Compito di Istituzioni di Algebra Superiore di gennaio 2007

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

Risoluzione:
(a) $\alpha - 3 = i\sqrt{2}$
$(\alpha - 3)^2 = -2$
$\alpha^2 - 6\alpha + 11 = 0$.

Pertanto α è radice del polinomio $x^2 - 6x + 11 \in \mathbb{Q}[x]$. Questo polinomio è monico e le sue due radici sono α e $3 - i\sqrt{2}$, 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 $2-\alpha$ dividiamo il polinomio minimo di α per $2-x$ (ottenuto sostituendo x ad α). La divisione con resto dà

$$x^2 - 6x + 11 = (-x + 2)(-x + 4) + 3$$

da cui sostituendo α ad x si ha

$$0 = \alpha^2 - 6\alpha + 11 = (2 - \alpha)(4 - \alpha) + 3$$

e

$$(2 - \alpha)\frac{(4 - \alpha)}{-3} = 1.$$

Pertanto $(2 - \alpha)^{-1} = (\alpha - 4)/3$.

(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 $x^2 - 6x + 11$ su $\mathbb{Q}$. Infatti le due radici del polinomio sono α e $3 - i\sqrt{2} = 6 - \alpha$ e chiaramente $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, 6 - \alpha)$.

2. Sia $f(x) = x^4 - 4x^2 - 5 \in \mathbb{Q}[x]$.
(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) Si ha che $f = (x^2 - 5)(x^2 + 1)$. Quindi le radici di f sono $\pm\sqrt{5}$ e $\pm i$. Quindi $\Sigma = \mathbb{Q}(\sqrt{5}, i)$.

(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 $|\Sigma : \mathbb{Q}|$.

$$|\Sigma : \mathbb{Q}| = |\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}(\sqrt{5})||\mathbb{Q}(\sqrt{5}) : \mathbb{Q}|.$$

Il polinomio minimo di i su $\mathbb{Q}(\sqrt{5})$ è x^2+1: infatti è un polinomio monico a coefficienti in $\mathbb{Q}$ che ha i come radice ed è irriducibile su $\mathbb{Q}(\sqrt{5})$ perchè è un poliomio di grado due con due radici non reali (e quindi non ha radici in $\mathbb{Q}(\sqrt{5}) \subset \mathbb{R}$). Quindi $|\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}(\sqrt{5})| = 2$.
Il polinomio minimo di $\sqrt{5}$ su $\mathbb{Q}$ è $x^2 - 5$, polinomio monico a coefficienti in $\mathbb{Q}$ che si annulla in $\sqrt{5}$ e irriducibile su $\mathbb{Q}$ perchè di grado 2 e privo di radici in $\mathbb{Q}$. Quindi $|\mathbb{Q}(\sqrt{5}) : \mathbb{Q}| = 2$. Così, $|\Sigma : \mathbb{Q}| = 2 \cdot 2 = 4$ e $|Gal(\Sigma : \mathbb{Q})| = 4$.
Gli elementi di $Gal(\Sigma : \mathbb{Q})$ sono unicamente determinati dalla loro azione su $\sqrt{5}$ e i. Sappiamo inoltre che ogni elemento di $Gal(\Sigma : \mathbb{Q})$ manda una radice di un polinomio a coefficienti in $\mathbb{Q}$ in un'altra radice dello stesso polinomio. Quindi gli elementi di $Gal(\Sigma : \mathbb{Q})$ sono:

$$\sigma_1 = id, \qquad \sigma_2 : \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ i \mapsto i \end{cases},$$

$$\sigma_3 : \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ i \mapsto -i \end{cases}, \quad \sigma_4 : \begin{cases} \sqrt{5} \mapsto \sqrt{5} \\ i \mapsto -i \end{cases}$$

Scritti come permutazioni sulle radici di f sono quindi:

$$\sigma_1 = id, \sigma_2 = (\sqrt{5}, -\sqrt{5}), \sigma_3 = (\sqrt{5}, -\sqrt{5})(i, -i), \sigma_4 = (i, -i).$$

(c) Per il teorema di corrispondenza di Galois, il reticolo dei sottocampi di Σ è in corrispondenza biunivoca con il reticolo dei sottogruppi di $Gal(\Sigma : \mathbb{Q})$. Dal punto (b) si ricava che $Gal(\Sigma : \mathbb{Q})$ è isomorfo al gruppo di Klein e quindi contiene, oltre al sottogruppo identico e a sè stesso, tre sottogruppi di ordine 2. Si ottiene che i sottocampi di Σ sono: Σ, $\mathbb{Q}$ e

$$\Sigma_{\langle\sigma_2\rangle} = \{a \in \Sigma \mid \sigma_2(a) = a\},$$

$$\Sigma_{\langle\sigma_3\rangle} = \{a \in \Sigma \mid \sigma_3(a) = a\},$$

$$\Sigma_{\langle\sigma_4\rangle} = \{a \in \Sigma \mid \sigma_4(a) = a\}.$$

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 $|\Sigma_{\langle\sigma_i\rangle} : \mathbb{Q}| = 2$ per $i = 2, 3, 4$.

Consideriamo prima $\Sigma_{\langle\sigma_2\rangle}$. Chiaramente l'automorfismo σ_2 lascia fissa la radice i. Perciò $i \in \Sigma_{\langle\sigma_2\rangle}$ e $\mathbb{Q}(i) \subseteq \Sigma_{\langle\sigma_i\rangle}$. D'altra parte $|\mathbb{Q}(i) : \mathbb{Q}| = 2 = |\Sigma_{\langle\sigma_2\rangle} : \mathbb{Q}|$. Quindi $\Sigma_{\langle\sigma_2\rangle} = \mathbb{Q}(i)$. Con ragionamento analogo si dimostra che $\Sigma_{\langle\sigma_4\rangle} = \mathbb{Q}(\sqrt{5})$ e $\Sigma_{\langle\sigma_3\rangle} = \mathbb{Q}(i\sqrt{5})$.

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

3. Dare una costruzione esplicita del campo F di ordine 8.
Dire se F ha estensioni di grado 2 e se è algebricamente chiuso, motivando adeguatamente le risposte.
Descrivere il reticolo dei sottocampi di F e il gruppo $Aut(F)$.

Risoluzione:

Una costruzione esplicita del campo F di ordine 8 si ottiene come

$$\frac{\mathbb{Z}_2[x]}{\langle f\rangle}$$

dove f è un polinomio irriducibile di grado 3 in $\mathbb{Z}_2[x]$. Come f si può scegliere $x^3 + x + 1$, che è irriducibile perchè di grado 3 e privo di radici in $\mathbb{Z}_2$. Quindi

$$\frac{\mathbb{Z}_2[x]}{\langle x^3 + x + 1\rangle} = \mathbb{Z}_2(\alpha)$$

con α radice di f.

F ha estensioni di grado 2. Infatti i teoremi di esistenza e struttura dei campi finiti ci assicurano che esiste un campo finito H di ordine 64 e questo contiene un sottocampo H_1 di ordine 8. Per l'unicità a meno di isomorfismo di ogni campo finito di ordine fissato, il sottocampo H_1 è isomorfo a F e quindi H è un'estensione di F (cioè esiste un monomorfismo di campi da F in H). Sia α un elemento di H che non sta in F. Poichè $|H : F| = 2$, α è algebrico su F e il polinomio minimo di α su F è un polinomio irriducibile in $F[x]$ di grado 2. Pertanto F non è algebricamente chiuso.

F ha un unico sottocampo di ordine 2^m per ogni m divisore di 3. Quindi gli unici sottocampi di F sono F e $\mathbb{Z}_2$. Il gruppo degli automorfismi di F è un gruppo ciclico di ordine 3 generato dall'automorfismo di Frobenius $\varphi : F \to F; x \mapsto x^2$.

4. Sia $f = x^3 + 15x^2 - 6x \in \mathbb{Z}_p[x]$.
(a) Determinare per quali valori del primo p il polinomio f ha radici multiple.
(b) Per i valori di p calcolati al punto (a), determinare tutte le radici di f.

Risoluzione:
(a) Il polinomio f ha radici multiple se e solo se il massimo comun divisore (f, f') tra f e la sua derivata formale f' è un polinomio di grado positivo. Calcoliamo quindi f' e (f, f').

$$f' = 3x^2 + 30x - 6$$

Quindi se $p = 3$, $f' = 0$ e $(f, f') = f$: f ha radici multiple. Se $p \neq 3$, calcoliamo (f, f') utilizzando il metodo delle divisioni successive. Si ha

$$f = f' \cdot \frac{(x+5)}{3} - 54x.$$

Poichè il resto della divisione è $-54x$, si ha che se $p = 2, 3$, allora $-54x = 0$ e quindi f' divide f. Quindi anche per $p = 2$, f ha radici multiple.

Se infine $p \neq 2, 3$, facendo un'altra divisione (f' diviso $-54x$) otteniamo il resto -2 che, essendo una costante diversa da 0 (perchè $p \neq 2$) è il massimo comun divisore (f, f'). Pertanto in questo caso f non ha radici multiple.

Quindi, riassumendo, si ha che f ha radici multiple per $p = 2, 3$.

(b) Caso $p = 2$. Si ha che $f = x^3 + x^2 = x^2(x + 1)$. Quindi le radici di f sono 0 (di molteplicità 2) e 1.

Caso $p = 3$. Si ha che $f = x^3$ e quindi f ha una sola radice, 0, di molteplicità 3.

5. Sia G un grupo finito e siano H e K due suoi sottogruppi, con $K \leq H$. Si dimostri che $[G : K] = [G : H][H : K]$.

Risoluzione:
Per il teorema di Lagrange abbiamo che

$$|G| = |K|[G : K], |G| = |H|[G : H], |H| = |K|[H : K].$$

Sostituendo opportunamente si ottiene:

$$|K|[G : K] = |H|[G : H] = |K|[H : K][G : K]$$

e quindi semplificando $|K|$

$$[G : K] = [G : H][H : K].$$