Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 06-05-2020

Proprietà delle estensioni finite

Proposizione

$F \subseteq K \subseteq L$ estensioni. Allora $F \subseteq L$ è finita $\iff$ $F \subseteq K$ e $K \subseteq L$ sono finite. Inoltre in tal caso $[L : F] = [L : K][K : F]$.

Dimostrazione.

$[K : F] \leq [L : F]$ (perché K è un F-sottospazio vettoriale di L) e $[L : K] \leq [L : F]$ (perché ogni insieme di generatori di L su F lo è anche su K), dunque basta dimostrare l'ultima affermazione.
$[K : F] = m$ e $[L : K] = n \implies K \cong F^m$ come F-spazi vettoriali e $L \cong K^n$ come K- e quindi anche come F-spazi vettoriali $\implies$ $L \cong (F^m)^n \cong F^{mn}$ come F-spazi vettoriali $\implies [L : F] = mn$. □

Osservazione

$\{\alpha_1, \ldots, \alpha_m\}$ F-base di K e $\{\beta_1, \ldots, \beta_n\}$ K-base di $L \implies$ $\{\alpha_i\beta_j : i = 1, \ldots, m \text{ e } j = 1, \ldots, n\}$ F-base di L: basta dimostrare che è un insieme di generatori, il che è vero perché ogni elemento di L è della forma $\sum_{j=1}^{n} b_j\beta_j$ con $b_j = \sum_{i=1}^{m} a_{i,j}\alpha_i$ e $a_{i,j} \in F$.

Estensione generata da un sottoinsieme

- B anello commutativo, $A \subseteq B$ sottoanello, $U \subseteq B \implies$
  $A[U]$ indica il più piccolo sottoanello di B contenente A e U, cioè l'intersezione di tutti i sottoanelli di B contenenti A e U.
  Inoltre è facile vedere che

  $$A[U] = \{f(b_1, \ldots, b_n) \,:\, f \in A[X_1, \ldots, X_n],\ b_1, \ldots, b_n \in U\}.$$

  In particolare $A[b] := A[\{b\}] = \{f(b) \,:\, f \in A[X]\}\ \forall\, b \in B$.
- $K \subseteq L$ estensione, $U \subseteq L$ sottoinsieme $\implies$
  $K(U)$ indica il più piccolo sottocampo di L contenente K e U, cioè l'intersezione di tutti i sottocampi di L contenenti K e U.
  Chiaramente $K[U] \subseteq K(U)$ e è facile vedere che

  $$K(U) = \left\{\alpha\beta^{-1} \,:\, \alpha, \beta \in K[U],\ \beta \neq 0\right\} \cong Q(K[U])$$

  (l'inclusione $K[U] \to K(U)$ si estende a un omomorfismo iniettivo $Q(K[U]) \to K(U)$, che è anche suriettivo).
  Ovviamente $K \subseteq K(U)$ è un estensione, detta generata da U (su K).

Estensioni finitamente generate e estensioni semplici

Definizione

Un'estensione $K \subseteq L$ è finitamente generata se $\exists\, U \subseteq L$ finito tale che $L = K(U)$. L'estensione è semplice se $\exists\, \alpha \in L$ tale che $L = K(\alpha) := K(\{\alpha\})$.

Esempio

Un'estensione $K \subseteq L$ è semplice nei seguenti casi.

- $[L : K] = p$ primo: date estensioni $K \subseteq K' \subseteq L$, da

$$p = [L : K] = [L : K'][K' : K]$$

  segue $[L : K'] = 1$ e $[K' : K] = p$ o $[L : K'] = p$ e $[K' : K] = 1$, e quindi $K' = L$ o $K' = K$.
  Allora $L = K(\alpha)\ \forall\, \alpha \in L \setminus K$.
- L (e quindi anche K) è finito: $\exists\, \alpha \in L$ tale che $L^* = \langle \alpha \rangle \implies L = K(\alpha)$.

Elementi algebrici e elementi trascendenti

Definizione

$K \subseteq L$ estensione. Si dice che $\alpha \in L$ è algebrico su K se $\exists\, 0 \neq f \in K[X]$ tale che $f(\alpha) = 0$.
Altrimenti si dice che α è trascendente su K.

Proposizione

$K \subseteq L$ estensione, $\alpha \in L$.

1. *α trascendente su K $\implies$ $K[\alpha] \cong K[X]$ e $K(\alpha) \cong K(X)$ come K-algebre.*
2. *α algebrico su K $\implies$ $\exists!\, \mathrm{m}_\alpha = \mathrm{m}_{\alpha,K} \in K[X]$ monico (detto polinomio minimo di α su K) tale che*

$$\{f \in K[X] \,:\, f(\alpha) = 0\} = (\mathrm{m}_\alpha).$$

Inoltre m_α è irriducibile in $K[X]$ e $K[\alpha] = K(\alpha) \cong K[X]/(\mathrm{m}_\alpha)$ come K-algebre.

Dimostrazione della Proposizione

$g\colon K[X] \to L$, $f \mapsto f(\alpha)$ è un omomorfismo di K-algebre (è l'unico tale che $X \mapsto \alpha$); inoltre $\mathrm{im}(g) = \{f(\alpha) : f \in K[X]\} = K[\alpha]$ e $\ker(g) = \{f \in K[X] : f(\alpha) = 0\}$.

1. $\ker(g) = \{0\} \implies K[X] \cong \mathrm{im}(g) = K[\alpha]$ (come K-algebre), quindi anche $K(X) = Q(K[X]) \cong Q(K[\alpha]) \cong K(\alpha)$.
2. $\ker(g)$ ideale non nullo di $K[X]$ dominio a ideali principali tale che $K[X]^* = K^* \implies \exists!\, \mathrm{m}_\alpha \in K[X]$ monico tale che $\ker(g) = (\mathrm{m}_\alpha) \implies$ per il primo teorema di isomorfismo

$$K[\alpha] = \mathrm{im}(g) \cong K[X]/\ker(g) \cong K[X]/(\mathrm{m}_\alpha)$$

come anelli, ma è facile vedere che l'isomorfismo (essendo indotto da g) è anche di K-algebre.
$K[\alpha] \subseteq L$ sottoanello $\implies K[\alpha] \cong K[X]/(\mathrm{m}_\alpha)$ dominio $\implies$ (m_α) ideale primo non nullo $\implies \mathrm{m}_\alpha$ irriducibile e (m_α) ideale massimale $\implies K[\alpha] \cong K[X]/(\mathrm{m}_\alpha)$ campo $\implies$ $K[\alpha] = K(\alpha)$ (dato che in ogni caso $K[\alpha] \subseteq K(\alpha)$).

Grado di un'estensione semplice

Lemma

$0 \neq f \in K[X] \implies \dim_K(K[X]/(f)) = \deg(f)$.

Corollario

$K \subseteq L$ estensione, $\alpha \in L \implies$ sono equivalenti:

1. *α è algebrico su K;*
2. *$K[\alpha] = K(\alpha)$;*
3. *$[K(\alpha) : K] < \infty$, e in questo caso $[K(\alpha) : K] = \deg(\mathrm{m}_\alpha)$.*

Dimostrazione.

1 $\implies$ 2 Per la parte 2 della Proposizione.

2 $\implies$ 3 $K[\alpha] = K(\alpha)$ campo $\implies$ $K[\alpha] \not\cong K[X] \implies$
α algebrico su K per la parte 1 della Proposizione $\implies$
$K(\alpha) \cong K[X]/(\mathrm{m}_\alpha)$ per la parte 2 della Proposizione $\implies$
$[K(\alpha) : K] = \dim_K(K[X]/(\mathrm{m}_\alpha)) = \deg(\mathrm{m}_\alpha)$ per il Lemma.

3 $\implies$ 1 Per la parte 1 della Proposizione, dato che $\dim_K(K(X)) = \infty$.

Dimostrazione del Lemma

- $d := \deg(f)$, $K[X]_{<d} := \{g \in K[X] \,:\, g = 0 \text{ o } \deg(g) < d\}$ K-sottospazio vettoriale di $K[X]$ tale che $\dim_K(K[X]_{<d}) = d$ (una base di $K[X]_{<d}$ è $\{X^i \,:\, 0 \leq i < d\}$).
- La funzione

$$\psi \colon K[X] \to K[X]$$
$$g \mapsto r \text{ con } g = qf + r,\ q \in K[X] \text{ e } r \in K[X]_{<d}$$

  è ben definita e K-lineare (esercizio).
- $\mathrm{im}(\psi) = K[X]_{<d}$ (perché $\psi(g) = g$ se $g \in K[X]_{<d}$) e $\ker(\psi) = \{qf \,:\, q \in K[X]\} = (f) \implies$

$$K[X]/(f) = K[X]/\ker(\psi) \cong \mathrm{im}(\psi) = K[X]_{<d}$$

  come K-spazi vettoriali per il primo teorema di isomorfismo $\implies \dim_K(K[X]/(f)) = \dim_K(K[X]_{<d}) = d$.

Osservazione

Una K-base di $K[X]/(f)$ è $\{X^i + (f) \,:\, 0 \leq i < d\}$.

Estensioni algebriche e estensioni finite

Definizione

Un'estensione $K \subseteq L$ è algebrica se α è algebrico su K $\forall\, \alpha \in L$.

Proposizione

$K \subseteq L$ estensione $\implies$ sono equivalenti:

1. *$K \subseteq L$ è finita;*
2. *$K \subseteq L$ è algebrica e finitamente generata;*
3. *$\exists\, \alpha_1, \ldots, \alpha_n \in L$ algebrici su K tali che $L = K(\alpha_1, \ldots, \alpha_n)$.*

Dimostrazione.

$1 \implies 2$ $\alpha \in L \implies [K(\alpha) : K] \leq [L : K] < \infty \implies \alpha$ algebrico su K.
$L = \langle \alpha_1, \ldots, \alpha_n \rangle_K \implies L = K(\alpha_1, \ldots, \alpha_n)$.

$2 \implies 3$ Chiaro.

$3 \implies 1$ α_i algebrico su $K \implies \alpha_i$ algebrico su $K_i := K(\alpha_1, \ldots, \alpha_{i-1})$
$\implies [K_{i+1} = K_i(\alpha_i) : K_i] < \infty \;\forall\, i = 1, \ldots, n \implies$
$[L : K] = \prod_{i=1}^{n} [K_{i+1} : K_i] < \infty$.

Proprietà delle estensioni algebriche

Osservazione

$K \subseteq K' \subseteq L$ estensioni, $\alpha \in L$ algebrico su $K \implies$ α algebrico su K' e $[K'(\alpha) : K'] \leq [K(\alpha) : K] < \infty$: $\mathrm{m}_{\alpha,K} \in K[X] \subseteq K'[X]$ tale che $\mathrm{m}_{\alpha,K}(\alpha) = 0 \implies \mathrm{m}_{\alpha,K'} \mid \mathrm{m}_{\alpha,K}$ in $K'[X] \implies \deg(\mathrm{m}_{\alpha,K'}) \leq \deg(\mathrm{m}_{\alpha,K})$.

Proposizione

$F \subseteq K \subseteq L$ estensioni. Allora $F \subseteq L$ algebrica $\iff$ $F \subseteq K$ e $K \subseteq L$ algebriche.

Dimostrazione.

$\implies$ Chiaro.

$\impliedby$ $\beta \in L \implies \beta$ algebrico su $K \implies \exists\, \alpha_0, \ldots, \alpha_n \in K$ non tutti nulli tali che $\sum_{i=0}^{n} \alpha_i \beta^i = 0 \implies \beta$ algebrico su $F' := F(\alpha_0, \ldots, \alpha_n)$; $\alpha_0, \ldots, \alpha_n$ algebrici su $F \implies$ per la Proposizione precedente $F \subseteq F'$ e $F' \subseteq F'(\beta)$ finite $\implies$ $F \subseteq F'(\beta)$ finita $\implies$ $F \subseteq F(\beta)$ finita $\implies \beta$ algebrico su F.

Chiusura algebrica in un'estensione

Definizione-Proposizione

$K \subseteq L$ estensione $\implies$ $\overline{K}^L := \{\alpha \in L : \alpha$ algebrico su $K\}$ è un sottocampo di L, detto chiusura algebrica di K in L.
Inoltre l'estensione $K \subseteq \overline{K}^L$ è algebrica e $\overline{\overline{K}^L}^L = \overline{K}^L$.

Dimostrazione.

Chiaramente $K \subseteq \overline{K}^L$ (in particolare $1 \in \overline{K}^L$).
$\alpha, \beta \in \overline{K}^L \implies$ per la Proposizione di prima $K \subseteq K(\alpha, \beta)$ è un'estensione algebrica $\implies$ $\alpha - \beta, \alpha\beta \in K(\alpha, \beta)$ sono algebrici su $K \implies \alpha - \beta, \alpha\beta \in \overline{K}^L$.
Analogamente $0 \neq \alpha \in \overline{K}^L \implies K \subseteq K(\alpha)$ estensione algebrica $\implies \alpha^{-1} \in K(\alpha)$ algebrico su $K \implies \alpha^{-1} \in \overline{K}^L$.
Per definizione l'estensione $K \subseteq \overline{K}^L$ è algebrica. Analogamente è algebrica l'estensione $\overline{K}^L \subseteq \overline{\overline{K}^L}^L$, e quindi anche $K \subseteq \overline{\overline{K}^L}^L$ per la Proposizione precedente. Allora $\overline{\overline{K}^L}^L \subseteq \overline{K}^L$, per cui $\overline{\overline{K}^L}^L = \overline{K}^L$. □

Chiusura algebrica di un campo

Definizione

Una chiusura algebrica di un campo K è un'estensione algebrica $K \subseteq \overline{K}$ con $\overline{K}$ algebricamente chiuso.

Corollario

$K \subseteq L$ estensione con L algebricamente chiuso $\implies$ $K \subseteq \overline{K}^L$ è una chiusura algebrica di K.

Dimostrazione.

$K \subseteq \overline{K}^L$ estensione algebrica per la Definizione-Proposizione.
$\overline{K}^L$ algebricamente chiuso: $f \in \overline{K}^L[X] \setminus \overline{K}^L \subseteq L[X] \setminus L \implies$
$\exists\, \alpha \in L$ tale che $f(\alpha) = 0$ (perché L algebricamente chiuso) $\implies$
α algebrico su $\overline{K}^L \implies \alpha \in \overline{\overline{K}^L}^L = \overline{K}^L$. □

Esempio

$\mathbb{Q} \subseteq \overline{\mathbb{Q}} := \overline{\mathbb{Q}}^{\mathbb{C}}$ è una chiusura algebrica di $\mathbb{Q}$. Si dice che $\alpha \in \mathbb{C}$ è algebrico (risp. trascendente) se $\alpha \in \overline{\mathbb{Q}}$ (risp. $\alpha \notin \overline{\mathbb{Q}}$).