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 $i \neq j$, ↯. 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.

□

[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.