PARZIALE DI ALGEBRA 3, 22/11/2016

COGNOME e Nome .....

MATRICOLA .....

Esercizio 1. Sia K il campo di spezzamento di $T^{15}-1 \in \mathbb{Q}[T]$.

i. Mostrare che $\mathbb{Q} \subset K$ è una estensione finita di Galois. Determinarne il grado.
ii. Sia G il gruppo di Galois dell'estensione $\mathbb{Q} \subset K$. Determinare G come gruppo astratto.
iii. Dire se gli elementi di K sono costruibili con riga e compasso a partire da $A = \{0, 1\}$.
iv. Determinare il numero di sottocampi $\mathbb{Q} \subset L \subset K$ di grado 4 su $\mathbb{Q}$.
v. Esibire dei generatori di G.
vi. $(*)$ Per ciascun campo L in (iv) esibirne dei generatori come estensioni di $\mathbb{Q}$.

Soluzione:

(i) Il campo $\mathbb{Q}$ è un campo di caratteristica 0 e quindi è un campo perfetto. In particolare il polinomio $T^{15}-1$ è un polinomio separabile. L'estensione $\mathbb{Q} \subset K$ è dunque il campo di spezzamento di un polinomio separabile e quindi è finita e di Galois. Il grado è $\varphi(15) = \varphi(5)\varphi(4) = 8$ (φ è la funzione di Eulero).

(ii) Sia μ_{15} il sottogruppo moltiplicativo di K^* delle radici di $T^{15}-1$. È un gruppo ciclico di ordine 15. Fissato un generatore ζ otteniamo un isomorfismo di gruppi $\eta\colon \mu_{15} \cong \mathbb{Z}/15\mathbb{Z}$. Abbiamo un isomorfismo di gruppi

$$\rho\colon G \to \big(\mathbb{Z}/15\mathbb{Z}\big)^*$$

definito come segue. Sia $\sigma \in G$. Allora $\sigma|_{\mu_{15}}\colon \mu_{15} \to \mu_{15}$ è un isomorfismo di gruppi e, tramite η, definisce un isomorfismo $\tilde{\sigma}\colon \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$. Allora $\rho(\sigma)$ è caratterizzato dalla proprietà che $\tilde{\sigma}(a) = \rho(\sigma) \cdot a$. Per il Teorema Cinsese dei Resti $\mathbb{Z}/15\mathbb{Z} \cong (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ e quindi

$$(\mathbb{Z}/15\mathbb{Z})^* \cong (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

visto che $(\mathbb{Z}/5\mathbb{Z})^*$ è ciclico di ordine 4, generato ad esempio dalla classe di 2.

(iii) La risposta è affermativa. Dato l'isomorfismo $G \cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, possiamo scrivere $\mathbb{Q} \subset L_1 \subset L_2 \subset K$ con L_1 corrispondente al sottogruppo $(\mathbb{Z}/4\mathbb{Z}) \times \{0\}$ e L_2 corrispondente al sottogruppo $(2\mathbb{Z}/4\mathbb{Z}) \times \{0\}$. Per il teorema fondamentale della teoria di Galois $\mathbb{Q} \subset L_1$, $L_1 \subset L_2$ e $L_2 \subset K$ sono estensioni di grado 2. Segue che ogni elemento di K è costruibile con riga e compasso.

(iv) I campi richiesti corrispondono a sottogruppi di G di ordine 2, ovvero ad elementi di G di ordine 2. Dato l'isomorfismo $G \cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, gli elementi di ordine 2 sono 3: α, β, γ corrispondenti ai 3 elementi $(2,0)$, oppure $(2,1)$, oppure $(0,1)$ di ordine 2 in $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

(v) Segue che G è abeliano di ordine 8 generato da due elementi σ e γ, di ordine 4 e 2 rispettivamente, definiti come segue. Poniamo $\sigma(\zeta) = \zeta^7$ (osserviamo che $7 \equiv 2$ modulo 5 e $7 \equiv 1$ modulo 3 e quindi $7 \in (\mathbb{Z}/15\mathbb{Z})^*$ viene inviato nell'elemento $(2,1) \in (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$). Analogamente definiamo γ tramite $\gamma(\zeta) = \zeta^{11}$ (osserviamo che $11 \equiv 1$ modulo 5 e $11 \equiv 2$ modulo 3 e quindi $11 \in (\mathbb{Z}/15\mathbb{Z})^*$ viene inviato nell'elemento $(1,-1) \in (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$).

(vi) Il campo corrispondente al sottogruppo generato da γ è il 5^o-campo ciclotomico. Infatti $\zeta_5 = \zeta^3$ è radice primitiva dell'unità di ordine 5 ed è fissata dall'elemento γ di cui al punto precedente. Il campo corrispondente a β (=coniugio complesso come si verifica dal punto

precedente) è $K \cap \mathbb{R} = \mathbb{Q}(\zeta + \overline{\zeta})$: sicuramente $\mathbb{Q}(\zeta + \overline{\zeta}) \subset K \cap \mathbb{R}$ e inoltre K ha grado 2 su $\mathbb{Q}(\zeta+\overline{\zeta})$ in quanto il polinomio minimo di ζ è $T^2-(\zeta+\overline{\zeta})T+1$. Infine il campo corrispondente ad α è il campo composto $\mathbb{Q}(\zeta_5 + \overline{\zeta}_5, \zeta_3)$. Infatti sia $\zeta_5 + \overline{\zeta}_5$ che ζ_3 sono fissati da α e tale campo è una estensione biquadratica di $\mathbb{Q}$.

Esercizio 2. Si consideri il polinomio $f(X) = (X^2 - 5)(X^2 - 7) \in \mathbb{Q}[X]$ e sia E un campo di spezzamento di $f(X)$. Sia K il 4^o campo ciclotomico.

i. Si mostri che l'estensione $\mathbb{Q} \subset E$ è finita e di Galois. Se ne calcoli il grado e il gruppo di Galois H.
ii. Si determini il reticolo dei sottocampi $\mathbb{Q} \subset E$.
iii. Sia L il campo composto $K \cdot E$. Si dimostri che l'estensione $\mathbb{Q} \subset L$ è finita e di Galois. Se ne calcoli il grado e il gruppo di Galois G.
iv. Si trovi $\alpha \in L$ tale che $L = \mathbb{Q}(\alpha)$.
v. Si determinino i sottocampi di $\mathbb{Q} \subset L$ di grado 2 su $\mathbb{Q}$.

Soluzione: L'estensione $\mathbb{Q} \subset E$ è il campo di spezzamento di un polinomio separabile in quanto $\mathbb{Q}$ è di caratteristcia 0 e quindi perfetto. Quindi è finita e di Galois. Il grado di $\mathbb{Q} \subset E$ è 4 in quanto $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5})$ ha grado due e $\sqrt{7} \notin \mathbb{Q}(\sqrt{5})$ (calcolo immediato).

Il 4^o campo ciclotomico è $\mathbb{Q}(i)$ che ha grado 2 su $\mathbb{Q}$. Siccome $E \subset \mathbb{R}$ concludo che $i \notin E$ e quindi L ha grado 2 su E, ovvero grado 8 su $\mathbb{Q}$. Inoltre $\mathbb{Q} \subset L$ è finito di Galois in quanto campo di spezzamento di $f(X)(X^2 + 1)$.

Ogni automorfismo di E (risp. L) è univocamente determinato da dove invia i generatori. Ogni automorfismo invia una radice di $X^2 - 5$ (risp. $X^2 - 7$, risp $X^2 + 1$) in una radice di $X^2 - 5$ (risp. $X^2 - 7$, risp $X^2 + 1$).

(ii) Quindi $H \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ con generatori σ e τ dove $\sigma(\sqrt{5}) = -\sqrt{5}$ e $\sigma(\sqrt{7}) = \sqrt{7}$ e $\tau(\sqrt{5}) = \sqrt{5}$ e $\tau(\sqrt{7}) = -\sqrt{7}$.

(iii) Analogamente $G \cong (\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})$ con generatori σ, τ, ξ dove $\sigma(\sqrt{5}) = -\sqrt{5}$ e $\sigma(\sqrt{7}) = \sqrt{7}$ e $\sigma(i) = i$, $\tau(\sqrt{5}) = \sqrt{5}$ e $\tau(\sqrt{7}) = -\sqrt{7}$ e $\tau(i) = i$ e $\xi(\sqrt{5}) = \sqrt{5}$ e $\xi(\sqrt{7}) = \sqrt{7}$ e $\xi(i) = -i$.

(iv) Sia $\alpha = \sqrt{5} + \sqrt{7} + i$. Siccome una $\mathbb{Q}$-base di L è $\{1, \sqrt{5}, \sqrt{7}, i, \sqrt{15}, \sqrt{-5}, \sqrt{-7}, \sqrt{-15}$ l'orbita di α per l'azione di G, ovvero $\{\pm\sqrt{5} \pm \sqrt{7} + \pm i\}$ ha cardinalià 8 e quindi il polinomio minimo di α su $\mathbb{Q}$ ha grado 8, ovvero $\mathbb{Q}(\alpha)$ ha grado 8 su $\mathbb{Q}$ e quindi $L = \mathbb{Q}(\alpha)$ per moltiplicatività dei gradi.

(v) Ho sicuramente i 7 campi $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-7})$ e $\mathbb{Q}(\sqrt{-15})$ che sono tutti distinti in quanto $\{1, \sqrt{5}, \sqrt{7}, i, \sqrt{15}, \sqrt{-5}, \sqrt{-7}, \sqrt{-15}\}$ è $\mathbb{Q}$-base di L. I sottocampi cercati corrispondono ai possibili quozienti di $(\mathbb{Z}/2\mathbb{Z})^3$ di ordine 2 cioè isomorfi a $\mathbb{Z}/2\mathbb{Z}$. Questi sono determinati da dove vengono inviati i generatori $(1, 0, 0)$, $(0, 1, 0)$ e $(0, 0, 1)$ ovvero 0 oppure 1. Almeno uno degli elementi deve essere inviato in 1 (altrimenti il quoziente è di ordine 1). Ho quindi 7 scelte.

Esercizio 3. (*TeoGal*)

Sia F un campo e sia n un intero positivo, coprimo con la caratteristica di F nel caso in cui quest'ultima sia positiva. Sia $F \subset E$ un campo di spezzamento di $f(T) = T^n - 1$.

i. Mostrare che l'estensione $F \subset E$ è finita e di Galois. Sia G il gruppo di Galois.
ii. Mostrare che esiste un omomorfismo iniettivo $\rho\colon G \to (\mathbb{Z}/n\mathbb{Z})^*$.
iii. Nel caso in cui $F = \mathbb{Q}$ dimostrare che ρ è un isomorfismo nel caso in cui n sia primo.
iv. $(*)$ Mostrare (iii) per n generale.

Soluzione: Per i punti (i) e (ii) vedere la soluzione del primo esercizio. Per (iv) basta dimostrare che il polinomio minimo di una radice primitiva n-esima dell'unità ha grado $\varphi(n)$. Questo è dimostrato in Milne. Se $n = p$ si può mostrare direttamente che il polinomio

$X^{p-1} + \cdots + 1$ è irriducibile su $\mathbb{Q}$ sostituendo $X = Y + 1$ e applicando il criterio di Eisenstein per il primo p.