Corso di Algebra 2 – a.a. 2013-2014

Prova scritta del 23.9.2014

1. Sia $p(X) = X^4 - 10X^2 + 20$. Calcolare il gruppo di Galois di $p(X)$ sui razionali e descrivere esplicitamente la corrispondenza di Galois.

2. Sia G il sottogruppo $\{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$ del gruppo moltiplicativo dei quaternioni. Sia F un campo.

   (a) Mostrare che i gruppi simmetrici S_4 e S_5 non hanno sottogruppi isomorfi a G.

   (b) Mostrare che non esistono polinomi di grado 4 o 5 in $F[X]$ il cui gruppo di Galois sia isomorfo a G.

3. Descrivere, a meno di isomorfismo, tutti i gruppi di ordine $275 = 5^2 \cdot 11$. Per quelli abeliani determinare i divisori elementari.

Soluzioni

1. Effettuiamo il cambio di variabile $Y = X^2$ e risolviamo l'equazione

$$Y^2 - 10Y + 20 = 0.$$

Si vede facilmente che le sue soluzioni sono $5 \pm \sqrt{5}$. Ora, siano $\alpha, \beta \in \mathbb{C}$ tali che

$$\alpha^2 = 5 + \sqrt{5},$$
$$\beta^2 = 5 - \sqrt{5}.$$

Allora, le radici di $p(X)$ sono $\{\pm\alpha, \pm\beta\}$. Notiamo che $(\alpha\beta)^2 = 20$, dunque possiamo supporre che

$$\alpha\beta = \sqrt{2}0 = 2\sqrt{5},$$

a meno di scambiare α con $-\alpha$. Dunque, le radici di $p(X)$ sono effettivamente $\{\pm\alpha, \pm\frac{2\sqrt{5}}{\alpha}\}$, e un campo di spezzamento di $p(X)$ su $\mathbb{Q}$ è dato da $\mathbb{Q}(\alpha, \sqrt{5})$. Osserviamo però che

$$\sqrt{5} = \alpha^2 - 5 \in \mathbb{Q}(\alpha),$$

dunque $\mathbb{Q}(\alpha, \sqrt{5}) = \mathbb{Q}(\alpha)$. Il polinomio $p(X)$ è irriducibile per il criterio di Eisenstein, dunque troviamo che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Ora, sia $G = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. Sappiamo che $|G| = 4$. Un elemento $f \in G$ è determinato dal suo valore $f(\alpha)$, che a sua volta deve essere una radice di $p(X)$. Poniamo

$$f(\alpha) = \frac{2\sqrt{5}}{\alpha}.$$

Notiamo ora che

$$\begin{aligned} f(\sqrt{5}) &= f(\alpha^2 - 5) = f(\alpha)^2 - 5 \\ &= \frac{20}{\alpha^2} - 5 = \frac{20}{5 + \sqrt{5}} - 5 \\ &= \frac{20(5 - \sqrt{5})}{20} - 5 \\ &= -\sqrt{5}. \end{aligned}$$

Un calcolo diretto ci mostra che $f^2(\alpha) = f(f(\alpha)) = -\alpha$. Dunque, f non ha ordine 2 in G, e necessariamente ha ordine 4. Concludiamo che $G = \langle f \rangle \cong C_4$. L'unico sottogruppo non banale di G è quello generato da f^2. Notiamo subito che $f^2(\sqrt{5}) = \sqrt{5}$, e deduciamo così che il campo fisso del sottogruppo $\langle f^2 \rangle$ è $\mathbb{Q}(\sqrt{5})$.

2. (a) S_5 contiene sottogruppi isomorfi a S_4; quindi basta dimostrare il risultato per S_5. Il gruppo G contiene 6 elementi di ordine 4, e precisamente $\{\pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$. Gli elementi di S_5 si ripartiscono, a seconda della loro decomposizione in cicli, nelle seguenti classi: l'identità, i 2-cicli, i 3-cicli, i 4-cicli, i 5-cicli, i prodotti di due 2-cicli disgiunti, i prodotti di un 2-ciclo e di un 3-ciclo disgiunti. Tra questi, i soli elementi di ordine 4 sono i 4-cicli, che sono permutazioni dispari. Ne segue che il prodotto di due elementi di S_5 aventi ordine 4 è una permutazione pari, e quindi non può avere ordine 4. Per contro $\mathbf{ij} = \mathbf{k}$ ha ordine 4.

   (b) Sia $P(X)$ un polinomio a coefficienti in F, sia d il suo grado, e sia $L = F[a_1, \dots, a_e]$ un campo di spezzamento di P su F, dove $a_1, \dots, a_e$, $e \le d$, sono le radici di P. Il gruppo di Galois di P è $Gal(L/F)$, che agisce sulle radici di P permutandole. Inoltre, se un elemento di $Gal(L/F)$ agisce come l'identità sulle radici, agisce in modo banale su tutto L. In altre parole, $Gal(L/F)$ è isomorfo a un sottogruppo di S_e, e quindi di S_d. Quando $d = 4$ o $d = 5$ segue quindi dal punto precedente che $Gal(L/F)$ non può essere isomorfo a G.

3. Sia G un gruppo di ordine 275. Il numero degli 11-Sylow di G divide 25 ed è congruo a 1 modulo 11, quindi deve essere uguale a 1. Dunque G contiene un unico 11-Sylow, che è normale. I 5-Sylow di G hanno ordine 5^2, quindi sono abeliani e più esattamente isomorfi a C_{25} o a $C_5 \times C_5$, dove C_k indica il gruppo ciclico di ordine k. Inoltre sono tutti coniugati e quindi tutti isomorfi tra loro. In conclusione G è isomorfo a un prodotto semidiretto $H \rtimes_\alpha K$, dove $H = C_{11}$, K è C_{25} o $C_5 \times C_5$ e α è un omomorfismo $K \to \mathrm{Aut}(H)$. Ricordiamo che $\mathrm{Aut}(H) \simeq C_{10}$. L'ordine dell'immagine di α divide sia 10 che 25 e quindi non può che valere 1 o 5. Nel primo caso α l'omomorfismo banale, mentre nel secondo l'immagine di α è L, l'unico sottogruppo di ordine 5 di C_{10}, cioè il sottogruppo generato dal quadrato di un qualsiasi generatore di C_{10}. Omomorfismi α non banali esistono sempre. Ad esempio se $K = C_{25}$ si può prendere come α la composizione del passaggio al quoziente $K \to K/\Gamma$ con un isomorfismo tra K/Γ e L, dove Γ è l'unico sottogruppo di ordine 5 di K. Se invece $K = C_5 \times C_5$ si può prendere come α la composizione della proiezione $K \to C_5$ su uno dei due fattori con un isomorfismo tra C_5 e L. Inoltre in ognuno dei due casi due omomorfismi α non banali differiscono solo per un automorfismo di K. Ne segue che la classe di isomorfismo del prodotto semidiretto $H \rtimes_\alpha K$ non dipende dal particolare α scelto. La conclusione è che esistono, a meno di isomorfismo, quattro gruppi di ordine 275:

$$
\begin{aligned}
&C_{11} \times C_{25} \simeq C_{275} \\
&C_{11} \times (C_5 \times C_5) \simeq C_{55} \times C_5 \\
&C_{11} \rtimes_\alpha C_{25} \\
&C_{11} \rtimes_\beta (C_5 \times C_5)
\end{aligned}
$$

dove $\alpha : C_{25} \to C_{10} \simeq \mathrm{Aut}(C_{11})$ e $\beta : C_5 \times C_5 \to C_{10} \simeq \mathrm{Aut}(C_{11})$ sono omomorfismi non banali. I primi due gruppi dell'elenco sono abeliani e i loro divisori elementari sono 275 per il primo, e 55 e 5 per il secondo.