Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 13-05-2020

Esistenza della chiusura algebrica

Lemma

K campo $\implies \exists\, K \to K'$ estensione tale che ogni polinomio non costante a coefficienti in K ha una radice in K'.

Teorema

Ogni campo K ha una chiusura algebrica $K \subseteq \overline{K}$.

Dimostrazione.

- Posto $K_0 := K$, per il Lemma induttivamente $\forall\, n \in \mathbb{N}$ $\exists\, K_n \subseteq K_{n+1}$ estensione tale che $f \in K_n[X] \setminus K \implies f$ ha una radice in K_{n+1}.
- $L := \bigcup_{n \in \mathbb{N}} K_n$ campo (esercizio) tale che $K \subseteq L$ estensione con L algebricamente chiuso: $f \in L[X] \setminus L \implies \exists\, n \in \mathbb{N}$ tale che $f \in K_n[X] \implies f$ ha una radice in $K_{n+1} \subseteq L$.
- $\overline{K} := \overline{K}^L$ tale che $K \subseteq \overline{K}$ chiusura algebrica di K (già visto).

Dimostrazione del Lemma

$U := \{f \in K[X] \,:\, f \text{ irriducibile e monico}\}$, $A := K[X_f \,:\, f \in U]$.

$I := (f(X_f) \,:\, f \in U) \subsetneq A$ ideale: per assurdo $I = A \implies \exists\, f_1, \ldots, f_n \in U$ distinti e $g_1, \ldots, g_n \in A$ tali che

$$h := \sum_{l=1}^{n} f_l(X_{f_l})g_l = 1.$$

$K \subseteq L$ campo di spezzamento di $\prod_{l=1}^{n} f_l \implies \forall\, l = 1, \ldots, n$ $\exists\, \alpha_l \in L$ tale che $f_l(\alpha_l) = 0$. Valutando $h = 1$ in

$$X_f = \begin{cases} \alpha_l & \text{se } f = f_l \text{ per qualche } l = 1, \ldots, n \\ 0 & \text{altrimenti} \end{cases}$$

si ottiene $0 = 1$ in L, assurdo.

$\exists\, J \subset A$ ideale massimale tale che $I \subseteq J \implies K' := A/J$ campo e $\pi|_K \colon K \to K'$ (con $\pi \colon A \to K'$ proiezione) estensione di campi con la proprietà richiesta: dato $f \in K[X] \setminus K$, posso supporre $f \in U$ $\implies f(\pi(X_f)) = \pi(f(X_f)) = 0$ perché $f(X_f) \in I \subseteq J = \ker(\pi)$.

Estensioni normali

Definizione

Un'estensione algebrica $K \subseteq L$ è normale se $\mathrm{m}_{\alpha,K}$ si spezza su L $\forall\, \alpha \in L$.

Esempio

$K \subseteq \overline{K}$ chiusura algebrica di $K \implies K \subseteq \overline{K}$ è normale.

Proposizione

Un'estensione finita $K \subseteq L$ è normale $\iff$ è campo di spezzamento di un polinomio.

Dimostrazione di $\implies$.

$\exists\, \alpha_1, \ldots, \alpha_n \in L$ algebrici su K tali che $L = K(\alpha_1, \ldots, \alpha_n) \implies$ $K \subseteq L$ campo di spezzamento di $f := \prod_{l=1}^{n} \mathrm{m}_{\alpha_l,K}$:
f si spezza su L perché $\mathrm{m}_{\alpha_1,K}, \ldots, \mathrm{m}_{\alpha_n,K}$ per ipotesi si spezzano su L e $L = K(U)$ con $U := \{\alpha \in L \,:\, f(\alpha) = 0\}$, dato che $\alpha_1, \ldots, \alpha_n \in U$ e $L = K(\alpha_1, \ldots, \alpha_n)$. $\square$

Dimostrazione di $\Longleftarrow$

- $K \subseteq L$ campo di spezzamento di $f \in K[X] \setminus \{0\} \implies \exists\, c \in K^*$ e $\alpha_1, \dots, \alpha_n \in L$ tali che $f = c \prod_{l=1}^{n}(X - \alpha_l)$ e $L = K(\alpha_1, \dots, \alpha_n)$.
- $\alpha \in L \implies \exists\, L \subseteq L'$ campo di spezzamento di $\mathrm{m}_{\alpha,K}$. Dato $\beta \in L'$ tale che $\mathrm{m}_{\alpha,K}(\beta) = 0$, devo dimostrare $\beta \in L$.
- $\exists!$ K-omomorfismo $i \colon K(\alpha) \to L'$ tale che $i(\alpha) = \beta$.
- $K(\alpha) \subseteq L$ campo di spezzamento di f, $f = i(f)$ si spezza su $L' \implies \exists$ $K(\alpha)$-omomorfismo $j \colon L \to L'$ (cioè tale che $j|_{K(\alpha)} = i$).
- j K-omomorfismo $\implies \forall\, l = 1, \dots, n$

$$f(j(\alpha_l)) = j(f)(j(\alpha_l)) = j(f(\alpha_l)) = j(0) = 0$$

$\implies j(\alpha_l) \in \{\alpha_1, \dots, \alpha_n\} \subseteq L \implies j(L) \subseteq L \implies \beta = i(\alpha) = j(\alpha) \in j(L) \subseteq L$.

Esempi

- $K \subseteq L$ campo di spezzamento di $f \in K[X]$ irriducibile (dunque estensione normale), $\deg(f) = n \implies n \mid [L : K] \mid n!$. Quindi $n = 2 \implies [L : K] = 2$, $n = 3 \implies [L : K] = 3$ o 6.
- $K \subseteq L$ estensione di grado $2 \implies K \subseteq L$ normale: $\alpha \in L \setminus K \implies L = K(\alpha) \implies \deg(\mathrm{m}_{\alpha,K}) = [K(\alpha) : K] = 2$ $\implies K \subseteq L$ campo di spezzamento di $\mathrm{m}_{\alpha,K}$.
- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ estensione non normale di grado 3: $\mathrm{m}_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2$ non si spezza su $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ (le sue altre radici complesse sono $\omega\sqrt[3]{2}$ e $\omega^2\sqrt[3]{2}$ con $\omega^3 = 1$ e $\omega \neq 1$).
- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ estensione normale (perché campo di spezzamento di $X^3 - 2$) di grado 6.
- $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ estensione normale (perché campo di spezzamento di $X^3 - 2$) di grado 3.
- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ estensioni normali (perché di grado 2), ma $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ non normale.

Esercizio

$K \subseteq L$ estensione finita, $n := [L : K]$.

1. $n = p$ o p^2 (con p numero primo), $K \subseteq L$ campo di spezzamento di $f \in K[X]$ irriducibile $\implies \deg(f) = n$.
2. $K \subseteq L$ normale e semplice $\implies \exists\, f \in K[X]$ irriducibile tale che $\deg(f) = n$ e $K \subseteq L$ campo di spezzamento di f.

Esercizio

$K \subseteq L$ estensione finita, $n := [L : K]$.

1. $n = p$ o p^2 (con p numero primo), $K \subseteq L$ campo di spezzamento di $f \in K[X]$ irriducibile $\implies \deg(f) = n$.
2. $K \subseteq L$ normale e semplice $\implies \exists\, f \in K[X]$ irriducibile tale che $\deg(f) = n$ e $K \subseteq L$ campo di spezzamento di f.

1. $d := \deg(f) \implies d \mid n \mid d!$.
   $n = p \implies d = 1$ o p perché $d \mid p$, e $d \neq 1$ perché $p \nmid 1!$.
   $n = p^2 \implies d = 1, p$ o p^2 perché $d \mid p^2$, e $d \neq 1, p$ perché $p^2 \nmid 1!$ e $p^2 \nmid p! = (p-1)!p$.
2. $K \subseteq L$ semplice $\implies \exists\, \alpha \in L$ tale che $L = K(\alpha)$.
   $K \subseteq L$ finita (e quindi algebrica) $\implies \alpha$ algebrico su K.
   $f := \mathrm{m}_{\alpha,K} \in K[X]$ irriducibile e $\deg(f) = [K(\alpha) : K] = n$.
   $K \subseteq L$ normale $\implies f$ si spezza su L.
   $\alpha_1 = \alpha, \dots, \alpha_n$ radici di f in $L \implies$
   $L = K(\alpha) \subseteq K(\alpha_1, \dots, \alpha_n) \subseteq L \implies L = K(\alpha_1, \dots, \alpha_n)$
   $\implies K \subseteq L$ campo di spezzamento di f.

K campo $\implies$ il gruppo degli automorfismi di K è

$$\mathrm{G}(K) := \{\sigma \colon K \to K \;:\; \sigma \text{ isomorfismo di anelli}\} < S(K).$$

Il gruppo di Galois di un'estensione $F \subseteq K$ è

$$\mathrm{G}_F(K) := \{\sigma \in \mathrm{G}(K) \;:\; \sigma(a) = a \;\forall\, a \in F\} < \mathrm{G}(K).$$

Osservazione

$F \subseteq K$ (sotto)campo primo di $K \implies \mathrm{G}_F(K) = \mathrm{G}(K)$: infatti $\{\alpha \in K \;:\; \sigma(\alpha) = \alpha \;\forall\, \sigma \in \mathrm{G}(K)\}$ è un sottocampo di K (esercizio), e dunque contiene F.

Esempio

$\mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \mathrm{G}(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$ perché $\sigma \in \mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) \implies \sigma(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ radice di $X^3 - 2 \implies \sigma(\sqrt[3]{2}) = \sqrt[3]{2} \implies \sigma = \mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}$.

Invece $\mathrm{G}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \mathrm{G}(\mathbb{Q}(\sqrt{2})) \cong C_2$ (si vedrà).

Osservazione

$F \subseteq K \subseteq L$ estensioni con $F \subseteq L$ normale.

- $K \subseteq L$ è normale: $\alpha \in L \implies \mathrm{m}_{\alpha,K}$ si spezza su L perché $\mathrm{m}_{\alpha,K} \mid \mathrm{m}_{\alpha,F}$ e per ipotesi $\mathrm{m}_{\alpha,F}$ si spezza su L.
- Anche quando $F \subseteq L$ è finita, $F \subseteq K$ può non essere normale: per esempio, $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ e $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

Proposizione

$F \subseteq K \subseteq L$ estensioni con $F \subseteq L$ finita e normale. Allora $F \subseteq K$ è normale $\iff$ K è $\mathrm{G}_F(L)$-stabile (cioè $\sigma(K) = K$ $\forall\, \sigma \in \mathrm{G}_F(L)$, o, equivalentemente, $\sigma(K) \subseteq K$ $\forall\, \sigma \in \mathrm{G}_F(L)$)

Esempio

Con le ipotesi della Proposizione, L finito $\implies$ $F \subseteq K$ normale: $\sigma \in \mathrm{G}_F(L) \implies \sigma|_{L^*} \in \mathrm{Aut}(L^*) \implies \sigma(K^*) \subseteq K^*$ ($K^* < L^*$ caratteristico perché L^* è ciclico) $\implies \sigma(K) \subseteq K$.

Dimostrazione della Proposizione

$\Longrightarrow$ $\sigma \in \mathrm{G}_F(L) \implies \sigma(K) \subseteq K$:

$\alpha \in K \implies \mathrm{m}_{\alpha,F}(\sigma(\alpha)) = \sigma(\mathrm{m}_{\alpha,F}(\alpha)) = \sigma(0) = 0 \implies$ $\sigma(\alpha) \in K$ perché $\mathrm{m}_{\alpha,F}$ si spezza su K.

$\Longleftarrow$ $F \subseteq L$ normale e finita $\implies$ $F \subseteq L$ campo di spezzamento di $f \in F[X] \setminus \{0\}$.

$\alpha \in K \implies \mathrm{m}_{\alpha,F}$ si spezza su L, e va dimostrato che si spezza su K, cioè che $\beta \in L$ tale che $\mathrm{m}_{\alpha,F}(\beta) = 0 \implies$ $\beta \in K$.

$\exists!$ F-omomorfismo $i\colon F(\alpha) \to L$ tale che $i(\alpha) = \beta$.
$F(\alpha) \subseteq L$ campo di spezzamento di f, $f = i(f)$ si spezza su L $\implies \exists$ $F(\alpha)$-omomorfismo (e quindi F-omomorfismo) $\sigma\colon L \to L$ (cioè tale che $\sigma|_{F(\alpha)} = i$).

$\sigma(L) \subseteq L$, $\dim_F(\sigma(L)) = \dim_F(L) < \infty \implies \sigma(L) = L \implies$ $\sigma \in \mathrm{G}_F(L) \implies \beta = i(\alpha) = \sigma(\alpha) \in \sigma(K) = K$.