

Esercizio **3.5.6** (Polinomi di Swinnerton-Dyer).

Siano p_1, \dots, p_n i primi n primi (cioè $p_1 = 2, p_2 = 3, \dots$). Sia $F_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$. Anche poniamo

$$\mathcal{E}_n = \{\epsilon = (\epsilon_1, \dots, \epsilon_n) \mid \epsilon_i \in \{0, 1\}\}.$$

Per $\epsilon \in \mathcal{E}_n$ mettiamo

$$\alpha_\epsilon = (\sqrt{p_1})^{\epsilon_1} \cdots (\sqrt{p_n})^{\epsilon_n}.$$

Consideriamo la seguente affermazione

$$\text{Gal}(F_n/\mathbb{Q}) = \{\sigma_\epsilon \mid \epsilon \in \mathcal{E}_n\}, \quad \text{dove } \sigma_\epsilon(\sqrt{p_i}) = (-1)^{\epsilon_i} \sqrt{p_i}, \quad \text{e } \{\alpha_\epsilon \mid \epsilon \in \mathcal{E}_n\} \text{ è una base di } F_n \text{ su } \mathbb{Q}. \quad (1)$$

Vogliamo provare (1) con induzione su n .

1. Provare che F_n è il campo di spezzamento di $(x^2 - p_1) \cdots (x^2 - p_n)$ su \mathbb{Q} .
2. Provare (1) per $n = 1$.
3. Adesso assumiamo che (1) sia vero per un $n \geq 1$. Vogliamo provarlo per $n + 1$.
 - (a) Sia $\alpha \in F_n$ con $\sigma(\alpha) = \pm \alpha$ per ogni $\sigma \in \text{Gal}(F_n/\mathbb{Q})$. Provare che $\alpha = a\alpha_\epsilon$, per certi $a \in \mathbb{Q}$ e $\epsilon \in \mathcal{E}_n$. (Suggerimento: scriviamo α come combinazione lineare dei α_ϵ , e assumiamo che il coefficiente di due, diciamo $\alpha_{\epsilon(1)}$ e $\alpha_{\epsilon(2)}$, sia non zero, e dedurre una contraddizione.)
 - (b) Provare che $\sqrt{p_{n+1}} \notin F_n$.
 - (c) Finire la dimostrazione.

4. Poniamo

$$S_n = \prod_{\epsilon \in \mathcal{E}_n} (x - ((-1)^{\epsilon_1} \sqrt{p_1} + \cdots + (-1)^{\epsilon_n} \sqrt{p_n})).$$

Provare che $S_n \in \mathbb{Q}[x]$.

5. Sia $f \in \mathbb{Q}[x]$ il polinomio minimo di $\sqrt{p_1} + \cdots + \sqrt{p_n}$. Provare che ogni $(-1)^{\epsilon_1} \sqrt{p_1} + \cdots + (-1)^{\epsilon_n} \sqrt{p_n}$ per $\epsilon \in \mathcal{E}_n$ è una radice di f .
6. Provare che $f = S_n$; e che quindi S_n è irriducibile.

S_n è detto polinomio di Swinnerton-Dyer; si può provare che sta in $\mathbb{Z}[x]$. Abbiamo per esempio

$$\begin{aligned} S_5 = & x^{32} - 448x^{30} + 84864x^{28} - 9028096x^{26} + 602397952x^{24} - 26625650688x^{22} + 801918722048x^{20} \\ & - 16665641517056x^{18} + 239210760462336x^{16} - 2349014746136576x^{14} + 15459151516270592x^{12} \\ & - 65892492886671360x^{10} + 172580952324702208x^8 - 255690851718529024x^6 \\ & + 183876928237731840x^4 - 44660812492570624x^2 + 2000989041197056. \end{aligned}$$