Caratteristica di un campo

Considero $\phi : \mathbb{Z} \to \mathbb{K}$ con $\phi(1) = 1$. Notiamo che $\ker \phi$ è un'ideale di $\mathbb{Z}$, ed è quindi principale (i.e. $\ker \phi = (d)$).

$d = 0$ $\to$ $\mathbb{K} \supset \text{Imm}\ \phi \cong \mathbb{Z}$. Inoltre $\mathbb{K}$ contiene anche gli inversi di $\text{Imm}\ \phi$, ossia una copia di $\mathbb{Q}$. $\mathbb{K}$ è comunque infinito e si pone **$\text{char}\ \mathbb{K} = 0$.**

$d \neq 0$ $\to$ d dev'essere primo, altrimenti: sia $d = ab$, $\phi(a), \phi(b) \neq 0 \Rightarrow$

$\Rightarrow \phi(ab) = \phi(d) = 0$, impossibile perché $\mathbb{K}$ è un campo, quindi un dominio, $\lightning$. Allora sia $d = p$ primo. $\underbrace{\mathbb{Z}/(p)}_{\mathbb{Z}_p} \cong \text{Imm}\ \phi \subset \mathbb{K}$. Si pone **$\text{char}\ \mathbb{K} = p$.**

Oss. Notiamo che $\mathbb{K}$ è uno spazio vettoriale su $\mathbb{Z}_p$. Sia $v \in \mathbb{K}$, vale che

$$\underbrace{v + \dots + v}_{p \text{ volte}} = \underbrace{(1 + \dots + 1)}_{p \text{ volte}} v = (\phi(1) + \dots + \phi(1))\, v = \phi(p)\, v = 0v = 0$$

Oss. Esistono campi di caratteristica prima infiniti.

es. $\mathbb{Z}_p'(x) = \left\{ \dfrac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in \mathbb{Z}_p[x],\ g(x) \neq 0 \right\}$ ha infiniti elementi, ma caratteristica p.

Omomorfismo di Frobenius di campi di caratt. p

$$F: \mathbb{K} \to \mathbb{K}, \quad a \mapsto a^{\overbrace{p}^{\operatorname{char}\mathbb{K}}}$$ OMOMORFISMO DI FROBENIUS

OSS. F è iniettivo perché $\ker F$ è ideale di un campo, ossia o è (0) o $\underbrace{\mathbb{K} \text{ stesso}}_{\text{impossibile}}$.

Teorema $\psi: E \to E$ omomorfismo con E campo $\Rightarrow$ $\operatorname{Fix}_\psi = \{\alpha \in E \mid \psi(\alpha) = \alpha\}$ è sottocampo di E.

Def. Sia F campo e sia $f(x) \in F[x]$ un polinomio non nullo. Una estensione finita E di F ($F \subseteq E$, $[E:F] < \infty$) si dice CAMPO DI SPEZZAMENTO su F se:

(i) in $E[x]$ $f(x)$ si fattorizza come prodotto di polinomi di grado 1 (i.e. ha tutte le radici)

(ii) ogni sottocampo proprio di $E[x]$ contenente F non ammette almeno una radice di $f(x)$ (i.e. $E[x]$ è minimale).

OSS. Se $f(x)$ ammette già tutte le radici in $F[x]$, il suo campo di spezzamento è F stesso.

NOTA $[F:K]$ viene anche chiamato **GRADO**.

Prop. $\mathbb{K}$ campo, sia $f(x) \in \mathbb{K}[x]$ di grado n non nullo. Se E è un campo di sp. di $f(x)$ su $\mathbb{K}$, $[E:K] \leq n!$.

OSS. I camp: di spezzamento non sono generalmente unici, benché siano **isomorfi**.

es. $\mathbb{Q}(\sqrt[3]{2}, w)$ e $\mathbb{Q}(\sqrt[3]{2}, w^2)$ sono entrambi camp: di spezzamento di x^3-2 su $\mathbb{Q}$. Infatti: $\mathbb{Q}(\sqrt[3]{2}, w) \cong \mathbb{Q}(\sqrt[2]{2}, w^2)$.

Conseguenze di Frobenius

Sia L campo finito, allora $\operatorname{char} L = p$. $[L : \mathbb{Z}_p] = m \in \mathbb{N}$. Allora $|L| = p^m$ (infatti $L = \operatorname{Span}(l_1, \dots, l_m)$).

Considero $L^* = L \setminus \{0\}$, per Lagrange se $g \in L^*$, $g^{|L^*|} = 1 \Rightarrow$

$\Rightarrow g^{|L^*|+1} = g \Rightarrow g^{p^m} = g$. Inoltre $0^{p^m} = 0$.

Ossia tutti gli elementi di L sono tutte le radici di $x^{p^m} - x$, ossia L è un campo di sp. di $x^{p^m} - x$ su L.

Teorema Dato p primo e $m \geq 1$, $\exists$ L campo con p^m elementi.

Considero R un campo di spezzamento di $x^{p^m} - x$ su $\mathbb{Z}_p$, $\underbrace{F^m}_{F \circ F \circ \dots \circ F \text{ n volte}} : R \to R$, $r \to r^{p^m}$ e Fix_{F^m}.

Gli elementi di Fix_{F^m} sono esattamente le radici di $x^{p^m} - x$. Tali radici sono distinte per il criterio della derivata: $p^m x^{p^m - 1} - 1 \equiv -1$ non ha fattori in comune con $x^{p^m} - x$ che siano non invertibili.

Quindi $x^{p^m} - x$ ha p^m radici in Fix_{F^m}; essendo p^m il massimo di radici che può avere, si conclude che $|Fix_{F^m}| = p^m$, ossia è il campo ricercato.

□

OSS. Poiché $Fix_{F^m} \subset R$ contiene ogni radice di $x^{p^m} - x$, si conclude anche che $Fix_{F^m} = R$.