

Capitolo 4

Campi di Galois

4.1 Generalità sui campi finiti

Nel seguito denoteremo con F_q un campo finito d'ordine q e caratteristica p . In queste ipotesi il sottocampo fondamentale di F_q è isomorfo a Z_p , il campo dei resti modulo l'intero primo p .

PROPOSIZIONE 4.1.1. *Siano F_q un campo finito e $F_{q'}$ un suo sottocampo d'ordine q' . Allora*

(i) *esiste un intero positivo h tale che $|F_q| = q = p^h$;*

(ii) *se $|F_{q'}| = p^{h'}$, h' divide h ;*

(iii) *se h è primo, Z_p è l'unico sottocampo proprio di F_q .*

DIMOSTRAZIONE. È un semplice corollario della prop.3.3.24. □

DEFINIZIONE 4.1.2. Un campo finito F_q prende il nome di *campo di Galois*, e spesso si denota con $GF(q)$, se è estensione algebrica semplice di Z_p , per qualche primo p . □

ESEMPIO 4.1.3. Se $g(x) \in Z_p[x]$ è un polinomio irriducibile su Z_p di grado $h > 1$, allora il campo $Z_p(a)$ estensione algebrica di Z_p mediante l'aggiunta di una radice a di $g(x)$, per la (3.10), è del tipo

$$Z_p(a) = \{m_0 + m_1a + m_2a^2 + \dots + m_{h-1}a^{h-1} : (m_0, m_1, \dots, m_{h-1}) \in Z_p^h\}$$

e quindi $Z_p(a)$ è un campo di Galois d'ordine $q = p^h$.

Per esempio, usando il polinomio $x^2 - x - 1 \in Z_3[x]$ irriducibile su $Z_3 = \{0, 1, -1\}$, possiamo costruire un campo di Galois d'ordine 9

$$GF(9) = \{0, 1, -1, a, -a, 1+a, 1-a, -1+a, -1-a\},$$

ove a ha la proprietà $a^2 - a - 1 = 0$. □

Nel seguito supporremo costantemente $q = p^h$ e denoteremo con F_q^* l'insieme degli elementi non nulli di F_q , cioè il gruppo moltiplicativo di F_q .

ESERCIZIO 4.1.4. *Provare che il gruppo delle trasformazioni affini di F_q (cfr.2.2.13) ha ordine $q(q-1)$.* \square

PROPOSIZIONE 4.1.5. *Denotati con a_1, a_2, \dots, a_{q-1} gli elementi non nulli di F_q , risulta:*

$$a^{q-1} = 1 \quad , \quad \text{per ogni } a \in F_q^*; \quad (4.1)$$

$$a^q = a \quad , \quad \text{per ogni } a \in F_q; \quad (4.2)$$

$$a_1 a_2 \cdots a_{q-1} = -1. \quad (4.3)$$

DIMOSTRAZIONE. La (4.1) é vera perché il gruppo moltiplicativo F_q^* é finito e ha ordine $q-1$. La (4.2) é ovvia conseguenza della (4.1) e assicura che il polinomio $x^q - x$ può essere scritto nella forma

$$x^q - x = x(x - a_1)(x - a_2) \cdots (x - a_{q-1}); \quad (4.4)$$

cosí , uguagliando i coefficienti dei termini di primo grado, si ha

$$(-1)^{q-1} a_1 a_2 \cdots a_{q-1} = a_1 a_2 \cdots a_{q-1} = -1$$

e resta provata anche la (4.3). \square

ESERCIZIO 4.1.6. *Usando la (4.4), provare che la somma di tutti gli elementi di un campo finito d'ordine maggiore di due é uguale a zero.* \square

ESERCIZIO 4.1.7. *Provare che un polinomio del tipo $(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_t) \in F_q$, con $\alpha_1, \alpha_2, \dots, \alpha_t$ elementi a due a due distinti di F_q , é divisibile per $x^q - x$.* \square

OSSERVAZIONE 4.1.8. In un campo finito non vale il principio di identità dei polinomi. La (4.2), infatti, mostra che il polinomio non nullo $x^q - x \in F_q[x]$ ha funzione polinomiale identicamente nulla. \square

PROPOSIZIONE 4.1.9. *Ogni campo finito d'ordine $q = p^h$ é campo di spezzamento del polinomio $x^q - x$ su Z_p . Di conseguenza campi finiti dello stesso ordine sono isomorfi.*

DIMOSTRAZIONE. La prima parte segue dalla (4.4) e dalla definizione di campo di spezzamento. La seconda parte segue dalla prop.3.3.49 . \square

PROPOSIZIONE 4.1.10. *Per ogni primo p e per ogni intero positivo h , esiste un unico campo finito d'ordine $q = p^h$, a meno di isomorfismi.*

DIMOSTRAZIONE. In forza del precedente teorema, basta provare che esiste un campo d'ordine q . A tale scopo, supponiamo $h > 1$, altrimenti Z_p é il campo desiderato e, posto $f(x) = x^q - x$, sia F il campo di spezzamento di $f(x)$ su Z_p . Poiché il polinomio derivato di $f(x)$ é $f'(x) = qx^{q-1} - 1 = -1$, risulta $MCD(f, f') = 1$ e quindi $f(x)$ non possiede radici multiple in una qualsiasi estensione di Z_p . Ne segue che $|F| \geq q$. D'altra parte, se $a, b \in F$ sono radici di $f(x)$, si ha subito che $ab, \frac{a}{b} (b \neq 0)$ e $a \pm b$ sono ancora radici di $f(x)$. Ne segue che le q radici di $f(x)$ formano un sottocampo F_q di F d'ordine q e quindi deve essere $F = F_q$. \square

PROPOSIZIONE 4.1.11. *Per ogni divisore k di h esiste un unico sottocampo di F_q d'ordine p^k .*

DIMOSTRAZIONE. Sia F la chiusura algebrica di Z_p . Allora, per ogni intero positivo t , F contiene il campo di spezzamento di $x^{p^t} - x$ su Z_p , che ha ordine p^t . In particolare F contiene (un sottocampo isomorfo a) F_q ed un sottocampo F_{p^k} d'ordine p^k . Ora, se $h = km$, per ogni elemento $a \in F_{p^k}$ si ha $a^{p^k} = a$ e quindi

$$a^q = a^{p^{km}} = a^{(p^k)^m} = a.$$

Ne segue che $F_{p^k} \subseteq F_q$ e resta provato che F_q contiene almeno un sottocampo d'ordine p^k . Ora, se F' e F'' sono due sottocampi di F_q dello stesso ordine, ragionando come prima, si ottiene $F' \subseteq F''$ e $F'' \subseteq F'$, cioè $F' = F''$. L'asserto é così completamente provato. \square

PROPOSIZIONE 4.1.12. *Sia $L(h)$ l'insieme dei divisori positivi di h con la struttura di reticolo indotta dalla relazione di divisibilità. Il reticolo dei sottocampi di F_q é isomorfo a $L(h)$.*

DIMOSTRAZIONE. Ricordiamo che risulta

$$\sup(n, m) = \text{mcm}(n, m) \quad \text{e} \quad \inf(n, m) = \text{MCD}(n, m),$$

per ogni $m, n \in L(h)$. Allora dalle 4.1.1 e 4.1.11 si ha subito che l'applicazione

$$n \in L(h) \rightarrow F_{p^n} \subseteq F_q$$

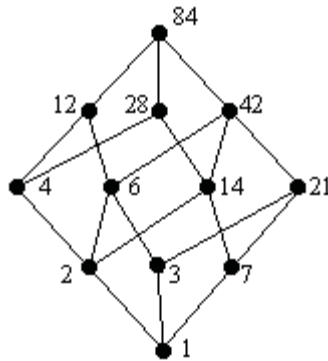
é un isomorfismo di reticoli. \square

ESEMPIO 4.1.13. Il reticolo dei sottocampi di $F_{p^{84}}$, essendo $84 = 2^2 \cdot 3 \cdot 7$, é dato da

$$(\{F_p, F_{p^2}, F_{p^3}, F_{p^4}, F_{p^6}, F_{p^7}, F_{p^{12}}, F_{p^{14}}, F_{p^{21}}, F_{p^{28}}, F_{p^{42}}, F_{p^{84}}\}, \leq)$$

ove $F_{p^i} \leq F_{p^j}$ se, e soltanto se, i divide j . Tale reticolo é dunque isomorfo a quello dei divisori positivi di 84, che ha il seguente diagramma di Hasse:

Figura 4.1: Il Reticolo dei sottocampi di $GF(84)$



\square

Ricordiamo che l'ordine o periodo $o(a)$ di un elemento $a \in F_q^*$ é l'ordine che ha a come elemento del gruppo moltiplicativo F_q^* , cioè é il piú piccolo intero positivo m tale che $a^m = 1$. Inoltre, se $a^n = 1$ per un intero n , allora m deve dividere n .

PROPOSIZIONE 4.1.14. (teorema dell'elemento primitivo) *Il gruppo moltiplicativo F_q^* di F_q é ciclico, esiste cioè un elemento $g \in F_q^*$ di periodo $q - 1$.*

DIMOSTRAZIONE. Supponiamo $q - 1 > 2$, altrimenti l'asserto é banale, e sia

$$q - 1 = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$$

la decomposizione di $q - 1$ in fattori primi. Per ogni $i = 1, 2, \dots, t$, denotiamo con a_i un elemento di F_q^* tale che

$$a_i^{\frac{q-1}{p_i}} \neq 1$$

e poniamo

$$b_i = a_i^{\frac{q-1}{p_i^{r_i}}}.$$

L'esistenza degli elementi a_i é assicurata dal fatto che é $\frac{q-1}{p_i} < q - 1 = |F_q^*|$ e il polinomio

$$x^{\frac{q-1}{p_i}} - 1$$

ha al piú $\frac{q-1}{p_i}$ radici distinte in F_q^* . Ora, essendo

$$b_i^{p_i^{r_i}} = a_i^{q-1} = 1,$$

il periodo di b_i deve essere un divisore di $p_i^{r_i}$ e quindi é del tipo $p_i^{s_i}$, con

$$0 < s_i \leq r_i.$$

D'altra parte, avendosi

$$b_i^{p_i^{(r_i-1)}} = a_i^{\frac{q-1}{p_i}} \neq 1,$$

deve essere $s_i = r_i$ e cioè l'intero $p_i^{r_i}$ é il periodo dell'elemento b_i .

A questo punto proviamo che l'elemento

$$g = b_1 b_2 \cdots b_t$$

ha periodo $o(g) = q - 1$.

Se, per assurdo, supponiamo che $o(g)$ sia un divisore proprio di $q - 1$, esiste almeno un indice j per cui $o(g)$ divide $\frac{q-1}{p_j}$ e quindi risulta

$$g^{\frac{q-1}{p_j}} = b_1^{\frac{q-1}{p_j}} b_2^{\frac{q-1}{p_j}} \cdots b_t^{\frac{q-1}{p_j}} = 1.$$

D'altra parte, per ogni indice $i \neq j$, l'intero $p_i^{r_i} = o(b_i)$ divide $\frac{q-1}{p_j}$ e così é

$$b_i^{\frac{q-1}{p_j}} = 1$$

e quindi

$$b^{\frac{q-1}{p_j}} = b_j^{\frac{q-1}{p_j}} = 1.$$

Dall'ultima uguaglianza segue che il periodo $p_j^{r_j}$ di b_j divide $\frac{q-1}{p_j}$ e ciò é assurdo. Ne segue che g ha ordine $q-1$ e cioè che F_q^* é ciclico. \square

DEFINIZIONE 4.1.15. Un elemento $g \in F_q^*$ di periodo $q-1$ prende il nome di *elemento primitivo* o *radice primitiva* di F_q . \square

ESERCIZIO 4.1.16. *Provare che un elemento primitivo $g \in F_q$ non appartiene ad alcun sottocampo proprio di F_q .* \square

ESERCIZIO 4.1.17. *Trovare gli elementi primitivi di $GF(9)$ (cfr. 4.1.3).* \square

PROPOSIZIONE 4.1.18. F_q é estensione algebrica semplice di ogni suo sottocampo $F_{q'}$. Inoltre, per ogni intero positivo n , esiste un polinomio di grado n in $F_q[x]$ irriducibile su F_q . Ne segue che ogni campo finito é un campo di Galois.

DIMOSTRAZIONE. Se g é un elemento primitivo di F_q si ha $F_{q'}(g) = F_q$ e cioè la prima parte della proposizione. Analogamente, se c é un elemento primitivo del campo F_{q^n} d'ordine q^n , risulta $F_q(c) = F_{q^n}$. Allora, il polinomio minimo di c su F_q é di grado n , a coefficienti in F_q ed ivi irriducibile e l'asserto é completamente provato. \square

PROPOSIZIONE 4.1.19. *Sia $g(x) \in F_q[x]$ un polinomio irriducibile su F_q e a una sua radice in una estensione di F_q . Allora, se $h(x) \in F_q[x]$, risulta $h(a) = 0$ se, e soltanto se, $g(x)$ divide $h(x)$.*

DIMOSTRAZIONE. Detti n il grado di $g(x)$ e a_0 il suo coefficiente direttore, il polinomio $m(x) = a_0^{-1}g(x)$ é il polinomio minimo di a su F_q . Ne segue che $h(a) = 0$ se, e soltanto se, $m(x)$, e quindi $g(x)$, divide $h(x)$. \square

PROPOSIZIONE 4.1.20. *Un polinomio $g(x) \in F_q[x]$ irriducibile su F_q divide $x^{q^k} - x$, con k intero positivo, se, e soltanto se, il grado n di $g(x)$ divide k .*

DIMOSTRAZIONE. Nell'ipotesi che $g(x)$ divida $x^{q^k} - x$, denotiamo con a una radice di $g(x)$ in qualche estensione di F_q e osserviamo che, essendo $a^{q^k} = a$, risulta $a \in F_{q^k}$. Si ha allora che $F_q(a)$ é un sottocampo di F_{q^k} e

$$\dim_{F_q} F_{q^k} = k \quad , \quad \dim_{F_q} F_q(a) = n$$

onde, tenendo conto della prop.4.1.12, abbiamo che n divide k .

Viceversa, nell'ipotesi che n divida k , abbiamo ancora per la prop.4.1.12 che F_{q^n} é sottocampo di F_{q^k} e, detta a una radice di $g(x)$ in una estensione di F_q , risulta $F_q(a) = F_{q^n}$. Ne segue che, essendo $a \in F_{q^n} \subseteq F_{q^k}$, a é una radice di $x^{q^k} - x$ e quindi $g(x)$ divide $x^{q^k} - x$, come volevamo dimostrare. \square

PROPOSIZIONE 4.1.21. Sia $g(x) \in F_q[x]$ un polinomio di grado n irriducibile su F_q . Se a é una radice di $g(x)$ in una estensione di F_q , risulta:

- (i) tutte le radici di $g(x)$ sono semplici;
- (ii) gli elementi $a, a^q, a^{q^2}, \dots, a^{q^{n-1}}$ sono tutte e sole le radici di $g(x)$;
- (iii) F_{q^n} é il campo di spezzamento di $g(x)$ su F_q .

DIMOSTRAZIONE. Posto $g(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ e tenendo presente che tutti gli a_j appartengono ad F_q , per ogni intero positivo t , risulta

$$g(a^{q^t}) = a_0a^{nq^t} + a_1a^{(n-1)q^t} + \dots + a_{n-1}a^{q^t} + a_n =$$

$$a_0^t a^{nq^t} + a_1^t a^{(n-1)q^t} + \dots + a_{n-1}^t a^{q^t} + a_n^t = g(a)^{q^t} = 0.$$

Resta cosí provato che a^{q^t} é una radice di $g(x)$, per ogni intero positivo t . Allora, per ottenere (i) e (ii), basta provare che, se $0 < s < t < n$, risulta $a^{q^s} \neq a^{q^t}$. In queste ipotesi, se assumiamo $a^{q^s} = a^{q^t}$, essendo $a \in F_q(a) = F_{q^n}$, abbiamo

$$(a^{q^s})^{q^{n-t}} = (a^{q^t})^{q^{n-t}} \Rightarrow a^{q^{n-t+s}} = a^{q^n} = a.$$

Quindi $g(x)$ divide $x^{q^{n-t+s}} - x$ in forza di 4.1.19 e ció, per la 4.1.20, accade solo se n divide $n + s - t$, il che é evidentemente assurdo.

Infine, da $F_q(a) = F_{q^n}$ e dalle (i) e (ii), abbiamo

$$F_q(a) = F_q(a, a^q, \dots, a^{q^{n-1}}) = F_{q^n},$$

cioé la (iii). □

DEFINIZIONE 4.1.22. Per ogni elemento $a \in F_{q^n}$, gli elementi $a, a^q, a^{q^2}, \dots, a^{q^{n-1}}$ prendono il nome di *coniugati di a* rispetto ad F_q , o *q -coniugati di a* . □

ESERCIZIO 4.1.23. Tenendo presente l'ultima proposizione, provare che i q -coniugati di un elemento $a \in F_{q^n}$ sono fra loro distinti se, e soltanto se, il polinomio minimo di a su F_q ha grado n . □

DEFINIZIONE 4.1.24. Un campo F si dice *perfetto* se ogni polinomio a coefficienti in F ed ivi irriducibile ha tutte le radici semplici nel suo campo di spezzamento su F . Inoltre, un'estensione F' di F si dice *normale* se contiene il campo di spezzamento di ogni polinomio $f(x) \in F[x]$ irriducibile su F e avente almeno una radice in F' . □

La proposizione 4.1.21 assicura che vale il seguente teorema.

PROPOSIZIONE 4.1.25. Ogni campo finito F_q é perfetto. Inoltre, F_{q^n} é estensione normale di F_q .

4.2 Automorfismi

Cominciamo col ricordare alcune definizioni relative alle estensioni di campi.

DEFINIZIONE 4.2.1. Se F' é un'estensione di un campo F , un automorfismo f di F' prende il nome di F -*automorfismo* se $f(a) = a$, per ogni elemento $a \in F$. Gli F -automorfismi di F' formano un gruppo, che si chiama *gruppo di Galois* di F' su F e si denota con $G(F' : F)$. Il campo F' si dice *estensione di Galois* di F se, per ogni $a \in F' \setminus F$, esiste un F -automorfismo $f \in G(F' : F)$ tale che $f(a) \neq a$. In altre parole, F' é estensione di Galois di F se accade che il sottocampo di F' costituito da tutti gli elementi di F' uniti in ogni F -automorfismo é esattamente F .

Quando é $F' = F_{q^n}$ e $F = F_q$, un F_q -automorfismo di F' si dice anche q -*automorfismo*. \square

PROPOSIZIONE 4.2.2. Per ogni intero positivo r , l'applicazione

$$f_r = f_r^{(q,n)} : a \in F_{q^n} \rightarrow a^{q^r} \in F_{q^n} \quad (4.5)$$

é un q -*automorfismo*. Inoltre, per $0 < r < s < n$, risulta $f_r \neq f_s$.

DIMOSTRAZIONE. E' chiaro che f_r é un endomorfismo di F_{q^n} , avendosi

$$f_r(ab) = f_r(a)f_r(b) \quad , \quad (a+b)^{q^r} = a^{q^r} + b^{q^r} \quad ,$$

per ogni $a, b \in F_{q^n}$. Ora, nell'ipotesi $a^{q^r} = b^{q^r}$, abbiamo

$$0 = a^{q^r} - b^{q^r} = (a-b)^{q^r} \quad ,$$

quindi $a = b$ e f_r é iniettivo. Inoltre, essendo F_{q^n} finito, f_r risulta anche suriettivo e cosí é un automorfismo. Infine, risultando

$$a \in F_q \Rightarrow a^q = a \Rightarrow a^{q^r} = a \Rightarrow f_r(a) = a \quad ,$$

si ha la prima parte dell'asserto. La seconda parte é di facile verifica. \square

DEFINIZIONE 4.2.3. L'automorfismo f_r definito dalla (4.5) prende il nome di r -*esimo automorfismo di Frobenius* di F_{q^n} su F_q . \square

PROPOSIZIONE 4.2.4. Il gruppo dei q -*automorfismi* di F_{q^n} é ciclico d'ordine n ed é generato da f_1 . Inoltre, F_{q^n} é estensione di Galois di F_q .

DIMOSTRAZIONE. Per ottenere la prima parte dell'asserto, tenendo presente la proposizione precedente e il fatto che $f_r = (f_1)^r$, per ogni intero r tale che $0 < r < n$, dobbiamo soltanto provare che, se f é un q -*automorfismo*, allora esso é di Frobenius. In queste ipotesi, se

$$m(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in F[x]$$

é il polinomio minimo su F_q di un elemento primitivo g di F_{q^n} , essendo

$$\begin{aligned} m(f(g)) &= f(g)^n + a_1f(g)^{n-1} + \cdots + a_{n-1}f(g) + a_n \\ &= f(g)^n + f(a_1)f(g)^{n-1} + \cdots + f(a_{n-1})f(g) + f(a_n) \\ &= f(g^n + a_1g^{n-1} + \cdots + a_{n-1}g + a_n) \\ &= f(0) = 0, \end{aligned}$$

abbiamo che $f(g)$ é a sua volta una radice di $m(x)$. Allora, dalla (ii) di 4.1.21 segue che esiste un intero r , $0 < r < n$, tale che

$$f(g) = g^{q^r},$$

da cui si ha subito

$$f(a) = a^{q^r}, \text{ per ogni } a \in F_{q^n},$$

cioé $f = f_r$. La seconda parte segue dal fatto che $f_1(a) \neq a$, per ogni elemento $a \in F_{q^n} \setminus F_q$. \square

COROLLARIO 4.2.5. *Il gruppo $\text{Aut}(F_q)$ di tutti gli automorfismi di F_q é ciclico d'ordine h ed é generato dal primo automorfismo di Frobenius di F_q sul proprio sottocampo fondamentale Z_p , cioé $\text{Aut}(F_q) = G(F_q : Z_p)$. Inoltre, F_q é estensione di Galois di ogni suo sottocampo.*

DIMOSTRAZIONE. Segue dalla proposizione precedente e dal fatto che ogni automorfismo di un campo fissa tutti gli elementi del sottocampo fondamentale. \square

ESERCIZIO 4.2.6. *Un automorfismo σ di F_q si dice involutorio se é a quadrato identico, cioé $\sigma^2 = 1$. Provare che F_q ammette un automorfismo involutorio se, e solo se, q é una potenza pari p^{2t} della sua caratteristica p ; in questo caso σ é definito da*

$$\sigma : a \in F_q \rightarrow a^{p^t} \in F_q$$

ed é univocamente determinato. \square

Avvertiamo il lettore che a volte, se σ é un automorfismo di F_q e a un elemento di F_q , useremo la notazione esponenziale a^σ per denotare l'immagine $\sigma(a)$ di a in σ .

4.3 Radici dell'unitá e potenze

Per ogni intero positivo m , denotiamo con F_q^{*m} l'insieme degli elementi di F_q^* che sono potenze m -esime di elementi non nulli di F_q . Inoltre, denotiamo con $G(m)$ l'insieme delle radici m -esime dell'unitá di F_q . Poniamo cioé

$$F_q^{*m} = \{a \in F_q^* : a = b^m \text{ con } b \in F_q^*\}$$

e

$$G_q(m) = \{a \in F_q^* : a^m = 1\}.$$

PROPOSIZIONE 4.3.1. *Siano g un elemento primitivo di F_q , m un intero positivo e $d = \text{MCD}(q-1, m)$. Allora F_q^{*m} é un sottogruppo ciclico di F_q^* d'ordine $\frac{q-1}{d}$ e generato da g^d , inoltre risulta $F_q^{*m} = F_q^{*d}$. Analogamente, $G_q(m)$ é un sottogruppo ciclico di F_q^* d'ordine d e generato da $g^{\frac{q-1}{d}}$, inoltre risulta $G_q(m) = G_q(d)$.*

DIMOSTRAZIONE. Per ogni intero n , l'applicazione

$$u_n : a \in F_q^* \rightarrow a^n \in F_q^*$$

é un omomorfismo di gruppi tale che

$$\text{Ker}(u_n) = G_q(n) \quad , \quad \text{Im}(u_n) = F_q^{*n};$$

ne segue che $G_q(n)$ e F_q^{*n} sono sottogruppi di F_q^* . Ora, essendo $d = \text{MCD}(q-1, m)$, esistono due interi relativi k e t tali che $d = k(q-1) + tm$ e quindi, se $a^m = 1$, abbiamo

$$a^d = a^{k(q-1)+tm} = a^{k(q-1)} a^{tm} = (a^{q-1})^k (a^m)^t = 1,$$

cioé $\text{Ker}(u_m) \subseteq \text{Ker}(u_d)$. D'altra parte, se $a^d = 1$, posto $m = db$, abbiamo

$$a^m = a^{db} = (a^d)^b = 1,$$

cioé $\text{Ker}(u_d) \subseteq \text{Ker}(u_m)$, e quindi $\text{Ker}(u_d) = \text{Ker}(u_m)$.

L'ultima uguaglianza assicura che le immagini di u_m e u_d hanno lo stesso ordine e, essendo $\text{Im}(u_m) \subseteq \text{Im}(u_d)$, esse devono coincidere. A questo punto é immediato rendersi conto che é

$$\text{Im}(u_m) = \text{Im}(u_d) = \langle g^d \rangle \quad , \quad \text{Ker}(u_m) = \text{Ker}(u_d) = \langle g^{\frac{q-1}{d}} \rangle$$

e l'asserto é provato. □

ESERCIZIO 4.3.2. Siano m un intero positivo e $d = \text{MCD}(q-1, m)$. Provare che un elemento $a \in F_q^*$ é la potenza m -esima di qualche elemento di F_q^* se, e soltanto se, $a^{\frac{q-1}{d}} = 1$. □

ESERCIZIO 4.3.3. Provare che, se q é pari, ogni elemento di F_q^* é il quadrato di un unico elemento di F_q^* . Provare inoltre che, se q é dispari, ogni elemento quadrato di F_q^* é il quadrato di esattamente due elementi di F_q^* e quindi il numero dei quadrati non nulli é $\frac{q-1}{2}$. □

ESERCIZIO 4.3.4. Sia q dispari. Provare che in F_q l'inverso di un quadrato non nullo é un quadrato, il prodotto di due quadrati o di due non quadrati é un quadrato, il prodotto di un quadrato non nullo e di un non quadrato é un non quadrato. □

ESERCIZIO 4.3.5. Provare che un qualsiasi elemento di F_q ammette una, ed una sola, radice p -esima. □

ESERCIZIO 4.3.6. Sia $m > 1$ un intero che divide $q-1$. Provare che F_q contiene esattamente m radici m -esime dell'unitá. Dette a_1, a_2, \dots, a_m tali radici, provare che

$$(-1)^m a_1 a_2 \cdots a_m = -1 \quad e \quad a_1 + a_2 + \cdots + a_m = 0.$$

□

PROPOSIZIONE 4.3.7. Sia q dispari. Allora -1 é un quadrato in F_q se, e soltanto se, risulta $q \equiv 1 \pmod{4}$.

DIMOSTRAZIONE. Sia g un elemento primitivo di F_q . Se $q \equiv 1 \pmod{4}$, cioé $q = 4n + 1$, risulta

$$1 = g^{q-1} = g^{4n},$$

cioé

$$(g^{2n} - 1)(g^{2n} + 1) = 0$$

e, avendo g periodo $q - 1 = 4n$ in F_q^* , deve essere

$$g^{2n} = (g^n)^2 = -1,$$

il che significa che -1 é un quadrato in F_q .

Se $q \not\equiv 1 \pmod{4}$, allora é $q \equiv 3 \pmod{4}$, cioè $q = 4n + 3$ e abbiamo

$$1 = g^{q-1} = g^{4n+2} = (g^{2n+1})^2.$$

Essendo $g^{2n+1} \neq 1$, dalla 4.3.3 ricaviamo $g^{2n+1} = -1$, cioè -1 non é un quadrato in F_q e l'asserto é provato. \square

PROPOSIZIONE 4.3.8. *Se m é un intero positivo e poniamo*

$$S_m = \sum_{b \in F_q} b^m,$$

risulta

$$S_m = \begin{cases} -1 & \text{se } m \text{ é divisibile per } q-1 \\ 0 & \text{altrimenti} \end{cases}. \quad (4.6)$$

DIMOSTRAZIONE. Se $d = MCD(q-1, m)$, abbiamo $S_d = S_m$, cosí non é restrittivo supporre $m \leq q-1$. Inoltre, essendo $S_{q-1} = -1$ (cfr.(4.1)), possiamo supporre $m < q-1$ e quindi $q \neq 2$. In queste ipotesi, il gruppo $G_q(m)$ delle radici m -esime dell' unitá di F_q ha ordine $d = MCD(q-1, m) < q-1$ (cfr. 4.3.1) e quindi esiste in F_q^* un elemento c tale che $c^m \neq 1$. Allora, poiché la funzione $b \in F_q \rightarrow cb \in F_q$ é biunivoca, possiamo scrivere

$$S_m = \sum_{b \in F_q} b^m = \sum_{b \in F_q} (cb)^m = c^m \sum_{b \in F_q} b^m = c^m S_m,$$

cioé

$$(c^m - 1)S_m = 0.$$

Essendo $c^m - 1 \neq 0$, ne segue che $S_m = 0$ e l'asserto é provato. \square

OSSERVAZIONE 4.3.9. Notiamo che, se per convenzione si pone $0^0 = 0$, la (4.6) continua a valere anche nel caso $m = 0$. \square

Se m é un intero positivo, denotiamo con $F_q^{(m)}$ l'insieme degli elementi di F_q che risultano somma di potenze m -esime; poniamo cioè

$$F_q^{(m)} = \{a_1^m + a_2^m + \cdots + a_n^m \quad : \quad a_i \in F_q, \quad m \in \mathbb{N}^+\}.$$

PROPOSIZIONE 4.3.10. *Per ogni intero positivo m , $F_q^{(m)}$ é un sottocampo di F_q .*

DIMOSTRAZIONE. E' chiaro che $F_q^{(m)}$ é chiuso rispetto alla somma e al prodotto e che contiene 0 e 1. Inoltre, per ogni $a \in F_q^{(m)}$ con $a \neq 0$, risulta

$$a^{-1} = a^{m-1}(a^{-1})^m$$

e, poiché a^{m-1} e $(a^{-1})^m$ appartengono a $F_q^{(m)}$, si ha che a^{-1} é un elemento di $F_q^{(m)}$. Infine, avendosi anche $-1 = (p-1)1^m \in F_q^{(m)}$, si ha l'asserto. \square

PROPOSIZIONE 4.3.11. *Sia G un sottogruppo di F_q^* . Condizione necessaria e sufficiente affinché G sia il gruppo moltiplicativo di un sottocampo di F_q é che l'ordine di G sia del tipo $p^l - 1$, con l divisore di h .*

DIMOSTRAZIONE. E' chiaro che, se G é il gruppo moltiplicativo di un sottocampo di F_q , l'ordine di G deve essere del tipo $p^l - 1$, con l divisore di h .

D'altra parte, poiché F_q^* é ciclico d'ordine $q-1$, i suoi sottogruppi sono in corrispondenza biunivoca con i divisori positivi di $q-1$. Ne segue che, se $|G| = p^l - 1$ e l divide h , allora G deve necessariamente coincidere col gruppo moltiplicativo del sottocampo F_{p^l} di F_q . \square

PROPOSIZIONE 4.3.12. *Siano m un intero positivo e $d = \text{MCD}(q-1, m)$. Sia inoltre $q^* = p^l$ la piú piccola potenza di p tale che*

(i) l divide h ;

(ii) $\frac{p^h-1}{p^l-1}$ divide m .

Allora valgono le seguenti proprietà:

(j) $F_q^{(m)}$ coincide con l'unico sottocampo F_{q^*} di F_q d'ordine q^* ;

(jj) ogni elemento di $F_q^{(m)}$ può essere scritto come somma di al piú d potenze m -esime di elementi di F_q .

4.4 Le funzioni traccia e norma

Sia F_{q^m} una estensione di F_q di grado m e, per ogni $a \in F_{q^m}$, poniamo

$$T_r(a) = a + a^q + a^{q^2} + \dots + a^{q^{m-1}},$$

$$N(a) = aa^q a^{q^2} \dots a^{q^{m-1}} = a^{(q^m-1)/(q-1)}.$$

Poiché risulta $(T_r(a))^q = T_r(a)$ e $(N(a))^q = N(a)$, si ha che $T_r(a)$ e $N(a)$ sono elementi di F_q .

DEFINIZIONE 4.4.1. Le funzioni

$$T_r : a \in F_{q^m} \rightarrow T_r(a) \in F_q$$

e

$$N : a \in F_{q^m} \rightarrow N(a) \in F_q$$

prendono rispettivamente il nome di *traccia* e *norma* di F_{q^m} su F_q . La traccia e la norma di un campo finito F sul proprio sottocampo fondamentale si chiamano rispettivamente *traccia assoluta* e *norma assoluta* di F .

OSSERVAZIONE 4.4.2. Per ogni $a \in F_{q^m}$, la funzione

$$t_a : x \in F_{q^m} \rightarrow ax \in F_{q^m}$$

é un endomorfismo di F_{q^m} considerato come spazio vettoriale su F_q . Si può provare che la traccia e la norma di t_a sono rispettivamente uguali a $T_r(a)$ e $N(a)$. \square

PROPOSIZIONE 4.4.3. *L'applicazione traccia é suriettiva. Inoltre, se $a \in F_{q^m}$, risulta $T_r(a) = 0$ se, e soltanto se, esiste un elemento $b \in F_{q^m}$ tale che $a = b^q - b$.*

DIMOSTRAZIONE. Se pensiamo F_{q^m} come spazio vettoriale su F_q , si vede facilmente che T_r risulta una forma lineare il cui nucleo $Ker(T_r)$ coincide con le radici in F_{q^m} del polinomio

$$x + x^q + x^{q^2} + \dots + x^{q^{m-1}}.$$

Poiché tale polinomio ha al più q^{m-1} radici in F_{q^m} , il funzionale T_r é non nullo, quindi é suriettivo e il suo nucleo ha dimensione $m - 1$.

Osserviamo ora che l'insieme

$$S = \{b^q - b : b \in F_{q^m}\}$$

é un sottospazio vettoriale di F_{q^m} e che, essendo $T_r(b^q) = T_r(b)$ per ogni $b \in F_{q^m}$, risulta $S \subseteq Ker(T_r)$. D'altra parte, l'applicazione

$$b \in F_{q^m} \rightarrow b^q - b \in F_{q^m}$$

é lineare, ha per immagine S e per nucleo F_q . Ne segue che S ha dimensione $m - 1$, cioè la stessa dimensione di $Ker(T_r)$; quindi $S = Ker(T_r)$ e l'asserto é completamente provato. \square

PROPOSIZIONE 4.4.4. *L'applicazione norma é suriettiva. Inoltre, se $a \in F_{q^m}$, risulta $N(a) = 1$ se, e soltanto se, esiste un elemento $b \in F_{q^m}$ tale che $a = b^{q-1}$.*

DIMOSTRAZIONE. Osserviamo che la restrizione N^* di N a $F_{q^m}^*$ é un omomorfismo fra i gruppi $F_{q^m}^*$ e F_q^* e, in forza della 4.3.1, si ha

$$|Ker(N^*)| = MCD(q^m - 1, \frac{q^m - 1}{q - 1}) = \frac{q^m - 1}{q - 1},$$

$$|Im(N^*)| = \frac{q^m - 1}{(q^m - 1)/(q - 1)} = q - 1 = |F_q^*|,$$

cosí N é suriettiva. D'altra parte, essendo $N(b^{q-1}) = b^{(q^m-1)} = 1$ per ogni $b \in F_{q^m}^*$, per competare l'asserto basta provare che il sottogruppo di F_q^*

$$S' = \{b^{q-1} : b \in F_q^*\}$$

ha ordine $\frac{q^m-1}{q-1}$. A tale scopo osserviamo che l'applicazione

$$b \in F_{q^m}^* \rightarrow b^{q-1} \in F_q^*$$

é un endomorfismo di $F_{q^m}^*$ che ha per immagine S' e nucleo F_q^* . Ne segue che S' ha ordine $\frac{q^m-1}{q-1}$ e cioè l'asserto. \square