Appunti Aritmetica: Campi

Daniele Agostini

20 settembre 2009

1 Estensioni di Campi ed Elementi Algebrici

Definizione 1. Se F e K sono due campi tali che $F \subset K$, K si dice *estensione* di F e F si dice *sottocampo* di K.

Lemma 1. *Sia F un campo e sia K una sue estensione. Allora K è uno spazio vettoriale sul campo F.*

Dimostrazione. Poichè K è un campo è anche un gruppo additivo abeliano, inoltre, siano $u, v \in K$ e $\lambda, \mu \in F$, allora tutti questi sono elementi di K e quindi, per le proprietà di campo di K, vale che $\lambda v \in K$, $\lambda(u+v) = \lambda u + \lambda v$,$(\lambda + \mu)v = \lambda v + \mu v$ e $1 \in F, 1v = v$. Quindi tutti gli assiomi di spazio vettoriale sono verificati ed il lemma è dimostrato. □

Definizione 2 (Grado)**.** Sia F un campo e K una sua estensione; allora si dice *grado* di K su F la dimensione di K come spazio vettoriale su F, e si indica con $[K : F]$. Se $[K : F]$ è finito, K si dice essere un'*estensione semplice* di F.

Teorema 1. *Siano F, K, L campi tali che $L \subset K \subset F$. Allora L è un'estensione semplice di F se e solo se L è un'estensione semplice di K, K è un'estensione semplice di F e vale che $[L : F] = [L : K][K : F]$.*

Dimostrazione. Supponiamo che K non sia un'estensione semplice di F, allora esistono infiniti elementi di K linearmente indipendenti su F, ma allora questi stessi elementi possono essere considerati in L e quindi esistono anche infiniti elementi di L linearmente indipendenti su F, il che è assurdo perchè $[L : F]$ è finito. Ora, supponiamo che L non sia un'estensione semplice di K: allora esistono infiniti elementi di L linearmente indipendenti su K e quindi, a maggior ragione, linearmente indipendenti su F ma questo è assurdo per lo stesso motivo di prima. Invece, se $[L : K] = n \in \mathbb{N}$ e $[K : F] = m \in \mathbb{N}$, sia $(v_1, \ldots, v_n)$ una base di L su K e sia $(w_1, \ldots, w_m)$ una base di K su F. Quindi ogni elemento $v \in L$ si può scrivere come $v = k_1 v_1 + \cdots + k_n v_n$ con $k_1, \ldots, k_n \in K$. Ma a loro volta, ogni k_i può essere scritto come $k_i = f_{i1} w_1 + \cdots + f_{im} w_n$ con $f_{i1}, \ldots, f_{im} \in F$. E quindi $v = (f_{11} w_1 + \cdots + f_{1m} w_m) v_1 + \cdots + (f_{n1} w_1 + \cdots + f_{nm} w_m) v_n = \sum f_{ij} v_i w_j$. Allora abbiamo dimostrato che gli elementi $v_i w_j$ generano L come spazio vettoriale su F. Sono anche indipendenti? Proviamo: supponiamo che esistano $f_{ij} \in F$ tali che $\sum f_{ij} v_i w_j = 0$, allora possiamo raccogliere i v_i ed ottenere che $(f_{11} w_1 + \cdots + f_{1m} w_m) v_1 + \cdots + (f_{n1} w_1 + \cdots + f_{nm} w_m) v_n = 0$, ma poichè i v_i sono linearmente indipendenti, dev'essere che $f_{i1} w_1 + \cdots + f_{im} w_m = 0 \, i = 1, \ldots, n$, ma allora, per l'indipendenza lineare dei w_j, otteniamo che dev'essere $f_{ij} = 0 \, i = 1, \ldots, n \, j = 1, \ldots, m$, e quindi abbiamo mostrato che i $v_i w_j$ sono linearmente indipendenti; ma allora essi formano una base di L su K e poichè sono in numero di nm otteniamo che L è un'estensione semplice di F e che $[L : F] = [L : K][K : F]$. □

Definizione 3 (Elemento algebrico)**.** Sia F una campo e K una sua estensione. Allora un elemento $a \in K$ si dice *algebrico* su F se esiste un polinomio $p(x) \in F[x]$ di grado maggiore di 0 tale che $p(a) = 0$.

Siano F ed a come nella definizione precedente: consideriamo allora il sottoinsieme di $F[x]$, $A = \{\, p(x) \in F[x] \mid p(a) = 0 \,\}$. Si verifica facilmente che A è un ideale di $F[x]$, ma $F[x]$, in quanto anello euclideo, è PID, e perciò esiste $m(x) \in F[x]$ tale che $A = (m(x)) = \{\, m(x)k(x) \mid k(x) \in F[x] \,\}$. Questo ci porta alla seguente

Definizione 4 (Poliniomio minimo)**.** Siano F un campo, K una sua estensione ed $a \in K$ un elemento algebrico su F. Allora il *polinomio minimo* di a è il polinomio monico $m_a(x) \in F[x]$ tale che $(m_a(x)) = \{\, p(x) \in F[x] \mid p(a) = 0 \,\}$.

Lemma 2. *Siano F un campo, K una sua estensione ed $a \in K$ un elemento algebrico su F. Allora il polinomio minimo di a esiste, è unico, ha grado maggiore di 0 ed è il polinomio monico di grado minimo che ha a come radice o, equivalentemente,il polinomio monico irriducibile che ha a come radice.*

Dimostrazione. Sia $A = \{\, p(x) \in F[x] \mid p(a) = 0 \,\}$. Allora, poichè a è algebrico su F, dalla definizione segue subito che A è non vuoto e contiene polinomi di grado maggiore di 0. Allora il polinomio minimo $m_a(x)$ è il polinomio monico di grado minimo in A ed è unico in quanto monico (infatti tutti i polinomi di grado minimo in A sono associati tra loro). Se poi fosse che $\partial m_a(x) = 0$ allora $m_a(x) = m_a \in F$ e quindi $m_a m_a^{-1} = 1 \in A$ e allora $F \subset A$, ma questo è assurdo perchè l'unica costante che si annulla in a è 0. Supponiamo ora che $f(x) \in F[x]$ sia un polinomio monico e irriducibile tale che $f(a) = 0$; allora $f(x) \in A$ e quindi $f(x) = m_a(x)b(x)$, ma, poichè $f(x)$ è irriducibile e $\partial m_a(x) \geq 1$, dev'essere che $b(x) = b \in F$, inoltre, poichè $m_a(x)$ ed $f(x)$ sono entrambi monici, dev'essere che $b = 1$. Quindi $f(x) = m_a(x)$. □

Definizione 5. Sia F un campo, K una sua estensione e sia $a \in K$. Allora si indica con $F(a)$ il più piccolo sottocampo di K che contiene sia F, sia a: cioè, se L è un sottocampo di K che contiene F ed a, allora $F(a) \subset L$.

Ora mostriamo che una tale cosa non è una follia della nostra immaginazione, ma che esiste davvero. Per sveltire la notazione introduciamo un simbolo, $F[a]$, per l'insieme di tutti i polinomi di $F[x]$ valutati in a: cioè $F[a] = \{\, b_n a^n + \cdots + b_1 a + b_0 \mid n \in \mathbb{N}\ , b_i \in F \,\}$. Notiamo che $F[a]$ è un sottoinsieme di K.

Lemma 3. *Siano F un campo, K una sua estensione ed $a \in K$ un elemento algebrico su F. Allora*

(i) $F(a)$ è l'intersezione di tutti i sottocampi di K che contengono F ed a.

(ii) $F(a) = \{\, \frac{f}{g} \mid f, g \in F[a],\ g \neq 0 \,\}$.

Dimostrazione. (i) Sia M l'insieme di tutti i sottocampi di K che contengono F ed a. M è non vuoto, perchè $K \in M$, quindi sia $T = \bigcap_{L \in M} L$. L'intersezione di sottocampi è ancora un sottocampo ed inoltre F ed a sono contenuti in T, quindi $F(a) \subset T$. Però $F(a) \in M$, e poichè $T \subset L$ per ogni $L \in M$, vale anche che $T \subset F(a)$. Quindi $T = F(a)$.
(ii) Sia $U = \{\, \frac{f}{g} \mid f, g \in F[a],\ g \neq 0 \,\}$. Allora vediamo (senza scrivere tutto rigorosamente) che U è isomorfo al campo dei quozienti di $F[x]$ e quindi è un campo e, in particolare,è un sottocampo di K. Inoltre è chiaro che F e a sono contenuti in U, quindi $F(a) \subset U$. Però se $F(a)$ è un campo che contiene F ed a, allora deve contenere anche $F[a]$ per la chiusura

rispetto al prodotto ed alla somma, e deve contenere tutti i quozienti fra i vari elementi (a parte i quozienti per 0 che non esistono) per l'esistenza degli inversi e per la chiusura rispetto al prodotto. Ma allora $U \subset F(a)$ e quindi $U = F(a)$. $\square$

C'è però un modo molto migliore di ottenere $F(a)$ e lo mostreremo nel prossimo, importantissimo teorema, ma prima un lemma:

Lemma 4. *Sia F un campo e sia $p(x) \in F[x]$ un polinomio irriducibile. Allora abbiamo che $F[x]_{/(p(x))} \supset F$ e che $[F[x]_{/(p(x))} : F] = \partial p(x)$.*

Dimostrazione. Ora, l'enunciato del teorema non è corretto, infatti come può F essere contenuto in $F[x]_{/(p(x))}$? E' chiaro che questo non succede, però $F[x]_{/(p(x))}$ contiene un sottocampo isomorfo ad F ed è di questo che stiamo parlando. Per sveltire la notazione, poniamo $K = F[x]_{/(p(x))}$. Ora, stabiliamo un'applicazione

$$\begin{aligned} \psi : F &\longrightarrow K \\ a &\mapsto a + (p(x)) \end{aligned}$$

ora, è facile vedere che ψ è un omomorfismo di anelli. Inoltre $\text{Ker } \psi = \{ a \in F \mid a + (p(x)) = (p(x)) \} = \{ a \in F \mid a \in (p(x)) \} = \{ 0 \}$. Quindi ψ è un omomorfismo iniettivo e $F \cong \text{Im } \psi$ che è un sottocampo di K. A, questo punto, sia $n = \partial p(x)$ e consideriamo gli elementi $1 + (p(x)), x + (p(x)), \ldots, x^{n-1} + (p(x)) \in K$. Vediamo che questi elementi generano K, infatti un generico elemento di K ha la forma $f(x)+((p(x))$ con $f(x) \in F[x]$, ma allora, possiamo eseguire la divisione di $f(x)$ per $p(x)$ ed ottenere che $f(x)+(p(x)) = r(x)+q(x)p(x)+(p(x)) = r(x) + (p(x))$ con $r(x) = 0$ o $\partial r(x) < n$: quindi, sia $r(x) = a_{n-1}x^{n-1} + \cdots + a_0$, allora vediamo che $r(x) + (p(x)) = a_{n-1}(x^{n-1} + (p(x))) + \cdots + a_0(1 + (p(x)))$. Inoltre, questi stessi elementi sono linearmente indipendenti infatti, se esistessero $a_0, \ldots, a_{n-1} \in F$ tali che $a_{n-1}(x^{n-1} + (p(x))) + \cdots + a_0(1 + (p(x))) = 0$ allora, come sopra, dovrebbe essere che $k(x) = a_{n-1}x^{n-1} + \cdots + a_0 \in (p(x)) \implies p(x)|k(x)$, ma, poichè $\partial p(x) > \partial k(x)$, questo può accadere solo se $k(x) = 0$ e cioè se $a_{n-1} = \cdots = a_0 = 0$. Quindi gli elementi presentati sono una base di K su F e quindi $[K : F] = n$. $\square$

Teorema 2. *Siano F un campo, e K una sua estensione. Allora $a \in K$ è algebrico su F se e solo se $F(a)$ è un'estensione finita di F. Inoltre, se a è algebrico su F ed $m_a(x)$ è il suo polinomio minimo, si ha che $F[x]_{/(m_a(x))} \cong F(a)$ secondo un isomorfismo ψ per cui $\psi(x + (m_a(x))) = a$ e $\psi(b + (m_a(x))) = b \; \forall b \in F$.*

Dimostrazione. ($\Longrightarrow$) Se a è algebrico su F,consideriamo l'ideale $A = (m_a(x))$. Poichè $m_a(x)$ è irriducibile in $F[x]$, A è un ideale massimale di $F[x]$, e quindi $F[x]_{/(m_a(x))}$ è un campo. Ora, definiamo un'applicazione:

$$\begin{aligned} \phi : F[x] &\longrightarrow F(a) \\ f(x) &\mapsto f(a) \end{aligned}$$

Intanto vediamo che ϕ è ben definita, perchè $f(a) \in F[a]$ e, per quanto detto nella dimostrazione del Lemma 3, $F(a) \supset F[a]$. Ora, verifichiamo che ϕ è un omomorfismo di anelli, ma questo è vero perchè non è altro che l'omomorfismo di valutazione. Chi è il nucleo di questo omomorfismo? Troviamolo: $\text{Ker } \phi = \{ f(x) \in F[x] \mid f(a) = 0 \} = (m_a(x))$. Ed invece, che cos'è Im ϕ? Dai risultati generali sugli omomorfismi, sappiamo che Im ϕ è un sottocampo di $F(a)$, inoltre, vediamo che $\phi(x) = a \in \text{Im } \phi$ e che $\forall b \in F \; \phi(b) = b \in \text{Im } \phi$; quindi Im ϕ è un sottocampo di $F(a)$ che contiene F ed a, ma allora, per definizione

di $F(a)$, dev'essere che Im $\phi = F(a)$. Ma allora, per il Primo Teorema di Omomorfismo per Anelli, abbiamo che $F[x]_{/(m_a(x))} \cong F(a)$ secondo un isomorfismo ψ per cui $\psi(x + (m_a(x))) = a$ e $\psi(b + (m_a(x))) = b \; \forall b \in F$. In particolare, otteniamo che $[F(a) : F] = [F[x]_{/(m_a(x))} : F] = \partial m_a(x)$ e quindi $F(a)$ è un'estensione finita di F.
($\Longleftarrow$) Se $[F(a) : F] = n \in \mathbb{N}$, consideriamo gli elementi $1, a, a^2, \ldots, a^n \in F(a)$: essi sono in numero di $n + 1$ e quindi sono linearmante dipendenti su F, cioè esistono elementi $b_0, b_1, \ldots, b_n \in F$ tali che $b_0 + b_1 a + \cdots + b_n a^n = 0$. Ma allora, prendendo il polinomio $p(x) = b_0 + b_1 x \cdots + b_n x^n \in F[x]$, vediamo che $p(a) = 0$ e che quindi a è algebrico su F. □

Da questo teorema ne otteniamo subito un altro:

Teorema 3. *Sia F un campo e K una sua estensione. Allora gli elementi algebrici su F formano un sottocampo di K.*

Dimostrazione. Sia $S = \{\, a \in K \mid a \text{ è algebrico su } F \,\}$. Per vedere che S è un campo dobbiamo verificare che, comunque presi $a, b \in S$ con $b \neq 0$ gli elementi $a+b, -a, ab, \frac{a}{b}$ appartengano ad S. Ora, sicuramente questi elementi sono contenuti in $F(a, b)$, e se facciamo vedere che questo è un'estensione finita di F, grazie al teorema precedente abbiamo finito. Allora, poichè a, b sono algebrici su F, dev'essere che $[F(a) : F] = n$ e $[F(b) : F] = m$; ora calcoliamo $[F(a, b) : F(a)]$: abbiamo che il polinomio minimo di b in $F[x]$, indichiamolo con $m_b(x)$, ha grado m. Ma allora, poichè $F \subset F(a)$, b è algebrico su $F(a)$ e $[F(b) : F(a, b)] \leq m$. Quindi, per la formula dei gradi, $[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F] \leq mn$ e finiamo. □

In verità, nella dimostrazione abbiamo provato anche qualcosa in più di quanto ci proponevamo, e cioè che

Corollario 1. *Se a, b sono elementi algebrici su F di grado m, n allora anche $a + b, ab, \frac{a}{b}$ sono algebrici su F di grado al più mn.*

2 Campi di Spezzamento

Iniziamo con una definizione:

Definizione 6 (**Campo di Spezzamento**)**.** Sia F un campo e sia $p(x) \in F[x]$. Allora un'estensione $K \supset F$ si dice essere un campo di spezzamento di $p(x)$ su F se in $K[x]$ il polinomio $p(x)$ si spezza nel prodotto di fattori lineari e se questo non accade per nessun sottocampo di K.

Ora dimostriamo che i campi di spezzamento effettivamente esistono. Iniziamo con un Lemma:

Lemma 5. *Sia F un campo e sia $p(x) \in F[x]$ un polinomio irriducibile di grado n. Allora esiste un ampliamento di F di grado n che contiene una radice di $p(x)$.*

Dimostrazione. Consideriamo il campo $K = F[x]_{/(p(x))}$. In questo modo, K non è un' estensione di F, però contiene un sottocampo isomorfo a F. Infatti, definiamo un'applicazione come segue:

$$\begin{aligned} \phi : F &\longrightarrow K \\ a &\mapsto a + (p(x)) \end{aligned}$$

Allora ϕ è un omomorfismo, infatti, se $a, b \in F$ abbiamo che $\phi(a+b) = (a+b)+(p(x)) = (a+(p(x))+(b+(p(x)) = \phi(a)+\phi(b)$ e $\phi(ab) = ab+(p(x)) = (a+(p(x)))(b+(p(x)))$. Inoltre $a \in \text{Ker } \phi \iff a+(p(x)) = 0+(p(x)) \iff p(x)|a \iff a = 0$. Quindi ϕ è un omomorfismo iniettivo di anelli e, perciò, K contiene un sottocampo isomorfo a F. In questo senso possiamo dire che $F \subset K$. Ora, consideriamo l'elemento $\alpha = x+(p(x)) \in K$; si ha che $p(\alpha) = 0$: infatti , se $p(x) = a_n x^n + \cdots + a_1 x + a_0$, allora $p(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = a_n(x+(p(x)))^n + \cdots + a_1(x+(p(x))) + a_0 = a_n x^n + \cdots + a_1 x + a_0 + (p(x)) = p(x) + (p(x)) = 0 + (p(x)) = 0$. E, poichè $[K : F] = \partial p(x) = n$, abbiamo finito. □

Questo Lemma porta ad un interessante Corollario:

Corollario 2. *Sia F un campo e $f(x) \in F[x]$. Allora esiste un'estensione $K \supset F$ di grado $[K : F] \leq \partial f(x)$ che contiene una radice di $f(x)$.*

Dimostrazione. Sia p(x) un fattore irriducibile di $f(x)$. Allora, per il Lemma, il campo $K = F[x]_{/(p(x))}$ è un'estensione di grado $\partial p(x) \leq \partial f(x)$ che contiene una radice di $p(x)$ e quindi anche di $f(x)$. □

Con questo risultato, possiamo dimostrare il seguente

Teorema 4. *Sia F un campo e $f(x) \in F[x]$ un polinomi di grado $\partial f(x) = n$. Allora esiste un'estensione $K \supset F$ di grado $[K : F] \leq n!$ che contiene tutte le radici di $f(x)$.*

Dimostrazione. Vogliamo procedere per induzione sul grado n di $f(x)$. Se $n = 1$ allora $f(x) = ax + b$, $a \neq 0$ e quindi l'unica radice di $f(x)$ è $-\frac{b}{a} \in F$, inoltre $[F : F] = 1$ e perciò il teorema è dimostrato. Ora, supponiamo che il teorema sia vero per tutti i polinomi di grado minore di n. Allora, per il Corollario precedente, esiste un'estensione $K' \supset F$ di grado $[K' : F] \leq n$ in cui $f(x)$ ha una radice $\alpha \in K'$. Allora, in $K'[x]$, il polinomio si fattorizza come $f(x) = (x-\alpha)g(x)$ e $\partial g(x) = n-1$; quindi, per induzione, esiste un'estensione $K \supset K' \supset F$ di grado $[K : K'] \leq (n-1)!$ che contiene tutte le radici di $f(x)$. Ma allora, K è un' estensione di F che contiene tutte le radici di $f(x)$ e $[K : F] = [K : K'][K' : F] \leq (n-1)!n = n!$. Quindi il teorema è completamente dimostrato. □

Quindi il teorema mostra che esiste un ampliamento di F che contiene tutte le radici di $f(x)$. Quindi deve esistere anche un ampliamento di grado minimo con questa proprietà che è proprio un campo di spezzamento di $f(x)$ su F.

Ora enunciamo senza dimostrazione questo teorema:

Teorema 5. *Sia F una campo e $f(x) \in F[x]$. Allora due campi di spezzamento K, K' di $f(x)$ su F sono isomorfi secondo un isomorfismo che lascia fisso ogni elemento di F.*

3 Campi Finiti

3.1 Elementi Primitivi

Iniziamo con alcuni lemmi che ci serviranno per dimostrare il teorema.

Lemma 6. *Siano a, b due interi positivi. Allora $ab = (a, b)[a, b]$*

Presentiamo due dimostrazioni di questo fatto: una scalcagnata ma facile ed una algebrica ma complicata.

Dimostrazione. Iniziamo con la dimostazione scalcagnata. Sappiamo che (a,b) è il prodotto di tutti i fattori primi comuni ad a ed a b presi con il minimo esponente, mentre $[a,b]$ è il prodotto di tutti i fattori non comuni e di quelli comuni presi con il massimo esponente. Quindi $(a,b)[a,b]$ =(*fattori solo di* a)(*fattori solo di* b)(*fattori comuni col massimo esponente*)(*fattori comuni col minimo esponente*). Pensandoci un po' apparirà chiaro che questo non è altro che ab. □

Dimostrazione. Ecco la dimostrazione più raffinata. Dati gli elementi a,b consideriamo gli ideali da loro generati in $\mathbb{Z}$:(a) e (b). Sappiamo che sono sottogruppi additivi di $\mathbb{Z}$ e quindi anche sottogruppi normali (perchè tutti i sottogruppi di un gruppo abeliano lo sono). Allora per un Teorema di Omomorfismo (il secondo o il terzo, non ricordo bene) vale che $((a)+(b))/(a) \cong (b)/(a)\cap(b)$. Però sappiamo che $(a)+(b) = ((a,b))$ e che $(a)\cap(b) = ([a,b])$; quindi, se poniamo $m = (a,b)$ e $M = [a,b]$, abbiamo che $(m)/(a) \cong (b)/(M)$ e quindi $o((m)/(a)) = o((b)/(M))$. Poichè si ha che $o((m)/(a)) = \frac{a}{m}$ e che $o((b)/(M)) = \frac{M}{b}$ la tesi è dimostrata. □

Lemma 7. *Sia G un gruppo e sia $g \in G$ di ordine finito. Allora $o(g^c) = \frac{o(g)}{(o(g),c)}$.*

Dimostrazione. Sia $x = o(g^c)$. Intanto vediamo che $(g^c)^{\frac{o(g)}{(o(g),c)}} = g^{\frac{o(g)c}{(o(g),c)}} = (g^{o(g)})^{\frac{c}{(o(g),c)}} = e^{\frac{c}{(o(g),c)}} = e$. Quindi $x \mid \frac{o(g)}{(o(g),c)}$; tuttavia se $(g^c)^x = g^c x = e$ allora $o(g) \mid cx$, ma vale ovviamente anche che $c \mid cx$, quindi $[o(g),c] \mid cx \Rightarrow \frac{[o(g),c]}{c} \mid x \Rightarrow \frac{o(g)}{(o(g),c)} \mid x$. Quindi $x = \frac{o(g)}{(o(g),c)}$. □

Lemma 8. *Se G è un gruppo abeliano con due elementi di ordine a e b esiste anche un elemento di ordine $[a,b]$.*

Dimostrazione. Siano α e β i due elementi di ordine a,b rispettivamente. Consideriamo dapprima il caso in cui $(a,b) = 1$ e quindi $[a,b] = ab$. Prendiamo l'elemento $\alpha\beta$: vediamo che $(\alpha\beta)^{ab} = \alpha^{ab}\beta^{ab} = e^b e^a = ee = e$ e quindi $o(\alpha\beta) \mid ab$. Ora $(\alpha\beta)^{o(\alpha\beta)} = e \Rightarrow (\alpha\beta)^{o(\alpha\beta)a} = e^a = e \Rightarrow \alpha^{o(\alpha\beta)a}\beta^{o(\alpha\beta)a} = e \Rightarrow e\beta^{o(\alpha\beta)a} = e \Rightarrow \beta^{o(\alpha\beta)a} = e \Rightarrow b \mid o(\alpha\beta)a$ ma a e b sono coprimi, quindi $b \mid o(\alpha\beta)$. Allo stesso modo possiamo dimostrare che $a \mid o(\alpha\beta)$, e quindi $[a,b] = ab \mid o(\alpha\beta)$. Quindi abbiamo dimostrato che $o(\alpha\beta) = ab$. Se invece a e b non sono coprimi, abbiamo che $[a,b] = \frac{ab}{(a,b)}$; ma $a = o(\alpha)$ e $\frac{b}{(a,b)} = o(\beta^a)$ per il Lemma 2, inoltre è chiaro che $(a, \frac{b}{(a,b)}) = 1$. Quindi, per quanto già dimostrato, l'elemento $\alpha\beta^a$ ha ordine $[a,b]$. □

Teorema 6 (**Teorema dell'Elemento Primitivo**)**.** *Sia F un campo finito. Allora F^* è un gruppo ciclico.*

Dimostrazione. Sia q il numero di elementi di F, allora $o(F^*) = q-1$. Sia S l'insieme degli ordini degli elementi di F^*; per il Teorema di Lagrange si ha che $\forall a \in S\ a \mid q-1$ e perciò S è un insieme di neturali limitato superiormente che dunque ammette un massimo $M = \max S$. Per il Lemma 2 si ha che $\forall a \in S\ [a,M] \in S$ ma $[a,M] \geq M$ poichè è un suo multiplo e $[a,M] \leq M$ perchè $M = \max S$ e $[a,M] \in S$, quindi $M = [a,M]$ e perciò $a \mid M\ \forall a \in S$. Ora consideriamo il polinomio $p(x) = x^M - 1 \in F[x]$: per quanto appena detto, ogni elemento di F^* è radice di $p(x)$, quindi $p(x)$ ha almeno $q-1$ radici, ma, per il Teorema del Resto, dev'essere che $q-1 \leq \partial p(x) = M$. Ma $M \in S$ e quindi $M \mid q-1$ per quanto detto all'inizio. Ma allora $M = q-1$ e abbiamo finito, infatti esiste un elemento $k \in F^*$ tale che $o(k) = o(F^*)$, e quindi $F^* = (k)$. □

Corollario 3. *Se p è un numero primo, allora $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$.*

Dimostrazione. Z_p è un campo finito, allora, per il Teorema dell'Elemento Primitivo, $\mathbb{Z}_p^*$ è un gruppo ciclico di ordine $p-1$ che quindi è isomorfo a $\mathbb{Z}_{p-1}$. □

3.2 Classificazione dei Campi Finiti

Vogliamo dimostrare un teorema fondamentale che classifica completamente tutti i campi finiti. Il teorema è il seguente:

Teorema 7 (**Teorema di Classificazione dei Campi Finiti**). *Ogni campo finito ha p^n elementi, dove p è primo ed n è un intero positivo. Inoltre, per ogni p primo ed ogni n intero positivo esiste un campo con p^n elementi,e questo campo èunico a meno di isomorfismi.*

Comunque, per la strada, dimostreremo anche qualcosa di più. Iniziamo con il seguente lemma:

Lemma 9. *Sia K un campo finito, allora K ha caratteristica p per un certo primo p e contiene un sottocampo isomorfo a $\mathbb{Z}_p$.*

Dimostrazione. Consideriamo K come gruppo additivo, allora, poichè $o(K)$ è finito, esiste un ordine minimo m per tutti gli elementi di K: e questo numero è proprio la caratteristica di K. Dimostriamo che tale caratteristica dev'essere un numero primo: supponiamo che $m = ab$, allora $m \cdot 1 = ab \cdot 1 = 0$ (con $m \cdot 1$ indichiamo $1 + 1 + 1 + \cdots + 1$ m volte). Ma allora, se poniamo $x = b \cdot 1$, vediamo che $a \cdot x = 0$, ma , poichè la caratteristica m è il minimo intero positivo per cui ciò accade, dev'essere che $a = m$, e quindi m è un numero primo, che indichiamo con p. Ora, per dimostrare la seconda parte del lemma, consideriamo l'applicazione:

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow K \\ n &\mapsto n \cdot 1 \end{aligned}$$

E' facile vedere che ϕ è un omomorfismo di anelli (e non ho voglia di scriverlo qui). Ora, qual è il nucleo di questo omomorfismo? cerchiamolo: Ker $\phi = \{ n \in \mathbb{Z} \mid n \cdot 1 = 0 \}$ ma è immediato verificare che, allora, Ker $\phi = (p)$, cioè l'ideale generato dalla caratteristica di K: infatti, sia $n \in$ Ker ϕ, allora possiamo applicare la divisione euclidea ed ottenere che $n = kp + r$, con $r < p$; perciò $0 = n \cdot 1 = (kp + r) \cdot 1 = kp \cdot 1 + r \cdot 1 = 0 + r \cdot 1 = r \cdot 1$; ma, per definizione di caratteristica, dev'essere che $r = 0$ e quindi abbiamo finito. Un altro modo per dimostrare che Ker $\phi = (p)$ è quello di notare che Ker ϕ è un ideale in un anello euclideo ed inoltre $p \in$ Ker ϕ , quindi $(p) \subset$ Ker ϕ, ma (p) è un ideale massimale e non può essere che Ker $\phi = \mathbb{Z}$ perchè $1 \notin$ Ker ϕ; quindi dev'essere che Ker $\phi = (p)$. Concludendo, per il Primo Teorema di Omomorfismo per Anelli, abbiamo che Im ϕ è un sottocampo di K isomorfo a $\mathbb{Z}_{/(p)} = \mathbb{Z}_p$. □

Proseguiamo ora conun teorema importante di per sè:

Teorema 8. *Sia K un campo finito. Allora K è isomorfo ad un'estensione semplice di $\mathbb{Z}_p$, ove p è la caratteristica di K.*

Dimostrazione. Per il Lemma precedente,sappiamo che K ha caratteristica p per un certo primo p e che contiene un sottocampo isomorfo a $\mathbb{Z}_p$. Quindi, a meno di isomorfismo, possiamo ipotizzare $\mathbb{Z}_p \subset K$. Ora, dal Teorema dell'Elemento Primitivo, sappiamo che esiste un elemento $\alpha \in K^*$, che genera il gruppo moltiplicativo K^*; inoltre, tale elemento è algebrico su $\mathbb{Z}_p$, infatti è radice del polinomio $x^{o(\alpha)} - 1 \in \mathbb{Z}_p[x]$. Ora possiamo procedere

in due modi:
Primo Modo: Stabiliamo un'applicazione:

$$\begin{aligned} \varphi : \mathbb{Z}_p[x] &\longrightarrow K \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

φ è un omomorfismo di anelli, infatti $\varphi(f(x)+g(x)) = \varphi((f+g)(x)) = (f+g)(\alpha) = f(\alpha)+g(\alpha) = \varphi(f(x)) + \varphi(g(x))$ e $\varphi(f(x)g(x)) = \varphi((fg)(x)) = (fg)(\alpha) = f(\alpha)g(\alpha)$. Inoltre, φ è surgettivo, infatti $0 = \varphi(0)$,$\alpha = \varphi(x)$ ed ogni elemento non zero di K è potenza di α. Inoltre Ker $\phi = (m_\alpha(x))$, cioè l'ideale generato dal polinomio minimo di α (che abbiamo dimostrato essere algebrico su $\mathbb{Z}_p$). quindi, per il Primo Teorema di Omomorfismo per Anelli, otteniamo che $\mathbb{Z}_p[x]_{/(m_\alpha(x))} \cong K$.
Secondo Modo: Allora, consideriamo il campo $\mathbb{Z}_p(\alpha)$: sicuramente $K \supset \mathbb{Z}_p(\alpha)$, perchè $\mathbb{Z}_p \subset K$ e $\alpha \in K$, ma $\mathbb{Z}_p(\alpha)$ contiene anche tutte le potenze di α, che è elemento primitivo di K, e quindi $K \subset \mathbb{Z}_p(\alpha)$; allora vediamo che $K = \mathbb{Z}_p(\alpha)$. Ma allora abbiamo vinto, perchè $Z_p(\alpha)$ è un'estensione semplice di $\mathbb{Z}_p$, in quanto α è algebrico su $\mathbb{Z}_p$. □

Come corollario, otteniamo la prima parte del Teorema che vogliamo dimostrare:

Corollario 4. *Ogni campo finito ha p^n elementi, dove p è primo ed n è un intero positivo.*

Dimostrazione. Sia K un campo finito. Allora, per il Teorema precedente, $K \supset \mathbb{Z}_p$ e $[K : \mathbb{Z}_p] = n$, con n intero positivo. Allora, sia $(v_1, v_2, \ldots, v_n)$ una base di K come spazio vettoriale su $\mathbb{Z}_p$: ogni elemento di $\mathbb{Z}_p$ si può scrivere in modo unico come $a_1v_1 + a_2v_2 + \cdots + a_nv_n$ con $a_i \in \mathbb{Z}_p$, e, poichè per ogni a_i abbiamo p scelte, vediamo che K ha p^n elementi. □

Continuiamo con la seconda parte del Teorema:

Teorema 9. *Per ogni numero primo p ed ogni intero positivo n esiste un campo con p^n elementi.*

Dimostrazione. Consideriamo il polinomio $p(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$, faremo vedere che l'insieme delle sue radici è il campo che cerchiamo. Sappiamo che esiste un campo $K \supset \mathbb{Z}_p$ di spezzamento per $p(x)$: sia F il sottoinsieme di K costituito dalle radici di $p(x)$.
F è un campo: intanto dobbiamo dimostrare che $(F, +)$ è un sottogruppo di $(K, +)$ e che $(F^*, \cdot)$ è un sottogruppo di $(K^*, \cdot)$, quindi, poichè F è finito basta verificare che è chiuso rispetto a somma e prodotto: siano $a, b \in F$ allora $(a+b)^{p^n} = a^{p^n} + b^{p^n}$(perchè K è un campo di caratteristica p)$= a + b$ (perchè $a, b \in F$). Inoltre $(ab)^{p^n} = a^{p^n}b^{p^n} = ab$, quindi $a + b, ab \in F$. Inoltre la proprietà distributiva è già verificata per tuti gli elementi di K, quindi tutti gli assiomi sono soddisfatti e F è un campo.
F ha p^n elementi: abbiamo che $p'(x) = p^n x^{p^n-1} - 1 = -1$. Quindi $(p(x), p'(x)) = 1$ e, perciò, il polinomio $p(x)$ non ha radici multiple e quindi ha esattamente tante radici quanto il suo grado: $o(F) = \partial p(x) = p^n$. □

Vale la pena di analizzare un po' più a fondo il polinomio $x^{p^n} - x$: intanto dimostriamo un piccolo lemma che ci servirà in futuro:

Lemma 10. *Sia p un primo ed n, d due interi positivi. Allora $p^d - 1 | p^n - 1$ se e solo se $d|n$.*

Dimostrazione. ($\Longleftarrow$) Per ipotesi $n = kd$ con k intero positivo. Allora $p^n - 1 = p^{kd} - 1 = (p^d)^k - 1 = (p^d - 1)(p^{kd-1} + p^{kd-2} + \cdots + p + 1)$ e quindi $p^d - 1 | p^n - 1$.
($\Longrightarrow$) Possiamo applicare la divisione euclidea ed ottenere che $n = kd + r$, con $0 \leq r < d$. Allora $p^n - 1 = p^{kd+r} - 1 = p^{kd}p^r - 1 = p^{kd}(p^r - 1) + (p^{kd} - 1)$. Abbiamo che, per ipotesi, $p^d - 1 | p^{kd}(p^r - 1) + (p^{kd} - 1)$, ma, per la parte già dimostrata, $p^d - 1 | p^{kd} - 1$, e quindi dev'essere che $p^d - 1 | p^{kd}(p^r - 1)$. Ora, notiamo che $p^d - 1$ e p^{kd} sono coprimi perchè $p \nmid p^d - 1$(si può vedere facilmente modulo p), e, quindi, $p^d - 1 | p^r - 1$, ma questo è possibile solo se $r = 0$. Quindi la tesi è dimostrata. □

Teorema 10. *Sia $p(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ con p primo e n intero positivo. Allora $p(x)$ è il prodotto di tutti i polinomi monici e irriducibili in $\mathbb{Z}_p[x]$ che hanno grado divisore di n.*

Dimostrazione. Sia $q(x) \in \mathbb{Z}_p[x]$ un polinomio monico, irriducibile con grado $\partial q(x) = d | n$. Allora sia $K = \mathbb{Z}_p[x]_{/(q(x))}$ e sia $\alpha = x + (q(x)) \in K$, quindi $q(\alpha) = 0$, e perciò $q(x)$ è il polinomio minimo di α. Inoltre, poichè $o(K) = p^d$, abbiamo che $\alpha^{p^d} = \alpha$ e quindi $\alpha^{p^n} = \alpha^{p^{kd}} = \alpha$. Ma allora α è radice di $p(x)$ e quindi $q(x) | p(x)$.
Ora invece sia $q(x) \in \mathbb{Z}[x]$ un fattore monico e irriducibile di $p(x)$, vogliamo mostrare che $\partial q(x) = d | n$. Allora sia F il campo delle radici di $p(x)$ e sia $\beta \in F$ una radice di $q(x)$. Allora stabiliamo un'applicazione:

$$\begin{aligned} \phi : \mathbb{Z}_p[x] &\longrightarrow F \\ f(x) &\mapsto f(\beta) \end{aligned}$$

Se riguardiamo la dimostrazione del Teorema 2, vediamo che quest'applicazione è un omomorfismo di anelli che ha come nucleo l'ideale $(q(x))$ perchè $q(x)$ è il polinomio minimo di β. Allora, per il Primo Teorema di Omomorfismo per Anelli, otteniamo che esiste un sottocampo $F' \subset F$ isomorfo a $\mathbb{Z}_p[x]_{/(q(x))}$. Ora abbiamo tre strade:
Primo Modo: sappiamo che F è uno spazio vettoriale su F' di dimensione finita, sia essa $[F : F'] = m$. Allora ogni suo elemento può essere scritto in modo unico come combinazione lineare degli elementi di una base $(v_1, \ldots, v_m)$: $a_1v_1 + \cdots + a_nv_m$ $a_i \in F'$; ma allora, poichè per ognuno degli a_i abbiamo p^d scelte, vediamo che $o(F) = p^n = (p^d)^m = p^m d \implies d | n$.
Secondo Modo: consideriamo i gruppi moltiplicativi F^* e F'^*: si ha che $o(F^*) = p^n - 1$, $o(F'^*) = p^d - 1$ e che F'^* è un sottogruppo di F^*. Quindi, per il Teorema di Lagrange, dev'essere che $o(F'^*) | o(F^*) \Rightarrow p^d - 1 | p^n - 1$, ma, per il Lemma precedente, questo implica che $d | n$.
Terzo Modo: sia α l'elemento primitivo di F; allora α è algebrico su F': infatti $F' \supset Z_p$ ed α è radice di $x^o(\alpha) - 1 \in Z_p[x] \subset F'[x]$. Ora, stabiliamo un'applicazione

$$\begin{aligned} \varphi : F'[x] &\longrightarrow F \\ g(x) &\mapsto g(\alpha) \end{aligned}$$

Allora, riguardando la dimostrazione del Teorema 2, vediamo che questo è un omomorfismo di anelli, surgettivo che ha come nucleo l'ideale $(m_\alpha(x))$, ove $m_\alpha(x) \in F'[x]$ è il polinomio minimo di α. Allora, per il solito Primo Teorema, $F \cong F'[x]_{/(m_\alpha(x))}$. Ma allora, se $k = \partial m_\alpha(x)$, $p^n = o(F) = o(F'[x]_{/(m_\alpha(x))}) = o(F')^k = (p^d)^k = p^{kd}$; quindi $n = kd$ e la dimostrazione è completa. □

Possiamo ora concludere la nostra dimostrazione con quest'ultimo Teorema:

Teorema 11. *Due campi finiti con lo stesso numero di elementi sono isomorfi.*

Dimostrazione. Siano K e K' due campi con p^n elementi con p primo ed n intero positivo. Vogliamo far vedere che ognuno dei due campi è isomorfo al campo F delle radici del solito polinomio $p(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Allora, se α è un elemento primitivo di K, per un teorema precedente, abbiamo che $K \cong \mathbb{Z}_p[x]_{/m_\alpha(x)}$, dove $m_\alpha(x)$ è il polinomio minimo di α ed ha grado n. Quindi, poichè $m_\alpha(x)$ è un polinomio monico e irriducibile di grado n, si ha che $m_\alpha(x)|p(x)$ e che, quindi $\alpha \in F$. Allora stabiliamo un'applicazione:

$$\begin{aligned} \varphi : \mathbb{Z}_p[x] &\longrightarrow F \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

Riguardando la dimostrazione del Teorema 2, vediamo che φ è un omomorfismo di anelli che ha come nucleo l'ideale $(m_\alpha(x))$. Quindi per il Primo Teorema esiste un sottocampo di F isomorfo a $\mathbb{Z}_p[x]_{/m_\alpha(x)}$, ma, poichè $o(\mathbb{Z}_p[x]_{/m_\alpha}(x)) = o(F)$ questo sottocampo dev'essere F stesso. Quindi $K \cong \mathbb{Z}_p[x]_{/m_\alpha}(x) \cong F \implies K \cong F$. Allo stesso modo, possiamo dimostrare che $K' \cong F$ e quindi che $K \cong K'$. □

E così abbiamo completamente dimostrato il Teorema di Classificazione dei Campi Finiti. Un'ultima cosa: poichè, a meno di isomorfismi, esiste un solo campo finito con p^n elementi, si usa indicarlo con $\mathbb{F}_{p^n}$. Raccogliendo le idee che abbiamo utilizzato precedentemente, dimostriamo un piccolo lemma:

Lemma 11. *Si ha che $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$ se e soltanto se $a|b$.*

Dimostrazione. ($\Longrightarrow$) Se $\mathbb{F}_{p^b} \supset \mathbb{F}_{p^a}$ allora $\mathbb{F}_{p^b}$ è uno spazio vettoriale di dimensione $[\mathbb{F}_{p^b} : \mathbb{F}_{p^a}] = n \in \mathbb{N}$ su $\mathbb{F}_{p^b}$, quindi ogni suo elemento può essere scritto in modo unico come combinazione lineare degli elementi di una base $(v_1, \ldots, v_n)$: $a_1v_1 + \cdots + a_nv_n$ $a_i \in \mathbb{F}_{p^a}$; ma allora, poichè per ognuno degli a_i abbiamo p^a scelte, vediamo che $p^b = (p^a)^n = p^an \implies b = an \implies a|b$.
($\Longleftarrow$) Sappiamo che $\mathbb{F}_{p^b}$ può essere pensato come l'insieme delle radici del polinomio $x^{p^b} - x \in \mathbb{Z}_p[x]$, mentre $\mathbb{F}_{p^a}$ come l'insieme delle radici di $x^{p^a} - x \in \mathbb{Z}_p[x]$: allora, poichè $a|b$, $x^{p^b} - x$ è multiplo del prodotto di tutti i polinomi monici irriducibili in $\mathbb{Z}_p[x]$ di grado che divide a, ma questo prodotto è proprio $x^{p^a} - x$, e quindi $x^{p^a} - x|x^{p^b} - x$, da cui segue subito che tutte le radici del primo (cioè $\mathbb{F}_{p^a}$) sono anche radici del secondo, e quindi $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$. □

3.3 Campi di Spezzamento su $\mathbb{Z}_p[x]$

Determiniamo ora i campi di spezzamento dei polinomi irriducibili in $\mathbb{Z}_p[x]$. Iniziamo con un lemma:

Lemma 12. *Sia K un campo di caratteristica p. Allora l'applicazione:*

$$\begin{aligned} \phi_p : K &\longrightarrow K \\ a &\mapsto a^p \end{aligned}$$

è un omomorfismo di anelli, ed inoltre $\phi_p(a) = a$ se e solo se $a \in \mathbb{Z}_p$.

Dimostrazione. Intanto due parole sull'interpretazione del lemma: abbiamo dimostrato da un'altra parte che un campo di caratteristica p ha un sottocampo isomorfo a $\mathbb{Z}_p$, ed è a questo campo che ci riferiamo quando nell'enunciato troviamo "$\mathbb{Z}_p$". Ora, dimostriamo il Lemma: siano $a, b \in K$, allora

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{n-k}b^k.$$

Ora osserviamo che

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

Allora, se $k \neq 0, p$ abbiamo che $k! \nmid p$ e $(p-k)! \nmid p$, e quindi $p | \binom{p}{k}$. Ma allora, poichè p è la caratteristica di K, otteniamo che

$$\phi_p(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{n-k} b^k = a^p + b^p = \phi_p(a) + \phi_p(b)$$

. Inoltre, si verifica subito che $\phi_p(ab) = (ab)^p = a^p b^p = \phi_p(a)\phi_p(b)$. Quindi ϕ_p è un omomorfismo. Per il Piccolo Teorema di Fermat, abbiamo che, se $a \in \mathbb{Z}_p$ allora $a^p = a \implies \phi_p(a) = a$; invece, sia $a \in K$ tale che $\phi_p(a) = a^p = a$, allora a è radice del polinomio $q(x) = x^p - x \in \mathbb{Z}_p[x]$, ma, per quanto dimostrato prima, tutti i p elementi di $\mathbb{Z}_p$ sono radici di $q(x)$ e, per il Teorema del Resto, queste sono tutte le radici di $q(x)$; quindi $a \in \mathbb{Z}_p$. □

Dal lemma segue facilmente il seguente:

Corollario 5. *Sia K un campo di caratteristica p. Allora l'applicazione*

$$\phi_p : \ K[x] \longrightarrow K[x]$$

definita da

$$\phi_p : a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mapsto a_n^p x^n + a_{n-1}^p x^{n-1} + \cdots + a_1^p x + a_0^p$$

è un omomorfismo di anelli e $\phi_p(f(x)) = f(x)$ se e solo se $f(x) \mathbb{Z}_p[x]$.

C'è anche un corollario del corollario:

Corollario 6. *Sia $f(x) \in \mathbb{Z}_p[x]$ e sia α una radice di $f(x)$ in un'estensione di $\mathbb{Z}_p$. Allora anche α^p è una radice di $f(x)$.*

Dimostrazione. Sia K un'estensione di $\mathbb{Z}_p$ tale che $\alpha \in K$. Allora K ha caratteristica p,e quindi, sia ϕ_p come nel corollario precedente:allora $\phi_p(f(x)) = f(x)$ e $f(x) = (x - \alpha) g(x)\, g(x) \in K[x]$, e quindi $f(x) = \phi_p((x-\alpha)g(x)) = \phi_p((x-\alpha))\phi_p(g(x)) = (x - \alpha^p) h(x)\, h(x) = \phi_p(g(x)) \in K[x]$. Ma allora α^p è una radice di $f(x)$. □

Ora, possiamo dimostrare il seguente Teorema:

Teorema 12. *Sia $q(x) \in \mathbb{Z}_p[x]$ un polinomio irriducibile di grado $\partial q(x) = n$. Allora $\mathbb{F}_{p^n} = \mathbb{Z}_p[x]_{/(q(x))}$ è il campo di spezzamento di $q(x)$ su $\mathbb{Z}_p$. Inoltre,se $\alpha = x + (q(x))$, allora tutte e sole le radici di $q(x)$ sono $\alpha, \alpha^p, a^{p^2}, \ldots, a^{p^{n-1}}$.*

Dimostrazione. Intanto vediamo che possiamo sempre supporre che $q(x)$ sia monico (altrimenti basta moltiplicarlo per l'inverso del suo coefficiente direttivo, cosa che non ne cambia le radici). Ora, sappiamo che α è una radice di $q(x)$ per un risultato precedente,e quindi, per l'ultimo Corollario, anche α^{p^m}, $m \in \mathbb{N}$ è radice di $q(x)$. Poichè tutti questi elementi sono contenuti in $\mathbb{F}_{p^n}$, che è un campo finito, almeno due di essi devono essere uguali: $\alpha^{p^r} = \alpha^{p^s}$ con $r > s$, di conseguenza $\alpha^{p^{r-s}} = \alpha^{p^r p^{-s}} = (\alpha^{p^r})^{p^{-s}} = (\alpha^{p^s})^{p^{-s}} = \alpha^{p^0} = \alpha$. Quindi, sia k il minimo intero non negativo tale che $\alpha^{p^k} = \alpha$; allora gli elementi $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{k-1}}$ sono tutti distinti, infatti se esistessero i, j tali che $0 \leq i < j < k$ e $\alpha^{p^j} = \alpha^{p^i}$, allora (come sopra) $\alpha^{p^{j-i}} = \alpha$ e questo è assurdo perchè $j - i < k$. Consideriamo il polinomio

$g(x) = (x-\alpha)(x-\alpha^p)\dots(x-\alpha^{p^{k-1}})$: vediamo che $\phi_p(g(x)) = \phi_p(x-\alpha)\phi_p(x-\alpha^p)\dots\phi_p(x-\alpha^{p^{k-2}})\phi_p(x-\alpha^{p^{k-1}}) = (x-\alpha^p)(x-\alpha^{p^2})\dots(x-\alpha^{p^{k-1}})(x-\alpha) = g(x)$, quindi $g(x) \in \mathbb{Z}_p[x]$; inoltre, è chiaro che $g(\alpha) = 0$, ma α è radice di $f(x)$, irriducibile in $\mathbb{Z}_p[x]$ che quindi è il suo polinomio minimo in $\mathbb{Z}_p[x]$, e perciò $f(x)|g(x)$; tuttavia, $\partial g(x) = k \leq n = \partial f(x)$, e quindi dev'essere che $k = n$. Quindi gli n elementi $\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}$ sono tutti distinti e sono radici di $f(x)$, ma poichè $\partial f(x) = n$, queste sono tutte le radici di $f(x)$.
Abbiamo quasi fatto, dobbiamo far vedere che $\mathbb{F}_{p^n}$ è proprio il campo di spezzamento di $f(x)$ (naturalmente,a meno di isomorfismi): intanto osserviamo che, per un teorema, $\mathbb{F}_{p^n} \cong \mathbb{Z}_p(\alpha)$ e quindi, se F è campo di spezzamento di $f(x)$, allora $\mathbb{Z}_p(\alpha) \supset F$; ma,contemporaneamente, dev'essere che $F \supset \mathbb{Z}_p$ e $F \ni \alpha$ e quindi $F \supset \mathbb{Z}_p(\alpha)$, ma allora $F = \mathbb{Z}_p(\alpha)$ e abbiamo finalmente finito. □

Teorema 13. *Sia $f(x) \in \mathbb{F}_{p^[}x]$. Allora il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ è il campo $\mathbb{F}_{p^m}$, dove m è il minimo comune multiplo dei gradi di tutti i fattori di $f(x)$ irriducibili su $\mathbb{F}_p$.*

Dimostrazione. Trattiamo solamente il caso in cui $f(x)$ abbia solo due fattori irriducibili $a(x)$ e $b(x)$ di grado a, b rispettivamente; il caso generico si generalizza facilmente. Per il Teorema precedente, il campo di spezzamento di $a(x)$ è $\mathbb{F}_{p^a}$, mentre il campo di spezzamento di $b(x)$ è $\mathbb{F}_{p^b}$. Allora il campo di spezzamento di $f(x) = a(x)b(x)$ è il più piccolo campo che contiene $\mathbb{F}_{p^a} \cup \mathbb{F}_{p^b}$: intanto, notiamo che se $m = [a, b]$, allora $\mathbb{F}_{p^m} \supset \mathbb{F}_{p^a} \cup \mathbb{F}_{p^b}$, ora invece, supponiamo che per un campo $\mathbb{F}_{p^c}$ valga $\mathbb{F}_{p^c} \supset \mathbb{F}_{p^a}$ e $\mathbb{F}_{p^c} \supset \mathbb{F}_{p^b}$, allora deve essere che $a|c$ e $b|c$, e quindi $m|c$, ma allora $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^c}$. Quindi il Teorema è dimostrato. □