Università degli Studi di Padova

Facoltà di Scienze MM.FF.NN.
Dipartimento di Matematica Pura ed Applicata
Corso di Laurea in Matematica

Tesi di Laurea **A.A. 2003-2004**

Curve su Campi Finiti con Molti Punti Razionali

Relatore: Dott. Marco A. Garuti

Controrelatore: Prof. Francis Sullivan

Laureando: Dario Benetti

Università degli Studi di Padova

A mia madre
A mio padre

Indice

Introduzione

La storia del calcolo del numero dei punti di curve su campi finiti ebbe inizio con C. F. Gauss, il quale determinò il numero di punti di svariate curve definite su un campo primo $\mathbb{Z}/p\mathbb{Z}$. Per esempio, nel paragrafo 358 del suo *Disquisitiones Arithmeticæ* del 1801 calcolò il numero di punti della curva di Fermat

$$\mathcal{C}: x^3 + y^3 + z^3 \equiv 0 \pmod{p}, \tag{1}$$

dove p è un numero primo maggiore di 3. La soluzione che diede è particolarmente bella: se p non è congruo ad 1 modulo 3 allora il numero $\#\mathcal{C}(\mathbb{F}_p)$ dei punti $\mathbb{F}_p$-razionali della curva proiettiva definita da (1) è $p+1$, mentre se $p \equiv 1 \pmod 3$ c'è un unico modo di scrivere $4p = a^2 + 27b^2$, dove a e b sono interi e $a \equiv 1 \pmod 3$, e allora $\#\mathcal{C}(\mathbb{F}_p) = p+1+a$. Si noti che $|a| < 2p^{1/2}$.
Anche Jacobi lavorò sul numero delle soluzioni di tale congruenza, al fine di ottenere una stima della somma di Gauss.
Dopo di loro il problema del conteggio dei punti cadde nell'oblio per molto tempo.

Nel 1924 E. Artin introduce nella sua tesi una funzione zeta $\zeta_F(s)$ per il campo delle funzioni iperellittiche $F = \mathbb{F}_q(x,y)$ su un campo finito $\mathbb{F}_q$ con q dispari, dove y soddisfa l'equazione $y^2 = f(x)$, in analogia con la funzione zeta di Dedekind $\zeta_K(s) = \sum_{\mathfrak{A}} \mathcal{N}(\mathfrak{A})^{-s}$ per un campo di numeri K. Artin notò che sostituendo q^{-s} con t questa funzione zeta diventa una funzione razionale $Z_F(t)$ di t e che soddisfa un'equazione funzionale che lega $\zeta_F(s)$ con $\zeta_F(1-s)$. Inoltre lo stesso Artin congetturò che gli zeri di $Z_F(t)$ soddisfano $|t| = q^{1/2}$, l'analoga ipotesi di Riemann per i campi finiti. Artin formulò questi concetti in termini di ideali e classi di ideali, ma poco più tardi F. K. Schmidt descrisse tali idee usando un punto di vista più geometrico e scrisse la funzione zeta per una curva proiettiva assolutamente irriducibile liscia $\mathcal{X}$ definita su $\mathbb{F}_q$ nella forma

$$Z(\mathcal{X}, t) = \exp\Big(\sum_{m=1}^{\infty} \frac{N_m}{m} t^m \Big),$$

con $N_m = \#\mathcal{X}(\mathbb{F}_{q^m})$.
Lo stesso Schmidt osservò che il teorema di Riemann-Roch implica che per una curva di genere g la funzione $Z(\mathcal{X}, t)$ è della forma

$$Z(\mathcal{X}, t) := \frac{L(\mathcal{X}, t)}{(1-t)(1-qt)}, \tag{2}$$

dove $L(\mathcal{X}, t)$ è un polinomio di grado $2g$ soddisfacente l'equazione funzionale

$$Z(\mathcal{X}, t) = q^g t^{2g} Z\left(\mathcal{X}, \frac{1}{qt}\right).$$

Attorno al 1932 Hasse rese noto che la congettura di Artin implica che

$$|\#\mathcal{X}(\mathbb{F}_q) - (q-1)| \leq 2g\sqrt{q} \tag{3}$$

e la dimostrò per le curve ellittiche ($g = 1$).
Nel 1940 A. Weil provò la congettura di Artin, solo sedici anni dopo la sua formulazione. Weil mostrò che il polinomio $L(\mathcal{X}, t)$ definito dalla (2) è un polinomio a coefficenti interi della forma $L(\mathcal{X}, t) = \prod_{i=1}^{2g}(1 - \omega_i t)$, dove gli ω_i sono degli interi algebrici con $|\omega_i| = q^{1/2}$, e questo implica il famoso limite di Hasse-Weil (3).
La congettura di Artin (nota anche come teorema di Weil) ed una esauriente discussione sui limiti superiori dei punti razionali sono descritte nel *capitolo 2*.

Dopo il risultato ottenuto da Weil l'interesse per il problema del conteggio dei punti di una curva svanì nuovamente per parecchi anni. Più precisamente fino al 1980, quando il russo V. D. Goppa introdusse il così detto codice Goppa, un codice geometrico che può essere costruito tramite un'opportuna curva algebrica su un campo finito (si veda [Sch]). Succede che curve su un campo finito $\mathbb{F}_q$ che hanno molti punti $\mathbb{F}_q$-razionali rispetto al proprio genere formino dei buoni codici. Sfortunatamente però il numero dei punti razionali di una curva di dato genere è limitato dalla (3).
Quindi l'applicazione alla teoria dei codici, oltre che alla crittografia e alla recente costruzione di insiemi di punti quasi-aleatori (*quasi-random points*), tiene vivo l'interesse per questo problema, tant'è che molti matematici si occupano di queste questioni, portando notevoli miglioramenti.

I metodi usati per costruire curve su campi finiti con molti punti razionali sono vari ma si possono distinguere per il tipo di approccio.

I. Metodi dalla teoria dei campi di classe.

I metodi che si basano sulla teoria dei campi di classe utilizzano sottocampi di campi di classe di Hilbert o più in generale di campi di classe ray di campi di funzioni razionali nei quale un sostianzale numero di posti razionali si separano completamente. La teoria dei campi di classe è uno strumento potente per la determinazione di campi di funzioni con molti posti razionali ma ha lo svantaggio che spesso i metodi che utilizzano tale teoria producono meri risultati di esistenza e non danno una descrizione esplicita del campo. Visto che nelle applicazioni suddette è importante avere dei campi in forma esplicita, questo inconveniente è grave, ma solo da un punto di vista pratico, visto che ciò non toglie nulla all'eleganza ed alla bellezza della teoria stessa.
I principali matematici che hanno utilizzato questi metodi, oltre a J. P. Serre, sono R. Auer, K. Lauter, H. Niederreiter e C. P. Xing.
Nel *capitolo 3*, dopo un'introduzione alla teoria dei campi di classe, sono esposti il metodo di Serre ed il metodo ideato da Niederreiter e Xing che si basano sulla descrizione esplicita del gruppo di Galois rispettivamente di sottoestensioni del campo di classe ray e del campo di classe di Hilbert.

II. Prodotti fibrati di curve di Artin-Schreier.

Il prodotto fibrato di curve corrisponde a composizioni di estensioni di Galois e la potenza di questo metodo sta nel fatto che lavorando su queste estensioni galoisiane si riesce a controllare la loro composizione. L'idea di base è quella di considerare uno spazio vettoriale

i cui elementi sono la traccia di funzioni f che definiscono curve $\mathcal{X}_f$ di Artin-Schreier il cui prodotto fibrato dà una curva di genere e numero di punti razionali dipendenti rispettivamente dal genere e dal numero di punti razionali delle $\mathcal{X}_f$.
I principali matematici che hanno fatto uso di questo approccio sono J. Doumen, G. van der Geer, M. Q. Kawakita, S. Miura, V. Shabat e M. van der Vlugt.
Nel *capitolo 4* sono esposti tre metodi che si basano sul prodotto fibrato di curve di Artin-Schreier su $\mathbb{P}^1$. Il primo, ideato da van der Geer e van der Vlugt, fa uso esclusivamente del legame suddetto fra i generi ed i numeri di punti razionali. Invece il secondo (di Kawakita e Miura) ed il terzo (ancora di van der Geer e van der Vlugt) si basano anche sulla teoria delle forme quadratiche (si studia la forma quadratica definita dalle tracce di funzioni).

III. Metodi della teoria dei campi di classe basati sui moduli di Drinfeld di rango 1.

L'impiego delle proprietà del moduli di Drinfeld di rango 1 nel caso in cui la curva di base sia la retta proiettiva $\mathbb{P}^1$ produce delle buone curve associate ai sottocampi di campi di funzioni ciclotomici, le quali hanno il vantaggio di essere esplicite. Invece nel caso in cui la curva di base sia una curva qualsiasi, le curve trovate corrispondono ai sottocampi di campi di classe ray ristretti e forme esplicite di queste curve sono molto difficili da trovare.
I principali matematici che hanno affrontato il problema con l'utilizzo di questo metodo sono M. Gebhardt, E. U. Gekeler, H. Niederreiter, A. Schweizer e C. P. Xing.
Nel *capitolo 5* si trova un'esposizione riassuntiva del metodo ideato da Niederreiter e Xing che determinano dei buoni campi di funzioni dei campi di classe ray ristretti.

IV. Torri di curve con molti punti.

L'idea di questo metodo è quella di trovare delle torri costituite da combinazioni di estensioni di Kummer e di Artin-Schreier o semplicemente di composizioni di estensioni di Kummer. I campi di funzioni così ottenuti sono espliciti.
I sostenitori di questo metodo sono M. Kawakita, F. Özbudak, S. Sémirat e H. Stichtenoth.

V. Ulteriori risultati.

(i) Formule per $N_q(g)$ [1] con $g = 0, 1, 2$.
Per $g = 0$ si ha ovviamente $N_q(0) = q + 1$. Per $g = 1, 2$ sono state determinate delle formule precise da Serre in [Ser2] e [Ser4].

(ii) Curve esplicite.
Per esempi curve Hermitiane, di Suzuki, di Ree, la quartica di Klein, curve di Artin-Schreier, estensioni di Kummer, intersezioni complete e curve ottenute tramite ricerca computazionale.
La maggior parte dei matematici che si sono occupati di questo problema hanno utilizzato tale metodo.
Nel *capitolo 5* sono state trattate le curve di Hermite, di Suzuki e di Ree, dando una descrizione del loro campo di classe ray. Da notare che esse sono curve ottimali.

(iii) Curve ellittiche modulari $\mathcal{X}(n)$ associate ai sottogruppi di congruenze $\Gamma(n)$.
Questo metodo è stato usato da van der Geer e van der Vlugt.

[1] $N_q(g)$ è il massimo numero dei punti razionali che può avere una curva $\mathcal{X}/\mathbb{F}_q$ di genere g (esiste per il limite di Hasse-Weil).

(iv) Quozienti di curve con molti punti.
Questo metodo è stato usato da I. Duursma, F. Torres e J. P. Hansen.

Nel *capitolo 6* sono state riportate le tavole per il numero di punti razionali di curve di dato genere. Molti valori presenti nelle tavole sono determinati nei capitoli 3, 4 e 5.

Come si è capito, in questo lavoro sono stati esposti solo alcuni dei metodi elencati. La scelta di quali metodi trattare si è basata sulla potenzialità della teoria di produrre buone curve e non meno importante sui gusti e competenze personali. Tale selezione comunque non impedisce di farsi un'idea generale sugli approcci usati per tentare di risolvere il problema.

Nonostante molta strada sia stata fatta rimangono aperti molti quesiti legati al problema del calcolo del numero di punti razionali di curve su campi finiti:

- **Curve massimali.**

Una curva massimale $\mathcal{X}$ di genere g è una curva soddisfacente il limite di Hasse-Weil, i.e. con un numero di punti razionali pari a

$$\#\mathcal{X}(\mathbb{F}_q) = q + 1 + 2g\sqrt{q}\ .$$

Se $\mathcal{X}$ è una curva massimale di genere $g \neq 0$ su $\mathbb{F}_q$ allora q è un quadrato ed il suo genere soddisfa

$$g \leq g_0 = \sqrt{q}(\sqrt{q} - 1)/2\ .$$

Se $\mathcal{Y}$ è una curva dominata da $\mathcal{X}$ allora anch'essa è una curva massimale. Detto

$$g_1 = (\sqrt{q} - 1)^2/4\ ,$$

Fuhrmann, Garcia e Torres provano in [F-G-T] che o $g = g_0$ oppure $g \leq g_1$, dove vale l'uguaglianza se q è dispari e $g > (\sqrt{q} - 1)(\sqrt{q} - 2)/4$. Quindi sorge un naturale quesito:

Quesito 1 *Determinare per quali valori del genere esistono curve massimali. Caratterizzare queste curve.*

Le curve massimali con $g = g_0$ e $g = g_1$ sono già state caratterizzate: per $g = g_0$ le curve sono curve hermitiane e per $g = g_1$ le curve hanno equazione $y^q + y = x^{(\sqrt{q}+1)/2}$, le quali sono dominate da curve hermitiane. Per $g = g_2 = (\sqrt{q} - 1)(\sqrt{q} - 3)/8$ ci sono due tipi di curve massimali non-isomorfe per $\sqrt{q} \equiv 3 \pmod 4$, la curva di Fermat di grado $(\sqrt{q}+1)/2$ e la curva di Artin-Schreier $y^{\sqrt{q}} + y = x^{(\sqrt{q}+1)/4}$. Per ora non è nota l'esistenza di altri tipi di curve di genere g_2.
Le curve massimali conosciute sembrano provenire tutte da curve hermitiane, anche se questo non è ancora stato verificato. Ciò motiva il seguente quesito:

Quesito 2 (Stichtenoth) *Ogni curva massimale è immagine sotto un'applicazione dominante di una curva hermitiana?*

- **La funzione $N_q(g)$.**

Un'occhiata alle tavole date nel capitolo 6 suggerisce il seguente quesito:

Quesito 3 *Fissato q, la funzione $N_q(g)$ di g è una funzione non-decrescente?*

Un modo per cercare di risolverlo è quello di vedere come varia $N_q(g)$ in famiglie di curve (per esempio le curve iperellittiche, che possono avere al più $2(q+1)$ punti razionali), anche se non c'è alcuna valida ragione perché il quesito abbia risposta affermativa.
Per motivi applicativi si è fatto uno studio approfondito sul limite superiore della funzione $N_q(g)$. Anche se di poco interesse pratico sarebbe curioso studiare il limite inferiore di $N_q(g)$, i.e. migliorare la stima fissata dal limite di Hasse-Weil.

Quesito 4 *Data la coppia (q, g), quali valori può assumere il numero di punti di una curva proiettiva assolutamente irriducibile liscia di genere g su $\mathbb{F}_q$?*

Ringraziamenti

Sono grato a mia madre ed a mio padre per il loro sostegno morale ed economico.
Ringrazio i Proff. B. Scimemi e M. Bertolini per avermi fatto conoscere quella branchia della matematica che va sotto il nome di Teoria del Numeri.
Ringrazio molto il Dott. Marco A. Garuti per avermi seguito con tanta pazienza in questi ultimi dieci mesi e per avermi dato la possibilità di affrontare argomenti affascinanti della Geometria Algebrica.
Ringrazio simpaticamente lo zio Frankie che a suo modo mi ha sempre sostenuto.
Sono veramente riconoscente a coloro che mi hanno dato dei preziosi spunti e suggerimenti per compiere al meglio questo lavoro: Marco A. Garuti, Francis Sullivan, Daniele Chinellato, Matteo dalla Riva e Luca Mertens.
Ringrazio infine tutti coloro che con buon cuore mi hanno ceduto le proprie quote dell'aula degli schermi.

Padova, luglio 2004 Dario Benetti

In un mondo finito,
Dio esiste ed è unico.

K. Gödel

Capitolo 1

Teoria dei campi di funzioni algebriche

In questo capitolo verranno introdotti definizioni e risultati di base della teoria dei campi di funzioni algebriche: valutazioni, posti, divisori, il teorema di Riemann, estensioni algebriche, la formula di Hurwitz e la teoria della ramificazione, in particolare quella relativa alle estensioni di Galois.

In tutto il capitolo k indica un arbitrario campo, anche se nei capitoli successivi tratterò solamente campi di funzioni algebriche su campi finiti.
Molti risultati sono presentati senza dimostrazione perché si possono trovare in molti libri di testo. Il lettore può fare riferimento ai libri di Niederreiter e Xing [N-X] e di Stichtenoth [Sti2] principalmente. Si è fatto riferimento anche ai libri di Cassels e Fröhlich [C-F], Deuring [Deu] e di Moreno [Mor].

1.1 I posti

Definizione 1.1.1 Un'estensione F di k è chiamata **campo di funzioni algebriche (di una variabile) su** k se esiste un elemento $x \in F$ trascendente su k tale che F sia un'estensione algebrica finita di $k(x)$.

L'insieme $\tilde{k} := \{z \in F \mid z \text{ è algebrico su } k\}$ è contenuto in F come sottocampo. Tale sottocampo è chiamato **campo delle costanti** di F/k. Si ha che $k \subseteq \tilde{k} \subset F$ e che $F/\tilde{k}$ è un campo di funzioni algebriche (di una variabile) su $\tilde{k}$. Si dice che k è **algebricamente chiuso** in F o che k è il **campo completo delle costanti** di F se $\tilde{k} = k$.

Poiché verranno trattati solo campi di funzioni algebriche di una variabile F/k, farò a loro riferimento chiamandoli più semplicemente **campi di funzioni**. Se k è il campo completo delle costanti di F, indicherò F/k semplicemente con F.

Il più semplice esempio di un campo di funzioni è il **campo di funzioni razionali**; l'estensione F/k è detta **razionale** se $F = k(x)$ per qualche $x \in F$ trascendente su k.

Un arbitrario campo di funzioni F/k è spesso rappresentato come un'estensione algebrica semplice di un campo di funzioni razionali $k(x)$, i.e. $F = k(x, y)$, dove $\varphi(y) = 0$ per qualche polinomio irriducibile $\varphi(T) \in k(x)[T]$.

Definizione 1.1.2 Un **anello di valutazione** di un campo di funzioni F/k è un anello $\mathcal{O} \subseteq F$ soddisfacente le seguenti proprietà:

(i) $k \subsetneqq \mathcal{O} \subsetneqq F$;

(ii) Per ogni $z \in F$, $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Proposizione 1.1.3 *Sia $\mathcal{O}$ un anello di valutazione del campo delle funzioni F/k. Allora:*

(i) *$\mathcal{O}$ è un anello locale (si veda l'appendice A), i.e. $\mathcal{O}$ ha un'unico ideale massimale $\mathfrak{M} = \mathcal{O} \setminus \mathcal{U}$, dove $\mathcal{U} := \{z \in \mathcal{O} \mid \text{esiste } w \in \mathcal{O} \text{ con } wz = 1\}$ è il gruppo delle unità di $\mathcal{O}$;*

(ii) *Per $x \in F^* := F \setminus \{0\}$, $x \in \mathfrak{M}$ se e solo se $x^{-1} \notin \mathcal{O}$;*

(iii) *Per il campo $\tilde{k}$ delle costanti di F/k si ha che $\tilde{k} \subseteq \mathcal{O}$ e $\tilde{k} \cap \mathfrak{M} = \{0\}$.*

Definizione 1.1.4 Un **posto** P del campo di funzioni F/k è l'ideale massimale $\mathfrak{M}_P$ di qualche anello di valutazione $\mathcal{O}$ di F/k.
Un elemento $t \in P$ tale che $P = t\mathcal{O}$ è chiamato **uniformizzante** per P.

Indico con $\mathbf{P}_F$ l'insieme dei posti di F/k, i.e.

$$\mathbf{P}_F := \{P \mid P \text{ è un posto di } F/k\} .$$

Se $\mathcal{O}$ è un anello di valutazione di F/k e P è il suo ideale massimale, allora $\mathcal{O}$ è univocamente determinato da P (infatti $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$ per la proposizione 1.1.3(ii)). $\mathcal{O}_P := \mathcal{O}$ è chiamato **anello di valutazione del posto** P. Analogamente si definisce $\mathcal{U}_P$.

Definizione 1.1.5 Una **valutazione** di un campo F è una mappa suriettiva

$$\nu : F \to \Gamma \cup \{\infty\}$$

dove Γ è un gruppo abeliano totalmente ordinato non vuoto (per esempio $(\mathbb{R}, +, \geq)$) soddisfacente le seguenti proprietà:

(i) $\nu(x) = \infty$ se e solo se $x = 0$;

(ii) $\nu(xy) = \nu(x) + \nu(y)$ per ogni $x, y \in F$;

(iii) $\nu(x + y) \geq \min(\nu(x), \nu(y))$ per ogni $x, y \in F$.

Se $\Gamma = (\mathbb{Z}, +)$ la valutazione $\nu : F \to \mathbb{Z} \cup \{\infty\}$ è chiamata **valutazione discreta** di F.
La coppia ordinata (F, ν) è chiamata **campo di valutazione**.

Definizione 1.1.6 Un campo di valutazione (F, ν) è detto **completo** (rispetto a ν) se ogni successione di Cauchy[1] di elementi di F è convergente (ad un elemento di F) rispetto a ν.

[1] $(x_r)_{r \in \mathbb{N}}$ è di Cauchy se dato $N \in \mathbb{N}$ esiste un indice n_0 tale che $\nu(x_n - x_m) > N$ per $n, m \geq n_0$.

Definizione 1.1.7 Per un campo di valutazione (F, ν_F), un **completamento** di F è un'estensione E di F con valutazione discreta ν_E tale che

(i) ν_F è la restrizione di ν_E ad F;

(ii) E è completo rispetto a ν_E;

(iii) F è denso in E, i.e. per $x \in E$ esiste una sequenza di elementi di F che convergono ad x rispetto a ν_E.

Proposizione 1.1.8 (i) *Per ogni campo di valutazione (F, ν_F) esiste un completamento (E, ν_E) unico a meno di isomorfismi.*

(ii) *Se (E, ν) è un campo di valutazione discreta completo allora ν ha un'unica estensione ad ogni estensione algebrica di E.*

Per ogni posto $P \in \mathbf{P}_F$ è possibile associare una funzione $\nu_P : F \to \mathbb{Z} \cup \{\infty\}$ soddisfacente le proprietà di valutazione discreta di F/k.
Scelto un qualsiasi uniformizzante t per P, ogni elemento non nullo $z \in F$ è rappresentabile in maniera unica come $z = t^n u$, dove $n \in \mathbb{Z}$ e $u \in \mathcal{U}_P$. Posso quindi porre $\nu_P(z) := n$ e $\nu_P(0) := \infty$.

Definizione 1.1.9 Il completamento del campo di funzioni $F/\mathbb{F}_q$ rispetto alla valutazione ν_P è chiamato **completamento P-adico** di $F/\mathbb{F}_q$. Tale completamento verrà denotato con F_P.

In accordo con la proposizione 1.1.8 esiste un unico completamento P-adico per ogni posto P di F.

Teorema 1.1.10 *Sia F/k un campo di funzioni.*

(i) *Per un qualsiasi posto $P \in \mathbf{P}_F$, la funzione ν_P è una valutazione discreta di F/k. Inoltre si ha che*

$$\begin{aligned} \mathcal{O}_P &= \{z \in F \mid \nu_P(z) \geq 0\}\,, \\ \mathcal{U}_P &= \{z \in F \mid \nu_P(z) = 0\}\,, \\ P &= \{z \in F \mid \nu_P(z) > 0\}\,. \end{aligned}$$

Un elemento $x \in F$ è un uniformizzante per P se e solo se $\nu_P(x) = 1$;

(ii) *Viceversa, se ν è una valutazione discreta di F/k, allora l'insieme*

$$P := \{z \in F \mid \nu(z) > 0\}$$

è un posto di F/k e

$$\mathcal{O}_P := \{z \in F \mid \nu(z) \geq 0\}$$

è il corrispondente anello di valutazione;

(iii) *Un qualsiasi anello di valutazione $\mathcal{O}$ di F/k è un sottoanello massimale proprio di F.*

Definizione 1.1.11 Sia P un posto di F/k e $\mathcal{O}_P$ il suo anello di valutazione. $\tilde{F}_P := \mathcal{O}_P/P$ è chiamato **campo di classe dei residui** di P.
L'applicazione

$$\begin{array}{ccc} F & \longrightarrow & \tilde{F}_P \cup \{\infty\} \, , \\ x & \longmapsto & x(P) \end{array}$$

dove $x(P) = \infty$ per $x \notin \mathcal{O}_P$, è chiamata **applicazione delle classi dei residui** rispetto a P.

Definizione 1.1.12 Il **grado** di un posto P, denotato con $\deg(P)$, è definito come

$$\deg(P) := [\tilde{F}_P : k] \, .$$

L'oggetto della seguente definizione verrà usato molto spesso.

Definizione 1.1.13 Un posto di grado 1 è chiamato **posto razionale**.

Il grado di un posto è sempre finito:

Proposizione 1.1.14 *Se P è un posto di F/k e $0 \neq x \in P$, allora*

$$\deg(P) \leq [F : k(x)] < \infty \, .$$

Corollario 1.1.15 *Il campo delle costanti $\tilde{k}$ di F/k è un'estensione finita di k.*

Definizione 1.1.16 Sia $z \in F$ e $P \in \mathbf{P}_F$. Si dice che P è uno **zero** di z se e solo se $\nu_P(z) > 0$ e che P è un **polo** di z se e solo se $\nu_P(z) < 0$.
Se $\nu_P(z) = m > 0$, si dice che P è uno zero di z di **ordine** m; se $\nu_P(z) = m < 0$, si dice che P è uno polo di z di **ordine** m.

1.2 Campi di funzioni razionali

Sia $F = k(x)$ dove x è trascendente su k.
Dato un polinomio monico ed irriducibile $p(x) \in k[x]$ considero l'anello di valutazione di $k(x)/k$

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], \; p(x) \nmid g(x) \right\} \, ,$$

con ideale massimale

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], \; p(x) | f(x), \; p(x) \nmid g(x) \right\} \, . \tag{1.1}$$

In particolare se $p(x)$ è lineare, i.e. $p(x) = x - \alpha$, $\alpha \in k$, uso la notazione

$$P_\alpha := P_{x-\alpha} \in \mathbf{P}_{k(x)} \, .$$

Esiste un ulteriore anello di valutazione di $k(x)/k$, chiamato

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], \; \deg(f(x)) \leq \deg(g(x)) \right\} \, ,$$

con ideale massimale

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x],\ \deg(f(x)) < \deg(g(x)) \right\} . \tag{1.2}$$

P_∞ è chiamato **posto infinito** di $k(x)$.

Proposizione 1.2.1 *Sia $F = k(x)$ un campo di funzioni razionali.*

(i) *Sia $P = P_{p(x)} \in \mathbf{P}_{k(x)}$ il posto definito dalla (1.1), dove $p(x)$ è un polinomio irriducibile. Allora $p(x)$ è un uniformizzante per P. Inoltre c'è un isomorfismo*

$$k[x]/(p(x)) \to \mathcal{O}_P/P \quad , \quad f(x) \mapsto f(x)(P) .$$

Di conseguenza $\deg(P) = \deg(p(x))$.

(ii) *Sia $P = P_\infty$ definito dalla (1.2). Allora* $\deg(P) = 1$ *ed un uniformizzante per P è $t = 1/x$. La valutazione discreta corrispondente ν_∞ è data da*

$$\nu_\infty(f(x)/g(x)) = \deg(g(x)) - \deg(f(x)) ,$$

$f(x), g(x) \in k[x]$.

(iii) *k è il campo completo delle costanti di $k(x)/k$.*

Teorema 1.2.2 *Non ci sono ulteriori posti del campo delle funzioni razionali $k(x)/k$ oltre ai posti $P_{p(x)}$ definito dalla (1.1) e P_∞ definito dalla (1.2).*

Corollario 1.2.3 *I posti di $k(x)/k$ di grado 1 sono in corrispondenza biunivoca con $k \cup \{\infty\}$. In particolare se k è il campo finito $\mathbb{F}_q$ di ordine q allora $k(x)$ ha $q+1$ posti razionali.*

In termini di geometria algebrica, $k \cup \{\infty\}$ è interpretato come la retta proiettiva $\mathbb{P}^1(k)$ su k, cosicché i posti di $k(x)/k$ di grado 1 corrispondono univocamente ai punti di $\mathbb{P}^1(k)$.

1.3 Indipendenza delle valutazioni

Per un posto $P \in \mathbf{P}_F$ ed una funzione $f \in F$ tale che $\nu_P(f) \geq 0$ denoto con $f(P)$ la classe dei residui $f + P$ di f in $\tilde{F}_P$.
Considero una successione $\{t_r\}_{r \in \mathbb{Z}}$ di elementi di F tale che

$$\nu_P(t_r) = r \ \text{ per ogni } \ r \in \mathbb{Z} .$$

Per la data funzione f posso trovare un intero v tale che $\nu_P(f) \geq v$. Quindi

$$\nu_P\left(\frac{f}{t_v}\right) \geq 0 .$$

Detto $a_v = f/t_v(P)$ il valore della funzione f/t_v in P, posso costruire una successione (di elementi di $\tilde{F}_P$) nel seguente modo: la funzione $f/t_v - a_v$ soddisfa

$$\nu_P\left(\frac{f}{t_v} - a_v\right) \geq 1 ,$$

quindi

$$\nu_P\left(\frac{f-a_vt_v}{t_{v+1}}\right)\geq 0\ .$$

Pongo

$$a_{v+1}=\left(\frac{f-a_vt_v}{t_{v+1}}\right)(P)\ .$$

Esso è un elemento di $\tilde{F}_P$ e $\nu_P(f-a_vt_v-a_{v+1}t_{v+1})\geq v+2$. Si ottiene così una successione $\{a_r\}_{v\leq r\leq m}$ con $m>v$ di elementi di $\tilde{F}_P$ tale che

$$\nu_P\Big(f-\sum_{r=v}^{k}a_rt_r\Big)\geq k+1\ ,$$

per ogni $v\leq k\leq m$. Ma se pongo

$$a_{m+1}=\left(\frac{f-\sum_{r=v}^{m}a_rt_r}{t_{m+1}}\right)(P)$$

ho che $a_{m+1}\in\tilde{F}_P$ e che $\nu_P\big(f-\sum_{r=v}^{m+1}a_rt_r\big)\geq m+2$; quindi posso continuare la costruzione degli a_r ed ottenere così una successione infinita $\{a_r\}_{v\leq r<\infty}$ di elementi di $\tilde{F}_P$ tali che

$$\nu_P\Big(f-\sum_{r=v}^{m}a_rt_r\Big)\geq m+1\ ,$$

per ogni $m\geq v$.
Da questa costruzione ottengo dunque la serie formale

$$f=\sum_{r=v}^{\infty}a_rt_r\ ,$$

chiamata **espansione locale** di f in P. Una tipica scelta di t_r è $t_r=t^r$ con t uniformizzante per P.

Teorema 1.3.1 (di approssimazione) *Siano F/k un campo di funzioni, $P_1,P_2,\ldots,P_n$ posti di F/k a due a due distinti, $x_1,x_2,\ldots,x_n\in F$ ed $r_1,r_2,\ldots,r_n\in\mathbb{Z}$. Allora esiste $x\in F$ tale che*

$$\nu_{P_i}(x-x_i)=r_i\quad,\quad i=1,2,\ldots,n\ .$$

Corollario 1.3.2 *Ogni campo di funzioni ha un numero infinito di posti.*

Proposizione 1.3.3 *Sia F/k un campo di funzioni e siano $P_1,P_2,\ldots,P_n$ zeri di un elemento $x\in F$. Allora*

$$\sum_{i=1}^{n}\nu_{P_i}(x)\cdot\deg(P_i)\leq[F:k(x)]\ .$$

Corollario 1.3.4 *In un campo di funzioni F/k ogni elemento $x\in F^*$ ha solo un numero finito di zeri e poli.*

1.4 I divisori

Da ora e fino alla fine del capitolo k sarà il campo completo delle costanti di F.

Definizione 1.4.1 Il gruppo (additivo) abeliano libero generato dai posti di F/k è chiamato **gruppo dei divisori** di F/k ed è denotato con $\mathrm{Div}(F)$.
Gli elementi di $\mathrm{Div}(F)$ sono chiamati **divisori** di F/k. Essi sono rappresentabili tramite serie formali del tipo

$$D = \sum_{P \in \mathbf{P}_F} n_P P \, ,$$

dove gli $n_P \in \mathbb{Z}$ sono quasi tutti nulli, i.e. tutti uguali a zero tranne un numero finito.

L'elemento neutro di $\mathrm{Div}(F)$ è il divisore

$$0 := \sum_{P \in \mathbf{P}_F} r_P P \, , \; r_P = 0 \quad \text{per ogni } P \, .$$

La somma tra due divisori $D = \sum n_P P$ e $D' = \sum n'_P P$ è data da

$$D + D' = \sum_{P \in \mathbf{P}_F} (n_P + n'_P) P \, .$$

Dato $Q \in \mathbf{P}_F$ e $D = \sum n_P P \in \mathrm{Div}(F)$ posso definire $\nu_Q(D) := n_Q$. Allora

$$D = \sum_{P \in \mathbf{P}_F} \nu_P(D) P \, .$$

Definizione 1.4.2 Sia D un divisore di F/k. Il **supporto** di D è definito essere l'insieme

$$\mathrm{supp}(D) := \{ P \in \mathbf{P}_F \mid \nu_P(D) \neq 0 \} \, .$$

Definizione 1.4.3 Il **grado** di un divisore è definito come

$$\deg(D) := \sum_{P \in \mathrm{supp}(D)} \nu_P(D) \cdot \deg(P) \, .$$

Posso definire un ordine parziale su $\mathrm{Div}(F)$: dati due divisori D_1, D_2 si ha che

$$D_1 \leq D_2 \overset{\text{def}}{\iff} \nu_P(D_1) \leq \nu_P(D_2) \, , \; P \in \mathbf{P}_F \, .$$

Definizione 1.4.4 Un divisore $D \geq 0$ è chiamato **divisore positivo** (o **divisore effettivo**).
Un divisore della forma $D = P$ con $P \in \mathbf{P}_F$ è chiamato **divisore primo**.

Per il corollario 1.3.4 ha senso dare la seguente

Definizione 1.4.5 Sia $x \in F^*$ e denoto con $\mathbf{Z}$ (rispettivamente con $\mathbf{N}$) l'insieme degli zeri (rispettivamente dei poli) di x in $\mathbf{P}_F$. Allora si definisce il **divisore degli zeri** (rispettivamente **divisore dei poli**) di x come

$$(x)_0 := \sum_{P \in \mathbf{Z}} \nu_P(x) P \quad \Big(\text{rispettivamente } (x)_\infty := \sum_{P \in \mathbf{N}} (-\nu_P(x)) P \Big) \, .$$

Il divisore

$$(x) := (x)_0 - (x)_\infty$$

è chiamato **divisore principale** di x.

I divisori principali godono delle seguenti proprietà:

(i) $(x) = \sum_{P \in \mathbf{P}_F} \nu_P(x) P$.

(ii) $\deg(x) = 0$; più precisamente $\deg(x)_0 = \deg(x)_\infty = [F : k(x)]$.

(iii) $(x) = 0$ se e solo se $x \in k$ [2].

Definizione 1.4.6 Il **gruppo dei divisori principali** di F/k è definito essere l'insieme (dotato dell'operazione somma)

$$\mathrm{Princ}(F) := \{(x) \mid x \in F^*\} .$$

$\mathrm{Princ}(F)$ è un sottogruppo di $\mathrm{Div}(F)$, perché per $x, y \in F^*$ si ha $(xy) = (x) + (y)$ (per la proprietà (i)).

Per un divisore $D \in \mathrm{Div}(F)$ definisco l'insieme

$$\mathcal{L}(D) := \{x \in F \mid (x) \geq -D\} \cup \{0\} .$$

Esso è uno spazio vettoriale su k di dimensione finita (vedi [Ful, prop. 3, §2, cap. 8]).

Definizione 1.4.7 Per $D \in \mathrm{Div}(F)$, l'intero $l(D) := \dim_k(\mathcal{L}(D))$ è chiamato **dimensione** del divisore D.

Due divisori D e D' si dicono **linearmente equivalenti**, $D \sim D'$, se $D = D' + (x)$ per qualche $x \in F^*$. È immediato vedere che $\sim$ è una relazione di equivalenza.
È importante osservare che due divisori linearmente equivalenti hanno la stessa dimensione e (per la proprietà (ii)) lo stesso grado. Inoltre un divisore principale ha dimensione 1.

Teorema 1.4.8 (Riemann) *Sia F/k un campo di funzioni di genere g. Per ogni divisore $D \in \mathrm{Div}(F)$,*

$$l(D) \geq \deg(D) + 1 - g ,$$

dove vale l'uguaglianza per $\deg(D) \geq 2g - 1$.

Il teorema di Riemann è spesso usato per definire il genere di F in maniera implicita. Dunque è possibile definire il **genere** di F come l'intero

$$g = g(F) := \max\{\deg(D) - l(D) + 1 \mid D \in \mathrm{Div}(F)\} .$$

Ponendo $D = 0$ in questa definizione si prova che il genere è un intero non negativo.

Cito due conseguenze di questo importante teorema.

[2] Il fatto di prendere la chiusura algebrica qui risulta esenziale.

Definizione 1.4.9 Un divisore D di un campo di funzioni F di genere g è chiamato **non-speciale** se per esso vale l'uguaglianza nel teorema di Riemann, i.e. se

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

Corollario 1.4.10 *Se D è un divisore non-speciale di F e D' è un divisore di F tale che $D' \geq D$ allora D' è non-speciale.*

Dim. Poiché $D' \geq D$, il divisore $G := D' - D$ è effettivo.
Poiché vale la relazione

$$l(D+G) \leq l(D) + \deg(G) \ ,$$

ho che

$$l(D') \leq l(D) + \deg(G) = \deg(D) + 1 - g + \deg(D' - D) = \deg(D') + 1 - g \ .$$

□

Definizione 1.4.11 Sia P un posto di F. Un intero $n > 0$ è detto essere un **numero di polo** di P se esiste un elemento $x \in F^*$ tale che $(x)_\infty = nP$. Diversamente n è detto essere un **numero di lacuna** (*gap number*) di P.

Corollario 1.4.12 (Teorema della lacuna di Weierstrass) *Sia F un campo di funzioni di genere $g \geq 1$ e sia P un posto razionale di F. Allora esistono esattamente g numeri di lacuna $i_1, i_2, \ldots, i_g$ di P soddisfacenti*

$$1 = i_1 < i_2 < \cdots < i_g \leq 2g - 1 \ .$$

Dim. È un'immediata conseguenza di questi tre fatti:

(i) Per ogni $i \geq 1$ si ha che $\mathcal{L}((i-1)P) = \mathcal{L}(iP)$ se e solo se i è un numero di lacuna di P;

(ii) $l(iP) \leq l((i-1)P) + 1$;

(iii) $l(0 \cdot P) = 1$ e $l((2g-1)P) = g$. □

1.5 I gruppi delle classi di divisori e di ideali

In tutto il paragrafo il campo completo delle costanti k di F è finito.

Definizione 1.5.1 Il gruppo quoziente

$$\mathrm{Pic}(F) := \mathrm{Div}(F)/\mathrm{Princ}(F)$$

è chiamato **gruppo delle classi dei divisori** (o **gruppo di Picard**). Per un divisore $D \in \mathrm{Div}(F)$, il corrispondente elemento in $\mathrm{Pic}(F)$ è indicato con $[D]$, la **classe dei divisori** contenente D (quindi $[D] = [D']$ se e solo se $D \sim D'$).

Indico con $\mathrm{Div}^0(F)$ il sottoinsieme di $\mathrm{Div}(F)$ formato da tutti i divisori di F di grado 0. Allora $\mathrm{Div}^0(F)$ è un sottogruppo di $\mathrm{Div}(F)$, chiamato **gruppo dei divisori di grado zero** di F.
Per la proprietà (ii) dei divisori principali ho che

$$\mathrm{Princ}(F) \subseteq \mathrm{Div}^0(F) \ .$$

Definizione 1.5.2 Il gruppo quoziente

$$\mathrm{Cl}(F) := \mathrm{Div}^0(F)/\mathrm{Princ}(F)$$

è chiamato **gruppo delle classi di divisori di grado zero** di F. La cardinalità di $\mathrm{Cl}(F)$ è chiamata **numero delle classi di divisori** di F ed è denotata con $h(F)$.

Scelto un sottoinsieme proprio di $\mathbf{P}_F$ non vuoto $\mathcal{S}$, definisco il **dominio degli $\mathcal{S}$-posti** di F come

$$\mathcal{O}_{\mathcal{S}} := \{z \in F \mid \nu_P(z) \geq 0 \text{ per ogni } P \in \mathcal{S}\} \ .$$

Allora $\mathcal{O}_{\mathcal{S}}$ è un dominio di Dedekind (si veda l'appendice A). In particolare

$$\mathcal{O}_{\mathcal{S}} = \bigcap_{P \in \mathcal{S}} \mathcal{O}_P \ .$$

Definizione 1.5.3 Un sottoinsieme non vuoto $\mathfrak{A}$ di F è detto essere un **$\mathcal{S}$-ideale frazionario** (o un **$\mathcal{S}$-ideale**) di F se:

(i) $\mathfrak{A} \neq \{0\}$;

(ii) $\mathfrak{A}$ è un $\mathcal{O}_{\mathcal{S}}$-modulo;

(iii) Esiste un elemento $a \in F^*$ tale che $a\mathfrak{A} \subseteq \mathcal{O}_{\mathcal{S}}$.

Da osservare che se un $\mathcal{S}$-ideale $\mathfrak{A}$ sta in $\mathcal{O}_{\mathcal{S}}$, allora esso è un ideale ordinario dell'anello $\mathcal{O}_{\mathcal{S}}$. In questo caso si dice che $\mathfrak{A}$ è un **$\mathcal{S}$-ideale intero**.
Indico con $\mathcal{I}_{\mathcal{S}} = \mathcal{I}_{\mathcal{S}}(F)$ l'insieme degli $\mathcal{S}$-ideali. Per ogni coppia di $\mathcal{S}$-ideali $\mathfrak{A}$, $\mathfrak{B}$ di F, gli insiemi

$$\mathfrak{A} + \mathfrak{B} = \{x + y \mid x \in \mathfrak{A} \ , \ \ y \in \mathfrak{B}\} \ ,$$
$$\mathfrak{A} \cdot \mathfrak{B} = \Big\{ \sum_{i=1}^{n} x_i y_i \mid x_i \in \mathfrak{A} \ , \ \ y_i \in \mathfrak{B} \ , \ \ n \in \mathbb{Z}_{>0} \Big\} \ ,$$

e $\mathfrak{A} \cap \mathfrak{B}$ sono $\mathcal{S}$-ideali. Dunque $\mathcal{I}_{\mathcal{S}}$ è dotato della struttura di gruppo abeliano moltiplicativo.

Definizione 1.5.4 Se $z \in F^*$ allora l'$\mathcal{S}$-ideale $z\mathcal{O}_{\mathcal{S}}$ è chiamato **$\mathcal{S}$-ideale principale**. L'insieme degli $\mathcal{S}$-ideali principali è un sottogruppo di $\mathcal{I}_{\mathcal{S}}$ chiamato **gruppo degli $\mathcal{S}$-ideali principali** ed è denotato con $\mathrm{Princ}_{\mathcal{S}} = \mathrm{Princ}_{\mathcal{S}}(F)$.

Definizione 1.5.5 Il gruppo quoziente

$$\mathrm{Cl}(\mathcal{O}_{\mathcal{S}}) := \mathcal{I}_{\mathcal{S}}/\mathrm{Princ}_{\mathcal{S}}$$

è chiamato **gruppo delle classi di ideali frazionari di $\mathcal{O}_{\mathcal{S}}$** o **gruppo delle classi degli $\mathcal{S}$-ideali** di F.

Proposizione 1.5.6 *Se $\mathbf{P}_F \setminus \mathcal{S}$ è un insieme finito non vuoto allora* $\mathrm{Cl}(\mathcal{O}_\mathcal{S})$ *è un gruppo abeliano finito.*

Se $\mathbf{P}_F \setminus \mathcal{S}$ è un insieme finito non vuoto la cardinalità di $\mathrm{Cl}(\mathcal{O}_\mathcal{S})$ è chiamata **numero delle classi di ideali frazionari** di $\mathcal{O}_\mathcal{S}$ ed è indicato con $h(\mathcal{O}_\mathcal{S})$.

C'è una stretta relazione fra il gruppo delle classi di divisori di grado zero $\mathrm{Cl}(F)$ di F ed il gruppo delle classi di ideali frazionari $\mathrm{Cl}(\mathcal{O}_\mathcal{S})$ di $\mathcal{O}_\mathcal{S}$. Tale relazione è presentata qui solamente nel caso in cui $\mathbf{P}_F \setminus \mathcal{S}$ consista di un singolo posto (si veda l'articolo di Rosen [Ros1] per il caso generale).

Proposizione 1.5.7 *Se $\mathcal{S} = \mathbf{P}_F \setminus \{P\}$ per qualche posto P allora esiste una sequenza esatta*

$$0 \to \mathrm{Cl}(F) \to \mathrm{Cl}(\mathcal{O}_\mathcal{S}) \to \mathbb{Z}/d\mathbb{Z} \to 0 \ ,$$

dove d è il grado $\deg(P)$ *di P. In particolare*

$$h(\mathcal{O}_\mathcal{S}) = dh(F)$$

e pertanto $\mathrm{Cl}(F)$ *è isomorfo a* $\mathrm{Cl}(\mathcal{O}_\mathcal{S})$ *se P è un posto razionale.*

Dim. Considero l'omomorfismo

$$\vartheta : \mathrm{Div}^0(F) \to \mathrm{Cl}(\mathcal{O}_\mathcal{S}) \ , \ \sum_Q m_Q Q \mapsto \Big(\prod_{Q \neq P} \mathfrak{M}_Q(\mathcal{S})^{m_Q} \Big) \cdot \mathrm{Princ}_\mathcal{S} \ .$$

Allora è facile verificare che $\ker(\vartheta) = \mathrm{Princ}(F)$ e così ϑ induce un monomorfismo

$$\theta : \mathrm{Cl}(F) \to \mathrm{Cl}(\mathcal{O}_\mathcal{S}) \ .$$

Definisco un altro omomorfismo

$$\varphi : \mathcal{I}_\mathcal{S} \to \mathbb{Z}/d\mathbb{Z} \ , \ \prod_{Q \neq P} \mathfrak{M}_Q(\mathcal{S})^{m_Q} \mapsto \sum_{Q \neq P} m_Q \deg(Q) + d\mathbb{Z} \ .$$

Si osservi che φ è suriettivo perché la funzione grado $\mathrm{Div}(F) \to \mathbb{Z}$ è suriettiva (per il [Sti2, cor. V.1.11]). Inoltre, poiché $\mathrm{Princ}_\mathcal{S} \subseteq \ker(\varphi)$, φ induce un epimorfismo

$$\phi : \mathrm{Cl}(\mathcal{O}_\mathcal{S}) \to \mathbb{Z}/d\mathbb{Z} \ .$$

È ora facile vedere che $\ker(\phi) = \mathrm{im}(\theta)$. □

Sia $D = \sum_P \nu_P(D)P$ un divisore effettivo di F. Se $x \in F^*$, dico che

$$x \equiv 1 \pmod{D}$$

se $x \in \{y \in \mathcal{O}_P \mid \nu_P(y-1) \geq \nu_P(D)\}$ per ogni $P \in \mathrm{supp}(D)$.

Sia $\mathcal{S}$ un sottoinsieme proprio di $\mathbf{P}_F$ tale che $\mathrm{supp}(D) \subseteq \mathcal{S}$ e $\mathbf{P}_F \setminus \mathcal{S}$ sia finito. Indico con $\mathcal{I}_{D,\mathcal{S}}$ il sottogruppo di $\mathcal{I}_\mathcal{S}$ formato dagli $\mathcal{S}$-ideali che sono relativamente primi con D, i.e.

$$\mathcal{I}_{D,\mathcal{S}} := \{\mathfrak{A} \in \mathcal{I}_\mathcal{S} \mid \nu_P(\mathfrak{A}) = 0 \text{ per ogni } P \in \mathrm{supp}(D)\} \ .$$

Definisco anche il sottogruppo $\mathrm{Princ}_{D,\mathcal{S}}$ di $\mathcal{I}_\mathcal{S}$ come

$$\mathrm{Princ}_{D,\mathcal{S}} = \mathrm{Princ}_D(\mathcal{O}_\mathcal{S}) := \{x \in \mathcal{O}_\mathcal{S} \mid x \in F^* \ , \ x \equiv 1 \pmod{D}\} \ .$$

Definizione 1.5.8 Il gruppo quoziente

$$\mathrm{Cl}_D(\mathcal{O}_\mathcal{S}) := \mathcal{I}_{D,\mathcal{S}}/\mathrm{Princ}_{D,\mathcal{S}}$$

è chiamato **gruppo delle classi $\mathcal{S}$-ray** ($\mathcal{S}$-*ray class group*) modulo D.

Se $D = 0$ il gruppo delle classi $\mathcal{S}$-ray modulo 0 coincide con il gruppo delle classi degli $\mathcal{S}$-ideali $\mathrm{Cl}(\mathcal{O}_\mathcal{S})$.

1.6 Estensioni algebriche

Si assuma fino alla fine del paragrafo che F'/k' e F/k siano due campi di funzioni, che F'/F sia un'estensione finita e separabile (si confronti l'appendice A) e che $k' \supseteq k$ con k finito.

In questo paragrafo intendo enunciare la formula del genere di Hurwitz.

Sia P un posto di F e P' un posto che sta **sopra** P, i.e. $P \subseteq P'$. Questo fatto è spesso indicato con $P'|P$. Scelto un uniformizzante $t_P \in F$ per P, allora l'intero $\nu_{P'}(t_P)$ è chiamato **indice di ramificazione** di P' su P. Esso non dipende dalla scelta dell'uniformizzante t_P per P. Denoto $\nu_{P'}(t_P)$ con $e_{P'}(F'/F)$ o con $e(P'|P)$. Come si vedrà nella successiva proposizione, $1 \leq e_{P'}(F'/F) \leq [F' : F]$. Si dice che l'estensione è **ramificata** per P' (o che P' è **ramificato** in F'/F) se $e_{P'}(F'/F) > 1$ e che è **non-ramificata** per P' (o che P' è **non-ramificato** in F'/F) se $e_{P'}(F'/F) = 1$. Inoltre P' è detto **totalmente ramificato** in F'/F se $e_{P'}(F'/F) = [F' : F]$.
Siano $\tilde{F}'_{P'}$ e $\tilde{F}_P$ i campi delle classi dei residui di P' e P rispettivamente. Allora $\tilde{F}'_{P'}/\tilde{F}_P$ è un'estensione finita ed il suo grado $[\tilde{F}'_{P'} : \tilde{F}_P]$ è chiamato **grado relativo** di P' su P ed è denotato con $f_{P'}(F'/F)$ o $f(P'|P)$.

La seguente proposizione mi mette in relazione i gradi relativi con gli indici di ramificazione di posti di F' che stanno sopra ad un fissato posto di F.

Proposizione 1.6.1 *Sia P un posto di F e siano $P'_1, P'_2, \ldots, P'_r$ dei posti distinti di F' che stanno sopra P. Allora*

$$\sum_{i=1}^{r} e(P'_i|P) f(P'_i|P) = [F' : F] \, .$$

Se $e(P'|P) = f(P'|P) = 1$ per ogni posto $P'|P$ allora si dice che P si **separa completamente** in F'/F. Dalla proposizione 1.6.1 deduco in questo caso che ci sono esattamente $[F' : F]$ posti di F' che stanno sopra P.
Se invece un posto P'_i della proposizione 1.6.1 è totalmente ramificato in F'/F allora dalla stessa proposizione si deduce che $r = 1$. In questo caso ha quindi senso dire che P è **totalmente ramificato** in F'/F o che F'/F è **totalmente ramificata** per P.

Sia $\mathcal{S}$ un sottoinsieme proprio di $\mathbf{P}_F$ non vuoto e $\mathcal{T}$ un sottoinsieme di $\mathbf{P}_{F'}$ formato da tutti i posti di F' che stanno sopra ai posti di $\mathcal{S}$. Allora $\mathcal{T}$ è chiamato **sopra-insieme**

di $\mathcal{S}$ rispetto all'estensione F'/F. La chiusura intera (vedere l'appendice A) di $\mathcal{O}_{\mathcal{S}}$ in F' è data da

$$\mathcal{O}_{\mathcal{T}} := \{z \in F' \mid \nu_{P'}(z) \geq 0 \text{ per ogni } P' \in \mathcal{T}\} .$$

Considero il caso in cui $\mathcal{S}$ è formato da un singolo posto P di F e sia ancora $\mathcal{T}$ il sopra-insieme di $\mathcal{S}$ rispetto all'estensione F'/F. Una base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ di F'/F è chiamata **P-intera** se

$$\mathcal{O}_{\mathcal{T}} = \alpha_1\mathcal{O}_P + \alpha_2\mathcal{O}_P + \cdots + \alpha_n\mathcal{O}_P .$$

Per una qualsiasi base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ di F'/F si definisce il **discriminante** della base come

$$\Delta_{F'/F} = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) := \det\big(\mathrm{Tr}_{F'/F}(\alpha_i\alpha_j)\big) = \det\big(\sigma_i(\alpha_j)\big)^2 ,$$

dove $\mathrm{Tr}_{F'/F}$ è la funzione traccia e $\sigma_1, \sigma_2, \ldots, \sigma_n$ sono le F-immersioni di F' in una chiusura algebrica di F (si confronti l'appendice A sia per la definizione della funzione traccia e le sue proprietà sia per la definizione di chiusura algebrica). Si osservi che $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$ perché l'estensione è separabile.

Definizione 1.6.2 Sia $\mathcal{S}$ un sottoinsieme proprio di $\mathbf{P}_F$ non vuoto e sia $\mathcal{T}$ il suo sopra-insieme rispetto ad F'/F. Si definisce il **codifferente** di $\mathcal{O}_{\mathcal{T}}$ come

$$\mathrm{co}(\mathcal{O}_{\mathcal{T}}) := \{z \in F' \mid \mathrm{Tr}_{F'/F}(z\mathcal{O}_{\mathcal{T}}) \subseteq \mathcal{O}_{\mathcal{S}}\} .$$

Il codifferente gode delle seguenti proprietà:

(i) $\mathrm{co}(\mathcal{O}_{\mathcal{T}})$ è un $\mathcal{T}$-ideale di F' che contiene $\mathcal{O}_{\mathcal{T}}$;

(ii) $\big(\mathrm{co}(\mathcal{O}_{\mathcal{T}})\big)^{-1}$ è un ideale intero di $\mathcal{O}_{\mathcal{T}}$.

Definizione 1.6.3 Il **differente** di $\mathcal{O}_{\mathcal{T}}$ rispetto ad $\mathcal{O}_{\mathcal{S}}$ è definito come

$$\mathfrak{D}_{\mathcal{S}}(F'/F) := \big(\mathrm{co}(\mathcal{O}_{\mathcal{T}})\big)^{-1} .$$

Se $\mathcal{S}$ è costituito da un'unico posto P di F, denoterò il differente di $\mathcal{O}_{\mathcal{T}}$ semplicemente con $\mathfrak{D}_P(F'/F)$.

Definizione 1.6.4 Sia P' un posto di F' che sta sopra ad un posto P di F. Si definisce l'**esponente differente** di P' su P come

$$d(P'|P) := \nu_{P'}\big(\mathfrak{D}_P(F'/F)\big) .$$

Proposizione 1.6.5 *Per ogni sottoinsieme proprio $\mathcal{S}$ di $\mathbf{P}_F$ non vuoto ho che*

$$\mathfrak{D}_{\mathcal{S}}(F'/F) = \prod_{P\in\mathcal{S}} \prod_{P'|P} \mathfrak{M}_{P'}(\mathcal{T})^{d(P'|P)} .$$

L'esponente differente $d(P'|P)$ è un intero non negativo. Si ha $d(P'|P) = 0$ per quasi ogni posto P' di F', i.e. per tutti tranne un numero finito. Ha quindi senso dare la seguente

Definizione 1.6.6 Il **divisore differente** di $F'|F$ è definito come

$$\mathrm{Diff}(F'/F) = \sum_{P\in\mathbf{P}_F} \sum_{P'|P} d(P'|P)P' \ .$$

Si osservi che il divisore differente $\mathrm{Diff}(F'/F)$ è un divisore effettivo di F'.

Teorema 1.6.7 (Formula di Hurwitz) *Sia F'/k' un'estensione finita e separabile di F/k. Allora*

$$2g(F') - 2 = \frac{[F' : F]}{[k' : k]}\big(2g(F) - 2\big) + \deg\big(\mathrm{Diff}(F'/F)\big) \ , \tag{1.3}$$

dove $g(F')$ e $g(F)$ sono il genere di F' ed F rispettivamente.

La formula di Hurwitz è uno strumento potente per calcolare il genere di F'. Per poterla usare però si deve capire come si possono determinare gli esponenti differenti dei posti di F'. C'è una relazione fra l'indice di ramificazione e l'esponente differente, dato dalla seguente

Proposizione 1.6.8 *Per un posto P' di F' che sta sopra ad un posto P di F si ha che*

(i) $d(P'|P) \geq e(P'|P) - 1$*;*

(ii) $d(P'|P) = e(P'|P)-1$ *se e solo se* $e(P'|P)$ *è relativamente primo con la caratteristica di k.*

La proposizione 1.6.8(ii) mostra che se P' è non-ramificato in F'/F allora $d(P'|P) = 0$. Si dice che l'estensione F'/F è **non-ramificata** se tutti i posti di F' sono non-ramificati in F'/F. In questo caso $\mathrm{Diff}(F'/F) = 0$ e la formula di Hurwitz assume una forma molto semplice. Ancora la proposizione 1.6.8(ii) suggerisce le seguenti definizioni. Si dice che P' è **moderatamente ramificato** in F'/F se $e(P'|P) > 1$ ed $e(P'|P)$ non è divisibile per la caratteristica di k. Si dice anche che P' è **ramificato in maniera selvaggia** in F'/F se $e(P'|P)$ è divisibile per la caratteristica di k.

La seguente proposizione dà un metodo per determinare gli esponenti differenti dei posti totalmente ramificati di estensioni semplici (si veda anche l'appendice A):

Proposizione 1.6.9 *Sia $F' = F(\alpha)$ un'estensione finita, semplice e separabile di F e sia P' un posto di F' che sta sopra ad un posto P di F. Si supponga che P' sia totalmente ramificato in F'/F e che α sia un uniformizzante per P'. Allora*

$$d(P'|P) = \nu_{P'}\big(f'(\alpha)\big) \ ,$$

dove $f(x) \in F[x]$ è il polinomio minimo di α su F ed $f'(x)$ è la derivata di $f(x)$.

1.7 Teoria della ramificazione di estensioni di Galois

In tutto il paragrafo assumo che F'/k' sia un'estensione di Galois finita di F/k con $k' \supseteq k$, dove k è un campo finito. Indico con $G := \mathrm{Gal}(F'/F)$ il gruppo di Galois di F'/F.

Sia $\sigma \in G$ un automorfismo e sia P' un posto di F' che sta sopra ad un posto P di F. L'insieme

$$\sigma(P') := \{\sigma(x) \mid x \in P'\} \tag{1.4}$$

è chiaramente un posto di F' che sta sopra P.

Definizione 1.7.1 Il posto $\sigma(P')$ definito dalla (1.4) è chiamato **posto coniugato** di P'.

Il gruppo di Galois G agisce transitivamente sull'insieme dei posti F' che stanno sopra P:

Proposizione 1.7.2 *Siano Q_1 e Q_2 due posti di F' che stanno sopra ad un posto P di F. Allora esiste un automorfismo $\sigma \in G$ tale che $\sigma(Q_1) = Q_2$.*

Dim. Suppongo per assurdo che $\sigma(Q_1) \neq Q_2$ per ogni $\sigma \in G$. Allora dal teorema di approssimazione 1.3.1 segue che deve esistere un elemento $x \in F'$ tale che $\nu_{\sigma(Q_1)}(x) = 0$ e $\nu_{\sigma(Q_2)}(x) > 0$ per ogni $\sigma \in G$. Allora per $i = 1, 2$ ho che

$$\begin{aligned}
\nu_P\big(\mathrm{N}_{F'/F}(x)\big) &= \frac{1}{e(Q_i|P)}\nu_{Q_i}\big(\mathrm{N}_{F'/F}(x)\big) \\
&= \frac{1}{e(Q_i|P)}\sum_{\sigma\in G}\nu_{Q_i}\big(\sigma(x)\big) \\
&= \frac{1}{e(Q_i|P)}\sum_{\sigma\in G}\nu_{Q_i}\big(\sigma^{-1}(x)\big) \\
&= \frac{1}{e(Q_i|P)}\sum_{\sigma\in G}\nu_{\sigma(Q_i)}(x)\ .
\end{aligned}$$

L'ultima espressione è 0 per $i = 1$ ed è positiva per $i = 2$, assurdo. □

Dalla proprietà di transitività ottengo un risultato importante che mi mette in relazione gli indici di ramificazione, i gradi residui e gli esponenti differenti dei posti di F' che stanno su un fissato posto di F.

Teorema 1.7.3 *Sia F'/F un'estensione di Galois finita. Siano $Q_1, Q_2, \ldots, Q_r$ dei posti di F' che stanno sopra $P \in \mathbf{P}_F$. Allora per $1 \leq i, j \leq r$ si ha che*

$$e(Q_i|P) = e(Q_j|P)\ ,\quad f(Q_i|P) = f(Q_j|P)\ ,\quad d(Q_i|P) = d(Q_j|P)\ .$$

Dim. Fisso i e j. Sia t un uniformizzante per P e $\sigma \in G$ tale che $\sigma(Q_i) = Q_j$. Allora

$$e(Q_i|P) = \nu_{Q_i}(t) = \nu_{\sigma(Q_i)}\big(\sigma(t)\big) = \nu_{Q_j}(t) = e(Q_j|P)\ .$$

Dalla definizione di $\sigma(Q_i)$ ho che $\mathcal{O}_{\sigma(Q_i)} = \sigma(\mathcal{O}_{Q_i})$ e $\mathfrak{M}_{\sigma(Q_i)} = \sigma(\mathfrak{M}_{Q_i})$. Quindi

$$\mathcal{O}_{Q_j}/\mathfrak{M}_{Q_j} = \mathcal{O}_{\sigma(Q_i)}/\mathfrak{M}_{\sigma(Q_i)} = \sigma(\mathcal{O}_{Q_i})/\sigma(\mathfrak{M}_{Q_i}) \cong \mathcal{O}_{Q_i}/\mathfrak{M}_{Q_i}$$

e ciò implica che $f(Q_i|P) = f(Q_j|P)$.
Sia $\mathcal{T} = \{Q_1, Q_2, \ldots, Q_r\}$ l'insieme dei posti di F' che stanno in P. Allora $\mathfrak{D}_P(F'/F)$ assume la forma

$$\mathfrak{D}_P(F'/F) = \prod_{h=1}^{r}\mathfrak{M}_{Q_h}(\mathcal{T})^{d(Q_h|P)}\ .$$

Dunque

$$\sigma\big(\mathfrak{D}_P(F'/F)\big) = \prod_{h=1}^{r} \sigma\big(\mathfrak{M}_{Q_h}(\mathcal{T})\big)^{d(Q_h|P)} .$$

Per la definizione di codifferente ho che

$$\sigma\big(\mathfrak{D}_P(F'/F)\big) = \mathfrak{D}_P(F'/F)$$

e per l'unicità della decomposizione degli ideali ottengo

$$d(Q_j|P) = d\big(\sigma(Q_i|P)\big) = d(Q_i|P) .$$

□

Posso riscrivere la proposizione 1.6.1 come segue:

Corollario 1.7.4 *Si supponga che F'/F sia un'estensione di Galois finita e che ci sono esattamente r posti di F' che stanno sopra ad un posto P di F. Allora*

$$e_P(F'/F) f_P(F'/F) r = [F' : F] .$$

In particolare $e_P(F'/F)$ ed $f_P(F'/F)$ dividono $[F' : F]$.

Se $e_P(F'/F) > 1$ si dice che F'/F è **ramificata** per P (o che P è **ramificato** in F'/F). Invece si dice che F'/F è **non-ramificata** per P (o che P è **non-ramificato** in F'/F) se $e_P(F'/F) = 1$. Inoltre, se $e_P(F'/F) > 1$ si dice che P è **moderatamente ramificato** in F'/F se $e_P(F'/F)$ non è divisibile per la caratteristica di k e che P è **ramificato in maniera selvaggia** in F'/F se $e_P(F'/F)$ è divisibile per la caratteristica di k.

Definizione 1.7.5 Sia Q un posto di F' che sta sopra $P \in \mathbf{P}_F$. Per ogni intero $i \geq -1$ si definisce l'i-esimo **gruppo di ramificazione** come

$$\begin{aligned} G_i(Q|P) = G_i(Q, F'/F) &:= \{\sigma \in G \mid \nu_Q(\sigma(x) - x) \geq i + 1 \text{ per ogni } x \in \mathcal{O}_Q\} \\ &= \big\{\sigma \in G \mid (\sigma - \mathrm{id})(\mathcal{O}_Q) \subseteq \mathfrak{M}_Q^{i+1}\big\} . \end{aligned}$$

Il sottocampo F_i di F'/F fissato da $G_i(Q|P)$ è chiamato i-esimo **campo di ramificazione**. In particolare i gruppi $G_{-1}(Q|P)$ e $G_0(Q|P)$ sono chiamati rispettivamente **gruppo di decomposizione** e **gruppo d'inerzia** di Q sopra P e vengono denotati rispettivamente con $G_Z(Q|P)$ e $G_T(Q|P)$. I corrispondenti campi di ramificazione $F_{-1} =: Z$ e $F_0 =: T$ sono chiamati rispettivamente **campo di decomposizione** e **campo d'inerzia** di Q sopra P.

Si osservi che il gruppo di decomposizione $G_Z(Q|P)$ può essere descritto anche come

$$G_Z(Q|P) = \{\sigma \in G \mid \sigma(Q) = Q\} . \tag{1.5}$$

Proposizione 1.7.6 *Se Q_1 e Q_2 sono due posti di F' che stanno sopra $P \in \mathbf{P}_F$ allora $G_i(Q_1|P)$ e $G_i(Q_2|P)$ sono coniugati per $i \geq -1$. Più precisamente*

$$G_i\big(\sigma(Q)|P\big) = \sigma G_i(Q|P)\sigma^{-1}$$

per ogni $\sigma \in G$ e $Q|P$.

Dim. Si noti che

$$\begin{aligned}
\tau \in G_i\big(\sigma(Q)|P\big) &\iff (\tau - \mathrm{id})(\mathcal{O}_{\sigma(Q)}) \subseteq \mathfrak{M}_{\sigma(Q)}^{i+1} \\
&\iff (\tau - \mathrm{id})\big(\sigma(\mathcal{O}_Q)\big) \subseteq \sigma(\mathfrak{M}_Q^{i+1}) \\
&\iff (\sigma^{-1}\tau\sigma - \mathrm{id})(\mathcal{O}_Q) \subseteq \mathfrak{M}_Q^{i+1} \\
&\iff \sigma^{-1}\tau\sigma \in G_i(Q|P) \\
&\iff \tau \in \sigma G_i(Q|P)\sigma^{-1} \ .
\end{aligned}$$

□

Proposizione 1.7.7 *Sia Q un posto di F' che sta sopra $P \in \mathbf{P}_F$ e sia Z il campo di decomposizione di Q sopra P. Sia R un posto di Z tale che $Q|R$. Allora si ha che*

(i) $[F' : Z] = |G_Z(Q|P)| = e(Q|P)f(Q|P)$;

(ii) $e(R|P) = f(R|P) = 1$, *i.e. P si separa completamente in Z/F;*

(iii) *Q è l'unico posto di F' che sta sopra R.*

Dim. (i) Poiché G agisce transitivamente sull'insieme dei posti di F' che stanno sopra P, posso trovare $\sigma_1, \sigma_2, \ldots, \sigma_r \in G$ tali che $\{\sigma_1(Q), \sigma_2(Q), \ldots, \sigma_r(Q)\}$ sia l'insieme di tutti i posti di F' che stanno sopra P. Dalla (1.5) ho che $\sigma(Q) = Q$ per ogni $\sigma \in G_Z(Q|P)$. Quindi $\sigma_1, \sigma_2, \ldots, \sigma_r$ rappresentano le classi laterali sinistre di $G_Z(Q|P)$. Per ogni $\tau \in G$ ho che $\tau(Q) = \sigma_i(Q)$ per qualche $1 \le i \le r$. Allora $\tau^{-1}\sigma_i(Q) = Q$. Segue dalla definizione di gruppo di decomposizione che $\tau^{-1}\sigma_i \in G_Z(Q|P)$, i.e. τ e σ_i stanno nella stessa classe laterale sinistra di $G_Z(Q|P)$. Dunque ho provato che

$$\frac{|G|}{|G_Z(Q|P)|} = r \ ,$$

i.e.

$$|G_Z(Q|P)| = \frac{[F' : F]}{r} = e(Q|P)f(Q|P) \ .$$

(ii) Il gruppo di decomposizione di Q sopra R è ovviamente uguale a $\mathrm{Gal}(F'/Z)$. Per (i) si ha che

$$e(Q|R)f(Q|R) = e(Q|P)f(Q|P)$$

e quindi

$$e(R|P)f(R|P) = \frac{e(Q|P)}{e(Q|R)} \cdot \frac{f(Q|P)}{f(Q|R)} = 1 \ .$$

Questo equivale a dire che $e(R|P) = f(R|P) = 1$.
(iii) Segue direttamente da (i) e da (ii). □

L'esponente differente per un posto è determinato dall'ordine dei propri gruppi di ramificazione.

Teorema 1.7.8 (Formula di Hilbert) *Sia F'/F un'estensione di Galois finita e sia $G_i(Q|P)$ l'i-esimo gruppo di ramificazione di un posto Q di F' che sta sopra $P \in \mathbf{P}_F$. Allora l'esponente differente di Q sopra P è dato da*

$$d(Q|P) = \sum_{i=0}^{\infty} \big(|G_i(Q|P)| - 1\big) \ .$$

Poiché k è finito, per ogni $P \in \mathbf{P}_F$ una qualsiasi estensione del campo di classe dei residui di P è un'estensione di Galois.
Si è visto nella dimostrazione del teorema 1.7.3 che per ogni $\sigma \in G$ c'è un isomorfismo

$$\mathcal{O}_Q/\mathfrak{M}_Q \cong \mathcal{O}_{\sigma(Q)}/\mathfrak{M}_{\sigma(Q)} ,$$

dove Q è un qualsiasi posto di F'. Più precisamente c'è un isomorfismo

$$\overline{\sigma} : \tilde{F}'_Q \to \tilde{F}'_{\sigma(Q)} , \ \overline{z} \mapsto \overline{\sigma}(\overline{z}) = \overline{\sigma(z)}$$

per ogni $z \in \mathcal{O}_Q$. Tale isomorfismo induce un omomorfismo (di gruppi)

$$\mathrm{Gal}(F'/F) \to \mathrm{Gal}(\tilde{F}'_Q/\tilde{F}_P) , \ \sigma \mapsto \overline{\sigma} .$$

Proposizione 1.7.9 *Sia Q un posto di F' che sta sopra $P \in \mathbf{P}_F$ e sia Z il campo di decomposizione di Q sopra P. Allora l'omomorfismo*

$$\mathrm{Gal}(F'/Z) \to \mathrm{Gal}(\tilde{F}'_Q/\tilde{F}_P) , \ \sigma \mapsto \overline{\sigma}$$

è suriettivo. Inoltre $G_T(Q|P)$ è il nucleo di tale omomorfismo e quindi un sottogruppo normale di $G_Z(Q|P)$.

Dim. Sia $z \in \mathcal{O}_Q$ tale che $\tilde{F}'_Q = \tilde{F}_P(\overline{z})$. Sia $R \in \mathbf{P}_Z$ tale che Q stia sopra R. Allora $\mathcal{O}_Q$ è la chiusura intera di $\mathcal{O}_R$ in F' perché Q è il solo posto che sta sopra R, in accordo con la proposizione 1.7.7. Dunque esiste un polinomio monico $f(x) \in \mathcal{O}_R[x]$ che è anche il polinomio minimo di z su Z.
Qualsiasi elemento μ di $\mathrm{Gal}(\tilde{F}'_Q/\tilde{F}_P)$ è univocamente determinato da $\mu(\overline{z})$. Ma $\mu(\overline{z})$ è uno zero di $\overline{f}(x) \in \tilde{Z}_R[x] = \tilde{F}_P[x]$, quindi esiste $\sigma \in \mathrm{Gal}(F'/Z)$ tale che $\overline{\sigma(z)} = \mu(\overline{z})$, e ciò implica $\overline{\sigma} = \mu$. Questo mostra che l'omomorfismo è suriettivo.
Per $\sigma \in \mathrm{Gal}(F'/Z)$ e per ogni $z \in \mathcal{O}_Q$ si ha che

$$\begin{aligned} \overline{\sigma} = \overline{\mathrm{id}} &\iff \overline{\sigma}(\overline{z}) = \overline{z} \\ &\iff \sigma(z) - z \in \mathfrak{M}_Q \\ &\iff (\sigma - \mathrm{id})(\mathcal{O}_Q) \subseteq \mathfrak{M}_Q \\ &\iff \sigma \in G_T(Q|P) . \end{aligned}$$

Questo prova che $G_T(Q|P)$ è il nucleo dell'omomorfismo. □

Sia P un posto non-ramificato in F'/F e Q un posto di F' che sta sopra P. Allora la proposizione 1.7.9 mi assicura l'esistenza di un isomorfismo

$$\mathrm{Gal}(F'/Z) \cong \mathrm{Gal}(\tilde{F}'_Q/\tilde{F}_P) .$$

I campi delle classi dei residui $\tilde{F}_P$ ed $\tilde{F}'_Q$ sono stati assunti finiti e quindi $\mathrm{Gal}(\tilde{F}'_Q/\tilde{F}_P)$ è ciclico. Dunque esiste un unico $\sigma \in \mathrm{Gal}(F'/Z)$ tale che $\overline{\sigma}$ sia il generatore canonico di $\mathrm{Gal}(\tilde{F}'_Q/\tilde{F}_P)$, i.e. $\overline{\sigma} : a \mapsto a^r$ per ogni $a \in \tilde{F}'_Q$, con $r = |\tilde{F}_P|$. Ovviamente σ soddisfa la proprietà

$$\sigma(z) \equiv z^r \pmod{\mathfrak{M}_Q} \quad \text{per ogni } z \in \mathcal{O}_Q . \tag{1.6}$$

Questo unico σ è chiamato **automorfismo di Frobenius** o **simbolo di Frobenius** di Q sopra P ed è denotato con $\left[\frac{F'/F}{Q}\right]$. Chiaramente $\left[\frac{F'/F}{Q}\right]$ è caratterizzato dalla (1.6). Inoltre, per ogni $\tau \in G$ si ha che

$$\left[\frac{F'/F}{\tau(Q)}\right] = \tau \left[\frac{F'/F}{Q}\right] \tau^{-1} .$$

Quindi se F'/F è un'estensione abeliana (si veda l'appendice A), allora il simbolo di Frobenius non dipende da Q ma solo dal posto P di F al quale Q sta sopra. In questo caso il simbolo di Frobenius viene indicato con $\left[\frac{F'/F}{P}\right]$ ed è chiamato **simbolo di Artin** di P in F'/F.

Proposizione 1.7.10 *Sia F'/F un'estensione abeliana finita e sia E un sottocampo di F'/F. Si supponga che F'/F sia non-ramificata per $P \in \mathbf{P}_F$. Allora P è completamente separato in E/F se e solo se il simbolo di Artin di P in F'/F sta in* $\mathrm{Gal}(F'/E)$.

1.8 Campi di funzioni e curve algebriche

Gli argomenti di questo paragrafo, che riguardano le curve algebriche ed il legame con i loro campi di funzioni, sono solo enunciati. Un'esposizione completa di dimostrazioni si può trovare in [Har] ed in [Sil]. Tutte le nozioni base invece si possono trovare nell'appendice B.

Definizione 1.8.1 Una varietà proiettiva (affine) di dimensione 1 definita su $\mathbb{F}_q$ è chiamata **curva (algebrica) proiettiva (affine)**[3] su $\mathbb{F}_q$.

Poiché verranno trattate sostanzialmente solo curve proiettive assolutamente irriducibili lisce, mi riferirò a loro chiamandole semplicemente **curve**, specificando altrimenti.

Per una curva $\mathcal{X}/\mathbb{F}_q$ ed un punto P di $\mathcal{X}$, l'anello locale $\overline{\mathbb{F}}_q[\mathcal{X}]_P$ è un anello di valutazione discreta di $\overline{\mathbb{F}}_q(\mathcal{X})$ ed il suo unico ideale massimale $\overline{\mathfrak{M}}_P$ è un posto di $\overline{\mathbb{F}}_q(\mathcal{X})$. L'intersezione $\overline{\mathbb{F}}_q[\mathcal{X}]_P \cap \mathbb{F}_q(\mathcal{X})$ è ancora un anello di valutazione discreta di $\mathbb{F}_q(\mathcal{X})$ e l'intersezione $\overline{\mathfrak{M}}_P \cap \mathbb{F}_q(\mathcal{X})$ è un posto di grado m di $\mathbb{F}_q(\mathcal{X})$, dove m è il grado della $\mathbb{F}_q$-orbita di $\mathcal{X}$ contenente P (si consulti l'appendice).

Un **morfismo** fra due curve $\mathcal{X}$ e $\mathcal{Y}$ è un'applicazione razionale

$$\phi : \mathcal{X} \to \mathcal{Y}$$

regolare in ogni punto (si veda l'appendice B).

Definizione 1.8.2 Un'**isogenia** fra due curve $\mathcal{X}$ e $\mathcal{Y}$ è un morfismo suriettivo con nucleo finito. Un'isogenia fra due curve $\mathcal{X}$ e $\mathcal{Y}$ è indicata con $\mathcal{X} \sim \mathcal{Y}$.

Il seguente risultato descrive la relazione tra le curve e i campi di funzioni.

Teorema 1.8.3 *L'applicazione $\delta : \mathcal{X}/\mathbb{F}_q \mapsto \mathbb{F}_q(\mathcal{X})$ induce una naturale corrispondenza fra le classi di isomorfismi di curve su $\mathbb{F}_q$ ed i campi di funzioni (di una variabile) con campo completo delle costanti $\mathbb{F}_q$.*

Le classi di isomorfismi citate nel teorema 1.8.3 derivono dalla conoscenza del noto risultato che due curve su $\mathbb{F}_q$ sono $\mathbb{F}_q$-isomorfe se e solo se i loro campi di funzioni sono $\mathbb{F}_q$-isomorfi. L'applicazione δ del teorema 1.8.3 induce anche una corrispondenza fra le $\mathbb{F}_q$-orbite di $\mathcal{X}$ ed i posti di $\mathbb{F}_q(\mathcal{X})$:

[3] Verranno considerate solo curve irriducibili.

Teorema 1.8.4 *Sia $\mathcal{X}/\mathbb{F}_q$ una curva. Allora:*

(i) *δ induce una corrispondenza $P \in \mathcal{X} \mapsto \overline{\mathfrak{M}}_P$ tra i punti di $\mathcal{X}$ ed i posti di $\overline{\mathbb{F}}_q(\mathcal{X})$.*

(ii) *Se $\mathcal{P}$ è una $\mathbb{F}_q$-orbita di $\mathcal{X}$ e P_1, P_2 sono due punti di $\mathcal{P}$ allora*

$$\overline{\mathfrak{M}}_{P_1} \cap \mathbb{F}_q(\mathcal{X}) = \overline{\mathfrak{M}}_{P_2} \cap \mathbb{F}_q(\mathcal{X})$$

è un posto di grado $\deg(\mathcal{P})$ di $\mathbb{F}_q(\mathcal{X})$. Dunque δ induce una corrispondenza biunivoca fra le $\mathbb{F}_q$-orbite di grado m di $\mathcal{X}/\mathbb{F}_q$ ed i posti di grado m di $\mathbb{F}_q(\mathcal{X})$ per ogni $m \geq 1$. In particolare δ induce una corrispondenza biunivoca fra i punti razionali di $\mathcal{X}/\mathbb{F}_q$ ed i posti razionali di $\mathbb{F}_q(\mathcal{X})$.

È importante osservare che grazie alla corrispondenza δ data nel teorema 1.8.3 è possibile associare alla curva $\mathcal{X}/\mathbb{F}_q$ un genere $g(\mathcal{X})$ che è ancora un intero non negativo. Inoltre, date due curve $\mathcal{X}$ e $\mathcal{Y}$ su $\mathbb{F}_q$ che corrispondono allo stesso campo di funzioni $F/\mathbb{F}_q$ di genere $g(F)$, allora $g(F) = g(\mathcal{X}) = g(\mathcal{Y})$.

Per questi motivi, quando in seguito definirò delle caratteristiche dei campi di funzioni, tali definizioni si intenderanno naturalmente estese anche alle loro curve associate. In analogia con i campi di funzioni quindi si ha che un **divisore** di $\mathcal{X}$ è una serie formale del tipo

$$D := \sum_{P \in \mathcal{X}} n_P P \ ,$$

dove gli n_P sono degli interi quasi tutti nulli. Il **grado** di D è definito come

$$\deg(D) = \sum_{P \in \mathcal{X}} n_P \ .$$

I divisori di $\mathcal{X}$ formano un gruppo additivo, $\mathrm{Div}(\mathcal{X})$, chiamato **gruppo di divisori**.
Un **divisore principale** (f) di una funzione razionale non nulla $f \in \overline{\mathbb{F}}_q(\mathcal{X})$ è definito come

$$(f) := \sum_{P \in \mathcal{X}} \nu_P P \ ,$$

dove ν_P è la valutazione discreta di $\overline{\mathbb{F}}_q(\mathcal{X})$ corrispondente all'anello di valutazione $\overline{\mathbb{F}}_q[\mathcal{X}]_P$ e $\nu_P(f)$ indica l'**ordine** di f per P. Il grado dei divisori principali è 0. I divisori principali formano un sottogruppo $\mathrm{Princ}(\mathcal{X})$ del gruppo dei divisori $\mathrm{Div}(\mathcal{X})$ ed il gruppo quoziente $\mathrm{Pic}(\mathcal{X}) := \mathrm{Div}(\mathcal{X})/\mathrm{Princ}(\mathcal{X})$ è chiamato **gruppo delle classi dei divisori** di $\mathcal{X}$ o **gruppo di Picard** di $\mathcal{X}$.

Definizione 1.8.5 Sia $\mathcal{X}/\mathbb{F}_q$ una curva. Il gruppo quoziente

$$\mathrm{Jac}(\mathcal{X}) := \mathrm{Div}^0(\mathcal{X})/\mathrm{Princ}(\mathcal{X}) \ ,$$

dove $\mathrm{Div}^0(\mathcal{X})$ indica il gruppo dei divisori di grado 0, è chiamato **jacobiana** di $\mathcal{X}$.

Si osservi che la jacobiana di una curva $\mathcal{X}$ è una varietà abeliana di dimensione pari al genere di $\mathcal{X}$.

Capitolo 2

La funzione zeta

In tutto il capitolo verranno trattati solamente campi di funzioni $F/\mathbb{F}_q$ su campi finiti con $q = p^n$ elementi, dove p è la caratteristica di $\mathbb{F}_q$ ed $n \geq 1$.

2.1 Estensioni di campi finiti

Per ogni $m \geq 1$ considero l'estensione

$$F^{(m)} = F \cdot \mathbb{F}_{q^m} .$$

Sia $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$. Allora $F^{(m)} = F(\alpha)$. Il gruppo di Galois $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ è ciclico con generatore

$$\sigma : \beta \mapsto \beta^q \quad \text{per ogni} \quad \beta \in \mathbb{F}_{q^m} .$$

Lemma 2.1.1 *Sia $F/\mathbb{F}_q$ un campo di funzioni con campo completo delle costanti $\mathbb{F}_q$. Usando le notazioni precedenti si ha che*

(i) *$F^{(m)}/F$ è un'estensione ciclica (vedere l'appendice A) di grado $[F^{(m)} : F] = m$ e*

$$\mathrm{Gal}(F^{(m)}/F) \cong \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) .$$

(ii) *Il campo completo delle costanti di $F^{(m)}$ è $\mathbb{F}_{q^m}$.*

(iii) *Sia $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ una base di $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$. Allora $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ è una base P-intera di $F^{(m)}/F$ per ogni $P \in \mathbf{P}_F$.*

Dim. (i) Sia $f(x) \in \mathbb{F}_q[t]$ il polinomio minimo di α su $\mathbb{F}_q$. Intendo provare che f è irriducibile su F. Suppongo per assurdo che f si fattorizzi su F come $f = gh$, dove g ed h sono polinomi monici di grado $\deg(g), \deg(h) \geq 1$. Chiaramente tutte le radici di g e di h sono elementi di $\mathbb{F}_{q^m}$. Quindi posso dire che g ed h sono polinomi in $\mathbb{F}_{q^m}[t]$; in particolare i coefficienti di g ed h sono algebrici su $\mathbb{F}_q$. Dunque, poiché $\mathbb{F}_q$ è algebricamente chiuso in F, i coefficienti di g ed h sono elementi di $\mathbb{F}_q$. Ma questo contraddice l'irriducibilità di f su $\mathbb{F}_q$. Questo prova che $[F^{(m)} : F] = m$ e che $\mathrm{Gal}(F^{(m)}/F) \cong \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.
(ii) Poiché $\mathbb{F}_{q^m}/\mathbb{F}_q$ è un'estensione finita, il campo completo delle costanti di $F^{(m)}$ contiene

$\mathbb{F}_{q^m}$. Sia $z \in F^{(m)}$ un elemento algebrico su $\mathbb{F}_{q^m}$; allora $\mathbb{F}_{q^m}(z)/\mathbb{F}_q$ è un'estensione finita. Da (i) ho che

$$m = [F^{(m)} : F] = [F \cdot \mathbb{F}_{q^m}(z) : F] = [\mathbb{F}_{q^m}(z) : \mathbb{F}_q] \ ,$$

quindi $\mathbb{F}_{q^m} = \mathbb{F}_{q^m}(z)$, i.e. $z \in \mathbb{F}_{q^m}$. Dunque $\mathbb{F}_{q^m}$ è il campo completo delle costanti di $F^{(m)}$.
(iii) Chiaramente $\alpha_1, \alpha_2, \ldots, \alpha_m$ sono elementi di $\mathcal{O}_\mathcal{T}$, dove $\mathcal{T}$ è il sopra-insieme di $\mathcal{S} = \{P\}$ rispetto ad $F^{(m)}/F$. Poiché il discriminante $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_m)$ di $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ è un elemento di $\mathbb{F}_q^*$ si ha che

$$\nu_P\big(\Delta(\alpha_1, \alpha_2, \ldots, \alpha_m)\big) = 0 \ .$$

la conclusione discende ora dalla [Wei, prop. 4-8-8]. □

Per il lemma 2.1.1 posso identificare $\mathrm{Gal}(F^{(m)}/F)$ con $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ nel modo seguente. Sia $\{\alpha_1 = 1, \alpha_2, \ldots, \alpha_m\}$ una base di $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$; allora per ogni $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ e per ogni $x = \sum_{i=1}^m \alpha_i x_i \in F^{(m)}$ con $x_i \in F$ posso porre

$$\sigma(x) = \sum_{i=1}^m \sigma(\alpha_i) x_i \ .$$

Allora σ è un automorfismo di Galois di $F^{(m)}/F$ e tutti gli elementi di $\mathrm{Gal}(F^{(m)}/F)$ sono ottenuti in questo modo.

Teorema 2.1.2 *Per un'estensione $F^{(m)}/F$ si ha che*

(i) *$F^{(m)}/F$ è non-ramificata per tutti i posti di F.*

(ii) *$F^{(m)}/\mathbb{F}_{q^m}$ ha lo stesso genere di $F/\mathbb{F}_q$.*

(iii) *Per un posto P di F ed un posto Q di $F^{(m)}$ che sta sopra P valgono le seguenti:*

  (a) $\deg(Q) = d/\mathrm{MCD}(d, m)$, *dove* $d = \deg(P)$;

  (b) $f(Q|P) = m/\mathrm{MCD}(d, m)$;

  (c) *Ci sono esattamente* $\mathrm{MCD}(d, m)$ *posti di $F^{(m)}$ che stanno sopra P.*

Dim. (i) Sia P un posto di F e sia $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ una base di $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$. Per il lemma 2.1.1(iii) e la sua dimostrazione ho che $\nu_P\big(\Delta(\alpha_1, \alpha_2, \ldots, \alpha_m)\big) = 0$ e che $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ è una base P-intera di $F^{(m)}/F$. Dal teorema del discriminante di Dedekind (si veda [Wei, teo. 4-8-14]) segue che P è non-ramificato in $F^{(m)}/F$.
(ii) È un'immediata conseguenza di (i) e della formula di Hurwitz (1.3).
(iii) Intendo come prima cosa mostrare che $\tilde{F}_Q^{(m)}$ è, a meno di isomorfismi, il campo $\tilde{F}_P \cdot \mathbb{F}_{q^m}$. Ovviamente $\tilde{F}_P \cdot \mathbb{F}_{q^m}$ può essere visto come sottocampo di $\tilde{F}_Q^{(m)}$. Sia ora $\mathcal{T}$ il sopra-insieme di $\{P\}$ rispetto ad $F^{(m)}/F$. Sia $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ una base di $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$. Per ogni elemento $x(Q) \in \tilde{F}_Q^{(m)}$ con qualche $x \in \mathcal{O}_\mathcal{T}$ (per il teorema di approssimazione 1.3.1), esistono m elementi $x_1, x_2, \ldots, x_m \in \mathcal{O}_P$ tali che

$$x = \sum_{i=1}^m x_i \alpha_i \ .$$

Questo perché $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ è una base P-intera di $F^{(m)}/F$. Quindi

$$x(Q) = \sum_{i=1}^{m} x_i(Q)\alpha_i = \sum_{i=1}^{m} x_i(P)\alpha_i \in \tilde{F}_P \cdot \mathbb{F}_{q^m} \ ,$$

e questo mostra che $\tilde{F}_Q^{(m)} = \tilde{F}_P \cdot \mathbb{F}_{q^m}$. Ma allora

$$\deg(Q) = \left[\tilde{F}_Q^{(m)} : \mathbb{F}_{q^m}\right] = \left[\tilde{F}_P \cdot \mathbb{F}_{q^m} : \mathbb{F}_{q^m}\right] = \left[\mathbb{F}_{q^d} \cdot \mathbb{F}_{q^m} : \mathbb{F}_{q^m}\right] = \frac{d}{\mathrm{MCD(d,m)}} \ .$$

Inoltre ho che

$$f(Q|P) = \left[\tilde{F}_Q^{(m)} : \tilde{F}_P\right] = \left[\tilde{F}_P \cdot \mathbb{F}_{q^m} : \tilde{F}_P\right] = \left[\mathbb{F}_{q^d} \cdot \mathbb{F}_{q^m} : \mathbb{F}_{q^d}\right] = \frac{m}{\mathrm{MCD(d,m)}} \ .$$

Poiché per (i) si ha $e(Q|P) = 1$ è chiaro che ci sono esattamente $\mathrm{MCD}(d, m)$ posti di $F^{(m)}$ che stanno sopra P. □

Dal teorema segue che per un posto $P \in \mathbf{P}_F$ di grado $\deg(P) = d$ e per un posto Q di $F^{(m)}$ che sta sopra P, il gruppo di decomposizione $G_Z(Q|P)$ è isomorfo a $\mathrm{Gal}(\mathbb{F}_{q^d} \cdot \mathbb{F}_{q^m}/\mathbb{F}_{q^d})$ e l'i-esimo gruppo di ramificazione di Q sopra P è banale per $i \geq 0$.

2.2 Il teorema di Weil

Proposizione 2.2.1 *Un campo di funzioni $F/\mathbb{F}_q$ ha un numero finito di posti razionali.*

Dim. Scelgo un elemento $x \in F \setminus \mathbb{F}_q$. Allora $F/\mathbb{F}_q(x)$ è un'estensione finita. Tutti i posti razionali di F stanno sopra ai posti razionali di $\mathbb{F}_q(x)$. Per ogni posto razionale P di $\mathbb{F}_q(x)$ esistono al più $[F : \mathbb{F}_q(x)]$ posti razionali che stanno sopra P. Inoltre per il corollario 1.2.3 esistono esattamente $q + 1$ posti razionali di $\mathbb{F}_q(x)$. Quindi il numero dei posti razionali di F è al più $(q + 1)[F : \mathbb{F}_q(x)]$. □

Indico con N_m il numero dei posti razionali di $F^{(m)}/\mathbb{F}_{q^m}$ il quale è finito per la proposizione 2.2.1. Un posto razionale di $F^{(m)}/\mathbb{F}_{q^m}$ è detto essere un **posto $\mathbb{F}_{q^m}$-razionale** di F. Per ogni intero $d \geq 1$ denoto il numero dei posti di F di grado d con B_d. Per il teorema 2.1.2 un posto di F di grado d si separa in posti razionali di $F^{(m)}$ se e solo se d divide m. Nel caso in cui d divide m un posto di F di grado d si separa in esattamente d posti razionali di $F^{(m)}$. Dunque sussiste la relazione

$$N_m = \sum_{d|m} dB_d \ . \tag{2.1}$$

Definizione 2.2.2 La **funzione zeta** di $F/\mathbb{F}_q$ è definita come la serie di potenze formali

$$Z(F, t) = Z(t) := \exp\Big(\sum_{m=1}^{\infty} \frac{N_m}{m} t^m\Big) \in \mathbb{C}[[t]] \ .$$

Esempio 2.2.3 Calcolo la funzione zeta del campo delle funzioni razionali su $\mathbb{F}_q$. Poiché il numero dei posti $\mathbb{F}_{q^m}$-razionali del campo delle funzioni razionali è $q^m + 1$ per ogni $m \geq 1$

ho che

$$\begin{aligned}\log\big(Z(t)\big) &= \sum_{m=1}^{\infty}\frac{q^m+1}{m}t^m = \sum_{m=1}^{\infty}\frac{(qt)^m}{m}+\sum_{m=1}^{\infty}\frac{t^m}{m}\\ &= -\log(1-qt)-\log(1-t) = \log\frac{1}{(1-t)(1-qt)}\,,\end{aligned}$$

i.e.

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

Teorema 2.2.4 *La funzione zeta di $F/\mathbb{F}_q$ può essere rappresentata anche come segue:*

(i)
$$Z(t) = \prod_{P\in\mathbf{P}_F}\big(1-t^{\deg(P)}\big)^{-1}\,;$$

(ii)
$$Z(t) = \sum_{m=0}^{\infty}A_m t^m\,,$$

dove A_m è il numero dei divisori effettivi di F di grado m.

Dim. (i) Ho che

$$\begin{aligned}\log\Big(\prod_{P\in\mathbf{P}_F}\big(1-t^{\deg(P)}\big)^{-1}\Big) &= \log\big(\prod_{d=1}^{\infty}(1-t^d)^{-B_d}\big)\\ &= \sum_{d=1}^{\infty}(-B_d)\log(1-t^d) = \sum_{d=1}^{\infty}B_d\sum_{d=1}^{\infty}\frac{t^{dm}}{m}\\ &= \sum_{m=1}^{\infty}\sum_{d|m}\frac{dB_d t^m}{m} = \sum_{m=1}^{\infty}\frac{N_m}{m}t^m\,.\end{aligned}$$

Quindi

$$Z(t) = \exp\big(\sum_{m=1}^{\infty}\frac{N_m}{m}t^m\big) = \prod_{P\in\mathbf{P}_F}\big(1-t^{\deg(P)}\big)^{-1}\,.$$

(ii) Da (i) ho che

$$\begin{aligned}Z(t) &= \prod_{P\in\mathbf{P}_F}\big(1-t^{\deg(P)}\big)^{-1} = \prod_{P\in\mathbf{P}_F}\sum_{m=0}^{\infty}t^{\deg(mP)}\\ &= \sum_{A\in\mathrm{Div}(F),\ A\geq 0}t^{\deg(A)} = \sum_{m=0}^{\infty}A_m t^m\,.\end{aligned}$$

□

Definizione 2.2.5 Sia $F/\mathbb{F}_q$ un campo di funzioni ed m un intero positivo. L'm**-esima funzione zeta** $Z_m(t)$ di $F/\mathbb{F}_q$ è definita come la funzione zeta di $F\cdot\mathbb{F}_{q^m}/\mathbb{F}_{q^m}$.

C'è una stretta relazione fra $Z_m(t)$ e $Z(t) = Z_1(t)$.

Proposizione 2.2.6 *Per ogni intero positivo m si ha che*

$$Z_m(t^m) = \prod_{\zeta^m=1} Z(\zeta t) \ ,$$

dove il prodotto è esteso a tutte le radici m-esime dell'unità.

Dim. Pongo $F^{(m)} = F \cdot \mathbb{F}_{q^m}$. Per il teorema 2.2.4

$$\begin{aligned} Z_m(t^m) &= \prod_{Q \in \mathbf{P}_{F^{(m)}}} \left(1 - t^{m\deg(Q)}\right)^{-1} \\ &= \prod_{P \in \mathbf{P}_F} \prod_{Q|P} \left(1 - t^{m\deg(Q)}\right)^{-1} . \end{aligned}$$

Sia P un fissato posto di F. Dal teorema 2.1.2 ho che il grado dei posti di $F^{(m)}$ che stanno sopra P è $l := d/\mathrm{MCD(d, m)}$ e che ci sono esattamente d/l posti di $F^{(m)}$ che stanno sopra P. Quindi

$$\begin{aligned} \prod_{Q|P} \left(1 - t^{m\deg(Q)}\right)^{-1} &= \left(1 - t^{ml}\right)^{-d/l} = \prod_{\zeta^m=1} \left(1 - (\zeta t)^d\right)^{-1} \\ &= \prod_{\zeta^m=1} \left(1 - (\zeta t)^{\deg(P)}\right)^{-1} . \end{aligned}$$

Dunque

$$Z_m(t^m) = \prod_{\zeta^m=1} \prod_{P \in \mathbf{P}_F} \left(1 - (\zeta t)^{\deg(P)}\right)^{-1} = \prod_{\zeta^m=1} Z(\zeta t) \ .$$

□

Enuncio solamente il seguente importante teorema che è stato provato da A. Weil.

Teorema 2.2.7 *Sia $F/\mathbb{F}_q$ un campo di funzioni di genere g. Allora*

(i) *$Z(F, t)$ è una funzione razionale della forma*

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

dove $L(F, t) \in \mathbb{Z}[t]$ è un polinomio di grado $2g$ a coefficenti interi ed $L(F, 0) = 1$. Inoltre $L(F, 1)$ è uguale al numero delle classi dei divisori $h(F)$ di F.

(ii) *Il polinomio $L(F, t)$ si fattorizza nella forma*

$$L(F, t) = \prod_{i=1}^{2g} (1 - \omega_i t) \in \mathbb{C}[t] \ ,$$

dove gli ω_i sono tali che $|\omega_i| = q^{1/2}$ per ogni $1 \leq i \leq 2g$.

Ci sono diversi modi per dimostrare il teorema. Una dimostrazione elementare, dovuta a Bombieri, è presente in [Sti2]; il metodo che fa uso della coomologia l-adica si può trovare in [F-K].

Definizione 2.2.8 Il polinomio $L(F,t) = L(t) := (1-t)(1-qt)Z(F,t)$ è chiamato **polinomio** L di $F/\mathbb{F}_q$. Per un intero positivo m, il polinomio L di $F \cdot \mathbb{F}_{q^m}/\mathbb{F}_{q^m}$ è chiamato **m-esimo polinomio** L di $F/\mathbb{F}_q$ ed è denotato con $L_m(t)$, i.e.

$$L_m(t) = (1-t)(1-q^m t)Z_m(t) \; .$$

Corollario 2.2.9 *Per il polinomio L di $F/\mathbb{F}_q$ valgono i seguenti risultati:*

(i)
$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right) \quad (equazione\ funzionale) \; ;$$

(ii) *Se $L(t) = a_0 + a_1 t + \cdots + a_{2g}t^{2g} \in \mathbb{Z}[t]$ allora $a_{2g-i} = q^{g-i}a_i$ per ogni $0 \leq i \leq g$;*

(iii) *Se $L(t) = \prod_{i=1}^{2g}(1-\omega_i t)$ allora*
$$L_m(t) = \prod_{i=1}^{2g}(1-\omega_i^m t) \; .$$

Dim. (i) Se $L(t) = \prod_{i=1}^{2g}(1-\omega_i t)$ allora q/ω_i è il complesso coniugato di ω_i e quindi il reciproco di uno zero di $L(t)$ per ogni $1 \leq i \leq 2g$. Quindi
$$L(t) = \prod_{i=1}^{2g}(1-\frac{q}{\omega_i}t) = q^g t^{2g} L\left(\frac{1}{qt}\right) \; .$$

(ii) Da (i) ho che
$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right) = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}}t + \cdots + q^g a_0 t^{2g} \; .$$

(iii) Per la proposizione 2.2.6 ho che
$$\begin{aligned} L_m(t^m) &= (1-t^m)(1-q^m t^m)Z_m(t^m) \\ &= (1-t^m)(1-q^m t^m)\prod_{\zeta^m=1} Z(\zeta t) \\ &= (1-t^m)(1-q^m t^m)\prod_{\zeta^m=1} \frac{L(\zeta t)}{(1-\zeta t)(1-\zeta q t)} \\ &= \prod_{\zeta^m=1} L(\zeta t) = \prod_{\zeta^m=1}\prod_{i=1}^{2g}(1-\omega_i \zeta t) \\ &= \prod_{i=1}^{2g}\prod_{\zeta^m=1}(1-\omega_i\zeta t) = \prod_{i=1}^{2g}(1-\omega_i^m t^m) \; . \end{aligned}$$

Quindi
$$L_m(t) = \prod_{i=1}^{2g}(1-\omega_i^m t) \; .$$

□

Corollario 2.2.10 *Siano* $1/\omega_1, 1/\omega_2, \ldots, 1/\omega_{2g}$ *gli zeri del polinomio* L *di* $F/\mathbb{F}_q$ *ed* $L(t) = \sum_{i=0}^{2g} a_i t^i$. *Allora il numero dei posti razionali* $N(F)$ *di* $F/\mathbb{F}_q$ *è uguale a*

$$N(F) = N_1 = q + 1 - \sum_{i=1}^{2g} \omega_i = q + 1 + a_1 \ .$$

In generale il numero N_m *dei posti* $\mathbb{F}_{q^m}$*-razionali di* $F/\mathbb{F}_q$ *è uguale a*

$$N_m = q^m + 1 - \sum_{i=1}^{2g} \omega_i^m \ ,$$

per ogni $m \geq 1$.

Dim. Per la definizione di $Z_m(t)$ ho che

$$N_m = \frac{d}{dt}\Big(\log\big(Z_m(t)\big)\Big)|_{t=0} \ . \tag{2.2}$$

Per il teorema 2.2.7(i) ho che

$$\frac{d}{dt}\Big(\log\big(Z_m(t)\big)\Big)|_{t=0} = \Big(\frac{L'(t)}{L(t)} + \frac{1}{1-t} + \frac{q}{1-qt}\Big)|_{t=0} = a_1 + 1 + q \ . \tag{2.3}$$

Combinando (2.2) con (2.3) ottengo

$$N_1 = q + 1 + a_1 = q + 1 - \sum_{i=1}^{2g} \omega_i \ .$$

Per il corollario 2.2.9(iii), $\omega_1^m, \omega_2^m, \ldots, \omega_{2g}^m$ sono il reciproco degli zeri dell'm-esimo polinomio L. Quindi

$$N_m = q^m + 1 - \sum_{i=1}^{2g} \omega_i^m \ .$$

□

2.3 Limiti superiori per il numero di posti razionali

Per i posti di grado $d \geq 2$ di un campo di funzioni $F/\mathbb{F}_q$ ho la seguente condizione di esistenza:

Proposizione 2.3.1 *Sia* $F/\mathbb{F}_q$ *un campo di funzioni di genere* g. *Si supponga che per qualche intero* $d \geq 2$ *si abbia*

$$q^d - 2gq^{d/2} > \sum_{n|d\,,\ n<d} (q^n + 2gq^{n/2}) \ .$$

Allora esiste almeno un posto di F *di grado* d.

Dim. Siano $\omega_1, \omega_2, \ldots, \omega_{2g}$ i reciproci degli zeri del polinomio L di F. Per $n \geq 1$ sia B_n il numero dei posti di grado n. Allora per il corollario 2.2.10 ho che

$$B_d = \frac{1}{d} \sum_{n|d} \mu\left(\frac{d}{n}\right) \left(q^n - \sum_{i=1}^{2g} \omega_i^n\right)$$

per $d \geq 2$, dove μ è la funzione di Möbius (si veda [Jac, p.151] p. 151). Quindi, per il teorema 2.2.7(ii) ottengo

$$B_d \geq \frac{1}{d}\Big(q^d - 2gq^{d/2} - \sum_{n|d\,,\, n<d} \left(q^n + 2gq^{n/2}\right)\Big) > 0\ .$$

□

Definizione 2.3.2 Per una fissata potenza q di un numero primo ed un intero $g \geq 0$ denoto con $N_q(g)$ il massimo numero di posti razionali che può avere un campo di funzioni $F/\mathbb{F}_q$ di genere g.

Definizione 2.3.3 Un campo di funzioni $F/\mathbb{F}_q$ di genere g è detto **ottimale** se il suo numero di posti razionali $N(F)$ è uguale a $N_q(g)$.

Teorema 2.3.4 (Limite di Hasse-Weil) *Sia $F/\mathbb{F}_q$ un campo di funzioni di genere g. Il numero $N(F)$ di posti razionali di $F/\mathbb{F}_q$ soddisfa la relazione*

$$|N(F) - (q+1)| \leq 2gq^{1/2}\ .$$

Dim. Per il corollario 2.2.10 ed il teorema 2.2.7(ii) ottengo

$$|N(F) - (q+1)| = |\sum_{i=1}^{2g} \omega_i| \leq \sum_{i=1}^{2g} |\omega_i| = 2gq^{1/2}\ .$$

□

Definizione 2.3.5 Un campo di funzioni $F/\mathbb{F}_q$ di genere g è chiamato **massimale** se il suo numero di posti razionali $N(F)$ incontra il limite di Hasse-Weil, i.e. se

$$N(F) = q + 1 + 2gq^{1/2}\ .$$

Chiaramente un campo di funzioni massimale è ottimale. È ovvio che un campo di funzioni $F/\mathbb{F}_q$ è massimale solo se $g(F) = 0$ o q è un quadrato.

Il limite di Hase-Weil è attendibile solo quando il genere è relativamente piccolo rispetto a q (sarà chiarito nell'osservazione 2.3.8). Quando il genere è relativamente grande rispetto a q si possono usare dei limiti migliori, che ora vedremo.

Proposizione 2.3.6 (Limite di Serre) *Sia $F/\mathbb{F}_q$ un campo di funzioni di genere g. Allora il numero dei posti razionali $N(F)$ di $F/\mathbb{F}_q$ soddisfa*

$$|N(F) - (q+1)| \leq g[2q^{1/2}]\ , \tag{2.4}$$

dove $[x]$ indica la parte intera di $x \in \mathbb{R}$.

Dim. Pongo $r = [2q^{1/2}]$. Siano $\omega_1, \omega_2, \ldots, \omega_{2g}$ i reciproci degli zeri del polinomio L di $F/\mathbb{F}_q$, ordinati in modo che $\omega_{g+i} = \overline{\omega}_i$ per ogni $i = 1, 2, \ldots, g$. Pongo

$$\gamma_i := \omega_i + \omega_{g+i} + r + 1 = \omega_i + \overline{\omega}_i + r + 1 \, .$$

Allora $\gamma_i \geq r + 1 - |\omega_i + \overline{\omega}_i| \geq r + 1 - 2q^{1/2} > 0$ per ogni $i = 1, 2, \ldots, g$. Poiché $\omega_1, \omega_2, \ldots, \omega_{2g}$ sono gli zeri del polinomio monico $t^{2g}L(1/t) \in \mathbb{Z}[t]$, essi sono interi algebrici e così $\prod_{i=1}^{g} \gamma_i > 0$ è un intero, i.e.

$$\prod_{i=1}^{g} \gamma_i \geq 1 \, .$$

Quindi

$$1 + r - \frac{1}{g}\big(N(F) - q - 1\big) = \frac{1}{g}\big(g + gr + \sum_{i=1}^{g}(\omega_i + \overline{\omega}_i)\big) = \frac{1}{g}\sum_{i=1}^{g}\gamma_i \geq \Big(\prod_{i=1}^{g}\gamma_i\Big)^{1/g} \geq 1 \, ,$$

i.e. $N(F) \leq q + 1 + gr$. Questo prova il limite superiore. Il limite inferiore si trova in modo analogo, sostituendo γ_i con $\delta_i = r + 1 - (\omega_i + \overline{\omega}_i)$. □

Per g sufficientemente grande neanche il limite di Serre è molto indicativo. Un limite migliore è quello trovato in [Iha] da Ihara:

Teorema 2.3.7 (Limite di Ihara) *Sia $F/\mathbb{F}_q$ un campo di funzioni di genere g. Allora il numero dei posti razionali $N(F)$ di $F/\mathbb{F}_q$ soddisfa*

$$N(F) \leq \frac{1}{2}\big(\sqrt{(8q+1)g^2 + (4q^2 - 4q)g} - (g - 2q - 2)\big) \, . \tag{2.5}$$

Dim. Procedendo in modo analogo alla dimostrazione della proposizione 2.3.6 ho che

$$N_m = q^m + 1 - \sum_{i=1}^{g}(\omega_i^m + \overline{\omega}_i^m) \, .$$

Pongo $\alpha_i := \omega_i + \overline{\omega}_i$ per ogni $1 \leq i \leq g$. Allora

$$N(F) = N = q + 1 - \sum_{i=1}^{g}\alpha_i \leq q^2 + 1 + 2qg - \sum_{i=1}^{g}\alpha_i^2 = N_2 \, ,$$

dove ho usato la relazione $\omega_i\overline{\omega}_i = q$. Usando la disuguaglianza di Cauchy-Schwarz $g\big(\sum_{i=1}^{g}\alpha_i^2\big) \geq \big(\sum_{i=1}^{g}\alpha_i\big)^2$ ottengo che

$$N \leq q^2 + 1 + 2qg - \frac{1}{g}\big(\sum_{i=1}^{g}\alpha_i\big)^2 = q^2 + 1 + 2qg - \frac{1}{g}(q + 1 - N)^2 \, .$$

Semplificando ho che

$$N^2 + (g - (2q+2))N + (q+1)^2 - (q^2+1)g - 2qg^2 \leq 0 \, .$$

Risolvendo rispetto ad N trovo

$$N \leq \frac{1}{2}\big(\sqrt{(8q+1)g^2 + (4q^2 - 4q)g} - g + (2q+2)\big) \, ,$$

che è quanto richiesto. □

Osservazione 2.3.8 Il limite di Ihara è migliore del limite di Hasse-Weil quando

$$2(q+1+2g\sqrt{q}) > \sqrt{(8q+1)g^2+(4q^2-4q)g} - g + (2q+2)\ ,$$

i.e. quando

$$g > \frac{\sqrt{q}(\sqrt{q}-1)}{2}\ ,$$

i.e. quando il genere è grande rispetto all'ordine di $\mathbb{F}_q$.

Quello che intendo fare è cercare il limite superiore minimo. Pongo $\omega_j = e^{i\vartheta_j}$, dove $\vartheta_j \in \mathbb{R}$ per ogni $1 \leq j \leq g$. Con ragionamento analogo a quello fatto nella dimostrazione della proposizione 2.3.6 ho che

$$\begin{aligned} N_m &= q^m + 1 + \sum_{j=1}^{g}(\omega_j + \overline{\omega}_j) = q^m + 1 - q^{m/2}\sum_{j=1}^{g}\left(e^{im\vartheta_j} + e^{-im\vartheta_j}\right) \\ &= q^m + 1 - 2q^{m/2}\sum_{j=1}^{g}\cos(m\vartheta_j)\ . \end{aligned}$$

Dividendo per $q^{m/2}$ ottengo

$$2\sum_{j=1}^{g}\cos(m\vartheta_j) + N_m q^{-m/2} = q^{m/2} + q^{-m/2}\ . \tag{2.6}$$

Considero ora le serie formali

$$f(\vartheta) := 1 + 2\sum_{m=1}^{\infty} c_m \cos(m\vartheta) \quad \text{e} \quad \Psi_d(t) := \sum_{m=1}^{\infty} c_{md}t^{md}\ ,$$

dove i $c_m \in \mathbb{R}$. Moltiplicando per c_m la relazione (2.6) e sommando sugli m ottengo

$$\sum_{j=1}^{g} 2\sum_{m=1}^{\infty} c_m\cos(m\vartheta_j) + \sum_{m=1}^{\infty} c_m N_m q^{-m/2} = \sum_{m=1}^{\infty} c_m q^{m/2} + \sum_{m=1}^{\infty} c_m q^{-m/2}$$

i.e.

$$\sum_{j=1}^{g} f(\vartheta_j) + \sum_{m=1}^{\infty} c_m N_m q^{-m/2} = g + \Psi_1(q^{1/2}) + \Psi_1(q^{-1/2})\ .$$

Usando la relazione (2.1) ho che

$$\begin{aligned} \sum_{m=1}^{\infty} c_m N_m q^{-m/2} &= \sum_{m=1}^{\infty} c_m\Big(\sum_{d|m} dB_d\Big)q^{-m/2} \\ &= \sum_{d=1}^{\infty} dB_d\Big(\sum_{m=1}^{\infty} c_{md}q^{-md/2}\Big) = \sum_{d=1}^{\infty} dB_d\Psi_d(q^{-1/2})\ . \end{aligned}$$

Ho dimostrato la seguente

Proposizione 2.3.9 (Formula esplicita di Weil) *Usando le notazioni precedenti, si ha che*

$$\sum_{j=1}^{g} f(\vartheta_j) + \sum_{d=1}^{\infty} dB_d\Psi_d(1/\sqrt{q}) = g + \Psi_1(\sqrt{q}) + \Psi_1(1/\sqrt{q})\ .$$

Serre utilizza tale formula per ottenere un nuovo limite superiore di $N(F)$:

Corollario 2.3.10 *Sia $F/\mathbb{F}_q$ un campo di funzioni di genere g. Siano c_m dei reali non negativi per ogni $m \in \mathbb{Z}_{>0}$ e sia $f(\vartheta) \geq 0$ per ogni $\vartheta \in \mathbb{R}$. Inoltre si assuma che solo un numero finito dei c_m sia diverso da 0. Allora*

$$N(F) \leq \frac{g}{\Psi(1/\sqrt{q})} + 1 + \frac{\Psi(\sqrt{q})}{\Psi(1/\sqrt{q})} \,, \tag{2.7}$$

dove $\Psi = \Psi_1$.

Dim. Ho che

$$\begin{aligned} N \cdot \Psi_1(1/\sqrt{q}) &= g + \Psi_1(\sqrt{q}) + \Psi_1(1/\sqrt{q}) - \sum_{d=2}^{\infty} dB_d \Psi_d(1/\sqrt{q}) - \sum_{j=1}^{g} f(\vartheta_j) \\ &\leq g + \Psi_1(\sqrt{q}) + \Psi_1(1/\sqrt{q}) \,, \end{aligned}$$

perché per ipotesi $f(\vartheta_j) \geq 0$ e $c_m \geq 0$. □

Osservazione 2.3.11 (i) Per una qualsiasi scelta dei c_m soddisfacenti le condizioni del corollario 2.3.10 ottengo un limite superiore. Per esempio il limite di Hasse-Weil corrisponde alla scelta $f(\vartheta) = 1 + \cos\vartheta$.

(ii) Dalla (2.7) ho che

$$g \geq (N-1)\Psi(1/\sqrt{q}) - \Psi(\sqrt{q}) = (N-1) \sum_{m=1}^{\infty} c_m q^{-m/2} - \sum_{m=1}^{\infty} c_m q^{m/2} \,.$$

Il problema è ora di trovare una scelta ottimale dei c_m in modo da minimizzare il limite superiore. Equivalentemente, dato un numero di posti razionali N di un campo di funzioni $F/\mathbb{F}_q$, per l'osservazione 2.3.11(ii), basta scegliere i c_m in modo tale da trovare il più grande limite inferiore di g.
Oesterlé risolse il problema dando una formula per q e g qualsiasi:

Teorema 2.3.12 (Limite di Oesterlé) *Sia $F/\mathbb{F}_q$ un campo di funzioni di genere g e siano $\lambda = N - 1$ ed n un intero tale che $q^{n/2} < \lambda \leq q^{(n+1)/2}$. Se*

$$u = \frac{q^{(n+1)/2} - \lambda}{\lambda q^{1/2} - q^{n/2}} \,,$$

allora esiste un'unica soluzione $\vartheta \in [\pi/(n+1), \pi/n)$ per l'equazione

$$\cos\big((n+1)\vartheta\big) + u\cos\big((n-1)\vartheta/2\big) = 0 \,.$$

Inoltre, se si pone $a_m = (n-m)\cos(m\vartheta)\sin(\vartheta) + \sin\big((n-m)\vartheta\big)$ e $c_m = a_m/a_0$ allora

$$g \geq \sum_{m=1}^{n-1} c_m(\lambda q^{-m/2} - q^{m/2}) = \frac{(\lambda-1)\sqrt{q}\cos(\vartheta) + q - \lambda}{q - 2\sqrt{q}\vartheta + 1} \,.$$

La dimostrazione del teorema, che si trova in [Hans], fa uso della teoria della misura (su $\mathbb{S}^1$).

Come conclusione del capitolo introduco brevemente il valore asintotico di $N_q(g)$ per un fissato q e $g \to \infty$:

Definizione 2.3.13 Per una fissata potenza q di un numero primo si definisce

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g} \, .$$

Dalla (2.4) ho che $A(q) \leq [2q^{1/2}]$ per ogni q. Dalla (2.5) ottengo invece

$$A(q) \leq \frac{1}{2}\big(\sqrt{8q+1}-1\big) \, . \tag{2.8}$$

Anche per il valore asintotico sorge il problema di trovare il limite migliore. Un possibile candidato è il seguente:

Teorema 2.3.14 (Limite di Vlăduţ-Drinfeld) *Per ogni potenza q di un numero primo si ha che*

$$A(q) \leq \sqrt{q} - 1 \, . \tag{2.9}$$

Dim. Come nella dimostrazione della proposizione 2.3.6 ho $N_m = q^m+1-\sum_{i=1}^{g}(\omega_i^m+\overline{\omega}_i^m)$. Posso scrivere $\omega_i = \sqrt{q}\xi_i$, dove $|\xi_i| = 1$. Allora per un intero positivo n qualsiasi

$$0 \leq \sum_{i=1}^{g} |1+\xi_i+\xi_i^2+\cdots+\xi_i^n|^2 = \sum_{i=1}^{g} \Big(\sum_{m=0}^{n} \xi_i^m\Big)\Big(\sum_{m=0}^{n} \overline{\xi}_i^m\Big) \, ;$$

ma

$$(1+\xi_i+\cdots+\xi_i^n)(1+\overline{\xi}_i+\cdots+\overline{\xi}_i^n) = \sum_{m=0}^{n}(n+1-m)(\xi_i^m+\overline{\xi}_i^m) \, ,$$

quindi

$$\begin{aligned} 0 &\leq g(n+1) + \sum_{m=1}^{n}(n+1-m)\sum_{i=1}^{g}(\xi_i^m+\overline{\xi}_i^m) \\ &= g(n+1) + \sum_{m=1}^{n}(n+1-m)\frac{q^m+1-N_m}{q^{m/2}} \\ &\leq g(n+1) + \sum_{m=1}^{n}(n+1-m)\frac{q^m+1-N}{q^{m/2}} \, . \end{aligned}$$

Risolvendo rispetto ad N trovo che

$$\begin{aligned} N\sum_{m=1}^{n}(n+1-m)\frac{1}{q^{m/2}} &\leq g(n+1) + \sum_{m=1}^{n}(n+1-m)q^{m/2} + \sum_{m=1}^{n}(n+1-m)\frac{1}{q^{m/2}} \\ N &\leq 1 + \frac{g(n+1)+\sum(n+1-m)q^{m/2}}{\sum(n+1-m)q^{-m/2}} \, . \end{aligned}$$

Asintoticamente

$$A(q) \leq \frac{n+1}{\sum (n+1-m)q^{-m/2}} \to \frac{1}{\sum q^{-m/2}} = \left(\frac{q^{-m/2}}{1-q^{-m/2}}\right)^{-1} = \sqrt{q}-1 \quad \text{per} \quad g \to \infty \, .$$

□

Al fine di determinare il limite superiore migliore per $A(q)$ si sono determinati dei limiti inferiori per $A(q)$; ci sono esenzialmente due casi:

(i) Se q è un quadrato, Tsfasman, Vlăduţ e Zink provano in [T-V-Z] che $A(q) \geq \sqrt{q}-1$, i.e. il limite di Vlăduţ-Drinfeld è in questo caso il migliore.

(ii) Se q non è un quadrato Serre in [Ser3] prova, usando torri di campi di classe di Hilbert (si veda il capitolo 3), che $A(q) \geq c \log_2 q$, dove $c > 1/96$.

Un'esauriente esposizione dei limiti inferiori di $N_q(g)$ si può trovare in [N-X] ed in [Voi].

Capitolo 3

Teoria dei campi di classe

Dato un campo di funzioni (in una variabile) $F/\mathbb{F}_q$, tutte le estensioni abeliane finite di F possono essere descritte tramite la teoria dei campi di classe. Quello che si intende fare è costruire dei campi di funzioni con molti posti razionali considerando le estensioni abeliane finite di un dato campo di funzioni.
In questo capitolo verranno discussi alcuni importanti risultati della teoria dei campi di classe, in particolar modo verrà focalizzata l'attenzione sui campi di classe ray e di Hilbert, che serviranno a determinare il numero di punti razionali di una curva. Verrà esposto anche il metodo di Serre per determinare l'esistenza di curve caratterizzate dal genere e dal numero di punti razionali.

I risultati più noti sono stati riportati senza dimostrazione. I riferimenti principali per questo capitolo sono i libri di Niederreiter e Xing [N-X], di Stichtenoth [Sti2] e di Weiss [Wei]. Per il metodo di Serre si è fatto riferimento al libro dello stesso Serre [Ser1] ed agli articoli di Schoof [Sch] e della Lauter [Lau].

3.1 Gruppi di ramificazione e conduttori

Per ottenere informazioni riguardanti i campi di funzioni su campi finiti è utile considerare i loro completamenti, una tecnica comune alla geometria algebrica e alla teoria algebrica dei numeri.

Un anello di valutazione di un campo di valutazione completo (F, ν), in accordo con il teorema 1.1.10 può essere definito come l'insieme

$$\mathcal{O}_F := \{x \in K \mid \nu(x) \geq 0\} \ .$$

Detto questo, l'unico ideale massimale di $\mathcal{O}_F$ è

$$\mathfrak{M}_F := \{x \in F \mid \nu(x) > 0\} \ ,$$

ed il gruppo delle unità di $\mathcal{O}_F$ è

$$\mathcal{U}_F := \{x \in F \mid \nu(x) = 0\} .$$

In accordo con la definizione 1.1.11 l'anello quoziente $\mathcal{O}_F/\mathfrak{M}_F$ è chiamato **campo di classe dei residui** di F.

Sia (F, ν_F) un campo di valutazione completo rispetto alla valutazione discreta ν_F. Per un'estensione di Galois E/F, considero l'unica estensione di ν_F per E e sia ν_E l'equivalente valutazione discreta di E. Per ogni intero $i \geq -1$ sia $G_i(E/F)$ il gruppo

$$G_i(E/F) = \{\sigma \in \mathrm{Gal}(E/F) \mid \nu_E(\sigma(a) - a) \geq i + 1 \text{ per ogni } a \in \mathcal{O}_E\},$$

dove $\mathcal{O}_E = \{x \in E \mid \nu_E(x) \geq 0\}$ è l'anello di valutazione di E. Il gruppo $G_i(E/F)$ è chiamato i-esimo **gruppo di ramificazione (in notazione inferiore)** di E/F. Si noti che $G_{-1}(E/F) = \mathrm{Gal}(E/F)$. Il gruppo $G_0(E/F)$ è anche chiamato **gruppo d'inerzia** di E/F.

Considero ora un campo di funzioni $F/\mathbb{F}_q$ ed un posto P di F. Sia E/F un'estensione di Galois finita e Q un posto di E che sta sopra P. Denoto il completamento P-adico di F con F_P ed il completamento Q-adico di E con E_Q.

Teorema 3.1.1 (i) *Se E/F è un'estensione di Galois, allora E_Q/F_P è un'estensione di Galois e l'applicazione*

$$\eta : G_Z(Q|P) \to \mathrm{Gal}(E_Q/F_P),$$

dove $G_Z(Q|P)$ è il gruppo di decomposizione di Q su P, è un isomorfismo.

(ii) *L'i-esimo gruppo di ramificazione $G_i(E/F)$ di Q sopra P è isomorfo all'i-esimo gruppo di ramificazione $G_i(E_Q/F_P)$, per ogni $i \geq -1$.*

Dim. Si ha che

$$|G_Z(Q|P)| \leq |\mathrm{Aut}(E_Q/F_P)| \leq [E_Q : F_P]$$

e queste disuguaglianze diventano uguaglianze se e solo se (i) è vera.
Suppongo che $[\mathrm{Gal}(E/F) : G_Z(Q|P)] = r$, i.e. che esistano esattamente r posti di E che stanno sopra P. Siano $\sigma_1(Q), \sigma_2(Q), \ldots, \sigma_r(Q)$ i posti distinti di E che stanno sopra P, $\sigma_i \in \mathrm{Gal}(E/F)$, $i = 1, 2, \ldots, r$. Allora

$$|\mathrm{Gal}(E/F)| = r|G_Z(Q|P)| = \sum_{i=1}^{r} |G_Z(\sigma_i(Q)|P)|$$

$$\leq \sum_{i=1}^{r} [E_{\sigma_i(Q)} : F_P] = [E : F] = |\mathrm{Gal}(E/F)| .$$

Quindi vale l'uguaglianza.
(ii) segue direttamente da (i). □

Per il teorema quindi posso identificare $G_i(E_Q/F_P)$ con $G_i(Q|P)$, $i \geq -1$.
Sia, per un numero reale $u \geq -1$,

$$G_u := G_{[u]}(E_Q/F_P).$$

Indico con g_i l'ordine di $G_i(E_Q/F_P)$. Posto

$$\varphi(u) = \begin{cases} \frac{1}{g_0}(g_1 + g_2 + \cdots + g_{[u]} + (u - [u])g_{[u]+1}) & \text{se } u > 0 \\ u & \text{se } -1 \leq u \leq 0, \end{cases}$$

si ha, in particolare,

$$\varphi(m)+1=\frac{1}{g_0}\sum_{i=0}^{m} g_i \quad , \quad m\in\mathbb{Z}_{\geq -1}.$$

La funzione φ ammette inversa in $[-1,\infty)$ che denoto con ψ.

Lemma 3.1.2 *Se $v\in\mathbb{Z}_{\geq -1}$, allora $u=\psi(v)\in\mathbb{Z}_{\geq -1}$.*

Dim. Posso assumere $u>0$. Per la definizione di φ ho che

$$g_0\big(\varphi(u)+1\big)=g_0(v+1)=g_0+g_1+g_2+\cdots+g_{[u]}+(u-[u])g_{[u]+1}) \ .$$

Poiché $G_{[u]+1}$ è un sottogruppo di G_i per ogni $i=1,2,\ldots,[u]$, ho che

$$u-[u]=\frac{g_0(v+1)-\sum_{i=0}^{[u]} g_i}{g_{[u]+1}}$$

è un intero, i.e. u è un intero. □

Per ogni $v\in\mathbb{R}_{\geq -1}$ definisco il **gruppo di ramificazione in notazione superiore** di (E_Q/F_P) come

$$G^v:=G^v(E_Q/F_P):=G_{\psi(v)},$$

o analogamente

$$G^{\varphi(u)}:=G^{\varphi(u)}(E_Q/F_P):=G_u.$$

Allora $G^{-1}=\mathrm{Gal}(E_Q/F_P)$ e $G^0=G_0(E_Q/F_P)$.
Avendo identificato $\mathrm{Gal}(E_Q/F_P)$ con $G_Z(Q|P)$, G^v e G_u sono sottogruppi di $G_Z(Q|P)$. Quindi ha senso parlare di gruppo di ramificazione in notazione superiore di Q sopra P e porre $G^v(Q|P):=G^v(E_Q/F_P)$.

Teorema 3.1.3 (Hasse-Arf) *Supposto che E_Q/F_P sia un'estensione abeliana finita, se $G_i\neq G_{i+1}$ allora $\varphi(i)$ è un intero.*

Fino alla fine del paragrafo assumo che E/F sia un'estensione abeliana finita. Sia P un posto di F. Allora ha senso parlare di indice di ramificazione $e_P(E/F)$ di P in E/F e di esponente differente $d_P(E/F)$ di P in E/F, come in una qualsiasi estensione di Galois. Inoltre, dalla proposizione 1.7.6 segue che il gruppo di ramificazione $G_i(Q|P)$ e il gruppo di ramificazione in notazione superiore di Q sopra P sono indipendenti dalla scelta di Q sopra P. Quindi posso porre $G_i(P,E/F):=G_i(Q|P)$ e $G^i(P,E/F):=G^i(Q|P)$ rispettivamente per l'i-esimo gruppo di ramificazione e l'i-esimo gruppo di ramificazione in notazione superiore di P in E/F.

Sia $a_P(E/F)$ il più piccolo intero $k\geq 0$ tale che $|G_i(P,E/F)|=1$ per ogni $i\geq k$. La quantità

$$c_P(E/F):=\frac{d_P(E/F)+a_P(E/F)}{e_P(E/F)}$$

è chiamata **esponente del conduttore** di P in E/F.

Teorema 3.1.4 *Sia E/F un'estensione abeliana finita di un campo di funzioni su $\mathbb{F}_q$ e sia P un posto di F. Allora:*

(i) *$c_P(E/F)$ è un intero non negativo;*

(ii) *P è non-ramificato in E/F se e solo se $c_P(E/F) = 0$ e P è moderatamente ramificato in E/F se e solo se $c_P(E/F) = 1$;*

(iii) *$c_P(E/F)$ è il più piccolo intero $k \geq 0$ tale che $G^v = \{\mathrm{id}\}$ per ogni $v \geq k$.*

Dim. (i) Posso supporre $a = a_P(E/F) \geq 1$. Dalla definizione di $c_P(E/F)$ e dal teorema della formula di Hilbert 1.7.8 ho che

$$c_P(E/F) = \frac{\sum_{i=0}^{a-1}(g_i - 1) + a}{g_0} = \frac{1}{g_0}\sum_{i=0}^{a-1} g_i = \varphi(a-1) + 1 \ .$$

In accordo con la definizione di a, $G_{a-1}(P, E/F) \neq G_a(P, E/F)$. Dal teorema di Hasse-Arf segue che $\varphi(a-1)$ è un intero, i.e. $c_P(E/F)$ è un intero non negativo.
(ii) P è non-ramificato in E/F se e solo se $g_0 = |G_0(P, E/F)| = e_P(E/F) = 1$. Questo equivale a dire che $a_P(E/F) = 0$, i.e. $c_P(E/F) = 0$.
La seconda parte si dimostra in modo analogo.
(iii) Posso supporre $c_P(E/F) \geq 1$. Allora

$$\psi(c_P(E/F)) = \psi(\varphi(a-1)+1) > \psi(\varphi(a-1)) = a - 1 \ .$$

Poiché $c_P(E/F)$ è un intero, per il lemma 3.1.2 $\psi(c_P(E/F))$ è un intero. Quindi si ha che $\psi(c_P(E/F)) \geq a$.
Inoltre

$$G^v \subseteq G^{c_P(E/F)} = G_{\psi(c_P(E/F))} \subseteq G_a = \{\mathrm{id}\}$$

per ogni $v \geq c_P(E/F)$, dunque

$$G^{c_P(E/F)-1} = G^{\varphi(a-1)} = G_{a-1} \neq \{\mathrm{id}\} \ .$$

□

Definizione 3.1.5 Sia E/F un'estensione abeliana finita di un campo di funzioni su $\mathbb{F}_q$. Il **conduttore** di E/F è il divisore effettivo di F così definito:

$$\mathrm{Cond}(E/F) := \sum_{P \in \mathbf{P}_F} c_P(E/F)P \ .$$

3.2 Campi globali

In ogni campo di funzioni $F/\mathbb{F}_q$ e per ogni elemento x di F si ha

(i) $\nu_P(x) = 0$ per tutti tranne un numero finito di $P \in \mathbf{P}_F$;

(ii) $\sum_{P \in \mathbf{P}_F} \nu_P(x)\deg(P) = 0$.

Per un campo di funzioni $F/\mathbb{F}_q$, tramite l'immersione canonica $F \hookrightarrow F_P$, dove F_P denota il completamento P-adico di F, posso identificare F con le sue immagini in F_P e scrivere $a = (a)_P \in \prod_P F_P$ per ogni $a \in F$, dove $\prod_P F_P = \prod_{P \in \mathbf{P}_F} F_P$ è l'anello prodotto diretto. Denoto con $\mathcal{O}_{F_P}$, $\mathfrak{M}_{F_P}$ e $\mathcal{U}_{F_P}$ rispettivamente l'anello di valutazione di F_P, l'ideale massimale di $\mathcal{O}_{F_P}$ ed il gruppo delle unità di $\mathcal{O}_{F_P}$.

Un **adèle** di $\prod_P F_P$ è un elemento $(x_P)_{P \in \mathbf{P}_F} = (x_P) \in \prod_P F_P$ tale che $x_P \in \mathcal{O}_{F_P}$ per tutti tranne un numero finito di posti P di F. L'insieme degli adèle è dotato di struttura d'anello con identità. Tale anello è chiamato **anello degli adèle** di F ed è denotato con $\mathcal{A}_F$. Poiché ogni elemento di F è un adèle (F può essere visto come un sottospazio di $\mathcal{A}_F$ tramite l'immersione diagonale $F \to \mathcal{A}_F$, $x \mapsto (\dots, x, \dots)$), posso vedere F come sottoanello di $\mathcal{A}_F$. In questo contesto, gli elementi di F sono chiamati **adèle principali** di F. Le unità di $\mathcal{A}_F$ sono chiamate **idèle** di F. L'insieme degli idèle viene denotato con $\mathcal{J}_F$. Esso è dotato della struttura di gruppo moltiplicativo e consiste negli elementi $(x_P) \in \prod_P F_P^*$ tali che $x_P \in \mathcal{U}_{F_P}$ per tutti tranne un numero finito di $P \in \mathbf{P}_F$. Il gruppo $\mathcal{J}_F$ è chiamato **gruppo degli idèle** di F. Chiaramente $F^* \subset \mathcal{J}_F \subset \mathcal{A}_F$. Il gruppo quoziente $\mathcal{C}_F := \mathcal{J}_F/F^*$ è chiamato **gruppo delle classi di idèle** di F.

Teorema 3.2.1 *Per un campo di funzioni $F/\mathbb{F}_q$ il seguente diagramma commutativo ha righe e colonne esatte:*

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mathbb{F}_q^* & \to & F^* & \to & \mathrm{Princ}(F) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mathcal{U}_F & \to & \mathcal{J}_F & \to & \mathrm{Div}(F) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mathcal{U}_F/\mathbb{F}_q^* & \to & \mathcal{C}_F & \to & \mathrm{Pic}(F) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 0 & &
\end{array}$$

Dim. Il gruppo degli idèle ammette un naturale omomorfismo suriettivo

$$\begin{array}{ccc} \mathcal{J}_F & \longrightarrow & \mathrm{Div}(F) \\ (x_P) & \longmapsto & \displaystyle\sum_P \nu(x_P) P \end{array} .$$

Il nucleo di tale omomorfismo è composto dagli idèle che hanno valutazione nulla in tutti i posti, i.e. $\mathcal{U}_F$. Per $a \in F^*$, $a \in \mathcal{U}_F$ se e solo se $\nu_P(a) = 0$ per ogni $P \in \mathbf{P}_F$. Quindi $\mathcal{U}_F \cap F^* = \mathbb{F}_q^*$.
Le altre sequenze sono ovvie. □

Sia $\mathcal{S}$ un sottoinsieme proprio di $\mathbf{P}_F$ tale che $\mathbf{P}_F \setminus \mathcal{S}$ sia finito. Considero l'insieme

$$\begin{array}{rcl} \mathcal{A}_{\mathcal{S}} & := & \displaystyle\prod_{P \notin \mathcal{S}} F_P \times \prod_{P \in \mathcal{S}} \mathcal{O}_{F_P} \\ & = & \{(x_P) \in \mathcal{A}_F \mid \nu_P(x_P) \geq 0 \text{ per ogni } P \in \mathcal{S}\} \ . \end{array}$$

Esso è un sottoanello di $\mathcal{A}_F$, chiamato **dominio degli $\mathcal{S}$-adèle** di $\mathcal{A}_F$.
Il gruppo delle unità dell'anello $\mathcal{A}_{\mathcal{S}}$ è chiamato **gruppo degli $\mathcal{S}$-idèle** di F ed è denotato con $\mathcal{J}_{\mathcal{S}}$. Chiaramente

$$\mathcal{J}_{\mathcal{S}} = \prod_{P \notin \mathcal{S}} F_P^* \times \prod_{P \in \mathcal{S}} \mathcal{U}_{F_P} \ .$$

Pongo $F_{\mathcal{S}} = F \cap \mathcal{A}_{\mathcal{S}}$ e $F^*_{\mathcal{S}} = F^* \cap \mathcal{J}_{\mathcal{S}}$.
Definisco come **gruppo delle classi degli $\mathcal{S}$-idèle** il gruppo quoziente $\mathcal{C}_{\mathcal{S}} := \mathcal{J}_{\mathcal{S}}/F^*_{\mathcal{S}}$.
Poiché $\mathcal{C}_{\mathcal{S}} \cong (F^* \cdot \mathcal{J}_{\mathcal{S}})/F^*$, ho l'immersione canonica

$$\mathcal{C}_{\mathcal{S}} = \mathcal{J}_{\mathcal{S}}/F^*_{\mathcal{S}} \hookrightarrow \mathcal{C}_F = \mathcal{J}_F/F^* \ .$$

Il gruppo delle classi di idèle è collegato con il gruppo delle classi $\mathcal{S}$-ray (si veda la definizione 1.5.8). Per un posto P di F ed un intero $n \geq 1$ definisco l'n-esimo gruppo delle unità

$$\mathcal{U}^{(n)}_{F_P} = \{x \in \mathcal{U}_{F_P} \mid \nu_P(x-1) \geq n\} \ .$$

Sia $D = \sum_P m_P P$ un divisore effettivo di F tale che $\mathrm{supp}(D) \subseteq \mathcal{S}$. Definisco un sottogruppo $\mathcal{J}^D_{\mathcal{S}}$ di $\mathcal{J}_{\mathcal{S}}$ come

$$\mathcal{J}^D_{\mathcal{S}} = \prod_{P \notin \mathcal{S}} F^*_P \times \prod_{P \in \mathcal{S}} \mathcal{U}^{(m_P)}_{F_P}$$

e lo chiamo **sottogruppo delle $\mathcal{S}$-congruenze** modulo D. Il suo gruppo delle classi è definito essere

$$\mathcal{C}^D_{\mathcal{S}} = (F^* \cdot \mathcal{J}^D_{\mathcal{S}})/F^* \ .$$

Proposizione 3.2.2 *Detto $\mathrm{Cl}_D(\mathcal{O}_{\mathcal{S}})$ il gruppo delle classi $\mathcal{S}$-ray modulo D, si ha che*

$$\mathcal{C}_F/\mathcal{C}^D_{\mathcal{S}} \cong \mathcal{J}_F/(F^* \cdot \mathcal{J}^D_{\mathcal{S}}) \cong \mathrm{Cl}_D(\mathcal{O}_{\mathcal{S}}) \ .$$

In particolare $\mathcal{C}_F/\mathcal{C}^D_{\mathcal{S}}$ è un gruppo finito.

Dim. Il primo isomorfismo deriva dal terzo teorema di isomorfismo per gruppi. Pongo

$$\mathcal{J}^D = \left\{(x_P) \in \mathcal{J}_F \mid x_P \in \mathcal{U}^{(m_P)}_{F_P} \text{ per ogni } P \in \mathrm{supp}(D)\right\} \ .$$

Ho che $\mathcal{J}_F = F^* \cdot \mathcal{J}^D$, perché per ogni idèle $(x_P) \in \mathcal{J}_F$ posso usare il teorema di approssimazione 1.3.1 per ottenere uno $z \in F^*$ tale che

$$\nu_P(x_P z - 1) \geq m_P \ \text{ per ogni } \ P \in \mathrm{supp}(D) \ .$$

Quindi $(x_P z) \in \mathcal{J}^D$.
Considero la funzione

$$\phi : \mathcal{C}_F \to \mathrm{Cl}(\mathcal{O}_{\mathcal{S}})$$

definita nel seguente modo. Preso un idèle $(x_P) \in \mathcal{J}_F$ scritto come $(x_P) = (y)(z_P)$, con $y \in F^*$ e $(z_P) \in \mathcal{J}^D$, pongo

$$\phi((x_P)F^*) = \left(\prod_{P \in \mathcal{T}} \mathfrak{M}_P(\mathcal{S})^{\nu_P(z_P)}\right) \mathrm{Princ}_{D,\mathcal{S}} \ ,$$

dove $\mathcal{T} = \mathcal{S} \setminus \mathrm{supp}(D)$. ϕ è ben definita, infatti gli elementi di $\mathcal{J}^D \cap F^*$ sono esattamente quelli generati dagli $\mathcal{S}$-ideali principali in $\mathrm{Princ}_{D,\mathcal{S}}$.
ϕ è ovviamente un omomorfismo suriettivo di gruppi. Inoltre $\mathcal{C}^D_{\mathcal{S}} = (F^* \cdot \mathcal{J}^D_{\mathcal{S}})/F^* \subseteq \ker(\phi)$ e quindi posso scrivere un qualsiasi elemento del nucleo nella forma $(z_P)F^*$, $(z_P) \in \mathcal{J}^D$. Ma $(z_P)F^* \in \ker(\phi)$ implica che per qualche $u \in \mathcal{J}^D \cap F^*$ si ha che

$$\nu_P(z_P) = \nu_P(u) \text{ per ogni } P \in \mathcal{T} \ .$$

Considero l'idèle $(w_P) = (z_P)(u^{-1})$. Ho che $\nu_P(w_P) = 0$ per ogni $P \in \mathcal{T}$. Per $P \in \mathrm{supp}(D)$ ho che $z_P, u \in \mathcal{U}^{(m_P)}_{F_P}$ e quindi $w_P \in \mathcal{U}^{(m_P)}_{F_P}$ e ciò implica $\nu_P(w_P) = 0$. Ma allora $(w_P) \in \mathcal{J}_{\mathcal{S}}$ e poiché anche $(w_P) \in \mathcal{J}^D$, $(w_P) \in \mathcal{J}_{\mathcal{S}} \cap \mathcal{J}^D = \mathcal{J}^D_{\mathcal{S}}$. Di conseguenza $(z_P)F^* = (w_P)F^* \in \mathcal{C}^D_{\mathcal{S}}$, quindi $\ker(\phi) = \mathcal{C}^D_{\mathcal{S}}$ e $\mathcal{C}_F/\mathcal{C}^D_{\mathcal{S}} \cong \mathrm{Cl}_D(\mathcal{O}_{\mathcal{S}})$. □

3.3 Campi di classe ray e campi di classe di Hilbert

In questo paragrafo come prima cosa verranno enunciati alcuni risultati della teoria dei campi di classe. Tali risultati verranno poi applicati per ottenere i campi di classe ray.

Inizio enunciando un risultato centrale della teoria dei campi di classe locali. Sia F il completamento di un campo di funzioni su $\mathbb{F}_q$ rispetto ad una delle valutazioni discrete di F, diciamo ν_F, e sia E/F un'estensione abeliana finita. Allora esiste un'**applicazione di reciprocità di Artin locale** $\theta_{E/F} : F^* \to \mathrm{Gal}(E/F)$ tale che:

(i) $\ker(\theta_{E/F}) = N_{E/F}(E^*)$, $\mathrm{im}(\theta_{E/F}) = \mathrm{Gal}(E/F)$.

(ii) Se E/F è non-ramificata (i.e. $G_0(E/F) = \{\mathrm{id}\}$) allora $\theta_{E/F}(x) = \pi^{\nu_F(x)}$ per ogni $x \in F^*$, dove π è l'automorfismo di Frobenius di E/F.

(iii) $\theta_{E/F}$ trasforma il v-esimo gruppo delle unità $\mathcal{U}_F^{(v)}$ di F nel gruppo di ramificazione in notazione superiore $G^v(E/F)$ per ogni $v \in \mathbb{Z}_{\geq 0}$.

Quindi E/F è non-ramificata se e solo se $\theta_{E/F}(\mathcal{U}_F) = \{\mathrm{id}\}$.

Nel caso globale, detti $F/\mathbb{F}_q$ un campo di funzioni e E/F un estensione abeliana finita, definisco l'**applicazione di reciprocità di Artin globale** come prodotto di applicazioni di reciprocità locali:

$$\theta_{E/F} := \prod_P \theta_P : \mathcal{J}_F \to \mathrm{Gal}(E/F) \ ,$$

dove $\theta_P = \theta_{E_Q/F_P}$ è l'applicazione di reciprocità locale di Artin $F_P^* \to \mathrm{Gal}(E_Q/F_P) \cong G_Z(Q|P) \hookrightarrow \mathrm{Gal}(E/F)$ per un posto Q di E che sta sopra $P \in \mathbf{P}_F$. Poiché E/F è abeliana, $G_Z(Q|P)$ non dipende dalla scelta di Q in E sopra P. Quindi θ_P è ben definita. Per $x = (x_P) \in \mathcal{J}_F$ si ha che

$$\theta_{E/F}(x) = \prod_P \theta_P(x_P) \ .$$

Poiché l'applicazione di reciprocità globale di Artin $\theta_{E/F}$ è un omomorfismo suriettivo di nucleo $F^* \cdot \mathrm{N}_{E/F}(\mathcal{J}_E)$, dove $\mathrm{N}_{E/F} : \mathcal{J}_E \to \mathcal{J}_F$ è l'estensione canonica della norma da E ad F, essa induce un omomorfismo suriettivo

$$(\cdot, E/F) : \mathcal{C}_F \to \mathrm{Gal}(E/F) \ ,$$

chiamato **norma residua simbolica** di E/F. Il suo nucleo è

$$(F^* \cdot \mathrm{N}_{E/F}(\mathcal{J}_E))/F^* =: \mathcal{N}_{E/F} \ .$$

La **chiusura abeliana** F^{ab} **di** F è l'unione di tutte le estensioni abeliane finite di F in una finita chiusura separabile $\overline{F}$ di F fissata.

Teorema 3.3.1 (i) **(Reciprocità di Artin)** *Per un'estensione abeliana finita E/F di un campo di funzioni $F/\mathbb{F}_q$ esiste un isomorfismo canonico*

$$\mathcal{C}_F/\mathcal{N}_{E/F} \cong \mathrm{Gal}(E/F)$$

indotto dalla norma residua simbolica $(\cdot, E/F)$.

(ii) **(Teorema di esistenza)** *Per ogni sottogruppo M di $\mathcal{C}_F$ di indice finito esiste un'unica estensione abeliana finita E di F contenuta nella chiusura abeliana F^{ab} di F tale che $\mathcal{N}_{E/F} = M$.*

(iii) *Date due estensioni abeliane finite E_1/F, E_2/F in F^{ab}, $E_1 \subseteq E_2$ se e solo se $\mathcal{N}_{E_1/F} \supseteq \mathcal{N}_{E_2/F}$.*

Proposizione 3.3.2 *Sia M un sottogruppo di $\mathcal{C}_F$ di indice finito e sia $E \subseteq F^{\mathrm{ab}}$ un'estensione abeliana finita di F tale che $\mathcal{N}_{E/F} = M$. Sia H un sottogruppo di $\mathcal{J}_F$ contenente F^* tale che $M = H/F^*$. Per un posto P di F si ha che*

(i) *P è non-ramificato in E/F se e solo se $\mathcal{U}_{F_P} \subseteq H$;*

(ii) *P si separa completamente in E/F se e solo se $F_P^* \subseteq H$.*

Dim. (i) Sia $\theta_{E/F}$ l'applicazione di reciprocità di Artin globale. Allora

$$\theta_{E/F}(\mathcal{U}_{F_P}) = \theta_P(\mathcal{U}_{F_P}) \times \prod_{R \neq P} \theta_R(\{1\}) = G_0(P, E/F) \ .$$

Si ha che $\mathcal{U}_{F_P} \subseteq H$ se e solo se $\theta_{E/F}(\mathcal{U}_{F_P}) = \{\mathrm{id}\}$. Questo equivale a dire che il gruppo $G_0(P, E/F) = \{\mathrm{id}\}$, i.e. P è non-ramificato in E/F.
(ii) P si separa completamente in E/F se e solo se $G_{-1}(P, E/F) = \{\mathrm{id}\}$. Questo equivale a dire che l'elemento di Frobenius $\pi_P = 1$ se e solo se $\theta_{E/F}(F_P^*) = \{\mathrm{id}\}$ e ciò equivale a dire che $F_P^* \subseteq H$. □

Per un divisore effettivo D di F ed un sottoinsieme proprio $\mathcal{S}$ di $\mathbf{P}_F$ tale che $\mathbf{P}_F \setminus \mathcal{S}$ è finito e $\mathrm{supp}(D) \subseteq \mathcal{S}$, $\mathcal{C}_{\mathcal{S}}^D$ è un sottogruppo di $\mathcal{C}_F$ di indice finito (si confronti la proposizione 3.2.2). Dunque, per il teorema di esistenza 3.3.1(ii), esiste un'unica estensione $F_{\mathcal{S}}^D/F$, $F_{\mathcal{S}}^D \subseteq F^{\mathrm{ab}}$, tale che

$$\mathcal{N}_{F_{\mathcal{S}}^D/F} = \mathcal{C}_{\mathcal{S}}^D \ .$$

Per la definizione di $\mathcal{C}_{\mathcal{S}}^D$ e la proposizione 3.3.2(ii) tutti i posti in $\mathbf{P}_F \setminus \mathcal{S}$ si separano completamente in $F_{\mathcal{S}}^D/F$.

Definizione 3.3.3 Il campo $F_{\mathcal{S}}^D$ è chiamato **campo di classe ray** di modulo D.

Teorema 3.3.4 (del conduttore) *Sia E/F un'estensione abeliana finita di un campo di funzioni $F/\mathbb{F}_q$, $E \subseteq F^{\mathrm{ab}}$, e sia $\mathcal{S}$ un insieme di posti di F tale che $\mathbf{P}_F \setminus \mathcal{S}$ sia non vuoto, finito e che tutti i posti in $\mathbf{P}_F \setminus \mathcal{S}$ si separino completamente in E/F. Denoto il conduttore* $\mathrm{Cond}(E/F)$ *con C. Allora:*

(i) *E è un sottocampo di $F_{\mathcal{S}}^C$;*

(ii) *Se D è un divisore effettivo di F tale che* $\mathrm{supp}(D) \subseteq \mathcal{S}$ *ed $E \subseteq F_{\mathcal{S}}^D$, allora $D \geq C$.*

Dim. Per un divisore positivo D di F con $\mathrm{supp}(D) \subseteq \mathcal{S}$, per il teorema 3.3.1(iii) ho che $E \subseteq F_{\mathcal{S}}^D$se e solo se $\mathcal{N}_{E/F} \supseteq \mathcal{C}_{\mathcal{S}}^D$. Questo equivale a dire che $F^* N_{E/F}(\mathcal{J}_E) \supseteq F^* \cdot \mathcal{J}_{\mathcal{S}}^D$. Sia

$\theta_{E/F}$ l'applicazione di reciprocità di Artin globale da $\mathcal{J}_F$ a $\mathrm{Gal}(E/F)$. Per un posto P di $\mathcal{S}$ ed un intero n ho che

$$\{\mathrm{id}\} = \theta_{E/F}(\mathcal{U}_{F_P}^{(n)}) = \theta_P(\mathcal{U}_{F_P}^{(n)}) = G^n(P, E/F) \text{ se e solo se } n \geq \nu_P(C) \ .$$

Questo significa che

$$F^* \cdot \mathcal{J}_{\mathcal{S}}^D \subseteq F^* \cdot N_{E/F}(\mathcal{J}_E) = \ker(\theta_{E/F}) \text{ se e solo se } D \geq C \ .$$

Questo completa la dimostrazione di (i) e di (ii). □

Corollario 3.3.5 *Sia $\mathcal{S}$ un sottoinsieme proprio di $\mathbf{P}_F$ tale che $\mathbf{P}_F \setminus \mathcal{S}$ sia finito e sia D un divisore effettivo di F tale che* $\mathrm{supp}(D) \subseteq \mathcal{S}$. *Allora* $\mathrm{Cond}(F_{\mathcal{S}}^D/F) = D$.

Per un divisore effettivo D di F e un sottoinsieme proprio $\mathcal{S}$ di $\mathbf{P}_F$ tale che $\mathrm{supp}(D) \subseteq \mathcal{S}$ e $\mathbf{P}_F \setminus \mathcal{S}$ sia finito, si ha quindi che $F_{\mathcal{S}}^D$ è un'estensione abeliana finita con

$$\mathrm{Gal}(F_{\mathcal{S}}^D/F) \cong \mathcal{C}_F/\mathcal{C}_{\mathcal{S}}^D \cong \mathrm{Cl}_D(\mathcal{O}_{\mathcal{S}}) \ ,$$

dove il secondo isomorfismo viene dalla proposizione 3.2.2.

Nel caso $D = 0$ il campo di classe ray $F_{\mathcal{S}}^D$ ha la proprietà che $F_{\mathcal{S}}^0/F$ è un'estensione abeliana ovunque non-ramificata nella quale tutti i posti di $\mathbf{P}_F \setminus \mathcal{S}$ si separano completamente. Oltre a ciò, $F_{\mathcal{S}}^0$ è massimale, nel senso che se E/F è un'estensione abeliana non-ramificata, $E \subseteq F^{\mathrm{ab}}$, nella quale tutti i posti in $\mathbf{P}_F \setminus \mathcal{S}$ si separano completamente, allora E è un sottocampo di $F_{\mathcal{S}}^D$.
Chiamo $F_{\mathcal{S}}^0$ il **campo di classe di $\mathcal{S}$-Hilbert** (*$\mathcal{S}$-Hilbert class field*) e lo denoto con $\mathcal{H}_{\mathcal{S}}$.

Proposizione 3.3.6 *Sia $\mathcal{H}_{\mathcal{S}}$ il campo di classe di $\mathcal{S}$-Hilbert di $F/\mathbb{F}_q$. Allora:*

(i) $\mathrm{Gal}(\mathcal{H}_{\mathcal{S}}/F) \cong \mathrm{Cl}(\mathcal{O}_{\mathcal{S}})$*;*

(ii) *Il simbolo di Artin* $\left[\frac{\mathcal{H}_{\mathcal{S}}/F}{P}\right]$ *di un posto P di F corrisponde alla classe dei residui di P in* $\mathrm{Cl}(\mathcal{O}_{\mathcal{S}})$ *sotto l'isomorfismo dato in* (i)*;*

(iii) *$\mathcal{H}_{\mathcal{S}}$ è un sottocampo di $F_{\mathcal{S}}^D$ per un qualsiasi divisore effettivo D di F tale che* $\mathrm{supp}(D) \subseteq \mathcal{S}$*;*

(iv) *$\mathbb{F}_{q^d}$ è algebricamente chiuso in $\mathcal{H}_{\mathcal{S}}$, dove d è il massimo comun divisore dei gradi dei posti in $\mathbf{P}_F \setminus \mathcal{S}$.*

3.4 Il metodo di Serre

Questo metodo usa la teoria dei campi di classe per campi di funzioni su campi finiti per costruire curve con molti punti razionali.

Sia $F/\mathbb{F}_q$ il campo di funzioni di una curva $\mathcal{X}$.
Un ricoprimento abeliano di $\mathcal{X}$ corrisponde ad un'estensione abeliana di F la quale corrisponde ad un sottogruppo di $\mathcal{C}_F$ di indice finito. Inoltre la teoria dei campi di classe

assicura che per ogni quoziente finito di $\mathcal{C}_F$ esiste un'estensione abeliana di F tale che il suo gruppo di Galois sia proprio questo quoziente. Quindi, per costruire curve su $\mathbb{F}_q$ come ricoprimenti di $\mathcal{X}$ è sufficiente considerare i quozienti finiti di $\mathcal{C}_F$.

Considero un divisore effettivo $D = \sum_{P \in \mathbf{P}_F} n_P P$ di $\mathcal{X}$ e definisco l'insieme

$$U_D := \left\{ (x_P) \in \mathcal{U}_F/\mathbb{F}_q^* \mid x_P \equiv 1 \pmod{t_P^{n_P}} \right\} ,$$

dove t_P è l'uniformizzante del posto P.
Si possono presentare due casi:

(i) Se $D = 0$, $\mathcal{C}_{\mathcal{S}}^D/\mathbb{F}_q^*$ è uguale a $\mathcal{U}_F/\mathbb{F}_q^*$ ed il quoziente di $\mathcal{C}_F/\mathcal{C}_{\mathcal{S}}^D$ è proprio il gruppo di Picard $\mathrm{Pic}(\mathcal{X})$.

(ii) Se $D \neq 0$ la seguente sequenza è esatta:

$$0 \to (\mathcal{U}_F/\mathbb{F}_q^*)/U_D \to \mathcal{C}_F/U_D \to \mathrm{Pic}(\mathcal{X}) \to 0 ,$$

dove il primo gruppo si può descrivere in maniera esplicita:

$$(\mathcal{U}_F/\mathbb{F}_q^*)/U_D = \prod_{P \in D} \mathbb{F}_q[[t_P]]^*/\{x \in \mathbb{F}_q[[t_P]]^* \mid x \equiv 1 \pmod{t_P^{n_P}}\} .$$

Dalla sequenza esatta

$$0 \longrightarrow \mathrm{Jac}(\mathcal{X}) \longrightarrow \mathrm{Pic}(\mathcal{X}) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0$$

si vede che per ogni grado m esiste un campo di classe ray corrispondente al quoziente ciclico di ordine m di $\mathbb{Z}$. Questo è l'estensione del campo delle costanti $\mathbb{F}_{q^m}(\mathcal{X})$. In generale il grado di un'estensione abeliana finita E/F corrispondente ad un $M \subseteq \mathcal{C}_F$ è uguale all'indice di $\deg(M)$ in $\mathbb{Z}$.

Sia $\mathcal{X}_E$ la curva corrispondente all'estensione finita E/F del campo di funzioni $F/\mathbb{F}_q$. Detti

$$S := \{ P \in F \mid P \text{ è un posto completamente separato in } E ,\ \deg(P) = 1 \}$$

ed

$$R := \{ P \in F \mid P \text{ è un posto totalmente ramificato in } E ,\ \deg(P) = 1 \} ,$$

si ha che

$$\#\mathcal{X}_E(\mathbb{F}_q) \geq [E : F] \cdot \#S + \#R ,$$

i.e. più il grado di un'estensione è "grande", maggiore sarà il numero dei punti razionali (si veda [Lor, p. 118]). Ma considerare estensioni "grandi" comporta ad avere curve di genere "grande" (per la formula di Hurwitz (1.3)); buoni risultati si possono ottenere, per esempio, quando tanti posti si separano senza variare il grado dell'estensione. Per semplicità considero la situazione in cui D è un multiplo di un unico posto ed F è il campo di funzioni della retta proiettiva $\mathbb{F}_q(t)$. Allora $\mathrm{Pic}(F) = \mathbb{Z}$ (la funzione grado è un isomorfismo), così se in un'opportuna estensione un solo posto razionale si separa, allora, come vedremo nel successivo teorema, il gruppo di Galois di tale estensione è isomorfo a $(\mathcal{U}_F/\mathbb{F}_q^*)/U_D$, che è dato dal seguente

Lemma 3.4.1 *Sia $D = n_P P$ con $\deg(P) = d \geq 1$. Allora*

$$(\mathcal{U}_F/\mathbb{F}_q^*)/U_D \cong \left(\mathbb{F}_q[t]/(p(t)^{n_P})\right)^*/\mathbb{F}_q^* ,$$

dove $p(t)$ è l'uniformizzante per P, i.e. un polinomio irriducibile di grado d dipendente da P.

Dim. Il conduttore D ha solo un posto nel suo supporto e $\mathcal{C}_{\mathcal{S}}^D$, dove $\mathcal{S} = \mathbf{P}_F \setminus \{P\}$, è il gruppo delle unità per ogni posto che non sta nel supporto di D, quindi

$$\mathcal{U}_F/\mathcal{C}_{\mathcal{S}}^D \cong \mathcal{U}_{F_P}/(1 + \mathfrak{M}_{F_P}^{n_P}) ,$$

dove $\mathfrak{M}_{F_P}$ è l'ideale massimale dell'anello di valutazione discreta $\mathcal{O}_{F_P}$. Allora l'omomorfismo di gruppi

$$\mathcal{U}_{F_P} \to \left(\mathcal{O}_{F_P}/\mathfrak{M}_{F_P}^{n_P}\right)^*$$

è suriettivo ed il suo nucleo è $1 + \mathfrak{M}_{F_P}^{n_P}$. Dunque, per la proposizione 1.2.1(i), ho che

$$\mathcal{O}_{F_P}/\mathfrak{M}_{F_P}^{n_P} \cong \mathbb{F}_q[t]/(p(t)^{n_P}) ,$$

ovvero

$$\left(\mathcal{O}_{F_P}/\mathfrak{M}_{F_P}^{n_P}\right)^* \cong \left(\mathbb{F}_q[t]/(p(t)^{n_P})\right)^* .$$

Quozientando rispetto alle unità in $\mathcal{U}_F/\mathbb{F}_q^*$ ottengo quanto voluto. □

Osservazione 3.4.2 (i) Nella dimostrazione del lemma 3.4.1 si è visto che sussiste l'isomorfismo $\mathcal{O}_{F_P}/\mathfrak{M}_{F_P}^{n_P} \cong \mathbb{F}_q[t]/(p(t)^{n_P})$; vale anche il seguente isomorfismo, che userò nei successivi esempi:

$$\mathcal{O}_{F_P}/\mathfrak{M}_{F_P}^{n_P} \cong \mathbb{F}_q[t]/t^{n_P} ,$$

i.e.

$$(\mathcal{U}_F/\mathbb{F}_q^*)/U_D \cong (\mathbb{F}_q[t]/t^{n_P})^*/\mathbb{F}_q^* .$$

(ii) Se il supporto di D contiene più di un posto, il lemma 3.4.1 è applicabile per ogni primo separatamente. Il quoziente $(\mathcal{U}_F/\mathbb{F}_q^*)/U_D$ è la somma diretta dei fattori ottenuti.

La separazione di più posti in un'opportuna estensione fa si che il gruppo di Galois G sia un quoziente di $(\mathcal{U}_F/\mathbb{F}_q^*)/U_D$:

Teorema 3.4.3 *Sia $D = n_{P_1} P_1$, $\deg(P_1) = 1$. Allora*

$$G \cong \left(\mathbb{F}_q[t]/((t-\alpha_1)^{n_{P_1}})\right)^*/(\mathbb{F}_q^* \cdot < t-\alpha_2, t-\alpha_3, \ldots, t-\alpha_r >)$$

è il gruppo di Galois dell'estensione nella quale gli r posti razionali $P_1, P_2, \ldots, P_r$, con uniformizzante rispettivamente $(t-\alpha_1), (t-\alpha_2), \ldots, (t-\alpha_r) \in \mathbb{F}_q[t]$, sono completamente separati.

Dim. Per la proposizione 1.7.7 un posto P di F si separa completamente se e solo se il suo gruppo di decomposizione è banale. Dalla definizione di gruppo di decomposizione si deduce che per separare un posto razionale basta quozientare il gruppo con questo elemento.

Localmente posso quozientare $\mathcal{U}_{F_P}$ con l'ideale primo corrispondente a P, che è generato da un polinomio della forma $t-\alpha$, $\alpha \in \mathbb{F}_q$.
Il primo posto che si separa uccide il fattore $\mathbb{Z}$ da $\mathcal{C}_F/U_D$. Dalla descrizione di $(\mathcal{U}_F/\mathbb{F}_q^*)/U_D$ data nel lemma 3.4.1 ottengo il risultato voluto quozientando per il sottogruppo generato dagli elementi $t-\alpha_2, t-\alpha_3, \ldots, t-\alpha_r$. □

Per il teorema 3.1.4(ii), il coefficiente del posto P non-ramificato vale zero nel conduttore D dell'estensione. In altre parole, i posti che ramificano devono stare nel supporto di D.
Per studiare la ramificazione di questi posti è utile la seguente:

Definizione 3.4.4 Sia G il gruppo di Galois di un'estensione galoisiana finita E_Q/F_P, dove F_P è il completamento P-adico di F ed E_Q è il completamento Q-adico di E, Q posto di E che sta sopra $P \in \mathbf{P}_F$. Inoltre E_Q/F_P sia tale che il campo dei residui dell'estensione è separabile. Allora per ogni $\sigma \in G$ si definisce il **carattere di Artin** $a_G(\sigma)$ come

$$\begin{aligned} a_G(\sigma) &= -f \cdot v_G(\sigma),\ \sigma \neq 1, \text{ e} \\ a_G(1) &= f \sum_{\sigma \neq 1} v_G(\sigma), \end{aligned}$$

dove $v_G(\sigma) := \nu_E(\sigma(t)-t)$ con t uniformizzante per E, ed f è il grado residuo di $Q|P$.

Definizione 3.4.5 Il **conduttore di Artin** di un carattere χ di G è definito come

$$c(\chi) = (\chi, a_G(\sigma)) = \frac{1}{|G|} \sum_{\sigma \in G} a_G(\sigma)\chi(\sigma^{-1}) \ .$$

Globalmente, se E/F è un'estensione galoisiana finita con gruppo di Galois G e χ è un carattere di G, si definisce il **conduttore globale** di χ la quantità

$$\mathrm{Cond}(\chi) = \prod_{\mathfrak{p}} \mathfrak{p}^{c_{\mathfrak{p}}(\chi)} \ ,$$

dove $c_{\mathfrak{p}}(\chi) := c(\chi, a_{\mathfrak{p}})$, con $a_{\mathfrak{p}}$ carattere di Artin indotto dal carattere di Artin $a_{\mathfrak{P}}$ associato al gruppo di decomposizione $G_Z(\mathfrak{P}|\mathfrak{p})$, $\mathfrak{P}$ primo che sta sopra $\mathfrak{p}$.
Serre introduce il concetto di conduttore di un carattere χ di G per determinare una relazione nota con il nome di formula del discriminante-conduttore. In termini di conduttore, il discriminante dell'estensione E/F è

$$\Delta_{E/F} = \prod_{\chi} \mathrm{Cond}(\chi)^{\chi(1)} \ .$$

Da tale relazione si ottiene una formula per il genere in termini di conduttori dei caratteri di G:

Proposizione 3.4.6 (Führerproduktdiskriminantformel) *Se E/F è un'estensione galoisiana finita con gruppo di Galois G e χ è un carattere irriducibile di G, allora il genere $g(E)$ del ricoprimento è legato al genere della base $g(F)$ come segue:*

$$2g(E) - 2 = [E:F](2g(F)-2) + \deg\left(\prod_{\chi} \mathrm{Cond}(\chi)\right) \ ,$$

dove $\deg\left(\prod_\chi \mathrm{Cond}(\chi)\right) := \sum_\chi \sum_{\mathfrak{p}} c_{\mathfrak{p}}(\chi) \cdot \deg(\mathfrak{p})$.

La formula segue dalla formula di Hurwitz (1.3). Per la dimostrazione si rimanda il lettore alla bibliografia (ad esempio [Ser1]).

Corollario 3.4.7 *Sia $D = P$, $\deg(P) = d \geq 1$. Il conduttore di un carattere χ non banale di $G \cong (\mathcal{U}_F/\mathbb{F}_q^*)/U_D$ è il grado residuo f dell'estensione.*

Dim. In questo caso $|G| = e = (q^d - 1)/(q - 1)$, quindi l'ordine di G è primo con la caratteristica del campo. Ciò significa che non c'è ramificazione selvaggia, quindi $G_1 = \{\mathrm{id}\}$. Poiché nessun elemento non banale sta in G_1, ho che $v_G(\sigma) = 1$ per ogni $\sigma \in G$, $\sigma \neq 1$.
Ora

$$\begin{aligned} c(\chi) &= \frac{1}{e}\Big(a_G(1)\chi(1) + \sum_{\sigma\neq 1} a_G(\sigma)\chi(\sigma^{-1})\Big) \\ &= \frac{1}{e}\Big(f(|G|-1) + \sum_{\sigma\neq 1} -f\cdot\chi(\sigma)\Big)\ . \end{aligned}$$

Questo implica che $c(\chi) = 0$ se χ è banale. Se invece χ non è banale, allora $\sum_{\sigma\in G}\chi(\sigma) = 0$, così $\sum_{\sigma\neq 1}\chi(\sigma) = -\chi(1) = -1$. Dunque

$$c(\chi) = \frac{1}{e}\left(f(|G|-1) + (-f)(-1)\right) = f\ .$$

□

Esempio 3.4.8 Sia $F/\mathbb{F}_2$ un campo di funzioni, $F = \mathbb{F}_2(t)$, e sia $D = P$, $\deg(P) = 3$ (per esempio $P = (t^3 + t + 1) = (T)$). Poiché P ha grado 3, $\mathcal{O}_{F_P} = \mathbb{F}_2[[T]] \cong \mathbb{F}_8[[t]]$ e

$$\begin{aligned} \left(\mathcal{U}_F/\mathbb{F}_2^*\right)/U_D &= \mathbb{F}_2[[T]]^*/\left(1 + T\mathbb{F}_2[[T]]\right) \\ &\cong \mathbb{F}_8[[t]]^*/\left(1 + t\mathbb{F}_8[[t]]\right) \\ &\cong \left(\mathbb{F}_8[[t]]/ < t >\right)^* = \mathbb{F}_8^*\ . \end{aligned}$$

Quindi la seguente sequenza è esatta:

$$0 \to \mathbb{F}_8^* \to \mathcal{C}_F/U_D \to \mathbb{Z} \to 0\ .$$

Per uccidere il fattore infinito di $\mathcal{C}_F/U_D$ considero un punto $\mathbb{F}_2$-razionale R e siano E il campo invariante dell'elemento di Frobenius di R e $\mathcal{X}$ la curva corrispondente all'estensione E/F. Ora

$$G = \mathrm{Gal}(E/F) \cong (\mathcal{U}_F/\mathbb{F}_2^*)/U_D \cong \mathbb{F}_8^*$$

è ciclico di ordine 7, quindi G ha sei caratteri ciclici non banali di grado 3. Dalla proposizione 3.4.6 si ha che

$$2g - 2 = 7\cdot(-2) + 6\cdot 3\ ,$$

i.e. $g = 3$. Poiché per costruzione R si separa completamente, tutti i punti sopra R di $\mathcal{X}$ sono razionali. Allora $\mathcal{X}$ è di genere 3 con almeno sette punti razionali. Il limite di Oesterlé (si veda il teorema 2.3.12) dice che una curva con otto punti razionali ha genere $g \geq 4$, quindi $\mathcal{X}$ ha proprio sette punti ed è quindi massimale per tale genere.

Esempio 3.4.9 Sia $F/\mathbb{F}_2$ un campo di funzioni e sia $D = 4P_\infty$, P_∞ posto razionale. Come nell'esempio 3.4.8, ho che

$$0 \to (\mathcal{U}_F/\mathbb{F}_2^*)/U_D \to \mathcal{C}_F/U_D \to \mathbb{Z} \to 0 \,,$$

dove $(\mathcal{U}_F/\mathbb{F}_2^*)/U_D = \mathbb{F}_2[[T]]^*/\{x \in \mathbb{F}_2[[T]]^* \mid x \equiv 1 \pmod{T^4}\}$ e $T = 1/t$. Quindi

$$(\mathcal{U}_F/\mathbb{F}_2^*)\,/U_D = \left(\mathbb{F}_2[t]/ < t^4 >\right)^* \,.$$

Si può calcolare che

$$(\mathcal{U}_F/\mathbb{F}_2^*)\,/U_D \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

con generatori $1+t$ e $1+t^3$.
Sia E il campo invariante degli elementi di Frobenius degli altri due punti della retta proiettiva 0 e 1. Per costruzione i punti 0, 1 sono separati e P_∞ è ramificato, dunque

$$\mathrm{Gal}(E/F) \cong ((\mathcal{U}_F/\mathbb{F}_2^*)\,/U_D)\,/(t-1) \cong \mathbb{Z}/2\mathbb{Z} \,.$$

Quindi il grado della curva corrispondente all'estensione è 2 e poiché il suo carattere non banale di conduttore $1/t$ ha grado 4, ho che

$$2g - 2 = 2 \cdot (-2) + 4 \,.$$

Trovo quindi una curva di genere 1 con cinque punti razionali, massimale per il genere.

Esempio 3.4.10 (Serre) Sia $F/\mathbb{F}_2$ un campo di funzioni dove il punto P_∞ di $\mathbb{P}^1$ si separa completamente e siano P_2 l'unico posto di grado 2 e P_3 uno dei due posti di grado 3. Cosidero il campo di classe ray di modulo $P_2 + P_3$.
Ci sono due caratteri di conduttore P_2. Essi hanno grado 2. I sei caratteri di conduttore P_3 hanno grado 3 ed i rimanenti dodici caratteri non banali hanno conduttore di grado $2 + 3 = 5$.
Detta $\mathcal{X}$ la curva associata all'estensione, dalla proposizione 3.4.6 ho che

$$2g - 2 = 21 \cdot (2 \cdot 0 - 2) + 2 \cdot 2 + 6 \cdot 3 + 12 \cdot 5 \,,$$

i.e. $g = 21$. Poiché tutti i punti di $\mathcal{X}$ che stanno su P_∞ sono razionali, trovo che la curva $\mathcal{X}$ è di genere 21 ed ha 21 punti razionali, i.e. è massimale per tale genere.

La proposizione 3.4.6 esprime il genere di una curva in termini di gradi dei conduttori dei caratteri del gruppo di Galois. Nella prossima proposizione invece viene espresso il genere di una curva puramente in termini dei gradi dell'estensione e delle sue sottoestensioni:

Proposizione 3.4.11 *Per ogni $1 \le i \le n_P$, sia n_i il grado dell'estensione per la quale esiste un insieme di r posti razionali della base ($D = iP$) che si separano. Sia E l'estensione ottenuta per $i = n_P$. Allora*

$$2g(E) - 2 = -2n_{n_P} + \sum_{i=1}^{n_P} (n_i - n_{i-1})i \,.$$

Dim. La ramificazione avviene per un solo primo, dunque posso considerare la questione in maniera locale.
Dati gli interi arbitrari m, n con $m < n$, la seguente sequenza di gruppi è esatta:

$$0 \to \left(\mathcal{U}_F/\mathbb{F}_q^*\right)^m / \left(\mathcal{U}_F/\mathbb{F}_q^*\right)^n \to \left(\mathcal{U}_F/\mathbb{F}_q^*\right) / \left(\mathcal{U}_F/\mathbb{F}_q^*\right)^n \to \left(\mathcal{U}_F/\mathbb{F}_q^*\right) / \left(\mathcal{U}_F/\mathbb{F}_q^*\right)^m \to 0 \,.$$

Ogni carattere di $\left(\mathcal{U}_F/\mathbb{F}_q^*\right) / \left(\mathcal{U}_F/\mathbb{F}_q^*\right)^m$ è anche un carattere di $\left(\mathcal{U}_F/\mathbb{F}_q^*\right) / \left(\mathcal{U}_F/\mathbb{F}_q^*\right)^n$. Tali caratteri sono caratteri banali di $\left(\mathcal{U}_F/\mathbb{F}_q^*\right)^m / \left(\mathcal{U}_F/\mathbb{F}_q^*\right)^n$ ed hanno conduttore m. È quindi sufficiente contare il numero dei caratteri non banali per ogni $m \leq n_P$. □

Esempio 3.4.12 Siano $q = 4$ e $D = n_P P$ dove $n_P = 4$ e $\deg(P) = 1$. Separando gli altri quattro posti razionali di $F = \mathbb{F}_4(t)$ si ottiene un'estensione di grado 2 nella quale il carattere non banale ha conduttore 4. Ottengo una curva ellittica con il massimo numero di punti su $\mathbb{F}_4$: $g = 1$ e $N_4(g) = 9$.
Se scelgo P come posto corrispondente a 0, allora gli altri quattro posti da separare sono il posto all'infinito, $t+1$, $t+x$ e $t+(x+1)$, dove 0, 1, x, $x+1$ sono gli elementi di $\mathbb{F}_4$. Essi sono legati dalla relazione $x^2 = x+1$. Se scelgo il posto all'infinito per uccidere il fattore infinito nel prodotto $(\mathcal{U}_F/\mathbb{F}_q^*)/U_D \times \mathrm{Pic}(F)$, allora mi rimangono da determinare le immagini degli altri tre elementi in $(\mathbb{F}_4[t]/t^i)^*/\mathbb{F}_4^*$, $i = 1, 2, 3, 4$.
Per prima cosa si noti che, in generale, se $J_i = (\mathbb{F}_q[t]/t^i)^*/\mathbb{F}_q^*$ allora l'ordine di J_i è q^{i-1} e l'ordine di un elemento della forma $1 - \alpha t$ in J_i è p^l, dove p è la caratteristica di $\mathbb{F}_q$ ed l è la più piccola potenza di p tale che $p^l \geq i$.
Quando $i = 1$, J_i è chiaramente banale. Quando $i = 2$, J_i ha ordine 4 ed ogni elemento ha ordine 2, quindi quozientando i tre elementi ottengo il gruppo banale. Quando $i = 3$, J_i ha ordine 16 ma ogni elemento ha ordine 4 e così ottengo ancora il gruppo banale. Infine, quando $i = 4$, J_i ha ordine 64 e ogni elemento ha ordine 4, ma la seconda potenza del terzo elemento sta nel gruppo generato dagli altri due:

$$(t+1)^2(t+x)^2 \equiv (t+(x+1))^2 \pmod{t^4} .$$

Dunque il grado dell'estensione è 2.
Il calcolo del genere si basa sul fatto che solo il carattere non banale ha conduttore 4. Dalla formula del genere data nella proposizione 3.4.11 ho che

$$2g - 2 = -2 \cdot 2 + (2-1) \cdot 4 ,$$

i.e. $g = 1$.
Poiché un posto è totalmente ramificato e gli altri quattro sono completamente separati, la curva ha nove punti razionali ed è quindi massimale.

Esempio 3.4.13 Siano $q = 4$ e $D = n_P P$ dove $n_P = 6$ e $\deg(P) = 1$. Separando gli altri quattro punti razionali di $F = \mathbb{F}_4(t)$ si ottiene un'estensione di grado 8 nella quale un carattere ha conduttore 4 e sei caratteri hanno conduttore 6. Tale estensione corrisponde ad una curva di genere $g = 13$ con 33 punti razionali, il massimo possibile in accordo con il limite di Oesterlé.
Tenendo conto anche dell'esempio 3.4.12, posso come prima cosa vedere se ci sono caratteri di conduttore 5. Poiché $|J_5| = 4^4$ ed $l = 3$, non ci sono elementi di ordine maggiore di 8. Il quoziente ha ordine almeno 2, poiché contiene l'estensione corrispondente ad $i = 4$ come sottoestensione. Dico che l'ordine è proprio 2; la seconda potenza del terzo elemento è ancora contenuta nel gruppo generato dagli altri due:

$$(t+(x+1))^2 \equiv (t+1)^6(t+x)^6 \pmod{t^5} .$$

L'ordine del quoziente fatto rispetto a questi tre elementi non può essere maggiore di quello fatto rispetto agli altri due. Se l'ordine fosse 4 otterrei una curva di genere 4 con 17 punti razionali, in contraddizione con il limite di Oesterlé (si veda la Tavola 1). Poiché il grado

dell'estensione non aumenta da $i = 4$ a $i = 5$, non ci sono caratteri di conduttore 5.
L'ordine di J_6 è 4^5 ed ogni elemento ha ordine 8, ma ancora la seconda potenza del terzo elemento sta nel gruppo generato dagli altri due, perché

$$(t+1)^6(t+x)^6 \equiv (t+(x+1))^2 \pmod{t^6} .$$

Ancora il grado dell'estensione nella quale tutti e quattro i punti si separano non può essere più grande di 8, perché se il grado fosse 16 otterrei una curva di genere 29 con 65 punti razionali, e questo violerebbe il limite di Oesterlé (si veda la Tavola 1). Il grado dell'estensione è quindi 8 e così si ottiene una curva con 33 punti razionali di genere g tale che

$$2g - 2 = -2 \cdot 8 + 4 + 6 \cdot (8 - 2) .$$

Esempio 3.4.14 Siano $q = 4$ e $D = n_P P$ dove $n_P = 7$ e $\deg(P) = 1$. Separando gli altri quattro punti razionali di $F = \mathbb{F}_4(t)$ si ottiene un'estensione di grado 16 nella quale un carattere ha conduttore 4, sei caratteri hanno conduttore 6 ed otto caratteri hanno conduttore 7. Ottengo così un curva di genere 33 con 65 punti razionali[1].
L'ordine di J_7 è 4^6 e la quarta potenza del terzo elemento sta nel gruppo generato dagli altri due:

$$(t+1)^4(t+x)^4 \overset{(t^7)}{\equiv} (x+1)t^4 + x = t^4 + (x+1) = (t+(x+1))^4 .$$

L'estensione ha grado 16, infatti se avesse grado 32 otterrei una curva di genere 73 con 129 punti razionali, e ciò non è possibile.
Ottengo così una curva con 65 punti razionali di genere g dato da

$$2g - 2 = -2 \cdot 16 + 4 + 6 \cdot 6 + 7 \cdot (16 - 8) .$$

Poché su F ci sono solamente cinque posti razionali, uno dei quali sta nel supporto di D, non è possibile separare più di quattro posti. Separandone tre, si possono ottenere risultati interessanti:

Esempio 3.4.15 Per $q = 4$, $D = n_P P$, $n_p = 6$ e $\deg(P) = 1$ si ottiene una curva di genere 27 con 49 punti razionali.
Il primo carattere non banale si ottiene per $i = 4$ ed il grado di tale estensione è 4. Il grado vale 16 quando $i = 6$. Questa estensione corrisponde ad una curva con $3 \cdot 16 + 1 = 49$ punti razionali di genere dato da

$$2g - 2 = -2 \cdot 16 + 4 \cdot 3 + 6 \cdot (16 - 4) .$$

3.5 Campi di funzione dei campi di classe di Hilbert

Per un campo di funzioni $F/\mathbb{F}_q$ con un posto razionale P_∞, il campo di classe di $\mathcal{S}$-Hilbert $\mathcal{H}_\mathcal{S}$ di F, dove $\mathcal{S} := \mathbf{P}_F \setminus \{P_\infty\}$, è un'estensione abeliana finita non-ramificata di F nella quale P_∞ si separa completamente. Oltre a ciò, $[\mathcal{H}_\mathcal{S} : F] = h(F)$ ed il gruppo di Galois $\mathrm{Gal}(\mathcal{H}_\mathcal{S}/F)$ è isomorfo al gruppo $\mathrm{Cl}(F)$ delle classi dei divisori di grado zero di F. Questo isomorfismo induce una corrispondenza fra il simbolo di Artin in $\mathcal{H}_\mathcal{S}/F$ di un posto P di F e la classe dei divisori $[P - \deg(P)P_\infty]$.

[1] È il primo esempio trovato per questo genere su $\mathbb{F}_4$.

Per costruire un sottocampo K di $\mathcal{H}_{\mathcal{S}}/F$ con posti razionali $P_1, P_2, \ldots, P_r$ di F che si separano completamente in K/F si può scegliere K, in accordo con la proposizione 1.7.10, tale che $\mathrm{Gal}(\mathcal{H}_{\mathcal{S}}/K)$ contenga le classi di divisori $[P_i - P_\infty]$ per ogni $i = 1, 2, \ldots, r$.
Operando in questo modo si riesce ad enunciare alcuni principi generali per costruire un campo di funzioni con molti posti razionali.
Come prima cosa presento un semplice esempio per illustrare la potenza di questo metodo.

Esempio 3.5.1 Sia $F = \mathbb{F}_2(x, y)$ l'estensione di Artin-Schreier del campo delle funzioni razionali $\mathbb{F}_2(x)$ definito dall'equazione

$$y^2 + y = \frac{(x+1)(x^2+x+1)(x^3+x+1)}{x^3} .$$

Allora $g(F) = 3$ per il teorema A.2.2 e $h(F) = 24$. Sia P_∞ l'unico posto di F che sta sopra al posto infinito di $\mathbb{F}_2(x)$ e sia $\mathcal{H}_{\mathcal{S}}$ il campo di classe di $\mathcal{S}$-Hilbert di F, dove $\mathcal{S} = \mathbf{P}_F \setminus \{P_\infty\}$. Sia P l'unico zero di x in F e C il sottogruppo ciclico di $\mathrm{Cl}(F)$ generato dalle classi di divisori $[P - P_\infty]$. Poiché il divisore principale $(x) = 2P - 2P_\infty$ e vale il corollario 1.4.12 si ha che $|C| = 2$. Dunque, se K è un sottocampo di $\mathcal{H}_{\mathcal{S}}/F$ fissato da C, allora K/F è un'estensione non-ramificata di grado 12 nella quale P_∞ e P si separano completamente. Quindi $g(K) = 25$ e $N(K) \geq 24$. Ma $N_2(25) \leq 24$ per il teorema 2.3.12, dunque $N(K) = 24$ e K è un campo di funzioni ottimale.

Teorema 3.5.2 *Sia q dispari, S un sottoinsieme di $\mathbb{F}_q$, $n = |S|$. Si scelga un polinomio $f \in \mathbb{F}_q[x]$ tale che $\deg(f)$ sia dispari, f non abbia radici multiple e $f(c) = 0$ per ogni $c \in S$. Per il campo di funzioni $F = \mathbb{F}_q(x, y)$ con $y^2 = f(x)$ si assuma che il suo numero di classe $h(F)$ sia divisibile per $2^n m$ per qualche intero m. Allora esiste un campo di funzioni $K/\mathbb{F}_q$ tale che*

$$g(K) = \frac{h(F)}{2^{n+1}m}(\deg(f) - 3) + 1 \quad \text{e} \quad N(K) \geq \frac{(n+1)h(F)}{2^n m} ,$$

dove vale l'uguaglianza per $n = q$.

Dim. Poiché $F/\mathbb{F}_q(x)$ è un'estensione di Kummer, per il teorema A.2.1 ho che

$$g(F) = \frac{1}{2}(\deg(f) - 1) .$$

Per ogni $c \in S$ il posto $x - c$ di $\mathbb{F}_q(x)$ è totalmente ramificato in $F/\mathbb{F}_q(x)$ e quindi è un polo di x in $\mathbb{F}_q(x)$. Denoto con P_∞ l'unico posto di F che sta sopra al polo di x in $\mathbb{F}_q(x)$. Per il divisore principale $(x - c)$ dunque si ha che

$$(x - c) = 2P_c - 2P_\infty ,$$

dove P_c è un posto razionale di F, $c \in S$.
Di conseguenza la classe di divisori $[P_c - P_\infty]$ ha ordine 1 o 2 nel gruppo $\mathrm{Cl}(F)$ e quindi il sottogruppo S di $\mathrm{Cl}(F)$ è generato da tutte le classi di divisori $[P_c - P_\infty]$ con $c \in S$ ed ha ordine che divide 2^n. Segue che deve esistere un sottogruppo G di $\mathrm{Cl}(F)$ tale che $|G| = 2^n m$ e $G \subseteq S$.
Sia $\mathcal{H}_{\mathcal{S}}$ il campo di classe di $\mathcal{S}$-Hilbert di F, $\mathcal{S} = \mathbf{P}_F \setminus \{P_\infty\}$, e sia K un sottocampo di $\mathcal{H}_{\mathcal{S}}$ contenente F e fissato da G. Allora

$$[K : F] = \frac{h(F)}{2^n m} .$$

Per costruzione, i posti P_∞ e P_c, $c \in S$, si separano completamente nell'estensione K/F e questo dà il limite inferiore per $N(K)$ enunciato. Inoltre, K/F è un'estensione non-ramificata e quindi la formula per $g(K)$ segue direttamente dalla formula di Hurwitz (1.3). □

La costruzione data dal teorema 3.5.2 si basa su estensioni quadratiche del campo delle funzioni razionali. Tale costruzione può essere generalizzata come segue:

Teorema 3.5.3 *Sia $F/\mathbb{F}_q$ un campo di funzioni ed $L/\mathbb{F}_q$ un'estensione separabile finita di F. Sia $\mathcal{S} = \mathbf{P}_F \setminus \{P, P_1, P_2, \ldots, P_m\}$, dove P è un posto razionale di F ed i P_i sono arbitrari posti di F diversi da P, $i = 1, 2, \ldots, m$. Si supponga che qualche posto in $\mathcal{S}$ sia totalmente ramificato in L/F. Sia $\mathcal{T}'$ il sopra-insieme di $\mathcal{S}' = \{P, P_1, P_2, \ldots, P_m\}$ rispetto all'estensione L/F e si assuma che n posti razionali in $\mathcal{T}'$ siano positivi. Allora esiste un campo di funzioni $K/\mathbb{F}_q$ tale che*

$$g(K) = \frac{h(F)}{|G|}(g(L) - 1) \quad \text{e} \quad N(K) \geq \frac{h(F)n}{|G|} ,$$

dove G è il sottogruppo di $\mathrm{Cl}(F)$ generato dalle classi dei divisori $[P_1 - \deg(P_1)P]$, $[P_2 - \deg(P_2)P], \ldots, [P_m - \deg(P_m)P]$.

Dim. Sia J il sottogruppo di $\mathrm{Pic}(F)$ generato dalle classi dei divisori $[P], [P_1]$, $[P_2], \ldots, [P_m]$. Poiché $\mathcal{S}'$ contiene il posto razionale P, il gruppo $\mathrm{Pic}(F)$ è generato da $\mathrm{Cl}(F)$ e J. Dalla sequenza esatta

$$0 \to \mathrm{Cl}(F)/(J \cap \mathrm{Cl}(F)) \to \mathrm{Cl}(\mathcal{O}_S) \to \mathrm{Pic}(F)/\mathrm{Cl}(F) \cdot J \to 0$$

ottengo che

$$\mathrm{Cl}(\mathcal{O}_\mathcal{S}) \cong \mathrm{Cl}(F)/(J \cap \mathrm{Cl}(F)) ,$$

dove $\mathrm{Cl}(\mathcal{O}_S)$ è il gruppo delle classi degli $\mathcal{S}$-ideali di F. Segue che

$$r := |\mathrm{Cl}(\mathcal{O}_S)| = \frac{h(F)}{|G|} .$$

Per la condizione su $\mathcal{S}$ e per [Ros2, prop. 2.2] si ha che r divide $|\mathrm{Cl}(\mathcal{O}_\mathcal{T})|$, dove $\mathcal{O}_\mathcal{T}$ è il gruppo delle classi di $\mathcal{T}$-ideali di L, $\mathcal{T} := \mathbf{P}_L \setminus \mathcal{T}'$.
Sia $\mathcal{H}_\mathcal{T}$ il campo di classe di $\mathcal{T}$-Hilbert di L. Allora, visto che $n \geq 1$, $\mathrm{Gal}(\mathcal{H}_\mathcal{T}/L) \cong \mathrm{Cl}(\mathcal{O}_\mathcal{T})$ e $\mathcal{H}_\mathcal{T}$ è una chiusura algebrica di $\mathbb{F}_q$. Sia $K/\mathbb{F}_q$ un sottocampo di $\mathcal{H}_\mathcal{T}$ contenente L e fissato da un sottogruppo di $\mathrm{Cl}(\mathcal{O}_\mathcal{T})$ di ordine $\frac{1}{r}|\mathrm{Cl}(\mathcal{O}_\mathcal{T})|$. Allora $[K : L] = r$.
Poiché $\mathcal{H}_\mathcal{T}/L$ è un'estensione non-ramificata, la formula di Hurwitz (1.3) dà

$$g(K) - 1 = r(g(L) - 1) = \frac{h(F)}{|G|}(g(L) - 1) .$$

Inoltre tutti i posti in $\mathcal{T}'$ si separano completamente in K/L e quindi $N(K) \geq rn$. □

Esempio 3.5.4 *$g(K/\mathbb{F}_3) = 37$ ed $N(K/\mathbb{F}_3) = 48$.*
Considero il campo di funzioni $F = \mathbb{F}_3(x, y)$ e l'equazione

$$y_1^2 = x(x^4 - x^3 + x^2 - x + 1) .$$

Allora $g(F) = 2$, $N(F) = 6$ ed F ha sei posti di grado 2; quindi $h(F) = 24$. Il divisore principale (x) in F assume la forma $(x) = 2P_1 - 2P_\infty$, dove P_1, P_∞ sono posti razionali di F.
Sia $L = F(y_2)$ e considero l'equazione

$$y_2^2 = x + 1 \ .$$

Allora $g(L) = 4$ perché gli unici posti di F che ramificano nell'estensione di Kummer L/F sono quelli che stanno su $x + 1$. Ora posso ottenere K come nel teorema 3.5.3, ponendo $\mathcal{S} = \mathbf{P}_F \setminus \{P_\infty, P_1\}$. La condizione su $\mathcal{S}$ data dal teorema 3.5.3 è soddisfatta, infatti i posti di F che stanno su $x + 1$ sono totalmente ramificati in L/F.
Inoltre $n = 4$ perché tutti i posti in $\mathcal{S}'$ si separano completamente in L/F. Si ha anche $|G| = 2$.
Per il teorema 3.5.3 quindi $g(K/\mathbb{F}_3) = 37$ e $N(K/\mathbb{F}_3) \geq 48$. Ma per il metodo illustrato nel teorema 2.3.12 ho che $N(K/\mathbb{F}_3) \leq 54$, quindi $N(K/\mathbb{F}_3) = 48$.

Esempio 3.5.5 *$g(K/\mathbb{F}_3) = 51$ ed $N(K/\mathbb{F}_3) = 60$.*
Considero il campo di funzioni $F = \mathbb{F}_3(x, y_1)$ e l'equazione

$$y_1^2 = (x + 1)(x - 1)(x^2 + x - 1)(x^3 - x + 1) \ .$$

Allora $g(F) = 3$, $N(F) = 5$ ed F ha tre posti di grado 2 e cinque posti di grado 3, quindi $h(F) = 40$.
In F si ha che $(x + 1) = 2P_1 - 2P_\infty$ e $(x - 1) = 2P_2 - 2P_\infty$, dove P_1, P_2, P_∞ sono posti razionali di F.
Sia $L = F(y_2)$ e considero l'equazione

$$y_2^2 = x(x^2 + x - 1) \ .$$

Allora $g(L) = 6$ perché gli unici posti di F che ramificano nell'estensione di Kummer L/F sono quelli che stanno sopra x.
Ora posso ottenere K come dal teorema 3.5.3, ponendo $\mathcal{S} = \mathbf{P}_F \setminus \{P_1, P_2, P_\infty\}$. La condizione del teorema 3.5.3 su $\mathcal{S}$ è soddisfatta poiché i posti su F che stanno su x sono totalmente ramificati in L/F.
Inoltre $n = 6$ perché tutti i posti di $\mathcal{S}'$ si separano completamente in L/F. Si ha anche $|G| = 4$.
Per il teorema 3.5.3 quindi $g(K/\mathbb{F}_3) = 51$ e $N(K/\mathbb{F}_3) \geq 60$. Ma per il teorema 2.3.12 ho che $N(K/\mathbb{F}_3) \leq 69$, quindi $N(K/\mathbb{F}_3) = 60$.

Capitolo 4

Prodotti fibrati di curve di Artin-Schreier su $\mathbb{P}^1$

In questo capitolo verranno esposti tre metodi per determinare curve con molti punti razionali. Le curve ottenute saranno il prodotto fibrato (più precisamente la sua normalizzazione) di opportune famiglie di curve di Artin-Schreier.
Tali metodi nascono per esigenze applicative (teoria dei codici, crittografia) e perciò la terminologia usata negli articoli dai quali è tratta questa esposizione è altamente tecnica (la maggior parte del materiale è tratta dagli articoli di van der Geer e Van der Vlugt [G-V1], [G-V2], [G-V3], [G-V4]; per il secondo metodo si faccia riferimento all'articolo di Kawakita e Miura [K-M]).
Precisamente nel materiale da me raccolto vengono risolti alcuni problemi della teoria dei codici. Tale materiale è stato riesposto qui usando per il possibile le strutture e la terminologia note della matematica pura.
Il primo metodo utilizza informazioni che saranno date in modo completo. Il secondo ed il terzo metodo fanno riferimento anche alla teoria degli spazi quadratici, per i quali si troverà una completa esposizione in [Bue].

4.1 Lo spazio traccia e le curve $\mathcal{X}_{a,b}$

Considero un sotto-$\mathbb{F}_{q^m}$-spazio vettoriale V di $\mathbb{F}_{q^m}^n$ e definisco la **norma** di $v \in V$ la quantità $\mathrm{N}_{\mathbb{F}_{q^m}}(v) = \mathrm{N}(v) = \mathrm{N}((v_1, v_2, \ldots, v_n)) := \#\{i \mid v_i \neq 0\,,\ v_i \in \mathbb{F}_{q^m}\}$ (il valore assoluto è quello banale).
Una buona quantità di informazioni sullo spazio V possono essere dedotte dalla conoscenza del polinomio

$$P(x) = \sum_{v \in V} x^{\mathrm{N}(v)} = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]\,, \tag{4.1}$$

dove $a_i = \#\{v \in V \mid \mathrm{N}(v) = i\}$.
Per ragioni applicative è interessante capire come si può ottenere lo spazio V su un campo primo $\mathbb{F}_p$ da uno spazio U su un'estensione di $\mathbb{F}_p$. Considererò due modi per fare questo: applicare la funzione traccia o la mappa di restrizione. Definirò i due enti ed analizzeremo il primo modo anche nel caso di campi non primi.

Considero un'estensione di Galois $\mathbb{F}_{q^m}/\mathbb{F}_q$ di grado $m = [\mathbb{F}_{q^m} : \mathbb{F}_q]$. Sia

$$\mathrm{Tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q$$

la funzione traccia.
Considero un sotto-$\mathbb{F}_{q^m}$-spazio vettoriale U di $\mathbb{F}_{q^m}^n$. Per ogni elemento $u = (u_1, u_2, \ldots, u_n)$ in $\mathbb{F}_{q^m}^n$ definisco

$$\mathrm{Tr}(u) := (\mathrm{Tr}(u_1), \mathrm{Tr}(u_2), \ldots, \mathrm{Tr}(u_n)) \in \mathbb{F}_q^n \ .$$

In questo modo ottengo un'applicazione $\mathbb{F}_q$-lineare

$$\mathrm{Tr} : \mathbb{F}_{q^m}^n \to \mathbb{F}_q^n \ .$$

Definizione 4.1.1 Sia $U \subseteq \mathbb{F}_{q^m}^n$ un $\mathbb{F}_{q^m}$-spazio vettoriale.

(i) $U|_{\mathbb{F}_q} := U \cap \mathbb{F}_q^n$ è detta la **restrizione** di U ad $\mathbb{F}_q$.

(ii) $\mathrm{Tr}(U) := \{\mathrm{Tr}(u) \mid u \in U\} \subseteq \mathbb{F}_q^n$ è chiamato **spazio traccia** di U.

Un esempio di spazio traccia che userò più avanti è il seguente.
Fissato $h \geq 0$, pongo

$$\mathcal{R}_h = \left\{ R(x) = \sum_{i=0}^{h} c_i x^{q^i} \mid c_i \in \mathbb{F}_{q^m} \right\} .$$

Questo è un $\mathbb{F}_{q^m}$-spazio vettoriale di polinomi additivi.
Siano $\{x_1, x_2, \ldots, x_{q^m}\}$ gli elementi di $\mathbb{F}_{q^m}$ e considero l'applicazione $\mathbb{F}_{q^m}$-lineare

$$\varphi : \mathcal{R}_h \to \mathbb{F}_{q^m}^{q^m} \quad , \quad R(x) \mapsto \big(x_1 R(x_1), x_2 R(x_2), \ldots, x_{q^m} R(x_{q^m})\big) \ .$$

Lo spazio traccia $V_h = \mathrm{Tr}\big(\varphi(\mathcal{R}_h)\big)$ è definito come

$$V_h := \left\{ v_{R(x)} = (\mathrm{Tr}(x_i R(x_i))_{1 \leq i \leq q^m}) \mid R(x) \in \mathcal{R}_h \right\} \subseteq \mathbb{F}_q^{q^m} \ .$$

Poiché i polinomi additivi si comportano come funzioni $\mathbb{F}_q$-lineari, $\mathrm{Tr}(x_i R(x_i))_{1 \leq i \leq q^m}$ definisce una forma quadratica sull'$\mathbb{F}_q$-spazio vettoriale $\mathbb{F}_{q^m}$.
Dal teorema 90 di Hilbert (si consulti l'appendice A) ho che la norma $\mathrm{N}\left(v_{R(x)}\right)$ dell'elemento $v_{R(x)} \in V_h$ è data dalla relazione

$$\begin{aligned} \mathrm{N}(v_{R(x)}) &= \#\left\{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}(x_i R(x_i)) \neq 0 \,,\ 1 \leq i \leq q^m\right\} \\ &= q^m - \frac{1}{q}(\#\mathcal{X}_R(\mathbb{F}_{q^m}) - 1) \,, \end{aligned} \tag{4.2}$$

dove $\#\mathcal{X}_R(\mathbb{F}_{q^m}) = N_m$ è il numero dei punti $\mathbb{F}_{q^m}$-razionali della curva $\mathcal{X}_R$ data dall'equazione

$$y^q - y = xR(x) \ . \tag{4.3}$$

Quindi c'è una corrispondenza biunivoca fra gli elementi non nulli di V_h e le curve date in (4.3). In altre parole, gli spazi traccia sono legati a famiglie di curve di tipo Artin-Schreier (vedere l'appendice A) e la **distribuzione delle norme** (i.e. gli interi $a_1, a_2, \ldots, a_n$ dati in (4.1)) è equivalente alla distribuzione del numero di punti razionali sulle curve della famiglia. È importante notare che gli elementi di V_h di norma "piccola" corrispondono a curve con tanti punti razionali.

Un altro esempio di curve che studierò in seguito sono delle particolari curve di Artin-Schreier, chiamate curve a-b, che denoto con $\mathcal{X}_{a,b}$, $a, b \in \mathbb{Z}$ (una trattazione più dettagliata, completa di dimostrazioni, si può trovare in [Miu]):

Definizione 4.1.2 Siano a e b interi relativamente primi tra loro e soddisfacenti la condizione $2 \leq a < b$. Una **curva** $\mathcal{X}_{a,b}$ è una curva proiettiva definita dall'equazione (affine)

$$f(x,y) := \sum_{ai+bj \leq ab} \alpha_{ij} x^i y^j = 0 \ , \tag{4.4}$$

dove $\alpha_{ij} \in F$, $\alpha_{0a} \neq 0$, $\alpha_{b0} \neq 0$.

Teorema 4.1.3 *Sia $\mathcal{X}$ una curva $\mathcal{X}_{a,b}$ definita su $\mathbb{F}_q$.*

(i) *L'equazione* (4.4) *è assolutamente irriducibile su $\mathbb{F}_q$.*

(ii) *Il genere di $\mathcal{X}$ soddisfa*

$$g(\mathcal{X}) \leq \frac{(a-1)(b-1)}{2} \ ,$$

dove vale l'uguaglianza se e solo se $\mathcal{X}$ è liscia almeno in tutti i suoi punti $P \neq P_\infty$, dove P_∞ è il punto all'infinito.

Un tipo di curva $\mathcal{X}_{a,b}$ è il seguente: sia $P(x) \in \mathbb{F}_{q^m}[x]$ e $d := \deg(P(x))$ tale che $\mathrm{MCD}(q,d) = 1$ (MCD è il massimo comun divisore). La curva proiettiva $\mathcal{X}_{q,d}$ definita dall'equazione (affine)

$$y^q - y = P(x)$$

è una curva del tipo $\mathcal{X}_{a,b}$ che può essere singolare solamente nel punto all'infinito. Quindi per il teorema 4.1.3 il suo genere è

$$g(\mathcal{X}_{q,d}) = \frac{(q-1)(d-1)}{2}. \tag{4.5}$$

Dal teorema 90 di Hilbert si ha che il numero di punti razionali su $\mathbb{F}_{q^m}$ di $\mathcal{X}_{q,d}$ è

$$\#\mathcal{X}_{q,d}(\mathbb{F}_{q^m}) = \#\{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}(P(x)) = 0\} \cdot q + 1 \ . \tag{4.6}$$

4.2 Il prodotto fibrato di curve di Artin-Schreier

Sia W un sottospazio r-dimensionale di un $\mathbb{F}_q$-spazio vettoriale V di $\mathbb{F}_q^n$. La **norma di** W è definita come

$$\begin{aligned} \mathrm{N}(W) &:= \frac{1}{q^r - q^{r-1}} \sum_{w \in W} \mathrm{N}(w) \\ &= n - \#\{1 \leq i \leq n \mid w_i = 0 \ \text{ per ogni } w \in W\} \ . \end{aligned}$$

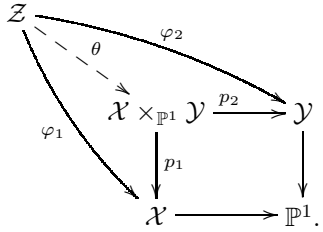
Come gli spazi traccia sono collegati con curve di tipo Artin-Schreier, in maniera analoga i sottospazi degli spazi traccia sono legati al prodotto fibrato di tali curve. Vediamolo in dettaglio.

Definizione 4.2.1 Siano $\mathcal{X}$, $\mathcal{Y}$ due curve sopra $\mathbb{P}^1$, i.e. due curve con un fissato morfismo in $\mathbb{P}^1$. Si definisce il **prodotto fibrato** di $\mathcal{X}$ ed $\mathcal{Y}$ su $\mathbb{P}^1$, denotato con $\mathcal{X} \times_{\mathbb{P}^1} \mathcal{Y}$, come una curva con morfismi $p_1 : \mathcal{X} \times_{\mathbb{P}^1} \mathcal{Y} \to \mathcal{X}$ e $p_2 : \mathcal{X} \times_{\mathbb{P}^1} \mathcal{Y} \to \mathcal{Y}$ tali che

(i) Il diagramma con i morfismi $\mathcal{X} \to \mathbb{P}^1$ e $\mathcal{Y} \to \mathbb{P}^1$ sia commutativo:

$$\begin{array}{ccc} \mathcal{X} \times_{\mathbb{P}^1} \mathcal{Y} & \xrightarrow{p_2} & \mathcal{Y} \\ \downarrow{\scriptstyle p_1} & & \downarrow \\ \mathcal{X} & \longrightarrow & \mathbb{P}^1; \end{array}$$

(ii) Data una terza curva $\mathcal{Z}$ sopra $\mathbb{P}^1$ e dati i morfismi $\varphi_1 : \mathcal{Z} \to \mathcal{X}$ e $\varphi_2 : \mathcal{Z} \to \mathcal{Y}$ tale che il diagramma con i morfismi $\mathcal{X} \to \mathbb{P}^1$ e $\mathcal{Y} \to \mathbb{P}^1$ sia commutativo, allora esiste un unico morfismo $\theta : \mathcal{Z} \to \mathcal{X} \times_{\mathbb{P}^1} \mathcal{Y}$ tale che $\varphi_1 = p_1 \circ \theta$ e $\varphi_2 = p_2 \circ \theta$:



I morfismi p_1 e p_2 sono chiamati **proiezioni** del prodotto fibrato sui suoi fattori.

Teorema 4.2.2 *Date due curve $\mathcal{X}$ e $\mathcal{Y}$ su $\mathbb{P}^1$, il prodotto fibrato $\mathcal{X} \times_{\mathbb{P}^1} \mathcal{Y}$ esiste ed è unico a meno di isomorfismi.*

Il teorema discende da un fatto più generale. Si può trovare una sua dimostrazione in [Har, p. 87].

Considero un sotto-$\mathbb{F}_{q^m}$-spazio vettoriale $\mathcal{L}$ di dimensione finita del campo delle funzioni razionali $\mathbb{F}_{q^m}(x)$ tale che $\mathcal{L} \cap \mathbb{F}_{q^m} = \{0\}$. Sia $\mathbf{P}$ un fissato sottoinsieme di $\mathbb{P}^1(\mathbb{F}_{q^m})$ contenente i poli di ordine relativamente primo con p di ogni elemento di $\mathcal{L} \setminus \{0\}$. Da notare che per V_h si ha $\mathbf{P} = \{\infty\}$.
Considero lo spazio traccia V di dimensione $n = q^m + 1 - \#\mathbf{P}$, i cui elementi sono della forma

$$v_f = (\mathrm{Tr}(f(x_i))_{1 \le i \le n}) \ ,$$

dove $\{x_1, x_2, \ldots, x_n\}$ è l'insieme degli elementi di $\mathbb{P}^1(\mathbb{F}_{q^m}) \setminus \mathbf{P}$. Sia W un sotto-$\mathbb{F}_q$-spazio r-dimensionale di V di base $w_{f_1}, w_{f_2}, \ldots, w_{f_r}$. A questi elementi corrispondono delle funzioni $f_1, f_2, \ldots, f_r$ di $\mathcal{L}$, le quali formano un sotto-$\mathbb{F}_q$-spazio vettoriale r-dimensionale $\mathcal{L}_W$ di $\mathcal{L}$.
Sia $\mathcal{X}_{f_i}$ la curva definita dall'equazione (affine)

$$y_i^q - y_i = f_i(x) \quad , \ i = 1, 2, \ldots, r \ .$$

Ognuna di queste curve è un'estensione di Artin-Schreier di $\mathbb{P}^1$ che quindi corrisponde ad un ricoprimento

$$\phi_i : \mathcal{X}_{f_i} \to \mathbb{P}^1 \ ,$$

dato dall'inclusione $\mathbb{F}_{q^m}(x) \subset \mathbb{F}_{q^m}(x, y_i)$ per ogni $i = 1, 2, \ldots, r$.
Allora è possibile associare al sottospazio W di V la curva

$$\mathcal{X}_W = \text{normalizzazione di } (\mathcal{X}_{f_1} \times_{\mathbb{P}^1} \mathcal{X}_{f_2} \times_{\mathbb{P}^1} \cdots \times_{\mathbb{P}^1} \mathcal{X}_{f_r}) \ , \tag{4.7}$$

la normalizzazione (si confronti l'appendice B) del prodotto fibrato delle $\mathcal{X}_{f_i}$ su $\mathbb{P}^1$ rispetto ai morfismi ϕ_i. A meno di isomorfismi, come si può verificare in [G-V4], questo non dipende dalla base di W scelta.

Vale la seguente generalizzazione della (4.2) che mette in relazione la norma di un sottospazio W ed il numero di punti $\mathbb{F}_{q^m}$-razionali di $\mathcal{X}_W$:

Proposizione 4.2.3 *La norma di un sottospazio W di dimensione r di uno spazio traccia V di $\mathbb{F}_{q^m}$ è legato al numero di punti $\mathbb{F}_{q^m}$-razionali di $\mathcal{X}_W$ dalla relazione*

$$\mathrm{N}(W) = n - \frac{1}{q^r}\Big(\#\mathcal{X}_W(\mathbb{F}_{q^m}) - \sum_{P\in\mathbf{P}_1} q^{s_P}\Big)\ ,$$

dove: $\mathbf{P}_1$ è l'insieme dei $P \in \mathbf{P}$ tali che esiste $f \in \mathcal{L}_W$ regolare in P con $\mathrm{Tr}\big(f(P)\big) = 0$ oppure P sia un polo di qualche $f \in \mathcal{L}_W \setminus \{0\}$; $s_P = \#\{f \in \mathcal{L}_W \mid f$ è regolare in $P \in \mathbf{P}_1\}$.

Dim. Sia $z(W) = \#\{1 \le i \le n \mid w_i = 0$ per ogni $w \in W\}$. Quindi $\mathrm{N}(W) = n - z(W)$.
Un punto $P \in \mathbb{P}^1(\mathbb{F}_{q^m}) \setminus \mathbf{P}$ è uno zero comune a tutti gli elementi di W se e solo se $\mathrm{Tr}(f(P)) = 0$ per ogni $f \in \mathcal{L}_W$. Questo equivale a dire che il numero di punti $\mathbb{F}_{q^m}$-razionali della curva $\mathcal{X}_{f_i}$ che stanno sopra P è uguale a q per ogni $i = 1, 2, \ldots, r$. Ora la fibra sopra P su $\mathcal{X}_W$ od ha q^r punti $\mathbb{F}_{q^m}$-razionali o non ha nessun punto razionale su $\mathbb{F}_{q^m}$. Ciò dipende se tutte le curve $\mathcal{X}_{f_i}$ o meno hanno q punti $\mathbb{F}_{q^m}$-razionali sopra P (per le proprietà del prodotto fibrato si faccia riferimento a [Liu]). Quindi $\mathcal{X}_W$ ha $q^r z(W)$ punti $\mathbb{F}_{q^m}$-razionali sopra i punti $P \in \mathbb{P}^1(\mathbb{F}_{q^m}) \setminus \mathbf{P}$.
Rimangono da considerare i punti P di $\mathbf{P}$. Dal corollario 1.7.4, per un punto P di $\mathbf{P}$ ho che $e_P f_P s = [\mathbb{F}_{q^m}(x, y_i) : \mathbb{F}_{q^m}(x)] = q$, dove s è il numero dei punti di $\mathcal{X}_{f_i}$ che stanno sopra P, $1 \le i \le r$. Voglio che $f_P = 1$ per ogni $P \in \mathbf{P}$. Quando questo accade ottengo punti $\mathbb{F}_{q^m}$-razionali su $\mathcal{X}_W$ se e solo se $P \in \mathbf{P}$ è totalmente ramificato ($e_P = q$) in ogni estensione od è completamente separato ($e_P = 1$) nelle estensioni in cui non è totalmente ramificato. Questo perché se P è un punto di ramificazione per un rivestimento di Artin-Schreier, allora è un punto di ramificazione totale, come si verifica immediatamente dall'equazione. Dunque se P è un polo comune a tutte le f_i, $1 \le i \le r$, allora ho un punto $\mathbb{F}_{q^m}$-razionale su $\mathcal{X}_W$. Altrimenti devo porre la condizione $\mathrm{Tr}\big(f_j(P)\big) = 0$ per tutte le f_j che sono regolari in P, $j = 1, 2, \ldots, r$. Indico con $\mathbf{P}_0$ l'insieme

$$\mathbf{P}_0 = \big\{P \in \mathbf{P} \mid f \in \mathcal{L}_W \text{ è regolare in } P \text{ e } \mathrm{Tr}\big(f(P)\big) \neq 0\big\}\ .$$

Allora $\mathbf{P}_1 = \mathbf{P} \setminus \mathbf{P}_0$. I punti $\mathbb{F}_{q^m}$-razionali di $\mathbf{P}_0$ non danno nessun punto $\mathbb{F}_{q^m}$-razionale su $\mathcal{X}_W$. Quindi devo guardare i punti $\mathbb{F}_{q^m}$-razionali di $\mathbf{P}_1$. Ogni punto $\mathbb{F}_{q^m}$-razionale di $\mathbf{P}_1$ mi dà q^{s_P} punti $\mathbb{F}_{q^m}$-razionali su $\mathcal{X}_W$.
Dunque

$$\#\mathcal{X}_W(\mathbb{F}_{q^m}) = q^r z(W) + \sum_{P\in\mathbf{P}_1} q^{s_P}\ ,$$

i.e.

$$z(W) = \frac{1}{q^r}\big(\#\mathcal{X}_W(\mathbb{F}_{q^m}) - \sum_{P\in\mathbf{P}_1} q^{s_P}\big)\ .$$

□

Definizione 4.2.4 La **traccia di Frobenius** di una curva $\mathcal{X}$ su $\mathbb{F}_{q^m}$ è definita come

$$\tau_{\mathcal{X}} := q^m + 1 - \#\mathcal{X}(\mathbb{F}_{q^m}) \, .$$

Per dimostrare il successivo teorema ci serve questo importante risultato provato da E. Kani e M. Rosen in [Ka-R] (la dimostrazione fa uso della struttura dell'algebra degli endomorfismi di $\mathrm{Jac}(\mathcal{X}_W)$):

Lemma 4.2.5 *Sia W un sottospazio r-dimensionale di uno spazio traccia V di $\mathbb{F}_{q^m}$ al quale è associata la curva definita in* (4.7)*. Allora c'è un'isogenia*

$$\mathrm{Jac}(\mathcal{X}_W) \ \sim \prod_{f \in (\mathcal{L}_W \setminus \{0\})/\mathbb{F}_q^*} \mathrm{Jac}(\mathcal{X}_f) \, . \tag{4.8}$$

Teorema 4.2.6 *Sia W un sottospazio r-dimensionale di uno spazio traccia V di $\mathbb{F}_{q^m}$. La traccia di Frobenius $\tau_{\mathcal{X}_W} = \tau_W$ soddisfa*

$$(q-1)\tau_W = \sum_{f \in \mathcal{L}_W \setminus \{0\}} \tau_f \, , \tag{4.9}$$

dove $\tau_f = \tau_{\mathcal{X}_f}$.
Il genere della curva $\mathcal{X}_W$ è dato dalla relazione

$$(q-1)g(\mathcal{X}_W) = \sum_{f \in \mathcal{L}_W \setminus \{0\}} g(\mathcal{X}_f) \, . \tag{4.10}$$

Dim. Dalla definizione di norma di un sottospazio W ho che

$$\sum_{w \in W} \mathrm{N}(w) = \sum_{w \in W \setminus \{0\}} \mathrm{N}(w) = (q^r - q^{r-1})\mathrm{N}(W) \, .$$

Applicando la proposizione 4.2.3 trovo che

$$\sum_{w \in W} \mathrm{N}(w) = (q^r - q^{r-1})\Big(n - \frac{1}{q^r}\big(n - \tau_W - \sum_{P \in \mathbf{P}_1} q^{s_P} - \#\mathbf{P}\big)\Big) \, . \tag{4.11}$$

Inoltre ho che

$$\begin{aligned} \mathrm{N}(w) &= n - \frac{1}{q}\big(\#\mathcal{X}_W(\mathbb{F}_{q^m}) - \#\mathbf{Q}_f\big) \\ &= n - \frac{1}{q}\big(n - \tau_f - (\#\mathbf{Q}_f - \#\mathbf{P})\big) \end{aligned}$$

dove $\mathbf{Q}_f$ indica la cardinalità dell'insieme

$$\mathbf{Q}_f = \{Q \in \mathcal{X}_f(\mathbb{F}_{q^m}) \mid Q \text{ sta sopra } P \in \mathbf{P}_1\} \, .$$

Questo mi dà

$$\sum_{w \in W} \mathrm{N}(w) = (q^r - 1)n - \frac{1}{q}\Big(\sum_{f \in \mathcal{L}_W \setminus \{0\}} \big(n - \tau_f - (\#\mathbf{Q}_f - \#\mathbf{P})\big)\Big) \, . \tag{4.12}$$

Ora

$$\begin{aligned}\#\mathbf{Q}_f &= \#\{P \in \mathbf{P}_1 \mid f \text{ è regolare in } P\} \cdot q + \big(\#\mathbf{P} - \#\{P \in \mathbf{P}_1 \mid f \text{ è regolare in } P\}\big) \\ &= \#\{P \in \mathbf{P}_1 \mid f \text{ è regolare in } P\} \cdot (q-1) + \#\mathbf{P}\ ,\end{aligned}$$

quindi la (4.12) diventa

$$\sum_{w \in W} \mathrm{N}(w) = (q^r - 1)n - \frac{1}{q}\Big(\sum_{f \in \mathcal{L}_W \setminus \{0\}} \big(n - \tau_f - \#\{P \in \mathbf{P}_1 \mid f \text{ è regolare in } P\} \cdot (q-1)\big)\Big). \tag{4.13}$$

Confrontando i membri di destra della (4.11) e della (4.13) si ottiene il primo risultato.
Per il lemma 4.2.5 e poiché la dimensione della jacobiana di una curva coincide con il genere della curva stessa si ha che

$$g(\mathcal{X}_W) \ = \sum_{f \in (\mathcal{L}_W \setminus \{0\})/\mathbb{F}_q^*} g(\mathcal{X}_f)\ . \tag{4.14}$$

Noto che ogni elemento λ del gruppo moltiplicativo $\mathbb{F}_q^*$ definisce un isomorfismo

$$\begin{aligned}\varphi_\lambda : \mathcal{X}_f &\to \mathcal{X}_{\lambda f}\ . \\ y &\mapsto \lambda^{-1} y\end{aligned}$$

Quindi la (4.14) diventa

$$(q-1)g(\mathcal{X}_W) \ = \sum_{f \in \mathcal{L}_W \setminus \{0\}} g(\mathcal{X}_f)\ .$$

□

Esistono vari metodi per ottenere spazi lineari di curve con molti punti, tutti legati alla teoria dei codici. Essi si basano sul fatto che prendendo il prodotto fibrato corrispondente a questi spazi lineari, si ottengono nuove curve con molti punti razionali.

4.3 Primo metodo

Per q potenza di un numero primo ed m pari, il nucleo della mappa canonica $\mathbb{F}_q$-lineare

$$\begin{aligned}\phi :\ \mathcal{R}_{m/2} &\longrightarrow V_{m/2} \\ R &\longmapsto \phi(R) = (\mathrm{Tr}(x_i R(x_i))_{1 \le i \le q^m})\end{aligned}$$

ha dimensione $m/2$ ed è costituito dai polinomi additivi $R(x) = ax^{q^{m/2}}$ con $a \in \mathbb{F}_{q^m}$ soddisfacente $a^{q^{m/2}} + a = 0$.
Per $a \neq 0$ le curve corrispondenti, date dalle equazioni (affini)

$$y^q - y = ax^{q^{m/2}+1}\ ,$$

hanno genere $g = (q-1)q^{m/2}/2$ e $q^{m+1} + 1$ punti $\mathbb{F}_{q^m}$-razionali.
Si osservi che tutte le curve sono massimali.

Usando la costruzione del prodotto fibrato e le relazioni (4.9) e (4.10) si ottiene il seguente risultato:

Teorema 4.3.1 *Per m pari ed $1 \leq r \leq m/2$ esiste uno spazio r-dimensionale L di curve su $\mathbb{F}_{q^m}$ con $q^{m+1}+1$ punti razionali. Dal corrispondente prodotto fibrato ottengo una curva massimale $\mathcal{X}_L$ su $\mathbb{F}_{q^m}$ di genere e numero di punti razionali dati da*

$$g(\mathcal{X}_L) = \frac{(q^r-1)q^{m/2}}{2} \ , \quad \#\mathcal{X}_L(\mathbb{F}_{q^m}) = q^{m+r}+1 \ .$$

Esempio 4.3.2 Con $q=2$ trovo una curva di genere 1 su $\mathbb{F}_4$ con nove punti razionali; su $\mathbb{F}_{16}$ trovo due curve, una di genere 2 con 33 punti razionali e l'altra di genere 6 con 65 punti razionali; su $\mathbb{F}_{64}$ trovo tre curve, la prima di genere 4 con 129 punti razionali, la seconda di genere 12 con 257 punti razionali, la terza di genere 28 con 513 punti razionali.

Esempio 4.3.3 Con $q=3$ trovo una curva di genere 3 su $\mathbb{F}_9$ con 28 punti razionali; su $\mathbb{F}_{81}$ trovo due curve, una di genere 9 con 244 punti razionali e l'altra di genere 36 con 730 punti razionali.

Per m dispari il nucleo dell'applicazione canonica

$$\begin{array}{rccl} \phi: & \mathcal{R}_{(m+1)/2} & \longrightarrow & V_{(m+1)/2} \\ & R & \longmapsto & \phi(r) = (\mathrm{Tr}(x_i R(x_i))_{1\leq i\leq q^m}) \end{array}$$

ha dimensione m ed è formato dai polinomi additivi

$$R(x) = ax^{q^{(m+1)/2}} - (ax)^{q^{(m-1)/2}} \ , \ a \in \mathbb{F}_{q^m} \ .$$

Per $a \neq 0$ le curve corrispondenti hanno genere $(q-1)q^{(m+1)/2}/2$ e $q^{m+1}+1$ punti razionali su $\mathbb{F}_{q^m}$.
Nello stesso modo di prima si trova il seguente:

Teorema 4.3.4 *Per m dispari ed $1 \leq r \leq m$ esiste un sottospazio r-dimensionale L di curve su $\mathbb{F}_{q^m}$ con $q^{m+1}+1$ punti razionali. Dal corrispondente prodotto fibrato ottengo una curva $\mathcal{X}_L$ su $\mathbb{F}_{q^m}$ di genere e numero di punti razionali dati da*

$$g(\mathcal{X}_L) = \frac{(q^r-1)q^{(m+1)/2}}{2} \ , \quad \#\mathcal{X}_L(\mathbb{F}_{q^m}) = q^{m+r}+1 \ .$$

Esempio 4.3.5 Con $q=2$ trovo tre curve su $\mathbb{F}_8$, la prima di genere 2 con 17 punti razionali (il limite superiore è 18), la seconda di genere 6 con 33 punti razionali (il limite superiore è 36) e la terza di genere 14 con 65 punti razionali (è ottimale); su $\mathbb{F}_{32}$ trovo cinque curve di genere ripettivamente 4, 12, 28, 60, 124 con 65 (il limite superiore è 77), 129 (165), 257 (298), 513 (542) e 1024 (ottimale) punti razionali rispettivamente.

Esempio 4.3.6 Con $q=3$ trovo una curva ottimale di genere 3 con 10 punti su $\mathbb{F}_3$; su $\mathbb{F}_{27}$ trovo tre curve, la prima di genere 9 con 82 punti razionali (110), la seconda di genere 36 con 244 punti razionali (315) ed infine la terza di genere 117 con 730 punti razionali (877).

4.4 Secondo metodo

Riporto una generalizzazione del metodo di van der Geer e van der Vlugt esposto in [G-V5] data da Kawakita e Miura in [K-M].

Questo metodo consiste nello studio della forma quadratica

$$Q(x) := \sum_{i=1}^{M} \mathrm{Tr}(a_i x)\mathrm{Tr}(b_i x) \in \mathbb{F}_{q^m}[x] \ ,$$

dove $M := (m-w)/2$, w intero tale che $0 \leq w \leq m$ e $m - w \equiv 0 \pmod 2$, $a_1, a_2, \ldots, a_M$, $b_1, b_2, \ldots, b_M \in \mathbb{F}_{q^m}$.

Lemma 4.4.1 *Se n è pari allora*

$$\#\left\{(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n \mid x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n = 0\right\} = q^{n+1} + (q-1)q^{(n-2)/2} \ .$$

Dim. Per $r \in \mathbb{Z}_{>0}$, $t \in \mathbb{F}_q$ pongo

$$\beta(r,t) := \#\{(x_1, x_2, \ldots, x_{2r}) \in \mathbb{F}_q^{2r} \mid x_1x_2 + x_3x_4 + \cdots + x_{2r-1}x_{2r} = t\} \ .$$

Intendo provare, per induzione su r, che

$$\beta(r,0) = q^{2r-1} + (q-1)q^{(2r-2)/2} \ . \tag{4.15}$$

Per $r = 1$ è chiaro che $\beta(r,0) = 2q-1$.
Se la formula (4.15) vale per $r-1$ allora

$$\begin{aligned}
\beta(r,0) &= \beta(r-1,0)\beta(1,0) + \sum_{t\in\mathbb{F}_q^*} \beta(r-1,t)\beta(1,-t) \\
&= \beta(r-1,0)(2q-1) + \sum_{t\in\mathbb{F}_q^*} \beta(r-1,t)(q-1) \\
&= \beta(r-1,0)(2q-1) + (q-1)\sum_{t\in\mathbb{F}_q^*} \beta(r-1,t) \\
&= \beta(r-1,0)(2q-1) + (q-1)\left(q^{2r-2} - \beta(r-1,0)\right) \\
&= q\beta(r-1,0) + q^{2r-2}(q-1) = q^{2r-1} + (q-1)q^{r-1} \ .
\end{aligned}$$

□

Proposizione 4.4.2 *Se $a_1, a_2, \ldots, a_M, b_1, b_2, \ldots, b_M$ sono linearmente indipendenti su $\mathbb{F}_q$, allora*

$$\#\{x \in \mathbb{F}_{q^m} \mid Q(x) = 0\} = \frac{q^m + (q-1)\sqrt{q^{m+w}}}{q} \ .$$

Dim. Sia $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}$ una base normale di $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$. Pongo

$$a_i = \sum_{j=1}^{m} a_{ij}\alpha^{q^{j-1}} \quad \text{e} \quad b_i = \sum_{j=1}^{m} b_{ij}\alpha^{q^{j-1}} \ ,$$

dove $a_{ij}, b_{ij} \in \mathbb{F}_q$ per $i, j = 1, 2, \ldots, m$.
Definisco la matrice $m \times m$

$$A := \left(\mathrm{Tr}\big(\alpha^{q^{i-1}}\alpha^{q^{j-1}}\big)\right)_{1\leq i,j\leq m}$$

e la matrice $2M \times m$

$$B := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ b_{11} & b_{12} & \dots & b_{1m} \\ \vdots & \vdots & & \vdots \\ a_{M1} & a_{M2} & \dots & a_{Mm} \\ b_{M1} & b_{M2} & \dots & b_{Mm} \end{pmatrix} .$$

Scrivo ogni elemento $u \in \mathbb{F}_{q^m}$ come

$$u = \sum_{i=1}^{m} u_i \alpha^{q^{i-1}} ,$$

$u_1, u_2, \dots, u_m \in \mathbb{F}_q$. Pongo $\mathbf{u} := (u_1, u_2, \dots, u_m)$.
Poiché $a_1, a_2, \dots, a_M, b_1, b_2, \dots, b_M$ sono linearmente indipendenti su $\mathbb{F}_q$ ho che il rango di B è $\mathrm{rk}_{\mathbb{F}_q}(B) = 2M$. Definisco una matrice invertibile $m \times m$

$$B' := \begin{pmatrix} B \\ * \end{pmatrix} .$$

Poiché anche A è una matrice invertibile, la matrice $B' \cdot A$ è una trasformazione lineare non-singolare su $\mathbb{F}_q^m$.
Pongo $(x_1, x_2, \dots, x_m)^t := B' \cdot A \cdot \mathbf{u}^t$, i.e.

$$\begin{aligned} x_1 &= \mathrm{Tr}(a_1 u) , \\ x_2 &= \mathrm{Tr}(b_1 u) , \\ &\dots \\ x_{2M-1} &= \mathrm{Tr}(a_M u) , \\ x_{2M} &= \mathrm{Tr}(b_M u) . \end{aligned}$$

Per questa trasformazione lineare e per il lemma 4.4.1 ho che

$$\begin{aligned} &\#\left\{u \in \mathbb{F}_{q^m} \mid Q(u) = 0\right\} \\ &\quad = \#\left\{u \in \mathbb{F}_{q^m} \mid \sum_{i=1}^{M} \mathrm{Tr}(a_i u)\mathrm{Tr}(b_i u) = 0\right\} \\ &\quad = \#\left\{\mathbf{u} \in \mathbb{F}_q^m \mid \sum_{i=1}^{M} \mathrm{Tr}(a_i \sum_{j=1}^{m} \alpha^{q^{j-1}} u_j)\mathrm{Tr}(b_i \sum_{j=1}^{m} \alpha^{q^{j-1}} u_j)\right\} \\ &\quad = \#\left\{(x_1, x_2, \dots, x_m) \in \mathbb{F}_q^m \mid x_1x_2 + x_3x_4 + \dots + x_{2M-1}x_{2M} = 0\right\} \\ &\quad = \#\left\{(x_1, x_2, \dots, x_m) \in \mathbb{F}_q^m \mid x_1x_2 + x_3x_4 + \dots + x_{m-w-1}x_{m-w} = 0\right\} \\ &\quad = \#\left\{(x_1, x_2, \dots, x_{m-w}) \in \mathbb{F}_q^{m-w} \mid x_1x_2 + x_3x_4 + \dots + x_{m-w-1}x_{m-w} = 0\right\} \cdot q^w \\ &\quad = \left(q^{m-w-1} + (q-1)q^{(m-w-2)/2}\right) q^w \\ &\quad = \frac{q^m + (q-1)\sqrt{q^{m+w}}}{q} . \end{aligned}$$

□

Teorema 4.4.3 *Esistono un intero h ed un polinomio $R(x) \in \mathcal{R}_h$ tali che*

$$Q(x) \equiv \mathrm{Tr}\left(xR(x)\right) \quad \left(\mathrm{mod}\ \left(x^{q^m} - x\right)\right) .$$

Usando un tale $R(x)$, sia $\mathcal{X}_R$ la curva di equazione

$$y^q - y = xR(x) \ .$$

(i) *Se $a_1, a_2, \ldots, a_M, b_1, b_2, \ldots, b_M$ sono linearmente indipendenti su $\mathbb{F}_q$, allora il numero dei punti razionali di $\mathcal{X}_R$ su $\mathbb{F}_{q^m}$ è*

$$\#\mathcal{X}_R(\mathbb{F}_{q^m}) = q^m + 1 + (q-1)\sqrt{q^{m+w}} \ .$$

(ii) *Si assuma una delle seguenti affermazioni:*

1. *q è pari e $\deg(R(x)) \geq 2$;*
2. *q è dispari e $\deg(R(x)) \geq 1$.*

Allora il genere di $\mathcal{X}_R$ è dato da

$$g(\mathcal{X}_R) = \frac{(q-1)\deg(R(x))}{2} \ .$$

Dim. (i) segue direttamente dalla proposizione 4.4.2 e dalla (4.9).
(ii) segue dalla (4.10). □

Fissati m e w, il teorema prova l'esistenza di un polinomio $R(x)$, al quale è associata la curva $\mathcal{X}_R$, di grado più piccolo rispetto agli altri polinomi di $\mathcal{R}_h$ che danno curve con lo stesso numero di punti $\mathbb{F}_{q^m}$-razionali di $\mathcal{X}_R$ ma con genere più alto. Questo significa che esiste un intero minimo h tale che $R(x) \in \mathcal{R}_h$.

È possibile determinare delle condizioni sugli $a_1, a_2, \ldots, a_M, b_1, b_2, \ldots, b_M$ dipendenti da h. Fissato h, sotto queste condizioni è possibile ottenere un polinomio $R(x) \in \mathcal{R}_h$ tale che

$$Q(x) \equiv \mathrm{Tr}(xR(x)) \quad \Big(\mathrm{mod}\big(x^{q^m} - x\big)\Big) \ .$$

La curva associata a tale $R(x)$ è, nel caso m pari, massimale.

Lemma 4.4.4 *Sia m pari, $k = m/2$ ed $x \in \mathbb{F}_{q^m}$. Se*

$$\sum_{i=1}^{M} \left(a_i^{q^k} b_i + a_i b_i^{q^k}\right) = 0 \ , \tag{4.16}$$

allora

$$\mathrm{Tr}\Big(\sum_{i=1}^{M} \left(a_i^{q^k} b_i x^{q^k+1}\right)\Big) = 0 \ .$$

Dim. Pongo

$$y := \sum_{i=1}^{M} \left(a_i^{q^k} b_i x^{q^k+1}\right) \ .$$

Ho che

$$y^{q^k} \sum_{i=1}^{M} a_i^{q^{2k}} b_i^{q^k} x^{q^{2k}+q^k} = \sum_{i=1}^{M} a_i b_i^{q^k} x^{q^k+1} = \sum_{i=1}^{M} a_i^{q^k} b_i x^{q^k+1} = -y \ ,$$

dove nel penultimo passaggio ho fatto uso della (4.16).
Quindi

$$\mathrm{Tr}(y) = \sum_{j=0}^{2k-1} y^{q^j} = \sum_{j=0}^{k-1} y^{q^j} + \sum_{j=k}^{2k-1} y^{q^j} = \sum_{j=0}^{k-1} y^{q^j} + \sum_{j=0}^{2k-1} \left(-y^{q^j}\right) = 0 \, .$$

□

Proposizione 4.4.5 (i) *Sia m dispari. Se*

$$\sum_{i=1}^{M} \left(a_i^{q^j} b_i + a_i b_i^{q^j}\right) = 0$$

per $j = 1, 2, \ldots, (m-1)/2$, allora

$$Q(x) \equiv \mathrm{Tr}\left(xR(x)\right) \quad \left(\mathrm{mod}\big(x^{q^m} - x\big)\right) \, ,$$

dove

$$R(x) = \sum_{i=1}^{M} a_i b_i x + \sum_{j=1}^{h} \sum_{i=1}^{M} \left(a_i^{q^j} b_i + a_i b_i^{q^j}\right) x^{q^j} \in \mathcal{R}_h \, .$$

(ii) *Sia m pari. Se*

$$\sum_{i=1}^{M} \left(a_i^{q^j} b_i + a_i b_i^{q^j}\right) = 0$$

per $j = 1, 2, \ldots, m/2$, allora

$$Q(x) \equiv \mathrm{Tr}\left(xR(x)\right) \quad \left(\mathrm{mod}\big(x^{q^m} - x\big)\right) \, ,$$

dove per $h = m/2$

$$R(x) = \sum_{i=1}^{M} a_i b_i x + \sum_{j=1}^{(m-2)/2} \sum_{i=1}^{M} \left(a_i^{q^j} b_i + a_i b_i^{q^j}\right) x^{q^j} + \sum_{i=1}^{M} a_i^{q^{m/2}} b_i x^{q^{m/2}} \in \mathcal{R}_h$$

e per $h \leq (m-2)/2$

$$R(x) = \sum_{i=1}^{M} a_i b_i x + \sum_{j=1}^{h} \sum_{i=1}^{M} \left(a_i^{q^j} b_i + a_i b_i^{q^j}\right) x^{q^j} \in \mathcal{R}_h \, .$$

Dim. (i) Siano $a, b, x \in \mathbb{F}_{q^m}$. Ho che

$$\mathrm{Tr}(ax)\mathrm{Tr}(bx) = \mathrm{Tr}\left(\mathrm{Tr}(ax)bx\right) = \mathrm{Tr}\Big(\sum_{j=0}^{m-1} (ax)^{q^j} bx\Big) = \sum_{j=0}^{m-1} \mathrm{Tr}\left(a^{q^j} b x^{q^j+1}\right) \, .$$

Poiché per $0 \leq j < m$

$$\mathrm{Tr}\left(a^{q^j} b x^{q^j+1}\right) = \mathrm{Tr}\left(\left(a^{q^j} b x^{q^j+1}\right)^{q^{m-j}}\right) = \mathrm{Tr}\left(a b^{q^{m-j}} x^{q^{m-j}+1}\right)$$

e

$$\sum_{j=(m+1)/2}^{m-1} \mathrm{Tr}\left(a^{q^j} b x^{q^j+1}\right) = \sum_{j=(m+1)/2}^{m-1} \mathrm{Tr}\left(ab^{q^{m-j}} x^{q^{m-j}+1}\right) = \sum_{j=1}^{(m-1)/2} \mathrm{Tr}\left(ab^{q^j} x^{q^j+1}\right) ,$$

ho che

$$\begin{aligned} \mathrm{Tr}(ax)\mathrm{Tr}(bx) &= \mathrm{Tr}(abx^2) + \sum_{j=1}^{(m-1)/2} \mathrm{Tr}\left(a^{q^j} b x^{q^j+1}\right) + \sum_{j=1}^{(m-1)/2} \mathrm{Tr}\left(ab^{q^j} x^{q^j+1}\right) \\ &= \mathrm{Tr}(abx^2) + \sum_{j=1}^{(m-1)/2} \mathrm{Tr}\left(\left(a^{q^j} b + ab^{q^j}\right) x^{q^j+1}\right) . \end{aligned}$$

Da questa si deduce che

$$\begin{aligned} Q(x) &= \sum_{i=1}^{M} \mathrm{Tr}(a_i x)\mathrm{Tr}(b_i x) \\ &\equiv \sum_{i=1}^{M} \left(\mathrm{Tr}(a_i b_i x^2) + \sum_{j=1}^{(m-1)/2} \mathrm{Tr}\left(\left(a_i^{q^j} b_i + a_i b_i^{q^j}\right) x^{q^j+1}\right)\right) \quad \left(\mathrm{mod}\left(x^{q^m} - x\right)\right) \\ &\equiv \mathrm{Tr}\left(x\left(\sum_{i=1}^{M} a_i b_i x + \sum_{j=1}^{(m-1)/2} \sum_{i=1}^{M} \left(a_i^{q^j} b_i + a_i b_i^{q^j}\right) x^{q^j}\right)\right) \quad \left(\mathrm{mod}\left(x^{q^m} - x\right)\right) . \end{aligned}$$

Annullando i coefficienti x^{q^j} per $j = h+1, \ldots, (m-1)/2$ si prova (i).
(ii) In maniera analoga al punto (i) si prova che

$$Q(x) \equiv \mathrm{Tr}\left(x\left(\sum_{i=1}^{M} a_i b_i x + \sum_{j=1}^{m/2-1} \sum_{i=1}^{M} \left(a_i^{q^j} b_i + a_i b_i^{q^j}\right) x^{q^j} + \sum_{i=1}^{M} a_i^{q^{m/2}} b_i x^{q^{m/2}}\right)\right) \left(\mathrm{mod}\left(x^{q^m} - x\right)\right) .$$

Il caso $h = m/2$ è chiaro.
Se $h \leq (m-2)/2$, per il lemma 4.4.4 posso togliere il coefficiente di $x^{q^{m/2}}$ e annullando i coefficenti x^{q^j} per $j = h+1, \ldots, (m-2)/2$ si prova (ii). □

Si ottengono curve massimali eseguendo i calcoli nel caso (ii) della proposizione 4.4.5 con $w = m-2$ ed $h = (m-2)/2$. Più precisamente:

Proposizione 4.4.6 *Sia m pari. Si assuma una delle seguenti affermazioni:*

1. *q è pari ed* $m \geq 4$*;*
2. *q è dispari.*

Allora esiste una curva massimale di genere

$$g = \frac{(q-1)q^{(m-2)/2}}{2}$$

su $\mathbb{F}_{q^m}$. *La sua equazione (affine) è*

$$y^q - y = xR(x) \ ,$$

dove

$$R(x) = bx + \sum_{j=1}^{(m-2)/2} \left(b + b^{q^j}\right) x^{q^j} \in \mathcal{R}_{(m-2)/2}$$

con $b^{q^{m/2}} + b = 0$ *e* $b^q - b \neq 0$.

Dim. Poiché $b^{q^{m/2}} + b = 0$ e $b^q - b \neq 0$ posso considerare la proposizione 4.4.5(ii) nel caso $a_1 = 1, a_2 = a_3 = \cdots = a_M = 0, b_1 = b, b_2 = b_3 = \cdots = b_M = 0$. Si ottiene che

$$Q(x) \equiv \mathrm{Tr}(xR(x)) \quad \left(\mathrm{mod}\big(x^{q^m} - x\big)\right)$$

dove

$$R(x) = bx + \sum_{j=1}^{(m-2)/2} \left(b + b^{q^j}\right) x^{q^j} \ .$$

Sia $\mathcal{X}_R$ la curva di equazione

$$y^q - y = xR(x) \ .$$

Poiché 1 e b sono linearmente indipendenti su $\mathbb{F}_q$, dal teorema 4.4.3 ho che

$$\#\mathcal{X}_R(\mathbb{F}_{q^m}) = q^m + 1 + (q-1)q^{(m-2)/2}\sqrt{q^m}$$

ed il genere di $\mathcal{X}_R$ soddisfa

$$g(\mathcal{X}_R) = \frac{(q-1)q^{(m-2)/2}}{2} \ .$$

Poiché il limite di Hasse-Weil per una curva di genere g su $\mathbb{F}_{q^m}$ è $q^m + 1 + 2g\sqrt{q^m}$, si ha che $\mathcal{X}_R$ è masimale su $\mathbb{F}_{q^m}$. □

Le curve trovate in questo modo sono tutte curve $\mathcal{X}_{a,b}$.

Applico ora il teorema 4.2.6 alla proposizione 4.4.6:

Proposizione 4.4.7 *Sia* m *un intero pari. Si assuma una delle seguenti affermazioni:*

1. q *è pari,* $m \geq 4$ *ed* $r \leq m/2 - 1$*;*
2. q *è dispari ed* $r \leq m/2$.

Allora esiste una curva massimale di genere

$$g = \frac{(q^r - 1)q^{(m-2)/2}}{2}$$

su $\mathbb{F}_{q^m}$. *Essa coincide con la normalizzazione del prodotto fibrato delle curve di equazioni (affini)*

$$y_i^q - y_i = xS_i(x) \ ,$$

dove

$$S_i(x) := b_i x + \sum_{j=1}^{(m-2)/2} \left(b_i + b_i^{q^j} \right) x^{q^j} \tag{4.17}$$

per $i = 1, 2, \ldots, r$ *, con* $b_i^{q^{m/2}} + b_i = 0$, $b_i^q - b_i \neq 0$ *per* $i = 1, 2, \ldots, r$ *e* $b_1, b_2, \ldots, b_r$ *linearmente indipendenti su* $\mathbb{F}_q$.

Dim. Sia $B := \left\{ b \in \mathbb{F}_{q^m} \mid b^{q^{m/2}} + b = 0 \text{ e } b^q - b \neq 0 \right\} \cup \{0\}$. Si ha che

$$\dim_{\mathbb{F}_q}(B) = \begin{cases} m/2 - 1 & \text{se } q \text{ è pari}, \\ m/2 & \text{se } q \text{ è dispari}. \end{cases}$$

Per $r \leq \dim_{\mathbb{F}_q}(B)$ gli interi $b_1, b_2, \ldots, b_r$ sono linearmente indipendenti su $\mathbb{F}_q$. In queste condizioni allora anche gli $xS_1(x), xS_2(x), \ldots, xS_r(x)$ sono linearmente indipendenti su $\mathbb{F}_q$, dove S_i è dato dalla (4.17).
Siano ora $b := \sum_{i=1}^r \mu_i b_i$ ed $S(x) := \sum_{i=1}^r \mu_i S_i(x)$, dove $\mu_1, \mu_2, \ldots, \mu_r \in \mathbb{F}_q$, e sia $\mathcal{X}_r$ la curva di equazione (affine)

$$y^q - y = xS(x) .$$

Poiché $b \in B$ ed $S(x) = bx + \sum_{j=1}^{(m-2)/2} \left(b + b^{q^j} \right) x^{q^j}$, per la proposizione 4.4.6 ho che

$$\#\mathcal{X}_r(\mathbb{F}_{q^m}) = q^m + 1 + (q-1)q^{(m-2)/2}\sqrt{q^m}$$

e

$$g(\mathcal{X}_r) = \frac{(q-1)q^{(m-2)/2}}{2} .$$

□

4.5 Terzo metodo

Anche questo metodo riguarda lo studio delle forme quadratiche, associate ad uno spazio V_h.

Sia $q = p$. Per un fissato $R(x) \in \mathcal{R}_h \setminus \{0\}$ considero la famiglia $\mathcal{F}_R$ 1-dimensionale di curve di equazione

$$y^q - y = xR(x) + bx , \ b \in \mathbb{F}_{q^m} .$$

Per $h = 0$ le equazioni che definiscono tali curve assumono la forma

$$y^q - y = ax^2 + bx , \ b \in \mathbb{F}_{q^m} .$$

Quindi le curve considerate sono curve $\mathcal{X}_{a,b}$. Caratterizzo $\#\mathcal{X}_{a,b}(\mathbb{F}_{q^m})$:

Proposizione 4.5.1 (i) *Sia* m *dispari. Allora* $\#\mathcal{X}_{a,b}(\mathbb{F}_{q^m}) = q^m + 1 \pm \sqrt{q^{m+1}}$ *se e solo se* b *soddisfa l'equazione di una delle quadriche* $\mathrm{Tr}(x^2/4a) = t$ *in* $\mathbb{F}_{q^m}$ *con* $t \in \mathbb{F}_q^*$.

(ii) *Sia* m *pari. Si assuma che* $\#\mathcal{X}_{a,0}(\mathbb{F}_{q^m}) = q^m + 1 \mp (q-1)\sqrt{q^m}$. *Allora si ha che* $\#\mathcal{X}_{a,b}(\mathbb{F}_{q^m}) = q^m + 1 \mp \sqrt{q^{m+1}}$ *se e solo se* b *soddisfa l'equazione della quadrica* $\mathrm{Tr}(x^2/4a) = 0$ *in* $\mathbb{F}_{q^m}$.

In entrambi i casi il segno è determinato dal simbolo di Legendre $\left(\frac{t}{q}\right)$.

Dim. È possibile trasformare l'equazione della curva $\mathcal{X}_{a,b}$ in $\mathcal{F}_R$ con $x \mapsto x - \beta$, $\beta = b/2a$ ed ottenere l'equazione

$$y^q - y = ax^2 - a\beta^2 \ .$$

Se pongo $t = \mathrm{Tr}(a\beta^2)$ e se fisso un elemento $\tau \in \mathbb{F}_{q^m}$ tale che $\mathrm{Tr}(\tau) = t$ ho che

$$\#\mathcal{X}_{a,b}(\mathbb{F}_{q^m}) = \#\mathcal{Y}_{a,t}(\mathbb{F}_{q^m}) \ ,$$

dove $\mathcal{Y}_{a,t}$ è la curva data dall'equazione

$$y^q - y = ax^2 - \tau \ .$$

Quindi, per fissati $t \in \mathbb{F}_q$ e $b \in \mathbb{F}_{q^m}$ tali che $\mathrm{Tr}(b^2/4a) = t$, le curve $\mathcal{X}_{a,b}$ hanno lo stesso numero di punti razionali, diciamolo $\#\mathcal{Y}_{a,t}(\mathbb{F}_{q^m})$.
Dalla teoria delle forme quadratiche [Bue] trovo che, per m dispari

$$\#\mathcal{Y}_{a,t}(\mathbb{F}_{q^m}) = q^m + 1 \pm \sqrt{q^{m+1}}$$

con $t \in \mathbb{F}_q^*$, e per m pari

$$\#\mathcal{Y}_{a,t}(\mathbb{F}_{q^m}) = q^m + 1 \mp \sqrt{q^{m+1}}$$

con $t \in \mathbb{F}_q^*$, dove il segno dipende dal simbolo di Legendre $\left(\frac{t}{q}\right)$. Si deduce che i $b \in \mathbb{F}_{q^m}$ che corrispondono alle curve $\mathcal{X}_{a,b}$ con lo stesso numero di punti soddisfano le equazioni delle quadriche $\mathrm{Tr}(x^2/4a) = t$ nel $\mathbb{F}_{q^m}$-spazio affine. □

La teoria degli spazi quadratici mi assicura che per m dispari l'indice di Witt dello spazio quadratico $(\mathbb{F}_{q^m}, \mathrm{Tr}(x^2/4a))$ è uguale ad $(m-1)/2$ e che la quadrica $Q_{a,t}$ contiene un $\mathbb{F}_q$-spazio affine di dimensione $(m-1)/2$ se essa ha $(q^m + \sqrt{q^{m+1}})/q$ punti.
Per m pari, se $\#Q_{a,0} = (q^m + (q-1)\sqrt{q^m})/q$ allora lo spazio quadratico menzionato ha indice di Witt $m/2$ e questo implica che la quadrica $Q_{a,0}$ contiene un $\mathbb{F}_q$-spazio affine di dimensione $m/2$.

Teorema 4.5.2 (i) *Se m è dispari allora per $1 \le r \le (m-1)/2$ esiste una curva $\mathcal{X}_r$ di genere*

$$g(\mathcal{X}_r) = \frac{q^r(q-1)}{2}$$

con un numero di punti pari a

$$\#\mathcal{X}_r(\mathbb{F}_{q^m}) = q^m + 1 + \sqrt{q^{m+1}} \ .$$

(ii) *Se m è pari allora per $1 \le r \le m/2$ esiste una curva $\mathcal{X}_r$ di genere*

$$g(\mathcal{X}_r) = \frac{q^r(q-1)}{2}$$

massimale:

$$\#\mathcal{X}_r(\mathbb{F}_{q^m}) = q^m + 1 + q^r(q-1)\sqrt{q^m} \ .$$

Dim. (i) Segue da quanto detto prima che per un fissato $a \in \mathbb{F}_{q^m}^*$ esiste una curva $\mathcal{X}_{a,b}$ con $\#\mathcal{X}_{a,b}(\mathbb{F}_{q^m}) = q^m + 1 + \sqrt{q^{m+1}}$ punti, dove b varia tra gli $\mathbb{F}_q$-spazi vettoriali di dimensione $r = 1, 2, \ldots, (m-1)/2$ in $\mathbb{F}_{q^m}$. Basta fare il prodotto fibrato di tali curve per ottenere quanto voluto.

(ii) Analogamente, per un fissato $a \in \mathbb{F}_{q^m}^*$ trovo un $\mathbb{F}_q$-spazio vettoriale di b per il quale $\#\mathcal{X}_{a,b}(\mathbb{F}_{q^m}) = q^m + 1 + (q-1)\sqrt{q^m}$. Usando il prodotto fibrato corrispondente trovo la curva desiderata. □

Esempio 4.5.3 Per $q^m = p^m = 3^3 = 27$ trovo una curva di genere 3 con 55 punti (il limite superiore è 58).
Per $q^m = p^m = 3^4 = 243$ trovo una curva di genere 3 con 325 punti (il limite superiore è 337) ed una curva di genere 9 con 487 punti (il limite superiore è 523).

Focalizzo l'attenzione nel caso di campi di caratteristica 3.

Proposizione 4.5.4 *Per $q = p = 3$, m pari ed $1 \le r \le m/2$ esiste una curva $\mathcal{X}_r$ su $\mathbb{F}_{q^m}$ di genere*

$$g(\mathcal{X}_r) = (3^r - 1)/2$$

massimale:

$$\#\mathcal{X}_r(\mathbb{F}_{q^m}) = q^m + 1 + 2\sqrt{q^m}\ .$$

Dim. Considero una curva $\mathcal{X}_a$ di equazione $y^3 - y = ax^2$ con $\#\mathcal{X}_a(\mathbb{F}_{q^m}) = q^m + 1 + 2\sqrt{q^m}$ punti. Allora per ogni $t \in \mathbb{F}_{q^m}^*$ la curva $\mathcal{X}_{at^2}$ ha lo stesso numero di punti.
Poiché m è pari $\mathbb{F}_{q^{m/2}} \subseteq \mathbb{F}_{q^m}^2$ e questo implica l'esistenza di un sottospazio r-dimensionale di curve massimali per $1 \le r \le m/2$.
Il prodotto fibrato corrispondente dà una curva su $\mathbb{F}_{q^m}$ con le desiderate proprietà. □

Per m dispari la situazione è più complicata:

Proposizione 4.5.5 *Per $q = p = 3$ ed $m \ge 3$ dispari esiste una curva di genere 4 con $q^m + 1 + 4\sqrt{q^{m+1}}$ punti razionali su $\mathbb{F}_{q^m}$.*

Dim. Si è visto nella dimostrazione della proposizione 4.5.1 che per $a \in \left(\mathbb{F}_{q^m}^*\right)^2$ le curve $\mathcal{X}_{a,b}$ di equazione $y^3 - y = ax^2 + bx$ con $\tau_{X_{a,b}} = -\sqrt{q^{m+1}}$ sono caratterizzate dall'avere $\mathrm{Tr}(b^2/4a) = r$ per un fissato $r \in \mathbb{F}_3^*$.
Considero la curva $\mathcal{X}_{1,b}$ date da $y^3 - y = x^2 + bx$ con b soddisfacente

$$\mathrm{Tr}(b^2) = r\ . \tag{4.18}$$

Costruisco il prodotto fibrato $\mathcal{X}_{1,b} \times_{\mathbb{P}^1} \mathcal{X}_{t^2,bt}$ come in [G-V3, prop. 4.3], quindi richiedendo che $t \in \mathbb{F}_{q^m}^* \setminus \mathbb{F}_3^*$ con $1 + t^2, 2 + t^2 \in \left(\mathbb{F}_{q^m}^*\right)^2$, i.e. esistono $u, v \in \mathbb{F}_{q^m}^*$ tali che

$$1 + t^2 = u^2 \quad , \quad 2 + t^2 = v^2\ . \tag{4.19}$$

La varietà algebrica $\mathcal{E}$ associata è data dalle equazioni

$$s^2 + t^2 - u^2 = 0 \quad , \quad 2s^2 + t^2 - v^2 = 0\ ,$$

i.e. $\mathcal{E}$ è l'intersezione di due quadriche non-singolari in $\mathbb{P}^3$, quindi una curva di genere 1.
Questa curva ha un punto $\mathbb{F}_3$-razionale. Poiché $\#\mathcal{E}(\mathbb{F}_3) = 4$ gli zeri del polinomio caratteristico di Frobenius su $\mathbb{F}_3$ sono $\pm\sqrt{-3}$. Questo implica che $\#\mathcal{E}(\mathbb{F}_{q^m}) = q^m + 1$.
Ci sono quattro punti $\mathbb{F}_{q^m}$-razionali su $\mathcal{E}$ con $s = 0$ e non ci sono punti $\mathbb{F}_{q^m}$-razionali

con $s \neq 0$ e $t \in \mathbb{F}_3^*$. Quindi è possibile trovare una soluzione appropriata della (4.19) se $q+1-4>0$, i.e. $q \geq 3^2$.
Considero la componente $\mathcal{X}_{1+t^2,b(1+t)}$ della jacobiana di $\mathcal{X}_{1,b} \times_{\mathbb{P}^1} \mathcal{X}_{t^2,bt}$. Questa curva è isomorfa alla curva data dall'equazione

$$y^3 - y = x^2 + \frac{b(1+t)}{u}x \ .$$

La condizione $\mathrm{Tr}\left(b^2(1+t)^2/u^2\right)$ deriva dalla condizione

$$\mathrm{Tr}\left(\frac{t}{1+t^2}b^2\right) = 0 \ . \tag{4.20}$$

Per la componente $\mathcal{X}_{2+t^2,b(2+t)}$ si ha analogamente

$$\mathrm{Tr}\left(\frac{t}{1+t}b^2\right) = 0 \ . \tag{4.21}$$

Le tre condizioni (4.18), (4.20) e (4.21) sono equivalenti al seguente sistema di equazioni:

$$\begin{aligned} &X^3 - X = b^2 - A \quad \text{con } \mathrm{Tr}(A) = r \ , \\ &Y^3 - Y = \left(t/(1+t^2)\right) b^2 \ , \\ &Z^3 - Z = \left(t/(1+t)\right) b^2 \ . \end{aligned} \tag{4.22}$$

Queste equazioni definiscono una curva, che può essere vista come un prodotto fibrato su $\mathbb{P}^1$ dove b è una coordinata su $\mathbb{P}^1$.
Per definire bene il prodotto fibrato devo richiedere che $1, 1/(1+t), 1/(1+t^2)$ siano indipendenti su $\mathbb{F}_3$, cosicché la sola costante nello spazio di funzioni generato da $x^2 - A$, $\left(t/(1+t^2)\right) x^2$ e $\left(1/(1+t)\right) x^2$ è zero.
Questa è un'altra condizione su t che mi esclude al più sei suoi possibili valori. Quindi un appropriato valore di t esiste se $q+1-10>0$, i.e. $q \geq 3^3$.
La (4.10) mi assicura che la (4.22) ha genere 13.
Il limite di Hasse-Weil implica l'esistenza di una soluzione $b \in \mathbb{F}_{q^m}^*$ di (4.18), (4.20) e (4.21) per $m \geq 7$. Questa b determina una curva $\mathcal{X}_{1,b} \times_{\mathbb{P}^1} \mathcal{X}_{t^2,bt}$ soddisfacente le condizioni della proposizione.
Per $m = 3$ ed $m = 5$ una verifica computazionale conferma l'esistenza di un appropriato b. □

Esempio 4.5.6 Esiste una curva di genere 4 su $\mathbb{F}_{27}$ con 64 punti razionali (il limite superiore è 68).

Proposizione 4.5.7 *Per $q = p = 3$ con $m \equiv 0 \pmod 4$ esiste una curva massimale di genere 12 su $\mathbb{F}_{q^m}$.*

Dim. Il campo $\mathbb{F}_{81}$ contiene quattro elementi aventi le seguenti proprietà:

(i) Soddisfano l'equazione $t^4 + 2t^2 + 2 = 0$;

(ii) $t^2 + 1$ e $t^2 + 2$ sono quadrati in $\mathbb{F}_{81}^*$;

(iii) $1 + 2t^{-2} = (1+t^2)^{-1}$ e $1 + t^{-2} = (2+t^2)^{-1}$.

Considero una curva $\mathcal{X}_a$ massimale su $\mathbb{F}_{q^m}$ definita da $y^3 - y = ax^2$. Allora segue da (ii) che per i t precedenti $\mathcal{X}_a \times_{\mathbb{P}^1} \mathcal{X}_{at^2}$ è una curva massimale di genere 4.
Sia $\mathcal{X}_b$ la curva di equazione $y^3 - y = bx$, $b \in \mathbb{F}_{q^m}^*$. Cerco b tale che esista un'isogenia fra la jacobiana del prodotto fibrato di $\mathcal{X}_a, \mathcal{X}_{at^2}, \mathcal{X}_b$ su $\mathbb{P}^1$ ed il prodotto di dodici curve ellittiche massimali (uso la (4.8) tenendo conto che la jacobiana di una curva ellittica è la curva ellittica stessa).
Per la proposizione 4.5.1 le condizioni per b sono:

$$\mathrm{Tr}\left(b^2/4a\right) = 0 \quad \text{e} \quad \mathrm{Tr}\left(b^2/4at^2\right) = 0\,, \tag{4.23}$$

$$\mathrm{Tr}\left(b^2/4a(1+t^2)\right) = 0 \quad \text{e} \quad \mathrm{Tr}\left(b^2/4a(2+t^2)\right) = 0\,.$$

Il teorema di Chevalley-Warning (si veda [I-R, p. 143]) assicura l'esistenza di un tale $b \in \mathbb{F}_{q^m}^*$ per $m > 8$.
Poiché vale la (iii), è sufficiente trovare $b \in \mathbb{F}_{q^m}^*$ soddisfacente la (4.23).
Poiché il sotto-$\mathbb{F}_q$-spazio vettoriale V generato dagli elementi corrispondenti a $\mathrm{Tr}(x^2/4a)$ e $\mathrm{Tr}(x^2/4at^2)$ ha norma $8(q - \sqrt{q})/9$, il sistema di equazioni (4.23) ha soluzioni b in $\mathbb{F}_{q^m}^*$ per ogni $m \equiv 0 \pmod 4$. Questo prova l'esistenza di una curva massimale di genere 12 su $\mathbb{F}_{q^m}$ con $m \equiv 0 \pmod 4$. □

Esempio 4.5.8 Esiste una curva su $\mathbb{F}_{81}$ ottimale di genere 12.

Capitolo 5

Altri metodi

5.1 I moduli di Drinfeld di rango 1

Per quanto riguarda i moduli di Drinfeld di rango 1 ho riportato un'esposizione riassuntiva di quella data in [N-X], nella quale si possono trovare tutte le dimostrazioni.

5.1.1 Campi di classe ray ristretti

Sia $F/\mathbb{F}_q$ un campo di funzioni di caratteristica p con $q = p^m$, $m \in \mathbb{Z}_{>0}$. Si assuma che $N(F) \geq 1$ e sia P_∞ un posto razionale.

Definizione 5.1.1 Una **funzione segno** $\mathrm{sgn} : F_{P_\infty}^* \to \mathbb{F}_q^*$ è un omomorfismo di gruppi tale che:

(i) $\mathrm{sgn}(\alpha) = \alpha$ per ogni $\alpha \in \mathbb{F}_q^*$;

(ii) $\mathrm{sgn}\left(\mathcal{U}_{F_{P_\infty}}^{(1)}\right) = \{1\}$.

Fissato un elemento $x \in F_{P_\infty}^*$, due qualsiasi funzioni segno su $F_{P_\infty}^*$ sono legate da un fattore moltiplicativo dipendente solo da x. Ciò comporta l'esistenza di esattamente $q-1$ funzioni segno in $F_{P_\infty}^*$.

Fissata, per l'intero paragrafo, una funzione segno su $F_{P_\infty}^*$, definisco il sottogruppo $F_{P_\infty}^{\mathrm{sgn}}$ come

$$F_{P_\infty}^{\mathrm{sgn}} = \{x \in F_{P_\infty}^* \mid \mathrm{sgn}(x) = 1\} .$$

Sia $D = \sum_P m_P P$ un divisore effettivo di F tale che $P_\infty \notin \mathrm{supp}(D)$. Considero il sottogruppo di $\mathcal{J}_F$ dato da

$$F_{P_\infty}^{\mathrm{sgn}} \times \prod_{P \neq P_\infty} \mathcal{U}_{F_P}^{(m_P)} .$$

Allora $F^*\big(F_{P_\infty}^{\mathrm{sgn}} \times \prod_{P \neq P_\infty} \mathcal{U}_{F_P}^{(m_P)}\big)/F^*$ è un gruppo di $\mathcal{C}_F$ di indice infinito. Dunque, per la teoria dei campi di classe esiste un'estensione abeliana $F^D(P_\infty)/F$ con $F^D(P_\infty) \subseteq F^{\mathrm{ab}}$

tale che

$$\mathcal{N}_{F^D(P_\infty)} = F^*\Big(F_{P_\infty}^{\mathrm{sgn}} \times \prod_{P\neq P_\infty} \mathcal{U}_{F_P}^{(m_P)}\Big)/F^* \ .$$

Il campo $F^D(P_\infty)$ è chiamato **campo di classe ray ristretto** (*narrow ray class field*) di modulo D ed $F^D(P_\infty)/F$ l'**estensione di classe ray ristretta** di modulo D.
Sia $\mathcal{S} = \mathbf{P}_F \setminus \{P_\infty\}$ e considero l'anello degli interi

$$\mathcal{O}_\mathcal{S} = \{x \in F \mid \nu_P(x) \geq 0 \text{ per ogni } P \in \mathbf{P}_F \text{ con } P \neq P_\infty\} \ . \tag{5.1}$$

Per un divisore effettivo D di F tale che $P_\infty \notin \mathrm{supp}(D)$, sia $\mathcal{I}_D(\mathcal{O}_\mathcal{S})$ il gruppo degli ideali frazionari di $\mathcal{O}_\mathcal{S}$ che sono relativamente primi con D, i.e.

$$\mathcal{I}_D(\mathcal{O}_\mathcal{S}) = \{\mathfrak{I} \in \mathcal{I}_\mathcal{S} \mid \nu_P(\mathfrak{I}) = 0 \text{ per ogni } P \in \mathrm{supp}(D)\} \ .$$

Detto

$$\mathcal{P}_D^+(\mathcal{O}_\mathcal{S}) = \{x\mathcal{O}_\mathcal{S} \mid x \in F^*,\ \mathrm{sgn}(x) = 1 \text{ e } x \equiv 1 \pmod D\} \ ,$$

il gruppo fattoriale

$$\mathrm{Cl}_D^+(\mathcal{O}_\mathcal{S}) := \mathcal{I}_D(\mathcal{O}_\mathcal{S})/\mathcal{P}_D^+(\mathcal{O}_\mathcal{S})$$

è chiamato **gruppo delle classi ray ristretto** di $\mathcal{O}_\mathcal{S}$ modulo D rispetto a sgn.

Il principale teorema sui campi di classe ray ristretti è il seguente:

Teorema 5.1.2 (i) *Usando le notazioni precedenti, si hanno i seguenti isomorfismi:*

$$\begin{aligned}\mathrm{Gal}(F_{P_\infty}/F) &\cong \mathcal{C}_F/\Big(F^*\big(F_{P_\infty}^{\mathrm{sgn}} \times \prod_{P\neq P_\infty} \mathcal{U}_{F_P}^{(m_P)}\big)/F^*\Big) \\ &\cong \mathcal{J}_F/\Big(F^*\big(F_{P_\infty}^{\mathrm{sgn}} \times \prod_{P\neq P_\infty} \mathcal{U}_{F_P}^{(m_P)}\big)\Big) \cong \mathrm{Cl}_D^+(\mathcal{O}_\mathcal{S}) \ ;\end{aligned}$$

(ii) *$F_\mathcal{S}^D$ è un sottocampo di $F^D(P_\infty)$ e $\mathrm{Gal}\big(F(P_\infty)^D/F_\mathcal{S}^D\big) \cong \mathbb{F}_q^*$;*

(iii) *L'indice di ramificazione di P_∞ in $F^D(P_\infty)/F$ è uguale a $q-1$, i.e.*

$$e_{P_\infty}\big(F^D(P_\infty)/F\big) = e_{P_\infty}\big(F^D(P_\infty)/F_\mathcal{S}^D\big) = q-1 \ .$$

Inoltre P_∞ si separa in $[F_\mathcal{S}^D : F]$ posti di $F^D(P_\infty)$ con campo di classe dei residui $\mathbb{F}_q$. In particolare, $\mathbb{F}_q$ è il campo completo delle costanti di $F^D(P_\infty)$.

5.1.2 Moduli di Drinfeld di rango 1

L'anello degli interi $\mathcal{O}_\mathcal{S}$ definito dalla (5.1) è un dominio di Dedekind con numero di classe $h(\mathcal{O}_\mathcal{S}) = |\mathrm{Cl}(\mathcal{O}_\mathcal{S})| = h(F)$, dove $h(F)$ è il numero delle classi dei divisori del campo F. Sia $\mathcal{H}_\mathcal{S}$ il campo di classe di $\mathcal{S}$-Hilbert di F e sia $\pi : c \mapsto c^p$ l'endomorfismo di Frobenius di $\mathcal{H}_\mathcal{S}$. Considero l'anello dei polinomi tortili sinistro (*left twisted polynomial ring*) $\mathcal{H}_\mathcal{S}[x]_\pi$ i cui elementi sono polinomi del tipo $\sum_{i=0}^k a_i x^i$, $a_i \in \mathcal{H}_\mathcal{S}$, con la regola moltiplicativa

$$xa = a^p x \ \text{ per ogni } a \in \mathcal{H}_\mathcal{S} \ .$$

Sia $D : \mathcal{H}_\mathcal{S}[x]_\pi \to \mathcal{H}_\mathcal{S}$ l'applicazione che associa ogni polinomio in $\mathcal{H}_\mathcal{S}[x]_\pi$ al suo termine costante.

Definizione 5.1.3 Un $\mathcal{O}_\mathcal{S}$**-modulo di Drinfeld di rango** 1 su $\mathcal{H}_\mathcal{S}$ è un omomorfismo di anelli

$$\begin{aligned} \phi : \mathcal{O}_\mathcal{S} &\to \mathcal{H}_\mathcal{S}[x]_\pi \\ a &\mapsto \phi_a \end{aligned}$$

tale che:

(i) Non tutti gli elementi di $\mathcal{H}_\mathcal{S}[x]_\pi$ nell'immagine di ϕ sono polinomi costanti;

(ii) $D \circ \phi = 1_{\mathcal{O}_\mathcal{S}}$;

(iii) $\deg(\phi_a) = -m\,\nu_{P_\infty}(a)$ per ogni $a \in \mathcal{O}_\mathcal{S} \setminus \{0\}$, dove $\deg(\phi_a)$ è il grado di ϕ_a come polinomio in $\mathcal{H}_\mathcal{S}[x]_\pi$.

Osservazione 5.1.4 (i) L'applicazione ϕ è iniettiva;

(ii) Per ogni $\mathcal{O}_\mathcal{S}$-modulo di Drinfeld di rango 1 si ha che $\phi_\alpha = \alpha$ per ogni $\alpha \in \mathbb{F}_q$;

(iii) ϕ_a è un'applicazione $\mathbb{F}_q$-lineare su $\mathcal{H}_\mathcal{S}$ per ogni $a \in \mathcal{O}_\mathcal{S}$.

Definizione 5.1.5 Si dice che un $\mathcal{O}_\mathcal{S}$-modulo di Drinfeld di rango 1 su $\mathcal{H}_\mathcal{S}$ è sgn**-normalizzato** se $\mathrm{sgn}(a)$ è uguale al coefficiente direttivo di ϕ_a per ogni $a \in \mathcal{O}_\mathcal{S}$.

Si può vedere in [Hay] che un $\mathcal{O}_\mathcal{S}$-modulo di Drinfeld di rango 1 su $\mathcal{H}_\mathcal{S}$ sgn-normalizzato esiste sempre e che l'anello dei polinomi tortili $\mathcal{H}_\mathcal{S}[x]_\pi$ è un dominio ad ideali principali sinistri.

Dati un $\mathcal{O}_\mathcal{S}$-modulo di Drinfeld di rango 1 su $\mathcal{H}_\mathcal{S}$ ed un ideale non nullo $\mathfrak{M}$ di $\mathcal{O}_\mathcal{S}$, sia $\mathfrak{I}_{\mathfrak{M},\phi}$ l'ideale sinistro generato in $\mathcal{H}_\mathcal{S}[x]_\pi$ dai polinomi tortili ϕ_a, $a \in \mathfrak{M}$. Per quanto detto prima, esso è un ideale principale sinistro, $\mathfrak{I}_{\mathfrak{M},\phi} = \mathcal{H}_\mathcal{S}[x]_\pi \phi_\mathfrak{M}$, per un unico polinomio tortile $\phi_\mathfrak{M}(x) \in \mathcal{H}_\mathcal{S}[x]_\pi$.
Sia L una $\mathcal{H}_\mathcal{S}$-algebra. Allora per un polinomio $f(x) = \sum_{i=0}^{k} a_i x^i \in \mathcal{H}_\mathcal{S}[x]_\pi$ l'**azione** di $f(x)$ su L è così definita:

$$f(x)(t) = \sum_{i=0}^{k} a_i t^{p^i} \quad \text{per ogni } t \in L\ .$$

Sia $\overline{\mathcal{H}}_\mathcal{S}$ una fissata chiusura algebrica di $\mathcal{H}_\mathcal{S}$ il cui gruppo additivo $(\overline{\mathcal{H}}_\mathcal{S}, +)$ sia dotato della struttura di $\mathcal{O}_\mathcal{S}$-modulo sotto l'azione di ϕ.

Definizione 5.1.6 Sia ϕ un $\mathcal{O}_\mathcal{S}$-modulo di Drinfeld di rango 1 su $\mathcal{H}_\mathcal{S}$ sgn-normalizzato ed $\mathfrak{M}$ un ideale non nullo di $\mathcal{O}_\mathcal{S}$. Il **modulo di $\mathfrak{M}$-torsione** $\Lambda_\phi(\mathfrak{M})$ associato a ϕ è definito come

$$\Lambda_\phi(\mathfrak{M}) := \{t \in (\overline{\mathcal{H}}_\mathcal{S}, +) \mid \phi_\mathfrak{M}(t) = 0\}\ .$$

Proprietà 5.1.7 (i) $\Lambda_\phi(\mathfrak{M})$ è un insieme finito di cardinalità $|\Lambda_\phi(\mathfrak{M})| = p^{\deg(\phi_\mathfrak{M})}$;

(ii) $\Lambda_\phi(\mathfrak{M})$ è un $\mathcal{O}_\mathcal{S}$-modulo di $(\overline{\mathcal{H}}_\mathcal{S}, +)$ ed un $\mathcal{O}_\mathcal{S}$-modulo ciclico isomorfo ad $\mathcal{O}_\mathcal{S}/\mathfrak{M}$;

(iii) $\Lambda_\phi(\mathfrak{M})$ ha $\phi(\mathfrak{M}) = |(\mathcal{O}_\mathcal{S}/\mathfrak{M})^*|$ generatori come $\mathcal{O}_\mathcal{S}$-modulo ciclico, dove $(\mathcal{O}_\mathcal{S}/\mathfrak{M})^*$ è il gruppo delle unità dell'anello $\mathcal{O}_\mathcal{S}/\mathfrak{M}$.

Gli elementi di $\Lambda_\phi(\mathfrak{M})$ sono chiamati **elementi di $\mathfrak{M}$-torsione** in $(\overline{\mathcal{H}}_\mathcal{S}, +)$. Aggiungendo questi elementi di $\mathcal{H}_\mathcal{S}$ ottengo un campo $\mathcal{H}_\mathcal{S}(\Lambda_\phi(\mathfrak{M}))$ che è un campo di classe ray ristretto.
Per un ideale non nullo $\mathfrak{M}$ di $\mathcal{O}_\mathcal{S}$ definisco il corrispondente divisore effettivo

$$D := \sum_{P \in \mathcal{S}} \nu_P(\mathfrak{M}) P \in \mathrm{Div}(F) \ .$$

Dunque posso denotare $\Lambda_\phi(\mathfrak{M})$ con $\Lambda_\phi(D)$ ed è possibile identificare gli ideali primi $\mathfrak{p}$ di $\mathcal{O}_\mathcal{S}$ con i posti P di F.

Teorema 5.1.8 *Sia ϕ un $\mathcal{O}_\mathcal{S}$-modulo di Drinfeld di rango 1 su $\mathcal{H}_\mathcal{S}$. Allora il campo $\mathcal{H}_\mathcal{S}(\Lambda_\phi(D))$ è F-isomorfo al campo di ray ristretto $F^D(P_\infty)$ di modulo D per ogni divisore effettivo.*

5.1.3 Campi di funzioni dei campi di classe ray ristretti

Siano $P_1, P_2, \ldots, P_m, P, P_\infty$ $m+2$ posti razionali distinti di $F/\mathbb{F}_p$. Si definiscono i semigruppi moltiplicativi

$$S = \{ f \in \mathcal{O}_\mathcal{S} \quad | \quad f(P) = 1,\ \mathrm{sgn}(f) = 1 \text{ e } \nu_Q(f) = 0 \text{ per ogni posto } Q \neq P_1, P_2, \ldots, P_m, P, P_\infty \text{ di } F \}$$

e

$$S(n) = \{ \overline{f} \in (\mathcal{O}_\mathcal{S}/\mathfrak{M}_P^n)^* \mid f \in S \} \ ,$$

dove n è un intero positivo ed $\overline{f}$ la classe dei residui di f modulo $\mathfrak{M}_P^n$.
Per $r \geq 1$ pongo

$$S_r = \{ f \in S \mid \nu_P(f-1) = r \} \ \text{ e } \ S_r(n) = \{ \overline{f} \in S(n) \mid f \in S_r \} \ .$$

Da notare che S_r può essere vuoto. Considero la successione di insiemi non vuoti (partendo dall'indice più piccolo) $S_{i_1}, S_{i_2}, S_{i_3}, \ldots$.

Lemma 5.1.9 *Con le notazioni precedenti, si supponga che gli interi positivi l ed n soddisfano la relazione $i_l < n \leq i_{l+1}$. Allora:*

(i) $|S_{i_j}(n)| = (p-1)p^{l-j}$ *per ogni* $j = 1, 2, \ldots, l$;

(ii) $|S(n)| = p^l$.

Se m, n sono due qualsiasi interi positivi, denoto con $T_p(m)$ l'insieme dei primi m interi positivi che non sono divisibili per p, i.e.

$$T_p(m) = \left\{ i \in \mathbb{Z} \mid p \nmid i \, , \ i = 1, 2, \ldots, m + \left[\frac{m}{p-1} \right] \right\} \ ,$$

e con $s_p(m,n)$ il numero

$$s_p(m,n) = \sum_{i \in T_p(m)} \left(\left[\log_p \frac{n}{i} \right] + 1 \right) . \tag{5.2}$$

Lemma 5.1.10 *Sia $F/\mathbb{F}_p$ un campo di funzioni con almeno $m+2$ posti razionali, diciamo $P_1, P_2, \ldots, P_m, P, P_\infty$. Se $(f_i) = h(F)P_i - h(F)P_\infty$, $f_i \equiv 1 \pmod{\mathfrak{M}_P}$, $1 \le i \le m$, e $\mathrm{MCD}(h(F), p) = 1$, allora $S(n)$ è generato dall'insieme $\{\overline{f}_1, \overline{f}_2, \ldots, \overline{f}_m\}$.*

Enuncio ora il primo dei due teoremi che prova l'esistenza di un campo di funzioni con molti punti razionali usando estensioni di classe ray ristrette:

Teorema 5.1.11 *Sia $F/\mathbb{F}_p$ un campo di funzioni con almeno $m+2$ punti razionali distinti $P_1, P_2, \ldots, P_m, P, P_\infty$, $m \ge 1$. Sia $E = \mathcal{H}_{\mathcal{S}}(\Lambda(\mathfrak{p}^n))$ il campo di classe ray ristretto di modulo $\mathfrak{p}^n$ determinato dall'$\mathcal{O}_{\mathcal{S}}$-modulo di Drinfeld di rango 1 $\mathrm{sgn}-$ normalizzato ϕ su $\mathcal{H}_{\mathcal{S}}$, $\mathcal{S} = \mathbf{P}_F \setminus \{P_\infty\}$. Supposto che $n - \left[\frac{n-1}{p}\right] \ge m$ e $(P_1, P_2, \ldots, P_m) = \mathrm{Cl}(\mathcal{O}_{\mathcal{S}})$, allora esiste un sottocampo $K/\mathbb{F}_p$ dell'estensione E/F tale che*

(i)
$$g(K) = 1 + \frac{1}{2}p^{n-1-s}(2g(F) - 2 + n) - \frac{1}{2}\Big(\sum_{r=1}^{s} p^{j_r - r} + \frac{p^{n-1-s} - 1}{p-1} + 1\Big) ,$$

dove $s = s_p(m, n)$ è dato dalla (5.2) e $j_1, j_2, \ldots, j_s$ sono s interi soddisfacenti la condizione $1 \le j_1 < j_2 < \cdots < j_s < n$. Inoltre, nel caso in cui $i_s < n \le i_{s+1}$, ho che $j_r = i_r$ per ogni $r = 1, 2, \ldots, s$, dove i_r è come nel lemma 5.1.9.

(ii) *$N(K) \ge p^{n-1-s}(m+1) + 1$, dove l'uguaglianza vale se $P_1, P_2, \ldots, P_m, P, P_\infty$ sono tutti posti razionali di F.*

Esempio 5.1.12 Considero il campo delle funzioni ellittiche $F = \mathbb{F}_2(x, y)$ definito dall'equazione
$$y^2 + y = x^3 + x .$$
Questo campo ha cinque posti razionali: uno è il posto all'infinito P_∞, il quale è un polo di x, e gli altri quattro posti sono $P = (0,0)$, $P_1 = (0,1)$, $P_2 = (1,0)$, $P_3 = (1,1)$, dove $R = (a, b)$ indica un posto razionale di F determinato da $(x, y) \equiv (a, b) \pmod{\mathfrak{M}_R}$. Considero i seguenti tre elementi di $\mathcal{O}_{\mathcal{S}}$, $\mathcal{S} = \mathbf{P}_F \setminus \{P_\infty\}$:
$$f_1 := xy + y + 1 \ , \ \ f_2 := xy + x^2 + 1 \ , \ \ f_3 := xy + x^2 + x + 1 .$$
I loro divisori principali associati sono
$$(f_i) = 5P_i - 5P_\infty \ , \ \ i = 1, 2, 3 .$$
Scelgo x come uniformizzante per P. Allora f_1, f_2, f_3 hanno la seguente espansione locale per P:
$$\begin{aligned} f_1 &= 1 + x + x^5 + x^6 + x^7 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{17} + \cdots , \\ f_2 &= 1 + x^3 + x^4 + x^5 + x^7 + x^9 + x^{13} + x^{17} + \cdots , \\ f_3 &= 1 + x + x^3 + x^4 + x^5 + x^7 + x^9 + x^{13} + x^{17} + \cdots . \end{aligned}$$
Sia, per $n \ge 6$, $E = \mathcal{H}_{\mathcal{S}}(\Lambda(\mathfrak{p}^n))$. Poiché il numero di classe $h(F)$ di F è 5, per il lemma 5.1.10 $S(n)$ è generato da $\overline{f}_1$, $\overline{f}_2$, $\overline{f}_3$.
Ovviamente S_1, S_2, S_3, S_4, S_6, S_8, S_{12} ed S_{16} sono non vuoti. Inoltre, poiché $f_1^3 f_2 f_3$ ha espansione locale per P
$$f_1^3 f_2 f_3 = 1 + x^5 + x^7 + x^8 + \cdots ,$$

anche S_5 ed S_{10} sono non vuoti.
Considero ora il gruppo $S(16)$. Noto che $\overline{f}_1$ genera un gruppo ciclico di ordine 16 in $S(16)$ ed $\overline{f}_2$ genera un gruppo ciclico di ordine 8. Ma

$$f_3^4 \equiv (f_1 f_2)^4 \pmod{\mathfrak{p}^{16}} ,$$

quindi $\{\overline{f}_1, \overline{f}_2, \overline{f}_3\}$ genera un sottogruppo di ordine al più 2^9 in $S(16)$. Per il lemma 5.1.9 ci sono al più nove insiemi S_r con $r < 16$ soddisfacenti $S_r \neq \varnothing$. Quindi $S_7 = S_9 = S_{11} = S_{13} = S_{14} = S_{15} = \varnothing$.
Per il teorema 5.1.11 ottengo un'estensione $K_n/\mathbb{F}_2$ con $n = 8, 10, 12, 14, 15$ tale che $\big(g(K_n), N(K_n)\big) = (5,9), (15,17), (39,33), (95,65), (215,129)$ rispettivamente. Da notare che i primi tre valori sono ottimali e che, considerando il limite di Oesterlé dato nel teorema 2.3.12, per gli altri due si ha $65 \leq N_2(95) \leq 68$ e $129 \leq N_2(215) \leq 135$ (si consulti le tavole 1 e 3).

Esempio 5.1.13 Sia $F = \mathbb{F}_3(x, y)$ un campo di funzioni su $\mathbb{F}_3$ definito dall'equazione

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

Allora $g(F) = 1$ ed F ha sette posti razionali: uno è il polo di x denotato al solito con P_∞ e gli altri sono $P = (0,1)$, $P_1 = (0,2)$, $P_2 = (1,1)$, $P_3 = (1,2)$, $P_4 = (2,1)$, $P_5 = (2,2)$. Sia $E = \mathcal{H}_{\mathcal{S}}(\Lambda(\mathfrak{p}^n))$, $\mathcal{S} = \mathbf{P}_F \setminus \{P_\infty\}$. Considero i cinque seguenti elementi di $\mathcal{O}_{\mathcal{S}}$:

$$\begin{aligned}
f_1 &:= 2(x+1)^2 y + 2x^3 + 2x^2 + 2 , \\
f_2 &:= 2x^2 y + (x+2)^3 + (x+2)^2 + 1 , \\
f_3 &:= x^2 y + (x+2)^3 + (x+2)^2 + 1 , \\
f_4 &:= (x+2)^2 y + 2(x+1)^3 + 2(x+1)^2 + 2 , \\
f_5 &:= (x+2)^2 y + (x+1)^3 + (x+1)^2 + 1 .
\end{aligned}$$

I corrispondenti divisori principali sono

$$(f_i) = 7P_i - 7P_\infty , \ 1 \leq i \leq 5 .$$

Scelgo x come uniformizzante per P. Allora le f_i hanno la seguente espansione locale per P:

$$\begin{aligned}
f_1 &= 1 + x^2 + x^3 + x^7 + \cdots , \\
f_2 &= 1 + x + 2x^4 + 2x^5 + x^7 + \cdots , \\
f_3 &= 1 + x + 2x^2 + 2x^3 + x^4 + x^5 + 2x^7 + \cdots , \\
f_4 &= 1 + 2x^2 + 2x^3 + 2x^4 + x^6 + x^8 + \cdots , \\
f_5 &= 1 + x + x^2 + x^3 + 2x^4 + x^6 + x^8 + \cdots .
\end{aligned}$$

Quindi S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_9 ed S_{12} sono non vuoti e l'insieme $\{\overline{f}_1, \overline{f}_2, \overline{f}_3, \overline{f}_4, \overline{f}_5\}$ genera un sottogruppo di $S(12)$ di ordine al più $3^2 \cdot 3^3 \cdot 3 \cdot 3 \cdot 3 = 3^8$. Ciò comporta, per il lemma 5.1.10, che $|S(12)| \leq 3^8$. Dal lemma 5.1.9 quindi si ha che $S_8 = S_{10} = S_{11} = \varnothing$.
Per il teorema 5.1.11 ottengo quindi un'estensione $K_n/\mathbb{F}_3$ con $n = 9, 11, 12$ tale che $\big(g(K_n), N(K_n)\big) = (10,19), (43,55), (151,163)$ rispettivamente, per cui ho i seguenti valori: $19 \leq N_3(10) \leq 21$ [1], $55 \leq N_3(43) \leq 60$ e $163 \leq N_3(151) \leq 171$ (si consulti le tavole 2 e 4).

[1] Nel 2003 M. Grassl trovò espilicitamente una curva di genere 10 con 20 punti razionali (si confronti la tavola 2).

Teorema 5.1.14 *Sia $q = p^r$, p numero primo ed $r \geq 1$ e per un dato intero $m \geq 1$ sia $F/\mathbb{F}_q$ un campo di funzioni di genere $g(F)$ con $N(F) \geq m+1$. Si supponga che F abbia almeno un posto di grado $d > 1$ con $rd > m$.*
Assunto che $N_q(1 + p(g(F) - 1)) < (m+1)p$ quando $g(F) \geq 1$, allora per ogni intero l tale che $1 \leq l \leq rd - m$ esiste un campo di funzioni $K_l/\mathbb{F}_q$ tale che

(i) *Il numero dei posti razionali di $K_l/\mathbb{F}_q$ soddisfa $N(K_l) \geq (m+1)p^l$ e $p^l | N(K_l)$. Inoltre $N(K_l) = (m+1)p^l$ se $N(F) = m+1$.*

(ii) *Il genere di $K_l/\mathbb{F}_q$ è dato da*

$$g(K_l) = p^l(g(F) + d - 1) + 1 - d \, .$$

Esempio 5.1.15 Sia $F = \mathbb{F}_2(x, y)$ un campo di funzioni ellittiche su $\mathbb{F}_2$ definito dall'equazione

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

con cinque punti razionali. Allora esistono posti di F di grado d per ogni $d \geq 5$. Ponendo $m = 4$, poiché $N_2(1 + 2(g(F) - 1)) = N_2(1) = 5 < 10 = 2(m+1)$, dal teorema 5.1.14 ho che per ogni $d \geq 5$ esiste un campo di funzioni $K_d/\mathbb{F}_2$ tale che

$$g(K_d) = 1 + (2^{d-4} - 1)d \ , \ \ N(K_d) = 5 \cdot 2^{d-4} \, .$$

I campi K_5, K_6, K_7 sono ottimali.

Esempio 5.1.16 Sia $F/\mathbb{F}_2(x, y)$ un campo di funzioni su $\mathbb{F}_2$ definito dall'equazione

$$y^2 + y = \frac{x(x+1)}{x^3 + x + 1} \, .$$

Allora $g(F) = 2$ ed F ha sei posti razionali.
Esistono posti di F di grado d per ogni $d \geq 6$ (si confronti la proposizione 2.3.1). Posto $m = 5$ le condizioni del teorema sono soddisfatte e quindi per ogni $d \geq 6$ esiste un campo di funzioni $K_d/\mathbb{F}_2$ tale che

$$g(K_d) = 1 + 2^{d-5}(d+1) - d \ , \ \ N(K_d) = 6 \cdot 2^{d-5} \, .$$

Il campo K_6 è ottimale e $24 = N(K_7) \leq N_2(26) \leq 25$ e $N(K_8) \leq N_2(65) \leq 50$ (si consulti le tavole 1 e 3).

5.2 Curve esplicite

Nell'affrontare il problema di trovare curve con molti punti razionali (rispetto al genere), J. P. Hansen e H. Stichtenoth si concentrarono su famiglie di curve con gruppi di automorfismi "grandi" (si confronti [Sti1]), in particolare famiglie di gruppi associati alla varietà di Deligne-Lusztig (Hansen definisce e studia queste varietà in [Hanj]).
Le curve costruite dai gruppi di Hermite, di Suzuki e di Ree sono irriducibili ed ottimali. Senza scendere nei dettagli, che si possono trovare in [Lau], [Sti2] e [Hanj], darò una descrizione del campo di classe ray delle curve hermitiane, di Suzuki e di Ree.

5.2.1 Le curve hermitiane

Definizione 5.2.1 Sia $q = p^m$ la potenza m-esima di un numero primo. Il campo di funzioni $H = \mathbb{F}_{q^2}(x, y)$ su $\mathbb{F}_{q^2}$ con

$$y^q + y = x^{q+1}$$

è chiamato **campo di funzioni hermitiano**. La curva corrispondente è detta **curva hermitiana**.

Osservazione 5.2.2 (i) Una curva hermitiana è una curva del tipo Artin-Schreier definita su un campo di ordine una potenza pari;

(ii) Una curva hermitiana ha genere $g = q(q-1)/2$;

(iii) Il numero di punti di una curva hermitiana è $q^3 + 1$ (è una curva massimale);

(iv) $H/\mathbb{F}_{q^2}$ è un campo di funzioni massimale.

Le curve hermitiane possono essere ulteriormente caratterizzate:

Lemma 5.2.3 *Sia $F = \mathbb{F}_{q^2}(x)$ e si consideri l'estensione H/F definita dall'equazione $y^q + y = x^{q+1}$. Questa estensione ha grado q, è totalmente ramificata per P_∞ e completamente separata per tutti gli altri posti razionali.*
Inoltre la filtrazione del suo gruppo di ramificazione per P_∞ è

$$G = G_1 = G_2 = \cdots = G_{q+1} ,$$
$$G_{q+2} = \{1\} .$$

Teorema 5.2.4 *Sia $F = \mathbb{F}_{q^2}(x)$ e $D = (q+2)P_\infty$. Allora l'estensione abeliana di F ottenuta separando tutti i posti razionali di F ha grado q. La curva corrispondente è una curva hermitiana.*

Da questo teorema e dal metodo di Serre (si confronti il paragrafo 3.4) ottengo il seguente

Corollario 5.2.5 *Sia $\mathbb{F}_{q^2}$ un campo finito con q^2 elementi, q una potenza di un primo. Sia $k = q + 2$. Allora*

$$|(\mathbb{F}_{q^2}[t]/t^k)^*/\mathbb{F}_{q^2}^* \cdot < 1 - \alpha t \mid \alpha \in \mathbb{F}_{q^2}^* > | = q .$$

Inoltre questo quoziente è banale se $k < q + 2$, nel qual caso tutti i polinomi si riducono in fattori di grado 1.

Esempio 5.2.6 Con $q^2 = 4$, $k = 4$, si ottiene una curva ellittica con nove punti. Questo caso è stato trattato nell'esempio 3.4.12, nel quale si è verificato che l'estensione ha effettivamente grado 2.

Viene naturale chiedersi se le curve hermitiane possono essere generalizzate per campi di ordine una potenza dispari, in maniera da ottenere una famiglia di curve (ottimali). Una soluzione parziale al problema è stata data per campi di caratteristica 2 e 3: le curve di Suzuki e di Ree, che definirò a breve, soddisfano quanto richiesto. Inoltre la descrizione del loro campo di classe ray è simile a quella data per le curve hermitiane: Mentre quest'ultime sono ottenute separando tutti i $q = p^{2m}$ punti della retta proiettiva di modulo $D = (p^m + 2)P_\infty$, le curve di Suzuki e di Ree si basano sulla possibilità di ottenere la separazione di tutti i q punti quando $q = p^{2m+1}$ e $D = (p^{m+1} + 2)P_\infty$.

5.2.2 Le curve di Suzuki

Le **curve di Suzuki** sono varietà di Deligne-Lusztig costruite dal campo algebrico lineare Sz(q), $q = 2^{2m+1}$ (si veda [H-B]). Esse sono definite su $\mathbb{F}_q$ dall'equazione

$$y^q + y = x^{q_0}(x^q + x) \ ,$$

dove $q_0 = 2^m$.

Osservazione 5.2.7 (i) Una curva di Suzuki è una curva irriducibile di genere $q_0(q-1)$;

(ii) Una curva di Suzuki è una curva ottimale con $1 + q^2$ punti. Lo si capisce dal fatto che si può scegliere un polinomio trigonometrico

$$f(\theta) = 1 + 2\sum_{n=1}^{+\infty} c_n \cos(n\theta)$$

con $c_1 = \sqrt{2}/2$, $c_2 = 1/4$, $c_i = 0$ per $i > 2$ e notare che così facendo si incontra il limite di Oesterlé.

Lemma 5.2.8 *Detto $F = \mathbb{F}_q(x)$, $q = 2^{2m+1}$, considero l'estensione S/F definita dall'equazione $y^q - y = x^{q_0}(x^q - x)$, $q_0 = 2^m$. Questa estensione ha grado q, è totalmente ramificata per P_∞ e completamente separata per tutti gli altri posti razionali.*
Inoltre la filtrazione del suo gruppo di ramificazione per P_∞ è

$$G = G_1 = G_2 = \cdots = G_{2q_0+1} \ ,$$
$$G_{2q_0+2} = \{1\} \ .$$

Teorema 5.2.9 *Sia $F = \mathbb{F}_q(x)$ e $D = (q+2)P_\infty$. Allora l'estensione abeliana di F ottenuta separando tutti i posti razionali di F nel campo di classe ray di modulo D ha grado q. La curva corrispondente è una curva di Suzuki.*

Come per le curve hermitiane, vale il seguente

Corollario 5.2.10 *Sia $\mathbb{F}_q$ un campo finito con $q = 2^{2m+1} = 2q_0^2$ elementi. Sia $k = 2q_0+2$. Allora*

$$|(\mathbb{F}_q[t]/t^k)^*/\mathbb{F}_q^* \cdot < 1 - \alpha t \mid \alpha \in \mathbb{F}_q^* > | = q \ .$$

Inoltre questo quoziente è banale se $k < 2q_0 + 2$, nel qual caso tutti i polinomi si riducono in fattori di grado 1.

Esempio 5.2.11 Quando $q = 8$, $q_0 = 2$ ho un ricoprimento di grado 8 di $\mathbb{P}^1$ nel campo di classe ray di modulo $D = 6P_\infty$, nel quale tutti gli otto punti si separano. La curva è di genere 14 ed ha 65 punti razionali.

5.2.3 Le curve di Ree

Le **curve di Ree** sono varietà di Deligne-Lusztig costruite dal gruppo algebrico di Ree R(q), $q = 3^{2m+1}$ (si veda [H-B]). Esse possono essere viste come dei ricoprimenti abeliani di $\mathbb{P}^1$ di grado q^2.
La seguente osservazione è stata fatta da K. Lauter in [Lau]:

Osservazione 5.2.12 (i) Il genere di una curva di Ree è

$$g = \frac{3}{2} q_0 (q-1)(q+q_0+1) \ , \ \ q_0 = 3^m \ .$$

(ii) Una curva di Ree è una curva ottimale con $1+q^3$ punti. Lo si capisce dal fatto che si può scegliere un polinomio trigonometrico

$$f(\theta) = 1 + 2 \sum_{n=1}^{+\infty} c_n \cos(n\theta)$$

con $c_1 = \sqrt{3}/2$, $c_2 = 7/12$, $c_3 = \sqrt{3}/6$, $c_4 = 1/12$, $c_i = 0$ per $i > 2$ e notare che così facendo si incontra il limite di Oesterlé.

Le curve di Ree ottenute separando tutti i q posti nel campo di classe ray di modulo $D = (3^{m+1}+2)P_\infty$ su $\mathbb{P}^1$ dà luogo ad un'estensione di $\mathbb{P}^1$ di grado q.
Da qui si intende ottenere un'estensione di grado q^2. J. P. Pedersen [Ped] determinò le equazioni del campo di funzioni corrispondente alla curva di Ree: $R = \mathbb{F}_q(x, y_1, y_2)$ con equazioni

$$\begin{aligned} y_1^q - y_1 &= x^{q_0}(x^q - x) \ , \\ y_2^q - y_2 &= x^{q_0}(y_1^q - y_1) \ . \end{aligned}$$

Chiamo $R_1 = \mathbb{F}_q(x, y_1)$ il campo definito dalla prima equazione. La curva corrispondente ad R_1 è un ricoprimento di $\mathbb{P}^1$ di grado q e genere

$$g_1 = \frac{3}{2} q_0 (q-1) \ .$$

Il seguente lemma è stato determinato da Hansen e Pedersen (si veda [Hanj-P]):

Lemma 5.2.13 *Se R è il campo delle funzioni delle curve di Ree, allora la filtrazione del suo gruppo di ramificazione per P_∞ è come segue:*

$$\begin{aligned} &G_0 = G_1 = \cdots = G_{3q_0+1} \ , \\ &G_{3q_0+2} = G_{3q_0+3} = \cdots = G_{3q_0+q+1} \ , \\ &G_{3q_0+q+2} = \{1\} \ , \end{aligned}$$

con $|G_0| = q^2$ e $|G_{3q_0+2}| = q$.

Tale lemma mi dà la seguente caratterizzazione di R come ricoprimento abeliano di $\mathbb{P}^1$ di grado q^2 (si veda [Lau]):

Teorema 5.2.14 *Sia $F = \mathbb{F}_q(x)$, $D = (3^{m+1}+3)P_\infty$, dove $q = 3^{2m+1}$. Allora l'estensione abeliana di F ottenuta separando tutti gli altri posti razionali di F nel campo di classe ray di modulo D ha grado q^2. La curva corrispondente è una curva di Ree.*

Capitolo 6

Tavole

Ho riportato per comodità le tavole dei valori di $N_q(g)$, il massimo numero di posti razionali di un campo di funzioni di dato genere g, o dell'intervallo che inquadra $N_q(g)$. Se non è conoscuto il preciso valore di $N_q(g)$, o viene dato un intervallo $a - b = a_q(g) - b_q(g)$, o non viene dato alcun valore. Quando risulta esserci un intervallo, significa che esiste un campo di funzioni con almeno a posti razionali su $\mathbb{F}_q$ e che il limite superiore migliore per $N_q(g)$ è b (si veda il capitolo 2). Quando la casella è vuota, significa che non è ancora stata provata l'esistenza di un campo di funzioni con almeno $[b/\sqrt{2}]$ posti razionali, i.e. quando $a_q(g) \leq [b_q(g)/\sqrt{2}]$. Il motivo di questa limitazione sta nel fatto che nella maggioranza dei casi considerati il limite superiore $b_q(g)$ è il limite di Ihara (2.5) e poiché il limite asintotico (2.9) di Vlăduţ-Drinfeld è aprossimativamente il limite asintotico di Ihara (2.8) è ragionevole pensare di non considerare campi di funzioni "poveri".
Poiché $N_q(0) = q+1$ per ogni q, i valori di $N_q(0)$ non sono rappresentati in nessuna tavola.

La tavola 1 riporta i valori di $N_q(g)$ con $q = 2^m$, $1 \leq m \leq 7$ e $g \leq 50$. Da notare che $g = 50$ è il più grande genere per il quale si conosca il valore preciso di $N_2(g)$. È per questo motivo che la tavola 1 arriva fino a tale valore per il genere.
La tavola 2 riporta i valori di $N_q(g)$ con $q = 3^m$, $1 \leq m \leq 4$ e $g \leq 50$.
Una versione completa di referenze di queste due tavole si può trovare in [G-V6].
La tavola 3 riporta i valori di $N_q(g)$ con $q = 2^m$, $1 \leq m \leq 4$ e $g > 50$.
La tavola 4 riporta i valori di $N_q(g)$ con $q = 3^m$, $1 \leq m \leq 3$ e $g > 50$.
Infine la tavola 5 riporta i valori di $N_5(g)$ per $g = 9, 11, 17, 22$.
Queste ultime tre tavole si possono trovare in parte in [N-X] ed in parte in [Sti2]. Da notare che i valori della tavola 5 provengono tutti da costruzioni di campi di funzioni espliciti (si veda [N-X, p. 116]).

Tavola 1 p=2

$g \setminus p$	2	4	8	16	32	64	128
1	5	9	14	25	44	81	150
2	6	10	18	33	53	97	172
3	7	14	24	38	64	113	192
4	8	15	25	45	71-74	129	215
5	9	17	29-30	49-53	83-85	132-145	227-234
6	10	20	33-35	65	86-96	161	243-258
7	10	21-22	34-38	63-69	98-107	177	258-283
8	11	21-24	34-42	61-75	97-118	169-193	266-302
9	12	26	45	72-81	108-128	209	288-322
10	13	27	42-49	81-87	113-139	225	289-345
11	14	26-29	48-53	80-91	120-150	201-236	
12	14-15	29-31	49-57	83-97	129-161	257	321-388
13	15	33	56-61	97-102	129-172	225-268	
14	15-16	32-35	65	97-107	146-183	241-284	353-437
15	17	33-37	57-67	98-113	158-194	258-300	386-455
16	17-18	36-38	56-71	95-118	147-204	267-316	
17	17-18	40	63-74	112-123	154-212		
18	18-19	41-42	65-77	113-129	161-220	281-348	
19	20	37-43	60-80	129-134	172-228	315-364	
20	19-21	40-45	68-83	127-139	177-236	297-380	
21	21	41-47	72-86	129-145	185-244	281-396	
22	21-22	42-48	74-89	129-150		321-412	
23	22-23	45-50	68-92	126-155			
24	21-23	49-52	81-95	129-161	225-267	337-444	513-653
25	24	51-53	86-97	144-166		335-460	
26	24-25	55	82-100	150-171		385-476	
27	24-25	50-56	96-103	145-176	213-290	401-492	
28	25-26	53-58	97-106	145-181	257-298	513	577-745
29	25-27	52-60	97-109	161-187	227-306		
30	25-27	53-61	96-112	162-191	273-313	401-535	609-784
31	27-28	60-63	89-115	165-196		386-547	578-807
32	26-29	57-65	90-118				
33	28-29	65-66	97-121	193-207			
34	27-30	65-68	98-124	183-212		447-582	
35	29-31	64-69	112-127		253-352		
36	30-31	64-71	107-130	185-222		441-604	
37	30-32	66-72	121-132	208-227			
38	30-33	64-74	129-135	193-233	291-375	449-627	
39	33	65-75	120-138	194-238			
40	32-34	75-77	103-141	225-243	293-390	489-650	
41	33-35	65-78	118-144	216-249	308-398		
42	33-35	75-80	129-147	209-254	307-405	513-672	
43	33-36	72-81	116-150	226-259	306-413	483-684	
44	33-37	68-83	130-153	226-264	325-420		
45	33-37	80-84	144-156	242-268	313-428		

Tavola 1 (cont.) p**=2.**

$g \setminus p$	2	4	8	16	32	64	128
46	34-38	81-86	129-158	243-273			
47	36-38	73-87	126-161				
48	34-39	80-89	128-164	243-282			
49	36-40	81-90	130-167	213-286			
50	40	91-92	130-170	255-291		561-762	

Tavola 2 p**=3.**

$g \setminus p$	3	9	27	81
1	7	16	38	100
2	8	20	48	118
3	10	28	56	136
4	12	30	64	154
5	13	32-35	72-75	160-172
6	14	35-40	76-85	190
7	16	40-43	82-95	180-208
8	17-18	40-47	92-105	226
9	19	48-50	99-113	244
10	20-21	54	94-123	226-262
11	20-22	55-58	100-133	220-280
12	22-23	56-62	109-143	298
13	24-25	64-65	136-153	256-312
14	24-26	56-69		278-330
15	28	64-73	136-170	292-348
16	27-29	74-77	144-178	370
17	25-30	74-81		288-384
18	26-31	67-84	148-192	
19	32	84-88		
20	30-34	70-91		
21	32-35	88-95	163-213	352-455
22	30-36	78-98		
23	32-37	92-101		
24	31-38	91-104	208-234	
25	36-40	82-108	196-241	392-527
26	36-41	110-111		
27	39-42	91-114		
28	37-43	105-117		
29	42-44	104-120		
30	37-46	91-123	196-276	
31	40-47	120-127		460-635
32	40-48	92-130		

Tavola 2 (cont.) p**=3.**

$g \setminus p$	3	9	27	81
33	46-49	128-133	220-297	
34	45-50	111-136		494-689
35	47-51	116-139		
36	48-52	118-142	244-318	730
37	52-54	120-145	236-325	568-742
38		105-149		
39	48-56	140-152	271-340	
40	56-57	118-155	244-346	
41	50-58	128-158		
42	52-59	122-161	280-360	
43	55-60	120-164		
44		119-167	278-374	
45	54-62	136-170		
46	55-63	162-173		
47	54-65	154-177	299-395	
48	55-66	163-180	325-402	676-885
49	64-67	168-183	316-409	656-898
50	63-68	182-186	312-416	

Tavola 3 $p=2$, $g>50$.

$g \setminus p$	2	4	8	16
51	36-41	88-93		250-295
52	34-42			
53	40-42		120-179	
54	42-43		129-181	257-309
55	41-43			273-313
56	38-44			
57	40-45	63-102		
58	41-45			273-327
59	40-46	77-105		
60	41-47			257-336
61	41-47	99-108		
62	44-48			
63	42-48			
64	42-49			291-354
65	48-50	98-114		
66	48-50			
67	44-51			
68	49-51			
69	49-52			
70	46-53	105-121		
71	49-53			
72	48-54			
73	48-54			312-393
74	49-55			
75	49-56			
76	50-56	99-130		315-407
77	52-57		195-242	
78	48-57		175-245	
79	52-58			
80	56-59			
81	56-59	129-137		
82	53-60			
83	57-60			
84	57-61			
85	52-62			324-446
86	56-62			
87	56-63			
88	56-63	123-147		
89	57-64			
90	56-65			
91	57-65	144-151		325-472
92	60-66	143-152		
93	56-66		192-284	
94	56-67	129-155		
95	65-68			

Tavola 3 (cont.) $p=2$, $g>50$.

$g \setminus p$	2	4	8	16
97		99-159		
101		125-165		340-516
103	65-72			
105		129-170		
106				325-538
109		165-176		
113		161-181		
114		161-183		
115		168-184		
118			257-348	513-590
121		150-192		
123				533-611
125		176-198		
126	81-86			
140				577-685
141			259-407	
145		195-225		
148		215-229		
149			324-428	
154		168-237		
156				650-754
158		209-243		
161		194-247		
162		209-248		
181		220-274		
183		220-276		
186				725-884
191		258-287		
193		257-290		
199		216-298		
208		243-309		
210		257-312		
215	129-135			
225			453-616	
226				825-1054
234		301-343		
235				898-1090
241		245-353		
245				936-1131
257		321-373		
274		321-396		
279				994-1267
295		344-423		
298		384-427		
306				1025-1374

Tavola 3 (cont.) $p=2$, $g>50$.

$g \setminus p$	2	4	8	16
321		385-456		
337		429-523		
352				1155-1557
367				1209-1616
370		417-520		
373		429-523		
376			755-977	
379		456-531		
449		513-619		
451		480-622		
461			936-1178	
466		513-641		
471	257-272			
492		559-673		
511				1845-2181
571		645-772		
577		641-779		
598				2049-2521
621		688-834		
705		769-939		
716				2305-2980
750		817-994		
766		855-1014		
769		771-1018		
906				2885-3719
936				2990-3835
937		1026-1223		
1015		1152-1318		
1021				3280-4163
1108		1197-1430		
1195				3586-4812
1207		1344-1550		
1731		1760-2179		
2083		2112-2596		
2435		2464-3011		
2476				7488-9525

Tavola 4 $p=3$, $g>50$.

$g \setminus p$	3	9	27
52		175-192	
55		164-201	
60		190-217	

Tavola 4 (cont.) $p=3$, $g>50$.

$g \setminus p$	3	9	27
61		192-220	
69	82-88		
70		189-247	
79		228-273	
81		245-279	
82		192-282	
90		244-304	
93		196-313	
95		272-318	
101		275-335	
102		244-338	
109		298-358	
112		315-366	
119		308-386	
131		320-419	
136		354-433	
142		327-449	
151	163-171	427-642	
154		357-483	
183		487-563	
186		455-571	
209			896-1404
212		427-642	
217		488-656	
223		570-672	
226		500-681	
231		568-694	
238		609-713	
258	244-275		
286		678-840	
301		732-879	
334		793-965	
365		812-1045	
367		756-1050	
371		815-1061	
396		875-1125	
406		892-1151	
451		915-1267	
487		1056-1359	
556		1323-1536	
634		1464-1735	
667		1342-1819	
669		1459-1824	
700		1525-1903	

Tavola 5 $p=5$.

g	9	11	17	22
$N_5(g)$	26	32	42	51

Appendice A

Teoria dei campi e degli anelli commutativi

A.1 Estensioni di campi

I risultati esposti in questa appendice si possono trovare in molti libri di testo, ad esempio in [Jac], [N-X], [Sti2] e [A-M]. Per le dimostrazioni si rimanda il lettore a queste letture.

In tutto il paragrafo E e F indicano campi qualsiasi se non specificato altrimenti.

Siano E e F campi tali che $E \supseteq F$ come sottocampo. Allora si dice che E **estende** F come campo. L'**estensione** di F ad E è indicata con E/F.
Considerato E come F-spazio vettoriale, la sua dimensione è chiamata **grado** di E/F ed è indicata con $[E : F]$. E/F è chiamata **estensione finita** se $[E : F] = n < \infty$ ed in tal caso esiste una **base** $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ di E su F, i.e. ogni $\gamma \in E$ è rappresentabile in maniera unica come combinazione lineare degli α_i, $i = 1, 2, \ldots, n$.

Se $E \supseteq K \supseteq F$ come campi e E/K e K/F sono estensioni finite, allora vale il teorema dei gradi: $[E : F] = [E : K][K : F]$.

Un elemento $\alpha \in E$ si dice **algebrico su** F se esiste un polinomio non nullo $f(x) \in F[x]$ (l'anello dei polinomi in una variabile su F) tale che $f(\alpha) = 0$. Tra i polinomi per i quali $f(\alpha) = 0$ esiste un unico polinomio di grado minimo, monico (i.e. di coefficiente direttivo 1) ed irriducibile, chiamato **polinomio minimo** di α su F.
L'estensione E/F è chiamata **estensione algebrica** se tutti gli elementi di E sono algebrici su F.

Siano $\gamma_1, \gamma_2, \ldots, \gamma_n \in E$. Il più piccolo sottocampo di E che contiene F e gli elementi γ_i, $i = 1, 2, \ldots, n$, è denotato con $F(\gamma_1, \gamma_2, \ldots, \gamma_n)$.
L'estensione $F(\gamma_1, \gamma_2, \ldots, \gamma_n)/F$ è finita se e solo se γ_i è algebrico su F, per ogni $1 \leq i \leq n$.

Siano E_1/F, E_2/F estensioni e considero l'omomorfismo fra campi

$$\sigma : E_1 \to E_2 \quad \text{con } \sigma(a) = a \quad \text{per ogni } a \in F \ ,$$

chiamata **immersione** di E_1 in E_2. σ è iniettiva e perciò induce un isomorfismo di E_1 in $\sigma(E_1) \subseteq E_2$. Se σ è suriettiva si dice che σ è un **F-isomorfismo**.
Se $f_1(x), f_2(x), \ldots, f_r(x) \in F[x]$ sono polinomi monici di grado $d_i \geq 1$, $i = 1, 2, \ldots, r$, allora esiste un'estensione E/F tale che $f_i(x) = \prod_{j=1}^{d_i}(x - \alpha_{ij})$, con $\alpha_{ij} \in E$ ed $E = F(\{\alpha_{ij} | \, 1 \leq i \leq r \, , \, 1 \leq j \leq d_i\})$. Il campo E, unico a meno di F-isomorfismi, è chiamato **campo di riducibilità completa** o **campo di spezzamento** di $f_1(x), \ldots, f_r(x)$ su F.

Un campo F si dice **algebricamente chiuso** se ogni polinomio $f(x) \in F[x]$ ha uno zero in F (per esempio $\mathbb{C}$).
Per ogni campo F esiste un'estensione E/F tale che E sia algebricamente chiuso. Tale campo, indicato con $\overline{F}$, è unico a meno di F-isomorfismi ed è chiamato **chiusura algebrica** di F.
Data un'estensione E/F, esiste un'immersione $\sigma : E \to \overline{F}$. Se $[E : F] < \infty$ allora il numero delle immersioni distinte di E in $\overline{F}$ su F è al più $[E : F]$.

Sia F un campo ed $1 \in F$ l'elemento neutro (rispetto alla moltiplicazione). Sia, per ogni $m \in \mathbb{Z}_{>0}$,

$$\underline{m} = \underbrace{1 + 1 + \cdots + 1}_{m-volte}.$$

Se $\underline{m} \neq 0$ per ogni $m > 0$ si dice che F ha caratteristica 0. Altrimenti esiste un unico numero primo p tale che $\underline{p} = 0$ e si dice che F ha caratteristica p.
La **caratteristica** di un campo viene indicata con $\mathrm{char}(F)$.
Se $\mathrm{char}(F) = 0$ allora $F \supseteq \mathbb{Q}$.
Se $\mathrm{char}(F) = p > 0$ allora $F \supseteq \mathbb{Z}/p\mathbb{Z}$. In questo caso $(a + b)^q = a^q + b^q$, dove $a, b \in F$ e $q = p^j$, $j \geq 0$.

Sia $f(x) = \prod_{i=1}^{n}(x - \alpha_i) \in E[x]$, $\alpha_i \in E$ campo di riducibilità completa di f. Il polinomio $f(x)$ è chiamato **separabile** se $\alpha_i \neq \alpha_j$ per ogni $i \neq j$, altrimenti $f(x)$ è detto **inseparabile**.
Se $\mathrm{char}(F) = 0$ allora ogni polinomio irriducibile è separabile.
Se $\mathrm{char}(F) = p > 0$ allora ogni polinomio irriducibile $f(x) = \sum a_i x^i \in F[x]$ è separabile se e solo se $a_i \neq 0$ per qualche i che non è congruente a 0 modulo p.

Sia E/F un'estensione algebrica. Un elemento $\alpha \in E$ è chiamato **separabile** su F se il suo polinomio minimo è separabile.
Se ogni elemento di E è separabile su F si dice che E/F è un'**estensione separabile**.
Se $\mathrm{char}(F) = 0$ allora tutte le estensioni algebriche sono separabili.
Se E/F è un'estensione finita di grado n, allora tale estensione è separabile se e solo se esistono n immersioni distinte $\sigma_i : E \to \overline{F}$ su F, $i = 1, 2, \ldots, n$.

Sia E/F estensione algebrica e $\mathrm{char}(F) = p > 0$. Un elemento $\gamma \in E$ è chiamato **puramente inseparabile** su F se $\gamma^{p^r} \in F$ per qualche intero $r \geq 0$. In tal caso, il polinomio minimo di γ su F è $x^{p^e} - c$, con $c \in F$ ed $e \leq r$.
L'estensione E/F si dice **puramente inseparabile** se ogni elemento di E è puramante inseparabile su F.

Data un'arbitraria estensione E/F, esiste un unico campo intermedio K, $E \supseteq K \supseteq F$,

tale che K/F è separabile ed E/K è puramente inseparabile.

Un campo F è chiamato **perfetto** se tutte le sue estensioni algebriche sono separabili.
Se $\mathrm{char}(F) = 0$ allora F è perfetto.
Se $\mathrm{char}(F) = p > 0$ allora F è perfetto se e solo se l'applicazione $F \to F$ definita da $x \mapsto x^p$ è biettiva.

Un'estensione algebrica E/F è chiamata **semplice** se $E = F(\alpha)$ per qualche $\alpha \in E$. L'elemento α è detto **elemento primitivo** per E/F.

Sia E/F un'estensione; indico il gruppo degli automorfismi di E su F con $\mathrm{Aut}(E/F)$.
Se $[E : F] < \infty$, $|\mathrm{Aut}(E/F)| \leq [E : F]$, dove $|G|$ indica l'**ordine** del gruppo G.
L'estensione E/F è detta essere di **Galois** se $|\mathrm{Aut}(E/F)| = [E : F]$. In tal caso

$$\mathrm{Gal}(E/F) := \mathrm{Aut}(E/F)$$

viene chiamato **gruppo di Galois** di E/F.

Le seguenti condizioni, per estensioni finite di grado r, sono equivalenti:

(i) E/F è di Galois;

(ii) E è il campo di riducibilità completa dei polinomi separabili $f_1(x), f_2(x), \ldots, f_r(x)$ di $F[x]$ su F;

(iii) E/F è separabile ed ogni polinomio irriducibile $p(x) \in F[x]$ che ha uno zero in E si separa in fattori lineari in $E[x]$ (si dice solitamente che quindi l'estensione è **normale**).

Sia $G = \mathrm{Gal}(E/F)$. Definisco

$$\mathcal{H} := \{\, H \subseteq G \mid H \ \text{ sottogruppo di } \ G\}$$

e

$$\mathcal{F} := \{\, K \subseteq E \mid K \text{ sottocampo di } E\,,\ K \supseteq F\}.$$

Per un campo intermedio K di E/F (i.e. $K \in \mathcal{F}$), l'estensione E/K è di Galois; dunque è definita una mappa

$$\begin{array}{ccc} \mathcal{F} & \to & \mathcal{H} \\ K & \mapsto & \mathrm{Gal}(E/K) \end{array} \quad . \tag{A.1}$$

Viceversa, dato un sottogruppo H di G, definisco il campo degli elementi fissati da H come

$$E^H := \{\, c \in E \mid \sigma(c) = c\,, \text{ per ogni } \ \sigma \in H\}.$$

In questo modo ottengo una mappa

$$\begin{array}{ccc} \mathcal{H} & \to & \mathcal{F} \\ H & \mapsto & E^H \end{array} \quad . \tag{A.2}$$

Teorema A.1.1 (Fondamentale della teoria di Galois) (i) *Le mappe* (A.1) *e* (A.2) *sono una l'inversa dell'altra, i.e. c'è una corrispondenza biunivoca fra* $\mathcal{H}$ *ed* $\mathcal{F}$*, chiamata* **corrispondenza di Galois**.

(ii) *Per $H \in \mathcal{H}$ si ha $[E : E^H] = |H|$ e $[E^H : F] = (G : H) := |G|/|H|$ (indice di G su H).*

(iii) *Se $H \subseteq G$ come sottogruppo allora $H = \mathrm{Gal}(E/E^H)$;*
Se K è un campo intermedio di E/F allora $K = E^H$ con $H = \mathrm{Gal}(E/K)$.

(iv) *Per sottogruppi H_1, $H_2 \subseteq G$, $H_1 \subseteq H_2$ se e solo se $E^{H_1} \supseteq E^{H_2}$;*
Per campi intermedi K_1,K_2 di E/F, $K_1 \subseteq K_2$ se e solo se $\mathrm{Gal}(E/K_1) \supseteq \mathrm{Gal}(E/K_2)$.

(v) *Presi due campi intermedi K_1,K_2 di E/F, indico con $K = K_1 \circ K_2$; allora*

$$\mathrm{Gal}(E/K) = \mathrm{Gal}(E/K_1)\mathrm{Gal}(E/K_2) \ .$$

Inoltre, il gruppo di Galois di $E/(K_1 \cap K_2)$ è il sottogruppo di G generato da $\mathrm{Gal}(E/K_1)$ e $\mathrm{Gal}(E/K_2)$.

(vi) *Un sottogruppo $H \subseteq G$ è normale (i.e. $\sigma H \sigma^{-1} = H$ per ogni $\sigma \in G$) se e solo se l'estensione E^H/F è di Galois. In tal caso $\mathrm{Gal}(E^H/F) \cong G/H$ (il gruppo di Galois di E^H/F è isomorfo al gruppo quoziente G su H).*

Sia E/F un'estensione di Galois. Si dice che E/F è un'**estensione abeliana** se il gruppo $\mathrm{Gal}(E/F)$ è abeliano.

Sia E/F un'estensione finita. Un elemento $x \in E$ che non è algebrico su F è detto **trascendente** su F.
Un sottoinsieme finito $\{a_1, a_2, \ldots, a_n\} \subseteq E$ si dice **algebricamente indipendente** su F se non esiste un polinomio non nullo $f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ (anello dei polinomi in n variabili su F) tale che $f(a_1, a_2, \ldots, a_n) = 0$. Un arbitrario sottoinsieme S di E è detto algebricamente indipendente su F se tutti i sottoinsiemi finiti di S sono algebricamente indipendenti su F.
Una **base di trascendenza** di E/F è un sottoinsieme di E algebricamente indipendente massimale. Ogni base di trascendenza di E/F ha la stessa cardinalità, il **grado di trascendenza** di E/F.
Se E/F è un'estensione finita di grado di trascendenza n e $\{a_1, a_2, \ldots, a_n\}$ è una base di trascendenza di E/F, il campo $F(a_1, a_2, \ldots, a_n) \subseteq E$ è F-isomorfo a $F(x_1, x_2, \ldots, x_n)$, il campo delle frazioni dell'anello $F[x_1, x_2, \ldots, x_n]$. L'estensione $E/F(a_1, a_2, \ldots, a_n)$ è algebrica.

Un'estensione di Galois E/F si dice **ciclica** se $\mathrm{Gal}(E/F)$ è un gruppo ciclico. Due particolari estensioni cicliche sono l'estensione di Kummer e l'estensione di Artin-Schreier.

A.2 Estensioni di Kummer e di Artin-Schreier

Queste estensioni sono interessanti esenzialmente per due ragioni: la prima è che le equazioni che le definiscono possono essere espresse in maniera esplicita; la seconda è che se sono estensioni di un campo di funzioni $F/\mathbb{F}_q$, q potenza di un numero primo p, il loro genere è facile da calcolare.

Sia $n > 1$ un intero. Un elemento f di $F/\mathbb{F}_q$ è chiamato **n-esimo elemento degenere di Kummer** se esiste un elemento u di F ed un divisore $d > 1$ di n tale che $f = u^d$. Altrimenti si dice che f è un **n-esimo elemento non-degenere di Kummer**.
Sia $n > 1$ un divisore di $q-1$ e sia $f \in F$ un n-esimo elemento non-degenere di Kummer. Sia y uno zero del polinomio $T^n - f$. Allora $E := F(y)$ è un'estensione ciclica di F di grado n, chiamata **estensione di Kummer**.
Per le estensioni di Kummer vale il seguente

Teorema A.2.1 *Sia $f(x) := \alpha \prod_{i=1}^{r} p_i(x)^{n_i} \in \mathbb{F}_q[x]$, dove $p_1(x), p_2(x), \ldots, p_r(x)$ sono $r \geq 1$ polinomi irriducibili in $\mathbb{F}_q[x]$ distinti ed α è un elemento non nullo di $\mathbb{F}_q$. Si supponga che $n > 1$ divida $q-1$ e $\mathrm{MCD}(n_i, n) = 1$ per qualche $1 \leq i \leq r$. Sia y uno zero di $T^n - f$. Allora $E := \mathbb{F}_q(x, y)$ è un'estensione ciclica di $\mathbb{F}_q(x)$ di grado n, il campo completo delle costanti di E è $\mathbb{F}_q$ ed il genere di E è*

$$g(E) = 1 - \frac{1}{2}\big(n - \mathrm{MCD}(\deg(f), n)\big) + \frac{1}{2}\sum_{i=1}^{r}\big(n - \mathrm{MCD}(n_i, n)\big)\deg(p_i)\ .$$

Un elemento $f \in F/\mathbb{F}_{q^m}$, dove m è un intero positivo, è chiamato **elemento degenere di Artin-Schreier** se esiste un elemento u di F tale che $u^q - u = f$. Diversamente, f è detto **elemento non-degenere di Artin-Schreier**.
Una condizione sufficiente affinché $f \in F$ sia un elemento non-degenere di Artin-Schreier è che per qualche $P \in \mathbf{P}_F$ e qualche $z \in F$ si abbia $\nu_P\big(f - (z^q - z)\big) < 0$ ed anche $\mathrm{MCD}\big(\nu_P\big(f - (z^q - z)\big), p\big) = 1$.
Sia $f \in F$ un elemento non-degenere di Artin-Schreier. Sia y uno zero del polinomio $T^q - T - f$. Allora $E := F(y)$ è un'estensione ciclica di F di grado q, chiamata **estensione di Artin-Schreier**.
Sia $f \in F$ un elemento non-degenere di Artin-Schreier. Poiché l'intero $\nu_P\big(f - (z^q - z)\big)$ per un posto $P \in \mathbf{P}_F$ ed un elemento $z \in F$ è univocamente determinato, posso definire

$$m_P := \begin{cases} -1 & \text{se } \nu_P\big(f - (z^q - z)\big) \geq 0 \\ -\nu_P\big(f - (z^q - z)\big) & \text{se } \nu_P\big(f - (z^q - z)\big) < 0 \text{ ed è relativamente primo con } p \end{cases}$$

per qualche $z \in F$.
Per le estensioni di Artin-Schreier è importante il seguente teorema, che è un'immediata conseguenza del teorema di Hurwitz.

Teorema A.2.2 *Sia $F/\mathbb{F}_{q^m}$ un campo di funzioni di genere $g(F)$. Sia $f \in F$ un elemento non-degenere di Artin-Schreier e sia y uno zero di $T^q - T - f$. Si supponga che esista un posto R di F tale che $m_R > 0$. Allora il campo completo delle costanti di $E := F(y)$ è $\mathbb{F}_{q^m}$ ed il genere di E soddisfa*

$$g(E) = qg(F) + \frac{q-1}{2}\big(-2 + \sum_{P \in \mathbf{P}_F}(m_P + 1)\deg(P)\big)\ .$$

A.3 Norma e traccia

Sia E/F estensione finita di grado n. Ad ogni elemento $\alpha \in E$ è associata un'applicazione F-lineare $\mu_\alpha : E \to E$ definita come $\mu_\alpha(z) := \alpha z$, $z \in E$.
La **norma** di α rispetto all'estensione E/F è definita come:

$$\mathrm{N}_{E/F}(\alpha) := \det(\mu_\alpha).$$

La **traccia** di α rispetto all'estensione E/F è definita come:

$$\mathrm{Tr}_{E/F}(\alpha) := \mathrm{trac}(\mu_\alpha).$$

In dettaglio, se $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ è una base di E/F e

$$\alpha\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j \ \text{ con } \ a_{ij} \in F$$

allora

$$\mathrm{N}_{E/F}(\alpha) = \det\left((a_{ij})_{1\le i,j\le n}\right) \quad \text{e} \quad \mathrm{Tr}_{E/F}(\alpha) = \sum_{i=1}^{n} a_{ii}.$$

Vediamo alcune loro proprietà:

(i) Per α,$\beta \in E$, $a \in F$ ed $n = [E : F]$ valgono le relazioni per la norma:

  (a) $\mathrm{N}_{E/F}(\alpha\beta) = \mathrm{N}_{E/F}(\alpha)\mathrm{N}_{E/F}(\beta)$;
  (b) $\mathrm{N}_{E/F}(\alpha) = 0$ se e solo se $\alpha = 0$;
  (c) $\mathrm{N}_{E/F}(a) = a^n$.

  E per la traccia:

  (a) $\mathrm{Tr}_{E/F}(\alpha + \beta) = \mathrm{Tr}_{E/F}(\alpha) + \mathrm{Tr}_{E/F}(\beta)$;
  (b) $\mathrm{Tr}_{E/F}(a\alpha) = a\mathrm{Tr}_{E/F}(\alpha)$;
  (c) $\mathrm{Tr}_{E/F}(a) = na$.

  In particolare, $\mathrm{Tr}_{E/F}$ è F-lineare.

(ii) Un'estensione finita E/F è separabile se e solo se esiste un elemento $\gamma \in E$ tale che $\mathrm{Tr}_{E/F}(\gamma) \neq 0$ (i.e. $\mathrm{Tr}_{E/F}$ è suriettiva).

(iii) Se E/K ed K/F sono estensioni finite allora, per $\alpha \in E$,

$$\mathrm{N}_{E/F}(\alpha) = \mathrm{N}_{K/F}\left(\mathrm{N}_{E/K}(\alpha)\right) \quad \text{e} \quad \mathrm{Tr}_{E/F}(\alpha) = \mathrm{Tr}_{K/F}\left(\mathrm{Tr}_{E/K}(\alpha)\right).$$

(iv) Sia $f(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0 \in F[x]$ il polinomio minimo di α su F e sia $[E : F] = n = rs$ $(s = [E : F(\alpha)])$. Allora

$$\mathrm{N}_{E/F}(\alpha) = (-1)^n a_0^s \quad \text{e} \quad \mathrm{Tr}_{E/F}(\alpha) = -sa_{r-1}.$$

(v) Sia E/F separabile di grado n e considero le n distinte immersioni $\sigma_i : E \to \overline{F}$, $i = 1, 2, \ldots, n$. Allora, per $\alpha \in E$,

$$\mathrm{N}_{E/F}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad \text{e} \quad \mathrm{Tr}_{E/F}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

(vi) In particolare, se E/F è di Galois con gruppo di Galois G, allora, per $\alpha \in E$,

$$\mathrm{N}_{E/F}(\alpha) = \prod_{\sigma\in G} \sigma(\alpha) \quad \text{e} \quad \mathrm{Tr}_{E/F}(\alpha) = \sum_{\sigma\in G} \sigma(\alpha).$$

A.4 Campi finiti

Sia $p > 0$ un numero primo e $q = p^n$ una potenza di p. Esiste un campo finito $\mathbb{F}_q$ con $|\mathbb{F}_q| = q$, unico a meno di isomorfismi. Esso è il campo di spezzamento del polinomio $x^q - x$ sul campo $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
In questo modo ottengo tutti i campi finiti di caratteristica p.

Il gruppo moltiplicativo di $\mathbb{F}_q$ è un gruppo ciclico di ordine $q-1$:

$$\mathbb{F}_q = \{0, \beta, \beta^2, \ldots, \beta^{q-1} = 1\},$$

dove β è un generatore del gruppo moltiplicativo.

Per $m \in \mathbb{Z}_{\geq 1}$, $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ e l'estensione $\mathbb{F}_{q^m}/\mathbb{F}_q$ è di Galois di grado m. Inoltre il gruppo di Galois $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ è ciclico ed è generato dall'**automorfismo di Frobenius**

$$\begin{array}{rcl} \pi : \mathbb{F}_{q^m} & \to & \mathbb{F}_{q^m}. \\ \alpha & \mapsto & \alpha^q \end{array}$$

In particolare, tutti i campi finiti sono perfetti.

La norma e la traccia per l'estensione $\mathbb{F}_{q^m}/\mathbb{F}_q$ assumono le seguenti forme:

$$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha^{1+q+q^2+\cdots+q^{m-1}} \quad \text{e} \quad \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} \ ,$$

con $\alpha \in \mathbb{F}_{q^m}$.
Il teorema 90 di Hilbert dice che per ogni $\alpha \in \mathbb{F}_{q^m}$

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0 \iff \alpha = \beta^q - \beta \ , \ \beta \in \mathbb{F}_{q^m} \ .$$

A.5 Elementi di algebra commutativa

Sia R un anello commutativo con identità 1. Un **insieme moltiplicativo** di R è un sottoinsieme $\mathcal{S}$ di R tale che $1 \in \mathcal{S}$ ed $\mathcal{S}$ è chiuso rispetto alla moltiplicazione. La relazione

$$(a, s) \sim (b, t) \quad \overset{\text{def}}{\iff} \quad (at - bs)u = 0 \text{ per qualche } u \in \mathcal{S}$$

su $R \times \mathcal{S}$ è una relazione di equivalenza. Denoto con $\mathcal{S}^{-1}R$ l'insieme di queste classi di equivalenza. Nel caso particolare in cui $\mathcal{S} = R \setminus \mathfrak{p}$, dove $\mathfrak{p}$ è un ideale primo di R (i.e. $xy \in \mathfrak{p}$ allora x o y sta in $\mathfrak{p}$), scrivo $R_\mathfrak{p}$ in luogo di $\mathcal{S}^{-1}R$. Si verifica che $R_\mathfrak{p}$ ha un unico ideale massimale (formato dagli elementi r/s, $r \in \mathfrak{p}$ e $s \in \mathcal{S}$), i.e. è un **anello locale**. Il procedimento di passaggio da R ad $R_\mathfrak{p}$ prende il nome di **localizzazione** in $\mathfrak{p}$.

Sia T un anello commutativo con identità ed R un sottoanello di T. Un elemento x di T si dice **intero** su R se x è uno zero di un polinomio monico a coefficenti in R.

L'insieme S degli elementi di T che sono interi su R è un sottoanello di T che contiene R, chiamato **chiusura intera** di R. Se $S = R$ allora R è detto **integralmente chiuso** in T.

Un **anello noetheriano** R è un anello in cui ogni ideale è finitamente generato.

Una **catena** di ideali primi di R è una successione finita strettamente crescente di ideali primi $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$. La **lunghezza** di una catena è il numero di inclusioni presenti nella catena. Si definisce la **dimensione di Krull** di R come l'estremo superiore delle lunghezze di tutte le catene di ideali primi in R; essa è un intero non negativo oppure $+\infty$ (per esempio un campo ha dimensione 0 e $\mathbb{Z}$ ha dimensione 1).

Un **dominio di Dedekind** è un dominio noetheriano integralmente chiuso di dimensione 1.
I domini di Dedekind godono della seguente proprietà: ogni ideale non nullo si fattorizza in maniera unica come prodotto di ideali primi.

Appendice B

Varietà algebriche

In questa appendice descrivo gli oggetti base utilizzati nello studio delle curve algebriche. Per un'esposizione completa di dimostrazioni si rimanda il lettore alla bibliografia (si veda [Har] e [Sil]).
Per semplicità considero il caso di un campo finito $\mathbb{F}_q$ di ordine q. Sia $\overline{\mathbb{F}}_q$ una fissata chiusura algebrica di $\mathbb{F}_q$ e $G = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

B.1 Varietà affini

Sia n un intero positivo. Lo **spazio affine n-dimensionale** su $\mathbb{F}_q$ è l'insieme delle n-uple

$$\mathbb{A}^n = \mathbb{A}^n(\overline{\mathbb{F}}_q) := \{P = (x_1, x_2, \ldots, x_n) \mid x_i \in \overline{\mathbb{F}}_q\}.$$

Per un fissato intero m, si definisce l'**insieme dei punti $\mathbb{F}_{q^m}$-razionali** (o l'**insieme dei punti razionali su $\mathbb{F}_{q^m}$**) come

$$\mathbb{A}^n(\mathbb{F}_{q^m}) = \{P = (x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{F}_{q^m}\}.$$

Un elemento $P = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n$ è detto **punto** ed ogni a_i è chiamato **coordinata** di P. Un punto $P \in \mathbb{A}^n(\mathbb{F}_{q^m})$ è chiamato **punto $\mathbb{F}_{q^m}$-razionale** (o **punto razionale su $\mathbb{F}_{q^m}$**). Chiamerò P **punto razionale** se è $\mathbb{F}_q$-razionale. È chiaro che il numero dei punti $\mathbb{F}_{q^m}$-razionali di $\mathbb{A}^n$ è q^{mn}.
Definisco l'azione di Galois di G su $\mathbb{A}^n$ con

$$\sigma(P) = \big(\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)\big)$$

per ogni $\sigma \in G$ e $P = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n$. È chiaro che dati due qualsiasi automorfismi $\sigma, \tau \in G$ si ha che $(\sigma\tau)(P) = \sigma(\tau(P))$. In particolare posso definire l'azione di Frobenius come

$$\pi(a_1, a_2, \ldots, a_n) = (a_1^q, a_2^q, \ldots, a_n^q)\ .$$

Quindi posso caratterizzare i punti razionali nel seguente modo:

$$\mathbb{A}^n(\mathbb{F}_q) = \{P \in \mathbb{A}^n \mid \sigma(P) = P \text{ per ogni } \sigma \in G\} = \{P \in \mathbb{A}^n \mid \pi(P) = P\}\ .$$

Per un fissato punto $P \in \mathbb{A}^n$ chiamo la G-orbita

$$\{\sigma(P) \mid \sigma \in G\}$$

la $\mathbb{F}_q$**-orbita** di P. Due punti in una $\mathbb{F}_q$-orbita sono chiamati $\mathbb{F}_q$**-coniugati**.
Sia *pcl* una $\mathbb{F}_q$-orbita di $P = (a_1, a_2, \ldots, a_n)$. Allora

$$\mathcal{P} = \{\sigma(P) \mid \sigma \in G\} = \left\{\sigma(P) \mid \sigma \in \mathrm{Gal}\big(\mathbb{F}_q(a_1, a_2, \ldots, a_n)/\mathbb{F}_q\big)\right\} .$$

La cardinalità di $\mathcal{P}$ è chiamata **grado** di $\mathcal{P}$ e la si denota con $\deg(\mathcal{P})$. Essa coincide con il grado dell'estensione $\mathbb{F}_q(a_1, a_2, \ldots, a_n)/\mathbb{F}_q$. Da osservare che una $\mathbb{F}_q$-orbita di grado m si separa in m punti $\mathbb{F}_{q^r}$-razionali se e solo se m divide r.
Siano $\mathbb{F}_q[X] := \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ ed $\overline{\mathbb{F}}_q[X] := \overline{\mathbb{F}}_q[x_1, x_2, \ldots, x_n]$ gli anelli dei polinomi in n variabili su $\mathbb{F}_q$ ed $\overline{\mathbb{F}}_q$ rispettivamente. Per ogni polinomio $f(X) \in \overline{\mathbb{F}}_q[X]$ denoto l'insieme degli zeri di $f(X)$ con

$$V(f) = \{P \in \mathbb{A}^n \mid f(P) = 0\} .$$

In generale, dato un sottoinsieme S di $\overline{\mathbb{F}}_q[X]$, si definisce l'**insieme degli zeri** $V(S)$ di S l'insieme degli zeri comuni di tutti i polinomi in S, i.e.

$$V(S) = \{P \in \mathbb{A}^n \mid f(P) = 0 \text{ per ogni } f \in S\} .$$

Definizione B.1.1 Un **insieme algebrico affine** è un qualsiasi insieme della forma $V(S)$ per qualche sottoinsieme S di $\overline{\mathbb{F}}_q[X]$.
L'insieme $V(S)$ è detto essere **definito su** $\mathbb{F}_q$ se S è un sottoinsieme di $\mathbb{F}_q[X]$.

Denoto con $V/\mathbb{F}_q$ un insieme algebrico affine V definito su $\mathbb{F}_q$. L'insieme dei punti razionali di $V/\mathbb{F}_q$ è

$$V(\mathbb{F}_q) = V \cap \mathbb{A}^n(\mathbb{F}_q) ,$$

i.e. un punto $P \in V$ è razionale se e solo se $\pi(P) = P$.

Sia $J = (j_1, j_2, \ldots, j_n)$ una n-upla di interi non negativi. Scrivo X^J in luogo di $x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$. Per un polinomio $f(X) = \sum c_J X^J \in \overline{\mathbb{F}}_q[X]$ ed un automorfismo $\sigma \in G$ definisco l'azione $\sigma(f(X)) = \sum \sigma(c_J) X^J$. Allora $f(X) \in \mathbb{F}_q[X]$ se e solo se $\sigma(f) = f$ per ogni $\sigma \in G$. Questo equivale a dire che $\pi(f) = f$.

Per un punto $P \in \mathbb{A}^n$, un polinomio $f(X) \in \overline{\mathbb{F}}_q[X]$ ed un automorfismo $\sigma \in G$ si ha che

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

Quindi un punto $\mathbb{F}_q$-chiuso $\mathcal{P}$ è un sottoinsieme di $V/\mathbb{F}_q$ così come un punto in $\mathcal{P}$ appartiene a V. Dunque ha senso parlare di $\mathbb{F}_q$**-orbita** di un insieme algebrico affine definito su $\mathbb{F}_q$.

Per un insieme algebrico affine $V/\mathbb{F}_q$ pongo

$$\mathfrak{I}(V) = \{f \in \overline{\mathbb{F}}_q[X] \mid f(P) = 0 \text{ per ogni } P \in V\}$$

e

$$\mathfrak{I}(V/\mathbb{F}_q) = \mathfrak{I}(V) \cap \mathbb{F}_q[X] = \{f \in \mathbb{F}_q[X] \mid f(P) = 0 \text{ per ogni } P \in V\} .$$

È facile vedere che $\mathfrak{I}(V)$ ed $\mathfrak{I}(V/\mathbb{F}_q)$ sono ideali di $\overline{\mathbb{F}}_q[X]$ ed $\mathbb{F}_q[X]$ rispettivamente.
Un insieme algebrico affine è chiamato **riducibile** se esistono due sottoinsiemi algebrici

affini V_1, V_2 propri di V tali che $V = V_1 \cap V_2$. Se V è non vuoto e non è riducibile si dice che V è **irriducibile**. Un insieme algebrico affine V è irriducibile se e solo se $\mathfrak{I}(V)$ è un ideale primo di $\overline{\mathbb{F}}_q[X]$. Per un insieme algebrico affine $V/\mathbb{F}_q$ si dice anche che $V/\mathbb{F}_q$ è **assolutamente irriducibile** se V è irriducibile.

Definizione B.1.2 Un insieme algebrico affine $V/\mathbb{F}_q$ è chiamato **varietà affine** se V è irriducibile.

Definizione B.1.3 Sia $V/\mathbb{F}_q$ una varietà affine. L'**anello delle coordinate** di $V/\mathbb{F}_q$ è definito come

$$\mathbb{F}_q[V] := \mathbb{F}_q[X]/\mathfrak{I}(V/\mathbb{F}_q) \ .$$

Poiché $\mathfrak{I}(V/\mathbb{F}_q)$ è un ideale primo, $\mathbb{F}_q[V]$ è un dominio d'integrità. Il suo campo delle frazioni è chiamato **campo di funzioni** di V ed è denotato con $\mathbb{F}_q(V)$. Analogamente si definisce l'**anello delle coordinate assoluto** $\overline{\mathbb{F}}_q(V)$ di V, che è il campo delle frazioni di $\overline{\mathbb{F}}_q[V]$.

Se $V/\mathbb{F}_q$ è una varietà affine assolutamente irriducibile allora per due qualsiasi polinomi $a, b \in \overline{\mathbb{F}}_q[X]$ con $a-b \in \mathfrak{I}(V)$ ed un qualsiasi automorfismo $\sigma \in G$ ho che $\sigma(a)(P) = \sigma(b)(P)$ per ogni $P \in V$. Quindi posso definire l'azione di Galois di G su $\overline{\mathbb{F}}_q[V]$, V varietà affine. Inoltre è possibile estendere l'azione di Galois al campo delle frazioni $\overline{\mathbb{F}}_q(V)$ ponendo $\sigma(f/g) = \sigma(f)/\sigma(g)$, $f, g \in \overline{\mathbb{F}}_q[V]$.
Dati due polinomi $f, g \in \mathbb{F}_q[X]$, ho che $f - g \in \mathfrak{I}(V)$ se e solo se $f - g \in \mathfrak{I}(V/\mathbb{F}_q)$. Quindi $\mathbb{F}_q[V]$ si immerge in maniera naturale in $\overline{\mathbb{F}}_q[V]$ e dunque $\mathbb{F}_q(V)$ è un sottocampo di $\overline{\mathbb{F}}_q(V)$. Inoltre ho che

$$\begin{aligned} \overline{\mathbb{F}}_q[V] &= \overline{\mathbb{F}}_q \cdot \mathbb{F}_q[V] \ , \\ \overline{\mathbb{F}}_q(V) &= \overline{\mathbb{F}}_q \cdot \mathbb{F}_q(V) \ , \end{aligned}$$

e

$$\begin{aligned} \mathbb{F}_q[V] &= \{f \in \overline{\mathbb{F}}_q[V] \mid \sigma(f) = f \text{ per ogni } \sigma \in G\} \ , \\ \mathbb{F}_q(V) &= \{h \in \overline{\mathbb{F}}_q(V) \mid \sigma(h) = h \text{ per ogni } \sigma \in G\} \ . \end{aligned}$$

Il campo $\mathbb{F}_q$ è il campo completo delle costanti del campo di funzioni $\mathbb{F}_q(V)$.

Sia $V/\mathbb{F}_q$ una varietà affine e $P \in V$. L'**anello locale** di V per P è definito come

$$\overline{\mathbb{F}}_q[V]_P := \{h \in \overline{\mathbb{F}}_q(V) \mid h(P) = f(P)/g(P) \ , \ f, g \in \overline{\mathbb{F}}_q[V] \text{ e} g(P) \neq 0\} \ .$$

Una funzione in $\overline{\mathbb{F}}_q[V]_P$ è chiamata **funzione regolare** (o **definita**) in P. Il suo ideale massimale è

$$\overline{\mathfrak{M}}_P = \overline{\mathfrak{M}}_P := \{h \in \overline{\mathbb{F}}_q[V]_P \mid h(P) = 0\} \ .$$

Se P è un posto razionale di V allora l'**anello locale** di $V/\mathbb{F}_q$ per P è

$$\mathbb{F}_q[V]_P := \{h \in \mathbb{F}_q(V) \mid h(P) \text{ è ben definita } \} = \overline{\mathbb{F}}_q[V]_P \cap \mathbb{F}_q(V)$$

ed il suo ideale massimale è

$$\mathfrak{M}_P = \mathfrak{M}_P := \{h \in \mathbb{F}_q[V]_P \mid h(P) = 0\} = \overline{\mathfrak{M}}_P \cap \mathbb{F}_q(V) \ .$$

Definizione B.1.4 La **dimensione** della varietà affine $V/\mathbb{F}_q$ è definita essere il grado di trascendenza di $\overline{\mathbb{F}}_q(V)$ su $\overline{\mathbb{F}}_q$. È denotata con $\dim(V)$.

Definizione B.1.5 Sia $V/\mathbb{F}_q \subseteq \mathbb{A}^n$ una varietà affine ed $f_1, f_2, \ldots, f_m \in \mathbb{F}_q[X]$ un insieme di generatori di $\mathfrak{I}(V)$. Allora si dice che V è **liscia** (o **non-singolare**) in P se la matrice $m \times n$

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

ha rango $n - \dim(V)$. Se V è liscia in ogni suo punto allora si dice che V è **liscia** (o **non-singolare**).

B.2 Varietà proiettive

Sia n un intero positivo. Lo **spazio proiettivo n-dimensinale** su $\mathbb{F}_q$, denotato con $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ o $\mathbb{P}^n$, è l'insieme delle classi di equivalenza delle $(n+1)$-uple non nulle $(a_0, a_1, \ldots, a_n)$ di elementi di $\overline{\mathbb{F}}_q$ sotto la seguente relazione di equivalenza:

$$(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n)$$

se esiste un elemento non nullo λ di $\overline{\mathbb{F}}_q$ tale che $a_i = \lambda b_i$ per ogni $0 \le i \le n$.
Un elemento di $\mathbb{P}^n$ è chiamato **punto**. Denoto la classe di equivalenza contenente la $(n+1)$-upla $(a_0, a_1, \ldots, a_n)$ con $[a_0, a_1, \ldots, a_n]$. Per un punto $P = [a_0, a_1, \ldots, a_n]$ ogni a_i è chiamato **coordinata omogenea** per P.
Un punto dell'insieme

$$\mathbb{P}^n(\mathbb{F}_{q^m}) := \big\{[a_0, a_1, \ldots, a_n] \in \mathbb{P}^n \mid a_i \in \mathbb{F}_{q^m} \text{ per } 0 \le i \le n\big\}$$

è chiamato **punto $\mathbb{F}_{q^m}$-razionale** (o **punto razionale su $\mathbb{F}_{q^m}$**). Un punto $\mathbb{F}_q$-razionale è chiamato **punto razionale**. Il numero dei punti razionali in $\mathbb{P}^n$ è $(q^{n+1}-1)/(q-1)$.
Considero l'azione di Galois di G su $\mathbb{P}^n$ data da

$$\sigma\big([a_0, a_1, \ldots, a_n]\big) = \big[\sigma(a_0), \sigma(a_1), \ldots, \sigma(a_n)\big]$$

per ogni $\sigma \in G$ e $[a_0, a_1, \ldots, a_n] \in \mathbb{P}^n$. Poiché

$$\sigma\big([\lambda a_0, \lambda a_1, \ldots, \lambda a_n]\big) = \big[\sigma(\lambda)\sigma(a_0), \sigma(\lambda)\sigma(a_1), \ldots, \sigma(\lambda)\sigma(a_n)\big]\ ,$$

l'azione precedente è ben definita. In particolare definisco l'azione di Frobenius come

$$\pi\big([a_0, a_1, \ldots, a_n]\big) = [a_0^q, a_1^q, \ldots, a_n^q]\ .$$

Usando l'azione di Galois precedente, posso caratterizzare i punti razionali nel seguente modo:

$$\mathbb{P}^n(\mathbb{F}_q) = \{P \in \mathbb{P}^n \mid \sigma(P) = P \text{ per ogni } \sigma \in G\} = \{P \in \mathbb{P}^n \mid \pi(P) = P\}\ .$$

Per un fissato punto $P \in \mathbb{P}^n$ chiamo la G-orbita di P

$$\{\sigma(P) \mid \sigma \in G\}$$

la **$\mathbb{F}_q$-orbita** di P. Due punti in una $\mathbb{F}_q$-orbita sono chiamati **$\mathbb{F}_q$-coniugati**.
Sia $\mathcal{P}$ una $\mathbb{F}_q$-orbita di $P = [a_0, a_1, \ldots, a_n]$ con $a_i \neq 0$. Allora

$$\mathcal{P} = \{\sigma(P) \mid \sigma \in G\} = \big\{\sigma(P) \mid \sigma \in \mathrm{Gal}\big(\mathbb{F}_q(a_0/a_i, a_1/a_i, \ldots, a_n/a_i)/\mathbb{F}_q\big)\big\}\ .$$

La cardinalità di $\mathcal{P}$ è chiamata **grado** di $\mathcal{P}$ ed è denotata con $\deg(\mathcal{P})$. Il grado di $\mathcal{P}$ coincide con il grado dell'estensione $\mathbb{F}_q(a_0/a_i, a_1/a_i, \ldots, a_n/a_i)/\mathbb{F}_q$.
Una $\mathbb{F}_q$-orbita di grado m si separa in m punti $\mathbb{F}_{q^r}$-razionali se e solo se m divide r.

Considero la seguente applicazione per ogni $i = 1, 2, \ldots, n+1$:

$$\phi_i : \mathbb{A}^n \to \mathbb{P}^n \quad , \quad (a_1, a_2, \ldots, a_n) \mapsto [a_1, a_2, \ldots, a_{i-1}, 1, a_i, \ldots, a_n] \; . \tag{B.1}$$

Allora ϕ_i è iniettiva, i.e. $\mathbb{A}^n$ si immerge in $\mathbb{P}^n$. Questo significa che ϕ_i induce un'applicazione biettiva tra le $\mathbb{F}_q$-orbite di $\mathbb{A}^n$ con quelli di $\mathbb{P}^n$ che hanno la i-esima coordinata omogenea diversa da zero. Inoltre il grado di una $\mathbb{F}_q$-orbita $\mathcal{P}$ di $\mathbb{A}^n$ è uguale al grado di $\phi_i(\mathcal{P})$.

Un polinomio $f \in \overline{\mathbb{F}}_q[X] = \overline{\mathbb{F}}_q[x_0, x_1, \ldots, x_n]$ è chiamato **polinomio omogeneo** di grado d se per ogni $\lambda \in \overline{\mathbb{F}}_q$ si ha

$$f(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_0, x_1, \ldots, x_n) \; .$$

Un ideale di $\overline{\mathbb{F}}_q[X]$ è detto **ideale omogeneo** se è generato da polinomi omogenei.

Definizione B.2.1 Un **insieme algebrico proiettivo** è un insieme V della forma

$$Z(\mathfrak{I}) = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ per ogni polinomio omogeneo } f \in \mathfrak{I}\}$$

per qualche ideale omogeneo $\mathfrak{I}$ di $\overline{\mathbb{F}}_q[X]$. Un insieme V è detto essere **definito su** $\mathbb{F}_q$ se $\mathfrak{I}$ è generato da polinomi omogenei di $\mathbb{F}_q[X]$.

Denoto con $V/\mathbb{F}_q$ un insieme algebrico proiettivo V definito su $\mathbb{F}_q$.
L'insieme dei punti razionali di un insieme algebrico proiettivo $V = Z(\mathfrak{I})$ su $\mathbb{F}_q$ è

$$V(\mathbb{F}_q) = V \cap \mathbb{P}^n(\mathbb{F}_q) \; ,$$

i.e. un punto $P \in V$ è razionale se e solo se $\pi(P) = P$.
Per un punto $P \in \mathbb{P}^n$, un polinomio omogeneo $f(X) \in \overline{\mathbb{F}}_q[X]$ ed un automorfismo $\sigma \in G$ ho che

$$\sigma(f(P)) = \sigma(f)(\sigma(P)) \; ,$$

quindi anche per gli insiemi algebrici proiettivi ha senso parlare di $\mathbb{F}_q$**-orbita**.

Per un insieme algebrico proiettivo $V/\mathbb{F}_q$ indico con $\mathfrak{I}(V)$ l'ideale di $\overline{\mathbb{F}}_q[X]$ generato dall'insieme

$$\{P \in \overline{\mathbb{F}}_q[X] \mid f \text{ è un polinomio omogeneo e } f(P) = 0 \text{ per ogni } P \in V\} \; .$$

Definisco l'**anello delle coordinate omogenee** di V come $\overline{\mathbb{F}}_q[X](V) := \overline{\mathbb{F}}_q[X]/\mathfrak{I}(V)$.

Un insieme algebrico proiettivo è chiamato **riducibile** se esistono due insiemi algebrici proiettivi V_1 e V_2 propri di V tali che $V = V_1 \cup V_2$. Se V è non vuoto e non è riducibile si dice che V è **irriducibile**. Un insieme algebrico proiettivo V è irriducibile se e solo se $\mathfrak{I}(V)$ è un ideale primo di $\overline{\mathbb{F}}_q[X]$. Si dice che un insieme algebrico proiettivo $V/\mathbb{F}_q$ è **assolutamente irriducibile** se V è irriducibile.

Definizione B.2.2 Un insieme algebrico proiettivo $V/\mathbb{F}_q$ è chiamato **varietà proiettiva** se V è irriducibile.

Lemma B.2.3 *Sia ϕ_i definita come in* (B.1) *e si ponga $U_i = \phi_i(\mathbb{A}^n)$. Se V è una varietà proiettiva, allora $\phi_i^{-1}(V \cap U_i)$ o è vuoto od è una varietà affine, per ogni $1 \leq i \leq n+1$. Inoltre esiste un j, $1 \leq j \leq n+1$, tale che $\phi_j^{-1}(V \cap U_j) \neq \varnothing$.*

Definizione B.2.4 Sia $V/\mathbb{F}_q$ una varietà proiettiva e si scelga un i tale che si abbia $\phi_i^{-1}(V \cap U_i) \neq \varnothing$. La **dimensione** di V è definita essere la dimensione di $\phi_i^{-1}(V \cap U_i)$ ed è denotata con $\dim(V)$.
Il **campo di funzioni** $\mathbb{F}_q(V)$ è il campo di funzioni $\mathbb{F}_q\big(\phi_i^{-1}(V \cap U_i)\big)$ ed il **campo di funzioni assoluto** $\overline{\mathbb{F}}_q(V)$ di V è il campo di funzioni assoluto $\overline{\mathbb{F}}_q\big(\phi_i^{-1}(V \cap U_i)\big)$.

Sia $V/\mathbb{F}_q$ una varietà proiettiva. Allora $\mathbb{F}_q$ è il campo completo delle costanti di $\mathbb{F}_q(V)$. La definizione di **anello locale** di $V/\mathbb{F}_q$ è analoga a quella del caso delle varietà affini.

Definizione B.2.5 Sia $V/\mathbb{F}_q \subseteq \mathbb{P}^n$ una varietà proiettiva e $P = [a_0, a_1, \ldots, a_n] \in V$. Allora si dice che V è **liscia** (o **non-singolare**) in P se $\phi_i^{-1}(V \cap U_i)$ è liscia in $(a_0/a_i, a_1/a_i, \ldots, a_{i-1}/a_i, a_{i+1}/a_i, \ldots, a_n/a_i)$. Se V è liscia in ogni suo punto allora si dice che V è **liscia** (o **non-singolare**).

B.3 Applicazioni fra varietà

Definizione B.3.1 Siano $V_1, V_2 \subseteq \mathbb{P}^n$ due varietà proiettive. Un'**applicazione razionale** di V_1 a V_2 è un'applicazione della forma

$$\phi : V_1 \to V_2 \quad , \quad \phi = [f_0, f_1, \ldots, f_n]$$

dove $f_0, f_1, \ldots, f_n \in \overline{\mathbb{F}}_q(V_1)$ hanno la proprietà che per ogni punto $P \in V_1$ per il quale $f_0, f_1, \ldots, f_n$ sono tutte definite,

$$\phi(P) = \big[f_0(P), f_1(P), \ldots, f_n(P)\big] \in V_2 \ .$$

Se V_1 e V_2 sono definite su $\mathbb{F}_q$ allora G agisce su ϕ nella maniera naturale:

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

per ogni $\sigma \in G$ e per ogni $P \in V_1$.
Se per qualche $\lambda \in \overline{\mathbb{F}}_q$ non nullo si ha $\lambda f_0, \lambda f_1, \ldots, \lambda f_n \in \mathbb{F}_q(V_1)$, allora ϕ è detta essere **definita su** $\mathbb{F}_q$.

Definizione B.3.2 Un'applicazione razionale

$$\phi = [f_0, f_1, \ldots, f_n] : V_1 \to V_2$$

è detta essere **regolare** (o **definita**) in $P \in V_1$ se esiste una funzione $g \in \overline{\mathbb{F}}_q(V_1)$ tale che

(i) Per ogni $0 \leq i \leq n$, gf_i è regolare in P;

(ii) Per qualche $0 \leq i \leq n$, $(gf_i)(P) \neq 0$.

Se una tale funzione g esiste allora si pone

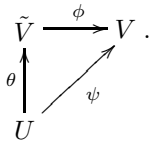
$$\phi(P) = \left[(gf_0)(P), (gf_1)(P), \ldots, (gf_n)(P)\right] .$$

Un'applicazione razionale regolare in ogni punto è chiamata **morfismo**.

Definizione B.3.3 Siano V_1 e V_2 due varietà. Si dice che V_1 e V_2 sono **isomorfe**, $V_1 \cong V_2$, se esistono due morfismi $\phi : V_1 \to V_2$ e $\psi : V_2 \to V_1$ tali che $\psi \circ \phi$ e $\phi \circ \psi$ siano l'applicazione identica su V_1 e V_2 rispettivamente. $V_1/\mathbb{F}_q$ e $V_2/\mathbb{F}_q$ si dicono **isomorfi su** $\mathbb{F}_q$ se i morfismi ϕ e ψ sono definiti su $\mathbb{F}_q$.

Definizione B.3.4 Una varietà V è chiamata **normale in un punto** P di V se $\overline{\mathbb{F}}_q[V]_P$ è un anello integralmente chiuso in $\overline{\mathbb{F}}_q[V]$. V si dice **normale** se è normale in ogni suo punto.

Se V è una varietà allora esiste una varietà normale affine $\tilde{V}$ ed un morfismo $\phi : \tilde{V} \to V$ con la proprietà che se U è una varietà normale e $\psi : U \to V$ un **morfismo dominante** (i.e. $\psi(U)$ è denso in V) allora esiste un unico morfismo $\theta : U \to \tilde{V}$ tale che $\psi = \phi \circ \theta$:



$\tilde{V}$ è chiamata la **normalizzazione** di V.

Bibliografia

[A-M] M. F. Atiyah e I. G. Macdonald, *Introduction to Commutative Algebra*, edizione italiana, Feltrinelli, Milano, 1981.

[Bue] D. A. Buell, *Binary Quadratic Forms, Classical Theory and Modern Computation*, Springer (Edwards Brothers Inc.), Michigan, 1989.

[C-F] J. W. S. Cassels e A. Fröhlich (editori), *Algebraic Number Theory*, Academic Press, Londra, 1967.

[Deu] M. Deuring, *Lectures on the Theory of Algebraic Functions of One Variable*, Lecture Notes in Math. **314**, Springer, Berlino, 1973.

[F-K] E. Freitag e R. Kiehl, *Etale Cohomology and the Weil Conjecture*, Springer, Berlino, 1988.

[F-G-T] R. Fuhrmann, A. Garcia e F. Torres, On maximal curves, *J. Number Theory* **67**, 29-51 (1997).

[Ful] W. Fulton, *Algebraic Curves, an Introduction to Algebraic Geometry*, The Benjamin/Cummings Publishing Company Inc., Massachusetts, 1968.

[G-V1] G. van der Geer e M. van der Vlugt, Artin-Schreier curves and codes, *J. Algebra* **139**, 256-272 (1991).

[G-V2] G. van der Geer e M. van der Vlugt, Reed-Muller codes and supersingolar curves, *I. Compositio Math.* **84**, 333-367 (1992).

[G-V3] G. van der Geer e M. van der Vlugt, Generalized Hamming weights of codes and curves over finite fields with many points, *Proc. Conf. on Algebraic Geometry* (Ramat Gan, 1993), Israel Math. Conf. Proc. **9**, pp. 417-432, Bar-Ilan University, Ramat Gan, 1996.

[G-V4] G. van der Geer e M. van der Vlugt, Fibre products of Artin-Schreier curves and generalized Hamming weights of codes, *J. Comb. Theory A* **70**, 337-348 (1995).

[G-V5] G. van der Geer e M. van der Vlugt, Quadratic forms, generalized Hamming weights of codes and curves over finite fields with many points, *J. Number Theory* **59**, 20-36 (1996).

[G-V6] G. van der Geer e M. van der Vlugt, Table of curves with many points (updated version 29 February 2004. Next update: August 2004).
`http://www.science.uva.nl/~geer/`

[Hanj] J. P. Hansen, Deligne Lusztig varieties and group codes, *Coding Theory and Algebraic Geometry. Proceedings, Luminy 1991* (H. Stichtenoth e M. A. Tsfasman editori), Lecture Notes in Math. **1518**, pp. 63-81, Springer, Berlino, 1992.

[Hanj-P] J. P. Hansen e J. P. Pedersen, Automorphism groups of Ree type, Deligne-Lusztig curves and function fields, *J. Reine Angew. Math.* **440**, 99-109 (1993).

[Hans] S. H. Hansen, *Rational Points on Curves over Finite Fields*, Lect. Notes Ser., Aarhus Univ. Mat. Istitute, 1995.

[Har] R. Hartshorne, *Algebraic Geometry*, Springer, New York, 1977.

[Hay] D. R. Hayes, A brief introduction to Drinfeld modules, *The Arithmetic of Function Fields* (D. Goss, D. R. Hayes e M. I. Rosen editori), pp. 1-32, W. de Gruyter, Berlino, 1992.

[H-B] B. Huppert e N. Blackburn, *Finite Groups III*, Springer, Berlino, 1982.

[Iha] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokio Sect. IA Math.* **28**, n. 3, 721-724 (1981).

[I-R] K. Ireland e M. Rosen, *A Classical Introduction to Modern Number Theory*, second edition, Springer, New York, 1993.

[Jac] N. Jacobson, *Basic Algebra I*, second edition, W. H. Freeman and Company, New York, 1996.

[Ka-R] E. Kani e M. Rosen, Idempotent relations and factors of Jacobians, *Math. Ann.* **284**, 307-327 (1989).

[K-M] M. Q. Kawakita e S. Miura, Quadratic forms, fibre products and some plane curve with many points, *Acta Arithmetica* **105**, 371-386 (2002).

[Lau] K. Lauter, Deligne-Lusztig curves as ray class fields, *Manuscripta Math.* **98**, 87-96 (1999).

[Liu] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, edizione inglese, Oxford University Press, Oxford, 2002.

[Lor] D. Lorenzini, *An Introduction to Arithmetic Geometry*, Graduate Studies in Mathemetics **9**, American Mathematical Society, Providence, 1996.

[Miu] S. Miura, Algebraic geometric codes and certain plane curves, *IEICE Trans. Fund. J75-A*, n. 11, 1735-1745 (1992).

[Mor] C. J. Moreno, *Algebraic Curves over Finite Fields*, Cambridge Tracts in Math. **97**, Cambridge University Press, Cambridge, 1991.

[N-X] H. Niederreiter & C.P. Xing, *Rational Points on Curves over Finite Fields, Theory and Applications*, London Mathematical Society **285**, Cambridge University Press, Cambridge, 2001.

[Ped] J. P. Pedersen, A function field related to the Ree group, *Coding Theory and Algebraic Geometry. Proceedings, Luminy 1991* (H. Stichtenoth e M. A. Tsfasman editori), Lecture Notes in Math. **1518**, pp. 122-131, Springer, Berlino, 1992.

[Ros1] M. Rosen, S-units and S-class group in algebraic function fields, *J. Algebra* **26**, 98-108 (1973).

[Ros2] M. Rosen, The Hilbert class field in function fields, *Exposition. Math.* **5**, 365-378 (1987).

[Sch] R. Schoof, Algebraic curves and coding theory, *UTM* **336**, Università di Trento (1990).

[Ser1] J. P. Serre, *Local Fields*, Springer, New York, 1979.

[Ser2] J. P. Serre, Nombre de points des courbes algébiques sur $\mathbb{F}_q$, *Sém. de Théorie des Nombres de Bordeaux*, esposizione **22** (1982).

[Ser3] J. P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C. R. Acad. Sci. Paris Sér. I Math.* **296**, 397-402 (1983).

[Ser4] J. P. Serre, Rational points on curves over finite fields, *Notes of Lectures at Harvard University* (1985).

[Sil] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[Sti1] H. Stichtenoth, Ueber die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, *Arch. Math.* **24**, 527-544 e 615-631 (1973).

[Sti2] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, New York, 1993.

[T-V-Z] M. A. Tsfasman, S. G. Vlăduţ e T. Zink, Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* **109**, 21-28 (1982).

[V-D] S. G. Vlăduţ e V. G. Drinfeld, Number of points of an algebraic curve, *Functional Anal. Appl.* **17**, n. 1, 53-54 (1983).

[Voi] J. Voight, Curves over finite fields with many points: an introduction.
`http://www.math.berkeley.edu/~jvoight/expository/`

[Wei] E, Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

Ringraziamenti speciali

Padova, 6 luglio 2004

È doveroso da parte mia ringraziare tutte le persone che mi sono rimaste vicine nel (lungo!) periodo dell'università.
Era mia intenzione ringraziarli e fargli sapere qui quanto sono stati importanti per me, ma ahimè il tempo è tiranno!
Ringrazio i vecchi compagni villaverlesi, che con loro ho trascorso dei momenti festivi veramente intensi.
Ringrazio molto i numerosi compagni di appartamento; grazie a loro ho imparato a pulire e fare da mangiare...
Ringrazio i matematici presenti e futuri, giovani e vecchi, con i quali ho potuto parlare veramente di matematica...e non solo.

Ringrazio con Attenzione il Rabbino, Carlo-Luigi-lo Zio-il Nonno, Hainz e Christian, Walter ed Elena...

Ringrazio Tonfolo, Scheggia e Pallino...

Ringrazio tutti quelli che hanno sopportato le mie battute...

Ringrazio Alessandra anche se non le piace il calcio...

Devo ringraziare la Signora Gabriella per avermi fatto notare che il "Moment" fa passare il mal di testa...

Ringrazio Sara.

Ciao,
Dario