Corso di Algebra 2 – a.a. 2013-2014

Prova scritta del 2.2.2015

1. Sia $p(X) = X^6 - 3X^4 + 3X^2 - 2 \in \mathbb{Q}[X]$. Determinare il gruppo di Galois di $p(X)$ sui razionali e dire se $p(X)$ è risolubile per radicali.

2. Sia p un primo. Sia $P(X) \in \mathbb{F}_p[X]$ il polinomio $X^5 - 2$.

   (a) Dire se $P(X)$ è irriducibile per $p = 3$ e per $p = 11$.

   (b) Calcolare il gruppo di Galois di P su $\mathbb{F}_p$ per $p = 3$ e per $p = 11$.

3. Siano p e q numeri primi distinti, e sia G un gruppo di ordine p^2q^2.

   (a) Mostrare che G non è semplice.

   (b) Mostrare che G è risolubile.

   (c) Mostrare che G è abeliano se e solo se un suo p-sottogruppo di Sylow è contenuto nel centro di G.

Soluzioni

1. Scriviamo

$$\begin{aligned} p(X) &= X^6 - X^4 + X^2 - 2X^4 + 2X^2 - 2 \\ &= (X^2 - 2)(X^4 - X^2 + 1). \end{aligned}$$

   Notiamo che $X^4 - X^2 + 1 = \Phi_{12}(X)$ è il 12° polinomio ciclotomico. Sia

$$\zeta = e^{\frac{i\pi}{6}} = \frac{\sqrt{3}}{2} + \frac{i}{2}.$$

   ζ è una radice dodicesima primitiva dell'unità. Osserviamo che $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{3}+i) = \mathbb{Q}(\sqrt{3}, i)$. Infatti, $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\sqrt{3}, i)$ ed entrambe le estensioni hanno grado 4 su $\mathbb{Q}$. Dunque, un campo di spezzamento di $p(X)$ su $\mathbb{Q}$ è dato da $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$. Inoltre,

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) : \mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8,$$

   poiché $i \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$ e $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Possiamo già concludere che $p(X)$ è risolubile per radicali, poiché il gruppo di Galois di $p(X)$ su $\mathbb{Q}$ ha ordine 8, e ogni gruppo di ordine 8 è risolubile.

   Notiamo che $K_1 = \mathbb{Q}(\sqrt{2}), K_2 = \mathbb{Q}(\sqrt{3}), K_3 = \mathbb{Q}(i)$ sono estensioni normali (quadratiche) di $\mathbb{Q}$. Allora, sono ben definiti gli omomorfismi di restrizione:

$$\mathrm{res}_i : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(K_i/\mathbb{Q}).$$

   Prendendo il loro prodotto diretto, otteniamo un omomorfismo

$$F = (\mathrm{res}_1, \mathrm{res}_2, \mathrm{res}_3) : \mathrm{Gal}(K/\mathbb{Q}) \to \prod_{i=1}^{3} \mathrm{Gal}(K_i/\mathbb{Q}).$$

F è iniettivo: infatti, se $\alpha \in \ker F$, allora $\alpha_{|K_i} = \mathrm{id}$ per ogni i, ma i K_i generano K come estensione su $\mathbb{Q}$, dunque $\alpha = \mathrm{id}$. Inoltre, F è suriettivo. Infatti, sia $(\alpha_1, \alpha_2, \alpha_3) \in \prod_{i=1}^{3} \mathrm{Gal}(K_i/\mathbb{Q})$; poiché $K_i \cap K_j = \mathbb{Q}$ per $i \neq j$, possiamo definire $\alpha \in \mathrm{Gal}(K/\mathbb{Q})$ semplicemente sui generatori:

$$\alpha : \begin{cases} \sqrt{2} & \mapsto \alpha_1(\sqrt{2}) \\ \sqrt{3} & \mapsto \alpha_2(\sqrt{3}) \\ i & \mapsto \alpha_3(i) \end{cases}$$

ed estenderlo univocamente su K. Tale α, per costruzione, è un elemento della controimmagine di $(\alpha_1, \alpha_2, \alpha_3)$. Concludiamo che F è un isomorfismo, e in particolare $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2 \times C_2$.

2. (a) Per il teorema di Abel $P(X)$ è irriducibile se e solo se non ha radici in $\mathbb{F}_p$. Supponiamo dapprima che $p = 3$. Se $h \in \mathbb{F}_3$, allora $h^5 = h^3h^2 = h \cdot h^2 = h^3 = h$. Quindi la sola radice di $P(X)$ in $\mathbb{F}_3$ è $2 = -1$. Inoltre $P(X) = X^5 + 1 = (X+1)(X^4 - X^3 + X^2 - X + 1)$. Il polinomio $Q(X) = X^4 - X^3 + X^2 - X + 1$ è irriducibile. Infatti non ha radici in $\mathbb{F}_3$, per quanto appena detto, e se fosse prodotto di due polinomi monici di primo grado questi dovrebbero avere lo stesso termine noto. Se questo fosse 1 si dovrebbe avere che

$$Q(X) = (X^2 + aX + 1)(X^2 + bX + 1)$$

da cui $a + b = -1$ e $ab + 2 = 1$, cioè $ab = -1$. L'ultima di queste relazioni implica che uno tra a e b vale 1 e l'altro -1. Ma allora $a + b = 0$. Se invece i termini noti fossero uguali a -1 si dovrebbe avere che

$$Q(X) = (X^2 + aX - 1)(X^2 + bX - 1)$$

da cui $a + b = -1$ e $a + b = 1$, una contraddizione.

Supponiamo invece che $p = 11$. Il gruppo moltiplicativo $\mathbb{F}_{11}^*$ è ciclico di ordine 10 e quindi il suo sottogruppo costituito da tutte le quinte potenze ha ordine 2 ed è perciò $\{1, -1\}$. Ne segue che 2 non è la quinta potenza di un elemento di $\mathbb{F}_{11}$, e quindi che $P(X)$ non ha radici in $\mathbb{F}_{11}$, cioè che è irriducibile.

(b) Supponiamo che $p = 11$. Sia ξ una radice di $P(X)$. Il campo $L = \mathbb{F}_{11}[\xi]$ è una estensione normale di $\mathbb{F}_{11}$ di grado 5 e quindi è un campo di spezzamento per $P(X)$. Il gruppo di Galois di L su $\mathbb{F}_{11}$ è ciclico di ordine 5 e generato dall'omomorfismo di Frobenius.

Supponiamo invece che $p = 3$. Il campo di spezzamento di $P(X)$ coincide con quello di $Q(X)$. Se ξ è una radice di $Q(X)$, allora il ragionamento fatto per $p = 11$ mostra che $L = \mathbb{F}_3[\xi]$ è un campo di spezzamento di $Q(X)$ e ha grado 4 su $\mathbb{F}_3$. Il gruppo di Galois di L su $\mathbb{F}_3$ è ciclico di ordine 4 e generato dall'omomorfismo di Frobenius.

3. (a) Supponiamo che $p < q$. Il numero n_q dei q-Sylow è della forma $1 + kq$ e divide p^2. Dunque $n_q = 1$ oppure q divide $p - 1$ oppure q divide $p^2 - 1$. La seconda di queste possibilità non si presenta in quanto $p < q$. Nel terzo caso $q \big| (p+1)(p-1)$ e quindi q divide $p - 1$, il che è impossibile, oppure divide $p + 1$, cioè $q = p + 1$, il che accade solo quando $p = 2$ e $q = 3$. In conclusione, o vi è un unico q-Sylow, che è quindi normale, oppure l'ordine di G è 12. Ma sappiamo che i gruppi di ordine non primo < 60 non sono semplici.

(b) Supponiamo sempre che $p < q$. Per il punto precedente G ha un sottogruppo normale non banale H. Basta mostrare che sia H che il quoziente G/H sono risolubili. Entrambi questi gruppi hanno ordine primo, quadrato di un primo, oppure prodotto di due primi, oppure prodotto di un primo e del quadrato di un altro. Nei primi due casi abbiamo a che fare con gruppi abeliani, quindi risolubili. Un gruppo di ordine pq ha un sottogruppo normale di ordine q con quoziente di ordine p, e quindi è risolubile. Un gruppo di ordine p^2q o pq^2 non è semplice, quindi ragionando come sopra si mostra che è risolubile.

(c) Siano P e Q un p-Sylow e un q-Sylow. Se G è abeliano, coincide con il suo centro, quindi P è contenuto nel centro di G. Viceversa, supponiamo che P sia contenuto nel centro di G. Allora P è normale. Sappiamo che $G = PQ$, cioè che ogni elemento di G è della forma $g = g_1g_2$ con $g_1 \in P$ e $g_2 \in Q$. Ma allora $gQg^{-1} = g_1g_2Qg_2^{-1}g_1^{-1} = g_1Qg_1^{-1} = Q$; l'ultima di queste uguaglianze segue dal fatto che P è contenuto nel centro di G. In conclusione anche Q è normale, e quindi G è prodotto diretto di P e Q. La tesi segue dal fatto che sia P che Q sono abeliani, dato che i loro ordini sono quadrati di primi.