

# 1 Groups

## 1.6 Direct products and direct sum

1. We can easily get that  $SO(n, \mathbb{R}) \triangleleft O(n, \mathbb{R})$  and  $\{\pm E_n\} \triangleleft O(n, \mathbb{R})$ . If  $n$  is odd,  $SO(n, \mathbb{R}) \cap \{\pm E_n\} = \{E_n\}$ , if  $n$  is even,  $SO(n, \mathbb{R}) \cap \{\pm E_n\} = \{\pm E_n\}$ . While if  $n$  is odd, for any  $A \in O(n, \mathbb{R})$ ,  $(-E_n \cdot A) \cdot (-E_n) \in SO(n, \mathbb{R}) \cdot \{\pm E_n\}$ . Hence  $O(n, \mathbb{R}) \cong SO(n, \mathbb{R}) \times \{\pm E_n\}$  if  $n$  is odd, while  $O(n, \mathbb{R}) \not\cong SO(n, \mathbb{R}) \times \{\pm E_n\}$  if  $n$  is even.
2. If  $H_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$ ,  $H_2 = \mathbb{Z}_3 \times \mathbb{Z}_3$ ,  $K_1 = K_2 = \mathbb{Z}_6$ , then  $H_1 \times H_2 \cong K_1 \times K_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_6$ , while any of  $H_1$  and  $H_2$  is not isomorphic to  $K_j$  for  $j = 1, 2$ .
3. Let  $G = \langle a \rangle$ ,  $H = \langle b \rangle$ ,  $|a| = n$ ,  $|b| = m$ . If  $(m, n) = 1$ , then  $G \times H = \langle (a, b) \rangle$ . In fact,  $(a, b)^k = (a^k, b^k) = (e, e)$ , then  $m \mid k$  and  $n \mid k$ , while  $(m, n) = 1$ , thus  $mn \mid k$ , hence  $|(a, b)| = mn$ , therefore  $\langle (a, b) \rangle \leq G \times H$ , whence  $|G \times H| = mn$ . Hence  $G \times H = \langle (a, b) \rangle$ . Conversely,  $G \times H = \langle (a, b) \rangle$ , then  $|(a, b)| = mn$ . Suppose  $d = (m, n)$ , then  $(a, b)^{\frac{mn}{d}} = (a^{\frac{mn}{d}}, b^{\frac{mn}{d}}) = (e, e)$ , thus  $mn \mid \frac{mn}{d}$ , hence  $d = 1$ .
4. For any  $\sigma \in S_4$ ,  $\sigma(ij)(kl)\sigma^{-1} = \sigma(ij)\sigma^{-1}\sigma(kl)\sigma^{-1} = (\sigma(i)\sigma(j))(\sigma(k)\sigma(l))$ , thus  $K \triangleleft S_4$ , while  $H \subseteq A_4$ , hence  $K \triangleleft A_4$ . Since  $[A_4 : K] = 3$ , hence  $A_4/K \cong \mathbb{Z}_3$ . Let  $B = \{x_1 := (12)(34), x_2 := (13)(24), x_3 := (14)(23)\}$ ,  $S_4 \times B \rightarrow B$ ,  $(\sigma, (ij)(kl)) \mapsto (\sigma(i)\sigma(j))(\sigma(k)\sigma(l))$ , then  $B$  is a  $S_4$ -set.  $K \subseteq \text{Ker}\varphi$  where  $\varphi : S_4 \rightarrow \text{Sym}(B) = S_3$  is a group homomorphism induced by  $S_4$ -set. Since  $(23)x_1 = x_2$ ,  $(12) \in \text{Im}\varphi$ , while  $(14)x_2 = x_3$ ,  $(23) \in \text{Im}\varphi$ . Hence  $\text{Im}\varphi \supseteq \langle (12), (23) \rangle = S_3$ , then  $\varphi$  is surjective. As  $S_4/\text{Ker}\varphi \cong S_3$ ,  $|\text{Ker}\varphi| = 4$ , thus  $K = \text{Ker}\varphi$ . Therefore  $S_4/K \cong S_3$ .
5. Suppose  $N \cap K = \{e\}$  and  $N \cap H = \{e\}$ . For any  $n \in N$  and any  $k \in K$ , since  $nkn^{-1}k^{-1} = (nkn^{-1})k \in K$  ( $\because K \triangleleft G$ ),  $n(kn^{-1}k^{-1}) \in N$  ( $\because N \triangleleft G$ ) and  $N \cap K = \{e\}$ ,  $nkn^{-1}k^{-1} = e$ , i.e.  $nk = kn$ . Similarly,  $nh = hn$  for any  $h \in H$ . As any  $g \in G$ ,  $g = hk$  for some  $h \in H, k \in K$ , then  $ng = nhk = hkn = gn$ , thus  $N \subseteq C(G)$ . For example, (1)  $G = S_3 \times S_3$ ,  $N = \{(a, b) | a, b \in \langle (123) \rangle\}$ , then  $N \cap S_3 = \langle (123) \rangle$ ,  $N \not\subseteq C(G) = \{((1), (1))\}$ . (2)  $G = GL(3, \mathbb{R}) \times GL(3, \mathbb{R})$ ,  $N = \{(kE, lE) | kl = 1\}$ , then  $N \subseteq C(G)$ ,  $N \cap GL(3, \mathbb{R}) \times \{E\} = \{(E, E)\}$ ,  $N \cap \{E\} \times GL(3, \mathbb{R}) = \{(E, E)\}$ .
6.  $|G| = 21 = 3 \times 7$ , according to Sylow Theorem, there is only one Sylow 7-subgroup  $H_1 \triangleleft G$ , and there are 7 Sylow 3-subgroups or one Sylow 3-subgroup.
  - (a) If  $G$  has only one Sylow 3-subgroup  $K$ , then  $G \cong \mathbb{Z}_3 \times \mathbb{Z}_7 \cong \mathbb{Z}_{21}$ .
  - (b) If  $G$  has 7 Sylow 3-subgroups. Let  $H_1 = \langle a \rangle$ ,  $H_2 = \langle b \rangle$  is a Sylow 3-subgroup. Since  $H_1 \triangleleft G$ ,  $bab^{-1} \in \langle a \rangle$ , hence there is  $r \in \{2, 3, 4, 5, 6\}$  such that  $bab^{-1} = a^r$ , then  $ba = a^r b$  and  $G = \{a^i b^j | 1 \leq i \leq 7, 1 \leq j \leq 3\}$ . As  $(ba)^7 = a^{2r^2+3r+2}b \neq e$ ,  $(ba)^3 = a^{r^2+r+1}b = e$ , thus  $\text{ord}(ba) = 7$  or 3. If  $\text{ord}(ba) = 21$ , according to Exercise 1.6.3,  $G$  is cyclic, hence  $r = 2$  or 4. If  $ba = a^2b$ , then  $b^2a = a^4b^2$ , let  $b' = b^2$ , then  $b'a = b^4b'$ , on this case,  $G = \{a^2b^j | 1 \leq i \leq 7, 1 \leq j \leq 3, ba = a^4b, a^7 = b^3 = e\}$ .

7. For any  $a_1, a_2 \in H$  and any  $b_1, b_2 \in K$ , then  $(a_1 b_1) a_2 (a_1 b_1)^{-1} = a_1 b_1 a_2 b_1^{-1} a_1^{-1} = a_1 a_2 b_1 b_1^{-1} a_1^{-1} = a_1 a_2 a_1^{-1} \in H$  for  $ab = ba$ . Similarly,  $(a_1 b_1) b_2 (a_1 b_1)^{-1} \in K$ . Hence  $H \triangleleft G, K \triangleleft G$ . Define  $\varphi : H \times K \rightarrow G$ ,  $\varphi((a, b)) = ab$  for any  $(a, b) \in H \times K$ . It is obvious that  $\varphi((a_1, b_1)(a_2, b_2)) = a_1 a_2 b_1 b_2 = a_1 b_1 a_2 b_2 = \varphi((a_1, b_1))\varphi((a_2, b_2))$ . Therefore  $\varphi$  is a homomorphism from  $H \times K$  to  $G$ .

8. (a) Since  $E(x) = e$  for any  $x \in X$  and  $E \in G^X$ ,  $G^X \neq \emptyset$ . For any  $f, g, h \in G^X$ , then  $((fg)h)(x) = (f(x)g(x))h(x) = f(x)(g(x)h(x)) = (f(gh))(x)$ , thus  $(fg)h = f(gh)$ .  $(f \cdot E)(x) = f(x)e = f(x) = ef(x) = (E \cdot f)(x)$ , then  $f \cdot E = E \cdot f = f$ . Define  $h(x) = f(x)^{-1}$ , then  $(fh)(x) = f(x)h(x) = e = h(x)f(x) = (hf)(x)$ , then  $hf = fh = E$ . Therefore  $G^X$  is a group.

(b) Define  $\varphi_x : G^X \rightarrow G$ ,  $\varphi_x(f) = f(x)$ , then  $\varphi(fg) = (fg)(x) = f(x)g(x) = \varphi_x(f)\varphi_x(g)$ , thus  $\varphi$  is a group homomorphism. Suppose  $\pi_x(\{g_y\}_{y \in X}) = g_x$ , then there is unique group homomorphism  $\Phi : G^X \rightarrow \prod_{i \in X} G$  satisfies  $\pi_x \circ \Phi = \varphi_x$ . Let  $\Psi : \prod_{i \in X} G \rightarrow G^X$ ,  $\Psi(\{g_y\}_{y \in X})(x) = g_x$ , then

$$\psi(\{g_y\}_{y \in X}\{g'_y\}_{y \in X}) = g_x g'_x = \psi(\{g_y\}_{y \in X})\psi(\{g'_y\}_{y \in X}),$$

$\Psi$  is a group homomorphism. Since

$$\pi_x(\Phi\Psi)(\{g_y\}_{y \in X}) = \varphi_x(\Psi(\{g_y\}_{y \in X})) = \Psi(\{g_y\}_{y \in X})(x) = g_x$$

and  $\pi(id_{\prod_{i \in X} G}(\{g_y\}_{y \in X})) = g_x$  for any  $x \in X$ ,  $\Phi \circ \Psi = id_{\prod_{i \in X} G}$  (Proposition 1.6.2). If  $\Phi(f) = \{g_y\}_{y \in X}$ , then  $f(x) = \varphi_x(f) = \pi_x(\Phi(f)) = \pi_x(\{g_y\}_{y \in X}) = g_x$ , thus  $\Psi \circ \Phi(f)(x) = \Psi(\{g_y\}_{y \in X})(x) = g_x = f(x)$ , hence  $\Psi \circ \Phi(f) = f$ . Therefore  $\Psi \circ \Phi(f) = id_{G^X}$ . Whence  $G^X \cong \prod_{i \in X} G$ .

(c) If  $\theta : G \rightarrow G$ ,  $\theta(a) = 0$  for any  $a \in G$ , then  $\theta \in \text{End}(G)$  and  $\theta + f = f + \theta = f$  for any  $f \in \text{End}(G)$ . For any  $f \in \text{End}(G)$ ,  $(-f)(a) := -f(a)$ , then  $(-f)(a+b) = -(f(a)+f(b)) = (-f(a)) + (-f(b))$ , thus  $-f \in \text{End}(G)$ . For any  $f, g \in \text{End}(G)$ ,  $(f+g)(a+b) = f(a+b) + g(a+b) = f(a) + f(b) + g(a) + g(b) = (f+g)(a) + (f+g)(b)$  for any  $a, b \in G$ , then  $f+g \in \text{End}(G)$ , thus  $\text{End}(G) \leq G^X$ .

9. Since  $N \triangleleft G$ ,  $h^{-1}nh \in N$  for any  $n \in N$  and any  $h \in H$ . Define  $\varphi : H \rightarrow \text{Aut}(N)$ ,  $h \mapsto \varphi(h)(n \mapsto hnh^{-1})$ , then

$$\varphi(h)(n_1 n_2) = h(n_1 n_2)h^{-1} = hn_1 h^{-1} h n_2 h^{-1} = \varphi(h)(n_1)\varphi(h)(n_2),$$

$\varphi(h)\varphi(h^{-1}) = \varphi(h^{-1})\varphi(h) = id_N$ , thus  $\varphi(h) \in \text{Aut}(N)$ . While  $\varphi(h_1 h_2)(n) = h_1 h_2 n (h_1 h_2)^{-1} = \varphi(h_1)(h_2 n h_2^{-1}) = \varphi(h_1)\varphi(h_2)(n)$ , then  $\varphi(h_1 h_2) = \varphi(h_1)\varphi(h_2)$ , thus  $\varphi$  is a homomorphism. Define  $\Phi : G \rightarrow N \rtimes_{\varphi} H$ ,  $\Phi(nh) = (n, h)$ . If  $n_1 h_1 = n_2 h_2$ , then  $n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H$ , thus  $n_2^{-1} n_1 = h_2 h_1^{-1} = e$ , therefore  $n_1 = n_2, h_1 = h_2$ ,  $\Phi$  is well-defined. It is obvious that  $\Phi$  is surjective.

$$\begin{aligned} \Phi((n_1 h_1)(n_2 h_2)) &= \Phi(n_1 (h_1 n_2 h_1^{-1}) h_1 h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2) \\ &= (n_1, h_1)(n_2, h_2) = \Phi(n_1 h_1)\Phi(n_2 h_2) \end{aligned} \quad (1)$$

for any  $n_1 h_1, n_2 h_2 \in G$ . Since  $(e, e)$  is the identity of  $N \rtimes_{\varphi} H$ ,  $\Phi$  is monomorphic. Hence  $G \cong N \rtimes_{\varphi} H$ .

10. Suppose  $\mathbb{Z}_4 = \{e, a, a^2, a^3\}$ ,  $\mathbb{Z}_4 \rtimes_{\varphi} \mathbb{Z}_2 = \{(a^i, \bar{0}), (a^i, \bar{1}) | i = \pm 1\}$ , then  $(a^i, \bar{0})(a^j, \bar{1}) = (a^i \varphi(\bar{0})(a^j, \bar{0} + \bar{1}) = (a^{i+j}, \bar{1})$ ,  $(a^i, \bar{1})(a^j, \bar{0}) = (a^i \varphi(\bar{1})(a^j, \bar{1} + \bar{0}) = (a^{i-j}, \bar{1})$ ,  $(a^i, \bar{0})(a^j, \bar{0}) = (a^i \varphi(\bar{0})(a^j, \bar{0} + \bar{0}) = (a^{i+j}, \bar{0})$ ,  $(a^i, \bar{1})(a^j, \bar{1}) = (a^i \varphi(\bar{1})(a^j, \bar{1} + \bar{1}) = (a^{i-j}, \bar{0})$ ,  $(a^i, \bar{1})(a^i, \bar{1}) = (e, \bar{0})$ ,  $(a^i, \bar{0})(a^i, \bar{0}) = (a^{2i}, \bar{0})$ ,  $(e, \bar{1})(a, \bar{0})(e, \bar{1}) = (a^{-1}, \bar{0}) = (a^3, \bar{0})$ . Define  $\Phi : \mathbb{Z}_4 \rtimes_{\varphi} \mathbb{Z}_2 \rightarrow D_4$ ,  $\Phi((a^i, \bar{0})) = \sigma^i$ ,  $\Phi((e, \bar{1})) = \tau$ , then  $\sigma^4 = id$ ,  $\tau^2 = id$ ,  $\tau^{-1} \sigma \tau = \sigma^3$ , hence  $\mathbb{Z}_4 \rtimes_{\varphi} \mathbb{Z}_2 \cong D_4$ .

11. 11

12. (1) Define  $\psi : G \rightarrow Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ ,  $\psi(A) = f$  where  $f((a, b)) = (A(a, b)^T)^T$ . Since  $Ker \psi = E_2$ ,  $\psi$  is injective.  $(AB(a, b)^T)^T = fg(a, b)$ , then  $\psi(AB) = fg = \psi(A)\psi(B)$ , thus  $\psi$  is monomorphic. While  $|Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)| = 6 = |G|$ ,  $\psi$  is isomorphic. Hence  $G \cong Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ .
- (2)  $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\varphi} \mathbb{Z}_2 = \{(a, b, c) | a, b, c \in \mathbb{Z}_2\}$ , we have  $(a_1, b_1, \bar{0})(a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_2)$ ,  $(a_1, b_1, \bar{1})(a_2, b_2, c_2) = (a_1 + b_2, b_1 + a_2, \bar{1} + c_2)$ . Let  $x_1 = (\bar{0}, \bar{0}, \bar{0})$ ,  $x_2 = (\bar{1}, \bar{0}, \bar{0})$ ,  $x_3 = (\bar{0}, \bar{1}, \bar{0})$ ,  $x_4 = (\bar{0}, \bar{0}, \bar{1})$ ,  $x_5 = (\bar{1}, \bar{1}, \bar{0})$ ,  $x_6 = (\bar{1}, \bar{0}, \bar{1})$ ,  $x_7 = (\bar{0}, \bar{1}, \bar{1})$ ,  $x_8 = (\bar{1}, \bar{1}, \bar{1})$ . Then

	$x_1$	$x_2$	$x_3$	$x_4$	$x_5$	$x_6$	$x_7$	$x_8$
$x_1$	$x_1$	$x_2$	$x_3$	$x_4$	$x_5$	$x_6$	$x_7$	$x_8$
$x_2$	$x_2$	$x_1$	$x_5$	$x_6$	$x_3$	$x_4$	$x_8$	$x_7$
$x_3$	$x_3$	$x_5$	$x_1$	$x_7$	$x_2$	$x_8$	$x_4$	$x_6$
$x_4$	$x_4$	$x_7$	$x_6$	$x_1$	$x_8$	$x_3$	$x_2$	$x_5$
$x_5$	$x_5$	$x_3$	$x_2$	$x_8$	$x_1$	$x_7$	$x_6$	$x_4$
$x_6$	$x_6$	$x_8$	$x_4$	$x_2$	$x_7$	$x_5$	$x_1$	$x_3$
$x_7$	$x_7$	$x_4$	$x_8$	$x_3$	$x_6$	$x_1$	$x_5$	$x_2$
$x_8$	$x_8$	$x_6$	$x_7$	$x_5$	$x_4$	$x_2$	$x_3$	$x_1$

Let  $x_6 = a$ ,  $x_7 = a^3$ ,  $x_5 = a^2$ ,  $x_1 = e$ ,  $a^4 = e$ , then  $\langle a \rangle = \{x_1, x_6, x_5, x_7\}$ . Let  $x_2 = b$ , then  $b^2 = e$ ,  $x_3 = ba^2$ ,  $x_4 = ba$ ,  $x_8 = ba^3$ ,  $ba^2b = a^2$ ,  $bab = a^3$ . Hence  $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\varphi} \mathbb{Z}_2 \cong D_4^*$ .

13.  $H \xrightarrow{\varphi} Im \varphi = Im \psi \xrightarrow{\psi^{-1}} H$  and  $H \xrightarrow{\psi} Im \psi = Im \varphi \xrightarrow{\varphi^{-1}} H$  for  $Im \varphi = Im \psi \leq Aut(K)$ . Define  $f : K \rtimes_{\psi} H \rightarrow K \rtimes_{\varphi} H$ ,  $f((k, h)) = (k, \varphi^{-1} \psi(h))$ , then  $f((k_1, h_1)(k_2, h_2)) = f(k_1 \psi(h_1)(k_2), h_1 h_2) = (k_1 \psi(h_1)(k_2), \varphi^{-1} \psi(h_1 h_2))$ , while  $f((k_1, h_1))f((k_2, h_2)) = (k_1, \varphi^{-1} \psi(h_1))(k_2, \varphi^{-1} \psi(h_2)) = (k_1 \psi(h_1)(k_2), \varphi^{-1} \psi(h_1 h_2))$ , thus  $f$  is a homomorphism, and inverse map is  $f^{-1}(k, h) = (k, \psi^{-1} \varphi(h))$ . Hence  $K \rtimes_{\psi} H \cong K \rtimes_{\varphi} H$ .

14. Since  $a^2 = b^2 = e$ ,  $x = aba...aba$  or  $x = baba...bab$  or  $x = ab...ab$  or  $x = ba...ba$  for any  $x \in \langle a, b \rangle$ . While  $a(ab)a = ba = b^{-1}a^{-1} = (ab)^{-1} \in \langle ab \rangle$  and  $b(ab)b = ba = (ab)^{-1} \in \langle ab \rangle$ , thus  $\langle ab \rangle \triangleleft \langle a, b \rangle$ . Since  $x = \underbrace{ba...ba}_n = (ab)^{-n} \in \langle ab \rangle$  or  $x = \underbrace{ba...ba}_n b = (ab)^{-n+1}a \in \langle ab \rangle < a \rangle$ , then

$\langle a, b \rangle = \langle ab \rangle \langle a \rangle$ . Let  $x \in \langle ab \rangle \cap \langle a \rangle$ , while  $\langle a \rangle = \{e, a\}$ , if  $x \neq e$ , then  $a = (ab)^n$  or  $a = (ab)^{-n}$ . If  $a = (ab)^n = ab \dots ab$ , then  $\underbrace{ba \dots ba}_{n-1} b = e$ , thus  $\underbrace{abab \dots ab}_{n-2} a = e$ , repeat this process, then  $bab = e$  and  $aba = e$ , hence  $a = e, b = e$ . It is contradiction. Similarly,  $a = (ab)^{-n}$  induces contradiction, too. Hence  $\langle ab \rangle \cap \langle a \rangle = \{e\}$ ,  $G = \langle ab \rangle \rtimes \langle a \rangle$ .

15. Suppose  $|G| = p_1^{n_1} \dots p_s^{n_s}$ ,  $P_i (1 \leq i \leq s)$  is Sylow  $p_i$ -subgroup. Since  $G$  is abelian,  $P_i \triangleleft G$  and  $P_i \cap P_j = \{e\}$ ,  $G = P_1 \oplus \dots \oplus P_s$ . While  $P_i \cong \mathbb{Z}_{p_i^{n_i}}$ , then  $G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{n_s}}$ .
16. According to Fundamental Theorem of Abelian Group,  $G = \mathbb{Z}_{p_1^{l_{11}}} \oplus \dots \oplus \mathbb{Z}_{p_1^{l_{1s_1}}} \oplus \dots \oplus \mathbb{Z}_{p_n^{l_{ns_n}}}$  for  $G$  is a finite abelian group. Without loss of generality, let  $l_{i1} \leq l_{i2} \leq \dots \leq l_{is_i}$ . Suppose  $n_r = p_n^{l_{ns_n}} \dots p_1^{l_{1s_1}}$ ,  $n_{r-1} = p_n^{l_{ns_{n-1}}} \dots p_1^{l_{1s_{1-1}}}$ , and by this analogy, we get  $n_1, \dots, n_r$  and  $n_i \mid n_{i+1}$  for  $1 = 2, \dots, r-1$ . Since any  $p_i, p_j (i \neq j)$  are prime,  $\mathbb{Z}_{p_n^{l_{ns_n}}} \oplus \dots \oplus \mathbb{Z}_{p_1^{l_{1s_1}}} \cong \mathbb{Z}_{n_r}$ . Hence  $G \cong \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_r}$ .
17. (a) It is obvious that  $mG \neq \emptyset$ . For any  $ma, mb \in mG$ , then  $(-ma) + (mb) = m(b-a) \in mG$ , hence  $mG$  is a subgroup.
- (b) Define  $\varphi : G^n / (mG^n) \rightarrow (G/mG)^n$ ,  $(a_1, \dots, a_n) + mG^n \mapsto (a_1 + mG, \dots, a_n + mG)$ . If  $(a_1, \dots, a_n) + mG^n = (b_1, \dots, b_n) + mG^n$ , then  $(a_1 - b_1, \dots, a_n - b_n) \in mG^n$ , thus  $a_i - b_i \in mG$  for  $i = 1, \dots, n$ , hence  $\varphi$  is well-defined. If  $(a_1, \dots, a_n) + mG^n \in \text{Ker} \varphi$ , then  $(a_1 + mG, \dots, a_n + mG) = (0, \dots, 0)$ , thus  $a_i \in mG$  for  $i = 1, \dots, n$ . Hence  $(a_1, \dots, a_n) + mG^n = mG^n$ , i.e.  $\varphi$  is injective. It is obvious that  $\varphi$  is surjective.

$$\begin{aligned}
& \varphi((a_1, \dots, a_n) + mG^n + (b_1, \dots, b_n) + mG^n) \\
&= \varphi((a_1 + b_1, \dots, a_n + b_n) + mG^n) \\
&= (a_1 + b_1 + mG, \dots, a_n + b_n + mG) \\
&= (a_1 + mG, \dots, a_n + mG) + (b_1 + mG, \dots, b_n + mG) \\
&= \varphi((a_1, \dots, a_n) + mG^n) + \varphi((b_1, \dots, b_n) + mG^n).
\end{aligned} \tag{2}$$

Therefore  $\varphi$  is isomorphic, i.e.  $G^n / (mG^n) \cong (G/mG)^n$ .

18. If  $m < n$ , define  $\varphi : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ ,  $(a_1, \dots, a_n) \mapsto (a_1, \dots, a_m)$ , then  $\varphi$  is surjective and  $\varphi(ab) = \varphi(a)\varphi(b)$  for any  $a, b \in \mathbb{Z}^n$ , but  $\text{Ker} \varphi = \{(0, \dots, 0, a_{m+1}, \dots, a_n) \mid a_i \in \mathbb{Z}, i = m+1, \dots, n\} \neq \{0\}$ . Hence  $n \leq m$ . Similarly,  $\mathbb{Z}^m \not\cong \mathbb{Z}^n$  for  $n < m$ . Therefore  $m = n$ . Conversely, If  $m = n$ , it is obvious that  $\mathbb{Z}^m \cong \mathbb{Z}^n$ .
19. Define  $\bar{f} : \mathbb{Z}(X) \rightarrow A$ ,  $(a_x)_{x \in X} \mapsto \sum_{x \in X} a_x f(x)$ , then

$$\begin{aligned}
\bar{f}((a_x)_{x \in X} + (b_x)_{x \in X}) &= \bar{f}((a_x + b_x)_{x \in X}) = \sum_{x \in X} (a_x + b_x) f(x) \\
&= \sum_{x \in X} a_x f(x) + \sum_{x \in X} b_x f(x) = \bar{f}((a_x)_{x \in X}) + \bar{f}((b_x)_{x \in X})
\end{aligned} \tag{3}$$

Hence  $\bar{f}$  is a homomorphism.  $\bar{f}\lambda(x) = f(x)$  for any  $x \in X$ , then  $\bar{f}\lambda = f$ . If there is  $\psi : \mathbb{Z}(X) \rightarrow A$  such that  $\psi\lambda = f$ , then  $\psi((a_x)_{x \in X}) = \psi(\sum_{x \in X} a_x \lambda(x)) = \sum_{x \in X} a_x \psi\lambda(x) = \sum_{x \in X} a_x f(x) = \sum_{x \in X} a_x \bar{f}\lambda(x) = \bar{f}(\sum_{x \in X} a_x \lambda(x)) = \bar{f}((a_x)_{x \in X})$ , hence  $\psi = \bar{f}$ .

20. According to the Fundamental Theorem of Abelian Group,  $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{e_s}} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_r$ , then  $G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{e_s}} \oplus \mathbb{Z}^r$