Corso di Algebra 2 – a.a. 2011-2012

Prova scritta del 27.9.2012

1. Sia G un gruppo di ordine $385 = 5 \cdot 7 \cdot 11$.
   (a) Quanti possono essere i 5-Sylow, i 7-Sylow e gli 11-Sylow di G?
   (b) Mostrare che un 7-Sylow di G è contenuto nel centro di G.

2. Sia F un campo di spezzamento di $(X^5 - 2)(X^2 - 5)$ su $\mathbb{Q}$.
   (a) Mostrare che, se η è una radice quinta primitiva dell'unità, allora $(2(\eta + \eta^4) + 1)^2 = 5$ e quindi $\mathbb{Q}[\eta + \eta^4] = \mathbb{Q}[\sqrt{5}]$.
   (b) Trovare tutti i sottocampi di F che hanno grado 4 su $\mathbb{Q}$.

3. Si consideri il campo $K = \mathbb{F}_3(t)$, dove t è una indeterminata su $\mathbb{F}_3$. Sia $L \supset K$ un campo di spezzamento di $P(X) = X^6 + t^2 + t - 1$ su K.
   (a) Mostrare che il polinomio $P(X)$ è irriducibile in $K[X]$.
   (b) Trovare due sottocampi $F_1 \neq F_2$ di L contenenti K tali che $Gal(L/F_1) = Gal(L/F_2)$.

Soluzioni

1. (a) Il numero degli 11-Sylow è congruo a 1 modulo 11 e divide 35, quindi vale 1. Il numero dei 7-Sylow è congruo a 1 modulo 7 e divide 55, quindi vale 1. In particolare, l'unico 7-Sylow e l'unico 11-Sylow sono normali. Infine il numero dei 5-Sylow è congruo a 1 modulo 5 e divide 77, quindi può essere uguale solo a 1 o a 11. Un esempio in cui si presenta la prima di queste possibilità è il prodotto diretto $C_5 \times C_7 \times C_{11}$ di tre gruppi ciclici di ordini 5, 7 e 11. Un esempio in cui si presenta la seconda di questa possibilità è fornito dal prodotto diretto di un gruppo ciclico di ordine 7 e di un gruppo non abeliano di ordine $55 = 5 \cdot 11$. Un tale gruppo esiste perchè 11 è congruo a 1 modulo 5.
   (b) Siano H, K e M l'unico 11-Sylow, l'unico 7-Sylow e un 5-Sylow. Dato che H e K sono normali e hanno intersezione $\{1\}$, il prodotto HK è diretto, e quindi è un gruppo abeliano. In particolare ogni elemento di K commuta con ogni elemento di H, oltre che, ovviamente, con ogni elemento di K. Il prodotto KM è un sottogruppo di G in quanto uno dei due fattori è normale e quindi $KM = MK$. Inoltre $K \cap M = \{1\}$ e quindi KM ha ordine $\#K \cdot \#M = 7 \cdot 5$. Dato che 7 non è congruo a 1 modulo 5 il gruppo KM è abeliano, e quindi in particolare ogni elemento di K commuta con ogni elemento di M. Dato che ogni elemento di G è un prodotto di elementi di H, K e M ogni elemento di K commuta con ogni elemento di G.

2. (a) $(2(\eta + \eta^4) + 1)^2 = 4(\eta^2 + 2 + \eta^3) + 4(\eta + \eta^4) + 1 = 4(1 + \eta + \eta^2 + \eta^3 + \eta^4) + 5 = 5$ dato che, per ogni n, la somma di tutte le radici n-esime dell'unità vale zero. Inoltre $2(\eta + \eta^4) + 1$ è positivo e dunque uguale a $\sqrt{5}$. Quindi $\mathbb{Q}[\sqrt{5}] \subset \mathbb{Q}[\eta + \eta^4]$, e viceversa $\mathbb{Q}[\eta + \eta^4] \subset \mathbb{Q}[\sqrt{5}]$ perché $\eta + \eta^4 = (\sqrt{5} - 1)/2$.
   (b) Il campo F contiene un campo di spezzamento di $X^5 - 2$, quindi tutte le radici quinte dell'unità. Poniamo $L = \mathbb{Q}[\eta]$, dove $\eta \in F$ è una radice quinta primitiva dell'unità. Dato che L contiene $\sqrt{5}$ per il punto (a), F coincide con il campo di spezzamento di

$X^5 - 2$. Dunque $F = \mathbb{Q}[\eta, \zeta] = L[\zeta]$, dove $\zeta = \sqrt[5]{2}$. Notiamo che $[F : \mathbb{Q}] = [F : L][L : \mathbb{Q}] = 5 \cdot 4 = 20$. Il gruppo di Galois $G = Gal(F/\mathbb{Q})$ ha quindi ordine 20. Dato che L è una estensione Galoisiana di $\mathbb{Q}$, per il teorema fondamentale della teoria di Galois $Gal(F/L)$ è un sottogruppo normale di G e ha ordine pari a $[F : L] = 5$; quindi è l'unico 5-sottogruppo di Sylow di G. Dato che, sempre per il teorema fondamentale della teoria di Galois, i sottogruppi di ordine 5 di G, cioè di indice 4 in G, sono in corrispondenza biunivoca con i sottocampi di F di grado 4 su $\mathbb{Q}$, esiste un solo sottocampo con queste caratteristiche, ed è L.

3. (a) Il polinomio $P(X)$ è irriducibile per il criterio di Eisenstein. Infatti è della forma $X^6 + a$, dove $a = t^2 + t - 1 \in \mathbb{F}_3[t]$ non ha radici in $\mathbb{F}_3$ e quindi, in quanto di grado 2, è irriducibile, cioè primo.

   (b) Sia $\zeta \in L$ una radice di $P(X)$. Allora

$$P(X) = X^6 - \zeta^6 = (X^3 - \zeta^3)(X^3 + \zeta^3) = (X - \zeta)^3(X + \zeta)^3,$$

dato che siamo in caratteristica 3. Quindi le sole radici di $P(X)$ sono ζ e $-\zeta$, e $L = K[\zeta]$. Poniamo $F_1 = L$ e $F_2 = K[\zeta^3]$. Dato che $F_2 \subset F_1$, $\{1\} = Gal(L/F_1) < Gal(L/F_2)$. Se $\varphi \in Gal(L/F_2)$, allora $0 = \varphi(\zeta^3) - \zeta^3 = (\varphi(\zeta) - \zeta)^3$. Ne segue che $\varphi(\zeta) = \zeta$, cioè che $\varphi = 1$, e dunque che $Gal(L/F_1) = Gal(L/F_2)$. D'altra parte $[K[\zeta] : K] = 6$, $[K[\zeta^3] : K] = 2$, quindi $F_1 \neq F_2$.