Teoria di Galois: Esercizi 1

1. Provare che non esistono $a, b \in \mathbb{Q}$ con $(a + \sqrt{2})^2 = 3$ e che $x^2 - 3$ è irriducibile in $\mathbb{Q}(\sqrt{2})[x]$. Provare che $|\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}| = 4$. Trovare una base di $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ su $\mathbb{Q}$ (suggerimento: la dimostrazione della formula dei gradi dà un metodo per trovare una base in questo caso).

2. Provare che $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$ è un campo di spezzamento di $x^3 - 2 \in \mathbb{Q}[x]$. Quale è il grado di $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$ su $\mathbb{Q}$?

3. Sia F un campo di caratteristica $p > 0$ e $a \in F$ tale che *non* esiste $b \in F$ con $b^p = a$. Si sa che questo implica che il polinomio $f = x^p - a$ è irriducibile in $F[x]$ (vedere Lemma 5.6.30). Sia K una estensione di F che ha una radice $\alpha \in K$ di f.

   (a) Dimostrare che $F(\alpha)$ è un campo di spezzamento di f e che $|F(\alpha) : F| = p$.

   (b) Sia $\beta \in F(\alpha) \setminus F$. Si dimostri che $\beta^p \in F$.

   (c) Provare che il polinomio minimo di β su F è $x^p - \beta^p$.

   (d) Dimostrare che l'estensione $F(\alpha)/F$ è *puramente inseparabile* (cioè, ogni elemento $\beta \in F(\alpha) \setminus F$ è inseparabile).

4. Sia F un campo di caratteristica $p > 0$. Allora F è chiamato *perfetto* se l'insieme $\{a^p \mid a \in F\}$ è uguale a F, o in altre parole, se ogni $a \in F$ ha una radice p-esima in F. Dimostrare che F è perfetto se e solo se ogni estensione algebrica di F è separabile. (Suggerimento: per una direzione usare l'esercizio precedente. Per l'altra: il polinomio minimo di un elemento non separabile di una estensione deve essere un polinomio in x^p, poi i coefficienti sono anche della forma a^p per $a \in F$, visto che F è perfetto, poi...).

5. (Polinomi di Artin-Schreier) Sa F un campo di caratteristica $p > 0$, $a \in F$ e $f = x^p - x + a$ tale che f non ha radici in F. Si sa che questo implica che f è irriducibile in $F[x]$. Sia α una radice di f in una estensione di F.

   (a) Provare che $\alpha + i$ per $0 \leq i \leq p - 1$ sono radici di f.

   (b) Provare che $F(\alpha)$ è un campo di spezzamento di f e che $F(\alpha)/F$ è di Galois.

   (c) Provare che $|F(\alpha) : F| = p$ e che $\mathrm{Gal}(F(\alpha)/F)$ è isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

6. (Polinomi di Swinnerton-Dyer). Siano $p_1, \ldots, p_n$ i primi n primi (cioè $p_1 = 2$, $p_2 = 3, \ldots$). Sia $F_n = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Anche poniamo

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

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

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

Consideriamo la seguente affermazione

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

Vogliamo provare (1) con induzione su n.

(a) Provare che F_n è il campo di spezzamento di $(x^2 - p_1)\cdots(x^2 - p_n)$ su $\mathbb{Q}$.

(b) Provare (1) per $n = 1$.

(c) Adesso assumiamo che (1) sia vero per un $n \geq 1$. Vogliamo provarlo per $n + 1$.

  i. Sia $\alpha \in F_n$ con $\sigma(\alpha) = \pm\alpha$ per ogni $\sigma \in \mathrm{Gal}(F_n/\mathbb{Q})$. 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 nonzero, e dedurre una contraddizione.)

  ii. Provare che $\sqrt{p_{n+1}} \notin F_n$.

  iii. Finire la dimostrazione.

(d) Poniamo

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

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

(e) 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.

(f) 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

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

7. Sia F un campo, $f \in F[x]$ irriducibile e separabile e $E \supset F$ un campo di spezzamento di f. Siano $\alpha_1, \ldots, \alpha_n \in E$ le radici di f. Dimostrare che per $i \neq j$ esiste un $\sigma \in \mathrm{Gal}(E/F)$ con $\sigma(\alpha_i) = \alpha_j$. (Suggerimento: usare la dimostrazione del fatto che due campi di spezzamento sono isomorfi.)

8. Sia F un campo di caratteristica 0, $f \in F[x]$ irriducibile, e $E \supset F$ un campo di spezzamento di f. Siano $\alpha_1, \ldots, \alpha_n \in E$ le radici di f. Dimostrare che per $i \neq j$ la differenza $\alpha_i - \alpha_j$ non sta in F. (Suggerimento: assumiamo che $\alpha_i = \alpha_j + a$ per un certo $a \in F$; con l'esercizio precedente si trova un $\sigma \in \mathrm{Gal}(E/F)$ con $\sigma(\alpha_i) = \alpha_j$ e $\sigma(\alpha_j) = \alpha_k$ (certo k); dedurre che $\alpha_i = \alpha_k + 2a$. Concludere che le differenze fra due radici sono $a, 2a, \ldots$)