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

Prova scritta del 22.9.2015

Esercizio 1. *Sia* $P(X) = X^{30} + X^{20} + X^{10} + 1 \in \mathbb{F}_2[X]$.

1. *Determinare una fattorizzazione di* $P(X)$ *in irriducibili.*
2. *Determinare un campo di spezzamento* L *di* $P(X)$ *su* $\mathbb{F}_2$.
3. *Determinare l'ordine dell'omomorfismo di Frobenius* $\phi : L \to L$.
4. *Determinare il gruppo di Galois di* $P(X)$ *su* $\mathbb{F}_2$.

Soluzione. 1. Si ha $P(X) = (X^5 - 1)^6 = (X-1)^6(X^4 + X^3 + X^2 + X + 1)^6$. Il polinomio $\phi_5(X) = X^4 + X^3 + X^2 + X + 1$ è irriducibile su $\mathbb{F}_2$ perché non ha radici in $\mathbb{F}_2$ e non si fattorizza come prodotto di due polinomi di grado 2. Infatti se $X^4 + X^3 + X^2 + X + 1 = (X^2 + aX + b)(X^2 + cX + d)$ si avrebbe $bd = 1$ quindi $b = d = 1$; $b + d + ac = 1$, dunque $a = c = 1$ e $a + c = 1$ che è assurdo.

2. Per quanto visto sopra, un campo di spezzamento L di $P(X)$ su $\mathbb{F}_2$ è $\mathbb{F}_2(\eta)$, con η una radice quinta primitiva dell'unità.

3. Sia $\phi : \mathbb{F}_2(\eta) \to \mathbb{F}_2(\eta)$ l'omomorfismo di Frobenius. Si ha $\phi(\eta) = \eta^2$, quindi $\phi^i(\eta) = \eta^{2^i}$. Dunque l'ordine di ϕ è il più piccolo intero positivo i tale che $2^i \equiv 1 \mod 5$, pertanto $o(\phi) = 4$.

4. Il gruppo di Galois di $P(X)$ è ciclico generato dall'omomorfismo di Frobenius di L e dunque è isomorfo a $\mathbb{Z}/4$. □

Esercizio 2. *Dire se i seguenti polinomi sono risolubili per radicali e determinare il loro gruppo di Galois su* $\mathbb{Q}$.

1. $g(X) = X^3 + 9X + 3 \in \mathbb{Q}[X]$.
2. $h(X) = X^5 + 5X^4 - 5X^3 - 25X^2 + 5X + 25 \in \mathbb{Q}[X]$.

Soluzione. 1. $g(X)$ è risolubile per radicali perché, essendo di grado 3, il suo gruppo di Galois è un sottogruppo di S_3 che è un gruppo risolubile.

Il polinomio $g(X)$ è irriducibile grazie al criterio di Eisenstein applicato con il primo $p = 3$, quindi il gruppo di Galois di $g(X)$ è isomorfo o a $\mathbb{Z}/3$ o a S_3. Per determinarlo dobbiamo vedere se il discriminante Δ di g ha una radice in $\mathbb{Q}$. Si ha $\Delta = -4 \cdot 9^3 - 27 \cdot 9 = -3^5 \cdot 13$ che non ha radici in $\mathbb{Q}$. Quindi il gruppo di Galois di g è isomorfo a S_3.

2. Si ha $h(X) = X^4(X+5) - 5X^2(X+5) + 5(X+5) = (X+5)(X^4 - 5X^2 + 5)$, quindi il gruppo di Galois di h è il gruppo di Galois di $f(X) = X^4 - 5X^2 + 5$. $f(X)$ (e quindi $h(X)$) è risolubile per radicali perché, essendo di grado 4, il suo gruppo di Galois è un sottogruppo di S_4 che è un gruppo risolubile. Il polinomio $f(X) =$

$X^4 - 5X^2 + 5$ è irriducibile grazie al criterio di Eisenstein applicato con il primo $p = 5$. In $\mathbb{R}[X]$ si ha una fattorizzazione $f(X) = (X^2 - \frac{5+\sqrt{5}}{2})(X^2 - \frac{5-\sqrt{5}}{2}) = (X-a)(X+a)(X-b)(X+b)$, con $a = \sqrt{\frac{5+\sqrt{5}}{2}}$, $b = \sqrt{\frac{5-\sqrt{5}}{2}}$. Si ha inoltre $b = 2a - 5a^{-1}$, quindi un campo di spezzamento di f su $\mathbb{Q}$ è $\mathbb{Q}(a)$ e si ha $[\mathbb{Q}(a) : \mathbb{Q}] = 4$ perché il polinomio minimo di a su $\mathbb{Q}$ è f. Dunque il gruppo di Galois G di f è un sottogruppo transitivo di S_4 di cardinalità 4. Poiché è transitivo sulle radici, esiste un elemento $\sigma \in G$ tale che $\sigma(a) = b$. Ma $\sigma^2(a) = \sigma(b) = \sigma(2a - 5a^{-1}) = 2\sigma(a) - 5\sigma(a)^{-1} = 2b - 5b^{-1} = -a$. Quindi σ ha ordine 4 e $G \cong \mathbb{Z}/4$. $\square$

Esercizio 3. *Sia G un gruppo di cardinalità 200.*

1. *Dimostrare che G è un prodotto semidiretto. .*
2. *Supponiamo inoltre che i 2-Sylow di G siano abeliani e i 5-Sylow siano ciclici. Dare un esempio di un tale gruppo G non abeliano nei seguenti casi:*
   (a) *I 2-Sylow sono isomorfi a $\mathbb{Z}/8$.*
   (b) *I 2-Sylow sono isomorfi a $\mathbb{Z}/4 \times \mathbb{Z}/2$.*
   (c) *I 2-Sylow sono isomorfi a $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.*

Soluzione. 1. Il numero dei 5-Sylow è congruo a 1 modulo 5 e divide 8, dunque c'è un unico 5-Sylow H che è normale in G. Sia K un 2-Sylow. Dato che H è normale in G si ha che $KH = HK$ è un sottogruppo di G. L'intersezione $H \cap K$ è banale perché $|H \cap K|$ deve dividere sia $|H| = 25$ che $|K| = 8$. Quindi $H \cap K$ ha cardinalità pari a $|H| \cdot |K| = 200$, pertanto $G = HK$ cioè G è prodotto semidiretto di H e K.

2. (a) Poiché abbiamo dimostrato che G è isomorfo ad un prodotto semidiretto del 5-Sylow $H \cong \mathbb{Z}/25$ e di un 2-Sylow $K \cong \mathbb{Z}/8$, per dare un esempio di un tale gruppo che non sia abeliano basta esibire un omomorfismo non banale $\phi : K \to Aut(H)$. Sia y un generatore di K e x un generatore di H. Per determinare ϕ basta definire $\phi(y)(x) = x^i$ in modo tale che $o(\phi(y))|o(y) = 8$. Dunque dobbiamo avere $(\phi(y))^8(x) = x^{i^8} = x$ e quindi $i^8 \equiv 1 \mod 25$. Scegliamo $i = 7$, cioè definiamo $\phi(y)(x) = x^7$. Si ha $7^2 = 49 \equiv -1 \mod 25$, pertanto $7^4 \equiv 7^8 \equiv 1 \mod 25$.

(b) Dobbiamo dare un omomorfismo non banale $\phi : K \cong \mathbb{Z}/4 \times \mathbb{Z}/2 \to Aut(\langle x \rangle)$. Si ha $K \cong \langle y, z \mid y^4 = 1,\ z^2 = 1,\ yz = zy \rangle$ e quindi è sufficiente definire $\phi(y)(x) = x^i$, $\phi(z)(x) = x^j$ in modo che $i^4 \equiv 1 \mod 25$, $j^2 \equiv 1 \mod 25$. Scegliamo per esempio $i = 7$ e $j = 24 \equiv -1 \mod 25$.

(c) Dobbiamo dare un omomorfismo non banale $\phi : K \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \to Aut(\langle x \rangle)$. Si ha $K \cong \langle y, z, w \mid y^2 = z^2 = w^2 = 1\ yz = zy, yw = wy, zw = wz \rangle$ e quindi è sufficiente definire $\phi(y)(x) = x^i$, $\phi(z)(x) = x^j$, $\phi(w)(x) = x^k$ in modo che $i^2 \equiv j^2 \equiv k^2 \equiv 1 \mod 25$. Scegliamo per esempio $i = k = 1$ e $j = 24 \equiv -1 \mod 25$. $\square$