Corso di Algebra 2 – a.a. 2011-2012

Prova scritta del 3.7.2012

1. Sia G un gruppo di ordine $875 = 5^3 \cdot 7$.
   (a) mostrare che un 7-Sylow di G è contenuto nel centro di G.
   (b) quali sono gli ordini possibili per il centro di G?
2. Poniamo $f(X) = x^7 - 2 \in \mathbb{Q}[X]$. Sia L un campo di spezzamento di f su $\mathbb{Q}$.
   (a) Determinare $Gal_{\mathbb{Q}}(f)$.
   (b) Trovare una estensione intermedia $L \supset F \supset \mathbb{Q}$ tale che $[F : \mathbb{Q}] = 3$. È unica?
3. Sia $K = \mathbb{F}_5$ il campo con 5 elementi. Poniamo $P(X) = X^3 + X + 1 \in K[X]$.
   (a) Mostrare che P è irriducibile.
   (b) Calcolare il gruppo di Galois $Gal_K(P)$.
   (c) Mostrare che il discriminante di P è il quadrato di un elemento di K.

Soluzioni

1. Il numero dei 7-Sylow è congruo a 1 modulo 7 e divide 5^3; la sola possibilità è che valga 1. Quindi c'è un solo 7-Sylow H, che è normale. Analogamente, il numero dei 5-Sylow è congruo a 1 modulo 5 e divide 7. Dunque c'è un unico 5-Sylow K, anch'esso normale. Ne segue che G è prodotto diretto di H e di K. Il centro di G è il prodotto di H, che è ciclico, e del centro W di K. Il quoziente di K modulo W non può essere ciclico, e W non è ridotto a $\{1\}$, dato che K è un p-gruppo. Quindi il centro di G può coincidere con G o avere ordine $5 \cdot 7 = 35$. Il primo caso si presenta quando G è abeliano. Per vedere che anche il secondo è possibile basta mostrare che esistono gruppi non abeliani di ordine 5^3. Sia M un gruppo ciclico di ordine 5^2. Il gruppo degli automorfismi di M si identifica al gruppo moltiplicativo di $\mathbb{Z}/(5^2)$, che ha ordine 20 e quindi contiene un sottogruppo di ordine 5. Quindi esiste un omomorfismo iniettivo $\varphi : L \to \mathrm{Aut}(M)$, dove L è ciclico di ordine 5. Il gruppo $M \ltimes_\varphi L$ non è abeliano e ha ordine 5^3.
2. (a) $L = \mathbb{Q}[\sqrt[7]{2}, \eta]$, dove η è una radice settima primitiva dell'unità. Il grado $[L : \mathbb{Q}]$ è divisibile per $[\mathbb{Q}[\sqrt[7]{2}] : \mathbb{Q}]$, che vale 7 dato che f è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein, ed è anche divisibile per $[\mathbb{Q}[\eta] : \mathbb{Q}] = 6$. Quindi $[L : \mathbb{Q}] = 6 \cdot 7 = 42$. Poniamo $E = \mathbb{Q}[\eta]$. Il gruppo di Galois $H = Gal(L/E)$ è ciclico di ordine 7, si identifica al gruppo delle radici settime dell'unità ed è normale in $G = Gal(L/\mathbb{Q})$; in particolare è l'unico 7-sottogruppo di Sylow di G. Il gruppo di Galois $Gal(E/\mathbb{Q}) \simeq Gal(L/\mathbb{Q}[\eta])$ si identifica al gruppo moltiplicativo di $\mathbb{Z}/(7)$ ed è quindi ciclico di ordine 6. Il gruppo G è il prodotto semidiretto $H \ltimes_\alpha (\mathbb{Z}/(7))^*$, dove $\alpha : (\mathbb{Z}/(7))^* \to \mathrm{Aut}(H)$ e $\alpha(m)$ è l'automorfismo "elevamento alla m-esima potenza" per ogni $m \in (\mathbb{Z}/(7))^*$.
   (b) Per il teorema fondamentale della teoria di Galois i sottocampi di L di grado 3 su $\mathbb{Q}$ sono in corrispondenza biunivoca con i sottogruppi di G di indice 3. Se M è un tale sottogruppo, deve necessariamente contenere H, che è l'unico sottogruppo di G di ordine 7. Inoltre M/H è un sottogruppo di ordine 2 del gruppo ciclico $(\mathbb{Z}/(7))^*$. Dato

che questo sottogruppo è unico, anche M è unico. Il campo F che stiamo cercando è costituito dagli elementi di L lasciati fissi da M. Il campo fisso di H è $\mathbb{Q}[\eta]$. Il campo F è costituito dagli elementi di $\mathbb{Q}[\eta]$ che sono lasciati fissi dal sottogruppo di ordine due di $(\mathbb{Z}/(7))^*$, cioè da $\{\pm 1\}$. Ricordiamo che $(\mathbb{Z}/(7))^*$ agisce sulle radici settime dell'unità per elevamento a potenza. Ne segue che un elemento di $\mathbb{Q}[\eta]$ non appartenente a $\mathbb{Q}$ che è lasciato fisso da $\{\pm 1\}$ è ad esempio $\eta + \eta^6$. Dunque $\mathbb{Q}[\eta + \eta^6]$ è un sottocampo di F che contiene propriamente $\mathbb{Q}$. Dato che $[F : \mathbb{Q}] = 3$ è primo, la sola possibilità è che $F = \mathbb{Q}[\eta + \eta^6]$.

3. (a) Si verifica direttamente che P non ha radici in K; dato che ha grado 3 questo implica che è irriducibile.

   (b) Se ζ è una radice di P, allora $K[\zeta]$ ha grado 3 su K. Dato che ogni estensione finita di un campo finito è una estensione di Galois, $L = K[\zeta]$ è un campo di spezzamento per P su K. Il gruppo di Galois $Gal_K(P) = Gal(L/K)$ è ciclico di ordine 3, generato dall'automorfismo di Frobenius Φ.

   (c) Un polinomio separabile di grado n a cofficienti in un campo E ha gruppo di Galois contenuto in A_n se e solo se il suo discriminante è il quadrato di un elemento di E. La tesi segue allora dalla parte (b). Un ragionamento più diretto è il seguente. Osserviamo che le tre radici di P sono ζ, $\Phi(\zeta) = \zeta^p$ e $\Phi^2(\zeta) = \zeta^{p^2}$, e che $\Phi^3(\zeta) = \zeta$. D'altra parte il discriminante di P è $\big((\zeta - \Phi(\zeta))(\zeta - \Phi^2(\zeta))(\Phi(\zeta) - \Phi^2(\zeta))\big)^2$ e $\Phi\big((\zeta - \Phi(\zeta))(\zeta - \Phi^2(\zeta))(\Phi(\zeta) - \Phi^2(\zeta))\big) = (\Phi(\zeta) - \Phi^2(\zeta))(\Phi(\zeta) - \zeta)(\Phi^2(\zeta) - \zeta) = (\zeta - \Phi(\zeta))(\zeta - \Phi^2(\zeta))(\Phi(\zeta) - \Phi^2(\zeta))$. Dunque $(\zeta - \Phi(\zeta))(\zeta - \Phi^2(\zeta))(\Phi(\zeta) - \Phi^2(\zeta))$ appartiene a K.