Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2020-2021
AL310 - Istituzioni di Algebra Superiore
25 Novembre 2020 - Esercitazione 4

Esercizio 1. Mostrare che $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$.

Soluzione: Premettiamo un breve inciso teorico, che ha interesse in sé.

Sia $\mathbb{F} \subseteq \mathbb{K}$ un' estensione separabile e finita, con $[\mathbb{K} : \mathbb{F}] = n$. Siano $\varphi_1, \varphi_2, \ldots, \varphi_n$ gli $\mathbb{F}$-isomorfismi distinti di $\mathbb{K}$ in $\overline{\mathbb{F}}$. Definiamo la *traccia* di un elemento $\alpha \in \mathbb{K}$ come $\mathrm{Tr}_{\mathbb{F}}^{\mathbb{K}}(\alpha) = \varphi_1(\alpha) + \varphi_2(\alpha) + \cdots + \varphi_n(\alpha)$. Si verifica facilmente che (vedi sotto)

1. $\mathrm{Tr}_{\mathbb{F}}^{\mathbb{K}}(\alpha) \in \mathbb{F}, \quad \forall \alpha \in \mathbb{K}$
2. $\mathrm{Tr}_{\mathbb{F}}^{\mathbb{K}} \colon \mathbb{K} \to \mathbb{F}$ è una mappa $\mathbb{F}$-lineare.

Per giustificare la terminologia, consideriamo il caso $\mathbb{K} = \mathbb{F}(\alpha)$ con α algebrico e separabile (per il teorema dell'elemento primitivo, possiamo sempre ricondurci a tale situazione).

Consideriamo la mappa $\mathbb{F}$-lineare $\varphi_\alpha : \mathbb{K} \to \mathbb{K}$ definita da $\varphi_\alpha(v) = \alpha v$, $\forall v \in \mathbb{K}$. Se $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1\alpha + a_0$ è il polinomio minimo di α su $\mathbb{F}$, allora la matrice che rappresenta la mappa φ_α con rispetto alla base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ è data da

$$M_\alpha = \begin{pmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ 0 & 0 & 1 & \cdots & -a_3 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{n-1} \end{pmatrix}.$$

Un semplice calcolo mostra che $\det(M_\alpha - \lambda I_n) = (-1)^n m_\alpha(\lambda)$, ovvero il polinomio *caratteristico* di M_α coincide con il polinomio minimo di α. Pertanto

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}}^{\mathbb{K}}(\alpha) &= \text{somma delle radici di } m_\alpha \\ &= \text{somma degli autovalori di } M_\alpha \\ &= \text{ traccia della matrice } M_\alpha. \end{aligned}$$

In particolare,

$$\mathrm{Tr}_{\mathbb{F}}^{\mathbb{K}}(\alpha) = -a_{n-1} \tag{1}$$

(questo mostra in particolare che $\mathrm{Tr}_{\mathbb{F}}^{\mathbb{K}}(\alpha) \in \mathbb{F}$.)

Torniamo ora al nostro problema originale.

Supponiamo per assurdo che $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{2})$. Poiché $\sqrt[3]{3}$ ha grado tre su $\mathbb{Q}$ si ha allora che $\mathbb{K} := \mathbb{Q}(\sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{2})$(ma anche $= \mathbb{Q}((\sqrt[3]{2})^2) = \mathbb{Q}(\sqrt[3]{6})$). Sempre assumendo per assurdo che $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{2})$ abbiamo che esistono $a_0, a_1, a_2 \in \mathbb{Q}$ tali che

$$\sqrt[3]{3} = a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 \tag{2}$$

Prendendo la traccia di ambo i membri, tenendo conto della (1) e del fatto che $\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{K}}(a_0) = 3a_0$, perché i 3 $\mathbb{Q}$-isomorfismi di $\mathbb{K}$ in $\mathbb{C}$ sono l'identità su $\mathbb{Q}$, otteniamo

$$0 = 3a_0 + 0 + 0 \Rightarrow a_0 = 0.$$

Moltiplicando per $\sqrt[3]{2}$ la (2) diventa

$$\sqrt[3]{6} = a_1(\sqrt[3]{2})^2 + a_2 \cdot 2 \tag{3}$$

e prendendo nuovamente la traccia otteniamo

$$0 = 0 + 6a_2 \Rightarrow a_2 = 0.$$

Siamo ricondotti quindi all'uguaglianza $\sqrt[3]{3} = a_1\sqrt[3]{2}$. Elevando al cubo e scrivendo $a_1 = m/n$ (con $\mathrm{MCD}(m, n) = 1$) si deduce $3n^3 = 2m^3$, in contraddizione con teorema fondamentale dell'aritmetica.

Norma e traccia NON fanno parte del programma e quindi non consiglio di svolgere esercizi su questo argomento.

Esercizio 2. Sia $\mathbb{F} \subset \mathbb{K}$ un'estensione algebrica di campi e sia A un anello tale che $\mathbb{F} \subseteq A \subseteq \mathbb{K}$. Mostrare che A è un campo (Gabelli 5.1.).

Soluzione: Per semplicità di notazioni, supporremo che le inclusioni siano valide anche in senso insiemistico. A è un dominio di integrità, essendo contenuto nel campo $\mathbb{K}$. D'altra parte, l'inclusione $\mathbb{F} \subseteq \mathbb{K}$ implica che $1_{\mathbb{K}} = 1_{\mathbb{F}} \in \mathbb{F} \subseteq A$ e quindi A è anche unitario. Consideriamo ora $a \in A$ con $a \neq 0$. Essendo a un elemento di $\mathbb{K}$, esso è algebrico su $\mathbb{F}$ e quindi $\mathbb{F}(a) = \mathbb{F}[a]$. Dentro il campo $\mathbb{F}(a)$ esiste l'inverso moltiplicativo a^{-1} di a, ma allora tale elemento è contenuto in A, poiché esso contiene l'anello $\mathbb{F}[a]$ generato da a e $\mathbb{F}$.

Esercizio 3. Mostrare che le radici del polinomio $p(x) = x^{10} - \sqrt[5]{2}x^5 + \sqrt{5}x^2 + \sqrt[10]{10} \in \mathbb{R}[x]$ sono numeri algebrici (Gabelli 5.3.).

Soluzione: Per risolvere l'esercizio non è necessario trovare esplicitamente un polinomio a coefficienti razionali che si annulla su tutte le radici di $p(x)$. Consideriamo l'estensione $\mathbb{F} = \mathbb{Q}(-\sqrt[5]{2}, \sqrt{5}, \sqrt[10]{10})$, i.e. l'estensione ottenuta aggiungendo a $\mathbb{Q}$ i coefficienti di $p(x)$. Tale estensione è finitamente generata e algebrica, in quanto i coefficienti di $p(x)$ sono algebrici su $\mathbb{Q}$. Ne deduciamo che l'estensione $\mathbb{Q} \subseteq \mathbb{F}$ è finita. Se $\alpha_1, \alpha_2, \ldots, \alpha_{10} \in \mathbb{C}$ sono le radici di $p(x)$, l'estensione $\mathbb{L} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_{10})$ è finitamente generata e algebrica su $\mathbb{F}$ e quindi finita su $\mathbb{F}$. Per il teorema sulla moltiplicatività del grado delle estensioni si ha che l'estensione $\mathbb{Q} \subseteq \mathbb{L}$ è finita. D'altra parte, $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{10}) \subseteq \mathbb{L}$ e pertanto anche l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{10})$ è finita. Ne segue che $\alpha_1, \alpha_2, \ldots, \alpha_{10}$ sono algebrici su $\mathbb{Q}$.

Esercizio 4. Siano $a, b \in \mathbb{R}$. Mostrare che se $a + b$ e ab sono numeri algebrici, allora anche a e b lo sono (Gabelli 5.4.).

Soluzione: Per ipotesi, l'estensione $\mathbb{Q} \subseteq \mathbb{F} := \mathbb{Q}(a + b, ab)$ è algebrica e finitamente generata e quindi finita. Consideriamo il polinomio

$$x^2 - (a + b)x + ab \in \mathbb{F}[x].$$

Si vede subito che a, b sono radici di tali polinomio e quindi l'estensione $\mathbb{F} \subseteq \mathbb{F}(a,b)$ è finita. Per la moltiplicatività del grado delle estensioni si ha anche che $\mathbb{Q} \subseteq \mathbb{F}(a,b)$ è finita. Quindi a e b sono algebrici su $\mathbb{Q}$ (non ho evidenziato, come nella soluzione precedente, il fatto ovvio che $\mathbb{Q}(a,b) \subseteq \mathbb{F}(a,b)$).

Esercizio 5. Mostrare che un campo finito non può essere algebricamente chiuso (Gabelli 5.7.).

Soluzione: La dimostrazione ricorda quella di Euclide sull'infinità dei numeri primi. Sia $\mathbb{F}$ un campo finito ed indichiamo con $\alpha_1, \alpha_2, \ldots, \alpha_n$ i suoi elementi. Consideriamo il polinomio

$$p(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) + 1 \in \mathbb{F}[x].$$

Si vede subito che $p(\alpha_j) = 1$ per $j = 1, 2, \ldots, n$. Pertanto $p(x)$ non ha nessuna radice in $\mathbb{F}$ e questo mostra che $\mathbb{F}$ non è algebricamente chiuso.

Esercizio 6. Sia $\mathbb{K} = \cup_{n\geq 1}\mathbb{F}_{p^n}$. Mostrare che $\mathbb{K}$ è un campo e che costituisce una chiusura algebrica di $\mathbb{F}_p$ (Gabelli 5.9.).

Soluzione: $0, 1 \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n} \forall n$ e quindi costituiscono gli elementi neutri di $\mathbb{K}$. Consideriamo ora $x, y \in \mathbb{K}$ (con $y \neq 0$). Allora esistono $\overline{n}, \overline{m}$ tali che $x \in \mathbb{F}_{p^{\overline{n}}}$ e $y \in \mathbb{F}_{p^{\overline{m}}}$. Detto $r = \mathrm{mcm}(\overline{m}, \overline{n})$ si ha che $x, y \in \mathbb{F}_{p^r}$. Poiché quest'ultimo è un campo, abbiamo che $x - y, xy^{-1} \in \mathbb{F}_{p^r} \subseteq \mathbb{K}$.

Per mostrare che $\mathbb{K}$ è una chiusura algebrica di $\mathbb{F}_p$ è sufficiente mostrare che è algebrico e che ogni polinomio su $\mathbb{F}_p$ si spezza linearmente su $\mathbb{K}$ (Gabelli, Proposizione 5.1.11). È algebrico perche ciascun $\mathbb{F}_{p^n}$ è costituito dalle radici del polinomio $x^{p^n} - x$. D'altra parte, dato un polinomio $f(x) = f_1(x)f_2(x)\cdots f_n(x) \in \mathbb{F}_p[x]$ con f_i irriducibili e di grado d_i si ha che un campo si spezzamento di f è proprio $\mathbb{F}_{p^r} \subseteq \mathbb{K}$ dove $r = \mathrm{mcm}(d_1, d_2, \ldots, d_n)$.

Esercizio 7. Mostrare che il campo $\mathbb{F}(x)$ delle funzioni razionali in una indeterminata x non è algebricamente chiuso (Gabelli 5.10.).

Soluzione: È sufficiente esibire un polinomio di secondo grado a coefficienti in $\mathbb{F}(x)$ irriducibile su $\mathbb{F}(x)$ Osserviamo che $\mathbb{F}(x)$ è il campo dei quozienti dell'UFD $\mathbb{F}[x]$. Consideriamo il polinomio $p(T) = T^2 - x \in (\mathbb{F}[x])[T] \subseteq (\mathbb{F}(x))[T]$. In virtù del lemma di Gauss è sufficiente dimostrare l'irriducibilità di tale polinomio di II grado in $(\mathbb{F}[x])[T]$. Poiché x è irriducibile (e quindi primo in un UFD) in $\mathbb{F}[x]$, l'irriducibilità di $p(T)$ segue dal criterio di Eisenstein.

Esercizio 8. Sia $\mathbb{F} \subseteq \mathbb{K}$ un'estensione algebrica di campi di grado n e sia $\alpha \in \mathbb{K}$. Mostrare che, se esistono n $\mathbb{F}$-isomorfismi $\varphi_1, \varphi_2, \ldots, \varphi_n$ di $\mathbb{K}$ in $\overline{\mathbb{F}}$ tali che

$$\varphi_i(\alpha) \neq \varphi_j(\alpha) \quad \text{se } i \neq j \tag{4}$$

allora $\mathbb{K} = \mathbb{F}(\alpha)$. (Gabelli 5.11.).

Soluzione: Sia t il numero di radici distinte del polinomio minimo m_α di α. Gli $\mathbb{F}$-isomorfismi distinti di $\mathbb{F}(\alpha)$ in $\overline{\mathbb{F}}$ sono quindi t. D'altra parte, per l'ipotesi (4), le restrizioni $\varphi_i|_{\mathbb{F}(\alpha)}$ costituiscono n distinti $\mathbb{F}$-isomorfismi di $\mathbb{F}(\alpha)$ in $\overline{\mathbb{F}}$. Pertanto $n \leq t$. D'altra parte, $t \leq \deg(m_\alpha) \leq n$ e pertanto deve essere $t = \deg(m_\alpha) = n$. Ma allora α ha grado n e quindi $\mathbb{K} = \mathbb{F}(\alpha)$.

Esercizio 9. Determinare i coniugati su $\mathbb{Q}$ di $\theta = \sqrt[4]{3}$, $1+\theta$ e $\theta+\theta^2$. (Gabelli 5.17.).

Soluzione: Il polinomio minimo di θ su $\mathbb{Q}$ è $x^4 - 3$. Le radici sono

$$\alpha = \alpha_1 = \theta, \alpha_2 = i\theta, \alpha_3 = -\theta, \alpha_4 = -i\theta.$$

Di conseguenza i $\mathbb{Q}$-isomorfismi di $\mathbb{Q}(\alpha)$ (in $\mathbb{C}$) sono dati da

$$\Psi_i \colon \mathbb{Q}(\alpha) \to \mathbb{C} \quad \text{definito da } f(\alpha) \mapsto f(\alpha_i), \quad i = 1, 2, 3, 4.$$

I coniugati di $f(\theta)$ sono costituiti dall'insieme $\{f(\Psi_i(\theta)) : i = 1, 2, 3, 4\}$. In tutte e tre i casi dell'esercizio, la cardinalità di tale insieme è pari a 4, in quanto i tre elementi hanno grado 4 su $\mathbb{Q}$. Ad esempio i coniugati di $\theta + \theta^2$ sono: $\{\theta + \theta^2, i\theta - \theta^2, -\theta + \theta^2, -i\theta - \theta^2\}$.

Esercizio 10. Sia ξ una radice primitiva undicesima dell'unità. Determinare i coniugati su $\mathbb{Q}$ di $\alpha = \xi + \xi^{-1}$ (Gabelli 5.18.).

Soluzione: In questo caso calcolare il polinomio minimo di α non è immediatato (esiste una tecnica generale che utilizza i polinomi di Chebyshev). D'altra parte, noi conosciamo le immersioni distinte (in realtà automorfismi) di $\mathbb{Q}(\xi)$ in $\mathbb{C}$: $\Psi_k(\xi) = \xi^k$, con $k = 1, 2, \ldots, 10$ (Gabelli Paragrafo 4.4.3). Si vede subito che $\Psi_k|_{\mathbb{Q}(\alpha)} = \Psi_{k'}|_{\mathbb{Q}(\alpha)}$ sse $k' = 11 - k$. Quindi i coniugati di α sono dati da $\{\Psi_i(\alpha) : i = 1, 2, 3, 4, 5\}$.

Esercizio 11. Siano $\alpha = \sqrt[3]{2}$ e ξ una radice primitiva terza dell'unità e $\mathbb{K} = \mathbb{Q}(\alpha, \xi)$. Mostrare che $\alpha - \alpha\xi$ è un elemento primitivo, mentre $\alpha + \alpha\xi$ non lo è. (Gabelli 5.24.).

Soluzione: Si vede facilmente che $[\mathbb{K} : \mathbb{Q}] = 6$. Quindi per mostrare che $\alpha - \alpha\xi$ è un elemento primitivo è sufficiente mostrare che ha grado 6. Calcoliamo il suo polinomio minimo. Posto $x = \alpha(1 - \xi)$ ed elevando al cubo otteniamo

$$x^3 = 2(1 - 3\xi + 3\xi^2 - \xi^3) = 6(-\xi + \xi^2)$$

ed elevando al quadrato

$$x^6 = 36(\xi^2 + \xi^4 - 2\xi^3) = 36(\xi + \xi^2 - 2) = 36(1 + \xi + \xi^2 - 3) = -108.$$

Essendo il polinomio $x^6 + 108$ irriducibile su $\mathbb{Q}$ (Gabelli, Teorema 4.4.17 : -108 non è un quadrato né un cubo in $\mathbb{Q}$) concludiamo che $\alpha - \alpha\xi$ ha grado 6.

In maniera simile si vede che $m_{\alpha+\alpha\xi}(x) = x^3 + 2$ e pertanto $\alpha + \alpha\xi$ non può essere un elemento primitivo.