Compito di Istituzioni di Algebra Superiore di dicembre 2006

1. Sia $\alpha = 2 + i\sqrt{3} \in \mathbb{C}$.
(a) Determinare il polinomio minimo di α su $\mathbb{Q}$.
(b) Scrivere $(1+\alpha)^{-1}$ come polinomio in α.
(c) Dire se $\mathbb{Q}(\alpha)$ è estensione normale di $\mathbb{Q}$.

Risoluzione:
(a) $\alpha - 2 = i\sqrt{3}$
$(\alpha - 2)^2 = -3$
$\alpha^2 - 4\alpha + 7 = 0$.

Pertanto α è radice del polinomio $x^2 - 4x + 7 \in \mathbb{Q}[x]$. Questo polinomio è monico e le sue due radici sono α e $2 - i\sqrt{3}$, entrambe numeri non razionali. Quindi il polinomio è irriducibile (perchè polinomio di secondo grado senza radici nel campo) ed è il polinomio minimo di α su $\mathbb{Q}$.

(b) Poichè α è algebrico su $\mathbb{Q}$, abbiamo che $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$, cioè ogni elemento in $\mathbb{Q}(\alpha)$ si può scrivere come polinomio in α. Inoltre dal teorema di struttura delle estensioni semplici sappiamo che una base di $\mathbb{Q}(\alpha)$ come spazio vettoriale su $\mathbb{Q}$ è $\{1, \alpha\}$.

Per trovare l'inverso di $\alpha+1$ dividiamo il polinomio minimo di α per $x+1$ (ottenuto sostituendo x ad α). La divisione con resto dà

$$x^2 - 4x + 7 = (x+1)(x-5) + 12$$

da cui sostituendo α ad x si ha

$$0 = \alpha^2 - 4\alpha + 7 = (1+\alpha)(\alpha - 5) + 12$$

e

$$(\alpha + 1)\frac{(\alpha - 5)}{-12} = 1.$$

Pertanto $(\alpha - 1)^{-1} = (5 - \alpha)/12$.

(c) $\mathbb{Q}(\alpha)$ è un'estensione di grado due su $\mathbb{Q}$, quindi è un'estensione normale di $\mathbb{Q}$. Infatti Ogni estensione di grado due è un'estensione normale. In questo caso si può vedere che $\mathbb{Q}(\alpha)$ è il campo di spezzamento del polinomio $x^2 - 4x + 7$ su $\mathbb{Q}$. Infatti le due radici del polinomio sono α e $2 - i\sqrt{3} = 4 - \alpha$ e chiaramente $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, 4 - \alpha)$.

2. Sia $f(x) = x^3 + 6 \in \mathbb{Q}[x]$.
(a) Determinare il campo di spezzamento Σ di f su $\mathbb{Q}$.
(b) Determinare il gruppo di Galois $Gal(\Sigma : \mathbb{Q})$, scrivendo i suoi elementi come permutazioni delle radici di f.
(c) Descrivere il reticolo dei sottocampi di Σ.

Risoluzione:

(a) Le radici di f sono $-\sqrt[3]{6}$, $-\sqrt[3]{6}\omega$ e $-\sqrt[3]{6}\omega^2$, dove ω è una radice primitiva dell'unità, ad esempio $e^{\frac{2\pi}{3}}$. Quindi $\Sigma = \mathbb{Q}(\sqrt[3]{6}, \omega)$.

(b) Σ è un'estensione normale separabile di $\mathbb{Q}$ in quanto campo di spezzamento di un polinomio in caratteristica 0. Quindi è un'estensione di Galois di $\mathbb{Q}$ e così la cardinalità del gruppo di Galois $Gal(\Sigma : \mathbb{Q})$ è uguale a $|\Sigma : \mathbb{Q}|$. Calcoliamo $|\Sigma : \mathbb{Q}|$.

$$|\Sigma : \mathbb{Q}| = |\mathbb{Q}(\sqrt[3]{6}, \omega) : \mathbb{Q}| = |\mathbb{Q}(\sqrt[3]{6}, \omega) : \mathbb{Q}(\sqrt[3]{6})||\mathbb{Q}(\sqrt[3]{6}) : \mathbb{Q}|.$$

Il polinomio minimo di ω su $\mathbb{Q}(\sqrt[3]{6})$ è $x^2 + x + 1$: infatti è un polinomio monico a coefficienti in $\mathbb{Q}$ che ha ω come radice ed è irriducibile su $\mathbb{Q}(\sqrt[3]{6})$ perchè è un poliomio di grado due con due radici non reali (e quindi non ha radici in $\mathbb{Q}(\sqrt[3]{6}) \subset \mathbb{R}$). Quindi $|\mathbb{Q}(\sqrt[3]{6}, \omega) : \mathbb{Q}(\sqrt[3]{6})| = 2$.
Il polinomio minimo di $\sqrt[3]{6}$ su $\mathbb{Q}$ è $x^3 - 6$, polinomio monico a coefficienti in $\mathbb{Q}$ che si annulla in $\sqrt[3]{6}$ e irriducibile su $\mathbb{Q}$ perchè di grado 3 e privo di radici in $\mathbb{Q}$. Quindi $|\mathbb{Q}(\sqrt[3]{6}) : \mathbb{Q}| = 3$. Così, $|\Sigma : \mathbb{Q}| = 2 \cdot 3 = 6$ e $|Gal(\Sigma : \mathbb{Q})| = 6$.
Poichè f è irriducibile su $\mathbb{Q}$ (si ripete il ragionamento fatto nel paragrafo precedente) sappiamo che $Gal(\Sigma : \mathbb{Q})$ è isomorfo ad un gruppo di permutazioni sull'insieme delle radici di f, cioè ad un sottogruppo di Sym(3). D'altra parte $|\mathrm{Sym}(3)| = 6 = |Gal(\Sigma : \mathbb{Q})|$: quindi $Gal(\Sigma : \mathbb{Q}) = \mathrm{Sym}(3)$. Gli elementi di $Gal(\Sigma : \mathbb{Q})$ scritti come permutazioni sulle radici di f sono quindi:

$$id, \sigma_2 = (-\sqrt[3]{6}, -\sqrt[3]{6}\omega), \sigma_3 = (-\sqrt[3]{6}, -\sqrt[3]{6}\omega^2), \sigma_4 = (-\sqrt[3]{6}\omega, -\sqrt[3]{6}\omega^2),$$

$$\sigma_5 = (-\sqrt[3]{6}, -\sqrt[3]{6}\omega, -\sqrt[3]{6}\omega^2), \sigma_6 = (-\sqrt[3]{6}, -\sqrt[3]{6}\omega^2, -\sqrt[3]{6}\omega).$$

(c) Per il teorema di corrispondenza di Galois, il reticolo dei sottocampi di Σ è in corrispondenza biunivoca con il reticolo dei sottogruppi di $Gal(\Sigma : \mathbb{Q}) = \mathrm{Sym}(3)$. Ricordando che Sym(3) ha tre sottogruppi di ordine 2, ciclici

generati dagli elementi di ordine 2, e un sottogruppo di ordine 3, ciclico generato dagli elementi di ordine 3, si ottiene che i sottocampi di Σ sono: Σ, $\mathbb{Q}$ e

$$\Sigma_{\langle\sigma_2\rangle} = \{a \in \Sigma \mid \sigma_2(a) = a\},$$
$$\Sigma_{\langle\sigma_3\rangle} = \{a \in \Sigma \mid \sigma_3(a) = a\},$$
$$\Sigma_{\langle\sigma_4\rangle} = \{a \in \Sigma \mid \sigma_4(a) = a\},$$
$$\Sigma_{\langle\sigma_5\rangle} = \{a \in \Sigma \mid \sigma(a) = a\, \forall \sigma \in \langle\sigma_5\rangle\} = \{a \in \Sigma \mid \sigma_5(a) = a\}.$$

Per identificare questi campi osserviamo quanto segue. Dal teorema di corrispondenza sappiamo che $|\Sigma_{\langle\sigma_i\rangle} : \mathbb{Q}| = |Gal(\Sigma : \mathbb{Q}) : \langle\sigma_i\rangle| = \frac{|Gal(\Sigma:\mathbb{Q})|}{|\langle\sigma_i\rangle|}$. Quindi $|\Sigma_{\langle\sigma_i\rangle} : \mathbb{Q}| = 3$ per $i = 2, 3, 4$ e $|\Sigma_{\langle\sigma_5\rangle} : \mathbb{Q}| = 2$.

Consideriamo prima $\Sigma_{\langle\sigma_4\rangle}$. Chiaramente l'automorfismo σ_4 lascia fissa la radice $-\sqrt[3]{6}$. Perciò $-\sqrt[3]{6} \in \Sigma_{\langle\sigma_4\rangle}$ e $\mathbb{Q}(-\sqrt[3]{6}) \subseteq \Sigma_{\langle\sigma_4\rangle}$. D'altra parte $|\mathbb{Q}(-\sqrt[3]{6}) : \mathbb{Q}| = 3 = |\Sigma_{\langle\sigma_4\rangle} : \mathbb{Q}|$. Quindi $\Sigma_{\langle\sigma_4\rangle} = \mathbb{Q}(-\sqrt[3]{6}) = \mathbb{Q}(\sqrt[3]{6})$. Con ragionamento analogo si dimostra che $\Sigma_{\langle\sigma_2\rangle} = \mathbb{Q}(\sqrt[3]{6}\omega^2)$ e $\Sigma_{\langle\sigma_3\rangle} = \mathbb{Q}(\sqrt[3]{6}\omega)$.

Infine consideriamo $\Sigma_{\langle\sigma_5\rangle}$. Si verifica che $\omega \in \Sigma_{\langle\sigma_5\rangle}$ e $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2$. Allora $\mathbb{Q}(\omega) \subseteq \Sigma_{\langle\sigma_5\rangle}$ e poichè hanno lo stesso grado su $\mathbb{Q}$ devono coincidere: $\Sigma_{\langle\sigma_5\rangle} = \mathbb{Q}(\omega)$.

Questi quattro sottocampi intermedi a due a due si intersecano in $\mathbb{Q}$ che è il sottocampo fondamentale e a due a due generano Σ.

3. (a) Si dica se il poliomio $x^3 + x^2 + 1$ è irriducibile in $\mathbb{Z}_5[x]$.
(b) Si dia una costruzione esplicita del campo F di ordine 125.
(c) Dire se 3 è un quadrato in F, motivando la risposta.

Risoluzione:

(a) Il polinomio $f = x^3 + x^2 + 1$ è di grado 3 e quindi è irriducibile in $\mathbb{Z}_5[x]$ se e solo se non ha radici in $\mathbb{Z}_5$. Verifichiamolo direttamente:
$f(0) = 1 \neq 0$, $f(1) = 3 \neq 0$, $f(2) = 13 = 3 \neq 0$, $f(3) = 37 = 2 \neq 0$, $f(4) = f(-1) = 1 \neq 0$. Quindi il polinomio è irriducibile.

(b) Un campo F di ordine 125 è un'estensione di grado 3 del campo $\mathbb{Z}_5$. Possiamo quindi costruire F così:

$$F = \frac{\mathbb{Z}_5[x]}{\langle x^3 + x^2 + 1\rangle} = \mathbb{Z}_5[\alpha]$$

dove α è uno zero del polinomio $f = x^3 + x^2 + 1$.

(c) Osserviamo che 3 non è un quadrato in $\mathbb{Z}_5$, infatti nessun elemento di $\mathbb{Z}_5$ elevato al quadrato da 3. Supponiamo che 3 sia un quadrato in F. Allora deve esistere un elemento $\omega \in F \setminus \mathbb{Z}_5$ tale che $\omega^2 = 3$. Consideriamo l'estensione $\mathbb{Z}_5(\omega)$. Poichè $\omega \in F$ abbiamo che $\mathbb{Z}_5(\omega) \subseteq F$ e $|\mathbb{Z}_5(\omega) : \mathbb{Z}_5| = 2$ perchè il polinomio minimo di ω su $\mathbb{Z}_5$ è $x^2 - 3$. Per il teorema dei gradi si ha che $2 = |\mathbb{Z}_5(\omega) : \mathbb{Z}_5|$ divide $|F : \mathbb{Z}_5| = 3$: contraddizione. Pertanto 3 non è un quadrato in F.

4. Calcolare il polinomio ciclotomico $\Phi_{15}(x)$. Fattorizzare $\Phi_{15}(x)$ in irriducibili in $\mathbb{Z}_{31}[x]$.

Risoluzione:

$$\Phi_{15}(x) = \frac{x^{15} - 1}{\Phi_1 \Phi_3 \Phi_5} = \frac{(x^5 - 1)(x^{10} + x^5 + 1)}{(x^5 - 1)\Phi_3} = \frac{x^{10} + x^5 + 1}{x^2 + x + 1} =$$

$$= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$$

Osserviamo che $\Phi_{15}(x)$ ha radici nel campo $\mathbb{Z}_{31}$ se e solo se $\mathbb{Z}_{31}$ contiene radici primitive quindicesime dell'unità, cioè elementi il cui ordine moltiplicativo è 15. Il gruppo moltiplicativo del campo $\mathbb{Z}_{31}$ è un gruppo ciclico di ordine 30 e quindi contiene elementi di ordine n per ogni n divisore di 30. In particolare contiene elementi di ordine 15, cioè radici di $\Phi_{15}(x)$. Quanti sono questi elementi? Sempre dalla struttura dei gruppi ciclici sappiamo che tutti gli elementi di ordine 15 sono contenuti nell'unico sottogruppo di ordine 15 di $\mathbb{Z}_{31}^*$ e ne sono i generatori. Il numero dei generatori di un gruppo ciclico di ordine 15 è $\varphi(15) = \varphi(3)\varphi(5) = 3 \cdot 4 = 8$. Pertanto le radici di $\Phi_{15}(x)$ in $\mathbb{Z}_{31}$ sono 8, pari al grado del polinomio; quindi $\Phi_{15}(x)$ si fattorizza completamente in $\mathbb{Z}_{31}[x]$. Con un po' di pazienza si trova che 9 ha periodo moltiplicativo 15 in $\mathbb{Z}_{31}$. Dopodichè gli altri elementi di ordine 15 sono $9^2 = 19, 9^4 = 20, 9^7 = 10, 9^8 = 28, 9^{11} = 14, 9^{13} = 18, 9^{14} = 7$ (si noti che gli esoinenti sono tutti i numeri naturali minori di 15 e coprimi con 15). Quindi la fattorizzazione di $\Phi_{15}(x)$ è

$$\Phi_{15}(x) = (x - 9)(x - 19)(x - 20)(x - 10)(x - 28)(x - 14)(x - 18)(x - 7).$$

5. Sia G un gruppo in cui ogni elemento $a \in G$ soddisfa la relazione $a^2 = 1$. Dimostrare che G è abeliano.

Risoluzione:

Bisogna dimostrare che per ogni $a, b \in G$ si ha $ab = ba$.

Siano dunque a e b due elementi qualsiasi in G. Allora $ab \in G$ e quindi $a^2 = 1 = b^2 = (ab)^2$. Segue

$$1 = (ab)^2 = (ab)(ab) = abab$$

e moltiplicando ambo i mebri a destra per ba otteniamo l'uguaglianza da dimostrare

$$ba = ababba = abab^2a = aba^2 = ab.$$