Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2020-2021
AL310 - Istituzioni di Algebra Superiore
9 dicembre 2020 - Esercitazione 5

Esercizio 1. Sia $\mathbb{K} = \mathbb{C}(x)$. Siano σ l'automorfismo di $\mathbb{K}$ definito da $f(x) \mapsto f(ix)$ e τ l'automorfismo di $\mathbb{K}$ definito da $f(x) \mapsto f(1/x)$. Determinare i campi fissi di σ e τ (Gabelli, Esercizio 7.2).

Soluzione: È facile mostrare (vedi Gabelli, Esercizio 7.1) che $\mathbb{K}^\sigma = \mathbb{K}^{<\sigma>}$, dove $< \sigma >$ indica il sottogruppo degli automorfismi di $\mathbb{K}$ generato da σ. Dall'applicazione ripetuta di σ a x

$$x \xrightarrow{\sigma} ix \xrightarrow{\sigma} -x \xrightarrow{\sigma} -ix \xrightarrow{\sigma} x$$

deduciamo che σ ha ordine 4.

Mostriamo che $\mathbb{C}(x^4) \subseteq \mathbb{K}^{<\sigma>}$ (e di conseguenza $< \sigma > \leq \mathrm{Gal}_{\mathbb{C}(x^4)}(\mathbb{C}(x))$):

$$\sigma f(x^4) = f((ix)^4) = f(i^4x^4) = f(x^4).$$

D'altra parte $[\mathbb{C}(x) : \mathbb{C}(x^4)] = 4$ poiché il polinomio minimo di x su $\mathbb{C}(x^4)$ è dato da $T^4 - x^4$ (per l'irriducibilità di tale polinomio in $(\mathbb{C}(x^4))[T]$ vedi nota finale). In conclusione

$$4 = |< \sigma >| \leq |\mathrm{Gal}_{\mathbb{C}(x^4)}(\mathbb{C}(x))| \leq [\mathbb{C}(x) : \mathbb{C}(x^4)] = 4$$

e quindi $< \sigma >= \mathrm{Gal}_{\mathbb{C}(x^4)}(\mathbb{C}(x))$ e $\mathbb{K}^\sigma = \mathbb{C}(x^4)$.

In maniera simile si vede che $\mathbb{K}^\tau = \mathbb{C}(x + 1/x)$.

Esercizio 2. Sia $F = \mathbb{F}_2(\tau)$. Mostrare che il polinomio $m(x) = x^4 + \tau^2x^2 + \tau^2$ è irriducibile e non separabile. Determinare un campo di spezzamento $\mathbb{K}$ di $m(x)$ e verificare che $\mathbb{K} = \mathbb{K}_i\mathbb{K}_s$ (Gabelli, Esercizio 7.7).

Soluzione: $m(x)$ è irriducibile perché è τ^2- Eisenstein (vedi nota finale). Inoltre $m'(x) = 0$ e quindi $m(x)$ non è separabile. Se α è una sua radice, allora la sua molteplicità è 2 o 4 (Gabelli, Corollario 5.3.7).

Se dividiamo $m(x)$ per $(x + \alpha)^2 = x^2 + \alpha^2$ otteniamo che

$$m(x) = (x^2 + \alpha^2)(x^2 + \tau^2 + \alpha^2)$$

e quindi le radici di m sono α e $\alpha + \tau$, entrambe di molteplicità 2.

Essendo α una radice di $m(x)$, abbiamo che

$$\alpha^4 + \tau^2\alpha^2 + \tau^2 = 0$$

da cui deduciamo

$$\tau = \frac{\alpha^2}{1 + \alpha} \quad \text{e } \alpha = \frac{\alpha^2 + \tau}{\tau}$$

(attenzione! a lezione ho cancellato la prima relazione, ma serviva per l'altra inclusione : $F(\alpha) \supseteq F(\alpha^2, \tau)$).

Pertanto $\mathbb{K} = F(\alpha) = F(\alpha^2, \tau)$ e abbiamo la seguenti estensioni (frecce = inclusioni):

$$\begin{array}{ccccc} & & F(\alpha^2) & & \\ & \nearrow & & \searrow & \\ F & & & & \mathbb{K} = F(\alpha) = F(\alpha^2, \tau). \\ & \searrow & & \nearrow & \\ & & F(\tau) & & \end{array}$$

α^2 è separabile su F: il suo polinomio minimo è $m_{\alpha^2}(x) = x^2 + \tau^2 x + \tau^2$ e $m'_{\alpha^2}(x) = \tau^2 \neq 0$. D'altra parte il polinomio minimo di τ su F è $m_\tau(x) = x^2+\tau^2$ che non è separabile in quanto $m'_\tau(x) = 0$ (e τ è totalmente inseparabile essendo l'unica radice di $m_\tau(x)$). Quindi $\mathbb{K}_i = F(\tau)$ e $\mathbb{K}_s = F(\alpha^2)$ e $\mathbb{K} = \mathbb{K}_i\mathbb{K}_s$.

Esercizio 3. Siano $p_1, p_2, \dots, p_n$ primi distinti e sia $\mathbb{K} = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$. Determinare $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$ (Gabelli, Esercizio 7.8).

Soluzione: Come preannunciato a lezione, presento per prima cosa la dimostrazione standard che $[\mathbb{K} : \mathbb{Q}] = 2^n$ (che richiede un'astuta applicazione del metodo di dimostrazione per induzione).

In realtà conviene dimostrare un enunciato più generale.

Siano $a_1, a_2, \dots, a_n \in \mathbb{N}$ tali che $\sqrt{a_{i_1} a_{i_2} \cdots a_{i_k}} \notin \mathbb{Q}$ per ciascun sottinsieme non vuoto $\{i_1, i_2, \dots, i_k\}$ di $\{1, 2, \dots, n\}$. Allora per ogni $n \in \mathbb{N}$ vale

$$P(n) : \qquad [\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}) : \mathbb{Q}] = 2^n.$$

La base dell'induzione ($n = 1$) è ovvia.

Per il passo induttivo, utilizzerò il seguente risultato, la cui facile dimostrazione è lasciata per esercizio (cf. Esercitazione 2, es. n. 5).

Lemma. Sia $\mathbb{L}$ un campo di caratteristica diversa da 2 e siano $a, b \in \mathbb{L}$. Se nessuno fra $\sqrt{a}$, $\sqrt{b}$ e $\sqrt{ab}$ appartiene a $\mathbb{L}$ allora $[\mathbb{L}(\sqrt{a}, \sqrt{b}) : \mathbb{L}] = 4$.

Supponiamo ora che $P(k)$ valga per ogni $k < n$ e mostriamo che anche $P(n)$ è vera. Sia $\mathbb{L} = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_{n-2}})$. Per ipotesi induttiva $[\mathbb{L} : \mathbb{Q}] = 2^{n-2}$. Per verificare $P(n)$ è sufficiente mostrare che $[\mathbb{L}(\sqrt{a_n}, \sqrt{a_{n-1}}) : \mathbb{L}] = 4$. Questo segue dal lemma poiché nessuno fra $\sqrt{a_{n-1}}, \sqrt{a_n}, \sqrt{a_n a_{n-1}}$ può appartenere ad $\mathbb{L}$, in quanto altrimenti verrebbe violata l'ipotesi induttiva $P(n-1)$.

Determinamo ora $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$. Per $i = 1, 2, \dots, n$ definiamo gli automorfismi Ψ_i di $\mathbb{K}$ ponendo:

$$\Psi_i(\sqrt{p_j}) = \begin{cases} \sqrt{p_j} & \text{se } i \neq j \\ -\sqrt{p_j} & \text{se } j = i. \end{cases}$$

Notare che $\Psi_i^2 = id$ e $\Psi_i \circ \Psi_j = \Psi_j \circ \Psi_i$. Se $S \subseteq \{1, 2, \dots, n\}$ poniamo

$$\Psi_S(\sqrt{p_j}) = \begin{cases} \sqrt{p_j} & \text{se } j \notin S \\ -\sqrt{p_j} & \text{se } j \in S. \end{cases}$$

Osserviamo che se $S = \{i_1, i_2, \dots, i_k\}$ allora $\Psi_S = \Psi_{i_1} \circ \Psi_{i_2} \circ \cdots \circ \Psi_{i_k}$ e che $\Psi_{S_1} \neq \Psi_{S_2}$ se S_1 e S_2 sono sottoinsiemi distinti di $\{1, 2, \dots, n\}$. Quindi abbiamo 2^n distinti automorfismi di $\mathbb{K}$. Ne deduciamo che

$$2^n \leq |\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})| \leq [\mathbb{K} : \mathbb{Q}] = 2^n$$

e quindi

$$|\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})| = [\mathbb{K} : \mathbb{Q}] = 2^n.$$

Possiamo pertanto concludere che l'estensione $\mathbb{Q} \subseteq \mathbb{K}$ è di Galois e che $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K}) \cong < \Psi_1 > \times < \Psi_2 > \times \cdots \times < \Psi_n > \cong \mathbb{Z}_2^n$ (per dimostrare che $\mathbb{Q} \subseteq \mathbb{K}$ è di Galois si può anche osservare che $\mathbb{K}$ è il campo di spezzamento in $\mathbb{C}$ del polinomio $(x^2 - p_1)(x^2 - p_2) \cdots (x^2 - p_n)$).

Esercizio 4. Sia α una radice del polinomio $f(x) = x^4 - 8x^2 + 36$. Mostrare che il campo di spezzamento di $f(x)$ in $\mathbb{C}$ è $\mathbb{Q}(\alpha)$ e che il gruppo degli automorfismi è un gruppo di Klein (Gabelli, Esercizio 7.10).

Soluzione: $f(x)$ non ha radici razionali ed inoltre si può scrivere come

$$f(x) = (x^2 + 6 + \sqrt{20}x)(x^2 + 6 - \sqrt{20}x)$$

e pertanto è irriducibile su $\mathbb{Q}$. Le radici sono

$$\alpha_1 = \alpha = \sqrt{5} + i \quad \alpha_2 = \sqrt{5} - i \quad \alpha_3 = -\sqrt{5} + i \quad \alpha_4 = -\sqrt{5} - i.$$

Osserviamo che

$$\alpha_2 = \frac{6}{\sqrt{5} + i} \in \mathbb{Q}(\alpha)$$

e di conseguenza anche $\alpha_3 = -\alpha_2$ e $\alpha_4 = -\alpha$ sono in $\mathbb{Q}(\alpha)$ che risulta pertanto il campo di spezzamento in $\mathbb{C}$ di $f(x)$ (e questo contiene anche $\sqrt{5}$ ed i). Poiché $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, il gruppo di Galois può essere $\mathbb{Z}_4$ o un gruppo di Klein. La prima possibilità non si può presentare in quanto $Q(\alpha)$ ha due sottocampi distinti di grado 2 su $\mathbb{Q}$: $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{5})$.

Esercizio 5. Esplicitare la corrispondenza di Galois per n-esimo ampliamento ciclotomico $\mathbb{Q}(\xi)$, per $n = 5, 6, 8$ Gabelli, (parte di Esercizio 7.16).

Soluzione:

Fissato n indicheremo con ξ una radice primitiva n-esima dell'unità e con Ψ_k l'automorfismo di $\mathbb{Q}(\xi)$ definito da $\Psi_k(\xi) = \xi^k$.

• Caso $n = 5$. Abbiamo che $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi)) =< \Psi_3 > \cong \mathbb{Z}_4$ che possiede un unico sottogruppo non banale: $< \Psi_3^2 > = < \Psi_4 >$ di indice e cardinalità 2. Per la corrsipondenza di Galois abbiamo un unico sottocampo di grado 2 su $\mathbb{Q}$, il campo fisso di Ψ_4, ovvero $\mathbb{Q}(\xi + \xi^4) = \mathbb{Q}(\xi + \xi^{-1}) = \mathbb{Q}(\cos(2\pi/5))$.

• Caso $n = 6$. Abbiamo che $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi)) =< \Psi_5 > \cong \mathbb{Z}_2$. Pertanto non possiede sottogruppi non banali.

• Caso $n = 8$. Abbiamo che $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi)) =< \Psi_3 > \times < \Psi_5 > \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ che possiede tre sottogruppi non banali (tutti di indice 2): $< \Psi_3 >$, $< \Psi_5 >$, $< \Psi_7 = \Psi_3\Psi_5 >$. I corrispondenti campi fissi sono: $\mathbb{Q}(\xi + \xi^3)$, $\mathbb{Q}(\xi^2)$, $\mathbb{Q}(\xi + \xi^7)$. (Errata :$\mathbb{Q}(\xi + \xi^5)$ Corrige : $\mathbb{Q}(\xi^2)$).

In questi casi è facile trovare un'espressione tramite radicali dell'elemento primitivo dei sottocampi: ad esempio, poiché $\xi = \exp(2\pi/8) = 1/\sqrt{2} + i/\sqrt{2}$ abbiamo che $\xi + \xi^3 = i\sqrt{2}$. Tuttavia, per trovare una risolvente si può facilmente lavorare con gli ξ (vedi esercizio successivo).

Esercizio 6. Sia ξ una radice primitiva settima dell'unità. Determininare il polinomio minimo di $\alpha = \xi^3 + \xi^5 + \xi^6$ su $\mathbb{Q}$ (Gabelli, parte di Esercizio 7.18).

Soluzione: Il gruppo degli automorfismi di $\mathbb{Q}(\xi)$ è ciclico di ordine 6 e generato da Ψ_3, l'automorfismo definito da $\xi \mapsto \xi^3$. Abbiamo che $\Psi_3(\alpha) = \xi^2 + \xi + \xi^4$ e $\Psi_3^2(\alpha) = \alpha$. Pertanto il polinomio minimo di α è dato da

$$m_\alpha(x) = x^2 - (\alpha + \Psi_3(\alpha))x + \alpha\Psi_3(\alpha) = x^2 + x + 2.$$

.

Nota. Sia $\mathbb{F}$ un campo e x un'indeterminata ed indichiamo con $\mathbb{F}(x)$ il campo delle funzioni razionali nell'indeterminata x. Abbiamo osservato (Esercitazione 2, es. n. 15) che x^n è trascendente su $\mathbb{F}$ e quindi $\mathbb{F}(x^n) \cong \mathbb{F}(s)$ per un'altra indeterminata s. x è algebrico su $\mathbb{F}(x^n)$, in quanto x è uno zero del polinomio $T^n - x^n \in \mathbb{F}(x^n)[T]$. Mostriamo che tale polinomio è irriducibile in $\mathbb{F}(x^n)[T]$. Abbiamo

$$\mathbb{F}(x^n)[T] \cong \mathbb{F}(s)[T] \tag{1}$$

e $\mathbb{F}(s)$ è il campo dei quozienti di $\mathbb{F}[s]$. Per il lemma di Gauss, un polinomio monico irriducibile in $(\mathbb{F}[s])[T]$ lo è anche in $(\mathbb{F}(s))[T]$. Il polinomio $T^n - s$ (che corrisponde a $T^n - x^n$ tramite l'isomorfismo (1)) è irriducibile in $(\mathbb{F}[s])[T]$ in quanto s è irriducibile e anche primo nell'UFD $\mathbb{F}[s]$ e quindi si può applicare il criterio di Eisenstein.