Realizzabilità su $\mathbb{Q}$ del gruppo simmetrico
Ilaria Del Corso

Teorema 1 (Teorema di irriducibilità di Hilbert) *Sia $r \geq 1$ e sia $f(T_1, \ldots, T_n, X_1, \ldots, X_r) \in \mathbb{Q}[T_1, \ldots, T_n, X_1, \ldots, X_r]$ un polinomio in $n + r$ indeterminate, irriducibile. Allora esistono infinite n-uple $(a_1, \ldots, a_n) \in \mathbb{Q}^n$ tali che $f(a_1, \ldots, a_n, X_1, \ldots, X_r)$ è un polinomio irriducibile di $\mathbb{Q}[X_1 \ldots, X_r]$.*

Ricordiamo inoltre il seguente teorema dimostrato in classe:

Teorema 2 *Siano k un campo, $T_1, \ldots, T_n$ indeterminate distinte e siano $s_1, \ldots, s_n$ le funzioni simmetriche elementari in $T_1, \ldots, T_n$. Poniamo $L = k(T_1, \ldots, T_n)$ e $F = k(s_1, \ldots, s_n)$. L'estensione L/F è di Galois e il suo gruppo di Galois è isomorfo a S_n.*

Osservazione. Le funzioni simmetriche elementari $s_1, \ldots, s_n$ nelle indeterminate $T_1, \ldots, T_n$ sono algebricamente indipendenti.

Da questi due teoremi possiamo dedurre il seguente

Corollario 3 *Per ogni $n \geq 2$ il gruppo simmetrico S_n si realizza come gruppo di Galois su $\mathbb{Q}$.*

Dim. Applichiamo il Teorema 2 con $k = \mathbb{Q}$; si ha $\mathrm{Gal}(L/F) \cong S_n$. Osserviamo che l'estensione L/F è finita e separabile, quindi, per il teorema dell'elemento primitivo, è semplice, cioè esiste un elemento $\alpha = \alpha(T_1, \ldots, T_n)$ tale che $L = F(\alpha)$; dalla dimostrazione del teorema dell'elemento primitivo si ha anche che $\alpha = \alpha(T_1, \ldots, T_n)$ può essere scelto in $\mathbb{Q}[T_1, \ldots, T_n]$.
Sia f il polinomio minimo di $\alpha(T_1 \ldots, T_n)$ su $F[X]$, allora $f = f(s_1, \ldots, s_n, X) \in \mathbb{Q}[s_1, \ldots, s_n, X]$ e

$$f(s_1, \ldots, s_n, X) = \prod_{\sigma \in S_n} (X - \alpha(T_{\sigma(1)}, \ldots, T_{\sigma(n)}))$$

in $\mathbb{Q}[T_1, \ldots T_n, X]$.
Poiché $s_1, \ldots, s_n$ sono algebricamente indipendenti, il teorema di irriducibilità di Hilbert garantisce che esistono $a_1, \ldots, a_n \in \mathbb{Q}$ tali che il polinomio $\bar{f}(X) = f(a_1, \ldots, a_n, X)$ rimane irriducibile in $\mathbb{Q}[X]$. Sia $\bar{\alpha}$ una sua radice, mostriamo che $\mathbb{Q}(\bar{\alpha})/\mathbb{Q}$ è un'estensione di Galois con gruppo di Galois S_n.
Sicuramente $[\mathbb{Q}(\bar{\alpha}) : \mathbb{Q}] = \deg(\bar{f}) = n!$. Inoltre, dette $\tau_1, \ldots, \tau_n$ le radici in $\bar{\mathbb{Q}}$ del polinomio $p(X) = X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n$, si ha che l'insieme delle radici di $\bar{f}(x) = f(a_1, \ldots, a_n, X)$ è $\{\alpha(\tau_{\sigma(1)} \ldots, \tau_{\sigma(n)})\}_{\sigma \in S_n}$. Ne segue che $\mathbb{Q}(\bar{\alpha}) \subseteq \mathbb{Q}(\tau_1, \ldots, \tau_n)$.
Ora $\mathbb{Q}(\tau_1, \ldots, \tau_n)$ è il campo di spezzamento del polinomio $p(X)$ su $\mathbb{Q}$; poiché $p(x)$ ha grado n, $\mathrm{Gal}(\mathbb{Q}(\tau_1, \ldots, \tau_n)/\mathbb{Q})$ è isomorfo ad un sottogruppo di S_n. Confrontando i gradi delle estensioni otteniamo che $\mathbb{Q}(\bar{\alpha}) = \mathbb{Q}(\tau_1, \ldots, \tau_n)$ e ne deduciamo che il suo gruppo di Galois è isomorfo ad S_n. □

Osservazione. Nel Corollario precedente potevamo scegliere $\alpha(T_1 \ldots, T_n) = T_1 + 2T_2 + \cdots + nT_n$. Infatti l'orbita di $T_1 + 2T_2 + \cdots + nT_n$ sotto l'azione del gruppo di Galois S_n è $\{T_{\sigma(1)} + 2T_{\sigma(2)} + \cdots + nT_{\sigma(n)}\}_{\sigma \in S_n}$. Poichè questi elementi sono tutti distinti, $T_1 + 2T_2 + \cdots + nT_n$ ha $n!$ coniugati su F e quindi è un generatore dell'estensione L/F.