# Prova scritta di Algebra 2 - 13/7/2022

**Esercizio 1.** Sia $\alpha = \sqrt{2}$, $\beta = \sqrt{5}$ e $E := \mathbb{Q}(\alpha, \beta)$.

(1) Provare che $\beta \notin \mathbb{Q}(\alpha)$ e calcolare $[E : \mathbb{Q}]$.
(2) Dimostrare che $\gamma = \alpha + \beta$ è un elemento primitivo per l'estensione $E/\mathbb{Q}$.
(3) Dimostrare che $f(X) := X^4 - 14X^2 + 9$ è il polinomio minimo di $\gamma$ su $\mathbb{Q}$.
(4) Dimostrare che $E$ è il campo di spezzamento di $f$ su $\mathbb{Q}$. (Suggerimento: $f(\alpha - \beta) = 0$.)
(5) Determinare il gruppo $\mathrm{Gal}(E/\mathbb{Q})$.

(1) $\mathbb{Q}(\alpha)$ è uno spazio vettoriale su $\mathbb{Q}$ con base $\{1, \alpha\}$. Se fosse $\beta = \sqrt{5} \in \mathbb{Q}(\alpha)$, ci sarebbero $q_0, q_1 \in \mathbb{Q}$ tali che $\sqrt{5} = q_0 + q_1\alpha$. Elevando al quadrato troviamo $5 = q_0^2 + 2q_1^2 + 2q_0q_1\alpha$. Per l'unicità dell'espressione in una base concludiamo $5 = q_0^2 + 2q_1^2$ e $2q_0q_1 = 0$. Se $q_1 = 0$ allora $q_0^2 = 5$, assurdo perché $\sqrt{5} \notin \mathbb{Q}$. Se invece $q_0 = 0$, allora $2q_1^2 = 5$ e anche questo è assurdo (entrambe le cose si dimostrano scrivendo $q_i = m/n$ con $(m, n) = 1$). Questo dimostra che $\beta \notin \mathbb{Q}(\alpha)$. Dunque $[E : \mathbb{Q}(\alpha)] > 1$. Ma $\beta^2 = 5 \in \mathbb{Q}(\alpha)$, quindi $[E : \mathbb{Q}(\alpha)] \leq 2$. L'unica possibilità è $[E : \mathbb{Q}(\alpha)] = 2$. Quindi $[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

(2) Ovviamente $Q(\gamma) \subset E$. Dobbiamo dimostrare l'inclusione opposta. Calcoliamo

$$\gamma^2 = 7 + 2\sqrt{10}$$
$$\sqrt{10} = \frac{\gamma^2 - 7}{2}$$

dunque $\sqrt{10} \in \mathbb{Q}(\gamma)$. Quindi anche $\sqrt{10}\,\gamma \in \mathbb{Q}(\gamma)$ e

$$\sqrt{10}\,\gamma = \sqrt{10}\sqrt{2} + \sqrt{10}\sqrt{5} = 2\sqrt{2} + 5\sqrt{5} = 2\alpha + 5\beta.$$

Ma allora

$$\sqrt{10}\,\gamma - 2\gamma = 3\beta \in \mathbb{Q}(\gamma),$$

quindi $\beta \in \mathbb{Q}(\gamma)$ e quindi anche $\alpha = \gamma - \beta \in \mathbb{Q}(\gamma)$. Quindi $E = \mathbb{Q}(\alpha, \beta) \subset |Q(\gamma)$.

(3)

$$\gamma^2 = 7 + 2\sqrt{10}$$
$$\gamma^4 = 49 + 40 + 28\sqrt{10} = 89 + 28\sqrt{10}$$
$$f(\gamma) = 89 + 28\sqrt{10} - 14 \cdot 7 - 28\sqrt{10} + 9 = 0.$$

Dunque $m_{\gamma,\mathbb{Q}}|f$. Ma $\deg f = 4 = [E : \mathbb{Q}] = \deg m_{\gamma,\mathbb{Q}}$, quindi $f = m_{\gamma,\mathbb{Q}}$.

(4)

$$(\alpha - \beta)^2 = 7 - 2\sqrt{10}$$
$$(\alpha - \beta)^4 = 49 + 40 - 28\sqrt{10} = 89 - 28\sqrt{10}$$
$$f(\alpha - \beta) = 89 - 28\sqrt{10} - 14 \cdot 7 + 28\sqrt{10} + 9 = 0.$$

Siccome $f$ è un polinomio pari, cioè $f(X) = f(-X)$, allora $f(-\gamma) = f(\beta - \alpha) = 0$. Quindi le radici di $f$ sono $\pm\gamma$ e $\pm(\alpha - \beta)$. Siccome $E = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma, \alpha - \beta)$, $E$ è il campo di spezzamento di $f$.

(5) Ogni $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ soddisfa

$$\sigma(\alpha) = \pm\alpha, \qquad \sigma(\beta) = \pm\beta.$$

Quindi ci sono al massimo 4 possibilità. Siccome $E/\mathbb{Q}$ è di Galois, $|\operatorname{Gal}(E/\mathbb{Q})| = 4$, dunque tutte e quattro le possibilità si presentano, ossia $\mathrm{Gal}(E/\mathbb{Q})$ contiene 4 automorfismi che soddisfano le relazioni seguenti:

$$\begin{aligned}
&\sigma_1(\alpha) = \alpha, && \sigma_1(\beta) = \beta \\
&\sigma_2(\alpha) = \alpha, && \sigma_2(\beta) = -\beta \\
&\sigma_3(\alpha) = -\alpha, && \sigma_3(\beta) = \beta \\
&\sigma_4(\alpha) = -\alpha, && \sigma_4(\beta) = -\beta.
\end{aligned}$$

Si vede subito che ognuno di questi automorfismi ha ordine 2: $\sigma_j \circ \sigma_j = \mathrm{id}_E$. Dunque $\mathrm{Gal}(E/\mathbb{Q}) = \mathbb{Z}/2 \times \mathbb{Z}/2$.
Si può anche ragionare in modo diverso. Per esempio si può sfruttare che $E$ è il campo di spezzamento di $f$ e che inoltre $E = \mathbb{Q}(\gamma)$. Dunque tutte le radici di $f$ si possono esprimere in termini di $\gamma$. Infatti

$$\gamma, \quad -\gamma, \quad \alpha - \beta = -\frac{3}{\gamma}, \quad \beta - \alpha = \frac{3}{\gamma}. \tag{0.1}$$

Sia $\tau \in \mathrm{Gal}(E/\mathbb{Q})$. Allora $\tau(\gamma)$ è ancora una radice di $f$ e $\tau$ è determinato da $\tau(\gamma)$. Siccome $|\operatorname{Gal}(E/\mathbb{Q})$ le possibilità sono esattamente

queste:

$$\sigma_1(\gamma) = \gamma$$
$$\sigma_2(\gamma) = \alpha - \beta$$
$$\sigma_3(\gamma) = -\alpha + \beta$$
$$\sigma_4(\gamma) = -\alpha - \beta.$$

Sfruttando le relazioni **??** possiamo calcolare le potenze di questi vari elementi. Per esempio

$$\sigma_3 \circ \sigma_3(\gamma) = \sigma_3(-\alpha + \beta) = \sigma_3(3/\gamma) = 3/\sigma_3(\gamma) = 3/(\beta - \alpha) = 3/(3/\gamma) = \gamma.$$

Dunque $\sigma_3 \circ \sigma_3 = \sigma_1 = \mathrm{id}_E$. Nello stesso modo si vede che tutti gli elementi hanno periodo 1 o 2.

**Esercizio 2.**

(1) Dimostrare che un gruppo di ordine 105 ha un 5-Sylow normale o un 7-Sylow normale.
(2) Classificare i gruppi di ordine 105 che hanno un 5-Sylow normale.

(1) Esaminando i casi si vede che $n_3 \in \{1, 7\}$, $n_5 \in \{1, 21\}$, $n_7 \in \{1, 15\}$. Ogni 7-Sylow contiene 6 elementi di ordine 7. Inoltre se $P$ e $P'$ sono due 7-Sylow distinti, allora $P \cap P' = \{e\}$. Indicando con $G_n$ l'insieme degli elementi di $G$ di ordine $n$, abbiamo

$$|G_7| = 6 \cdot n_7.$$

Per lo stesso motivo

$$|G_5| = 4 \cdot n_5, \qquad |G_3| = 2 \cdot n_3$$

Se fosse $n_5 = 21$ e $n_7 = 15$, avremmo $21 \cdot 4 + 15 \cdot 6 = |G_5| + |G_7| < o(G) = 105$, assurdo. Dunque o $n_5 = 1$ o $n_7 = 1$.

(2) Se $P_5 \lhd G$, allora $n_5 = 1$. Vogliamo dimostrare esiste un altro sottogruppo di Sylow normale. Questo garantirà che $G$ è un prodotto semidiretto. Quindi vogliamo dimostrare che o $n_3 = 1$ o $n_7 = 1$. Se fosse $n_7 \neq 1$ e $n_3 > 1$, allora $n_7 = 15$ e $n_3 = 7$. Dunque $|G_3| = 2 \cdot 7 = 14$, $|G_7| = 15 \cdot 6 = 90$. Inoltre $|G_5| = 4$ e $G_1 = \{e\}$. Quindi $|G_1| + |G_3| + |G_5| + |G_7| = 109 > 105$, assurdo. Quindi o $n_3 = 1$ o $n_7 = 1$. Se $n_3 = 1$, allora $P_3 \lhd G$, dunque $P_3P_5$ è un sottogruppo normale di $G$ e $G = (P_3P_5) \rtimes P_7 \cong \mathbb{Z}/15 \rtimes_\theta \mathbb{Z}/7$, dove $\theta : \mathbb{Z}/7 \to \mathrm{Aut}(\mathbb{Z}/15) \cong \mathbb{Z}/3^* \times \mathbb{Z}/5^* \cong \mathbb{Z}/2 \times \mathbb{Z}/4$. Dunque $\theta$ è il morfismo banale e $G \cong \mathbb{Z}/15 \times \mathbb{Z}/7 = \mathbb{Z}/105$.

Se invece $n_7 = 1$, allora $P_5P_7$ è un sottogruppo normale di $G$ e $G = (P_5P_7) \rtimes P_3 \cong \mathbb{Z}/35 \rtimes_\theta \mathbb{Z}/3$, dove $\theta : \mathbb{Z}/3 \to \mathrm{Aut}(\mathbb{Z}/35) \cong \mathbb{Z}/5^* \times \mathbb{Z}/7^* \cong \mathbb{Z}/4 \times \mathbb{Z}/6$. Possiamo scrivere $\theta = (\theta_1, \theta_2)$ dove $\theta_1 : \mathbb{Z}/3 \to \mathrm{Aut}(\mathbb{Z}/5) \cong \mathbb{Z}/4$ e $\theta_2 : \mathbb{Z}/3 \to \mathrm{Aut}(\mathbb{Z}/7) \cong \mathbb{Z}/6$. Allora $\theta_1$ è il morfismo banale. Quindi $\mathbb{Z}/3$ agisce banalmente su l fattore $\mathbb{Z}/5$ e

$$G = \mathbb{Z}/35 \rtimes_\theta \mathbb{Z}/3 = \mathbb{Z}/5 \times (\mathbb{Z}/7 \rtimes_{\theta_2} \mathbb{Z}/3).$$

Per $\theta_2$ ci sono 3 possibilità: $\theta_{20}([1]_3) = [0]_6$, $\theta_{21}([1]_3) = [2]_6$ o $\theta_{22}([1]_3) = [4]_6$. Nel primo caso $\theta$ è il morfismo banale e e $G \cong \mathbb{Z}/15 \times \mathbb{Z}/7 = \mathbb{Z}/105$ come prima.
Il secondo e il terzo caso danno gruppi isomorfi. Infatti sia $\beta : \mathbb{Z}/3 \to \mathbb{Z}/3$ il morfismo $\beta([m]_3) := [2m]_3$. Allora $\beta \in \mathrm{Aut}(\mathbb{Z}/3)$ e $\theta_{22} = \theta_{21} \circ \beta$. Per l'Esercizio 80 delle *Dispense* concludiamo che $\mathbb{Z}/7 \rtimes_{\theta_{21}} \mathbb{Z}/3 \cong \mathbb{Z}/7 \rtimes_{\theta_{22}} \mathbb{Z}/3)$. Quindi basta considerare il caso $\theta_2 = \theta_{21}$. In questo caso $\theta_{21}$ non è il morfismo banale, quindi otteniamo un gruppo

$$G = \mathbb{Z}/5 \times (\mathbb{Z}/7 \rtimes_{\theta_2} \mathbb{Z}/3)$$

non abeliano.

**Esercizio 3.** Poniamo

$$A := \mathrm{Hom}(\mathbb{Z}/9 \oplus \mathbb{Z}/81, \mathbb{Z}/54 \oplus \mathbb{Z}/6).$$

(1) Scrivere $A$ come somma diretta di gruppi ciclici.
(2) Calcolare i divisori elementari di $A$.

(1)

$$\begin{gathered} A := \mathrm{Hom}(\mathbb{Z}/9 \oplus \mathbb{Z}/81, \mathbb{Z}/54 \oplus \mathbb{Z}/6) = \\ = \mathrm{Hom}(\mathbb{Z}/9, \mathbb{Z}/54) \oplus \mathrm{Hom}(\mathbb{Z}/9, \mathbb{Z}/6) \oplus \\ \oplus \mathrm{Hom}(\mathbb{Z}/81, \mathbb{Z}/54) \oplus \mathrm{Hom}(\mathbb{Z}/81, \mathbb{Z}/6) = \\ = \mathbb{Z}/9 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/27 \oplus \mathbb{Z}/3. \end{gathered}$$

(2) $A = (\mathbb{Z}/3)^2 \oplus \mathbb{Z}/9 \oplus \mathbb{Z}/27$.