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[1], 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** $\varphi_{\alpha,K} : K[x] \to K[\alpha]$ di α su K, spesso abbreviato come φ_α se è sottinteso che si sta lavorando su K, come l'omomorfismo univocamente determinato dalla relazione:

$$p \overset{\varphi_\alpha}{\longmapsto} p(\alpha).$$

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 α.

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

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

[1] 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 $L = K(\alpha)$. Tale α si definisce **elemento primitivo** di L su K.

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

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

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

Osservazione. Se $\alpha \in K$ è algebrico, allora $\operatorname{Ker} \varphi_\alpha$ è generato da un irriducibile dacché $K[x]$ è un PID. In particolare $K[x]/\operatorname{Ker} \varphi_\alpha$ 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 $\operatorname{Ker} \varphi_\alpha$. Per semplicità si definisce $\deg_K \alpha$ come il grado di μ_α.

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

Osservazione. Se $\alpha \in K$ è trascendente, allora $\operatorname{Ker} \varphi_\alpha$ 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 α è algebrico su K se e solo se $[K(\alpha) : K]$ è finito.

Dimostrazione. Se α 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 $1, \alpha, \ldots, \alpha^n$. Dal momento che questi sono $n+1$ elementi in $K(\alpha)$, devono essere necessariamente linearmente dipendenti. Pertanto esistono a_0, $a_1, \ldots, a_n$ tali per cui $a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0$. Pertanto esiste un polinomio con coefficienti in K che annulla α, e dunque α è algebrico. □

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 α è algebrico, e così L. □

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 α 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 Ω:

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

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

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

Teorema (delle torri algebriche)**.** Siano $K \subseteq L \subseteq F$ campi. Allora F/K è un'estensione finita se e solo se L/K e F/L sono estensioni finite.

In particolare[2], se F/K è un'estensione finita, vale che:

$$[F : K] = [F : L][L : K].$$

Dimostrazione. Se F/K è un'estensione finita, allora a maggior ragione L/K è un'estensione finita dal momento che L è un K-sottospazio vettoriale di F, che è un K-spazio vettoriale. Inoltre, anche F/L è un'estensione finita, dacché una base di F/K è un insieme di generatori su F/L, dal momento che $K \subseteq L$.

Si mostra adesso che se L/K e F/L sono estensioni finite, allora F è uno spazio finito-dimensionale su K e vale che:

$$[F : K] = [F : L][L : K].$$

[2]Si può generalizzare questa formula ad F spazio vettoriale su K e L con $K \subseteq L$, a patto che K e L siano campi.

Siano $[F : L] = m$ e $[L : K] = n$. Sia $\mathcal{B}_F = (f_1, \ldots, f_m)$ una base di F su L, e sia $\mathcal{B}_L = (l_1, \ldots, l_n)$ una base di L su K.

Si dimostra che la seguente è una base di F su K:

$$\mathcal{B}_F\mathcal{B}_L = \{f_1 l_1, \ldots, f_1 l_n, \ldots, f_m l_n\},$$

dove si osserva che $|\mathcal{B}_F\mathcal{B}_L| = [F : L][L : K]$. Si mostra innanzitutto che $\mathcal{B}_F\mathcal{B}_L$ è un insieme di generatori. Sia $f \in F$. Allora si può scrivere f come combinazione lineare finita con scalari in L:

$$f = \sum_{i=1}^{m} \beta_i f_i.$$

A sua volta, allora, si può scrivere ogni $\beta_i \in L$ come combinazione lineare finita con scalari in K:

$$\beta_i = \sum_{j=1}^{n} \gamma_j^{(i)} l_j.$$

Combinando queste due identità, si verifica che $\mathcal{B}_F\mathcal{B}_L$ genera F come K-spazio vettoriale:

$$f = \sum_{i=1}^{m} \sum_{j=1}^{n} \gamma_j^{(i)}\, l_j f_i.$$

Infine, si verifica che $\mathcal{B}_F\mathcal{B}_L$ è un insieme linearmente indipendente. Si consideri l'equazione:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \gamma_j^{(i)}\, l_j f_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \gamma_j^{(i)} l_j \right) f_i = 0.$$

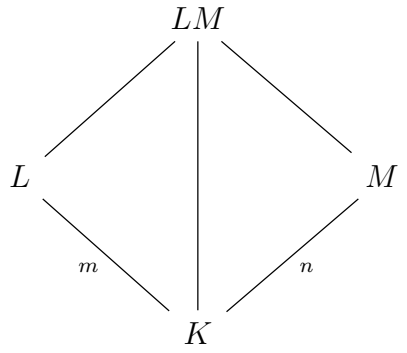
Poiché $\mathcal{B}_F$ è linearmente indipendente, si deduce che:

$$\sum_{j=1}^{n} \gamma_j^{(i)} l_j = 0.$$

Tuttavia, $\mathcal{B}_L$ è a sua volta linearmente indipendente, e quindi $\gamma_j^{(i)} = 0$, $\forall\, i, j$. Dunque $\mathcal{B}_F\mathcal{B}_L$ è linearmente indipendente, e quindi è una base dacché è anche un insieme di generatori per F come K-spazio vettoriale. Pertanto F è un'estensione finita di K e vale la tesi. □

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 $\mathrm{mcm}(m, n) \mid [LM : K]$.

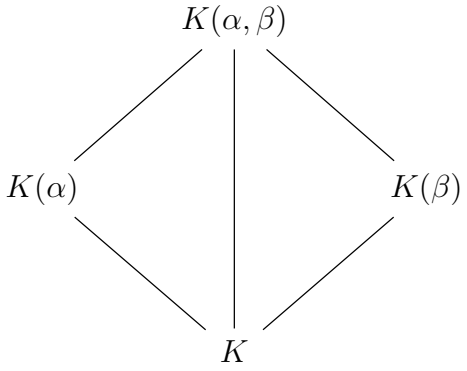
Dimostrazione. Si consideri il seguente diamante di estensioni:



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 $\text{mcm}(m, n) \mid [LM : K]$. □

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 α e $\beta \in A$. Si consideri il seguente diamante di estensioni:



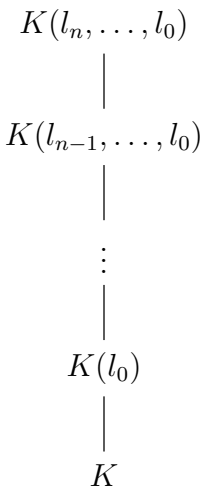
Dal momento che $K(\alpha, \beta) = K(\alpha)K(\beta)$ e sia $[K(\alpha) : K]$ che $[K(\beta) : K]$ sono finiti dacché α e β sono algebrici, $K(\alpha, \beta)$ è un'estensione finita di K, ed è dunque un'estensione algebrica. Pertanto $\alpha \pm \beta$, $\alpha\beta$, α^{-1} (se $\alpha \neq 0$) e β^{-1}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

Le estensioni finite sono completamente caratterizzate in qualità di estensioni finitamente generate da elementi algebrici sul campo di riferimento, come mostra la:

Proposizione. L/K è un'estensione finita se e solo se è un'estensione finitamente generata da elementi algebrici.

Dimostrazione. Se L è un'estensione finita su K, allora esiste una base finita $\mathcal{B} = \{l_1, \ldots, l_n\} \subseteq L$ tale per cui $L = K(l_1, \ldots, l_n)$. Poiché L è un'estensione finita, L è anche algebrica, e quindi $\mathcal{B}$ è composta da elementi algebrici su K. Pertanto L è un'estensione finitamente generata da elementi algebrici su K.

Sia ora $L = K(l_1, \ldots, l_n)$ con l_i elemento algebrico su K. Allora, per il teorema delle torri algebriche, L è un'estensione finita su K dal momento che questi due campi sono i due estremi della seguente torre di estensioni:



dove ogni campo interno della torre è un'estensione finita del sottocampo corrispondente dal momento che L/K è un'estensione algebrica, da cui la tesi. □

Proposizione. Sia $K \subseteq L \subseteq F$ una torre di estensioni. Allora F/K è un'estensione algebrica se e solo se lo sono sia L/K che F/L.

Dimostrazione. Se F/K è un'estensione algebrica, a maggior ragione F/L è algebrica, dal momento che ogni elemento $f \in K$ è radice di un polinomio a coefficienti in K, e quindi, in particolare, di un polinomio a coefficienti in L. Allora stesso tempo, ogni elemento di L è un elemento di F, e quindi tale elemento è ancora algebrico su K, e così anche L/K è un'estensione algebrica.

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

Chiaramente anche $K(l_n, \ldots, l_0)$ è un'estensione finita su K dal momento che è finitamente generata da elementi algebrici su K, dacché L è un'estensione algebrica su K.

Per il teorema delle torri algebriche, allora $K(l_n, \ldots, l_0, f)$ è un'estensione finita su K. Dal momento allora che $K(f) \subseteq K(l_n, \ldots, l_0, f)$, anche questa è un'estensione finita, e quindi f è algebrico. Pertanto si conclude che F/K è un'estensione algebrica, da cui la tesi. □

Infine, si presenta un risultato interessante che lega l'algebricità di L/K e M/K a quella di LM/K:

Proposizione. Siano $K \subseteq L$, M. Allora le estensioni ${}^{L}\!/_{K}$ e ${}^{M}\!/_{K}$ sono algebriche se e solo se ${}^{LM}\!/_{K}$ è algebrica.

Dimostrazione. Siano ${}^{L}\!/_{K}$ e ${}^{M}\!/_{K}$ algebriche. Sia $\alpha \in LM = L(M)$. Dal momento che $L(M)$ è un L-spazio vettoriale i cui vettori sono gli elementi di M, allora α può scriversi come combinazione lineare finita di elementi in M con coefficienti in L, ossia:

$$\alpha = \sum_{i=1}^{n} \lambda_i m_i.$$

Poiché L e M sono estensioni algebriche su K, $K' := K(\lambda_1, \ldots, \lambda_n, m_1, \ldots, m_n)$ è un'estensione finitamente generata da elementi algebrici ed è pertanto finita su K. Poiché $K(\alpha) \subseteq K'$, $K(\alpha)$ è un'estensione finita su K e dunque α è algebrico su K. Pertanto LM è un'estensione algebrica su K.

Se ${}^{LM}\!/_{K}$ è un'estensione algebrica, allora in particolare ogni elemento di L, che appartiene a L, è algebrico su K, e così ${}^{L}\!/_{K}$ è un'estensione algebrica. Analogamente lo è anche ${}^{M}\!/_{K}$, da cui la tesi. □