0.1 Estensioni finite

Lezioni del 05-06/11/2019 (appunti grezzi)

Definizione

Un'estensione di campi $\mathbb{L}/\mathbb{K}$ si dice finita se $|\mathbb{L} : \mathbb{K}| < \infty$.

Proposizione

Sia $\mathbb{L}/\mathbb{K}$ un'estensione finita. Allora, ogni elemento $a \in \mathbb{L}$ è algebrico su $\mathbb{K}$.

Dimostrazione. Sia $\phi_a : \mathbb{K}[x] \to \mathbb{L}$ la valutazione in a. Poiché $\dim_{\mathbb{K}} \mathbb{K}[x] = \infty$ (una base sono tutti i monomi $1, x, x^2, ...$) e $|\mathbb{L} : \mathbb{K}| = \dim_K(L) < \infty$, ϕ_a non è iniettiva, cioè $\ker(\phi_a) \neq \{0_K\}$. Dunque, per $f \in \ker(\phi_a) \setminus \{0_K\}$, si ha $f(a) = \phi_a(f) = 0$. ∎

Proposizione

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi, e sia $a \in \mathbb{L}$. Allora, sono equivalenti
(i) a è algebrico su $\mathbb{K}$
(ii) $|\mathbb{K}(a) : \mathbb{K}| < \infty$
(iii) esiste un'estensione finita M/K, $M \subseteq L$ tale che $a \in M$

Dimostrazione. Per la proposizione precedente, sappiamo già che (iii) implica (i). Vediamo che (i) implica (ii). Infatti, $K[a] = \mathrm{Im}(\phi_a) \simeq K[x]/\ker(\phi_a)$ è un campo, e $K(a) = K[a]$ implica che $|K[a] : K| = |K[a] : K| = \deg^\star(\min_{a,K}) < \infty$. Mostriamo ora che non (i) implica non (ii). Infatti, non (i) sse a è trascendente su K. Quindi, $\phi_a : K[x] \to L$ è iniettiva, e $K(a) \supseteq im(\phi_a) \simeq K[x]$ perché $K(a)$ contiene il sottospazio vettoriale $im(\phi_a)$ e $\dim_K(K(a)) = \infty$. Dunque, il fatto che (i) implica (ii) e non (i) implica non (ii), sappiamo che (i) se e solo se (ii). Ma (ii) implica (iii) è banale: infatti prendo $M = K(a)$. ∎

Definizione

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi. Denotiamo con $\mathrm{alg}_{\mathbb{K}}(\mathbb{L})$ l'insieme degli elementi $a \in L$ algebrici su K.

Proposizione

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi. Allora, $\mathrm{alg}_{\mathbb{K}}(\mathbb{L})$ è un sottocampo di $\mathbb{L}$.

Dimostrazione. Siano $a, b \in \mathrm{alg}_{\mathbb{K}}(\mathbb{L})$. Basta dimostrare che $a+b$, ab e a^{-1} stanno in $\mathrm{alg}_{\mathbb{K}}(\mathbb{L})$. Poiché $a \in \mathrm{alg}_{\mathbb{K}}(\mathbb{L})$, per la proposizione 2 sappiamo che $|K(a) : K| < \infty$. Poiché $b \in \mathrm{alg}_{\mathbb{K}}(\mathbb{L})$, esiste $\min_{b,K}(x) \in K[x] \subseteq K(a)[x]$. Dunque, b è algebrico su $K(a)$, da cui

$$|K(\{a, b\}) : K| = |K(a)(b) : K(a)| \cdot |K(a) : K| < \infty$$

per la Formula del grado. Poiché $a + b, ab, a^{-1} \in K(\{a, b\})$,per la Proposizione 2 sappiamo che $a + b, ab, a^{-1} \in \mathrm{alg}_{\mathbb{K}}(\mathbb{L})$. ∎

Trovare esplicitamente i polinomi che annullano $a + b, ab$ e a^{-1} sarebbe stato un incubo!

Definizione

Un campo $\mathbb{K}$ si dice algebricamente chiuso se ogni polinomio $f \in \mathbb{K}[x]$ con $\deg^\star(f) \geq 1$ ammette una radice.

Esempio. Per il Teorema Fondamentale dell'Algebra (lui dice Teorema di Gauss) sappiamo che $\mathbb{C}$ è un campo algebricamente chiuso. La dimostrazione è tutt'altro che banale e richiede o l'analisi complessa o la Teoria di Galois. $\square$

Denotiamo con $\overline{\mathbb{Q}} = \mathrm{alg}_{\mathbb{Q}}(\mathbb{C})$.

Proposizione

$\overline{\mathbb{Q}}$ è un campo algebricamente chiuso.

Dimostrazione. Sia $f = \sum_{i=0}^{n} a_i x^i \in \overline{\mathbb{Q}}[x]$ con $\deg^\star(f) \geq 1$. Poiché $f \in C[x]$ essendo $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, per il Teorema Fondamentale dell'Algebra esiste $c \in \mathbb{C}$ tale che $f(c) = 0$. Definiamo $M = \overline{\mathbb{Q}}(\{a_0, a_1, \dots, a_n\})$. Allora, per la formula del grado

$$|M : Q| = |M : Q(\{a_0, \dots, a_{n-1}\})| \cdot |Q(\{a_0, \dots, a_{n-1}\}) : Q(\{a_0, \dots, a_{n-2}\})| \cdot \dots$$

Ma sappiamo che $|M : Q(\{a_0, \dots, a_{n-1}\})| \leq \deg^\star(\min_{a_n,Q})$ e induttivamente $|M : Q| \leq \prod_{i=0}^{n} \deg^\star(\min_{a_i,Q})$. Quindi, $|M(c) : Q| = |M(c) : M| \cdot |M : Q|$, dove $|M(c) : M| \leq n$ e $|M : Q| \leq \infty$. Dunque, per la Proposizione 2 concludiamo che $c \in \overline{\mathbb{Q}}$. $\blacksquare$

Proposizione 2.X.Y: Costruzione di Kronecker

Sia $\mathbb{K}$ un campo e sia $f \in \mathbb{K}[x]$ con $\deg^\star(f) \geq 1$. Allora, esiste un'estensione $\mathbb{L}/\mathbb{K}_0$ finita e un elemento $a \in \mathbb{L}$ tale che $f(a) = 0$, dove $\mathbb{K}_0 \simeq \mathbb{K}$.

Dimostrazione. Poiché $K[x]$ è un dominio principale, possiamo scrivere $f = h \cdot f_0$ dove $h \in K[x]$ è primo e dunque irriducibile. Definiamo $L = K[x]/\langle h \rangle$. Poiché $\langle h \rangle \lhd K[x]$ è un ideale massimale, tale L è un campo. Definiamo $K_0 = \{b + \langle h \rangle : b \in K\}$, cioè $K_0 = \pi(K)$, dove $\pi \colon K[x] \to L$ è la proiezione canonica. Poiché $\langle h \rangle$ è un ideale primo, $K \cap \langle h \rangle \{0_K\}$, quindi la restrizione $\pi_K \colon K \to K_0$ è un isomorfismo. Inoltre, $|L : K_0| = \deg^\star(h) < \deg^\star(f) < \infty$, quindi abbiamo trovato un'estensione finita. Sia $h = \sum_{k=0}^{n} a_k x^k$, e sia $I = \langle h \rangle$. Detto $a = x + I \in L$, si ha che

$$h(a) = \sum_{k=0}^{n} a_k (x+I)^k = \sum_{k=0}^{n} a_k (x^k + I) = \left(\sum_{k=0}^{n} a_k x^k \right) + I = h + I = I = O_L.$$

Questo mostra che per ogni polinomio troviamo $a \in L$ tale che $f(a) = 0$, come desiderato. $\blacksquare$