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

Prova scritta del 13.9.2016

Esercizio 0.1. *Sia* $P(X) = X^8 - X^7 - 5X + 5 \in \mathbb{Q}[X]$.

1. *Determinare una fattorizzazione di* $P(X)$ *in irriducibili.*
2. *Dire se è risolubile per radicali.*
3. *Determinare il gruppo di Galois di* $P(X)$ *su* $\mathbb{Q}$ *e su* $\mathbb{Q}(5^{\frac{1}{7}})$.

Risoluzione. 1. $P(X) = (X^7 - 5)(X - 1)$ e $X^7 - 5$ è irriducibile grazie al criterio di Eisenstein applicato con il primo 5.

2. Le radici di $X^7 - 5$ in $\mathbb{C}$ sono $\{\alpha\xi^i\}_{i=0,...,6}$, dove $\alpha = 5^{\frac{1}{7}}$ e $\xi = e^{2\pi i/7}$. Quindi un campo si spezzamento di $P(X)$ su $\mathbb{Q}$ è $\mathbb{Q}(\alpha, \xi)$. Si ha $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, \xi)$ e $\alpha^7 = 5 \in \mathbb{Q}$ e $\xi^7 = 1 \in \mathbb{Q} \subset \mathbb{Q}(\alpha)$. Quindi $\mathbb{Q}(\alpha, \xi)$ è un'estensione radicale di $\mathbb{Q}$ e dunque P è risolubile per radicali.

3. Sia G il gruppo di Galois di P su $\mathbb{Q}$ e sia $L := \mathbb{Q}(\alpha, \xi)$. La cardinalità di G è uguale al grado dell'estensione $[L : \mathbb{Q}]$. Si ha $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, \xi), \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 42$. Infatti il polinomio minimo di α su $\mathbb{Q}$ è $X^7 - 5$, quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$ e $[\mathbb{Q}(\alpha, \xi), \mathbb{Q}(\alpha)] \leq 6$ perché ξ è una radice del polinomio $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}(\alpha)[X]$. Inoltre $7|[L : \mathbb{Q}]$. D'altra parte $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, \xi), \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}]$ e $[\mathbb{Q}(\xi) : \mathbb{Q}] = 6$ perché il polinomio minimo di ξ su $\mathbb{Q}$ è il polinomio ciclotomico $f(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$. Quindi $6|[L : \mathbb{Q}]$ e dunque $|G| = [L : \mathbb{Q}] = 42$. Inoltre abbiamo anche dimostrato che $[\mathbb{Q}(\alpha, \xi), \mathbb{Q}(\alpha)] = 6$ e quindi f è irriducibile su $\mathbb{Q}(\alpha)$ ed è il polinomio minimo di ξ su $\mathbb{Q}(\alpha)$. Osserviamo che $\forall g \in G$, $g(\alpha)$ è una radice di $X^7 - 5$, quindi $g(\alpha) = \alpha\xi^i$ per qualche $i = 0, ..., 6$, mentre $g(\xi)$ è una radice di f, pertanto $g(\xi) = \xi^j$ per qualche $j = 1, ..., 6$. Descriviamo esplicitamente due elementi σ e τ di G dando l'azione su α e su ξ nel modo seguente: $\sigma(\alpha) = \alpha$, $\sigma(\xi) = \xi^3$; $\tau(\alpha) = \alpha\xi$, $\tau(\xi) = \xi$. Si verifica immediatamente che $o(\tau) = 7$ e $o(\sigma) = 6$. Inoltre $\sigma\tau\sigma^{-1} = \tau^3$, quindi $G \cong \mathbb{Z}/7 \rtimes_\phi \mathbb{Z}/6$ con $\phi : \mathbb{Z}/6 \cong \langle\sigma\rangle \to Aut(\mathbb{Z}/7) \cong Aut(\langle\tau\rangle)$, $\phi(\sigma)(\tau) = \sigma\tau\sigma^{-1} = \tau^3$.

Sia H il gruppo di Galois di P su $\mathbb{Q}(\alpha)$. Si ha $|H| = [L : \mathbb{Q}(\alpha)] = 6$ come abbiamo visto sopra. Inoltre l'automorfismo σ di L descritto sopra sta chiaramente in H perché fissa α. Poiché l'ordine di σ è 6, si ha $H \cong \langle\sigma\rangle \cong \mathbb{Z}/6$. □

Esercizio 0.2. *Determinare il gruppo di Galois dell'estensione* $\mathbb{F}_7(\alpha) : \mathbb{F}_7$ *nei seguenti casi:*

1. α *è una radice di* $g(X) = X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_7[X]$.
2. α *è una radice di* $h(X) = X^4 + X^3 + 1 \in \mathbb{F}_7[X]$.

Risoluzione. 1. Osserviamo che il gruppo moltiplicativo del campo $\mathbb{F}_7$ è ciclico di ordine 6, quindi per ogni $a \in \mathbb{F}_7$, $a \neq 0$ si ha $a^6 = 1$, quindi a è una radice di $X^6 - 1 = (X-1)g(X)$ che ha grado 6. Dunque si ha $X^6 - 1 = (X-1)(X-2)(X-3)(X-4)(X-5)(X-6) \in \mathbb{F}_7[X]$ e pertanto $g(X) = (X-2)(X-3)(X-4)(X-5)(X-6) \in \mathbb{F}_7[X]$. Dunque tutte le radici α di g stanno in $\mathbb{F}_7$ quindi $\mathbb{F}_7(\alpha) = \mathbb{F}_7$ e il gruppo di Galois di $\mathbb{F}_7(\alpha) : \mathbb{F}_7$ è banale per qualunque radice α di g.

2. Osserviamo che h non ha radici in $\mathbb{F}_7$. Con un calcolo diretto si vede anche che h non si fattorizza come prodotto di due polinomi di grado 2. Pertanto h è irriducibile e dunque $[\mathbb{F}_7(\alpha) : \mathbb{F}_7] = deg(h) = 4$ e il gruppo di Galois di $\mathbb{F}_7(\alpha) : \mathbb{F}_7$ è ciclico di ordine 4. □

Esercizio 0.3. *Sia G un gruppo di cardinalità $2p^n$ con p un primo dispari e $n \geq 2$. Supponiamo inoltre che il centro di G contenga un elemento σ di ordine 2.*

1. *Dimostrare che il centro di G contiene un elemento di ordine $2p$.*

2. *Classificare G a meno di isomorfismo nel caso in cui $n = 2$.*

Risoluzione. 1. Per il teorema di Sylow Il numero N_p dei p-Sylow è congruo a 1 modulo p e divide 2, quindi è uguale a 1. Pertanto c'è un'unico p-Sylow H che è normale in G. Poiché $|H| = p^n$, sappiamo che il centro di H, $Z(H)$ è non banale ed ha quindi cardinalità p^k con $1 \leq k \leq n$. Per il teorema di Cauchy sappiamo che esiste un elemento $y \in Z(H)$ di ordine p. Sia $\langle y \rangle$ il sottogruppo di $Z(H)$ generato da y. Il sottogruppo di G generato da σ è un 2-Sylow e poiché per ipotesi σ sta nel centro di G, per ogni $g \in G$ si ha che $g\sigma g^{-1} = \sigma$. Quindi il 2-Sylow $K := \langle \sigma \rangle$ è normale in G e dunque K è l'unico 2-Sylow di G. Dunque H e K sono due sottogruppi normali di G e la loro intersezione è banale perché $|H \cap K|$ deve dividere sia $|H| = p^n$, sia $|K| = 2$. Pertanto $G = HK \cong H \times K$. L'elemento σy ha ordine $2p$ e sta nel centro di G perché commuta con σ e con ogni elemento di H.

2. Abbiamo dimostrato sopra che $G \cong H \times K \cong H \times \mathbb{Z}/2$. Poiché $|H| = p^2$ sappiamo che H è abeliano e dunque è isomorfo o a $\mathbb{Z}/p \times \mathbb{Z}/p$ o a $\mathbb{Z}/p^2$. Quindi o $G \cong \mathbb{Z}/p \times \mathbb{Z}/p \times \mathbb{Z}/2$, oppure $G \cong \mathbb{Z}/p^2 \times \mathbb{Z}/2$. □