Estensioni normali e gruppo di Galois

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. Per scopi didattici, si considerano solamente campi perfetti, e dunque estensioni che sono sempre separabili, purché non esplicitamente detto diversamente.

Si introduce adesso il fondamentale concetto di *estensione normale*, prerequisito per introdurre a sua volta la teoria di Galois.

Definizione (estensione normale)**.** Un'estensione algebrica L/K si dice **normale** se per ogni K-immersione $\varphi : L \to \overline{K}$ vale che $\varphi(L) = L$.

Questa definizione viene immediatamente caratterizzata attraverso i coniugati dei suoi elementi, come mostra la:

Proposizione. Sono equivalenti i seguenti fatti:

(i) L/K è un'estensione normale,

(ii) Per ogni $\alpha \in L/K$, ogni coniugato di α appartiene a L,

(iii) L/K è il campo di spezzamento di una famiglia di polinomi di $K[x]$.

Dimostrazione. Si mostra l'equivalenza delle proprietà:

(i) $\implies$ *(ii)* Sia $\varphi : L \to \overline{K}$ una K-immersione di L. Allora, poiché L è normale su K, $\varphi(L) = L$. Sia $\alpha \in L \setminus K$. Dal momento che $K \subseteq K(\alpha) \subseteq L$, $\varphi|_{K(\alpha)}$ è in particolare una K-immersione di $K(\alpha)$, e quindi deve associare ad α un suo coniugato. Dal momento però che $\varphi(\alpha) \in L$, questo significa che ogni coniugato di α appartiene ad L.

(ii) $\implies$ *(iii)* Sia $\mathcal{F}$ la famiglia dei polinomi minimi degli elementi di L/K. Si dimostra che L è il campo di spezzamento di $\mathcal{F}$ su K. Chiaramente $\mathcal{F} \subseteq L$, dal momento che L contiene una radice per ipotesi di ogni polinomio minimo, e per (ii) contiene tutti i suoi coniugati (e dunque tutte le radici di ogni polinomio della famiglia $\mathcal{F}$). Inoltre vale anche che $L \subseteq \mathcal{F}$, dal momento che ogni elemento di L è radice di un polinomio di $\mathcal{F}$, per costruzione. Pertanto $L = \mathcal{F}$.

$(iii) \implies (i)$ Sia $\varphi : L \to \overline{K}$ una K-immersione di L. Sia $\alpha \in L \setminus K$.Dal momento per che L è campo di spezzamento di una famiglia $\mathcal{F}$ di polinomi, L è generato dalle radici di $\mathcal{F}$. Per ogni α generatore di L, allora, φ deve mappare α ad un suo coniugato, ancora appartenente ad L dacché $\mathcal{F}$ è campo di spezzamento. Pertanto $\varphi(\alpha) \in L$. Allora, dal momento che L è generato dalle radici di $\mathcal{F}$, ogni suo elemento viene ancora mappato ad un elemento di L, e quindi L/K è un'estensione normale.

$\square$

Osservazione. Per esempio, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ non è normale, dal momento che $\sqrt[3]{2}\zeta_3$, un coniugato di $\sqrt[3]{2}$, non appartiene a $\mathbb{Q}(\sqrt[3]{2})$. Al contrario, $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ è normale, dal momento che l'unico coniugato di ζ_3 è ζ_3^2.

Dimostriamo inoltre che le estensioni di grado 2 sono sempre normali, come mostra la:

Proposizione. Sia L/K un'estensione di grado 2. Allora L è normale su K, se $\operatorname{char} K \neq 2$.

Dimostrazione. Chiaramente L è un'estensione algebrica di K, essendo finita. Sia[1] allora $\alpha \in L \setminus K$. Dal momento che $\alpha \notin K$, $[K(\alpha) : K] = 2$, e quindi $L = K(\alpha)$. Inoltre $\deg_K \alpha = 2$, pertanto, poiché $\operatorname{char} K \neq 2$, esiste un polinomio irriducibile $p(x) = x^2 + bx + c$ con b, $c \in K$ di cui α è radice. In particolare, α, $\overline{\alpha} = \frac{-b \pm \sqrt{\Delta}}{2}$, dove $\overline{\alpha}$ il coniugato di α. Allora α, $\overline{\alpha} \in K(\sqrt{\Delta})$. Dal momento allora che $L = K(\alpha) = K(\sqrt{\Delta})$, L è campo di spezzamento di $p \in K[x]$, e dunque, per la proposizione precedente, è normale su K. $\square$

Infine, si esplora la normalità su un diagramma di estensioni.

Proposizione (normalità nel composto e nell'intersezione)**.** Siano L/K e M/K estensioni normali. Allora LM/K e $L \cap M/K$ sono a loro volta normali.

$$
\begin{tikzcd}
 & LM \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
L \arrow[dr, dash] & & M \arrow[dl, dash] \\
 & L \cap M \arrow[d, dash] & \\
 & K &
\end{tikzcd}
$$

[1] L è di grado 2 su K, e quindi K deve essere un suo sottinsieme proprio.

Dimostrazione. Chiaramente LM e $L \cap M$ sono estensioni algebriche di K, in quanto sia L che M lo sono. Sia $\varphi : LM \to \overline{K}$ una K-immersione di LM. Allora $\varphi(LM) = \varphi(L(M)) = L(\varphi(M)) = L(M) = LM$, e quindi LM è normale su K. Analogamente, se $\varphi : L \cap M \to \overline{K}$ è una K-immersione di $L \cap M$, $\varphi(L \cap M) = \varphi(L) \cap \varphi(M) = L \cap M$, e quindi $L \cap M$ è normale su K. □

Proposizione. Sia $K \subseteq F \subseteq L$ una torre di campi. Allora ${}^{L}\!/_{K}$ normale $\implies$ ${}^{L}\!/_{F}$ normale.

Dimostrazione. Poiché L è normale su K, L è un campo di spezzamento di una famiglia $\mathcal{F}$ di polinomi di $K[x]$. A maggior ragione, allora, L è campo di spezzamento di $\mathcal{F}$ come polinomi di $F[x]$, e quindi è normale anche su F. □

Si può adesso introdurre la teoria di Galois introducendo prima l'insieme $\operatorname{Aut}_K L$ e poi il gruppo $\operatorname{Gal}({}^{L}\!/_{K})$.

Definizione. Si definisce l'insieme $\operatorname{Aut}_K L$ come l'insieme delle K-immersioni di L, ossia delle immersioni $\varphi : L \to \overline{K}$ tali per cui $\varphi|_K = \operatorname{Id}_K$.

Se L è normale su K, le immersioni di $\operatorname{Aut}_K L$ possono essere ristrette al codominio su L (infatti $\varphi(L) = L$ per definizione) e sono tali per cui mandano gli elementi di L nei loro coniugati su K. Inoltre, se L è un'estensione finita di K, la separabilità di L garantisce che[2] $|\operatorname{Aut}_K L| = [L : K]$. Pertanto, riducendoci a considerare le estensioni normali e separabili di K, ogni immersione, ristretta opportunamente sul codominio, ammette un inverso, e quindi si può considerare $\operatorname{Aut}_K L$ come gruppo sulla composizione, denotato come $\operatorname{Gal}({}^{L}\!/_{K})$. Tali estensioni sono speciali, e vengono pertanto dette *di Galois*.

Definizione (estensioni di Galois)**.** Si dice che ${}^{L}\!/_{K}$ è un'**estensione di Galois** se L è sia normale che separabile su K.

Definizione (gruppo di Galois di ${}^{L}\!/_{K}$)**.** Si definisce il gruppo di Galois di ${}^{L}\!/_{K}$, denotato come $\operatorname{Gal}({}^{L}\!/_{K})$, il gruppo rispetto alla composizione delle immersioni di $\operatorname{Aut}_K L$ ristrette sul codominio a L.

La maggior parte dei teoremi della teoria di Galois si fondano particolarmente sul fatto che il gruppo di Galois di un campo di spezzamento di un irriducibile f agisce sulle radici di f, come mostra la:

Proposizione. Sia $f(x) \in K[x]$ un irriducibile. Allora, se L è il suo campo di spezzamento, $\operatorname{Gal}({}^{L}\!/_{K})$ agisce fedelmente e transitivamente sulle radici di L. Pertanto $\operatorname{Gal}({}^{L}\!/_{K}) \hookrightarrow S_n$, dove $n = [L : K] = \deg f(x)$, e quindi $n \mid [L : K] \mid n!$.

[2]In generale, se L è un'estensione finita e normale di K, $|\operatorname{Aut}_K L| = [L : K]$ se e solo se L separabile su K.

Dimostrazione. Si consideri l'azione $\Xi : \mathrm{Gal}(L/K) \to S(\{\alpha_1, \ldots, \alpha_n\})$ tale per cui $\varphi \overset{\Xi}{\mapsto} [\alpha_i \mapsto \varphi(\alpha_i)]$, dove[3] le α_i sono le radici distinte di $f(x)$. Allora chiaramente $n \mid [L : K]$, dal momento che $[K(\alpha_1) : K] = n$ e $K(\alpha_1) \subseteq L$.

Inoltre Ξ è un'azione fedele dacché $\operatorname{Ker} \Xi$ è banale. Infatti l'unica K-immersione che fissa ogni radice è necessariamente l'identità. Allora Ξ è un'immersione di $\mathrm{Gal}(L/K)$ in $S(\{\alpha_1, \ldots, \alpha_n\}) \cong S_n$, e quindi $[L : K] = \left|\mathrm{Gal}(L/K)\right| \mid n!$. Infine, esiste sempre una K-immersione di L che mappa un qualsiasi α_i ad un altro α_j, purché $i \neq j$. Pertanto $\mathrm{Gal}(L/K)$ agisce transitivamente sulle radici di $f(x)$. $\square$

[3]Si ricorda l'ipotesi di K campo perfetto; pertanto $f(x)$ è separabile.