Esercizi di Algebra 2 - 13/4/2022

Esercizio 1. Quali dei seguenti gruppi abeliani sono isomorfi:

$$A := \mathbb{Z}/6 \oplus \mathbb{Z}/36, \quad B := \mathbb{Z}/6 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/18,$$
$$C := \mathbb{Z}/12 \oplus \mathbb{Z}/18, \quad D := \mathbb{Z}/9 \oplus (\mathbb{Z}/2)^3 \oplus \mathbb{Z}/3.$$

Svolgimento. Fattori invarianti: A: $6, 36$; B: $2, 6, 18$.
$C = \mathbb{Z}/4 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/9 = (\mathbb{Z}/2 \oplus \mathbb{Z}/3) \oplus (\mathbb{Z}/4 \oplus \mathbb{Z}/9) = \mathbb{Z}/6 \oplus \mathbb{Z}/36$, fattori invarianti: $6, 36$.
$D = \mathbb{Z}/2 \oplus (\mathbb{Z}/2 \oplus \mathbb{Z}/3) \oplus (\mathbb{Z}/2 \oplus \mathbb{Z}/9) = \mathbb{Z}/2 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}/18$, fattori invarianti: $2, 6, 18$.
Quindi $A \cong C \ncong B \cong D$. □

Esercizio 2. Quale dei gruppi sopra contiene un sottogruppo isomorfo a $\mathbb{Z}/2 \oplus \mathbb{Z}/6$?

Svolgimento. Tutti. □

Esercizio 3. Scrivere nella forma dei divisori elementari i seguenti gruppi abeliani:

$$\mathrm{Hom}(\mathbb{Z}/6, \mathbb{Z}/12), \qquad \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/12), \qquad \mathrm{Hom}(\mathbb{Z}^2, \mathbb{Z}/12),$$
$$\mathrm{Hom}(\mathbb{Z} \oplus \mathbb{Z}/2, \mathbb{Z}/14), \qquad \mathrm{Hom}(\mathbb{Z}/3 \oplus \mathbb{Z}/9, \mathbb{Z}/7 \oplus \mathbb{Z}/21).$$

Esercizio 4. Sia $V_4 \cong (\mathbb{Z}/2)^2$ il gruppo di Klein. Dimostrare che $\mathrm{Aut}\, V_4 \cong \mathrm{GL}(2, 2) \cong S_3$.

Svolgimento. Sia

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Allora $A^2 = B^3 = I$. Sia $X := V_4 - \{e\}$. X consiste di 3 elementi di ordine 2. Se identifichiamo V_4 con lo spazio vettoriale $V := (\mathbb{Z}/2)^2$ allora $X = V - \{0\}$. Allora è chiaro che $\mathrm{GL}(V)$ è transitivo su X. Otteniamo un morfismo $\mathrm{GL}(V) \to S_X = S_3$. È evidentemente iniettivo. È anche suriettivo perché le immagini di A e B generano S_3. □

Esercizio 5. Classificare i gruppi abeliani di ordine 16 e trovare quello che ha l'ordine del gruppo degli automorfismi più grande possibile.

Svolgimento. Un gruppo di ordine 16 è somme di gruppi ciclici di ordine una potenza di due: $G = \mathbb{Z}/(2^{n_1}) \oplus \cdots \mathbb{Z}/(2^{n_l})$ dove $n_1 + \cdots + n_k = 4$ e possiamo supporre $n_1 \leq \cdots \leq n_k$. In sostanza n_i è una partizione di 4. Queste partizioni sono

$$
\begin{aligned}
4 =& 1+1+1+1 \\
4 =& 1+1+2 \\
4 =& 2+2 \\
4 =& 1+3 \\
4 =& 4.
\end{aligned}
$$

I gruppi corrispondenti sono i seguenti.

$$
\begin{array}{lll}
G_1 = (\mathbb{Z}/2)^4 & \operatorname{Aut} G_1 = \mathrm{GL}(4,2) & |\operatorname{Aut} G_1| = 20160 \\
G_2 = (\mathbb{Z}/2)^2 \oplus \mathbb{Z}/4 & \operatorname{Aut} G_2 = ? & |\operatorname{Aut} G_2| \leq 336 \\
G_3 = (\mathbb{Z}/4)^2 & \operatorname{Aut} G_3 = ? & |\operatorname{Aut} G_3| \leq 132 \\
G_4 = \mathbb{Z}/2 \oplus \mathbb{Z}/8 & \operatorname{Aut} G_4 = ? & |\operatorname{Aut} G_4| \leq 24 \\
G_5 = \mathbb{Z}/16 & \operatorname{Aut} G_5 = \mathbb{Z}/16^* & |\operatorname{Aut} G_5| = 8.
\end{array}
$$

Vediamo come ottenere le stime.
Consideriamo G_2. Questo gruppo ha 8 elementi di ordine quattro e 7 elementi di ordine 2. Inoltre è generato da $(\bar{1},0,0),(0,\bar{1},0),(0,0,\bar{1})$. Se $f \in \operatorname{Aut} G_2$, allora $f(\bar{1},0,0)$ è un elemento di ordine 2, quindi ho 7 possibilità. $f(0,\bar{1},0)$ è un altro elemento di ordine 2, distinto dal precedente (perché f è iniettiva), dunque ho 6 possibilità. Infine $f(0,0,\bar{1})$ è un elemento di ordine 4, dunque ho 8 possibilità. In totale ho $6 \cdot 7 \cdot 8 = 336$ possibilità. Per ciascuna di queste possibilità c'è al più un automorfismo di G_2. Infatti se due automorfismi coincidono sui generatori coincidono dovunque.
Per G_3 usiamo la stessa idea: ci sono 12 elementi di ordine 4. D'altronde G_3 è generato da $(1,0)$ e $(0,1$, entrambi di ordine 4. Quindi ho al più $12 \cdot 11 = 132$ possibilità.
Il gruppo G_4 ha 3 elementi di ordine 2 e 8 elementi di ordine 8. È generato da $(\bar{1},0)$ e $(0,\bar{1})$ di ordine rispettivamente 2 e 8. Quindi in totale ho al più $3 \cdot 8 = 24$ automorfismi. □

Esercizio 6. Sia D_n il gruppo diedrale formato dalle isometrie di un n-agono, ossia $|D_n| = 2n$.

(1) Sia H un gruppo. Dimostrare che H è abeliano se e solo se $\varphi : H \to H, \varphi(h) = h^{-1}$ è un morfismo.
(2) Dimostrare che $D_n = C_n \rtimes_\theta C_2$ dove θ manda il generatore di C_2 in $\varphi \in \operatorname{Aut} C_n$.
(3) Dimostrare che se $n = 2m$ e m è dispari, allora $D_n \cong C_2 \times D_m$.
(4) Se $n = 2m$ e m pari, è vero o falso che $D_n \cong C_2 \times D_m$?

Esercizio 7. Siano H ed N gruppi e sia $\theta : H \to \operatorname{Aut} N$. Dimostrare che $G := N \rtimes_\theta H$ è abeliano se e solo se H ed N sono abeliani e θ è il morfismo banale (ossia $N \rtimes_\theta H = N \times H$).

Esercizio 8. Sia G un gruppo e siano N ed H sottogruppi tali che $N \lhd G$, $H \cap N = \{e\}$ e $NH = G$. Se non esistono morfismi non banali $H \to \operatorname{Aut} N$, allora anche H è normale e $G \cong N \times H$.

Svolgimento. Per ipotesi $G = N \rtimes_\theta H$ con $\theta_h(n) = hnh^{-1}$. Se $\theta \equiv \mathrm{id}_N$, allora $[H, N] = \{e\}$, dunque $H \lhd G$ e G è il prodotto diretto interno di N ed H. □

Esercizio 9. Esiste un gruppo semplice di ordine 2019, 2020, 2021 o 2022?

Svolgimento. $2019 = 3 \cdot 673$ e 673 è primo. Si vede subito che $n_{673} = 1$, dunque esiste un sottogruppo normale e $G \cong P_{6763} \rtimes_\theta P_3$. Siccome 672 è divisibile per 3, ho vari casi, ma c'è sempre un sottogruppo normale. Dunque un gruppo di ordine 2019 non è semplice.

$2020 = 2^2 \cdot 5 \cdot 101$ e $P_{101} \lhd G$.

$2021 = 43 \cdot 47$ dunque di questo ordine c'è solo il gruppo ciclico.

$2022 = 2 \cdot 3 \cdot 337$ e $P_{337} \lhd G$. □

Esercizio 10. Sia G un gruppo di ordine $p^a \cdot m$ con $p \nmid m$. Dimostrare che $p > m$, allora $n_p = 1$.

Svolgimento. $n_p = 1 + kp$ con $k \geq 0$. Ma se $k > 0$ allora $1 + kp > p > m$, dunque $1 + kp \nmid m$. Ma $n_p | m$, dunque $k = 0$. □

Esercizio 11 (Compito del 23/06/2020)**.** Sia p un numero primo. e sia G un gruppo di ordine $p(2p + 5)$.

(1) Dimostrare che se $2p + 5$ è primo, allora G è ciclico.
(2) Dimostrare che se $p > 2$, allora G ha un unico p-Sylow.
(3) Dimostrare che se $p = 47$, allora G è abeliano.

Svolgimento. (1) Se $2p + 5$ è primo, $p \neq 2$ e allora $p \nmid 2p + 4$.
(2) Prima escludo il caso $p|(2p+5)$ (cioè $p = 5$). Poi ho $(1+kp)m = 2p+5$, dunque $(mk-2)p = 5-m$. Supponiamo per assurdo $k|geq1$. Se fosse $m = 1$ avrei che $p|4$. Dunque $m \geq 2$, $mk - 2 \geq 0$ e $m \leq 5$. Quindi $p > 2$ divide un numero minore di 3, assurdo. Dunque $k = 1$ e $n_p = 1$.
(3) $n_{47} = 1 + 47k|99$, dunque $n_{47} = 1$. Per lo stesso motivo anche $n_{11} = 1$. Infatti sia $n_{11} = 1 + 11k|9 \cdot 47$, ossia $(1 + 11k)m = 3^2 \cdot 47$. Se $47|(1 + 11K)$, allora $1 + 11k = 47s$ con $k, s > 0$. Ma $n_{11}|3^3 \cdot 47$, dunque $s|3^2$. Possiamo velocemente escludere i casi possibili, cioè $s = 1, s = 2, s = 3$. Dunque $47 \nmid (1 + 11k)$, quindi $47|m$ e $(1 + 11k)m' = 3^2$. Ma allora necessariamente $k = 0$ e $n_{11} = 1$. Morale $P_{11} \lhd G$. Inoltre $P_{47} \lhd G$ per il punto (2). Segue che $N := P_{11} \cdot P_{547}$ è un sottogruppo normale di G ed è isomorfo a $\mathbb{Z}/11 \times \mathbb{Z}/47 = \mathbb{Z}/(11 \cdot 47)$. Fissiamo un 3-Sylow H. Allora $G = N \rtimes_\theta H$, dove $\theta_h \in \operatorname{Aut} N$ è la restrizione del coniugio in G. Ma $\operatorname{Aut} N \cong \mathbb{Z}/(11 \cdot 47)^* \cong \mathbb{Z}/11 \times \mathbb{Z}/46 = \mathbb{Z}/2 \times \mathbb{Z}/11 \times \mathbb{Z}/23$. Pertanto θ è il morfismo banale, perche $\operatorname{Aut} N$ non ha nessun elemento di ordine 3. Dunque $G \cong N \times H$ e G è abeliano. □

Esercizio 12. Un gruppo di ordine 45 è abeliano.

Svolgimento. $45 = 3^2 \cdot 5$. Si vede subito che $n_3 = n_5 = 1$, quindi $P_3, P_5 \lhd G$ e $G \cong P_3 \times P_5$. Siccome i gruppi di ordine 3^2 e di ordine 5 sono tutti abeliani, G è abeliano. □

Esercizio 13. Se $o(G) = 30$ allora G ha un p-Sylow normale. (Suggerimento: dimostrare che o $n_3 = 1$ o $n_5 = 1$.)

Svolgimento. Se non fosse così, avremmo $n_3 = 10$ e $n_5 = 6$. Ma allora ci sarebbero 20 elementi di ordine 3 e 24 elementi di ordine 5. Troppi! □

Esercizio 14. Dimostrare che se $o(G) = 56$, allora esiste un p-Sylow normale.

Svolgimento. $56 = 2^3 \cdot 7$. $n_7 = 1$ o 8. Supponiamo $n_7 = 8$. Allora trovo $6 \cdot 8 = 48$ elementi di ordine 7. Sia P_2 un 2-Sylow. Quindi $G = G_7 \sqcup P_2$. Quindi $P_2 \lhd G$. □

Esercizio 15. Classificare i gruppi di ordine 76. (Suggerimento: ci sono 4 classi di isomorfismo di gruppi di ordine 76.)

Svolgimento. $76 = 2^2 \cdot 19$. $n_{19} = 1$. Dunque $P_{19} \lhd G$. Sia P_2 un 2-Sylow. Allora $G = P_{19} \rtimes_\theta P_2$. Ovviamente $P_2 = V_4$ oppure $P_2 = \mathbb{Z}/4$. $\operatorname{Aut} P_{19} = \mathbb{Z}/18$. Gli unici morfismi $\theta : \mathbb{Z}/4 \to \mathbb{Z}/18$ sono quello banale, che dà $\mathbb{Z}/76$ e quello che manda $[1]_4$ in $[9]_{18}$, che dà un prodotto semidiretto $\mathbb{Z}/19 \ltimes \mathbb{Z}/4$.

Consideriamo ora i morfismi $\theta : V_4 \to \mathbb{Z}/18$. Ogni elemento di ordine 2 in V_4 deve finire in un elemento di ordine 1 o 2 in $\mathbb{Z}/18$, dunque o in $[0]_{18}$ o in $[9]_{18}$. Se tutto V_4 va a finire in $[0]_{18}$ allora θ è il morfismo banale e il corrispondente gruppo $\mathbb{Z}/19 \rtimes V_4$ è semplicemente il prodotto diretto

$$\mathbb{Z}/19 \times V_4 = \mathbb{Z}/19 \times (\mathbb{Z}/2)^2.$$

Se θ non è banale, osserviamo che il numero di elementi che vanno a finire in $[9]_{18}$ è per forza 2. Infatti sia $V_4 = \{e, a, b, c = a + b\}$. Se $\theta(a) = [9]_{18}$ e $\theta(b) = [0]_{18}$, allora $\theta(c) = [9]_{18}$. Mentre se $\theta(a) = \theta(b) = [9]_{18}$, allora $\theta(c) = \theta(a) + \theta(b) = [9]_{18} + [9]_{18} = [0]_{18}$. Quindi abbiamo 3 morfismi non banali $V_4 \to \mathbb{Z}/18 \cong \operatorname{Aut} \mathbb{Z}/19$. Per l'Esercizo 80 degli *Appunti*, se $\theta' \circ \beta = \theta$ dove $\beta \in \operatorname{Aut} V_4$, allora $\mathbb{Z}/19 \rtimes_\theta V_4 \cong \mathbb{Z}/19 \rtimes_{\theta'} V_4$. Siccome $S_3 = \operatorname{Aut} V_4$ agisce transitivamente sugli elementi di ordine 2 di V_4, risulta che i 3 morfismi non banali che abbiamo trovato sono tutti ottenuti l'uno dall'altro componendo con un $\beta \in \operatorname{Aut} V_4$. Quindi possiamo considerare solo uno di questi morfismi, ossia $\theta : V_4 \to \mathbb{Z}/18 \cong \operatorname{Aut} N$

$$\theta(1,0) = [0]_{18}, \quad \theta((0,1) = \theta(1,1)[9]_{18}.$$

Otteniamo così l'ultimo gruppo possibile:

$$G_4 = \mathbb{Z}/19 \rtimes_\theta V_4.$$

Siccome il primo fattore $\mathbb{Z}/2$ agisce banalmente su $\mathbb{Z}/19$, $G_4 = \mathbb{Z}/2 \times (\mathbb{Z}/2 \ltimes \mathbb{Z}/19) = \mathbb{Z}/2 \times D_{19} = \mathbb{Z}/2 \ltimes \mathbb{Z}/38 = D_{38}$ (Esercizio 6). Riassumendo abbiamo trovato questi 4 gruppi:

$$\mathbb{Z}/76, \quad \mathbb{Z}/19 \rtimes_\theta \mathbb{Z}/4, \quad (\mathbb{Z}^2)^2 \times \mathbb{Z}/19, \quad D_{38}.$$

Nel secondo gruppo, $\theta([1]_4) = [9]_{18} =$ il solito automorfismo φ. $\square$

Esercizio 16. Sfruttando l'esercizio 13 classificare i gruppi di ordine 30.

Svolgimento. Sia G un gruppo di ordine 30, Fissiamo un 3-Sylow P_3 e un 5-Sylow P_5. Per l'esercizio 13 uno dei due è normale. Quindi il prodotto $N := P_3P_5$ è un sottogruppo di G ed è normale perché ha indice 2. Sia P_2 un 2-Sylow qualsiasi. Allora $G = P_3P_5 \rtimes P_2$. Quindi G è un prodotto semidiretto

$$G = (\mathbb{Z}/3 \times \mathbb{Z}/5) \rtimes_\theta \mathbb{Z}/2.$$

Osserviamo che ogni automorfismo di $\mathbb{Z}/3 \times \mathbb{Z}/5 = \mathbb{Z}/15$ manda ciascuno dei due fattori in sé stesso (per esempio perché i due fattori sono i sottogruppi di Sylow normali). Da questo segue che entrambi i sottogruppi P_3 e P_5 sono normali.

Per classificare i gruppi basta capire quali sono le possibilità per il morfismo

$$\theta : \mathbb{Z}/2 \to \operatorname{Aut} \mathbb{Z}/15 \cong \mathbb{Z}/15^* \cong \mathbb{Z}/3^* \times \mathbb{Z}/5^* \cong \mathbb{Z}/2 \times \mathbb{Z}/4,$$

e controllare che i gruppi ottenuti in questo modo siano tutti non isomorfi. Ovviamente $\theta = (\theta_1, \theta_2)$ dove $\theta_1 : \mathbb{Z}/2 \to \mathbb{Z}/2$ e $\theta_2 : \mathbb{Z}/2 \to \mathbb{Z}/4$. Per θ_1 ci sono due possibilità: $\theta_1([1]_2) = [0]_2$ o $\theta_1([1]_2) = [1]_2$. Per θ_2 ci sono altre due possibilità: $\theta_2([1]_2) = [0]_4$ o $\theta_2([1]_2) = [2]_4$. In totale abbiamo quattro possibilità

(1) $\theta_1([1]_2) = [0]_2$ e $\theta_2([1]_2) = [0]_4$. θ è il morfismo banale e $G = \mathbb{Z}/2 \times \mathbb{Z}/15 = \mathbb{Z}/30$.
(2) $\theta_1([1]_2) = [1]_2$ e $\theta_2([1]_2) = [0]_4$. In questo caso θ agisce banalmente su $\mathbb{Z}/5$. Quindi P_5 commuta con P_2 e posso portarlo fuori dal prodotto semidiretto (questo ragionamento è formalizzato nell'Esercizio 20): $G = P_5 \times (P_3 \rtimes P_2) \cong \mathbb{Z}/5 \times (\mathbb{Z}/3 \rtimes_{\theta_1} \mathbb{Z}/2)$. Infine chi è $(\mathbb{Z}/3 \rtimes_{\theta_1} \mathbb{Z}/2)$? Nell'isomorfismo $\operatorname{Aut} Z/3 \cong \mathbb{Z}/2$ l'elemento $[1]_2$ corrisponde all'automorfismo $x \mapsto -x$. Dall'Esercizio otteniamo 6 $\mathbb{Z}/3 \rtimes_{\theta_1} \mathbb{Z}/2 = S_3$ e $G = \mathbb{Z}/5 \times S_3$.
(3) $\theta_1([1]_2) = [0]_2$ e $\theta_2([1]_2) = [2]_4$. Questo caso è molto simile: θ agisce banalmente su $\mathbb{Z}/3$, P_3 commuta con P_2 e posso portarlo fuori dal prodotto semidiretto: $G = P_3 \times (P_5 \rtimes P_2) \cong \mathbb{Z}/3 \times (\mathbb{Z}/5 \rtimes_{\theta_2} \mathbb{Z}/2)$. Anche qui $[2]_4 \in \mathbb{Z}/4$ rappresenta l'unico automorfismo non banale di ordine 2 di $Z5$ che è $x \mapsto -x$. Dunque $\mathbb{Z}/5 \rtimes_{\theta_2} \mathbb{Z}/2 = D_5$ e $G = \mathbb{Z}/3 \times D_5$.
(4) $\theta_1([1]_2) = [1]_2$ e $\theta_2([1]_2) = [2]_4$. Qui $\theta_1([1]_2)$ è l'automorfismo $x \mapsto -x$ nel gruppo $\mathbb{Z}/3$ e $\theta_2([1]_2)$ è l'automorfismo $x \mapsto -x$ nel gruppo

$\mathbb{Z}/5$. Pertanto $\theta([1]_2) = (\theta_1([1]_2), \theta_2([1]_2))$ è l'automorfismo $x \mapsto -x$ nel gruppo prodotto cioè $Z/3 \times \mathbb{Z}/5 = \mathbb{Z}_15$. Morale $G = D_{15}$.

$\square$

Esercizio 17. Siano K, N, H gruppi e sia $\theta : H \to \operatorname{Aut} N$ un morfismo. Poniamo $\bar{\theta}_h := (\mathrm{id}_K, \theta_h) \in \operatorname{Aut} K \times N$. Sia F l'applicazione identica dell'insieme $K \times N \times H$. Dimostrare che F è un isomorfismo del gruppo $K \times (N \rtimes_\theta H)$ sul gruppo $(K \times N) \rtimes_{\bar{\theta}} H$.

Esercizio 18. Sia $G = \langle g \rangle$ un gruppo ciclico di ordine n e sia d un divisore di n. Allora $\{x \in G : o(x)|d\} = \langle g^{n/d} \rangle$.

Svolgimento. Sia $o(x) = e|d$. Allora $\langle x \rangle$ è un sottogruppo di ordine e e quindi coincide con $\langle g^{m/e} \rangle$ che è l'unico sottogruppo di G di questo ordine (Proposizione 51 (4) delle note). Inoltre $g^{m/e} = (g^{m/d})^{d/e}$, dunque $\langle g^{m/e} \rangle \subset \langle g^{m/d} \rangle$, quindi $\{x \in G : o(x)|d\} =\subset \ sxg^{m/d}\rangle$. L'inclusione opposta è ovvia.

$\square$

Esercizio 19. Sia A un gruppo abeliano e sia $C = \mathbb{Z} \cdot x$ un gruppo ciclico generato da x (in notazione additiva).

(1) L'applicazione $F : \operatorname{Hom}(C, A) \to A, F(f) := f(x)$ è un morfismo di gruppi iniettivo.
(2) Se $C = \mathbb{Z}$, allora $\operatorname{Im} F = A$.
(3) Se $C = \mathbb{Z}/n$ allora $\operatorname{Im} F = \{a \in A : o(a)|n\}$.
(4) Se $C = \mathbb{Z}/n$ e $A = \mathbb{Z}/m$, allora $\operatorname{Im} F \cong \mathbb{Z}/(m, n)$ (dove (m, n) indica il massimo comun divisore di m ed n).

Svolgimento. (1) Basta osservare che se $f, f' \in \operatorname{Hom}(C, A)$, allora $F(f + f') = (f + f')(x) = f(x) + f'(x)$. Abbiamo sfruttato solamente la definizione della somma in $\operatorname{Hom}(C, A)$.
(2) Ovvio.
(3) Ricordiamo che se $f : G \to G'$ è un morfismo di gruppi, allora $o(f(g))|o(g)$ per ogni $g \in G$. Dunque $o(f(x))|n$, quindi $\operatorname{Im} F \subset \{a \in A : o(a)|n\}$. Per il viceversa basta usare il Teorema di Omomorfismo: dato $a \in A$ considero il morfismo $\tilde{f} : \mathbb{Z} \to A$ tale che $\tilde{f}(1) = a$. Se $o(a)|n$, $n\mathbb{Z} \subset \ker \tilde{f}$, dunque $\tilde{f}$ passa al quoziente $f : \mathbb{Z}/n\mathbb{Z} \to A$.
(4) Poniamo $d := (m, n)$. Per ogni $a \in \mathbb{Z}/m$, $o(a)|m$. Dunque se $A = \mathbb{Z}/m$, $\{a \in A : o(a)|n\} = \{a \in \mathbb{Z}/m : o(a)|d\}$. Per l'esercizio precedente $\{a \in \mathbb{Z}/m : o(a)|d\} = \langle [m/d]_m \rangle$ e quest'ultimo è un gruppo ciclico di ordine d.

$\square$

Esercizio 20. Siano N_1, N_2, H gruppi e siano $\theta_i : H \to \operatorname{Aut} N_i$ dei morfismi. Poniamo $\theta = (\theta_1, \theta_2)$. Dimostrare che se $\theta_1 = \mathrm{id}_{N_1}$ l'applicazione identica dell'insieme $N_1 \times N_2 \times H$ dà un isomorfismo

$$(N_1 \times N_2) \rtimes_\theta H \cong N_1 \times (N_2 \rtimes_{\theta_2} H).$$

Esercizio 21. Sia V uno spazio vettoriale e sia $\operatorname{Aff}(V)$ il gruppo delle affinità di V, ossia le trasformazioni della forma $f(v) = Av + v_0$ con $A \in \mathrm{GL}(V)$ e $v_0 \in V$. Dimostrare che $\operatorname{Aff}(V) = V \rtimes_\theta \mathrm{GL}(V)$, dove $\theta_A(v) = Av$.