Corso di Algebra 2 – a.a. 2012-2013

Prova scritta del 11.6.2013

1. (a) Mostrare che il polinomio $P(X) = X^5 - 6X^2 + 2 \in \mathbb{Q}[X]$ non è risolubile per radicali e calcolarne il gruppo di Galois.

   (b) Mostrare che il polinomio $Q(X) = X^6 - 3X^2 + 3 \in \mathbb{Q}[X]$ è risolubile per radicali.

2. Sia p un primo dispari, sia $\Phi_p(X)$ il p-esimo polinomio ciclotomico, sia $\zeta \neq 1$ una radice p-esima dell'unità, e poniamo $L = \mathbb{Q}[\zeta]$.

   (a) Mostrare che L contiene una sola estensione F di grado 2 su $\mathbb{Q}$.

   (b) Mostrare che in $F[X]$ il polinomio Φ_p è prodotto di due fattori irriducibili Q e R e dire quali sono le radici di Q e di R.

3. (a) Mostrare che a meno di isomorfismo vi è un solo gruppo non abeliano G di ordine $5^2 \cdot 11^2$ i cui sottogruppi di Sylow sono ciclici.

   (b) Determinare il centro di G e i normalizzanti dei sottogruppi di Sylow di G.

Soluzioni

1. (a) Il polinomio P è di Eisenstein rispetto al primo 2, quindi è irriducibile; inoltre ha grado primo $p = 5$. Si sa che se ha esattamente $p - 2$ radici reali il suo gruppo di Galois è il gruppo simmetrico S_5. Mostriamo che P ha esattamente 3 radici reali. La derivata di P è $5X^4 - 12X = X(5X^3 - 12)$; per valori reali dell'argomento si annulla solo quando $X = 0$ o $X = \eta = \left(\frac{12}{5}\right)^{1/3}$. D'altra parte $P(0) = 2 > 0$ e

$$P(\eta) = \left(\frac{12}{5} - 6\right)\eta^2 + 2 = -\frac{18}{5}\eta^2 + 2 < 0$$

   perché $\eta > 1$. Dato che $P(X) \to \pm\infty$ per $X \to \pm\infty$ ne segue che $P(X)$ si annulla solo per tre valori reali di X, uno minore di 0, uno strettamente compreso tra 0 e η e uno maggiore di η. Quindi il gruppo di Galois di P è S_5, che contiene il gruppo semplice A_5 e quindi non è risolubile. Se ne deduce che $P(X)$ non è risolubile per radicali.

   (b) Le radici di $Q(X)$ sono $\pm\sqrt{a}$, $\pm\sqrt{b}$, $\pm\sqrt{c}$, dove a, b, c sono le radici del polinomio cubico $S(X) = X^3 - 3X + 3$. Dato che ogni polinomio cubico è risolubile per radicali, esiste una estensione per radicali L di $\mathbb{Q}$ che contiene a, b e c. Ne segue che $L[\sqrt{a}, \sqrt{b}, \sqrt{c}]$ è una estensione per radicali di $\mathbb{Q}$ contenente tutte le radici di Q.

2. (a) L è la p-esima estensione ciclotomica di $\mathbb{Q}$ ed è il campo di spezzamento di $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Il gruppo di Galois $Gal(L/\mathbb{Q})$ si identifica a $(\mathbb{Z}/(p))^*$, che è ciclico di ordine $p - 1$. Per il teorema fondamentale della teoria di Galois le estensioni di grado 2 di $\mathbb{Q}$ contenute in L sono in corrispondenza biunivoca con i sottogruppi di $Gal(L/\mathbb{Q})$ di indice 2, cioè di ordine $\frac{p-1}{2}$. Dato che ogni gruppo ciclico finito contiene un unico sottogruppo di ordine d per ogni divisore d del suo ordine, ne segue che L contiene un'unica estensione di grado 2 di $\mathbb{Q}$.

(b) Il gruppo $Gal(L/F)$ si identifica all'unico sottogruppo di ordine $\frac{p-1}{2}$ di $Gal(L/\mathbb{Q})$, che è il sottogruppo costituito da tutti i quadrati. Le radici di Φ_p sono tutte della forma ζ^i, dove i è un intero modulo p non nullo, e si possono dividere in due gruppi, quelle per cui i è un quadrato e quelle per cui non lo è. Sia $\alpha = \beta^2$ un elemento di $Gal(L/F)$, dove $\beta \in Gal(L/\mathbb{Q})$. L'automorfismo β manda ζ in una potenza ζ^h, dove h è un intero non nullo modulo p. Quindi $\alpha(\zeta^i) = \alpha(\zeta)^i = \zeta^{h^2 i}$. D'altra parte i è un quadrato modulo p se e solo se lo è $h^2 i$. Ne segue che α permuta tra loro le radici ζ^i per cui i è un quadrato modulo p e fa lo stesso per le radici ζ^i per cui i non è un quadrato modulo p. Ora poniamo

$$Q(X) = \prod_{\substack{i \in (\mathbb{Z}/(p))^* \\ i \text{ è un quadrato}}} (X - \zeta^i) \; ; \quad R(X) = \prod_{\substack{i \in (\mathbb{Z}/(p))^* \\ i \text{ non è un quadrato}}} (X - \zeta^i)$$

Per quanto detto sopra $Q(X)$ e $R(X)$ sono invarianti per l'azione di $Gal(L/F)$ e quindi i loro coefficienti appartengono al campo fisso di $Gal(L/F)$, che è F. Inoltre, chiaramente,

$$Q(X)R(X) = \prod_{i \in (\mathbb{Z}/(p))^*} (X - \zeta^i) = \Phi_p(X)$$

Se i e j sono quadrati modulo p il loro rapporto è un quadrato modulo p, quindi $j = k^2 i$ per qualche k. In altri termini $\zeta^j = \gamma(\zeta^i)$, dove γ è l'elemento di $Gal(L/F)$ corrispondente a k^2. Ne segue che $Gal(L/F)$ agisce transitivamente sulle radici ζ^i di Φ_p per cui i è un quadrato. Un analogo ragionamento mostra che lo stesso vale per le radici ζ^i per cui i non è un quadrato. Questo mostra che Q e R sono irriducibili in $F[X]$.

3. (a) Sia G un gruppo di ordine $5^2 \cdot 11^2$ con sottogruppi di Sylow ciclici. Il numero degli 11-Sylow divide 25 ed è congruo a 1 modulo 11, quindi vale 1. Dunque G ha un unico 11-Sylow H, che è normale. Sia K un 5-Sylow. Il gruppo G è un prodotto semidiretto $H \rtimes_\varphi K$, dove φ è un omomorfismo $K \to \mathrm{Aut}(H)$. Il gruppo G è non abeliano se e solo se φ non è banale. Dato che H è ciclico di ordine 11^2 il suo gruppo di automorfismi si identifica al gruppo moltiplicativo $(\mathbb{Z}/(11^2))^*$, che è ciclico di ordine $11^2 - 11 = 110 = 2 \cdot 5 \cdot 11$; un generatore di questo gruppo è ad esempio la classe di 2. In particolare $\mathrm{Aut}(H)$ ha un unico sottogruppo L di ordine 5. L'ordine dell'immagine di φ divide l'ordine di K, cioè 5^2, e l'ordine di $\mathrm{Aut}(H)$. Quindi se φ non è banale ha per immagine L. Osserviamo che esiste un unico omomorfismo suriettivo $K \to L$, a meno di automorfismi di K. Quindi, a meno di isomorfismo, vi è un unico gruppo non abeliano con le caratteristiche richieste.

(b) Usiamo le notazioni del punto (a). Il nucleo di φ è l'unico sottogruppo di ordine 5 di K, che indichiamo con M. Ogni elemento di G si scrive in modo unico sotto la forma hk, dove $h \in H$, $k \in K$. Un tale elemento appartiene al centro di G se e solo se commuta con ogni altro elemento $h'k' \in G$. Dato che H e K sono abeliani ciò si traduce in

$$h\varphi_k(h')kk' = hkh'k' = h'k'hk = h'\varphi_{k'}(h)k'k = \varphi_{k'}(h)h'kk' \qquad \forall\ h' \in H,\ k' \in K$$

cioè

$$h\varphi_k(h') = \varphi_{k'}(h)h' \qquad \forall\ h' \in H,\ k' \in K \tag{1}$$

Per $k' = 1$ questo dice che

$$\varphi_k(h') = h' \qquad \forall\ h' \in H$$

cioè che $k \in \ker(\varphi) = M$. Quando $k \in M$ la condizione (1) diventa

$$h = \varphi_{k'}(h) \qquad \forall\ k' \in K \tag{2}$$

o anche, vista la descrizione di $\mathrm{Aut}(H)$ e dell'immagine di φ, cioè di L,

$$h = h^n \qquad \forall\ n \text{ tale che } n^5 \equiv 1 \mod 121 \tag{3}$$

Ora $3^5 = 243 \equiv 1 \mod 121$. Se $h = h^3$ allora $h^2 = 1$, il che implica $h = 1$ perché l'ordine di H non è divisibile per 2. In conclusione, il centro di G è M.
Dato che H è normale il suo normalizzatore è G. Quanto a K, un elemento hk di G, dove $h \in H$ e $k \in K$, appartiene a $N(K)$ se e solo se $hkk'k^{-1}h^{-1} \in K$ per ogni $k' \in K$, cioè se e solo se $h\ell h^{-1} \in K$ per ogni $\ell \in K$. Ma dato che

$$h\ell h^{-1} = h\varphi_\ell(h^{-1})\ell$$

questa condizione si traduce in

$$h\varphi_\ell(h^{-1}) \in K \qquad \forall\ \ell \in K$$

e dato che $H \cap K = \{1\}$ in

$$\varphi_\ell(h) = h \qquad \forall\ \ell \in K$$

Come si è mostrato sopra, questo succede solo quando $h = 1$. In conclusione, $N(K) = K$.