

# Chapter 1

# Groups

## 1.1 Semigroups, monoids and groups

**Exercise 1.1.1.** Give examples other than those in the text of semigroups and monoids that are not groups.

**Answer.** Semigroup:  $(\mathbf{Z}_+, +)$

Monoid:  $(\mathbf{Z}_+, \times)$

**Exercise 1.1.2.** Let  $G$  be a group (written additively),  $S$  a nonempty set, and  $M(S, G)$  the set of all functions  $f : S \rightarrow G$ . Define addition in  $M(S, G)$  as follows:  $(f + g) : S \rightarrow G$  is given by  $s \mapsto f(s) + g(s) \in G$ . Prove that  $M(S, G)$  is a group, which is abelian if  $G$  is.

**Answer.** Firstly we check  $M(S, G)$  is a group

1.  $f + g : s \mapsto f(s) + g(s) \in G$ , so  $f + g \in M(S, G)$
2.  $(f + g) + h : s \mapsto (f(s) + g(s)) + h(s)$ ,  $G$  is a group, so  $s \mapsto (f(s) + g(s)) + h(s) \Leftrightarrow s \mapsto f(s) + (g(s) + h(s))$ ,  $(f + g) + h = f + (g + h)$ .
3. Take the unit element as  $e' : s \mapsto e$ .  $f + e' : s \mapsto f(s) + e'(s) = f(s) + e = f(s)$ , so  $f + e' = f$ . Similarly,  $e' + f = f$ .
4. For any  $f \in M(S, G)$ , take  $f^{-1} : s \mapsto (f(s))^{-1}$ , whence  $f(s) + (f(s))^{-1} = (f(s))^{-1} + f(s) = e$ .

In conclusion,  $M(S, G)$  is a group. If  $G$  is abelian  $f + g : s \mapsto f(s) + g(s) = g(s) + f(s)$ ,  $f + g = g + f$ , so  $M(S, G)$  is abelian.

**Exercise 1.1.3.** Is it true that a semigroup which has a left identity element and in which every element has a right inverse (see Proposition 1.3) is a group?

**Answer.** If  $e$  is the left identity,  $\forall a \in A, ea = a$  and  $\forall a \in A, \exists a^{-1} s.t. aa^{-1} = e$ . We have proved that if  $cc = c$ , then  $c = e$ .

$$(a^{-1}a)(a^{-1}a) = a^{-1}(aa^{-1})a = a^{-1}(ea) = a^{-1}a \Rightarrow a^{-1}a = e$$

$a^{-1}$  is also the left inverse.  $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$ ,  $e$  is also the right identity.

**Exercise 1.1.4.** Write out a multiplication table for the group  $D_4^*$ .

**Answer.**  $D_4^* = \{R, R^2, R^3, I, T_x, T_y, T_{13}, T_{24}\}$

	$I$	$R$	$R^2$	$R^3$	$T_x$	$T_y$	$T_{13}$	$T_{24}$
$I$	$I$	$R$	$R^2$	$R^3$	$T_x$	$T_y$	$T_{13}$	$T_{24}$
$R$	$R$	$R^2$	$R^3$	$I$	$T_{13}$	$T_{24}$	$T_y$	$T_x$
$R^2$	$R^2$	$R^3$	$I$	$R$	$T_y$	$T_x$	$T_{24}$	$T_{13}$
$R^3$	$R^3$	$I$	$R$	$R^2$	$T_{24}$	$T_{13}$	$T_x$	$T_y$
$T_x$	$T_x$	$T_{24}$	$T_y$	$T_{13}$	$I$	$R^2$	$R^3$	$R$
$T_y$	$T_y$	$T_{13}$	$T_x$	$T_{24}$	$R^2$	$I$	$R$	$R^3$
$T_{13}$	$T_{13}$	$T_y$	$T_{24}$	$T_x$	$R^3$	$R$	$I$	$R^2$
$T_{24}$	$T_{24}$	$T_x$	$T_{13}$	$T_y$	$R$	$R^3$	$R^2$	$I$

**Exercise 1.1.5.** Prove that the symmetric group on  $n$  letters,  $S_n$ , has order  $n!$ .

**Answer.** For a set  $A$  whose order is  $n$ , we prove there's  $n!$  different bijections by induction

1. For  $n = 1$ , trivial.
2. Assume  $n = k$ , there's  $k!$  bijections. For  $n = k + 1$ , fix one element in  $A$ , and take  $a \mapsto a$ , there's  $k$  free elements, so there's  $k! \cdot (k + 1)$  bijections in total.

By induction, we get the result.

**Exercise 1.1.6.** Write out an addition table for  $Z_2 \oplus Z_2$ .  $Z_2 \oplus Z_2$  is called the Klein four group.

**Answer.**  $Z_2 = \{1, 0\}$ ,  $Z_2 \oplus Z_2 = \{(1, 1), (1, 0), (0, 1), (0, 0)\}$

	$(1, 1)$	$(1, 0)$	$(0, 1)$	$(0, 0)$
$(1, 1)$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(1, 0)$	$(0, 1)$	$(0, 0)$	$(1, 1)$	$(1, 0)$
$(0, 1)$	$(1, 0)$	$(1, 1)$	$(0, 0)$	$(0, 1)$
$(0, 0)$	$(1, 1)$	$(1, 0)$	$(0, 1)$	$(0, 0)$

**Exercise 1.1.7.** If  $p$  is prime, then the nonzero elements of  $Z_p$  form a group of order  $p - 1$  under multiplication. Show that this statement is false if  $p$  is not prime.

**Answer.** For the set  $Z_p \setminus \{\bar{0}\}$

1.  $Z_p \setminus \{\bar{0}\}$  is obviously associative and communicative.
2. Take  $\bar{1}$  as the identity element,  $\forall \bar{a} \in Z_p \setminus \{\bar{0}\}, \bar{1} \times \bar{a} = \bar{a}$ .
3. We prove there is a unique element  $a^{-1} \in Z_p \setminus \{\bar{0}\}$  s.t.  $aa^{-1} = \bar{1}$ . Assume there exists  $\bar{b}, \bar{c}$  and  $\bar{a} \cdot \bar{b} = \bar{k}, \bar{a} \cdot \bar{c} = \bar{k}$ , then  $a(b - c) \equiv 0 \pmod{p}$ .  $p$  is a prime, so  $\text{lcm}(p, a) = 1, \text{lcm}(p, b - c) = 1$ , so  $\bar{b} = \bar{c}$ . There is at most one element s.t.  $\bar{a}\bar{b} = \bar{k}$ . Take  $\bar{b} = \bar{1}, \bar{2}, \dots, p - 1$ ,  $\bar{k}$  travels through  $\bar{b} = \bar{1}, \bar{2}, \dots, p - 1$ . There exists an element  $\bar{b} \in Z_p \setminus \{\bar{0}\}, \bar{a}\bar{b} = \bar{1}$ .

$Z_p \setminus \{\bar{0}\}$  is a group. If  $p$  is not a prime, the inverse element is not always unique. Take  $a|p$ , there's more than one inverse element in  $Z_p \setminus \{\bar{0}\}$ .

- Exercise 1.1.8.** (a) The relation given by  $a \sim b \Leftrightarrow a - b \in \mathbf{Z}$  is a congruence relation on the additive group  $\mathbf{Q}$  [see Theorem 1.5].  
 (b) The set  $\mathbf{Q}/\mathbf{Z}$  of equivalence classes is an infinite abelian group.

- Answer.** (a) For group  $(\mathbf{Q}, +)$ ,  $a_1 \sim b_1 \Leftrightarrow a_1 - b_1 = k_1 \in \mathbf{Z}$ ,  $a_2 \sim b_2 \Leftrightarrow a_2 - b_2 = k_2 \in \mathbf{Z}$ , so  $(a_1 + a_2) - (b_1 + b_2) = ((k_1 + b_1) + (k_2 + b_2)) - (b_1 + b_2) = k_1 + k_2 \in \mathbf{Z}$ .  $a \sim b$  is a congruence relation.  
 (b) 1 if  $a + b \geq 1$ ,  $\bar{a} + \bar{b} = a + \bar{b} - 1$ . If  $a + b < 1$ ,  $\bar{a} + \bar{b} = a + \bar{b}$ .  
 2  $\mathbf{Q}/\mathbf{Z}$  is obviously associative and communicative.  
 3 Take the identity element as  $\bar{0}$ ,  $\bar{0} + \bar{a} = \bar{a}$ .  
 4 If  $\bar{a} \neq \bar{0}$ , take  $(\bar{a})^{-1} = 1 - \bar{a}$ , then  $\bar{a} + 1 - \bar{a} = \bar{0}$   
 so  $\mathbf{Q}/\mathbf{Z}$  is a abelian group. (Infinite remains to be certified)

**Exercise 1.1.9.** Let  $p$  be a fixed prime. Let  $R_p$  be the set of all those rational numbers whose denominator is relatively prime to  $p$ . Let  $R^p$  be the set of rationals whose denominator is a power of  $p$  ( $p^i, i > 0$ ). Prove that both  $R_p$  and  $R^p$  are abelian groups under ordinary addition of rationals.

**Answer.** Trivial.

**Exercise 1.1.10.** Let  $p$  be a prime and let  $Z(p^\infty)$  be the following subset of the group  $\mathbf{Q}/\mathbf{Z}$ :

$$Z(p^\infty) = \{a/b \in \mathbf{Q}/\mathbf{Z} \mid a, b \in \mathbf{Z} \text{ and } b = p^i \text{ for some } i \geq 0\}$$

Show that  $Z(p^\infty)$  is an infinite group under the addition operation of  $\mathbf{Q}/\mathbf{Z}$ .

**Answer.**  $Z(p^\infty) = \{a/b \mid a, b \in \mathbf{Z}, b = p^i, i \geq 0\}$ . Take  $a = \frac{\bar{a}_1}{b_1}$ ,  $b = \frac{\bar{a}_2}{b_2}$ .  
 $b^{-1} = \frac{b_2 \bar{a}_2}{b_2}$

$$\begin{aligned} a + b^{-1} &= \frac{\bar{a}_1}{b_1} + \frac{b_2 \bar{a}_2}{b_2} = \frac{\bar{a}_1}{p^{s_1}} + \frac{p^{s_2} \bar{a}_2}{p^{s_2}} \\ &= \frac{a_1 \cdot p^{s_2} + p^{s_1}(p^{s_2} - a_2)}{p^{s_1+s_2}} \in Z(p^\infty) \end{aligned}$$

Therefore,  $Z(p^\infty)$  is a subgroup of  $\mathbf{Q}/\mathbf{Z}$ .  $\frac{1}{p^i} \in Z(p^\infty)$  for any  $i \in \mathbf{Z}$ , so  $Z(p^\infty)$  is infinite,  $\mathbf{Q}/\mathbf{Z}$  is also infinite.

**Exercise 1.1.11.** The following conditions on a group  $G$  are equivalent:

- i  $G$  is abelian;
- ii  $(ab)^2 = a^2b^2$  for all  $a, b \in G$ ;
- iii  $(ab)^{-1} = a^{-1}b^{-1}$  for all  $a, b \in G$ ;
- iv  $(ab)^n = a^n b^n$  for all  $n \in \mathbf{Z}$  and all  $a, b \in G$ ;
- v  $(ab)^n = a^n b^n$  for three consecutive integers  $n$  and all  $a, b \in G$ . Show that  
 $v \Rightarrow i$  is false if ‘three’ is replaced by ‘two’.

**Answer.**  $i \Leftrightarrow iii$ :  $((ab)b^{-1})a^{-1} = (ab)(b^{-1}a^{-1}) = e$ , so  $(ab)^{-1} = b^{-1}a^{-1}$ .  
 If iii,  $b^{-1}a^{-1} = a^{-1}b^{-1}$  for any  $a, b \in G$ ,  $G$  is abelian. If i,  $G$  is abelian,  
 $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$ .

iv  $\Rightarrow$  v, iv  $\Rightarrow$  ii and i  $\Rightarrow$  iv are trivial.

ii  $\Rightarrow$  i:

$$(ab)(ab) = aabb \Rightarrow a^{-1}(ab)^2b^{-1} = a^{-1}aabb b^{-1} = ba = ab$$

so  $G$  is abelian.

v  $\Rightarrow$  i:  $a^n b^n = (ab)^n$ ,  $a^{n-1} b^{n-1} = (ab)^{n-1}$ ,  $a^{n+1} b^{n+1} = (ab)^{n+1}$ .

$$(b^{-1})^n (a^{-1})^n = ((ab)^n)^{-1} = ((ab)^{-1})^n$$

$$((ab)^{-1})^n (ab)^{n+1} = (b^{-1})^n a b^{n+1}$$

$$((ab)^{-1})^n (ab)^{n-1} = b^{-1} a^{-1} = (b^{-1})^n a^{-1} b^{n-1}$$

$$a = (b^{-1})^n a b^n \quad b^{-1} a^{-1} b = (b^{-1})^n a^{-1} b^n$$

So  $a^{-1} = b^{-1} a^{-1} b$ , which means  $G$  is abelian.

If “three” is replaced by “two”:  $a^n b^n = (ab)^n$ ,  $a^{n+1} b^{n+1} = (ab)^{n+1}$ .

$$(b^{-1})^n (a^{-1})^n = ((ab)^{-1})^n \quad a = (b^{-1})^n a b^n$$

For the group  $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ , taking any  $a \in S_3$ , we can check that  $a^6 = (1)$ . If  $n = 6$ , then  $a = (b^{-1})^n a b^n$  for any  $a, b \in S_3$ . But  $S_3$  is nonabelian.

**Exercise 1.1.12.** If  $G$  is a group,  $a, b \in G$  and  $bab^{-1} = a^r$  for some  $r \in \mathbf{N}$ , then  $b^j a b^{-j} = a^{r^j}$  for all  $j \in \mathbf{N}$ .

**Answer.**  $bab^{-1} = a^r$ . We prove it by induction. For  $j = 1$ , it's always true. Assume  $j = k$  the equation is correct,  $b^k a b^{-k} = a^{r^k}$ .  $ba^{r^k} b^{-1} = (a^{r^k})^r = a^{r^{k+1}}$ . For  $j = k + 1$ , it's also true.

**Exercise 1.1.13.** If  $a^2 = e$  for all elements  $a$  of a group  $G$ , then  $G$  is abelian.

**Answer.**

$$a^2 = e \Rightarrow a^2 a^{-1} = e a^{-1} = a(a a^{-1}) = a e \Rightarrow a = a^{-1}$$

$$ab = a^{-1} b^{-1} = (ab)^{-1} = (ba)^{-1}$$

So  $ab = ba \forall a, b \in G$ .  $G$  is abelian.

**Exercise 1.1.14.** If  $G$  is a finite group of even order, then  $G$  contains an element  $a \neq e$  such that  $a^2 = e$ .

**Answer.** Suppose not.  $\forall a \neq e, aa \neq e \Leftrightarrow a \neq a^{-1}$ . We can classify the group into some subsets.  $G = \bigcup_{a \neq e} \{a, a^{-1}\} \cup \{e\}$ . Notice that  $\{a, a^{-1}\} \cap \{b, b^{-1}\} = \emptyset$  if  $a \neq b$ , so  $|G| = 2n + 1$ , That's contradictory!

**Exercise 1.1.15.** Let  $G$  be a nonempty finite set with an associative binary operation such that for all  $a, b, c \in G$ ,  $ab = ac \Rightarrow b = c$  and  $ba = ca \Rightarrow b = c$ . Then  $G$  is a group. Show that this conclusion may be false if  $G$  is infinite.

**Answer.**  $G$  is a semigroup. Fix  $a \in G$  and take  $b$  travels through all elements in  $G$ , then  $ab$  travels through all elements in  $G$ .

There exists an element  $e_1$  s.t.  $ae_1 = a \forall a \in G$ . Similarly, we can find  $e_2$  s.t.  $e_2a = a \forall a \in G$ .  $e_2e_1 = e_1 = e_2 = e$ .  $e$  is the identity element of  $G$ . Easily, we can find that  $\forall a \in G, \exists! a^{-1} \in G$  s.t.  $a^{-1}a = aa^{-1} = e$  because  $ab = ac \Rightarrow b = c$  and  $ba = ca \Rightarrow b = c$ .

$G$  is a group. If  $G$  is infinite,  $G$  may not be a group, for example:  $(\mathbb{Z}_+, \times)$ .

**Exercise 1.1.16.** Let  $a_1, a_2, \dots$  be a sequence of elements in a semigroup  $G$ . Then there exists a unique function  $\Psi : \mathbb{N}^* \rightarrow G$  such that  $\Psi(1) = a_1, \Psi(2) = a_1a_2, \Psi(3) = (a_1a_2)a_3$  and for  $n \geq 1, \Psi(n+1) = (\Psi(n))a_{n+1}$ . Note that  $\Psi(n)$  is precisely the standard  $n$  product  $\prod_{i=1}^n a_i$ .

**Answer.** Applying the Recursion Theorem with  $a = a_1, S = G$  and  $f_n : G \rightarrow G$  given by  $x \mapsto xa_{n+2}$  yields a function  $\phi : \mathbb{N} \rightarrow G$ . Let  $\Psi = \phi\theta$ , where  $\theta : \mathbb{N}^* \rightarrow \mathbb{N}$  is given by  $k \mapsto k - 1$ .

## 1.2 Homomorphisms and subgroups

**Exercise 1.2.1.** If  $f : G \rightarrow H$  is a homomorphism of groups, then  $f(e_G) = e_H$  and  $f(a^{-1}) = f(a)^{-1}$  for all  $a \in G$ . Show by example that the first conclusion may be false if  $G, H$  are monoids that are not groups.

**Answer.** For example,  $(\mathbf{Z}_+, +)$  and  $(\mathbf{N}, \times)$  are monoids. Denote  $f : \mathbf{Z}_+ \rightarrow \mathbf{N}$  as  $f(x) = 0 \forall x \in \mathbf{Z}_+$ .  $f$  is a homomorphism satisfies those conditions.

**Exercise 1.2.2.** A group  $G$  is abelian if and only if the map  $G \rightarrow G$  given by  $x \mapsto x^{-1}$  is automorphism.

**Answer.** If  $G$  is abelian,  $f(x) = x^{-1}$  is a monomorphism and epimorphism.  
 $f(a)f(b) = a^{-1}b^{-1} = (ab)^{-1} = f(ab)$   
 If  $f(x) = x^{-1}$  is a isomorphism,  $f(a)f(b) = a^{-1}b^{-1} = f(ab) = (ab)^{-1} = b^{-1}a^{-1} \forall a, b \in G$ , so  $G$  is abelian.

**Exercise 1.2.3.** Let  $Q_8$  be the group (under ordinary matrix multiplication) generated by complex matrices  $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  and  $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ , where  $i^2 = -1$ . Show that  $Q_8$  is a nonabelian group of order 8.  $Q_8$  is called the quaternion group.

**Answer.** The multiply operation is associative by the difinition.  $A^4 = B^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$  which is the identity element.

$$A^{-1} = A^3 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \in G \quad B^{-1} = B^3 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \in G$$

So  $\forall A^i B^j \in G, (A^i B^j)^{-1} \in G$ .  $G$  is a group. Now we examine the order of  $G$  is 8.

$$BA = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

$$A^3 B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix}$$



So  $BA = A^3B$ . Take  $X = A^{s_1}B^{s_2}A^{s_3}B^{s_4} \dots A^{s_{2n-1}}B^{s_{2n}} = A^{s_1}B^{s_2-1}A^3B^{s_3-1}B^{s_4} \dots A^{s_{2n-1}}B^{s_{2n}} = \dots$ . In finite steps, we can change it into  $X = A^aB^b$ .  $A^4 = B^4 = I$ , so we only consider  $1 \leq a, b \leq 4$ .  $A^2 = B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ , we list all:  $Q_8 = \{A, A^2, B, BA, AB, A^2B, AB^2, I\}$ . The order of  $Q_8$  is 8.

**Exercise 1.2.4.** Let  $H$  be the group (under ordinary matrix multiplication) of real matrices generated by  $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  and  $D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . Show that  $H$  is a nonabelian group of order 8 which is not isomorphic to the quaternion group, but is isomorphic to the group  $D_4^*$ .

**Answer.**  $C^4D^2 = I, DC = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = C^3D$ . Similarly, we can prove  $H$  is a nonabelian group of order 8.  $H = \{C, C^2, C^3, I, D, CD, C^2D, C^3D\}$ . Assume  $G \cong H$  and the isomorphism is  $f$ . Let  $f(D) = X$ ,  $f(D^2) = X^2 = f(I) = I$ , so  $X^2 = I$ . But  $f^{-1}(I) = I \Rightarrow X \neq I \Rightarrow X = AB$  or  $X = A^2$  or  $X = B^2$ .

If  $X = A^2$ , consider  $f(C) = Y, f(C^2D) = Z$ , we have  $(Y, Z) = (B^2, AB)$  or  $(Y, Z) = (AB, B^2)$ .  $f(C^2D) = f(C^2)f(D) \Leftrightarrow Z = XY$ . That's contradictory!

If  $X = B^2$ , the proof is similar.

If  $X = AB$ ,  $(Y, Z) = (A, B)$  or  $(Y, Z) = (B, A)$ . That's contradictory! So  $f$  doesn't exist.  $G$  is not isomorphic to  $H$ .

Now we prove  $H \cong D_4^*$ . For any point  $(x, y)^T$  inside the square

$$T_x = (x, -y)^T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} (x, y)^T = CD(x, y)^T$$

$$T_y = (-x, y)^T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} (x, y)^T = C^3D(x, y)^T$$

$$T_{13} = (-y, x)^T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} (x, y)^T = C^3(x, y)^T$$

$$T_{24} = (y, -x)^T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} (x, y)^T = C(x, y)^T$$

so  $D_4^* = \langle T_x, T_y, T_{13}, T_{24} \rangle = H = \langle C, D \rangle$ .

**Exercise 1.2.5.** Let  $S$  be a nonempty subset of a group  $G$  and define a relation on  $G$  by  $a \sim b$  if and only if  $ab^{-1} \in S$ . Show that  $\sim$  is an equivalence relation if and only if  $S$  is a subgroup of  $G$ .

**Answer.** If  $\sim$  is an equivalence relation

1.  $a \sim b \Rightarrow b \sim a$ ;
2.  $a \sim a$ ;
3.  $a \sim b, b \sim c \Rightarrow a \sim c$ .

2  $\Leftrightarrow aa^{-1} = e \in S$ . 1  $\Rightarrow a \sim e \Rightarrow e \sim a \forall a \in S$ , so  $ae^{-1} = a \in S, ea^{-1} = a^{-1} \in S$ . If  $a, b \in S, b^{-1} \in S$ , so  $ae^{-1} \in S, e(b^{-1})^{-1} \in S$ . By 3,  $a \sim e, e \sim b^{-1} \Rightarrow a \sim b^{-1} \Rightarrow ab \in S$ .  $S$  is a subgroup of  $G$ .

If  $S$  is a subgroup of  $G$

1.  $aa^{-1} \in S \Rightarrow a \sim a$ ;
2.  $ab^{-1} \in S \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in S \Rightarrow (a \sim b \Rightarrow b \sim a)$ ;
3.  $ab^{-1} \in S, bc^{-1} \in S \Rightarrow (ab^{-1})(bc^{-1}) = ac^{-1} \in S$ , which means  $a \sim b, b \sim c \Rightarrow a \sim c$

In conclusion,  $\sim$  is an equivalence relation.

**Exercise 1.2.6.** A nonempty finite subset of a group is a subgroup if and only if it is closed under the product in  $G$ .

**Answer.**  $\Rightarrow$ : Trivial.

$\Leftarrow$ :  $S$  is apparently associative.  $\forall a, b \in S, ab \in S$ .  $S$  is a finite set, so there exists  $m > n \in \mathbf{N}$  s.t.  $a^m = a^n$ .

**Exercise 1.2.7.** If  $n$  is a fixed integer, then  $\{kn | n \in \mathbf{Z}\} \subset \mathbf{Z}$  is an additive subgroup of  $\mathbf{Z}$ , which is isomorphic to  $\mathbf{Z}$ .

**Answer.** Denote  $Z^n = \{kn | k \in \mathbf{Z}\}$ . We can easily check that  $Z^n$  is a subgroup of  $\mathbf{Z}$ . Now we build an isomorphism between  $Z^n$  and  $\mathbf{Z}$ . Take  $f : Z^n \rightarrow \mathbf{Z}$  as  $f(kn) = k, f^{-1}(n) = kn$ .  $f$  is a bijection so  $Z^n$  and  $\mathbf{Z}$  are isomorphic.

**Exercise 1.2.8.** The set  $\{\sigma \in S_n | \sigma(n) = n\}$  is a subgroup of  $S_n$  which is isomorphic to  $S_{n-1}$ .

**Answer.** Denote  $S_n^{(n)} = \{\sigma \in S_n | \sigma(n) = n\}$ .  $\forall \sigma_1, \sigma_2 \in S_n^{(n)}, \sigma_1\sigma_2(n) = \sigma_1(\sigma_2(n)) = \sigma_1(n) = n$ , so  $\sigma_1\sigma_2 \in S_n^{(n)}$ . By the above exercise,  $S_n^{(n)}$  is a subgroup of  $S_n$ . Now we build an isomorphism between  $S_n^{(n)}$  and  $S_{n-1}$ . Take  $f : S_{n-1} \rightarrow S_n^{(n)}$  as  $f(\sigma) = \sigma'$ , where  $\sigma'(x) = \begin{cases} n, & x = n \\ \sigma(n), & x \neq n \end{cases}$ .  $\sigma' \in S_n^{(n)}$  and  $f$  is a bijection, so  $S_{n-1} \cong S_n^{(n)}$ .

**Exercise 1.2.9.** Let  $f : G \rightarrow H$  be a homomorphism of groups,  $A$  a subgroup of  $G$ , and  $B$  a subgroup of  $H$ .

- (a)  $\text{Ker } f$  and  $f^{-1}(B)$  are subgroups of  $G$ .
- (b)  $f(A)$  is a subgroup of  $H$ .

**Answer.** (a)  $f$  is a homomorphism, so  $f(e) = e', e \in \text{Ker } f$ .  $\forall a \in \text{Ker } f$ ,  $f(aa^{-1}) = f(a)f(a^{-1}) = e'$ , so  $f(a^{-1}) = f(a)^{-1} = e'^{-1} = e'$ .  $\forall a, b \in \text{Ker } f$ ,  $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e' \Rightarrow ab^{-1} \in \text{Ker } f$ , which means  $\text{Ker } f$  is a subgroup of  $G$ . The proof of  $f^{-1}(B)$  is a subgroup of  $G$  is similar.

(b)  $f$  is a homomorphism,  $f(e) = e'$ .  $\forall a, b \in A, ab^{-1} \in A$ , so  $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in f(A)$ ,  $f(A)$  is a subgroup of  $H$ .

**Exercise 1.2.10.** List all subgroups of  $Z_2 \oplus Z_2$ . Is  $Z_2 \oplus Z_2$  isomorphic to  $Z_4$ ?

**Answer.**  $Z_2 \oplus Z_2$ :  $\{(1, 1), (1, 0), (0, 1), (0, 0)\}, \{(1, 1), (0, 0)\}, \{(0, 0)\}, \{(1, 0), (0, 0)\}, \{(0, 1), (0, 0)\}, \{(0, 1), (1, 0), (0, 0)\}$ .  
 $Z_4$ :  $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}, \{\bar{0}, \bar{2}\}, \{\bar{0}\}$ .  
 $Z_4$  and  $Z_2 \oplus Z_2$  are not isomorphic because they have different subgroups.

**Exercise 1.2.11.** If  $G$  is a group, then  $C = \{a \in G | ax = xa \text{ for all } x \in G\}$  is a abelian subgroup of  $G$ .  $C$  is called the center of  $G$ .

**Answer.** Take  $a, b \in C, ab = ba$ ,  $C$  is commutative.  $\forall a, b \in C, x \in G$ ,  $b^{-1} \in G$ , so  $ab^{-1} = b^{-1}a$ .

$$ax = axbb^{-1} = abxb^{-1} = baxb^{-1} = bxab^{-1} = abb^{-1}x = bab^{-1}x$$

so  $b^{-1}ax = ab^{-1}x = xab^{-1}$ ,  $ab^{-1} \in C$ ,  $C$  is a subgroup of  $G$ .

**Exercise 1.2.12.** The group  $D_4^*$  is not cyclic, but can be generated by two elements. The same is true of  $S_n$  (nontrivial). What is the minimal number of generators of the additive group  $\mathbf{Z} \oplus \mathbf{Z}$ ?

**Answer.**  $\mathbf{Z} \oplus \mathbf{Z} = \{(a, b) | a \in \mathbf{Z}, b \in \mathbf{Z}\} = \langle (0, 0), (1, 0), (0, 1) \rangle$ . We can easily check the spanning set is the minimal.

**Exercise 1.2.13.** If  $G = \langle a \rangle$  is a cyclic group and  $H$  is any group, then every homomorphism  $f : G \rightarrow H$  is completely determined by the element  $f(a) \in H$ .

**Answer.**  $\forall x \in G$ , there exist  $m \in \mathbf{N}$  s.t.  $x = a^m$ , so  $f(x) = f(a^m) = f(a)^m \Rightarrow \text{Im} f = \langle f(a) \rangle$ .  $f : a^m \mapsto f(a)^m \forall m \in \mathbf{N}$ .  $f$  is completely determined by  $f(a) \in H$ .

**Exercise 1.2.14.** The following cyclic subgroups are all isomorphic: the multiplication group  $\langle i \rangle$  in  $\mathbf{C}$ , the additive group  $\mathbf{Z}_4$  and the subgroup  $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \right\rangle$  of  $S_4$ .

**Answer.**  $\langle i \rangle = \{i, -1, -i, 1\}$ ,  $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ ,  $\langle (1234) \rangle = \{(1234), (13)(24), (1432), (1)\}$ . Denote  $f : \langle i \rangle \rightarrow Z_4$  as  $f(i) = \bar{i}$ ,  $g : Z_4 \rightarrow \langle (1234) \rangle$  as  $g(i) = (1234)^i$ . From the exercise above we know  $f$  and  $g$  are homomorphisms, and they are bijections, so  $\langle i \rangle \cong Z_4 \cong \langle (1234) \rangle$ .

**Exercise 1.2.15.** Let  $G$  be a group and  $\text{Aut}G$  is the set of all automorphisms of  $G$ .

- (a)  $\text{Aut}G$  is a group with composition of functions as binary operation.
- (b)  $\text{Aut}\mathbf{Z} \cong Z_2$  and  $\text{Aut}Z_6 \cong Z_2$ ;  $\text{Aut}Z_8 \cong Z_2 \oplus Z_2$ ;  $\text{Aut}Z_p \cong Z_{p-1}$  ( $p$  prime).
- (c) What is  $\text{Aut}Z_n$  for arbitrary  $n \in \mathbf{N}^*$ ?

**Answer.** We only prove the third question.

For  $\bar{a} \in Z_n$ , the order of  $\bar{a}$  is  $|\bar{a}| = \frac{n}{(n,a)}$ . When  $(n,a) = 1$ ,  $\bar{a}$  is a generator of  $Z_n$ . Denote Euler function as  $\varphi(x)$  and  $Z_n^* = \{\bar{a} \in Z_n | (a,n) = 1\}$ , then  $|Z_n^*| = \varphi(n)$ . For  $\sigma \in \text{Aut}Z_n$ ,  $\sigma$  is completely determined by  $\sigma(\bar{1}) = \bar{a}$ , and we denote  $\sigma$  as  $\sigma_a$ . For  $\sigma_a, \sigma_b \in \text{Aut}Z_n$ ,  $\sigma_a(\sigma_b(\bar{1})) = \sigma_a(\bar{b}) = \bar{a}\bar{b} = \sigma_{ab}(\bar{1})$ . We have proved  $\text{Aut}Z_n \cong Z_n^*$ .

Now we give out a lemma to show the structure of  $Z_n^*$ .

**Lemma.** If  $n = st$ ,  $(s,t) = 1$ , then  $Z_n^* \cong Z_s^* \oplus Z_t^*$ .

The proof of this lemma is quite simple. Consider the mapping  $f^* : Z_n^* \rightarrow Z_s^* \oplus Z_t^*$  which is defined by  $(x \bmod n) \mapsto (x \bmod s, x \bmod t)$ . Since for any  $a, b \in Z_n^*$ ,  $f^*(a)f^*(b) = (a \bmod s, a \bmod t)(b \bmod s, b \bmod t) = (ab \bmod s, ab \bmod t) = f^*(ab)$ ,  $f^*$  is a well defined homomorphism. For  $x \in \text{Ker}f^*$ ,  $x \equiv 1 \bmod s$ ,  $x \equiv 1 \bmod t$ , so  $x \equiv 1 \bmod [s,t]$ ,  $x \equiv 1 \bmod n$ ,  $f^*$  is a monomorphism. Since  $|f^*(Z_n^*)| = |Z_n^*| = \varphi(n) = \varphi(s)\varphi(t) = |Z_s^* \oplus Z_t^*|$ ,  $f^*$  is an epimorphism.  $Z_n^* \cong Z_s^* \oplus Z_t^*$

For  $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ ,  $Z_n^* \cong Z_{p_1^{k_1}}^* \oplus Z_{p_2^{k_2}}^* \oplus \cdots \oplus Z_{p_m^{k_m}}^*$ . Now we consider the structure of  $Z_{p^k}^*$ .

For  $p = 2$ ,  $Z_2^* \cong Z_1$ ,  $Z_4^* \cong Z_2$ ,  $Z_{2^k}^* \cong Z_2 \oplus Z_{2^{k-2}}$ .

For other odd prime  $p$ ,  $Z_{p^k}^* \cong Z_{(p-1)p^{k-1}}$ .

In order to prove the result, we need the Lagrange theorem in number theory.

**Lemma** (Lagrange).  $f(x) \in Z[n]$ ,  $f(x) \equiv k$  has at most  $n$  solutions when  $\bmod p$ , where  $p$  is an odd prime.

We use induction to prove the lemma.

1.  $n = 1$ , the proof is trivial.
2. Assume for  $n \leq m-1$  the lemma is correct, and for  $n = m$ ,  $f(x) \equiv k$  has  $m+1$  solutions.  $f(x) - f(x_{m+1}) = (x - x_{m+1})g(x) \equiv 0 \bmod p$ . Take  $x = x_i, i = 1, 2, \dots, m$ ,  $(x_i - x_{m+1})g(x_i) \equiv 0 \bmod p$ ,  $x_i \neq x_{m+1}$ , so  $g(x_i) \equiv 0 \bmod p$ . That's contradictory to the induction assumptions!

The lemma is proved.

Come back to the original question. Firstly, we consider  $k = 1$  and  $p$  is an odd prime. For any factor  $d$  of  $p - 1$ , denote  $S(d) = \{\bar{a} \in Z_p^* | \text{ord}_p(a) = d\}$ .  $S(d)$  forms a partition of  $Z_p^*$ . If  $S(d) \neq \emptyset$ , there exists  $\bar{a} \in S(d)$  and  $a^d \equiv 1 \pmod{p}$ . By Lagrange theorem,  $a^d \equiv 1 \pmod{p}$  has at most  $d$  solutions. Notice that  $\{1, a, a^2, \dots, a^{d-1}\}$  are the solutions of the equation,  $a^i \not\equiv a^j \pmod{p}$ , whence  $S(d) \subset \langle \bar{a} \rangle$ . For  $k = 1, 2, \dots, d-1$ ,  $\text{ord}_p(a^k) = |a^k| = \frac{d}{(d,k)} = d \Leftrightarrow (d, k) = 1$ . Thus  $|S(d)| = \varphi(d)$ .

From  $Z_p^* = \bigcup_{d|p-1} S(d)$ , we get

$$p - 1 = |Z_p^*| = \sum_{d|p-1} |S(d)| \leq \sum_{d|p-1} \varphi(d) = p - 1$$

If  $d|p-1$ ,  $|S(d)| = \varphi(d)$ . Particularly, when  $d = p-1$ ,  $|S(p-1)| = \varphi(p-1) \neq 0$ ,  $Z_p^*$  has a element of order  $p-1$ ,  $Z_p^*$  is a cyclic group.

Secondly, we consider  $k \geq 2$ . Take  $a \in \mathbf{Z}$  and  $\bar{a}$  is the class of  $x \equiv a \pmod{p^k}$ . For  $s \geq t$ , we have a group homomorphism  $f_{s,t} : Z_{p^s}^* \rightarrow Z_{p^t}^*$  which is defined by  $(a \pmod{p^s}) \mapsto (a \pmod{p^t})$ . Since  $a \equiv b \pmod{p^s} \Rightarrow a \equiv b \pmod{p^t}$ ,  $f$  is well defined.  $\text{Ker} f_{s,t} = \{up^t + 1 \pmod{p^s} | u = 0, 1, \dots, p^{s-t} - 1\}$ . If  $2t \geq s$ , since  $(up^t + 1)(vp^t + 1) \equiv uv p^{2t} + (u+v)p^t + 1 \equiv (u+v)p^t + 1 \pmod{p^s}$ ,  $\text{Ker} f_{s,t} \cong Z_{p^{s-t}}$  is a cyclic group. There exists a isomorphism  $g_{s,t} : Z_{p^s}^* / \text{Ker} f_{s,t} \rightarrow Z_{p^t}^*$ .

$$\{\bar{1}_{p^k}\} = \text{Ker} f_{k,k} < \text{Ker} f_{k,k-1} < \dots < \text{Ker} f_{k,1} < Z_{p^k}^*$$

**Lemma.** Suppose  $i \geq 2$ ,  $\bar{a}_{p^k} \in \text{Ker} f_{k,i}$ , but  $\bar{a}_{p^k} \notin \text{Ker} f_{k,i+1}$ , then  $\bar{a}_{p^k}^p \in \text{Ker} f_{k,i+1}$  and  $\bar{a}_{p^k}^p \notin \text{Ker} f_{k,i+2}$ .

This lemma can be proved by LTE. Here we use the language in group theory to prove it.  $f_{k,i+2}(\bar{a}_{p^k}) = \bar{a}_{p^{i+2}}$ ,  $\bar{a}_{p^{i+2}} \in f_{k,i+2}(\text{Ker} f_{k,i}) = \text{Ker} f_{i+2,i}$ .  $\text{Ker} f_{i+2,i} \cong Z_{p^2}$  since  $2i \geq i+2$ .  $\bar{a}_{p^{i+2}} \notin f_{k,i+2}(\text{Ker} f_{k,i+1}) = \text{Ker} f_{i+2,i+1} \cong Z_p$ .  $\text{Ker} f_{i+2,i+1}$  contains all the elements whose order is  $p$  in  $\text{Ker} f_{i+2,i}$ , so  $|\bar{a}_{p^{i+2}}| = p^2$ .  $\bar{a}_{p^{i+2}}^p \in \text{Ker} f_{i+2,i+1}$ ,  $\bar{a}_{p^{i+2}}^p \notin \text{Ker} f_{i+2,i+2}$ ,  $\bar{a}_{p^k}^p \in g_{k,i+2}^{-1}(\bar{a}_{p^{i+2}}^p) \subset g_{k,i+2}^{-1}(\text{Ker} f_{i+2,i+1}) = \text{Ker} f_{k,i+1}$ ,  $\bar{a}_{p^k}^p \notin g_{k,i+2}^{-1}(\text{Ker} f_{i+2,i+2}) = \text{Ker} f_{k,i+2}$ .

For  $i = 1$ , if  $p$  is an odd prime,  $\text{Ker} f_{3,1} = \langle p + 1_{p^3} \rangle \cong Z_{p^2}$ , if  $p = 2$ ,  $\text{Ker} f_{3,1} = \{\bar{1}_8, \bar{3}_8, \bar{5}_8, \bar{7}_8\} \cong Z_2 \oplus Z_2$ . Thus, for  $\bar{a}_{p^k} \in \text{Ker} f_{k,2}$ ,  $\bar{a}_{p^k} \notin \text{Ker} f_{k,3}$ , using the lemma above for several times, we get  $\bar{a}_{p^k}^{p^{k-2}} \in \text{Ker} f_{k,2}$ ,  $\bar{a}_{p^k}^{p^{k-3}} \notin \text{Ker} f_{k,k}$ ,  $|\bar{a}_{p^k}| = p^{k-2}$ ,  $\text{Ker} f_{k,2} \cong Z_{p^{k-2}}$ .

If  $p$  is an odd prime, we can further obtain  $\text{Ker} f_{k,1} \cong Z_{p^{k-1}}$ .

Suppose  $x$  is a generator of  $Z_p^*$ , assume  $a \in g_{k,1}^{-1}(x)$ ,  $g_{k,1}^{-1}(x) = a\text{Ker}f_{k,1}$ , and  $a^{p-1} \in g_{k,1}^{-1}(x^{p-1}) = g_{k,1}^{-1}(1_p) = \text{Ker}f_{k,1}$ . If  $a^{p-1} \notin \text{Ker}f_{k,2}$ , then  $|a^{p-1}| = p^{k-1}$ . If  $a^{p-1} \in \text{Ker}f_{k,2}$ ,  $\forall h \in \text{Ker}f_{k,1}, h \notin \text{Ker}f_{k,2}$ . Since  $(ah)^{p-1} = (a^{p-1}h^p)h^{-1}$ ,  $(ah)^{p-1} \in \text{Ker}f_{k,1}$ ,  $(ah)^{p-1} \notin \text{Ker}f_{k,2}$ , whence  $|(ah)^{p-1}| = p^{k-1}$ ,  $Z_{p^k}^* \cong Z_{(p-1)p^{k-1}}$ .  
If  $p = 2$ ,  $Z_{2^k}^* = \text{Ker}f_{k,1} \cong Z_{2^{k-2}} \oplus Z_2$ .

For  $\text{Aut}\mathbf{Z}$ , assume there exist  $f \neq 1_G, -1_G, f \in \text{Aut}\mathbf{Z}$ . WLOG,  $f(1) = x \neq \pm 1, f(-1) = y$ .  $f(1) + f(-1) = f(0) = x + y = 0$ . Assume  $af(1) + bf(-1) = f(a - b) = 1 = (a - b)x$ , since  $x \neq \pm 1$ , there is a contradiction.  $\text{Aut}\mathbf{Z} \cong Z_2$ .

**Exercise 1.2.16.** For each prime  $p$  the additive subgroup  $Z(p^\infty)$  of  $\mathbf{Q}/\mathbf{Z}$  is generated by the set  $\{1/\bar{p}^n | n \in \mathbf{N}^*\}$ .

**Answer.** We prove that  $\left\langle \bigcup_{n=1}^{\infty} \frac{1}{p^n} \right\rangle \cong Z(p^\infty)$ .  $\forall x \in Z(p^\infty), x = \frac{\bar{a}}{b} = \frac{\bar{a}}{p^k}$ .

Expand  $a$  as  $a = \sum_{i=0}^{k-1} p^i a_i$ , where  $a_i = 1, 2, \dots, p-1$ .  $x = \frac{\bar{a}}{b} = \sum_{i=0}^{k-1} \frac{\bar{a}_i}{p^{k-i}} = \sum_{i=1}^k \frac{\bar{a}_{k-i}}{p^i}$ . Denote  $f : \left\langle \bigcup_{n=1}^{\infty} \frac{1}{p^n} \right\rangle \rightarrow Z(p^\infty)$  as  $f\left(\sum_{i=1}^n \frac{a_i}{p^i}\right) = \sum_{i=1}^n \frac{a_i}{p^i}$ .  $f$  is an isomorphism because every  $x \in Z(p^\infty)$  can be written in such form.

**Exercise 1.2.17.** Let  $G$  be an abelian group and let  $H, K$  be subgroups of  $G$ . Show that the join  $H \vee K$  is the set  $\{ab | a \in H, b \in K\}$ . Extend this result to any finite number of subgroups of  $G$ .

**Answer.**  $H \vee K = \langle H \cup K \rangle, I = \{ab | a \in H, b \in K\}$ .  $G$  is abelian so  $I$  is a subgroup of  $G$ .  $H < I, K < I, (H \cup K) \subset I$ .  $\langle H \cup K \rangle \subset I \Rightarrow \langle H \cup K \rangle = I$ .

For any  $ab \in I, a \in H, b \in K$ , we prove that  $ab$  is contained in any subgroup which contains  $H \cup K$ .

Assume  $\langle H \cup K \rangle \subset J$ , so  $a \in J, b \in J \Rightarrow ab \in J$ , which means  $I \subset J$ .  $\langle H \cup K \rangle = I$ .

$G$  is abelian group,  $H_1, H_2, \dots, H_n$  are  $n$  subgroups.  $\left\langle \bigcup_{i=1}^n H_i \right\rangle = \left\{ \prod_{i=1}^n h_i | h_i \in H_i, i = 1, 2, \dots, n \right\}$ . This proposition can be proved by induction.

- Exercise 1.2.18.** 1. Let  $G$  be a group and  $\{H_i | i \in I\}$  a family of subgroups. State and prove a condition that will imply that  $\bigcup_{i \in I} H_i$  is a subgroup, that is  $\bigcup_{i \in I} H_i = \left\langle \bigcup_{i \in I} H_i \right\rangle$ .
2. Given an example of a group  $G$  and a family of subgroups  $\{H_i | i \in I\}$  such that  $\bigcup_{i \in I} H_i \neq \left\langle \bigcup_{i \in I} H_i \right\rangle$ .

**Answer.** I didn't find a sufficient and necessary condition for this question, just choose one as you like:)

- Exercise 1.2.19.** 1. The set of all subgroups of a group  $G$ , partially ordered by set theoretic inclusion, forms a complete lattice in which the g.l.b of  $\{H_i | i \in I\}$  is  $\bigcap_{i \in I} H_i$  and the l.u.b is  $\left\langle \bigcap_{i \in I} H_i \right\rangle$ .
2. Exhibit the lattice of subgroups of the groups  $S_3, D_4^*, Z_6, Z_{27}$  and  $Z_{36}$ .

- Answer.** 1. The subset relation  $<$  forms a partially ordered relation. By the definition of  $\left\langle \bigcup_{i \in I} H_i \right\rangle$ ,  $\left\langle \bigcup_{i \in I} H_i \right\rangle$  is the smallest set contains  $\bigcup_{i \in I} H_i$ , so it's l.u.b. For glb, we know that  $\bigcap_{i \in I} H_i \subset H_i \forall i \in I$ , and  $\forall H \supset \bigcap_{i \in I} H_i$ , there exists  $x \in H, x \notin H_j \ j \in I$ , so  $\bigcap_{i \in I}$  is glb.
2.  $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ .



The Hasse figure of the lattice of  $S_3$

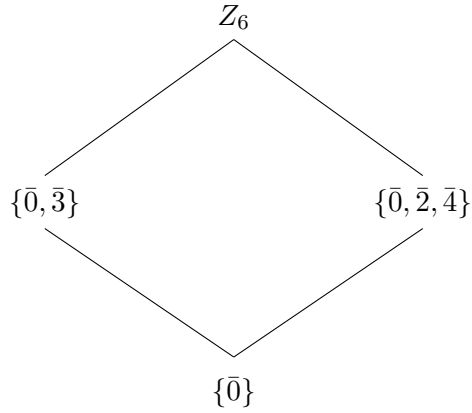


$$D_4^* = \{R, R^2, R^3, I, T_x, T_y, T_{13}, T_{24}\}.$$



The Hasse figure of the lattice of  $D_4^*$

$$Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}.$$



The Hasse figure of the lattice of  $Z_6$

The Hasse figure of the lattice of  $Z_{27}$ The Hasse figure of the lattice of  $Z_{36}$

### 1.3 Cyclic groups

**Exercise 1.3.1.** Let  $a, b$  be elements of group  $G$ . Show that  $|a| = |a^{-1}|$ ;  $|ab| = |ba|$ , and  $|a| = |cac^{-1}|$  for all  $c \in G$ .

**Answer.** We only consider that  $|a|, |b|, |c|$  are finite. Assume  $a^k = e$ ,  $(ab)^m = e$ ,  $(ac^{-1})^n = e$ ,  $k, m, n \neq 0$ .  $a^k \cdot (a^{-1})^k = e$ , so  $k$  is also the order of  $a^{-1}$ ,  $|a^{-1}| = k$ .  $(ab)^m = e = a(ba)^{m-1}b \Rightarrow (ba)^{m-1} = a^{-1}b^{-1}$ ,  $(ba)^m = a^{-1}b^{-1}ba = e$ .  $m$  is the order of  $ba$ .  $(cac^{-1})^r = cac^{-1}cac^{-1} \dots cac^{-1} = ca^rc^{-1} = e$ , so  $a^r = e$ , whence  $r = k$ .

**Exercise 1.3.2.** Let  $G$  be an abelian group containing elements  $a$  and  $b$  of orders  $m$  and  $n$  respectively. Show that  $G$  contains an element whose order is the least common multiple of  $m$  and  $n$ .

**Answer.** If  $(m, n) = 1$ , we know that  $\forall a^i, i = 1, 2, \dots, m, b^j, j = 1, 2, \dots, n$ ,  $a^i b^j \neq e$ , since if  $a^i = b^j$ ,  $|a^i| = n = |b^{-j}| = |b^j| = m$ .  $G$  is abelian, so  $(ab)^k = a^k b^k \Rightarrow |ab| = mn = [m, n]$ .

If  $m|n$  or  $n|m$ , then  $a$  or  $b$  is the element we want. We consider  $m \nmid n$  and  $n \nmid m$ . Factorise  $n = p_1^{t_1} p_2^{t_2} \dots p_l^{t_l}$ ,  $m = p_1^{s_1} p_2^{s_2} \dots p_l^{s_l}$ , where  $p_1, \dots, p_l$  are primes and  $t_1, \dots, t_l, s_1, \dots, s_l \geq 0$ . We can choose a new arrangement of  $p_1, \dots, p_l$  and make  $t_1 \geq s_1, t_2 \geq s_2, \dots, t_i \geq s_i, t_{i+1} < s_{i+1}, \dots, t_l < s_l$ .

$$(m, n) = p_1^{s_1} \dots p_i^{s_i} p_{i+1}^{t_{i+1}} \dots p_l^{t_l}, [m, n] = p_1^{t_1} \dots p_i^{t_i} p_{i+1}^{s_{i+1}} \dots p_l^{s_l}$$

Take  $x = a^{p_{i+1}^{s_{i+1}} \dots p_l^{s_l}}$ ,  $y = b^{p_1^{t_1} \dots p_i^{t_i}}$ , then  $|x| = p_1^{t_1} \dots p_i^{t_i}$ ,  $|y| = p_{i+1}^{s_{i+1}} \dots p_l^{s_l}$ . Thus  $(x, y) = 1$ , the order of  $xy$  is  $|x| \cdot |y| = p_1^{t_1} \dots p_i^{t_i} p_{i+1}^{s_{i+1}} \dots p_l^{s_l} = [m, n]$ .

**Exercise 1.3.3.** Let  $G$  be an abelian group of order  $pq$ , with  $(p, q) = 1$ . Assume there exist  $a, b \in G$  such that  $|a| = p, |b| = q$  and show that  $G$  is cyclic.

**Answer.** From **Exercise 1.3.2** we know  $a^i b^j \neq e$  for  $i < p, j < q$ .  $|G| = pq$  for all  $a^i b^j$  and  $a^m b^n$  with  $i \neq m, b \neq n, a^i b^j \neq a^m b^n$ . So  $G$  can be generated by  $ab$ .  $G$  is cyclic.

**Exercise 1.3.4.** If  $f : G \rightarrow H$  is a homomorphism,  $a \in G$ , and  $f(a)$  has finite order in  $H$ , then  $|a|$  is infinite or  $|f(a)|$  divides  $|a|$ .

**Answer.** Assume  $|f(a)| = n$ ,  $|a| = m$ , and  $n \nmid m$ . Trivially,  $m \geq n$ . Assume  $\gcd(m, n) = k \leq n$ .  $a^m = e \Rightarrow f(a)^m = e' = f(a)^n$ . By Bezout theorem  $\exists x, y \in \mathbf{Z}$  s.t.  $f(a)^{mx+ny} = f(a)^k = e'$ ,  $k \leq n$ , that's contradictory!

**Exercise 1.3.5.** Let  $G$  be the multiplicative group of all nonsingular  $2 \times 2$  matrices with rational entries. Show that  $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  has order 4 and  $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$  has order 3, but  $ab$  has infinite order. Conversely, show that the additive group  $Z_2 \oplus \mathbf{Z}$  contains nonzero elements  $a, b$  of infinite order such that  $a + b$  has finite order.

**Answer.** The verification of  $|a| = 4$  and  $|b| = 3$  is trivial.  $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$   
 $\det(ab = \lambda I) = 0 \Rightarrow \lambda_1 = \lambda_2 = 1$ .  $ab$  is not diagonalizable. By induction, we have  $(ab)^n = \begin{pmatrix} 1 & 2^{n-1} \\ 0 & 1 \end{pmatrix}$  which means  $(ab)$  has infinite order.  
 For  $a = (\bar{0}, 1), b = (\bar{0}, -1) \in Z_2 \oplus \mathbf{Z}$ ,  $a, b$  have infinite order, but  $a + b = (\bar{0}, 0)$  has finite order 1.

**Exercise 1.3.6.** If  $G$  is a cyclic group of order  $n$  and  $k|n$ , then  $G$  has exactly one subgroup of order  $k$ .

**Answer.** Assume  $a^n = e$ ,  $mk = n$ , we verify that  $\langle a^m \rangle$  is a subgroup of order  $k$ .  $\forall x, y \in \mathbf{Z}_+$ ,  $a^{xm} \cdot a^{-ym} = a^{(x-y)m} \in \langle a^m \rangle$ , so  $\langle a^m \rangle$  is a subgroup.  $a^{km} = e$ ,  $a^{sm} \neq e$  for  $s < k$ , so  $|\langle a^m \rangle| = k$ .

**Exercise 1.3.7.** Let  $p$  be prime and  $H$  a subgroup of  $Z(p^\infty)$ .

- (a) Every element of  $Z(p^\infty)$  has finite order  $p^n$  for some  $n \geq 0$ .
- (b) If at least one element of  $H$  has order  $p^k$  and no element of  $H$  has order greater than  $p^k$ , then  $H$  is the cyclic subgroup generated by  $1/\bar{p}^k$ , whence  $H \cong Z_{p^k}$ .

- (c) If there is no upper bound on the orders of elements of  $H$ , then  $H = Z(p^\infty)$ .
- (d) The only proper subgroups of  $Z(p^\infty)$  are the finite cyclic groups  $C_n = \langle 1/\bar{p}^n \rangle$  ( $n = 1, 2, \dots$ ). Furthermore,  $\langle 0 \rangle = C_0 < C_1 < C_2 < C_3 < \dots$ .
- (e) Let  $x_1, x_2, \dots$  be elements of an abelian group  $G$  such that  $|x_1| = p, px_2 = x_1, px_3 = x_2, \dots, px_{n+1} = x_n, \dots$ . The subgroup generated by the  $x_i (i \geq 1)$  is isomorphic to  $Z(p^\infty)$ .

**Answer.** (a)  $\forall x \in Z(p^\infty), x = \frac{a}{p^n}$  where  $a < p^n, p \nmid a$ .  $p$  is a prime, so  $\gcd(p, a) = 1$ .  $m \cdot a | p^n \Rightarrow m = p^n$ . Thus  $m \cdot \frac{a}{p^n} = e$ ,  $p^n$  is the smallest number satisfies it.  $\frac{a}{p^n}$  has order  $p^n$ .

- (b) For all  $x \in Z(p^\infty)$ , if  $x$  has order smaller than  $p^k$ ,  $x$  must have the form  $x = \frac{a}{p^i} (i \leq k)$ ,  $(p, a) = 1$ , so  $x \in \langle \frac{1}{p^k} \rangle$ . If not, assume  $x = \frac{a}{p^i} (i > k)$ , then  $p^k \cdot x = \frac{a}{p^{i-k}} \neq 1$ .
- (c) Assume not,  $H < Z(p^\infty), H \neq Z(p^\infty)$ . There exist  $y \in H$  s.t.  $y$  has order  $p^m, m \geq n$ .  $y = \frac{b}{p^m}, (p, b) = 1$ , so there exists  $b^{-1} \in \{1, 2, \dots, p-1\}$ ,  $bb^{-1} \equiv 1 \pmod{p^m}$ . But  $ab^{-1}p^{m-n}y = \frac{a}{p^n} = x \in H$ , that's contradictory! Conversely,  $H = Z(p^\infty)$ .
- (d) From (b), we know that if there's least upper bound  $p^n$  for elements in a subgroup  $S$ , then  $S = C_n$ .

$$\langle 0 \rangle = C_0 < C_1 < C_2 < C_3 < \dots < Z(p^\infty)$$

is easy to verify.

- (e) We can verify that  $f : x_i \mapsto \frac{1}{p^i}$  is a well defined isomorphism.  $f(e) = f(px_1) = 1, f(px_{i+1}) = f(x_i) = \frac{1}{p^i} = p \cdot \frac{1}{p^{i+1}}$ .  $f$  is obviously a bijection, so  $H \cong Z(p^\infty)$ .

**Exercise 1.3.8.** A group that has only a finite number of subgroups must be finite.

**Answer.** Suppose not. If the order of all subgroups are finite,  $G$  must be finite. So there exists a infinite subgroup  $H < G$ .  $\forall a \in G$ , if  $\forall n \in \mathbf{N}, a^n \neq e$ . then we can construct infinite subgroups  $\langle a \rangle, \langle a^2 \rangle, \langle a^3 \rangle, \dots$ . If  $\forall a \in G, \exists n \in \mathbf{N}, a^n = e$ , so  $\langle a \rangle$  is a proper subgroup of  $G$ , we can take  $b \in G \ni \langle a \rangle$  to construct another subgroup. By induction, there are infinite subgroups in  $G$ . That's contradictory, so  $G$  must be finite.

**Exercise 1.3.9.** If  $G$  is an abelian group, then the set  $T$  of all elements of  $G$  with finite order is a subgroup of  $G$ .

**Answer.** We can easily verify that  $\forall a, b \in T, |a| = m, |b| = n$  and  $|ab^{-1}| \leq mn$  is finite.  $T$  is a subgroup of  $G$ .

**Exercise 1.3.10.** An infinite group is cyclic if and only if it is isomorphic to each of its proper subgroups.

**Answer.** If  $G$  is cyclic,  $G \cong \mathbf{Z}$ ,  $S < G$ . For any subgroup of  $\mathbf{Z}$ , it has the form  $\{na\}, a \in \mathbf{Z}$ . We can construct a isomorphism  $f : n \mapsto na$ , so  $S \cong \{na\} \Rightarrow G \cong S$ .

If  $\forall S < G, G \cong S$  and  $|G| = |S|$  is finite. We prove there exists  $S < G$  s.t.  $|S| = \aleph_0$ . Take  $a \in G$  and  $S = \{na | n \in \mathbf{Z}\}$ ,  $S$  is a subgroup. If there exists  $ma = 0$ ,  $S$  must be finite, contradictory! Thus,  $S \cong \mathbf{Z} \cong G$ .  $G$  is a infinite cyclic group.

## 1.4 Cosets and counting

**Exercise 1.4.1.** Let  $G$  be a group and  $\{H_i | i \in I\}$  a family of subgroups. Then for any  $a \in G$ ,  $(\bigcap_i H_i)a = \bigcap_i H_i a$ .

**Answer.**  $\bigcap_i H_i$  is a subgroup of  $G$ . Take  $x \in \bigcap_i H_i$ ,  $x \in H_i$ ,  $\forall i \in I$ . Then  $xa \in H_i a$ ,  $\forall i \in I$ , so  $xa \in \bigcap_i (H_i a)$ . Thus,  $(\bigcap_i H_i)a = \bigcap_i (H_i a)$ .

**Exercise 1.4.2.** (a) Let  $H$  be the cyclic subgroup (of order 2) of  $S_3$  generated by  $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ . Then no left cosets of  $H$  (except  $H$  itself) is also a right coset. There exists  $a \in S_3$  such that  $aH \cap Ha = \{a\}$ .

(b) If  $K$  is the cyclic subgroup (of order 3) of  $S_3$  generated by  $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ , then every left coset of  $K$  is also a right coset of  $K$ .

**Answer.** (a)  $H = \{(12), (1)\}$ .  $S_3 = \{(12), (13), (23), (1), (123), (132)\}$ . For  $a \in H$ ,  $aH = Ha = H$ .

$a = (13)$ ,  $aH = \{(13), (123)\}$ ,  $Ha = \{(13), (132)\}$ .

$a = (23)$ ,  $aH = \{(23), (132)\}$ ,  $Ha = \{(23), (123)\}$ .

$a = (123)$ ,  $aH = \{(123), (23)\}$ ,  $Ha = \{(132), (13)\}$ .

$a = (132)$ ,  $aH = \{(132), (13)\}$ ,  $Ha = \{(123), (23)\}$ .

(b)  $K = \{(123), (132), (1)\}$ . For  $a \in K$ ,  $aK = Ka = K$ .

$a = (12)$ ,  $aK = Ka = \{(12), (23), (13)\}$ .

$a = (13)$ ,  $aK = Ka = \{(12), (23), (13)\}$ .

$a = (23)$ ,  $aK = Ka = \{(12), (23), (13)\}$ .

**Exercise 1.4.3.** The following conditions on a finite group  $G$  are equivalent.

(i)  $|G|$  is prime.

(ii)  $G \neq \langle e \rangle$  and  $G$  has no proper subgroups.

(iii)  $G \cong Z_p$  for some prime  $p$ .

**Answer.** (i) $\Rightarrow$ (ii): If there exists  $S < G$ ,  $S \neq G$ , then  $|S| \mid |G| = p$ . That's contradictory!

(ii) $\Rightarrow$ (iii):  $\forall a \in G$ , take  $S = \{na | n = 1, 2, \dots, p\}$ . If there exists  $ma = na$ ,  $(1 \leq m < n \leq p)$ ,  $(n - m)a = 0$ . So there exists subgroup  $S$ , and  $|S| = n - m < p$ . That's contradictory! So  $S < G$ ,  $|S| = |G| \Rightarrow S = G \cong Z_p$ .

(iii) $\Rightarrow$ (i): Trivial.

**Exercise 1.4.4.** Let  $a$  be an integer and  $p$  be a prime such that  $p \nmid a$ . Then  $a^{p-1} \equiv 1 \pmod{p}$ .

**Answer.**  $(Z_p \setminus \{\bar{0}\}, \times)$  is a group of order  $p - 1$ . From **Exercise 1.1.7**, we know that  $\forall \bar{a} \in Z_p \setminus \{\bar{0}\}$  and  $b \in Z_p \setminus \{\bar{0}\}$ , taking different  $\bar{b}$  we will have different  $\bar{a}\bar{b} \in Z_p \setminus \{\bar{0}\}$ .  $\bar{a}\bar{b}$  travels through all the elements in  $Z_p \setminus \{\bar{0}\}$ . So

$$\prod_{i=1}^{p-1} (\bar{i} \cdot \bar{a}) = \prod_{i=1}^{p-1} \bar{i}$$

By the definition of  $Z_p \setminus \{\bar{0}\}$ ,  $Z_p \setminus \{\bar{0}\}$  is commutative. So

$$(\bar{a})^{p-1} \left( \prod_{i=1}^{p-1} \bar{i} \right) = \prod_{i=1}^{p-1} \bar{i} \Rightarrow (\bar{a})^{p-1} = \bar{1}$$

**Exercise 1.4.5.** Prove that there are only two distinct groups of order 4 (up to isomorphism), namely  $Z_4$  and  $Z_2 \oplus Z_2$ .

**Answer.** The only cyclic group of order 4 is  $Z_4$ . For a group  $G$  of order 4 which is not cyclic,  $\forall a \in G, a \neq e$ , if  $|a| = 2$ ,  $G \cong Z_2 \oplus Z_2$ . If there exists  $a \in G, |a| = 4$ ,  $G \cong Z_4$ . If there exists  $a \in G, |a| = 3$ , denote  $a^2 = b, a^3 = e$ . Then  $b^2 = a^4 = a$ ,  $\{e, a, b\} < G$ , which is contradictory to the Lagrange theorem.

**Exercise 1.4.6.** Let  $H, K$  be subgroups of a group  $G$ . Then  $HK$  is a subgroup of  $G$  if and only if  $HK = KH$ .

**Answer.** If  $HK = KH$ , for  $a_1b_1, a_2b_2 \in HK$ ,

$$(a_1b_1)(a_2b_2)^{-1} = (a_1b_1)(b_2^{-1}a_2^{-1}) = (a_1b_1)(a_3b_3)$$

since  $b_2^{-1}a_2^{-1} \in KH = HK$ , there exists  $b_2^{-1}a_2^{-1} = a_3b_3$ .

$$(a_1b_1)(a_3b_3) = a_1(b_1a_3)b_3 = a_1a_4b_4b_3$$



since  $b_1a_3 \in KH = HK$ , there exists  $b_1a_3 = a_4b_4$ .  $(a_1b_1)(a_2b_2)^{-1} = a_1a_4b_4b_3 = a_5b_5 \in HK$ . Thus  $HK$  is a subgroup of  $G$ .

If  $HK$  is a subgroup of  $G$ ,  $\forall b_1a_1 \in KH$ , there exists  $(a_1^{-1}b_1^{-1}) \in HK$  s.t.  $b_1a_1 = (a_1^{-1}b_1^{-1})^{-1} \in HK$ . So  $KH \subset HK$ .  $\forall a_1b_1 \in HK$ ,  $(a_1b_1)^{-1} = b_1^{-1}a_1^{-1} \in HK$ , so  $\exists a_2b_2 \in HK$  s.t.  $b_1^{-1}a_1^{-1} = a_2b_2$ .  $a_1b_1 = b_2^{-1}a_2^{-1} \in KH$ . So  $HK \subset KH$ . Thus  $HK = KH$ .

**Exercise 1.4.7.** Let  $G$  be a group of order  $p^k m$ , with  $p$  prime and  $(p, m) = 1$ . Let  $H$  be a subgroup of order  $p^k$  and  $K$  a subgroup of order  $p^d$ , with  $0 < d \leq k$  and  $K \not\subset H$ . Show that  $HK$  is not a subgroup of  $G$ .

**Answer.** Assume  $HK < G$ ,  $|HK| = p^k n$ ,  $n|m$ . We can get  $[HK : H] = n = [K : K \cap H]$ .  $[K : K \cap H] | p^k \Rightarrow n | p^k$ . That's contradictory to  $(m, p^k) = 1$ .

**Exercise 1.4.8.** If  $H$  and  $K$  are subgroups of finite index of a group  $G$  such that  $[G : H]$  and  $[G : K]$  are relatively prime, then  $G = HK$ .

**Answer.** Assume  $[G : H] = m$ ,  $[G : K] = n$ ,  $(m, n) = 1$ . Then  $|H| = np$ ,  $|K| = mp$ .  $H \cap K < H$ ,  $H \cap K < G \Rightarrow |H \cap K| | p$ .

$$[G : H] = m \geq [K : H \cap K] = \frac{|K|}{|H \cap K|} \geq m$$

Thus  $[G : H] = [K : H \cap K] = m$ ,  $G = HK$ .

**Exercise 1.4.9.** If  $H, K$  and  $N$  are subgroups of a group  $G$  such that  $H < N$ , then  $HK \cap N = H(K \cap N)$ .

**Answer.**  $\forall x = hk \in HK \cap N$ ,  $\exists h_1^{-1} \in H$  s.t.  $h_1^{-1}hk \in K \cap N$ .  $H < N$  so  $\forall h_1^{-1} \in H$ ,  $h_1^{-1}hk \in N$ . Take  $h_1^{-1} = h^{-1}$ ,  $h_1^{-1}hk = k \in K$ . So  $HK \cap N \subset H(K \cap N)$ .

$\forall x = hk \in H(K \cap N)$  where  $h \in H$ ,  $k \in K \cap N$ .  $hk \in HK$ ,  $h, k \in N \Rightarrow hk \in N$ . So  $H(K \cap N) \subset HK \cap N$ .

Thus,  $HK \cap N = H(K \cap N)$ .

**Exercise 1.4.10.** Let  $H, K, N$  be subgroups of a group  $G$  such that  $H < K$ ,  $H \cap N = K \cap N$ , and  $HN = KN$ . Show that  $H = K$ .

**Answer.** Assume there exists  $x \in K \setminus H$ .  $K \bigcup_{i \in I} Ha_i$ ,  $\forall h_i \in H$  there exists  $a \in K$  s.t.  $x = h_1a$ . Take  $n_1 \in N$ . Since  $HN = KN$ ,  $xn_1 \in HN$ , there exists  $h_2 \in H$ ,  $n_2 \in N$  s.t.  $xn_1 = h_2n_2 = h_2an_1$ . So  $a = n_2n_1^{-1} \in N$ ,  $a \in K \cap N = H \cap N \Rightarrow a \in H, x \in H$ . That's contradictory!

**Exercise 1.4.11.** Let  $G$  be a group of order  $2n$ ; then  $G$  contains an element of order 2. If  $n$  is odd and  $G$  abelian, there is only one element of order 2.

**Answer.** The proof of the first part is exactly the same as **Exercise 1.1.14**. Assume there exists  $a, b \in G$ ,  $a^2 = b^2 = e$ . We can check  $H = \{e, a, b, ab\}$  is a subgroup of  $G$ .  $|H| \mid |G| \Rightarrow 4 \mid 2n \Rightarrow 2 \mid n$ , which is contradictory to  $n$  is odd. So there's only one element  $a$  s.t.  $a^2 = e$ .

**Exercise 1.4.12.** If  $H$  and  $K$  are subgroups of a group  $G$ , then  $[H \vee K : H] \geq [K : H \cap K]$ .

**Answer.** The question is a direct corollary of Proposition 4.8.

**Exercise 1.4.13.** If  $p > q$  are primes, a group of order  $pq$  has at most one subgroup of order  $p$ .

**Answer.**  $H \cap K < H$ ,  $H \cap K < K$ ,  $H \neq K \neq H \cap K$ .  $|H \cap K| \mid p$  and  $|H \cap K| \neq q$ , so  $H \cap K = \{e\}$ . From **Exercise 1.3.12**,

$$[H \vee K : H] \geq [K : K \cap H] = p$$

$$|H \vee K| = |H| \cdot [H \vee K : H] \geq p^2$$

But  $H \vee K \in G$ ,  $|H \vee K| \leq pq < p^2$ . That's contradictory!

**Exercise 1.4.14.** Let  $G$  be a group and  $a, b \in G$  such that (i)  $|a| = 4 = |b|$ ; (ii)  $a^2 = b^2$ ; (iii)  $ba = a^3b = a^{-1}b$ ; (iv)  $a \neq b$ ; (v)  $G = \langle a, b \rangle$ . Show that  $|G| = 8$  and  $G \cong Q_8$ .

**Answer.** The proof is exactly the same as **Exercise 1.2.3**.

## 1.5 Normality, quotient groups, and homomorphisms

**Exercise 1.5.1.** If  $N$  is a subgroup of index 2 in a group  $G$ , then  $N$  is normal in  $G$ .

**Answer.**  $\forall a \in G \setminus N, G = N \cup Na = N \cup aN$  and  $N \cap Na = \emptyset, N \cap aN = \emptyset$ . So  $\forall x \in Na, x \in G \setminus N \Rightarrow x \in aN, Na \subset aN$ . Similarly,  $aN \subset Na$ , whence  $Na = aN, N \triangleleft G$ .

**Exercise 1.5.2.** If  $\{N_i | i \in I\}$  is a family of normal subgroups of a group  $G$ , then  $\bigcap_{i \in I} N_i$  is a normal subgroup of  $G$ .

**Answer.**  $\bigcap_{i \in I} N_i$  is a subgroup of  $G$ .  $N_i (i \in I)$  are normal subgroups of  $G$ , so  $\forall a \in G, aN_i a^{-1} = \{an_i a^{-1} | n_i \in N_i\} = N_i$ .  $\forall x = ana^{-1} \in a(\bigcap_{i \in I} N_i)a^{-1}$ ,  $n \in N_i \Rightarrow x \in a(\bigcap_{i \in I} N_i)a^{-1} \subset \bigcap_{i \in I} aN_i a^{-1} = \bigcap_{i \in I} N_i$ .  $\bigcap_{i \in I} N_i$  are normal subgroup of  $G$ .

**Exercise 1.5.3.** Let  $N$  be a subgroup of a group  $G$ .  $N$  is normal in  $G$  if and only if (right) congruence modulo  $N$  is a congruence relation on  $G$ .

**Answer.** If  $N \triangleleft G$ .  $\forall a, b \in G, ab^{-1} \in N \Leftrightarrow a^{-1}b \in N$ . If  $a_1 \equiv b_1 \pmod{N}, a_2 \equiv b_2 \pmod{N}$ , then  $a_2 b_2^{-1} \in N, a_1 N = Na_1 = Nb_1 \Rightarrow a_1 N b_1^{-1} = N$ . So  $a_1 a_2 b_1^{-1} b_2^{-1} = (a_1 a_2)(b_1 b_2)^{-1} \in N$ . Similarly,  $(a_1 a_2)^{-1}(b_1 b_2) \in N$ . Congruence modulo  $N$  is a congruence relation.

If congruence modulo  $N$  is a congruence relation.  $\forall a_1 \equiv b_1 \pmod{N}, a_2 \equiv b_2 \pmod{N}$ , we will have  $a_1 a_2 \equiv b_1 b_2 \pmod{N}$ . Take  $n \in N$  and fix  $a_2 \in G$ , define  $b_2 = n^{-1} a_2$ . Then  $\forall n \in N, n$  can be expressed as  $a_2 b_2^{-1}, a_2 \equiv b_2 \pmod{N}$ .  $\forall a_1 \in G$  and  $\forall b_1 \equiv a_1 \pmod{N}, a_1 n b_1^{-1} = a_1 a_2 b_2^{-1} b_1^{-1} \in N$ . Take  $b_1 = a_1$  and  $n$  varies in  $N, a_1 n a_1^{-1} \in N \Rightarrow a_1 N a_1^{-1} \subset N$ . Thus  $N \triangleleft G$ .

**Exercise 1.5.4.** Let  $\sim$  be an equivalence relation on a group  $G$  and let  $N = \{a \in G | a \sim e\}$ . Then  $\sim$  is a congruence relation on  $G$  if and only if  $N$  is a normal subgroup of  $G$  and  $\sim$  is congruence modulo  $N$ .

**Answer.** If  $G \triangleleft N$  and  $\sim$  is congruence modulo  $N$ .  $\forall a \in G$ ,  $aNa^{-1} \subset N$ .  $\forall a_1, b_1, a_2, b_2 \in G$ ,  $a_1b_1^{-1} \in N$ ,  $a_2b_2^{-1} \in N$ .  $a_1a_2(b_1b_2)^{-1} = a_1a_2b_2^{-1}b_1^{-1}$ , denote  $n = a_2b_2^{-1} \in N$ ,  $a_1a_2b_2^{-1}b_1^{-1} = a_1nb_1^{-1} \in a_1Nb_1^{-1}$ .  $\forall n \in N$ , there exists  $n' = b_1^{-1}a_1, n' \in N$  s.t.  $a_1n = b_1n'$ . So  $a_1nb_1^{-1} = b_1n'b_1^{-1} \in b_1Nb_1^{-1} \subset N$ . That means  $(a_1a_2)(b_1b_2)^{-1} \in N$ ,  $a \sim b$  is a congruence relation.

If  $a \sim b$  is a congruence relation. We first prove  $N$  is a subgroup of  $G$ .  $\forall a \in N$ ,  $a \sim e$ ,  $a^{-1} \sim a^{-1} \Rightarrow e \sim a^{-1}$ , so  $a^{-1} \sim e$ ,  $a^{-1} \in N$ .  $\forall a, b \in N$ ,  $b^{-1} \sim e$ ,  $a \sim e \Rightarrow ab^{-1} \in e$ , thus  $N < G$ .

$\forall x \in G$ ,  $xN = \{xa | a \sim e\} = \{xa | xa \sim xe\} = \{ax | ax \sim e\} = Nx$ , so  $N$  is normal in  $G$ .  $x \sim y \Leftrightarrow y \in xN$ .  $\sim$  is congruence modulo  $N$ .

**Exercise 1.5.5.** Let  $N < S_4$  consist of all those permutations  $\sigma$  such that  $\sigma(4) = 4$ . Is  $N$  normal in  $S_4$ ?

**Answer.**  $N = \{(1), (12), (13), (23), (123), (132)\}$ . Take  $a = (14) \in G$ ,  $a^{-1} = (14)$ ,  $a^{-1}(12)a = (24) \notin N$ . So  $N$  is not normal in  $S_4$ .

**Exercise 1.5.6.** Let  $H < G$ ; then the set  $aHa^{-1}$  is a subgroup for each  $a \in G$ , and  $H \cong aHa^{-1}$ .

**Answer.**  $H < G$ ,  $aHa^{-1} = \{aha^{-1} | h \in H\}$ .  $\forall x, y \in aHa^{-1}$ ,  $x = ah_1a^{-1}$ ,  $y = ah_2a^{-1}$ .  $y^{-1} = ah_2^{-1}a^{-1}$ ,  $xy = ah_1h_2^{-1}a^{-1} \in aHa^{-1}$ , so  $aHa^{-1} < G$ . Take  $f : H \rightarrow aHa^{-1}$  as  $f(h) = aha^{-1}$ . If  $f(h_1) = f(h_2) = ah_1a^{-1} = ah_2a^{-1}$ , then  $h_1 = h_2$ , so  $f$  is an injection.  $f$  is a surjection because  $\forall x \in aHa^{-1}$ ,  $f(a^{-1}xa) = x$ ,  $a^{-1}xa \in H$ . In conclusion,  $H \cong aHa^{-1}$ .

**Exercise 1.5.7.** Let  $G$  be a finite group and  $H$  a subgroup of  $G$  of order  $n$ . If  $H$  is the only subgroup of  $G$  of order  $n$ , then  $H$  is normal in  $G$ .

**Answer.** Applying **Exercise 1.5.6**,  $\forall a \in G$ ,  $aHa^{-1} \cong H$ .  $|aHa^{-1}| = |H| = n \Rightarrow aHa^{-1} = H$ . Whence  $H \triangleleft G$ .

**Exercise 1.5.8.** All subgroups of the quaternion group are normal.

**Answer.**  $Q_8 = \{a, b, a^2, ba, ab, a^2b, ab^2, a^2b^2\}$  where  $a^2 = b^2$ ,  $a_1b = ba = a^3b$  and  $|a| = |b| = 4$ . There are several subgroups  $\{a, a^2, ab^2, a^2b^2\}$ ,  $\{b, a^2, a^2b, a^2b^2\}$ ,  $\{ab, a^2b^2\}$ ,  $\{ba, a^2b^2\}$ ,  $\{a^2, a^2b^2\}$ . From **Exercise 1.5.1**, we know the first two subgroups are normal in  $G$ . For  $\{ab, a^2b^2\}$ ,  $\{ba, a^2b^2\}$ ,  $\{a^2, a^2b^2\}$ , we can check that  $ab, ba, a^2$  is communicative in  $G$ , that is  $\forall x \in G, xabx^{-1} = ab, xba x^{-1} = ba, xa^2x^{-1} = a^2$ . They are all normal in  $G$ .

**Exercise 1.5.9.** (a) If  $G$  is a group, then the center of  $G$  is a normal subgroup of  $G$ ;

(b) the center of  $S_n$  is the identity subgroup for all  $n > 2$ .

**Answer.** (a) By the definition of center  $C$ ,  $\forall x \in G$  and  $a \in C$ ,  $ax = xa$ , so  $xCx^{-1} = C$ .  $C$  is normal in  $G$ .

(b)  $\forall x \in S_n$ ,  $x$  can be expressed as

$$x = (a_1a_2 \cdots a_{i_1})(a_{i_1+1}a_{i_1+2} \cdots a_{i_2}) \cdots (a_{i_{n-1}+1}a_{i_{n-1}+2} \cdots a_{i_n})$$

Those cycles  $(a_1a_2 \cdots a_{i_1})$ ,  $(a_{i_1+1}a_{i_1+2} \cdots a_{i_2})$ , ...,  $(a_{i_{n-1}+1}a_{i_{n-1}+2} \cdots a_{i_n})$  are all disjoint, so they are communicative.

If there exists cycles whose length is longer than 2. WLOG, assume  $i_1 > 2$ . Take  $y = (a_1a_2)$ ,

$$y^{-1}xy = (a_1a_2)(a_1a_2 \cdots a_{i_1})(a_1a_2) \cdots (a_{i_{n-1}+1}a_{i_{n-1}+2} \cdots a_{i_n})$$

$(a_1a_2)(a_1a_2 \cdots a_{i_1})(a_1a_2) = (a_2a_1a_3 \cdots a_{i_1})$ , so  $y^{-1}xy \neq x$ ,  $x \notin C$ .

If  $x = (a_1a_2)(a_3a_4) \cdots (a_{2n-1}a_{2n})$  and  $n \geq 2$ . Take  $y = (a_1a_3)$ ,

$$\begin{aligned} y^{-1}xy &= (a_1a_3)(a_1a_2)(a_3a_4) \cdots (a_{2n-1}a_{2n})(a_1a_3) \\ &= (a_1a_3)(a_1a_2)(a_3a_4)(a_1a_3) \cdots (a_{2n-1}a_{2n}) \\ &= (a_1a_4)(a_2a_3) \cdots (a_{2n-1}a_{2n}) \\ &\neq x \end{aligned}$$

So  $x \notin C$ .

If  $x = (a_1a_2)$ . Take  $y = (a_1a_3)$ ,  $y^{-1}xy = (a_2a_3) \neq x$ , so  $x \notin C$ .

In conclusion,  $C = \{(1)\}$ .

**Exercise 1.5.10.** Find subgroups  $H$  and  $K$  of  $D_4^*$  such that  $H \triangleleft K$  and  $K \triangleleft D_4^*$ , but  $H$  is not normal in  $D_4^*$ .

**Answer.**  $D_4^* = \{I, R, R^2, R^3, T_x, T_y, T_{13}, T_{24}\}$ . Take  $K = \{I, R, T_x, T_y\}$ ,  $H = \{I, T_x\}$ . We can easily verify that  $H \triangleleft K$  and  $K \triangleleft D_4^*$  but  $K \not\triangleleft D_4^*$ .

**Exercise 1.5.11.** If  $H$  is a cyclic subgroup of a group  $G$  and  $H$  is normal in  $G$ , then every subgroup of  $H$  is normal in  $G$ .

**Answer.** Assume  $K < H \triangleleft G$ ,  $H$  has the generator  $a$ , and  $K$  has the generator  $a^n$ . Here we used: *Every subgroup of a cyclic group is cyclic.* This can be easily proved by the conclusion  $H \cong Z_m$  for some  $m \in \mathbf{Z}$ .  $\forall x \in G$ ,  $h = a^s \in H$ ,  $x^{-1}a^s x = a^t \in H$ . Assume  $x^{-1}ax = a^m$ , then  $x^{-1}a^n x = (x^{-1}ax)^n = a^{mn} = a^k$ , so  $n|k$ ,  $a^k \in K$ .  $x^{-1}Kx \subset K$ ,  $K$  is normal in  $G$ .

**Exercise 1.5.12.** If  $H$  is a normal subgroup of a group  $G$  such that  $H$  and  $G/H$  are finitely generated, then so is  $G$ .

**Answer.** Assume  $A = \{a_1, a_2, \dots, a_m\}$ ,  $B = \{b_1, b_2, \dots, b_n\}$ .  $H = \langle A \rangle$ ,  $G/H = \langle \{Hb_i | b_i \in B\} \rangle$ . We prove that  $G$  can be generated by  $A \cup B$ .  $\forall x \in G$ ,  $x$  is in one of the right cosets of  $H$ ,  $x \in Ha$ .  $Ha \in G/H$  so  $Ha = \prod_{b_i \in B} Hb_i^{s_i} = H(\prod_{b_i \in B} b_i^{s_i})$ . Thus  $a^{-1}(\prod_{b_i \in B} b_i^{s_i}) = a' \in H$ .  $H$  is generated by  $A$  so  $xa^{-1} = \prod_{a_i \in A} a_i^{t_i}$ ,  $a' = \prod_{a_i \in A} a_i^{-r_i}$ . Then

$$x = (\prod_{a_i \in A} a_i^{t_i + r_i})(\prod_{b_i \in B} b_i^{s_i}) \in \langle A \cup B \rangle$$

Thus  $G \subset \langle A \cup B \rangle$  is finitely generated.

**Exercise 1.5.13.** (a) Let  $H \triangleleft G$ ,  $K \triangleleft G$ . Show that  $H \vee K$  is normal in  $G$ .  
 (b) Prove that the set of all normal subgroups of  $G$  forms a complete lattice under inclusion.

**Answer.** (a)  $\forall x \in G, a \in H \vee K$ , we need to prove  $x^{-1}ax \in H \vee K$ .  
 $a \in H \vee K$  so  $a$  can be expressed as

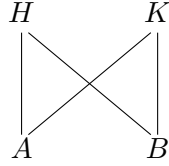
$$a = b_1^{n_1} b_2^{n_2} \cdots b_t^{n_t} \quad \text{where } b_i \in H \text{ or } b_i \in K, i = 1, 2, \dots, t$$

so  $x^{-1}ax = x^{-1}b_1^{n_1} \cdots b_t^{n_t}x = (x^{-1}b_1x)^{n_1} (x^{-1}b_2x)^{n_2} \cdots (x^{-1}b_tx)^{n_t}$ .  
 $H \triangleleft G, K \triangleleft G$ , so  $x^{-1}b_ix \in H \vee K, i = 1, 2, \dots, t$  and

$$x^{-1}ax = (x^{-1}b_1x)^{n_1} (x^{-1}b_2x)^{n_2} \cdots (x^{-1}b_tx)^{n_t} \in H \vee K$$

$H \vee K \triangleleft G$ .

(b) Actually, in **Exercise 1.2.19** and (a), we have proved lub exists.  
 Now we only consider glb. For  $H \triangleleft G, K \triangleleft G$ . If  $H \cap K \triangleleft G$ , then their glb is  $H \cap K$ . If not, assume there exists  $A < H \cap K, B < H \cap K, A, B$  are both normal in  $H$  and  $K$ . And there doesn't exist  $I$  s.t.  $A \triangleleft I \triangleleft H, A \triangleleft I \triangleleft K, B \triangleleft I \triangleleft H, B \triangleleft I \triangleleft K$ . Just like the figure:



But  $A < H \cap K, B < H \cap K \Rightarrow A \vee B < H \cap K$ . So  $A \vee B \triangleleft H, A \vee B \triangleleft K$ . That's contradictory! There is only one lower bound for  $\{H, K\}$ . Notice that  $\{e\} < H \cap K$  so there exists at least one subgroup satisfies the condition. We have proved normality forms a lattice.

**Exercise 1.5.14.** If  $N_1 \triangleleft G_1, N_2 \triangleleft G_2$  then  $(N_1 \times N_2) \triangleleft (G_1 \times G_2)$  and  $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$ .

**Answer.** Take  $a \in (N_1 \times N_2), a = (n_1, n_2)$  where  $n_1 \in N_1, n_2 \in N_2$ .  
 $\forall x \in (G_1 \times G_2), x = (g_1, g_2)$  where  $g_1 \in G_1, g_2 \in G_2$ .  $x^{-1} = (g_1^{-1}, g_2^{-1})$ ,  
 $x^{-1}ax = (g_1^{-1}n_1g_1, g_2^{-1}n_2g_2)$ .  $N_1 \triangleleft G_1, N_2 \triangleleft G_2$ , so  $g_1^{-1}n_1g_1 \in N_1, g_2^{-1}n_2g_2 \in N_2$ .  
 $x^{-1}ax \in (N_1 \times N_2)$ . Thus  $(N_1 \times N_2) \triangleleft (G_1 \times G_2)$ .

Assume  $G_1 = \bigcup_{i \in I} N_1 a_i, G_2 = \bigcup_{j \in J} N_2 b_j$ . Then  $G_1 \times G_2 = \bigcup_{i \in I} N_1 a_i \times \bigcup_{j \in J} N_2 b_j$ .

Denote  $A = \{a_i | i \in I\}, B = \{b_j | j \in J\}$ . We construct two bijections  $(G_1 \times G_2)/(N_1 \times N_2) \rightarrow A \times B$  and  $(G_1/N_1) \times (G_2/N_2)$ .

$$f : N_1 a_i \times N_2 b_j \mapsto (a_i, b_j)$$



$$g : (N_1 a_i, N_2 b_j) \mapsto (a_i, b_j)$$

Take  $h = g^{-1} \circ f$ ,  $f, g$  are bijections, so  $h$  is an isomorphism.  $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$ .

**Exercise 1.5.15.** Let  $N \triangleleft G$  and  $K \triangleleft G$ . If  $N \cap K = \langle e \rangle$  and  $N \vee K = G$ , then  $G/N \cong K$ .

**Answer.** Assume  $G = \bigcup_{i \in I} N a_i$ , we construct  $f : k \rightarrow G/N$ . We prove that  $\forall x, y \in K$ ,  $x, y$  belong to different cosets of  $N$ . Suppose not.  $\exists x, y \in K$ ,  $x, y \in N a_i$ , then  $xy^{-1} \in N \Rightarrow x = y$ . That's contradictory! So  $f$  is a monomorphism.

$G = H \vee K$ , so  $G = HK$ . we can write  $x$  as  $pq$ , where  $p \in H$ ,  $q \in K$ .  $|G/H| = [G : H] = [HK : H] = [K : K \cap H] = |K|$ .  $f$  is an epimorphism. Thus,  $G/N \cong K$ .

**Exercise 1.5.16.** If  $f : G \rightarrow H$  is a homomorphism,  $H$  is abelian and  $N$  is a subgroup of  $G$  containing  $\text{Ker } f$ , then  $N$  is normal in  $G$ .

**Answer.** Assume there exists  $x \in G$ ,  $x \notin N$  s.t.  $f(x) \in f(N)$ .  $\exists n \in N$ ,  $f(x) = f(n)$ ,  $f(xn^{-1}) = f(x)f(n)^{-1} = e' \Rightarrow xn^{-1} \in \text{Ker } f \Rightarrow x \in N$ . That's contradictory!  $\forall x \in G$ ,  $n \in N$ ,  $f(x^{-1}nx) = f(x^{-1})f(n)f(x) = f(n) \in f(N)$ , so  $x^{-1}nx \in N$ . Thus,  $N \triangleleft G$ .

**Exercise 1.5.17.** (a) Consider the subgroups  $\langle 6 \rangle$  and  $\langle 30 \rangle$  of  $\mathbf{Z}$  and show that  $\langle 6 \rangle / \langle 30 \rangle \cong Z_5$ .

(b) For any  $k, m > 0$ ,  $\langle k \rangle / \langle km \rangle \cong Z_m$ ; in particular,  $\mathbf{Z} / \langle m \rangle = \langle 1 \rangle / \langle m \rangle \cong Z_m$ .

**Answer.** (a)  $\langle 6 \rangle = \{6n | n \in \mathbf{Z}\}$ ,  $\langle 30 \rangle = \{30n | n \in \mathbf{Z}\}$ . So  $\langle 6 \rangle / \langle 30 \rangle = \{\langle 30 \rangle, \langle 30 \rangle + 6, \langle 30 \rangle + 12, \langle 30 \rangle + 18, \langle 30 \rangle + 24\} \cong Z_5$

(b)  $\langle km \rangle \triangleleft \langle k \rangle$ ,  $\langle k \rangle = \bigcup_{i \in I} (\langle km \rangle + a_i)$ . For  $x \in \langle k \rangle$ ,  $x \equiv a_i \pmod{km}$ , then  $x \in \langle km \rangle + a_i$ .  $f : \langle k \rangle / \langle km \rangle \rightarrow \{a_i | i \in I\}$  defined by  $f(\langle km \rangle + a_i) = a_i$  is a bijection. We check that  $g : \{a_i | i \in I\} \rightarrow Z_m$  is also a bijection. Define

$b_i \equiv \frac{a_i}{k} \pmod{m}$ ,  $g(a_i) = b_i$ . If there exists  $b_i = b_j$  for  $i \neq j$ ,  $a_i \equiv a_j \pmod{km}$ . That's contradictory! So  $g$  is an injection.  $g$  is obviously a surjection, so  $g$  is a bijection. Take  $h = g \circ f : \langle k \rangle / \langle km \rangle \rightarrow Z_m$  is an isomorphism, so  $\langle k \rangle / \langle km \rangle \cong Z_m$ .

**Exercise 1.5.18.** If  $f : G \rightarrow H$  is a homomorphism with kernel  $N$  and  $K < G$ , then prove that  $f^{-1}(f(K)) = KN$ . Hence  $f^{-1}(f(K)) = K$  if and only if  $N < K$ .

**Answer.** Take  $x \in f^{-1}(f(K))$ , then there exists  $k \in K$  s.t.  $f(x) = f(k)$ .  $f(xk^{-1}) = f(x)f(k)^{-1} = e' \in f(K) \Rightarrow xk^{-1} \in \text{Ker } f = N$ . Thus,  $x \in Nk \subset NK$ ,  $f^{-1}(f(K)) \subset NK$ .

$\forall x = nk \in NK$ , where  $n \in N$  and  $k \in K$ .  $f(x) = f(n)f(k) = e'f(k) \in f(K)$ , so  $NK \subset f^{-1}(f(K))$ .

Thus,  $f^{-1}(f(K)) = NK$ . Hence  $f^{-1}(f(K)) = K$  if and only if  $N < K$ .

**Exercise 1.5.19.** If  $N \triangleleft G$ ,  $[G : H]$  finite,  $H < G$ ,  $|H|$  finite, and  $[G : N]$  and  $|H|$  are relatively prime, then  $H < N$ .

**Answer.**  $N \triangleleft G \Rightarrow NH < G$ . By the second isomorphism theorem,  $NH/N \cong H/H \cap N \Rightarrow [NH : N] = [H : H \cap N]$ . Assume  $[G : N] = m$ ,  $|H| = n$ ,  $|G| = mnp$  where  $(m, n) = 1$ . Then  $|N| = np$ ,  $N < NH$ , assume  $|NH| = knp$ ,  $NH < G \Rightarrow knp | mnp \Rightarrow k | m$ .  $[NH : N] = [H : H \cap N] = k \Rightarrow k | n$ . So  $k = 1$ ,  $NH = N$  which means  $H < N$ .

**Exercise 1.5.20.** If  $N \triangleleft G$ ,  $|N|$  finite,  $H < G$ ,  $[G : N]$  finite, and  $[G : H]$  and  $|N|$  are relatively prime, then  $N < H$ .

**Answer.**  $N \triangleleft G \Rightarrow NH < G$ . By the second isomorphism theorem,  $NH/N \cong H/H \cap N \Rightarrow [NH : N] = [H : H \cap N]$ . Assume  $[G : H] = m$ ,  $|N| = n$ ,  $|G| = mnp$  where  $(m, n) = 1$ . Then  $|H| = np$ ,  $H < NH$ , assume  $|NH| = knp$ ,  $NH < G \Rightarrow knp | mnp \Rightarrow k | m$ .  $[NH : N] = [H : H \cap N] = kp \Rightarrow kp | np \Rightarrow k | n$ . So  $k = 1$ ,  $NH = H$  which means  $N < H$ .

**Exercise 1.5.21.** If  $H$  is a subgroup of  $Z(p^\infty)$  and  $H \neq Z(p^\infty)$ , then  $Z(p^\infty)/H \cong Z(p^\infty)$ .

**Answer.** From **Exercise 1.3.7(b)**, we know that  $H$  has the form  $\langle \frac{\bar{1}}{p^n} \rangle$ .

Take  $x_i = \frac{\bar{1}}{p^{n+i}} + H$ ,  $x_1 = \frac{\bar{1}}{p^{n+1}} + H$ .

$$\sum_{m=1}^p x_1 = \frac{\bar{p}}{p^{n+1}} + pH = \frac{\bar{1}}{p^n} + H = H$$

$$\sum_{m=1}^p x_i = \frac{\bar{p}}{p^{n+i}} + pH = \frac{\bar{1}}{p^{n+i-1}} + H = x_{i-1}$$

Take  $A = \{x_i | i \in \mathbf{Z}_+\}$ ,  $\langle A \rangle \cong Z(p^\infty)$  by **Exercise 1.3.7(e)**.  $\forall x \in \langle A \rangle$ ,  $x \in Z(p^\infty)/H$ , so  $\langle A \rangle \subset Z(p^\infty)/H$ . Take  $x \in Z(p^\infty)/H$ ,  $x = y + H$  where  $y = \sum_{i=1}^m \frac{a_i}{p^{n+i}}$ ,  $x = \sum_{i=1}^m (\frac{a_i}{p^{n+i}} + H) \in \langle A \rangle$ . Thus,  $Z(p^\infty)/H \subset \langle A \rangle$ ,  $\langle A \rangle = Z(p^\infty)/H \cong Z(p^\infty)$ .

## 1.6 Symmetric, alternating, and dihedral groups

**Exercise 1.6.1.** Find four different subgroups of  $S_4$  that are isomorphic to  $S_3$  and nine isomorphic to  $S_2$ .

**Answer.**  $S_4 = \{(1), (12), (13), (14), (23), (24), (34), (123), (124), (132), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23), (1234), (1243), (1324), (1342), (1423), (1432)\}$ .

$A_1 = \{(1), (12), (13), (23), (123), (132)\}$ ;

$A_2 = \{(1), (12), (14), (24), (124), (142)\}$ ;

$A_3 = \{(1), (13), (14), (34), (134), (143)\}$ ;

$A_4 = \{(1), (23), (24), (34), (234), (243)\}$ ;

$A_1 \cong A_2 \cong A_3 \cong A_4$ .

$B_1 = \{(1), (12)\}$ ;  $B_2 = \{(1), (13)\}$ ;  $B_3 = \{(1), (14)\}$ ;  $B_4 = \{(1), (23)\}$ ;  $B_5 = \{(1), (24)\}$ ;  $B_6 = \{(1), (34)\}$ ;  $B_7 = \{(1), (12)(34)\}$ ;  $B_8 = \{(1), (13)(24)\}$ ;  $B_9 = \{(14)(23)\}$ ;

$B_1 \cong B_2 \cong B_3 \cong B_4 \cong B_5 \cong B_6 \cong B_7 \cong B_8 \cong B_9$ .

**Exercise 1.6.2.** (a)  $S_n$  is generated by the  $n - 1$  transpositions  $(12), (13), (14), \dots, (1n)$ .

(b)  $S_n$  is generated by the  $n - 1$  transpositions  $(12), (23), (34), \dots, (n - 1)n$ .

**Answer.** (a)  $\forall x \in S_n$ ,  $x$  can be written as a product of transpositions.

Actually, for any transposition  $(ij)$ , we can obtain it by  $(1i)(1j)(1i) = (ij)$ . So  $x \in \langle (12), (13), \dots, (1n) \rangle$ ,  $S_n \subset \langle (12), (13), \dots, (1n) \rangle$ .

(b) We can construct  $(1i)$  inductively since  $(1i) = (1i-1)(i-1i)(i-1)$ .

From (a), we have  $\forall x \in S_n$ ,  $x \in \langle (12), (13), \dots, (1n) \rangle$ . Thus  $S_n \subset \langle (12), (13), \dots, (1n) \rangle \subset \langle (12), (23), (34), \dots, (n-1)n \rangle$ .

**Exercise 1.6.3.** If  $\sigma = (i_1 i_2 \dots i_r) \in S_n$  and  $\tau \in S_n$ , then  $\tau \sigma \tau^{-1}$  is the  $r$ -cycle  $(\tau(i_1) \tau(i_2) \dots \tau(i_r))$ .

**Answer.**  $\sigma(i_n) = i_{n+1}$  for  $n = 1, 2, \dots, r - 1$ ,  $\sigma(i_r) = i_1$ . Assume  $\tau(i_n) = j_n$ ,  $n = 1, 2, \dots, r - 1$  and  $I = \{i_n | n = 1, 2, \dots, r - 1\}$ ,  $J = \{j_n | n = 1, 2, \dots, r - 1\}$ . For  $x \notin J$ ,  $\tau \sigma \tau^{-1}(x) = \tau \tau^{-1}(x) = x$ . For  $x = j_k \in J$ ,  $\tau^{-1}(x) = i_k$ ,  $\sigma(\tau^{-1}(x)) = i_{k+1}$ ,  $\tau(\sigma(\tau^{-1}(x))) = j_{k+1}$  and  $\tau \sigma \tau^{-1}(j_r) = j_1$ . Thus  $\tau \sigma \tau^{-1} = (\tau(i_1) \tau(i_2) \dots \tau(i_r))$ .

**Exercise 1.6.4.** (a)  $S_n$  is generated by  $\sigma_1 = (12)$  and  $\tau = (123 \cdots n)$ .  
 (b)  $S_n$  is generated by  $(12)$  and  $(23 \cdots n)$ .

**Answer.** (a) Denote  $\sigma_i = \tau\sigma_{i-1}\tau^{-1}$ . Applying **Exercise 1.6.3**,  $\sigma_i = (i\ i+1)$ . By **Exercise 1.6.2(b)**,  $S_n \subset \langle (12), (23), (34), \dots, (n-1\ n) \rangle = \langle \sigma_1, \sigma_2, \dots, \sigma_{n-1} \rangle \subset \langle \tau, \sigma_1 \rangle$ .  $S_n$  can be generated by  $\tau$  and  $\sigma_1$ .  
 (b) Denote  $\sigma_1 = (12)$ ,  $\tau = (23 \cdots n)$ ,  $\sigma_i = \tau\sigma_{i-1}\tau^{-1}$ . Applying **Exercise 1.6.3**,  $\sigma_i = (i\ i+1)$ . By **Exercise 1.6.2(a)**,  $S_n \subset \langle (12), (13), \dots, (1n) \rangle = \langle \sigma_1, \sigma_2, \dots, \sigma_{n-1} \rangle \subset \langle \tau, \sigma_1 \rangle$ .  $S_n$  can be generated by  $\tau$  and  $\sigma_1$ .

**Exercise 1.6.5.** Let  $\sigma, \tau \in S_n$ . If  $\sigma$  is even (odd), then so is  $\tau\sigma\tau^{-1}$ .

**Answer.** Assume  $\sigma = (x_1x_2) \cdots (x_{2m-1}x_{2m})$ ,  $\tau = (y_1y_2) \cdots (y_{2m-1}y_{2m})$ . Then  $\tau^{-1} = (y_{2m-1}y_{2m}) \cdots (y_1y_2)$ .  $\sigma$  is odd (even) if and only if  $n$  is odd (even).  $\tau\sigma\tau^{-1}$  has  $2m+n$  transpositions. We can add  $(ij) = (ji) = (1)$  into some segments of  $\tau\sigma\tau^{-1}$  without changing it. So  $\tau\sigma\tau^{-1}$  is odd (even) if and only if  $2m+n$  is odd (even).  $2m+n \equiv n \pmod{2}$  so  $\tau\sigma\tau^{-1}$  is odd (even) if and only if  $\sigma$  is odd (even).

**Exercise 1.6.6.**  $A_n$  is the only subgroup of  $S_n$  of index 2.

**Answer.** For any subgroup  $N < S_n$  and  $[S_n : N] = 2$ , we have  $N \triangleleft S_n$ .

Assume there exists  $k$ -circle  $\sigma = (i_1i_2 \cdots i_k) \in N$ . Then for any other  $k$ -circle  $(j_1j_2 \cdots j_k)$ , take  $\tau = (i_1j_1)(i_2j_2) \cdots (i_kj_k)$ , by **Exercise 1.6.3**,  $\tau\sigma\tau^{-1} = (j_1j_2 \cdots j_k) \in N$ . Thus  $N$  contains all the  $k$ -circles.

For  $n \geq 5$ . If there exists 3-circle in  $N$ , then all the 3-circles are contained in  $N$ ,  $A_n \subset N \subset S_n \Rightarrow A_n = N$ .

If there exists 2-circle in  $N$ , then all the 2-circles are contained in  $N$ . Notice  $(1i)(1j) = (1ij) \in N$  is a 3-circle, so  $A_n = N$ .

If there only contain  $x$  in the form of  $(a_1a_2 \cdots a_{n_1})(b_1b_2 \cdots b_{n_2}) \cdots$  where  $n_i \geq 4$  and every two circles are disjoint. Take  $\tau_i : \{a_i | i = 1, 2, \dots, n_1\} \rightarrow \{a_i | i = 1, 2, \dots, n_1\}$ . We can obtain product of two  $n_1$ -circles

$$x^{-1}\tau x\tau^{-1} = (a_1a_2 \cdots a_{n_1})(\tau(a_1)\tau(a_2) \cdots \tau(a_{n_1})) \in N$$

By the arbitrariness of  $\tau$ , take

$$(\tau(a_1)\tau(a_2)\cdots\tau(a_n)) = (a_1a_4a_5\cdots a_na_3a_2)$$

then  $x^{-1}\tau x\tau^{-1} = (a_1a_3)(a_2a_4)$  is a product of 2-circles. We can take  $a_1, a_2, a_3, a_4$  arbitrarily. WLOG, take  $(12)(34) \in N$  and  $(12)(35) \in N$ ,  $(12)(35)(12)(34) = (345) \in N$ . Then there exists 3-circle in  $N$ ,  $N = A_n$ .

In conclusion, when  $n \geq 5$ ,  $S_n$  has only one normal subgroup  $A_n$ .

For  $n = 2, 3, 4$ , we can verify it by enumeration.

**Exercise 1.6.7.** Show that  $N = \{(1), (12)(34), (13)(24), (14)(23)\}$  is a normal subgroup of  $S_4$  contained in  $A_4$  such that  $S_4/N \cong S_3$  and  $A_4/N \cong Z_3$ .

**Answer.** Assume  $\sigma = (i_1i_2)(i_3i_4) \in N$ ,  $\forall \tau \in S_4$ ,  $\tau(i_n) = j_n$ ,  $J = \{j_n | n = 1, 2, 3, 4\}$ . For  $x \notin J$ ,  $\tau\sigma\tau^{-1}(x) = \tau\tau^{-1}(x) = x$ . For  $x = j_k \in J$ ,  $\tau^{-1}(x) = i_k$ ,  $\sigma\tau^{-1}(x) = i_{3k-4[\frac{k}{2}]-1}$ ,  $\tau\sigma\tau^{-1}(x) = (\tau(i_i)\tau(i_2))(\tau(i_3)\tau(i_4)) \in N$ . So  $N \triangleleft S_4$ .  $S_4/N = \{N, N(12), N(13), N(23), N(123), N(132)\} \cong S_3$ .  $A_4/N = \{N, N(123), N(132)\} \cong Z_3$ .

**Exercise 1.6.8.** The group  $A_4$  has no subgroup of order 6.

**Answer.**  $|A_4| = 12$ , assume there exists  $N < A_4$ ,  $|N| = 6$ . Then  $N \triangleleft A_4$ . From **Exercise 1.6.6**, we know that all 3-circles are contained in  $N$ . But there're 8 3-circles in total, so  $N$  can't exist.

**Exercise 1.6.9.** For  $n \geq 3$  let  $G_n$  be the multiplicative group of complex matrices generated by  $x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  and  $y = \begin{pmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{pmatrix}$ , where  $i^2 = -1$ . Show that  $G_n \cong D_n$ .

**Answer.** Take a mapping  $f : G_n \rightarrow D_n$  as  $f(x) = (2n)(3n-1)\cdots$ ,  $f(y) = (123\cdots n)$ .  $|f(x)| = |x| = 2$ ,  $|f(y)| = |y| = n$ .  $f$  is obviously a monomorphism.  $\forall a \in D_n$ ,  $a = f(x)^n f(y)^m$ ,  $m = 1, 2$ , then  $a = f(x^n y^m)$ ,  $f$  is a epimorphism. Thus  $G_n \cong D_n$ .

**Exercise 1.6.10.** Let  $a$  be the generator of order  $n$  of  $D_n$ . Show that  $\langle a \rangle \triangleleft D_n$  and  $D_n / \langle a \rangle \cong Z_2$ .

**Answer.**  $|\langle a \rangle| = n$ ,  $b$  is the other generator of  $D_n$ ,  $a^n = b^2 = (1)$ .  $\forall k \in \mathbf{Z}$ ,  $a^k b = b a^{-k}$  can be easily proved by induction. So  $\forall x = a^m b^n \in D_n$ ,  $x = a^{m'} b^{n'}$ , here  $m' \equiv m \pmod{2}$ ,  $n' \equiv n \pmod{2}$ .  $D_n = \{e, a, a^2, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}\}$ .  $|D_n| = 2n$ . Thus,  $\langle a \rangle \triangleleft D_n$ .  $D_n / \langle a \rangle = \{\langle a \rangle, \langle a \rangle b\} \cong Z_2$ .

**Exercise 1.6.11.** Find all normal subgroups of  $D_n$ .

**Answer.** The subgroups of  $\langle a \rangle$  is always normal in  $D_n$ .  $\langle a^m \rangle < \langle a \rangle$ .  $\forall x \in D_n$  and  $a^{km} \in \langle a^m \rangle$ ,  $x = a^t$  or  $x = ba^t$ .

$$x^{-1} a^{km} x = a^{-t} a^{km} a^t = a^{km} \in \langle a^m \rangle$$

or

$$x^{-1} a^{km} x = a^{-t} b^{-1} a^{km} b a^t = a^{-t} b a^{km} b a^t = a^{-t} a^{-km} b^2 a^t = a^{-km} \in \langle a^m \rangle$$

so  $\langle a^m \rangle \triangleleft D_n$ .

Consider the subgroup  $S$  which only contains  $ba^i, i = 1, \dots, n$ . Since  $ba^i \cdot ba^j = a^{j-i} \in S$  ( $i \neq j$ ), so  $S = \{e, ba^k\}$ .

If  $n$  is odd, take  $x = a^{\frac{n-1}{2}} \in D_n$ .

$$x^{-1} ba^k x = a^{\frac{1-n}{2}} ba^k a^{\frac{n-1}{2}} = ba^{k+n-1} \notin S$$

so  $S \not\triangleleft D_n$  for all  $k = 1, 2, \dots, n$ .

If  $n$  is even, take  $x = a^{\frac{n-2}{2}} \in D_n$ ,  $n \geq 6$ .

$$x^{-1} ba^k x = a^{\frac{2-n}{2}} ba^k a^{\frac{n-2}{2}} = ba^{k+n-2} \notin S$$

so  $S \not\triangleleft D_n$  for all  $k = 1, 2, \dots, n$ .

If  $n = 2$ , all the subgroups are normal since  $|D_2| = 4$ .

For subgroup  $S$  contains both  $ba^i$  and  $a^j$ . It can be written as  $S = \langle a^d, ba^r \rangle$ , where  $d|n$ ,  $0 \leq r \leq d-1$ . If  $\exists a^m, a^n \in S$ ,  $(m, n) = d$ , then there exist  $x, y \in \mathbf{Z}$  s.t.  $a^{mx+ny} = a^d \in \mathbf{Z}$ . Thus,  $S = \langle a^d, ba^r \rangle$ .

Take  $x = a^{\frac{n-w}{2}}$ , then  $x^{-1} ba^r x = ba^{r+n-w}$ .

If  $d \geq 3$ , take  $w \equiv n \pmod{2}$ ,  $x^{-1}ba^r x \notin S$ .

If  $d = 2$ , then  $n = 2s$  and  $S = \{e, a^s, ba^s, b\}$ .  $Sa^k = \{a^k, a^{s+k}, ba^{s-k}, ba^{-k}\}$ ,  $k = 1, 2, \dots, s-1$ .  $ba^k = ba^{-k}$  or  $ba^k = ba^{s-k} \Rightarrow k = \frac{s}{2}$ . So for  $s = 2$ ,  $n = 4$ ,  $S$  is a normal subgroup of  $D_4$ .

**Exercise 1.6.12.** The center of the group  $D_n$  is  $\langle e \rangle$  if  $n$  is odd and isomorphic to  $Z_2$  if  $n$  is even.

**Answer.** If  $n$  is odd,  $C$  is the center of  $D_n$ ,  $C \triangleleft D_n \Rightarrow C < \langle a \rangle$ . Take  $a^d \in C$ ,  $x = ba^m$ ,

$$x^{-1}ax = a^{-m}b^{-1}a^d ba^m = a^{-m}ba^d ba^m = a^{-d} = a^d$$

so  $d = 0$ ,  $C = \{e\}$ .

If  $n$  is even,  $n \geq 6$ .  $C$  is the center of  $D_n$ .  $C \triangleleft D_n \Rightarrow C < \langle a \rangle$  or  $C = \{e, ba^k\}$ .

If  $C = \{e, ba^k\}$ ,  $C \cong Z_2$ .

If  $C < \langle a \rangle$ , take  $a^d \in C$ ,  $x = ba^m$ ,

$$x^{-1}ax = a^{-m}b^{-1}a^d ba^m = a^{-m}ba^d ba^m = a^{-d} = a^d$$

so  $d = \frac{n}{2}$  or  $d = 0$ ,  $C = \{a^{\frac{n}{2}}, e\} \cong Z_2$ .

**Exercise 1.6.13.** For each  $n \geq 3$  let  $P_n$  be a regular polygon of  $n$  sides (for  $n = 3$ ,  $P_n$  is an equilateral triangle; for  $n = 4$ , a square). A *symmetry* of  $P_n$  is a bijection  $P_n \rightarrow P_n$  that preserves distances and maps adjacent vertices on to adjacent vertices.

- (a) The set  $D_n^*$  of all symmetries of  $P_n$  is a group under the binary operation of composition of functions.
- (b) Every  $f \in D_n^*$  is completely determined by its actions on the vertices of  $P_n$ . Number the vertices consecutively  $1, 2, \dots, n$ ; then each  $f \in D_n^*$  determines a unique permutation  $\sigma_f$  of  $\{1, 2, \dots, n\}$ . The assignment  $f \mapsto \sigma_f$  defines a monomorphism of groups  $\varphi: D_n^* \rightarrow S_n$ .
- (c)  $D_n^*$  is generated by  $f$  and  $g$ , where  $f$  is a rotation of  $2\pi/n$  degrees about the center of  $P_n$  and  $g$  is a reflection about the “diameter” through the center and vertex 1.
- (d)  $\sigma_f = (123 \cdots n)$  and  $\sigma_g = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}$ , whence  $\text{Im } \varphi = D_n$  and  $D_n^* \cong D_n$ .



**Answer.** In the following analysis, all the numbers are mod  $n$ .

- (a) Consider  $n$  points  $A_i = (\cos \frac{2\pi i}{n}, \sin \frac{2\pi i}{n})^t$ ,  $i = 1, 2, \dots, n$ .  $f$  is the transposition of  $A_i \mapsto A_j$  with the conservation of  $n$  regular polygon structure. So  $f$  must be a bijection.  $D_n^*$  is the set of  $f$ . By the definition,  $D_n^* \subset S_n$ . We prove  $D_n^*$  is a subgroup of  $S_n$ .

Notice that  $A_{i+1} = \begin{pmatrix} \cos \frac{2\pi i}{n} & -\sin \frac{2\pi i}{n} \\ \sin \frac{2\pi i}{n} & \cos \frac{2\pi i}{n} \end{pmatrix} A_i$ .

Denote  $X = \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}$ . To construct the polygon, we must have

$$f(A_{i+1}) = \begin{pmatrix} \cos \frac{2\pi i}{n} & -\sin \frac{2\pi i}{n} \\ \sin \frac{2\pi i}{n} & \cos \frac{2\pi i}{n} \end{pmatrix} f(A_i)$$

or

$$f(A_i) = \begin{pmatrix} \cos \frac{2\pi i}{n} & -\sin \frac{2\pi i}{n} \\ \sin \frac{2\pi i}{n} & \cos \frac{2\pi i}{n} \end{pmatrix} f(A_{i+1})$$

We need to verify that  $\forall f_1, f_2 \in D_n^*$ ,  $f_1 f_2^{-1} \in D_n^*$ . Assume  $B_i = f_2(A_i)$ ,  $B_{i+1} = f_2(A_{i+1})$ . Then  $B_i = X B_{i+1}$  or  $B_i = X^{-1} B_{i+1}$ . Denote  $B_i = A_j$ , then  $B_{i+1} = A_{j-1}$  or  $B_{i+1} = A_{j+1}$ . WLOG, assume  $B_{i+1} = A_{j+1}$ , then  $f_1(A_j) = X f_1(A_{j+1})$  or  $f_1(A_j) = X^{-1} f_1(A_{j+1})$ . So  $f_1 f_2^{-1} \in D_n^*$ .  $D_n^*$  is a subgroup of  $S_n$ .

- (b) Assume  $A_i = f(A_1)$ . If  $f(A_2) = A_{i+1}$ , since  $f$  is a bijection, by induction, we can prove  $f(A_k) = A_{k+i-1}$ .  $\varphi : D_n^* \rightarrow S_n$  can be defined as  $\varphi : f \mapsto (1i \ 2i-1 \ 3i-2 \dots)$ . If  $f(A_2) = A_{i-1}$ , similarly, we can also prove  $f(A_k) = A_{i+1-k}$ .  $\varphi$  can be defined as  $\varphi : f \mapsto (1i)(2i-1)(3i-2)\dots$ . This means  $f$  is completely determined by  $f(A_1)$  and  $f(A_2)$ .  $D_n^*$  can be embedded into  $S_n$ .

- (c) Denote  $\alpha = \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}$ ,  $\beta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ .  $f : A_i \mapsto \alpha A_i$ ,  $g : A_i \mapsto \beta A_i$ .  $f$  is the rotation of  $\frac{2\pi}{n}$  degrees counter-clockwisely.  $g$  is the reflection about  $x$ -axis. Now we prove  $\forall x \in D_n^*$ ,  $x$  can be factorised into finite product of  $f$  and  $g$ . From (b),  $x$  is fully defined by  $x(A_1)$  and  $x(A_2)$ . Assume  $x(A_1) = A_i$ .

If  $x(A_2) = A_{i+1}$ ,  $x(A_k) = A_{i-1+k} = \alpha^{i-1} A_k$ ,  $k = 1, 2, \dots, n$ . So  $x = f^{i-1}$ .

If  $x(A_2) = A_{i-2}$ ,  $x(A_k) = A_{i+1-k} = \alpha^{i+1} A_{-k} = \alpha^{i+1} \beta A_k$ . So  $x = f^{i+1} g$ . Thus  $D_4^* \subset \langle f, g \rangle$ .

- (d)  $\alpha^n = \beta^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . We can easily verify that  $|f| = n$  and  $|g| = 2$ . From

**Exercise 1.6.9**,  $\langle f, g \rangle \cong D_n$ ,  $|\langle f, g \rangle| = |D_n| = 2n$ . From (b),  $x \in D_n^*$

if completely determined by  $x(A_1)$  and  $x(A_2)$ . There are  $2n$  different ways to obtain  $x(A_1)$  and  $x(A_2)$ . So  $|D_n^*| = |\langle f, g \rangle| = 2n$ .  $D_n^* \subset \langle f, g \rangle$ , so  $D_n^* = \langle f, g \rangle$ . Thus,  $D_n^* \cong \langle f, g \rangle \cong D_n$ .

## 1.7 Categories: products, coproducts, and free objects

**Exercise 1.7.1.** A *pointed set* is a pair  $(S, x)$  with  $S$  a set and  $x \in S$ . A morphism of pointed sets  $(S, x) \rightarrow (S', x')$  is a triple  $(f, x, x')$ , where  $S \rightarrow S'$  is a function such that  $f(x) = x'$ . Show that pointed sets form a category.

**Answer.** Let  $\mathcal{S}$  be the category and 4 objects of  $\mathcal{S}$  are  $(A, a)$ ,  $(B, b)$ ,  $(C, c)$ ,  $(D, d)$ .  $f$ ,  $g$  and  $h$  are morphisms defined by  $f : A \rightarrow B$ ,  $g : B \rightarrow C$ ,  $h : C \rightarrow D$  with  $f(a) = b$ ,  $g(b) = c$ ,  $h(c) = d$ .

$$(A, a) \xrightarrow{f} (B, b) \xrightarrow{g} (C, c) \xrightarrow{h} (D, d)$$

category  $\mathcal{S}$

$$\text{hom}(A, B) \times \text{hom}(B, C) \rightarrow \text{hom}(A, C)$$

because  $g \circ f : A \rightarrow C$  with  $g(f(a)) = g(b) = c = g \circ f(a)$ . Similarly,  $(h \circ g) \circ f = h \circ (g \circ f)$  with  $(h \circ g) \circ f(a) = h \circ (g \circ f)(a) = d$ . Take  $1_B$  consist of those functions  $i : B \rightarrow B$  with  $i(b) = b$ . Then  $1_B \circ f = f$  and  $g \circ 1_B = g$ . So  $\mathcal{S}$  is a category.

**Exercise 1.7.2.** If  $f : A \rightarrow B$  is an equivalence in a category  $\mathcal{C}$  and  $g : B \rightarrow A$  is the morphism such that  $g \circ f = 1_A$ ,  $f \circ g = 1_B$ , show that  $g$  is unique.

**Answer.** Assume there exist  $g$  and  $g'$  satisfies the condition.

$$A \begin{array}{c} \xrightarrow{f} \\ \xleftarrow{g} \end{array} B \qquad A \begin{array}{c} \xrightarrow{f} \\ \xleftarrow{g'} \end{array} B$$

$$\text{So } g' \circ (f \circ g) = g' \circ 1_B = g' = (g' \circ f) \circ g = 1_A \circ g = g.$$

**Exercise 1.7.3.** In the category  $\mathcal{G}$  of groups, show that the group  $G_1 \times G_2$  together with the homomorphisms  $\pi_1 : G_1 \times G_2 \rightarrow G_1$  and  $\pi_2 : G_1 \times G_2 \rightarrow G_2$  is a product for  $\{G_1, G_2\}$ .

**Answer.** Take  $\tau_1 : G_1 \rightarrow G_1 \times G_2$  as  $\tau_1(g_1) = (g_1, e)$ ;  $\tau_2 : G_2 \rightarrow G_1 \times G_2$  as  $\tau_2(g_2) = (e, g_2)$ ;  $\pi_1 : G_1 \times G_2 \rightarrow G_1$  as  $\pi_1(g_1, g_2) = g_1$ ;  $\pi_2 : G_1 \times G_2 \rightarrow G_2$  as  $\pi_2(g_1, g_2) = g_2$ . Then

$$G_1 \xrightleftharpoons[\tau_1]{\pi_1} G_1 \times G_2 \xrightleftharpoons[\tau_2]{\pi_2} G_2$$

For any object  $B$  such that

$$G_1 \xleftarrow{\varphi_1} B \xrightarrow{\varphi_2} G_2$$

For any  $x \in B$ , define  $f : B \rightarrow G_1 \times G_2$  as  $f(x) = (\varphi_1(x), \varphi_2(x))$ . Then  $\pi_1(f(x)) = \varphi_1(x)$ ,  $\pi_1 \circ f = \varphi_1$ ,  $\pi_2(f(x)) = \varphi_2(x)$ ,  $\pi_2 \circ f = \varphi_2$ . Thus

$$\begin{array}{ccccc} & & B & & \\ & \swarrow \varphi_1 & \downarrow f & \searrow \varphi_2 & \\ G_1 & \xrightleftharpoons[\tau_1]{\pi_1} & G_1 \times G_2 & \xrightleftharpoons[\tau_2]{\pi_2} & G_2 \end{array}$$

Next we verify the uniqueness. If there exist  $f$  and  $f'$  satisfies the condition,

$$\pi_1(f(x)) = \pi_1(f'(x)) = \varphi_1(x)$$

$$\pi_2(f(x)) = \pi_2(f'(x)) = \varphi_2(x)$$

Thus  $f(x) = f'(x)$  for all  $x \in B$ , so  $f = f'$ .

**Exercise 1.7.4.** In the category  $\mathcal{A}$  of abelian groups, show that the group  $A_1 \times A_2$  together with the morphisms  $\tau_1 : A_1 \rightarrow A_1 \times A_2$  and  $\tau_2 : A_2 \rightarrow A_1 \times A_2$  is a coproduct of  $\{A_1, A_2\}$ .

**Answer.** Take  $\tau_1 : A_1 \rightarrow A_1 \times A_2$  as  $\tau_1(a_1) = (a_1, e)$ ;  $\tau_2 : A_2 \rightarrow A_1 \times A_2$  as  $\tau_2(a_2) = (e, a_2)$ ;  $\pi_1 : A_1 \times A_2 \rightarrow A_1$  as  $\pi_1(a_1, a_2) = a_1$ ;  $\pi_2 : A_1 \times A_2 \rightarrow A_2$  as  $\pi_2(a_1, a_2) = a_2$ . Then

$$A_1 \xrightleftharpoons[\tau_1]{\pi_1} A_1 \times A_2 \xrightleftharpoons[\tau_2]{\pi_2} A_2$$

For any object  $B$  such that

$$A_1 \xrightarrow{\varphi_1} B \xleftarrow{\varphi_2} A_2$$

For any  $(a_1, a_2) \in A_1 \times A_2$ , define  $f : A_1 \times A_2 \rightarrow B$  as  $f(a_1, a_2) = \varphi_1(a_1)\varphi_2(a_2)$ . Then  $f(\tau_1(a_1)) = f(a_1, e) = \varphi_1(a_1)e = \varphi_1(a_1)$ ,  $f \circ \tau_1 = \varphi_1$ ,  $f(\tau_2(a_2)) = f(e, a_2) = e\varphi_2(a_2) = \varphi_2(a_2)$ ,  $f \circ \tau_2 = \varphi_2$ .

$$\begin{array}{ccccc} & & B & & \\ & \nearrow \varphi_1 & \uparrow f & \nwarrow \varphi_2 & \\ A_1 & \xleftarrow{\pi_1} & A_1 \times A_2 & \xrightarrow{\pi_2} & A_2 \\ & \xleftarrow{\tau_1} & & \xleftarrow{\tau_2} & \end{array}$$

Next we verify the uniqueness. If there exist  $f$  and  $f'$  satisfies the condition,

$$f(\tau_1(a_1)) = f'(\tau_1(a_1)) = f(a_1, e) = f'(a_1, e)$$

$$f(\tau_2(a_2)) = f'(\tau_2(a_2)) = f(e, a_2) = f'(e, a_2)$$

$$\begin{aligned} f(\tau_1(a_1), \tau_2(a_2)) &= f(\tau_1(a_1))f(\tau_2(a_2)) \\ &= f'(\tau_1(a_1), \tau_2(a_2)) = f'(\tau_1(a_1))f'(\tau_2(a_2)) \end{aligned}$$

so  $f = f'$ .

**Exercise 1.7.5.** Every family  $\{A_i | i \in I\}$  in the category of sets has a coproduct.

**Answer.** We examine  $\bigcup A_i = \{(a, i) \in (\cup A_i) \times I | a \in A_i\}$  which satisfies the condition. Define the morphism  $\pi_i : A_i \rightarrow \bigcup A_i$  as  $\pi_i(a) = (a, i)$ . For any  $B$  such that  $\exists \varphi_i : A_i \rightarrow B$ .

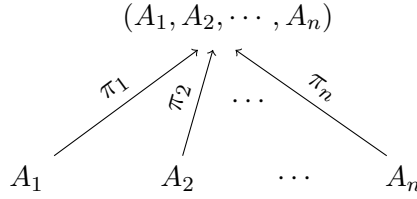
$$\begin{array}{ccccccc} & & B & & & & \\ & \nearrow \varphi_1 & \uparrow \varphi & \nwarrow \varphi_n & & & \\ A_1 & & A_2 & \cdots & & & A_n \end{array}$$

$\varphi(a) = x \in B$ . Take  $\varphi(a, i) = \varphi_i(a)$  defined on the subset of  $\cup A_i \times I$ , we can verify that the domain of  $\varphi$  is  $\cup A_i$ . Then take  $f = \varphi$ ,  $f(\pi_i(a)) = \varphi_i(a)$ ,  $f \circ \pi_i = \varphi_i$ .

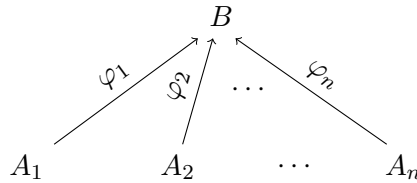
The uniqueness is obvious.

- Exercise 1.7.6.** (a) Show that in the category  $\mathcal{S}_*$  of pointed sets product always exist; describe them.  
 (b) Show that in  $\mathcal{S}_*$  every family of objects has a coproduct, describe the coproduct.

**Answer.** (a) Define  $\otimes$  as an operator between points and other elements in the pointed set.  $\forall a \in A_i$ ,  $a \otimes a_i = a_1 \times a = a$ . For a family of sets with their points  $\{(A_i, a_i | i \in I)\}$ , consider  $(A_1, A_2, \dots, A_n) = \{(a'_1, a'_2, \dots, a'_n)\}$ . Define morphisms  $\pi_i(a) = (a_1, a_2, \dots, a, \dots, a_n)$ ,  $\pi_i : A_i \rightarrow (A_1, A_2, \dots, A_n)$ .



For any  $B$  such that  $\exists \varphi_i : A_i \rightarrow B$ .



Take  $f : (A_1, A_2, \dots, A_n) \rightarrow B$  as

$$f(a'_1, a'_2, \dots, a'_n) = \varphi_1(a'_1) \otimes \varphi_2(a'_2) \otimes \dots \otimes \varphi_n(a'_n)$$

Then  $f \circ \pi_i(a) = f(a_1, a_2, \dots, a, \dots, a_n) = \varphi_1(a_1) \otimes \dots \otimes \varphi_i(a) \otimes \dots \otimes \varphi_n(a_n) = \varphi_i(a)$ . So  $f \circ \pi_i = \varphi_i$ .

Next we verify the uniqueness. If there exist  $f$  and  $f'$  satisfies the condition. Then  $\exists i \in I$  and  $a \in A_i$  s.t.  $f(a_1, a_2, \dots, a, \dots, a_n) \neq f'(a_1, a_2, \dots, a, \dots, a_n)$ . But  $f(\pi_i(a)) = f'(\pi_i(a))$ , so  $f = f'$ .

(b) The proof is similar to **Exercise 1.7.5**.

**Exercise 1.7.7.** Let  $F$  be a free object on a set  $X(i : X \rightarrow F)$  in a concrete category  $\mathcal{C}$ . If  $\mathcal{C}$  contains an object whose underlying set has at least two elements in it, then  $i$  is an injective map of sets.

**Answer.** Assume  $A \in \text{obj}(\mathcal{C})$ ,  $A$  has at least two elements and  $X \xrightarrow{f} A$ .  $X \xrightarrow{i} F$  and  $F$  is free on  $X$ , so there exists a morphism  $\bar{f}$  s.t.  $F \xrightarrow{\bar{f}} A$ . If  $|X| = 1$ ,  $i$  must be injective. For  $|X| \geq 2$ . Suppose  $i$  is not injective. Take  $x_1, x_2 \in X$  and  $i(x_1) = i(x_2) \in F$ ,  $f(x_1) = a_1$ ,  $f(x_2) = a_2$ .  $\bar{f}(i(x_1)) = \bar{f}(i(x_2)) = f(x_1) = f(x_2) = a_1 = a_2$ . That means all the elements in  $A$  are identical. That's contradictory to the assumption.

**Exercise 1.7.8.** Suppose  $X$  is a set and  $F$  is a free object on  $X$  (with  $i : X \rightarrow F$ ) in the category of groups. Prove that  $i(X)$  is a set of generators for the group  $F$ .

**Answer.** Assume  $G$  the subgroup of  $F$  is the group generated by  $i(X)$ . Since  $X \xrightarrow{i} G$  and  $X \xrightarrow{i} F$ , we can obtain unique morphism  $\varphi$  such that  $F \xrightarrow{\varphi} G$  and  $\varphi \circ i = i$ .

Consider morphism  $1_F : F \rightarrow F$  which is the identical homomorphism.  $F$  is free so  $1_F$  is the unique homomorphism. Take  $\subset : G \rightarrow F$  as a morphism defined as  $\forall g \in G, \subset(g) = g$ . Then

$$\begin{array}{ccccc}
 & & G & & \\
 & \nearrow i & \uparrow \varphi & \searrow \subset & \\
 X & \xrightarrow{i} & F & \xrightarrow{1_F} & F
 \end{array}$$

$\subset \circ \varphi \circ i = 1_F \circ i = i$  so  $\subset \circ \varphi = 1_F$ . Thus  $\subset$  is an epimorphism,  $F \subset G$ . So  $F = G$  can be generated by  $i(X)$ .

## 1.8 Direct products and direct sums

**Exercise 1.8.1.**  $S_3$  is not the direct product of any family of its proper subgroups. The same is true of  $Z_{p^n}$  ( $p$  prime,  $n \geq 1$ ) and  $\mathbb{Z}$ .

**Answer.** We list all the subgroups of  $S_3$ :  $\{(1), (12)\}$ ,  $\{(1), (13)\}$ ,  $\{(1), (23)\}$ ,  $\{(1), (123), (132)\}$ . Only  $\{(1), (123), (132)\}$  is normal, so  $S_3$  isn't a direct product of any family of its proper subgroups.

For  $Z_{p^n}$ ,  $Z_{p^i} \triangleleft Z_{p^n}$  for all  $i = 1, 2, \dots, n-1$  but  $Z_{p^i} \cap Z_{p^j} \neq \{e\}$ . So  $Z_{p^n}$  isn't a direct product of any family of its proper subgroups.

For  $\mathbb{Z}$ .  $\forall N_1 \triangleleft \mathbb{Z}$ ,  $N_2 \triangleleft \mathbb{Z}$ , we have  $N_1 = \langle a_1 \rangle$  and  $N_2 = \langle a_2 \rangle$ . Thus,  $N_1 \cap N_2 = \langle a_1 a_2 \rangle \neq \{e\}$ . So  $\mathbb{Z}$  isn't a direct product of any family of its proper subgroups.

**Exercise 1.8.2.** Give an example of groups  $H_i, K_i$  such that  $H_1 \times H_2 \cong K_1 \times K_2$  and no  $H_i$  is isomorphic to any  $K_j$ .

**Answer.** Take  $H_1 \cong K_1 \times K_2$ ,  $H_2 = \{e\}$ . We verify that  $H_1 \times H_2 \cong K_1 \times K_2$ . There exists  $f : H_1 \rightarrow K_1 \times K_2$  which is an isomorphism. There exists canonical projection  $\pi_1 : H_1 \times H_2 \rightarrow H_1$  and  $\pi_1$  is an epimorphism.  $\text{Ker} \pi_1 = \{(e_1, e_2)\}$  thus  $\pi_1$  is also a monomorphism. Therefore  $\bar{f} = f \circ \pi_1$  is a well defined isomorphism.  $H_1 \times H_2 \cong K_1 \times K_2$  but neither  $H_1$  nor  $H_2$  are isomorphic to any  $K_i, i = 1, 2$ .

**Exercise 1.8.3.** Let  $G$  be an (additive) abelian group with subgroups  $H$  and  $K$ . Show that  $G \cong H \oplus K$  if and only if there are homomorphisms

$$H \begin{array}{c} \xleftarrow{\pi_1} \\ \xrightarrow{\tau_1} \end{array} G \begin{array}{c} \xleftarrow{\pi_2} \\ \xrightarrow{\tau_2} \end{array} K$$

such that  $\pi_1 \tau_1 = 1_H$ ,  $\pi_2 \tau_2 = 1_K$ ,  $\pi_1 \tau_2 = 0$  and  $\pi_2 \tau_1 = 0$ , where 0 is the map sending every element onto the zero (identity) element, and  $\tau_1 \pi_1(x) + \tau_2 \pi_2(x) = x$  for all  $x \in G$ .

**Answer.** If  $G \cong H \oplus K$ . Denote  $f : G \rightarrow H \oplus K$  which is an isomorphism. Then there are canonical products  $\pi'_1, \pi'_2, \tau'_1, \tau'_2$ .



$$\begin{array}{ccccc} & \xleftarrow{\pi'_1} & H \oplus K & \xleftarrow{\pi'_2} & \\ & \tau'_1 & & \tau'_2 & \\ & \xrightarrow{\pi'_1} & H \oplus K & \xrightarrow{\pi'_2} & \\ & \tau'_1 & & \tau'_2 & \end{array}$$

Thus

$$\begin{array}{ccccc} & & G & & \\ & \swarrow \pi_1 & \uparrow f & \searrow \pi_2 & \\ & \pi'_1 & \downarrow f & \pi'_2 & \\ H & \xleftarrow{\pi'_1} & H \oplus K & \xleftarrow{\pi'_2} & K \\ & \tau'_1 & & \tau'_2 & \end{array}$$

Take  $\tau_1 = f \circ \tau'_1$ ,  $\tau_2 = f \circ \tau'_2$ ,  $\pi_1 = \pi'_1 \circ f^{-1}$ ,  $\pi_2 = \pi'_2 \circ f^{-1}$ .

$$\pi_1 \tau_1 = \pi'_1 f^{-1} f \tau'_1 = \pi'_1 \tau'_1 = 1_H$$

$$\pi_2 \tau_2 = \pi'_2 f^{-1} f \tau'_2 = \pi'_2 \tau'_2 = 1_K$$

$$\pi_1 \tau_2 = \pi'_1 f^{-1} f \tau'_2 = \pi'_1 \tau'_2 = 0$$

$$\pi_2 \tau_1 = \pi'_2 f^{-1} f \tau'_1 = \pi'_2 \tau'_1 = 0$$

$\forall x \in G$ ,  $x = hk$  where  $h \in H$  and  $k \in K$ .

$$\begin{aligned} \tau_1 \pi_1(x) + \tau_2 \pi_2(x) &= f(\tau'_1 \pi'_1(h, k)) + f(\tau'_2 \pi'_2(h, k)) \\ &= f(\tau'_1(h)) + f(\tau'_2(k)) \\ &= f(h, e) + f(e, k) \\ &= f(h + e, e + k) = f(h, k) \\ &= x \end{aligned}$$

If there exist  $\pi_1, \pi_2, \tau_1, \tau_2$  satisfies the condition. There are canonical projections  $\pi'_1, \pi'_2, \tau'_1, \tau'_2$  between  $H$  and  $H \oplus K$ ,  $K$  and  $H \oplus K$ .

$$\begin{array}{ccccc} & & G & & \\ & \swarrow \pi_1 & \uparrow f & \searrow \pi_2 & \\ & \pi'_1 & \downarrow f & \pi'_2 & \\ H & \xleftarrow{\pi'_1} & H \oplus K & \xleftarrow{\pi'_2} & K \\ & \tau'_1 & & \tau'_2 & \end{array}$$

For  $f = \tau'_1\pi_1 + \tau'_2\pi_2$  which is a well defined homomorphism.  $\forall h \in H$  and  $k \in K$ ,  $\tau'_1(h) + \tau'_2(k) = (h, k) \in H \oplus K$ . Thus  $f(x) = (e_1, e_2)$  if and only if  $\pi_1(x) = e_1$  and  $\pi_2(x) = e_2$ .  $\tau_1\pi_1(x) + \tau_2\pi_2(x) = \tau_1(e_1) + \tau_2(e_2) = e = x$ . Thus  $\text{Ker } f = \{e\}$ .  $f$  is a monomorphism.  $\forall (h, k) \in H \oplus K$ , take  $x = \tau_1(h) + \tau_2(k) \in G$ , then

$$\begin{aligned} f(x) &= \tau'_1\pi_1\tau_1(h) + \tau'_1\pi_1\tau_2(h) + \tau'_2\pi_2\tau_1(k) + \tau'_2\pi_2\tau_2(k) \\ &= \tau'_1(h) + \tau'_2(k) = (h, k) \in H \oplus K \end{aligned}$$

$f$  is an epimorphism. Thus  $G \cong H \oplus K$ .

**Exercise 1.8.4.** Give an example to show that the weak direct product is not a coproduct in the category of all groups.

**Answer.** Consider  $S_3$  and  $S_3 \times S_3$ .

$$\begin{array}{ccc} & & S_3 \times S_2 \\ & \nearrow & \uparrow \text{dashed} \\ S_3 & \longrightarrow & S_3 \times S_3 \end{array}$$

Since there doesn't exist homomorphism  $S_3 \rightarrow S_2$ , there is no homomorphism  $S_3 \times S_3 \rightarrow S_3 \times S_2$ .

**Exercise 1.8.5.** Let  $G, H$  be finite cyclic groups. Then  $G \times H$  is cyclic if and only if  $(|G|, |H|) = 1$ .

**Answer.** Assume  $|G| = m$ ,  $|H| = n$ , then  $G \cong Z_m$ ,  $H \cong Z_n$  and  $G \times H \cong Z_m \oplus Z_n$ .

If  $(|G|, |H|) = 1$ . Consider  $(x_1, x_2) \in Z_m \oplus Z_n$ . By *Chinese Remainder Theorem*, there exists  $x$  such that  $a \equiv x \pmod{\text{lcm}(m, n)}$  and  $a \equiv x_1 \pmod{m}$ ,  $a \equiv x_2 \pmod{n}$ . Thus,  $a(1, 1) = (x_1, x_2)$ .  $Z_m \oplus Z_n < \langle (1, 1) \rangle$ .  $\langle (1, 1) \rangle < Z_m \oplus Z_n$  is trivial. So  $Z_m \oplus Z_n = \langle (1, 1) \rangle \cong G \times H$  is cyclic.

If  $G \times H$  is cyclic. Assume  $l = \text{gcd}(m, n)$  and there exist  $x$  such that  $x_1 \equiv x \pmod{m}$ ,  $x_2 \equiv x \pmod{n}$ . Take  $x_1 \not\equiv x_2 \pmod{l}$ , it can be chosen properly. Consider  $(x_1, x_2) \in Z_m \oplus Z_n$ ,  $x = k_1m + x_1 = k_2n + x_2 \Rightarrow x_1 \equiv x_2 \pmod{l}$ . That's contradictory!

**Exercise 1.8.6.** Every finitely generated abelian group  $G \neq \langle e \rangle$  in which every element (except  $e$ ) has order  $p$  ( $p$  prime) is isomorphic to  $Z_p \oplus Z_p \oplus \cdots \oplus Z_p$  ( $n$  summands) for some  $n \geq 1$ .

**Answer.** Assume  $\{a_1, a_2, \dots, a_n\}$  generates  $G$ .  $|a_i| = p$  for  $i = 1, 2, \dots, n$  so  $\langle a_i \rangle \cong Z_p$ . Now we show that  $G = \prod_{i=1}^n {}^w \langle a_i \rangle \cong \sum_{i=1}^n Z_p$ .  $G = \langle a_1, a_2, \dots, a_n \rangle$  and  $\langle a_1 \rangle \triangleleft G$  for  $i = 1, 2, \dots, n$ . If exist  $\langle a_i \rangle$  s.t.  $\prod_{j=1, j \neq i}^n \langle a_j \rangle \cap \langle a_i \rangle \neq \{e\}$ . Then there exists  $a_i^{s_i} = a_1^{s_1} \cdots a_{i-1}^{s_{i-1}} a_{i+1}^{s_{i+1}} \cdots a_n^{s_n}$ .  $(s_i, p) = 1$  so  $\exists 1 \leq t_i \leq p-1$  such that  $s_i t_i \equiv 1 \pmod{p}$ . So  $a_i^{s_i t_i} = a_1^{s_1 t_i} \cdots a_{i-1}^{s_{i-1} t_i} a_{i+1}^{s_{i+1} t_i} \cdots a_n^{s_n t_i} = a_i$ .  $\{a_1, a_2, \dots, a_n\}$  can generate  $G$ . That's contradictory! So  $\prod_{j=1, j \neq i}^n \langle a_j \rangle \cap \langle a_i \rangle = \{e\}$ , which means  $G = \prod_{i=1}^n {}^w \langle a_i \rangle \cong \sum_{i=1}^n Z_p$ .

**Exercise 1.8.7.** Let  $H, K, N$  be nontrivial normal subgroups of a group  $G$  and suppose  $G = H \times K$ . Prove that  $N$  is in the center of  $G$  or  $N$  intersects one of  $H, K$  nontrivially. Give examples to show that both possibilities can actually occur when  $G$  is nonabelian.

**Answer.** If  $N \cap H = N \cap K = \{e\}$ .  $G = HK$ .  $\forall h \in H$  and  $k \in K$ , since  $H \cap K = \{e\}$ ,  $hk = kh$ . For any  $hk \in N$ , and  $h_1 \in H \subset HK$ ,  $h_1^{-1} h k h_1 = h_1^{-1} h h_1 k \in N$ . Assume  $h' = h_1^{-1} h_1 \in H$ ,  $h' k \in N$ . Thus  $h'^{-1} k^{-1} k h = h'^{-1} h \in N$ . So  $h'^{-1} h = e$ ,  $h = h'$ ,  $h$  is in the center  $C(H)$  of group  $H$ . Similarly,  $k \in C(K)$  which is the center of  $K$ . Then  $\forall hk \in N$  and  $h_1 k_1 \in G$ ,  $k_1^{-1} h_1^{-1} h k h_1 k_1 = h_1^{-1} h h_1 k_1^{-1} k k_1 = hk$ .  $N \subset N(G)$ . For  $N \cup H \neq \emptyset$ , the example can be trivial:  $N < H$  and  $N \triangleleft G$ . There's many cyclic group satisfy the condition. For  $N \subset C(G)$ . Take  $G = D_4^* \times D_4^*$ ,  $H = D_4^* \times \{I\}$ ,  $K = \{I\} \times D_4^*$ .  $\{I, R^2\}$  is normal in  $D_4^*$ . Denote  $N$  is the subgroup  $\{(I, I), (R^2, R^2)\}$ . We can verify that  $N$  satisfies the condition.

**Exercise 1.8.8.** Corollary 8.7 is false if one of the  $N_i$  is not normal.

**Answer.** Consider  $N_1, N_2, \dots, N_n$  are all finite. WLOG, assume  $N_1$  is not normal.  $G = \left\langle \bigcup_{i=1}^n N_i \cup N_1 \right\rangle$  and  $N_1 N_2 \cdots N_n \subset G$ . Denote  $A = N_2 N_3 \cdots N_n$ . Then  $\exists a \in A$  such that  $a^{-1} n a = n' \notin N_1$ . Thus  $n' a \in G$  but  $n' a \notin N_1 N_2 \cdots N_n$  so  $|G| > |N_1 N_2 \cdots N_n| = |N_1| \times |N_2| \times \cdots \times |N_n| = |N_1 \times N_2 \times \cdots \times N_n|$ .

**Exercise 1.8.9.** If a group  $G$  is the (internal) direct product of its subgroups  $H, K$ , then  $H \cong G/K$  and  $G/H \cong K$ .

**Answer.**  $H \cap K = \{e\}$ .  $G = H \times K = HK$ . Thus  $HK/H \cong K/(K \cap H) = K$ ,  $HK/K \cong H/(K \cap H) = H$ .

**Exercise 1.8.10.** If  $\{G_i | i \in I\}$  is a family of groups, then  $\prod^w G_i$  is the internal weak product its subgroups  $\{\tau_i(G_i) | i \in I\}$ .

**Answer.** Take  $\tau_i(g) = (e_1, e_2, \dots, g, \dots, e_n)$ ,  $g \in G_i$ .  $\tau_i(G_i)$  is normal in  $\prod_{i \in I}^w G_i$ .  $\tau_i(G_i) \cap \tau_j(G_j) = \{(e_1, e_2, \dots, e_n)\}$  which is the identity element in  $\prod_{i \in I}^w G_i$ .  $\forall (g_1, g_2, \dots, g_n) \in \prod_{i \in I}^w G_i$ , we have

$$(g_1, g_2, \dots, g_n) = (g_1, e_2, \dots, e_n)(e_1, g_2, \dots, e_n) \cdots (e_1, e_2, \dots, g_n)$$

Thus  $\prod_{i \in I}^w G_i \subset \left\langle \bigcup_{i \in I} \tau_i(G_i) \right\rangle$  and

$$\left\langle \bigcup_{i \in I} \tau_i(G_i) \right\rangle = \tau_1(G_1) \tau_2(G_2) \cdots \tau_n(G_n) \subset \prod_{i \in I}^w G_i$$

Therefore  $\prod_{i \in I}^w G_i$  is the direct product of  $\tau_i(G_i)$ .

**Exercise 1.8.11.** Let  $\{N_i | i \in I\}$  be a family of subgroups of a group  $G$ . Then  $G$  is the internal weak product of  $\{N_i | i \in I\}$  if and only if:

- (i)  $a_i a_j = a_j a_i$  for all  $i \neq j$  and  $a_i \in N_i$ ,  $a_j \in N_j$ ;

- (ii) every nonidentity element of  $G$  is uniquely a product  $a_{i_1} \cdots a_{i_n}$ , where  $i_1, \dots, i_n$  are distinct elements of  $I$  and  $e \neq a_{i_k} \in N_{i_k}$  for each  $k$ .

**Answer.** Trivial.

**Exercise 1.8.12.** A normal subgroup  $H$  of a group  $G$  is said to be a **direct factor** (**direct summand** if  $G$  is additive abelian) if there exists a (normal) subgroup  $K$  of  $G$  such that  $G = H \times K$ .

- (a) If  $H$  is a direct factor of  $K$  and  $K$  is a direct factor of  $G$ , then  $H$  is normal in  $G$ .  
 (b) If  $H$  is a direct factor of  $G$ , then every homomorphism  $H \rightarrow G$  may be extended to an endomorphism  $G \rightarrow G$ . However, a monomorphism  $H \rightarrow G$  need not be extendible to an automorphism  $G \rightarrow G$ .

**Answer.** (a)  $G = K \times K' = (H \times H') \times K'$ . So  $\forall g \in G$ ,  $g = hh'k'$  with  $h \in H$ ,  $h' \in H'$  and  $k' \in K'$ .  $\forall h_1 \in H$  and  $g \in G$ ,  $g^{-1}h_1g = k'^{-1}h'^{-1}h^{-1}h_1hh'k' = (h^{-1}h_1h)(h'^{-1}h')(k'^{-1}k') = h^{-1}h_1h \in H$ . Thus  $H \triangleleft G$ .

- (b) If  $G = H \times K$ . For a homomorphism  $f : H \rightarrow G$ , we construct a homomorphism  $\bar{f} : G \rightarrow G$ ,  $\forall g \in G$ ,  $g$  can be uniquely written as  $g = hk$  where  $h \in H$ ,  $k \in K$ . Take  $\tau(g) = h$  which is a homomorphism  $\tau : G \rightarrow H$ . We can get  $\bar{f} = f \circ \tau : G \rightarrow G$  is an endomorphism but it needn't to be an automorphism.

**Exercise 1.8.13.** Let  $\{G_i | i \in I\}$  be a family of groups and  $J \subset I$ . The map  $\alpha : \prod_{j \in J} G_j \rightarrow \prod_{i \in I} G_i$  given by  $\{a_j\} \mapsto \{b_i\}$ , where  $b_j = a_j$  for  $j \in J$  and  $b_i = e_i$  (identity in  $G_i$ ) for  $i \notin J$ , is a monomorphism of groups and  $\prod_{i \in I} G_i / \alpha(\prod_{j \in J} G_j) \cong \prod_{i \in I-J} G_i$ .

**Answer.** Define a map  $\beta : \prod_{i \in I} G_i \rightarrow \prod_{i \in I-J} G_i$  given by  $\{a_i\} \mapsto \{b_i\}$  and for those  $i \in I - J$ ,  $\exists b_i \in \{b_i\}$  s.t.  $a_i = b_i$ . Thus  $\beta(\{a_i\})\beta(\{a'_i\}) = \beta(\{a_i a'_i\})$ ,  $\beta$  is a well defined homomorphism.  $\text{Ker } \beta = \{\{a_i\} \in \prod_{i \in I} G_i | a_i = e_i \text{ for } i \in I - J\} = \alpha(\prod_{j \in J} G_j)$ . We verify  $\beta$  is an epimorphism.  $\forall \{b_i\} \in \prod_{i \in I-J} G_i$ , take

$\{a_i\} \in \prod_{i \in I} G_i$  where  $a_i = b_i$  for  $i \in I - J$ . Then  $\beta(\{a_i\}) = \{b_i\}$ . Thus  $\beta$  is an isomorphism,  $\text{Im}\beta = \prod_{i \in I-J} G_i \cong \prod_{i \in I} G_i / \alpha(\prod_{j \in J} (G_j))$ .

**Exercise 1.8.14.** For  $i = 1, 2$  let  $H_i \triangleleft G_i$  and give examples to show that each of the following statements may be false:

- (a)  $G_1 \cong G_2$  and  $H_1 \cong H_2 \Rightarrow G_1/H_1 \cong G_2/H_2$ .
- (b)  $G_1 \cong G_2$  and  $G_1/H_1 \cong G_2/H_2 \Rightarrow H_1 \cong H_2$ .
- (c)  $H_1 \cong H_2$  and  $G_1/H_1 \cong G_2/H_2 \Rightarrow G_1 \cong G_2$ .

**Answer.** (a) Take  $G_1 = G_2 = Z_2 \times Z_4$ ,  $H_1 = Z_2 \times \{\bar{0}\}$ ,  $H_2 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{2})\}$ .  
 (b) Take  $G_1 = G_2 = Z_2 \times Z_4$ ,  $H_1 = \{\bar{0}\} \times Z_4$ ,  $H_2 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{2}), (\bar{1}, \bar{2})\}$ .  
 (c) Take  $H_1 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{2})\}$ ,  $H_2 = Z_2$  and  $G_1 = Z_2 \times Z_4$ ,  $G_2 = Z_2 \times K_4$ .

## 1.9 Free groups, free products, generators and relations

**Exercise 1.9.1.** Every nonidentity elements in a free group  $F$  has a infinite order.

**Answer.** Define the length of a word  $x = a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_n^{\lambda_n}$  is  $n$  and denote it as  $\text{len}(x)$ . Assume  $\text{len}(x) = n$  for some  $n \in F$  and  $\text{len}(1) = 0$ , we prove that  $\text{len}(x^m) \geq n \forall m \geq 1$ .

Let  $k$  be the largest integer such that  $a_{n-j}^{\lambda_{n-j}} = a_n^{-\lambda_j}$  for  $j = 0, 1, \dots, k-1$ . If  $k > \lfloor \frac{n}{2} \rfloor$ . For even  $k$ ,  $a_{\frac{n}{2}}^{\lambda_{\frac{n}{2}}} = a_{\frac{n}{2}+1}^{-(\lambda_{\frac{n}{2}+1})}$ ,  $a_{\frac{n}{2}-1}^{\lambda_{\frac{n}{2}-1}} = a_{\frac{n}{2}+2}^{-(\lambda_{\frac{n}{2}+2})}$ ,  $\dots$  which means  $x = a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_n^{\lambda_n} = 1$ . For odd  $k$ ,  $a_{\lfloor \frac{n}{2} \rfloor + 1}^{\lambda_{\lfloor \frac{n}{2} \rfloor + 1}} = a_{\lfloor \frac{n}{2} \rfloor + 1}^{-(\lambda_{\lfloor \frac{n}{2} \rfloor + 1})}$ , which is contradictory to  $x$  is reduced. So  $k \leq \lfloor \frac{n}{2} \rfloor$ .

Divide  $x = x_1 x_2 x_3$  where  $x_1 = a_1^{\lambda_1} \cdots a_k^{\lambda_k}$ ,  $x_2 = a_{k+1}^{\lambda_{k+1}} \cdots a_{n-k}^{\lambda_{n-k}}$ ,  $x_3 = a_{n-k+1}^{\lambda_{n-k+1}} \cdots a_n^{\lambda_n}$ .  $x_3 x_1 = 1$ . So  $\text{len}(x) = \text{len}(x_1) + \text{len}(x_2) + \text{len}(x_3) = n$ .  $x^m = x_1 x_2 x_3 x_1 x_2 x_3 \cdots x_1 x_2 x_3 = x_1 x_2^m x_3$ .  $\text{len}(x^m) = \text{len}(x_1) + m \cdot \text{len}(x_2) + \text{len}(x_3) \geq n$ . So  $\forall m \geq 1$ ,  $x^m \neq 1$ ,  $|x|$  is infinite.

**Exercise 1.9.2.** Show that the free group on the set  $\{a\}$  is an infinite cyclic group, and hence isomorphic to  $\mathbf{Z}$ .

**Answer.**  $F(\{a\}) = \langle a \rangle$  and thus it's a infinite cyclic group.  $F(\{a\}) \cong \mathbf{Z}$ .

**Exercise 1.9.3.** Let  $F$  be a free group and let  $N$  be the subgroup generated by the set  $\{x^n | x \in F, n \text{ a fixed integer}\}$ . Show that  $N \triangleleft F$ .

**Exercise 1.9.4.** Let  $F$  be the free group on the set  $X$ , and let  $Y \subset H$ . If  $H$  is the smallest normal subgroup of  $F$  containin  $Y$ , then  $F/H$  is a free group.

**Exercise 1.9.5.** The group defined by generators  $a, b$  and relations  $a^8 = b^2a^4 = ab^{-1}ab = e$  has order at most 16.

**Exercise 1.9.6.** The cyclic group of order 6 is the group defined by generators  $a, b$  and relations  $a^2 = b^3 = a^{-1}b^{-1}ab = e$ .

**Exercise 1.9.7.** Show that the group defined by generators  $a, b$  and relations  $a^2 = e, b^3 = e$  is infinite and nonabelian.

**Exercise 1.9.8.** The group defined by generators  $a, b$  and relations  $a^n = e (3 \leq n \in \mathbf{N}^*)$ ,  $b^2 = e$  and  $abab = e$  is the dihedral group  $D_n$ .

**Exercise 1.9.9.** The group defined by the generator  $b$  and  $b^m = e (m \in \mathbf{N}^*)$  is the cyclic group  $Z_m$ .

**Exercise 1.9.10.** The operation of free product is communicative and associative: for any groups  $A, B, C$ ,  $A * B \cong B * A$  and  $A * (B * C) \cong (A * B) * C$ .

**Exercise 1.9.11.** If  $N$  is normal subgroup of  $A * B$  generated by  $A$ , then  $(A * B)/N \cong B$ .

**Exercise 1.9.12.** If  $G$  and  $H$  each have more than one element, then  $G * H$  is an infinite group with center  $\langle e \rangle$ .



**Exercise 1.9.13.** A free group is a free product of infinite cyclic groups.

**Exercise 1.9.14.** If  $G$  is the group defined by generators  $a, b$  and relations  $a^2 = e, b^3 = e$ , then  $G \cong Z_2 * Z_3$ .

**Exercise 1.9.15.** If  $f : G_1 \rightarrow G_2$  and  $g : H_1 \rightarrow H_2$  are homomorphisms of groups, then there is a unique homomorphism  $h : G_1 * H_1 \rightarrow G_2 H_2$  such that  $h|_{G_1} = f$  and  $h|_{H_1} = g$ .