Caratteristica di un campo

Sia F un campo e sia $\varphi_F : \mathbb{Z} \longrightarrow \mathbb{Z}$ l'omomorfismo (di anelli) definito da

$$\widetilde{\varphi_F}(n) = \overbrace{1_F + \cdots + 1_F}^{n \text{ volte}} .$$

Dal I Teorema di omomorfismo si ha che esiste un omomorfismo iniettivo

$$\varphi_F : \mathbb{Z}/\operatorname{Ker}\varphi_F \quad \longrightarrow \quad F$$

ed è banale verificare che è un omomorfismo di anelli.

Poiché $\operatorname{Ker}\varphi_F$ è un sottogruppo di $\mathbb{Z}$, si ha che $\operatorname{Ker}\varphi_F = n\mathbb{Z}$ con $n \in \mathbb{N}$.

Osserviamo che non può essere $n = 1$ in quanto in F si ha $1_F \neq 0_F$, e che n non può essere un numero composto, perché se fosse $n = ab$ con $a, b < n$ avremmo che $\overline{a}\overline{b} = \overline{0}$ con $\overline{a} \neq \overline{0}$ e $\overline{b} \neq \overline{0}$, da cui $\widetilde{\varphi_F}(\overline{a})\widetilde{\varphi_F}(\overline{b}) = 0$ e questo è assurdo poiché F è un campo.

Ne segue che

$$\operatorname{Ker}\varphi_F = \begin{array}{c} \nearrow \\ \\ \searrow \end{array} \begin{array}{l} 0 \\ \\ p\mathbb{Z} \text{ con } p \text{ primo} \end{array}$$

Se $\operatorname{Ker}\varphi_F = 0 \Rightarrow \mathbb{Z} \subset F$ e poiché F è un campo $\mathbb{Q} \subset F$, in particolare il campo contiene infiniti elementi.

Se $\operatorname{Ker}\varphi_F = p\mathbb{Z} \Rightarrow \mathbb{Z}/p\mathbb{Z} \subset F$.

Definizione 0.1.

Si dice che il campo F ha **caratteristica** 0 (in simboli $\operatorname{char} F = 0$) se $\operatorname{Ker}\varphi_F = 0$. Si dice che la **caratteristica** di F è un **primo** p se $\operatorname{Ker}\varphi_F = p\mathbb{Z}$.

Campi finiti

Definizione 0.2.

Un campo si dice **finito** se ha cardinalità finita.

Proposizione 0.3.

Sia F un campo finito. Allora $\operatorname{char} F = p$ e $|F| = p^n$.

DIMOSTRAZIONE.

Abbiamo visto che $\operatorname{char} F = 0$ oppure $\operatorname{char} F = p$ e che campi di caratteristica 0 devono contenere $\mathbb{Q}$ e quindi sono infiniti.

Sia quindi $p = \operatorname{char} F$, allora $\mathbb{Z}/p\mathbb{Z} \subset F$. Sia $n = [F : \mathbb{Z}/p\mathbb{Z}]$ (essendo F finito deve in particolare avere dimensione finita su $\mathbb{Z}/p\mathbb{Z}$) e sia $\{v_1, \dots, v_n\}$ una $\mathbb{Z}/p\mathbb{Z}-$ base.

Allora ogni elemento di F si scrive in modo unico come $a_1v_1 + \cdots + a_nv_n$ con $a_i \in \mathbb{Z}/p\mathbb{Z}$. Poiché ogni a_i può assumere esattamente p valori, F ha p^n elementi. ▲

Osservazione 0.4.

La proposizione precedente mostra che non esistono campi finiti di cardinalità qualsiasi ma solo di ordine potenze di un primo. Ad esempio non esistono campi con 6 elementi

Teorema 0.5.

$\forall p$ primo e $\forall n \in \mathbb{N}$ esiste un campo finito con p^n elementi.

DIMOSTRAZIONE.

Se un tale campo esiste deve avere caratteristica p e quindi deve contenere il campo $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Inoltre $F \supset \mathbb{F}_p$ deve essere un'estensione finita e quindi algebrica.

Occorre quindi cercare F tra le estensioni di $\mathbb{F}_p$ tali che $\mathbb{F}_p \subset F \subset \overline{\mathbb{F}_p}$.

Osservo che se $|F| = p^n$ allora $|F^*| = p^n - 1$ e poiché F^* è un gruppo moltiplicativo $\forall \alpha \in F^*$ si ha $\alpha^{p^n-1} = 1$. Ne segue che occorre cercare gli elementi di F tra le radici del polinomio

$$x^{p^n} - x = x(x^{p^n-1} - 1)$$

in una fissata chiusura algebrica $\overline{\mathbb{F}_p}$ di $\mathbb{F}_p$.

Sia $F := \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} = \alpha\}$.

Allora $\#F = \#\{$ radici distinte di $f(x) = x^{p^n} - x$ in $\overline{\mathbb{F}_p}\}$.

Per il criterio della derivata, poiché $f'(x) = -1$ e quindi $(f, f') = 1$, si ha che $f(x)$ ha tutte radici distinte in $\overline{\mathbb{F}_p}$, e quindi ha esattamente p^n radici, cioè $|F| = p^n$. Vediamo che l'insieme F che abbiamo costruito è un campo.

Siano $\alpha, \beta \in F$ (cioè $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$), $\alpha \neq 0$,

allora $\alpha + \beta, \alpha\beta, -\alpha, \alpha^{-1} \in F$: infatti

$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$ (poiché $\operatorname{char} F = p$)

$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$

$(-\alpha)^{p^n} = (-1)^{p^n}\alpha^{p^n} = -\alpha$

$(\alpha^{-1})^{p^n} = \alpha^{-p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$ ▲

Osservazione 0.6.

Il campo che abbiamo costruito è il campo di spezzamento su $\overline{\mathbb{F}_p}$ di $x^{p^n} - x$.

Corollario 0.7.

Siano p un primo, $n \in \mathbb{N}$. Sia $\overline{\mathbb{F}_p}$ una fissata chiusura algebrica di $\mathbb{F}_p$. Esiste un unico sottocampo F di $\overline{\mathbb{F}_p}$ con p^n elementi e

$$F = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} = \alpha\}$$

Dimostrazione.

Il teorema precedente assicura l'esistenza. Inoltre dalla dimostrazione si ha che un qualsiasi campo con p^n elementi contenuto in $\overline{\mathbb{F}_p}$ deve essere contenuto in F . Poiché F ha esattamente p^n elementi, segue la tesi. ▲

Definizione 0.8.

Fissata una chiusura algebrica $\overline{\mathbb{F}_p}$ di $\mathbb{F}_p$ chiamiamo $\mathbb{F}_{p^n}$ il suo unico sottocampo con p^n elementi, cioè

$$\mathbb{F}_{p^n} := \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} = \alpha\}.$$

Osservazione 0.9.

- $\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$ perché quest'ultimo non è un campo.
- $\mathbb{F}_{p^n} \cong (\mathbb{Z}/p\mathbb{Z})^n$ come spazio vettoriale su $\mathbb{Z}/p\mathbb{Z}$ ma **NON** come anelli se $n \geq 2$.

Teorema 0.10.

Ogni sottogruppo moltiplicativo finito di un campo è ciclico.

Dimostrazione.

Sia K un campo e sia $G < K^*$, $|G| = n$. Devo mostrare che G è ciclico. Sia $d \in \mathbb{N}$. Il polinomio $f_d(x) = x^d - 1$ ha al più d radici in K e quindi, $\forall d \mid n$, ha al più d radici in G , cioè il gruppo G contiene al più d elementi di ordine che divide d .

Sia $G_d = \{\alpha \in G \mid \alpha^d = 1\}$, si ha $|G_d| \leq d$.

Se $H < G$ e $|H| = d \Rightarrow H \subset G_d$, e per motivi di cardinalità $H = G_d$. Ne segue che G ha al più un sottogruppo di ordine $d \quad \forall d \mid n$.

Sia $k_d = \#$ elementi di ordine d di G, allora $k_d = \begin{cases} \nearrow \\ \searrow \end{cases} \begin{matrix} \Phi(d) \\ 0 \end{matrix}$

D'altra parte $n = |G| = \sum_{d \mid n} k_d \leq \sum_{d \mid n} \Phi(d) = n$. Necessariamente $k_d = \Phi(d) \quad \forall d \mid n$ e in particolare $k_n = \Phi(n)$, quindi G è ciclico. ▲

Corollario 0.11.

F un campo finito, allora F^* è ciclico.

(In particolare $\mathbb{F}_p^* = \mathbb{Z}/p\mathbb{Z}^*$ è ciclico.)

Corollario 0.12.

Sia $\mathbb{F}_{p^n}^* = <\alpha> \Rightarrow \mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$.

Proposizione 0.13.

$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n$

Dimostrazione.

" $\Rightarrow$ " Sia $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = d$. Poiché $\mathbb{F}_p \subset \mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ si ha $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \cdot [\mathbb{F}_{p^m} : \mathbb{F}_p] = dm$, cioè $m \mid n$.

" $\Leftarrow$ " Sia $n = md$ e sia $\alpha \in \mathbb{F}_{p^m}^*$ (cioè $\alpha^{p^m-1} = 1$). Devo mostrare che $\alpha \in \mathbb{F}_{p^n}^*$, cioè $\alpha^{p^n-1} = 1$.

Osservo che $p^m - 1 \mid p^{md} - 1$, infatti

$p^m \equiv 1 \ (p^m - 1) \Rightarrow$

$p^{md} \equiv 1^d \equiv 1 \ (p^m - 1) \Rightarrow p^m - 1 \mid p^{md} - 1 = p^n - 1$

Quindi $p^n - 1 = \lambda(p^m - 1)$ da cui $\alpha^{p^m-1} = 1 \Rightarrow \alpha^{p^n-1} = \alpha^{\lambda(p^m-1)} = 1^\lambda = 1$ ▲

Campi di spezzamento su $\mathbb{F}_p$

Sia $f(x) \in \mathbb{F}_p[x]$ un polinomio irriducibile. Sia $n = \deg f$ e siano $\{\alpha_1, \ldots, \alpha_n\}$ le sue radici in una fissata chiusura algebrica $\overline{\mathbb{F}_p}$ di $\mathbb{F}_p$.

(Si può dimostrare, usando il criterio della derivata, che un polinomio irriducibile su $\mathbb{F}_p$ ha tutte le radici distinte, quindi le radici distinte sono tante quanto il grado, cioè n).

$\forall i = 1, \dots, n$ si ha $\mathbb{F}_p[\alpha_i] \cong \mathbb{F}_p[x]/(f(x))$ cioè $\mathbb{F}_p[\alpha_i]$ è l'unica sottoestensione di $\overline{\mathbb{F}_p}$ di grado n su $\mathbb{F}_p$, quindi $\mathbb{F}_p[\alpha_i] = \mathbb{F}_{p^n}$, $\forall i = 1, \dots, n$.

In particolare $\alpha_1, \dots \alpha_n \in \mathbb{F}_{p^n} = \mathbb{F}_P[\alpha_1]$ quindi $\mathbb{F}_{p^n}$ è il campo di spezzamento su $\mathbb{F}_p$ di un qualsiasi polinomio irriducibile di grado n.

Teorema 0.14.

Sia $f \in \mathbb{F}_p[x]$ e sia $f(x) = f_1^{e_1}(x) \cdots f_r^{e_r}(x)$ la sua fattorizzazione; poniamo $\deg f_i = d_i$, $\forall i = 1, \dots, n$.

Il campo di spezzamento di f su $\mathbb{F}_p$ è $\mathbb{F}_{p^d}$ dove $d = [d_1, \dots, d_r]$.

Dimostrazione.

Sia $\mathbb{F}_{p^d}$ il campo di spezzamento di f su $\mathbb{F}_p$.

Per definizione $\mathbb{F}_{p^d}$ è l'estensione di $\mathbb{F}_p$ generata da tutte le radici di f, o equivalentemente, da tutte le radici di $f_1(x), \dots, f_r(x)$.

Per quanto visto il campo di spezzamento di f_i su $\mathbb{F}_p$ è $\mathbb{F}_{p^{d_i}}$. Ne segue che $\forall i$ $\mathbb{F}_{p^{d_i}} \subset \mathbb{F}_{p^d}$ cioè $d_i \mid d$ $\forall i$ e poiché $\mathbb{F}_{p^d}$ è generato dalle radici di $f_1(x), \dots, f_r(x)$, d è il minimo intero tale che $d_i \mid d \Rightarrow d = [d_1, \dots, d_r]$. ▲

Campo di spezzamento su $\mathbb{F}_p$ di $x^n - 1$.

Sia $f(x) = x^n - 1 \in \mathbb{F}_p[x]$, $n = p^a m \quad (m, p) = 1$.

Allora, poiché il campo $\mathbb{F}_p$ ha caratteristica p, vale

$$f_n(x) = (x^m - 1)^{p^a} = f_m(x)^{p^a},$$

quindi, posto $G_n = \{a \in \overline{\mathbb{F}_p} \mid \alpha^n = 1\}$, si ha che $G_n = G_m$ e quindi il campo di spezzamento di $f_n(x)$ coincide con quello di $f_m(x)$. Sia $\mathbb{F}_{p^d}$ questo campo di spezzamento.

Lemma 0.15.

$G_n = G_m$ è un gruppo ciclico di ordine m.

Dimostrazione.

$G_m < \mathbb{F}_{p^d}^*$ e quindi è ciclico, in quanto sottogruppo moltiplicativo finito di un campo. Inoltre $|G_m| = \#$ radici distinte di $f_m(x)$ in $\overline{\mathbb{F}_p}$.

Poiché $f'(x) = mx^{m-1} \neq 0$, si ha $(f_m, f'_m) = 1$ e quindi per il criterio della derivata segue che f_m ha m radici distinte. ▲

Lemma 0.16.

$G_n = G_m \subset \mathbb{F}_{p^k} \iff m \mid p^k - 1$

DIMOSTRAZIONE.

" $\Rightarrow$ " $G_m < \mathbb{F}_{p^k}^* \Rightarrow m = |G_m| \mid |\mathbb{F}_{p^k}^*| = p^k - 1$.

" $\Leftarrow$ " Sia $p^k - 1 = ml$ allora $\alpha^m = 1$ implica che $\alpha^{p^k-1} = \alpha^{ml} = 1^l = 1$ e quindi $\forall \alpha \in G_m$ si ha $\alpha \in \mathbb{F}_{p^k}^*$. ▲

Teorema 0.17.

Sia $n = p^a m$, $(m, p) = 1$. Il campo di spezzamento di $f_m(x) = x^m - 1$ su $\mathbb{F}_p$ è $\mathbb{F}_{p^d}$ con $d = \mathrm{ord}_{\mathbb{Z}/m\mathbb{Z}^*} p$.

DIMOSTRAZIONE.

Il campo di spezzamento di f_m su $\mathbb{F}_p$ è $\mathbb{F}_{p^d}$ con d tale che contenga le radici di f_n , cioè tale che $G_n = G_m \subset \mathbb{F}_{p^d}$.

Per il Lemma 0.16 si ha $G_m \subset \mathbb{F}_{p^k} \iff m \mid p^k - 1$ e quindi cerchiamo il minimo k tale che $p^k \equiv 1 \ (m)$ che non è altro che l'ordine moltiplicativo di p modulo m . ▲

Esempio 0.18.

Campo di spezzamento di $f_7(x) = x^7 - 1$ su $\mathbb{F}_3$ e su $\mathbb{F}_{11}$.

$\mathbb{F}_3$: $3^k \equiv 1 \ (7)$ ha come soluzione minima $k = 6$ (2 e 3 non funzionano). Ne segue che in $\mathbb{F}_3$ il polinomio $x^7 - 1$ si fattorizza come $(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$, cioè il fattore di grado 6 è necessariamente irriducibile.

$\mathbb{F}_{11}$: $11^k \equiv 1 \ (7)$ si calcola che l'ordine è $k = 3$, quindi il campo di spezzamento è $\mathbb{F}_{11^3}$.

Ne segue che la fattorizzazione di $x^7 - 1$ contiene almeno un polinomio irriducibile di grado 3 e che gli altri fattori irriducibili hanno grado che divide 3 , quindi 1 o 3 . In particolare $x^7 - 1 = (x-1)h(x)g(x)$ con $h(x)$ e $g(x)$ irriducibili di grado 3 perché l'unica radice di $x^7 - 1$ in $\mathbb{F}_{11}$ è 1 (non ci sono elementi di ordine 7 in $\mathbb{F}_{11}^*$).