Corso di Algebra 2 - a.a. 2015-2016

Prova scritta del 18.7.2016

Esercizio 0.1. *Sia* $P(X) = X^5 + 3X^4 + 2X^3 + X^2 + X + 2 \in \mathbb{F}_5[X]$.

1. *Determinare una fattorizzazione di* $P(X)$ *in irriducibili.*

2. *Determinare il gruppo di Galois di* $P(X)$ *su* $\mathbb{F}_5$.

Risoluzione. 1. Si verifica che $P(1) = 0$ e $P(X) = (X-1)(X^4 + 4X^3 + X^2 + 2X + 3)$. Sia $f(X) := X^4 + 4X^3 + X^2 + 2X + 3$. Si verifica che $f(X)$ non ha radici in $\mathbb{F}_5$. Vediamo che non si fattorizza come prodotto di due polinomi di grado 2. Supponiamo che $f(X) = (X^2 + aX + b)(X^2 + cX + d)$. Si deve avere

a) $bd = 3$,

b) $c + a = 4$,

c) $1 = b + d + ac$,

d) $2 = ad + bc$.

Abbiamo 4 possibilità per b e d:

1) $b = 1$, $d = 3$

2) $b = 2$, $d = 4$

3) $b = 3$, $d = 1$

4) $b = 4$, $d = 2$.

Nel caso 1), da b) e c) si ottiene $a^2 - 4a - 3 = 0$ che non ha soluzioni in $\mathbb{F}_5$. Nel caso 2) da b) e c) si ottiene $ac = a(4-a) = 0$, quindi o $a = 0$ e $c = 4$, o $a = 4$ e $c = 0$ e in entrambi i casi, usando la d) si ottiene una contraddizione. I casi 3) e 4) sono analoghi. Quindi f è irriducibile.

2. Il gruppo di Galois di $P(X)$ è il gruppo di Galois di $f(X)$. Poiché $f(X)$ è una quartica irriducibile, il suo gruppo di Galois è un sottogruppo transitivo di S_4 ed è anche ciclico perché siamo su $\mathbb{F}_5$, quindi è isomorfo a $\mathbb{Z}/4\mathbb{Z}$. □

Esercizio 0.2. *Dire se le seguenti estensioni di campi sono di Galois e determinare il loro gruppo di Galois.*

1. $\mathbb{Q}(5^{1/7}) : \mathbb{Q}$.

2. $\mathbb{F}_5(\alpha) : \mathbb{F}_5$, *dove* α *è una radice di* $X^3 + X + 1 \in \mathbb{F}_5[X]$.

3. $\mathbb{Q}(7^{1/5}, \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})) : \mathbb{Q}$.

Risoluzione. 1. L'estensione non è di Galois perché non è normale. Infatti $5^{1/7}$ è una radice del polinomio $f(X) = X^7 - 5$ che è irriducibile su $\mathbb{Q}[X]$ grazie al criterio di Eisenstein applicato con il primo 5. Le altre radici di $f(X)$ sono $5^{1/7}\xi^i$, $i = 1, ..., 6$, dove ξ è una radice settima primitiva di 1. Quindi $\mathbb{Q}(5^{1/7})$ contiene una radice di f ma non contiene le altre radici perché queste non sono reali, mentre $\mathbb{Q}(5^{1/7}) \subset \mathbb{R}$. Il

gruppo di Galois G di $\mathbb{Q}(5^{1/7}) : \mathbb{Q}$ è banale perché per ogni elemento $g \in G$, $g(5^{1/7})$ deve essere una radice di f in $\mathbb{Q}(5^{1/7})$ e quindi si deve avere $g(5^{1/7}) = 5^{1/7}$.

2. Dato che α è algebrico su $\mathbb{F}_5$, l'estensione $\mathbb{F}_5(\alpha) : \mathbb{F}_5$ è algebrica e finita e poiché siamo in caratteristica positiva è anche normale e separabile, quindi è di Galois.

Il polinomio $g(X) = X^3 + X + 1$ non ha radici in $\mathbb{F}_5$, quindi α non appartiene a $\mathbb{F}_5$ e $g(X)$ è irriducibile e dunque $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 3$. e quindi il gruppo di Galois di $\mathbb{F}_5(\alpha) : \mathbb{F}_5$ è isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

3. Sia $\beta := 7^{1/5}$ e $\zeta := \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5})$ e sia $L := \mathbb{Q}(\beta, \zeta)$. L'estensione $L : \mathbb{Q}$ è di Galois perché è un campo di spezzamento del polinomio $X^5 - 7$, quindi è finita e normale. Inoltre è separabile perché siamo in caratteristica zero. Calcoliamo il grado dell'estensione: $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Si ha $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ perché α è una radice di $X^5 - 7$ che è irriducibile su $\mathbb{Q}$ grazie al criterio di Eisenstein applicato con il primo 7. Si ha inoltre $[L : \mathbb{Q}(\alpha)] \leq 4$ perché ζ è una radice di $X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}(\alpha)[X]$. Quindi $[L : \mathbb{Q}] \leq 20$ e $5|[L : \mathbb{Q}]$. Inoltre usando di nuovo la regola della torre si ottiene $[L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}]$ e$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ perché il polinomio minimo di ζ su $\mathbb{Q}$ è $X^4 + X^3 + X^2 + X + 1$. Quindi $4|[L : \mathbb{Q}]$ e pertanto $[L : \mathbb{Q}] = 20$. Sia G il gruppo di Galois di $L : \mathbb{Q}$. Sappiamo che $|G| = 20$. Costruiamo direttamente due elementi di G, σ, τ nel modo seguente: $\sigma(\alpha) = \alpha$, $\sigma(\zeta) = \zeta^2$; $\tau(\alpha) = \alpha\zeta$, $\tau(\zeta) = \zeta$. L'ordine di σ è 4, mentre l'ordine di τ è 5. Inoltre si verifica direttamente che $\sigma\tau\sigma^{-1} = \tau^2$, quindi $G \cong \langle \tau,\ \sigma \mid \tau^5 = 1,\ \sigma^4 = 1,\ \sigma\tau\sigma^{-1} = \tau^2 \rangle$, ossia G è un prodotto semidiretto di $\langle\tau\rangle \rtimes_\phi \langle\sigma\rangle \cong \mathbb{Z}/5\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$ dove $\phi(\sigma)(\tau) = \sigma\tau\sigma^{-1} = \tau^2$.

□

Esercizio 0.3. *Sia G un gruppo di cardinalità 550. Supponiamo inoltre che esista un unico 2-Sylow H.*

1. *Dire se il centro di G è banale.*
2. *Dimostrare che G contiene un sottogruppo normale ciclico di ordine 22.*
3. *Dire se G è risolubile.*
4. *Dare un esempio di un tale gruppo G che non sia abeliano e in cui i 5-Sylow non siano ciclici.*

Soluzione. 1. Poiché esiste un unico 2-Sylow H, questo è normale in G. Sia σ il generatore di H. Per ogni $g \in G$, $g\sigma g^{-1} \in H = \{1, \sigma\}$, quindi $g\sigma g^{-1} = \sigma$, pertanto σ sta nel centro di G che quindi è non banale.

2. Il numero N_{11} di 11-Sylow è congruo a 1 modulo 11 e divide $|G| = 2 \cdot 11 \cdot 5^2$. Quindi $N_{11} = 1 + 11k$ e $N_{11}|50$, pertanto $N_{11} = 1$. Allora esiste un unico 11-Sylow K normale in G. $HK = KH$ è un sottogruppo di G e $H \cap K$ è banale perché la sua cardinalità deve dividere sia $|H| = 2$ che $|K| = 11$, quindi HK ha cardinalità 22. Inoltre $\forall g \in K$ si ha $g\sigma = \sigma g$, quindi $HK \cong H \times K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \cong \mathbb{Z}/22\mathbb{Z}$. Infine HK è normale in G perché $\forall g \in G$, $\forall k \in K$, $\forall i = 1, 2$, si ha $g(\sigma^i k)g^{-1} =$

$(g\sigma^i g^{-1})(gkg^{-1}) = \sigma^i gkg^{-1} = \sigma^i k'$ con $k' = gkg^{-1} \in K$ perché K è normale in G. Quindi HK è un sottogruppo normale di G ciclico di ordine 22.

3. G è risolubile perché basta prendere la serie $1 < N < G$, con $N = HK$ normale in G, N è abeliano (è ciclico) e G/N è abeliano perché la sua cardinalità è 5^2 che è il quadrato di un primo.

4. Sia L un 5-Sylow. Per ipotesi L non è ciclico, quindi $L \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. $N = HK$ è un sottogruppo normale di G, quindi $LN = NL$ è un sottogruppo di G. L'intersezione $N \cap L$ è banale perché la sua cardinalità deve dividere sia $|L| = 25$, sia $|N| = 22$. Quindi $|NL| = 550 = |G|$ e pertanto $LN = NL = G$ e G è un prodotto semidiretto di L e N. Quindi per descrivere G dobbiamo dare un omomorfismo $\psi : L \to Aut(N)$. Osserviamo che $\forall x \in L$, $x \neq 1$, $o(x) = 5$ e $o(\psi(x))|o(x) = 5$. $L = \langle z, w \mid z^5 = 1,\ w^5 = 1,\ zw = wz \rangle$, $N = .\langle \sigma, \tau \mid \sigma^2 = 1,\ \tau^{11} = 1,\ \sigma\tau = \tau\sigma \rangle$. Consideriamo l'omomorfismo seguente: $\psi(z)(\sigma) = \sigma$, $\psi(z)(\tau) = \tau^4$, $\psi(w)(\sigma) = \sigma$, $\psi(w)(\tau) = \tau$. Si ha $o(\psi(z)) = 5$, $o(\psi(w)) = 1$ e chiaramente $\psi(z)$ e $\psi(w)$ commutano, dato che $\psi(w) = Id_N$. Quindi ψ è ben definito e G non è abeliano perché $\psi(z) \neq Id_N$. □