Teoremi rilevanti sui campi finiti

§1.1 Campo di spezzamento di un irriducibile in $\mathbb{F}_p$

Teorema 1.1.1

Sia $f(x)$ un polinomio irriducibile in $\mathbb{F}_p$ e sia n il suo grado. Allora $\mathbb{F}_{p^n}$ è il suo campo di spezzamento.

Dimostrazione. Dacché $f(x)$ è irriducibile, $\mathbb{F}_p/((f(x))$ è un campo con p^n elementi, ed è quindi isomorfo a $\mathbb{F}_{p^n}$.

Sia $\alpha = x + (f(x))$ una radice di $f(x)$ in $\mathbb{F}_{p^n}$. Dal momento che $f(x)$ è irriducibile in $\mathbb{F}_p$, esso è il polinomio minimo di α. Tuttavia, poiché $\alpha \in \mathbb{F}_{p^n}$, α è anche radice di $x^{p^n} - x$. Pertanto si deduce che $f(x)$ divide $x^{p^n} - x$.

Dunque, poiché $x^{p^n} - x$ in $\mathbb{F}_{p^n}$ è prodotto di fattori lineari, tutte le radici di $f(x)$ sono già in $\mathbb{F}_{p^n}$.

Inoltre, $\mathbb{F}_{p^n}$ è il più piccolo sottocampo contenente α, dacché $\mathbb{F}_{p^n} \cong \mathbb{F}_p/(f(x)) \cong \mathbb{F}_p(\alpha)$. Quindi si deduce che $\mathbb{F}_{p^n}$ è un campo di spezzamento per $f(x)$, ossia la tesi. □

Lemma 1.1.2

Sia $f(x)$ un irriducibile di grado n su $\mathbb{F}_p[x]$ e sia α una sua radice in $\mathbb{F}_{p^n}$. Allora $f(\mathcal{F}^k(\alpha)) = 0$, $\forall\, k \geq 0$ [a].

[a] $\mathcal{F}$ è l'omomorfismo di Frobenius, definito come $\mathcal{F} : \mathbb{F}_p \to \mathbb{F}_p$, $a \mapsto a^p$.

Dimostrazione. Sia $f(x) = a_n x^n + \ldots + a_0$ a coefficienti in $\mathbb{F}_p$. Si dimostra la tesi applicando il principio di induzione su k.

(*passo base*) $f(\mathcal{F}^0(\alpha)) = f(\alpha) = 0$.

(*passo induttivo*) Per l'ipotesi induttiva, $f(\mathcal{F}^{k-1}(\alpha)) = 0$. Allora, si verifica algebricamente che:

$$f(\mathcal{F}^k(\alpha)) = a_n(\mathcal{F}^k(\alpha))^n + \ldots + a_0 = \mathcal{F}(a_n)\mathcal{F}((\mathcal{F}^{k-1}(\alpha))^n) + \ldots + \mathcal{F}(a_0) = \mathcal{F}(f(\mathcal{F}^{k-1}(\alpha))) = \mathcal{F}(0) = 0,$$

dove si è usato che $\mathcal{F}(a_i) = a_i$, $\forall\, 0 \leq i \leq n$, dacché ogni elemento di $\mathbb{F}_p$ è radice di $x^p - x$. □

Teorema 1.1.3

Sia $f(x)$ un irriducibile di grado n su $\mathbb{F}_p[x]$ e sia α una sua radice in $\mathbb{F}_{p^n}$. Allora vale la seguente fattorizzazione in $\mathbb{F}_{p^n}$:

$$f(x) = \prod_{i=0}^{n-1} \left(x - \alpha^{p^i}\right) = \prod_{i=0}^{n-1} \left(x - \mathcal{F}^i(\alpha)\right),$$

dove ogni fattore non è associato.

Dimostrazione. Si verifica innanzitutto che vale chiaramente che $\alpha^{p^i} = \mathcal{F}^i(\alpha)$. Dal momento che α è radice, allora ogni α^{p^i} lo è, per il *Lemma 1.1.2*.

Affinché tutti i fattori della moltiplicazione non siano associati è sufficiente dimostrare che n è il più piccolo esponente j per cui $\mathcal{F}^j(\alpha) = \alpha$. Infatti, siano $\mathcal{F}^i(\alpha) = \mathcal{F}^j(\alpha)$ con $0 \leq j < i < n$, allora, applicando più volte $\mathcal{F}$, si ricava che:

$$\mathcal{F}^n(\alpha) = \mathcal{F}^{j+n-i}(\alpha) \implies \mathcal{F}^{j+n-i}(\alpha) = \alpha,$$

che è assurdo, dacché $j < i < n \implies j + n - i < n$, ↯.

Innanzitutto, si verifica che $\mathcal{F}^n(\alpha) = \alpha^{p^n} = \alpha$, dacché $\alpha \in \mathbb{F}_{p^n}$. Infine, sia t il più piccolo esponente j per cui $\mathcal{F}^j(\alpha) = \alpha$. Se j fosse minore di n, α sarebbe radice di $x^{p^t} - x$. Tuttavia questo è assurdo, dal momento che così α apparterrebbe a $\mathbb{F}_{p^t} \neq \mathbb{F}_{p^n}$, quando invece il più piccolo campo che lo contiene è $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_{p^n}$, ↯. □

§1.2 L'inclusione $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ e il polinomio $x^{p^n} - x$

Lemma 1.2.1

Sia α una radice di $x^{p^d} - x$ con $d \mid n$. Allora α è anche una radice di $x^{p^n} - x$.

Dimostrazione. Sia $s \in \mathbb{N}$ tale che $n = ds$. Si verifica la tesi applicando il principio di induzione su $k \in \mathbb{N}$.

(*passo base*) Per ipotesi, $\alpha^{p^d} = \alpha$.

(*passo induttivo*) Per ipotesi induttiva, $\alpha^{p^{(k-1)d}} = \alpha$. Allora si ricava che:

$$\alpha^{p^{(k-1)d}} = \alpha \implies \alpha^{p^{kd}} = \alpha^{p^d} = \alpha.$$

In particolare, $\alpha^{p^n} = \alpha^{p^{ds}} = \alpha$, da cui la tesi.

□

Teorema 1.2.2

$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ se e solo se $m \mid n$.

Dimostrazione. Si dimostrano le due implicazioni separatamente.

($\implies$) Dal momento che $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, si ricava la seguente catena di estensioni:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n},$$

dalla quale, applicando il *Teorema delle Torri Algebriche*, si desume la seguente equazione:

$$\underbrace{[\mathbb{F}_{p^n} : \mathbb{F}_p]}_{n} = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \underbrace{[\mathbb{F}_{p^m} : \mathbb{F}_p]}_{d},$$

e quindi che m divide n.

($\impliedby$) Sia $m \mid n$. Si consideri $\alpha \in \mathbb{F}_{p^m}$. α è sicuramente radice di $x^{p^m} - x$, e poiché m divide n, è anche radice di $x^{p^n} - x$, per il *Lemma 1.2.1*. Allora α appartiene al campo di spezzamento di $x^{p^n} - x$ su $\mathbb{F}_p$, ossia $\mathbb{F}_{p^n}$. Pertanto $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

□

Corollario 1.2.3

$\forall\, 1 \leq i \leq n$. Allora, detta m_i il grado di $g_i(x)$, il campo di spezzamento di $f(x)$ è $\mathbb{F}_{p^k}$, dove $k = \mathrm{mcm}(m_1, m_2, \ldots, m_n)$.

Dimostrazione. Il campo di spezzamento di $f(x)$ è il più piccolo campo rispetto all'inclusione che ne contenga tutte le radici, ossia il più piccolo campo che contenga $\mathbb{F}_{p^{m_1}}$, $\mathbb{F}_{p^{m_2}}$, $\ldots$, $\mathbb{F}_{p^{m_n}}$. Si dimostra che tale campo è proprio $\mathbb{F}_{p^k}$.

Innanzitutto $\mathbb{F}_{p^k}$, per il *Teorema 1.2.2*, contiene tutti i campi di spezzamento dei fattori irriducibili di $f(x)$, dacché m_i divide k $\forall\, 1 \leq i \leq n$.

Sia supponga esista adesso un altro campo $\mathbb{F}_{p^t} \subseteq \mathbb{F}_{p^k}$ con tutte le radici. Sicuramente $t \mid k$, per il *Teorema 1.2.2*. Inoltre, dal momento che dovrebbe includere ogni campo $\mathbb{F}_{p^{m_i}}$, sempre per il *Teorema 1.2.2*, m_i divide t $\forall\, 1 \leq i \leq n$.

Allora t è un multiplo comune di tutti i m_i, e quindi k, in quanto minimo comune multiplo, lo divide. Si conclude allora che $t = k$, e quindi che $\mathbb{F}_{p^k}$ è un campo di spezzamento di $f(x)$. □

Teorema 1.2.4

$x^{p^n} - x$ è il prodotto di tutti i polinomi irriducibili in $\mathbb{F}_p$ di grado divisore di n.

Dimostrazione. La proposizione è equivalente a affermare che ogni polinomio irriducibile in $\mathbb{F}_p$ ha grado divisore di n se e solo se divide $x^{p^n} - x$. Si dimostrano le due implicazioni separatamente.

$(\implies)$ Sia $f(x)$ un polinomio irriducibile in $\mathbb{F}_p$ di grado d, con $d \mid n$. Si consideri allora il campo $\mathbb{F}_{p^d} \cong \mathbb{F}_p/(f(x))$, e sia α una radice di $f(x)$ in tale campo.

Per il *Lemma 1.2.1* si verifica che α è anche una radice di $x^{p^n} - x$. Poiché $f(x)$ è irriducibile, esso è il polinomio minimo di α, e quindi si deduce che $f(x)$ divide $x^{p^n} - x$.

$(\impliedby)$ Sia $f(x)$ un polinomio irriducibile in $\mathbb{F}_p$ di grado d che divide $x^{p^n} - x$. Si consideri allora il campo $\mathbb{F}_{p^d} \cong \mathbb{F}_p/(f(x))$, e sia α una radice di $f(x)$ in tale campo. Allora $\mathbb{F}_{p^d} \cong \mathbb{F}_p(\alpha)$, dacché $f(x)$, in quanto irriducibile, è il polinomio minimo di α.

Dacché $f(x)$ divide $x^{p^n} - x$, α è anche una radice di $x^{p^n} - x$, e quindi che $\alpha \in \mathbb{F}_{p^n}$. Dal momento che chiaramente anche $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$, si deduce che $\mathbb{F}_{p^d} \cong \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$. Allora, per il *Teorema 1.2.2*, d divide n. □