Estensioni algebriche di $\mathbb{K}$

§1.1 Morfismi di valutazione, elementi algebrici e trascendenti

Si definisce adesso il concetto di *omomorfismo di valutazione*, che impiegheremo successivamente nello studio dei quozienti $\mathbb{K}[x]/(f(x))$ e dei cosiddetti *elementi algebrici* (o *trascendenti*).

Definizione 1.1.1. Sia B un anello commutativo, e sia $A \subseteq B$ un suo sottoanello. Si definisce **omomorfismo di valutazione** di $\alpha \in B$ in A l'omomorfismo:

$$\varphi_\alpha : A[x] \to B,\ f(x) \mapsto f(\alpha).$$

Osservazione. L'omomorfismo di valutazione è effettivamente un omomorfismo di anelli. Innanzitutto $\varphi_\alpha(1) = 1$. Inoltre vale la linearità:

$$\varphi_\alpha(f(x)) + \varphi_\alpha(g(x)) = f(\alpha) + g(\alpha) = (f+g)(\alpha) = \varphi_\alpha((f+g)(x)) = \\ = \varphi_\alpha(f(x) + g(x)),$$

così come la moltiplicatività:

$$\varphi_\alpha(f(x))\varphi_\alpha(g(x)) = f(\alpha)g(\alpha) = (fg)(\alpha) = \varphi_\alpha((fg)(x)) = \varphi_\alpha(f(x)g(x)).$$

Si evidenziano adesso le principali proprietà di tale omomorfismo.

Proposizione 1.1.2
$\operatorname{Im}\varphi_\alpha = A[\alpha]$

Dimostrazione. Sicuramente $\operatorname{Im}\varphi_\alpha \subseteq A[\alpha]$, dacché ogni immagine di φ_α è una valutazione di un polinomio a coefficienti in A in α.

Sia dunque $a = a_n\alpha^n + \ldots + a_0 \in A[\alpha]$. Allora $\varphi_\alpha(a_nx^n + \ldots + a_0) = a$. Pertanto $a \in \operatorname{Im}\varphi_\alpha$, da cui $A[\alpha] \in \operatorname{Im}\varphi_\alpha$.

Poiché vale la doppia inclusione, si desume che $\operatorname{Im}\varphi_\alpha = A[\alpha]$. □

Prima di applicare il *Primo teorema d'isomorfismo*, si distinguono due importanti casi, sui quali si baseranno le definizioni di *elemento algebrico* e di *elemento trascendente*.

Definizione 1.1.3. Sia $\alpha \in B$. Se $\operatorname{Ker}\varphi_\alpha = (0)$, allora si dice che α è un **elemento trascendente** di B su A.

Osservazione. Equivalentemente, se $\alpha \in B$ è trascendente su A, significa che non vi è alcun polinomio non nullo in $A[x]$ che ha α come soluzione.

Esempio 1.1.4

Per esempio, il numero di Nepero-Eulero e è trascendente su $\mathbb{Q}[x]$[a]. Quindi $\operatorname{Ker}\varphi_e = (0)$, e dunque, dal *Primo teorema di isomorfismo*, vale che:

$$\mathbb{Q}[x] \cong \mathbb{Q}[x]/(0) \cong \mathbb{Q}[e].$$

[a] Per una dimostrazione di questo fatto, si guardi a [H, pp. 234-237]

Possiamo generalizzare questo esempio nel seguente teorema.

Teorema 1.1.5

Sia B un campo e sia $A \subseteq B$ un suo sottoanello. Se $\alpha \in B$ è trascendente su A, allora vale la seguente relazione:

$$A[x] \cong A[\alpha].$$

Dimostrazione. Si consideri l'omomorfismo φ_α. Dacché α è trascendente, $\operatorname{Ker}\varphi_\alpha = (0)$. Allora, combinando il *Primo teorema di isomorfismo* con la *Proposizione 1.1.2*, si ottiene proprio $A[x] \cong A[x]/(0) \cong A[\alpha]$, ossia la tesi. □

Definizione 1.1.6. Sia $\alpha \in B$. Se $\operatorname{Ker}\varphi_\alpha \neq (0)$, allora si dice che α è un **elemento algebrico** di B su A, mentre il generatore monico[a] non nullo di $\operatorname{Ker}\varphi_\alpha$ si dice **polinomio minimo** di α su A. Il grado di tale polinomio minimo è detto **grado di** α.

[a] Vi potrebbero essere infatti più generatori di $\operatorname{Ker}\varphi_\alpha$, sebbene tutti associati tra loro. L'attributo *monico* garantisce così l'unicità del polinomio minimo.

Osservazione. Equivalentemente, se $\alpha \in B$ è trascendente su A, significa che esiste un polinomio non nullo in $A[x]$ che ha α come soluzione. In particolare, ogni polinomio in $A[x]$ che ha α come soluzione è un multiplo del suo polinomio minimo su A.

Esempio 1.1.7

Sia $\alpha \in A$. Allora α è banalmente un elemento algebrico su A, il cui polinomio minimo è $x-\alpha$. Vale dunque che $\operatorname{Ker}\varphi_\alpha = (x-\alpha)$, da cui, secondo il *Primo teorema di isomorfismo*, si ricava che:

$$A[x]/(x-\alpha) \cong A[\alpha] \cong A.$$

Esempio 1.1.8

$i \in \mathbb{C}$ è un elemento algebrico su $\mathbb{R}$. Infatti, si consideri φ_i: poiché i è soluzione di x^2+1, si ha che $x^2+1 \in \operatorname{Ker}\varphi_i$, che è quindi non vuoto.

Inoltre, dal momento che x^2+1 è irriducibile in $\mathbb{R}[x]$, esso è generatore di $\operatorname{Ker}\varphi_i$. Inoltre, poiché monico, è anche il polinomio minimo di i su $\mathbb{R}$.

Allora, poiché dalla *Proposizione 1.1.2* $\operatorname{Im}\varphi_i = \mathbb{R}[i]$, si deduce dal *Primo teorema di isomorfismo* che:

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{R}[i] \cong \mathbb{C}.$$

Ancora una volta possiamo generalizzare questo esempio con il seguente teorema.

Teorema 1.1.9

Sia B un campo e sia $A \subseteq B$ un suo sottoanello. Se $\alpha \in B$ è algebrico su A, allora, detto $f(x)$ il polinomio minimo di α, vale la seguente relazione:

$$A[x]/(f(x)) \cong A[\alpha].$$

Dimostrazione. Si consideri l'omomorfismo φ_α. Dacché $\operatorname{Ker}\varphi_\alpha = (f(x))$ per definizione di polinomio minimo, combinando il *Primo teorema di isomorfismo* con la *Proposizione 1.1.2*, si ottiene proprio $A[x]/(f(x)) \cong A[\alpha]$, ossia la tesi. □

Definizione 1.1.10. Sia B un campo e sia $A \subseteq B$ un suo sottoanello. Allora, dato $\alpha \in B$, si definisce con la notazione $A(\alpha)$ il sottocampo di B che contiene A e α che sia minimale rispetto all'inclusione.

Osservazione. Le notazioni $\mathbb{K}(\alpha,\beta)$ e $\mathbb{K}(\alpha)(\beta)$ sono equivalenti.

Proposizione 1.1.11

Sia B un campo e sia $A \subseteq B$ un suo sottoanello. Se $\alpha \in B$ è algebrico su A, allora $A(\alpha) = A[\alpha]$.

Dimostrazione. Se α è algebrico, allora $\operatorname{Ker} \varphi_\alpha = (f(x)) \neq (0)$, dove $f(x) \in A[x]$ è irriducibile. Pertanto $A[x]/(f(x))$ è un campo.

Dunque dal *Teorema 1.1.9* si ricava che:

$$A[x]/(f(x)) \cong A[\alpha].$$

Pertanto $A[\alpha]$ è un campo. Dacché $A[\alpha] \subseteq A(\alpha)$ e $A(\alpha)$ è minimale rispetto all'inclusione, si deduce che $A[\alpha] = A(\alpha)$, ossia la tesi. □

Osservazione. Il teorema che è stato appena enunciato non vale per gli elementi trascendenti. Infatti, $A[\alpha]$ sarebbe isomorfo a $A[x]$, che non è un campo. Al contrario $A(\alpha)$ è un campo, per definizione.

Proposizione 1.1.12

Sia B un campo e sia $A \subseteq B$ un suo sottoanello. Se α, $\beta \in B$ sono algebrici su A e condividono lo stesso polinomio minimo, allora $A[\alpha] \cong A[\beta]$.

Dimostrazione. Sia $f(x)$ il polinomio minimo di α e β. Dal *Primo teorema di isomorfismo* e dalla *Proposizione 1.1.2* si desume che $A[x]/(f(x)) \cong A[\alpha]$. Analogamente si ricava che $A[x]/(f(x)) \cong A[\beta]$. Pertanto $A[\alpha] \cong A[\beta]$. □

§1.2 Teorema delle torri ed estensioni algebriche

Definizione 1.2.1. Siano $A \subseteq B$ campi. Allora si denota come $[B : A]$ la dimensione dello spazio vettoriale B costruito su A, ossia $\dim B_A$. Tale dimensione è detta **grado dell'estensione**.

Teorema 1.2.2 (*Teorema delle torri algebriche*)

Siano $A \subseteq B \subseteq C$ campi[a]. Allora:

$$[C : A] = [C : B][B : A].$$

[a] In realtà è sufficiente che C sia uno spazio vettoriale su A e B e che $A \subseteq B$, posto che A e B siano campi.

Dimostrazione. Siano $[C : B] = m$ e $[B : A] = n$. Sia $\mathcal{B}_C = (a_1, \dots, a_m)$ una base di C su B, e sia $\mathcal{B}_B = (b_1, \dots, b_n)$ una base di B su A.

Si dimostra che la seguente è una base di C su A:

$$\mathcal{B}_A\mathcal{B}_B = \{a_1b_1, \dots, a_1b_n, \dots, a_mb_n\}.$$

(i) $\mathcal{B}_C\mathcal{B}_B$ genera A su C.

Sia $c \in C$. Allora si può descrivere a nel seguente modo:

$$c = \sum_{i=1}^{m} \beta_i a_i, \quad \text{con } \beta_i \in B, \ \forall\, 1 \leq i \leq m.$$

A sua volta, allora, si può descrivere ogni β_i nel seguente modo:

$$\beta_i = \sum_{j=1}^{n} \gamma_j^{(i)} b_j, \quad \text{con } \gamma_j^{(i)} \in A, \ \forall\, 1 \leq j \leq n.$$

Combinando le due equazioni, si verifica che $\mathcal{B}_C\mathcal{B}_B$ genera C su A:

$$c = \sum_{i=1}^{m}\sum_{j=1}^{n} \gamma_j^{(i)} b_j a_i, \quad \text{con } \gamma_j^{(i)} \in A, \ \forall\, 1 \leq i \leq m, \ 1 \leq j \leq n.$$

(ii) $\mathcal{B}_C\mathcal{B}_B$ è linearmente indipendente.

Si consideri l'equazione:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} \gamma_j^{(i)} b_j a_i = 0, \quad \text{con } \gamma_j^{(i)} \in A, \ \forall\, 1 \leq i \leq m, \ 1 \leq j \leq n.$$

Poiché $\mathcal{B}_C$ è linearmente indipendente, si deduce che:

$$\sum_{j=1}^{n} \gamma_j^{(i)} b_j = 0, \ \forall\, 1 \leq i \leq m.$$

Tuttavia, $\mathcal{B}_B$ è a sua volta linearmente indipendente, e quindi $\gamma_j^{(i)} = 0$, $\forall\, i, j$. Dunque $\mathcal{B}_C\mathcal{B}_B$ è linearmente indipendente.

Dal momento che $\mathcal{B}_C\mathcal{B}_B$ è linearmente indipendente e genera C su A, consegue che essa sia una base di C su A. Quindi $[C : A] = mn = [C : B][B : A]$, da cui la tesi. □

Definizione 1.2.3. Siano $A \subseteq B$ campi. Se $[B : A] \neq \infty$, allora si dice che BA è un'**estensione finita** di A. Altrimenti si dice che B è un'**estensione infinita** di A.

Proposizione 1.2.4

Siano $A \subseteq B \subseteq C$ campi. Allora, se C è un'estensione finita di A, anche B lo è. Inoltre C è un'estensione finita di B.

Dimostrazione. Dal momento che B è un sottospazio dello spazio vettoriale C costruito su A, e questo ha dimensione finita, anche B su A ha dimensione finita. Quindi $[B : A] \neq \infty$, e B è dunque un'estensione finita di A.

Infine, dacché una base di C su A è un generatore finito di C su B, si deduce che $[C : B] \neq \infty$, e quindi che C è un'estensione finita di B. □

Teorema 1.2.5

Siano $A \subseteq B$ campi. Allora $a \in B$ è algebrico su A se e solo se $[A(a) : A] \neq \infty$, ossia solo se $A(a)$ è un'estensione finita di A.

Dimostrazione. Si dimostrano le due implicazioni separatamente.

($\Longrightarrow$) Se $a \in B$ è algebrico su A, allora dal *Teorema 1.1.9* si ricava che:

$$A[x]/(f(x)) \cong A[a] \cong A(a).$$

Dacché $A[x]/(f(x))$ ha dimensione finita, anche $A(a)$ ha dimensione finita, e quindi è un'estensione finita di A.

($\Longleftarrow$) Sia $A(a)$ un'estensione finita di A e sia $[A(a) : A] = m$. Allora $I = (1, a, a^2, \ldots, a^m)$ è linearmente dipendente, dal momento che contiene $m + 1$ elementi. Quindi esiste una sequenza finita non nulla $(\alpha_i)_{i=0\to m}$ con elementi in A tale che:

$$\alpha_m a^m + \ldots + \alpha_2 a^2 + \alpha_1 a + \alpha_0 = 0.$$

Quindi a è soluzione del polinomio:

$$f(x) = \alpha_m x^m + \ldots + \alpha_2 x^2 + \alpha_1 x + \alpha_0 \in A[x],$$

pertanto a è algebrico su A, da cui la tesi. □

Definizione 1.2.6. Siano $A \subseteq B$ campi. Allora si dice che B è un'**estensione algebrica** di A se ogni elemento di B è algebrico su A.

Proposizione 1.2.7

Siano $A \subseteq B$ campi. Se B è un'estensione finita di A, allora B è una sua estensione algebrica.

Dimostrazione. Sia $\alpha \in B$ e si consideri la catena di campi $A \subseteq A(\alpha) \subseteq B$. Dacché $[B : A] \neq \infty$, per la *Proposizione 1.2.4* anche $[A(\alpha) : A] \neq \infty$. Pertanto, dal *Teorema 1.2.5*, α è algebrico. Così tutti gli elementi di B sono algebrici in A, e dunque, per definizione, B è un'estensione algebrica di A. □

Teorema 1.2.8

Siano $A \subseteq B$ campi e siano β_1, β_2, …, β_n elementi algebrici di B su A, con $n \geq 1$. Allora $[A(\beta_1, \beta_2, \ldots, \beta_n) : A] \neq \infty$.

Dimostrazione. Si procede applicando il principio di induzione su n.

(*passo base*) La tesi è verificata per il *Teorema 1.2.5*.

(*passo induttivo*) Per l'ipotesi induttiva, si sa che $[A(\beta_1, \beta_2, \ldots, \beta_{n-1}) : A] \neq \infty$.

Poiché β_n è algebrico su A, sin da subito si osserva che $[A(\beta_n) : A] \neq \infty$ per il *Teorema 1.2.5*. Sia allora $f(x)$ il polinomio minimo di β_n appartenente a $A[x]$. Esso è un polinomio che ammette β_n come radice anche in $A(\beta_1, \beta_2, \ldots, \beta_{n-1})[x]$, e quindi $\operatorname{Ker} \varphi_{\beta_n} \neq (0)$ ammette un generatore $p(x)$, che divide $f(x)$. Si ottiene pertanto la seguente disuguaglianza:

$$[A(\beta_1, \beta_2, \ldots, \beta_{n-1})(\beta_n) : A(\beta_1, \beta_2, \ldots, \beta_{n-1})] = \deg p(x) \leq \deg f(x) = [A(\beta_n) : A].$$

Poiché $[A(\beta_n) : A]$ è finito, anche $[A(\beta_1, \beta_2, \ldots, \beta_{n-1})(\beta_n) : A(\beta_1, \beta_2, \ldots, \beta_{n-1})]$ lo è.

Combinando i due risultati, si ottiene con il *Teorema delle torri algebriche* che:

$$[A(\beta_1, \beta_2, \ldots, \beta_n) : A] = [A(\beta_1, \beta_2, \ldots, \beta_{n-1})(\beta_n) : A(\beta_1, \beta_2, \ldots, \beta_{n-1})] \cdot [A(\beta_1, \beta_2, \ldots, \beta_{n-1}) : A] \neq \infty,$$

da cui la tesi.

□

Corollario 1.2.9

Siano $A \subseteq B$ campi e siano α, $\beta \in B$ elementi algebrici su A. Allora $A(\alpha, \beta)$ è un'estensione algebrica.

Dimostrazione. Dal *Teorema 1.2.8* si ricava che $[A(\alpha, \beta) : A] \neq \infty$. Quindi $A(\alpha, \beta)$ è un'estensione finita di A, ed in quanto tale, per la *Proposizione 1.2.7*, essa è algebrica. □

Osservazione. Esistono estensioni algebriche che hanno grado infinito. Un esempio notevole è $\mathcal{A}$, l'insieme dei numeri algebrici di $\mathbb{C}$ su $\mathbb{Q}$. Infatti, si ponga $[\mathcal{A} : \mathbb{Q}] = n - 1 \in \mathbb{N}$ e si consideri $x^n - 2$. Dal momento che per il *Criterio di Eisenstein* tale polinomio è irriducibile, si ricava che $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.

Poiché $\sqrt[n]{2}$ è algebrico, si deduce che $\mathbb{Q}(\sqrt[n]{2}) \subseteq \mathcal{A}$, dal momento che per il *Corollario 1.2.9* ogni elemento di $\mathbb{Q}(\sqrt[n]{2})$ è algebrico su $\mathbb{Q}$. Tuttavia questo è un assurdo dal momento che $\mathbb{Q}(\sqrt[n]{2})$ ha dimensione maggiore di $\mathcal{A}$, di cui è sottospazio vettoriale.

Proposizione 1.2.10

Siano $A \subseteq B$ campi e sia $\alpha \in B$. Se $[A(\alpha) : A]$ è dispari, allora $A(\alpha^2) = A(\alpha)$.

Dimostrazione. Innanzitutto, si osserva che $A(\alpha^2) \subseteq A(\alpha)$, ossia che $A(\alpha)$ è un'estensione di $A(\alpha^2)$. Grazie a questa osservazione è possibile considerare il grado di $A(\alpha)$ su $A(\alpha^2)$, ossia $[A(\alpha) : A(\alpha^2)]$. Poiché α è radice del polinomio $x^2 - \alpha^2$ in $A(\alpha^2)$, si deduce che tale grado è al più 2.

Si applichi il *Teorema delle torri algebriche* alla catena di estensioni $A \subseteq A(\alpha^2) \subseteq A(\alpha)$:

$$[A(\alpha) : A] = \underbrace{[A(\alpha) : A(\alpha^2)]}_{\leq 2}[A(\alpha^2) : A].$$

Se $[A(\alpha) : A(\alpha^2)]$ fosse 2, $[A(\alpha) : A]$ sarebbe pari, ↯. Pertanto $[A(\alpha) : A(\alpha^2)] = 1$, da cui si ricava che $[A(\alpha) : A] = [A(\alpha^2) : A]$, ossia che $A(\alpha^2)$ ha la stessa dimensione di $A(\alpha)$ su A.

Dal momento che $A(\alpha^2)$ è un sottospazio vettoriale di $A(\alpha)$, avere la sua stessa dimensione equivale a coincidere con lo spazio stesso. Si conclude allora che $A(\alpha^2) = A(\alpha)$. □

Osservazione. Si osserva che la *Proposizione 1.2.10* si può generalizzare facilmente ad un esponente n qualsiasi, finché sia data come ipotesi la non divisibilità di $[A(\alpha) : A]$ per nessun numero primo minore o uguale di n.

Si può infatti considerare, per la dimostrazione generale, il polinomio $x^n - \alpha^n$, la cui esistenza

> implica che $[A(\alpha) : A(\alpha^n)]$ sia minore o uguale di n.

Teorema 1.2.11

Siano $A \subseteq B \subseteq C$ campi. Se B è un'estensione algebrica di A e C è un'estensione algebrica di B, allora C è un'estensione algebrica di A.

Dimostrazione. Per mostrare che C è un'estensione algebrica di A, verificheremo che ogni suo elemento è algebrico in A. Sia dunque $c \in C$.

Poiché per ipotesi c è algebrico su B, esiste un polinomio $f(x) \in B[x]$ tale che c ne sia radice. Sia $f(x)$ il polinomio minimo di c su B, descritto come:

$$f(x) = b_0 + b_1 x + \ldots + b_n x^n, \quad n = [B(c) : B].$$

Dacché B è un'estensione algebrica di A, ogni coefficiente b_i di $f(x)$ è algebrico su A, ossia $[A(b_i) : A] \neq \infty$. Allora, per il *Teorema 1.2.8*, $[A(b_0, \ldots, b_n) : A] \neq \infty$.

Anche $[A(c, b_0, \ldots, b_n) : A(b_0, \ldots, b_n)] \neq \infty$, dal momento che c è soluzione di $f(x) \in A(b_0, \ldots, b_n)[x]$.

Allora, per il *Teorema delle torri algebriche*, $[A(c, b_0, \ldots, b_n) : A] = [A(c, b_0, \ldots, b_n) : A(b_0, \ldots, b_n)][A(b_0, \ldots, b_n) : A] \neq \infty$. Quindi $A(c, b_0, \ldots, b_n)$ è un'estensione finita di A.

Poiché $A \subseteq A(c) \subseteq A(c, b_0, \ldots, b_n)$ è una catena di estensione di campi, per la *Proposizione 1.2.4*, $A(c)$ è un'estensione finita di A, ed in quanto tale, per la *Proposizione 1.2.7*, è anche algebrica. Quindi c è algebrico su A, da cui la tesi. □

Teorema 1.2.12

Sia A un campo, e sia $f(x) \in A[x]$. Allora esiste sempre un estensione di A in cui siano contenute tutte le radici di $f(x)$.

Dimostrazione. Si dimostra il teorema applicando il principio di induzione sul grado di $f(X)$.

(*passo base*) Sia $\deg f(x) = 0$. Allora A stesso è un campo in cui sono contenute tutte le radici, dacché esse non esistono.

(*passo induttivo*) Sia $\deg f(x) = n$. Sia $f_1(x)$ un irriducibile di $f(x)$ e sia $\gamma(x) \in A[x]$ tale che $f(x) = f_1(x)\gamma(x)$. Allora $A[x]/(f_1(x))$ è un campo in cui $f_1(x)$ ammette radice.

Poiché $\deg \gamma(x) < n$, per il passo induttivo esiste un campo C che estende $A[x]/(f_1(x))$ in cui risiedono tutte le sue radici. Dacché C contiene $A[x]/(f_1(x))$, sia le radici di $f_1(x)$ che di $\gamma(x)$ risiedono in C. Tuttavia queste sono tutte le radici di $f(x)$, si conclude che C, che è un'estensione di $A[x]/(f_1(x))$, e quindi anche di A, è il campo ricercato. □

§1.3 Campi di spezzamento di un polinomio

Pertanto ora è possibile enunciare la definizione di *campo di spezzamento*.

Definizione 1.3.1. Si definisce **campo di spezzamento** di un polinomio $f(x) \in A[x]$ un campo C con le seguenti caratteristiche:

- $f(x)$ si fattorizza in $C[x]$ come prodotto di irriducibili di primo grado (i.e. in $C[x]$ risiedono tutte le radici di $f(x)$),
- Se B è un campo tale che $A \subseteq B \subsetneq C$, allora $f(x)$ non si fattorizza in $B[x]$ come prodotto di irriducibili di primo grado.

Osservazione. Per il *Teorema 1.2.12* esiste sempre un campo di spezzamento di un polinomio, dunque la definizione data è una buona definizione.

Osservazione. In generale i campi di spezzamento non sono uguali, sebbene siano tutti isomorfi tra loro[a].

[a] Per la dimostrazione di questo risultato si rimanda a TODO

Teorema 1.3.2

Sia A un campo e sia $B \supseteq A$ un campo di spezzamento di $f(x) \in A[x]$ su A, con $f(x)$ non costante. Sia $\deg f(x) = n$. Allora $[B : A] \leq n!$.

Dimostrazione. Siano $\lambda_1, \lambda_2, \ldots, \lambda_n$ le radici di $f(x)$. Allora $[\mathbb{K}(\lambda_1) : \mathbb{K}] \leq n$, dacché λ_1 è radice di $f(x)$.

Sia ora $f(x) = (x - \lambda_1)g(x)$, con $\deg g(x) = n - 1$. Sicuramente λ_2 è radice di $g(x)$, pertanto $[\mathbb{K}(\lambda_1, \lambda_2) : \mathbb{K}(\lambda_1)] \leq n - 1$. Reiterando il ragionamento si può applicare infine il *Teorema delle torri algebriche*:

$$[\mathbb{K}(\lambda_1, \ldots, \lambda_n) : \mathbb{K}] = [\mathbb{K}(\lambda_1, \ldots, \lambda_n) : \mathbb{K}(\lambda_1, \ldots, \lambda_{n-1})] \cdots [\mathbb{K}(\lambda_1) : \mathbb{K}] \leq 1 \cdot 2 \cdots n = n!,$$

da cui la tesi. □

Riferimenti bibliografici

[H] I.N. Herstein. *Algebra*. Editori Riuniti University Press, 2010. ISBN: 9788864732107.