Corso di Algebra 2 - a.a. 2015-2016
Prova scritta del 16.1.2017

Esercizio 1
Sia $P(X) = X^4 + 3X - 3 \in \mathbb{Q}[X]$.

1. Determinare una fattorizzazione di $P(X)$ in irriducibili in $\mathbb{Q}[X]$ e in $\mathbb{F}_5[X]$.

2. Determinare il gruppo di Galois di $P(X)$ su $\mathbb{Q}$.

3. Dire se è risolubile per radicali su $\mathbb{Q}$.

4. Determinare il gruppo di Galois di $P(X)$ su $\mathbb{F}_5[X]$.

Risoluzione. 1. $P(X)$ è irriducibile in $\mathbb{Q}[X]$ grazie al criterio di Eisenstein applicato con il primo 3.

In $\mathbb{F}_5[X]$ abbiamo la seguente fattorizzazione in polinomi irriducibili:

$$X^4 + 3X - 3 = (X - 4)(X^3 + 4X^2 + X + 2).$$

Infatti il polinomio $k(X) = X^3 + 4X^2 + X + 2$ è irriducibile in $\mathbb{F}_5[X]$ perché non ha radici in $\mathbb{F}_5$.

2. Si calcola il discriminante Δ di $P(X)$ e si vede che $\Delta < 0$, quindi non è il quadrato di un numero razionale. La cubica risolvente di P è $g(X) = X^3 + 12X - 9$. Per il lemma di Gauss $g(X)$ è irriducibile su $\mathbb{Q}$ se e solo se è irriducibile su $\mathbb{Z}$. Se $g(X)$ ammettesse una fattorizzazione non banale in $\mathbb{Z}[X]$, ammetterebbe anche una fattorizzazione non banale in $\mathbb{F}_5[X]$, ma questo è impossibile perché $g(X)$ non ha radici in $\mathbb{F}_5$. Quindi $g(X)$ è irriducibile in $\mathbb{Q}[X]$. Questo ci permette di concludere che il gruppo di Galois di $P(X)$ su $\mathbb{Q}$ è isomorfo a S_4.

3. Poiché il gruppo di Galois di $P(X)$ su $\mathbb{Q}$ è S_4 che è un gruppo risolubile, il polinomio $P(X)$ è risolubile per radicali.

4. Dato che in $\mathbb{F}_5[X]$ si ha la fattorizzazione in irriducibili $X^4 + 3X - 3 = (X - 4)(X^3 + 4X^2 + X + 2)$, il gruppo di Galois G di $P(X)$ su $\mathbb{F}_5$ è uguale al gruppo di Galois della cubica irriducibile $k(X) = X^3 + 4X^2 + X + 2$. Pertanto G è ciclico ed è isomorfo ad un sottogruppo transitivo di S_3, dunque è isomorfo a $\mathbb{Z}/3$.

□

Esercizio 2
Sia $f(X) = (X^2 - X + 1)(X^9 - 3) \in \mathbb{Q}[X]$.

1. Determinare un campo di spezzamento di $f(X)$ su $\mathbb{Q}$.

2. Determinare il gruppo di Galois G di $f(X)$ su $\mathbb{Q}$.

Risoluzione. 1. Osserviamo che $X^9 - 3$ è irriducibile grazie al criterio di Eisenstein applicato con il primo 3. Sia α la radice reale di $X^9 - 3$. Le altre radici complesse di $X^9 - 3$ sono $\alpha\epsilon^i$, dove ϵ è una radice primitiva nona di 1, possiamo scegliere $\epsilon = e^{\frac{2\pi i}{9}}$. Il polinomio $X^2 - X + 1$ è il polinomio ciclotomico ϕ_6 le cui radici sono $-\epsilon^3, -\epsilon^6$. Pertanto un campo di spezzamento per $f(X)$ su $\mathbb{Q}$ è $\mathbb{Q}(\alpha, \epsilon)$.

2. Osserviamo innanzitutto che il polinomio minimo di α su $\mathbb{Q}$ è $X^9 - 3$, mentre il polinomio minimo di ϵ su $\mathbb{Q}$ è il polinomio ciclotomico $\phi_9(X) = X^6 + X^3 + 1$. Abbiamo $|G| = [\mathbb{Q}(\alpha, \epsilon) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \epsilon) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 6 \cdot 9 = 54$, dato che il polinomio minimo di α su $\mathbb{Q}$ è $X^9 - 3$ e ϵ è radice di $\phi_9(X) = X^6 + X^3 + 1 \in \mathbb{Q}(\alpha)[X]$.

Costruiamo esplicitamente due elementi $\sigma, \tau : \mathbb{Q}(\alpha, \epsilon) \to \mathbb{Q}(\alpha, \epsilon)$ del gruppo di Galois G:

$$\sigma(\alpha) = \alpha, \ \sigma(\epsilon) = \epsilon^2,$$

$$\tau(\alpha) = \alpha\epsilon, \ \tau(\epsilon) = \epsilon.$$

Osserviamo che σ ha ordine 6, mentre τ ha ordine 9. Inoltre si ha: $\sigma \circ \tau(\alpha) = \sigma(\alpha\epsilon) = \sigma(\alpha)\sigma(\epsilon) = \alpha\epsilon^2$, $\tau^2 \circ \sigma(\alpha) = \tau^2(\alpha) = \tau(\alpha\epsilon) = \alpha\epsilon^2$; $\sigma \circ \tau(\epsilon) = \sigma(\epsilon) = \epsilon^2$, $\tau^2 \circ \sigma(\epsilon) = \tau^2(\epsilon^2) = \epsilon^2$. Quindi abbiamo dimostrato che $\sigma \circ \tau = \tau^2 \circ \sigma$, equivalentemente $\sigma \circ \tau \circ \sigma^{-1} = \tau^2$. Pertanto il sottogruppo H di G generato da σ e τ, $H = \langle \sigma, \ \tau, \mid \sigma^6 = 1, \ \tau^9 = 1, \ \sigma\tau\sigma^{-1} = \tau^2 \rangle$ è un prodotto semidiretto $\langle \tau \rangle \rtimes \langle \sigma \rangle \cong \mathbb{Z}/9 \rtimes \mathbb{Z}/6$. Dunque $|H| = 54$ e quindi $H = G$.

□

Esercizio 3 Siano G e H due gruppi, $\phi : G \to H$ un omomorfismo suriettivo e sia K il nucleo di ϕ. Supponiamo che K sia abeliano. Definiamo un omomorfismo $\psi : H \to Aut(K)$ nel modo seguente: sia $h \in H$ e sia $g \in G$ tale che $\phi(g) = h$, $\psi(h)(k) := gkg^{-1}$, $\forall k \in K$.

1. Dimostrare che l'omomorfismo ψ è ben definito.

2. Sia $G = Q_8$ il gruppo dei quaternioni, sia $H = \langle x, y \mid x^2 = y^2 = 1, xy = yx \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ e sia $\phi : G \to H$, $\phi(i) := x$, $\phi(j) := y$. Determinare il nucleo K di ϕ e dire se $\psi : H \to Aut(K)$ è l'omomorfismo banale, $\psi(h) = Id_K$, $\forall h \in K$.

Risoluzione. 1. Sia $h \in H$ dato che ϕ è suriettivo, sappiamo che esiste un $g \in G$ tale che $\phi(g) = h$. Poiché K è normale in G, $\forall k \in K$ e $\forall g \in G$ si ha $gkg^{-1} \in K$. Sia ora $g' \in G$ tale che $\phi(g) = \phi(g') = h$. Si ha $\phi(gg'^{-1}) = \phi(g)(\phi(g'))^{-1} = hh^{-1} = 1$, dunque esiste un $a \in K$ tale che $gg'^{-1} = a$, equivalentemente $g = ag'$. Allora $\forall k \in K$ si ha $\psi(h)(k) = gkg^{-1} = a(g'kg'^{-1})a^{-1} = g'kg'^{-1}aa^{-1} = g'kg'^{-1}$ dato che a e $g'kg'^{-1}$ sono due elementi di K che per ipotesi è abeliano. Pertanto $\psi(h)$ non dipende dalla scelta di un elemento $g \in G$ tale che $\phi(g) = h$ e dunque ψ è ben definita.

2. L'omomorfismo ϕ è suriettivo quindi per il primo teorema di omomorfismo si ha $H \cong G/K$, dunque $|H| = 4 = \frac{|G|}{|K|} = \frac{8}{|K|}$, quindi $|K| = 2$. Chiaramente $i^2 = j^2 = -1 \in K$ perché $\phi(i^2) = (\phi(i))^2 = x^2 = 1 = y^2 = (\phi(j))^2 = \phi(j^2)$. Dunque $K = \langle (-1) \rangle \cong \mathbb{Z}/2$.

Si ha $\psi(x)(-1) = i(-1)i^{-1} = -1$, $\psi(y)(-1) = j(-1)j^{-1} = -1$, dunque $\psi(x) = \psi(y) = Id_K$ e dato che x, y generano H, $\psi(h) = Id_K$, $\forall h \in H$, cioè ψ è l'omomorfismo banale.

$\square$