Introduzione alla teoria dei campi

§1.1 La caratteristica di un campo

Si consideri il seguente omomorfismo:

$$\psi : \mathbb{Z} \to \mathbb{K},$$

completamente determinato dalla condizione $\psi(1) = 1$, dacché $\mathbb{Z}$ è generato da 1. Si studia innanzitutto il caso in cui $\operatorname{Ker}\psi = (0)$. In questo caso, ψ è un monomorfismo, e dunque $\mathbb{Z} \cong \operatorname{Im}\psi$.

Pertanto, $\mathbb{K}$ ammetterebbe come sottoanello una copia isomorfa di $\mathbb{Z}$. Inoltre, poiché $\mathbb{K}$ è un campo, deve anche ammetterne gli inversi, e quindi ammetterebbe come sottocampo una copia isomorfa di $\mathbb{Q}$. La seguente definizione classificherà questi tipi di campo.

Definizione 1.1.1. Si dice che un campo $\mathbb{K}$ è di **caratteristica zero** ($\operatorname{char}\mathbb{K} = 0$), quando $\operatorname{Ker}\psi = (0)$.

Altrimenti, se $\operatorname{Ker}\psi \neq (0)$, dacché $\mathbb{Z}$ è un anello euclideo, $\operatorname{Ker}\psi$ deve essere monogenerato da un intero n, ossia $\operatorname{Ker}\psi = (n)$.

Tuttavia non tutti gli interi sono ammissibili. Sia infatti n non primo, allora $n = ab$ con a, $b \neq \pm 1$. Si nota innanzitutto che $\psi(a) \neq 0$, se infatti fosse nullo, n dovrebbe dividere a, impossibile dal momento che $|a| < |n|$, ↯. Analogamente anche $\psi(b) \neq 0$.

Se n fosse generatore di $\operatorname{Ker}\psi$ si ricaverebbe allora che:

$$\underbrace{\psi(a)}_{\neq 0}\underbrace{\psi(b)}_{\neq 0} = \psi(n) = 0,$$

che è assurdo, dal momento che $\mathbb{K}$, in quanto campo, è anche un dominio. Quindi n deve essere un numero primo. In particolare, allora $\mathbb{Z}_p = \mathbb{Z}/(p) \cong \operatorname{Im}\psi$, ossia $\mathbb{K}$ contiene una copia isomorfa di $\mathbb{Z}_p$, a cui ci riferiremo semplicemente con $\mathbb{F}_p$.

Allora, poiché sia $\mathbb{K}$ che $\mathbb{F}_p$ sono campi, $\mathbb{K}$ è uno spazio vettoriale su $\mathbb{F}_p$. Si può dunque classificare quest'ultimo tipo di campi con la seguente definizione:

Definizione 1.1.2. Si dice che un campo $\mathbb{K}$ è di **caratteristica** p ($\operatorname{char}\mathbb{K} = p$) quando $\operatorname{Ker}\psi = (p)$, con p primo.

Osservazione. La caratteristica di un campo **non** distingue i campi finiti dai campi infiniti. Esistono infatti campi infiniti di caratteristica p, come il campo delle funzioni razionali su $\mathbb{Z}_p$:

$$\mathbb{Z}_p(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x),\, g(x) \in \mathbb{Z}_p[x],\, g(x) \neq 0 \right\}.$$

Infatti $\psi(p) = p\,\psi(1) = 0$.

§1.2 Prime proprietà dei campi di caratteristica p

Come si è appena visto, un campo $\mathbb{K}$ di caratteristica p contiene al suo interno un sottocampo $\mathbb{F}_p$ isomorfo a $\mathbb{Z}_p$, ed è per questo uno spazio vettoriale su di esso. A partire da questa informazione si può dimostrare la seguente proposizione.

Proposizione 1.2.1

Sia $\mathbb{K}$ un campo di caratteristica p. Allora, per ogni elemento v di $\mathbb{K}$, $pv = 0$.

Dimostrazione. Considerando ogni elemento di $\mathbb{K}$ come vettore e p come scalare, si ricava che:

$$pv = \underbrace{(1 + \ldots + 1)}_{p \text{ volte}} v = \underbrace{(\psi(1) + \ldots + \psi(1))}_{p \text{ volte}} v = \psi(p)v = 0v = 0.$$

□

Mentre, partendo da questa proposizione, si può dimostrare il seguente teorema.

Teorema 1.2.2 (*Teorema del binomio ingenuo*)

Siano a e b elementi di un campo di caratteristica p. Allora $(a+b)^p = a^p + b^p$.

Dimostrazione. Per dimostrare la tesi si applica la formula del binomio di Newton nel seguente modo:

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

Tuttavia, dal momento che p è un fattore di tutti i binomiali per $1 \leq i \leq p-1$, tutti i termini computati con queste i sono nulli per la *Proposizione 1.2.1*. Si desume così l'identità della tesi. □

§1.3 L'omomorfismo di Frobenius

Definizione 1.3.1. Dato un campo $\mathbb{K}$ di caratteristica p, si definisce **omomorfismo di Frobenius** per il campo $\mathbb{K}$ la funzione:

$$\mathcal{F} : \mathbb{K} \to \mathbb{K},\ a \mapsto a^p.$$

Osservazione. In effetti, l'omomorfismo di Frobenius è un omomorfismo.

Infatti, $\mathcal{F}(1) = 1^p = 1$. Inoltre tale funzione rispetta la linearità per il *Teorema del binomio ingenuo*:

$$\mathcal{F}(a+b) = (a+b)^p = a^p + b^p = \mathcal{F}(a) + \mathcal{F}(b),$$

e chiaramente anche la moltiplicatività:

$$\mathcal{F}(ab) = (ab)^p = a^p b^p = \mathcal{F}(a)\mathcal{F}(b).$$

Proposizione 1.3.2

L'omomorfismo di Frobenius di un campo $\mathbb{K}$ di caratteristica p è un monomorfismo.

Dimostrazione. Si prenda in considerazione $\operatorname{Ker}\mathcal{F}$. Esso è sicuramente un ideale diverso da $\mathbb{K}$, dacché $1 \notin \operatorname{Ker}\mathcal{F}$. Tuttavia, se $\operatorname{Ker}\mathcal{F} \neq (0)$, $\operatorname{Ker}\mathcal{F}$, dal momento che $\mathbb{K}$, in quanto campo, è un anello euclideo, e quindi un PID, è monogenerato da un invertibile.

Se però così fosse, $\operatorname{Ker}\mathcal{F}$ coinciderebbe con il campo $\mathbb{K}$ stesso, ↯. Quindi $\operatorname{Ker}\mathcal{F} = (0)$, da cui la tesi. □

Proposizione 1.3.3

Sia $\mathbb{K}$ un campo finito di caratteristica p. Allora l'omomorfismo di Frobenius è un automorfismo.

Dimostrazione. Dalla *Proposizione 1.3.2* è noto che $\mathcal{F}$ sia già un monomorfismo. Dal momento che il dominio e il codominio sono lo stesso e constano entrambi dunque di un numero finito di elementi, se $\mathcal{F}$ non fosse surgettivo, vi sarebbe un elemento di $\mathbb{K}$ a cui non è associato nessun elemento di $\mathbb{K}$ mediante $\mathcal{F}$.

Per il principio dei cassetti, allora, spartendo $|\mathbb{K}|$ elementi in $|\mathbb{K}| - 1$ elementi, vi sarebbe almeno un elemento dell'immagine a cui sarebbero associati due elementi del dominio. Tuttavia questo è assurdo dal momento che $\mathcal{F}$ è un monomorfismo. Quindi $\mathcal{F}$ è un epimorfismo.

Dacché $\mathcal{F}$ è contemporaneamente un endomorfismo, un monomorfismo e un epimorfismo, è allora anche un automorfismo. □

Proposizione 1.3.4

Sia $\mathbb{K}$ un campo di caratteristica p e si definisca l'insieme dei punti fissi del suo omomorfismo di Frobenius:

$$\mathrm{Fix}(\mathcal{F}^n) = \{a \in \mathbb{K} \mid \mathcal{F}^n(a) = a\}.$$

Allora $\mathrm{Fix}(\mathcal{F}^n)$ è un sottocampo di $\mathbb{K}$.

Dimostrazione. Affinché $\mathrm{Fix}(\mathcal{F}^n)$ sia un sottocampo di $\mathbb{K}$, la sua somma e la sua moltiplicazione devono essere ben definite, e ogni suo elemento deve ammettere un inverso sia additivo che moltiplicativo.

Siano allora a, $b \in \mathrm{Fix}(\mathcal{F}^n)$. $\mathcal{F}^n$ è un omomorfismo, in quanto è composizione di omomorfismi (in particolare, dello stesso omomorfismo $\mathcal{F}$). Sfruttando le proprietà degli omomorfismi si dimostra dunque che $a + b \in \mathrm{Fix}(\mathcal{F}^n)$:

$$\mathcal{F}^n(a + b) = \mathcal{F}^n(a) + \mathcal{F}^n(b) = a + b,$$

e che $ab \in \mathrm{Fix}(\mathcal{F}^n)$:

$$\mathcal{F}^n(ab) = \mathcal{F}^n(a)\mathcal{F}^n(b) = ab.$$

Analogamente si dimostra che $-a \in \mathrm{Fix}(\mathcal{F}^n)$:

$$\mathcal{F}^n(-a) = -\mathcal{F}^n(a) = -a,$$

e che $a^{-1} \in \mathrm{Fix}(\mathcal{F}^n)$:

$$\mathcal{F}^n(a^{-1}) = \mathcal{F}^n(a)^{-1} = a^{-1}.$$

□

§1.4 Classificazione dei campi finiti

Teorema 1.4.1

Ogni campo finito $\mathbb{K}$ di caratteristica p consta di p^n elementi, con $n \in \mathbb{N}^+$.

Dimostrazione. Come già detto precedentemente, $\mathbb{K}$ è uno spazio vettoriale su una copia isomorfa di $\mathbb{Z}_p$, $\mathbb{F}_p$.

Si consideri allora il grado $[\mathbb{K} : \mathbb{F}_p]$. Sicuramente questo grado non è infinito, dal momento che $\mathbb{K}$ non ha infiniti elementi. Quindi $[\mathbb{K} : \mathbb{F}_p] = n \in \mathbb{N}$.

Sia dunque $(k_1, k_2, \dots, k_n)$ una base di $\mathbb{K}$ su $\mathbb{F}_p$. Ogni elemento a di $\mathbb{K}$ si potrà dunque scrivere come:

$$a = \alpha_1 k_1 + \ldots + \alpha_n k_n, \quad \alpha_1, \dots, \alpha_n \in \mathbb{F}_p,$$

e dunque vi saranno in totale p^n elementi, dove ogni p è contato dal numero di elementi che è possibile associare ad ogni coefficiente, ossia $|\mathbb{F}_p| = p$, per il numero di elementi appartenenti alla base, ossia $[\mathbb{K} : \mathbb{F}_p] = n$, da cui la tesi. □

Teorema 1.4.2

Per ogni $n \in \mathbb{N}^+$ e per ogni numero primo p esiste un campo finito con p^n elementi.

Dimostrazione. Si consideri il polinomio $x^{p^n} - x$ su $\mathbb{Z}_p$ e un suo campo di spezzamento A. $\mathrm{Fix}(\mathcal{F}^n)$, per la *Proposizione 1.3.4*, è un sottocampo, e contiene esattamente le radici di $x^{p^n} - x$, che in A si spezza in fattori lineari, per definizione.

La derivata di $x^{p^n} - x$ è $p^n x^{p^n - 1} - 1 \equiv -1$, dacché A è uno spazio vettoriale su $\mathbb{Z}_p$, e pertanto vale ancora la *Proposizione 1.2.1*. Dal momento che -1 e $x^{p^n} - x$ non hanno fattori lineari in comune, per il *Criterio della derivata*, $x^{p^n} - x$ non ammette radici multiple.

Allora $\mathrm{Fix}(\mathcal{F}^n)$ è un campo con p^n elementi, ossia tutte le radici di $x^{p^n} - x$ (e coincide quindi con il campo di spezzamento A), da cui la tesi. □