

# 1 Groups

## 1.5 Homomorphisms and normal subgroup

1. Define

$$\begin{aligned}\varphi: S_n &\rightarrow GL(n, \mathbb{P}) \\ \sigma &\mapsto (e_\sigma(1), \dots, e_\sigma(n))\end{aligned}$$

According to Example 1.5.1  $\varphi$  is a homomorphism. If  $(e_\sigma(1), \dots, e_\sigma(n)) = (e_\tau(1), \dots, e_\tau(n))$ , then  $\sigma(i) = \tau(i), i = 1, \dots, n$ . So  $\sigma = \tau$ , hence  $\varphi$  is injective.

$\forall (e_{i_1}, \dots, e_{i_n}) \in W$ , if we let  $\sigma = \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix}$  then  $\varphi(\sigma) = (e_{i_1}, \dots, e_{i_n})$ .

Hence  $\varphi: S_n \rightarrow W$  is surjective, and hence an isomorphism.

2. Define

$$\begin{aligned}\varphi: H &\rightarrow a^{-1}Ha \\ h &\mapsto a^{-1}ha\end{aligned}$$

If  $\forall h_1, h_2 \in H$   $\varphi(h_1) = \varphi(h_2)$ , i.e.,  $a^{-1}h_1a = a^{-1}h_2a$ , then  $h_1 = h_2$ . So  $\varphi$  is injective.

$\forall a^{-1}ha \in a^{-1}Ha$  we have that  $\varphi(h) = a^{-1}ha$ . So  $\varphi$  is surjective. Hence  $\varphi$  is isomorphism.

3. If  $H$  is a normal, according to the definition,  $aHa^{-1} \subseteq H = a(a^{-1}Ha)a^{-1} \subseteq aHa^{-1}$ , hence  $H = aHa^{-1}$ . Since  $H = aHa^{-1}$ ,  $Ha = aHa^{-1}a = aH$ . Suppose  $Ha = aH$ , for any  $x \in H$ , then  $ax \in aH$ , thus there exists  $y \in H$  such that  $ax = ya$ , therefore  $axa^{-1} = yaa^{-1} = y \in H$ , that is  $H$  is normal.

4.  $S \neq \emptyset$  for  $e \in S$ . Let  $\langle S \rangle = \{x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} | x_i \in S, \epsilon_i = \pm 1, n \in \mathbb{Z}\}$ , for any  $x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} \in \langle S \rangle$  and any  $g \in G$ , then

$$gx_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} g^{-1} = (gx_1 g^{-1})^{\epsilon_1} (gx_2 g^{-1})^{\epsilon_2} \dots (gx_n g^{-1})^{\epsilon_n}.$$

Since  $gSg^{-1} \subseteq S$  for  $g \in G$ ,

$$gx_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} g^{-1} \in \langle S \rangle.$$

Hence  $\langle S \rangle \triangleleft G$ .

5.  $G = \{\pm 1, \pm i, \pm j, \pm k\}$ , then  $C(G) = \{\pm 1\}$  is normal. Hence  $\langle i \rangle = \{\pm 1, \pm i\}$ , while  $[G : \langle i \rangle] = 2$ , thus  $\langle i \rangle \triangleleft G$ . Similarly,  $\langle \pm i \rangle$  and  $\langle \pm j \rangle, \langle \pm k \rangle$  are normal. While the order of subgroup  $P$  of  $G$  perhaps is 1, 2, 4, 8. If  $|P| = 1$ , then  $P = \{1\}$  is normal. If  $|P| = 2$ , then  $P = \langle -1 \rangle$  is normal. While  $G$  has not other element whose order is 2, thus there is only one subgroup whose order is 2. While elements whose order is 4 are  $\pm i, \pm j, \pm k$ , therefore  $G$  has 3 subgroups whose order is 4.
6. For any  $a \in G$  and any  $b \in H$ ,  $aba^{-1} = baa^{-1} = b \in H$  for  $H \leq C(G)$ , hence  $H \triangleleft G$ . If  $G/H = \langle aH \rangle$ , then  $G = \{a^k h | h \in H, k \in \mathbb{Z}\}$ . For any  $a^{k_1} h_1, a^{k_2} h_2 \in G$ ,  $a^{k_1} h_1 \cdot a^{k_2} h_2 = a^{k_1+k_2} h_1 h_2 = a^{k_2} h_2 \cdot a^{k_1} h_1$ , therefore  $G$  is abelian.

7. Suppose there exists an isomorphism  $\varphi : (\mathbb{Z}, +) \rightarrow (\mathbb{Q}, +)$ , then  $\varphi^{-1} : (\mathbb{Q}, +) \rightarrow (\mathbb{Z}, +)$  is an isomorphism. Hence for any  $n \geq 1$ ,  $\mathbb{Z} = \varphi^{-1}(\mathbb{Q}) = \varphi^{-1}(n\mathbb{Q}) = n\varphi^{-1}(\mathbb{Q}) = n\mathbb{Z}$ , it is impossible, therefore any bijection between  $\mathbb{Z}$  and  $\mathbb{Q}$  is not an isomorphism between the group  $(\mathbb{Z}, +)$  and the group  $(\mathbb{Q}, +)$ .
8. Let  $A = \{x_1, x_2, \dots, x_{n-1}\}$ , construct

$$\begin{array}{ccc} A & \xrightarrow{\lambda} & F(A) \\ & \searrow f_1 & \swarrow \varphi_1 \\ & B_n & \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{\lambda} & F(A) \\ & \searrow f_2 & \swarrow \varphi_2 \\ & S_n & \end{array}$$

where  $f_1(x_i) = \sigma_i, f_2(x_i) = (i, i+1), \lambda(x_i) = x_i$ , then according to Theorem 1.5.2, there exists a unique group homomorphism  $\varphi_i$  such that  $\varphi_i \circ \lambda = f_i$ . Considering

$$\begin{array}{ccc} F(A) & \xrightarrow{\varphi_1} & B_n \\ & \searrow \varphi_2 & \\ & S_n & \end{array}$$

since  $\text{Ker}\varphi_1$  is a normal group generated by

$$\{x_i x_{i+1} x_i x_{i+1}^{-1} x_i^{-1} x_{i+1}^{-1} | i = 1, \dots, n-1\},$$

while  $\text{Ker}\varphi_2$  is a normal group generated by

$$\{x_i x_{i+1} x_i x_{i+1}^{-1} x_i^{-1} x_{i+1}^{-1}, x_i^2 | i = 1, \dots, n-1\}.$$

Then  $\text{Ker}\varphi_2 \supseteq \text{Ker}\varphi_1$ , and  $\varphi_i$  induce isomorphism  $\overline{\varphi}_1 : F(A)/\text{Ker}\varphi_1 \rightarrow B_n$  and isomorphism  $\overline{\varphi}_2 : F(A)/\text{Ker}\varphi_2 \rightarrow S_n$  respectively. Define  $\psi : F(A)/\text{Ker}\varphi_1 \rightarrow F(A)/\text{Ker}\varphi_2$ ,  $\psi(a\text{Ker}\varphi_1) = a\text{Ker}\varphi_2$ , then  $\psi$  is a group isomorphism. Hence  $\overline{\varphi}_2 \circ \psi \circ \overline{\varphi}_1^{-1} : B_n \rightarrow S_n$  is a group homomorphism. Since  $\psi$  is surjective,  $\overline{\varphi}_2 \circ \psi \circ \overline{\varphi}_1^{-1}$  is epimorphism.

9.  $N \subseteq H \Leftrightarrow NH = H$  or  $N \cap H = N$ . Since  $N$  is a normal subgroup,  $NH/N = H/N \cap H$ , then  $[G : H] = [G : NH][NH : H] = [G : NH][N : H \cap H]$ . Since  $(|N|, [G : H]) = 1$  and  $[N : H \cap N][G : H]$ ,  $([N : H \cap N], |N|) = 1$ , but  $[N : H \cap N][|N|]$ ,  $[N : H \cap N] = 1$ , i.e.  $N \subseteq H$ .  $N \triangleleft H$  for  $N \triangleleft G$ .
10. (a)  $G_1 = G_2 = (\mathbb{Z}, +), H_1 = 2\mathbb{Z}, H_2 = 3\mathbb{Z}, H_1 \cong H_2$ , but  $G_1/H_1 \not\cong G_2/H_2$ .
- (b)  $G_1 = G_2 = (\mathbb{Z}[x], +), H_1 = (\mathbb{Z}, +), H_2 = (\mathbb{Z} + x\mathbb{Z}, +), G_1/H_1 \cong G_2/H_2$ , but  $H_1 \not\cong H_2$ .

- (c)  $G_1 = \mathbb{Z}_6, G_2 = S_3, H_1 = 2\mathbb{Z}_6, H_2 = \langle (123) \rangle, H_1 \cong H_2$  and  $G_1/H_1 \cong G_2/H_2 \cong \mathbb{Z}_2$ , but  $G_1 \not\cong G_2$ .
11. For any  $f(n) \in f(N)$  and any  $a \in G$ , there exists  $a_1 \in G$  such that  $f(a_1) = a$  for  $f$  is an isomorphism. Then  $af(n)a^{-1} = f(a_1)f(n)f(a_1)^{-1} = f(a_1na_1^{-1}) \in f(N)$ , moreover,  $f(n)^{-1} = f(n^{-1}) \in f(N)$ ,  $f(N)$  is closed under multiplication, and  $e = f(e) \in f(N)$ , so  $f(N) \triangleleft G$ . Define  $\varphi : G/N \rightarrow G/f(N)$ ,  $aN \rightarrow f(a)f(N)$ . If  $aN = bN$ , then  $a^{-1}b \in N$ , hence  $f(a^{-1}b) = f(a)^{-1}f(b) \in f(N)$ , thus  $\varphi$  is well-defined. If  $aN \in \text{Ker}\varphi$ , i.e.  $f(a)f(N) = f(N)$ , then  $f(a) \in f(N)$ , thus  $f(a) = f(n)$  for some  $n \in N$ . Since  $f$  is injective,  $a = n \in N$ , then  $aN = N$ , hence  $\varphi$  is injective. Since  $f$  is an isomorphism,  $\varphi$  is surjective. Therefore  $G/N \cong G/f(N)$ .
12. (1) For any  $x, y \in G$ ,  $I_a(xy) = a(xy)a^{-1} = axa^{-1} \cdot aya^{-1} = I_a(x)I_a(y)$ .  $I_{a^{-1}}I_a(xy) = a^{-1}(axya^{-1})a = xy$ , hence  $I_{a^{-1}}I_a = \text{id}_G$ . Similarly,  $I_aI_{a^{-1}} = \text{id}_G$ . Therefore  $I_a$  is an automorphism.
- (2)  $(I_a)^{-1} = I_{a^{-1}}$ ,  $\text{id}_G = I_e$  and  $I_a \circ I_b = I_{ab}$ , hence  $\text{Inn}(G)$  is a subgroup of  $\text{Aut}(G)$ . For any  $\varphi \in \text{Aut}(G)$ ,  $\varphi \circ I_a \circ \varphi^{-1}(x) = \varphi(a\varphi^{-1}(x)a^{-1}) = \varphi(a)x\varphi(a)^{-1} = I_{\varphi(a)}(x)$  for any  $x \in G$ . Therefore  $\text{varphi} \circ I_a \circ \varphi^{-1} = I_{\varphi(a)} \in \text{Inn}(G)$ , then  $\text{Inn}(G) \triangleleft \text{Aut}(G)$ .
- (3) If  $\varphi$  is a nonidentity automorphism of  $G$ , since  $G$  is an abelian group,  $\text{Inn}(G) = \{\text{id}_G\}$ , hence  $\varphi$  is not an automorphism. Therefore  $\varphi$  is an outer automorphism.
- (4) It is obvious that  $\varphi$  is an automorphism of  $GL(n, \mathbb{P})$ . If  $\varphi = I_A$  for  $A \in GL(n, \mathbb{P})$ , then  $\varphi(B = (B^{-1})^T = ABA^{-1})$  for any  $B \in GL(n, \mathbb{P})$ .
- Take  $B = \begin{pmatrix} 1 & & & \\ & 2 & & \\ & & \ddots & \\ & & & n \end{pmatrix}$ , then  $\varphi(B) = \begin{pmatrix} 1 & & & \\ & \frac{1}{2} & & \\ & & \ddots & \\ & & & \frac{1}{n} \end{pmatrix}$  has eigenvalues:  $1, \frac{1}{2}, \dots, \frac{1}{n}$ . While eigenvalues of  $ABA^{-1}$  are  $1, 2, \dots, n$ , hence  $(B^{-1})^T \neq ABA^{-1}$ . It is contradiction, thus  $\varphi \neq I_A$  for any  $A$ . Therefore  $\varphi$  is an outer automorphism.
13. If  $\varphi : G \rightarrow G$ ,  $a \rightarrow a^{-1}$ , is an automorphism, then  $ab = \varphi((ab)^{-1}) = \varphi(b^{-1}a^{-1}) = \varphi(b^{-1})\varphi(a^{-1}) = ba$  for any  $a, b \in G$ , hence  $G$  is abelian. On the contrary, if  $G$  is abelian, then  $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b)$  for any  $a, b \in G$ , hence  $\varphi$  is an endomorphism. At the same time,  $\varphi$  is bijective, therefore  $\varphi$  is an automorphism. If  $G$  is abelian, then  $\psi(ab) = (ab)^k = a^kb^k = \psi(a)\psi(b)$  for any  $a, b \in G$ , hence  $\psi$  is an endomorphism.
14. Suppose  $\lambda : \{x, y, z\} \rightarrow G$ ,  $\xi(x) = a^2, \xi(y) = b^2, \xi(z) = ab$ , according to Theorem 1.5.2, there exists a unique group homomorphism  $\varphi : G \rightarrow F(\{a, b\})$ ,  $\text{Im}(\varphi) = \langle x, y, z \rangle$ . While  $\varphi(x^{k_1}y^{k_2}) = a^{2k_1}b^{2k_2}$ ,  $\varphi(x^{k_1}z^{k_2}) = a^{2k_1+1}(ba)^{k_2-1}b$ ,  $\varphi(y^{k_1}z^{k_2}) = b^{2k_1-1}(ba)^{k_2}b$ ,  $\varphi(y^{k_1}x^{k_2}) = b^{2k_1}(a)^{2k_2}$ ,  $\varphi(z^{k_1}x^{k_2}) =$

$(ab)^{k_1}(a)^{2k_2} = a(ba)^{k_1}a^{2k_2-1}$ ,  $\varphi(z^{k_1}y^{k_2}) = (ab)^{k_1}(b)^{2k_2} = a(ba)^{k_1-1}b^{2k_2+1}$ , hence reduced words in  $G$  through the action of  $\varphi$  are still reduced. Thus  $\varphi$  is injective, therefore  $\varphi$  is an isomorphism between  $G$  and  $\langle x, y, z \rangle$ .

15. (1) For any  $\varphi \in \text{Aut}(\mathbb{Z}^n)$ , let  $e_i = (0, \dots, 1, \dots, 0)^T$  where all rows are 0 except the  $i_{th}$ , then  $\varphi(e_i) = ((a_{1i}, \dots, a_{ni})^T) = \sum_{k=1}^n a_{ik}e_k$ . Suppose  $\varphi^{-1}(e_i) = (b_{1i}, \dots, b_{ni})^T = \sum_{k=1}^n b_{ki}e_k$ , then  $e_i = \varphi\varphi^{-1}(e_i) = \sum_{k=1}^n b_{ki}\varphi(e_k) = \sum_{k=1}^n \sum_{s=1}^n b_{ki}a_{sk}e_s$ , hence  $\sum_{k=1}^n a_{sk}b_{ki} = \delta_{is}$ , therefore  $(\varphi(e_1), \varphi(e_2), \dots, \varphi(e_n)) \in GL(n, \mathbb{Z})$  and it's inverse matrix is  $(\varphi^{-1}(e_1), \dots, \varphi^{-1}(e_n))$ . Define  $\Phi : \text{Aut}(\mathbb{Z}^n) \rightarrow GL(n, \mathbb{Z})$  such that  $\varphi \rightarrow (\varphi(e_1), \dots, \varphi(e_n))$ . If  $\Phi(\varphi) = \Phi(\psi)$ , then for any  $(a_1, \dots, a_n)^T \in \mathbb{Z}^n$ ,

$$\varphi((a_1, \dots, a_n)^T) = \sum_{k=1}^n a_k \varphi(e_k) = \sum_{k=1}^n a_k \psi(e_k) = \psi((a_1, \dots, a_n)^T),$$

hence  $\Phi$  is injective. For any  $(\alpha_1, \dots, \alpha_n) \in GL(n, \mathbb{Z})$ , then  $\varphi((a_1, \dots, a_n)^T) = \sum_{k=1}^n a_k \alpha_k \in \text{Aut}(\mathbb{Z}^n)$ ,  $\varphi^{-1}((a_1, \dots, a_n)^T) = \sum_{k=1}^n a_k \beta_k$  where  $(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n)^{-1}$ . Since  $\Phi(\varphi) = (\alpha_1, \dots, \alpha_n)$ , hence  $\Phi$  is bijective. We can easily testified that  $\Phi(\varphi \circ \psi) = \Phi(\varphi)\Phi(\psi)$ . Therefore  $\text{Aut}(\mathbb{Z}^n) \cong GL(n, \mathbb{Z})$ .

- (2) Suppose  $A = \{x_1, x_2, \dots, x_n\}$ ,  $\lambda : A \rightarrow F(A)$  which is free group of  $A$ . Define  $\varphi : A \rightarrow \mathbb{Z}_n$ ,  $\varphi(x_i) = e_i$ , then there exists a unique group homomorphism  $\psi : F(A) \rightarrow \mathbb{Z}_n$  such that  $\psi(x_i) = e_i$ . It is obvious that  $\psi$  is epimorphism. Let  $N = \langle \{x_i x_j x_i^{-1} x_j^{-1} \mid 1 \leq i, j \leq n\} \rangle$  is a normal subgroup, then  $N \subseteq \text{Ker}\psi$ . For any  $x_{i_1}^{k_1}, \dots, x_{i_m}^{k_m} \in \text{Ker}\psi$ , then

$$x_{i_1}^{k_1} \dots x_{i_m}^{k_m} = x_{i_1}^{k_1-1} x_{i_1} x_{i_2} x_{i_1}^{-1} x_{i_2}^{-1} x_{i_1}^{1-k_1} x_{i_1}^{k_1-1} x_{i_2} x_{i_1} x_{i_2}^{-1} x_{i_2}^{k_2} \dots x_{i_m}^{k_m}.$$

$x_{i_1}^{k_1} \dots x_{i_m}^{k_m} \in N$  iff  $x_{i_1}^{k_1-1} x_{i_2} x_{i_1} x_{i_2}^{k_2-1} \dots x_{i_m}^{k_m} \in N$ . While

$$x_{i_1}^{k_1-1} x_{i_2} x_{i_1} x_{i_2}^{k_2-1} \dots x_{i_m}^{k_m} = x_{i_1}^{k_1-2} x_{i_1} x_{i_2} x_{i_1}^{-1} x_{i_2}^{-1} x_{i_1}^{2-k_1} x_{i_1}^{k_1-2} x_{i_2} x_{i_1}^2 x_{i_2}^{k_2-1} \dots x_{i_m}^{k_m},$$

so  $x_{i_1}^{k_1-2} x_{i_2} x_{i_1}^2 x_{i_2}^{k_2-1} \dots x_{i_m}^{k_m} \in N$ . Hence iff  $x_{i_2} x_{i_1}^{k_1} x_{i_2}^{k_2-1} \dots x_{i_m}^{k_m} \in N$ , and then iff  $x_{i_2}^{k_2} x_{i_1}^{k_1} x_{i_3}^{k_3} \dots x_{i_m}^{k_m} \in N$ . Since  $\varphi(x_{i_1}^{k_1} \dots x_{i_m}^{k_m}) = k_1 e_{i_1} + \dots + k_m e_{i_m} = 0$ , that is the sum of occurrence number about  $e_{i_1}$  is 0. Through above process, we get that  $x_{i_1}$  is not occur in  $x_{i_2}^{k_2} \dots x_{i_m}^{k_m}$ , therefore  $x_{i_1}^{k_1} \dots x_{i_m}^{k_m} \in N$ . Thus  $\text{Ker}\psi = N$ . According to the Fundamental Theorem of Homomorphism, then  $F[\{x_1, \dots, x_n\}] / \langle x_i x_j x_i^{-1} x_j^{-1} \rangle \cong \mathbb{Z}^n$ .

16.  $HN_G(P)/H \cong N_G(P)/H \cap N_G(P) = N_G(P)/N_H(P)$ . For any  $g \in G$ ,  $gPg^{-1} \subseteq gHg^{-1} \subseteq H$ , then there exists  $a \in H$  such that  $gPg^{-1} = a^{-1}Pa$ , hence  $agPg^{-1}a^{-1}$ , thus  $ag \in N_G(P)$ , therefore  $g = a^{-1}(ag) \in HN_G(P)$ .

17. Suppose  $X$  is a  $G$ -set. Define  $\varphi : G \rightarrow \text{Sym}(X)$ ,  $\varphi(a) = L_a$ , the left translation. Since  $L_a \circ L_{a^{-1}} = \text{id}_X = L_{a^{-1}} L_a$  for any  $L_a \in \text{Sym}(X)$ ,  $\varphi(ab) = L_{ab}$ . For any  $x \in X$ , we have  $L_{ab}(x) = a(bx) = L_a(bx) = L_a \circ L_b(x)$ . Thus  $L_{ab} = L_a \circ L_b$  and  $\varphi(ab) = \varphi(a)\varphi(b)$ . On the contrary, suppose  $\varphi : G \rightarrow \text{Sym}(X)$ . For any  $g \in G$  and  $x \in X$ , define  $G \cdot x := \varphi(g)(x)$ . Then  $e \cdot x = \varphi(e)(x) = \text{id}_x(x) = x$ . For any  $f, g \in G$  and any  $x \in X$ ,  $(fg) \cdot x = \varphi(fg)(x) = (\varphi(f) \cdot \varphi(g))(x) = \varphi(f)(\varphi(g)(x)) = f \cdot (g \cdot x)$ . Hence  $X$  is a  $G$ -set.
18. Define  $G \times G/H \rightarrow G/H$ ,  $(g, aH) \mapsto ga \cdot H$ . Then there is a homomorphism  $\varphi : G \rightarrow \text{Sym}(G/H)$ . If  $\varphi(g) = \text{id}$ , then  $gH = H$  and  $g \in H$ . Hence  $\text{Ker}\varphi \subseteq H$ ,  $\text{Ker}\varphi \triangleleft G$ . Since  $[G : \text{Ker}\varphi] = [G : H][H : \text{Ker}\varphi]$ ,  $[H : \text{Ker}\varphi] \mid [G : \text{Ker}\varphi]$ . On the other hand,  $G/\text{Ker}\varphi \cong \text{Im}\varphi \leq \text{Sym}(G/H)$ , then  $|\text{Im}\varphi| \mid p!$ , hence  $[G : \text{Ker}\varphi] \mid p!$ . If a prime  $q$  satisfies  $q \mid [G : \text{Ker}\varphi]$ , then  $q \leq p$ . By the assumption on  $p$ , we have  $q = p$ . Hence  $[G : \text{Ker}\varphi] = p$  and  $\text{Ker}\varphi = H \triangleleft G$ .
19. Without loss of generality, we could Suppose  $H = \langle a_1, \dots, a_s \rangle$ ,  $K/H = \langle b_1H, \dots, b_nH \rangle$ , then  $K = \{b_{i_1}^{s_1} a_{i_1} \dots b_{i_n}^{s_n} a_{i_n} \mid b_{i_j} \in \{b_1, \dots, b_n\}, a_{i_j} \in H, s_i \in \mathbb{Z}\}$ , thus  $K = \langle b_i a_j \mid 1 \leq j \leq s, 1 \leq i \leq n \rangle$ , hence  $K$  is finitely generated.
20. Since  $N \triangleleft G$ ,  $NP = PN \leq G$ ,  $PN/N \leq G/N$ ,  $[G/N : PN/N] = [G : PN]$ . Since  $[G : P] = [G : PN][PN : P]$ ,  $p \nmid [G : PN] = [G/N : PN/N]$ . As  $NP/N \cong P/N \cap P$ ,  $|NP/N| = p^n$  for some  $n$ . Therefore  $NP/N$  is a Sylow  $p$ -subgroup of  $G/N$ .
21. Define  $\varphi : \langle k \rangle / \langle km \rangle \rightarrow \mathbb{Z}_m$ ,  $\varphi(kl + \langle km \rangle) = \bar{l}$ . For any  $kl_1 + \langle km \rangle, kl_2 + \langle km \rangle \in \langle k \rangle / \langle km \rangle$ , then  $\varphi(kl_1 + \langle km \rangle + kl_2 + \langle km \rangle) = \bar{l}_1 + \bar{l}_2 = \overline{l_1 l_2} = \varphi(kl_1 + \langle km \rangle) + \varphi(kl_2 + \langle km \rangle)$ . If  $kl + \langle km \rangle \in \text{Ker}\varphi$ , i.e.  $\varphi(kl + \langle km \rangle) = \bar{0}$ , thus  $l = mn$ , ( $n \in \mathbb{Z}$ ), hence  $kl + \langle km \rangle = \langle km \rangle$ , therefore  $\varphi$  is injective. If  $\bar{l} \in \mathbb{Z}_m$ , then there is  $kl + \langle km \rangle \in \langle k \rangle / \langle km \rangle$  such that  $\varphi(kl + \langle km \rangle) = \bar{l}$ , hence  $\varphi$  is surjective. Therefore  $\langle k \rangle / \langle km \rangle \cong \mathbb{Z}_m$ .
22. If  $a + \text{tor}(H) \in \text{tor}(H/\text{tor}(H))$ , then there is  $n_1 > 0$  such that  $n_1(a + \text{tor}(H)) = n_1a + \text{tor}(H) = 0 + \text{tor}(H)$ , thus  $n_1a \in \text{tor}(H)$ , hence there exists  $n_2 > 0$  such that  $n_2(n_1a) = 0$ , i.e.  $(n_2n_1)a = 0$ , therefore  $a \in \text{tor}(H)$ . Whence  $a + \text{tor}(H) = 0 + \text{tor}(H)$ , hence  $H/\text{tor}(H)$  is torsionfree.
23. Let  $P := \begin{pmatrix} \frac{1}{\sqrt{2}}E_n & \frac{1}{\sqrt{2}}E_n \\ -\frac{1}{\sqrt{2}}E_n & \frac{1}{\sqrt{2}}E_n \end{pmatrix}$ ,  $J := \begin{pmatrix} 0 & E_n \\ E_n & 0 \end{pmatrix}$ ,  $Q := \begin{pmatrix} \frac{1}{\sqrt{2}}E_n & -\frac{1}{\sqrt{2}}E_n \\ \frac{1}{\sqrt{2}}E_n & \frac{1}{\sqrt{2}}E_n \end{pmatrix}$ ,  $S := \begin{pmatrix} E_n & 0 \\ 0 & -E_n \end{pmatrix}$ . Then  $PQ = E_{2n}$ . Define  $\varphi : O(n+n, \mathbb{R}) \rightarrow G$ ,  $\varphi(A) = QAP$ , then  $(QAP)^T J (QAP) = QSP = J$ , thus  $\varphi$  is well-defined. Since  $Q, P \in GL(2n, \mathbb{R})$ ,  $\varphi$  is surjective. For any  $A, B \in O(n+n, \mathbb{R})$ , then  $\varphi(AB) = QABP = (QAP)(QBP) = \varphi(A)\varphi(B)$ , hence  $\varphi$  is isomorphic.

24. Let  $\iota : S \rightarrow F(S)$  which is free group of  $S$ . Then

$$\begin{array}{ccccc}
 S & \xrightarrow{\iota} & F(S) & & \\
 \downarrow \iota & \searrow \lambda & \downarrow \varphi(Th1.5.2) & & \\
 G & \xleftarrow{\exists \lambda} & & & \\
 & \swarrow \varphi & F(S) & \xleftarrow{\psi} & G
 \end{array}$$

$\psi \circ \varphi : F(S) \rightarrow F(S)$  and  $id_{F(S)} : F(S) \rightarrow F(S)$  satisfy  $\psi \circ \varphi \circ \iota = id_{F(S)} \circ \iota$ , hence  $\psi \circ \varphi = id_{F(S)}$ . Similarly,  $\varphi \circ \psi = id_G$ . Therefore  $F(S) \cong G$ .