Secondo compitino di Algebra 1
15 dicembre 2021

Cognome e nome: .....

Numero di matricola: ..... Aula: .....

IMPORTANTE: Non si possono consultare libri e appunti. Non si possono usare calcolatrici, computer o altri dispositivi elettronici. Non si può scrivere con la matita. Ogni passaggio va motivato (eccetto che nel quiz).

Esercizio 1. QUIZ rapido (1 punto, date la risposta senza dimostrazione): scrivere un intero m tale che il gruppo di Galois $Aut(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ sia isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$.

$m = 156$

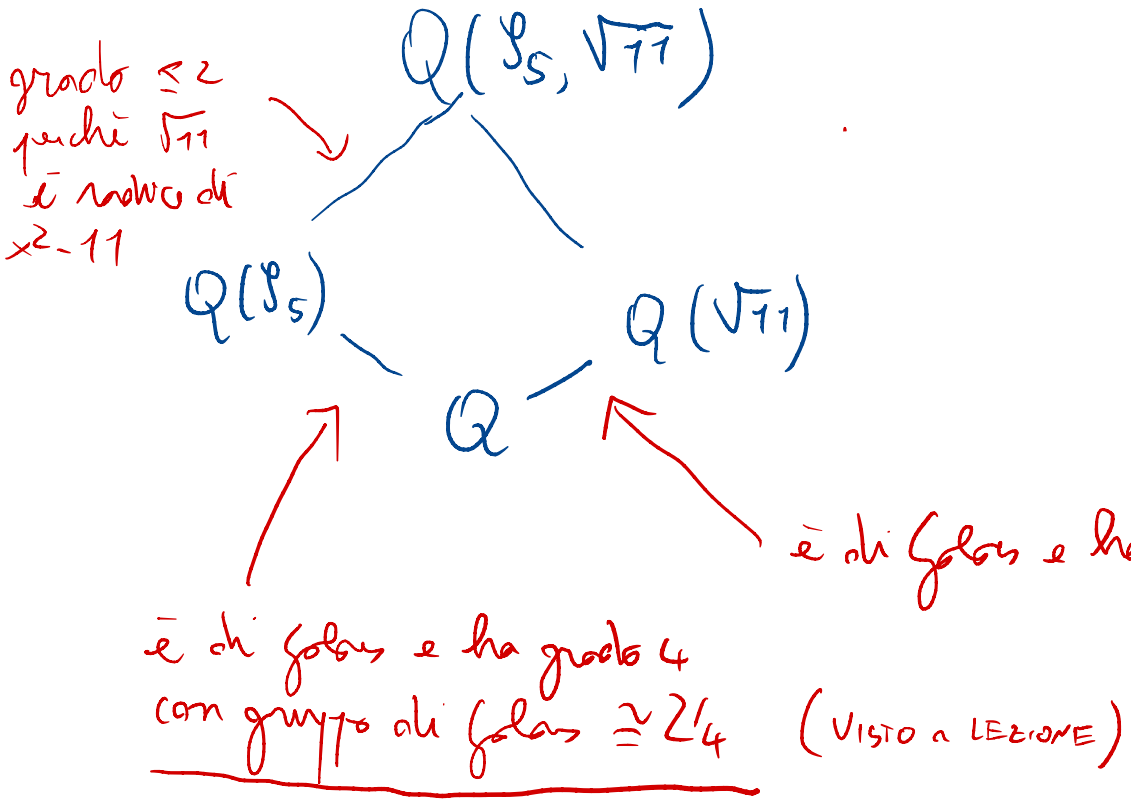
Esercizio 2. (8 punti, con dimostrazione) Si consideri in $\mathbb{Q}[x]$ il polinomio $f(x) = (x^5 - 1)(x^2 - 11)$ e sia K il suo campo di spezzamento su $\mathbb{Q}$.

1. Calcolare $[K : \mathbb{Q}]$
2. Descrivere il gruppo di Galois $G = Aut(K/\mathbb{Q})$.
3. Dire quanti sono i sottocampi di K che hanno ordine 4 su $\mathbb{Q}$ e per ognuno di essi esibire un generatore (ossia scriverli nella forma $\mathbb{Q}(\alpha)$).
4. Considerare il polinomio $f(x) = (x^5-1)(x^2-11)$ in $\mathbb{F}_7[x]$, e determinare il suo campo di spezzamento E su $\mathbb{F}_7$ e il gruppo di Galois $Aut(E/\mathbb{F}_7)$.

(per scrivere la soluzione potete usare le prossime facciate, che sono vuote)

TRACCIA SOLUZIONE

① Il campo K è $\mathbb{Q}(\sqrt[5]{}, \sqrt{11})$. Il grado si calcola col seguente diagramma:



Sappiamo per il teo. di corrispondenza che c'è un'unica sottoestensione L con $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}(\zeta_5)$ e $[L:\mathbb{Q}]=2$.
Come abbiamo visto a lezione, vale $L = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$.
Allora $\mathbb{Q}(\zeta_5) \cap \mathbb{Q}(\sqrt{11}) = \mathbb{Q}$.
Le forse infatti $\mathbb{Q}(\sqrt{11}) \subseteq \mathbb{Q}(\zeta_5)$ allora dovrebbe essere $\mathbb{Q}(\sqrt{11}) = \mathbb{Q}(\sqrt{5})$ e questo è falso come è noto (se $p \neq q$ primi distinti, $\mathbb{Q}(\sqrt{p}) \neq \mathbb{Q}(\sqrt{q})$)
In particolare $\sqrt{11} \notin \mathbb{Q}(\zeta_5)$ e dunque $[K : \mathbb{Q}(\zeta_5)] = 2$.
Per il teorema delle torri, $[K:\mathbb{Q}] = [K:\mathbb{Q}(\zeta_5)][\mathbb{Q}(\zeta_5):\mathbb{Q}] = 2 \cdot 4 = 8$
(2) Di più adesso utilizzare il teorema (esercizio svolto a lezione) per cui (vedi osservazioni accanto al diagramma):

$$\mathrm{Aut}(K/\mathbb{Q}) \cong \mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \times \mathrm{Aut}(\mathbb{Q}(\sqrt{11})/\mathbb{Q})$$

Dunque

$$\mathrm{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}/4 \times \mathbb{Z}/2$$

Ora osserviamo che se $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ abbiamo le seguenti scelte:

$$\sigma(\zeta_5) = \begin{cases} \zeta_5 \\ \zeta_5^2 \\ \zeta_5^3 \\ \zeta_5^4 \end{cases} \qquad \sigma(\sqrt{11}) = \begin{cases} \sqrt{11} \\ -\sqrt{11} \end{cases}$$

I valori $\sigma(\zeta_5)$ e $\sigma(\sqrt{11})$ determinano univocamente σ. Dunque ho al massimo 8 scelte per σ.
Ma so già che $|\mathrm{Aut}(K/\mathbb{Q})| = 8$, allora tutte le 8 scelte danno luogo ad un elemento di $\mathrm{Aut}(K/\mathbb{Q})$.

In particolare considero

$$\sigma_1 : \zeta_5 \to \zeta_5^2 \qquad \text{e} \qquad \rho : \sqrt{11} \to -\sqrt{11}$$

$$\sqrt{11} \to \sqrt{11} \qquad\qquad \zeta_5 \to \zeta_5$$

Si verifica subito che $o(\sigma_1) = 4$ e $o(\rho) = 2$.
Inoltre $\rho \notin (\sigma)$. Dunque σ_1 e ρ generano $\mathrm{Aut}(K/\mathbb{Q})$.

(3) Per il teo di CORRISPONDENZA un s. campo di grado 4 su $\mathbb{Q}$ è il campo fisso di un s. gruppo di

ordine 2 di $Aut(K/Q)$.

Tali 2-gruppi sono tre: $(\sigma_1^2), (\rho), (\sigma_1^2\rho)$.

Vale che $Fix(\rho) = Q(\vartheta_5)$ (infatti ϑ_5 è fissato da ρ dunque

$$Fix(\rho) \geq Q(\vartheta_5) \geq Q.$$

Dato che $[Fix(\rho) : Q] = 4$

e $[Q(\vartheta_5) : Q] = 4$

si conclude per ragioni di grado).

ARGOMENTO STANDARD.
Sia $M = Q(\sqrt{5}, \sqrt{11})$.
Vale che M è est. di Galois di Q
e $Aut(M/Q) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
L'orbita di $\sqrt{5}+\sqrt{11}$ è data
da $\pm\sqrt{5} \pm \sqrt{11}$ dunque
$[Q(\sqrt{5}+\sqrt{11}) : Q] = 4$ dunque
$M = Q(\sqrt{5}+\sqrt{11})$

Vale che $Fix(\sigma_1^2) = Q(\sqrt{5}, \sqrt{11}) = Q(\sqrt{5}+\sqrt{11})$

Infatti σ_1 fissa $\sqrt{11}$, inoltre σ_1^2 manda ϑ_5 in $\vartheta_5^4 = \vartheta_5^{-1} = \overline{\vartheta_5}$ dunque coincide con la restrizione del coniugio a K; da questo si ricava che σ_1^2 fissa $\sqrt{5}$. Dunque $Fix(\sigma_1^2) \geq Q(\sqrt{5}, \sqrt{11})$ e si conclude per ragioni di grado.

Vale che $Fix(\sigma_1^2\rho) = Q(\sqrt{5}, \sqrt{11}(\vartheta_5 - \vartheta_5^{-1}))$

Infatti $\sqrt{11}(\vartheta_5 - \vartheta_5^{-1})$ viene fissato da $\sigma_1^2\rho$

$$\sqrt{11}(\vartheta_5 - \vartheta_5^{-1}) \xrightarrow{\rho} (-\sqrt{11})(\vartheta_5 - \vartheta_5^{-1}) \xrightarrow{\sigma_1^2} (-\sqrt{11})(\vartheta_5^{-1} - \vartheta_5)$$

e anche $\sqrt{5}$ viene fissato da $\sigma_1^2\rho$ (è fissato sia da σ_1^2 sia da ρ).

Dunque $Fix(\sigma_1^2 p) \supseteq Q(\sqrt{5}, \sqrt{11}(\zeta_5 - \zeta_5^{-1})) = T$

e si conclude per ragioni di grado:

$$Q \subseteq Q(\sqrt{5}) \subseteq Q(\sqrt{5}, \sqrt{11}(\zeta_5 - \zeta_5^{-1}))$$

$\uparrow$ grado 2

$\uparrow$ grado = 2 infatti:
grado ≥ 2 perché $\sqrt{11}(\zeta_5 - \zeta_5^{-1}) \in \mathbb{C} \setminus \mathbb{R}$
e ≤ 2 perché $[Fix(\sigma_1^2 p) : Q] = 4$

Infine $T = Q(\sqrt{11}(\zeta_5 - \zeta_5^{-1}))$. Basta mostrare che $\sqrt{5} \in T$. Infatti $(\sqrt{11}(\zeta_5 - \zeta_5^{-1}))^2 = 11(\zeta_5^2 + \zeta_5^{-2} - 2) \Rightarrow \zeta_5^2 + \zeta_5^{-2} \in T$. Ma $\zeta_5^2 + \zeta_5^{-2} = -\zeta_5 - \zeta_5^{-1} - 1$ dunque $\zeta_5 + \zeta_5^{-1} \in T$. Ma $\zeta_5 + \zeta_5^{-1} = \frac{-1+\sqrt{5}}{2} \Rightarrow \sqrt{5} \in T$. (abbiamo già menzionato il fatto che $Q(\sqrt{5}) = Q(\zeta_5 + \zeta_5^{-1})$).

(4) $(x^5 - 1)(x^2 - 11) = (x^5 - 1)(x+2)(x-2)$ in $\mathbb{Z}/7\mathbb{Z}[x]$

Il campo di spezzamento coincide dunque con quello di $x^5 - 1$. Ora tale campo $K = \mathbb{F}_{7^n}$ deve contenere tutte le radici quinte di 1. Se $a \neq 1$ è una tale radice allora $o(a) = 5$. Ma $o(a)$ divide $|K^*| = 7^n - 1$

Il più piccolo n per cui $5 \mid 7^n - 1$, ossia $7^n \equiv 1 \ (5)$, è $n = 4$. Viceversa $\mathbb{F}_{7^4}^*$ è ciclico di ordine $7^4 - 1$ e dunque contiene esattamente un s. gruppo di ordine 5. Gli elementi di questo s. gruppo sono le 5 radici quinte di 1. Dunque $K = \mathbb{F}_{7^4}$ e

$\mathrm{Aut}(\mathbb{F}_{7^4}/\mathbb{F}_7) \cong \mathbb{Z}/4$ come sappiamo dalla teoria.

Esercizio 3. (10 punti, con dimostrazione) Sia $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

1. Scrivere l'orbita di $\sqrt{2} + \sqrt{3}$ rispetto agli elementi di $\mathrm{Aut}(K/\mathbb{Q})$.
2. Mostrare che $\alpha = \sqrt{\sqrt{2} + \sqrt{3}} \notin K$ e determinarne il polinomio minimo $p(x)$ su $\mathbb{Q}$.
3. Sia L il campo di spezzamento di $p(x)$ su $\mathbb{Q}$. Mostrare che $i \in L$ e determinare $[L : \mathbb{Q}]$.
4. Calcolare $N = \mathrm{Gal}(L/\mathbb{Q}[i])$.
5. Descrivere $G = \mathrm{Gal}(L/\mathbb{Q})$ come prodotto semidiretto $N \rtimes H$ per un opportuno gruppo H.

Soluzione:

1. Le estensioni $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ sono di grado 2 e quindi di Galois su $\mathbb{Q}$. Inoltre sono distinte perché 2 non è un quadrato in $\mathbb{Q}(\sqrt{3})$. Infatti se fosse $(a + \sqrt{3}b)^2 = 2$ con $a, b \in \mathbb{Q}$, seguirebbe $ab = 0$ e dunque $2 = a^2$ oppure $2 = 3b^2$, entrambe impossibili. Dunque $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ è di Galois su $\mathbb{Q}$ di grado 4, con gruppo di Galois non ciclico, in quanto ci sono due sottoestensioni non banali distinte, e dunque $H = \mathrm{Aut}(K/\mathbb{Q}) = \mathbb{Z}/2 \times \mathbb{Z}/2$. Un generico σ elemento di H è determinato da

$$\begin{cases} \sigma : \sqrt{2} \mapsto \pm\sqrt{2} \\ \sigma : \sqrt{3} \mapsto \pm\sqrt{3} \end{cases}$$

dunque gli elementi σ così descritti sono tutti realizzati (sono al più 4 in un gruppo di 4 elementi) e l'orbita di $\sqrt{2} + \sqrt{3}$ è data da

$$\{\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3}\}.$$

2. Si ha $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$ e $(\sqrt{2} + \sqrt{3})^4 = 49 + 20\sqrt{6}$. Quindi

$$(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 = -1.$$

Quindi $\sqrt{2}+\sqrt{3}$ è radice del polinomio $x^4 - 10x^2 + 1$. Inoltre segue che $\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ e poiché $\sqrt{6}(\sqrt{2}+\sqrt{3}) = 3\sqrt{2}+2\sqrt{3}$ segue che $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ e $\sqrt{3} \in (\sqrt{2} + \sqrt{3})$. Dunque $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

e $\sqrt{2}+\sqrt{3}$ ha grado 4 su $\mathbb{Q}$. Pertanto x^4-10x^2+1 è il polinomio minimo di $\sqrt{2}+\sqrt{3}$ su $\mathbb{Q}$.

Chiaramente, siccome $\alpha^2=\sqrt{2}+\sqrt{3}$, abbiamo che

$$p(x)=x^8-10x^4+1$$

annulla α. Mostrando che $\alpha\notin\mathbb{Q}(\sqrt{2}+\sqrt{3})$ ne seguirà che $p(x)$ è il polinomio minimo di α su $\mathbb{Q}$. Consideriamo ora $\tau\in H=\mathrm{Aut}(K/\mathbb{Q})$ tale che $\tau(\sqrt{2})=\sqrt{2},\tau(\sqrt{3})=-\sqrt{3}$. Non è dunque possibile che $\alpha\in K\subset\mathbb{R}$ perché AVREMMO che $(\tau(\alpha))^2=\tau(\alpha^2)=\sqrt{2}-\sqrt{3}<0$, il che non può succedere, perché in $\mathbb{R}$ tutti i quadrati sono maggiori o uguali a 0. Dunque $\alpha\notin K$ e poiché $p(\alpha)=0$ abbiamo che $[\mathbb{Q}(\alpha):\mathbb{Q}]=8$ e $p(x)$ è il polinomio minimo di α.

3. Le radici di $q(x)=x^4-10x^2+1$ sono $\pm\sqrt{2}\pm\sqrt{3}$. Poiché $-\sqrt{2}+\sqrt{3}=(\sqrt{2}+\sqrt{3})^{-1}$ e $\sqrt{2}-\sqrt{3}=-(\sqrt{2}+\sqrt{3})^{-1}$, possiamo dire che le radici di $q(x)$ sono $\pm(\sqrt{2}+\sqrt{3})^{\pm1}$. Quindi le radici di $p(x)$ sono $\pm\alpha^{\pm1},\pm i\alpha^{\pm1}$. Di conseguenza il campo di spezzamento L è $\mathbb{Q}(\alpha,i\alpha)=\mathbb{Q}(\alpha,i)\ni i$. Poiché $i\notin\mathbb{Q}(\alpha)\subset\mathbb{R}$, abbiamo

$$[L:\mathbb{Q}]=[\mathbb{Q}(\alpha,i):\mathbb{Q}(\alpha)]\cdot[\mathbb{Q}(\alpha):\mathbb{Q}]=2\cdot8=16.$$

4. Per cardinalità gli automorfismi in $N=\mathrm{Aut}(L/\mathbb{Q}(i))$ sono tutti e soli quelli determinati da

$$\alpha\mapsto(i)^k\alpha^{\pm1}\qquad k\in\mathbb{Z}/4.$$

Chiaramente $\varphi\in N$ definito da $\varphi(\alpha)=i\alpha$ ha ordine 4, mentre $\psi\in N$ definito da $\psi(\alpha)=\alpha^{-1}$ ha ordine 2. Poiché $\psi\notin\langle\varphi\rangle$ segue che $\langle\varphi\rangle\cap\langle\psi\rangle=\{1\}$ e $\langle\varphi\rangle\cdot\langle\psi\rangle=N$. Inoltre poiché $\psi\varphi\psi^{-1}=\varphi^3$, il gruppo N è isomorfo a D_4.

5. Poiché $\mathbb{Q}(i)/\mathbb{Q}$ è un'estensione di Galois, il sottogruppo N di $G=\mathrm{Aut}(L/\mathbb{Q})$ è normale e isomorfo a D_4 per il punto precedente.

Poiché l'estensione $L/\mathbb{Q}(\alpha)$ è di grado 2, è di Galois con gruppo di Galois isomorfo a $\mathbb{Z}_2$. Tale gruppo non è normale in G in quanto l'estensione $\mathbb{Q}(\alpha)/\mathbb{Q}$ non è di Galois. Poiché $L=\mathbb{Q}(\alpha,i)$ abbiamo che

$$\mathrm{Aut}(L/\mathbb{Q}(i))\cap\mathrm{Aut}(L/\mathbb{Q}(\alpha))=\{1\}.$$

Ne segue che $\mathrm{Aut}(L/\mathbb{Q}(i))\cdot\mathrm{Aut}(L/\mathbb{Q}(\alpha))=\mathrm{Aut}(L/\mathbb{Q})$ e che $G=\mathrm{Aut}(L/\mathbb{Q})$ è isomorfo a $D_4\rtimes\mathbb{Z}_2$.

Sia ora c il coniugio ristretto a L.
Dunque $c(a)=a$ e $c(i)=-i$ e $\mathrm{Aut}\left(L/\mathbb{Q}(a)\right)=$
$=(c)$. Per descrivere $D_4\rtimes\mathbb{Z}_2$ restano

da calcolare i coniugi $c\varphi c$ e $c\psi c$.

Vale $c\varphi c(a) = -ia = \varphi^3(a)$

$c\varphi c(i) = i = \varphi^3(i)$

dunque $c\varphi c = \varphi^3 = \varphi^{-1}$

Inoltre $c\psi c(a) = a^{-1} = \psi(a)$

$c\psi c(i) = i = \psi(i)$

dunque $c\psi c = \psi$.