Compito di Istituzioni di Algebra Superiore dell' 11 settembre 2008

1. Sia $u = 3 - i\sqrt{2} \in \mathbb{C}$.

a) Determinare il polinomio minimo di u su $\mathbb{Q}$;

b) scrivere $(2-u)^{-1}$ come polinomio in u a coefficienti in $\mathbb{Q}$;

c) dire se $\mathbb{Q}(u)$ è estensione normale di $\mathbb{Q}$.

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

Pertanto u è radice del polinomio $x^2 - 6x + 11 \in \mathbb{Q}[x]$. Le radici di questo polinomio sono $3 \pm i\sqrt{2} \notin \mathbb{Q}$. Quindi, essendo di grado 2 e privo di radici in $\mathbb{Q}$, è irriducibile in $\mathbb{Q}[x]$. Così $x^2 - 6x + 11$ è il polinomio minimo di u su $\mathbb{Q}$.

(b) Facendo la divisione euclidea di $x^2 - 6x + 11$ per $x - 2$ e sostituendo u al posto di x si ha

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

da cui
$(u-2)(u-4) = -3$
$(2-u)(u-4)/3 = 1$
$(2-u)^{-1} = (u-4)/3$.

(c) $\mathbb{Q}(u)$ è estensione normale di $\mathbb{Q}$ perchè estensione di grado 2 oppure perchè è campo di spezzamento del polinomio $x^2 - 6x + 11$.

2. Si consideri il polinomio $f(x) = x^3 - 5 \in \mathbb{Q}[x]$.

a) Si determini il campo di spezzamento Σ di $f(x)$ su $\mathbb{Q}$ e si calcoli $|\Sigma : \mathbb{Q}|$;

b) si scrivano gli elementi di $\mathrm{Gal}(\Sigma : \mathbb{Q})$ come permutazioni sulle radici di $f(x)$ e si dica a quale gruppo è isomorfo $\mathrm{Gal}(\Sigma : \mathbb{Q})$;

d) si determinino i sottocampi di Σ specificando quali di essi sono estensioni di Galois di $\mathbb{Q}$.

Risoluzione:

(a) Le radici di f sono $\sqrt[3]{5}$, $\omega\sqrt[3]{5}$ e $\omega^2\sqrt[3]{5}$ con ω radice primitiva terza dell'unità. Quindi $\Sigma = \mathbb{Q}(\sqrt[3]{5}, \omega)$. Abbiamo che $|\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}| = 3$ in quanto estensione semplice con polinomio minimo di $\sqrt[3]{5}$ su $\mathbb{Q}$ uguale a $x^3 - 5$. Osserviamo poi che il polinomio minimo di ω su $\mathbb{Q}(\sqrt[3]{5})$ è $x^2 + x + 1$ in quanto questo polinomio ha ω come radice ed è irriducibile su $\mathbb{Q}(\sqrt[3]{5})$ perchè è irriducibile in $\mathbb{R}[x]$. Quindi per la formula dei gradi

$$|\mathbb{Q}(\sqrt[3]{5}, \omega) : \mathbb{Q}| = |\mathbb{Q}(\sqrt[3]{5}, \omega) : \mathbb{Q}(\sqrt[3]{5})||\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}| = 3 \cdot 2 = 6.$$

(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 $|\Sigma : \mathbb{Q}| = 6$.

Gli elementi di $Gal(\Sigma : \mathbb{Q})$ sono unicamente determinati dalla loro azione su $\sqrt[3]{5}$ e ω. 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:

$$\sigma_1 = id, \qquad \sigma_2 : \begin{cases} \sqrt[3]{5} \mapsto \sqrt[3]{5} \\ \omega \mapsto \omega^2 \end{cases},$$

$$\sigma_3 : \begin{cases} \sqrt[3]{5} \mapsto \omega\sqrt[3]{5} \\ \omega \mapsto \omega \end{cases}, \quad \sigma_4 : \begin{cases} \sqrt[3]{5} \mapsto \omega\sqrt[3]{5} \\ \omega \mapsto \omega^2 \end{cases}$$

$$\sigma_5 : \begin{cases} \sqrt[3]{5} \mapsto \omega^2\sqrt[3]{5} \\ \omega \mapsto \omega \end{cases}, \quad \sigma_6 : \begin{cases} \sqrt[3]{5} \mapsto \omega^2\sqrt[3]{5} \\ \omega \mapsto \omega^2 \end{cases}$$

Scritti come permutazioni sulle radici di f sono quindi:

$$\sigma_1 = id, \sigma_2 = (\omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}), \sigma_3 = (\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}),$$

$$\sigma_4 = (\sqrt[3]{5}, \omega\sqrt[3]{5}),$$

$$\sigma_5 = (\sqrt[3]{5}, \omega^2\sqrt[3]{5}, \omega\sqrt[3]{5}), \sigma_6 = (\sqrt[3]{5}, \omega^2\sqrt[3]{5}).$$

Segue che $Gal(\Sigma : \mathbb{Q}) \cong$ Sym(3).

(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

$$\Sigma_{\langle\sigma_2\rangle} = \{a \in \Sigma \mid \sigma_2(a) = a\},$$
$$\Sigma_{\langle\sigma_4\rangle} = \{a \in \Sigma \mid \sigma_4(a) = a\},$$
$$\Sigma_{\langle\sigma_6\rangle} = \{a \in \Sigma \mid \sigma_6(a) = a\},$$
$$\Sigma_{\langle\sigma_3\rangle} = \{a \in \Sigma \mid \sigma(a) = a \,\forall\sigma \in \langle\sigma_3\rangle\} = \{a \in \Sigma \mid \sigma_3(a) = a\}.$$

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 $i = 2, 4, 6$ e $|\Sigma_{\langle\sigma_3\rangle} : \mathbb{Q}| = 2$.

Consideriamo prima $\Sigma_{\langle\sigma_2\rangle}$. Chiaramente l'automorfismo σ_2 lascia fissa la radice $\sqrt[3]{5}$. Perciò $\sqrt[3]{5} \in \Sigma_{\langle\sigma_2\rangle}$ e $\mathbb{Q}(\sqrt[3]{5}) \subseteq \Sigma_{\langle\sigma_2\rangle}$. D'altra parte $|\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}| = 3 = |\Sigma_{\langle\sigma_2\rangle} : \mathbb{Q}|$. Quindi $\Sigma_{\langle\sigma_2\rangle} = \mathbb{Q}(\sqrt[3]{5})$. Con ragionamento analogo si dimostra che $\Sigma_{\langle\sigma_4\rangle} = \mathbb{Q}(\omega^2\sqrt[3]{5})$ e $\Sigma_{\langle\sigma_6\rangle} = \mathbb{Q}(\sqrt[3]{5}\omega)$.

Infine consideriamo $\Sigma_{\langle\sigma_3\rangle}$. Si verifica che $\omega \in \Sigma_{\langle\sigma_3\rangle}$ e $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2$. Allora $\mathbb{Q}(\omega) \subseteq \Sigma_{\langle\sigma_3\rangle}$ e poichè hanno lo stesso grado su $\mathbb{Q}$ devono coincidere: $\Sigma_{\langle\sigma_3\rangle} = \mathbb{Q}(\omega)$.

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. Di questi, $\mathbb{Q}(\omega)$ è l'unica estensione di Galois di $\mathbb{Q}$ in quanto corrisponde all'unico sottogruppo normale proprio non banale di Sym(3).

3. Sia p un primo e F un campo finito di ordine p^n.

a) Determinare n nel caso in cui la dimensione di F come spazio vettoriale sul suo sottocampo primo sia 4.

b) Nelle ipotesi del punto (a), descrivere il reticolo dei sottocampi di F.

c) Per $p = 5$ dire se F contiene una radice primitiva tredicesima dell'unità.

Risoluzione:

Risoluzione:

(a) Il sottocampo primo di F è $\mathbb{Z}_p$ e quindi $F \cong (\mathbb{Z}_p)^4$ come spazio vettoriale. Cosi $|F| = p^4$ e $n = 4$.

(b) F ha un unico sottocampo di ordine p^m per ogni m divisore di 4. Quindi gli unici sottocampi di F sono F, $\mathbb{Z}_p$ e un campo intermedio di ordine p^2.

(c) Per $p = 5$ abbiamo che $|F| = 5^4 = 625$. Esso contiene una radice primitiva tredicesima dell'unità se e solo se contiene un elemento di ordine moltiplicativo 13. Poichè il gruppo moltiplicativo di F è ciclico questo si verifica se e solo se 13 divide il suo ordine cioè $5^4 - 1 = 624 = 2^4 \cdot 3 \cdot 13$. Quindi F contiene una radice primitiva tredicesima dell'unità.

4. Scomporre il polinomio $x^{18} - 1$ in fattori irriducibili in $\mathbb{Q}[x]$ e in $\mathbb{Z}_3[x]$.

Risoluzione:

$$\begin{gathered} x^{18} - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6 \Phi_9 \Phi_{18} = (x^9 - 1)(x^9 + 1) = \\ = (x^3 - 1)(x^6 + x^3 + 1)(x^3 + 1)(x^6 - x^3 + 1) = \\ = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)(x + 1)(x^2 - x + 1)(x^6 - x^3 + 1) \end{gathered}$$

Questi fattori sono irriducibili in $\mathbb{Q}[x]$ perche' sono polinomi ciclotomici e essi sono irriducibili per il teorema di Gauss.

Consideriamoli ora come polinomi in $\mathbb{Z}_3[x]$. Abbiamo

$$x^{18} - 1 = (x^9 + 1)(x^9 - 1) = (x^3 - 1)^3 (x^3 + 1)^3 = (x - 1)^9 (x + 1)^9.$$

5. Sia R un anello commutativo con unità. Dimostrare che R è un campo se e solo se gli unici suoi ideali sono R e $\{0_R\}$.

Risoluzione:

Sia R un campo e sia I un ideale di R, $I \neq \{0\}$. Allora I contiene un elemento $a \neq 0$, e a è invertibile perchè R è un campo. Quindi per ogni $r \in R$ abbiamo

$$r = r(a^{-1}a) = (ra^{-1})a \in I$$

cioè $I = R$.

Viceversa supponiamo che R non abbia ideali non banali. Sia a un elemento di $R \setminus 0$. Allora Ra è un ideale diverso dall'ideale nullo e quindi $Ra = R$. Pertanto, $1 \in Ra$, ovvero esiste $r \in R$ tale che $ra = 1$, cioè $r = a^{-1}$.