Campi Finiti

Def. Un dominio integro D è un anello in cui vale la regola

$$\boxed{ax = bx\,,\quad x \neq 0 \quad \Rightarrow \quad a = b}$$

$\boxed{\text{EX}}$ Un dominio integro finito è un campo.

Dim. D dominio integro finito.
Fisso $\alpha \in D$, $\alpha \neq 0$, voglio trovare $x \in D$ tale che $\alpha \cdot x = 1$. Sia

$$f_\alpha : D \to D$$
$$x \mapsto \alpha \cdot x$$

Siccome D è un dominio e $\alpha \neq 0$, f_α è iniettiva. D'altra parte D è finito dunque f_α è surgettiva (principio della piccionaia).
Ma allora $\exists\, x \in D$ t.c. $\alpha \cdot x = f_\alpha(x) = 1$.

QED

$\rightsquigarrow$ $\mathbb{Z}/n\mathbb{Z}$ è integro $\Leftrightarrow$ n è primo

$\Leftrightarrow$ è un campo.

D dominio integro, definisco

$$\phi : \mathbb{Z} \to D \qquad \text{omomorfismo (non nullo)}$$

$$n \mapsto \underbrace{1 + \dots + 1}_{n \text{ volte}}$$

Definisco la caratteristica di D come segue

$$\boxed{\mathrm{Char}(D) = \text{unico generatore positivo di } \mathrm{Ker}(\phi)}.$$

Nota: siccome $\mathbb{Z}/\mathrm{Ker}(\phi) \simeq$ sottoanello di D, che è integro, $\mathbb{Z}/\mathrm{Ker}(\phi)$ è integro. Dunque

$$\boxed{\mathrm{Char}(D) = 0 \text{ oppure } \mathrm{Char}(D) = p \text{ primo.}}$$

Nota:

$\leadsto$ $\mathrm{Char}(D) = 0 \Rightarrow \mathbb{Z} \subseteq D$.

$\leadsto$ $\mathrm{Char}(D) = p \Rightarrow \mathbb{F}_p \subseteq D$.

Fatto: $\mathbb{F}$ campo finito $\Rightarrow |\mathbb{F}| = p^n$ con $n \geq 1$
p primo.

Dim.

$$|\mathbb{F}| < \infty \Rightarrow \mathrm{Char}(\mathbb{F}) \neq 0$$

Sia $p = \mathrm{Char}(\mathbb{F})$. $\mathbb{F}$ ha una naturale struttura di $\mathbb{F}_p$-spazio vettoriale

$$\cdot : \mathbb{F}_p \times \mathbb{F} \to \mathbb{F}$$
$$\underline{k} \cdot x = \underbrace{(1 + \dots + 1)}_{k \text{ volte}} \cdot x$$

prodotto di $\mathbb{F}$.

$$|\mathbb{F}| < +\infty \Rightarrow \dim_{\mathbb{F}_p}(\mathbb{F}) < +\infty$$

Dunque se $n = \dim_{\mathbb{F}_p}(\mathbb{F})$ ho che

$$\mathbb{F} \simeq \underbrace{\mathbb{F}_p \times \dots \times \mathbb{F}_p}_{n \text{ volte}}$$

isom. di $\mathbb{F}_p$-spazi vettoriali

$$\Rightarrow |\mathbb{F}| = |\underbrace{\mathbb{F}_p \times \dots \times \mathbb{F}_p}_{n \text{ volte}}| = \underbrace{|\mathbb{F}_p| \cdots |\mathbb{F}_p|}_{n \text{ volte}} = p^n.$$

QED.

TEOREMA DI CLASSIFICAZIONE DEI CAMPI FINITI:

Per ogni p primo e $n \geq 1$ esiste un campo finito $\mathbb{F}$ di caratteristica p con p^n elementi.

Inoltre due campi finiti con lo stesso numero di elementi sono isomorfi.

ESISTENZA: $\overline{\mathbb{F}}_p$ = chiusura algebrica di $\mathbb{F}_p$.

Considero

$$\mathbb{F}_{p^n} = \left\{ \alpha \in \overline{\mathbb{F}}_p \text{ t.c. } \alpha^{p^n} - \alpha = 0 \right\} \subseteq \overline{\mathbb{F}}_p$$

Chiaramente $|\mathbb{F}_{p^n}| = p^n$. Dico che $\mathbb{F}_{p^n}$ è un sotto_campo di $\overline{\mathbb{F}}_p$. Infatti:

$$\alpha, \beta \in \mathbb{F}_{p^n} \Rightarrow (\alpha+\beta)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{i} \cdot \alpha^i \cdot \beta^{p^n - i}$$

$$= \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$$

p divide $\binom{p^n}{i}$ per $0 < i < p^n$ e $\mathrm{Char}(\overline{\mathbb{F}}_p) = p$

$$\Rightarrow \alpha + \beta \in \mathbb{F}_{p^n}$$

e le altre verifiche sono immediate.

UNICITÀ: osservo per cominciare che per ogni $n \geq 1$

$\mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}_p}$ è l'unico sottocampo di $\overline{\mathbb{F}_p}$ con cardinalità p^n. Infatti:

$$\begin{array}{l} K \subseteq \overline{\mathbb{F}_p} \text{ sottocampo} \\ \text{con } |K| = p^n \end{array} \Rightarrow \alpha^{p^n} = \alpha \quad \forall \alpha \in K$$

↑ teo. di Lagrange

$$\Rightarrow K \subseteq \mathbb{F}_{p^n}$$

$$\Rightarrow K = \mathbb{F}_{p^n}$$

↑ perché hanno la stessa cardinalità.

Con questa osservazione per mostrare la tesi basta far vedere che preso un campo finito $\mathbb{F}$ di $\mathrm{Char} = p$ esiste un immersione (= omo. iniettivo) $\phi : \mathbb{F} \hookrightarrow \overline{\mathbb{F}_p}$.

$\mathbb{F}^*$ è ciclico, prendo $g \in \mathbb{F}^*$ generatore.

Definisco

$$\begin{array}{ll} \varphi : \mathbb{F}_p[z] \to \mathbb{F} & \text{omomorfismo} \\ u(z) \mapsto u(g) & \text{surgettivo} \end{array}$$

$\mathrm{Ker}(\varphi) = (q(z)) \subseteq \mathbb{F}_p[z]$ con $q(z)$ irriducibile.

$\left(\mathbb{F}_p[z]/(q(z)) \cong \mathbb{F} \text{ che è un} \right.$

Prendo $\alpha \in \overline{\mathbb{F}_p}$ radice di $q(z) \in \mathbb{F}_p[z]$.

Definisco:

$$\phi : \mathbb{F} \simeq \mathbb{F}_p[z]/(q(z)) \longrightarrow \overline{\mathbb{F}_p}$$

$$[u(z)] \longmapsto u(\alpha)$$

ϕ è ben definito $\left(u(\alpha) + q(\alpha) \cdot k(\alpha) = u(\alpha) \right)$

ϕ è un omomorfismo (verifica immediata).

ϕ è iniettivo:

$$\phi[u(z)] = 0 \Rightarrow u(\alpha) = 0$$

$z - \alpha$ è fattore comune $\Rightarrow \gcd(q(z), u(z)) \neq 1$

$q(z)$ è irrid. $\Rightarrow u(z) = k(z) \cdot q(z)$

$\Rightarrow \gcd = q(z)$

$\Rightarrow q(z) \mid u(z) \Rightarrow [u(z)] = [k(z) \cdot q(z)] = 0$

QED.

EX Mostrare che se $\mathbb{F}$ è un campo finito allora vale la formula

$$\boxed{\prod_{\alpha\in\mathbb{F}^*} \alpha = -1}$$ (formula di Wilson)

Dim. Considero il polinomio

$$z^{n-1}-1 \in \mathbb{F}[z] \quad \text{dove } n=|\mathbb{F}|.$$

Per il teo. di Lagrange

$$\alpha^{n-1}=1 \quad \text{per ogni } \alpha\in\mathbb{F}^*$$

$\Rightarrow$ tutti gli elementi di $\mathbb{F}^*$ sono radici di $z^{n-1}-1$

$$\Rightarrow \quad \boxed{z^{n-1}-1 = \prod_{\alpha\in\mathbb{F}^*}(z-\alpha)}$$

$|\mathbb{F}^*|=n-1$ e $\deg(z^{n-1}-1)=n-1$

Valutando in $z=0$ si trova che

$$-1 = \prod_{\alpha\in\mathbb{F}^*} -\alpha = (-1)^{|\mathbb{F}|-1}\cdot\prod_{\alpha\in\mathbb{F}^*}\alpha = \prod_{\alpha\in\mathbb{F}^*}\alpha.$$

se $\operatorname{char}(\mathbb{F})=2$ $\quad -1=1$ ok

se $\operatorname{char}(\mathbb{F})>2$ $\quad |\mathbb{F}|$ è dispari ok

$\rightsquigarrow$ Nota: se applico questo risultato nel caso $\mathbb{F}=\mathbb{Z}/p\mathbb{Z}$ trovo che

$$\boxed{(p-1)! \equiv -1 \pmod p}$$