

# Estensioni di campo ed elementi algebrici e trascendenti

di Gabriel Antonio Videtta

**Nota.** Una buona introduzione alle estensioni di campo è già stata fatta nel corso di Aritmetica<sup>1</sup>, e pertanto l'esposizione in questo documento dell'argomento sarà del tutto *straightforward*.

Per  $K$ ,  $L$  ed  $F$  si intenderanno sempre dei campi. Se non espressamente detto, si sottintenderà anche che  $K \subseteq L$ ,  $F$ , e che  $L$  ed  $F$  sono estensioni costruite su  $K$ . Per  $[L : K]$  si intenderà  $\dim_K L$ , ossia la dimensione di  $L$  come  $K$ -spazio vettoriale.

Lo studio della teoria dei campi è inevitabile quando si intende studiare la risolubilità delle equazioni, come ben illustra la teoria di Galois. In particolare, questa teoria si basa in parte sullo studio delle estensioni, ossia dei “sovracampi”, del campo di partenza che si sta studiando. A questo proposito tornano utili le seguenti definizioni:

**Definizione** (estensione di campo). Si dice che  $L$  è un'estensione di campo di  $K$  se  $K \subseteq L$ , e si scrive  $L/K$  per studiare  $L$  in riferimento a  $K$ . Si dice che  $L$  è un'estensione finita se  $[L : K]$  è finito.

**Definizione** (omomorfismo di valutazione). Sia  $\alpha \in K$ . Allora si definisce l'**omomorfismo di valutazione**  $\varphi_{\alpha, K} : K[x] \rightarrow K[\alpha]$  di  $\alpha$  su  $K$ , spesso abbreviato come  $\varphi_\alpha$  se è sottinteso che si sta lavorando su  $K$ , come l'omomorfismo univocamente determinato dalla relazione:

$$p \xrightarrow{\varphi_\alpha} p(\alpha).$$

**Osservazione.** L'omomorfismo di valutazione è sempre surgettivo e la preimmagine di un elemento di  $K[\alpha]$  è per esempio lo stesso elemento a cui si è sostituito  $x$  al posto di  $\alpha$ .

**Definizione.** Sia  $\alpha \in K$ . Allora si definisce  $K(\alpha)$  come la più piccola estensione di  $K$  che contiene  $\alpha$ , ossia:

$$K(\alpha) = \bigcap_{\substack{F_i/K \text{ campo} \\ \alpha \in F_i}} F_i.$$

---

<sup>1</sup>Questa parte di teoria è reperibile al seguente link: <https://git.phc.dm.unipi.it/g.videtta/notes/src/branch/main/Primo%20anno/Aritmetica/Teoria%20dei%20campi>.

**Definizione** (estensione semplice). Un'estensione  $L/K$  si dice **semplice** se esiste  $\alpha \in L$  tale per cui  $L = K(\alpha)$ .

**Osservazione.** Come suggerisce la definizione di  $K(\alpha)$ , se  $L/K$  è un campo che contiene  $\alpha$ ,  $K(\alpha) \subseteq L$ .

**Definizione** (elementi algebrici e trascendenti). Sia  $\alpha \in K$ . Allora  $\alpha$  si dice **algebrico** su  $K$  se  $\exists p \in K[x]$  tale per cui  $p(\alpha) = 0$ . Se  $\alpha$  non è algebrico, si dice che  $\alpha$  è **trascendente**.

**Osservazione.** Se  $\alpha \in K$ ,  $\alpha$  è algebrico se e solo se  $\text{Ker } \varphi_\alpha$  è non banale. Analogamente  $\alpha$  è trascendente se e solo se  $\text{Ker } \varphi_\alpha$  è banale.

**Osservazione.** Se  $\alpha \in K$  è algebrico, allora  $\text{Ker } \varphi_\alpha$  è generato da un irriducibile dacché  $K[x]$  è un PID. In particolare  $K[x]/\text{Ker } \varphi_\alpha$  è un campo, e dunque, per il Primo teorema di isomorfismo, lo è anche  $K[\alpha]$ . Dal momento che  $K[\alpha] \subseteq K(\alpha)$ , allora vale in questo caso che  $K(\alpha) = K[\alpha]$ .

**Definizione.** Sia  $\alpha \in K$  algebrico su  $K$ . Si definisce il **polinomio minimo**  $\mu_\alpha \in K[x]$  come il generatore monico di  $\text{Ker } \varphi_\alpha$ . Per semplicità si definisce  $\deg_K \alpha$  come il grado di  $\mu_\alpha$ .

**Osservazione.** Se  $\alpha \in K$  è algebrico, allora  $K[x]/\text{Ker } \varphi_\alpha$  è uno spazio vettoriale su  $K$  di dimensione  $\deg_K \alpha$ . In particolare vale allora che  $[K(\alpha) : K] = [K[x]/\text{Ker } \varphi_\alpha : K] = \deg_K \alpha$ . Inoltre  $\mu_\alpha$  è irriducibile su  $K$  dal momento che  $\text{Ker } \varphi_\alpha$  è massimale.

**Osservazione.** Se  $\alpha \in K$  è trascendente, allora  $\text{Ker } \varphi_\alpha$  è banale e dunque, per il Primo teorema di isomorfismo,  $K[x] \cong K[\alpha]$ .

La caratterizzazione degli elementi algebrici e trascendenti si conclude mediante la seguente proposizione:

**Proposizione** (caratterizzazione degli elementi algebrici e trascendenti). Sia  $\alpha \in K$ . Allora  $\alpha$  è algebrico su  $K$  se e solo se  $[K(\alpha) : K]$  è finito.

*Dimostrazione.* Se  $\alpha$  è algebrico, allora  $[K(\alpha) : K]$  è pari a  $\deg_K \alpha$ . Se invece  $[K(\alpha) : K]$  è pari ad  $n \in \mathbb{N}^+$ , si considerino  $1, \alpha, \dots, \alpha^n$ . Dal momento che questi sono  $n+1$  elementi in  $K(\alpha)$ , devono essere necessariamente linearmente dipendenti. Pertanto esistono  $a_0, a_1, \dots, a_n$  tali per cui  $a_n \alpha^n + \dots + a_1 \alpha + a_0 = 0$ . Pertanto esiste un polinomio con coefficienti in  $K$  che annulla  $\alpha$ , e dunque  $\alpha$  è algebrico.  $\square$

A partire dalla definizione di elemento algebrico si può anche definire la nozione di *estensione algebrica*:

**Definizione** (estensione algebrica). Si consideri  $L/K$ . Allora si dice che  $L$  è un'**estensione algebrica** se ogni elemento di  $L$  è algebrico su  $K$ .

Le estensioni finite sono privilegiate in questo senso, dal momento che sono sempre algebriche, come illustra la:

**Proposizione** (estensione finita  $\implies$  estensione algebrica). Sia  $L$  un'estensione finita di  $K$ . Allora  $L$  è un'estensione algebrica di  $K$ .

*Dimostrazione.* Sia  $\alpha \in L$ . Dal momento che  $K \subseteq K(\alpha) \subseteq L$ ,  $K(\alpha)$  è un sottospazio di  $L$ , che è spazio vettoriale su  $K$ . Dal momento che  $L$  è un'estensione finita,  $[L : K]$  è finito, e dunque lo è anche  $[K(\alpha) : K]$ , per cui  $\alpha$  è algebrico, e così  $L$ .  $\square$

**Osservazione.** Mentre ogni estensione finita è algebrica, non è vero che ogni estensione algebrica è finita. Per esempio, la chiusura algebrica  $\overline{\mathbb{Q}}$  di  $\mathbb{Q}$  non è finita su  $\mathbb{Q}$ . Infatti, per ogni  $n \in \mathbb{N}^+$ ,  $p_n(x) = x^n - 2$  è irriducibile in  $\mathbb{Q}[x]$  per il criterio di Eisenstein, e dunque, detta  $\alpha$  una radice di  $p_n$ ,  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ , e quindi, dal momento che  $\mathbb{Q}(\alpha) \subseteq \overline{\mathbb{Q}}$ ,  $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$ . Pertanto il grado di  $\overline{\mathbb{Q}}$  su  $\mathbb{Q}$  non è finito, benché  $\overline{\mathbb{Q}}$  sia un'estensione algebrica per definizione.

**Osservazione.** Se  $L$  è un'estensione semplice, allora  $L$  è algebrica se e solo se  $L$  è un'estensione finita.

Definiamo infine il composto di due estensione  $L, M$  di  $K$  su uno stesso campo  $\Omega$ :

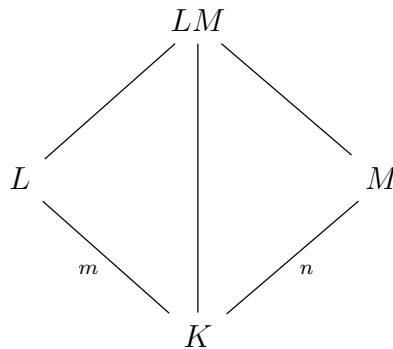
**Definizione** (composto di due estensioni). Siano  $L, M \subseteq \Omega$  estensioni di  $K$  con  $\Omega$  a sua volta campo. Si definisce allora il **composto**  $LM$  di  $L$  e  $M$  come il più piccolo sottocampo di  $\Omega$  che contiene sia  $L$  che  $M$ . Talvolta si scrive anche  $L(M) = LM$ .

**Osservazione.** Se  $L = K(\alpha_1, \dots, \alpha_m)$  e  $M = K(\beta_1, \dots, \beta_n)$ , allora vale che:

$$LM = K(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n).$$

**Proposizione.** Siano  $L$  e  $M$  due campi tali per cui  $K \subseteq L, M$ . Allora, se  $[L : K] = m \in \mathbb{N}^+$  e  $[M : K] = n \in \mathbb{N}^+$ ,  $LM$  è un'estensione finita di  $K$  e  $\text{mcm}(m, n) \mid [LM : K]$ .

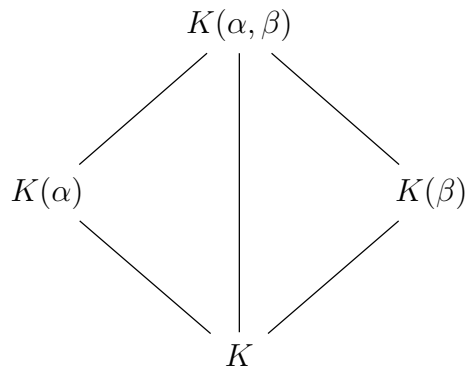
*Dimostrazione.* Si consideri il seguente diamante di estensioni:



Dal momento che  $LM = L(M)$  è un  $L$ -spazio vettoriale e  $M$  è un'estensione finita di  $K$ , il grado di  $LM$  su  $L$  è finito. Pertanto, applicando il teorema delle torri algebriche,  $m \mid [LM : K]$ . Analogamente  $n \mid [LM : K]$ , e quindi  $\text{mcm}(m, n) \mid [LM : K]$ .  $\square$

**Proposizione.** Sia  $L$  un'estensione di campo di  $K$ . Allora  $A = \{\alpha \in L \mid \alpha \text{ algebrico su } K\}$  è un campo, e quindi un'estensione algebrica di  $K$ .

*Dimostrazione.* Siano  $\alpha$  e  $\beta \in A$ . Si consideri il seguente diamante di estensioni:

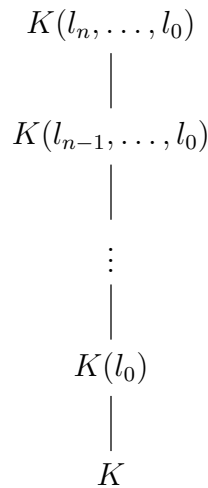


Dal momento che  $K(\alpha, \beta) = K(\alpha)K(\beta)$  e sia  $[K(\alpha) : K]$  che  $[K(\beta) : K]$  sono finiti dacché  $\alpha$  e  $\beta$  sono algebrici,  $K(\alpha, \beta)$  è un'estensione finita di  $K$ , ed è dunque un'estensione algebrica. Pertanto  $\alpha \pm \beta$ ,  $\alpha\beta$ ,  $\alpha^{-1}$  (se  $\alpha \neq 0$ ) e  $\beta^{-1}$  (se  $\beta \neq 0$ ) sono elementi algebrici di  $K$ , e quindi  $A$  è un campo, e a maggior ragione un'estensione algebrica di  $K$ .  $\square$

**Proposizione.** Se  $K \subseteq L \subseteq F$  è una torre di estensioni e  $L/K$  è algebrica così come  $F/L$ , allora anche  $F/K$  è algebrica.

*Dimostrazione.* Sia  $f \in F$ . Allora, poiché  $F$  è algebrico su  $L$ , esistono  $l_0, \dots, l_n \in L$  tali per cui, detto  $p(x) = l_n x^n + \dots + l_1 x + l_0 \in L[x]$ , vale che  $p(f) = 0$ . In particolare  $f$  è algebrico su  $K(l_n, \dots, l_0)$ , e quindi  $K(l_n, \dots, l_0, f)$  è un'estensione finita su  $K(l_n, \dots, l_0)$ .

Chiaramente  $K(l_n, \dots, l_0)$  è un'estensione finita su  $K$  dal momento che questi due campi sono i due estremi della seguente torre di estensioni:



Infatti ogni campo della torre è un'estensione finita del sottocampo corrispondente dal momento che  $L/K$  è un'estensione algebrica<sup>2</sup>.

---

<sup>2</sup>In particolare questo dimostra che un'estensione algebrica e finitamente generata è anche finita. Si può generalizzare il risultato mostrando che un'estensione è finita se e solo se finitamente generata da elementi algebrici.

Per il teorema delle torri algebriche, allora  $K(l_n, \dots, l_0, f)$  è un'estensione finita di  $K$ . Dal momento allora che  $K(f) \subseteq K(l_n, \dots, l_0, f)$ , anche questa è un'estensione finita, e quindi  $f$  è algebrico, da cui la tesi.  $\square$