Compito di Istituzioni di Algebra Superiore di dicembre 2007

1. Sia $\alpha = \cos \pi/4 + i \sin \pi/4 \in \mathbb{C}$.
(a) Determinare il polinomio minimo di α su $\mathbb{Q}$.
(b) Dimostrare che $-i \in \mathbb{Q}(\alpha)$ e calcolare $|\mathbb{Q}(\alpha) : \mathbb{Q}(-i)|$.
(c) Esprimere $-i$ come potenza di α.
(d) Determinare l'inverso moltiplicativo di α.

Risoluzione:
(a) $\alpha = \sqrt{2}/2 + i\sqrt{2}/2$
$4\alpha^2 = (\sqrt{2} + i\sqrt{2})^2 = 2(1 + 2i - 1) = 4i$
$\alpha^2 = i$
$\alpha^4 = -1$.

Pertanto α è radice del polinomio $x^4 + 1 \in \mathbb{Q}[x]$. È facile verificare che $x^4 + 1 = \phi_8(x)$ e quindi il polinomio è irriducibile su $\mathbb{Q}$ per il teorema di Gauss sull'irriducibilità dei polinomi ciclotomici. Quindi x^4+1 è il polinomio minimo di α su $\mathbb{Q}$.

(b) Dai calcoli fatti al punto (a) segue che $\alpha^2 = i$. Quindi i e $-i$ stanno in $\mathbb{Q}(\alpha)$. Per calcolare $|\mathbb{Q}(\alpha) : \mathbb{Q}(-i)|$ possiamo utilizzare la formula dei gradi:

$$|\mathbb{Q}(\alpha) : \mathbb{Q}| = |\mathbb{Q}(\alpha) : \mathbb{Q}(-i)||\mathbb{Q}(-i) : \mathbb{Q}|.$$

Dal punto (a) sappiamo che $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$. D'altra parte $\mathbb{Q}(-i) = \mathbb{Q}(i)$ e $|\mathbb{Q}(i) : \mathbb{Q}| = 2$ essendo il polinomio minimo di i su $\mathbb{Q}$ uguale a $x^2 + 1$. Segue che $|\mathbb{Q}(\alpha) : \mathbb{Q}(-i)| = 2$.

(c) Abbiamo che $i = \alpha^2$ e $\alpha^4 = -1$. Quindi $-i = \alpha^6$.

(d) Elevando al quadrato la relazione $\alpha^4 = -1$ otteniamo $\alpha^8 = 1$, da cui si ha che

$$\alpha^{-1} = \alpha^7 = \alpha^4\alpha^3 = -\alpha^3.$$

2. Sia $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.
(a) Determinare il campo di spezzamento Σ di f su $\mathbb{Q}$.
(b) Si calcoli $|Gal(\Sigma : \mathbb{Q})|$ e si scrivano gli elementi di $Gal(\Sigma : \mathbb{Q})$ come permutazioni delle radici di f.
(c) Dire se $\mathbb{Q}(\sqrt[4]{2})$ è estensione normale di $\mathbb{Q}$ se il sottogruppo di $Gal(\Sigma : \mathbb{Q})$

corrispondente a $\mathbb{Q}(\sqrt[4]{2})$ è un sottogruppo normale di $Gal(\Sigma : \mathbb{Q})$, motivando la risposta.

Risoluzione:

(a) Le radici di f sono $\pm\sqrt[4]{2}$ e $\pm i\sqrt[4]{2}$. Quindi $\Sigma = \mathbb{Q}(\sqrt[4]{2}, i)$.

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

$$|\Sigma : \mathbb{Q}| = |\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}| = |\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})||\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}|.$$

Il polinomio minimo di i su $\mathbb{Q}(\sqrt[4]{2})$ è x^2+1: infatti è un polinomio monico a coefficienti in $\mathbb{Q}$ che ha i come radice ed è irriducibile su $\mathbb{Q}(\sqrt[4]{2})$ perchè è un poliomio di grado due con due radici non reali (e quindi non ha radici in $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$). Quindi $|\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})| = 2$.

Il polinomio minimo di $\sqrt[4]{2}$ su $\mathbb{Q}$ è $x^4 - 2$. Chiaramente è un polinomio monico a coefficienti in $\mathbb{Q}$ che si annulla in $\sqrt[4]{2}$. Bisogna verificare che è irriducibile su $\mathbb{Q}$. Dal punto (a) segue che è privo di radici in $\mathbb{Q}$. Se ammettesse una fattorizzazione come prodotto di due polinomi di secondo grado avremmo che

$$x^4-2 = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(b+ac+d)x^2+(ad+bc)x+bd$$

da cui il sistema

$$\begin{cases} a+c=0 \\ b+ac+d=0 \\ ad+bc=0 \\ bd=-2 \end{cases} \qquad \begin{cases} a=-c \\ b-a^2+d=0 \\ a(d-b)=0 \\ bd=-2 \end{cases}$$

Poichè l'equazione $bd = -2$ non ha soluzioni intere se $b = \pm d$, deve essere $b \neq \pm d$ e quindi dalla terza equazione si ricava $a = 0$. Allora dalla seconda equazione di ottiene $b = -d$, una contraddizione. Quindi il sistema non ha soluzioni intere e pertanto il polinomio $x^4 - 2$ è irriducibile su $\mathbb{Q}$ (per il Lemma di Gauss).

Così, $|\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| = 4$, $|\Sigma : \mathbb{Q}| = 2 \cdot 4 = 8$ e $|Gal(\Sigma : \mathbb{Q})| = 8$.

Gli elementi di $Gal(\Sigma : \mathbb{Q})$ sono unicamente determinati dalla loro azione su $\sqrt[4]{2}$ 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:

$$\sigma_1 = id, \qquad \sigma_2 : \begin{cases} \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto i \end{cases},$$

$$\sigma_3 : \begin{cases} \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto -i \end{cases}, \quad \sigma_4 : \begin{cases} \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ i \mapsto i \end{cases}$$

$$\sigma_5 : \begin{cases} \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ i \mapsto -i \end{cases}, \quad \sigma_6 : \begin{cases} \sqrt[4]{2} \mapsto -i\sqrt[4]{2} \\ i \mapsto i \end{cases}$$

$$\sigma_7 : \begin{cases} \sqrt[4]{2} \mapsto -i\sqrt[4]{2} \\ i \mapsto -i \end{cases}, \quad \sigma_8 : \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto -i \end{cases}$$

Scritti come permutazioni sulle radici di f sono quindi:

$$\sigma_1 = id, \sigma_2 = (\sqrt[4]{2}, -\sqrt[4]{2})(i\sqrt[4]{2}, -i\sqrt[4]{2}), \sigma_3 = (\sqrt[4]{2}, -\sqrt[4]{2}),$$

$$\sigma_4 = (\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}).$$

$$\sigma_5 = (\sqrt[4]{2}, i\sqrt[4]{2})(-\sqrt[4]{2}, -i\sqrt[4]{2}), \sigma_6 = (\sqrt[4]{2}, -i\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}),$$

$$\sigma_7 = (\sqrt[4]{2}, -i\sqrt[4]{2})(-\sqrt[4]{2}, -i\sqrt[4]{2}), \sigma_8 = (i\sqrt[4]{2}, -i\sqrt[4]{2}).$$

(c) Osserviamo che $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$. Infatti se fosse $i\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$ si avrebbe la contraddizione

$$i = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}} \in \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}.$$

Allora il polinomio $x^4 - 2$ ha una radice in $\mathbb{Q}(\sqrt[4]{2})$ ma non tutte le sue radici stanno in $\mathbb{Q}(\sqrt[4]{2})$. Per definizione questo significa che $\mathbb{Q}(\sqrt[4]{2})$ non è estensione normale di $\mathbb{Q}$. Per il teorema di corrispondenza di Galois il sottogruppo del gruppo di Galois corrispondente a $\mathbb{Q}(\sqrt[4]{2})$ non è un sottogruppo normale.

3. (a) Dimostrare che il polinomio $x^3 - 2$ è irriducibile in $\mathbb{Z}_7[x]$.
(b) Dare una costruzione esplicita del campo F di ordine 343.
(c) Descrivere il reticolo dei sottocampi di F e il gruppo $Aut(F)$.

Risoluzione:

(a) Il polinomio $f = x^3 - 2$ è di grado 3 e quindi è irriducibile in $\mathbb{Z}_7[x]$ se e solo se non ha radici in $\mathbb{Z}_7$. Verifichiamolo direttamente:
$f(0) = -2 \neq 0$, $f(1) = -1 \neq 0$, $f(2) = 6 \neq 0$, $f(3) = 25 = 4 \neq 0$, $f(4) = f(-3) = -29 = -1 \neq 0$, $f(5) = f(-2) = -10 = -3 \neq 0$, $f(6) = f(-1) = -3 \neq 0$. Quindi il polinomio è irriducibile.

(b) Un campo F di ordine 343 è un'estensione di grado 3 del campo $\mathbb{Z}_7$. Possiamo quindi costruire F così:

$$F = \frac{\mathbb{Z}_7[x]}{\langle x^3 - 2 \rangle} = \mathbb{Z}_7[\alpha]$$

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

(c) F ha un unico sottocampo di ordine 7^m per ogni m divisore di 3. Quindi gli unici sottocampi di F sono F e $\mathbb{Z}_7$. Il gruppo degli automorfismi di F è un gruppo ciclico di ordine 3 generato dall'automorfismo di Frobenius $\varphi : F \to F; x \mapsto x^7$.

4. Calcolare il polinomio ciclotomico $\Phi_{12}(x)$ e fattorizzarlo in $\mathbb{Z}_{37}[x]$.

Risoluzione:

$$\Phi_{12}(x) = \frac{x^{12} - 1}{\Phi_1 \Phi_2 \Phi_3 \Phi_4 \Phi_6} = \frac{(x^6 - 1)(x^6 + 1)}{(x^6 - 1)\Phi_4} = \frac{x^6 + 1}{x^2 + 1} = \frac{(x^2 + 1)(x^4 - x^2 + 1)}{x^2 + 1}$$

$$= x^4 - x^2 + 1.$$

Osserviamo che $\Phi_{12}(x)$ ha radici nel campo $\mathbb{Z}_{37}$ se e solo se $\mathbb{Z}_{37}$ contiene radici primitive dodicesime dell'unità, cioè elementi il cui ordine moltiplicativo è 12. Il gruppo moltiplicativo del campo $\mathbb{Z}_{37}$ è un gruppo ciclico di ordine 36 e quindi contiene elementi di ordine n per ogni n divisore di 36. In particolare contiene elementi di ordine 12, cioè radici di $\Phi_{12}(x)$. Quanti sono questi elementi? Sempre dalla struttura dei gruppi ciclici sappiamo che tutti gli elementi di ordine 12 sono contenuti nell'unico sottogruppo di ordine 12 di $\mathbb{Z}_{37}^*$ e ne sono i generatori. Il numero dei generatori di un gruppo

ciclico di ordine 12 è $\varphi(12) = \varphi(3)\varphi(4) = 2 \cdot 2 = 4$. Pertanto le radici di $\Phi_{12}(x)$ in $\mathbb{Z}_{37}$ sono 4, pari al grado del polinomio; quindi $\Phi_{12}(x)$ si fattorizza completamente in $\mathbb{Z}_{37}[x]$. Con un po' di pazienza si trova ad esempio che 14 ha periodo moltiplicativo 12 in $\mathbb{Z}_{37}$. Dopodichè gli altri elementi di ordine 12 sono $14^5 = 29, 14^7 = 23, 14^{11} = 8$ (si noti che gli esponenti sono tutti i numeri naturali minori di 12 e coprimi con 12). Quindi la fattorizzazione di $\Phi_{12}(x)$ è

$$\Phi_{12}(x) = (x-14)(x-29)(x-23)(x-8).$$

5. Sia F un campo finito di caratteristica p e sia $\phi : F \to F$ la mappa $x \mapsto x^a$. Provare che ϕ è un automofismo di F se e solo se a è una potenza di p.

Risoluzione:

Osserviamo che poichè F è commutativo si ha sempre

$$\phi(xy) = (xy)^a = x^a y^a = \phi(x)\phi(y).$$

Quindi si tratta di dimostrare che

$$\phi(x+y) = \phi(x) + \phi(y)$$

se e solo se a è una potenza di p. Per la formula del binomio si ha che

$$\phi(x+y) = (x+y)^a = \sum_{i=0}^{a} \binom{a}{i} x^i y^{a-i} = y^a + \sum_{i=1}^{a-1} \binom{a}{i} x^i y^{a-i} + x^a =$$

$$= \phi(x) + \phi(y) + \sum_{i=1}^{a-1} \binom{a}{i} x^i y^{a-i}$$

Il coefficiente binomiale $\binom{a}{i}$ è divisibile per p se e solo se a è una potenza di p e quindi il termine $\sum_{i=1}^{a-1} \binom{a}{i} x^i y^{a-i}$ è zero in $F[x]$ (che è un anello di caratteristica p) se e solo se a è una potenza di p. Pertanto si ha che ϕ è un omomorfismo se e solo se a è una potenza di p. Poichè ogni elemento non nullo di F è invertibile, è immediato che ϕ è iniettivo ed, essendo F finito, segue che è anche suriettivo.