COMPITO DI ALGEBRA 1

15 gennaio 2021

Esercizio 1.
Sia $G = \frac{\mathbb{Z}}{9\mathbb{Z}} \times \frac{\mathbb{Z}}{27\mathbb{Z}}$, sia A il gruppo degli automorfismi di G, e sia B il sottogruppo di A dato da $B = \{\psi \in A : \psi(x) = x \text{ per ogni } x \in G \text{ tale che } 3x = 0\}$.

1. Sia $\psi \in B$. Dimostrare che $\psi^3((1,0)) = (1,0)$.
2. Dimostrare che $\#B$ è una potenza di 3.
3. Determinare l'insieme dei numeri primi che dividono $\#A$.

SOLUZIONE. Sia $G[3] := \{g \in G : 3g = 0\}$. Si tratta di un sottogruppo (è il nucleo dell'omomorfismo $G \to G$ dato dalla moltiplicazione per 3), ed è caratteristico, perché per ogni $\varphi \in A$ e $x \in G[3]$ si ha $0 = 3x \Rightarrow 0 = \varphi(3x) = 3\varphi(x)$, ovvero $\varphi(x) \in G[3]$.

1. Sia $\psi \in B$. Per ipotesi si ha $\psi((3,0)) = (3,0)$, ovvero $3\psi((1,0)) = 3(1,0)$, o ancora $3(\psi((1,0)) - (1,0)) = 0$. Otteniamo quindi che $x := \psi((1,0)) - (1,0) \in G[3]$, e per ipotesi $\psi(x) = x$. Ne segue che $\psi^2((1,0)) = \psi((1,0)+x) = \psi((1,0)) + \psi(x) = (1,0) + x + x$, e infine

   $$\psi^3((1,0)) = \psi(\psi^2((1,0))) = \psi((1,0)+2x) = \psi((1,0))+2\psi(x) = (1,0)+3x = (1,0),$$

   dove si è usato il fatto che $x \in G[3]$ per dedurre $3x = 0$.

2. Dimostreremo che per ogni $\psi \in B$ si ha $\psi^9 = \mathrm{id}$. Questo implica la tesi. In effetti, sia q un primo che divide $\#B$: allora per il teorema di Cauchy esiste $\psi \in B$ di ordine q. D'altro canto $\psi^9 = \mathrm{id}$, quindi l'ordine di ψ divide 9, e quindi $q = 3$. Questo dimostra che l'unico primo nella fattorizzazione di $\#B$ è 3.

   Come sopra osserviamo che $\psi((0,9)) = (0,9)$, da cui $y := \psi((0,3)) - (0,3)$ appartiene a $G[3]$. Con calcoli del tutto analoghi ai precedenti si vede che $\psi^3((0,3)) = (0,3)$. Sia allora $z = \psi^3((0,1)) - (0,1)$: ancora una volta si ha $3z = \psi^3((0,3)) - (0,3) = 0$, ovvero $z \in G[3]$, e quindi in particolare $\psi^3(z) = z$. Procedendo ancora come nel punto 1 otteniamo

   $$\psi^6((0,1)) = \psi^3\psi^3((0,1)) = \psi^3((0,1)+z) = (0,1)+2z$$

   ed infine $\psi^9((0,1)) = \psi^3((0,1)+2z) = (0,1)+3z = (0,1)$. Ne segue che ψ^9 fissa entrambi i generatori $(1,0)$ e $(0,1)$ e quindi è l'identità di G.

3. Siccome $G[3]$ è un sottogruppo caratteristico di G, possiamo considerare l'omomorfismo
$$\begin{array}{rccc} \Phi: & A & \to & \mathrm{Aut}(G[3]) \\ & \psi & \mapsto & \psi|_{G[3]}. \end{array}$$
Per definizione, il nucleo di Φ è esattamente B. D'altro canto, il gruppo $G[3] = \frac{3\mathbb{Z}}{9\mathbb{Z}} \times \frac{9\mathbb{Z}}{27\mathbb{Z}}$ è isomorfo a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, quindi $\mathrm{Aut}(G[3]) \cong \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{F}_3)$ ha ordine $(3^2-1)(3^2-3) = 48$. Segue dal primo teorema di isomorfismo che A/B è isomorfo ad un sottogruppo di un gruppo di ordine 48. Per quanto già visto sappiamo che $\#B = 3^k$ per un certo $k \geq 0$, e quindi $\#A \mid 48 \cdot 3^k$, da cui i divisori primi di $\#A$ sono da ricercarsi nell'insieme $\{2, 3\}$. Infine, A contiene un sottogruppo isomorfo a $\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/27\mathbb{Z}) \cong (\mathbb{Z}/9\mathbb{Z})^\times \times (\mathbb{Z}/27\mathbb{Z})^\times$, che ha ordine $6 \cdot 18$, e quindi in effetti $\#A$ è divisibile sia per 2 che per 3.

Esercizio 2. Per ogni intero positivo n, sia A_n il gruppo alterno su n elementi.

1. Dimostrare che per ogni intero positivo n il gruppo S_n si immerge in A_{n+2}.
2. Determinare la classe di isomorfismo dei 2-sottogruppi di Sylow di A_6 e il loro numero.

Soluzione.

1. Per ogni permutazione σ di S_n indichiamo con $\tilde{\sigma}$ la permutazione di S_{n+2} definita da $\tilde{\sigma}(i) = \sigma(i)$ per $i = 1, \ldots, n$ e $\tilde{\sigma}(n+j) = n+j$ per $j = 1, 2$.

   Sia τ la trasposizione $(n+1, n+2)$, e sia $\phi\colon S_n \to A_{n+2}$ la mappa definita da $\phi(\sigma) = \tilde{\sigma}\tau^{\epsilon_\sigma}$, dove $\epsilon_\sigma = 0$ se σ è una permutazione pari e $\epsilon_\sigma = 1$ se σ è dispari. Chiaramente la mappa ϕ è ben definita perché $\phi(\sigma) \in A_{n+2}$ per ogni $\sigma \in S_n$. Mostriamo che ϕ è un omomorfismo iniettivo. Date $\sigma, \rho \in S_n$ osserviamo che banalmente vale $\widetilde{\sigma\rho} = \tilde{\sigma}\tilde{\rho}$, inoltre $\tau^{\epsilon_{\sigma\rho}} = \tau^{\epsilon_\sigma}\tau^{\epsilon_\rho}$ in quanto, se le permutazioni σ e ρ hanno la stessa segnatura, $\sigma\rho$ è pari ed entrambi i membri sono l'identità, se invece σ e ρ hanno segnatura diversa, $\sigma\rho$ è dispari ed entrambi i membri sono uguali a τ. Ne segue che:
   $$\phi(\sigma\rho) = \widetilde{\sigma\rho}\tau^{\epsilon_{\sigma\rho}} = \tilde{\sigma}\tilde{\rho}\tau^{\epsilon_\sigma}\tau^{\epsilon_\rho} = \tilde{\sigma}\tau^{\epsilon_\sigma}\tilde{\rho}\tau^{\epsilon_\rho} = \phi(\sigma)\phi(\rho),$$
   dove abbiamo usato che τ commuta con $\tilde{\rho}$ essendo le due permutazioni disgiunte. In nucleo di ϕ è banale perché $\phi(\sigma) = id$ se e solo se σ è pari e $\tilde{\sigma} = id$, quindi se e solo se $\sigma = id$.

2. <u>Prima dimostrazione.</u> $|A_6| = \frac{6!}{2} = 2^3 3^2 5$, quindi i 2-Sylow di A_6 hanno cardinalità 8. Dal punto (1) sappiamo che S_4, i cui 2-Sylow sono isomorfi a D_4, si immerge in

A_6. Ne segue che i 2-Sylow di A_6 sono isomorfi a D_4. Quanto al loro numero n_2, il Teorema di Sylow dice che $n_2|45$. Ricordiamo anche che i p-Sylow di un gruppo G sono sempre tutti coniugati ad un qualsiasi p-Sylow P, quindi il loro numero è uguale all'indice $[G : N_G(P)]$.

Osserviamo che in S_4 ci sono esattamente tre 2-Sylow, in quanto un 2-Sylow H ha indice $3 = \frac{24}{8}$, quindi il suo normalizzatore in S_4 coincide con H o è tutto S_4. Si esclude che il normalizzatore di H sia S_4 osservando che H non è normale (ad esempio perché contiene un 4-ciclo ma non tutti i 4 cicli). Ne segue che anche il sottogruppo $\phi(S_4)$ ottenuto nel punto (1) contiene esattamente 3 2-Sylow di A_6. D'altra parte, per ogni scelta di 4 elementi $\{x_1, x_2, x_3, x_4\}$ in $\{1, 2, \ldots, 6\}$ possiamo immergere il gruppo $S(\{x_1, x_2, x_3, x_4\})$, che è isomorfo ad S_4, in A_6 in modo analogo a quanto fatto nel punto (1). Le scelte dei 4 elementi sono $\binom{6}{4} = 15$, quindi in A_6 abbiamo 15 copie di S_4, ognuna delle quali contiene 3 2-Sylow. I 45 2-Sylow che si ottengono sono tutti distinti perchè differiscono per gli elementi di ordine 4, che in un 2-Sylow di $\phi(S(\{x_1, x_2, x_3, x_4\})$ sono del tipo $\sigma\tau$ con σ 4-ciclo sugli elementi x_1, x_2, x_3, x_4 e τ trasposizione sui rimanenti due elementi. I 2-Sylow sono quindi 45 perché $n_2|45$.

Seconda dimostrazione. Costruiamo un 2-Sylow P di A_6 che contiene la permutazione $\sigma = (1, 2, 3, 4)(5, 6)$. Dato che $P \cong D_4$ il sottogruppo $\langle\sigma\rangle$ è normale in P, quindi $P \leq N_{A_6}(\langle\sigma\rangle)$. Si verifica che σ e σ^{-1} sono coniugati in A_6, quindi $|N_{A_6}(\langle\sigma\rangle)| = \varphi(4)|Z_{A_6}(\sigma)|$. Ora $Z_{A_6}(\sigma) = Z_{S_6}(\sigma) \cap A_6$ e $Z_{S_6}(\sigma) = \langle(1, 2, 3, 4),\ (5, 6)\rangle$ (chiaramente $(1, 2, 3, 4)$ e $(5, 6)$ appartengono a $Z_{S_6}(\sigma)$ e si ha l'uguaglianza osservando che entrambi i gruppi hanno ordine 8). Da questo otteniamo che $Z_{A_6}(\sigma) = \langle\sigma\rangle$ e che $P = N_{A_6}(\langle\sigma\rangle)$ dato che hanno entrambi ordine 8.

In A_6 le permutazioni di ordine 4 sono tutte del tipo 4+2, e ce ne sono $\binom{6}{4}3!\binom{2}{2} = 90$. Ogni 2-Sylow, essendo isomorfo a D_4, ne contiene esattamente 2. Inoltre due 2-Sylow distinti non possono contenere uno stesso elemento ρ di ordine 4, in quanto altrimenti sarebbero entrambi contenuti nel normalizzatore del sottogruppo $\langle\rho\rangle$, mentre abbiamo visto che il normalizzatore di un elemento di ordine 4 ha ordine 8. Questo dimostra che in A_6 ci sono 45 2-Sylow.

Esercizio 3.
Sia K un campo e sia A il sottoanello di $K(x)$ definito da

$$A = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \mathrm{mcd}(g(x), (x^2 - 2)(x^3 - 7)) = 1 \right\}.$$

1. Dimostrare che ogni ideale di A è principale e generato da un polinomio di $K[x]$.

2. Determinare gli ideali primi di A per $K = \mathbb{F}_{13}$ e per $K = \mathbb{F}_{13^2}$.

SOLUZIONE. Scriviamo per semplicità $p(x) = (x^2 - 2)(x^3 - 7)$.

1. Sia $S = \{g(x) \in K[x] : (g(x), p(x)) = 1\}$. Si noti che S è una parte moltiplicativa: se $g_1(x), g_2(x) \in K[x]$ sono entrambi coprimi con $p(x)$, anche il loro prodotto lo è. La definizione di A mostra che A è la localizzazione $S^{-1}K[x]$, e dalla teoria sappiamo che ogni ideale J di $S^{-1}K[x]$ è della forma $S^{-1}I$ con I ideale di $K[x]$. È poi ben noto che $K[x]$ è un dominio ad ideali principali, per cui si ha $I = (h(x))$ per un opportuno $h(x) \in K[x]$. Infine, l'ideale $S^{-1}I = S^{-1}(h(x))$ è per definizione l'insieme degli elementi della forma $\frac{h(x)m(x)}{s(x)}$ con $m(x) \in K[x]$ e $s(x) \in S$, e quindi coincide con l'ideale generato da $h(x)$ in A. Ne segue che $J = (h(x))$ è principale e generato da un polinomio di $K[x]$.

2. Dalla teoria sappiamo che i primi di $S^{-1}K[x]$ sono in bigezione con i primi di $K[x]$ che non intersecano S. Gli ideali primi di $K[x]$ sono (0) e quelli della forma $(q(x))$ con $q(x)$ polinomio irriducibile in $K[x]$. Chiaramente $(0) \cap S = \emptyset$, quindi (0) è un ideale primo di A. Dato invece un polinomio $q(x) \in K[x]$ irriducibile e detto $P = (q(x))$ il corrispondente ideale primo, affermiamo che $P \cap S = \emptyset$ se e solo se $q(x) \mid p(x)$ in $K[x]$. In effetti, se $q(x) \mid p(x)$, allora ogni elemento di P (essendo multiplo di $q(x)$) ha un fattore in comune con $p(x)$, e quindi non sta in S. Viceversa, se $P \cap S = \emptyset$, allora in particolare $q(x) \notin S$, e quindi $(q(x), p(x)) \neq (1)$. Siccome $q(x)$ è irriducibile, questo implica $q(x) \mid p(x)$ come voluto. Si tratta quindi di fattorizzare $p(x)$ in $\mathbb{F}_{13}[x]$ e in $\mathbb{F}_{13^2}[x]$. Si verifica immediatamente che né $x^2 - 2$ né $x^3 - 7$ hanno radici in $\mathbb{F}_{13}$, e quindi sono irriducibili (essendo di grado ≤ 3). Nel caso $K = \mathbb{F}_{13}$ l'anello A ha quindi tre ideali primi: l'ideale (0) e gli ideali generati da $x^2 - 2$ e da $x^3 - 7$. Infine, $K = \mathbb{F}_{13^2}$ contiene le radici di ogni polinomio irriducibile di secondo grado in $\mathbb{F}_{13}[x]$, quindi esiste $\alpha \in \mathbb{F}_{13^2}$ tale che $x^2 - 2 = (x - \alpha)(x + \alpha)$. D'altro canto, il polinomio $x^3 - 7$ resta irriducibile in $\mathbb{F}_{13^2}$: se così non fosse avrebbe una radice β in $\mathbb{F}_{13^2}$, ma $[\mathbb{F}_{13}(\beta) : \mathbb{F}_{13}]$ è uguale al grado del polinomio minimo di β, che è $x^3 - 7$ (è monico, irriducibile e ha β come radice). Si ha perciò $[\mathbb{F}_{13}(\beta) : \mathbb{F}_{13}] = 3$, e quindi $\beta \notin \mathbb{F}_{13^2}$. Per $K = \mathbb{F}_{13^2}$ l'anello A ha perciò quattro ideali primi: (0), $(x - \alpha)$, $(x + \alpha)$ e $(x^3 - 7)$.

Esercizio 4.
Sia $K = \mathbb{Q}(\zeta_{24})$ e sia $a \in \mathbb{Z}$. Denotiamo con M il campo di spezzamento del polinomio $x^3 - a$ su K. Determinare, in funzione di a, il grado dell'estensione $M/\mathbb{Q}$ e il suo gruppo di Galois.

SOLUZIONE. Per $a = 0$ si ha e $M = K$, da cui $[M : \mathbb{Q}] = [K : \mathbb{Q}] = \varphi(24) = 8$ e $\mathrm{Gal}(M/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/24\,\mathbb{Z})^*$. Nel resto della soluzione supporremo quindi $a \neq 0$.
Indichiamo con F il campo di spezzamento di $f(x) = x^3 - a$ su $\mathbb{Q}$: le radici di $f(x)$ in $\mathbb{C}$ sono $\sqrt[3]{a}$, $\sqrt[3]{a}\zeta_3$ e $\sqrt[3]{a}\zeta_3^3$, quindi $F = \mathbb{Q}(\sqrt[3]{a}, \sqrt[3]{a}\zeta_3, \sqrt[3]{a}\zeta_3^3) = \mathbb{Q}(\sqrt[3]{a}, \zeta_3)$. Inoltre $f(x)$, che è un polinomio di grado 3, è riducibile su $\mathbb{Q}$ se e solo se una delle sue radici appartiene a $\mathbb{Q}$, quindi:
- se a non è un cubo in $\mathbb{Z}$ il polinomio $f(x)$ è irriducibile, $[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{a}, \zeta_3) : \mathbb{Q}(\sqrt[3]{a})][\mathbb{Q}(\sqrt[3]{a}) : \mathbb{Q}] = 2 \cdot 3 = 6$ e $\mathrm{Gal}(F/\mathbb{Q}) \cong S_3$.
- se $a = b^3$, con $b \in \mathbb{Z} \setminus \{0\}$, in $\mathbb{Q}[x]$ si ha $f(x) = (x - b)(x^2 + bx + b^2)$ e i due fattori sono irriducibili in quanto le radici di $x^2 + bx + b^2$ sono $b\zeta_3$ e $b\zeta_3^2$ che non sono reali. In questo caso $F = \mathbb{Q}(\zeta_3)$, $[F : \mathbb{Q}] = 2$ e $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/2\,\mathbb{Z}$.

D'altra parte, le uguaglianze $\zeta_{24}^3 = \zeta_8$, $\zeta_{24}^8 = \zeta_3$ e $\zeta_8^3\zeta_3^{-1} = \zeta_{24}$ dimostrano che $K = \mathbb{Q}(\zeta_8, \zeta_3)$. Ne segue che

$$M = KF = \mathbb{Q}(\zeta_8, \zeta_3, \sqrt[3]{a}) = F\,\mathbb{Q}(\zeta_8).$$

Osserviamo che $F \cap \mathbb{Q}(\zeta_8) = \mathbb{Q}$. Infatti si ha $[F \cap \mathbb{Q}(\zeta_8) : \mathbb{Q}] \mid ([F : \mathbb{Q}], [\mathbb{Q}(\zeta_8) : \mathbb{Q}]) = 2$; d'altra parte l'unica sottoestensione di grado 2 di F è $\mathbb{Q}(\zeta_3)$ (è ovvio che $\mathbb{Q}(\zeta_3) \subseteq F$, e non può esserci un'altra sottoestensione L di grado 2 su $\mathbb{Q}$ perché altrimenti $L\,\mathbb{Q}(\zeta_3)$ sarebbe una sottostensione di F di grado 4 su $\mathbb{Q}$, ma $4 \nmid [F : \mathbb{Q}]$), ma $\zeta_3 \notin \mathbb{Q}(\zeta_8)$ perché, come detto sopra, $K = \mathbb{Q}(\zeta_8, \zeta_3)$ ha grado $\varphi(24) = 8$ su $\mathbb{Q}$ mentre $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \varphi(8) = 4$.
Abbiamo quindi che $F/\mathbb{Q}$ e $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ sono due estensioni di Galois con intersezione $\mathbb{Q}$, quindi il loro composto M è un'estensione di Galois e $\mathrm{Gal}(M/\mathbb{Q})$ è isomorfo al prodotto diretto dei gruppi di Galois dei due fattori

$$\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{Gal}(F/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong \mathrm{Gal}(F/\mathbb{Q}) \times (\mathbb{Z}/8\,\mathbb{Z})^*,$$

dove, come abbiamo detto sopra, $\mathrm{Gal}(F/\mathbb{Q})$ è isomorfo a $\mathbb{Z}/2\,\mathbb{Z}$ o a S_3 rispettivamente se $a \neq 0$ è o non è un cubo in $\mathbb{Z}$. Tenendo conto anche del caso $a = 0$, questo dimostra anche che

$$[M : \mathbb{Q}] = [F : \mathbb{Q}][\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \begin{cases} 8 \text{ se } a \text{ è un cubo in } \mathbb{Z}; \\ 24 \text{ se } a \text{ non è un cubo in } \mathbb{Z}. \end{cases}$$