Corso di Algebra 2 – a.a. 2011-2012

Prova scritta del 18.6.2012

1. Mostrare che non esistono gruppi semplici di ordine $132 = 2^2 \cdot 3 \cdot 11$.

2. Indichiamo con C_k un gruppo ciclico di ordine k. Sia $F \supset K$ una estensione di Galois tale che $Gal(F/K) \simeq C_2 \times C_{12}$. Trovare il numero di estensioni intermedie $F \supset L \supset K$ tali che:

   (a) $[L : K] = 4$.

   (b) $[L : K] = 9$.

   (c) $Gal(L/K) \simeq C_4$.

3. Sia $f(X) \in \mathbb{Q}[X]$ un polinomio irriducibile. Supponiamo che $f(X)$ abbia sia radici reali che radici non reali.

   (a) Mostrare che il gruppo di Galois di f su $\mathbb{Q}$ non è abeliano.

   (b) Se non si suppone f irriducibile si può trarre la stessa conclusione?

Soluzioni

1. Il numero di 11-Sylow è congruo a 1 modulo 11 e divide $2^2 \cdot 3 = 12$, quindi vale 1 o 12. Nel primo caso vi è un unico 11-Sylow che quindi è normale. Nel secondo caso, dato che ogni elemento diverso da 1 di un 11-Sylow ha ordine 11 e l'intersezione di due diversi 11-Sylow è ridotta al solo elemento neutro, vi sono $12 \cdot 10 = 132 - 12$ elementi di ordine 11. Il numero di 3-Sylow è congruo a 1 modulo 3, quindi vale 1 o almeno 4. Nel primo caso vi è un unico 3-Sylow che quindi è normale. Nel secondo caso, ragionando come per gli 11-Sylow, si conclude che vi sono almeno $4 \cdot 2 = 8$ elementi di ordine 3. Restano al più 4 elementi di ordine diverso da 11 e da 3. D'altra parte un 2-Sylow contiene 4 elementi, e nessuno di questi ha ordine 11 o 3. Se ne conclude che vi è un unico 2-Sylow, che quindi è normale.

2. Le estensioni intermedie L sono in corrispondenza biunivoca con i sottogruppi di $G = Gal(F/K)$ tramite $L \mapsto Gal(F/L)$ e $[L : K]$ è l'indice di $Gal(F/L)$ in G.

   (a) dobbiamo contare i sottogruppi H di $G = C_2 \times C_{12}$ che hanno indice 4, cioè quelli di ordine 6. Un tale sottogruppo è sempre ciclico. Gli elementi di ordine 6 di G sono della forma (a, b), dove le possibilità per a e b sono le seguenti:

      i. $a = 1$, b ha ordine 6;

      ii. a è il generatore di C_2, b ha ordine 6;

      iii. a è il generatore di C_2, b ha ordine 3.

      Nel caso i H è l'unico sottogruppo di ordine 6 del fattore C_{12}. Nel caso iii H è il prodotto di C_2 e del sottogruppo di ordine 3 di C_{12}. Anche il caso ii dà luogo a un solo sottogruppo H. Infatti vi sono due possibili scelte per b, e passare dall'una all'altra equivale a passare da (a, b) al suo inverso, cioè da un generatore a un altro dello stesso sottogruppo di G. In conclusione ci sono tre sottocampi L con $[L : K] = 4$.

   (b) dobbiamo contare i sottogruppi di $C_2 \times C_{12}$ che hanno indice 9. Dato che l'indice di un sottogruppo deve dividere $\#(C_2 \times C_{12}) = 24$, non ce ne sono.

(c) Con le notazioni del punto (a), $Gal(L/K) \simeq G/H$. Questo gruppo è ciclico nei sottocasi ii e iii del punto (a). I campi L con le caratteristiche cercate sono quindi due.

3. (a) Il gruppo $G = Gal_{\mathbb{Q}}(f)$ contiene il coniugio complesso, che indichiamo con σ. Sia z una radice reale di f e sia w una radice non reale. Dato che f è irriducibile G agisce in modo transitivo sulle radici di f, quindi vi è un elemento $\tau \in G$ tale che $\tau(z) = w$. Allora $\sigma\tau(z) = \sigma(w) = \overline{w}$, mentre $\tau\sigma(z) = \tau(z) = w$. Dato che $\overline{w} \neq w$ ne deduciamo che $\sigma\tau \neq \tau\sigma$.

   (b) La conclusione non vale. Un controesempio è $f(X) = X^4 - 4 = (X^2 - 2)(X^2 + 2)$, il cui campo di spezzamento è $\mathbb{Q}[\sqrt{-1}, \sqrt{2}]$. Questo campo ha grado 4 su $\mathbb{Q}$ e quindi il suo gruppo di Galois è abeliano; per la precisione è il prodotto di due gruppi di ordine 2.