Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 15-05-2020

Polinomi separabili

Definizione

K campo. $f \in K[X]$ irriducibile è separabile (su K) se ha $\deg(f)$ radici distinte in un campo di spezzamento.

Ricordiamo che, se $K \subseteq L$ è un'estensione, $f \in K[X]$ e $\alpha \in L$ è radice di f (cioè $(X-\alpha) \mid f$), allora α è radice multipla di f (cioè $(X-\alpha)^2 \mid f$) $\iff$ α è radice della derivata f' di f.

Lemma

$f \in K[X]$ irriducibile è separabile $\iff$ $f' \neq 0$.

Dimostrazione.

$K \subseteq L$ campo di spezzamento di f.

$\implies$ $\exists\, \alpha \in L$ radice non multipla di f $\implies$ $f'(\alpha) \neq 0$ $\implies$ $f' \neq 0$.

$\impliedby$ $\deg(f') < \deg(f)$ $\implies$ $f \nmid f'$ $\implies$ $\mathrm{mcd}(f, f') = 1$ in $K[X]$ (perché f irriducibile in $K[X]$) $\implies$ $\exists\, g, h \in K[X]$ tali che $1 = gf + hf'$ $\implies$ $\mathrm{mcd}(f, f') = 1$ in $L[X]$ $\implies$ f non ha radici multiple in L, cioè f è separabile.

Omomorfismo di Frobenius

Corollario

$\mathrm{char}(K) = 0$, $f \in K[X]$ *irriducibile* $\implies$ f *separabile.*

Dimostrazione.

f irriducibile $\implies$ $n := \deg(f) > 0$; $f = \sum_{i=0}^{n} a_i X^i$ con $a_n \neq 0$
$\implies$ $f' = \sum_{i=1}^{n} i a_i X^{i-1} \neq 0$ (e $\deg(f') = n - 1$) perché $n a_n \neq 0$
$\implies$ f separabile per il Lemma. □

Definizione-Proposizione

A dominio, $\mathrm{char}(A) = p$ primo. L'omomorfismo di Frobenius (di A) è l'omomorfismo di anelli $\mathcal{F} : A \to A$, $a \mapsto a^p$.

Dimostrazione.

$\mathcal{F}(1) = 1$; $\forall\, a, b \in A$ $\mathcal{F}(ab) = (ab)^p = a^p b^p = \mathcal{F}(a)\mathcal{F}(b)$ e
$\mathcal{F}(a+b) = (a+b)^p = \sum_{i=o}^{p} \binom{p}{i} a^{p-i} b^i = a^p + b^p = \mathcal{F}(a) + \mathcal{F}(b)$
perché $p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!}$ per $0 < i < p$. □

Campi perfetti

Definizione

Un campo K è perfetto se $\mathrm{char}(K) = 0$ o $\mathrm{char}(K) = p$ primo e $\mathcal{F}\colon K \to K$ è suriettivo (nel qual caso $\mathcal{F} \in \mathrm{G}(K) = \mathrm{G}_{\mathbb{F}_p}(K)$).

Proposizione

K campo è perfetto $\iff$ f è separabile $\forall\, f \in K[X]$ irriducibile.

Dimostrazione.

Posso supporre $\mathrm{char}(K) = p$ primo.

$\Longrightarrow$ $f \in K[X]$ irriducibile $\Longrightarrow$ per il Lemma basta dimostrare $f' \neq 0$. Per assurdo $f' = 0 \implies f = \sum_{i=0}^{n} a_i X^{pi}$; K perfetto $\implies \exists\, b_i \in K$ tale che $a_i = \mathcal{F}(b^i) = b_i^p$ $\forall\, i = 0, \ldots, n \implies$ $f = \mathcal{F}(\sum_{i=0}^{n} b_i X^i) = (\sum_{i=0}^{n} b_i X^i)^p$, assurdo.

$\Longleftarrow$ $a \in K \implies \exists\, K \subseteq L$ estensione tale che $X^p - a$ ha una radice α in $L \implies \mathrm{m}_{\alpha,K} \mid (X^p - a) = X^p - \alpha^p = (X - \alpha)^p \implies$ $\mathrm{m}_{\alpha,K} = X - \alpha$ (perché $\mathrm{m}_{\alpha,K}$ monico e irriducibile, quindi separabile) $\implies \alpha \in K$ e $a = \alpha^p = \mathcal{F}(\alpha)$.

Esempi

- K finito $\implies$ K perfetto:
  $\mathrm{char}(K) = p$ primo e $\mathcal{F}\colon K \to K$ è suriettivo perché iniettivo.
- K algebricamente chiuso $\implies$ K perfetto:
  posso supporre $\mathrm{char}(K) = p$ primo $\implies$ $\mathcal{F}\colon K \to K$ è suriettivo perché $\forall\, a \in K$ $X^p - a$ ha una radice $b \in K$, cioè $a = b^p = \mathcal{F}(b)$.
- $K \subseteq L$ estensione algebrica, K perfetto $\implies$ L perfetto:
  per la Proposizione basta dimostrare $f \in L[X]$ irriducibile (e posso supporre monico) $\implies$ f separabile.
  $L \subseteq L'$ campo di spezzamento di f $\implies$ $L \subseteq L'$ algebrica $\implies$ $K \subseteq L'$ algebrica.
  $\alpha \in L'$ radice di f $\implies$ $f = \mathrm{m}_{\alpha,L} \mid \mathrm{m}_{\alpha,K}$.
  $\mathrm{m}_{\alpha,K}$ separabile per la Proposizione $\implies$ f separabile.
- $\mathrm{char}(K) = p$ primo $\implies$ $K(X)$ non perfetto:
  per assurdo $\exists\, f/g \in K(X)$ (con $f, g \in K[X]$ e $g \neq 0$) tale che $X = \mathcal{F}(f/g) = f^p/g^p$ $\implies$ $f^p = Xg^p$ in $K[X]$, assurdo.

Estensioni separabili

Definizione

$K \subseteq L$ estensione.

- $\alpha \in L$ è separabile su K se α è algebrico su K e $\mathrm{m}_{\alpha,K}$ è separabile.
- $K \subseteq L$ è separabile se α è separabile su K $\forall\, \alpha \in L$.

Osservazione

$F \subseteq K \subseteq L$ estensioni con $F \subseteq L$ separabile $\implies$ $F \subseteq K$ separabile (ovvio) e $K \subseteq L$ separabile (perché $\mathrm{m}_{\alpha,K} \mid \mathrm{m}_{\alpha,F}$ $\forall\, \alpha \in L$).

Corollario

K è perfetto $\iff$ ogni estensione algebrica di K è separabile.

Dimostrazione.

Segue dalla Proposizione, tenendo conto che $f \in K[X]$ irriducibile e monico $\implies$ $\exists\, K \subseteq L$ estensione algebrica e $\exists\, \alpha \in L$ tale che $f = \mathrm{m}_{\alpha,K}$.

K-omomorfismi da un'estensione finita

Teorema

$K \subseteq L$ e $i\colon K \to L'$ estensioni con $[L : K] < \infty \implies$

$$\#\{j\colon L \to L' \ :\ j \ K\text{-omomorfismo}\} \leq [L : K]$$

e vale l'uguaglianza $\iff$ $\mathrm{m}_{\alpha,K}$ ha $\deg(\mathrm{m}_{\alpha,K})$ radici distinte in L' (cioè $\mathrm{m}_{\alpha,K}$ è separabile e si spezza su L') $\forall\, \alpha \in L$.

Dimostrazione (inizio).

Date estensioni $K \subseteq K' \subseteq K'' \subseteq L$ e un K-omomorfismo $i'\colon K' \to L'$, posto

$$E(K'', i') := \{i''\colon K'' \to L' \ :\ i'' \text{ omomorfismo di anelli, } i''|_{K'} = i'\},$$

la disuguaglianza da dimostrare è $\#E(L, i) \leq n := [L : K]$.
Per induzione su n: chiaro per $n = 1$, quindi assumiamo $n > 1$.

Dimostrazione (fine)

$\forall\, \alpha \in L$ sappiamo che $e_\alpha := \#E(K(\alpha), i)$ soddisfa

$$e_\alpha = \#\{\alpha' \in L' \,:\, \mathrm{m}_{\alpha,K}(\alpha') = 0\} \leq \deg(\mathrm{m}_{\alpha,K}) = [K(\alpha) : K] =: n_\alpha$$

e che $e_\alpha = n_\alpha \iff \mathrm{m}_{\alpha,K}$ ha n_α radici distinte in L'.
$\alpha \notin K \implies n_\alpha > 1 \implies [L : K(\alpha)] = n/n_\alpha < n \implies$
$\forall\, i' \in E(K(\alpha), i)$ per induzione $\#E(L, i') \leq n/n_\alpha$ e vale l'uguale
$\iff \mathrm{m}_{\beta,K(\alpha)}$ ha $\deg(\mathrm{m}_{\beta,K(\alpha)})$ radici distinte in L' $\forall\, \beta \in L$.
Da $E(L, i) = \coprod_{i' \in E(K(\alpha), i)} E(L, i')$ segue

$$\#E(L, i) = \sum_{i' \in E(K(\alpha), i)} \#E(L, i') \leq e_\alpha n/n_\alpha \leq n_\alpha n/n_\alpha = n$$

e se vale l'uguale allora $e_\alpha = n_\alpha$, per cui $\mathrm{m}_{\alpha,K}$ ha $n_\alpha = \deg(\mathrm{m}_{\alpha,K})$ radici distinte in L' ($\forall\, \alpha \in L \setminus K$, ma ovviamente anche $\forall\, \alpha \in K$).
Viceversa, se $\mathrm{m}_{\alpha,K}$ ha $\deg(\mathrm{m}_{\alpha,K})$ radici distinte in L' $\forall\, \alpha \in L$, fissato $\alpha \in L \setminus K$ si ha $e_\alpha = n_\alpha$ e $\#E(L, i') = n/n_\alpha$
$\forall\, i' \in E(K(\alpha), i)$ (perché $\mathrm{m}_{\beta,K(\alpha)}$ ha $\deg(\mathrm{m}_{\beta,K(\alpha)})$ radici distinte in L' $\forall\, \beta \in L$, dato che $\mathrm{m}_{\beta,K(\alpha)} \mid \mathrm{m}_{\beta,K}$), e quindi $\#E(L, i) = n$.

Estensioni di Galois

Definizione

Un'estensione è di Galois se è finita, normale e separabile.

Osservazione

$F \subseteq K \subseteq L$ estensioni con $F \subseteq L$ di Galois $\implies$ $K \subseteq L$ di Galois.

Corollario

$K \subseteq L$ estensione finita $\implies$ $\#\mathrm{G}_K(L) \leq [L : K]$ *e vale l'uguaglianza* $\iff$ *$K \subseteq L$ è di Galois.*

Dimostrazione.

$j \colon L \to L$ K-omomorfismo $\implies$ j suriettivo (perché j omomorfismo iniettivo di K-spazi vettoriali e $\dim_K(L) < \infty$) $\implies$ per il Teorema

$$\#\mathrm{G}_K(L) = \#\{j \colon L \to L \,:\, j \text{ } K\text{-omomorfismo}\} \leq [L : K]$$

e vale l'uguaglianza $\iff$ $\mathrm{m}_{\alpha,K}$ separabile e si spezza su L $\forall\, \alpha \in L$ $\iff$ $K \subseteq L$ separabile e normale $\iff$ $K \subseteq L$ di Galois. $\square$

Campi finiti

K campo finito.

- $\mathrm{char}(K) = p$ primo $\implies$ $\mathbb{F}_p \subseteq K$ estensione finita.
- $n := [K : \mathbb{F}_p] \implies K \cong \mathbb{F}_p^n$ come $\mathbb{F}_p$-spazio vettoriale (quindi $K \cong C_p^n$ come gruppo abeliano) $\implies \#K = p^n$.
- $\alpha \in K^* \implies \alpha^{p^n-1} = 1$ (per il teorema di Lagrange) $\implies \alpha^{p^n} = \alpha \implies$ ogni elemento di K è radice di $X^{p^n} - X \implies \prod_{\alpha \in K}(X - \alpha) \mid (X^{p^n} - X) \implies X^{p^n} - X = \prod_{\alpha \in K}(X - \alpha) \implies \mathbb{F}_p \subseteq K$ campo di spezzamento di $X^{p^n} - X$.

p primo, $n > 0$.

- $\mathbb{F}_p \subseteq K'$ campo di spezzamento di $X^{p^n} - X \implies$

  $K := \{\alpha \in K' : \alpha \text{ radice di } X^{p^n} - X\} = \{\alpha \in K' : \mathcal{F}^n(\alpha) = \alpha\}$

  sottocampo di $K' \implies K = K'$.
- $(X^{p^n} - X)' = -1$ non ha radici $\implies X^{p^n} - X$ non ha radici multiple $\implies \#K = \deg(X^{p^n} - X) = p^n$.

Quanto appena visto dimostra i punti 1 e 2 del seguente enunciato.

Proposizione

1. *Ogni campo finito ha ordine una potenza di un numero primo.*
2. $\forall\, p$ *primo e* $\forall\, n > 0\ \exists!$ *a meno di isomorfismo un campo* $\mathbb{F}_{p^n}$ *di ordine* p^n*; inoltre* $\mathbb{F}_{p^n}$ *è campo di spezzamento di* $X^{p^n} - X$ *su* $\mathbb{F}_p$*.*
3. *L'estensione* $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ *è di Galois e* $\mathrm{G}_{\mathbb{F}_p}(\mathbb{F}_{p^n}) = \langle \mathcal{F} \rangle \cong C_n$*.*

Dimostrazione di 3.

$\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ è finita e normale (perché campo di spezzamento di un polinomio) e separabile (perché $\mathbb{F}_p$ è finito, quindi perfetto).
Per il Corollario $\#\mathrm{G}_{\mathbb{F}_p}(\mathbb{F}_{p^n}) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, e basta dimostrare $\mathrm{ord}(\mathcal{F}) \geq n$, vero perché $0 < i < n \implies$
$\#\{\alpha \in \mathbb{F}_{p^n} \,:\, \mathcal{F}^i(\alpha) = \alpha^{p^i} = \alpha\} \leq p^i < p^n \implies \mathcal{F}^i \neq \mathrm{id}_{\mathbb{F}_{p^n}}$. □