Corso di Algebra 2 - a.a. 2014-2015

Prova scritta del 22.9.2015

Esercizio 1. *Dire quali delle seguenti estensioni sono normali e determinarne il gruppo di Galois:*

1. $\mathbb{Q}(i,\omega):\mathbb{Q}$, *dove* $\omega = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$.
2. $\mathbb{Q}(\alpha):\mathbb{Q}$, *dove* $\alpha = 11^{\frac{1}{3}}$.
3. $\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}$

Soluzione. 1. L'estensione $\mathbb{Q}(i,\omega):\mathbb{Q}$ è normale perché è un campo di spezzamento del polinomio $f(X) = (X^2+1)(X^2+X+1)$. Infatti le radici di f in $\mathbb{C}$ sono $\pm i$, ω, ω^2, quindi un campo di spezzamento di f su $\mathbb{Q}$ è $\mathbb{Q}(i,\omega)$. Osserviamo che $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, quindi $\mathbb{Q}(i,\omega) = \mathbb{Q}(i,\sqrt{3})$.

Abbiamo $[\mathbb{Q}(i,\omega):\mathbb{Q}] = [\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}(\sqrt{3})]\cdot[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 4$. Infatti i è radice di $X^2+1 \in \mathbb{Q}(\sqrt{3})[X]$ e $i \notin \mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$, quindi $[\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}(\sqrt{3})] = 2$. Inoltre $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$ perché X^2-3 è il polinomio minimo di $\sqrt{3}$ su $\mathbb{Q}$. Questo ci dice anche che X^2+1 è irriducibile in $\mathbb{Q}(\sqrt{3})[X]$ e, usando il fatto che $4 = [\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}(i)]\cdot[\mathbb{Q}(i):\mathbb{Q}]$, abbiamo anche che $[\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}(i)] = 2$ e quindi X^2-3 è irriducibile su $\mathbb{Q}(i)$. Sia K il gruppo di Galois di $\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}$, abbiamo $|K| = [\mathbb{Q}(i,\omega):\mathbb{Q}] = 4$. Poiché X^2+1 è irriducibile in $\mathbb{Q}(\sqrt{3})[X]$, il gruppo di Galois H di $\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}(\sqrt{3})$ agisce transitivamente sulle radici di X^2+1, quindi esiste $\sigma \in H$ tale che $\sigma(i) = -i$. Dato che $H \subset K$, abbiamo che $\sigma \in K$ e $\sigma(i) = -i$, $\sigma(\sqrt{3}) = \sqrt{3}$. In modo analogo si vede che esiste $\tau \in K$ tale che $\tau(\sqrt{3}) = -\sqrt{3}$, $\tau(i) = i$. $\sigma\circ\tau(i) = \sigma(i) = -i = \tau\circ\sigma(i)$, $\sigma\circ\tau(\sqrt{3}) = \sigma(-\sqrt{3}) = -\sqrt{3} = \tau\circ\sigma(\sqrt{3})$, quindi $\sigma\circ\tau = \tau\circ\sigma$. Pertanto il sottogruppo generato da σ e τ in K è isomorfo a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ e dato che K ha ordine 4, $K \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2$.

2. L'estensione $\mathbb{Q}(\alpha):\mathbb{Q}$ non è normale. Infatti il polinomio $p(X) = X^3-11$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein applicato con il primo 11. α è una radice del polinomio p e le altre radici di p sono $\omega\alpha, \omega^2\alpha$. $\omega\alpha \notin \mathbb{Q}(\alpha)$ perché altrimenti si avrebbe $\omega \in \mathbb{Q}(\alpha) \subset \mathbb{R}$, mentre $\omega \notin \mathbb{R}$, quindi l'estensione non è normale.

Il gruppo di Galois di $\mathbb{Q}(\alpha):\mathbb{Q}$ è banale perché per ogni σ nel gruppo di Galois $\sigma(\alpha)$ è una radice di p e sta in $\mathbb{Q}(\alpha) \subset \mathbb{R}$, quindi $\sigma(\alpha) = \alpha$.

3. $\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}$ è normale perché è un campo di spezzamento di $g(X) = (X^3-11)(X^2+1)(X^2+X+1)$. Infatti le radici di g sono $\alpha, \alpha\omega, \alpha\omega^2, i, -i, \omega, \omega^2$.

$[\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}] = [\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}(i,\omega)]\cdot[\mathbb{Q}(i,\omega):\mathbb{Q}] \leq 12$ perché abbiamo mostrato sopra che $[\mathbb{Q}(i,\omega):\mathbb{Q}] = 4$ e $[\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}(i,\omega)] \leq 3$ dato che α è radice di $X^3-11 \in \mathbb{Q}(i,\omega)[X]$. Inoltre questo ci dice che $4|[\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}]$. Si ha $[\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}] = [\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}(\alpha)]\cdot[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}(\alpha)]\cdot 3$ perché il polinomio minimo di α su $\mathbb{Q}$ è X^3-11. Quindi $3,4|[\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}] \leq 12$, pertanto $[\mathbb{Q}(\alpha,i,\omega):\mathbb{Q}] = 12$.

Inoltre abbiamo anche così dimostrato che $[\mathbb{Q}(\alpha, i, \omega) : \mathbb{Q}(i, \omega)] = 3$ e quindi $X^3 - 11$ è irriducibile su $\mathbb{Q}(i, \omega)$.

Sia G il gruppo di Galois di $\mathbb{Q}(\alpha, i, \omega) : \mathbb{Q}$. L'ordine di G è il grado di $Q(\alpha, i, \omega) : \mathbb{Q}$ che è 12. Abbiamo visto che $[\mathbb{Q}(\alpha, i, \omega) : \mathbb{Q}(i, \omega)] = 3$, quindi un generatore del gruppo di Galois di $\mathbb{Q}(\alpha, i, \omega) : \mathbb{Q}(i, \omega)$ è dato dall'elemento $\sigma \in G$ di ordine 3 tale che $\sigma(i) = i$, $\sigma(\omega) = \omega$, $\sigma(\alpha) = \alpha\omega$. Analogamente guardando le estensioni $\mathbb{Q}(\alpha, i, \omega) : \mathbb{Q}(i, \alpha)$ e $\mathbb{Q}(\alpha, i, \omega) : \mathbb{Q}(\omega, \alpha)$ troviamo due elementi di ordine 2, $\tau, \epsilon \in G$ definiti da: $\tau(\alpha) = \alpha$, $\tau(i) = i$, $\tau(\omega) = \omega^2$, $\epsilon(\alpha) = \alpha$, $\epsilon(\omega) = \omega$, $\epsilon(i) = -i$. Si vede subito che ϵ e σ commutano, quindi il sottogruppo di G generato da ϵ e σ è isomorfo a $\mathbb{Z}/6\mathbb{Z}$ generato da $\eta := \epsilon \circ \sigma$ e, dato che ha indice due in G, è normale in G. Si vede poi con un semplice calcolo che $\tau \circ \eta \circ \tau^{-1} = \eta^{-1}$, quindi G è isomorfo al gruppo $\langle \eta, \tau \mid \eta^6 = 1, \tau^2 = 1, \tau \circ \eta \circ \tau^{-1} = \eta^{-1} \rangle \cong D_6$.

□

Esercizio 2. *Sia G un gruppo di cardinalità* 196*.*

1. *Dire se G è semplice.*
2. *Dire se G è risolubile.*
3. *Dare un esempio di un gruppo di cardinalità* 196 *non abeliano in cui né i 2-Sylow, né i 7-Sylow siano ciclici.*

Soluzione. 1. $|G| = 196 = 7^2 \cdot 2^2$. Il numero dei 7-Sylow è congruo a 1 modulo 7 e divide $|G|$, quindi è uguale ad 1, pertanto c'è un unico 7-Sylow H che è normale in G e la cardinalità di H è 49. Quindi G non è semplice.

2. Sia H l'unico 7-Sylow, H è normale in G, ha ordine 49 che è il quadrato di un primo, quindi H è abeliano e dunque risolubile. Consideriamo il gruppo G/H, $|G/H| = |G|/|H| = 4$, quindi G/H è abeliano e pertanto risolubile e allora anche G è risolubile.

3. H è abeliano di ordine 49 e per ipotesi non è ciclico, quindi $H \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Sia K un 2-Sylow, $|K| = 4$ e per ipotesi K non è ciclico, quindi $K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $HK = KH$ è un sottogruppo di G perché H è normale. $|H \cap K|$ deve dividere sia $|H| = 49$ che $|K| = 4$, quindi $H \cap K$ è banale e $|G| = |H| \cdot |K| = |HK|$. Quindi $G = HK$ è un prodotto semidretto. K agisce su H per coniugio, quindi abbiamo un omomorfismo $\phi : K \to Aut(H)$, $\phi(k)(h) = khk^{-1}$. Per dare un esempio di un gruppo G non abeliano dobbiamo trovare un omomorfismo ϕ come sopra non banale. $K \cong \langle x, y \mid x^2 = y^2 = 1,\ xy = yx \rangle$, $H \cong \langle \alpha, \beta \mid \alpha^7 = \beta^7 = 1,\ \alpha\beta = \beta\alpha \rangle$. Per definire ϕ, basta dare l'immagine dei generatori x, y e per definire $\phi(x)$ e $\phi(y)$ basta dare il loro valore sui generatori di di H, α e β. Definiamo ad esempio $\phi(x)(\alpha) = \beta$, $\phi(x)(\beta) = \alpha$, $\phi(y) = Id$, $\phi(x)$ e $\phi(y)$ sono chiaramente automorfismi di H. ϕ è ben definito perché $o(\phi(x)) = 2 = o(x)$, $o(\phi(y)) = 1 | o(y)$, $\phi(x) \circ \phi(y) = \phi(y) \circ \phi(x) = \phi(x)$.

Un altro esempio è il seguente: $\phi(x)(\alpha) = \alpha^{-1}$, $\phi(x)(\beta) = \beta$, $\phi(y) = Id$. □

Esercizio 3. *Sia $p(X) = X^{12} + X^6 + 1$. Determinare il gruppo di Galois di $p(X)$ su $\mathbb{F}_2$ e su $\mathbb{F}_3$.*

Soluzione. 1. Su $\mathbb{F}_2$, l'elevamento al quadrato è un omomorfismo, dunque $p(X) = (X^6 + X^3 + 1)^2$ e ci riduciamo a calcolare un campo di spezzamento di $X^6 + X^3 + 1$. Notiamo che

$$X^9 - 1 = (X^3 - 1)(X^6 + X^3 + 1),$$

dunque un campo di spezzamento è dato da $\mathbb{F}_2(\eta)$, con η una radice nona primitiva dell'unità. Il gruppo di galois G del polinomio è dunque ciclico e generato dal Frobenius $\phi\colon \mathbb{F}_2(\eta) \to \mathbb{F}_2(\eta)$. Dobbiamo dunque capire qual è l'ordine di ϕ, ossia il più piccolo intero $n \geq 1$ tale che $\phi^n(\eta) = \eta$, cioè:

$$\eta^{2^n} = \eta.$$

Esso si caratterizza anche come il più piccolo intero $n \geq 1$ tale che

$$2^n \equiv 1 \pmod 9.$$

Un calcolo diretto mostra che $n = 6$. Dunque, concludiamo che $G \cong C_6$.

2. Su $\mathbb{F}_3$, l'elevamento a terza potenza è un omomorfismo, dunque $p(X) = (X^4 + X^2 + 1)^3$. Notiamo che

$$X^6 - 1 = (X^2 - 1)(X^4 + X^2 + 1) = (X^2 - 1)^3,$$

dunque $X^4 + X^2 + 1 = (X^2 - 1)^2$. Concludiamo che

$$p(X) = (X^2 - 1)^6 = (X - 1)^6(X + 1)^6,$$

quindi si spezza completamente su $\mathbb{F}_3$, e il suo gruppo di Galois è banale. □