Il teorema dell'elemento primitivo e di corrispondenza 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 dimostrano in questo documento i due teoremi più importanti della teoria elementare delle estensioni di campo e di Galois, il *teorema dell'elemento primitivo* ed il *teorema di corrispondenza di Galois*.

Teorema (dell'elemento primitivo)**.** Sia ${}^{L}\!/\!_{K}$ un'estensione separabile e finita. Allora ${}^{L}\!/\!_{K}$ è semplice.

Dimostrazione. Si distinguono i casi in cui K è un campo finito o infinito.

(K finito) Poiché K è finito e L è un'estensione finita su K, a sua volta L è un campo finito. Pertanto L^* è un sottogruppo moltiplicativo finito di un campo, ed è pertant ciclico. Se $\alpha \in L^*$ è allora un generatore di L^*, vale che L è uguale a $K(\alpha)$. Pertanto ${}^{L}\!/\!_{K}$ è un'estensione semplice.

(K infinito) Si fornisce una dimostrazione costruttiva del teorema, che permette di trovare algoritmicamente un elemento primitivo per L. Poiché L è un'estensione finita di K, L è finitamente generato da elementi algebrici su K.

Sia allora $L = K(\alpha_1, \ldots, \alpha_n)$, dove $\{\alpha_i\}$ è una base di ${}^{L}\!/\!_{K}$ come K-spazio. È sufficiente che $K(\alpha_1, \alpha_2)$ sia semplice affinché anche L lo sia. Infatti si dimostrerebbe che $K(\alpha_1, \alpha_2) = K(\gamma)$ per qualche $\gamma \in K(\alpha_1, \alpha_2)$, e quindi $K(\alpha_1, \ldots, \alpha_n) = K(\gamma, \alpha_3, \ldots, \alpha_n)$. Reiterando allora il processo su $K(\gamma, \alpha_3)$ si troverà un elemento primitivo, e così, induttivamente, si dimostra che in particolare L è semplice. Se invece $n = 1$, la tesi è ovvia.

Sia allora, senza perdita di generalità, $L = K(\alpha, \beta)$. Sia $[L : K] = n$. Allora, poiché L è un'estensione separabile su K, esistono esattamente n distinte K-immersioni di L, dette φ_i. Si definisca allora $p(x) \in \overline{K}[x]$ tale per cui:

$$p(x) = \prod_{1 \leq i < j \leq n} (x\varphi_i(\alpha) + \varphi_i(\beta) - x\varphi_j(\alpha) - \varphi_j(\beta)).$$

Si dimostra che $p(x)$ non è nullo. Infatti, se lo fosse, almeno uno dei fattori della produttoria dovrebbe essere nullo. In tal caso si avrebbe $\varphi_i(\alpha) = \varphi_j(\alpha)$ e $\varphi_i(\beta) = \varphi_j(\beta)$, e dunque $\varphi_i \equiv \varphi_j$, benché $i \neq j$, $\lightning$. Allora $\deg p = \binom{n}{2} > 0$. Dal momento che K è infinito, esiste[1] $t \in K$ tale per cui $p(t) \neq 0$.

Detto $\gamma = \alpha t + \beta$, γ ha esattamente n coniugati. Infatti $\varphi_i(\gamma) \neq \varphi_j(\gamma) \; \forall \, i < j$, altrimenti γ annullerebbe $p(x)$. Pertanto $[K(\gamma) : K] = n = [K(\alpha, \beta) : K]$, da cui $K(\alpha, \beta) = K(\gamma)$, ossia la tesi.

□

Si illustrano adesso i prerequisiti per dimostrare il Teorema di corrispondenza di Galois:

Definizione. Sia L/K un'estensione di Galois. Allora, se $H \leq \mathrm{Gal}(L/K)$, si definisce $L^H = \mathrm{Fix}(H)$ come la sottoestensione di L su K degli elementi fissati da ogni $\varphi \in H$, ossia:

$$L^H = \{\alpha \in L \mid \varphi(\alpha) = \alpha \; \forall \, \varphi \in H\}.$$

Lemma. Sia L/K un'estensione di Galois. Allora, se $H \leq \mathrm{Gal}(L/K)$ vale che:

$$L^H = K \iff H = \mathrm{Gal}(L/K).$$

Dimostrazione. Sia $H = \mathrm{Gal}(L/K)$. Allora sicuramente $K \subseteq L^H$. Si mostra che non può valere $K \subsetneq L^H$. Se infatti $K \subsetneq L^H$, varrebbe che $[L^H : K] > 1$, e quindi esisterebbe una K-immersione non banale di L^H, detta $\varphi : L^H \to \overline{K}$. In particolare φ può estendersi a una K-immersione di L, detta $\tilde{\varphi}$. In particolare $\tilde{\varphi} \in \mathrm{Gal}(L/K)$, e quindi $\tilde{\varphi}$ deve fissare L^H per ipotesi. Tuttavia $\tilde{\varphi}$ ristretta a L^H non fissa L^H per ipotesi, $\lightning$. Pertanto $L^H = K$.

Sia adesso $L^H = K$. Per il Teorema dell'elemento primitivo, $\exists \, \alpha \in L^H$ tale per cui $L = K(\alpha)$. Si consideri allora il polinomio p a coefficienti in $\overline{K}$ tale per cui:

$$p(x) = \prod_{\varphi \in H} (x - \varphi(\alpha)).$$

[1] A livello algoritmico è sufficiente valutare $p(x)$ in al più $n + 1$ valori distinti in K per ottenere un x funzionale per la tesi.

Poiché l'identità di $\mathrm{Gal}(L/K)$ appartiene ad H, $(x-\alpha) \mid p(x)$, e quindi $p(\alpha) = 0$. Inoltre p è in realtà un polinomio a coefficienti in L^H. Se infatti $\rho \in H$,

$$\rho(p(x)) = \prod_{\varphi \in H} (x - \rho(\varphi(\alpha))) = p(x),$$

dove l'uguaglianza è dovuta al fatto[2] che le mappe $\{\rho \circ \varphi\}$ sono esattamente le mappe $\{\varphi\}$. Pertanto $\left|\mathrm{Gal}(L/K)\right| = [L : K] = [K(\alpha) : K] \leq \deg p(x) = |H|$ dal momento che α è radice di $p(x)$. Dal momento che vale anche che $\left|\mathrm{Gal}(L/K)\right| \geq |H|$, allora $H = \mathrm{Gal}(L/K)$, da cui la tesi. $\square$

Proposizione. Sia $\sigma \in \mathrm{Gal}\, L/K$. Allora, se $H \leq L/K$, vale che $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$.

Dimostrazione. Si osserva che:

$$\sigma(L^H) = \{\sigma(\alpha) \mid \alpha \in L,\, \varphi(\alpha) = \alpha \;\forall\, \varphi \in H\} = \{\beta \in L \mid \varphi(\sigma^{-1}(\beta)) = \sigma^{-1}(\beta) \;\forall\, \varphi \in H\},$$

dove si è sfruttato in modo cruciale il fatto che $\varphi \in H$ è bigettiva. Si conclude allora che:

$$\varphi(L^H) = \{\beta \in L \mid \sigma(\varphi(\sigma^{-1}(\beta))) = \beta \;\forall\, \varphi \in H\} = L^{\sigma H \sigma^{-1}}.$$

$\square$

Si può adesso dimostrare il Teorema di corrispondenza di Galois:

Teorema (di corrispondenza di Galois)**.** Sia $\mathcal{E}$ l'insieme delle sottoestensioni di L/K estensione di Galois. Sia $\mathcal{G}$ l'insieme dei sottogruppi di $\mathrm{Gal}(L/K)$. Allora $\mathcal{E}$ è in bigezione con $\mathcal{G}$ attraverso la mappa $\alpha : \mathcal{E} \to \mathcal{G}$ tale per cui:

$$F \overset{\alpha}{\mapsto} \mathrm{Gal}(L/F) \leq \mathrm{Gal}(L/K),$$

la cui inversa $\beta : \mathcal{G} \to \mathcal{E}$ è tale per cui:

$$H \overset{\beta}{\mapsto} L^H \subseteq L.$$

Inoltre, una sottoestensione F/K di L/K è normale su K se e solo se il corrispondente sottogruppo di $\mathrm{Gal}(L/K)$ è normale. Infine, se F/K è normale, F è in particolare di Galois[3] e vale che:

$$\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K) \big/ \mathrm{Gal}(L/F).$$

[2]In particolare è stato applicato l'*embedding* di Cayley su H attraverso l'elemento $\rho \in H$, e quest'azione si è rivelata essere transitiva.

[3]Si ricorda che si considera K un campo perfetto.

Dimostrazione. Le mappe α e β sono ovviamente ben definite. Si mostra direttamente che sono l'una l'inversa dell'altra. Sia $H \leq \mathrm{Gal}(L/K)$. Si osserva che:

$$\alpha(\beta(H)) = \alpha(L^H) = \mathrm{Gal}(L/L^H).$$

Sia $L^H = M$. Se si pone $K = \mathrm{Gal}(L/L^H)$, vale chiaramente che $H \leq K$ dal momento che H fissa per definizione tutti gli elementi di L^H. Dacché allora $L^H = M$, per il lemma precedente $H = K$, e quindi $\alpha(\beta(H)) = H$.

Analogamente si osserva che per $K \subseteq F \subseteq K$ vale che:

$$\beta(\alpha(F)) = \beta(\mathrm{Gal}(L/F)) = L^{\mathrm{Gal}(L/F)}.$$

Pertanto, detto $H = \mathrm{Gal}(L/F)$, per il lemma precedente vale che $L^H = F$, e quindi $\beta(\alpha(F)) = F$, dimostrando la prima parte del teorema.

Sia ora F/K una sottoestensione normale di L/K. Allora, se $\varphi \in \mathrm{Gal}(L/F)$ e $\sigma \in \mathrm{Gal}(L/K)$, $\tau = \sigma \circ \varphi \circ \sigma^{-1}$ è ancora un elemento di L/K. Pertanto, τ si può restringere ad una K-immersione di F. Poiché allora F è normale su K, $\tau(F) = F$, e quindi $\tau \in \mathrm{Gal}(L/F)$, e dunque $\mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/K)$.

Sia adesso $\mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/K)$. Sia φ una K-immersione di F su $\overline{K}$. Allora φ può essere estesa ad un elemento $\tilde{\varphi} \in \mathrm{Gal}(L/K)$. In particolare, se $H = \mathrm{Gal}(L/F)$, $\varphi(F) = \tilde{\varphi}(F) = L^{\varphi H \varphi^{-1}} = L^H = F$, dove si è sfruttata la normalità di H in $\mathrm{Gal}(L/K)$. Pertanto F è normale su K, e dunque, in quanto separabile per ipotesi, di Galois.

Si consideri adesso l'omomorfismo $\tau : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ dato dalla restrizione delle immersioni di $\mathrm{Gal}(L/K)$ su F. Chiaramente τ è una mappa surgettiva, dal momento che ogni K-immersione di $\mathrm{Gal}(F/K)$ può estendersi a K-immersione di $\mathrm{Gal}(L/K)$. Inoltre vale che $\operatorname{Ker} \tau$ è esattamente il sottogruppo di $\mathrm{Gal}(L/K)$ che fissa F, ossia $\mathrm{Gal}(L/F)$. Applicando allora il Primo teorema di isomorfismo vale che:

$$\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K) \big/ \mathrm{Gal}(L/F),$$

da cui la tesi. $\square$

Esempio (studio dei sottocampi di $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$)**.** Dal momento che $L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ è il campo di spezzamento dei polinomi $x^2 - 2$ e $x^2 - 3$, tale estensione è normale su $\mathbb{Q}$, e quindi di Galois. Inoltre, dal momento che $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, $[L : \mathbb{Q}] = 2 \cdot 2 = 4$, dal Teorema delle torri algebriche. Pertanto $\mathrm{Gal}(L/\mathbb{Q})$ è un gruppo di ordine 4.

Si definisce φ_{ij} con $i, j \in \{0, 1\}$ come le $\mathbb{Q}$-immersioni di L tali per cui $\sqrt{2} \xmapsto{\varphi_{ij}} (-1)^i \sqrt{2}$ e analogamente $\sqrt{3} \xmapsto{\varphi_{ij}} (-1)^j \sqrt{3}$. Dal momento che le varie φ_{ij} sono distinte, che ogni φ_{ij} ha ordine 2 e che ogni gruppo di ordine 4 è abeliano (o, più semplicemente, le varie φ_{ij} commutano tra loro), vale che $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Ogni sottoestensione di L ha grado su $\mathbb{Q}$ divisore di $[L : \mathbb{Q}]$, e quindi ha grado 1, 2 o 4. Se il grado è 4, la sottoestensione considerata è proprio L, mentre se il grado è 1 la sottoestensione è $\mathbb{Q}$ stesso. Si studiano ora le sottoestensioni di grado 2. Tali sottoestensioni corrispondono ai sottogruppi di $\mathrm{Gal}(L/\mathbb{Q})$ di ordine $4/2 = 2$. Inoltre, a priori, essendo $\mathrm{Gal}(L/\mathbb{Q})$ abeliano, tutte le sottoestensioni sono normali su $\mathbb{Q}$.

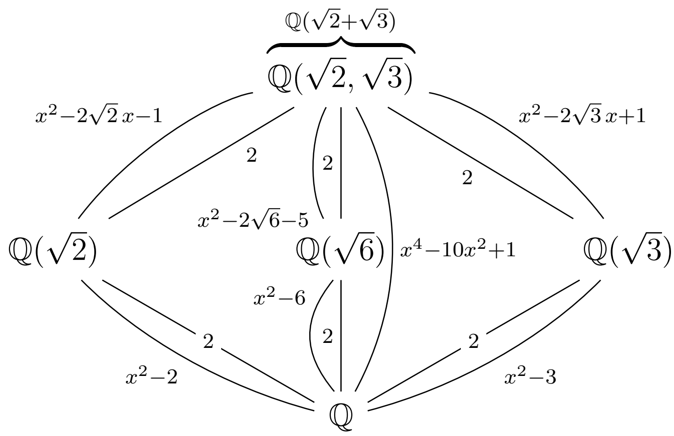
Ogni sottogruppo di ordine 2 è ciclico e generato da elementi di ordine 2, e quindi, mantenendo la corrispondenza con $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, da $(1, 0)$, $(0, 1)$ o $(1, 1)$. Pertanto esistono esattamente 3 sottoestensioni distinte di grado 2 su $\mathbb{Q}$.

In particolare queste sottoestensioni corrispondono ai sottocampi di L fissati da φ_{10}, φ_{01} e φ_{11}, ossia $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{6})$.

Inoltre $\alpha := \sqrt{2}+\sqrt{3}$ è un elemento primitivo di L, dal momento che non può appartenere né a $\mathbb{Q}(\sqrt{3})$ né a $\mathbb{Q}(\sqrt{2})$ (altrimenti tali sottoestensioni coinciderebbero con L, $\lightning$), e così nemmeno a $\mathbb{Q}(\sqrt{6})$ (altrimenti α si scriverebbe come combinazione lineare di 1 e $\sqrt{6}$, $\lightning$). Alternativamente α ha esattamente 4 coniugati tramite le varie[4] φ_{ij}, e quindi ha grado 4 su $\mathbb{Q}$. In particolare vale che:

$$\mu_\alpha(x) = \prod_{i=0}^{1}\prod_{j=0}^{1}(x + (-1)^i\sqrt{2} + (-1)^j\sqrt{3}) = x^4 - 10x^2 + 1.$$

In modo analogo si ottengono i polinomi minimi di $\sqrt{2}+\sqrt{3}$ su $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ e $\mathbb{Q}(\sqrt{6})$, rispettivamente $x^2 - 2\sqrt{2}x - 1 = (x - \sqrt{2})^2 - 3$, $x^2 - 2\sqrt{3}x - 1 = (x - \sqrt{3})^2 - 2$ e $x^2 - (\sqrt{2} + \sqrt{3})^2 = x^2 - 2\sqrt{6} - 5$. Tutte le informazioni sono infine raccolte nel seguente diagramma di estensioni:



[4]Tali 4 coniugati sono distinti dal momento che $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ è una base di L come $\mathbb{Q}$-spazio.

Tramite la corrispondenza di Galois abbiamo fatto corrispondere questo diagramma al seguente diagramma di gruppi:

$$\begin{tikzcd}
 & \{\mathrm{Id}_L \equiv \varphi_{00}\} \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\{\varphi_{00}, \varphi_{01}\} \arrow[dr, no head] & \{\varphi_{00}, \varphi_{11}\} \arrow[d, no head] & \{\varphi_{00}, \varphi_{10}\} \arrow[dl, no head] \\
 & \{\varphi_{01}, \varphi_{10}, \varphi_{01}, \varphi_{11}\} &
\end{tikzcd}$$