SOLUZIONI DEL COMPITINO DEL 19/11/2018

Esercizio 1. Si consideri il polinomio $f(X) = X^{36} - 1 \in \mathbb{Q}[X]$ e sia $E \subset \mathbb{C}$ il suo campo di spezzamento.

(1) Dimostrare che $\mathbb{Q} \subset E$ è una estensione di Galois e determinarne il grado.
(2) Descrivere il gruppo di Galois $G := \mathrm{Gal}(E/\mathbb{Q})$ come gruppo astratto. Dire quale sia il numero minimo di generatori.
(3) Determinare tutte le estensioni $\mathbb{Q} \subset K \subset E$ con $[K : \mathbb{Q}] = 3$.
(4) Esibire un numero minimo dei generatori di G.

Soluzione: Il campo $\mathbb{Q}$ ha caratteristica 0 e quindi è un campo perfetto. In particolare il polinomio $X^{36} - 1$ è separabile su $\mathbb{Q}$. Essendo E campo di spezzamento di un polinomio separalbile, l'estensione $\mathbb{Q} \subset E$ è di Galois. Essa è generata, come estensione di $\mathbb{Q}$, da una qualunque radice primitiva 36^a dell'unità che denoteremo con ζ (ad esempio $\zeta = e^{\frac{2\pi i}{36}}$). Infatti ζ genera il sottogruppo μ_{36} di $\mathbb{C}$ delle radici 36^e dell'unità che consiste di tutte e sole le radici complesse di $X^{36} - 1$. Il polinomio minimo di ζ è il 36^o polinomio ciclotomico $\Phi_{36}(X)$, che ha grado $\varphi(36) = \varphi(3^2)\varphi(4) = 12$.

L'applicazione $\eta\colon G \to \big(\mathbb{Z}/36\mathbb{Z}\big)^*$ che invia $\sigma \in g$ nell'unico elemento $\eta(\sigma) \in \big(\mathbb{Z}/36\mathbb{Z}\big)^*$ tale che $\sigma(\zeta) = \zeta^{\eta(\sigma)}$ à un omomorfismo di gruppi, iniettivo in quanto ogni $\sigma \in G$ è univocamente determinato da dove invia il generatore ζ dell'estensione $\mathbb{Q} \subset E$. Siccome $|G| = \varphi(36) = \#\big(\mathbb{Z}/36\mathbb{Z}\big)^*$ concludiamo che η è un isomorfismo di gruppi. Inoltre

$$\big(\mathbb{Z}/36\mathbb{Z}\big)^* \overset{CRT}{\cong} \big(\mathbb{Z}/9\mathbb{Z}\big)^* \times \big(\mathbb{Z}/4\mathbb{Z}\big)^* \cong \big(\mathbb{Z}/6\mathbb{Z}\big) \times \big(\mathbb{Z}/2\mathbb{Z}\big).$$

Ogni elemento di G ha ordine al più 6 e quindi G non è ciclico. Ovvero ho bisogno di almeno due generatori. D'altro canto il gruppo G è generato da due elementi σ e τ corrispondenti agli elementi $(1,0)$ e $(0,1)$ di $\big(\mathbb{Z}/6\mathbb{Z}\big) \times \big(\mathbb{Z}/2\mathbb{Z}\big)$, ovvero agli elementi $(2,1)$ e $(1,3)$ in $\big(\mathbb{Z}/9\mathbb{Z}\big)^* \times \big(\mathbb{Z}/4\mathbb{Z}\big)^*$ ovvero agli elementi 2 e 19 di $\big(\mathbb{Z}/36\mathbb{Z}\big)^*$. Quindi $\sigma(\zeta) = \zeta^2$ e $\tau(\zeta) = \zeta^{19}$. Concludiamo inoltre che il numero minimo di generatori di G è 2.

Il gruppo $\big(\mathbb{Z}/6\mathbb{Z}\big) \times \big(\mathbb{Z}/2\mathbb{Z}\big)$ è abeliano con un unico 2-Sylow isomorfo al gruppo di Klein e quindi ha un unico quoziente isomorfo a $\mathbb{Z}/3\mathbb{Z}$. Grazie al teorema fondameentale della teoria di Galois questo implica che ho una sola estensione $\mathbb{Q} \subset K \subset E$ con $[K : \mathbb{Q}] = 3$. Osserviamo che E contiene il 9^o campo ciclotomico L, in quanto $L = \mathbb{Q}(\zeta^4)$. Questo ha grado $\varphi(9) = 6$ su $\mathbb{Q}$. Concludo alllora che il sottocampo reale $K = L \cap \mathbb{R} = \mathbb{Q}(\zeta^4 + \overline{\zeta}^4)$ ha grado 3 su $\mathbb{Q}$. Questo è l'unico sottocampo cercato.

Esercizio 2. Sia $K \subset \mathbb{C}$ il 9^o campo ciclotomico e sia $L = \mathbb{Q}(\sqrt{3}) \subset \mathbb{C}$. Sia $E = K \cdot L \subset \mathbb{C}$ il campo composto.

(1) Mostrare che l'estensione $\mathbb{Q} \subset E$ è di Galois.
(2) Determinare il grado e un generatore di $K \cap \mathbb{R}$ su $\mathbb{Q}$.
(2) Determinare $K \cap L$ e calcolare il grado $[E : \mathbb{Q}]$.
(2) Determinare il gruppo di Galois $G := \mathrm{Gal}(E/\mathbb{Q})$ come gruppo astratto.

Soluzione: $\mathbb{Q} \subset K$ è il campo di spezzamento del 9^o campo ciclotomico che è separabile su $\mathbb{Q}$ essendo quest'ultimo un campo di caratteristica 0 e quindi pefetto. Sia $\zeta := e^{\frac{2\pi i}{9}}$. Come spiegato nel precedente esercizio l'applicazione $\eta\colon \mathrm{Gal}(K/\mathbb{Q}) \to \big(\mathbb{Z}/9\mathbb{Z}\big)^*$ che invia $\sigma \in g$ nell'unico elemento $\eta(\sigma) \in \big(\mathbb{Z}/9\mathbb{Z}\big)^*$ tale che $\sigma(\zeta) = \zeta^{\eta(\sigma)}$ à un isomorfismo di gruppi.

Siccome $\left(\mathbb{Z}/9\mathbb{Z}\right)^* \cong \mathbb{Z}/6\mathbb{Z}$ deduco che G è ciclico di ordine 6. Il coniugio complesso c definisce l'elemento di ordine 2 in $\mathrm{Gal}(K/\mathbb{Q})$. Quindi epr il Teorema fondamentale delal teoria di galois ho che $K \cap \mathbb{R}$ ha grado 3 su $\mathbb{Q}$. inoltre $F := \mathbb{Q}(\zeta + \overline{\zeta}) \subset K \cap \mathbb{R}$. Siccome ζ è radice del polinomio $X^2 - (\zeta + \overline{\zeta})X + 1 \in F[X]$ e $K = F(\zeta)$, concludo che $[K : F] \leq 2$ e quindi $[K : F] = 2$, $F : \mathbb{Q}] = 3$ e $F = K \cap \mathbb{R}$.

Analogamente $\mathbb{Q} \subset L$ è il campo di spezzamento del polinomio $X^2 - 2$ che è irriducibile su $\mathbb{Q}$. Quindi $\mathbb{Q} \subset L$ è di Galois con gruppo $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. Segue che E è il composto di estensioni galoisiane e quindi è di Galois su $\mathbb{Q}$ per la proposizione 3.20. Inoltre

$$[E : \mathbb{Q}] = \frac{[K : \mathbb{Q}][L : \mathbb{Q}]}{[K \cap L : \mathbb{Q}]}.$$

Siccome $[K \cap L : \mathbb{Q}]$ divide $[K : \mathbb{Q}]$ e $[L : \mathbb{Q}]$ e quindi $[K \cap L : \mathbb{Q}] = 2$ oppure $[K \cap L : \mathbb{Q}] = 1$. Nel secondo case ho che $[E : \mathbb{Q}] = 12$.

Nel primo caso, avrei $K \cap L = L$ per moltiplicatività dei gradi e K sarebbe il composto dell'estensione reale $K \cap \mathbb{R}$, che ha grado 3 su $\mathbb{Q}$ come abbiamo visto, e di L. In particolare $K \subset \mathbb{R}$ (assurdo). Quindi $K \cap L = \mathbb{Q}$.

Per la Proposizione 3.20 sappiamo che l'applicazione $\mathrm{Gal}(E/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ che invia $\sigma \in G$ in $(\sigma|_K, \sigma|_L)$ è un isomorfismo di gruppi. Quindi

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

Esercizio 3. [*TeoGal*] Siano $F \subset E$ ed $F \subset \Omega$ inclusioni di campi e si supponga che $F \subset E$ sia un'estensione finita e che Ω sia algebricamente chiuso.

(1) Si ricordi la definizione di elemento $\alpha \in E$ separabile su F e di estensione $F \subset E$ separabile.
(2) Si dia un esempio di estensione separabile (non banale, cioè tale che $E \neq F$) ed un esempio di estensione inseparabile.
(3) Si mostri che, se E è generata come estensione di F da un elemento α, allora α è separabile su F se e solo se $\#\mathrm{Hom}_F(E, \Omega) = [E : F]$.
(4) Si mostri che l'estensione $F \subset E$ è separabile se e solo se $\#\mathrm{Hom}_F(E, \Omega) = [E : F]$. [SUGG.: Usare, senza dimostrazione, la proposizione 2.7 detta "devstante" nell aa 2017/208 e ribattezzata "allucinogena" nell'aa 2018/2019]

Soluzione: (1) Seguendo le note di Milne diciamo che $F \subset E$ è separabile se ogni $\beta \in E$ è separabile su F, ovvero il polinomio minimo $f_\beta(T) \in F[T]$ di β è un polinomio avente radici distinte (in una qualunque chiusura algebrica).

(2) L'estensione $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ è separabile (essendo di Galois), mentre l'estensione $\mathbb{F}_p(X)[Y^p - X]/\mathbb{F}_p(X)$ con X trascendente su $\mathbb{F}_p$ è inseparabile. Infatti sia $\mathbb{F}_p(X) \subset \Omega$ campo di spezzamento di $Y^p - X \in F[Y]$ e sia $\alpha \in \Omega$ è una radice. Allora $Y^p - X = (Y - alpha)^p \in \Omega[Y]$. Quindi, se $f(Y) \in F[Y]$ è il polinomio minimo di α, allora $f(Y)$ divide $Y^p - X$ e quindi è della forma $(Y - alpha)^e$ come polinomio in $\Omega[Y]$, per un qualche $1 \leq e \leq p$. Siccome $\alpha \in \Omega$ è l'unica radice di $Y^p - X$ segue che $Y^p - X = f(Y)^f$ e quindi $f \cdot e = p$ ovvero $e = p$ e $f(Y) = Y^p - X$ che risulta iriducicibile e inseparabile oppure $f(Y) = Y - alpha$ ovvero esiste $\alpha = \frac{a(X)}{b(X)} \in F$ tale che $\alpha^p = \frac{a(X^p)}{b(X^p)} = X$ con $a(X)$ e $b(X) \in \mathbb{F}_p[X]$. Quindi $a(X^p) = b(X^p) \cdot X$ e per questioni di gradi questo è assurdo.

(3) Sia $f(X) \in F[X]$ il polinomio minimo di α su F. Allora l'omomorfismo di anelli $\Psi_\alpha \colon F[X] \to E$, che invia la classe di un polinomio $g(X)$ in $g(\alpha)$, induce un un F-isomorfismo di campi $\overline{\Psi}_\alpha \colon F[X]/(f(X)) \to E$. Segue che l'applicazione $\mathrm{Hom}_F(E, \Omega) \to \{\gamma \in \Omega | f(\gamma) = 0\}$, definita inviando un F-omomorfismo $\rho \colon E \to \Omega$ in $\rho(\alpha) = \rho\big(\overline{\Psi}_\alpha(X)\big)$ è una biezione. L'applicazione inversa è ottenuta associando ad una radice γ di $f(X)$ in Ω l'F-omomrfismo $E \to F$ ottenuto come il composto di $\overline{\Psi}_\alpha^{-1}$ con l'F-omomorfsmo $F[X]/(f(X)) \to \Omega$ che invia

la classe di un polinomio $g(X)$ in $g(\gamma)$. Qundi $\#\mathrm{Hom}_F(E,\Omega) = \#\{\gamma \in \Omega | f(\gamma) = 0\} \leq \deg(f(X)) = [E:F]$ e ho uguaglianza se e solo se $f(X)$ ha tutte radici distinte in Ω ovvero è separabile.

(4) Se $F \subset E$ è separabile, dati $\alpha_1, \ldots, \alpha_n$ generatori di E come estensione di F, si $g(X)$ il prodotto dei polinomi minimi $f_i(X)$ di α_i su F omettoend il fattore i-esimo se esiste $1 \leq j < i$ tale che $f_i(X) = f_j(X)$. I polinomi $f_i(X)$ sono separabili su F per ipotesi e quindi hanno tutti zeri distinti in Ω. Inoltre $g(X)$ è prodotto di polinomi coprimi a due a due e, quindi, ha tutti zeri distinti in Ω. Pe la Proposizione 2.7 segue che $\#\mathrm{Hom}_F(E,\Omega) = [E:F]$.

Supponiamo ora che $\#\mathrm{Hom}_F(E,\Omega) = [E:F]$. Sia $\alpha \in E$ e $K = F(\alpha)$. Per la prop. 2.7 ho che $\#\mathrm{Hom}_F(K,\Omega) \leq [K:F]$ e, per ogni $\rho \in \mathrm{Hom}_F(K,\Omega)$, l'insieme $\mathrm{Hom}_\rho(E,\Omega) := \{\tau \colon E \to \Omega | \tau|_K = \rho\}$ ha cardinalità $\leq [E:K]$. Quindi $\#\mathrm{Hom}_F(E,\Omega) \leq \#\mathrm{Hom}_F(K,\Omega)[E:K] \leq [K:F][E:K] = [E:F]$ per il lemma di moltiplicatività dei gradi. Avendo uguaglianza segue che $\#\mathrm{Hom}_F(K,\Omega) = [K:F]$ e, dal punto (3), concludo che α è separabile su F.