Esercizi di Algebra 2 - 4/6/2022

Esercizio 1. Consideriamo una estensione K/F finita e sia α un elemento di un campo che contiene K. Supponiamo che α sia algebrico su F. Allora

$$[K(\alpha) : K] \leq [F(\alpha) : F], \tag{0.1}$$

$$\operatorname{mcm}\big([K : F], [F(\alpha) : F]\big) \Big| [K(\alpha) : F] \leq [K : F] \cdot [F(\alpha) : F]. \tag{0.2}$$

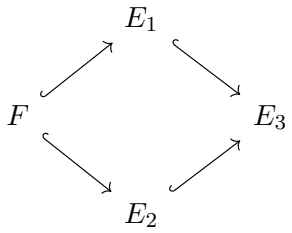
Più in generale, se abbiamo due estensioni finite E_1/F ed E_2/F, supponiamo $E_1 = F(\alpha_1, \ldots, \alpha_s)$ e $E_2 = F(\beta_1, \ldots, \beta_t)$ e poniamo

$$E_3 := F(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t) = E_1(\beta_1, \ldots, \beta_t) = E_2(\alpha_1, \ldots, \alpha_s).$$

Allora posto $n_i := [E_i : F]$, si ha

$$\operatorname{mcm}(n_1, n_2) | [E_3 : F] \leq n_1 n_2. \tag{0.3}$$

Dimostrarlo almeno in caratteristica 0. La situazione è riassunta dal seguente diagramma:



Svolgimento. Per dimostrare (0.1) basta osservare che $m_{\alpha,K} | m_{\alpha,F}$. Per dimostrare (0.2) consideriamo le due catene di campi:

$$\begin{aligned} F \subset K \subset K(\alpha) &\implies [K : F] | [K(\alpha) : F] \\ F \subset F(\alpha) \subset K(\alpha) &\implies [F(\alpha) : F] | [K(\alpha) : F]. \end{aligned}$$

Segue che il minimo comune multiplo di $[K : F]$ e $[F(\alpha) : F]$ divide $[K(\alpha) : F]$. D'altro canto

$$F \subset K \subset K(\alpha) \implies [K(\alpha) : F] = [K(\alpha) : K] \cdot [K : F],$$

e applicando (0.1) concludiamo.

Per dimostrare la (0.3) in caratteristica 0 basta ricordare che ogni estensione finita è semplice, dunque $E_2 = F(\gamma)$, $E_3 = E_1(\gamma)$ e quindi il caso generale segue da quello particolare.

In realtà il caso generale può essere ridotto a quello particolare anche ragionando per induzione su t, senza bisogno di ipotesi sulla caratteristica. Per prima cosa dimostriamo per induzione su s che dati $F \subset K$ ed $\alpha_i \in L$ dove L/K è algebrica, allora

$$[K(\alpha_1, \ldots, \alpha_s) : F(\alpha_1, \ldots, \alpha_s)] \leq [K : F].$$

Questa discende semplicemente da una applicazione iterata della (0.1):

$$\begin{aligned}&[K(\alpha_1,\dots,\alpha_s):F(\alpha_1,\dots,\alpha_s)]=\\&=[K(\alpha_1,\dots,\alpha_{s-1})(\alpha_s):F(\alpha_1,\dots,\alpha_{s-1})(\alpha_s)]\leq\\&\leq[K(\alpha_1,\dots,\alpha_{s-1})(\alpha_s):F(\alpha_1,\dots,\alpha_{s-1})(\alpha_s)]\leq\\&\leq[K(\alpha_1,\dots,\alpha_{s-1}):F(\alpha_1,\dots,\alpha_{s-1})]\leq\text{ ecc. ecc.}\end{aligned}$$

Ora dimostriamo la (0.3). Chiaramente $n_i|[E_3:F]$ per $i=1,2$, dunque $\mathrm{n}_1,\mathrm{n}_2\,|[E_3:F]$. Infine

$$\begin{aligned}&E_3=E_2(\alpha_1,\dots,\alpha_s)\\&[E_3:E_2]\cdot n_2=[E_2(\alpha_1,\dots,\alpha_s):E_2]\cdot n_2\leq\\&\leq[F(\alpha_1,\dots,\alpha_s):F]\cdot n_2=[E_1:F]\cdot n_2=n_1\cdot n_2.\end{aligned}$$

□

Esercizio 2. Sia $f(X)=X^5-7$, sia $K=\mathbb{Q}(\zeta_5)$ il quinto campo ciclotomico, $\zeta_5:=e^{2\pi i/5}$. Sia L il campo di spezzamento di f su K.

(1) Determinare $[L:K]$.
(2) Determinare esplicitamente il morfismo $\mathrm{Gal}(L/K)\to S_5$ descrivendo ogni elemento di $\mathrm{Gal}(L/K)$ come permutazione.

Svolgimento. (1) Partiamo da $E:=$campo di spezzamento di f su $\mathbb{Q}$. Possiamo determinare facilmente le radici di f: se $u:=\sqrt[5]{7}$ le radici di f sono $\zeta^i u$ per $i=0,\dots,4$ dove $\zeta=\zeta_5$. Dunque $E=\mathbb{Q}(u,\zeta u,\zeta^2u,\zeta^3u,\zeta^4u)=\mathbb{Q}(u,\zeta)=K(u)$. Quindi $K\subset E$. Pertanto il campo di spezzamento su K, cioè L, coincide con quello su $\mathbb{Q}$, cioè E. Infatti $L=K(u,\zeta u,\zeta^2u,\zeta^3u,\zeta^4u)=K(u)=E$ perché $\zeta\in K$. Dunque L/K è una estensione semplice. Per calcolare $[L:K]$ procediamo nel modo seguente. $[\mathbb{Q}(u):\mathbb{Q}]=\deg m_{u,\mathbb{Q}}$. Per Eisenstein f è irriducibile in $\mathbb{Q}[X]$, dunque $m_{u,\mathbb{Q}}=f$ e $[\mathbb{Q}(u):\mathbb{Q}]=5$. Invece $[\mathbb{Q}(\zeta):\mathbb{Q}]=4$, perché $m_{\zeta_5,\mathbb{Q}}=\Phi_4=1+X+X^2+X^3+X^4$. Quindi

$$20=\mathrm{mcm}(4,5)|[L:\mathbb{Q}]\leq 20=4\cdot 5.$$

Ossia $[L:\mathbb{Q}]=20$. Ora consideriamo la catena $\mathbb{Q}\subset K\subset L$. Siccome $[K:\mathbb{Q}]=4$, $[L:K]=5$.
(2) Per prima cosa numeriamo le radici: $\alpha_i:=\zeta^{i-1}u$. sappiamo che L/K è di Galois visto che è un campo di spezzamento. Dunque $|\,\mathrm{Gal}(L/K)|=[L:K]=5$. Sia $\sigma_i\in\mathrm{Gal}(L/K)$ l'elemento che manda α_1 in α_i. Dunque $\sigma_1=\mathrm{id}_L$. Invece $\sigma_2(u)=\zeta u$. Ricordando che $\zeta\in K$ e che gli automorfismi σ_j sono K-lineari otteniamo subito $\sigma_2(\zeta^i u)=\zeta^{i+1}u$. Dunque σ_2 manda α_i in α_{i+1} per $i<5$ e manda α_5 in α_1. Dunque σ_2 corrisponde alla permutazione $(12345)\in S_5$. Il calcolo è identico per gli altri elementi del gruppo di Galois:

$$\sigma_3(u)=\zeta^2u\Longrightarrow\sigma_3(\zeta^iu)=\zeta^{i+2}u.$$

In realtà si può anche osservare che $\sigma_3(u)=\sigma_2^2(u)$. Dunque $\sigma_3=\sigma_2^2$. Pertanto σ_3 corrisponde a $(12345)^2$. Nello stesso modo $\sigma_4=(12345)^3$ e $\sigma_5=(12345)^4$. □

Esercizio 3. Sia $p(X) = X^4 + 4X^2 - 2$. Determinare il gruppo di Galois di f sui razionali.

Svolgimento. □

Esercizio 4. Sia $f(X) = X^4 - 3$.

(1) f è irriducibile su $\mathbb{Q}(i)$?
(2) Determinare il gruppo di Galois di f su $\mathbb{Q}(i)$.

Svolgimento. (1) Cominciamo studiando E :=campo di spezzamento di f su $\mathbb{Q}$. Le radici di f sono $\pm u. \pm iu$ dove $u := \sqrt[4]{3}$. Dunque $E = \mathbb{Q}(u, iu) = \mathbb{Q}(u, i)$. Consideriamo la catena $\mathbb{Q} \subset \mathbb{Q}(u) \subset E$. Per prima cosa abbiamo $\mathbb{Q}(u) : \mathbb{Q}] = 4$ perché $f = X^4 - 3$ è irriducibile per Eisenstein e si annulla in u, dunque $f = m_{u,\mathbb{Q}}$. Inoltre $\mathbb{Q}(u) \subset \mathbb{R}$ perché $u \in \mathbb{R}$. Dunque $i \notin \mathbb{Q}(u)$. Quindi $[E : \mathbb{Q}(u)] > 1$. Siccome $X^2 + 1$ si annulla in u, $[E : \mathbb{Q}(u)] \leq 2$. Quindi $[E : \mathbb{Q}(u)] = 2$ e $[E : \mathbb{Q}] = 8$. Sia $K := \mathbb{Q}(i)$. Siccome $[K : \mathbb{Q}] = 2$ considerando la catena $\mathbb{Q} \subset K \subset E$ otteniamo $[E : K] = 4$. Inoltre $E = K(u)$, dunque $\deg m_{u,K} = [E : K] = 4$. Ma $f(u) = 0$ e $f \in \mathbb{Q}[X] \subset K[X]$. Dunque $m_{u,K} | f$. Siccome hanno lo stesso grado e sono monici $f = m_{u,K}$. Quindi f è irriducibile anche in $K[X]$.
(2) Siccome $K \subset E$, il campo di spezzamento di f su K coincide con quello su $\mathbb{Q}$, cioè coincide con E. Quindi vogliamo determinare $G := \mathrm{Gal}(E/K)$. Siccome E/K è normale è di Galois. Quindi $o(G) = 4$. Dobbiamo capire se è il gruppo di Klein o $\mathbb{Z}/4$. Siccome l'estensione E/K è semplice, gli elementi di G sono $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ dove

$$\sigma_1(u) = u, \qquad \sigma_2(u) = -u, \qquad \sigma_3(u) = iu, \qquad \sigma_4(u) = -iu.$$

Facendo un po' di conti si vede che $o(\sigma_4) > 2$, infatti

$$\sigma_4^2(u) = \sigma_4(-iu) = -i\sigma_4(u) = -i(-iu) = -u \neq u.$$

(Nel passaggio $\sigma_4(-iu) = -i\sigma_4(u)$ abbiamo usato che σ_4 è K-lineare!) Quindi σ_4 ha ordine 4 e G è ciclico. □

Esercizio 5. (Compito del 25 settembre 2020). Sia $f := X^5 + X^2 + 1$.

(1) Dimostrare che f è irriducibile su $\mathbb{Q}$.
(2) Trovare un campo $K \supset \mathbb{Q}$ tale che il gruppo di Galois di f su K sia isomorfo a $\mathbb{Z}/5$.
(3) Dimostrare che $\mathrm{Gal}(f)$ non è abeliano

Svolgimento. (1) Se riduciamo mod 2, f non ha radici, dunque non è diviso da fattori di grado 1. Se non fosse irriducibile in $\mathbf{F}_2[X]$ avrebbe necessariamente un fattore quadratico irriducibile. L'unico polinomio irriducibile di grado 2 in $\mathbf{F}_[X]$ è $q = X^2 + X + 1$. Se facciamo la divisione di f per q viene un resto non nullo. Dunque f non è divisibile per q ed è pertanto irriducibile.
(2) Cominciamo studiando il campo di spezzamento E di f su $\mathbb{Q}$. $E/\mathbb{Q}$ è di Galois. Siccome f è irriducibile, $\mathrm{Gal}(E/\mathbb{Q})$ è transitivo sulle radici,

dunque $\mathrm{Gal}(E/\mathbb{Q}) \subset S_5$ è un sottogruppo transitivo. Pertanto contiene un 5-ciclo, che genera un sottogruppo $H \subset \mathrm{Gal}(E/\mathbb{Q})$ con $o(H) = 5$. Vogliamo che H sia il gruppo di Galois dell'estensione E/K. Ma allora basta porre $K := E^H$. Automaticamente $\mathrm{Gal}(E/K) \cong H \cong \mathbb{Z}/5$. Si noti che per il punto (2) l'unica proprietà di f che abbiamo sfruttato è che è irriducibile.
(3) Supponiamo per assurdo che $E/\mathbb{Q}$ sia una estensione abeliana, cioè di Galois e con gruppo di Galois abeliano. Per la II parte del Teorema fondamentale, per ogni campo intermedio $\mathbb{Q} \subset F \subset E$, l'estensione $E/\mathbb{Q}$ sarebbe di Galois. Vediamo che questo non è vero sfruttando un fatto generale, che conviene enunciare separatamente.

Lemma 0.1. *Sia f un polinomio irriducibile che ha almeno una radice reale. Se $\mathrm{Gal}(f)$ è abeliano, allora tutte le radici di f sono reali.*

Dimostrazione. Sia E il campo di spezzamento di f e sia α una radice reale di f. Consideriamo il campo intermedio $F := \mathbb{Q}(\alpha)$. Se $\mathrm{Gal}(f) = \mathrm{Gal}(E/\mathbb{Q})$ è abeliano, allora $F/\mathbb{Q}$ è di Galois. Ma α è una radice di f in F, dunque per normalità f si spezza su F, dunque $E = F \subset \mathbb{R}$ e tutte le radici sono reali. □

Per concludere l'esercizio basta verificare che $f = X^5 + X^2 + 1$ ha una radice reale, ma anche una radice non reale. Siccome f ha grado dispari ha di sicuro una radice reale. La derivata f' ha solo due zeri reali, dunque f ha al massimo 3 zeri reali. □

Esercizio 6. Sia $p(X) = X^4 + 4X - 2$. Calcolare il gruppo di Galois di p.

Svolgimento. Il polinomio è biquadratico. Ossia posto $q(Y) = Y^2 + 4Y - 2$, abbiamo $p(X) = q(X^2)$. Le soluzioni di $q(Y) = 0$ sono $\sqrt{6} - 2$ e $-2 - \sqrt{6}$. Quindi le soluzioni di $p(X) = 0$ sono $\pm\alpha$ e $\pm\beta$ dove

$$\alpha := \sqrt{\sqrt{6} - 2}, \qquad \beta := i\sqrt{2 + \sqrt{6}}.$$

A questo punto è importante osservare la seguente relazione fra α e β

$$\alpha\beta = i\sqrt{2}. \tag{0.4}$$

Si arriva a questa relazione, per esempio razionalizzando $1/\beta$. Dunque il campo di spezzamento di p è $E = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, i\sqrt{2})$. Calcoliamo $[E : \mathbb{Q}]$ usando la catena $\mathbb{Q} \subset K := \mathbb{Q}(\alpha) \subset E = K(i\sqrt{2})$. p è irriducibile per Eisenstein. Dunque $p = m_{\alpha,\mathbb{Q}}$ e $[K : \mathbb{Q}] = 4$. Inoltre $i\sqrt{2} \notin K \subset \mathbb{R}$. Dunque $[E : K] = 2$ e $[E : \mathbb{Q}] = 8$. Quindi $|\mathrm{Gal}(E/K)| = 8$. Sia $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$. Allora $\sigma(\alpha)$ è ancora una radice di $m_\alpha = p$. Quindi

$$\sigma(\alpha) \in \{\pm\alpha, \pm\beta\}.$$

Inoltre $m_{i\sqrt{2}} = X^2 + 2$. Questo perché $m_{i\sqrt{2}} | (X^2 + 2)$ e $\deg m_{i\sqrt{2}} \geq 2$, visto che $i\sqrt{2} \notin \mathbb{Q}$. Dunque

$$\sigma(i\sqrt{2}) = \pm i\sqrt{2}.$$

Infinte σ è determinato da $\sigma(\alpha)$ e $\sigma(i\sqrt{2})$. Quindi abbiamo al massimo 8 possibili elementi di $\mathrm{Gal}(E/\mathbb{Q})$. Ma sappiamo già che questo gruppo contiene proprio 8 elementi. Dunque le 8 possibilità si verificano tutte e formano esattamente gli 8 elementi del gruppo. Pertanto, posto $\varepsilon := q\sqrt{2}$, gli 8 elementi di $\mathrm{Gal}(E/\mathbb{Q})$ sono σ_{ij}, $1 \leq i \leq 4$, $1 \leq j \leq 2$, determinati dalle seguenti condizioni:

$$\begin{aligned}
\sigma_{11}(\alpha) &= \alpha \quad & \sigma_{11}(\varepsilon) &= \varepsilon \\
\sigma_{12}(\alpha) &= \alpha \quad & \sigma_{11}(\varepsilon) &= -\varepsilon \\
\sigma_{21}(\alpha) &= -\alpha \quad & \sigma_{11}(\varepsilon) &= \varepsilon \\
\sigma_{22}(\alpha) &= -\alpha \quad & \sigma_{11}(\varepsilon) &= -\varepsilon \\
\sigma_{31}(\alpha) &= \beta \quad & \sigma_{11}(\varepsilon) &= \varepsilon \\
\sigma_{32}(\alpha) &= \beta \quad & \sigma_{11}(\varepsilon) &= -\varepsilon \\
\sigma_{41}(\alpha) &= -\beta \quad & \sigma_{11}(\varepsilon) &= \varepsilon \\
\sigma_{42}(\alpha) &= -\beta \quad & \sigma_{11}(\varepsilon) &= -\varepsilon.
\end{aligned}$$

Sfruttando (0.4), ossia $\beta = \varepsilon/\alpha$, si può facilmente calcolare il prodotto di due elementi di $\mathrm{Gal}(E/\mathbb{Q})$. Dopo un po' di esperimenti si trova che σ_{42} ha ordine 4 e che $\sigma_{12}\sigma_{42}\sigma_{12} = \sigma_{42}^3$. Quindi $\mathrm{Gal}(E/\mathbb{Q}) \cong D_4$. Per esempio:

$$\sigma_{12}\sigma_{42}\sigma_{12}(\alpha) = \sigma_{12}\sigma_{42}(\alpha) = \sigma_{12}(-\beta) = -\frac{\sigma_{12}(\varepsilon)}{\sigma_{12}(\alpha)} = \frac{\varepsilon}{\alpha} = \beta,$$

$$\sigma_{42}^2(\alpha) = \sigma_{42}(-\beta) = -\frac{\sigma_{42}(\varepsilon)}{\sigma_{42}(\alpha)} = -\alpha$$

$$\sigma_{42}^3(\alpha) = -\sigma_{42}(\alpha)\beta,$$

$$\sigma_{12}\sigma_{42}\sigma_{12}(\varepsilon) = -\varepsilon$$

$$\sigma_{42}^3(\varepsilon) = -\varepsilon.$$

Quindi $\sigma_{12}\sigma_{42}\sigma_{12} = \sigma_{42}^3$ perché questi due elementi del gruppo di Galois assumono gli stessi valori sia su α che su ε. □