Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

BASI DI CAMPI FINITI

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.ssa
MARTA MORIGI

Presentata da:
MARIA VIRGINIA BOLELLI

II Sessione
Anno Accademico 2015-2016

Introduzione

Questo elaborato si propone di approfondire lo studio dei campi finiti, in modo particolare soffermandosi sul problema dell'esistenza di una base normale per un campo finito.
La teoria dei campi finiti ha notevoli applicazioni in ambito crittografico, in particolare nei sistemi di crittografia a chiave pubblica, quali il crittosistema su curve ellittiche, introdotto da Miller e Koblitz [10, 7], e il crittosistema su curve iperellittiche, ideato da Koblitz [8]. Questi sistemi sono basati su campi finiti e loro estensioni, pertanto è di grande interesse l'ottimizzazione delle operazioni aritmetiche svolte su tali strutture. In particolare uno degli obiettivi è quello di migliorare l'operazione di inversione di un elemento del campo. Accanto all'algoritmo euclideo e alle sue generalizzazioni, l'algoritmo di Itoh e Tsujii [6] permette il calcolo dell'inverso sfruttando la rappresentazione degli elementi del campo finito utilizzando una base normale. Dunque risulta importante studiare le basi normali di campi finiti.

Nel primo capitolo si richiamano alcune nozioni di algebra, introducendo i campi finiti. In particolare, per ogni intero q che sia potenza di un primo p, esiste un unico campo finito di ordine q, denotato da $\mathbb{F}_q$.

Nel secondo capitolo si dimostrano le proprietà fondamentali dei campi finiti, introducendo alcune funzioni importanti quali Traccia e Norma, arrivando quindi a parlare di basi. In particolare si vedrà che data $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ un'estensione di campi finita, allora il numero totale di basi possibili per tale estensione è dato da

$$\prod_{i=0}^{m-1} (q^m - q^i).$$

Utilizzando la funzione traccia si introdurrà il concetto di base duale per $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$ e si dimostrerà che per ogni base di un'estensione di un campo finito esiste una sola base duale. Una base normale di un' estensione $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ è una base $\mathcal{A} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ per un certo $\alpha \in \mathbb{F}_{q^m}$. Vedremo che per ogni campo finito $\mathbb{F}_q$ e per ogni estensione finita $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ esiste sempre una

base normale di $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$; tale risultato va sotto il nome di Teorema della Base Normale.

Nel terzo capitolo vengono introdotti i polinomi linearizzati e un'operazione di moltiplicazione simbolica tra di essi, con proprietà analoghe al prodotto ordinario di polinomi. I polinomi linearizzati sono in realtà particolari applicazioni lineari e quindi sono computazionalmente più maneggevoli. Grazie a questi strumenti si giungerà ad una dimostrazione alternativa della base normale. Tale dimostrazione è in realtà una generalizzazione del teorema della base normale ai q-moduli. Inoltre si vedrà che il numero di basi normali di $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$ è dato da

$$\phi_q(x^m - 1) = q^n \prod_{j=1}^{r} (1 - q^{-n_j})$$

dove $\Phi_q(f(x)) = \Phi_q(f)$ è la funzione che conta il numero di polinomi in $\mathbb{F}_q[x]$ di grado più piccolo rispetto al grado di f e primi con f e gli n_i sono i gradi dei fattori monici e irriducibili di f su $\mathbb{F}_q[x]$.

Indice

Capitolo 1

Richiami

1.1 Campi ed Estensioni di Campi

Definizione 1.1 (Caratteristica)**.** La *caratteristica* di un campo K è definita come il più piccolo intero positivo m tale che:

$$m \cdot 1 = \overbrace{1 \cdot 1 \cdots 1}^{m \ volte} = 0$$

se un tale intero esiste, 0 altrimenti.

Definizione 1.2 (Sottocampo Fondamentale)**.** Sia K un anello. Si chiama *sottocampo fondamentale* o *campo primo* di K il più piccolo campo contenuto in esso.

Teorema 1.1.1. *Sia D un dominio. Allora la caratteristica di D è uguale a 0 oppure è uguale a p, con p primo.*

In particolare, se K è un campo di caratteristica p positiva, allora il sottoanello fondamentale è un sottocampo isomorfo a $\mathbb{Z}_p$ contenuto in un qualsiasi sottocampo di K.

Per la dimostrazione si veda [9, 1.45]

Definizione 1.3 (Estensione di Campi)**.** Sia K un campo. Diremo che F è un'*estensione* di K se K è un sottocampo di F o, più in generale, se esiste un morfismo iniettivo di campi $i : K \to F$.

Osservazione 1. Sia V un'estensione di K; V può allora essere considerato uno spazio vettoriale su K, dove la somma tra vettori (elementi di V) è la somma nel campo V, ed il prodotto tra scalari e vettori è il prodotto nel campo V, in quanto ogni elemento di K è in particolare un elemento di V.

Definizione 1.4 (Estensione Finita)**.** Sia F un'estensione di K. Se la dimensione di F su K è finita, allora F si dirà *estensione finita.*

Osservazione 2. Nel caso in cui si abbia un'estensione finita, la dimensione n di F su K si dirà grado dell'estensione e si indicherà con il simbolo $[F : K]$.

Teorema 1.1.2 (Teorema della Torre)**.** *Siano K, F, E campi tali che $K \subseteq F \subseteq E$. Si ha che $K \subseteq E$ è un'estensione finita se e solo se $F \subseteq E$ ed $K \subseteq F$ lo sono. In tal caso si ha che $[E : K] = [E : F][F : K]$.*

Per la dimostrazione si veda [3, pg 91]

Proposizione 1.1.3. *Sia K un campo finito di caratteristica p con p primo, allora per ogni $n \in \mathbb{N}$ si ha che $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ con $a, b \in K$.*

Per la dimostrazione si veda [9, 1.46]

Proposizione 1.1.4. *Sia K un campo di caratteristica p, con p primo. La funzione $\phi : K \to K$ tale che $\phi(\alpha) = \alpha^p$ è un morfismo di campi, detto Morfismo di Frobenius.*

Per la dimostrazione si veda [11, Remark 1.4 pg 9]

Teorema 1.1.5 (Lemma di Divisione per Polinomi)**.** *Siano K un campo, f e $g \in K[x]$, $g \neq 0$. Allora esistono univocamente determinati q ed $r \in K[x]$ tali che*

$$f = gq + r, \qquad \deg(r) < \deg(g).$$

I polinomi q ed r vengono detti rispettivamente il quoziente ed il resto della divisione di f per g.
Se $r=0$ diciamo che g divide f e scriviamo $g|f$.

Tale dimostrazione segue direttamente dall'algoritmo di divisione.

Definizione 1.5 (Polinomio Irriducibile)**.** Un polinomio $f(x)$, diverso dal polinomio nullo e non unità, a coefficienti in un campo K si dice *irriducibile*su K se una fattorizzazione $f(x) = g(x)h(x)$, con $g(x)$ e $h(x)$ in $K[x]$ implica che uno dei due polinomi tra $g(x)$ e $h(x)$ ha grado 0, cioè è invertibile.

1.2 Algebra Lineare

Si ricordano alcune definizioni relative ad una applicazione lineare T su uno spazio vettoriale qualsiasi.

Proposizione 1.2.1. *Sia K un campo e sia $K[x]$ l'anello dei polinomi a coefficienti in K. Allora vi è una corrispondenza biunivoca tra i $K[x]$-moduli e le coppie (V , T) dove V è un K spazio vettoriale e T una applicazione lineare da V in se stesso.*

Per la dimostrazione si veda [1, pg 434]

Definizione 1.6 (Polinomio caratteristico)**.** Sia T un'applicazione lineare che va da V in se stesso, ove V è uno spazio vettoriale su un campo K. Sia A la matrice associata a T rispetto ad una qualsiasi base dello spazio; allora si definisce *polinomio caratteristico* il polinomio $g(x) = \det(xI - A)$ dove I è la matrice identità.

Definizione 1.7 (Polinomio minimo)**.** Segue dalla Proposizione 1.2.1 che esiste una corrispondenza biunivoca tra i $K[x]$-moduli e le coppie (V , T). Allora è possibile definire un omomorfismo ϕ in tal modo:

$$\phi : K[x] \to \mathrm{Hom}(V)$$

tale che $p(x) \mapsto p(T)$ con $T \in \mathrm{Hom}(V)$. Il nucleo di tale applicazione è un ideale, in particolare tale ideale è principale in quanto gli anelli di polinomi sono domini ad ideali principali. Dunque si ha

$$\ker\phi = \{p(x) \in K[x] \text{ tali che } p(T) = 0\} = (m(x)).$$

Se $m(x)$ è l'unico generatore monico di $\ker\phi$ allora tale polinomio viene chiamato *polinomio minimo* di T su V.

Osservazione 3. Avendo definito il polinomio minimo associato ad una applicazione lineare T su uno spazio vettoriale V possiamo anche parlare di *annullatore* di T. In particolare si osserva che se $f(x) \in \ker\phi$ allora si ha che $f(T) = 0$. In tal caso diciamo che f è un annullatore per T.

Osservazione 4. Il polinomio minimo di un'applicazione lineare T divide il polinomio caratteristico della stessa applicazione.

Dimostrazione. Sia $g(x) = \det(xI - A)$ polinomio caratteristico di T su V, ove V è uno spazio vettoriale su un campo K, T è un' applicazione lineare da V in se stesso e sia A la matrice associata a T rispetto ad una qualsiasi base di V.

Ora, valutando tutto in A, si ottiene che $g(A) = \det(A - A) = \det(0I) = 0$, da cui $g(A) = 0$ e questo accade se e solo se $g(x) \in \ker\phi$ dove ϕ è

l'omomorfismo che compare nella Definizione 1.7. Si è visto che kerϕ = $(m(x))$ e dunque si ha che $m(x)$, il polinomio minimo di T su V, divide $g(x)$. □

Definizione 1.8 (Vettore ciclico)**.** Sia $T : V \to V$ un'applicazione lineare su V, spazio vettoriale su un campo K. Allora $v \in V$si dice *vettore ciclico* per T se span$\{v, T(v), \ldots, T^k(v)\} = V$ con $k \geq 0$, ovvero se i vettori $\{v, T(v), \ldots, T^k(v)\}$ generano V. In altre parole $v \in V$ è un vettore ciclico per T se V è un $K[T]$-modulo ciclico generato da v.

Teorema 1.2.2. *Sia V un modulo finitamente generato su un dominio euclideo R. Allora V è una somma diretta di moduli ciclici C_j e di un modulo libero R. Più precisamente esiste un isomorfismo*

$$\phi : V \longrightarrow R/(d_1) \times \ldots \times R/(d_k) \times R^r$$

dove r è un intero non negativo, gli elementi $d_1, \ldots, d_k$ sono diversi da zero e non invertibili. Esiste una decomposizione in cui

1. *d_i divide d_{i+1} per $i = 1, \ldots, k-1$,*
2. *d_i è la potenza di un elemento primo di R, cioè per $i = 1, \ldots, k-1$ esistono p_i primo in R ed e_i intero positivo tali che $d_i = p_i^{e_i}$.*

Per la dimostrazione si veda [1, pg 560]

Lemma 1.2.3. *Sia T un'applicazione lineare su uno spazio vettoriale V di dimensione finita. Allora T ha un vettore ciclico se e solo se il polinomio caratteristico e il polinomio minimo di T sono identici.*

Dimostrazione. Segue dalla Proposizione 1.2.1 che esiste una corrispondenza biunivoca tra i $K[x]$-moduli e le coppie (V , T), dove T è un'applicazione lineare da V in se stesso. E' possibile applicare il Teorema 1.2.2 a V:

$$V = V_1 \oplus \ldots \oplus V_k \tag{1.1}$$

dove dim$V_i = m_i$ e dim$V = m = m_1 + \ldots + m_k$. In virtù della corrispondenza si ha anche che

$$K[x] = K[x]/(d_1) \oplus \ldots \oplus K[x]/(d_k)$$

dove $d_i \in K[x]$, deg(d_i)=m_i e $d_1 | \ldots | d_k$. In particolare si ha che il polinomio minimo di T su V è d_k, mentre il polinomio caratteristico $g(x)$ ha grado pari ad m ed è monico. Ora, sia V un modulo ciclico; segue dalla (1.1)

che $V = V_1$ ma in realtà possiamo considerare $V_1 = K[x]/(d_1)$ e quindi, $\deg(d_1) = m = \dim V$ quindi il polinomio minimo ha grado uguale al polinomio caratteristico e, dato che il polinomio caratteristico divide il polinomio minimo per l'Osservazione 4, si ha che i due polinomi coincidono.

Viceversa, se i due polinomi coincidono, si ha che $\deg(f)=\deg(g) = m$. Dunque $V = K[x]/(f)$ dove f è un polinomio di grado m ed in particolare è il polinomio minimo. Quindi V è un modulo ciclico ed in particolare ha un vettore ciclico. □

1.3 Introduzione ai campi finiti

Lemma 1.3.1. *Sia F un campo finito con q elementi e sia F contenuto in K, dove K è anch'esso un campo finito. Allora K ha q^n elementi con $n = [K : F]$.*

Dimostrazione. Essendo K finito, in particolare è uno spazio vettoriale di dimensione finita su F. Sia $n = [K : F]$; allora K ha una base di n elementi su F. Sia $\{v_1, \ldots, v_n\}$ tale base, ogni elemento di K ha una rappresentazione unica nella forma $\alpha_1 v_1 + \ldots + \alpha_n v_n$ con $\alpha_1, \ldots, \alpha_n \in F$. Pertanto il numero degli elementi di K è uguale al numero degli $\alpha_1 v_1 + \ldots + \alpha_n v_n$ al variare di $\alpha_1, \ldots, \alpha_n \in F$; siccome ogni coefficiente può avere q valori, K deve chiaramente avere q^n elementi. □

Teorema 1.3.2. *Supponiamo che E sia un campo finito di caratteristica p, allora E contiene esattamente p^n elementi per qualche intero positivo n.*

Dimostrazione. Supponiamo che sia $\mathbb{F}_p$ il sottocampo primo di E . Applicando il Lemma 1.3.1, con $\mathbb{F}_p = F$ ed $E = K$, notiamo che ci sono soltanto p possibili scelte per ogni coordinata α_i, quindi il numero totale di elementi in E è

$$\overbrace{p \cdots p}^{n \ volte} = p^n.$$

□

Teorema 1.3.3. *Se un campo finito F ha q elementi, ogni elemento $a \in F$ verifica $a^q = a$.*

Per la dimostrazione si veda [9, 2.3]

Lemma 1.3.4. *Sia K un sottocampo di F, dove F è un campo con q elementi. Allora il polinomio $x^q - x \in K[x]$ si fattorizza in $F[x]$ come*

$$x^q - x = \prod_{a \in F} (x - a)$$

e F è il campo di spezzamento di $x^q - x$ su K.

Dimostrazione. Il grado di $x^q - x$ è uguale a q, in particolare si ha che tale polinomio ha q radici in F. Segue dal Teorema 1.3.3 che $a^q = a$ dunque $a \in F$. Perciò ogni elemento di F è radice del polinomio considerato, quindi:

$$x^q - x = \prod_{a \in F} (x - a)$$

e in particolare F è il suo campo di spezzamento su K. □

Teorema 1.3.5. *Sia p un numero primo e sia $n \in \mathbb{N}$. Allora esiste un campo $\mathbb{F}_{p^n}$ con p^n elementi e tale campo è unico a meno di isomorfismi. Precisamente, $\mathbb{F}_{p^n}$ è il campo di spezzamento del polinomio $x^{p^n} - x$ su $\mathbb{Z}_p$.*

Per la dimostrazione si veda [9, 2.5]

Teorema 1.3.6 (Criterio del Sottocampo)**.** *Sia $\mathbb{F}_q$ il campo finito con $q = p^n$ elementi. Allora ogni sottocampo di $\mathbb{F}_q$ ha ordine p^m, con $m|n$. Viceversa, se $m|n$, allora esiste esattamente un sottocampo di $\mathbb{F}_q$ con p^m elementi.*

Dimostrazione. Innanzitutto supponiamo che $\mathbb{F}_s$ sia un sottocampo di $\mathbb{F}_q$. Allora possiamo considerare le estensioni $\mathbb{F}_p \subseteq \mathbb{F}_s \subseteq \mathbb{F}_q$ ed applicare il Teorema 1.1.2:

$$n = [\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_q : \mathbb{F}_s][\mathbb{F}_s : \mathbb{F}_p] = mh$$

per un certo intero positivo h. Da questa relazione si ha che $m|n$ e in particolare, per il Lemma 1.3.1 , $\mathbb{F}_s$ ha ordine p^m .

Per il viceversa si noti che

$$\text{se } u \text{ divide } v \text{ allora } x^u - 1 \text{ divide } x^v - 1. \tag{1.2}$$

Infatti, se $v = uz$ allora $x^v - 1 = x^{uz} - 1 = (x^u - 1)(x^{u(z-1)} + x^{u(z-2)} + \ldots + x^u + 1)$. Quindi se $m|n$, allora $x^m - 1 | x^n - 1$ e ponendo $x = p$ si ottiene che $p^m - 1 | p^n - 1$. Utilizzando nuovamente (1.2) si ottiene che $x^{p^m-1} - 1$ divide $x^{p^n-1} - 1$ in $\mathbb{F}_p[x]$. Di conseguenza, $x^{p^m} - x$ divide $x^{p^n} - x = x^q - x$ in $\mathbb{F}_p[x]$. Così, ogni radice di $x^{p^m} - x$ è una radice di $x^q - x$ e quindi appartiene a $\mathbb{F}_q$.

Segue che $\mathbb{F}_q$ deve contenere come sottocampo un campo di spezzamento di $x^{p^m} - x$ su $\mathbb{F}_p$ che sappiamo avere ordine p^m. Se ci fossero due sottocampi distinti di ordine p^m in $\mathbb{F}_q$, insieme conterrebbero più di p^m radici di $x^{p^m} - x$ su $\mathbb{F}_q$, un'ovvia contraddizione.

□

Lemma 1.3.7. *Sia $f \in \mathbb{F}_q[x]$ un polinomio irriducibile e sia α una radice di f in un'estensione di $\mathbb{F}_q$. Allora si ha $h(\alpha) = 0$ per un certo polinomio $h \in \mathbb{F}_q$ se e solo se f divide h.*

Dimostrazione. Sia a il coefficiente direttore di f e sia $g(x) = a^{-1}f(x)$. In tal modo g è un polinomio monico e irriducibile su $\mathbb{F}_q$ che si annulla in α, duque, per definizione, è il polinomio minimo. Il polinomio minimo di α divide tutti i polinomi che si annullano in α e, dato che quindi g divide h per un qualche $h(x) \in \mathbb{F}_q[x]$, allora anche f divide h di conseguenza. □

Capitolo 2

Struttura dei Campi Finiti

Si denoti $q = p^n$, dove p è un numero primo e $n \in \mathbb{N}$.

2.1 Elementi Primitivi

Per un campo finito $\mathbb{F}_q$, si indica con il simbolo $\mathbb{F}_q^*$ il gruppo moltiplicativo di $\mathbb{F}_q$. Enunciamo ora un risultato fondamentale che caratterizza tale gruppo.

Teorema 2.1.1. *Per ogni campo finito $\mathbb{F}_q$, il gruppo moltiplicativo $\mathbb{F}_q^*$ di $\mathbb{F}_q$ è ciclico.*

Dimostrazione. Possiamo supporre $q \geq 3$. Sia $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ la decomposizione in fattori primi dell'ordine $h = q - 1$ di $\mathbb{F}_q^*$. Per ogni i, $1 \leq i \leq m$, il polinomio $x^{h/p_i} - 1$ ha al più h/p_i radici . Dato che $h/p_i < h$ segue che vi sono elementi non nulli di $\mathbb{F}_q$ che non sono radici di tale polinomio. Sia a_i uno di questi elementi e sia $b_i = a_i^{h/p_i^{r_i}}$. Si ha che $b_i^{p_i^{r_i}} = 1$, quindi l'ordine di b_i è un divisore di $p_i^{r_i}$ ed è dunque della forma $p_i^{s_i}$ con $0 \leq s_i \leq r_i$. D'altra parte, $b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1$ e quindi l'ordine di b_i è uguale a $p_i^{r_i}$.
Sia $b = b_1 b_2 \cdots b_m$ e, mostriamo che l'ordine di b è pari ad h.
Supponiamo per assurdo che l'ordine di b sia un divisore proprio di h, allora è per forza divisore di almeno uno degli interi h/p_i . In particolare non è restrittivo supporre che divida h/p_1. Dunque,

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1}.$$

Se $2 \leq i \leq m$ allora $p_i^{r_i}$ divide h/p_1 e conseguentemente $b_i^{h/p_1} = 1$. Allora necessariamente $b_1^{h/p_1} = 1$ e quindi l'ordine di b_1 divide $h/p_1 = p_1^{r_1-1} p_2^{r_2} \cdots p_m^{r_m}$

da cui segue che l'ordine di b_1 divide $p_1^{r_1-1}$. Ma per ipotesi l'ordine di b_1 è uguale a $p_1^{r_1}$. Siamo dunque arrivati ad un assurdo, l'ordine di b è uguale ad h e b è un generatore per $\mathbb{F}_q^*$. □

Definizione 2.1 (Elemento Primitivo)**.** Un generatore del gruppo ciclico $\mathbb{F}_q^*$ viene chiamato *elemento primitivo* di $\mathbb{F}_q$.

Con questa definizione possiamo dire che il Teorema 2.1.1 afferma che ogni campo finito contiene almeno un elemento primitivo.
L'esistenza di un elemento primitivo implica che ogni estensione di campi finita può essere pensata come un'estensione semplice sul suo sottocampo fondamentale.

Teorema 2.1.2. *Siano $\mathbb{F}_q$ un campo finito e $\mathbb{F}_r$ una sua estensione finita. Allora $\mathbb{F}_r$ è un'estensione semplice di $\mathbb{F}_q$.*

Dimostrazione. Sia ξ un elemento primitivo di $\mathbb{F}_r$. Chiaramente si ha $\mathbb{F}_q(\xi) \subseteq \mathbb{F}_r$. D'altro lato, $\mathbb{F}_q(\xi)$ contiene lo 0 e tutte le potenze di ξ e quindi tutti gli elementi di $\mathbb{F}_r$, quindi $\mathbb{F}_r \subseteq \mathbb{F}_q(\xi)$. In conclusione, si ha che $\mathbb{F}_q(\xi) = \mathbb{F}_r$. □

Una conseguenza diretta è il seguente risultato di esistenza di polinomi irriducibili su campi finiti.

Corollario 2.1.3. *Per ogni campo finito $\mathbb{F}_q$ e per ogni intero positivo n, esiste un polinomio irriducibile in $\mathbb{F}_q[x]$ di grado n .*

Dimostrazione. Sia $\mathbb{F}_r$ un'estensione finita di $\mathbb{F}_q$ di ordine q^n, in modo tale che $[\mathbb{F}_r\colon \mathbb{F}_q]{=}n$. Segue dal Teorema 1.1.3 che $\mathbb{F}_q(\xi) = \mathbb{F}_r$ per un qualche ξ in $\mathbb{F}_r$. Allora il polinomio minimo di ξ su $\mathbb{F}_q$ è irriducibile e di grado n in $\mathbb{F}_q[x]$(in quanto il polinomio minimo di un elemento è irriducibile e inoltre il suo grado è pari al grado dell'estensione). □

2.2 Polinomi Irriducibili ed Automorfismi

Si considerino ora polinomi irriducibili su campi finiti, lo scopo di questo paragrafo è studiare l'insieme delle radici di tali polinomi, osservandone e determinandone alcune proprietà.

Lemma 2.2.1. *Sia $f(x) \in \mathbb{F}_q[x]$ un polinomio monico irriducibile di grado m. Allora $f(x)$ divide $x^{q^n} - x$ se e solo se m divide n.*

Dimostrazione. Supponiamo che $f(x)$ divida $x^{q^n} - x$. Sia α una radice di $f(x)$ nel suo campo di spezzamento, allora α è anche radice di $x^{q^n} - x$ per ipotesi da cui si ha che $\alpha^{q^n} = \alpha$ e, applicando il Teorema 1.3.3 segue che $\alpha \in \mathbb{F}_{q^n}$. Inoltre si ha che $\mathbb{F}_q(\alpha)$ è un sottocampo di $\mathbb{F}_{q^n}$, ma dato che $[\ \mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e $[\ \mathbb{F}_{q^n} : \mathbb{F}_q] = n$ per il Teorema 1.1.2 si ha che m divide n.

Viceversa, se m divide n allora $\mathbb{F}_{q^n}$ contiene $\mathbb{F}_{q^m}$ come sottocampo, per il Teorema 1.3.6 . Se α è una radice di f nel suo campo di spezzamento allora $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e quindi $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Perciò si ha che $\alpha \in \mathbb{F}_{q^n}$, quindi $\alpha^{q^n} = \alpha$ e conseguentemente è radice di $x^{q^n} - x \in \mathbb{F}_q[x]$. Da qui si conclude che $f(x)$ divide $x^{q^n} - x$ in quanto tutte le radici di $f(x)$ sono radici di $x^{q^n} - x$. □

Teorema 2.2.2. *Sia $f(x)$ un polinomio irriducibile in $\mathbb{F}_q[x]$ di grado m, allora f ha una radice α in $\mathbb{F}_{q^m}$. Inoltre tutte le radici di f sono semplici e sono date dagli elementi distinti $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ di $\mathbb{F}_{q^m}$.*

Dimostrazione. Sia α una radice di f nel suo campo di spezzamento. Allora $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e quindi $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ e in particolare $\alpha \in \mathbb{F}_{q^m}$.
Ora mostriamo che se β è una radice di f allora anche β^q lo è. Sia $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$ con gli $a_i \in \mathbb{F}_q$ per ogni i tale che $0 \leq i \leq m$. Per la Proposizione 1.1.3 e grazie al Teorema 1.3.3 si ha che

$$f(\beta^q) = a_m\beta^{qm} + \ldots + a_1\beta^q + a_0 = a_m^q\beta^{qm} + \ldots + a_1^q\beta^q + a_0^q =$$

$$(a_m\beta^m + \ldots + a_1\beta + a_0)^q = f(\beta)^q$$

Perciò gli elementi $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ sono radici di f.
Bisogna mostrare che tali elementi sono distinti. Supponiamo per assurdo che $\alpha^{q^k} = \alpha^{q^j}$ con j e k interi tali che $0 \leq j < k \leq m-1$. Elevando tale identità alla q^{m-k} si ottiene

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha.$$

Ne segue quindi che $f(x)$ divide $x^{q^{m-k+j}} - x$ ma questo è possibile se e solo se m divide $m\text{-}k\text{+}j$ grazie al Lemma 2.2.1. Ma $0 < m\text{-}k\text{+}j < m$, che porta ad una contraddizione. Dunque gli elementi sono distinti. □

Corollario 2.2.3. *Sia $f(x)$ un polinomio irriducibile in $\mathbb{F}_q[x]$di grado m. Allora il campo di spezzamento di f su $\mathbb{F}_q$ è dato da $\mathbb{F}_{q^m}$.*

Dimostrazione. Segue dal Teorema 2.2.2 che f si spezza in $\mathbb{F}_{q^m}$. Perciò $\mathbb{F}_q(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ per una radice α di f in $\mathbb{F}_{q^m}$. Dunque $\mathbb{F}_{q^m}$ è il campo di spezzamento di $f(x)$ su $\mathbb{F}_q$. □

Corollario 2.2.4. *I campi di spezzamento di due polinomi irriducibili in* $\mathbb{F}_q[x]$ *dello stesso grado sono isomorfi.*

Teorema 2.2.5. *Per ogni campo finito* $\mathbb{F}_q$ *e per ogni* $n \in \mathbb{N}$*, il prodotto di tutti i polinomi monici irriducibili su* $\mathbb{F}_q$*, il cui grado divide* n*, è dato da* $x^{q^n} - x$*.*

Dimostrazione. Innanzitutto si osserva che tutti i polinomi monici irriducibili di $\mathbb{F}_q[x]$ che intervengono nella fattorizzazione di $g(x) = x^{q^n} - x$ sono esattamente quelli il cui grado divide n, grazie al Lemma 2.2.1. Derivando, si ottiene $g'(x) = -1$, quindi g non ha radici multiple nel suo campo di spezzamento su $\mathbb{F}_q$ e quindi ogni polinomio monico irriducibile il cui grado divide n compare una e una sola volta nella fattorizzazione di g. □

Diamo ora una definizione che riguarda gli automorfismi su campi finiti.

Definizione 2.2 (Elementi Coniugati)**.** Sia $\mathbb{F}_{q^m}$ un'estensione di $\mathbb{F}_q$ e sia $\alpha \in \mathbb{F}_{q^m}$. Allora gli elementi $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ sono chiamati *coniugati di* α rispetto a $\mathbb{F}_q$.

Osservazione 5. In realtà gli elementi coniugati sono le immagini distinte di α mediante tutti gli automorfismi di $\mathrm{Gal}(\mathbb{F}_{q^m}/\ \mathbb{F}_q)$, dove $\mathrm{Gal}(\mathbb{F}_{q^m}/\ \mathbb{F}_q)$= $\{\sigma \in \mathrm{Aut}(\mathbb{F}_{q^m}); \quad \sigma(a) = a \text{ per ogni } a \in \mathbb{F}_q\}$ e l'ordine di tale gruppo è uguale a m.

Osservazione 6. I coniugati di α rispetto a $\mathbb{F}_q$ sono distinti se e solo se il polinomio minimo di α su $\mathbb{F}_q$ ha grado m. Altrimenti, se il grado del polinomio minimo è pari a d, ove d è un divisore proprio di m, si ha che $\alpha \in \mathbb{F}_{q^d}$, quindi $\alpha^{q^d} = \alpha$ e i coniugati di α rispetto a $\mathbb{F}_q$ sono $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$. Inoltre ogni elemento è ripetuto m/d volte .

Teorema 2.2.6. *I coniugati di* $\alpha \in \mathbb{F}_q^*$ *rispetto ad ogni sottocampo di* $\mathbb{F}_q$ *hanno lo stesso ordine nel gruppo* $\mathbb{F}_q^*$*.*

Dimostrazione. Segue dal Teorema 2.1.1 che $\mathbb{F}_q^*$ è un gruppo ciclico. Inoltre in un gruppo ciclico di ordine m un generatore elevato alla k-esima potenza genera un sottogruppo di ordine $m/$ M.C.D (k, m). Tale risultato insieme al fatto che ogni potenza della caratteristica di $\mathbb{F}_q$ è prima con l'ordine di $\mathbb{F}_q^*$, che in questo caso è $q - 1$, dimostra quanto voluto. □

Corollario 2.2.7. *Se* α *è un elemento primitivo di* $\mathbb{F}_q$*, allora lo sono anche tutti i suoi coniugati.*

Teorema 2.2.8. *Gli automorfismi distinti di $\mathbb{F}_{q^m}$ che fissano gli elementi di $\mathbb{F}_q$ sono esattamente le funzioni $\sigma_0, \ldots, \sigma_{m-1}$ definite da $\sigma_j(a) = a^{q^j}$ per $a \in \mathbb{F}_{q^m}$ e $0 \leq j \leq m-1$.*

In realtà, utilizzando la Teoria di Galois si può enunciare e dimostrare il teorema nel seguente modo:

Teorema 2.2.9. *Gal$(\mathbb{F}_{q^m}/\mathbb{F}_q)$ è un gruppo ciclico di ordine m e consiste di tutti e soli gli automorfismi di Frobenius $\sigma_0, \ldots, \sigma_{m-1}$.*

Dimostrazione. Sia $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^m})$ e β un elemento primitivo di $\mathbb{F}_{q^m}$ con polinomio minimo $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0 \in \mathbb{F}_q[x]$. Allora si ha che anche $\sigma(\beta)$ è radice di $f(x)$ poichè:

$$0 = \sigma(\beta^m + \ldots + a_1\beta + a_0) =$$

$$\sigma(\beta)^m + \ldots + a_1\sigma(\beta) + a_0.$$

Ma, grazie al Teorema 2.2.2 si sa che data β una radice di $f(x)$, anche β^{q^j} lo è, per un qualche j tale che $0 \leq j \leq m-1$; segue quindi che $\sigma(\beta) = \beta^{q^j}$ ed in particolare, dato che σ è automorfismo, $\sigma(\alpha) = \alpha^{q^j}$ per tutti gli $\alpha \in \mathbb{F}_{q^m}$, da cui $\sigma = \sigma_j$.
Questo discorso si ripete per tutti i j tali che $0 \leq j \leq m-1$ ma, essendo i β^{q^j} diversi grazie al Teorema 2.2.2, si ha che i σ_j sono tutti distinti.
Inoltre, essendo β un elemento primitivo, ogni automorfismo $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ è individuato univocamente da $\sigma(\beta)$, quindi σ_1 è un generatore di $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ ed in particolare tale gruppo ha ordine m.

□

2.3 Traccia, Norma, Basi

In questo terzo paragrafo si definiscono due funzioni chiamate Traccia e Norma su $\mathbb{F}_{q^m}$, introducendo alcune proprietà. Si parlerà di basi per estensioni di campi finiti, dando la definizione di base duale e base normale, con l'obiettivo di dimostrare il teorema della base normale.

Siano K $= \mathbb{F}_q$ e F $= \mathbb{F}_{q^m}$. Considereremo essenzialmente F come spazio vettoriale di dimensione m su K

Definizione 2.3 ($\mathrm{Tr}_{F/K}(\alpha)$)**.** Per ogni $\alpha \in$ F si definisce *Traccia di α su K* l'elemento

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}.$$

Proposizione 2.3.1. *Sia F un'estensione di K. Allora* $\mathrm{Tr}_{F/K}(\alpha)^q = \mathrm{Tr}_{F/K}(\alpha)$, *e quindi* $\mathrm{Tr}_{F/K}(\alpha)$ *è un elemento di K.*

Dimostrazione. Si ha che

$$\begin{aligned}\mathrm{Tr}_{F/K}(\alpha)^q &= (\alpha + \alpha^q + \ldots + \alpha^{q^{m-1}})^q \\ &= \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^m} \\ &= \alpha^q + \alpha^q + \ldots + \alpha^{q^{m-1}} + \alpha \\ &= \mathrm{Tr}_{F/K}(\alpha)\end{aligned}$$

e quindi, applicando il Teorema 1.3.3 si ha che $\mathrm{Tr}_{F/K}(\alpha) \in K$. □

Teorema 2.3.2. *Si considerino* $K = \mathbb{F}_q$ *e* $F = \mathbb{F}_{q^m}$. *Allora si ha che la funzione* $\mathrm{Tr}_{F/K}(\alpha)$ *gode delle seguenti proprietà:*

1. $\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)$ *per ogni* $\alpha, \beta \in F$;
2. $\mathrm{Tr}_{F/K}(c\alpha) = c\mathrm{Tr}_{F/K}(\alpha)$ *per ogni* $c \in K, \alpha \in F$;
3. $\mathrm{Tr}_{F/K}$ *è un' applicazione lineare suriettiva da F a K , dove sia F sia K sono considerati come spazi vettoriali su K;*
4. $\mathrm{Tr}_{F/K}(a) = ma$ *per ogni* $a \in K$.

Dimostrazione.

1. Per ogni $\alpha, \beta \in$ F si ha:

$$\mathrm{Tr}_{F/K}(\alpha + \beta) = (\alpha + \beta) + (\alpha + \beta)^q + \ldots + (\alpha + \beta)^{q^{m-1}} =$$
$$\alpha + \beta + \alpha^q + \beta^q + \alpha^{q^{m-1}} + \beta^{q^{m-1}} = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta).$$

2. Analogamente al punto (1) si osserva che:

$$\mathrm{Tr}_{F/K}(c\alpha) = c\alpha + c^q\alpha^q + \ldots + c^{q^{m-1}}\alpha^{q^{m-1}} =$$
$$c\alpha + c\alpha^q + \ldots + c\alpha^{q^{m-1}} = c\mathrm{Tr}_{F/K}(\alpha).$$

3. Dalle proprietà (1) e (2) e dal fatto che $\mathrm{Tr}_{F/K}(\alpha) \in$ K per ogni $\alpha \in$ F segue che $\mathrm{Tr}_{F/K}$ è una applicazione lineare da F a K. Per dimostrare che è suriettiva basta dimostrare l'esistenza di $\alpha \in$ F tale che $\mathrm{Tr}_{F/K}(\alpha) \neq 0$. Sappiamo che $\mathrm{Tr}_{F/K}(\alpha) = 0$ se e solo se α è radice del polinomio $x^{q^{m-1}} + \ldots + x^q + x \in K[x]$ in F. Tale polinomio ha al più q^{m-1} radici in F e F ha q^m elementi, quindi sicuramente vi sarà un elemento per il quale la Traccia è diversa da zero.

4. Segue immediatamente dalla Definizione 2.3 e dal Teorema 1.3.3.

□

Osservazione 7. La funzione traccia $\mathrm{Tr}_{F/K}$ può essere usata per descrivere ogni applicazione lineare da F a K e tale descrizione è indipendente dalla scelta della base di F come spazio vettoriale su K.

Teorema 2.3.3. *Sia F un'estensione finita di un campo finito K, entrambi considerati come K spazi vettoriali. Allora le applicazioni lineari da F a K sono esattamente le funzioni L_β, $\beta \in F$ dove $L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$ per ogni $\alpha \in F$. Inoltre si ha $L_\beta \neq L_\gamma$ se β e γ sono elementi distinti di F.*

Dimostrazione. Ogni funzione L_β è un' applicazione lineare da F a K per il Teorema 2.3.2 , in particolare segue dal punto (3). Se β e $\gamma \in$ F con $\beta \neq \gamma$, si ha $L_\beta(\alpha) - L_\gamma(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha) - \mathrm{Tr}_{F/K}(\gamma\alpha) = \mathrm{Tr}_{F/K}((\beta - \gamma)\alpha) \neq 0$ per un qualche elemento $\alpha \in F$ dato che $\mathrm{Tr}_{F/K}$ è suriettiva, perciò L_β e L_γ sono diverse. Dato che K=$\mathbb{F}_q$ e F= $\mathbb{F}_{q^m}$, allora la funzione L_β descrive q^m differenti applicazioni lineari da F a K. D'altra parte ogni applicazione lineare da F a K si ottiene assegnando arbitrariamente elementi di K agli m elementi di una base data di F su K. Dato che questo può essere fatto in q^m modi diversi, le funzioni L_β esauriscono tutte le possibili applicazioni lineari da F a K . □

Teorema 2.3.4. *Sia F un'estensione finita di $K = \mathbb{F}_q$ e sia $\alpha \in F$; allora si ha che $\mathrm{Tr}_{F/K}(\alpha) = 0$ se e solo se $\alpha = \beta^q - \beta$ per un qualche $\beta \in F$.*

Dimostrazione. Se $\alpha = \beta^q - \beta$ per un qualche $\beta \in F$ allora $\mathrm{Tr}_{F/K}(\alpha) = 0$ per la Proposizione 2.3.1. Viceversa, si supponga $\alpha \in F$=$\mathbb{F}_{q^m}$, $\mathrm{Tr}_{F/K}(\alpha) = 0$ e sia β una radice di $x^q - x - \alpha$ in una qualche estensione di F. Allora $\beta^q - \beta = \alpha$ e

$$0 = \mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}} =$$

$$(\beta^q - \beta) + (\beta^q - \beta)^q + \ldots + (\beta^q - \beta)^{q^{m-1}} =$$

$$(\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \ldots + (\beta^{q^m} - \beta^{q^{m-1}}) =$$

$$\beta^{q^m} - \beta$$

da cui $\beta^{q^m} = \beta$ e quindi $\beta \in \mathbb{F}_{q^m} =$ F. □

Teorema 2.3.5 (Transitività della Traccia)**.** *Siano K un campo finito, F un'estensione finita di K e E un'estensione finita di F. Allora*

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha))$$

per ogni $\alpha \in E$.

Dimostrazione. Sia K= $\mathbb{F}_q$, allora si ha che se [F : K]=m e [E : F]=n, segue dal Teorema 1.1.2 che [E : K]=mn . Allora se $\alpha \in$ E si ha

$$\mathrm{Tr}_{F/K}(Tr_{E/F}(\alpha)) = \sum_{i=0}^{m-1} Tr_{E/F}(\alpha)^{q^i} = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{jm}} \right)^{q^i} =$$

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{jm+i}} = \sum_{k=0}^{mn-1} \alpha^{q^k} = Tr_{E/K}(\alpha).$$

□

Definizione 2.4 ($N_{F/K}(\alpha)$)**.** Per ogni $\alpha \in$ F si definisce *Norma di* α *su K* l'elemento

$$N_{F/K}(\alpha) = \alpha \cdot \alpha^q \cdot \cdots \cdot \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}.$$

Proposizione 2.3.6. *Sia F un'estensione di K. Allora si ha che* $N_{F/K}(\alpha)^q = N_{F/K}(\alpha)$ *, quindi* $N_{F/K}(\alpha)$ *è un elemento di K.*

Dimostrazione. Si ha che

$$\begin{aligned} N_{F/K}(\alpha)^q &= (\alpha\alpha^q \cdots \alpha^{q^{m-1}})^q \\ &= \alpha^q \alpha^{q^2} \cdots \ \alpha^{q^m} \\ &= \alpha^q \alpha^q \cdots \ \alpha^{q^{m-1}} \alpha \\ &= N_{F/K}(\alpha) \end{aligned}$$

e quindi, applicando il Teorema 1.3.3 si ha che $N_{F/K}(\alpha) \in K$. □

Teorema 2.3.7. *Si considerino K=*$\mathbb{F}_q$ *e F=*$\mathbb{F}_{q^m}$*. Allora si ha che la funzione* $N_{F/K}$ *gode delle seguenti proprietà:*

1. $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha) \cdot N_{F/K}(\beta)$ *per ogni* $\alpha, \beta \in F$*;*
2. $N_{F/K}$ *è una funzione suriettiva da F a K , e anche da F* a K*;*
3. $N_{F/K}(a) = a^m$ *per ogni* $a \in K$*;*

4. $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)$ *per ogni* $\alpha \in F$.

Dimostrazione.

1. Segue immediatamente dalla Definizione 2.4.

2. Per definizione, $N_{F/K}$ è una funzione da F a K. Dato che $N_{F/K}(\alpha) = 0$ se e solo se $\alpha = 0$ allora è anche una funzione da F* a K*, in particolare grazie ad (1) è omomorfismo. Ma, poiché gli elementi del suo nucleo $\ker(N_{F/K})$ sono dati dalle radici del polinomio $x^{(q^m-1)/(q-1)} - 1 \in K[x]$ in F, l'ordine d del nucleo soddisfa $d \leq (q^m-1)/(q-1)$. Tuttavia, segue dal teorema di omomorfismo per i gruppi che l'ordine dell'immagine di $N_{F/K}$ è $(q^m - 1)/d$ che è però maggiore o uguale di $q - 1$; si conclude che l'ordine dell'immagine coincide con l'ordine di K^* e perciò $N_{F/K}$ è una applicazione suriettiva da F* a K*, di conseguenza anche da F a K.

3. Segue dalla Definizione 2.4 e dal Teorema 1.3.3.

4. Si ha $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)^q$ per il punto (1). Inoltre, per la Proposizione 2.3.6 si ha che $N_{F/K}(\alpha)^q = N_{F/K}(\alpha)$, da cui $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)$ per ogni $\alpha \in$F.

□

Teorema 2.3.8 (Transitività della Norma)**.** *Siano K un campo finito, F un'estensione finita di K e E un'estensione finita di F. Allora*

$$N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha))$$

per tutti gli $\alpha \in E$.

Dimostrazione. Siano K = $\mathbb{F}_q$, [F : K]=m e [E : F]=n, in tal modo si ha [E : K]=mn per il Teorema 1.1.2. Allora se $\alpha \in$ E si ha

$$N_{F/K}(N_{E/F}(\alpha)) = N_{F/K}\big(\alpha^{(q^{mn}-1)/(q^m-1)}\big) =$$

$$\big(\alpha^{(q^{mn}-1)/(q^m-1)}\big)^{(q^m-1)/(q-1)} =$$

$$\alpha^{(q^{mn}-1)/(q-1)} = N_{E/K}(\alpha).$$

□

Dato che stiamo considerando essenzialmente F come spazio vettoriale di dimensione m su K, possiamo parlare di base per F su K. Quante sono le basi per un'estensione di campi finita?

Proposizione 2.3.9. *Siano K=$\mathbb{F}_q$ e F= $\mathbb{F}_{q^m}$. Allora il numero di basi di F su K è dato da* $(q^m-1)(q^m-q)(q^m-q^2)\cdots(q^m-q^{m-1})$.

Dimostrazione. Poiché la dimensione di F su K è uguale ad m, si ha che una base di F su K è costituita da m elementi. Quindi, per ottenere una base si scelgono m elementi dai q^m disponibili, in modo tale che siano linearmente indipendenti. I modi per determinare il primo elemento sono dati da (q^m-1) in quanto l'unico elemento che non si può scegliere è lo 0, cioè il vettore nullo. Per quanto riguarda il secondo, bisogna escludere tutti i multipli scalari del primo e quindi si avranno (q^m-q) possibilità. Per definire il terzo elemento, basta che esso non appartenga al sottospazio vettoriale generato dal primo e dal secondo elemento, dunque le possibilità che rimangono sono (q^m-q^2). Ragionando in tal modo si ottiene che il numero di basi di F su K è dato da $(q^m-1)(q^m-q)(q^m-q^2)\cdots(q^m-q^{m-1})$.

□

Tra tutte queste basi se ne introducono alcune che hanno determinate proprietà.

Definizione 2.5 (Base Duale)**.** Siano K un campo finito e F un'estensione finita di K. Allora due basi $\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$ e $\{\beta_1,\beta_2,\ldots,\beta_m\}$ di F su K si dicono *duali (o complementari)* se per ogni $1\le i,j\le m$ si ha:

$$\mathrm{Tr}_{F/K}(\beta_j\alpha_i)=\begin{cases}0 & \text{se } i\neq j\\ 1 & \text{se } i=j\end{cases}$$

Proposizione 2.3.10. *Sia F un'estensione finita di K tale che* $[F:K]=m$. *Allora per ogni* $\mathcal{A}=\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$ *base di F su K esiste unica una base duale* $\mathcal{B}=\{\beta_1,\beta_2,\ldots,\beta_m\}$.

Dimostrazione. Innanzitutto mostriamo l'esistenza di una base duale per una base qualsiasi. Sia $\mathcal{A}=\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$ una base generica di F su K, se $\alpha\in$ F allora si ha che $\alpha=c_1(\alpha)\alpha_1+\ldots+c_m(\alpha)\alpha_m$ e tale rappresentazione è unica. Per determinare i coefficienti $c_j(\alpha)$ si osserva che la funzione $\alpha\mapsto c_j(\alpha)$ è lineare, allora per il Teorema 2.3.3 esiste $\beta_j\in$ F tale che $c_j(\alpha)=\mathrm{Tr}_{F/K}(\beta_j\alpha)$. Se al posto di α si sostituiscono gli α_i per ogni $i=1,\ldots,m$ si ottiene

$$\mathrm{Tr}_{F/K}(\beta_i\alpha_i)=1$$

$$\mathrm{Tr}_{F/K}(\beta_j\alpha_i) = 0, \text{per } i \neq j.$$

Mostriamo che $\mathcal{B}$ è un insieme di elementi linearmente indipendenti. Si consideri

$$d_1\beta_1 + d_2\beta_2 + \ldots + d_m\beta_m = 0 \quad \text{con } d_i \in K \quad \text{per } 1 \leq i \leq m,$$

moltiplicando tutto per α_1 si ottiene:

$$d_1\alpha_1\beta_1 + d_2\alpha_1\beta_2 + \ldots + d_m\alpha_1\beta_m = 0 \quad \text{con } d_i \in K \quad \text{per } 1 \leq i \leq m.$$

Applicando la funzione traccia si ha $d_1 = 0$. Continuando con questo procedimento, moltiplicando ogni volta per α_i con $1 \leq i \leq m$, si ottiene che gli elementi sono linearmente indipendenti. Poichè F ha dimensione m su K e gli elementi $\beta_1, \ldots, \beta_m$ sono linearmente indipendenti, essi costituiscono una base di F su K. Quindi $\mathcal{B}$ è effettivamente base duale di $\mathcal{A}$.

Per quanto riguarda l'unicità si osserva che i $c_j(\alpha)$ che intervengono nella rappresentazione di α sono dati da $c_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j\alpha)$ e quindi, per ogni $\alpha \in$ F l'elemento β_j è univocamente determinato grazie al Teorema 2.3.3.

□

Definizione 2.6 (Base Normale)**.** Siano K=$\mathbb{F}_q$ e F= $\mathbb{F}_{q^m}$. Una base di F su K della forma $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ che consiste quindi di un elemento $\alpha \in F$ e dei suoi coniugati viene chiamata *base normale* di F su K.

Esempio 2.1. Sia $\alpha \in \mathbb{F}_8$ una radice del polinomio irriducibile $x^3+x^2+1 \in \mathbb{F}_2[x]$. Per la Proposizione 2.3.9 si ha che il numero di basi di $\mathbb{F}_8$ su $\mathbb{F}_2$ è dato da

$$(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168.$$

Tra tutte queste basi, consideriamo $\mathcal{B} = \{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$.
Si verifica che la base duale associata a $\mathcal{B}$ è data da

$$\mathcal{D} = \{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}.$$

Inoltre, osservando che $\alpha^4 = 1 + \alpha + \alpha^2$ si ha che $\mathcal{D} = \{\alpha, \alpha^2, \alpha^{2^2}\}$ è anche una base normale per $\mathbb{F}_8$ su $\mathbb{F}_2$.

Lemma 2.3.11 (Lemma di Artin)**.** *Siano $\Psi_1, \ldots, \Psi_m$ omomorfismi distinti da un gruppo G al gruppo moltiplicativo F* di un arbitrario campo F, siano $a_1, \ldots, a_m$ elementi di F non tutti nulli. Allora, per qualche $g \in G$ si ha*

$$a_1\Psi_1(g) + \ldots + a_m\Psi_m(g) \neq 0.$$

Dimostrazione. La dimostrazione viene condotta per induzione su m.
Il caso $m=1$ è banale.
Supponiamo quindi $m>1$; allora per ipotesi induttiva si ha che l'affermazione è vera per $m-1$ omomorfismi distinti. Si considerino $\Psi_1, \ldots, \Psi_m$ e $a_1, \ldots, a_m$ come nell'enunciato.
Se $a_1 = 0$ l'ipotesi d'induzione conduce direttamente al risultato.
Sia quindi $a_1 \neq 0$. Supponiamo per assurdo di avere

$$a_1\Psi_1(g) + \ldots + a_m\Psi_m(g) = 0 \text{ per ogni } g \in G. \tag{2.1}$$

Dato che $\Psi_1 \neq \Psi_m$, esiste $h \in G$ tale che $\Psi_1(h) \neq \Psi_m(h)$. Sostituendo g con hg nella (2.1) si ha

$$a_1\Psi_1(h)\Psi_1(g) + \ldots + a_m\Psi_m(h)\Psi_m(g) = 0 \text{ per ogni } g \in G.$$

Moltiplicando tutto per $\Psi_m(h)^{-1}$ si ottiene:

$$b_1\Psi_1(g) + \ldots + a_m\Psi_m(g) = 0 \text{ per ogni } g \in G,$$

dove $b_i = a_i\Psi_i(h)\Psi_m(h)^{-1}$ per $1 \leq i \leq m-1$. Sottraendo questa identità alla (2.1) si arriva a

$$c_1\Psi_1(g) + \ldots + c_{m-1}\Psi_{m-1}(g) = 0 \text{ per ogni } g \in G,$$

dove $c_i = a_i - b_i$ per $1 \leq i \leq m-1$. Ma $c_i = a_i - a_i\Psi_i(h)\Psi_m(h)^{-1} \neq 0$ e quindi abbiamo una contraddizione sull'ipotesi d'induzione. □

Teorema 2.3.12 (Teorema della Base Normale)**.** *Per ogni campo finito K e per ogni estensione finita F di K esiste sempre una base normale di F su K.*

Dimostrazione. Siano K=$\mathbb{F}_q$ e F=$\mathbb{F}_{q^m}$, con $m \geq 2$. Per il Teorema 2.2.8 , si sa che gli automorfismi di F che fissano K sono dati da $\epsilon, \sigma, \sigma^2, \ldots, \sigma^{m-1}$, dove ϵ è la funzione identità su F, e $\sigma(\alpha) = \alpha^q$ per $\alpha \in F$. Dato che $\sigma(c\alpha) = c\sigma(a)$ e $\sigma(\alpha+\beta) = \sigma(a) + \sigma(\beta)$, per ogni $\alpha, \beta \in F$ e $c \in K$, σ può essere considerata un'applicazione lineare su F. Inoltre, poiché $\sigma^m = \epsilon$ allora il polinomio $x^m - 1 \in K[x]$ annulla σ. Applicando il Lemma 2.3.11 agli endomorfismi di F* $\epsilon, \sigma, \sigma^2, \ldots, \sigma^{m-1}$, segue che non esiste nessun polinomio di grado minore di m che annulla σ. Perciò il polinomio $x^m - 1$ è il polinomio minimo di σ. Il polinomio caratteristico di σ è un polinomio monico, di grado m, divisibile dal polinomio minimo di σ, allora segue che il polinomio caratteristico è dato da $x^m - 1$. Il Lemma 1.2.3 implica l'esistenza di un elemento $\alpha \in F$ tale che F= span$\{\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots\}$. In realtà si vede

tutte le immagini distinte di α mediante gli automorfismi σ_j sono date da $\{\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{m-1}(\alpha)\}$ e poichè F ha dimensione m su K segue che F= span $\{\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{m-1}(\alpha)\}$ e quindi tali elementi formano una base di F su K. Dato che la base è composta da α e dai suoi coniugati, tale base è una base normale. □

A partire da tale teorema abbiamo dunque che per ogni estensione finita F di K esiste una base normale. Come è possibile però sapere se un insieme di determinati elementi forma una base per F su K? In questo contesto si introduce la definizione di discriminante.

Definizione 2.7 (Discriminante)**.** Sia K un campo finito e F una sua estensione finita di grado m su K. Allora il *discriminante* $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ degli elementi $\alpha_1, \ldots, \alpha_m \in F$ è definito dal determinante di ordine m della matrice

$$\begin{pmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_1\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_m) \\ \mathrm{Tr}_{F/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_2\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_2\alpha_m) \\ \ldots & \ldots & \ldots & \ldots \\ \mathrm{Tr}_{F/K}(\alpha_m\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_m\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_m\alpha_m) \end{pmatrix}$$

Segue dalla definizione che $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ è sempre un elemento di K.

Teorema 2.3.13. *Siano K un campo finito, F una sua estensione finita di grado m e $\alpha_1, \ldots, \alpha_m \in F$. Allora $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ è una base di F su K se e solo se $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$.*

Dimostrazione. Sia $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ una base di F su K. Mostriamo che $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$ mostrando che i vettori colonna della matrice definita da $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ sono linearmente indipendenti. Supponiamo che

$$c_1\mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + \ldots + c_m\mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0 \text{ per } 1 \leq j \leq m, \tag{2.2}$$

dove $c_1, \ldots, c_m \in K$. Se $\beta = c_1\alpha_1 + \ldots + c_m\alpha_m$ si ha $\mathrm{Tr}_{F/K}(\beta\alpha_j) = 0$ per $1 \leq j \leq m$ grazie alla (2.2) e, poiché span $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ = F segue che $\mathrm{Tr}_{F/K}(\beta\alpha) = 0$ per tutti gli $\alpha \in F$. Questo è possibile se solo $\beta = 0$ e quindi se $c_1\alpha_1 + \ldots + c_m\alpha_m = 0$, cioè se $c_1 = c_2 = \ldots = c_m = 0$.
Viceversa, si supponga che $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$ e $c_1\alpha_1 + \ldots + c_m\alpha_m = 0$ per qualche $c_1, \ldots, c_m \in K$. Allora moltiplicando tutto per α_j

$$c_1\alpha_1\alpha_j + \ldots + c_m\alpha_m\alpha_j = 0 \text{ per } 1 \leq j \leq m.$$

Applicando la funzione traccia si ottiene

$$c_1 \mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + \ldots + c_m \mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0 \text{ per } 1 \leq j \leq m.$$

Ma dato che i vettori colonna che definiscono $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ sono linearmente indipendenti, segue che $c_1 = c_2 = \ldots = c_m = 0$. Perciò $\alpha_1, \alpha_2, \ldots, \alpha_m$ sono linearmente indipendenti su K. Inoltre, tali elementi sono un insieme di generatori poiché sono tutti distinti e la dimensione di F su K è uguale ad m. Perciò $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ è una base di F su K. □

Osservazione 8. Vi è un altro determinante di ordine m che gioca lo stesso ruolo del discriminante. Gli elementi di questa nuova matrice sono però elementi dell'estensione F di K. Per $\alpha_1, \alpha_2, \ldots, \alpha_m \in F$, sia A la matrice $m \times m$ i cui elementi sono dati da $(A)_{ij} = \alpha_j^{q^{i-1}}$, dove q è il numero di elementi di K. Se ${}^tA$ denota la trasposta di A, un semplice calcolo mostra che ${}^tAA = B$ dove B è la matrice $m \times m$ i cui elementi son dati da $(B)_{ij} = \mathrm{Tr}_{F/K}(\alpha_i\alpha_j)$. Prendendo il determinante si ottiene

$$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) = \det(A)^2.$$

Corollario 2.3.14. *Siano $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{F}_{q^m}$. Allora $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ è una base di $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$ se e solo se il determinante della matrice*

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \ldots & \alpha_m^q \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \ldots & \alpha_m^{q^{m-1}} \end{pmatrix}$$

è diverso da zero.

Capitolo 3

Polinomi Linearizzati

L'ultimo paragrafo del secondo capitolo si è concluso con la dimostrazione del teorema della base normale. Introduciamo ora un'importante classe di polinomi, chiamati polinomi linearizzati, la quale permette di mostrare un risultato che generalizza tale teorema, fornendo in particolare una dimostrazione alternativa.

Prima di tutto diamo la definizione di ordine di un polinomio e alcuni risultati particolari legati ad essa.

3.1 Ordine di Polinomi

Lemma 3.1.1. *Sia $f \in \mathbb{F}_q[x]$ un polinomio di grado $m \geq 1$ con $f(0) \neq 0$. Allora esiste un intero positivo $e \leq q^m - 1$ tale che $f(x)$ divide $x^e - 1$.*

Dimostrazione. L'anello $\mathbb{F}_q[x]/(f)$ è costituito da $q^m - 1$ classi resto non nulle. Le classi $x^j + (f)$, $j = 0, 1, \ldots, q^m - 1$ sono tutte diverse da zero e quindi esistono interi r ed s con $0 \leq r < s \leq q^m - 1$ tali che $x^s \equiv x^r \bmod f(x)$. Dato che x e $f(x)$ sono primi tra loro, segue che $f(x)$ divide $x^{s-r} - 1$ e $0 \leq r - s \leq q^m - 1$, quindi prendendo $e = r - s$ si conclude. □

Definizione 3.1 (Ordine di un Polinomio)**.** Sia $f \in \mathbb{F}_q[x]$ un polinomio non nullo. Se $f(0) \neq 0$, allora il più piccolo intero positivo e tale che $f(x)$ divide $x^e - 1$ è chiamato *ordine di f* e si denota con $\mathrm{ord}(f) = \mathrm{ord}(f(x))$. Se $f(0) = 0$, allora $f(x) = x^h g(x)$, dove $h \in \mathbb{N}$ e $g \in \mathbb{F}_q[x]$ con $g(0) \neq 0$ univocamente determinato. In tal caso l'ordine di f è per definizione l'ordine di g.

Come si determina l'ordine di un polinomio irriducibile?

Teorema 3.1.2. *Sia $f \in \mathbb{F}_q[x]$ un polinomio irriducibile su $\mathbb{F}_q$ di grado m tale che $f(0) \neq 0$. Allora l'ordine di f è uguale all'ordine di ciascuna radice di f nel gruppo moltiplicativo $\mathbb{F}_{q^m}^*$.*

Dimostrazione. Dal Corollario 2.2.3 segue che $\mathbb{F}_{q^m}$ è il campo di spezzamento di f su $\mathbb{F}_q$. Inoltre, per il Teorema 2.2.6 , le radici di f hanno lo stesso ordine nel gruppo $\mathbb{F}_{q^m}^*$. Sia $\alpha \in \mathbb{F}_{q^m}^*$ una radice di f, supponendo l'ordine di α in $\mathbb{F}_{q^m}$ pari ad e, si ha che $\alpha^e = 1$ se e solo se $f(x)$ divide $x^e - 1$ per il Lemma 1.3.7. Quindi $e \geq \text{ord}(f)$. Ma, il più piccolo intero tale che $f(x)$ divide $x^e - 1$ è per definizione l'ordine del polinomio ed in particolare quindi l'ordine del polinomio coincide con l'ordine delle radici di f in $\mathbb{F}_{q^m}^*$. □

Corollario 3.1.3. *Se $f \in \mathbb{F}_q[x]$ è un polinomio irriducibile su $\mathbb{F}_q$ di grado m, allora* ord*(f) divide $q^m - 1$.*

Dimostrazione. Se $f(x) = cx$ con $c \in \mathbb{F}_{q^m}^*$, allora ord(f)= 1 ed in particolare 1 divide $q^m - 1$.
Altrimenti, il risultato segue dal Teorema 3.1.2 e dal fatto che $\mathbb{F}_{q^m}^*$ è un gruppo di ordine $q^m - 1$ e l'ordine di un elemento divide sempre l'ordine del gruppo. □

Lemma 3.1.4. *Sia c un intero positivo. Allora il polinomio $f \in \mathbb{F}_q[x]$ con $f(0) \neq 0$ divide $x^c - 1$ se e solo se* ord*(f) divide c.*

Dimostrazione. Se $e = \text{ord}(f)$ divide c, allora $f(x)$ divide $x^e - 1$ e $x^e - 1$ divide $x^c - 1$, quindi $f(x)$ divide $x^c - 1$.
Viceversa si ha che se $f(x)$ divide $x^c - 1$ allora $c \geq e$ quindi possiamo scrivere $c = me + r$ con $0 \leq r < e$ e $m \in \mathbb{N}$. Dato che $x^c - 1 = (x^{me} - 1)x^r + (x^r - 1)$, segue che $f(x)$ divide $(x^r - 1)$ il che è possibile solo per $r = 0$. Quindi e divide c. □

Corollario 3.1.5. *Siano e_1 ed e_2 interi positivi, d il massimo comun divisore di e_1 ed e_2. Allora il massimo comun divisore di $x^{e_1} - 1$ e $x^{e_2} - 1$ in $\mathbb{F}_q[x]$ è $x^d - 1$.*

Dimostrazione. Sia $f(x)$ il massimo comun divisore (monico) di $x^{e_1} - 1$ e $x^{e_2} - 1$. Dato che $x^d - 1$ è divisore comune di $x^{e_i} - 1, i = 1, 2$, per il Lemma 3.1.4 segue che $x^d - 1$ divide $f(x)$. D'altra parte $f(x)$ è il massimo comun divisore di $x^{e_i} - 1, i = 1, 2$ e quindi, per il Lemma 3.1.4 si ha che ord(f) divide e_1 e e_2. Di conseguenza, ord(f) divide d e perciò $f(x)$ divide $x^d - 1$ per il Lemma 3.1.4. Quindi $f(x) = x^d - 1$. □

Si enunciano ora due teoremi chiave che permetteranno in seguito di calcolare l'ordine di un generico polinomio.

Teorema 3.1.6. *Sia $g \in \mathbb{F}_q[x]$ irriducibile su $\mathbb{F}_q$ con $g(0) \neq 0$ e* ord*(g)= e, sia $f = g^b$ dove b è un intero positivo. Sia t il più piccolo intero tale che $p^t \geq b$ dove p è la caratteristica di $\mathbb{F}_q$. Allora* ord$(f) = ep^t$.

Dimostrazione. Sia $c = \text{ord}(f)$ e notando che la divisibilità di $x^c - 1$ per $f(x)$ implica la divisibilità di $x^c - 1$ per $g(x)$, si ottiene che e divide c per il Lemma 3.1.4. Inoltre, $g(x)$ divide $x^e - 1$ perciò $f(x)$ divide $(x^e - 1)^b$ e quindi divide anche $(x^e - 1)^{p^t} = x^{ep^t} - 1$, da cui c divide ep^t. Segue, da quello che abbiamo mostrato che $c = ep^u, 0 \leq u \leq t$. Notiamo ora che $x^e - 1$ ha solo radici semplici dato che e non è un multiplo di p per il Lemma 3.1.4 . Perciò tutte le radici di $x^{ep^u} - 1 = (x^e - 1)^{p^u}$ hanno molteplicità p^u. Ma $g(x)^b$ divide $x^{ep^u} - 1$, dai cui $p^u \geq b$, comparando la molteplicità delle radici, e quindi $u \geq t$. Perciò si ottiene che $u = t$ e $c = ep^t$. □

Teorema 3.1.7. *Siano $g_1, \ldots, g_k$ polinomi in $\mathbb{F}_q[x]$ non nulli e primi tra loro. Sia $f = g_1 \cdots g_k$. Allora l'ordine di f è uguale al minimo comune multiplo tra* ord*(g_1), …,* ord*(g_k).*

Dimostrazione. Senza perdere di generalità si consideri il caso in cui $g_i(0) \neq 0, \text{con } 1 \leq i \leq k$. Siano $e = \text{ord}(f)$, $e_i = \text{ord}(g_i)$ per $1 \leq i \leq k$ e sia $c = \text{m.c.m}(e_1, \ldots, e_k)$. Allora ogni g_i divide $x^{e_i} - 1$ e quindi g_i divide $x^c - 1$. Dato che i polinomi sono primi tra loro, si ottiene che $f(x)$ divide $x^c - 1$. Applicando il Lemma 3.1.4 si ottiene che e divide c.
D'altra parte f divide $x^e - 1$ e quindi ogni g_i divide $x^e - 1$. Applicando di nuovo il Lemma 3.1.4 si ottiene che ogni e_i divide e per ogni $1 \leq i \leq k$ e quindi che c divide e. Si conclude quindi che $c = e$. □

Osservazione 9. Utilizzando la stessa argomentazione del Teorema 3.1.7 si mostra che l'ordine del minimo comune multiplo di un numero finito di polinomi non nulli è uguale al minimo comune multiplo degli ordini di tali polinomi.

Osservazione 10. L'anello dei polinomi è un dominio a fattorizzazione unica, quindi ogni polinomio di grado positivo può essere scritto come prodotto di polinomi irriducibili. Dunque il Teorema 3.1.6 ed il Teorema 3.1.7 permettono di calcolare l'ordine di un qualsiasi polinomio.

Teorema 3.1.8. *Sia $\mathbb{F}_q$ un campo finito di caratteristica p e sia $f \in \mathbb{F}_q[x]$ un polinomio di grado positivo con $f(0) \neq 0$. Sia $f = af_1^{b_1} \cdots f_k^{b_k}$, con $a \in$*

$\mathbb{F}_q$, $b_1, \ldots, b_k \in \mathbb{N}$, *e* $f_1, \ldots, f_k$ *polinomi in* $\mathbb{F}_q[x]$ *monici irriducibili distinti, la fattorizzazione canonica di* f *in* $\mathbb{F}_q[x]$. *Allora* $\mathrm{ord}(f) = ep^t$ *, dove* e *è il minimo comune multiplo di* $\mathrm{ord}(f_1), \ldots, \mathrm{ord}(f_k)$ *e* t *è il più piccolo intero tale che* $p^t \geq \max(b_1, \ldots, b_k)$.

Osservazione 11. Un metodo per determinare l'ordine di un polinomio irriducibile f in $\mathbb{F}_q[x]$ tale che $f(0) \neq 0$ è basato sull'osservazione che l'ordine e di f è il più piccolo intero tale che $x^e \equiv 1 \bmod f(x)$. Inoltre, per il Corollario 3.1.3 e divide $q^m - 1$, dove m=deg(f). Supponendo $q^m \geq 2$ fattorizziamo nel prodotto di primi

$$q^m - 1 = \prod_{j=1}^{s} p_j^{r_j}.$$

Per $1 \leq j \leq s$ si calcola $x^{(q^m-1)/p_j} \bmod f(x)$. Se $x^{(q^m-1)/p_j} \not\equiv 1 \bmod f(x)$, allora e è un multiplo di $p_j^{r_j}$. Se $x^{(q^m-1)/p_j} \equiv 1 \bmod f(x)$, allora e non è un multiplo di $p_j^{r_j}$. In questo ultimo caso bisogna controllare se e è un multiplo di $p_j^{r_j-1}, p_j^{r_j-2}, \ldots, p_j$, calcolando

$$x^{(q^m-1)/p_j^2}, x^{(q^m-1)/p_j^3}, \ldots, x^{(q^m-1)/p_j^{r_j}} \bmod f(x).$$

Tale calcolo viene ripetuto per ogni fattore primo di $q^m - 1$.

3.2 Polinomi Linearizzati e loro Proprietà

Definizione 3.2 (Polinomio Linearizzato)**.** Sia $\mathbb{F}_{q^m}$ un'estensione finita di $\mathbb{F}_q$. Un polinomio della forma

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}, \quad \text{con } \alpha_i \in \mathbb{F}_{q^m}$$

viene chiamato *polinomio linearizzato* o *q-polinomio* su $\mathbb{F}_{q^m}$.

Osservazione 12. Siano F un'estensione arbitraria di $\mathbb{F}_{q^m}$ e $L(x)$ un polinomio linearizzato su $\mathbb{F}_{q^m}$, allora considerando F come spazio vettoriale su $\mathbb{F}_q$, si nota che $L(x)$ induce un'applicazione lineare su F, infatti:

$$L(\alpha + \beta) = L(\alpha) + L(\beta) \text{ per ogni } \alpha, \beta \in F,$$

$$L(c\beta) = cL(\beta) \text{ per ogni } c \in \mathbb{F}_q \text{ e per ogni } \beta \in F.$$

Ecco perchè tali polinomi vengono chiamati in questo modo.

I polinomi della forma $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$ hanno inoltre importanti proprietà per quanto riguarda l'insieme delle loro radici. Approfondiamo questo argomento con i prossimi risultati.

Teorema 3.2.1. *Siano $L(x)$ un polinomio linearizzato su $\mathbb{F}_{q^m}$ non nullo, $\mathbb{F}_{q^s}$ un'estensione di $\mathbb{F}_{q^m}$ contenente tutte le radici di $L(x)$. Allora ogni radice di $L(x)$ ha la stessa molteplicità, che è pari ad 1 oppure una potenza di q. Inoltre l'insieme delle radici di $L(x)$ forma un sottospazio vettoriale di $\mathbb{F}_{q^s}$.*

Dimostrazione. Innanzitutto segue dall'Osservazione 12 che l'insieme delle radici di $L(x)$ forma un sottospazio vettoriale di $\mathbb{F}_{q^s}$ in quanto ogni combinazione lineare di radici è ancora una radice.
Dunque rimane da verificare che ogni radice ha la stessa molteplicità. Consideriamo quindi $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$ e deriviamo: $L'(x) = \alpha_0$. Se $\alpha_0 \neq 0$ allora $L(x)$ ha solo radici semplici e quindi tutte con la molteplicità pari ad 1. Altrimenti si ha che $\alpha_0 = \alpha_1 = \ldots = \alpha_{k-1} = 0$ e $\alpha_k \neq 0$ per qualche $k \geq 1$, quindi si ha che

$$L(x) = \sum_{i=k}^{n} \alpha_i x^{q^i} = \sum_{i=k}^{n} \alpha_i^{q^{mk}} x^{q^i} = \left(\sum_{i=k}^{n} \alpha_i^{q^{(m-1)k}} x^{q^{i-k}} \right)^{q^k},$$

il che dice che $L(x)$ è la q^k-esima potenza di un polinomio linearizzato con radici semplici, perciò ogni radice di $L(x)$ ha la stessa molteplicità, pari a q^k. □

Lemma 3.2.2. *Siano $\beta_1, \ldots, \beta_n$ elementi di $\mathbb{F}_{q^m}$. Allora*

$$\det \begin{pmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \ldots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \ldots & \beta_2^{q^{n-1}} \\ \vdots & \vdots & & \vdots & \\ \beta_n & \beta_n^q & \beta_1^{q^2} & \ldots & \beta_n^{q^{n-1}} \end{pmatrix} = \beta_1 \prod_{j=1}^{n-1} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^{j} c_k \beta_k \right),$$

e quindi tale determinante è diverso da zero se e solo se $\beta_1, \ldots, \beta_n$ sono linearmente indipendenti su $\mathbb{F}_q$.

Dimostrazione. Sia

$$D_n = \det \begin{pmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \ldots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \ldots & \beta_2^{q^{n-1}} \\ \vdots & \vdots & & \vdots & \\ \beta_n & \beta_n^q & \beta_1^{q^2} & \ldots & \beta_n^{q^{n-1}} \end{pmatrix};$$

mostriamo che $D_n = \beta_1 \prod_{j=1}^{n-1} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\beta_{j+1} - \sum_{k=1}^{j} c_k \beta_k\right)$ per induzione su n.

Per $n=1$ la formula è verificata banalmente. Supponiamo quindi la formula vera per D_n e mostriamola per D_{n+1}.
Si consideri il polinomio dato da

$$D(x) = \det \begin{pmatrix} \beta_1 & \beta_1^q & \beta_1^{q^2} & \ldots & \beta_1^{q^n} \\ \beta_2 & \beta_2^q & \beta_2^{q^2} & \ldots & \beta_2^{q^n} \\ \vdots & \vdots & & \vdots & \\ \beta_n & \beta_n^q & \beta_1^{q^2} & \ldots & \beta_n^{q^n} \\ x & x^q & x^{q^2} & \ldots & x^{q^n} \end{pmatrix}.$$

Calcolando il determinante con il Teorema di Laplace, sviluppando secondo l'ultima riga, si ottiene:

$$D(x) = D_n x^{q^n} + \sum_{i=0}^{n-1} \alpha_i x^{q^i},$$

con $\alpha_i \in \mathbb{F}_{q^m}$ per $0 \leq i \leq n-1$.
Ora mostriamo che vale l'identità

$$D(x) = D_n \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(x - \sum_{k=1}^{n} c_k \beta_k\right), \tag{3.1}$$

sia nel caso in cui $\beta_1, \ldots, \beta_n$ siano linearmente indipendenti che viceversa.

Supponiamo inizialmente $\beta_1, \ldots, \beta_n$ linearmente indipendenti su $\mathbb{F}_q$. Allora $D(\beta_k) = 0$ per $1 \leq k \leq n$ e poiché D(x) è un polinomio linearizzato su $\mathbb{F}_{q^m}$ abbiamo che tutte le combinazioni lineari di $\beta_1, \ldots, \beta_n$ sono radici di D(x). Tale polinomio ha quindi q^n radici distinte (se non fossero distinte verrebbe negata l'ipotesi d'indipendenza lineare) ed in tal modo otteniamo la fattorizzazione (3.1).

Se invece $\beta_1, \ldots, \beta_n$ sono linearmente dipendenti su $\mathbb{F}_q$, allora $D_n = 0$ per ipotesi induttiva e $\sum_{k=1}^{n} b_k \beta_k = 0$ per qualche $b_1, \ldots, b_n \in \mathbb{F}_q$, non tutti nulli. Questo porta a dire che le prime n righe della matrice il cui determinante è D(x) sono linearmente dipendenti su $\mathbb{F}_q$, in quanto:

$$\sum_{k=1}^{n} b_k \beta_k^{q^j} = \left(\sum_{k=1}^{n} b_k \beta_k\right)^{q^j} = 0, \text{ per } j = 0, \ldots, n.$$

Perciò $D(x) = 0$ e l'identità (3.1) è soddisfatta in quanto D_n per ipotesi induttiva è uguale a 0.

Ora, valutando $D(x)$ in β_{n+1}:

$$D(\beta_{n+1}) = D_n \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\beta_{n+1} - \sum_{k=1}^{n} c_k \beta_k \right) = D_{n+1},$$

ed in particolare vale che $\beta_1, \ldots, \beta_n$ sono linearmente indipendenti se e solo se $D_{n+1} \neq 0$. □

Teorema 3.2.3. *Sia U un sottospazio vettoriale di $\mathbb{F}_{q^m}$, visto come spazio vettoriale su $\mathbb{F}_q$. Allora per ogni intero non negativo k il polinomio*

$$L(x) = \prod_{\beta \in U} (x - \beta)^{q^k}$$

è un polinomio linearizzato su $\mathbb{F}_{q^m}$.

Dimostrazione. Se si osserva che la potenza q^k-esima di un polinomio linearizzato è ancora un polinomio linearizzato, basta considerare il caso in cui $k = 0$. Sia $\{\beta_1, \ldots, \beta_n\}$ una base di U su $\mathbb{F}_q$, supponendo $\dim_{\mathbb{F}_q} U = n$. Il determinante D_n è diverso da zero per il Lemma 3.2.2 e quindi segue dall'espressione (3.1) che:

$$L(x) = \prod_{\beta \in U} (x - \beta) =$$

$$\prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(x - \sum_{k=1}^{n} c_k \beta_k \right) = D_n^{-1} D(x)$$

che mostra che $L(x)$ è un polinomio linearizzato su $\mathbb{F}_{q^m}$. □

Osservazione 13. Cerchiamo di capire come determinare le radici di q-polinomi. Sia $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$ un polinomio linearizzato su $\mathbb{F}_{q^m}$. L'obiettivo è ora quello di determinare le radici di tale polinomio appartenenti ad un'estensione finita F di $\mathbb{F}_{q^m}$. Si è gia osservato che la funzione $\beta \mapsto L(\beta)$, per ogni $\beta \in F$ è una applicazione lineare di F come spazio vettoriale su $\mathbb{F}_q$. Ma ogni applicazione lineare può essere rappresentata mediante una matrice e dunque L può essere descritta tramite una matrice ad elementi in $\mathbb{F}_q$. In particolare sia $\{\beta_1, \ldots, \beta_s\}$ una base di F su $\mathbb{F}_q$. In tal modo ogni $\beta \in F$ può essere scritto come

$$\beta = \sum_{j=1}^{s} c_j \beta_j \text{ con } c_j \in \mathbb{F}_q \text{ per } 1 \leq j \leq s;$$

allora

$$L(\beta) = \sum_{j=1}^{s} c_j L(\beta_j).$$

Sia

$$L(\beta_j) = \sum_{k=1}^{s} b_{kj}\beta_k \text{ per } 1 \leq j \leq s,$$

dove $b_{jk} \in \mathbb{F}_q$ per $1 \leq j,k \leq s$ e sia B la matrice $s \times s$ su $\mathbb{F}_q$ tale che l'elemento di posto (j,k) è dato da $(B)_{jk} = b_{kj}$. Allora se

$$B \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} = \begin{pmatrix} d_1 \\ \vdots \\ d_s \end{pmatrix}$$

si ha

$$L(\beta) = \sum_{k=1}^{s} d_k \beta_k.$$

Dunque l'equazione $L(\beta) = 0$ equivale al sistema lineare omogeneo

$$B \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{3.2}$$

Se rk B $= r$, dove rk è il rango della matrice B, ovvero il numero di righe o equivalentemente colonne linearmente indipendenti, allora il sistema ammette q^{s-r} soluzioni $(c_1, \ldots, c_s)$. Ogni vettore soluzione determina una radice di $L(x)$:

$$\beta = \sum_{j=1}^{s} c_j \beta_j.$$

3.3 q-Polinomi Affini

Utilizzando i polinomi affini e il metodo di determinazione delle radici di un polinomio linearizzato si mostrerà un metodo semplice per determinare le radici di un polinomio qualsiasi, basato sulla risoluzione di sistemi lineari.

Definizione 3.3 (q-Polinomio Affine)**.** Un polinomio della forma $A(x) = L(x) - \alpha$ dove $L(x)$ è un q-polinomio su $\mathbb{F}_{q^m}$ e $\alpha \in \mathbb{F}_{q^m}$, viene chiamato *$q$-polinomio affine* su $\mathbb{F}_{q^m}$.

Osservazione 14. Innanzitutto ci si domanda come si possano determinare le radici di q-polinomi affini. É facile osservare che $\beta \in F$, dove F è un'estensione finita di $\mathbb{F}_{q^m}$, è una radice di $A(x)$ se e solo se $L(\beta) = \alpha$. Utilizzando la (3.2) tale equazione è equivalente al sistema

$$B \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} = \begin{pmatrix} d_1 \\ \vdots \\ d_s \end{pmatrix} \tag{3.3}$$

dove $\alpha = \sum_{k=1}^{s} d_k \beta_k$ e B è la matrice definita nell'Osservazione 13. Ogni soluzione del sistema (3.3) determina una radice $\beta = \sum_{k=1}^{s} c_k \beta_k$ di $A(x)$ in F.

Osservazione 15. Si è mostrato che è piuttosto semplice determinare le radici di polinomi linearizzati e affini, in quanto ci si riconduce alla risoluzione di un sistema lineare. Considerando un polinomio $f(x)$ in $\mathbb{F}_{q^m}[x]$ di grado positivo, come si determinano le sue radici utilizzando i polinomi affini?

1. Si determina un multiplo affine $A(x)$ di $f(x)$.
2. Si ottengono tutte le radici di $A(x)$ in F, estensione finita di $\mathbb{F}_{q^m}$, utilizzando i risultati ottenuti nell'Osservazione 14.
3. Le radici di $f(x)$ sicuramente sono tra le radici di $A(x)$, per determinarle si calcola $f(\beta)$ per tutte le radici β di $A(x)$.

Osservazione 16. Lo scopo è determinare un multiplo affine $A(x)$ di un polinomio generico $f(x)$. Sia $f(x)$ un polinomio su $\mathbb{F}_{q^m}$ di grado $n \geq 1$.

1. Per ogni $i = 0, 1, \ldots, n-1$, si calcola l'unico polinomio $r_i(x)$ di grado minore o uguale a $n-1$ tale che $x^{q^i} \equiv r_i(x) \bmod f(x)$.
2. Si determinano degli elementi $\alpha_i \in \mathbb{F}_{q^m}$, non tutti nulli, tali che $\sum_{i=0}^{n-1} \alpha_i r_i(x)$ sia un polinomio costante. In particolare, si osserva che $\sum_{i=0}^{n-1} \alpha_i r_i(x)$ è un polinomio di grado al più $n-1$. Annullando i coefficienti di $x^{n-1}, \ldots, x$ si ottiene un sistema lineare omogeneo di $n-1$ equazioni in n incognite.
3. Si determina una soluzione non banale per tale sistema, arrivando ad ottenere $\alpha = \sum_{i=0}^{n-1} \alpha_i r_i(x)$, per qualche $\alpha \in \mathbb{F}_{q^m}$.
4. Si ottiene dunque che

$$\sum_{i=0}^{n-1} \alpha_i x^{q^i} \equiv \sum_{i=0}^{n-1} \alpha_i r_i(x) \equiv \alpha \bmod f(x).$$

da cui segue che

$$A(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i} - \alpha$$

è un multiplo di $f(x)$.

Osservando l'insieme delle radici di polinomi affini si riescono a determinare alcuni risultati simili a quelli riguardanti l'insieme delle radici di polinomi linearizzati.

Teorema 3.3.1. *Sia A(x) un q-polinomio affine su $\mathbb{F}_{q^m}$ di grado positivo, $\mathbb{F}_{q^s}$ un'estensione di $\mathbb{F}_{q^m}$ contenente tutte le radici di A(x). Allora ogni radice ha la stessa molteplicità, che è uguale ad 1 oppure una potenza di q. Inoltre lo spazio delle radici forma un sottospazio affine di $\mathbb{F}_{q^s}$, ove $\mathbb{F}_{q^s}$ è visto come spazio vettoriale su $\mathbb{F}_q$.*

Dimostrazione. I risultati sulla molteplicità di tali radici si dimostrano in maniera analoga al Teorema 3.2.1. Mostriamo che l'insieme delle radici di $A(x)$ forma un sottospazio affine di $\mathbb{F}_{q^s}$. Sia $A(x) = L(x) - \alpha$, dove $L(x)$ è un polinomio linearizzato e $\alpha \in \mathbb{F}_{q^m}$. Sia inoltre β una radice di $A(x)$. Allora abbiamo che γ è una radice di $A(x)$, se e solo se $L(\gamma) = \alpha = L(\beta)$, se e solo se $L(\gamma - \beta) = 0$, se e solo se $\gamma \in \beta + U$ dove U è il sottospazio vettoriale di $\mathbb{F}_{q^s}$ costituito dalle radici di $L(x)$. Perciò le radici di $A(x)$ formano un sottospazio affine di $\mathbb{F}_{q^s}$. □

Teorema 3.3.2. *Sia T un sottospazio affine di $\mathbb{F}_{q^m}$, considerato come uno spazio vettoriale su $\mathbb{F}_q$. Allora per ogni intero non negativo k il polinomio*

$$A(x) = \prod_{\gamma \in T} (x - \gamma)^{q^k}$$

è un q polinomio affine su $\mathbb{F}_{q^m}$.

Dimostrazione. Sia $T = \eta + U$ dove U è un sottospazio vettoriale di $\mathbb{F}_{q^m}$. Allora

$$L(x) = \prod_{\beta \in U} (x - \beta)^{q^k}$$

è un polinomio linearizzato per il Teorema 3.2.3, quindi possiamo supporre che esista un n positivo tale che $L(x) = \sum_{i=0}^{n} a_i x^{q^i}$ con $a_i \in \mathbb{F}_{q^m}$. Dunque

$$A(x) = \prod_{\gamma \in T} (x - \gamma)^{q^k}) = \prod_{\beta \in U} (x - \eta - \beta)^{q^k} = L(x - \eta).$$

$L(x-\eta)$ è un polinomio affine su $\mathbb{F}_{q^m}$:

$$\begin{aligned} L(x-\eta) &= a_0(x-\eta) + a_1(x-\eta) + \ldots + a_n(x-\eta)^{q^n} \\ &= a_0x - a_0\eta + a_1x^q - a_1\eta^q + \ldots + a_nx^{q^n} - a_n\eta^{q^n} \\ &= L(x) - \mu \\ \text{dove } \mu &= -(a_0\eta + a_1\eta^q + \ldots + a_n\eta^{q^n}), \end{aligned}$$

dunque $\mu \in \mathbb{F}_{q^m}$ in quanto combinazione lineare di elementi di $\mathbb{F}_{q^m}$, e quindi $A(x)$ è un polinomio affine su $\mathbb{F}_{q^m}$. □

3.4 Operazioni Simboliche

Definiremo ora un'operazione sull'insieme dei polinomi linearizzati che possiede le stesse proprietà della moltiplicazione. Un buon candidato è la composizione: tale operazione infatti gode sia della proprietà associativa, sia della proprietà distributiva. É vero che la composizione di due polinomi linearizzati è un'operazione commutativa?

Proposizione 3.4.1. *Siano $L_1(x)$ ed $L_2(x)$ polinomi linearizzati su $\mathbb{F}_q[x]$. Allora vale che $(L_1 \circ L_2)(x) = L_1(L_2(x)) = L_2(L_1(x)) = (L_2 \circ L_1)(x)$.*

Dimostrazione. Siano

$$L_1(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}, \qquad L_2(x) = \sum_{i=0}^{k} \beta_i x^{q^i}$$

con $\alpha_i, \beta_i \in \mathbb{F}_q$.

$$\begin{aligned} (L_1 \circ L_2)(x) &= L_1(L_2(x)) \\ &= \sum_{i=0}^{n} \alpha_i (L_2(x))^{q^i} = \alpha_0 L_2(x) + \alpha_1 (L_2(x))^q + \ldots + \alpha_n (L_2(x))^{q^n} \\ &= \alpha_0(\beta_0 x + \beta_1 x^q + \ldots + \beta_k x^{q^k}) + \ldots + \alpha_n(\beta_0 x + \beta_1 x^q + \ldots \\ &\quad + \beta_k x^{q^k})^{q^n} \\ &= \alpha_0\beta_0 x + \ldots + \alpha_0\beta_k x^{q^k} + \ldots + \alpha_n\beta_0^{q^n} x^{q^n} + \ldots + \alpha_n\beta_k^{q^n} x^{q^{k+n}} \\ &= \beta_0(\alpha_0 x + \ldots + \alpha_n x^{q^n}) + \ldots + \beta_k(\alpha_0 x q^k + \ldots + \alpha_n x^{q^{n+k}}) \\ &= \beta_0(\alpha_0 + \alpha_1 x^q + \ldots + \alpha_k x q^k) + \ldots + \beta_k(\alpha_0 + \alpha_1 x^q + \ldots \\ &\quad + \alpha_n x^{q^n})^{q^k} \\ &= \beta_0 L_1(x) + \beta_1 (L_1(x))^q + \ldots + \beta_k (L_1(x))^{q^k} = \sum_{i=0}^{k} \beta_i (L_1(x))^{q^i} \\ &= L_2(L_1(x)) = (L_2 \circ L_1)(x). \end{aligned}$$

□

Si noti che la composizione non è un'operazione commutativa in $\mathbb{F}_{q^m}[x]$, lo è però la sua restrizione ai polinomi linearizzati in $\mathbb{F}_q[x]$. A questo punto è possibile introdurre una nuova operazione commutativa.

Definizione 3.4 (Moltiplicazione Simbolica)**.** Siano $L_1(x)$ e $L_2(x)$ due q-polinomi su $\mathbb{F}_{q^m}$, allora la composizione di tali polinomi è ancora un polinomio linearizzato ed inoltre si definisce *moltiplicazione simbolica* tale operazione

$$L_1(x) \otimes L_2(x) = L_1(L_2(x)).$$

Definizione 3.5 (Polinomi Associati)**.** I polinomi

$$l(x) = \sum_{i=0}^{n} \alpha_i x^i \quad \text{e} \quad L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

in $\mathbb{F}_{q^m}[x]$ vengono chiamati polinomi *q-associati.*

D'ora in avanti si parlerà di polinomi associati intesi come polinomi q-associati.

Lemma 3.4.2. *Siano $L_1(x)$ e $L_2(x)$ polinomi linearizzati su $\mathbb{F}_q$ siano $l_1(x)$ e $l_2(x)$ rispettivamente i polinomi associati. Allora $l(x) = l_1(x)l_2(x)$ e $L(x) = L_1(x) \otimes L_2(x)$ sono a loro volta associati.*

Dimostrazione. Le equazioni

$$l(x) = \sum_i a_i x^i = \sum_j b_j x^j \sum_k c_k x^k = l_1(x)l_2(x)$$

e

$$L(x) = \sum_i a_i x^{q^i} = \sum_j b_j \left(\sum_k c_k x^{q^k} \right)^{q^j} = \sum_j b_j \sum_k c_k x^{q^{k+j}} = L_1(x) \otimes L_2(x)$$

sono verificate se e solo se

$$a_i = \sum_{k=0}^{i} b_k c_{i-k}$$

per ogni i. □

Definizione 3.6 (Divisione Simbolica)**.** Siano $L_1(x)$ e $L(x)$ polinomi linearizzati su $\mathbb{F}_q$. Diremo che L_1 *divide simbolicamente* $L(x)$ se $L(x) = L_1(x) \otimes L_2(x)$ per un qualche polinomio linearizzato $L_2(x)$ su $\mathbb{F}_q$.

Corollario 3.4.3. *Siano $L_1(x)$ e $L(x)$ polinomi linearizzati su $\mathbb{F}_q$ associati rispettivamente a $l_1(x)$ e $l(x)$. Allora $L_1(x)$ divide simbolicamente $L(x)$ se e solo se $l_1(x)$ divide $l(x)$.*

Teorema 3.4.4. *Siano $L_1(x)$ e $L(x)$ polinomi linearizzati su $\mathbb{F}_q$ associati rispettivamente a $l_1(x)$ e $l(x)$. Allora sono equivalenti:*

1. *$L_1(x)$ divide simbolicamente $L(x)$;*
2. *$L_1(x)$ divide in senso ordinario $L(x)$;*
3. *$l_1(x)$ divide $l(x)$.*

Dimostrazione. Per concludere la dimostrazione basta mostrare che (1) è equivalente a (2) dato che l'equivalenza tra (1) e (3) è vera per il Corollario 3.4.3. Supponiamo quindi che $L_1(x)$ divida simbolicamente $L(x)$, allora

$$L(x) = L_1(x) \otimes L_2(x) = L_2(x) \otimes L_1(x) = L_2(L_1(x))$$

per un certo polinomio linearizzato $L_2(x)$ su $\mathbb{F}_q$. Sia $L_2(x) = \sum_{i=0}^{n} a_i x^{q^i}$, allora

$$L(x) = a_0 L_1(x) + a_1 L_1(x)^q + \ldots + a_n L_n(x)^{q^n}, \tag{3.4}$$

perciò $L_1(x)$ divide $L(x)$ nel senso ordinario.
Viceversa, supponiamo che $L_1(x)$ divida in senso ordinario $L(x)$ e supponiamo anche che $L_1(x)$ non sia il polinomio nullo. Utilizzando l'algoritmo di divisione si può scrivere che $l(x) = k(x)l_1(x) + r(x)$ dove deg$(r)<$ deg (l_1). Passando agli associati si ottiene $L(x) = K(x) \otimes L_1(x) + R(x)$. Grazie all'implicazione già mostrata si ottiene, dalla (3.4), che $L_1(x)$ divide in senso ordinario $L(x)$ e quindi divide anche $R(x)$ ma, poiché $\deg(R(x)) < \deg(L_1(x))$, segue che $R(x)$ deve essere il polinomio identicamente nullo. Necessariamente $r(x) \equiv 0$, da cui $l(x) = l_1(x)k(x)$. Passando ai polinomi linearizzati si ottiene che $L(x) = L_1(x) \otimes K(x)$ concludendo la dimostrazione . □

Teorema 3.4.5. *Sia $f(x)$ un polinomio irriducibile in $\mathbb{F}_q[x]$ e sia F(x) il polinomio linearizzato associato a $f(x)$. Allora il grado di ogni fattore irriducibile di F(x)/ x in $\mathbb{F}_q[x]$ è uguale all'ordine di f.*

Dimostrazione. Distinguiamo due casi.

Il primo caso è quello in cui $f(0) = 0$. Dato che f è un polinomio irriducibile allora si ha che $f(x) = x$. Il polinomio linearizzato associato a f è dato da $F(x) = x^q$ e dunque $F(x)/x = x^{q-1}$. I suoi fattori irriducibili

sono dati dal polinomio $h(x) = x$ ed in particolare si ha che $\deg(h(x)) = 1 = \mathrm{ord}(f)$.

Il secondo caso è dato da $f(0) \neq 0$; siano $e = \mathrm{ord}(f)$ e $h(x) \in \mathbb{F}_q[x]$ un fattore irriducibile di $F(x)/x$ di grado d.

Innanzitutto si osserva che $h(x)$ non divide x; infatti se $f(0) \neq 0$, $F(x)/x$ non può avere x come fattore irriducibile. Questo perchè $F(x)$ è divisibile da x in quanto polinomio linearizzato, tuttavia non è divisibile da x^2 in quanto il termine noto di $f(x)$ non è nullo, dunque $F(x)/x$ non può avere x come fattore irriducibile, confermando il fatto che $h(x)$ non divide x.

Per ipotesi $f(x)$ divide $x^e - 1$ e quindi per il Teorema 3.4.4 $F(x)$ divide $x^{q^e} - x$. Dunque, d divide e per il Teorema 2.2.5. Utilizzando l'algoritmo di divisione, si può scrivere $x^d - 1 = g(x)f(x) + r(x)$, con $g(x), r(x) \in \mathbb{F}_q[x]$ e $\deg(r) < \deg(f)$. Passando ai polinomi linearizzati

$$x^{q^d} - x = G(x) \otimes F(x) + R(x),$$

e dato che $h(x)$ divide $x^{q^d} - x$ per il Teorema 3.4.4 e inoltre $h(x)$ divide $G(x) \otimes F(x)$, segue che $h(x)$ divide $R(x)$. Supponendo $r(x) \neq 0$, allora si ha che $r(x)$ e $f(x)$ sono primi tra loro e quindi, per il Teorema di Bezout si ha che esistono $s(x), k(x) \in \mathbb{F}_q[x]$ tali che

$$s(x)r(x) + k(x)f(x) = 1.$$

Passando agli associati:

$$S(x) \otimes R(x) + K(x) \otimes F(x) = x.$$

Dato che $h(x)$ divide $R(x)$ e $F(x)$, segue che $h(x)$ divide x, ma ciò non è possibile per quanto mostrato precedentemente. Si ha quindi che $R(x) = 0$, conseguentemente $r(x) = 0$, $f(x)$ divide $x^d - 1$ e quindi e divide d. Concludendo $e = d$. □

Definizione 3.7 (Polinomio Simbolicamente Irriducibile)**.** Un polinomio linearizzato $L(x)$ su $\mathbb{F}_q$ di grado strettamente maggiore di 1 si dice *simbolicamente irriducibile* se le sue uniche decomposizioni in polinomi linearizzati sono del tipo $L(x) = L_1(x) \otimes L_2(x)$, dove uno dei due tra $L_1(x)$ o $L_2(x)$ ha grado pari ad 1.

Osservazione 17. Un q-polinomio simbolicamente irriducibile è sempre riducibile in senso ordinario poiché ogni polinomio linearizzato di grado maggiore di 1 ha almeno un fattore non banale dato da x.

Osservazione 18. Un polinomio linearizzato è simbolicamente irriducibile su $\mathbb{F}_q$ se e solo se il suo associato è irriducibile su $\mathbb{F}_q$ e tale risultato segue dal Lemma 3.4.2 e dal Teorema 3.4.4. Infatti, se un polinomio generico è irriducibile, allora i suoi unici divisori sono 1 e se stesso. Passando ai polinomi linearizzati tramite gli associati, si ha che il polinomio linearizzato associato si decompone nel prodotto di due polinomi, di cui uno necessariamente ha grado pari ad 1, verificando quindi la definizione di polinomio simbolicamente irriducibile. In modo analogo si mostra il viceversa.

Osservazione 19. Ogni polinomio linearizzato su $\mathbb{F}_q$ di grado strettamente maggiore di 1 ha una fattorizzazione simbolica in fattori simbolicamente irriducibili essenzialmente unica, nel senso che tutte le altre fattorizzazioni simboliche si ottengono permutando l'ordine dei fattori e moltiplicando tali fattori per elementi di $\mathbb{F}_q^*$.
In particolare, la fattorizzazione simbolica di un polinomio linearizzato $L(x)$ su $\mathbb{F}_q$, si ottiene a partire dal suo polinomio associato $l(x)$. Difatti si fattorizza $l(x)$ decomponendolo canonicamente e quindi determinando i suoi fattori irriducibili in $\mathbb{F}_q[x]$. Ora, a partire dai fattori irriducibili di $l(x)$ si passa ai polinomi linearizzati associati. Quest'ultimi sono i fattori simbolicamente irriducibili di $L(x)$ in $\mathbb{F}_q[x]$.

Definizione 3.8 (Massimo Comune Divisore Simbolico)**.** Il *massimo comun divisore simbolico* di due (o più) polinomi linearizzati su $\mathbb{F}_q$ è il polinomio linearizzato su $\mathbb{F}_q$ di grado più alto che divide simbolicamente i polinomi di partenza.

Osservazione 20. Visto che ogni polinomio linearizzato si fattorizza in modo essenzialmente unico, anche il massimo comun divisore simbolico è individuato in modo essenzialmente unico, cioè a meno di moltiplicazioni per elementi di $\mathbb{F}_q^*$.

Proposizione 3.4.6. *Siano $L_1(x), \ldots, L_k(x)$ polinomi linearizzati su $\mathbb{F}_q$, $h(x) = \text{M.C.D}(L_1(x), \ldots, L_k(x))$. Allora le radici di $h(x)$ sono le radici comuni dei polinomi linearizzati $L_1(x), \ldots, L_k(x)$.*

Dimostrazione. Siano $\mathcal{A}$ l'insieme delle radici di $h(x)$ e $\mathcal{B}$ l'insieme delle radici comuni di $L_1(x), \ldots, L_k(x)\}$. Innanzitutto $\mathcal{A}$ è contenuto in $\mathcal{B}$ in quanto per definizione di massimo comun divisore $h(x)$ divide $L_i(x)$ per ogni i.

Viceversa, sia $\alpha \in \mathcal{B}$ e sia $g(x)$ il suo polinomio minimo su $\mathbb{F}_q$. Allora $g(x)$ divide tutti gli $L_i(x)$ e in particolare divide $h(x)$. Dunque, $\alpha \in \mathcal{A}$ e quindi $\mathcal{B}$ è contenuto in $\mathcal{A}$. □

Proposizione 3.4.7. *Siano $L_1(x), \ldots, L_k(x)$ polinomi linearizzati su $\mathbb{F}_q$, allora il massimo comun divisore $h(x)$ coincide con il massimo comun divisore simbolico $H(x)$, supponendo $H(x)$ monico senza perdere di generalità.*

Dimostrazione. Grazie alla Proposizione 3.4.6 si ha che le radici di $h(x)$ sono le radici comuni dei polinomi linearizzati considerati. Inoltre, per il Teorema 3.2.1, l'insieme delle radici di un polinomio linearizzato è uno spazio vettoriale su $\mathbb{F}_q$, così come l'intersezione di sottospazi vettoriali lo è. Dunque, l'insieme delle radici di $h(x)$ forma uno spazio vettoriale. Segue dal Teorema 3.2.3 che $h(x)$ è in realtà un q-polinomio su $\mathbb{F}_q$.

Banalmente si ha che $H(x)$ divide $h(x)$ in quanto, per definizione di massimo comun divisore simbolico $H(x)$ divide ogni $L_i(x)$ simbolicamente e quindi anche ordinariamente per il Teorema 3.4.4 dato che siamo in $\mathbb{F}_q$. A questo punto dato che $h(x)$ è il massimo comun divisore, si ha che $H(x)$ divide $h(x)$ e in particolare si osserva che $\deg(h(x)) \geq \deg(H(x))$.

Tuttavia si ha anche che $h(x)$ divide $L_i(x)$ ordinariamente, applicando nuovamente il Teorema 3.4.4 si ottiene che $h(x)$ divide $L_i(x)$ simbolicamente. Segue dalla definizione di massimo comun divisore simbolico che $H(x)$ è il polinomio di grado più alto che divide simbolicamente tutti gli $L_i(x)$; per quanto mostrato precedentemente si ha che $\deg(h(x)) \geq \deg(H(x))$, da cui $h(x)$ coincide con $H(x)$. □

3.5 q-Moduli

Definizione 3.9 (q-modulo)**.** Uno spazio vettoriale M di dimensione finita su $\mathbb{F}_q$, contenuto in una qualche estensione di $\mathbb{F}_q$ e che gode della proprietà che ogni q-esima potenza di un elemento di M appartiene ancora ad M, viene chiamato *q-modulo*.

Tale definizione ha origine da alcune riflessioni sulle radici di un polinomio linearizzato, infatti tali radici formano un sottospazio vettoriale non nullo di $\mathbb{F}_q$ grazie al Teorema 3.2.1. Inoltre si ha anche che la potenza q-esima di una radice è ancora una radice. Questo è facile da verificare poiché se β è tale che $L(\beta) = 0$, con $L(\beta) = a_0\beta + a_1\beta^q + \ldots + a_k\beta^{q^k}$, sostituendo β con β^q si

ha $L(\beta^q) = a_0\beta^q + a_1\beta^{q^2} + \ldots + a_k\beta^{q^{k+1}} = a_0^q\beta^q + a_1^q\beta^{q^2} + \ldots + a_k^q\beta^{q^{k+1}} = (a_0\beta + a_1\beta^q + \ldots + a_k\beta^{q^k})^q = 0$, sfruttando il fatto che $a_i \in \mathbb{F}_q$.

Riusciamo a stabilire dunque quando un polinomio è linearizzato osservando solo le sue radici?

Teorema 3.5.1. *Un polinomio monico $L(x)$ su $\mathbb{F}_q$ è linearizzato se e solo se ogni radice di $L(x)$ ha la stessa molteplicità, che è 1 oppure una potenza di q, e le radici formano un q-modulo.*

Dimostrazione. Se $L(x)$ è linearizzato su $\mathbb{F}_q$ il risultato segue dal Teorema 3.2.1 e dalla riflessione che segue la definizione di q-modulo.

Viceversa, le condizioni date e il Teorema 3.2.3 implicano che $L(x)$ è un polinomio linearizzato su una qualche estensione di $\mathbb{F}_q$, si vuole provare che lo è proprio su $\mathbb{F}_q$. Dunque mostriamo che i suoi coefficienti appartengono ad $\mathbb{F}_q$. Sia M il q-modulo costituito dalle radici di $L(x)$, allora

$$L(x) = \prod_{\beta \in M} (x - \beta)^{q^k}$$

per un qualche intero non negativo k. Dal fatto che M è un q-modulo segue che:

$$L(x)^q = \prod_{\beta \in M} (x^q - \beta^q)^{q^k} = \prod_{\beta \in M} (x^q - \beta)^{q^k} = L(x^q). \tag{3.5}$$

Se

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i},$$

allora

$$\sum_{i=0}^{n} \alpha_i^q x^{q^{i+1}} = L(x)^q = L(x^q) = \sum_{i=0}^{n} \alpha_i x^{q^{i+1}},$$

perciò per $0 \leq i \leq n$ si ha $\alpha_i^q = \alpha_i$ e perciò $\alpha_i \in \mathbb{F}_q$. Dunque $L(x)$ è un polinomio linearizzato su $\mathbb{F}_q$. □

In che modo possiamo caratterizzare i polinomi simbolicamente irriducibili sfruttando i q-moduli?

Teorema 3.5.2. *Un polinomio linearizzato $L(x)$ su $\mathbb{F}_q$ di grado strettamente maggiore di q è simbolicamente irriducibile su $\mathbb{F}_q$ se e solo se $L(x)$ ha radici semplici e il q-modulo M costituito dalle radici di $L(x)$ non contiene q-moduli diversi da quelli banali.*

Dimostrazione. Si supponga $L(x)$ simbolicamente irriducibile su $\mathbb{F}_q$. Supponiamo per assurdo che $L(x)$ abbia radici multiple, allora possiamo scrivere $L(x) = L_1(x)^q$, dove $L_1(x)$ è un q-polinomio di grado strettamente maggiore di 1. Ricordando che per la (3.5) si ha $L_1(x)^q = L_1(x^q)$, allora $L(x) = L_1(x^q) = x^q \otimes L_1(x)$, ma questo è assurdo poiché $L(x)$ è simbolicamente irriducibile. Dunque $L(x)$ ha solo radici semplici. Supponiamo ora che N sia un q-modulo contenuto in M; segue dal Teorema 3.5.1 che $L_2(x) = \prod_{\beta \in N}(x - \beta)$ è un q-polinomio su $\mathbb{F}_q$. Dato che $L_2(x)$ divide $L(x)$ in senso ordinario, lo divide anche simbolicamente. Ma $L(x)$ è simbolicamente irriducibile su $\mathbb{F}_q$, quindi $\deg(L_2)$ è uguale ad 1 oppure uguale a $\deg(L(x))$, perciò si ha che $N = \{0\}$ oppure $N = M$.

Viceversa, sia $L(x) = L_1(x) \otimes L_2(x)$ una decomposizione simbolica su $\mathbb{F}_q$. Allora $L_1(x)$ divide simbolicamente $L(x)$ e perciò lo divide anche in senso ordinario. Segue che $L_1(x)$ ha solo radici semplici e il q-modulo N costituito dalle radici di $L_1(x)$ è contenuto in M. Tuttavia N è $\{0\}$ oppure M, perciò il grado di $L_1(x)$ è 1 oppure uguale al grado di $L(x)$, il che implica che $L(x)$ è simbolicamente irriducibile su $\mathbb{F}_q$. □

Definizione 3.10 (Radice q-primitiva)**.** Sia $L(x)$ un q-polinomio su $\mathbb{F}_{q^m}$. Una radice ξ di $L(x)$ si chiama *radice q-primitiva* se non è radice di nessun q-polinomio di grado più basso di $L(x)$ su $\mathbb{F}_{q^m}$.

Proposizione 3.5.3. *Siano $L(x)$ un polinomio linearizzato su $\mathbb{F}_{q^m}$, ξ un elemento di un'estensione finita di $\mathbb{F}_{q^m}$, $g(x)$ il polinomio minimo di ξ su $\mathbb{F}_{q^m}$. Allora si ha che ξ è radice q-primitiva di $L(x)$ su $\mathbb{F}_{q^m}$ se e solo se $g(x)$ divide $L(x)$ e $g(x)$ non divide alcun q-polinomio di grado minore di $L(x)$.*

Dimostrazione. Sia ξ una radice q-primitiva di $L(x)$; allora $g(x)|L(x)$ per definizione di polinomio minimo e $g(x)$ non divide alcun q-polinomio di grado minore per definizione di radice q-primitiva.

Viceversa, se ξ non fosse radice q-primitiva, allora esisterebbe un q-polinomio $F(x)$ di grado minore di $L(x)$ di cui ξ è radice. Ma allora il polinomio minimo $g(x)$ di ξ dividerebbe $F(x)$, contraddicendo le ipotesi. □

Osservazione 21. Sia ξ un elemento di un'estensione finita di $\mathbb{F}_{q^m}$. Si osserva che è sempre possibile determinare un polinomio linearizzato su $\mathbb{F}_{q^m}$ per il quale ξ sia radice q-primitiva, supponendo di conoscere il polinomio minimo di ξ su $\mathbb{F}_{q^m}$. Se tale polinomio linearizzato è monico, allora si parla di *q-polinomio minimo* di ξ su $\mathbb{F}_{q^m}$. Per costruirlo si procede in modo analogo all'Osservazione 16:

1. Per ogni $i = 0, 1, \ldots, n$, si calcola l'unico polinomio $r_i(x)$ di grado minore o uguale di $n-1$ tale che $x^{q^i} \equiv r_i(x) \bmod g(x)$, ove $g(x)$ è il polinomio minimo di ξ su $\mathbb{F}_{q^m}$.

2. Si determinano dei coefficienti $\alpha_i \in \mathbb{F}_{q^m}$, non tutti nulli, tali che $\sum_{i=0}^{n} \alpha_i r_i(x) = 0$. Questo porta ad un sistema lineare omogeneo di n equazioni in $n+1$ incognite $\alpha_0, \ldots, \alpha_n$.

3. Tale sistema ha una soluzione non banale e con tale soluzione si ottiene:

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i} \equiv \sum_{i=0}^{n} \alpha_i r_i(x) \equiv 0 \bmod g(x).$$

$L(x)$ è un q-polinomio non nulllo su $\mathbb{F}_{q^m}$ e divisibile da $g(x)$ per costruzione. Scegliendo il vettore soluzione in modo tale che $L(x)$ sia monico e di grado minore possibile si ha che $g(x)$ divide $L(x)$ e inoltre $g(x)$ non divide alcun q-polinomio di grado più piccolo di $L(x)$ e quindi, per la Proposizione 3.5.3, si ha che ξ è radice q-primitiva. Rimane solo da verificare che tale $L(x)$ sia univocamente determinato ma questo è vero in quanto il sistema ottenuto al punto (3) è un sistema lineare che ammette una soluzione non banale dipendente da almeno un parametro. Imponendo che il coefficiente di grado più alto sia uguale ad 1, affinché il q-polinomio sia monico, e gli altri parametri in modo tale da ottenere il polinomio di grado minore possibile, la soluzione è univocamente determinata.

Teorema 3.5.4. *Sia ξ un elemento di un'estensione di campi finita di $\mathbb{F}_{q^m}$ e sia M(x) il suo q-polinomio minimo su $\mathbb{F}_{q^m}$. Allora un q-polinomio K(x) su $\mathbb{F}_{q^m}$ ha ξ come radice se e solo se $K(x) = L(x) \otimes M(x)$ per un qualche q-polinomio $L(x)$ su $\mathbb{F}_{q^m}$. In particolare se m=1 ciò significa che K(x) ha ξ come radice se e solo se K(x) è divisibile simbolicamente per M(x).*

Dimostrazione. Se $K(x) = L(x) \otimes M(x)$ allora $K(\xi) = 0$.

Viceversa, sia

$$M(x) = \sum_{j=0}^{t} \gamma_j x^{q^j}, \text{con } \gamma_t = 1$$

e si supponga che ξ sia radice di

$$K(x) = \sum_{h=0}^{r} \alpha_h x^{q^h}, r \geq t.$$

Siano $s = r - t$ e $\gamma_j = 0$, per $j < 0$ e si consideri il seguente sistema di $s+1$ equazioni in $s+1$ incognite:

$$\begin{aligned}
\beta_0 + \gamma_{t-1}^{q}\beta_1 + \gamma_{t-2}^{q^2}\beta_2 + \ldots + \gamma_{t-s}^{q^s}\beta_s &= \alpha_t \\
\beta_1 + \gamma_{t-1}^{q^2}\beta_2 + \ldots + \gamma_{t-s+1}^{q^s}\beta_s &= \alpha_{t+1} \\
\ddots + \quad + \quad \vdots \quad &\quad \vdots \\
\beta_{s-1} + \gamma_{t-1}^{q^s}\beta_s &= \alpha_{r-1} \\
\beta_s &= \alpha_r.
\end{aligned}$$

Per tale sistema esiste unica una soluzione in quanto la matrice dei coefficienti è una matrice quadrata a scala in cui gli elementi sulla diagonale sono tutti uguali ad 1, dunque ha rango massimo. Ponendo

$$L(x) = \sum_{i=0}^{s} \beta_i x^{q^i} \quad \text{e} \quad R(x) = K(x) - L(M(x))$$

si ottiene

$$\begin{aligned}
R(x) &= \sum_{h=0}^{r} \alpha_h x^{q^h} - \sum_{i=0}^{s} \beta_i \left(\sum_{j=0}^{t} \gamma_j x^{q^j} \right)^{q^i} \\
&= \sum_{h=0}^{r} \alpha_h x^{q^h} - \sum_{i=0}^{s} \beta_i \sum_{j=0}^{t} \gamma_j^{q^i} x^{q^{j+i}} \\
&= \sum_{h=0}^{r} \alpha_h x^{q^h} - \sum_{h=0}^{r} \left(\sum_{i=0}^{s} \gamma_{h-i}^{q^i} \beta_i \right) x^{q^h} \\
&= \sum_{h=0}^{r} \left(\alpha_h - \sum_{i=0}^{s} \gamma_{h-i}^{q^i} \beta_i \right) x^{q^h}.
\end{aligned}$$

Dunque $R(x)$ ha grado minore di q^t poiché se $h \geq t$ allora i coefficienti dell'equazione sono nulli. Ma poiché $R(\xi) = K(\xi) - L(M(\xi)) = 0$ per definizione di $M(x)$ si ottiene che $R(x)$ è il polinomio nullo. Dunque $K(x) = L(x) \otimes M(x)$. □

Proposizione 3.5.5. *Sia $\mathbb{F}_{q^m} \subseteq F$ un'estensione di campi finita e sia $\xi \in F$. Allora un q-polinomio $K(x) \in \mathbb{F}_{q^m}[x]$ ha ξ come radice se e solo se il q-polinomio minimo di ξ su $\mathbb{F}_{q^m}$ $M(x)$ divide $K(x)$.*

Dimostrazione. Se il q-polinomio minimo di ξ su $\mathbb{F}_{q^m}$ $M(x)$ divide $K(x)$ allora si ha che $K(x) = M(x)L(x)$ per un certo polinomio $L(x)$ su $\mathbb{F}_{q^m}$. Valutando tutto in ξ si ottiene $K(\xi) = 0$.

Viceversa, segue dal Teorema 3.5.4 che $K(x) = L(x) \otimes M(x)$ per un qualche q-polinomio $L(x)= \sum_{i=0}^{s} a_i x^{q^i}$ su $\mathbb{F}_{q^m}$. Sviluppando i conti si ha che

$$K(x) = L(x) \otimes M(x) = L(M(x)) = a_0 M(x) + a_1 M(x)^q + \ldots + a_s M(x)^{q^s}$$

da cui si nota che $M(x)$ divide $K(x)$. □

Osservazione 22. Si è interessati a capire quante sono le radici q-primitive di un polinomio $L(x)$ su $\mathbb{F}_q$. Sia N_L tale numero e distinguiamo alcuni casi.

Il primo caso è quello in cui $L(x)$ ha solo radici multiple. Allora sappiamo che $L(x) = L_1(x)^q$, dove $L_1(x)$ è un q-polinomio su $\mathbb{F}_q$. Ma dato che ogni radice di $L(x)$ è anche radice di $L_1(x)$ allora abbiamo che $N_L = 0$.

Se invece $L(x)$ ha grado 1, è ovvio che $N_L = 1$.

Se $L(x)$ ha grado $q^n > 1$ supponendolo monico senza perdere di generalità, sia

$$L(x) = \underbrace{L_1(x) \otimes \ldots \otimes L_1(x)}_{e_1} \otimes \ldots \otimes \underbrace{L_r(x) \otimes \ldots \otimes L_r(x)}_{e_r}$$

la fattorizzazione simbolica di $L(x)$, dove gli $L_i(x)$ sono monici e simbolicamente irriducibili. Come si ottiene N_L? Sottraendo dal numero totale di radici q^n il numero di radici di $L(x)$ che sono radici di q-polinomi di grado più piccolo di q^n. Come determiniamo tale numero?
Sia ξ una radice di $L(x)$ di quest'ultimo tipo, e sia $M(x)$ il suo q-polinomio minimo su $\mathbb{F}_q$. Allora $\deg(M) < q^n$, $M(x)$ divide simbolicamente $L(x)$ per il Teorema 3.5.4 e quindi divide simbolicamente uno dei polinomi $K_i(x)$ ottenuto dividendo simbolicamente $L(x)$ per uno dei fattori $L_i(x)$ per un qualche i. Sia $q^{n_i} = \deg(L_i(x))$, allora il numero di tutte le radici di $K_i(x)$ è dato da q^{n-n_i}. Dato che le radici di $K_i(x)$ sono anche radici di $L(x)$ allora si ha che $N_L = q^n -$ (numero di radici comuni dei $K_i(x)$). Bisogna però stare attenti alle radici comuni in quanto si rischia di toglierne troppe. Se $i_1, \ldots, i_s$ sono pedici distinti, allora il numero di radici comuni di $K_{i_1}, \ldots, K_{i_s}$ è uguale al grado del massimo comun divisore ordinario per la Proposizione 3.4.6 e per la Proposizione 3.4.7 tale grado è pari a quello del massimo comun divisore simbolico, e cioè a

$$q^{n-(n_{i_1}+\ldots+n_{i_s})}$$

in quanto il massimo comun divisore simbolico si ottiene dalla fattorizzazione di $L(x)$ cancellando un $L_i(x)$ per ogni i. Dunque, applicando il Principio di

Inclusione-Esclusione [2]

$$N_L = q^n - \sum_{i=1}^{r} q^{n-n_i} + \sum_{1\le i<j\le r} q^{n-(n_i+n_j)} + \ldots + (-1)^r q^{n-(n_1+\ldots+n_r)}$$
$$= q^n(1-q^{-n_1})\cdots(1-q^{-n_r}).$$

In realtà si può calcolare il numero di radici primitive di un q-polinomio a partire dal suo polinomio associato, definendo preliminarmente una funzione che ricorda la funzione di Eulero.

Definizione 3.11. Sia $f\in \mathbb{F}_q[x]$ un polinomio non nullo. Allora si definisce $\Phi_q(f(x)) = \Phi_q(f)$ la funzione che conta il numero di polinomi in $\mathbb{F}_q[x]$ di grado più piccolo rispetto al grado di f e primi con f.

Lemma 3.5.6. *La funzione Φ_q definita precedentemente ha le seguenti proprietà:*

1. $\Phi_q(f) = 1$ *se* $\deg(f) = 0$;
2. $\Phi_q(fg) = \Phi_q(f)\Phi_q(g)$, *se f e g sono primi tra loro;*
3. *Se* $\deg(f)=n \geq 1$, *allora*

$$\Phi_q(f) = q^n(1-q^{-n_1})\cdots(1-q^{-n_r}),$$

dove gli n_i sono i gradi dei polinomi monici e irriducibili che compaiono nella fattorizzazione canonica di f in $\mathbb{F}_q[x]$.

Dimostrazione.

1. La dimostrazione è banale.
2. Siano $\Phi_q(f) = s$ e $\Phi_q(g) = t$ e siano $f_1,\ldots,f_s$ e $g_1,\ldots g_t$ i polinomi contati da $\Phi_q(f)$ e $\Phi_q(g)$. Se $h \in \mathbb{F}_q[x]$ è tale che $\deg(h) < \deg(fg)$ e M.C.D(fg,h)=1 allora M.C.D(f,h)=1 e M.C.D(g,h)=1 da cui $h \equiv f_i \bmod f$ e $h \equiv g_j \bmod g$ per una coppia unica (i,j).
   Ma, d'altra parte, data una coppia (i,j) per il teorema cinese dei resti si ha che esiste un unico polinomio $h \in \mathbb{F}_q[x]$ tale che $h \equiv f_i \bmod f$ e $h \equiv g_j \bmod g$ e $\deg(h) < \deg(fg)$. Tale polinomio soddisfa la proprietà che M.C.D(f,h)= M.C.D(g,h)=1 da cui M.C.D(fg,h)=1.
   Dunque si è mostrato che esiste una corrispondenza tra le coppie (i,j) e i polinomi $h \in \mathbb{F}_q[x]$ tali che M.C.D(fg,h)=1 e $\deg(h) < \deg(fg)$, da cui si ha che $\Phi_q(fg) = \Phi_q(f)\Phi_q(g)$.

3. Sia $f = af_1^{p_1} \cdots f_r^{p_r}$ la fattorizzazione in irriducibili monici di f con $a \in \mathbb{F}_q$. Allora, per il punto (2) si ha che $\Phi_q(f) = \Phi_q(f_1^{p_1}) \cdots \Phi_q(f_r^{p_r})$. Cerchiamo di capire come si calcola $\Phi_q(f_i^{p_i})$. Siano $b \in \mathbb{F}_q[x]$ un polinomio irriducibile di grado m, e un intero positivo. Allora i polinomi $h \in \mathbb{F}_q[x]$ con $\deg(h) < \deg(b^e) = em$ che non sono primi con b^e sono esattamente quelli divisibili da b e sono quindi della forma $h = gb$ dove $\deg(g) < em - m$. Dato che vi sono q^{em-m} scelte diverse per g, si ha $\Phi_q(b^e) = q^{em} - q^{em-m} = q^{em}(1 - q^{-m})$. Per concludere:

$$\begin{aligned}\Phi_q(f) =& \Phi_q(f_1^{p_1}) \cdots \Phi_q(f_r^{p_r}) \\ =& q^{n_1^{p_1}}(1 - q^{-n_1}) \cdots q^{n_r^{p_r}}(1 - q^{-n_r}) \\ =& q^{n_1^{p_1} + \cdots + n_r^{p_r}}(1 - q^{-n_1}) \cdots (1 - q^{-n_r}) \\ =& q^n(1 - q^{-n_1}) \cdots (1 - q^{-n_r}).\end{aligned}$$

□

Proposizione 3.5.7. *Sia $L(x)$ un polinomio linearizzato su $\mathbb{F}_q$ e sia $l(x)$ il suo associato su $\mathbb{F}_q$. Allora si ha che $N_L = \Phi_q(l)$.*

Dimostrazione. Si è gia visto che se

$$L(x) = \underbrace{L_1(x) \otimes \ldots \otimes L_1(x)}_{e_1} \otimes \ldots \otimes \underbrace{L_r(x) \otimes \ldots \otimes L_r(x)}_{e_r}$$

è la fattorizzazzione simbolica di $L(x)$ in fattori simbolicamente irriducibili allora $N_L = q^n(1 - q^{-n_1}) \cdots (1 - q^{-n_r})$, dove $q^{n_i} = \deg(L_i)$, grazie all'Osservazione 22. Inoltre, passando agli associati sappiamo che

$$l(x) = l_1(x)^{e_1} \cdots l_r(x)^{e_r}$$

per l'Osservazione 19, dove $l_i(x)$ è il polinomio associato al q-polinomio $L_i(x)$. Dato che $n_i = \deg(l_i)$, calcolando $\Phi_q(l)$ mediante l'utilizzo della proprietà (3) del Lemma 3.5.6 si ha che:

$$\Phi_q(l) = q^n(1 - q^{-n_1}) \cdots (1 - q^{-n_r})$$

da cui si ottiene l'uguaglianza $N_L = \Phi_q(l)$. □

Teorema 3.5.8. *Sia $L(x)$ un polinomio affine su $\mathbb{F}_q[x]$ e sia $l(x)$ il suo polinomio associato. Allora il numero N_L di radici q-primitive per $L(x)$ è dato da $N_L = 0$ se $L(x)$ ha radici multiple, $N_L = \Phi_q(l)$ se $L(x)$ ha radici semplici.*

Dimostrazione. Segue dalla Proposizione 3.5.7 e dall'Osservazione 22. □

Corollario 3.5.9. *Ogni q-polinomio non nullo su $\mathbb{F}_q$ con radici semplici ha almeno una radice q-primitiva su $\mathbb{F}_q$.*

3.6 Basi per q-moduli

Teorema 3.6.1. *Sia M un q-modulo di dimensione $m \geq 1$ su $\mathbb{F}_q$. Allora si ha che esiste un elemento $\xi \in M$ tale che $\{\xi, \xi^q, \ldots, \xi^{q^{m-1}}\}$ è una base per M su $\mathbb{F}_q$.*

Dimostrazione. Per il Teorema 3.5.2 si ha che $L(x) = \prod_{\beta \in M}(x - \beta)$ è un q-polinomio su $\mathbb{F}_q$. Per il Corollario 3.5.9, $L(x)$ ha una radice q-primitiva ξ; inoltre $\xi, \xi^q, \ldots, \xi^{q^{m-1}}$ sono elementi di M. Se per assurdo tali elementi fossero linearmente dipendenti, allora si avrebbe che ξ sarebbe una radice di un polinomio di grado minore del grado di $L(x)$, ovvero $P(x) = c_0\xi + c_1\xi^q + \ldots + c_{m-1}\xi^{q^{m-1}}$, con $c_i \in \mathbb{F}_q$, il che è contraddittorio con l'ipotesi che ξ sia una radice q-primitiva di $L(x)$. Percio $\{\xi, \xi^q, \ldots, \xi^{q^{m-1}}\}$ è una base per M su $\mathbb{F}_q$. □

Considerando l'estensione data da $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ e osservando che $\mathbb{F}_{q^m}$ può essere visto come un q-modulo su $\mathbb{F}_q$, il Teorema 3.6.1 fornisce una seconda dimostrazione del Teorema della Base Normale, il quale dice che ogni estensione finita e quindi ogni spazio vettoriale ammette una base normale.

In quanti modi è possibile scegliere ξ con le proprietà del teorema precedente?

Teorema 3.6.2. *Esistono esattamente $\phi_q(x^m - 1)$ elementi in $\mathbb{F}_{q^m}$ tali che $\{\xi, \xi^q, \ldots, \xi^{q^{m-1}}\}$ sia una base per $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$.*

Dimostrazione. Si può applicare a $\mathbb{F}_{q^m}$ il Teorema 3.6.1 in quanto $\mathbb{F}_{q^m}$ può essere visto come un q-modulo su $\mathbb{F}_q$. Perciò sia

$$L(x) = \prod_{\beta \in \mathbb{F}_{q^m}} (x - \beta) = (x^{q^m} - x),$$

grazie al Lemma 1.3.4. Ogni q-radice primitiva di $L(x)$ su $\mathbb{F}_q$ produce una base del tipo desiderato.

D'altra parte se una radice ξ di $L(x)$ non è una radice q-primitiva su $\mathbb{F}_{q^m}$, allora gli elementi $\xi, \xi^q, \ldots, \xi^{q^{m-1}}$ grazie al ragionamento già mostrato nel Teorema 3.6.1 sono linearmente dipendenti su $\mathbb{F}_q$, dunque non potrebbero

formare una base. Quindi, il numero di $\xi \in \mathbb{F}_{q^m}$, tali che $\{\xi, \xi^q, \ldots, \xi^{q^{m-1}}\}$ sia una base è uguale al numero di radici primitive di $L(x)$, il quale è dato da $\phi_q(x^m - 1)$ per la Proposizione 3.5.7. □

Osservazione 23. Dato che ognuno degli elementi $\xi, \xi^q, \ldots, \xi^{q^{m-1}}$ produce la stessa base normale di $\mathbb{F}_{q^m}$ su $\mathbb{F}_q$, allora il numero di basi normali diverse in realtà è dato da $(1/m)\phi_q(x^m - 1)$.

Esempio 3.1. Sia $\alpha \in \mathbb{F}_8$ una radice del polinomio irriducibile $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Per l'Osservazione 23 si ha che il numero di basi normali di $\mathbb{F}_8$ è dato da $\frac{1}{3}\Phi_2(x^3 - 1)$. Ma, $\Phi_q(f) = q^n(1 - q^{-n_1}) \cdots (1 - q^{-n_r})$ per il Lemma 3.5.6, dove $q = 2$, $n = 3$ e gli n_i sono i gradi dei polinomi monici e irriducibili che intervengono nella fattorizzazione di $x^3 - 1 = (x - 1)(x^2 + x + 1)$ su $\mathbb{F}_2[x]$. Perciò: $n_1 = 1$ e $n_2 = 2$ da cui si ha che $\Phi_2(x^3 - 1) = 3$ ottenendo $\frac{1}{3}\Phi_2(x^3 - 1) = 1$. Perciò l'unica base normale è data in questo caso da

$$\mathcal{A} = \{\alpha, \alpha^2, 1 + \alpha + \alpha^2\},$$

che abbiamo visto nell'Esempio 2.1.

Bibliografia

[1] M. Artin: *Algebra, Second Edition*, Massachusetts Institute of Technology, 2010.

[2] M. Barnabei, F. Bonetti: *Matematica discreta elementare*, Pitagora editrice, Bologna, 2014, 69-73.

[3] D. Cox: *Galois Theory*, Wiley, 2012.

[4] J. Guajardo, C. Paar: *Itoh-Tsujii Inversion in Standard Basis and Its Application in Cryptography and Codes* in *Design, Codes and Cryptography*, Feb 2002, 207-216.

[5] M. Hazewinkel: *Handbook of Algebra , Volume 1, section 1D, capitolo 9,* Elsevier, Amsterdam , 1995.

[6] T. Itoh, S. Tsujii: *A Fast Algorithm for Computing Multiplicative Inverses in GF(2m) using Normal Bases. Information and Computation*, 1988, 78, 171-177.

[7] N. Koblitz: *Elliptic Curve Cryptosystems*, Mathematics of Computation, 1987, 48, 203-209.

[8] N. Koblitz: *Hyperelliptic Cryptosystems*, Journal of Cryptology, 1989, 1(3), 129-150.

[9] R. Lidl, H. Niederrheiter: *Encyclopedia of Mathematics and its Applications, Finite Fields*, Cambridge University Press, 1985.

[10] V. Miller: *Use of Elliptic Curves in Cryptography* in H. C. Williams (ed.): *Advances in Cryptology* - CRYPTO - 85, Lecture Notes in Computer Science Volume 218, Berlin, 1986, 417-428.

[11] J.S. Milne: *Fields and Galois Theory*, 2015.