CAMPI PERFETTI

In questa lezione F sarà un campo

Definizione Sia $q(x) \in F[x]$

consideriamo E campo di spezzamento di $q(x)$:

$$q(x) = (x-r_1)^{k_1} \dots (x-r_s)^{k_s}$$

Definiamo k_i la *molteplicità* di r_i;

r_i si dice *semplice* se $k_i = 1$

r_i si dice *multiplo* se $k_i > 1$

Oss: se esiste $\bar{E}$ un altro campo di spezzamento otteniamo le stesse molteplicità perché E ed $\bar{E}$ sono isomorfe.

È utile lavorare con campi di spezzamento di polinomi con tutti radici semplici (o con tutte le radici distinte come dicevamo prima)
È sempre possibile farlo? Più precisamente:
Ogni estensione che è un campo di spezzamento può essere visto come campo di spezz di un polinomio con tutte radici semplici?

Osservazione 1 sia $q(x) = q_1^{e_1}(x) \dots q_k^{e_k}(x) \in F[x]$ con $q_i(x)$ irriducibile, allora il campo di spezzamento di $q(x)$ coincide con il campo di spezzamento di $h(x) = q_1(x) \dots q_k(x)$

Osservazione 2 $q(x), h(x) \in F[x]$, irriducibili possono avere radici in comune in un estensione di F?

Siccome q, h irriducibili $MCD(q(x), h(x)) = 1$

Allora esistono $g(x)$ e $s(x) \in F[x]$ tali che

$g(x)q(x) + s(x)h(x) = 1$ (Lemma di Bezout)

Se in $E \supseteq F$ esiste $r \in E$ t.c. $q(r) = h(r) = 0$

abbiamo che $\underbrace{g(r)q(r) + s(r)h(r)}_{0} = 1$ in $E[x]$

ottenendo un assurdo.

Possiamo concludere $q(x)$ e $h(x)$ non hanno radici comuni in nessuna estensione di F.

Ci rimane da rispondere alla seguente domanda
Un polinomio irriducibile può avere radici multiple?

Def. Sia $q(x) = \sum_{k=0}^{n} a_k x^k \in F[x]$, definiamo

il polinomio derivato di $q(x)$

$$q'(x) = \sum_{k=1}^{n} k a_k x^{k-1}$$

[questa è una derivazione "formale" che vale in ogni campo F (non solo $\mathbb{R}$) che ricalca le regole dell'usuale derivazione]

Proposizione Siano $h, g \in F[x]$, abbiamo che:

1) $(h+g)' = h' + g'$

2) $(h \cdot g)' = h'g + g'h$

3) Se $h(x) = x$, $h'(x) = 1$

4) Se $h(x) = a$, $a \in F$ (h costante) allora $h'(x) = 0$

Dimostrazione per esercizio

Osservazione: non è vero il viceversa!

Sia $q(x) = x^p \in \mathbb{Z}_p[x]$, allora $q'(x) = p x^{p-1} = 0$

Teorema: $q(x) \in F[x]$ non costante

le radici di $q(x)$ nel campo di spezzamento sono semplici

$\Longleftrightarrow$

$MCD(q, q') = 1$ in $F[x]$

Problema: dimostrare il teorema

[Ritorniamo alle nostre domande: un polinomio irriducibile può avere radici multiple?]

Se $q(x)$ è irriducibile in $F[x]$ con radici multiple $\Rightarrow$ (Teorema)

$MCD(q, q') \neq 1 \Rightarrow q(x) \mid q'(x)$

(a meno di prodotti per elementi invertibili $q(x)$ ha solo due divisori $q(x)$ e 1)

Se $q'(x) \neq 0 \Rightarrow \deg q' < \deg q$ e questo è impossibile

Possiamo concludere:

$q(x)$ irriducibile con radici multiple $\Rightarrow q'(x) = 0$

Se $\operatorname{char} F = 0$, allora $q' = 0$ implica q costante e quindi q non può essere irriducibile

Prop: se $\operatorname{char} F = 0$, i polinomi irriducibili in $F[x]$ hanno tutti radici semplici

Def: 1) $q(x) \in F[x]$ si dice separabile se ogni fattore irriducibile di $q(x)$ ha solo radici semplici

2) F si dice perfetto se ogni polinomio di $F[x]$ è separabile

Prop $\operatorname{char} F = 0 \Rightarrow F$ perfetto

Oss: nei campi perfetti possiamo rappresentare ogni campo di spezzamento come campo di spezz di un polinomio senze radici multiple

---

Se $\operatorname{char} F = p$ consideriamo $q(x)$ t.c. $q'(x) = 0$

$$q(x) = \sum_{k=0}^{n} a_k x^k$$

$q'(x) = 0 \iff k a_k = 0$ per ogni $k = 1, \dots, n$

$\iff a_k = 0$ per ogni $k = 1, \dots, n$ $k \neq 0 \bmod p$

$\iff q(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots + a_{hp} x^{hp}$

$\iff q(x) = p(x^p)$ con $p(x) \in F[x]$

Domande: qualcuno di questi polinomi può essere irriducibile? Se la risposte è affermativa abbiamo trovato polinomi irriducibili con radici multiple

Proposizione 1) $\operatorname{char} F = p$, $\forall a, b \in F$ $(a+b)^p = a^p + b^p$

2) sia $\varphi : F \to F$ t.c. $\varphi(a) = a^p$ allora φ è un monomorfismo e $\varphi(F)$ è un sottocampo di F

Dimostrazione per esercizio

Notazione $F^p \overset{def}{=} \varphi(F) = \{a^p \mid a \in F\}$

Lemma: $\mathrm{char} F = p$, se $a \in F$ allora vale che

o $x^p - a$ è irriducibile in $F[x]$ oppure $x^p - a = [q(x)]^p$ con $q(x) \in F[x]$

Dimostrazione: Supponiamo che $x^p - a$ sia riducibile cioè esistano $g(x)$ e $h(x) \in F[x]$ tali che $x^p - a = g(x)h(x)$ e $\deg(g(x)) < p$

Sia E un campo di spezzamento di $x^p - a$ su F e sia $b \in E$ radice di $x^p - a \Rightarrow b^p - a = 0$

$\Rightarrow x^p - a = x^p - b^p = (x-b)^p = g(x)h(x)$ in $F[x]$.

$\Rightarrow g(x) = (x-b)^k$ e $b^k \in F$ (perché $g(x) \in F(x)$)

Abbiamo che b^p e $b^k \in F$

Siccome $k < p$ abbiamo che $MCD(p,k) = 1$

per cui esistono $\lambda, \mu \in \mathbb{Z}$ tali che $\lambda p + \mu k = 1$ (Lemma Bezout)

Otteniamo

$$\underset{\in F}{(b^p)^\lambda} + \underset{\in F}{(b^k)^\mu} = b^{p\lambda + k\mu} = b^1 = b \in F \quad (\text{somma di elementi di } F)$$

$$\Rightarrow (x^p - a) = (x-b)^p \text{ in } F[x]$$

Teorema $\quad \operatorname{char} F = p$

F perfetto $\iff F = F^p$

Dim

"$\Rightarrow$"

Sia $a \in F$ considero $x^p - a \in F[x]$

$x^p - a$ riducibile in $E[x]$ con E campo spezzamento

$\Rightarrow$ (per Lemma)

$(x^p - a) = (x-b)^p$ in $E[x]$

$\Rightarrow$

$x^p - a$ ha radici multiple

$\Rightarrow$ (perchè F perfetto)

$x^p - a$ riducibile in F

$\Rightarrow$ (per Lemma)

$(x^p - a) = (x-b)^p$ in $F[x]$ con $b \in F$

$\Rightarrow$

esiste b t.c $a = b^p$

$\Rightarrow$

$a \in F^p$

Osservazione:

In generale vale che se $a \notin F^p \Rightarrow x^p - a$ irriducibile

"$\Leftarrow$"

Sia $q(x)$ un polinomio irriducibile

Se $MCD(q(x), q'(x)) \neq 1 \Rightarrow q'(x) = 0$

$\Rightarrow q(x) = p(x^p)$ con $p(x) \in F[x]$

$\Rightarrow q(x) = \sum_{k=0}^{n} a_k (x^k)^p$

Per ipotesi $F = F^p$ e quindi per ogni k esisbe $b_k \in F$ tale che

$b_k^p = a_k \Rightarrow q(x) = \sum_{k=0}^{n} b_k^p (x^k)^p$

$\Rightarrow q(x) = \left(\sum_{k=0}^{n} b_k x^k \right)^p$

$\Rightarrow q(x)$ riducibile ASSURDO

Allora $MCD(q(x), q'(x)) = 1 \Rightarrow q(x)$ non ha radici multiple

Corollario Ogni campo finito è perfetto

Dim F finito $\Rightarrow$ char $F = p$

Sia $\varphi : F \to F$ t.c $\varphi(b) = b^p$

φ monomorfismo e F finito $\Rightarrow \varphi$ suriettivo $\Rightarrow$

$\Rightarrow F = \varphi(F) = F^p \Longrightarrow$ (Teorema) F perfetto

(per definizione)

Domande Esistono campi non perfetti?

Esempio $\mathbb{Z}_p(t) = \left\{ \frac{h(t)}{q(t)} \;\middle|\; \begin{matrix} h(t)\,q(t) \in \mathbb{Z}_p[t] \\ q(t) \neq 0 \end{matrix} \right\}$

$\mathbb{Z}_p(t)$ è il campo dei quozienti di $\mathbb{Z}_p(t)$

- $\mathbb{Z}_p(t)$ ha caratteristica p
- consideriamo $t \in \mathbb{Z}_p(t)$ e vedremo che $t \notin (\mathbb{Z}_p(t))^p$

Supponiamo per assurdo

$$t = \left[\frac{h(t)}{q(t)}\right]^p = \left(\frac{a_n t^n + \dots + a_0}{b_m t^m + \dots + b_0}\right)^p =$$

$$= \frac{a_n^p t^{np} + \dots + a_0^p}{b_m^p t^{mp} + \dots + b_0^p}$$

da cui $\underbrace{b_m^p t^{mp+1} + \dots + b_0^p t}_{\text{tutte potenze} \equiv 1 \bmod p} = \underbrace{a_n^p t^{np} + \dots + a_0^p}_{\text{tutte potenze} \equiv 0 \bmod p}$

unica possibilità $h(t) = q(t) = 0$ ASSURDO

$t \notin (\mathbb{Z}_p(t))^p \Rightarrow (\mathbb{Z}_p(t))^p \neq \mathbb{Z}_p(t) \Rightarrow \mathbb{Z}_p(t)$ non è perfetto