SOLUZIONI DEL COMPITO DI ALGEBRA 1

11 febbraio 2013

Esercizio 1. Dimostrare che il gruppo $\mathrm{Aut}(S_3 \times S_3)$ è isomorfo ad un prodotto semidiretto di $S_3 \times S_3$ e $\mathbb{Z}/2\mathbb{Z}$.

Soluzione esercizio 1. Per il teorema di decomposizione di un gruppo in prodotto semidiretto, dobbiamo individuare un sottogruppo normale H di $\mathrm{Aut}(S_3 \times S_3)$ isomorfo a $S_3 \times S_3$ ed un sottoguppo $K \cong \mathbb{Z}/2\mathbb{Z}$ tali che $H \cap K = \{id\}$ e $HK = \mathrm{Aut}(S_3 \times S_3)$ Ricordiamo innanzitutto che per ogni gruppo G si ha $\mathrm{Int}(G) \trianglelefteq \mathrm{Aut}(G)$ e $\mathrm{Int}(G) \cong G/Z(G)$. In questo caso, poiché il centro di un prodotto diretto è il prodotto diretto dei centri dei fattori, si calcola $\mathrm{Int}(S_3 \times S_3) \cong (S_3 \times S_3)/(Z(S_3) \times Z(S_3)) = S_3 \times S_3$; abbiamo quindi individuato il sottogruppo normale $H = Int(S_3 \times S_3) \cong S_3 \times S_3$. Il sottogruppo K sarà generato da un automorfismo non interno di ordine 2. Consideriamo l'automorfismo ψ che scambia le coordinate: questo ha ovviamente ordine 2 e non è interno, quindi posto $K = \langle \psi \rangle$ si ha $K \cong \mathbb{Z}/2\mathbb{Z}$ tali che $H \cap K = \{id\}$. Resta da far vedere che il sottogruppo HK è tutto il gruppo $\mathrm{Aut}(S_3 \times S_3)$: poiché $|HK| = |H| \cdot |K| = 6^2 \cdot 2 = 72$, basta vedere che $|\mathrm{Aut}(S_3 \times S_3)| = 72$. Sia $\varphi \in \mathrm{Aut}(S_3 \times S_3)$; poichè φ conserva l'ordine degli elementi, in particolare manda elementi di ordine 6 in elementi di ordine 6, quindi, se τ e σ denotano rispettivamente un 2-ciclo ed un 3-ciclo di S_3, si ha $\varphi(\tau, \sigma) = (\tau', \sigma')$ oppure $\varphi(\tau, \sigma) = (\sigma', \tau')$ con τ' 2-ciclo e σ' 3-ciclo. Elevando al quadrato e alla terza potenza si ottiene: $\varphi(id, \sigma) = (id, \sigma')$ oppure $\varphi(id, \sigma) = (\sigma', id)$ e $\varphi(\tau, id) = (\tau', id)$ oppure $\varphi(\tau, id) = (id, \tau')$. Inoltre se τ_1 e τ_2 sono due trasposizioni distinte, $\tau_1 \circ \tau_2 = \sigma$ è un 3-ciclo quindi $\varphi((\tau_1, id)(\tau_2, id)) = \varphi(\tau_1, id)\varphi(\tau_2, id)$ ha ordine 3 e quindi $\varphi(\tau_1, id)$ e $\varphi(\tau_2, id)$ sono entrambe del tipo (τ', id) oppure entrambe del tipo (id, τ'). Facendo lo stesso discorso a partire dalla coppia (σ, τ) si ottiene che, dato un automorfismo φ, gli elementi del tipo (id, τ) hanno tutti immagine (τ', id) se gli elementi del tipo (τ, id) hanno immagine (id, τ'), oppure tutti immagine (id, τ') se gli elementi del tipo (τ, id) hanno immagine (τ', id).

Posto $T_1 = \{(\tau, id) | \tau \in S_3,\ \tau \text{ 2-ciclo}\}$ e $T_2 = \{(id, \tau) | \tau \in S_3,\ \tau \text{ 2-ciclo}\}$ si ha che $T_1 \cup T_2$ è un insieme di generatori di $S_3 \times S_3$, quindi gli automorfismi cercati sono al più tanti quanti le possibili funzioni $\bar{\varphi} : T_1 \cup T_2 \to T_1 \cup T_2$ tali che $\bar{\varphi}(T_1) = (T_1)$ e $\bar{\varphi}(T_2) = (T_2)$ oppure $\bar{\varphi}(T_1) = (T_2)$ e $\bar{\varphi}(T_2) = (T_1)$. Poiché $|T_1| = |T_2| = 3$, gli automorfismi sono al piú $2 \cdot 3! \cdot 3! = 72$. Da questo segue che $HK = \mathrm{Aut}(S_3 \times S_3)$ e quindi $\mathrm{Aut}(S_3 \times S_3) \cong H \rtimes_\phi K$ dove $\phi : K \to \mathrm{Aut}(H)$ è definito da $\phi_\psi(\gamma) = \psi\gamma\psi^{-1}$.

Esercizio 2. Sia G il gruppo delle funzioni $f : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ definite da $f(x) = ax + b$ $\forall x \in \mathbb{Z}/7\mathbb{Z}$ con $a, b \in \mathbb{Z}/7\mathbb{Z}$ e $a \neq 0$ e consideriamo il suo sottogruppo $H := \{f \in G | f(x) = 2^t x + b \text{ con } t \in \mathbb{Z}\}$. Determinare le classi di coniugio in G e in H degli elementi $f(x) = x + 1$ e $g(x) = 2x + 1$ e le loro cardinalità.

Soluzione esercizio 2. Indichiamo con $f_{a,b}$ la funzione di G definita da $x \to ax+b$; si ha $f = f_{1,1}$ e $g = f_{2,1}$. Inoltre $Cl_G(f_{1,1}) = \{f_{a,b} \circ f_{1,1} \circ f_{a,b}^{-1} \mid f_{a,b} \in G\}$ e $Cl_H(f_{1,1}) = \{f_{a,b} \circ f_{1,1} \circ f_{a,b}^{-1} \mid f_{a,b} \in H\}$

e analogamente per $g = f_{2,1}$. Si calcola $f_{a,b} \circ f_{c,d}(x) = a(cx+d)+b = acx+ad+b = f_{ac,ad+b}$ e, poiché la funzione identità è $f_{1,0}$, ricaviamo che $f_{a,b}^{-1} = f_{c,d}$ con $c = a^{-1}$ e $d = -ba^{-1}$. Da questo si calcola

$$f_{a,b} \circ f_{1,1} \circ f_{a,b}^{-1}(x) = f_{a,b} \circ f_{1,1}(a^{-1}x - ba^{-1}) = f_{a,b}(a^{-1}x - ba^{-1} + 1) = x - b + a + b = x + a = f_{1,a}$$

e $Cl_G(f_{1,1}) = \{f_{1,a} \,|\, a \in \mathbb{Z}/7\mathbb{Z}^*\}$ ha quindi 6 elementi. La classe di coniugio in H si ottiene considerando i coniugati con $f_{a,b}$ e $a = 2^t$, da cui $Cl_H(f_{1,1}) = \{f_{1,2^t} \,|\, t \in \mathbb{Z}\}$ e, avendo 2 ordine 3 in $\mathbb{Z}/7\mathbb{Z}$, tale insieme ha 3 elementi.
Con un conto analogo ricaviamo che

$$f_{a,b} \circ f_{2,1} \circ f_{a,b}^{-1}(x) = f_{a,b} \circ f_{2,1}(a^{-1}x - ba^{-1}) = f_{a,b}(2a^{-1}x - 2ba^{-1} + 1) = 2x - 2b + a + b = 2x + a - b = f_{2,a-b},$$

da cui si ottiene $Cl_G(f_{2,1}) = \{f_{2,a-b} \,|\, a, b \in \mathbb{Z}/7\mathbb{Z},\ a \neq 0\} = \{f_{2,b} \,|\, b \in \mathbb{Z}/7\mathbb{Z}\}$ che contiene quindi 7 elementi. Infine $Cl_H(f_{2,1}) = \{f_{2,2^t-b} \,|\, b \in \mathbb{Z}/7\mathbb{Z},\ t \in \mathbb{Z}\}$ e anche questa classe ha 7 elementi perchè, fissato t al variare di b in $\mathbb{Z}/7\mathbb{Z}$ si ha che $2^t - b$ descrive tutti gli elementi di $\mathbb{Z}/7\mathbb{Z}$.

Esercizio 3. Sia A un anello commutativo con identità e sia x un'indeterminata. Dimostrare che $f(x) \in A[x]$ è nilpotente se e solo se tutti i suoi coefficienti sono nilpotenti.
Soluzione esercizio 3. Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$, vogliamo mostrare che $f(x)$ è nilpotente se e solo se $a_0, \ldots, a_n$ sono nilpotenti.
Ricordiamo che l'insieme degli elementi nilpotenti di un anello costituisce il nilradicale $\mathcal{N}$ che è un ideale, quindi se $a_0, \ldots, a_n$ sono nilpotenti, cioè appartengono al nilradicale, anche $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathcal{N}$ in quanto combinazione a coefficienti nell'anello $A[x]$ di elementi di $\mathcal{N}$ ed è quindi nilpotente.
Viceversa supponiamo che $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathcal{N}$, e mostriamo per indizione su $n = \deg f$ che i suoi coefficienti sono nilpotenti. Questo è ovvio per $n = 0$. Supponiamo vera la tesi per polinomi di grado $d < n$ e mostriamola per polinomi di grado n. Se il polinomio $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathcal{N}$, allora esiste $k > 0$ tale che $f(x)^k = 0$. Sviluppando il calcolo si ottiene che $f(x)^k = a_n^k x^{nk} +$ termini di grado più basso $= 0$; per il principio di identità dei polinomi si ha che $a_n^k = 0$, quindi che $a_n \in \mathcal{N}$. Ora, $f(x), a_n \in \mathcal{N}$, quindi anche il polinomio $g(x) = f(x) - a_n x^n = \sum_{i=0}^{n-1} a_i x^i \in \mathcal{N}$. Tale polinomio ha grado strettamente minore di n, quindi per ipotesi induttiva i suoi coefficienti $a_0, \ldots, a_{n-1}$ sono nilpotenti. Poiché avevamo già ottenuto che $a_n \in \mathcal{N}$ abbiamo la tesi.

Esercizio 4. Determinare, al variare del parametro intero a, il gruppo di Galois del campo di spezzamento del polinomio $(x^4 - 3)(x^2 - a)$ su $\mathbb{Q}$ e su $\mathbb{Q}(\sqrt{2})$.
Soluzione esercizio 4. Il polinomio $x^4 - 3$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein e le sue radici in $\mathbb{C}$ sono $\pm\sqrt[4]{3}$, $\pm i\sqrt[4]{3}$; il suo campo di spezzamento è quindi $K = \mathbb{Q}(\pm\sqrt[4]{3}, \pm i\sqrt[4]{3}) = \mathbb{Q}(\sqrt[4]{3}, i)$. Le radici di $x^2 - a$ sono $\pm\sqrt{a}$, quindi il campo di spezzamento cercato è $F = K(\sqrt{a}) = \mathbb{Q}(\sqrt[4]{3}, i, \sqrt{a})$. Consideriamo l'estensione $K/\mathbb{Q}$: $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{3})(i) : \mathbb{Q}(\sqrt[4]{3})][\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 2 \cdot 4 = 8$ in quanto $\sqrt[4]{3}$ ha grado 4 su $\mathbb{Q}$ perchè $x^4 - 3$ è il suo polinomio minimo, inoltre $i \notin \mathbb{Q}(\sqrt[4]{3})$ perchè questa è un'estensione reale e quindi $x^2 + 1$ è il suo polinomio minimo anche

su $\mathbb{Q}(\sqrt[4]{3})$. Essendo $K/\mathbb{Q}$ il campo di spezzamento di un polinomio di grado 4, il suo gruppo di Galois è un sottogruppo di S_4, e poichè ha ordine 8 è uno dei suoi 2-Sylow che sappiamo essere isomorfi a D_4. Quindi $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$.
Consideriamo ora l'estensione $F = K(\sqrt{a})/K$; il suo grado è 1 se $\sqrt{a} \in K$ e 2 se $\sqrt{a} \notin K$. Osserviamo che $\sqrt{a} \in K = \mathbb{Q}(\sqrt[4]{3}, i)$ se e solo se $\mathbb{Q}(\sqrt{a})$ è $\mathbb{Q}$ oppure una delle sottoestensioni quadratiche di K. Le sottoestensioni quadratiche di $K/\mathbb{Q}$ sono $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$, e $\mathbb{Q}(i\sqrt{3})$: infatti, è evidente che queste lo sono e non ce ne sono altre perché corrispondono ai sottogruppi di ordine 4 di D_4 che sono 3 ($\langle r\rangle, \langle r^2, s\rangle, \langle r^2, sr\rangle$). Abbiamo quindi che $F = K$ se e solo se $\mathbb{Q}(\sqrt{a})$ è $\mathbb{Q}$ oppure una tra $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$, o $\mathbb{Q}(i\sqrt{3})$ e quindi, per il criterio sull'uguaglianza di due estensioni quadratiche e ricordando che $a \in \mathbb{Z}$, se e solo se $a = \pm n^2$, $a = \pm 3n^2$ con $n \in \mathbb{Z}$. In questo caso $\mathrm{Gal}(F/\mathbb{Q}) = D_4$. Se a non è della forma $a = \pm n^2$, $a = \pm 3n^2$ con $n \in \mathbb{Z}$, allora $[F : \mathbb{Q}] = 16$ e poiché $\mathbb{Q}(\sqrt{a}) \cap K = \mathbb{Q}$ si ha che $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{a})/\mathbb{Q}) = D_4 \times \mathbb{Z}/2\mathbb{Z}$.
Calcoliamo ora il gruppo di Galois su $\mathbb{Q}(\sqrt{2})$. Il campo di spezzamento del polinomio su $\mathbb{Q}(\sqrt{2})$ è $F(\sqrt{2}) = \mathbb{Q}(\sqrt{2})(\sqrt[4]{3}, i, \sqrt{a})$. Osseviamo $\sqrt{2} \notin K$ (abbiamo calcolato esplicitamente le sottoestensioni di K di grado 2 su $\mathbb{Q}$). Se $\sqrt{2} \in F$ si ha $F(\sqrt{2}) = F$ e poiché $K \cap \mathbb{Q}(\sqrt{2}) = \mathbb{Q}$ si ha $F = K(\sqrt{2})$ e $\mathrm{Gal}(F(\sqrt{2})/\mathbb{Q}(\sqrt{2})) \cong \mathrm{Gal}(K/Q) \cong D_4$. Se $\sqrt{2} \notin F$ allora $\mathrm{Gal}(F(\sqrt{2}) : \mathbb{Q}(\sqrt{2})) \cong \mathrm{Gal}(F/Q)$ e questo è D_4 o $D_4 \times \mathbb{Z}/2\mathbb{Z}$ secondo quanto visto nella prima parte. Rimangono da caratterizzare gli interi a tali che $\sqrt{2} \in F = \mathbb{Q}(\sqrt[4]{3}, i, \sqrt{a})$, cioè gli a tali che $\mathbb{Q}(\sqrt{2})$ è una sottoestensione di grado 2 di $F/\mathbb{Q}$. Questo succede se e solo se $a = \pm 2n^2, \pm 6n^2$ con $n \in \mathbb{Z}$, infatti per tali valori di a chiaramente $\sqrt{2} \in F$, d'altra parte non ci sono altri valori di a per cui questo succede perché le sottoestensioni di grado 2 sono abeliane e quindi sono contenute nel sottocapo fissato dai commutatori e tale campo è $\mathbb{Q}(i, \sqrt{3}, \sqrt{a})$.