

Corso di Algebra 2 – a.a. 2013-2014

Prova scritta del 17.6.2014

1. Sia $p(X) = X^5 + X^4 - 2X^3 - 2X^2 - 2X + 1 \in \mathbb{Q}[X]$.
 - (a) Calcolare il gruppo di Galois di $p(X)$ sui razionali.
 - (b) Dire se $p(X) = 0$ è risolubile per radicali.
2. Sia K un campo di caratteristica $p > 0$ e sia F una sua estensione di grado finito. Sia n un intero positivo. Indichiamo con ϕ l'omomorfismo di Frobenius. Supponiamo che ϕ^n appartenga al gruppo di Galois di F su K .
 - (a) Mostrare che K è un campo finito e determinare il massimo numero N di elementi che può contenere.
 - (b) Mostrare che $\#(K) = N$ se e solo se $Gal(F/K)$ è generato da ϕ^n .
3. Sia G un gruppo di ordine $1125 = 3^2 \cdot 5^3$, tale che un suo 5-sottogruppo di Sylow sia ciclico.
 - (a) Mostrare che G è abeliano.
 - (b) Determinare tutte le classi di isomorfismo a cui G può appartenere.

Soluzioni

1. (a) Notiamo che, se ω è una radice cubica primitiva dell'unità, allora ω è radice di $p(X)$. Questo significa che il polinomio $X^2 + X + 1$ divide $p(X)$. Effettuando la divisione, si trova la fattorizzazione (in fattori irriducibili sui razionali):

$$p(X) = (X^2 + X + 1)(X^3 - 3X + 1)$$

Sia $\alpha \in \mathbb{R}$ una radice di $X^3 - 3X + 1$. Osserviamo che anche

$$F(\alpha) = \frac{\alpha - 1}{\alpha}$$

è radice di quel polinomio. Un campo di spezzamento di $X^3 - 3X + 1$ è dunque dato da $\mathbb{Q}(\alpha)$. Chiaramente, un campo di spezzamento di $X^2 + X + 1$ è dato da $\mathbb{Q}(\omega)$. Dunque, un campo di spezzamento di $p(X)$ su \mathbb{Q} è $\mathbb{Q}(\alpha, \omega)$. Calcoliamo il grado dell'estensione:

$$\begin{aligned} [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] &= 2, \\ [\mathbb{Q}(\alpha) : \mathbb{Q}] &= 3, \\ [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] &= [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 6. \end{aligned}$$

Notiamo poi che $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = 2$, poiché $\omega \notin \mathbb{R}$, e che $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)] = 3$, in quanto

$$\begin{aligned} 6 &= [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)] \cdot 2. \end{aligned}$$

Siano ora

$$\begin{aligned} H &= \text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}(\omega)) \cong C_3, \\ K &= \text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}(\alpha)) \cong C_2, \\ G &= \text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}). \end{aligned}$$

Poiché le estensioni $\mathbb{Q}(\alpha)/\mathbb{Q}$ e $\mathbb{Q}(\omega)/\mathbb{Q}$ sono normali, H e K sono sottogruppi normali di G . Concludiamo che $G \cong C_2 \times C_3 \cong C_6$.

- (b) Il gruppo di Galois di $p(X)$ è abeliano, quindi risolubile. Ne segue che $p(X) = 0$ è risolubile per radicali.
2. (a) Gli elementi di K sono lasciati fissi da ϕ^n . Ciò significa che, se $a \in K$, allora $a = \phi^n(a) = a^{p^n}$. Quindi gli elementi di K sono tutti radici del polinomio $X^{p^n} - X$. In altre parole K è un sottocampo di \mathbb{F}_{p^n} . Quindi $N = p^n$.
- (b) Sia $L \subset F$ il campo fisso di ϕ^n . Per ipotesi, $K \subset L$. Si sa che $L = \mathbb{F}_{p^n}$ e d'altra parte che il gruppo $\text{Gal}(F/L)$ è generato da ϕ^n . Ne segue che $\text{Gal}(F/K)$ è generato da ϕ^n se e solo se $K = L$, cioè se e solo se $\#(K) = p^n = N$.
3. (a) G ha un unico 5-Sylow, che dunque è normale; infatti il numero dei 5-Sylow da un lato divide 9 e dall'altro è congruo a 1 modulo 5. Sia K il 5-Sylow e sia H un 3-Sylow (di ordine 9). Sappiamo che G è isomorfo ad un prodotto semidiretto $K \rtimes_{\varphi} H$, per un qualche omomorfismo

$$\varphi : H \rightarrow \text{Aut}(K).$$

Poiché K è ciclico di ordine 5^3 , abbiamo che $\text{Aut}(K) \simeq (\mathbb{Z}/(5^3))^*$ è un gruppo di ordine $5^3 - 5^2 = 100$. D'altra parte

$$9 = \#(H) = \#(\varphi(H))\#(\ker \varphi),$$

dunque $\#(\varphi(H)) \mid 9$ e del resto $\#(\varphi(H)) \mid 100$. Concludiamo che $\#(\varphi(H)) = 1$, quindi φ è l'omomorfismo banale e G è isomorfo al prodotto diretto $K \times H$. Ora, H ha ordine il quadrato di un primo, dunque è abeliano; concludiamo che $G \cong K \times H$ è abeliano.

- (b) Il gruppo H è isomorfo a C_{125} , mentre K può essere isomorfo a C_9 o a $C_3 \times C_3$. Quindi G è isomorfo a $C_{1125} \simeq C_{125} \times C_9$ oppure a $C_{375} \times C_3 \simeq C_{125} \times C_3 \times C_3$.