

0.1 Campi di spezzamento

Definizione

Sia \mathbb{K} un campo e sia $f \in \mathbb{K}[x]$ con $\deg^*(f) = n \geq 1$. Un'estensione di campi \mathbb{L}/\mathbb{K} si dice campo di spezzamento di $f \in \mathbb{K}[x]$ se esistono $c_1, \dots, c_n \in \mathbb{L}$ e $c_f \in \mathbb{K}$ tali che:

- (i) $f(x) = c_f \prod_{i=1}^n (x - c_i) \in \mathbb{L}[x]$;
- (ii) $\mathbb{L} = \mathbb{K}(\{c_1, \dots, c_n\})$.

La condizione (i) ci dice che f si spezza in fattori lineari su $\mathbb{L}[x]$, e la condizione (ii) serve a limitare la grandezza di \mathbb{L} .

Il Teorema seguente è il teorema di esistenza e unicità del campo di spezzamento.

Teorema 2.3.1

Sia \mathbb{K} un campo e sia $f \in \mathbb{K}[x]$ non nullo con $\deg^*(f) = n \geq 1$. Allora,

- (a) esiste \mathbb{L}/\mathbb{K} campo di spezzamento di f ;
- (b) se \mathbb{L}_1/\mathbb{K} e \mathbb{L}_2/\mathbb{K} sono campi di spezzamento di f , esiste $\alpha: \mathbb{L}_1 \rightarrow \mathbb{L}_2$ isomorfismo di campi tale che la restrizione $\alpha|_{\mathbb{K}} = \text{id}_{\mathbb{K}}$.

Dimostrazione. Parte (a). Idea: esiste $a \in \mathbb{L}$ tale che $f(a) = 0$, quindi $f(x) = (x-a) \cdot f_0$, dove $\deg^*(f_0) = \deg^*(f) - 1$, e uso induzione forte. Come faccio? Definisco $\mathcal{P}(n)$ l'affermazione seguente:

- $\mathcal{P}(n)$: Sia \mathbb{K} un campo e sia $f \in \mathbb{K}[x]$ con $\deg^*(f) = n$. Allora, esiste un'estensione di campi \mathbb{L}/\mathbb{K} e esistono $c_1, \dots, c_n \in \mathbb{L}$ e $c_f \in \mathbb{K}$ tali che:

- (i) $f(x) = c_f \prod_{i=1}^n (x - c_i) \in \mathbb{L}[x]$;
- (ii) $\mathbb{L} = \mathbb{K}(\{c_1, \dots, c_n\})$.

Osserviamo che $\mathcal{P}(1)$ è vera: detto $f = a_1x + a_0$, basta prendere $L = K$ e $c_1 = -\frac{a_0}{a_1} \in \mathbb{K}$. Infatti, $f = a_1 \cdot (x - c_1)$ e $L = K = K(c_1)$. Assumiamo ora che $\mathcal{P}(k)$ sia vera per ogni $k < n$. Per la Costruzione di Kronecker, esiste \mathbb{L}/\mathbb{K} e $a \in L$ tale che $f(a) = 0$. Detto $K_1 = K(a) \subseteq L$, $f = (x - a) \cdot f_1$, dove $f_1 \in K_1[x]$, poiché per ipotesi induttiva vale $\mathcal{P}(n-1)$, esiste L/K_1 e esistono $c_1, \dots, c_{n-1} \in L$ tali che $f_1(x) = c_f \prod_{i=1}^{n-1} (x - c_i)$ e $L = K_1(\{c_1, \dots, c_{n-1}\})$. Allora, considerando L/K e $c_0 = a$, si ha che $f = c_f \prod_{i=0}^{n-1} (x - c_i) \in L[x]$ e $L = K_1(\{c_1, \dots, c_{n-1}\}) = K(\{c_0, \dots, c_{n-1}\})$, cioè $\mathcal{P}(n)$ è effettivamente vera.

Parte (b). Sia $\alpha: K_1 \rightarrow K_2$ isomorfismo di campi. Definiamo $(-)^{\alpha}: K_1[x] \rightarrow K_2[x]$ che preso $f = \sum_{k=0}^n a_k x^k$ lo manda in $f^{\alpha} = \sum_{k=0}^n \alpha(a_k) x^k$. Allora, tale funzione è un isomorfismo di anelli. Definisco $\mathcal{P}(n)$ l'affermazione seguente:

- $\mathcal{P}(n)$: Siano $\mathbb{K}_1, \mathbb{K}_2$ campi e sia $f \in \mathbb{K}_1[x]$ non nullo con $\deg^*(f) = n$. Allora, detto $\alpha: K_1 \rightarrow K_2$ isomorfismo di campi, L_1/K_1 il campo di spezzamento di $f \in K_1[x]$ e L_2/K_2 il campo di spezzamento di $f^{\alpha} \in K_2[x]$, esiste $\alpha_{\star}: L_1 \rightarrow L_2$ isomorfismo di campi tale che la restrizione $\alpha_{\star}|_{K_1} = \alpha$.

Osserviamo che $\mathcal{P}(1)$ è vera, perché preso $f = a_1x + a_0 = a_1(x - c_1)$, dove $c_1 = -\frac{a_0}{a_1} \in K_1$, e scelgo $L_1 = K_1$; inoltre, $f^\alpha = \alpha(a_1)x + \alpha(a_0)$ e $\alpha(c_1) = \frac{\alpha(a_0)}{\alpha(a_1)}$, cioè $f^\alpha = \alpha(a_1)(x - \alpha(c_1))$ e prendo $L_2 = K_2$, quindi $\alpha: L_1 \rightarrow L_2$ è l'isomorfismo tra campi richiesto. Supponiamo ora che $\mathcal{P}(k)$ sia vera per ogni $k < n$. Sia $f = h \cdot f_0$ di grado n con $h \in K_1[x]$ irriducibile, $\deg^*(h) > 0$. Allora, perché L_1/K_1 è campo di spezzamento per f_1 , esiste $c \in L_1$ tale che $h(c) = 0$. Dunque, $h(x) = (x - c) \cdot h_0(x) \in L_1[x]$. Sia $M_1 = K_1[c]$ (cioè, K_1 con l'aggiunta dell'elemento algebrico c), così che abbiamo $h(x) = (x - c)h_0(x) \in M_1[x]$. Allora, detto $f_1 = h_0(x) \cdot f_0(x) \in M_1[x]$, si ha $\deg^*(f_1) = n - 1$. Da $f = h \cdot f_0$, deduciamo che $f^\alpha = h^\alpha \cdot f_0^\alpha$, dove h^α è anch'esso irriducibile (se fosse $h^\alpha = h_1 \cdot h_2$, avremmo $h = h_1^{\alpha^{-1}} \cdot h_2^{\alpha^{-1}}$ dove $\alpha^{-1}: K_2 \rightarrow K_1$ è la funzione inversa di α). Poiché L_2/K_2 è campo di spezzamento di f^α , esiste $d \in L_2$ tale che $h^\alpha(d) = 0$. Detto $M_2 = K_2[d]$, L_1/M_1 è campo di spezzamento di f_1 e L_2/M_2 è campo di spezzamento di $f_2 = f_1^\alpha/(x - d)$. Resta da mostrare che esiste un isomorfismo di campi $\beta: M_1 \rightarrow M_2$ tale che $\beta(c) = d$, e $\beta|_{K_1} = \alpha$, perché in questo modo $f_1^\beta = f_2$. Infatti $f^\beta = (x - c)^\beta f_1^\beta = (x - d) \cdot f_2 = f^\alpha$, da cui effettivamente $f_1^\beta = f_2$. Per ipotesi induttiva, poiché vale $\mathcal{P}(n - 1)$, sappiamo che esiste un isomorfismo tra campi $\beta_*: L_1 \rightarrow L_2$ tale che $\beta_*|_{M_1} = \beta$, da cui $\beta_*|_{K_1} = \beta|_{K_1} = \alpha$, e abbiamo concluso perché ora prendiamo $\alpha_* = \beta_*$, quindi vale $\mathcal{P}(n)$. A quanto pare serve un pezzo del Teorema seguente per concludere. ■

Proposizione 2.3.2

Sia $\alpha: K_1 \rightarrow K_2$ isomorfismo di campi e siano $h \in K_1[x]$ irriducibile, L_1/K_1 estensione di campi, $c \in L_1$ tale che $h(c) = 0$, L_2/K_2 estensione di campi, $d \in L_2$ tale che $h^\alpha(d) = 0$. Allora, esiste un isomorfismo di campi $\beta: K_1[c] \rightarrow K_2[d]$ tale che $\beta|_{K_1} = \alpha$.

Dimostrazione. Vedi appunti cartacei per diagramma commutativo da aggiungere; lui ha anche messo un asterisco a sx nelle funzioni ma non so come metterlo adesso. Senza perdita di generalità siano h monico, cioè $h = \min_{c, K_1}$, e h^α monico (so già che è irriducibile), $h^\alpha(d) = 0$, quindi prendo $h^\alpha = \min_{d, K_2}$. Siano $\phi_c: K_1[x]/\langle h \rangle \rightarrow K_1[c]$, $\phi_d: K_2[x]/\langle h^\alpha \rangle \rightarrow K_2[d]$ le mappe indotte dalle valutazioni, $\alpha: K_1[x]/\langle h \rangle \rightarrow K_2[x]/\langle h^\alpha \rangle$ la mappa indotta da α del Teorema 2.3.1 punto (b). Definisco $\beta = \phi_d \circ \alpha \phi_c^{-1}: K_1[c] \rightarrow K_2[d]$. Questa è un isomorfismo perché composizione di isomorfismi, in quanto tutte le funzioni definite precedentemente sono isomorfismi per il *Primo teorema d'isomorfismo*. La verifica che $\beta|_{K_1} = \alpha$ è banale. Boh, sta cosa è completamente delirante. ■