Corso di Algebra 2 - a.a. 2014-2015
Prova scritta del 3.9.2015

Esercizio 0.1. *Sia $f(X) = X^{11} - 17 \in \mathbb{Q}[X]$.*

1. *Determinare un campo di spezzamento di f su $\mathbb{Q}$.*
2. *Dire se f è risolubile per radicali.*

Risoluzione. 1) f è irriducibile in $\mathbb{Q}[X]$ grazie al criterio di Eisenstein applicato con il primo $p = 17$. Le radici di f in $\mathbb{C}$ sono $\alpha := 17^{\frac{1}{11}}$, $\alpha\xi^i$, $i = 1, ..., 10$, dove ξ è una radice primitiva undicesima dell'unità (e.g. $\xi = e^{\frac{2\pi i}{11}}$). Quindi un campo di spezzamento di f su $\mathbb{Q}$ è $L = \mathbb{Q}(\alpha, \xi)$.

2) Abbiamo $[L : \mathbb{Q}] = [L : \mathbb{Q}(\xi)] \cdot [\mathbb{Q}(\xi) : \mathbb{Q}] \leq 110$ perché $[\mathbb{Q}(\xi) : \mathbb{Q}] = 10$ dato che il polinomio minimo di ξ su $\mathbb{Q}$ è il polinomio ciclotomico $\Phi_{11}(X) = X^{10} + X^9 + ... + X + 1$ e $[L : \mathbb{Q}(\xi)] \leq 11$ perché α è una radice di $X^{11} - 17 \in \mathbb{Q}(\xi)[X]$. Inoltre abbiamo mostrato che $10|[L : \mathbb{Q}]$. D'altra parte abbiamo anche $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$ e $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 11$ perché f è il polinomio minimo di α su $\mathbb{Q}$. Quindi $11|[L : \mathbb{Q}]$, $10|[L : \mathbb{Q}] \leq 110$, quindi $[L : \mathbb{Q}] = 110$. Sia $G := Gal(L, \mathbb{Q})$. $L : \mathbb{Q}$ è un'estensione di Galois, quindi $110 = [L : \mathbb{Q}] = |G|$. Mostriamo che un gruppo di ordine 110 è risolubile e questo ci dice che f è risolubile per radicali.

Per vedere che un gruppo G di ordine 110 è risolubile si osserva che il numero degli 11-Sylow è congruo a 1 modulo 11 e divide 10, quindi c'è un unico 11-Sylow $H \cong \mathbb{Z}/11\mathbb{Z}$ in G che pertanto è normale ed è risolubile perché è ciclico. Mostriamo che anche G/H è risolubile. Infatti $F := G/H$ ha cardinalità 10 e quindi posso prendere la serie di inclusioni $(e) \subset K \subset F$, dove K è l'unico 5-Sylow di F che quindi è normale in F ed è ciclico. Inoltre $|F/K| = 2$, quindi anche F/K è ciclico. Allora G è un gruppo che ha un sottogruppo normale H che è risolubile e tale che il quoziente G/H è risolubile. Quindi G è risolubile.

□

Esercizio 0.2.
1. *Determinare il gruppo di Galois di $P(X) = X^4 + 2X^2 - 2X + 2 \in \mathbb{Q}[X]$ su $\mathbb{Q}$.*
2. *Consideriamo ora $P(X)$ come polinomio in $\mathbb{F}_5[X]$. Determinare il suo gruppo di Galois su $\mathbb{F}_5$.*

Risoluzione. 1) P è irriducibile in $\mathbb{Q}[X]$ grazie al criterio di Eisenstein applicato con il primo $p = 2$. Il discriminante Δ di P è uguale a $2256 = 2^4 \cdot 3 \cdot 47$ non ha una radice quadrata in $\mathbb{Q}$. La cubica risolvente è il polinomio $g(X) = X^3 + 4X^2 - 4X - 4$. Mostriamo che g è irriducibile in $\mathbb{Q}[X]$. Per il lemma di Gauss g è irriducibile in $\mathbb{Q}[X]$ se e solo se lo è in $\mathbb{Z}[X]$. Quindi basta dimostrare che non esiste una fattorizzazione della forma $g(X) = (X - a)(X^2 + bX + c)$ con $a, b, c \in \mathbb{Z}$. Si vede facilmente che questo non è possibile. Allora g è irriducibile su $\mathbb{Q}$ e quindi il gruppo di Galois di P è il gruppo simmetrico Σ_4.

2) In $\mathbb{F}_5[X]$ si ha $P(X) = (X-3)(X^3+3X^2+X+1)$. La cubica $h(X) = X^3+3X^2+X+1$ è irriducibile in $\mathbb{F}_5[X]$ perché non ha radici in $\mathbb{F}_5$. Pertanto il gruppo di Galois di P è ciclico isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

□

Esercizio 0.3. *Sia G un gruppo di cardinalità* $3^5 \cdot 5$.

1. *Supponiamo che i 3-Sylow di G siano ciclici. Classificare G a meno di isomorfismo.*
2. *Supponiamo che i 3-Sylow di G siano isomorfi a* $(\mathbb{Z}/3\mathbb{Z})^5$. *Dare un esempio in cui G non è abeliano.*

Risoluzione. Se G è un gruppo di cardinalità $3^5 \cdot 5$, il numero dei 3-Sylow di G è congruo a 1 modulo 3 e divide $|G|$, quindi deve dividere 5 e pertanto può solo essere uguale a 1. Dunque esiste un unico 3 - Sylow H che è normale in G.

Sia K un 5-Sylow, $HK = KH$ è un sottogruppo di G perché H è normale in G. $|H \cap K|$ divide sia $|H| = 3^5$, sia $|K| = 5$, quindi $H \cap K = (e)$. Pertanto $|HK| = |H| \cdot |K| = |G|$ e quindi G è un prodotto semidiretto di H con K. $K \cong \mathbb{Z}/5\mathbb{Z} \cong \langle x \mid x^5 = 1 \rangle$ agisce per coniugio su H, quindi abbiamo un omomorfismo $\psi : K \to Aut(H)$, $\psi(g)(h) = ghg^{-1}$, $\forall g \in K$, $\forall h \in H$. L'ordine di $\psi(x)$ divide l'ordine di x che è 5, quindi o $\psi(x) = Id$, oppure $\psi(x)$ ha ordine 5.

1) Supponiamo che H sia ciclico, isomorfo a $\mathbb{Z}/243\mathbb{Z}$. Si ha $Aut(\mathbb{Z}/243\mathbb{Z}) \cong (\mathbb{Z}/243\mathbb{Z})^*$ che ha cardinalità uguale a $3^5 - 3^4 = 162$. Se l'ordine di $\psi(x)$ fosse 5, 5 dovrebbe dividere $|Aut(\mathbb{Z}/243\mathbb{Z})| = 162$ e questo è assurdo. Pertanto $\psi(x) = Id$ e quindi ψ è l'omomorfismo banale, ossia $gh = hg$, $\forall g \in K$, $\forall h \in H$ e allora $G \cong H \times K \cong \mathbb{Z}/243\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/(3^5 \cdot 5)\mathbb{Z}$.

2) Se $H \cong (\mathbb{Z}/3\mathbb{Z})^5$. Vogliamo definire un omomorfismo ψ come sopra che sia non banale, quindi dobbiamo definire l'immagine del generatore x di K, $\psi(x) \in Aut(H)$ in modo tale che $o(\psi(x)) = 5$. Per definire $\psi(x)$, basta definirlo sui generatori di $(\mathbb{Z}/3\mathbb{Z})^5$ dati da $(1,0,0,0,0)$, $(0,1,0,0,0)$, $(0,0,1,0,0)$, $(0,0,0,1,0)$, $(0,0,0,0,1)$. Poniamo:

$$\psi(x)(1,0,0,0,0) = (0,1,0,0,0),\ \psi(x)(0,1,0,0,0) = (0,0,1,0,0),$$

$$\psi(x)(0,0,1,0,0) = (0,0,0,1,0),\ \psi(x)(0,0,0,1,0) = (0,0,0,0,1),$$

$$\psi(x)(0,0,0,0,1) = (1,0,0,0,0).$$

Chiaramente si ha $\psi(x) \in Aut(H)$ e l'omomorfismo ψ è ben definito perché l'ordine di $\psi(x)$ è 5. Questo ci dice anche che ψ è un omomorfismo non banale, pertanto $G \cong H \rtimes_\psi K$ non è abeliano.

□