] Si veda, a tal proposito, [**Must**], capitolo 2.

Proposizione 2.1.3.

$$Z(X,t) = \prod_{x \in X_{cl}} \frac{1}{1 - t^{\deg(x)}} \tag{2.2}$$

Dimostrazione. Si pone $a_r = \#\{x \in X_{\mathrm{cl}} | \deg(x) = r\}$. Per la proposizione 1.3.2, $N_m = \sum_{r|m} r a_r$, dunque

$$\log(Z(X,t)) = \sum_{m \geq 1} \frac{N_m}{m} t^m = \sum_{m \geq 1} \sum_{r|m} \frac{r a_r}{m} t^m = \sum_{r \geq 1} \sum_{k \geq 1} \frac{r a_r}{kr} t^{kr} =$$
$$= \sum_{r \geq 1} (-a_r) \log(1 - t^r) = \sum_{r \geq 1} \log(1 - t^r)^{-a_r}$$

Sostituendo la prima e l'ultima serie nella serie esponenziale si ha la tesi, in quanto

$$\prod_{x \in X_{\mathrm{cl}}} \frac{1}{1 - t^{\deg(x)}} = \prod_{r \geq 1} \frac{1}{(1 - t^r)^{a_r}}$$

□

Sia k' un sottocampo di ordine q' di k ($k' \cong \mathbb{F}_{q'}$ e $k \cong \mathbb{F}_q$ con $q = (q')^s$, per qualche s): abbiamo visto in 1.1.5 che una varietà su k si può considerare, in modo naturale, una varietà su k'. É interessante allora chiedersi come cambi la funzione zeta quando si interpreta su k' una data varietà su k. Per la 2.2 è sufficiente sapere come cambia il grado dei punti chiusi della varietà: sia $x \in X_{\mathrm{cl}}$, il grado su k' di x è, per il Lemma della Torre,

$$\deg_{k'}(x) = [\kappa(x) : k'] = [\kappa(x) : k]\,[k : k'] = s \deg_k(x)$$

Dunque si ha semplicemente:

Proposizione 2.1.4. *Sia $k \cong \mathbb{F}_q$ un'estensione di $k' \cong \mathbb{F}_{q'}$ di grado s, allora*

$$Z(X/k', t) = Z(X/k, t^s)$$

Osservazione 2.1.5. Questa proposizione ha importanti conseguenze: supponiamo k, k' e X come nell'enunciato. Allora, ponendo $N'_i = \#(X/k')(\mathbb{F}_{(q')^i})$ e $N_i = \#(X/k)(\mathbb{F}_{(q)^i})$, si ha:

$$N'_i = \begin{cases} s\,N_i, & \text{se } s|i \\ 0, & \text{altrimenti} \end{cases}$$

L'insieme degli $\mathbb{F}_{p^{ks}}$-punti della varietà X, quando è considerata su k', consiste in s copie dell'insieme degli $\mathbb{F}_{p^{ks}}$-punti della varietà X (considerata su k), mentre vengono persi tutti gli altri $\mathbb{F}_{p^i}$-punti. Notiamo che questo è proprio quanto avevamo riscontrato attraverso il morfismo di Frobenius nell'osservazione 1.3.5.

Consideriamo ora invece k' un'estensione di k. Se X è una varietà su k, consideriamo la varietà su k') $X' = X \times_{\text{Spec } k} \text{Spec } k'$ (vedere la sezione 1.1). Come si calcola la funzione zeta di X'?

Osservazione 2.1.6. $\#X'(\mathbb{F}_{q^{rm}}) = \#X(\mathbb{F}_{q^{rm}})$ Questo deriva direttamente dall'osservazione 1.2.2

Sulla funzione zeta questo si traduce nel modo seguente:

Proposizione 2.1.7. *Sia ξ una radice primitiva r-esima dell'unità , allora*

$$Z(X', t^r) = \prod_{i=1}^{r} Z(X, \xi^i t)$$

Dimostrazione.

$$\log\left(\prod_{i=1}^{r} Z(X, \xi^i t)\right) = \sum_{i=1}^{r}\sum_{l\geq 1}\frac{N_l}{l}\xi^{il}t^l = \sum_{l\geq 1}\sum_{i=1}^{r}\frac{N_l}{l}\xi^{il}t^l = \sum_{l\geq 1}\frac{N_l}{l}\left(\sum_{i=1}^{r}\xi^{il}\right)t^l$$

E si conclude osservando che $\sum_{i=1}^{r}\xi^{il} = r$ se l è multiplo di r, mentre è nullo altrimenti. □

Nella prossima sezione vedremo alcuni semplici esempi di varietà e di calcolo della funzione zeta. Vedremo come si realizzano le proprietà che abbiamo trovato e come descrivono le varietà in esame.

2.2 Esempi di calcolo della funzione zeta

In questa sezione $q = p^h$, con p primo e $k \cong \mathbb{F}_q$. Cominciamo dall'esempio più semplice.

Esempio 2.2.1 (Spazio affine)**.** Sia $X = \mathbb{A}_k^N$, si ha $N_m = |X(\mathbb{F}_{q^m})| = q^{mN}$ (vedere l'osservazione 1.2.6). Dunque:

$$Z(\mathbb{A}_k^N, t) = \exp\left(\sum_{m\geq 1} \frac{q^{mN}}{m} t^m\right) = \exp\left(-\log(1-q^N t)\right) = \frac{1}{1-q^N t}$$

Osservazione 2.2.2. Cosa succede considerando lo spazio affine come varietà su un sottocampo? Sia $\mathbb{F}_{q'} \cong k' \subset k$ con $q = (q')^s$: per la proposizione 2.1.4 si ha

$$Z(\mathbb{A}_k^N/k', t) = Z(\mathbb{A}_k^N/k, t^s)$$

Dunque:

$$Z(\mathbb{A}_k^N/k', t) = \frac{1}{1-q^N t^s}$$

E l'osservazione 2.1.5 si traduce in:

$$\#(\mathbb{A}_k^N/k')(\mathbb{F}_{(q')^i}) = \begin{cases} s(q')^{iN}, & \text{se } s|i \\ 0, & \text{altrimenti} \end{cases}$$

Dunque lo spazio $\mathbb{A}_k^N$ considerato come varietà su k' è completamente diverso da $\mathbb{A}_{k'}^N$, infatti

$$\#\mathbb{A}_{k'}^N(\mathbb{F}_{(q')^i}) = (q')^{iN}$$

Prendiamo per esempio $\mathbb{F}_p \cong k' \subset k \cong \mathbb{F}_{p^s}$ e $N = 1$: la zeta di $\mathbb{A}_k^1$ su k è

$$Z(\mathbb{A}_k^1, t) = \frac{1}{1-p^s t} = \exp\left(\sum_{m\geq 1} \frac{p^{sm}}{m} t^m\right)$$

Gli $\mathbb{F}_{p^{sm}}$-punti sono:

$$\begin{aligned} \#\mathbb{A}_k^1(\mathbb{F}_{p^s}) &= p^s \\ \#\mathbb{A}_k^1(\mathbb{F}_{p^{2s}}) &= p^{2s} \\ &\vdots \end{aligned}$$

Su k' la zeta diventa invece:

$$Z(\mathbb{A}_k^1/k', t) = \frac{1}{1-p^s t^s} = \exp\left(\sum_{m\geq 1} \frac{p^{sm}}{m} t^{sm}\right)$$

Confrontiamo allora gli $\mathbb{F}_{p^m}$-punti di $\mathbb{A}^1_k$ su k' con quelli di $\mathbb{A}^1_{k'}$ (su k'):

$$\begin{aligned}
\#\mathbb{A}^1_k/k'(\mathbb{F}_p) &= 0 & \#\mathbb{A}^1_{k'}(\mathbb{F}_p) &= p \\
\#\mathbb{A}^1_k/k'(\mathbb{F}_{p^2}) &= 0 & \#\mathbb{A}^1_{k'}(\mathbb{F}_{p^2}) &= p^2 \\
&\vdots & &\vdots \\
\#\mathbb{A}^1_k/k'(\mathbb{F}_{p^r}) &= sp^s & \#\mathbb{A}^1_{k'}(\mathbb{F}_{p^s}) &= p^s \\
\#\mathbb{A}^1_k/k'(\mathbb{F}_{p^{s+1}}) &= 0 & \#\mathbb{A}^1_{k'}(\mathbb{F}_{p^{s+1}}) &= p^{s+1} \\
&\vdots & &\vdots
\end{aligned}$$

Osservazione 2.2.3. Cosa succede invece considerando la varietà su un'estensione finita di k, come nella proposizione 2.1.7? Prendendo $\mathbb{F}_q \cong k \subset k' \cong \mathbb{F}_{q'}$ con $q' = q^r$, troviamo una conferma del fatto che $\mathbb{A}^N_k \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k') \cong \mathbb{A}^N_{k'}$ (come avevamo già visto in 1.1.6). Infatti, la zeta di $\mathbb{A}^N_{k'}$ è

$$Z(\mathbb{A}^N_{k'}, t) = \frac{1}{1-(q')^N t} = \frac{1}{1-q^{rN}t}$$

Mentre la zeta di $\mathbb{A}^N_k \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k')$, calcolata in t^r, per la proposizione 2.1.7 è

$$Z(\mathbb{A}^N_k \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k'), t^r) = \prod_{i=1}^{r} Z(\mathbb{A}^N_k, \xi^i t) = \prod_{i=1}^{r} \frac{1}{1-q^N \xi^i t}$$

e dunque $Z(\mathbb{A}^N_{k'}, t^r) = Z(\mathbb{A}^N_k \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k'), t^r)$, infatti dai passaggi

$$\begin{aligned}
&\prod_{i=1}^{r}(t-\xi^i) = t^r - 1 \quad \Rightarrow \quad \prod_{i=1}^{r}(\xi^i - t) = (-1)^r(t^r-1) \\
\Rightarrow \quad &\prod_{i=1}^{r}\frac{1-\overline{\xi}^i t}{\overline{\xi}^i} = (-1)^r(t^r-1) \quad \Rightarrow \quad \prod_{i=1}^{r}\frac{1-\xi^i t}{\xi^i} = (-1)^r(t^r-1) \\
\Rightarrow \quad &\frac{\prod_{i=1}^{r} 1-\xi^i t}{(-1)^{r+1}} = (-1)^r(t^r-1) \quad \Rightarrow \quad \prod_{i=1}^{r}(1-\xi^i t) = (-1)^{2r+1}(t^r-1) = 1-t^r
\end{aligned}$$

segue $1 - t^r = (1-\xi^i t)\dots(1-\xi^r t)$ in cui sostituendo $q^N t$ a t si ottiene $(1-q^N\xi t)(1-q^N\xi^2 t)\dots(1-q^N\xi^r t) = 1 - q^{rN}t^r$.

Esempio 2.2.4 (GL_2)**.** Consideriamo le matrici invertibili 2×2. Possiamo pensarle come il sottoinsieme di uno spazio affine 4-dimensionale costituito dagli (a, b, c, d) con la proprietà $ad - bc \neq 0$. In altre parole possiamo pensarle come Spec $k[x_1, \ldots, x_4]_{(x_1x_4 - x_2x_3)}$.
Per calcolare la funzione zeta di questa varietà dobbiamo contare, al variare di $m \geq 1$ le matrici 2×2 invertibili a coefficienti in $\mathbb{F}_{q^m}$, ovvero il numero di basi di $\mathbb{F}_{q^m}^2$. Questo è $((q^m)^2 - 1)((q^m)^2 - q^m) = q^{4m} - q^{3m} - q^{2m} + q^m$, e quindi la funzione zeta è

$$\exp\left(\sum_{m\geq 1} \frac{q^{4m}}{m}t^m - \sum_{m\geq 1} \frac{q^{3m}}{m}t^m - \sum_{m\geq 1} \frac{q^{2m}}{m}t^m + \sum_{m\geq 1} \frac{q^m}{m}t^m\right) = \frac{(1-q^2t)(1-q^3t)}{(1-qt)(1-q^4t)}$$

Nei prossimi esempi calcoliamo la zeta su alcune coniche.

Esempio 2.2.5 (Iperbole, ovvero retta privata di un punto)**.** Poniamo $C = \mathrm{Spec}(k[x, y]/(xy - 1))$. Osserviamo che $N_m = C(\mathbb{F}_{q^m}) = q^m - 1$, infatti si ha la biiezione (illustrata in figura 2.1):

$$\mathbb{F}_q \setminus \{0\} \ni x \mapsto \left(x, \frac{1}{x}\right) \in \left\{(x, y) \in (\mathbb{F}_{q^m})^2 | xy - 1 = 0\right\}$$

Allora:

$$Z(C, t) = \exp\left(\sum_{m\geq 1} \frac{q^m - 1}{m}t^m\right) = \frac{\exp\left(\sum_{m\geq 1} \frac{q^m}{m}\right)}{\exp\left(\sum_{m\geq 1} \frac{1}{m}\right)} =$$
$$= \frac{\exp(-\log(1-qt))}{\exp(-\log(1-t))} = \frac{1-t}{1-qt}$$

Esempio 2.2.6 (Parabola)**.** Poniamo $C = \mathrm{Spec}(k[x, y]/(x^2 - y))$. Si ha la biiezione (illustrata in figura 2.2):

$$\mathbb{F}_{q^m} \ni x \mapsto (x, x^2) \in \left\{(x, y) \in (\mathbb{F}_{q^m})^2 | y = x^2\right\}$$

Allora i calcoli sono gli stessi dello spazio affine e si ha:

$$Z(C, t) = \frac{1}{1-qt}$$

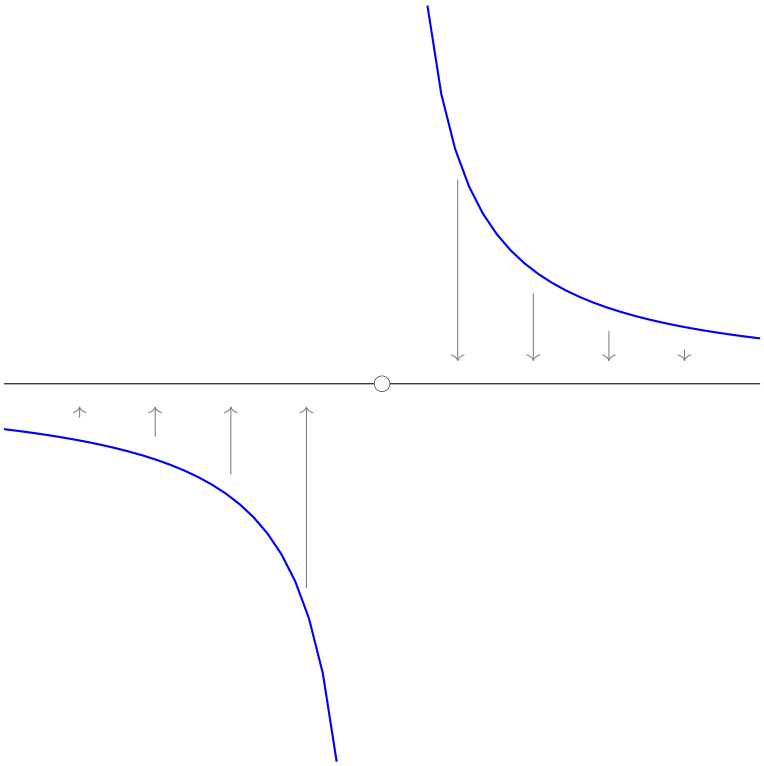


Figura 2.1

Osservazione 2.2.7. Osserviamo che le due corrispondenze biunivoche che abbiamo raffigurato, sono in realtà veri e propri isomorfismi tra gli schemi in esame. Infatti, la retta affine privata di un punto è isomorfa, come schema, a $\mathrm{Spec}(k[x]_x)$ e dunque basta osservare $k[x]_x = k[x, \frac{1}{x}] \cong k[x, y]/(xy - 1)$. Per la parabola, ancora più semplicemente si ha $k[x, y]/(y - x^2) \cong k[x, x^2] = k[x]$.

Esempio 2.2.8 (Circonferenza)**.** Sia $C = \mathrm{Spec}(k[x, y]/(x^2 + y^2 - 1))$. Questa volta per trovare il numero dei suoi punti sarà necessario un argomento più sofisticato. L'idea è la stessa che si può usare per trovare geometricamente le terne pitagoriche. Supponiamo di partire da un punto di $\mathscr{C} = \{(x, y) \in \mathbb{Q}^2 | x^2 + y^2 = 1\}$, per esempio il punto $(-1, 0)$, e tracciamo tutte le rette in $\mathbb{Q}^2$ (ovvero di coefficiente angolare λ razionale), come si vede in figura 2.3. Ciascuna di queste rette incontra la circonferenza in un altro

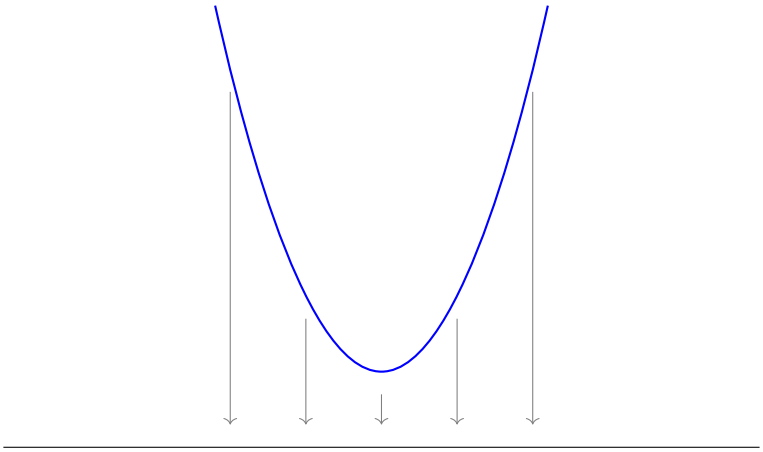


Figura 2.2

punto (in $\mathbb{Q}^2$). Infatti si ha:

$$\begin{cases} y = \lambda(x+1) \\ x^2 + y^2 = 1 \end{cases} \Rightarrow \begin{cases} y = \lambda(x+1) \\ (\lambda^2+1)x^2 + 2\lambda^2 x + \lambda^2 - 1 = 0 \end{cases}$$
$$\Rightarrow \begin{cases} y = \lambda(x+1) \\ (x+1)((\lambda^2+1)x + \lambda^2 - 1) = 0 \end{cases} \tag{2.3}$$

Poiché in $\mathbb{Q}$ risulta $1+\lambda^2 \neq 0$, esiste sempre una seconda soluzione razionale data da $x = \frac{1-\lambda^2}{1+\lambda^2}$. Viceversa, preso un punto di $\mathscr{C} \setminus \{(-1,0)\}$, esiste una retta in $\mathbb{Q}^2$ che lo congiunge con $(-1,0)$ (ovvero, la retta in $\mathbb{R}^2$ che lo congiunge con $(-1,0)$ ha coefficiente angolare razionale: esso è $\frac{y}{x-1} \in \mathbb{Q}$).

Osservazione 2.2.9. Questo dà una corrispondenza biunivoca da $[0,1] \cap \mathbb{Q}$ e l'insieme di tutte le terne pitagoriche primitive nella forma $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$.

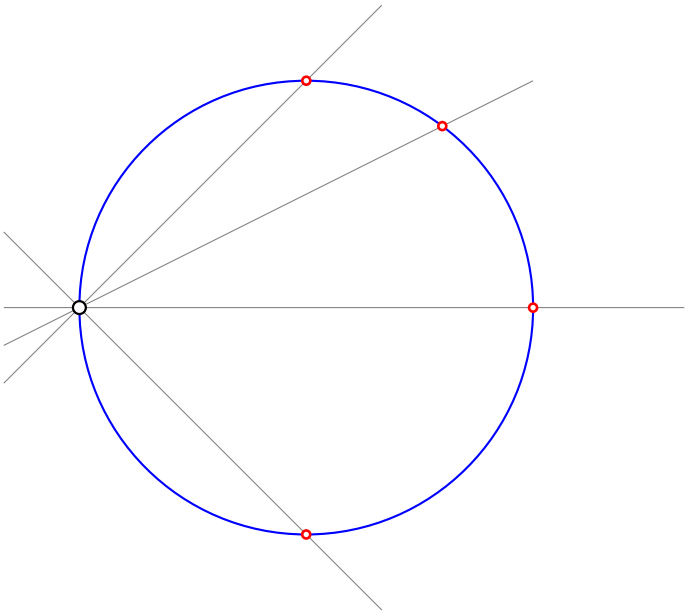


Figura 2.3

Inoltre a valori diversi di λ corrispondono punti diversi, infatti:

$$\begin{cases} \dfrac{1-\lambda^2}{1+\lambda^2} = \dfrac{1-\mu^2}{1+\mu^2} \\ \dfrac{2\lambda}{1+\lambda^2} = \dfrac{2\mu}{1+\mu^2} \end{cases} \Rightarrow \begin{cases} 1-\lambda^2+\mu^2-\lambda^2\mu^2 = 1-\mu^2+\lambda^2-\lambda^2\mu^2 \\ \lambda+\mu^2\lambda = \mu+\lambda^2\mu \end{cases}$$

$$\Rightarrow \begin{cases} 2(\lambda+\mu)(\lambda-\mu) = 0 \\ (\lambda\mu-1)(\lambda-\mu) = 1 \end{cases} \tag{2.4}$$

Dunque non può essere $\frac{1-\lambda^2}{1+\lambda^2} = \frac{1-\mu^2}{1+\mu^2}$ e $\frac{2\lambda}{1+\lambda^2} = \frac{2\mu}{1+\mu^2}$, a meno che $\lambda = \mu$. Cosa sarebbe cambiato se al posto di $\mathbb{Q}$ avessimo preso un campo finito? Osserviamo che quasi tutti i passaggi effettuati sono puramente algebrici e usano soltanto la struttura di campo di $\mathbb{Q}$. Dovremo prestare attenzione soltanto a due passaggi: non è detto in generale che $1+\lambda^2 \neq 0$ (questo infatti segue da $\lambda^2 \geq 0$) e che $2 \neq 0$ (proprietà che abbiamo usato in 2.4, ma che vale in quanto $\mathrm{char}(\mathbb{Q}) \neq 2$). Ricordiamo la seguente variante del criterio

di Eulero[2]

Lemma 2.2.10. *Sia k un campo finito di ordine q:*

(i) se $char(k) = 2$, ovvero q è pari, ogni elemento di k è un quadrato;

(ii) se $char(k) \neq 2$, ovvero q è dispari, allora $u \in k$ è un quadrato se e solo se $u^{\frac{q-2}{2}} = 1$.

Questo comporta immediatamente che -1 è un quadrato nei campi finiti di ordine q tali che q sia pari oppure $q \equiv 1 \bmod 4$. Una volta chiarito questo, possiamo finalmente contare le soluzioni di $x^2+y^2 = 1$ in $\mathbb{F}_{q^m}$. Distinguiamo i casi $\mathrm{char}(k) = 2$ (e dunque $q = 2^r$) e $\mathrm{char}(k) \neq 2$. Nel primo caso si ha semplicemente $x^2+y^2-1 = (x+y+1)^2$ e dunque in realtà la circonferenza è una retta doppia e $\#C(\mathbb{F}_{q^m}) = q^m$ (e anche nel calcolo della funzione zeta non cambierà nulla rispetto al caso della retta affine). Nel secondo caso, da un lato c'è la soluzione $(-1, 0)$, dall'altro, per ogni $m \in \mathbb{F}_{q^m}$ rifacendo i passaggi 2.3, si riottiene l'equazione $(m^2+1)x+m^2-1 = 0$: se m è una radice di -1, allora l'equazione non ha soluzione, altrimenti ha una sola soluzione.
Dunque, se $q \equiv 1 \bmod 4$:

$$\#C(\mathbb{F}_{q^m}) = q^m - 1 \tag{2.5}$$

E allora questo caso è identico a quello dell'iperbole.
Se invece $q \equiv 3 \bmod 4$:

$$\#C(\mathbb{F}_{q^m}) = \begin{cases} q^m - 1, & \text{se } m \text{ è pari} \\ q^m + 1, & \text{se } m \text{ è dispari} \end{cases}$$

In questo caso si ha

$$\exp\left(\sum_{m\geq 1} \frac{q^m - (-1)^m}{m} t^m\right) = \frac{\exp\left(\sum_{m\geq 1} \frac{q^m}{m} t^m\right)}{\exp\left(\sum_{m\geq 1} \frac{(-1)^m}{m} t^m\right)} = \frac{1+t}{1-qt}$$

[2]La dimostrazione è analoga a quella del criterio di Eulero originale.

Dunque complessivamente:

$$Z(C,t) = \begin{cases} \dfrac{1}{1-qt}, & \text{se } q = 2^r \\ \dfrac{1-t}{1-qt}, & \text{se } q \equiv 1 \bmod 4 \\ \dfrac{1+t}{1-qt}, & \text{se } q \equiv 3 \bmod 4 \end{cases}$$

2.3 La funzione zeta sulle coniche

Gli ultimi tre esempi della precedente sezione risultano paradigmatici per il caso delle coniche in generale.
Consideriamo

$$Q(x,y) = (x\ y)\mathbf{A}\begin{pmatrix} x \\ y \end{pmatrix} + \underline{\mathbf{b}}\begin{pmatrix} x \\ y \end{pmatrix} + c \tag{2.6}$$

dove

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix} \neq 0 \qquad \underline{\mathbf{b}} = (b_1\ b_2)$$

Intendiamo calcolare la funzione zeta per la varietà $\mathrm{Spec}(k[x,y]/(Q(x,y))$.
Distingueremo ellissi, parabole ed iperboli, a seconda che il numero di punti all'infinito della relativa chiusura proiettiva sia, rispettivamente, 0, 1 o 2.
Il nostro scopo è di contare le soluzioni di $Q(x,y) = 0$ nelle estensioni di k.
Se K è una tale estensione, le trasformazioni affini (o i cambiamenti di coordinate) di K^2 sono corrispondenze biunivoche, dunque possiamo applicarle liberamente.
Qualunque sia K, è possibile, attraverso trasformazioni affini, ridurre l'equazione $Q(x,y) = 0$ alla forma

$$x^2 + \delta y^2 + \eta_1 x + \eta_2 y + \theta = 0 \tag{2.7}$$

Osservazione 2.3.1. Dal lemma 2.2.10 si ricava che:

(i) Ogni elemento di un campo finito di caratteristica 2 ha una radice quadrata, e inoltre questa è unica infatti si ha $x^2 - v^2 = (x-v)^2$.

(*ii*) Ogni elemento di un campo finito di caratteristica diversa da 2 o è un quadrato, e allora ammette esattamente due radici quadrate (se non è nullo), oppure ammette due radici quadrate in tutte e sole le estensioni di grado pari di k. Infatti se $u^{\frac{q-1}{2}} \neq 1$, allora $u^{\frac{q-1}{2}} = -1$ e $u^{\frac{q^n-1}{2}} = \left(u^{\frac{q-1}{2}}\right)^{q^{n-1}+\cdots+1}$. Basta osservare allora che $q^{n-1}+\cdots+1$ ha la stessa parità di n

Converrà allora trattare separatamente i casi $\mathrm{char}(k) = 2$ e $\mathrm{char}(k) \neq 2$. Supponiamo dapprima $\mathrm{char}(k) \neq 2$.
É possibile allora il procedimento di completamento dei quadrati che permette di ridurre la (2.7) a una delle seguenti forme:

$$x^2 = 0 \tag{2.8}$$

$$x^2 = \gamma \tag{2.9}$$

$$\alpha x^2 = y \tag{2.10}$$

$$x^2 - \alpha y^2 = 0 \tag{2.11}$$

$$x^2 - \alpha y^2 = 1 \tag{2.12}$$

con $\alpha, \gamma \neq 0$.
Troviamo allora, caso per caso, il numero di soluzioni di ciascuna equazione. Indicheremo con $\mathbb{F}_{q^m}$ una generica estensione di k di grado m.

(*i*) La (2.8) è l'equazione di una retta doppia e per ogni $m \geq 1$ essa avrà q^m soluzioni in $\mathbb{F}_{q^m}^2$.

(*ii*) Per la (2.9) vi sono due possibilità:

- (*a*) Se γ è un quadrato, è l'equazione di due rette parallele razionali e ha $2q^m$ soluzioni in $\mathbb{F}_{q^m}^2$ per ogni $m \geq 1$
- (*b*) Altrimenti è l'equazione di due rette parallele non razionali e in $\mathbb{F}_{q^m}^2$ ha: $2q^m$ soluzioni per ogni m pari, 0 per m dispari.

(*iii*) La (2.10) è l'equazione di una parabola e possiamo ragionare nello stesso modo dell'esempio 2.2.6: la biiezione $\mathbb{F}_{q^m} \leftrightarrow \{(x, y) \in \mathbb{F}_{q^m}^2 \mid y = \alpha x^2\}$,

data da $x \mapsto (x, \alpha x^2)$ permette di affermare che per ogni $m \geq 1$, l'equazione ha q^m soluzioni in $\mathbb{F}_{q^m}^2$.

(iv) Per la (2.11) dobbiamo ancora distinguere due casi:

(a) Se α è un quadrato in k, essa diventa

$$(x + \sqrt{\alpha}y)(x - \sqrt{\alpha}y) = 0$$

Dove $\sqrt{\alpha}$ è una delle due radici quadrate di α. Dunque la conica è una coppia di rette distinte ($\sqrt{\alpha} \neq -\sqrt{\alpha}$), incidenti in $(0, 0)$. Pertanto la (2.11) ha $2q^m - 1$ soluzioni in $\mathbb{F}_{q^m}^2$ per ogni $m \geq 1$.

(b) Se invece α non è un quadrato, allora, per il lemma 2.3.1, la scomposizione precedente è possibile soltanto per le estensioni di grado pari. Avremo allora $2q^m - 1$ soluzioni per m pari e soltanto una (il punto $(0, 0)$) per m dispari.

(v) Per quanto riguarda la (2.12), infine, risulta che

(a) se α è un quadrato in k, allora essa diventa

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

dunque, modificando di poco l'argomento dell'esempio 2.2.5, abbiamo la biiezione

$$\mathbb{F}_{q^m} \setminus \{0\} \leftrightarrow \{(x, y) \in \mathbb{F}_{q^m}^2 \mid (x + \sqrt{\alpha}y)(x - \sqrt{\alpha}y) = 1\}$$

data da

$$\lambda \mapsto \left(\frac{\lambda + \frac{1}{\lambda}}{2}, \frac{\frac{1}{\lambda} - \lambda}{2\sqrt{\alpha}} \right)$$

Quindi si hanno $q^m - 1$ soluzioni per ogni m.

(b) Se invece α non è un quadrato in k, allora osserviamo che la conica non ha punti razionali all'infinito (è un'ellisse). Infatti l'equazione omogenea associata è

$$x^2 - \alpha y^2 = z^2$$

che per $z = 0$ dà $x^2 + \alpha y^2 = 0$, che ha soltanto la soluzione banale. Ma, per il Teorema di Chevalley-Warning[3] , la conica (proiettiva) ha almeno un punto a coordinate (omogenee) in k, dunque la conica (affine) ha almeno un punto razionale (x_0, y_0). Dunque si può riproporre l'argomento usato nell'esempio 2.2.8 e tracciare da questo punto tutte le rette $y = \lambda(x - x_0) + y_0$. Allora abbiamo

$$\begin{cases} x^2 - \alpha y^2 = 1 \\ y = \lambda(x - x_0) + y_0 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} (1 - \alpha\lambda^2)x^2 - 2\lambda\alpha(y_0 - \lambda x_0) - \alpha(y_0 - \lambda x_0)^2 \\ y = \lambda(x - x_0) + y_0 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} (x - x_0)((1 - \alpha\lambda^2)x - 2\lambda\alpha y_0 + (1 + \alpha\lambda^2)x_0) = 0 \\ y = \lambda(x - x_0) + y_0 \end{cases}$$

L'equazione $(1 - \alpha\lambda^2)x - 2\lambda\alpha y_0 + (1 + \alpha\lambda^2)x_0 = 0$ dà una soluzione per ogni λ, nelle estensioni di grado dispari e una per ogni λ diverso dalle due radici quadrate di $\frac{1}{\alpha}$, nelle estensioni di grado pari (vedere ancora il lemma 2.3.1). A queste dobbiamo aggiungere (x_0, y_0) e dunque abbiamo, come nell'esempio 2.2.8, $q^m + 1$ soluzioni se m è dispari, mentre $q^m - 1$ se m è pari.

Passiamo ora al caso in cui $\mathrm{char}(k) = 2$. Riprendiamo l'equazione (2.7). Per il lemma 2.3.1, δ ha una (unica) radice quadrata $\sqrt{\delta}$. Allora l'equazione diviene

$$(x + \sqrt{\delta}y)^2 + \eta_1(x + \sqrt{\delta}y) + (\eta_1\sqrt{\delta} + \eta_2)y + \theta = 0$$

Questo, tramite un'ultima trasformazione, porta ai casi seguenti:

$$x^2 = \gamma \tag{2.13}$$

$$x^2 + \beta x + \gamma = 0 \tag{2.14}$$

$$y = \alpha x^2 + \beta x + \gamma \tag{2.15}$$

[3]Si veda [**Ser**], capitolo 1, § 2.2.

(*i*) La (2.13) è l'equazione di una retta doppia (γ è sempre un quadrato)

(*ii*) Per la (2.14) distinguiamo il caso in cui il polinomio si spezzi in k, e allora abbiamo due rette parallele razionali, e il caso contrario, nel quale avremo due rette parallele aventi punti soltanto nelle estensioni pari di k.

(*iii*) La (2.15) permette la biiezione $\mathbb{F}_{q^m} \leftrightarrow \{(x, y) \,|\, y = \alpha x^2 + \beta x + \gamma\}$, data da $x \mapsto (x, \alpha x^2 + \beta x + \gamma)$.

Abbiamo allora tutto ciò che serve per il calcolo della funzione zeta. Essa assume le espressioni riassunte nella tabella 2.1.

Osserviamo che in tutti gli esempi studiati, in questa e nella precedente sezione, otteniamo una funzione razionale. Non si tratta di un caso: in realtà ciò avviene per qualunque varietà e questo è proprio l'enunciato di una delle congetture di Weil, dimostrata da Dwork nel 1960.

	Equazione	Conica	Funzione zeta
$\mathrm{char}(k)\neq 2$	$x^2 = 0$	Retta doppia	$\frac{1}{1-qt}$
	$x^2 = \gamma$	Coppia di rette parallele razionali (se γ è un quadrato)	$\frac{1}{(1-qt)^2}$
		Coppia di rette parallele non razionali (se γ non è un quadrato)	$\frac{1}{(1+qt)(1-qt)}$
	$\alpha x^2 = y$	Parabola	$\frac{1}{1-qt}$
	$x^2 - \alpha y^2 = 0$	Coppia di rette incidenti razionali (se α é un quadrato)	$\frac{1-t}{(1-qt)^2}$
		Coppia di rette incidenti non razionali (se α non è un quadrato)	$\frac{(1+t)(1-t)}{(1+qt)(1-qt)}$
	$x^2 - \alpha y^2 = 1$	Iperbole (se α è un quadrato)	$\frac{1-t}{1-qt}$
		Ellisse (se α non è un quadrato)	$\frac{1+t}{1-qt}$
$\mathrm{char}(k)=2$	$x^2 = \gamma$	Retta doppia	$\frac{1}{1-qt}$
	$x^2 + \beta x + \gamma = 0$	Coppia di rette parallele razionali (se il trinomio si spezza)	$\frac{1}{(1-qt)^2}$
		Coppia di rette parallele non razionali (se il trinomio non si spezza)	$\frac{1}{(1+qt)(1-qt)}$
	$y = \alpha x^2 + \beta x + \gamma$	Parabola	$\frac{1}{1-qt}$

Tabella 2.1

Bibliografia

[**Mum**] Mumford D., *The Red Book of Varieties and Schemes*, second expanded edition, Lecture Notes in Mathematics, Springer, New York, 1999

[**Must**] Mustaţă M., *Zeta Functions in Algebraic Geometry*, disponibile al sito www.math.Isa.umich.edu/∼mmustata/zeta_book.pdf

[**Ser**] Serre J.-P., *A Course in Arithmetic*, Graduate Texts in Mathematics, Springer, New York, 1973, disponibile al sito www.math.purdue.edu/∼lipman/MA598/Serre-Course%20in%20Arithmetic.pdf

[**Vak**] Vakil, R, *Math216: Foundation of Algebraic Geometry*, 2013, disponibile al sito math.stanford.edu/∼vakil/216blog/FOAGjun1113public.pdf