SOLUZIONI DEL COMPITO DI ALGEBRA 1

13 settembre 2013

1. a) Calcolare il centralizzatore in S_6 e in A_6 della permutazione $\sigma = (1,2,3)(4,5,6)$.
b) Determinare le classi di coniugio di A_5.

Soluzione esercizio 1.a) La classe di coniugio di σ in S_6 è costituita da tutte le permutazioni che con prodotto di 2 3-cicli, quindi $|Cl_{S_6}(\sigma)| = \binom{6}{3}\binom{3}{3}2!2!\frac{1}{2} = \frac{6!}{18}$; ne segue che $|Z_{S_6}(\sigma)| = 18$. Chiaramente $\langle(1,2,3)\rangle, \langle(4,5,6)\rangle \subseteq Z_{S_6}(\sigma)$; inoltre $H = \langle(1,2,3)\rangle\langle(4,5,6)$ è un sottogruppo di ${}_{S_6}(\sigma)$ (infatti i due sottogruppi commutano) e ha indice 2, basta quindi aggiungere un ulteriore elemento per generare tutto il centralizzatore. La permutazione che scambia tra loro i due 3-cicli è $\tau = (1,4)(2,5)(3,6)$ e risulta $\tau \in Z_{S_6}(\sigma) \setminus H$ perché le permutazioni in H commutano con entrambi i cicli di σ. Ne segue che $Z_{S_6}(\sigma) = \langle(1,2,3),(4,5,6),\tau\rangle$ e $Z_{A_6}(\sigma) = Z_{S_6}(\sigma) \cap A_6 = H$.

b) Le permutazioni di A_5 sono l'identità i 3-cicli, i 5-cicli e le permutazioni di tipo $(a,b)(c,d)$. Sappiamo che in S_n le classi di coniugio sono costituite dalle permutazioni che hanno la stessa decomposizione ciclica, e che in A_n le classi di coniugio di S_n possono costituire ancora un'unica classe di coniugio o dividersi in due classi con la stessa cardinalità. Più precisamente, vale $|Cl_{A_n}(\rho)| = |Cl_{S_n}(\rho)|/2$ se $Z_{A_n}(\rho) = Z_{S_n}(\rho)$ mentre $Cl_{A_n}(\rho) = Cl_{S_n}(\rho)$ se $Z_{A_n}(\rho) \subsetneq Z_{S_n}(\rho)$. Ricordiamo inoltre $|Z_{A_n}(\rho)| \cdot |Cl_{A_n}(\rho) = |A_n|$.
Ricordati questi fatti generali passiamo al calcolo delle classi di coniugio di A_5. Ovviamente una classe è costituita dalla sola identità. Per quanto riguarda i 3-cicli, questi sono coniugati in A_n per ogni $n \geq 5$, quindi costituiscono un'unica classe di coniugio in A_5. Le doppie trasposizioni in S_A sono in tutto $\binom{5}{2}\binom{3}{2}\frac{1}{2} = 15$ questa cosse di coniugio di S_5 non può spezzarsi in due in A_5 perchè ha cardinalità dispari, quindi le doppie trasposizioni costituiscono un'unica classe di coniugio in A_5. Consideriamo ora i 5-cicli: $|Cl_{S_5}((a,b,c,d,e))| = 4!$ e $Z_{S_5}((a,b,c,d,e)) = \langle(a,b,c,d,e)\rangle \subset A_5$, quindi i 5-cicli in A_5 si dividono in due classi di coniugio. Infatti $(1,2,3,4,5)$ e $(1,2,3,5,4,)$ non sono coniugate in A_5 perché $(1,2,3,4,5) = \tau(1,2,3,5,4,)\tau^{-1}$ se e solo se $\tau \in (4,5)Z((1,2,3,4,5))$ quindi le possibili τ sono tutte dispari.
Riepilogando le classi di coniugio di A_5 sono $Cl(id)$, $Cl((1,2,3))$, $Cl((1,2)(3,4))$, $Cl(1,2,3,4,5))$, $Cl((1,2,3,5,4))$.

2. Dimostrare che un gruppo di ordine p^4 ha sempre un sottogruppo abeliano di ordine p^3.

Soluzione esercizio 2. Sia G un gruppo di ordine p^4, allora $|Z(G)| = p^4, p^2, p$. Infatti, $|Z(G)| \neq 1$ in quanto il centro di un p-gruppo è non banale, e $|Z(G)| = p^3$ perché altrimenti $G/Z(G)$ sarebbe ciclico e sappiamo che questo non è possibile.
Se $|Z(G)| = p^4$, il gruppo G è abeliano, e quindi ha sottogruppi abeliani di ordine d per ogni d che divide l'ordine del gruppo; in particolare ha almeno un sottogruppo ordine p^3.
Sia $|Z(G)| = p^2$ e sia $x \notin Z(G)$ allora $C(x)$ contiene sia x che $Z(G)$, ma non è tutto G perchè $x \notin Z(G)$. Ne segue che $|C(x)| = p^3$ e tale gruppo è sicuramente abeliano perche' il suo centro contiene sia x che $Z(G)$.

Sia $|Z(G)| = p$; per la formula delle classi abbiamo $|G| = |Z(G)| + \sum_{x \in R'} |G|/|C(x)|$, da cui $p^4 = p + \sum_{x \in R'} |G|/|C(x)|$. Osserviamo che gli addendi della sommatoria non possono valere tutti p^2 (altrimenti il membro sinistro sarebbe divisibile per p e non per p^2, mentre deve valere p^4). Ne segue che esiste un $x \in G$ tale che $|C(x)| = p^3$. Questo sottogruppo è abeliano in quanto un gruppo non abeliano di ordine p^3 ha centro di ordine p, mente sia x che $Z(G)$ stanno nel centro di $C(x)$ e chiaramente $x \notin Z(G)$.

3. Siano A e R anelli commutativi con identità con $A \subseteq R$. Il conduttore C di A in R è definito da $C := \{\alpha \in R \,|\, \alpha R \subseteq A\}$.
a) Dimostrare che C è un ideale sia di R che di A.
b) Dimostrare che C è il più grande ideale di A che sia anche ideale di R.
c) Determinare il conduttore di A in R per $A = \mathbb{Z}[\sqrt{-3}]$ e $R = \mathbb{Z}[\zeta_3]$ dove $\zeta_3 = (-1 - \sqrt{-3})/2$.
Soluzione esercizio 3. a)Poiché R contiene l'dentità, è chiaro che $C \subseteq A$. Mostriamo che C è un ideale di R (a maggior ragione sarà un ideale di A). Siano $\alpha, \beta \in R$, dalle condizioni $\alpha R \subseteq A$ e $\beta R \subseteq A$ segue che $(\alpha + \beta)R = \alpha R + \beta R \subseteq A + A = A$ quindi $\alpha + \beta \in C$. Per $\alpha \in C$ e $r \in R$ si ha $(\alpha r)R \subseteq \alpha R \subseteq A$, quindi $\alpha r \in C$.
b) Sia $I \subseteq A$ un ideale di R; vale $IR \subseteq I \subseteq A$, quindi $I \subseteq C$, quindi C contiene tutti gli ideali di R contenuti in A e, avendo esso stesso questa proprietà, è il più grande ideale di R contenuto in A.
c) Sia $\alpha = x + \sqrt{-3}y \in A = \mathbb{Z}[\sqrt{-3}]$; $\alpha \in C$ se e solo se $(x + \sqrt{-3}y)(a + \zeta_3 b) \in A$ per ogni $a + \zeta_3 b \in R$. Essendo C un ideale questa condizione vale se e solo se $(x + \sqrt{-3}y)\zeta_3 \in A$. Ora $(x + \sqrt{-3}y)\zeta_3 = (x + \sqrt{-3}y)(-1 - \sqrt{-3})/2 = -\frac{1}{2}[(x - 3y) + \sqrt{-3}(x + y)]$ e questo elemento appartiene a $A = \mathbb{Z}[\sqrt{-3}]$ se e solo se $x \equiv y \pmod 2$. Abbiamo quindi che $C = \{x + \sqrt{-3}y \in A \,|\, x \equiv y \pmod 2\}$ (si può verificare facilmente che $C = (2, 1 + \sqrt{-3})A = 2R$.)

4. Sia ζ_{11} una radice 11-esima primitiva dell'unità e sia $K = \mathbb{Q}(\zeta_{11}, \sqrt{11})$. Determinare il gruppo di Galois e il reticolo delle sottoestensioni dell'estensione $K/\mathbb{Q}$.
Soluzione esercizio 4. Consideriamo le due sottoestensioni $E = \mathbb{Q}(\zeta_{11})$ e $F = \mathbb{Q}(\sqrt{11})$. Queste sono entrambe di Galois su $\mathbb{Q}$ e si ha $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/10\mathbb{Z}$ e $\mathrm{Gal}(F/\mathbb{Q}) \equiv \mathbb{Z}/2\mathbb{Z}$. Osserviamo che $E \cap F = \mathbb{Q}$: infatti, avendo F grado 2 su $\mathbb{Q}$, basta escludere che $F \subset E$. Se fosse $F \subset E$ allora essendo F un estensione reale, sarebbe contenuta in nella sottoestensione reale di E (che sappiamo essere $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$). Sappiamo che $[\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1}) : \mathbb{Q}] = 10/2 = 5$ e quindi non può contenere una sottoestensione di grado 2. Da questo segue che $E \cap F = \mathbb{Q}$; poiché $EF = K$, applicando un teorema noto, otteniamo che $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Si calcola facilmente che il gruppo $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ha oltre ai sottogruppi banali, 3 sottogruppi di ordine 10, 1 di ordine 5, 1 di ordine 4 e 3 di ordine 2. Dalla corrispondenza di Galois ricaviamo le sottoestensioni di $K/\mathbb{Q}$. Chiaramente i sottogruppi banali corrispondono alle sottoestensioni banali K e $\mathbb{Q}$. Le sottoestensioni di grado 2 su $\mathbb{Q}$ sono fissate dai sottogruppi di ordine 10 e quindi sono 3, L_1, L_2, L_3. C'è una sola sottoestensione di grado 4, fissata dal sottogruppo di ordine 5, e questa sarà necessariamente $L_1 L_2$ perché e facile osservare che tale estensione ha

grado 4. C'è una sola sottoestensione di grado 5 che è $M = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$; da questa otteniamo che le 3 estensioni di grado 10 sono ML_1,ML_2 e ML_3.
Possiamo anche descrivere esplicitamente le sottoestensioni di grado 3 (e quindi anche tutte le altre, che abbiamo espresso in termini di queste estensioni e di altre estensioni note). Poniamo $L_1 = \mathbb{Q}(\sqrt{11})$. Chiamiamo L_2 l'unica sottoestensione di grado 2 di $E = \mathbb{Q}(\zeta_{11})$; questa sottoestensione è fissata dal sottogruppo di ordine 5 di $\mathrm{Gal}(E/\mathbb{Q})$ che è $\langle\sigma_4\rangle$ dove σ_4 è l'automorfismo definito da $\sigma_5(\zeta_{11}) = \zeta_{11}^4$ Si verifica che $\alpha = \zeta_{11} + \zeta_{11}^4 + \zeta_{11}^5 + \zeta_{11}^9 + \zeta_{11}^3$ è fissato da σ_4, quindi $L_2 = \mathbb{Q}(\alpha)$. Si calcola che il polinomio minimo di α è x^2+x+3, da cui si ha $\alpha = (-1\pm\sqrt{-11})/2$, quindi $L_2 = \mathbb{Q}(\sqrt{-11})$ e da questo si ottiene anche che $L_3 = \mathbb{Q}(i)$.