A.A. 2010/2011 - Secondo foglio di esercizi di Algebra 3

1. Siano p_1, p_2 e p_3 tre numeri primi distinti. Dimostrare che $\mathbf{Q}\big[\sqrt{p_1p_2}, \sqrt{p_2p_3}\big]$ è un'estensione di Galois di $\mathbf{Q}$, calcolarne il gruppo di Galois ed il reticolo dei sottocampi.

2. Sia E il campo di spezzamento su $\mathbf{Q}$ del polinomio $f(X) := \big(X^2-3\big)\big(X^4+1\big)$.
(1) Si determini il grado $[E:\mathbf{Q}]$ di E su $\mathbf{Q}$.
(2) Si calcoli il gruppo di Galois $G := \mathrm{Gal}(E/\mathbf{Q})$ di E su $\mathbf{Q}$.
(3) Si determini il reticolo dei sottogruppi di G e dei sottocampi di E.

3. Sia K il sottocampo $\mathbf{Q}\big[2^{\frac{1}{2}}+3^{\frac{1}{3}}\big]$ di $\mathbf{R}$.
(1) Dimostrare che K non è normale su $\mathbf{Q}$.
(2) Determinare la chiusura normale L di K su $\mathbf{Q}$.
(3) Calcolare il gruppo di Galois $G = \mathrm{Gal}(L/\mathbf{Q})$.
(4) Trovare $\alpha \in K$ tale che $K = \mathbf{Q}[\alpha]$.
(5)* Trovare il reticolo dei sottogruppi di G e dei sottocampi di L.

4. Sia D_{10} il gruppo diedrale di ordine 10. Sia $K \subset F$ un'estensione di Galois avente gruppo di Galois G isomorfo a D_{10}. Descrivere il reticolo dei sottogruppi di G e dei sottocampi di F, specificando quali di essi siano di Galois.

5. 1) Sia φ la funzione di Eulero. Se $m = \prod_{i=1}^{k} p_i^{a_i}$, dove p_i è primo e $a_i \in \mathbf{N}$, dimostrare che

$$\varphi(m) = \prod_{i=1}^{k} \varphi(p^{a_i}) = \prod_{i=1}^{k} (p_i - 1)p^{a_i-1}.$$

[Suggerimento: applicare il Teorema Cinese del Resto a $\mathbf{Z}/m\mathbf{Z}$.]

2) Calcolare l'm-esimo polinomio ciclotomico Φ_m per $m \leq 21$. [Suggerimento: notare la formula induttiva

$$\Phi_m(x) = \frac{x^m - 1}{\prod_{d|m, d\neq m} \Phi_d(x)}$$

dove il prodotto è effettuato sui divisori positivi d di m, con $1 \leq d < m$.]

3) Descrivere la struttura di $\mathrm{Gal}\big(\mathbf{Q}[e^{2\pi i/m}]/\mathbf{Q}\big)$ per $m \leq 21$.

6. Sia μ la funzione su $\mathbf{N}$ definita da

$$\mu(n) = \begin{cases} (-1)^m & \text{se } n \text{ è prodotto di } m \text{ fattori primi distinti} \\ 0 & \text{altrimenti} \end{cases}.$$

Mostrare che
(i) l' n-esimo polinomio ciclotomico $\Phi_n(T)$ soddisfa

$$\Phi_n(T) = \prod_{d|n} \big(X^d - 1\big)^{\mu(n/d)};$$

(ii) se $\Phi_n(T) = T^m + a_{m-1}T^{m-1} + \cdots$ allora $a_{m-1} = -\mu(n)$.

(iii) se $\mathbf{F}_q$ è il campo con $q = p^n$ elementi, mostrare che ci sono

$$\sum_{d|n} \mu(n/d) q^d$$

elementi $\zeta \in \mathbf{F}_q$ tali che $\mathbf{F}_q = \mathbf{F}_p(\zeta)$.

7. Sia $\Phi_n(T)$ l' n-esimo polinomio ciclotomico.

(i) Sia $x \in \mathbf{Z}$ e sia p è un numero primo che divide $\Phi_n(x)$. Mostrare che allora p divide n oppure $p \equiv 1$ modulo n

(ii) Mostrare che esistono infiniti primi p tali che $p \equiv 1$ modulo n. (Sugg.: se fossero finiti $p_1, \ldots, p_t$, considerare un divisore di $\Phi_n\big(np_1 \cdots p_t\big)$.

(iii) Usando (ii), mostrare che per ogni N ed $a \in \mathbf{N}$ non nulli esiste un intero n ed una suriezione di gruppi abeliani

$$\big(\mathbf{Z}/n\mathbf{Z}\big)^* \longrightarrow \big(\mathbf{Z}/N\mathbf{Z}\big)^a.$$

(iv) Mostrare che mostrare che per ogni N ed $a \in \mathbf{N}$ non nulli esiste una estensione di Galois F di $\mathbf{Q}$ con gruppo di Galois

$$\mathrm{Gal}(F/\mathbf{Q}) \cong \big(\mathbf{Z}/N\mathbf{Z}\big)^a.$$

(v) Mostrare che per ogni gruppo abeliano finito A prodotto di gruppi ciclici esiste una estensione di Galois F di $\mathbf{Q}$ con gruppo di Galois A.

8. Sia $\mathbf{F}_q$ un campo finito con q elementi. Sia $\mathbf{F}_q \subset K$ una estensione finita e siano α e $\beta \in K$. Mostrare che se $\mathbf{F}_q(\alpha) \cap \mathbf{F}_q(\beta) \subset \mathbf{F}_q(\alpha + \beta)$ allora $\mathbf{F}_q(\alpha + \beta) = \mathbf{F}_q(\alpha, \beta)$.

9. Siano H ed N due sottogruppi finiti e sia

$$\Psi\colon H \longrightarrow \mathrm{Aut}(N), \qquad h \mapsto \psi_h$$

un omomorfismo di gruppi dove $\mathrm{Aut}(N)$ è il gruppo degli automorfismi di N come gruppo. Definisco $N \rtimes_\psi H$ come l'insieme $N \times H$ con moltiplicazione

$$\big(N \rtimes_\psi H\big) \times \big(N \rtimes_\psi H\big) \longrightarrow N \rtimes_\psi H, \quad \big((n,h),(n',h')\big) \mapsto \big(n\psi_h(n'), hh'\big),$$

$\mathbf{1} := (1,1)$ e inverso

$$N \rtimes_\psi H \longrightarrow N \rtimes_\psi H, \qquad (n,h) \mapsto \big(\psi_{h^{-1}}(n^{-1}), h^{-1}\big).$$

(i) Mostrare che $N \rtimes_\psi H$ è un gruppo e le applicazioni

$$N \longrightarrow N \rtimes_\psi H, \quad n \mapsto (n,1), \qquad H \longrightarrow N \rtimes_\psi H, \quad h \mapsto (1,h)$$

sono omomorfismi iniettivi di gruppi che idenitificano $N \rtimes_\psi H$ con il prodotto semidiretto dell'immagine di N per l'immagine di H.

(ii) Mostare che $N \rtimes_\psi H$ è il prodotto diretto $N \times H$ se e solo se Ψ è l'applicazione che manda ogni $h \in H$ nell'applicazione identica di N.

(iii) Sia G un gruppo prodotto semidiretto dei sottogruppi finiti A per B, con A normale in G. Sia

$$\psi\colon B \longrightarrow \mathrm{Aut}(A), \qquad \psi_b(a) = bab^{-1} \forall a \in A, b \in B.$$

Mostrare che ψ è un omomorfismo di gruppi e l'applicazione

$$A \rtimes_\psi B \longrightarrow G, (a,b) \mapsto a \cdot b$$

è un isomomorfismo di gruppi.

10. 1) Sia $K = \mathbf{Q}[2^{1/2}, 3^{1/2}]$. Trovare $\alpha \in K$ tale che $K = \mathbf{Q}[\alpha]$.

2) Sia $K = \mathbf{Q}[3^{1/2}, 5^{1/2}, (-7)^{1/2}]$. Trovare $\alpha \in K$ tale che $K = \mathbf{Q}[\alpha]$.

11. 1) Osservato che il numero complesso $\alpha = (-5)^{1/2} + 7^{1/2}$ è un intero algebrico, calcolare un polinomio monico con coefficienti in $\mathbf{Z}$ di cui α è radice.

2) Osservato che il numero reale $\alpha = 3^{1/2} + 5^{1/3}$ è un intero algebrico, calcolare un polinomio monico con coefficienti in $\mathbf{Z}$ di cui α è radice.

3) Calcolare il polinomio minimo di $3^{1/2} \cdot 5^{1/3}$.

4) Calcolare il polinomio minimo di $3^{1/2}+(-5)^{1/2}+11^{1/2}$. [Suggerimento: osservare che $3^{1/2} + (-5)^{1/2} + 11^{1/2}$ è un intero algebrico.]

12. Sia K/F un'estensione di campi di numeri e sia $(\alpha_1, \ldots, \alpha_n) \in K^n$.

1) Dimostrare che gli elementi $\alpha_1, \ldots, \alpha_n$ sono F-linearmente dipendenti se e solo se $\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n) = 0$.

2) Dimostrare che $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ appartiene a F. [Suggerimento: notare dapprima che il numero complesso $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ appartiene alla chiusura normale L di K/F in $\mathbf{C}$; mostrare poi che

$$\sigma(\mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n)) = \mathrm{disc}_{K/F}(\alpha_1, \ldots, \alpha_n)$$

per ogni σ in $\mathrm{Gal}(L/F)$.]

13. Dato $d \in \mathbf{Z} - \{0, 1\}$ privo di fattori quadratici, si definisca $D = d$ se $d \equiv 1 \pmod 4$ e $D = 4d$ se $d \equiv 2, 3 \pmod 4$. Si dimostri che $\mathbf{Q}[\sqrt{d}]$ è contenuto nel D-esimo campo ciclotomico $\mathbf{Q}[e^{2\pi i/D}]$. [Suggerimento: si fattorizzi d (a meno del segno) come prodotto di primi; si osservi poi che $\mathbf{Q}[\sqrt{p}]$ è contenuto in $\mathbf{Q}[e^{2\pi i/4p}]$ se p è un primo $\equiv 3 \pmod 4$ ...]

14. Mostrare che l'insieme $(\alpha_1, \ldots, \alpha_n) \subset \mathcal{O}_K$ è una base intera per $\mathcal{O}_K$ se e solo se $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}(\mathcal{O}_K)$.

15. Sia $K = \mathbf{Q}\big[\sqrt{m}, \sqrt{n}\big]$, con m e n interi coprimi tali che $m \equiv 1 \pmod 4$. Utilizzando il Teorema 4.14 e il Corollario 4.15 degli appunti, calcolare $\mathcal{O}_K$.