Corso di Algebra 2 – a.a. 2013-2014

Prova scritta del 16.1.2015

1. Sia $p(X) = X^8 + 3X^6 + X^5 + 3X^3 + X^2 + 3 \in \mathbb{Q}[X]$.
   (a) Calcolare il gruppo di Galois di $p(X)$ su $\mathbb{Q}$.
   (b) Dire se $p(X)$ è risolubile per radicali.
   (c) Descrivere esplicitamente la corrispondenza di Galois per $p(X)$.
2. Sia K un campo finito di caratteristica p. Sia $P(X)$ un polinomio monico di grado d a coefficienti in K, e sia L un campo di spezzamento di $P(X)$ su K.
   (a) Mostrare che se $P(X)$ è irriducibile allora $[L : K] = d$.
   (b) Nel caso in cui $K = \mathbb{F}_3$ e $d = 5$ determinare tutti i gradi $[L : K]$ possibili.
3. Siano p e q numeri primi tali che $q = p + 2$.
   (a) Mostrare che se $p > 3$ ogni gruppo di ordine p^2q^2 è abeliano.
   (b) Costruire esplicitamente almeno un gruppo non abeliano di ordine $3^2 5^2$.

Soluzioni

1. Abbiamo:
$$\begin{aligned} p(X) &= X^2(X^6 + X^3 + 1) + 3(X^6 + X^3 + 1) \\ &= (X^2 + 3)(X^6 + X^3 + 1). \end{aligned}$$
Notiamo che $X^6 + X^3 + 1 = \Phi_9(X)$, il nono polinomio ciclotomico. Sia ζ una radice nona primitiva dell'unità (prendiamo, per fissare le cose, $\zeta = \exp(\frac{2\pi i}{9})$). Un campo di spezzamento di $p(X)$ su $\mathbb{Q}$ è dato da $\mathbb{Q}(i\sqrt{3}, \zeta)$. Osserviamo che
$$\begin{aligned} \zeta^3 &= \exp\left(\frac{2\pi i}{3}\right) = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) \\ &= \frac{1}{2} + i\frac{\sqrt{3}}{2}. \end{aligned}$$
Dunque, $i\sqrt{3} \in \mathbb{Q}(\zeta)$, e $\mathbb{Q}(i\sqrt{3}, \zeta) = \mathbb{Q}(\zeta)$. È noto che $G = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong \mathbb{Z}_9^*$, che è un gruppo ciclico di ordine 6, in particolare risolubile. Un generatore è dato dall'automorfismo α tale che $\alpha(\zeta) = \zeta^2$.

G ha un sottogruppo K di ordine 3 (indice 2), $K = \langle \alpha^2 \rangle$, e un sottogruppo di ordine 2 (indice 3), $H = \langle \alpha^3 \rangle$. A K corrisponde un'estensione quadratica su $\mathbb{Q}$, che è sicuramente $\mathbb{Q}(i\sqrt{3})$. Di seguito, determiniamo l'estensione (di grado 3) corrispondente a K. α^3 ha ordine 2 in G, dunque
$$\alpha^3(\zeta + \alpha^3(\zeta)) = \zeta + \alpha^3(\zeta) = \zeta + \zeta^{-1} = e^{\frac{2\pi i}{9}} + e^{-\frac{2\pi i}{9}} = 2\cos\frac{2\pi}{9}$$

è un elemento lasciato fisso da α^3. Ora, osserviamo che

$$\begin{aligned}&\zeta^6+\zeta^3+1=0\\&\Rightarrow \zeta^3+\zeta^{-3}+1=0,\end{aligned}$$

inoltre $(\zeta+\zeta^{-1})^3=\zeta^3+\zeta^{-3}+3\zeta+3\zeta^{-1}$, e dunque

$$0=\zeta^3+\zeta^{-3}+1=(\zeta+\zeta^{-1})^3-3(\zeta+\zeta^{-1})+1.$$

In altre parole, $\zeta+\zeta^{-1}$ è radice di X^3-3X+1, che è un polinomio irriducibile su $\mathbb{Q}$. Concludiamo che $\mathbb{Q}(\zeta+\zeta^{-1})=\mathbb{Q}(2\cos\frac{2\pi}{9})$ è l'estensione di grado 3 corrispondente a K.

2. (a) Sia α una radice di P in una estensione di K. Il campo $F=K[\alpha]$ è una estensione di grado d di K; mostriamo che è un campo di spezzamento per P. Se p^k è il numero di elementi di K, allora F ha $(p^k)^d=p^{kd}$ elementi. Quindi F è un campo di spezzamento di $X^{p^{kd}}-X$ sul campo primo $\mathbb{F}_p$ ed è perciò normale su $\mathbb{F}_p$. Ne segue che F è una estensione normale anche di K e dunque, dato che è generato da radici di P, che è un campo di spezzamento di P su K.

   (b) Il polinomio P è il prodotto di un certo numero di fattori di grado 1 per un polinomio Q che non ha radici in K. Il campo L è un campo di spezzamento per Q. Dato che Q ha grado al più 5 le possibilità sono:

   i. Q è irriducibile di grado h con $2\leq h\leq 5$; $[L:K]=h$.
   ii. $Q=Q_1Q_2$, dove Q_1 e Q_2 sono irriducibili di gradi 2 e 3; dato che questi gradi sono primi fra loro $[L:K]=6$.
   iii. $Q=Q_1Q_2$, dove Q_1 e Q_2 sono irriducibili di grado 2; in questo caso il campo di spezzamento sia di Q_1 che di Q_2 è $\mathbb{F}_{3^2}$, che quindi coincide con L. Dunque $[L:K]=2$.

   Per mostrare che tutte le possibilità elencate si presentano effettivamente basta osservare che ci sono polinomi irriducibili su $\mathbb{F}_3$ di grado h per ogni $h>0$. In effetti $\mathbb{F}_{3^h}$ è una estensione di grado h di $\mathbb{F}_3$, ed è semplice, cioè della forma $\mathbb{F}[\vartheta]$ per qualche ϑ. Il polinomio minimo di ϑ su $\mathbb{F}_3$ è irriducibile di grado h.

3. (a) Se G è un gruppo di ordine p^2q^2 il numero dei suoi q-Sylow divide p^2, quindi può essere uguale solo a $1, p$ o p^2. Inoltre è congruo a 1 modulo q. Però $p-1$ e $p^2-1=(p+1)(p-1)$ non sono divisibili per q, dato che $p+1$ e $p-1$ sono strettamente minori di q. Il numero dei p-Sylow di G divide q^2, quindi può essere uguale solo a $1, q$ o q^2. Inoltre è congruo a 1 modulo p. Però $q-1=p+1$ non è divisibile per p, perché non lo è 1, e se p dividesse $q^2-1=(p+3)(p+1)$ allora dividerebbe $p+3$ e quindi anche 3.

   Quindi G è prodotto diretto del suo unico p-Sylow H e del suo unico q-Sylow K. D'altra parte gli ordini di H e K sono quadrati di primi e quindi H e K sono abeliani. Ne segue che $G\simeq H\times K$ è abeliano.

   (b) Sia K il prodotto diretto di due gruppi ciclici di ordine 5. Il gruppo $\mathrm{Aut}(K)$ si identifica al gruppo delle matrici 2×2 a coefficienti in $\mathbb{F}_5$. Questo gruppo contiene elementi di ordine 3, ad esempio

$$A=\begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix}$$

Sia H un gruppo di ordine 9, quindi ciclico o isomorfo al prodotto diretto di due gruppi ciclici di ordine 3. In ogni caso H ammette un omomorfismo non banale su un gruppo ciclico di ordine 3, e quindi sul sottogruppo di $\mathrm{Aut}(K)$ generato da A. Se chiamiamo α questo omomorfismo, $G = K \rtimes_\alpha H$ ha ordine $3^2 5^2$ e non è abeliano.