1 Groups
1.6 Direct products and direct sum

1. We can easily get that $SO(n,\mathbb{R}) \lhd O(n,\mathbb{R})$ and $\{\pm E_n\} \lhd O(n,\mathbb{R})$. 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 $O(n,\mathbb{R}) \ncong SO(n,\mathbb{R}) \times \{\pm E_n\}$ 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 $G =< a >, H =< b >, |a| = n, |b| = m$. If $(m,n) = 1$, then $G \times H =< (a,b) >$. 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 $< (a,b) > \leq G \times H$, whence $|G \times H| = mn$. Hence $G \times H =< (a,b) >$. Conversely, $G \times H =< (a,b) >$, 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 $K \lhd S_4$, while $H \subseteq A_4$, hence $K \lhd A_4$. Since $[A_4 : K] = 3$, hence $A_4/K \cong \mathbb{Z}_3$. Let $B = \{x_1 := (12)(34), x_2 := (13)(24), X_3 := (14)(23)\}$, $S_4 \times B \to B$, $(\sigma, (ij)(kl)) \mapsto (\sigma(i)\sigma(j))(\sigma(k)\sigma(l))$, then B is a S_4-set. $K \subseteq Ker\varphi$ where $\varphi : S_4 \to Sym(B) = S_3$ is a group homomorphism induced by S_4-set. Since $(23)x_1 = x_2$, $(12) \in Im\varphi$, while $(14)x_2 = x_3$, $(23) \in Im\varphi$. Hence $Im\varphi \supseteq< (12), (23) >= S_3$, then φ is surjective. As $S_4/Ker\varphi \cong S_3$, $|Ker\varphi| = 4$, thus $K = Ker\varphi$. 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 $nkn^{-1}k^{-1} = (nkn^{-1})k \in K(\because K \lhd G)$, $n(kn^{-1}k^{-1}) \in N(\because N \lhd G)$ 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, $(1)G = S_3 \times S_3$, $N = \{(a,b) | a, b \in< (123) >\}$, then $N \cap S_3 =< (123) >$, $N \nsubseteq C(G) = \{((1),(1))\}$. $(2)G = GL(3,\mathbb{R}) \times GL(3,\mathbb{R})$, $N = \{(kE, lE) | kl = 1\}$, 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 $H_1 \lhd G$, 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 $H_1 =< a >, H_2 =< b >$ is a Sylow 3-subgroup. Since $H_1 \lhd G$, $bab^{-1} \in< a >$, hence there is $r \in \{2,3,4,5,6\}$ such that $bab^{-1} = a^r$, then $ba = a^r b$ and $G = \{a^i b^j | 1 \leq i \leq 7, 1 \leq i \leq 3\}$. As $(ba)^7 = a^{2r^2+3r+2} b \neq e$, $(ba)^3 = a^{r^2+r+1} = e$, thus $ord(ba) = 7$ or 3. If $ord(ba) = 21$, according to Exercise 1.6.3, G is cyclic, hence $r = 2$ or 4. If $ba = a^2 b$, then $b^2 a = a^4 b^2$, let $b' = b^2$, then $b'a = a^4 b'$, on this case, $G = \{a^i b^j | 1 \leq i \leq 7, 1 \leq j \leq 3, ba = a^4 b, a^7 = b^3 = e\}$.

Another way:Notation: $m \equiv r(mod 7)$ means that the remainders of dividing m and r by 7 are same.

Let $H_1 =< a >, H_2 =< b >$ is a Sylow 3-subgroup. Since $H_1 \lhd G$, $bab^{-1} \in < a >$, hence there is $r \in \{1, 2, 3, 4, 5, 6\}$ such that $bab^{-1} = a^r$.

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^r b^{-1} = (b^a b{-}1)^r = a^{r^2}$ and by induction, we can get $a = b^3ab^{-3} = a^{r^3}$. Thus, $r^3 \equiv 1(mod 7)$.

Then we find all values of r satisfing the condition by direct computing. Due to the fact that $mn \equiv rs(mod 7)$ if $m \equiv r(mod 7), n \equiv s(mod 7)$, we can first compute the remainder when $r = 1, 2, 3, 5$ and get the rest by multiplication of remainders. Hence, $r = 1, 2, 4$.

If $r = 1$, $G =< a, b >$ is an abelian group. $|ab| = 21$, so G is a cyclic group and $G \cong \mathbb{Z}_{21}$.

If $r = 2$, $G = \{a^i b^j | 1 \leq i \leq 7, 1 \leq j \leq 3, ba = a^4 b, a^7 = b^3 = e\}$ is a nonabelian group.

If $r = 4$, let $b' = b^2$, then $b'ab'^{-1} = a^{16} = a^2$ which is the same with $r = 2$. On this case, $G = \{a^i b^j | 1 \leq i \leq 7, 1 \leq j \leq 3, bab^{-1} = a^2, a^7 = b^3 = e\}$ which is isomorphic with the case that $r = 2$.

(Set $U_7 := \{m \in \mathbb{Z}_+ | (m, 7) = 1 \text{ and } m < 7\} = \{1, 2, 3, 4, 5, 6\}$. Define the multiplication $\cdot$ as $m \cdot n = s$, where $s \in U_7$ and $7 | mn - s$. It's obvious that the multiplication is a binary operation on U_7 and satisfies associativity. The identity is 1. For any element $m \in U_7$, there exists an element n in U_7 such that $mn + 7k = 1$ for the sake of $(m, 7) = 1$. Then n is the inverse of m. Hence, U_7 is a group with respect to the multiplication. $< r >$ is a cyclic subgroup of U_7 and its order is 3.)

7. For any $a_1, a_2 \in H$ and any $b_1, b_2 \in K$, then $(a_1b_1)a_2(a_1b_1)^{-1} = a_1b_1a_2b_1^{-1}a_1^{-1} = a_1a_2b_1b_1^{-1}a_1^{-1} = a_1a_2a_1^{-1} \in H$ for $ab = ba$. Similarly, $(a_1b_1)b_2(a_1b_1)^{-1} \in K$. Hence $H \lhd G, K \lhd G$. Define $\varphi : H \times K \to G$, $\varphi((a, b)) = ab$ for any $(a, b) \in H \times K$. It is obvious that $\varphi((a_1, b_1)(a_2, b_2) = a_1a_2b_1b_2 = a_1b_1a_2b_2 = \varphi((a_1, b_1))\varphi((a_2, b_2))$. Therefore φ 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 $\varphi_x : G^X \to G$, $\varphi_x(f) = f(x)$, then $\varphi(fg) = (fg)(x) = f(x)g(x) = \varphi_x(f)\varphi_x(g)$, thus φ is a group homomorphism. Suppose $\pi_x(\{g_y\}_{y \in X}) = g_x$, then there is unique group homomorphism $\Phi : G^X \to \prod_{i \in X} G$ satisfies $\pi_x \circ \Phi = \varphi_x$. Let $\Psi : \prod_{i \in X} G \to G^X$, $\Psi(\{g_y\}_{y \in X})(x) = g_x$, then

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

   Ψ 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 $\pi(id_{\prod_{x\in X} G}(\{g_y\}_{y\in X})) = g_x$ for any $x \in X$, $\Phi \circ \Psi = id_{\prod_{x\in X} G}$ (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 $\theta : G \to G$, $\theta(a) = 0$ for any $a \in G$, then $\theta \in End(G)$ and $\theta + f = f + \theta = f$ for any $f \in End(G)$. For any $f \in End(G)$, $(-f)(a) := -f(a)$, then $(-f)(a+b) = -(f(a) + f(b)) = (-f(a)) + (-f(b))$, thus $-f \in End(G)$. For any $f, g \in End(G)$, $(f+g)(a+b) = f(a+b) + g(a+b) = f(a) + f(b) + g(a) + g(b) = (f+g)(a) + (f+g)(b)$ for any $a, b \in G$, then $f + g \in End(G)$, thus $End(G) \leq G^X$.

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

$$\varphi(h)(n_1n_2) = h(n_1n_2)h^{-1} = hn_1h^{-1}hn_2h^{-1} = \varphi(h)(n_1)\varphi(h)(n_2),$$

$\varphi(h)\varphi(h^{-1}) = \varphi(h^{-1})\varphi(h) = id_N$, thus $\varphi(h) \in Aut(N)$. While $\varphi(h_1h_2)(n) = h_1h_2n(h_1h_2)^{-1} = \varphi(h_1)(h_2nh_2^{-1}) = \varphi(h_1)\varphi(h_2)(n)$, then $\varphi(h_1h_2) = \varphi(h_1)\varphi(h_2)$, thus φ is a homomorphism. Define $\Phi : G \to N \rtimes_\varphi H$, $\Phi(nh) = (n, h)$. If $n_1h_1 = n_2h_2$, then $n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H$, thus $n_2^{-1}n_1 = h_2h_1^{-1} = e$, therefore $n_1 = n_2, h_1 = h_2$, Φ is well-defined. It is obvious that Φ is surjective.

$$\begin{aligned}\Phi((n_1h_1)(n_2h_2)) &= \Phi(n_1(h_1n_2h_1^{-1})h_1h_2) = (n_1\varphi(h_1)(n_2), h_1h_2)\\ &= (n_1, h_1)(n_2, h_2) = \Phi(n_1h_1)\Phi(n_2h_2)\end{aligned} \tag{1}$$

for any $n_1h_1, n_2h_2 \in G$. Since (e, e) is the identity of $N \rtimes_\varphi H$, Φ is monomorphic. Hence $G \cong N \rtimes_\varphi H$.

10. Suppose $\mathbb{Z}_4 = \{e, a, a^2, a^3\}$, $\mathbb{Z}_4 \rtimes_\varphi \mathbb{Z}_2 = \{(a^i, \overline{0}), (a^i, \overline{1}) | i = \pm 1\}$, then $(a^i, \overline{0})(a^j, \overline{1}) = (a^i\varphi(\overline{0})(a^j), \overline{0} + \overline{1}) = (a^{i+j}, \overline{1})$, $(a^j, \overline{1})(a^i, \overline{0}) = (a^j\varphi(\overline{1})(a^i), \overline{1} + \overline{0}) = (a^{j-i}, \overline{1})$, $(a^i, \overline{0})(a^j, \overline{0}) = (a^i\varphi(\overline{0})(a^j), \overline{0} + \overline{0}) = (a^{i+j}, \overline{0})$, $(a^i, \overline{1})(a^j, \overline{1}) = (a^i\varphi(\overline{1})(a^j), \overline{1} + \overline{1}) = (a^{i-j}, \overline{0})$, $(a^i, \overline{1})(a^i, \overline{1}) = (e, \overline{0})$, $(a^i, \overline{0})(a^i, \overline{0}) = (a^{2i}, \overline{0})$, $(e, \overline{1})(a, \overline{0})(e, \overline{1}) = (a^{-1}, \overline{0}) = (a^3, \overline{0})$. Define $\Phi : \mathbb{Z}_4 \rtimes_\varphi \mathbb{Z}_2 \to D_4$, $\Phi((a^i, \overline{0})) = \sigma^i, \Phi((e, \overline{1})) = \tau$, 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 $\psi : G \to Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$, $\psi(A) = f$ where $f((a, b)) = (A(a, b)^T)^T$. Since $Ker\psi = E_2$, ψ is injective. $(AB(a, b)^T)^T = fg(a, b)$, then $\psi(AB) = fg = \psi(A)\psi(B)$, thus ψ is monomorphic. While $|Aut(\mathbb{Z}_{\not{\mathbf{r}}} \times \mathbb{Z}_{\not{\mathbf{r}}})| = 6 = |G|$, ψ is isomorphic. Hence $G \cong Aut(\mathbb{Z}_{\not{\mathbf{r}}} \times \mathbb{Z}_{\not{\mathbf{r}}})$.

(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 $(a_1, b_1, \overline{0})(a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_2)$, $(a_1, b_1, \overline{1})(a_2, b_2, c_2) = (a_1 + b_2, b_1 + a_2, \overline{1} + c_2)$. Let $x_1 = (\overline{0}, \overline{0}, \overline{0})$, $x_2 = (\overline{1}, \overline{0}, \overline{0})$, $x_3 = (\overline{0}, \overline{1}, \overline{0})$, $x_4 = (\overline{0}, \overline{0}, \overline{1})$, $x_5 = (\overline{1}, \overline{1}, \overline{0})$,

$x_6 = (\overline{1}, \overline{0}, \overline{1})$, $x_7 = (\overline{0}, \overline{1}, \overline{1})$, $x_8 = (\overline{1}, \overline{1}, \overline{1})$. 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 $(a) = \{x_1, x_6, x_5, x_7\}$. 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 $f : K \rtimes_\psi H \to K \rtimes_\varphi H$, $f((k,h)) = (k, \varphi^{-1}\psi(h))$, then $f((k_1,h_1)(k_2,h_2)) = f(k_1\psi(h_1)(k_2), h_1h_2) = (k_1\psi(h_1)(k_2), \varphi^{-1}\psi(h_1h_2))$, while $f((k_1,h_1))f((k_2,h_2)) = (k_1, \varphi^{-1}\psi(h_1))(k_2, \varphi^{-1}\psi(h_2)) = (k_1\psi(h_1)(k_2), \varphi^{-1}\psi(h_1h_2))$, 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 $x \in < a, b >$. While $a(ab)a = ba = b^{-1}a^{-1} = (ab)^{-1} \in < ab >$ and $b(ab)b = ba = (ab)^{-1} \in < ab >$, thus $< ab > \lhd < a, b >$. Since $x = \underbrace{ba...ba}_{n} = (ab)^{-n} \in < ab >$ or $x = \underbrace{ba...ba}_{n} b = (ab)^{-n+1}a \in < ab >< a >$, then $< a, b > = < ab >< a >$. Let $x \in < ab > \cap < a >$, while $< a > = \{e, a\}$, if $x \neq e$, then $a = (ab)^n$ or $a = (ab)^{-n}$. If $a = (ab)^n = ab...ab$, then $\underbrace{ba..ba}_{n-1} b = e$, thus $\underbrace{abab...ab}_{n-2} a = e$, 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 $< ab > \cap < a > = \{e\}$, $G = < ab > \rtimes < a >$.

15. Suppose $|G| = p_1^{n_1}...p_s^{n_s}$, $P_i(1 \leq i \leq s)$ is Sylow p_i-subgroup. Since G is abelian, $P_i \lhd G$ and $P_i \cap P_j = \{e\}$, $G = P_1 \oplus ... \oplus P_s$. While $P_i \cong \mathbb{Z}_{p_i^{n_i}}$, then $G \cong \mathbb{Z}_{p_1^{n_1}} \oplus ... \oplus \mathbb{Z}_{p_s^{n_s}}$.

16. According to Fundamental Theorem of Abelian Group, $G = \mathbb{Z}_{p_1^{l_{11}}} \oplus ... \oplus \mathbb{Z}_{p_1^{l_{1s_1}}} \oplus ... \oplus \mathbb{Z}_{p_n^{l_{ns_n}}}$ for G is a finite abelian group. Without loss of generality, let $l_{i1} \leq l_{i2} \leq ... \leq l_{is_i}$. Suppose $n_r = p_n^{l_{ns_n}}...p_1^{l_{1s_1}}$, $n_{r-1} = p_n^{l_{n,s_n-1}}...p_1^{l_{1,s_1-1}}$, and by this analogy, we get $n_1, ..n_r$ and $n_i \mid n_{i+1}$ for $1 = 2, ..., r-1$. Since any $p_i, p_j (i \neq j)$ are prime, $\mathbb{Z}_{p_n^{l_{ns_n}}} \oplus ... \oplus \mathbb{Z}_{p_1^{l_{1s_1}}} \cong \mathbb{Z}_{n_r}$. Hence $G \cong \mathbb{Z}_{n_1} \oplus ... \oplus \mathbb{Z}_{n_r}$.

17. (a) It is obvious that $mG \neq \emptyset$. For any $ma, ma \in mG$, then $(-ma) + (mb) = m(b-a) \in mG$, hence mG is a subgroup.

(b) Define $\varphi : G^n/(mG^n) \to (G/mG)^n$, $(a_1, ..., a_n) + mG^n \mapsto (a_1 + mG, ..., a_n + mG)$. If $(a_1, ..., a_n) + mG^n = (b_1, ..., b_n) + mG^n$, then $(a_1 - b_1, ..., a_n - b_n) \in mG^n$, thus $a_i - b_i \in mG$ for $i = 1, ..., n$, hence φ is well-defined. If $(a_1, ..., a_n) + mG^n \in Ker\varphi$, then $(a_1 + mG, ..., a_n + mG) = (0, ..., 0)$, thus $a_i \in mG$ for $i = 1, ..., n$. Hence $(a_1, ..., a_n) + mG^n = mG^n$, i.e. φ is injective. It is obvious that φ is surjective.

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

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

18. If $m < n$, define $\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$, $(a_1, ..., a_n) \mapsto (a_1, ..., a_m)$, then φ is surjective and $\varphi(ab) = \varphi(a)\varphi(b)$ for any $a, b \in \mathbb{Z}^n$, but $Ker\varphi = \{(0, ..., 0, a_{m+1}, ..., a_n) | a_i \in \mathbb{Z}, i = m+1, ..., n\} \neq \{0\}$. Hence $n \leq m$. Similarly, $\mathbb{Z}^m \ncong \mathbb{Z}^n$ for $n < m$. Therefore $m = n$. Conversely, If $m = n$, it is obvious that $\mathbb{Z}^m \cong \mathbb{Z}^n$.

19. Define $\overline{f} : \mathbb{Z}^(X) \to A$, $(a_x)_{x\in X} \mapsto \sum\limits_{x\in X} a_x f(x)$, then

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

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

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