Chiusura algebrica di un campo e campi di spezzamento

di Gabriel Antonio Videtta

Nota. 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.

Questo documento si propone di illustrare le principali proprietà e caratteristiche dei campi algebricamente chiusi, delle chiusure algebriche e dei campi di spezzamento, col proposito di dare i mezzi necessari per approcciarsi alla teoria di Galois. Per questo motivo si presentano le seguenti definizioni:

Definizione (campo algebricamente chiuso)**.** Un campo K si dice **algebricamente chiuso** se ogni polinomio a coefficienti in K ammette una radice in K. Equivalentemente, K è algebricamente chiuso se ogni polinomio $p \in K[x]$ ha tutte le proprie radici in K, e quindi se gli irriducibili di K sono tutti e soli i polinomi di grado unitario.

Definizione (chiusura algebrica)**.** Un estensione ${}^{\Omega}\!/_{K}$ si dice **chiusura algebrica** di K, e si indica usualmente con $\overline{K}$, se Ω è un campo algebricamente chiuso e se Ω è un'estensione algebrica su K.

Osservazione. Per esempio, una chiusura algebrica di $\mathbb{R}$ è $\mathbb{C}$, per il Teorema fondamentale dell'algebra.

Proposizione. Sia Ω un campo algebricamente chiuso. Se allora K è un sottocampo di Ω, vale che K', il campo degli elementi algebrici su K, è una chiusura algebrica di K.

Dimostrazione. Chiaramente K' è un'estensione algebrica su K. Si verifica allora che K' è algebricamente chiuso. Sia $p \in K'[x]$. Dal momento che K è algebricamente chiuso, e che p appartiene anche a $K[x]$, allora p ammette una radice $\alpha \in \Omega$. Si mostra che α è algebrico su K. Poiché allora ${}^{K'(\alpha)}\!/_{K'}$ è un'estensione algebrica (infatti p annulla α per ipotesi) e ${}^{K'}\!/_{K}$ è algebrica per ipotesi, allora $K'(\alpha)$ è algebrica su K, e dunque α è algebrico su K, pertanto $\alpha \in K'$, da cui la tesi. $\square$

Osservazione. Poiché $\mathbb{Q}$ è un sottocampo di $\mathbb{C}$ e $\mathbb{C}$ è un campo algebricamente chiuso, il campo degli elementi algebrici di $\mathbb{Q}$ è una chiusura algebrica di $\mathbb{Q}$ per la proposizione precedente.

Adesso si enuncia, senza dimostrarlo, un teorema su cui si baserà buona parte della prossima teoria:

Teorema (esistenza ed unicità della chiusura algebrica)**.** Esiste ed è unica, a meno di K-isomorfismo[1], la chiusura algebrica di K.

Osservazione. Poiché il campo degli elementi algebrici di $\mathbb{Q}$ è una chiusura algebrica di $\mathbb{Q}$ ed è un insieme numerabile, $\mathbb{C}$ non può essere una chiusura algebrica di $\mathbb{Q}$ dacché $\mathbb{C}$ ha la cardinalità del continuo (e dunque non possono esistere bigezioni tra $\mathbb{C}$ e $\overline{\mathbb{Q}}$). Poiché $\mathbb{C}$ è però algebricamente chiuso, può solamente verificarsi che $\mathbb{C}$ non sia un'estensione algebrica di $\mathbb{Q}$. Più facilmente, $\pi \in \mathbb{R}$ non è algebrico su $\mathbb{Q}$, e così né $\mathbb{R}$ né $\mathbb{C}$ sono estensioni algebriche su $\mathbb{Q}$.

Definizione (campo di spezzamento)**.** Sia $\mathcal{F}$ una famiglia di polinomi di $K[x]$. Si definisce allora **campo di spezzamento** di $\mathcal{F}$ una estensione F di K tale per cui:

- ogni $p \in \mathcal{F}$ si decompone in fattori lineari in $F[x]$,
- se L è un'estensione su K tale per cui $L \subsetneq F$, allora esiste $p \in \mathcal{F}$ non si decompone in fattori lineari in $L[x]$.

Equivalentemente F è un'estensione minimale in cui ogni polinomio di $\mathcal{F}$ si decompone in fattori lineari.

Come per le chiusure algebriche, si enuncia il seguente teorema senza dimostrazione[2]:

Teorema (esistenza ed unicità del campo di spezzamento)**.** Esiste ed è unico, a meno di K-isomorfismo, il campo di spezzamento di $\mathcal{F}$ su K.

Definizione (coniugati di α)**.** Se $\alpha \in {}^{L}\!/\!_{K}$ è algebrico su K, si definiscono **coniugati** di α su K le radici di μ_α su K.

I coniugati di α sono speciali in quanto permettono di studiare le K-immersioni[3] di $K(\alpha)$ in $\overline{K}$, ossia di studiare i campi K-isomorfi a $K(\alpha)$ presenti in $\overline{K}$, come dimostra il:

Teorema (K-immersioni da $K(\alpha)$ in $\overline{K}$)**.** Sia $\alpha \in {}^{L}\!/\!_{K}$ algebrico su K. Allora, se d è il numero di coniugati distinti di α, esistono esattamente d K-immersioni di $K(\alpha)$ in $\overline{K}$ e sono tali da mandare α in un suo altro coniugato.

[1] Un K-isomorfismo è un isomorfismo tra estensioni di K che fissa K, ossia che ristretto a K è l'identità di K.

[2] L'esistenza di un campo di spezzamento è piuttosto facile da dimostrare, è sufficiente considerare l'estensione di K a cui si aggiungono tutte le radici del polinomio.

[3] Una K-immersione è un monomorfismo tra estensioni di K che fissa K.

Dimostrazione. Per considerare le K-immersioni di $K(\alpha)$ in K, si considera prima l'isomorfismo:

$$K(\alpha) \cong K[x]/(\mu_\alpha).$$

Per il Primo teorema di isomorfismo, esistono allora tanti omomorfismi da $K(\alpha)$ in $\overline{K}$ quanti sono gli omomorfismi da $K[x]$ in $\overline{K}$ che annullano (μ_α). Un omomorfismo φ da $K[x]$ a $\overline{K}$ che fissa K è completamente determinato da $\beta = \varphi(x)$ ed in particolare mappa $p \in K[x]$ a $p(\beta)$. Affinché allora (μ_α) appartenga a $\operatorname{Ker}\varphi$, $\mu_\alpha(\beta) = 0$, e quindi β deve essere un coniugato di α. Pertanto gli omomorfismi da $K(\alpha)$ a $\overline{K}$ sono tali per cui α venga mandato in β. Questi omomorfismi sono K-immersioni dal momento che l'unità viene preservata, da cui la tesi. $\square$

Definizione (polinomio separabile)**.** Un polinomio $p \in K[x]$ si dice **separabile** se p ha radici distinte in un suo campo di spezzamento.

Definizione (estensione separabile)**.** Un'estensione ${}^{L}\!\big/_{K}$ si dice **separabile** se per ogni $\alpha \in L$, $\mu_{\alpha,K}$ è un polinomio separabile.

Definizione (campo perfetto)**.** Un campo si dice **perfetto** se ogni suo polinomio irriducibile è separabile.

Osservazione. Le estensioni di un campo perfetto sono sempre separabili. Infatti il polinomio minimo su K è in particolare un irriducibile, e quindi ha radici distinte.

Nota. Si assumerà d'ora in poi che <u>*K è un campo perfetto*</u>, in modo tale da semplificare l'introduzione alla teoria di Galois.

Osservazione. Poiché K è perfetto, le K-immersioni di $K(\alpha)$ sono esattamente $[K(\alpha) : K] = \deg_K \alpha$.

Osservazione. Se $\varphi_i : K(\alpha) \hookrightarrow \overline{K}$ è un'estensione di $\varphi : K \hookrightarrow \overline{K}$, allora $\varphi_i(K(\alpha)) = K(\varphi_i(\alpha))$.

Poiché i campi considerati sono perfetti, si possono studiare in generale le estensioni di tutte le immersioni di K in $\overline{K}$, e quindi non solo le estensioni dell'identità, come dimostra il:

Teorema (estensioni di φ da $K(\alpha)$ in $\overline{K}$)**.** Sia $\alpha \in {}^{L}\!\big/_{K}$ algebrico su K. Allora per ogni $\varphi : K \hookrightarrow \overline{K}$ esistono esattamente $\deg_K \alpha$ estensioni $\varphi_i : K(\alpha) \hookrightarrow K$ di φ, ossia monomorfismi per cui $\varphi_i|_K = \varphi$. Tali estensioni sono tali da mappare α nelle radici di $\varphi(\mu_\alpha)$.

Dimostrazione. Per considerare le estensioni di φ da $K(\alpha)$ in K, si considera prima l'isomorfismo:

$$K(\alpha) \cong K[x]/(\mu_\alpha).$$

Per il Primo teorema di isomorfismo, esistono allora tanti omomorfismi da $K(\alpha)$ in $\overline{K}$ quanti sono gli omomorfismi da $K[x]$ in $\overline{K}$ che annullano (μ_α). Un omomorfismo φ_i da $K[x]$ a $\overline{K}$ tale per cui K viene mappato tramite φ è completamente determinato da $\beta = \varphi_i(x)$ ed in particolare mappa $p \in K[x]$ alla valutazione del polinomio q, ottenuto mappando i coefficienti di p tramite φ, in β, detto $\varphi(p)(\beta)$. Affinché allora (μ_α) appartenga a $\operatorname{Ker}\varphi$, deve valere $\varphi(\mu_\alpha)(\beta) = 0$, e quindi β deve essere una radice di $\varphi(\mu_\alpha)$. Pertanto gli omomorfismi da $K(\alpha)$ a $\overline{K}$ sono tali per cui α venga mandato nelle radici di $\varphi(\mu_\alpha)$. Questi omomorfismi sono ancora immersioni dal momento che l'unità viene preservata da φ_i. Dal momento che φ è a sua volta un'immersione, $\varphi(\mu_\alpha)$ è irriducibile dacché μ_α lo è, ed inoltre $\deg \varphi(\mu_\alpha) = \deg \mu_\alpha$. Pertanto, poiché K è un campo perfetto, le radici di $\varphi(\mu_\alpha)$ sono $\deg_K \alpha$, e quindi le estensioni di φ sono esattamente $\deg_K \alpha$. $\square$

A partire da questa proposizione, si può dimostrare un risultato più generale sulle estensioni finite di K, come mostra il fondamentale:

Teorema (estensioni di φ da ${}^{L}\!/_{K}$ in $\overline{K}$)**.** Sia $[L : K] = n$. Allora per ogni $\varphi : K \hookrightarrow \overline{K}$ immersione esistono esattamente n estensioni $\varphi_i : L \to \overline{K}$ di φ, ossia tali per cui $\varphi_i|_K = \varphi$.

Dimostrazione. Se $n = 1$, la tesi è del tutto ovvia. Si dimostra facilmente il teorema per $n \geq 2$ applicando il principio di induzione ed il teorema precedente. Se $n = 2$, L è un'estensione semplice di K e quindi esiste $\alpha \in L \setminus K$ tale per cui $L = K(\alpha)$. La tesi allora segue applicando il teorema precedente.

Se $n > 2$, sia $\alpha \in L \setminus K$. Sia $[K(\alpha) : K] = m$. Se $m = n$, allora $L = K(\alpha)$ e la tesi segue ancora applicando il teorema precedente. Se invece $m < n$, sia $[L : K(\alpha)] = d$. Per il teorema precedente esistono esattamente m estensioni φ_i di φ da $K(\alpha)$ in K. Invece, per il teorema delle torri algebriche, $n = md$, e quindi $d < n$. Applicando allora l'ipotesi induttiva, ogni φ_i può essere unicamente esteso in d modi da $K(\alpha)$ a L. Pertanto esistono solamente $n = md$ estensioni di φ, concludendo il passo induttivo. $\square$