(11) **es-campi**

Sia $\mathbb{F}$ il campo di spezzamento su $\mathbb{Q}$ del polinomio $(x^4-2)(x^2+2)$.

(a) Calcolare $[\mathbb{F}:\mathbb{Q}]$ ed esibire una base di $\mathbb{F}$ come spazio vettoriale su $\mathbb{Q}$.

(b) Calcolare il polinomio minimo di $\alpha = \sqrt[4]{2}+i$ su $\mathbb{Q}$.

(c) Mostrare che il solo elemento di $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ che fissa α è l'identità.

Soluzione:

(a) [4pt] Le radici di x^4-2 sono $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$, mentre quelle di x^2+2 sono $\pm\sqrt[2]{2}$. Di conseguenza, il campo di spezzamento di $(x^4-2)(x^2+2)$ il campo $\mathbb{F} = \mathbb{Q}[\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}, \pm\sqrt[2]{2}]$. Si vede subito che $\sqrt[4]{2}$ e $i = i\sqrt[4]{2}/\sqrt[4]{2}$ appartengono a $\mathbb{F}$. da cui $\mathbb{Q}(\sqrt[4]{2}, i) \subset \mathbb{F}$; inoltre anche $\mathbb{F} \subset \mathbb{Q}(\sqrt[4]{2}, i)$ poiché tutte le radici sopra elencate appartengono a $\mathbb{Q}(\sqrt[4]{2}, i)$. In conclusione, $\mathbb{F}$ coincide con $\mathbb{Q}(\sqrt[4]{2}, i)$.

Per calcolarne il grado dell'estensione notiamo che $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$, poiché x^4-2 è irriducibile in $\mathbb{Q}[x]$ per il criterio di Eisenstein, e quindi ha grado 4 su $\mathbb{Q}$. Inoltre, $i \notin \mathbb{Q}(\sqrt[4]{2})$, dal momento che non è reale. Ricordando che i soddisfa il polinomio x^2+1, non può che avere grado 2 su $\mathbb{Q}(\sqrt[4]{2})$, e quindi $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$. In conclusione $[\mathbb{F}:\mathbb{Q}] = 4 \times 2 = 8$. Una base si ottiene moltiplicando gli elementi di una base di $\mathbb{Q}(\sqrt[4]{2})$ su $\mathbb{Q}$ per gli elementi di una base di $\mathbb{F}$ su $\mathbb{Q}(\sqrt[4]{2})$. Si ottiene:

$$\{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}\} \times \{1, i\} = \{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}, i, i\sqrt[4]{2}, i\sqrt{2}, i\sqrt[4]{8}\}.$$

(b) [3pt] È possibile calcolare un polinomio soddisfatto da α come segue: da $\alpha = \sqrt[4]{2}+i$ segue $\alpha - i = \sqrt[4]{2}$ e quindi $(\alpha-i)^4 = 2$. Sviluppando il primo membro si ottiene $\alpha^4 - 6\alpha^2 + 1 - i(4\alpha^3 - 4\alpha) = 2$, da cui $\alpha^4 - 6\alpha^2 - 1 = 4i(\alpha^3 - \alpha)$. Elevando al quadrato entrambi i membri, si ha $(\alpha^4 - 6\alpha^2 - 1)^2 + 16(\alpha^3 - \alpha)^2 = 0$. Pertanto, α annulla il polinomio $(x^4-6x^2-1)^2 + 16(x^3-x)^2 = x^8 + 4x^6 + 2x^4 + 28x^2 + 1$. Mostrare l'irriducibilità di questo polinomio direttamente non è semplice; è invece facile mostrare che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$: lo facciamo in due modi diversi.

- Esprimendo le potenze di α nella base sopra individuata, si ottiene:

$$\alpha^0 = 1, \quad \alpha^1 = \sqrt[4]{2}+i, \quad \alpha^2 = -1 + \sqrt{2} + 2i\sqrt[4]{2},$$
$$\alpha^3 = -3\sqrt[4]{2} + \sqrt[4]{8} - i + 3i\sqrt{2}, \quad \alpha^4 = 3 - 6\sqrt{2} - 4i\sqrt[4]{2} + 4i\sqrt[4]{8}.$$

  Si vede immediatamente che α^4 non può essere combinazione lineare a coefficienti razionali delle potenze precedenti, perchè in nessuna di queste compare $i\sqrt[4]{8}$, che invece compare nell'espressione di α^4. Pertanto α^4 non soddisfa nessun polinomio di grado 4, e quindi neanche polinomi di grado inferiore. Essendo il suo grado un divisore di $[\mathbb{F}:\mathbb{Q}] = 8$, non può essere che 8.
- Un modo alternativo di procedere è quello di mostrare direttamente che $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[4]{2}, i)$. In effetti, sono elementi di $\mathbb{Q}(\alpha)$: $\beta = \alpha^+ 1 = \sqrt{2} + 2i\sqrt[4]{2}$, $\gamma = (\beta^2-2)/4 = -\sqrt{2} + i\sqrt[4]{8}$, $\delta = (\gamma^2-2)/2 = -\sqrt{2} - i\sqrt[4]{2}$. Questo mostra che $\eta = i\sqrt[4]{2} = \beta + \gamma$ appartiene a $\mathbb{Q}(\alpha)$, e quindi anche 1, $2 = -\eta^2$, $i\sqrt[4]{8} = \eta^3$. Insieme ad α formano 5 elementi linearmente indipendenti su $\mathbb{Q}$, e quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ è un divisore di 8 maggiore di 4: non può essere che 8.

(c) [3pt] Svolgiamo anche questo punto in più modi.

- Se $\phi \in \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ fissa α, fissa allora anche tutto $\mathbb{Q}(\alpha) = \mathbb{F}$. Ma per la corrispondenza di Galois l'unico automorfismo che fissa tutto $\mathbb{F}$ è l'identità.
- Se $\phi \in \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ fissa α, notiamo che $\phi(\sqrt[4]{2}+i) = \phi(\sqrt[4]{2}) + \phi(i)$. L'immagine di i attraverso un automorfismo può solo essere uguale ad i o a $-i$, mentre l'immagine di $\sqrt[4]{2}$ può essere soltanto $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. L'unica somma uguale ad α si ottiene quando ϕ manda sia $\sqrt[4]{2}$ che i in se stessi. Ma allora ogni elemento della base sopra descritta viene mandato in se stesso (si o ottengono tutti moltiplicando potenze di $\sqrt[4]{2}$ e di i) e quindi ϕ è l'identità.
- $\mathbb{F} = \mathbb{Q}(\alpha)$, e quindi $\phi(\alpha)$ determina ϕ. Ma allora ϕ è l'identità se e solo se $\phi(\alpha) = \alpha$.