1° COMPITINO DI ALGEBRA 1

7 novembre 2018

Soluzioni

1. Sia G il sottogruppo di S_6 generato dalle permutazioni $(1,2,3)$ e $(1,4)(2,5)(3,6)$.

(a) Descrivere G come prodotto semidiretto di gruppi abeliani.

(b) Per ogni divisore d dell'ordine di G, determinare se G ammetta un sottogruppo normale di ordine d.

SOLUZIONE:

(a) Siano $\sigma = (1,2,3)$ e $\tau = (1,4)(2,5)(3,6)$. Chiaramente l'elemento $\rho := \tau\sigma\tau^{-1} = (4,5,6)$ appartiene a G, e ρ e σ commutano. Siccome sia σ che ρ sono di ordine 3, il sottogruppo H di G generato da σ e τ è isomorfo a $(\mathbb{Z}/3\mathbb{Z})^2$. Osserviamo ora che τ normalizza H: in effetti,

$$\tau H \tau^{-1} = \tau\langle\sigma,\rho\rangle\tau^{-1} = \langle\tau\sigma\tau^{-1}, \tau\rho\tau^{-1}\rangle = \langle\rho,\sigma\rangle = H.$$

D'altro canto H è certamente normalizzato da ρ (visto che ρ commuta tanto con se stesso quanto con σ), quindi H è normale in G. Sia ora $K = \langle\tau\rangle$. Allora H e K sono sottogruppi di G, e siccome H è normale in G anche HK è un sottogruppo. D'altro canto HK contiene sia τ che σ, quindi HK contiene un insieme di generatori per G, da cui $G = HK$. Infine, $H \cap K = \{e\}$ (perché $|H| = 9$ e $|K| = 2$) e quindi $G \cong H \rtimes K \cong (\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$.

Dal momento che K è generato da τ, e l'azione di coniugio di τ, come verificato sopra, scambia σ e ρ, otteniamo anche che l'omomorfismo $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left((\mathbb{Z}/3\mathbb{Z})^2\right)$ che definisce il prodotto semidiretto manda un generatore di $\mathbb{Z}/2\mathbb{Z}$ nell'automorfismo $(x,y) \mapsto (y,x)$ di $(\mathbb{Z}/3\mathbb{Z})^2$.

(b) Dal punto precedente sappiamo che $|G| = 18$. È chiaro che G contiene sottogruppi normali di ordine 1 e 18; inoltre abbiamo già visto che H è normale in G, quindi G contiene un sottogruppo normale di ordine 9. Ci restano ora da considerare gli eventuali sottogruppi normali di ordine $2, 3, 6$: mostriamo che G ammette sottogruppi normali di ordine 3 e 6, ma nessun sottogruppo normale di ordine 2.

- Nessun sottogruppo di ordine 2 è normale: infatti se L fosse un sottogruppo normale di cardinalità 2 si avrebbe $HL = G$ con H, L normali in G, e dunque G sarebbe un prodotto diretto di gruppi abeliani. Ma questo non è possibile, perché come visto sopra G non è abeliano (ad esempio $\tau\sigma\tau^{-1} \neq \sigma$).

- Consideriamo l'elemento $\alpha = \rho\sigma^{-1}$: allora siccome ρ e σ commutano abbiamo $\rho\alpha\rho^{-1} = \alpha$ e $\tau\alpha\tau^{-1} = \tau\rho\tau^{-1}\tau\sigma^{-1}\tau^{-1} = \sigma\rho^{-1} = \alpha^{-1}$. In particolare vediamo che il sottogruppo generato da α è normalizzato da un insieme di generatori di G, e quindi $A := \langle\alpha\rangle$ è normale (e ovviamente di ordine 3, visto che $\alpha \in H$ e tutti gli elementi di H diversi dall'identità hanno ordine 3).

  (L'esempio precedente è utile anche per lo studio dell'esistenza di sottogruppi normali di ordine 6. Ai soli fini dell'esistenza di un sottogruppo normale di ordine 3, si può considerare in alternativa il sottogruppo $Z = \langle\sigma\rho\rangle$. Sicuramente il suo normalizzatore contiene H, visto che $Z < H$ e H è abeliano. Inoltre, $\tau\sigma\rho\tau^{-1} = \rho\sigma = \sigma\rho$, quindi anche τ appartiene al normalizzatore di Z. Ne segue che $Z \triangleleft G$ (anzi, si può verificare che Z è il centro di G).)

- Consideriamo infine il sottogruppo $B := AK$ (il fatto che sia un sottogruppo segue dal fatto che A è normale in G). È chiaro che B è il sottogruppo di G generato da α e da τ, e che $|B| = |A| \cdot |K| = 3 \cdot 2 = 6$. Inoltre il normalizzatore di B certamente contiene B (e quindi in particolare τ), e d'altro canto si ha

$$\rho B\rho^{-1} = \rho\langle\rho\sigma^{-1}, \tau\rangle\rho^{-1} = \langle\rho\sigma^{-1}, \rho\tau\rho^{-1}\rangle.$$

  Osserviamo infine che $\rho B\rho^{-1}$ contiene

$$(\rho\tau\rho^{-1})(\rho\sigma^{-1}) = \rho\tau\sigma^{-1} = \tau\tau\rho\tau\sigma^{-1} = \tau\sigma\sigma^{-1} = \tau,$$

  dunque $\rho B\rho^{-1}$ contiene sia $\rho\sigma^{-1}$ che τ, e dunque coincide con B (quanto appena visto mostra che $\rho B\rho^{-1} \supseteq \langle\rho\sigma^{-1}, \tau\rangle = B$, e ci deve essere uguaglianza per motivi di cardinalità). Ne segue quindi che B è normalizzato sia da ρ che da τ e quindi è normale in G.

  Nota. Una dimostrazione più concettuale dell'esistenza di un sottogruppo normale di ordine 6 si può ottenere dal fatto che A è il sottogruppo derivato di G: il quoziente G/A è allora un gruppo abeliano di ordine 6, quindi in particolare contiene un sottogruppo normale N di ordine 2. L'immagine inversa di N in G è il sottogruppo B descritto sopra.

2. Siano $p < q$ due numeri primi con $p \mid q-1$ e sia G un gruppo non abeliano di ordine pq.

(a) Dimostrare che G possiede un automorfismo di ordine q.

(b) Calcolare l'ordine di $Aut(G)$.

SOLUZIONE: (a) Siano x e y elementi di G di ordine rispettivamente q e p, e siano $H = \langle x\rangle$, $K = \langle y\rangle$. Allora $G \cong H \rtimes K$ e valgono le condizioni $x^q = y^p = e$ e $yxy^{-1} = x^k$, per un opportuno k di ordine p in $(\mathbb{Z}/q\mathbb{Z})^*$.

Definiamo $\varphi\colon G \to G$ come segue: $\varphi(x) = x, \varphi(y) = yx$ e, in generale, $\varphi(x^i y^j) = \varphi(x^i)\varphi(y^j) = x^i (yx)^j$. Dato che $yx = x^k y$, con semplici calcoli si verifica che $x^i (yx)^j = x^{i+k^{j-1}+k^{j-2}+\cdots+k+1} y^j$.

Verifichiamo ora che la funzione φ è un automorfismo di G di ordine q. Infatti, φ è un omomorfismo in quanto rispetta le regole che definiscono la moltiplicazione nel gruppo: $\varphi(x^q) = x^q = 1, \varphi(y^p) = (yx)^p = x^{k^{p-1}+k^{p-2}+\cdots+k+1} y^p = e$, in quanto $k^{p-1} + k^{p-2} + \cdots + k + 1 = \frac{k^p - 1}{k-1} \equiv 0 \pmod{p}$. (In alternativa, l'ordine di yx è un multiplo di p, in quanto la sua proiezione in G/H ha ordine p e, poiché G non è ciclico, si deve avere $(yx)^p = e$). Inoltre $\varphi(yxy^{-1}) = yx \cdot x \cdot x^{-1} y^{-1} = yxy^{-1} = x^k = \varphi(x^k)$.

L'omomorfismo φ è iniettivo perché dalla formula si ricava che $\varphi(x^i y^j) = e$ implica $j \equiv 0 \pmod{p}$ e $i \equiv 0 \pmod{q}$. L'omomorfismo φ è diverso dall'identità, in quanto $\varphi(y) = yx \neq y$. Per vedere che ha ordine q basta quindi verificare φ^q coincide con l'identità sui generatori di G. Abbiamo banalmente $\varphi^q(x) = x$ e inoltre $\varphi^q(y) = yx^q = y$.

(b) Per questioni di cardinalità, è immediato verificare che H è un sottogruppo caratteristico di G. D'altra parte, per ogni i con $0 < i < q$ si ottiene un automorfismo di G ponendo $\varphi(x) = x^i$, $\varphi(y) = y$ e, per estensione, $\varphi(x^a y^b) = x^{ai} y^b$. Da ciò segue che $|\operatorname{Orb}(x)| = q - 1$. La verifica che queste funzioni siano automorfismi è identica alla verifica precedente.

Nel punto (a) abbiamo trovato un sottogruppo S con q elementi di $\operatorname{Aut}(G)$ per il quale $\phi(x) = x$. In altri termini, $S \subseteq \operatorname{Stab}(x)$. Dimostriamo ora che $S = \operatorname{Stab}(x)$. Infatti, sia $\psi \in \operatorname{Aut}(G)$ tale che $\psi(x) = x$ e sia $\psi(y) = y^j x^\alpha$ per qualche $j = 1, \ldots, p-1$ e per qualche $\alpha = 0, \ldots, q-1$. Per rispettare le regole del gruppo, si deve avere $\psi(yxy^{-1}) = \psi(x^k) = x^k$, e dunque $\psi(yxy^{-1}) = y^j x^\alpha x x^{-\alpha} y^{-j} = x^{k^j}$, da cui necessariamente $k^j \equiv k \pmod{q}$, ossia $j = 1$. Ne segue che $\phi(y) = yx^\alpha$ per qualche α, ossia S ha esattamente q elementi. In conclusione,

$$|\operatorname{Aut}(G)| = |\operatorname{Stab}(x)| \cdot |\operatorname{Orb}(x)| = q(q-1)\,.$$

Seconda soluzione:

(a) Ricordiamo che $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ e rappresentiamo gli elementi di G come coppie (a, b) con $a \in \mathbb{Z}/q\mathbb{Z}$ e $b \in \mathbb{Z}/p\mathbb{Z}$. La regola di moltiplicazione in G è

$$(x_1, y_1)(x_2, y_2) = (x_1 + k^{y_1} x_2, y_1 + y_2)$$

per un certo $k \in (\mathbb{Z}/q\mathbb{Z})^\times$ di ordine p. Siano $x = (1, 0)$ e $y = (0, 1)$. Costruiremo un isomorfismo $\varphi : G \to G$ tale che $\varphi(x) = x$ e $\varphi(y) = xy = (1, 1)$. Un'induzione

immediata mostra che $(1,1)^r = (1+k+\cdots+k^{r-1}, r)$, quindi dobbiamo porre

$$\begin{aligned}\varphi((a,b)) &= \varphi((a,0)(0,b)) = \varphi(x)^a\varphi(y)^b = (a,0)(1,1)^b \\ &= (a,0)(1+k+\cdots+k^{b-1},b) = \left(a+\frac{k^b-1}{k-1},b\right).\end{aligned}$$

Verifichiamo ora che φ così definito è un omomorfismo. In effetti si ha

$$\varphi((a_1,b_1)(a_2,b_2)) = \varphi((a_1+k^{b_1}a_2, b_1+b_2)) = \left(a_1+k^{b_1}a_2+\frac{k^{b_1+b_2}}{k-1}, b_1+b_2\right) \quad (1)$$

mentre

$$\begin{aligned}\varphi((a_1,b_1))\varphi((a_2,b_2)) &= \left(a_1+\frac{k^{b_1}-1}{k-1},b_1\right)\left(a_2+\frac{k^{b_2}-1}{k-1},b_2\right) \\ &= \left(a_1+\frac{k^{b_1}-1}{k-1}+k^{b_1}\left(a_2+\frac{k^{b_2}-1}{k-1}\right), b_1+b_2\right),\end{aligned}$$

ed è immediato verificare che questa espressione coincide con (1). Inoltre φ è iniettivo: se $\varphi((a,b)) = \left(a+\frac{k^b-1}{k-1},b\right)$ è l'elemento neutro $(0,0)$, allora b è congruo a zero modulo p, e quindi $k^b-1 \equiv 0 \pmod q$ (ricordiamo che k è di ordine p in $(\mathbb{Z}/q\mathbb{Z})^\times$). Si deve allora avere $a \equiv 0 \pmod q$, e dunque $(a,b) = (0,0)$. L'omomorfismo φ è quindi iniettivo e dunque un automorfismo, e non è l'identità, perché $\varphi(y) \neq y$. Valgono poi $\varphi^q(x) = x$ e $\varphi^q(y) = x^q y = y$, quindi φ^q coincide con l'identità su un insieme di generatori, ed è dunque l'identità: φ è allora di ordine q come voluto.

(b) Consideriamo un generico automorfismo $\psi : G \to G$ e scriviamo $\psi(x) = (a,b)$, $\psi(y) = (c,d)$. Siccome $\psi(x)^q = (0,0)$, e la seconda coordinata di $(a,b)^q$ è qb, si deve avere $qb \equiv 0 \pmod p \Rightarrow b \equiv 0 \pmod p$. Inoltre si ha $\psi(x^k) = \psi(yxy^{-1}) = \psi(y)\psi(x)\psi(y)^{-1}$, da cui $\psi(x)^k\psi(y) = \psi(y)\psi(x)$, ovvero $(ak,0)(c,d) = (c,d)(a,0)$, e confrontando le prime coordinate otteniamo $ak + c \equiv c + k^d a \pmod q$. Siccome $a \not\equiv 0 \pmod q$ e k è di ordine p in $(\mathbb{Z}/q\mathbb{Z})^\times$, questo implica che $d = 1$ in $\mathbb{Z}/p\mathbb{Z}$. Ne segue che ci sono al massimo $q(q-1)$ scelte per ψ: in effetti ci sono $q-1$ scelte per a (che deve essere primo con q) e q scelte per c, mentre $b = 0$ e $d = 1$ sono fissati.

Infine, sia g un generatore modulo p. Ponendo $\chi(x) = gx$ e $\chi(y) = y$ si ottiene un automorfismo di ordine $q-1$ (verifiche simili a quelle della parte (a), ma più semplici), dunque $\#\operatorname{Aut}(G)$ è divisibile per $q-1$. D'altro canto la parte (a) mostra che $q \mid \#\operatorname{Aut}(G)$, quindi si ha $q(q-1) \mid \#\operatorname{Aut}(G)$, che combinato con la disuguaglianza $\#\operatorname{Aut}(G) \leq q(q-1)$ fornisce $\#\operatorname{Aut}(G) = q(q-1)$.

3. Sia G un gruppo di ordine 132. Dimostrare che G non è un gruppo semplice.

SOLUZIONE: Supponiamo per assurdo che G sia semplice. Allora un suo sottogruppo di Sylow P di ordine 11 non è normale. Per i teoremi di Sylow, il numero dei

sottogruppi coniugati a P è un divisore di 12 e congruo a 1 modulo 11, quindi, essendo diverso da 1, è necessariamente uguale a 12.

Siccome ogni sottogruppo di ordine 11 contiene 10 elementi di ordine 11, questo significa che in G ci sono $10 \cdot 12$ elementi di ordine 11.

Consideriamo un sottogruppo di Sylow Q di ordine 3. Se esso non è normale, allora ha almeno un numero di coniugati maggiore di 1 e congruo ad 1 modulo 3, cioè almeno 4 coniugati. Come sopra, questo significa che G contiene almeno $4 \cdot 2 = 8$ elementi di ordine 3.

Restano $132 - 120 - 8 = 4$ elementi il cui ordine può dividere 4. Siccome esiste un sottogruppo di Sylow di ordine 4, questo deve essere costituito esattamente da questi 4 elementi. In particolare, il 4-Sylow è unico e quindi normale, e dunque G non è semplice.