COMPITO DI ALGEBRA 1

19 febbraio 2019

Soluzioni

1. Consideriamo un 3-sottogruppo di Sylow P del gruppo simmetrico S_9.

(a) Dimostrare che P è isomorfo al prodotto semidiretto $(\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$. Si descriva in particolare l'omomorfismo $\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/3\mathbb{Z})^3)$.

(b) Per ogni divisore d di $|P|$, determinare quanti siano gli elementi di ordine d in P.

SOLUZIONE:

(a) Dal momento che tutti i 3-Sylow in un dato gruppo sono coniugati, e in particolare fra loro isomorfi, è sufficiente studiare un fissato 3-Sylow. Si osservi che ogni 3-Sylow di S_9 ha ordine 3^4, perché questa è la massima potenza di 3 che divide 9!

Consideriamo i tre 3-cicli $\alpha = (1,2,3)$, $\beta = (4,5,6)$ e $\gamma = (7,8,9)$ e il sottogruppo H da essi generato. Visto che α, β, γ sono di ordine 3 e commutano fra loro, è chiaro che $H \cong (\mathbb{Z}/3\mathbb{Z})^3$; inoltre, l'elemento $\delta = (174)(285)(396)$ normalizza H (perché $\delta\alpha\delta^{-1} = \beta$, $\delta\beta\delta^{-1} = \gamma$ e $\delta\gamma\delta^{-1} = \alpha$) ma non è in H, perché non commuta con α. Ne segue che $P := H\langle\delta\rangle$ è un sottogruppo di S_9 con $|H| \cdot |\langle\delta\rangle| = 3^4$ elementi, e dunque è un 3-Sylow. Quanto visto dimostra anche che $P \cong (\mathbb{Z}/3\mathbb{Z})^3 \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$, dove come sottogruppo normale isomorfo a $(\mathbb{Z}/3\mathbb{Z})^3$ possiamo prendere H e come ulteriore sottogruppo isomorfo a $\mathbb{Z}/3\mathbb{Z}$ possiamo prendere $\langle\delta\rangle$. Più precisamente, $H = \{\alpha^m\beta^n\gamma^p\}$ è identificato a $(\mathbb{Z}/3\mathbb{Z})^3$ tramite l'isomorfismo che porta $\alpha^m\beta^n\gamma^p$ nella terna (m,n,p), e $\langle\delta\rangle$ è identificato a $\mathbb{Z}/3\mathbb{Z}$ tramite l'isomorfismo che porta δ in $1 \in \mathbb{Z}/3\mathbb{Z}$. Infine, visto che il coniugio per δ permuta ciclicamente α, β, γ (e quindi gli esponenti (m,n,p)) si ha che $\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}((\mathbb{Z}/3\mathbb{Z})^3)$ è dato da $1 \mapsto \psi$, dove

$$\begin{array}{rccc} \psi: & (\mathbb{Z}/3\mathbb{Z})^3 & \to & (\mathbb{Z}/3\mathbb{Z})^3 \\ & (m,n,p) & \mapsto & (p,m,n). \end{array}$$

Verifichiamo che questo è in effetti l'ordine corretto degli esponenti: moltiplicando $\alpha^{m'}\beta^{n'}\gamma^{p'}\delta$ per $\alpha^m\beta^n\gamma^p\delta^i$ si trova

$$\alpha^{m'}\beta^{n'}\gamma^{p'}\delta\,(\alpha^m\beta^n\gamma^p)\,\delta^{-1}\delta\delta^i = \alpha^{m'}\beta^{n'}\gamma^{p'}\,(\beta^m\gamma^n\alpha^p)\,\delta^{i+1} = \alpha^{m'+p}\beta^{n'+m}\gamma^{p'+n}\delta^{i+1},$$

che in termini del prodotto semidiretto si traduce in

$$\begin{aligned}((m',n',p'),1)\cdot((m,n,p),i) &= ((m',n',p') + (p,m,n), i+1) \\ &= ((m',n',p') + \psi((m,n,p)), i+1)\end{aligned}$$

da cui appunto $\psi((m,n,p)) = (p,m,n)$.

(b) Come in ogni gruppo, in P c'è un unico elemento di ordine 1. Lavoriamo con elementi di P nella sua rappresentazione come prodotto semidiretto: sia $g = ((m,n,p),i)$. Allora se $i = 0$ l'elemento g sta nel sottogruppo $(\mathbb{Z}/3\mathbb{Z})^3$, e quindi ha ordine 3 a meno che non si tratti dell'identità. Se $i = 1$ si ha invece

$$\begin{aligned} g \cdot g \cdot g &= ((m,n,p),1) \cdot ((m,n,p),1) \cdot ((m,n,p),1) \\ &= ((m,n,p),1) \cdot (\psi((m,n,p)) + (m,n,p),2) \\ &= ((m,n,p),1) \cdot ((p,m,n) + (m,n,p),2) \\ &= ((m,n,p) + \psi((p,m,n) + (m,n,p)),0) \\ &= ((m,n,p) + (n,p,m) + (p,m,n),0) \\ &= ((m+n+p, m+n+p, m+n+p),0), \end{aligned}$$

per cui l'ordine di g è 3 se $m+n+p = 0$ ed è 9 altrimenti (infatti è chiaro che, detto $h = ((m+n+p, m+n+p, m+n+p),0)$, $h \cdot h \cdot h$ è l'identità). Un calcolo del tutto analogo mostra che la medesima conclusione vale per gli elementi del tipo $((m,n,p),2)$: essi sono di ordine 3 o 9 a seconda che $m+n+p = 0$ o meno. Ci resta solo da contare quante terne $(m,n,p) \in (\mathbb{Z}/3\mathbb{Z})^3$ soddisfino $m+n+p = 0$, ma questo è chiaro: fissati m ed n, esiste un unico p che renda vera l'uguaglianza, quindi ci sono 9 tali terne. Gli elementi di ordine 3 in P sono quindi quelli in $(\mathbb{Z}/3\mathbb{Z})^3$ (tranne l'identità) e altri 18, ovvero quelli della forma $((m,n,p),i)$ con $i = 1,2$ e $m+n+p = 0$; essi sono quindi $(27-1)+18 = 44$. Siccome abbiamo visto che ogni elemento ha ordine al massimo 9 (cosa peraltro chiara, visto che $P < S_9$), non ci sono elementi di ordine 27 o 81, e per differenza gli elementi di ordine 9 sono $3^4 - 1 - 44 = 36$.

2. Sia p un numero primo, sia G un p-gruppo finito non ciclico.

(a) Dimostrare che G possiede almeno due sottogruppi distinti di indice p.

(b) Sia H un sottogruppo di G non ciclico e non normale. Dimostrare che H contiene un sottogruppo K con $[H:K] = p$ che non è un sottogruppo normale di G.

SOLUZIONE: (a) Dimostriamo la tesi per induzione sull'ordine di G. La tesi è ovvia se G è abeliano, usando la decomposizione di G come prodotto di almeno due fattori ciclici. Se G non è abeliano, sia Z il suo centro. Allora G/Z ha ordine minore dell'ordine di G, non è ciclico, e quindi per ipotesi induttiva possiede due sottogruppi distinti di indice p. Per la corrispondenza biunivoca fra i sottogruppi tramite la proiezione $\pi\colon G \to G/Z$, essi corrispondono a due sottogruppi distinti di G di indice p.

(b) Per il punto (a) possiamo supporre che K_1 e K_2 siano due sottogruppi distinti di H di indice p. Se entrambi fossero normali in G, allora lo sarebbe anche il loro prodotto K_1K_2, che è uguale ad H in quanto contiene sia K_1 che K_2, assurdo.

3. (a) Sia A un dominio a fattorizzazione unica e sia K il suo campo delle frazioni. Sia $u \in K$ un elemento con la seguente proprietà: esiste un polinomio **monico** $p(x) \in A[x]$ tale che $p(u) = 0$. Dimostrare che $u \in A$.

(b) Per ogni intero positivo n sia $A_n = \{a + bni \mid a, b \in \mathbb{Z}\}$ il sottoanello di $\mathbb{Z}[i]$ generato da ni. Determinare per quali n l'anello A_n è a fattorizzazione unica.

Soluzione

(a) Per ipotesi il polinomio $p(x)$, considerato come polinomio a coefficienti in $K[x]$, ammette la radice u, per cui abbiamo una fattorizzazione $p(x) = (x-u)q(x)$ in $K[x]$. Dal momento che A è un UFD possiamo applicare il lemma di Gauss per dedurre che $p(x)$ si fattorizza come $p_1(x)p_2(x)$, dove $p_1(x), p_2(x) \in A[x]$ sono della forma $p_1(x) = \lambda_1(x-u), p_2(x) = \lambda_2 q(x)$ per certi $\lambda_1, \lambda_2 \in K^\times$. Abbiamo quindi ottenuto $p(x) = p_1(x)p_2(x)$, dove $p_1(x) \in A[x]$ è un polinomio di primo grado avente u come radice. Siccome il coefficiente dominante di $p_1(x)$ divide il coefficiente dominante di $p(x)$, che è 1 per ipotesi, ricaviamo che il coefficiente dominante di $p_1(x)$ è un'unità in A. Possiamo allora scrivere $p_1(x) = cx + d$ con $c \in A^\times$, e siccome $p_1(u) = 0$ otteniamo $cu + d = 0 \Rightarrow u = -c^{-1}d \in A$ dal momento che $c \in A^\times$.

(b) Per $n = 1$ abbiamo $A_1 = \mathbb{Z}[i]$, che come noto è a fattorizzazione unica. Mostriamo ora che per $n > 1$ nessun anello A_n è un UFD. Notiamo innanzitutto che il campo delle frazioni F_n di A_n è uguale $\mathbb{Q}(i)$ per ogni n: in effetti da un lato A_n è contenuto in $A_1 = \mathbb{Z}[i]$, per cui si ha che $F_n \subseteq F_1 = \mathbb{Q}(i)$; dall'altro, $i = \frac{ni}{n}$ appartiene al campo delle frazioni di F_n, e quindi (siccome chiaramente $\mathbb{Q} \subseteq F_n$) si ha $\mathbb{Q}(i) \subseteq F_n$. D'altro canto, l'elemento $i \in F_n$ è radice del polinomio monico $x^2 + 1 \in \mathbb{Z}[x] \subset A_n[x]$, per cui la parte (a) implica che – se A_n fosse a fattorizzazione unica – si dovrebbe avere $i \in A_n$. Ma questo è chiaramente assurdo: $\{a + bni \mid a, b \in \mathbb{Z}\}$ non contiene i a meno che $n = 1$.

4. Sia $p(x) = x^{12} + 2^2 3^6$ e sia K il suo campo di spezzamento su $\mathbb{Q}$.

(a) Dimostrare che esiste $\lambda \in \mathbb{Z}[i]$ tale che $\lambda^4 = -4$.

(b) Dimostrare che K coincide con $L = \mathbb{Q}(\zeta_3, i, \sqrt[3]{2})$.

(c) Determinare il gruppo di Galois di K su $\mathbb{Q}$.

Soluzione:

(a) Siccome $2 = -i(1+i)^2$ in $\mathbb{Z}[i]$ si ha $-4 = (1+i)^4$.

(b) Osserviamo innanzitutto che le radici di $p(x)$ sono $\zeta_{12}^j \sqrt[12]{-4} \cdot \sqrt[12]{3^6}$ per $j = 0, \ldots, 11$ (dove $\zeta_{12} = \exp(2\pi i/12)$). Possiamo riscrivere $\sqrt[12]{3^6}$ come $\sqrt{3}$ e $\sqrt[12]{-4} =$

$(1+i)^{4/12} = \sqrt[3]{1+i}$ (queste uguaglianze sono valide a meno di radici 12-esime dell'unità, che sono in K).

Ne segue in particolare, per un argomento standard, che $K = \mathbb{Q}(\sqrt[3]{1+i} \cdot \sqrt{3}, \zeta_{12})$, e quindi K contiene $\zeta_{12}^3 = \zeta_4 = i$ e $\zeta_{12}^4 = \zeta_3$. Siccome d'altro canto $\zeta_3 \cdot \zeta_4^{-1} = \zeta_{12}$ abbiamo l'uguaglianza $K = \mathbb{Q}(\zeta_3, i, \sqrt[3]{1+i} \cdot \sqrt{3})$, e un campo che contiene $i = \sqrt{-1}$ e $\zeta_3 = \frac{1+\sqrt{-3}}{2}$ contiene anche $\sqrt{3}$, per cui otteniamo $K = \mathbb{Q}(\zeta_3, i, \sqrt[3]{1+i})$. Ora K contiene $(1+i)\sqrt[3]{1+i} = \sqrt[3]{1+i}^4 = \sqrt[3]{-4} = -\sqrt[3]{2^2}$, e quindi contiene anche $\sqrt[3]{2} = 2/\sqrt[3]{4}$, il che prova $L \subseteq K$. Viceversa, L contiene $-\frac{\sqrt[3]{2}^2}{1+i} = \sqrt[3]{1+i}$, e quindi $L \supseteq K$, il che prova l'uguaglianza.

(c) Visto il punto precedente, $K = L$ è chiaramente il composto di K_1, il campo di spezzamento (su $\mathbb{Q}$) del polinomio $q(x) = x^3 - 2$, e di $K_2 = \mathbb{Q}(i)$. Siccome $[K_1 : \mathbb{Q}] = 6$ e $[K_2 : \mathbb{Q}] = 2$ si ha $[K : \mathbb{Q}] \leq [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}] = 12$, ed inoltre il gruppo di Galois di K su $\mathbb{Q}$ si immerge in $\mathrm{Gal}(K_1/\mathbb{Q}) \times \mathrm{Gal}(K_2/\mathbb{Q}) \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$.

D'altro canto, K contiene $\mathbb{Q}(\zeta_3, i) = \mathbb{Q}(\sqrt{-3}, \sqrt{-1})$ che – come noto – ha grado 4 su $\mathbb{Q}$ (dal momento che $(-3)/(-1) = 3$ non è un quadrato in $\mathbb{Q}$) e quindi $4 \mid [K : \mathbb{Q}]$; similmente, K contiene $\mathbb{Q}(\sqrt[3]{2})$, e quindi il suo grado è multiplo di 3. Ne segue che $12 \mid [K : \mathbb{Q}]$ e quindi $[K : \mathbb{Q}] = 12$. Otteniamo allora che G è isomorfo ad un sottogruppo di $S_3 \times \mathbb{Z}/2\mathbb{Z}$ di ordine 12: siccome $\#(S_3 \times \mathbb{Z}/2\mathbb{Z}) = 12$ si deve avere $G \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$ (che è anche isomorfo a D_6).