

# Contemporary Abstract Algebra - Joseph A. Gillian \*

Zhenyong Shin

July 2021

## 0 Preliminaries

### 0.1 Properties of Integers

**Axiom 0.1** (Well Ordering Principle). *Every nonempty set of positive integers contains a smallest number.*

**Note 0.1.** An integer  $t \in \mathbb{Z}, t > 0$  is a *divisor* of  $s \in \mathbb{Z}$  if  $\exists u \in \mathbb{Z} : s = tu$  or  $t \mid s$  ( $t$  divides  $s$ ). If  $t$  is not a divisor of  $s$  then  $t \nmid s$ . A *prime* is a positive integer greater than 1 whose only positive divisors are 1 and itself.  $s \in \mathbb{Z}$  is a *multiple* of  $t \in \mathbb{Z}$  if  $\exists u \in \mathbb{Z} : s = tu$  or  $t \mid s$ .

**Theorem 0.1** (Division Algorithm). *Let  $a, b \in \mathbb{Z}, b > 0$ . Then*

$$\exists! q, r \in \mathbb{Z} : a = bq + r, 0 \leq r < b.$$

*$q$  is the quotient upon dividing  $a$  by  $b$ ,  $r$  is the remainder upon dividing  $a$  by  $b$ .*

*Proof.* Existence: Consider the set  $S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}$ . If  $0 \in S$ , then

$$0 = a - bk \implies a = bk$$

and thus  $b \mid a$ . Let  $q = a/b, r = 0$ , then

$$a = bq + 0,$$

as desired. If  $0 \notin S$ , then since  $S$  is nonempty because

$$a > 0 \implies a - b \cdot 0 \in S$$

---

\*Recorded lectures available at: [https://www.youtube.com/watch?v=lx3qJ-zjn5Y&list=PLmU0F1lJY-Mn3Pt-r5zQ\\_-Ar8mAnBZTf2&t=0s](https://www.youtube.com/watch?v=lx3qJ-zjn5Y&list=PLmU0F1lJY-Mn3Pt-r5zQ_-Ar8mAnBZTf2&t=0s)

and

$$a < 0 \implies a - b(2a) = a(1 - 2b) \in S,$$

and  $a \neq 0$  since  $0 \notin S$ . It follows that by the Well Ordering Principle,  $S$  has a smallest member, say  $r = a - bq$ . Then  $a = bq + r, r \geq 0$ , so all that remains to be proved is that  $r < b$ .

Assume  $r \geq b$ , then

$$a - b(q + 1) = a - bq - b = r - b \geq 0,$$

so  $a - b(q + 1) \in S$ . But  $a - b(q + 1) < a - bq$ , this contradicts that  $r = a - bq$  is the smallest member of  $S$ . Thus  $r < b$  and

$$\exists q, r \in \mathbb{Z} : a = bq + r, 0 \leq r < b,$$

as desired.

Uniqueness: Assume

$$\exists q, q', r, r' \in \mathbb{Z} : a = bq + r, 0 \leq r < b \quad \text{and} \quad a = bq' + r', 0 \leq r' < b.$$

For convenience, assume  $r' \geq r$ . Then

$$bq + r = bq' + r' \implies b(q - q') = r' - r.$$

So  $b \mid (r' - r)$  and  $0 \leq r' - r \leq r' < b$ , hence  $r' - r = 0$ , and  $r' = r, q' = q$ .  $\square$

**Example 0.1.** For  $a = 17, b = 5$ , the division algorithm gives  $17 = 5 \cdot 3 + 2$ . For  $a = -23, b = 6$ , the division algorithm gives  $-23 = 6(-4) + 1$ .

**Definition 0.1.** The *greatest common divisor* (gcd) of two nonzero integers  $a, b$  is the largest common divisors of  $a, b$ , denoted by  $\gcd(a, b)$ . If  $\gcd(a, b) = 1$ , then  $a, b$  are *relatively prime*.

**Theorem 0.2** (GCD is a Linear Combination).

$$\forall a, b \in \mathbb{Z}, a \neq 0, b \neq 0, \exists s, t \in \mathbb{Z} : \gcd(a, b) = as + bt.$$

Moreover,  $\gcd(a, b)$  is the smallest positive integer of the form  $as + bt$ .

*Proof.* Consider the set  $S = \{am + bn : m, n \in \mathbb{Z}, am + bn > 0\}$ . If  $a, b < 0$ , then let  $m, n < 0$  so that  $am + bn > 0$ . Hence  $S \neq \emptyset$ . By the Well Ordering Principle,  $S$  has a smallest member. Let  $d = as + bt$  be the smallest member of

$S$ . WTS  $d = \gcd(a, b)$ . Since  $d > 0$ , by Theorem 0.1,  $a = dq + r, 0 \leq r < d$ . If  $r > 0$ , then

$$\begin{aligned} r &= a - dq \\ &= a - (as + bt)q \\ &= a - asq + btq \\ &= a(1 - sq) + b(-tq) \in S. \end{aligned}$$

Since  $0 \leq r < d$  and  $r \in S$ , this contradicts that  $d$  is the smallest member of  $S$ . Hence,  $r = 0$  and  $a = dq \implies d \mid a$ . Similarly,  $d \mid b$ . Hence  $d$  is a common divisor of  $a, b$ .

Let  $d'$  be a common divisor of  $a, b$ , so  $a = d'h, b = d'k$ . Then

$$\begin{aligned} d &= as + bt \\ &= (d'h)s + (d'k)t \\ &= d'(hs + kt), \end{aligned}$$

so  $d' \mid d$  and  $d' \leq d$ . Hence  $d = \gcd(a, b)$ . □

**Corollary 0.2.1.**

$$a, b \in \mathbb{Z}, \gcd(a, b) = 1 \iff \exists s, t \in \mathbb{Z} : as + bt = 1.$$

**Example 0.2.**

$$\begin{aligned} \gcd(4, 15) &= 1 \\ \gcd(4, 10) &= 2 \\ \gcd(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2) &= 2 \cdot 3^2. \end{aligned}$$

4 and 15 are relatively prime whereas 4 and 10 are not. Also,

$$4 \cdot 4 + 15(-1) = 1 \quad \text{and} \quad 4(-2) + 10 \cdot 1 = 2.$$

**Example 0.3.** For any integer  $n$  the integers  $n+1$  and  $n^2+n+1$  are relatively prime. Since

$$\begin{aligned} (n^2 + n + 1)(1) + (n + 1)(-n) &= n^2 + n + 1 - n(n + 1) \\ &= n^2 + n + 1 - n^2 - n \\ &= 1. \end{aligned}$$

**Lemma 0.1** (Euclid's Lemma). *Let  $p$  be a prime, then*

$$p \mid ab \implies p \mid a \vee p \mid b.$$

*Proof.* Assume  $p$  is a prime such that  $p \mid ab$  but  $p \nmid a$ . WTS  $p \mid b$ . Since  $p \nmid a$ , and the only integer that divides  $p$  is 1,  $\gcd(a, p) = 1$  and

$$\exists s, t \in \mathbb{Z} : 1 = as + pt.$$

Then

$$\begin{aligned} b(1) &= b(as + pt) \\ b &= bas + bpt \\ &= abs + ptb. \end{aligned}$$

Since  $p$  divides the RHS of this equation, it follows that  $p \mid b$ .  $\square$

**Theorem 0.3** (Fundamental Theorem of Arithmetic). *Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear. If*

$$n = p_1 p_2 \dots p_r \quad \text{and} \quad n = q_1 q_2 \dots q_s,$$

*where the  $p$ 's and  $q$ 's are primes, then  $r = s$  and, after renumbering the  $q$ 's,  $p_i = q_i, \forall i \in \mathbb{N}$ .*

**Example 0.4.** Let  $n \in \mathbb{Z}, n > 1$ ,  $\sqrt[n]{2}$  is irrational. Since if  $\sqrt[n]{2} = a/b, a, b \in \mathbb{Z}$ , and  $a/b$  is in lowest terms, then  $a^n = 2b^n$ . By Theorem 0.3,  $2 \mid a$ , say  $a = 2c$ . Then  $2^n c^n = 2b^n$  and therefore  $2^{n-1} c^n = b^n$ . But this implies  $2 \mid b$ . This contradicts that  $a/b$  is in lowest terms.

**Definition 0.2.**  $\forall a, b \in \mathbb{Z}$ ,  $\text{lcm}(a, b)$  is the smallest positive integer that is a multiple of both  $a, b$ .

**Note 0.2.** Proof that  $m = \text{lcm}(a, b), \forall s \in \mathbb{N} : a, b \mid s \implies m \mid s$ .

Let  $m = \text{lcm}(a, b)$  and let  $s \in \mathbb{N} : a, b \mid s$  be arbitrary. By Theorem 0.1,

$$\exists q, r \in \mathbb{Z} : s = mq + r, 0 < r \leq m.$$

Since

$$a, b \mid s \implies a, b \mid mq + r.$$

it follows that  $a, b \mid r$ . But

$$a, b \mid r, m = \text{lcm}(a, b), 0 < r \leq m \implies r = 0.$$

Hence  $s = mq, q \in \mathbb{Z} \implies m \mid s$ .

**Example 0.4.**

$$\begin{aligned}\text{lcm}(4, 6) &= 12 \\ \text{lcm}(4, 8) &= 8 \\ \text{lcm}(10, 12) &= 60 \\ \text{lcm}(6, 5) &= 30 \\ \text{lcm}(2^2 \cdot 3^2 \cdot 5, 3^3 \cdot 7^2) &= 2^2 \cdot 3^3 \cdot 5 \cdot 7^2.\end{aligned}$$

## 0.2 Modular Arithmetic

**Note 0.3.** If  $a = qn + r$ , where  $q$  is quotient and  $r$  is the remainder upon dividing  $a$  by  $n$ , then  $a \bmod n = r$ . In general, if  $a, b, n \in \mathbb{Z}$ ,  $n$  is positive, then

$$a \bmod n = b \bmod n \iff n \mid (a - b).$$

Moreover,

$$\begin{aligned}ab \bmod n &= (a \bmod n)(b \bmod n) \bmod n, \\ (a + b) \bmod n &= (a \bmod n + b \bmod n) \bmod n.\end{aligned}$$

## 0.3 Complex Numbers

**Theorem 0.4** (Properties of Complex Numbers). (i)  $(a + bi) + (c + di) = (a + c) + (b + d)i$  (closure under addition).

(ii)  $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$  (closure under multiplication).

(iii)  $\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \frac{c-di}{c-di} = \frac{(ac+bd) + (bc-ad)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i, c + di \neq 0$  (closure under division).

(iv)  $(a + bi)(a - bi) = a^2 + b^2$  (complex conjugation).

(v)  $\forall a + bi \in \mathbb{C}, a + bi \neq 0, \exists c + di \in \mathbb{C} : (a + bi)(c + di) = 1$  (inverses).

(vi)  $\forall a + bi = r(\cos \theta + i \sin \theta) \in \mathbb{C}, \forall n \in \mathbb{N}, (a + bi)^n = (r(\cos \theta + i \sin \theta))^n = r^n(\cos n\theta + i \sin n\theta)$  (powers).

(vii)  $\forall a + bi = r(\cos \theta + i \sin \theta) \in \mathbb{C}, \forall n \in \mathbb{N}, \sqrt[n]{r(\cos \theta + i \sin \theta)} = \sqrt[n]{r} \left( \cos \frac{\theta + 2\pi k}{n} + i \sin \frac{\theta + 2\pi k}{n} \right), k = 0, 1, \dots, n - 1$  ( $n^{\text{th}}$  roots of  $a + bi$ ).

## 0.4 Mathematical Induction

**Theorem 0.5** (First Principle of Mathematical Induction). *Let  $a \in S \subseteq \mathbb{Z}$ . Then*

$$(k \in \mathbb{Z}, k \geq a, k \in S \implies k + 1 \in S) \implies S = \{k \in \mathbb{Z} : k \geq a\}.$$

**Theorem 0.6** (Second Principle of Mathematical Induction). *Let  $a \in S \subseteq \mathbb{Z}$ . Then*

$$(n \in \mathbb{Z}, \forall k \in \mathbb{Z}, a \leq k < n, k \in S \implies n \in S) \implies S = \{k \in \mathbb{Z} : k \geq a\}.$$

## 0.5 Equivalence Relations

**Definition 0.3.** An equivalence relation on a set  $S$  is a set  $R$  of ordered pairs of elements of  $S$  s.t.

1.  $\forall a \in S, (a, a) \in R$  (reflexive property).
2.  $(a, b) \in R \implies (b, a) \in R$  (symmetric property).
3.  $(a, b) \in R, (b, c) \in R \implies (a, c) \in R$  (transitive property).

**Note 0.4.** A suggestive symbol  $\approx, \equiv, \sim$  is usually used to denote the relation. Using this notation, the three conditions for an equivalence become

1.  $\forall a \in S, a \sim a$ .
2.  $a \sim b \implies b \sim a$ .
3.  $a \sim b, b \sim c \implies a \sim c$ .

**Definition 0.4.** If  $\sim$  is an equivalence relation on a set  $S$  and  $a \in S$ , then the set  $[a] = \{x \in S : x \sim a\}$  is the *equivalence class of  $S$  containing  $a$* .

**Example 0.5.** Let  $S$  be the set of all triangles in a plane. If  $a, b \in S$ , define  $a \sim b$  if  $a, b$  have corresponding angles that are the same. Then,  $\sim$  is an equivalence relation on  $S$ .

**Example 0.6.** Let  $S$  be the set of all polynomials with real coefficients. If  $f, g \in S$ , define  $f \sim g$  if  $f' = g'$ , where  $f'$  is the derivative of  $f$ . Then  $\sim$  is an equivalence relation on  $S$ . Since two polynomials with equal derivatives differ by a constant,  $\forall f \in S, [f] = \{f + c : c \in \mathbb{R}\}$ .

**Example 0.7.** Let  $S = \mathbb{Z}, n \in \mathbb{N}$ . If  $a, b \in S$ , define  $a \approx b$  if  $a \bmod n = b \bmod n$ . Then  $\approx$  is an equivalence relation on  $S$  and  $[a] = \{a + kn : k \in \mathbb{Z}\}$ .

Since  $n \mid a - a$ , it follows that  $\forall a \in S, a \equiv a$ . Next, assume that  $a \equiv b$ , say,  $a - b = rn$ . Then,  $b - a = (-r)n$ , and therefore  $b \equiv a$ . Finally, assume that  $a \equiv b, b \equiv c$ , say,  $a - b = rn, b - c = sn$ . Then,

$$a - c = (a - b) + (b - c) = rn + sn = (r + s)n,$$

so  $a \equiv c$ .

**Definition 0.5.** A partition of a set  $S$  is a collection of nonempty disjoint subsets of  $S$  whose union is  $S$ .

**Example 0.8.** The sets  $\{0\}, \{1, 2, 3, \dots\}, \{\dots, -3, -2, -1\}$  constitute a partition of  $\mathbb{Z}$ .

**Example 0.9.**  $\mathbb{N}, \mathbb{Z}^-$  do not partition  $\mathbb{Z}$  since both contain 0.

**Theorem 0.7** (Equivalence Classes Partition). *The equivalence classes of an equivalence relation on a set  $S$  constitute a partition of  $S$ . Conversely, for any partition  $P$  of  $S$ , there is an equivalence relation on  $S$  whose equivalence classes are the elements of  $P$ .*

*Proof.* Let  $\sim$  be an equivalence relation on a set  $S$ . By the reflexive property,  $\forall a \in S, a \in [a]$ . So  $[a]$  is nonempty and the union of all equivalence classes is  $S$ . Assume  $[a], [b]$  are distinct equivalence classes. WTS  $[a] \cap [b] = \emptyset$ . For the sake of contradiction, assume  $c \in [a] \cap [b]$ . Let  $x \in [a]$ , then  $c \sim a, c \sim b$ , and  $x \sim a$ . By the symmetric property,  $a \sim c$ . Thus by transitivity,  $x \sim c, x \sim b$ . This proves  $[a] \subseteq [b]$ . Similarly,  $[b] \subseteq [a]$  and hence  $[a] = [b]$ . This contradicts that  $[a], [b]$  are distinct equivalence classes and hence  $[a] \cap [b] = \emptyset$ .  $\square$

## 0.6 Functions (Mappings)

**Definition 0.6** (Function (Mapping)). A function/mapping  $\phi : A \rightarrow B$  is a rule that assigns to each  $a \in A$  exactly one  $b \in B$ . The set  $A$  is the domain of  $\phi$ , and  $B$  is the range of  $\phi$ . If  $\phi(a) = b$ , then  $b$  is the image of  $a$  under  $\phi$ . The subset of  $B$  comprising all the images of elements of  $A$  is the image of  $A$  under  $\phi$ .

**Definition 0.7** (Composition of Functions). Let  $\phi : A \rightarrow B$  and  $\psi : B \rightarrow C$ . The composition  $\psi\phi : A \rightarrow C$  is defined as  $(\psi\phi)(a) = \psi(\phi(a)), \forall a \in A$ .

**Definition 0.8.** A function  $\phi$  from a set  $A$  is *one-to-one* if

$$\forall a_1, a_2 \in A, \phi(a_1) = \phi(a_2) \implies a_1 = a_2$$

or

$$\forall a_1, a_2 \in A, a_1 \neq a_2 \implies \phi(a_1) \neq \phi(a_2).$$

**Definition 0.9.** A function  $\phi : A \rightarrow B$  is *onto* if

$$\forall b \in B, \exists a \in A : \phi(a) = b.$$

**Theorem 0.8** (Properties of Functions). *Given functions  $\alpha : A \rightarrow B, \beta : B \rightarrow C, \gamma : C \rightarrow D$ , then*

(i)  $\gamma(\beta\alpha) = (\gamma\beta)\alpha$  (*associativity*).

(ii)  $\alpha, \beta$  are one-to-one  $\implies \beta\alpha$  is one-to-one.

(iii)  $\alpha, \beta$  are onto  $\implies \beta\alpha$  is onto.

(iv)  $\alpha$  is one-to-one and onto  $\implies \exists \alpha^{-1} : B \rightarrow A$  s.t.  $(\alpha^{-1}\alpha)(a) = a, \forall a \in A$  and  $(\alpha\alpha^{-1})(b) = b, \forall b \in B$ .

*Proof.* (i) Let  $a \in A$ . Then

$$(\gamma(\beta\alpha))(a) = \gamma((\beta\alpha)(a)) = \gamma(\beta(\alpha(a))).$$

But

$$((\gamma\beta)\alpha)(a) = (\gamma\beta)(\alpha(a)) = \gamma(\beta(\alpha(a))).$$

Hence  $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ . □

## 1 Introduction to Groups

## 2 Groups

### 2.1 Definition and Examples of Groups

**Definition 2.1.** If  $G$  is a set. A *binary operation* on  $G$  is a function that assigns each ordered pair  $(a, b) : a, b \in G$  an element of  $G$ .



**Definition 2.2.** If  $G$  is a set with a binary operation that assigns to each ordered pair  $(a, b) : a, b \in G$  an element  $ab \in G$ . Then  $G$  is a group under the binary operation, with properties

- (i)  $a, b, c \in G, a(bc) = (ab)c$  (associativity).
- (ii)  $\exists e \in G : \forall a \in G, ae = ea = a$ , where  $e$  is the *identity element* (identity).
- (iii)  $\forall a \in G, \exists b \in G : ab = ba = e$ , where  $b$  is the inverse of  $a$  (inverses).

If  $G$  has the property that  $\forall a, b \in G, ab = ba$ , then  $G$  is *abelian*.

**Example 2.1.** 1.  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  are groups under addition. In each case, the identity element is 0 and the inverse of  $a$  is  $-a$ . For  $\mathbb{Z}$ ,

- (i)  $\forall a, b, c \in \mathbb{Z}, a+(b+c) = (a+b)+c$ .
- (ii)  $\exists 0 \in \mathbb{Z} : \forall a \in \mathbb{Z}, a+0 = 0+a = a$ .
- (iii)  $\forall a \in \mathbb{Z}, \exists -a \in \mathbb{Z} : a+(-a) = (-a)+a = 0$ .

The same applies to  $\mathbb{Q}, \mathbb{R}$ .

- 2.  $\mathbb{Z}$  under multiplication is not a group. Since 1 is the identity element,  $\forall a \in \mathbb{Z}$ , there does not exist an  $b \in \mathbb{Z} : ab = ba = 1$ .
- 3. The subset  $\{1, -1, i, -i\}$  of  $\mathbb{C}$  is a group under complex multiplication. Since

- (i)  $\forall a, b, c \in \{1, -1, i, -i\}, a(bc) = (ab)c$ . For example,  $1(i(-i)) = 1(-i^2) = 1(-(-1)) = 1$  and  $(1i)(-i) = i(-i) = -i^2 = -(-1) = 1$ .
- (ii)  $\exists 1 \in \{1, -1, i, -i\} : \forall a \in \{1, -1, i, -i\}, a1 = 1a = a$ .
- (iii)  $\forall a \in \{1, -1, i, -i\}, \exists b \in \{1, -1, i, -i\} : ab = ba = 1$ . For example,  $-1(-1) = -1(-1) = 1$  and  $i(-i) = (-i)i = -i^2 = 1$ .

- 4.  $\mathbb{Q}^+$  is a group under multiplication. Since

- (i)  $\forall a, b, c \in \mathbb{Q}^+, a(bc) = (ab)c$ . For example,  $\frac{1}{2}(\frac{2}{3}\frac{3}{4}) = \frac{1}{2}\frac{6}{12} = \frac{6}{24} = \frac{1}{4}$  and  $(\frac{1}{2}\frac{2}{3})\frac{3}{4} = \frac{2}{6}\frac{3}{4} = \frac{6}{24} = \frac{1}{4}$ .
- (ii)  $\exists 1 \in \mathbb{Q}^+ : \forall a \in \mathbb{Q}^+, a(1) = 1(a) = a$ .
- (iii)  $\forall a \in \mathbb{Q}^+, \exists b \in \mathbb{Q}^+ : ab = ba = 1$ . For example,  $\frac{2}{3}(\frac{3}{2}) = \frac{3}{2}(\frac{2}{3}) = 1$ .

- 5.  $S = \mathbb{I}^+ \cup \{1\}$  under multiplication is not a group. Since  $\sqrt{2}(\sqrt{2}) = 2 \notin S$ , so  $S$  is not closed under multiplication.
- 6.  $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\}, a, b, c, d \in \mathbb{R}$  is a group under matrix addition. The identity element is  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ , and the inverse of  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  is  $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ .
- 7.  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}, n \geq 1$  is a group under addition modulo  $n$ . Since

- (i)  $\forall a, b, c \in \mathbb{Z}_n, a(bc) = (ab)c$ . For example, for  $\mathbb{Z}_3 = \{0, 1, 2\}$  under addition modulo 3,  $0 + (1 + 2) = 0 + 3 = 3 = 0$  and  $(0 + 1) + 2 = 1 + 2 = 3 = 0$ .
  - (ii)  $\exists n \in \mathbb{Z}_n : \forall a \in \mathbb{Z}_n, a + n = n + a = a$ . For example, for  $\mathbb{Z}_3 = \{0, 1, 2\}$  under addition modulo 3,  $1 + 3 = 3 + 1 = 4 = 1$  and  $2 + 3 = 3 + 2 = 5 = 2$ .
  - (iii)  $\forall a \in \mathbb{Z}_n, \exists n - a \in \mathbb{Z}_n : a + (n - a) = (n - a) + a = n$ . For example, for  $\mathbb{Z}_3 = \{0, 1, 2\}$  under addition modulo 3, 3 is the identity element and  $1 + (3 - 1) = (3 - 1) + 1 = 3$ .
8. The set  $\mathbb{R}^*$  of nonzero real numbers is a group under multiplication. Since
- (a)  $\forall a, b, c \in \mathbb{R}^*, a(bc) = (ab)c$ .
  - (b)  $\exists 1 \in \mathbb{R}^* : \forall a \in \mathbb{R}^*, 1a = a1 = a$ .
  - (c)  $\forall a \in \mathbb{R}^*, \exists 1/a \in \mathbb{R}^* : a(1/a) = (1/a)a = 1$ .

9. The set

$$GL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

of  $2 \times 2$  matrices with real entries and nonzero determinants is a non-Abelian group under matrix multiplication

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}.$$

Since

- (a) For any two  $2 \times 2$  matrices  $A, B$ ,  $\det(AB) = (\det A)(\det B)$ . So the product of two matrices with nonzero determinants also has a nonzero determinant. Associativity can be verified by direct calculations.
- (b) The identity is  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ .
- (c) The inverse of  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  is

$$\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}.$$

In particular, the determinant of a matrix determines if it has an inverse. Another useful fact about determinants is  $\det A^{-1} = (\det A)^{-1}$ .

This very important non-Abelian group is the *general linear group* of  $2 \times 2$  matrices over  $\mathbb{R}$ .

10. The set of all  $2 \times 2$  matrices with real entries is not a group under matrix multiplication since inverses do not exist when  $\det A = 0$ .
11. Define

$$U(n) = \{k \in \mathbb{N} : k < n, \gcd(k, n) = 1\}, n > 1.$$

Then  $U(n)$  is a group under multiplication modulo  $n$ .

Group	Operation	Identity	Form of Element	Inverse	Abelian
$\mathbb{Z}$	Addition	0	$k$	$-k$	Yes
$Q^+$	Multiplication	1	$m/n, m, n > 0$	$n/m$	Yes
$\mathbb{Z}_n$	Addition mod $n$	0	$k$	$n - k$	Yes
$\mathbb{R}^*$	Multiplication	1	$x$	$1/x$	Yes
$\mathbb{C}^*$	Multiplication	1	$a + bi$	$\frac{1}{a^2 + b^2}a - \frac{1}{a^2 + b^2}bi$	Yes
$GL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, ad - bc \neq 0$	$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$	No
$U(n)$	Multiplication mod $n$	1	$k, \gcd(k, n) = 1$	Solution to $kx \bmod n = 1$	Yes
$\mathbb{R}^n$	Componentwise addition	$(0, 0, \dots, 0)$	$(a_1, a_2, \dots, a_n)$	$(-a_1, -a_2, \dots, -a_n)$	Yes
$SL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, ad - bc = 1$	$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	No
$D_n$	Composition	$R_0$	$R_\alpha, L$	$R_{360-\alpha}, L$	No

Figure 2.1: Summary of Group Examples ( $\mathbb{F}$  can be any of  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ , or  $\mathbb{Z}_p$ ;  $L$  is a reflection).

## 2.2 Elementary Properties of Groups

**Theorem 2.1** (Uniqueness of the Identity). *Let  $G$  be a group. Then*

$$e_1, e_2 \in G : \forall a \in G, ae_1 = e_1a = a, ae_2 = e_2a = a \implies e_1 = e_2.$$

*Proof.* Assume  $G$  is a group and  $\forall a \in G, \exists e_1, e_2 \in G : ae_1 = e_1a = a, ae_2 = e_2a = a$ .

In particular, let  $a = e_2$ , then  $e_2e_1 = e_1e_2 = e_2$ . Let  $a = e_1$ , then  $e_1e_2 = e_2e_1 = e_1$ . It follows that  $e_2e_1 = e_2$  and  $e_2e_1 = e_1$ . Hence  $e_1 = e_2$ .  $\square$

**Theorem 2.2** (Cancellation). *Let  $G$  be a group. Then  $\forall a, b, c \in G$ ,*

$$ba = ca \implies b = c \quad \text{and} \quad ab = ac \implies b = c.$$

*Proof.* Let  $G$  be a group. Then  $\forall a \in G, \exists a^{-1} \in G : aa^{-1} = a^{-1}a = e$ . If

$ba = ca$ , then by associativity,

$$\begin{aligned} ba &= ca \\ (ba)a^{-1} &= (ca)a^{-1} \\ b(aa^{-1}) &= c(aa^{-1}) \\ be &= ce \\ b &= c. \end{aligned}$$

If  $ab = ac$ , then by associativity,

$$\begin{aligned} ab &= ac \\ a^{-1}(ab) &= a^{-1}(ac) \\ (a^{-1}a)b &= (a^{-1}a)c \\ eb &= ec \\ b &= c. \end{aligned}$$

□

**Theorem 2.3** (Uniqueness of Inverses). *Let  $G$  be a group. Then*

$$b_1, b_2 \in G : \forall a \in G, ab_1 = b_1a = e, ab_2 = b_2a = e \implies b_1 = b_2.$$

*Proof.* Let  $G$  be a group. Assume that  $\forall a \in G, \exists b_1, b_2 : ab_1 = b_1a = e, ab_2 = b_2a = e$ . Then by associativity,

$$\begin{aligned} e &= ab_1 = ab_2 = e \\ b_1(ab_1) &= b_1(ab_2) \\ (b_1a)b_1 &= (b_1a)b_2 \\ eb_1 &= eb_2 \\ b_1 &= b_2. \end{aligned}$$

□

**Theorem 2.4** (Socks-Shoes Property).  *$G$  is a group  $\implies \forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}$ .*

*Proof.* Let  $G$  be a group and  $a, b \in G$ . So  $ab, (ab)^{-1} \in G$ . It follows that

$$\begin{aligned} (ab)(ab)^{-1} &= e, \\ b(ab)^{-1} &= a^{-1}e, \\ (ab)^{-1} &= b^{-1}a^{-1}e = b^{-1}a^{-1}. \end{aligned}$$

□

Multiplicative Group		Additive Group	
$a \cdot b$ or $ab$	Multiplication	$a + b$	Addition
$e$ or $1$	Identity or one	$0$	Zero
$a^{-1}$	Multiplicative inverse of $a$	$-a$	Additive inverse of $a$
$a^n$	Power of $a$	$na$	Multiple of $a$
$ab^{-1}$	Quotient	$a - b$	difference

Figure 2.2

## 3 Finite Groups; Subgroups

### 3.1 Terminology and Notation

**Definition 3.1.** The number of elements of a group (finite or infinite) is its *order*, denoted as  $|G|$ .

**Note 3.1.** The group  $\mathbb{Z}$  has infinite order. The group  $U(10) = \{1, 3, 7, 9\}$  under multiplication modulo 10 has order 4.

**Definition 3.2.** The order of  $g \in G$ , denoted by  $|g| = n$ , is the smallest  $n \in \mathbb{N} : g^n = e$ . If no such  $n$  exists, then  $|g| = \infty$ . In additive notation,  $\exists n \in \mathbb{N} : ng = 0 \implies |g| = n$ .

**Definition 3.3.** Let  $G$  be a group. If  $H \subseteq G$  is a group under the operation of  $G$ , then  $H$  is a *subgroup* of  $G$ , denoted  $H \leq G$ . If  $H$  is a *proper subgroup* of  $G$ , then  $H < G$ .

**Note 3.2.**  $H = \{e\}$  is the *trivial* subgroup of  $G$ .  $H \neq \{e\}$  is a *nontrivial* subgroup of  $G$ .

$\mathbb{Z}_n$  under addition modulo  $n$  is not a subgroup of  $\mathbb{Z}$  under addition, because addition modulo  $n$  is not the operation of  $\mathbb{Z}$ .

### 3.2 Subgroup Tests

**Theorem 3.1** (One-Step Subgroup Test). *Let  $G$  be a group and  $H \subseteq G, H \neq \emptyset$ . Then*

$$a, b \in H, ab^{-1} \in H \implies H \leq G.$$

*In additive notation,*

$$a, b \in H, a - b \in H \implies H \leq G.$$

*Proof.* Let  $G$  be a group and  $H \subseteq G, H \neq \emptyset$ . Assume that  $a, b \in H, ab^{-1} \in H$ .

Since the operation of  $H$  is the same operation in  $G$ , the operation is associative. Since  $H \neq \emptyset \implies \exists x \in H$ . Let  $a = x, b = x$ , then

$$e = xx^{-1} = ab^{-1} \in H.$$

So  $H$  has an identity  $e$ . Next, let  $a = e, b = x$ , then

$$x^{-1} = ex^{-1} = ab^{-1} \in H.$$

So  $x \in H \implies x^{-1} \in H$ . Finally, since  $y \in H \implies y^{-1} \in H$ , let  $a = x, b = y^{-1}$ , then

$$xy = x(y^{-1})^{-1} = ab^{-1} \in H.$$

So  $x, y \in H \implies xy \in H$ . Hence  $H$  is a group under the operation in  $G$  and by Definition 3.3,  $H \leq G$ .  $\square$

**Note 3.3.** Although Theorem 3.1 is called One-Step Subgroup Test, there are actually four steps involved in applying the theorem:

1. Identify the property  $P$  that distinguishes the elements of  $H$ . That is, identify a defining condition.
2. Prove that the identity element has property  $P$ . This verifies  $H \neq \emptyset$ .
3. Assume that  $a, b$  have property  $P$ .
4. Use the assumption that  $a, b$  have property  $P$  to show that  $ab^{-1}$  has property  $P$ .

**Example 3.1.** 1. Let  $G$  be an Abelian group with identity  $e$ . Then  $H = \{x \in G : x^2 = e\}$  is a subgroup of  $G$ . The defining property of  $H$  is the condition  $x^2 = e$ . First,  $e^2 = e$ , so  $e \in H$  and  $H \neq \emptyset$ . Now assume that  $a, b \in H, a^2 = e, b^2 = e$ . Finally, since  $G$  is Abelian,

$$(ab^{-1})^2 = ab^{-1}ab^{-1} = aab^{-1}b^{-1} = a^2(b^2)^{-1} = ee^{-1} = e.$$

Hence  $ab^{-1} \in H$  and by Theorem 3.1,  $H \leq G$ .

2. Let  $G$  be an Abelian group under multiplication with identity  $e$ . Then  $H = \{x^2 : x \in G\}$  is a subgroup of  $G$ . The defining property  $P$  is that the elements have the form  $x^2$ . Since  $e^2 = e$ , the identity has the correct form and  $e \in H \implies H \neq \emptyset$ . Next, write two elements in  $H$  in the correct forms  $a^2, b^2$ . Since  $G$  is Abelian,

$$a^2(b^2)^{-1} = a^2(b^{-1})^2 = aab^{-1}b^{-1} = ab^{-1}ab^{-1} = (ab^{-1})^2,$$

which is the correct form. Hence  $H \leq G$ .

**Theorem 3.2** (Two-Step Subgroup Test). *Let  $G$  be a group and  $H \subseteq G, H \neq \emptyset$ . If*

- (i)  $a, b \in H, ab \in H$  ( $H$  is closed under the operation), and
- (ii)  $a \in H, a^{-1} \in H$  ( $H$  is closed under taking inverses),

*then  $H \leq G$ .*

*Proof.* Let  $G$  be a group and  $H \subseteq G, H \neq \emptyset$ . Assume that  $a, b \in H, ab \in H$  and  $a \in H, a^{-1} \in H$ . Then since the operation of  $H$  is the same as the operation of  $G$ , the operation is associative in  $H$ . Next, let  $a \in H$ . Then  $a^{-1} \in H, aa^{-1} \in H$  and

$$e = aa^{-1} \in H.$$

Hence,  $H$  is a group under the operation of  $G$  and  $H \leq G$ .  $\square$

**Note 3.4.** When applying Theorem 3.2, one proceeds exactly as in the case of Theorem 3.1, except one uses the assumption that  $a, b$  have property  $P$  to prove that  $ab$  has property  $P$  and that  $a^{-1}$  has property  $P$ .

**Example 3.2.** Let  $G$  be an Abelian group. Then  $H = \{x \in G : |x| \neq \infty\}$  is a subgroup of  $G$ . Since  $e^1 = e$ , it follows that  $e$  has finite order so  $e \in H$  and hence  $H \neq \emptyset$ . To apply Theorem 3.2, assume that  $a, b \in H, |a| = m, |b| = n$ . Then, since  $G$  is Abelian,

$$(ab)^{mn} = (a^m)^n (b^n)^m = e^n e^m = e.$$

Thus,  $ab$  has finite order and  $ab \in H$ . This does not show that  $|ab| = mn$ , but  $|ab| \leq mn$ . Moreover,

$$(a^{-1})^m = (a^m)^{-1} = e^{-1} = e.$$

So  $a^{-1}$  has finite order and  $a^{-1} \in H$ .

**Note 3.5.** The next example illustrate how to use Theorem 3.2 by introducing an important technique for creating new subgroups of Abelian groups from existing ones.

**Example 3.3.** Let  $G$  be an Abelian group and  $H, K \leq G$ . Then  $HK = \{hk : h \in H, k \in K\}$  is a subgroup of  $G$ . Since  $e \in H, e \in K$ , it follows that  $e = ee \in HK$  and hence  $HK \neq \emptyset$ . Next, let  $a, b \in HK$ . Then by definition of  $HK$

$$\exists h_1, h_2 \in H, k_1, k_2 \in K : a = h_1 k_1, b = h_2 k_2.$$

Since  $G$  is Abelian and  $H, K \leq G$ , it follows that

$$ab = (h_1 k_1)(h_2 k_2) = (h_1 h_2)(k_2 k_1) \in HK,$$

since  $h_1 h_2 \in H, k_1 k_2 \in K$ . Likewise,

$$a^{-1} = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} = h_1^{-1} k_1^{-1} \in HK,$$

since  $h_1^{-1} \in H, k_1^{-1} \in K$ . Hence  $HK \leq G$ .

**Note 3.6.** Any of the following ways guarantees that  $H \subseteq G$  is not a subgroup of  $G$ .

1. Show that  $e \notin H$ .
2. Show  $\exists a \in H : a^{-1} \notin H$ .
3. Show  $\exists a, b \in H : ab \notin H$ .

**Example 3.4.** Let  $G$  be the group of nonzero real numbers under multiplication, let  $H = \{x \in G : x = 1 \vee x \in \mathbb{I}\}$  and  $K = \{x \in G : x \geq 1\}$ . Then  $H \not\leq G$ , since  $\sqrt{2} \in H$  but  $\sqrt{2}\sqrt{2} \notin H$ . Also,  $K \not\leq G$ , since  $2 \in K$  but  $2^{-1} \notin K$ .

**Theorem 3.3** (Finite Subgroup Test). *Let  $H$  be a nonempty finite subset of a group  $G$ . Then  $a, b \in H, ab \in H \implies H \leq G$ .*

*Proof.* Let  $G$  be a group, and let  $H \subseteq G$ ,  $H$  is nonempty and finite. Assume that  $a, b \in H, ab \in H$ .

If  $a = e$ , then

$$a^{-1} = e^{-1} = e = a \in H.$$

Since  $a, b \in H, ab \in H, a^{-1} \in H$ , by Theorem 3.2,  $H \leq G$ .

If  $a \neq e$ , consider the sequence  $a, a^2, \dots$ . Since  $a, b \in H, ab \in H$ , it follows that

$$\begin{aligned} a &\in H \\ a^2 &= aa \in H \\ a^3 &= aa^2 \in H \\ &\vdots \end{aligned}$$

and hence  $a, a^2, \dots \in H$ . Since  $H$  is finite, not all of these elements are distinct. Assume  $a^i = a^j, i > j$ . Then

$$\begin{aligned} a^i &= a^j \\ a^i a^{-j} &= a^j a^{-j} \\ a^{i-j} &= e. \end{aligned}$$

Since  $a \neq e$ , it follows that  $i - j > 1$ . Thus

$$aa^{i-j-1} = a^{i-j} = e$$

and hence  $a^{i-j-1} = a^{-1}$ . But  $i - j > 1 \implies i - j - 1 > 0 \implies a^{i-j-1} \in H$ . So  $a, b \in H, ab \in H, a^{-1} \in H$  and by Theorem 3.2,  $H \leq G$ .  $\square$



### 3.3 Examples of Subgroups

**Definition 3.4.**  $\forall a \in G, \langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \dots\}$ .

**Theorem 3.4** ( $\langle a \rangle$  is a Subgroup). *Let  $G$  be a group, and let  $a \in G$ . Then,  $\langle a \rangle \leq G$ .*

*Proof.* Let  $G$  be a group and  $a \in G$ . Since  $a \in \langle a \rangle$ , it follows that  $\langle a \rangle \neq \emptyset$ . Let  $a^n, a^m \in \langle a \rangle$ . Then,  $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$ . Hence by Theorem 3.1,  $\langle a \rangle \leq G$ .  $\square$

$\langle a \rangle$  is the *cyclic subgroup* of  $G$  generated by  $a$ . If  $G = \langle a \rangle$ , then  $G$  is *cyclic* and  $a$  is a generator of  $G$ . A cyclic group may have many generators. Although the list  $\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots$  has infinitely many entries, the set  $\{a^n : n \in \mathbb{Z}\}$  might have only finitely many elements. Also, since  $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$ , every cyclic group is Abelian.

**Example 3.5.** 1. For  $U(10) = \{1, 3, 7, 9\}$  under multiplication modulo 10, since

$$3^0 = 1, 3^1 = 3, 3^2 = 9, 3^3 = 7, 3^4 = 1, 3^5 = 3^4 \cdot 3^1 = 1 \cdot 3 = 3, \dots$$

and since  $3 \cdot 7 = 1$  and 1 is the identity, it follows that  $3^{-1} = 7$ . So

$$3^{-1} = 7, 3^{-2} = 3^{-1} 3^{-1} = 7 \cdot 7 = 9, 3^{-3} = 3^{-2} 3^{-1} = 9 \cdot 7 = 3, \dots$$

Hence  $\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$  under multiplication modulo 10.

2. For  $\mathbb{Z}_{10}$  under addition modulo 10, since

$$0(2) = 0, 1(2) = 2, 2(2) = 4, 3(2) = 6, 4(2) = 8, 5(2) = 0, 6(2) = 2, \dots$$

and since  $-2 = 10(-1) + 8$ , it follows that

$$-1(2) = 8, -2(2) = -4 = 6, -3(2) = -6 = 4, -4(2) = -8 = 2, \dots$$

Hence,  $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$  and since  $a, b \in \langle 2 \rangle \implies ab \in \langle 2 \rangle$ . For instance,

$$0 \cdot 2 = 0, 2 \cdot 4 = 8, 8 \cdot 8 = 4, \dots \in \langle 2 \rangle.$$

Hence by Theorem 3.3,  $\langle 2 \rangle = \{2, 4, 6, 8, 0\} \leq \mathbb{Z}_{10}$ .

3. For  $\mathbb{Z}$ , since

$$\begin{aligned} \langle -1 \rangle &= \{\dots, -2(-1), -1(-1), 0(-1), 1(-1), 2(-1), \dots\} \\ &= \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z}. \end{aligned}$$

Hence  $\langle -1 \rangle = \mathbb{Z}$ .

4.

5.

For any  $a \in G$ , it is useful to think of  $\langle a \rangle$  as the smallest subgroup of  $G$  containing  $a$ . This notion can be extended to any collection  $S$  of elements from  $G$  by defining  $\langle S \rangle$  as the subgroup of  $G$  with the property that  $S \in \langle S \rangle$  and if  $H$  is any subgroup of  $G$  containing  $S$ , then  $H$  also contains  $\langle S \rangle$ . Thus  $\langle S \rangle$  is the smallest subgroup of  $G$  that contains  $S$ .  $\langle S \rangle$  is the subgroup generated by  $S$ .

**Example 3.6.** In  $\mathbb{Z}_{20}$ ,  $\langle 8, 14 \rangle = \{0, 2, 4, \dots, 18\} = \langle 2 \rangle$ .

In  $\mathbb{Z}$ ,  $\langle 8, 13 \rangle = \mathbb{Z}$ .

In  $D_4$ ,  $\langle H, V \rangle = \{H, H^2, V, HV\} = \{R_0, R_{180}, H, V\}$ .

In  $D_4$ ,  $\langle R_9, V \rangle = \{R_{90}, R_{90}^2, R_{90}^3, R_{90}^4, V, R_{90}V, R_{90}^2V, R_{90}^3V\} = D_4$ .

**Definition 3.5.** The center of a group  $G$  is

$$Z(G) = \{a \in G : \forall x \in G, ax = xa\}.$$

**Theorem 3.5** ( $Z(G)$  is a Subgroup). *Let  $G$  be a group and  $Z(G)$  be the center of  $G$ . Then  $Z(G) \leq G$ .*

*Proof.* Let  $G$  be a group and  $Z(G)$  be the center of  $G$ . Since  $\forall x \in G, ex = xe$ , it follows that  $e \in Z(G)$  and hence  $Z(G) \neq \emptyset$ . Assume that  $a, b \in Z(G)$ , then since the operation of  $G$  is associative,

$$\forall x \in G, (ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

Hence  $ab \in Z(G)$ .

Next, assume that  $a \in Z(G)$ . Then  $\forall x \in G, ax = xa$  and

$$\begin{aligned} ax &= xa, \\ a^{-1}(ax)a^{-1} &= a^{-1}(xa)a^{-1}, \\ (a^{-1}a)xa^{-1} &= a^{-1}x(aa^{-1}), \\ exa^{-1} &= a^{-1}xe, \\ xa^{-1} &= a^{-1}x. \end{aligned}$$

Hence  $a^{-1} \in Z(G)$  and by Theorem 3.2,  $Z(G) \leq G$ . □

**Example 3.7.** Let  $n \geq 3$ . Observe that since  $R \in D_n$ ,  $R = (R_{360/n})^k, k \in \mathbb{Z}$ , so  $R, R' \in D_n, RR' = R'R$ . Let  $R \in D_n$  be any rotation and let  $F \in D_n$  be any reflection. Since  $RF$  is a reflection, it follows that

$$RF = (RF)^{-1} = F^{-1}R^{-1} = FR^{-1}.$$

Thus

$$RF = FR \iff FR = RF = FR^{-1}.$$

By cancellation,  $R = R^{-1}$ . But  $R = R^{-1}$  only when  $R = R_0$  or  $R = R_{180}$  and  $R_{180}$  is in  $D_n$  only when  $n$  is even. So,

$$Z(D_n) = \begin{cases} \{R_0, R_{180}\} & , n \text{ is even,} \\ \{R_0\} & , n \text{ is odd.} \end{cases}$$

**Definition 3.6.** Let  $a$  be a fixed element of a group  $G$ . The *centralizer* of  $a$  in  $G$  is

$$C(a) = \{g \in G : ga = ag\}.$$

**Theorem 3.6** ( $C(a)$  is a Subgroup). *Let  $G$  be a group. Then*

$$\forall a \in G, C(a) \leq G.$$

*Proof.* Let  $G$  be a group,  $a \in G$  be arbitrary, and  $C(a)$  be a centralizer of  $a$  in  $G$ . Since  $e \in G, ea = ae$ , it follows that  $e \in C(a)$  and hence  $C(a) \neq \emptyset$ . Assume that  $x, y \in C(a)$ . Then, since the operation in  $G$  is associative,

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy).$$

Hence  $xy \in C(a)$ .

Next, assume that  $x \in C(a)$ . Then  $xa = ax$  and

$$\begin{aligned} xa &= ax, \\ x^{-1}(xa)x^{-1} &= x^{-1}(ax)x^{-1}, \\ (x^{-1}x)ax^{-1} &= x^{-1}a(xx^{-1}), \\ eax^{-1} &= x^{-1}ae, \\ ax^{-1} &= x^{-1}a. \end{aligned}$$

Hence  $x^{-1} \in C(a)$  and by Theorem 3.2,  $C(a) \leq G$ . □

Note that  $\forall a \in G, Z(G) \subseteq C(a)$ . Also,  $G$  is Abelian iff  $\forall a \in G, C(a) = G$ .

**Example 3.8.** In  $D_4$ ,

$$\begin{aligned} C(R_0) &= D_4 = C(R_{180}), \\ C(R_{90}) &= \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270}), \\ C(H) &= \{R_0, H, R_{180}, V\} = C(V), \\ C(D) &= \{R_0, D, R_{180}, D'\} = C(D'). \end{aligned}$$

## 4 Cyclic Groups

### 4.1 Properties of Cyclic Groups

**Definition 4.1.** Let  $G$  be a group. Then

$$\exists a \in G : G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\} \implies G \text{ is cyclic.}$$

$a \in G$  is a generator of  $G$ .

**Example 4.1.** 1.  $\mathbb{Z}$  under addition is cyclic. Since

$$\begin{aligned} \langle 1 \rangle &= \{n1 : n \in \mathbb{Z}\} \\ &= \{\dots, -2(1), -1(1), 0(1), 1(1), 2(1), \dots\} \\ &= \{\dots, -2, -1, 0, 1, 2, \dots\} \\ &= \mathbb{Z} \end{aligned}$$

and

$$\begin{aligned} \langle -1 \rangle &= \{n(-1) : n \in \mathbb{Z}\} \\ &= \{\dots, 2(-1), 1(-1), 0(-1), -1(-1), -2(-1), \dots\} \\ &= \{\dots, -2, -1, 0, 1, 2, \dots\} \\ &= \mathbb{Z}. \end{aligned}$$

Hence  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$  and  $-1, 1$  are the generators of  $\mathbb{Z}$ .

2.  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}, n \geq 1$  under addition modulo  $n$  is a cyclic group. Since

$$\begin{array}{ll} 1(1) = 1, & 0(1) = 0, \\ 2(1) = 2, & -1(1) = -1 = n-1, \\ \vdots & \vdots \\ (n-1)(1) = n-1, & -(n-1)(1) = 1, \\ n(1) = 0, & -n(1) = -n = 0, \\ \vdots & \vdots \end{array}$$

and

$$\begin{array}{ll} 1(-1) = -1 = n-1, & 0(-1) = 0, \\ 2(-1) = -2 = n-2, & -1(-1) = 1, \\ \vdots & \vdots \\ (n-1)(-1) = n-1, & -(n-1)(-1) = n-1, \\ \vdots & \vdots \end{array}$$

it follows that  $\mathbb{Z}_n = \langle 1 \rangle = \langle -1 \rangle$ . Hence  $1, -1 = n - 1$  are the generators of  $\mathbb{Z}_n$ .

3. For  $\mathbb{Z}_8$  under addition modulo 8. Since

$$\begin{aligned}\langle 1 \rangle &= \{1, 2, 3, 4, 5, 6, 7, 0\}, \\ \langle 3 \rangle &= \{3, 6, 1, 4, 7, 2, 5, 0\}, \\ \langle 5 \rangle &= \{5, 2, 7, 4, 1, 6, 3, 0\}, \\ \langle 7 \rangle &= \{7, 6, 5, 4, 3, 2, 1, 0\},\end{aligned}$$

it follows that  $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$ . Hence  $1, 3, 5, 7$  are the generators of  $\mathbb{Z}_8$ . On the other hand,  $2$  is not a generator since  $\langle 2 \rangle = \{2, 4, 6, 0\} \neq \mathbb{Z}_8$ .

4. For  $U(10) = \{1, 3, 7, 9\}$ , since  $\langle 3 \rangle = \{3, 9, 7, 1\}$ ,  $\langle 7 \rangle = \{7, 9, 3, 1\}$ , it follows that  $U(10) = \langle 3 \rangle = \langle 7 \rangle$ . Hence  $3, 7$  are generators of  $U(10)$ .
5. For  $U(8) = \{1, 3, 5, 7\}$ , since  $\langle 1 \rangle = \{1\}$ ,  $\langle 3 \rangle = \{3, 1\}$ ,  $\langle 5 \rangle = \{5, 1\}$ ,  $\langle 7 \rangle = \{7, 1\}$ , it follows that  $U(8) \neq \langle a \rangle, a \in U(8)$ . Hence  $U(8)$  is not cyclic.

**Theorem 4.1.** *Let  $G$  be a group and  $a \in G$ .*

$$(i) \quad |a| = \infty \implies (a^i = a^j \iff i = j).$$

$$(ii) \quad |a| = n \implies \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\} \text{ and } a^i = a^j \iff n \mid (i - j).$$

*Proof.* Let  $G$  be a group and  $a \in G$ .

(i) Assume that  $|a| = \infty$ . Then  $a^n \neq e, n \in \mathbb{N}$ .

( $\Rightarrow$ ) Assume that  $a^i = a^j$ . Then  $a^{i-j} = e$ , it follows that  $i - j = 0 \implies i = j$ .

( $\Leftarrow$ ) Assume that  $i = j$ . Then  $i - j = 0$  and hence  $a^{i-j} = a^0 = e \implies a^i = a^j$ .

Hence,  $|a| = \infty \implies (a^i = a^j \iff i = j)$ .

(ii) Assume that  $|a| = n$ , so  $a^n = e$ . Let  $a^k \in \langle a \rangle$  be arbitrary. By the division algorithm,

$$\exists q, r \in \mathbb{Z} : k = nq + r, 0 \leq r < n.$$

So

$$a^k = a^{nq+r} = a^{nq}a^r = (a^n)^qa^r = e^qa^r = ea^r = a^r.$$

Since  $0 \leq r < n$ , it follows that  $e \leq a^k < a^n$  and  $a^k \in \{e, a, a^2, \dots, a^{n-1}\}$ . Hence,  $\langle a \rangle \subseteq \{e, a, a^2, \dots, a^{n-1}\}$ .

Let  $a^k \in \{e, a, \dots, a^{n-1}\}$ . Then  $a^k \in \langle a \rangle = \{a^t : t \in \mathbb{Z}\}$  and  $\{e, a, \dots, a^{n-1}\} \subseteq$

$\langle a \rangle$ . Hence  $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ .

( $\Rightarrow$ ) Assume that  $a^i = a^j$ , so  $a^{i-j} = e$ . By the division algorithm,

$$\exists q, r \in \mathbb{Z} : i - j = nq + r, 0 \leq r < n.$$

So

$$e = a^{i-j} = a^{nq+r} = a^{nq}a^r = (a^n)^qa^r = e^qa^r = ea^r = a^r.$$

Since  $n$  is the smallest positive integer s.t.  $a^n = e$ , it follows that  $r = 0$  and  $i - j = nq \Rightarrow n \mid (i - j)$ .

( $\Leftarrow$ ) Assume that  $n \mid (i - j)$ , so  $i - j = nq$ . It follows that

$$a^{i-j} = a^{nq} = (a^n)^q = e^q = e$$

and hence  $a^i = a^j$ .

Hence  $|a| = n \Rightarrow \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$  and  $a^i = a^j \iff n \mid (i - j)$ .  $\square$

**Corollary 4.1.1.** *Let  $G$  be a group. Then  $\forall a \in G, |a| = |\langle a \rangle|$ .*

*Proof.* Let  $G$  be a group, let  $a \in G$  be arbitrary. Assume that  $|a| = n$ , then  $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ . It follows that  $|\langle a \rangle| = n$ .  $\square$

**Corollary 4.1.2.** *Let  $G$  be a group. Then  $\forall a \in G, a^k = e \iff |a| \mid k$ .*

*Proof.* From Theorem 4.1 (ii),  $a^k = e = a^0 \iff (n = |a|) \mid (k - 0 = k)$ .  $\square$

**Corollary 4.1.3.** *Let  $G$  be a group. Then  $\forall a \in G, a^k = e \iff k$  is a multiple of  $|a|$ .*

**Corollary 4.1.4.** *Let  $G$  be a finite group. Then*

$$a, b \in G, ab = ba \implies |ab| \mid |a||b|.$$

*Proof.* Let  $|a| = m, |b| = n$ . Then

$$(ab)^{mn} = (a^m)^n (b^n)^m = e^n e^m = e.$$

Hence by Corollary 4.1.2,  $|a| \mid mn = |a||b|$ .  $\square$

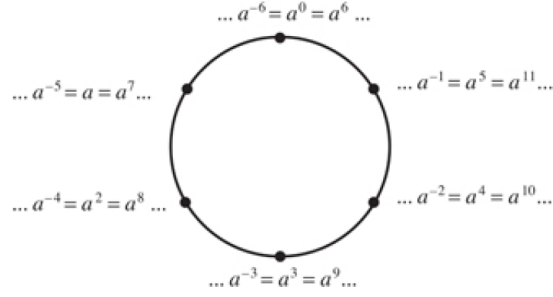


Figure 4.1: Powers of  $a$  for  $|a| = 6$ .

Figure 4.1 shows Theorem 4.1 and its corollaries for  $|a| = 6$ .

**Theorem 4.2.** *Let  $G$  be a group,  $a \in G$ ,  $|a| = n$ , and let  $k \in \mathbb{N}$ . Then*

- (i)  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and
- (ii)  $|a^k| = n / \gcd(n, k)$ .

*Proof.* Let  $G$  be a group,  $a \in G$ ,  $|a| = n$ , and let  $k \in \mathbb{N}$ .

(i) Let  $d = \gcd(n, k)$  and let  $k = dr$ . Since  $a^k = (a^d)^r \in \langle a^d \rangle$ , it follows that  $\langle a^k \rangle \subseteq \langle a^d \rangle$ . By Theorem 0.2,  $\exists s, t \in \mathbb{Z} : d = ns + kt$ . So

$$a^d = a^{ns+kt} = a^{ns} a^{kt} = (a^n)^s (a^k)^t = e (a^k)^t = (a^k)^t \in \langle a^k \rangle.$$

Hence,  $\langle a^d \rangle \subseteq \langle a^k \rangle$  and  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ .

(ii) Let  $d$  be any divisor of  $n$ . Then  $(a^d)^{n/d} = a^n = e \implies |a^d| \leq n/d$ . Let  $i \in \mathbb{N}, i < n/d$ . If  $(a^d)^i = a^{di} = e$ , then since  $|a| = n$ , it follows that  $di \geq n \implies i \geq n/d$ , contradicting that  $i < n/d$ . Hence  $|a^d| = n/d$ . Now let  $d = \gcd(n, k)$ , then

$$\begin{aligned} |a^k| &= |\langle a^k \rangle| \quad (\text{by Corollary 4.1.1}) \\ &= |\langle a^{\gcd(n,k)} \rangle| \quad (\text{by part (i)}) \\ &= |a^{\gcd(n,k)}| \\ &= |a^d| \\ &= n/d \\ &= n / \gcd(n, k). \end{aligned}$$

□

**Example 4.2.** 1. For  $|a| = 30$ , find  $\langle a^{26} \rangle, \langle a^{17} \rangle, \langle a^{18} \rangle, |a^{26}|, |a^{17}|, |a^{18}|$ .

Since  $\gcd(30, 26) = 2$ , by Theorem 4.2 (i),  $\langle a^{26} \rangle = \langle a^{\gcd(30, 26)} \rangle = \langle a^2 \rangle$ .  
Since

$$(a^2)^1 = a^2, (a^2)^2 = a^4, \dots, (a^2)^{14} = a^{28}, (a^2)^{15} = a^{30} = e, \\ (a^2)^{16} = a^{32} = a^{30}a^2 = ea^2 = a^2, (a^2)^{17} = a^{34} = a^{30}a^4 = ea^4 = a^4, \dots$$

and

$$(a^2)^0 = e, \\ (a^2)^{-1} = (a^2)^{-1} \cdot e = (a^2)^{-1}a^{30} = (a^2)^{-1}(a^2)^{15} = (a^2)^{14} = a^{28}, \\ (a^2)^{-2} = (a^2)^{-1}(a^2)^{-1} = a^{28}a^{28} = a^{56} = a^{30}a^{26} = a^{26}, \\ \vdots$$

it follows that  $\langle a^{26} \rangle = \langle a^2 \rangle = \{e, a^2, a^4, \dots, a^{26}, a^{28}\}$  and  $|a^{26}| = 30/\gcd(30, 26) = 30/2 = 15$ .

Since  $\gcd(30, 17) = 1$ , it follows that  $\langle a^{17} \rangle = \langle a^1 \rangle = \{e, a, a^2, \dots, a^{29}\}$  and  $|a^{17}| = 30/1 = 30$ .

Since  $\gcd(30, 18) = 6$ , it follows that  $\langle a^{18} \rangle = \langle a^6 \rangle$ . Since

$$(a^6)^1 = a^6, (a^6)^2 = a^{12}, (a^6)^3 = a^{18}, (a^6)^4 = a^{24}, (a^6)^5 = a^{30} = e, \dots$$

and

$$(a^6)^0 = e, (a^6)^{-1} = (a^6)^{-1}a^{30} = (a^6)^{-1}(a^6)^5 = (a^6)^4 = a^{24}, \dots,$$

it follows that  $\langle a^{18} \rangle = \langle a^6 \rangle = \{e, a^6, a^{12}, a^{18}, a^{24}\}$  and  $|a^{18}| = 30/\gcd(30, 18) = 30/6 = 5$ .

2. For  $|a| = 1000$ , find  $\langle a^{140} \rangle, \langle a^{400} \rangle, \langle a^{62} \rangle, |a^{140}|, |a^{400}|, |a^{62}|$ .

Since  $\gcd(1000, 140) = \gcd(2^3 5^3, 2^2 5 \cdot 7) = 2^2 5 = 20$ , it follows that  $\langle a^{140} \rangle = \langle a^{20} \rangle = \{e, a^{20}, a^{40}, a^{60}, \dots, a^{980}\}$  and  $|a^{140}| = 1000/20 = 50$ .

Since  $\gcd(1000, 400) = \gcd(2^3 5^3, 2^4 5^2) = 2^3 5^2 = 200$ , it follows that  $\langle a^{400} \rangle = \langle a^{200} \rangle = \{e, a^{200}, a^{400}, a^{600}, a^{800}\}$  and  $|a^{400}| = 1000/200 = 5$ .

Since  $\gcd(1000, 62) = \gcd(2^3 5^3, 2 \cdot 31) = 2$ , it follows that  $\langle a^{62} \rangle = \langle a^2 \rangle = \{e, a^2, a^4, a^6, a^{998}\}$  and  $|a^{62}| = 1000/2 = 500$ .

**Corollary 4.2.1.**  $G = \langle a \rangle, |G| = n \implies \forall g \in G, |g| \mid |G|$ .

*Proof.* Let  $G = \langle a \rangle, a \in G$  and  $|G| = |\langle a \rangle| = |a| = n$ . Let  $g \in G$  be arbitrary, since  $G = \langle a \rangle$ , it follows that  $g = a^k$ . By Theorem 4.2 (ii),

$$|g| = |a^k| = n/\gcd(n, k) = |G|/\gcd(n, k).$$



Hence,  $|a| \mid G, a \in G$ . □

**Corollary 4.2.2.** *Let  $|a| = n$ . Then*

$$(i) \quad \langle a^i \rangle = \langle a^j \rangle \iff \gcd(n, i) = \gcd(n, j), \text{ and}$$

$$(ii) \quad |a^i| = |a^j| \iff \gcd(n, i) = \gcd(n, j).$$

*Proof.* Let  $|a| = n$ .

(i)  $(\Rightarrow)$  Assume that  $\langle a^i \rangle = \langle a^j \rangle$ . By Theorem 4.2 (i),

$$\langle a^i \rangle = \langle a^j \rangle \implies \langle a^{\gcd(n, i)} \rangle = \langle a^{\gcd(n, j)} \rangle,$$

which implies that  $|a^{\gcd(n, i)}| = |a^{\gcd(n, j)}|$  since two sets are equal if they have the same members. By Theorem 4.2 (ii),

$$|a^{\gcd(n, i)}| = |a^{\gcd(n, j)}| \implies n / \gcd(n, i) = n / \gcd(n, j) \implies \gcd(n, i) = \gcd(n, j).$$

$(\Leftarrow)$  Assume that  $\gcd(n, i) = \gcd(n, j)$ . Then it follows that  $\langle a^i \rangle = \langle a^j \rangle$ .

(ii)  $(\Rightarrow)$  Assume that  $|a^i| = |a^j|$ . Then by Theorem 4.2 (ii),

$$|a^i| = |a^j|,$$

$$n / \gcd(n, i) = n / \gcd(n, j),$$

$$\gcd(n, i) = \gcd(n, j).$$

$(\Leftarrow)$  Assume that  $\gcd(n, i) = \gcd(n, j)$ . Then

$$\gcd(n, i) = \gcd(n, j),$$

$$n \cdot \gcd(n, i) = n \cdot \gcd(n, j),$$

$$n / \gcd(n, i) = n / \gcd(n, j),$$

$$|a^i| = |a^j| \quad (\text{by Theorem 4.2 (ii)}).$$

□

**Corollary 4.2.3.** *Let  $|a| = n$ . Then*

$$(i) \quad \langle a \rangle = \langle a^j \rangle \iff \gcd(n, j) = 1, \text{ and}$$

$$(ii) \quad |a| = |a^j| \iff \gcd(n, j) = 1.$$

**Example 4.3.** For  $U(50) = \{1, 3, 7, 9, 11, 13, 17, 19, \dots, 47, 49\}$ ,  $|U(50)| = 20$ . Since

$$3^1 \bmod 50 = 3, 3^2 \bmod 50 = 9, 3^3 \bmod 50 = 27, 3^4 \bmod 50 = 31, \dots,$$

$$3^0 \bmod 50 = 1, 3^{-1} \bmod 50 = 3^{19} \bmod 50 = 17, \dots,$$

it follows that  $U(50) = \langle 3 \rangle$  and 3 is a generator of  $U(50)$ . By Corollary 4.2.3,  $\gcd(50, 3) = 1 \iff \langle 3 \rangle = \langle 3^3 \rangle$ , so  $U(50) = \langle 3 \rangle = \langle 3^3 \rangle = \langle 27 \rangle$  and 27 is a generator of  $U(50)$ . The complete list of generators of  $U(50)$  is

$$\begin{aligned} 3^1 \bmod 50 &= 3, 3^3 \bmod 50 = 27, 3^7 \bmod 50 = 37, 3^9 \bmod 50 = 33, \\ 3^{11} \bmod 50 &= 47, 3^{13} \bmod 50 = 23, 3^{17} \bmod 50 = 13, 3^{19} \bmod 50 = 17. \end{aligned}$$

**Corollary 4.2.4.**  $k \in \mathbb{Z}_n$  is a generator of  $\mathbb{Z}_n \iff \gcd(n, k) = 1$ .

## 4.2 Classification of Subgroups of Cyclic Groups

**Theorem 4.3** (Fundamental Theorem of Cyclic Groups). *Let  $G$  be cyclic. Then*

$$H \leq G \implies H \text{ is cyclic.}$$

*Moreover, if  $|\langle a \rangle| = n$ , then*

1.  $H \leq \langle a \rangle \implies |H| \mid n$ .
2.  $k \mid n, k > 0, \exists H \leq \langle a \rangle : |H| = k, H = \langle a^{n/k} \rangle$ .

*Proof.* Let  $G$  be a cyclic group, so  $\exists a \in G: G = \langle a \rangle$ .

(i) Assume that  $H \leq G = \langle a \rangle$ . If  $H = \{e\}$ , then  $H$  is cyclic. If  $H \neq \{e\}$ , then

$$H \leq G = \langle a \rangle \implies \forall x \in H, x = a^t, t \in \mathbb{Z}.$$

If  $a^t \in H, t < 0$ , then

$$H \leq G \implies a^{-t} \in H, -t > 0.$$

Hence  $\exists a^t \in H, t > 0$ . Let  $m = \min\{t \in \mathbb{N} : a^t \in H\}$ . Then by closure,  $(a^m)^t \in H, t \in \mathbb{Z}$ . Hence  $\langle a^m \rangle \subseteq H$ .

Let  $b \in H$  be arbitrary. Then

$$H \leq G = \langle a \rangle \implies b = a^k, k \in \mathbb{Z}.$$

By the division algorithm,

$$\exists q, r \in \mathbb{Z} : k = mq + r, 0 \leq r < m.$$

So

$$a^k = a^{mq+r} = a^{mq} a^r$$

and

$$a^r = a^{-mq} a^k = (a^m)^{-q} a^k.$$

By closure,

$$(a^m)^{-q}, a^k \in H \implies a^{-mq}a^k = a^r \in H.$$

But

$$a^m \in H, m = \min\{t \in \mathbb{N} : a^t \in H\}, 0 \leq r < m \implies r = 0,$$

so

$$k = mq + r = mq \quad \text{and} \quad a^k = a^{mq}a^r = a^{mq} = (a^m)^q.$$

Hence,

$$a^k \in \langle a^m \rangle \implies H \subseteq \langle a^m \rangle$$

and

$$\langle a^m \rangle \subseteq H, H \subseteq \langle a^m \rangle \implies H = \langle a^m \rangle.$$

(ii) Let  $|G| = |\langle a \rangle| = n$ . Then

(a) Assume that  $H \leq G = \langle a \rangle$ . Then by Theorem 4.3 (i),  $H = \langle a^m \rangle$  and  $a^k \in H = \langle a^m \rangle \implies k = mq, q \in \mathbb{Z}$ . Since

$$|G| = |\langle a \rangle| = |a| = n \implies a^n = e \in H,$$

it follows that  $n = mq, q \in \mathbb{Z}$ . Let  $|H| = k$ , then by Theorem 4.2 (ii),

$$k = |H| = |\langle a^m \rangle| = |a^m| = n / \gcd(n, m) = n/m$$

and

$$n = km \implies k \mid n.$$

(b) Let  $k \in \mathbb{N} : k \mid n$  be arbitrary. Assume that  $H_1, H_2 \leq G = \langle a \rangle$  and  $|H_1| = |H_2| = k$ . Let  $H_1 = \langle a^{m_1} \rangle, H_2 = \langle a^{m_2} \rangle$ , then

$$|a| = n, |H_1| = |H_2| = k \implies n = m_1 k, n = m_2 k \implies m_1 = m_2 = n/k.$$

Hence  $H_1 = H_2 = \langle a^{n/k} \rangle$ . □

**Example 4.4.** Let  $G = \langle a \rangle$  and  $|G| = |\langle a \rangle| = |a| = 30$ , so  $a^{30} = e$ . Find the subgroups of  $G$ . By Theorem 4.3 (i),

$$H \leq G \implies H \text{ is cyclic.}$$

By Theorem 4.3 (ii) (a),

$$H \leq G = \langle a \rangle \implies |H| = k : k \mid 30.$$

So  $k \in \{-30, -15, \dots, -1, 1, 2, 3, 5, 6, 10, 15, 30\}$ . By Theorem 4.3 (ii) (b),  $\forall k \in \mathbb{N} : k \mid 30$ , there exists only one  $H \leq G = \langle a \rangle : |H| = k, H = \langle a^{30/k} \rangle$ . Hence the

list of subgroups of  $\langle a \rangle$  is

$$\begin{aligned}
k = 1 : H = \langle a^{30/1} \rangle &= \langle a^{30} \rangle = \{e\}, & |H| &= 1, \\
k = 2 : H = \langle a^{30/2} \rangle &= \langle a^{15} \rangle = \{e, a^{15}\}, & |H| &= 2, \\
k = 3 : H = \langle a^{30/3} \rangle &= \langle a^{10} \rangle = \{e, a^{10}, a^{20}\}, & |H| &= 3, \\
k = 5 : H = \langle a^{30/5} \rangle &= \langle a^6 \rangle = \{e, a^6, a^{12}, a^{18}, a^{24}\}, & |H| &= 5, \\
k = 6 : H = \langle a^{30/6} \rangle &= \langle a^5 \rangle = \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}\}, & |H| &= 6, \\
k = 10 : H = \langle a^{30/10} \rangle &= \langle a^3 \rangle = \{e, a^3, a^6, \dots, a^{27}\}, & |H| &= 10, \\
k = 15 : H = \langle a^{30/15} \rangle &= \langle a^2 \rangle = \{e, a^2, a^4, a^6, \dots, a^{28}\}, & |H| &= 15, \\
k = 30 : H = \langle a^{30/30} \rangle &= \langle a^1 \rangle = \{e, a, a^2, \dots, a^{29}\}, & |H| &= 30.
\end{aligned}$$

**Corollary 4.3.1.**  $\forall k \in \mathbb{N} : k \mid n$ , there exists only one  $\langle n/k \rangle \leq \mathbb{Z}_n : |\langle n/k \rangle| = k$ . Moreover, these are the only subgroups of  $\mathbb{Z}_n$ .

**Example 4.5.** For  $\mathbb{Z}_{30} = \{0, 1, 2, \dots, 29\} = \langle 1 \rangle$ , let  $k$  be a positive divisor of 30, so  $k \in \{1, 2, 3, 5, 6, 10, 15, 30\}$ . The list of subgroups of  $\mathbb{Z}_{30}$  is

$$\begin{aligned}
k = 1 : \langle 30/1 \rangle &= \langle 30 \rangle = \{0\}, & |\langle 30/1 \rangle| &= 1, \\
k = 2 : \langle 30/2 \rangle &= \langle 15 \rangle = \{0, 15\}, & |\langle 30/2 \rangle| &= 2, \\
k = 3 : \langle 30/3 \rangle &= \langle 10 \rangle = \{0, 10, 20\}, & |\langle 30/3 \rangle| &= 3, \\
k = 5 : \langle 30/5 \rangle &= \langle 6 \rangle = \{0, 6, 12, 18, 24\}, & |\langle 30/5 \rangle| &= 5, \\
k = 6 : \langle 30/6 \rangle &= \langle 5 \rangle = \{0, 5, 10, 15, 20, 25\}, & |\langle 30/6 \rangle| &= 6, \\
k = 10 : \langle 30/10 \rangle &= \langle 3 \rangle = \{0, 3, 6, 9, \dots, 27\}, & |\langle 30/10 \rangle| &= 10, \\
k = 15 : \langle 30/15 \rangle &= \langle 2 \rangle = \{0, 2, 4, 6, \dots, 28\}, & |\langle 30/15 \rangle| &= 15, \\
k = 30 : \langle 30/30 \rangle &= \langle 1 \rangle = \{0, 1, 2, \dots, 29\}, & |\langle 30/30 \rangle| &= 30.
\end{aligned}$$

**Example 4.6.** For  $\mathbb{Z}_{36}$ , find the generators of the subgroup of order 9. Since  $\mathbb{Z}_{36}$  is cyclic under addition modulo 36 and  $\mathbb{Z}_{36} = \langle 1 \rangle$ , by Theorem 4.3 (ii) (b), there exists exactly one  $H \leq \mathbb{Z}_{36} = \langle 1 \rangle : |H| = 9, H = \langle 1 \cdot (36/9) \rangle = \langle 4 \rangle$ . So 4 is a generator of  $H$ . By Corollary 4.2.3, since  $|4| = 9$ , it follows that  $\langle 4 \rangle = \langle 4j \rangle \iff \gcd(9, j) = 1$ . Since  $j \in \{1, 2, 4, 5, 7, 8\}$ , it follows that

$$\begin{aligned}
\langle 4 \cdot 1 \rangle &= \langle 4 \cdot 2 \rangle = \langle 4 \cdot 4 \rangle = \langle 4 \cdot 5 \rangle = \langle 4 \cdot 7 \rangle = \langle 4 \cdot 8 \rangle, \\
\langle 4 \rangle &= \langle 8 \rangle = \langle 16 \rangle = \langle 20 \rangle = \langle 28 \rangle = \langle 32 \rangle \\
&= \{0, 4, 8, 12, 16, 20, 24, 28, 32\}.
\end{aligned}$$

Hence 4, 8, 16, 20, 28, 32 are all generators of the subgroup of order 9.

In general, to find all the subgroups of  $\langle a \rangle$  of order 9 where  $|a| = 36$ , one has

$$\langle (a^4)^1 \rangle = \langle (a^4)^2 \rangle = \langle (a^4)^4 \rangle = \langle (a^4)^5 \rangle = \langle (a^4)^7 \rangle = \langle (a^4)^8 \rangle.$$

Note that once one has the generator  $a^{n/d}$  for the subgroup of order  $d$  where  $d$  is a divisor of  $|a| = n$ , all the generators of  $\langle a^d \rangle$  have the form  $(a^d)^j, j \in U(d)$ .

**Definition 4.2.** The *Euler phi function* is defined as

$$\phi(n) = \begin{cases} 1 & , n = 1 \\ \text{number of } k \in \mathbb{N} : k < n, \gcd(k, n) = 1 & , n > 1 \end{cases}$$

Notice that by definition of the group  $U(10)$ ,  $|U(10)| = \phi(10)$ . Figure 4.2 shows the first 12 values of  $\phi(n)$ .

$n$	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Figure 4.2: The first 12 values of  $\phi(n)$ .

**Theorem 4.4.** Let  $G$  be cyclic,  $|G| = n$ . If  $d \mid n, d \in \mathbb{N}$ , then the number of elements  $a \in G : |a| = d$  is  $\phi(d)$ .

*Proof.* Let  $G$  be cyclic,  $|G| = n$ . Assume that  $d \mid n, d > 0$ , then by Theorem 4.3, there exists only one  $H \leq G : |H| = d$ . Let  $H = \langle a \rangle$ . Since by Corollary 4.2.3,  $\langle a \rangle = \langle a^k \rangle \iff \gcd(d, k) = 1$ , and  $|a^k| = |\langle a^k \rangle| = \langle a \rangle = |a| = d$ . It follows that  $\phi(d)$  is the number of  $k \in \mathbb{N} : k < d, \gcd(d, k) = 1$  = the number of  $a^k \in H : |a^k| = d$ .  $\square$

**Corollary 4.4.1.** Let  $G$  be a group,  $|G| = n$ . Then the number of elements  $a \in G : |a| = d$  is a multiple of  $\phi(d)$ .

*Proof.* Let  $G$  be a group,  $|G| = n$ . If the number of elements  $a \in G : |a| = d$  is 0, then since 0 is a multiple of  $\phi(d)$ , the statement is true. If  $\exists a \in G : |a| = d$ , then by Theorem 4.4,  $\langle a \rangle$  has  $\phi(d)$  elements of order  $d$ .

If all elements of order  $d$  in  $G$  are in  $\langle a \rangle$ , then the number of elements of order  $d$  is a multiple of  $\phi(d)$ . If  $\exists b \in G : |b| = d, b \notin \langle a \rangle$ , then  $\langle b \rangle$  has  $\phi(d)$  elements of order  $d$ . So there are  $2\phi(d)$  elements of order  $d$  in  $G$  provided  $\langle a \rangle$  and  $\langle b \rangle$  have no elements of order  $d$  in common. If  $\exists c \in \langle a \rangle, \langle b \rangle : |c| = d$ , then  $\langle a \rangle = \langle b \rangle = \langle c \rangle$ , so  $b \in \langle a \rangle$ , a contradiction. Continuing in this fashion, the number of elements of order  $d$  in  $G$  is a multiple of  $\phi(d)$ .  $\square$

Theorem 4.4 together with the two number theorem properties that for any prime  $p$ ,

1.  $\phi(p^n) = p^n - p^{n-1}$ , and
2.  $\phi(p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}) = \phi(p_1^{k_1}) \phi(p_2^{k_2}) \dots \phi(p_m^{k_m})$ ,  $p_1, p_2, \dots, p_m$  are distinct,

simplify the task of determining orders of element in  $U(n)$  and whether or not  $U(n)$  is cyclic.

**Example 4.7.** Let  $U(n)$ ,  $n > 2$  be cyclic. Since  $2 \mid |U(n)| = \phi(n)$ , by Theorem 4.3, there exists only one  $H \leq U(n) : |H| = 2$ . Since  $\langle -1 \rangle = \langle n-1 \rangle \leq U(n)$  and  $|\langle n-1 \rangle| = |\langle -1 \rangle| = |-1| = 2$ , it follows that  $\langle n-1 \rangle$  is the only subgroup of order 2 of  $U(n)$ . But in  $U(80)$ ,  $9^2 = 1 \implies |9| = |\langle 9 \rangle| = 2$ ,  $\langle 9 \rangle \neq \langle 79 \rangle$ , and in  $U(120)$ ,  $11^2 = 1 \implies |11| = |\langle 11 \rangle| = 2$ ,  $\langle 11 \rangle \neq \langle 119 \rangle$ . Hence  $U(80), U(120)$  are not cyclic.

## 5 Permutation Groups

### 5.1 Definition and Notation

**Definition 5.1.** A *permutation* of a set  $A$  is a one-to-one and onto function  $f : A \rightarrow A$ . A *permutation group* of a set  $A$  is a set of permutation of  $A$  that forms a group under function composition.

**Note 5.1.** For example, define a permutation  $\alpha$  of the set  $\{1, 2, 3, 4\}$  as

$$\alpha(1) = 2, \alpha(2) = 3, \alpha(3) = 1, \alpha(4) = 4.$$

or in array form

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}.$$

Similarly, the permutation  $\beta$  of  $\{1, 2, 3, 4, 5, 6\}$  can be defined as

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}.$$

Let

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}, \gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix},$$

Figure 5.1 shows the composition of permutations  $\sigma$  and  $\gamma$ . Since  $(\gamma\sigma)(1) = \gamma(\sigma(1)) = \gamma(2) = 4$ , so  $\gamma\sigma$  maps 1 to 4.

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

Figure 5.1: Composition of permutations  $\sigma$  and  $\gamma$ .

**Example 5.1.** Let  $S_3$  be the set of all permutations of  $\{1, 2, 3\}$ . Then  $S_3$  under function composition is a group with six elements. The six elements are

$$\begin{aligned}\epsilon &= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \\ \beta &= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.\end{aligned}$$

Since

$$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \alpha^2\beta \neq \alpha\beta,$$

$S_3$  is non-Abelian. The relation  $\beta\alpha = \alpha^2\beta$  can be used to compute other products in  $S_3$  without resorting to the arrays. For example

$$\beta\alpha^2 = (\beta\alpha)\alpha = (\alpha^2\beta)\alpha = \alpha^2(\beta\alpha) = \alpha^2(\alpha^2\beta) = \alpha^4\beta = \alpha\beta.$$

**Example 5.2.**  $S_n$  is the set of all permutations of a set of  $n$  elements  $A = \{1, 2, \dots, n\}$  called the *symmetric group of degree  $n$* . Elements of  $S_n$  have the form

$$\alpha = \begin{bmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{bmatrix}.$$

Since  $\alpha$  is one-to-one, there are  $n$  choices for  $\alpha(1)$ ,  $n - 1$  choices for  $\alpha(2)$ ,  $\dots$ , 1 choice for  $\alpha(n)$ . So  $S_n$  has  $n! = n \cdot (n - 1) \cdot \dots \cdot 2 \cdot 1$  elements and  $|S_n| = n!$ .  $S_n$  is non-Abelian when  $n \geq 3$ , since any permutation  $\alpha$  only commute with the identity permutation  $\epsilon$ , i.e.  $\epsilon\alpha = \alpha\epsilon$ .

**Example 5.3.** Associate each motion in  $D_4$  with the permutation of the location of each of the four corners of a square.

## 5.2 Cycle Notation

**Note 5.2.** Consider the permutation

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}.$$

Figure 5.2 shows the cycle notation of  $\alpha$ . Figure 5.2 can also be expressed as  $\alpha = (1, 2)(3, 4, 6)(5)$  or  $\alpha = (12)(346)(5)$ .

As a second example, consider

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}.$$

In cycle notation,  $\beta = (2, 3, 1, 5)(6, 4)$  or  $(4, 6)(3, 1, 5, 2)$ . An expression of the form  $(a_1, a_2, \dots, a_m)$  is called a *cycle of length  $m$*  or an  *$m$ -cycle*.

A multiplication of cycle can be performed by thinking of a cycle as a permutation that fixes any symbol not appearing in the cycle. So the cycle  $(4, 6)$  can be thought of as the permutation  $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{bmatrix}$ . Then

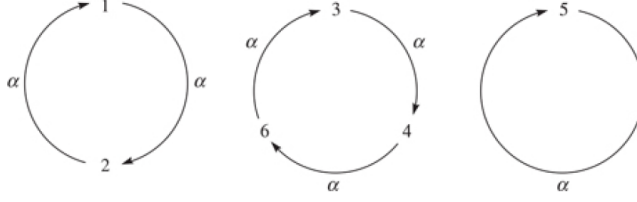


Figure 5.2: Cycle notation of  $\alpha$ .

the multiplication of cycles can be thought of as composition of permutations in array form. Let  $\alpha = (13)(27)(456)(8), \beta = (1237)(648)(5) \in S_8$ . Then  $\alpha\beta = (13)(27)(456)(8)(1237)(648)(5)$ . One proceeds by treating each of the cycles of  $\alpha\beta$  as a function  $f : \{1, \dots, 8\} \rightarrow \{1, \dots, 8\}$  and use function composition. Each cycle that does not contain a symbol fixes that symbol. For example, for  $\alpha\beta(1)$ , (5) fixes 1, then (648) fixes 1, then (1237) maps 1 to 2, then (8) fixes 2, then (456) fixes 2, then (27) maps 2 to 7, and lastly (13) fixes 7. So  $\alpha\beta(1) = 7$ . Thus one begins with  $\alpha\beta = (17\dots)\dots$ . Figure 5.3 shows  $\alpha\beta(1)$ .

$$1 \xrightarrow{(5)} 1 \xrightarrow{(648)} 1 \xrightarrow{(1237)} 2 \xrightarrow{(8)} 2 \xrightarrow{(456)} 2 \xrightarrow{(27)} 7 \xrightarrow{(13)} 7.$$

Figure 5.3:  $\alpha\beta(1) = 7$ .

Then, for  $\alpha\beta(7)$ , (5) fixes 7, (648) fixes 7, (1237) maps 7 to 1, (8) fixes 1, (456) fixes 1, (27) fixes 1, and (13) maps 1 to 3, so  $\alpha\beta(7) = 3$ . Figure 5.4 shows  $\alpha\beta(7) = 3$ . Hence,  $\alpha\beta = (173\dots)\dots$ . Eventually,  $\alpha\beta = (1732)(48)(56)$ .

$$7 \xrightarrow{(5)} 7 \xrightarrow{(648)} 7 \xrightarrow{(1237)} 1 \xrightarrow{(8)} 1 \xrightarrow{(456)} 1 \xrightarrow{(27)} 1 \xrightarrow{(13)} 3,$$

Figure 5.4:  $\alpha\beta(7) = 3$ .

For another example, if

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{bmatrix}, \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}.$$

Then in cycle notation,  $\alpha = (12)(3)(45), \beta = (153)(24), \alpha\beta = (12)(3)(45)(153)(24)$ . For  $\alpha\beta(1)$ , (24) fixes 1, (153) maps 1 to 5, (45) maps 5 to 4, (3) fixes 4, and (12) fixes 4. So  $\alpha\beta(1) = 4$ . Eventually,  $\alpha\beta = (14)(253)$ .

One can convert  $\alpha\beta$  back to array form without converting each cycle of  $\alpha\beta$  back to array form by observing that (14) means  $1 \rightarrow 4, 4 \rightarrow 1$ ; (253) means  $2 \rightarrow 5, 5 \rightarrow 3, 3 \rightarrow 2$ .

Any missing element in a cycle is mapped to itself. So  $\alpha = (12)(3)(45) = (12)(45)$  and the identity permutation

$$\epsilon = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$$



in cycle form is  $\epsilon = (1) = (2) = (3) = (4) = (5)$ .

### 5.3 Properties of Permutations

**Theorem 5.1.** *Every permutation of a finite set can be expressed as a cycle or as a product of disjoint cycles.*

*Proof.* Let  $\alpha$  be a permutation on  $A = \{1, 2, \dots, n\}$ . To write  $\alpha$  in disjoint form, choose any member of  $A$ , say  $a_1$ , and let

$$a_2 = \alpha(a_1), a_3 = \alpha(a_2) = \alpha(\alpha(a_1)) = \alpha^2(a_1), a_4 = \alpha^3(a_1), \dots$$

Since  $A$  is finite, eventually there will be a repetition

$$a_{m+1} = \alpha^m(a_1) = a_1, m \in \mathbb{N}.$$

If

$$\alpha^i(a_1) = \alpha^j(a_1), i, j \in \mathbb{N}, i < j,$$

then  $a_1 = \alpha^m(a_1) = \alpha^{j-i}(a_1)$ . The relationship among  $a_1, a_2, \dots, a_m$  is expressed as

$$\alpha = (a_1, a_2, \dots, a_m) \cdots$$

The three dots at the end indicate that  $A$  may have not been exhausted in this process. If so, then choose any element  $b_1 \in A$  not in the first cycle and repeat the process until

$$b_{k+1} = b_1 = \alpha^k(b_1), k \in \mathbb{N}.$$

If

$$\alpha^i(a_1) = \alpha^j(b_1), i, j \in \mathbb{N},$$

then

$$\alpha^{i-j}(a_1) = \alpha^j \alpha^{-j}(b_1) = \epsilon(b_1) = b_1 \implies b_1 = a_t, t \in \mathbb{N}.$$

This contradicts that  $b_1$  is not in the first cycle. Hence the new cycle has no elements in common with the first cycle. Continuing the process until  $A$  is exhausted, the permutation is expressed as

$$\alpha = (a_1, a_2, \dots, a_m)(b_1, b_2, \dots, b_k) \cdots (c_1, c_2, \dots, c_s).$$

□

**Theorem 5.2.** *If the pair of cycles  $\alpha = (a_1, a_2, \dots, a_m), \beta = (b_1, b_2, \dots, b_n)$  have no entries in common, then  $\alpha\beta = \beta\alpha$ .*

*Proof.* Let  $\alpha, \beta$  be the permutation of the set

$$S = \{a_1, a_2, \dots, a_m, b_1, b_2, \dots, b_n, c_1, c_2, \dots, c_k\},$$

where  $c$ 's are the members of  $S$  left fixed by both  $\alpha, \beta$  (there may not be any  $c$ 's). Let  $a_i$  be an arbitrary  $a$  element, then

$$(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1},$$

since  $\beta$  fixes all  $a$  elements.  $a_{i+1} = a_1$  if  $i = m$ . Similarly,

$$(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}.$$

Hence  $\alpha\beta = \beta\alpha$  for all  $a$  elements. The same can be applied to all  $b$  elements. Let  $c_i$  be an arbitrary  $c$  element, then

$$(\alpha\beta)(c_i) = \alpha(\beta(c_i)) = \alpha(c_i) = c_i,$$

and

$$(\beta\alpha)(c_i) = \beta(\alpha(c_i)) = \beta(c_i) = c_i.$$

So  $\alpha\beta = \beta\alpha$  for all  $c$  elements. Hence  $\alpha\beta = \beta\alpha$  for all elements in  $S$ .  $\square$

**Theorem 5.3.** *Let  $\alpha$  be a permutation of a finite set written in disjoint cycle form. Then  $|\alpha| = \text{lcm}(\text{the lengths of the cycles})$ .*

*Proof.* Let  $\alpha = (a_1, a_2, \dots, a_n)$  be an arbitrary cycle of length  $n$ . Then

$$\begin{aligned} \alpha(a_1) &= a_2, \\ \alpha(a_2) &= \alpha(\alpha(a_1)) = \alpha^2(a_1) = a_3, \\ \alpha(a_3) &= \alpha(\alpha^2(a_1)) = \alpha^3(a_1) = a_4, \\ &\vdots \\ \alpha(a_n) &= \alpha^n(a_1) = a_{n+1} = a_1. \end{aligned}$$

So  $\alpha^n(a_i) = a_i, i \in \{1, \dots, n\} \implies \alpha^n = \epsilon$  and  $|\alpha| = |(a_1, a_2, \dots, a_n)| = n$ . Hence a cycle of  $n$  length has order  $n$ .

Let  $\gamma = \alpha\beta = (a_1, \dots, a_m)(b_1, \dots, b_n)$  be a permutation of a finite set in disjoint cycle form, and let  $k = \text{lcm}(m, n)$ . WTS  $|\gamma| = |\alpha\beta| = \text{lcm}(m, n) = k$ .

Since  $|\alpha| = m, |\beta| = n$  and  $m, n \mid k$ , by Theorem 4.1,

$$\begin{aligned} \alpha^k &= \alpha^0 = \epsilon \iff m \mid (k - 0) = k, \\ \beta^k &= \beta^0 = \epsilon \iff n \mid (k - 0) = k. \end{aligned}$$

Hence  $\alpha^k = \epsilon, \beta^k = \epsilon$ . Since  $\alpha, \beta$  are disjoint, by Theorem 5.2,  $\alpha\beta = \beta\alpha$ . So

$$\gamma^k = (\alpha\beta)^k = \alpha^k \beta^k = \epsilon\epsilon = \epsilon$$

and  $|\gamma| = t \leq k$ .

By Theorem 4.1,

$$\gamma^k = \epsilon \iff |\gamma| = t \mid k,$$

and

$$|\gamma| = |\alpha\beta| = t \implies \gamma^t = (\alpha\beta)^t = \alpha^t\beta^t = \epsilon.$$

Since  $\alpha, \beta$  are disjoint, it follows that

$$\begin{aligned}\alpha^k(b_i) &= b_i, i \in \{1, \dots, n\}, \\ \beta^k(a_i) &= a_i, i \in \{1, \dots, m\}.\end{aligned}$$

Since  $\gamma^t = \alpha^t\beta^t = \epsilon$ , it follows that

$$\begin{aligned}\gamma^t(a_i) &= (\alpha^t\beta^t)(a_i) = \epsilon(a_i) = a_i, i \in \{1, \dots, m\}, \\ \gamma^t(b_i) &= (\alpha^t\beta^t)(b_i) = \epsilon(b_i) = b_i, i \in \{1, \dots, n\}.\end{aligned}$$

This is true iff  $\alpha^t = \epsilon, \beta^t = \epsilon$ . By Theorem 4.1,

$$\begin{aligned}\alpha^t = \alpha^0 = \epsilon &\iff m \mid (t - 0) = t, \\ \beta^t = \beta^0 = \epsilon &\iff n \mid (t - 0) = t,\end{aligned}$$

so  $t$  is a common multiple of  $m, n$ . Since  $k = \text{lcm}(m, n)$ , it follows that  $t \geq k$ . So

$$t \geq k, t \leq k \implies t = k$$

and hence  $|\gamma| = t = k$ .

The general cases involving more than two cycles can be proved in a similar manner.  $\square$

**Example 5.4.**

$$\begin{aligned} |(132)(45)| &= \text{lcm}(3, 2) = 6, \\ |(1432)(56)| &= \text{lcm}(4, 2) = 4, \\ |(123)(456)(78)| &= \text{lcm}(3, 3, 2) = 6, \\ |(123)(145)| &= |(14523)| = 5. \end{aligned}$$

**Example 5.5.** Determine the orders of the  $7! = 5040$  elements of  $S_7$ . For convenience, denote an  $n$ -cycle by  $(\underline{n})$ . Then, arranging all possible disjoint cycle structures of elements of  $S_7$  according to longest cycle lengths left to

right,

$$\begin{aligned}
& \overline{(7)}, \\
& \overline{(6)}(\overline{1}), \\
& \overline{(5)}(\overline{2}), \\
& \overline{(5)}(\overline{1})(\overline{1}), \\
& \overline{(4)}(\overline{3}), \\
& \overline{(4)}(\overline{2})(\overline{1}), \\
& \overline{(4)}(\overline{1})(\overline{1})(\overline{1}), \\
& \overline{(3)}(\overline{3})(\overline{1}), \\
& \overline{(3)}(\overline{2})(\overline{2}), \\
& \overline{(3)}(\overline{2})(\overline{1})(\overline{1}), \\
& \overline{(3)}(\overline{1})(\overline{1})(\overline{1})(\overline{1}), \\
& \overline{(2)}(\overline{2})(\overline{2})(\overline{1}), \\
& \overline{(2)}(\overline{2})(\overline{1})(\overline{1})(\overline{1}), \\
& \overline{(2)}(\overline{1})(\overline{1})(\overline{1})(\overline{1})(\overline{1}), \\
& \overline{(1)}(\overline{1})(\overline{1})(\overline{1})(\overline{1})(\overline{1})(\overline{1}).
\end{aligned}$$

By Theorem 5.3, the orders of the elements of  $S_7$  are

$$\begin{aligned}
& 7, \\
& \text{lcm}(6, 1) = \text{lcm}(3, 2, 2) = \text{lcm}(3, 2, 1, 1) = 6, \\
& \text{lcm}(5, 2) = 10, \\
& \text{lcm}(5, 1, 1) = 5, \\
& \text{lcm}(4, 3) = 12, \\
& \text{lcm}(4, 2, 1) = \text{lcm}(4, 1, 1, 1) = 4, \\
& \text{lcm}(3, 3, 1) = \text{lcm}(3, 1, 1, 1, 1) = 3, \\
& \text{lcm}(2, 2, 2, 1) = \text{lcm}(2, 2, 1, 1, 1) = \text{lcm}(2, 1, 1, 1, 1, 1) = 2, \\
& \text{lcm}(1, 1, 1, 1, 1, 1, 1) = 1.
\end{aligned}$$

**Example 5.6.** Determine the number of elements of order 12 in  $S_7$ . Since  $\text{lcm}(4, 3) = 12$ , by Theorem 5.2 and 5.3, only the number of permutations with disjoint cycle form  $(a_1 a_2 a_3 a_4)(a_5 a_6 a_7)$  is needed to be counted. First consider the cycle  $(a_1 a_2 a_3 a_4)$ . There are  $7 \cdot 6 \cdot 5 \cdot 4$  ways of choosing 4 out of 7 entries, but each choice of the cycle  $(a_1 a_2 a_3 a_4)$  is counted four times. For example,

$$(2741) = (1274) = (4127) = (7412).$$

Similarly, there are  $3 \cdot 2 \cdot 1$  ways of choosing 3 out of 7 entries for  $(a_5 a_6 a_7)$ , but each choice of  $(a_5 a_6 a_7)$  is counted three times. Hence, there are

$$\frac{(7 \cdot 6 \cdot 5 \cdot 4)(3 \cdot 2 \cdot 1)}{(4)(3)} = 420$$

elements of order 12 in  $S_7$ .

**Example 5.7.** Determine the number of elements of order 3 in  $S_7$ . Since  $\text{lcm}(3, 3, 1) = \text{lcm}(3, 1, 1, 1, 1) = 3$ , by Theorem 5.2 and 5.3, the elements of order 3 in  $S_7$  have the disjoint cycle form

$$(a_1 a_2 a_3)(a_4 a_5 a_6)(a_7) \quad \text{and} \quad (a_1 a_2 a_3)(a_4)(a_5)(a_6)(a_7).$$

or

$$(a_1 a_2 a_3)(a_4 a_5 a_6) \quad \text{and} \quad (a_1 a_2 a_3).$$

For  $(a_1 a_2 a_3)(a_4 a_5 a_6)$ , there are  $(7 \cdot 6 \cdot 5)/3$  ways of creating  $(a_1 a_2 a_3)$  and there are  $(4 \cdot 3 \cdot 2)/3$  ways of creating  $(a_4 a_5 a_6)$ . But  $(7 \cdot 6 \cdot 5)/3$  and  $(4 \cdot 3 \cdot 2)/3$  count  $(a_1 a_2 a_3)(a_4 a_5 a_6)$  and  $(a_4 a_5 a_6)(a_1 a_2 a_3)$  as distinct elements when they are identical. So there are

$$\frac{(7 \cdot 6 \cdot 5)(4 \cdot 3 \cdot 2)}{(3)(3)(2)} = 280$$

elements of order 3 in  $S_7$  with disjoint cycle form  $(a_1 a_2 a_3)(a_4 a_5 a_6)$ .

For  $(a_1 a_2 a_3)$ , there are  $(7 \cdot 6 \cdot 5)/3$  ways of creating  $(a_1 a_2 a_3)$ . So there are  $(7 \cdot 6 \cdot 5)/3 = 70$  elements of order 3 in  $S_7$  with the distinct cycle form  $(a_1 a_2 a_3)$ . Hence there are  $280 + 70 = 350$  elements of order 3 in  $S_7$ .

**Theorem 5.4.** Every permutation in  $S_n, n > 1$  is a product of 2-cycle.

*Proof.* The identity permutation  $\epsilon$  can be expressed as  $(12)(12)$ . So  $\epsilon$  can be expressed as a product of 2-cycle. By Theorem 5.1, every permutation can be written in the disjoint cycle form

$$(a_1 \dots a_k)(b_1 \dots b_t)(c_1 \dots c_s).$$

This is the same as

$$(a_1 a_k)(a_1 a_{k-1})(a_1 a_{k-2}) \dots (a_1 a_2)(b_1 b_t)(b_1 b_{t-1})(b_1 b_{t-2}) \dots (b_1 b_2) \\ \dots (c_1 c_s)(c_1 c_{s-1})(c_1 c_{s-2}) \dots (c_1 c_2).$$

□

**Example 5.8.**

$$(12345) = (15)(14)(13)(12) \\ (1632)(457) = (12)(13)(16)(47)(45)$$

**Example 5.9.**

$$(12345) = (54)(53)(52)(51) \\ (12345) = (54)(52)(21)(25)(23)(13)$$

**Lemma 5.1.** *If  $\epsilon = \beta_1\beta_2\ldots\beta_r$ , where  $\beta_1, \beta_2, \ldots, \beta_r$  are 2-cycles, then  $r$  is even.*

*Proof.* □

**Theorem 5.5.** *Let  $\alpha$  be a permutation. If*

$$\alpha = \beta_1\beta_2\ldots\beta_r \quad \text{and} \quad \alpha = \gamma_1\gamma_2\ldots\gamma_s,$$

*where  $\beta, \gamma$  are all 2-cycles, then  $r, s$  are both even or both odd.*

*Proof.* Let  $\alpha$  be a permutation and let

$$\alpha = \beta_1\beta_2\ldots\beta_r \quad \text{and} \quad \alpha = \gamma_1\gamma_2\ldots\gamma_s,$$

where  $\beta, \gamma$  are all 2-cycles. Then since the inverse of an 2-cycle is itself,

$$\begin{aligned} \alpha = \beta_1\beta_2\ldots\beta_r = \gamma_1\gamma_2\ldots\gamma_s &\implies \epsilon = \gamma_1\ldots\gamma_s\beta_1^{-1}\ldots\beta_r^{-1} \\ &= \gamma_1\ldots\gamma_s\beta_1\ldots\beta_r. \end{aligned}$$

By Lemma 5.4.1, if  $\epsilon = \beta_1\ldots\beta_t$ , where all  $\beta$  are 2-cycles, then  $t$  is even. So  $t = r + s$  is even  $\iff r, s$  are both even or both odd. □

**Definition 5.2.** Let  $\alpha$  be a permutation and let  $\alpha = \beta_1\ldots\beta_r$  where all  $\beta_i$ 's are 2-cycles. If  $r$  is even then  $\alpha$  is an *even* permutation. If  $r$  is odd then  $\alpha$  is an *odd* permutation.

**Theorem 5.6.** *The set of even permutations in  $S_n$  is a subgroup of  $S_n$ .*

*Proof.* Let  $A \in S_n$  be the set of even permutations. Let  $\alpha, \beta \in A$  be arbitrary. So

$$\alpha = \gamma_1\ldots\gamma_r, \beta = \sigma_1\ldots\sigma_s,$$

where  $\gamma$ 's and  $\sigma$ 's are 2-cycles and  $r, s$  are even. Since

$$\alpha\beta = \gamma_1\ldots\gamma_r\sigma_1\ldots\sigma_s$$

and  $r + s$  is even, it follows that  $\alpha\beta \in A$ . Next,

$$\begin{aligned} \alpha\alpha^{-1} &= \epsilon, \\ \gamma_1\ldots\gamma_r\alpha^{-1} &= \epsilon, \\ \alpha^{-1} &= \gamma_1^{-1}\ldots\gamma_r^{-1}\epsilon \\ &= \gamma_1^{-1}\ldots\gamma_r^{-1} \\ &= \gamma_1\ldots\gamma_r \\ &= \alpha \in A. \end{aligned}$$

Since  $\alpha, \beta \in A \implies \alpha\beta \in A$  and  $\alpha \in A \implies \alpha^{-1} \in A$ , by Theorem 3.2,  $A \leq S_n$ .  $\square$

**Definition 5.3.** The group of even permutation of  $n$  symbols is denoted by  $A_n$  and is called the *alternating group of degree  $n$* .

**Theorem 5.7.** Let  $A_n$  be an alternating group of degree  $n$ . Then

$$|A_n| = n!/2, n > 1.$$

*Proof.* For each odd permutation  $\alpha$ , the permutation  $(12)\alpha$  is even. By the cancellation property,  $(12)\alpha \neq (12)\beta$  when  $\alpha \neq \beta$ . So there are at least as many even permutations as there are odd ones. For each even permutation  $\alpha$ , the permutation  $(12)\alpha$  is odd. By the cancellation property,  $(12)\alpha \neq (12)\beta$  when  $\alpha \neq \beta$ . So there are at least as many odd permutations as there are even ones. Hence the numbers of even and odd permutations are the same. Since  $|S_n| = n!$ , it follows that  $|A_n| = n!/2$ .  $\square$

**Table 5.1** The Alternating Group  $A_4$  of Even Permutations of  $\{1, 2, 3, 4\}$

(In this table, the permutations of  $A_4$  are designated as  $\alpha_1, \alpha_2, \dots, \alpha_{12}$  and an entry  $k$  inside the table represents  $\alpha_k$ . For example,  $\alpha_3 \alpha_8 = \alpha_6$ .)

	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\alpha_4$	$\alpha_5$	$\alpha_6$	$\alpha_7$	$\alpha_8$	$\alpha_9$	$\alpha_{10}$	$\alpha_{11}$	$\alpha_{12}$
$(1) = \alpha_1$	1	2	3	4	5	6	7	8	9	10	11	12
$(12)(34) = \alpha_2$	2	1	4	3	6	5	8	7	10	9	12	11
$(13)(24) = \alpha_3$	3	4	1	2	7	8	5	6	11	12	9	10
$(14)(23) = \alpha_4$	4	3	2	1	8	7	6	5	12	11	10	9
$(123) = \alpha_5$	5	8	6	7	9	12	10	11	1	4	2	3
$(243) = \alpha_6$	6	7	5	8	10	11	9	12	2	3	1	4
$(142) = \alpha_7$	7	6	8	5	11	10	12	9	3	2	4	1
$(134) = \alpha_8$	8	5	7	6	12	9	11	10	4	1	3	2
$(132) = \alpha_9$	9	11	12	10	1	3	4	2	5	7	8	6
$(143) = \alpha_{10}$	10	12	11	9	2	4	3	1	6	8	7	5
$(234) = \alpha_{11}$	11	9	10	12	3	1	2	4	7	5	6	8
$(124) = \alpha_{12}$	12	10	9	11	4	2	1	3	8	6	5	7

Figure 5.5

## 6 Isomorphism

### 6.1 Definition and Examples

**Definition 6.1.** Let  $G, \bar{G}$  be two groups. Let  $\phi : G \rightarrow \bar{G}$  be a function s.t.

1.  $\forall a, b \in G, \phi(a) = \phi(b) \implies a = b$  (one-to-one),
2.  $\forall \bar{a} \in \bar{G}, \exists a \in G : \phi(a) = \bar{a}$  (onto),
3.  $\forall a, b \in G, \phi(ab) = \phi(a)\phi(b)$  (preservation of operations),

then  $\phi$  is an isomorphism from  $G$  to  $\bar{G}$ .

If there is an isomorphism from  $G$  to  $\bar{G}$ , then  $G$  and  $\bar{G}$  are isomorphic, denoted  $G \approx \bar{G}$ .

Figure 6.1 shows the visualization of Definition 6.1. Figure 6.2 shows the operation tables for  $G$  and  $\bar{G}$ . The operation table for  $\bar{G}$  can be obtained by replacing each entry  $x$  in the operation table for  $G$  by  $\phi(x)$ . Figure 6.3 shows the four cases of operations of  $G$  and  $\bar{G}$  involving  $\cdot$  and  $+$ .

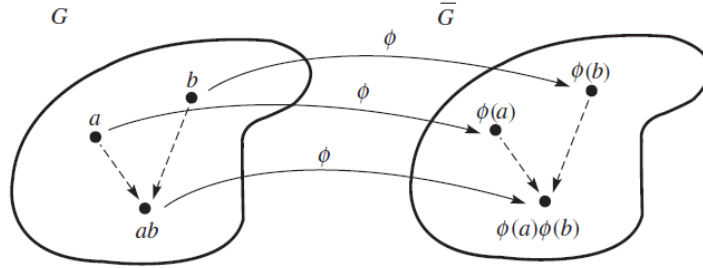


Figure 6.1

There are four steps involved in proving that  $G \approx \bar{G}$ .

1. **Mapping.** Define a function  $\phi : G \rightarrow \bar{G}$ .
2. **1-1.** Show that  $\forall a, b \in G, \phi(a) = \phi(b) \implies a = b$ .
3. **Onto.** Show that  $\forall \bar{g} \in \bar{G}, \exists g \in G : \phi(g) = \bar{g}$ .
4. **Operation-Preserving.** Show that  $\forall a, b \in G, \phi(ab) = \phi(a)\phi(b)$ .

**Example 6.1.** Let  $G = (\mathbb{R}, +)$  and  $\bar{G} = (\mathbb{R}^+, \cdot)$ . Show that  $G \approx \bar{G}$  under



$G$	-	-	-	$b$	-	-
-	-	-	-	-	-	-
-	-	-	-	-	-	-
$a$	-	-	-	$ab$	-	-
-	-	-	-	-	-	-
$\overline{G}$	-	-	-	$\phi(b)$	-	-
-	-	-	-	-	-	-
-	-	-	-	-	-	-
$\phi(a)$	-	-	-	$\phi(ab)$	-	-
-	-	-	-	-	-	-

Figure 6.2: Operation tables for  $G$  and  $\overline{G}$ . The operation table for  $\overline{G}$  can be obtained by replacing each entry  $x$  in the operation table for  $G$  by  $\phi(x)$ .

$G$ Operation	$G$ Operation	Operation Preservation
$\cdot$	$\cdot$	$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$
$\cdot$	$+$	$\phi(a \cdot b) = \phi(a) + \phi(b)$
$+$	$\cdot$	$\phi(a + b) = \phi(a) \cdot \phi(b)$
$+$	$+$	$\phi(a + b) = \phi(a) + \phi(b)$

Figure 6.3: The four cases of operations of  $G$  and  $\overline{G}$  involving  $\cdot$  and  $+$

$\phi(x) = 2^x$ . First, assume that  $\forall a, b \in G, \phi(a) = \phi(b)$ , then

$$\begin{aligned}\phi(a) &= \phi(b), \\ 2^a &= 2^b, \\ \log_2 2^a &= \log_2 2^b, \\ a &= b.\end{aligned}$$

So  $\forall a, b \in G, \phi(a) = \phi(b) \implies a = b$ . Next, let  $b \in \overline{G}$  be arbitrary. WTS  $\exists a \in G : 2^a = b$ . Since

$$\begin{aligned}2^a &= b, \\ \log_2 2^a &= \log_2 b, \\ a &= \log_2 b,\end{aligned}$$

it follows that  $\forall b \in \overline{G}, \exists a = \log_2 b \in G : \phi(a) = 2^a = 2^{\log_2 b} = b$ . Finally,

$$\forall a, b \in G, \phi(a + b) = 2^{a+b} = 2^a \cdot 2^b = \phi(a) \cdot \phi(b).$$

Hence  $G \approx \overline{G}$ .

**Example 6.2.** For any infinite cyclic group  $G = \langle a \rangle, a \in G, |G| = \infty$ , show that  $G \approx (\mathbb{Z}, +)$  under  $\phi(a^k) = k, k \in \mathbb{Z}$ .

First, assume that  $\forall a^i, a^j \in G, \phi(a^i) = \phi(a^j)$ , then

$$\phi(a^i) = \phi(a^j) \implies i = j.$$

By Theorem 4.1 (i),

$$|G| = |\langle a \rangle| = |a| = \infty \implies (a^i = a^j \iff i = j).$$

Hence  $\forall a^i, a^j \in G, \phi(a^i) = \phi(a^j) \implies a^i = a^j$ . Next, let  $k \in \mathbb{Z}$  be arbitrary. Since  $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ , it follows that  $\exists a^k \in \langle a \rangle : \phi(a^k) = k$ . Hence  $\forall k \in \mathbb{Z}, \exists a^k \in \langle a \rangle : \phi(a^k) = k$ . Finally,

$$\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j).$$

Hence,  $G \approx (\mathbb{Z}, +)$  under  $\phi(a^k) = k, k \in \mathbb{Z}$ .

For any finite cyclic group  $G = \langle a \rangle, a \in G, |G| = n$ , show that  $G \approx \mathbb{Z}_n$  under addition modulo  $n$  under  $\phi(a^k) = k \bmod n$ .

First, assume that  $\forall a^i, a^j \in G, \phi(a^i) = \phi(a^j)$ . Then

$$\begin{aligned}\phi(a^i) &= \phi(a^j), \\ i \bmod n &= j \bmod n, \\ (i - j) \bmod n &= 0 \implies n \mid (i - j).\end{aligned}$$

By Theorem 4.1 (ii),

$$|a| = n \implies (a^i = a^j \iff n \bmod (i - j)).$$

Hence  $\forall a^i, a^j \in G, \phi(a^i) = \phi(a^j) \implies a^i = a^j$ . Next, since  $|a| = n$ , it follows that

$$\begin{array}{ll} a^0 = a^n = a^{kn} = e, & a^{-1} = a^{n-1} = a^{kn-1}, \\ a^1 = a^{n+1} = a^{kn+1}, & a^{-2} = a^{n-2} = a^{kn-2}, \\ a^2 = a^{n+2} = a^{kn+2}, & a^{-3} = a^{n-3} = a^{kn-3}, \\ \vdots & \vdots \end{array}$$

Hence  $\forall a^k \in G, k \bmod n \in \{0, 1, \dots, n-1\}$  and so  $\forall x \in \mathbb{Z}_n, \exists a^k \in G : \phi(a^k) = k \bmod n = x$ . Finally,

$$\begin{aligned} \phi(a^i a^j) &= \phi(a^{i+j}) = (i+j) \bmod n \\ &= (i \bmod n + j \bmod n) \bmod n \\ &= (\phi(a^i) + \phi(a^j)) \bmod n. \end{aligned}$$

Hence  $G \approx \mathbb{Z}_n$  under addition modulo  $n$  under  $\phi(a^k) = k \bmod n$ .

**Example 6.3.** Let  $G = (\mathbb{R}, +)$ . Show that  $G$  and  $G$  are not isomorphic under  $\phi(x) = x^3$ .

First, assume  $\forall a, b \in G, \phi(a) = \phi(b)$ , then

$$\phi(a) = \phi(b) \implies a^3 = b^3 \implies a = b.$$

Hence  $\forall a, b \in G, \phi(a) = \phi(b) \implies a = b$ . Next, since  $\mathbb{I} \subseteq \mathbb{R}$  and

$$y^3 = x \implies y = \sqrt[3]{x} \in \mathbb{I} \subseteq \mathbb{R},$$

it follows that  $\forall x \in G, \exists y \in G : \phi(y) = y^3 = (\sqrt[3]{x})^3 = x$ . But

$$\forall a, b \in G, \phi(a+b) = (a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \neq \phi(a) + \phi(b).$$

Hence  $\phi$  is not operation-preserving and  $G$  and  $G$  are not isomorphic under  $\phi(x) = x^3$ .

**Example 6.4.** 1. Show that  $U(10)$  under multiplication modulo 10  $\approx \mathbb{Z}_4$  under addition modulo 4.

Note that  $\mathbb{Z}_{\cancel{4}} = \{1, 2, 3\}, U(10) = \{1, 3, 7, 9\} = \langle 3 \rangle$  and  $|U(10)| = 4$ . By Example 6.2,  $U(10) \approx \mathbb{Z}_4$  under  $\phi(3^k) = k \bmod 4$ . First, assume that  $\forall 3^i, 3^j \in U(10), \phi(3^i) = \phi(3^j)$ . Then

$$\begin{aligned} \phi(3^i) &= \phi(3^j), \\ i \bmod 4 &= j \bmod 4, \\ (i-j) \bmod 4 &= 0 \implies 4 \mid (i-j). \end{aligned}$$

By Theorem 4.1 (ii),

$$|3| = 4 \implies (3^i = 3^j \iff 4 \mid (i-j)).$$

Hence,

$$\forall 3^i, 3^j \in U(10), \phi(3^i) = \phi(3^j) \implies 3^i = 3^j.$$

Next, since

$$\begin{aligned} 1 &\in \mathbb{Z}_4, 1 = \phi(3^1) = \phi(3^5) = \phi(3^{4k}), \\ 2 &\in \mathbb{Z}_4, 2 = \phi(3^{4k+2}), \\ 3 &\in \mathbb{Z}_4, 3 = \phi(3^{4k+3}), \end{aligned}$$

it follows that  $\forall x \in \mathbb{Z}_4, \exists 3^k \in U(10) : \phi(3^k) = x$ . Finally,

$$\begin{aligned} \phi(3^i 3^j) &= \phi(3^{i+j}) \\ &= (i+j) \bmod 4 \\ &= i \bmod 4 + j \bmod 4 \\ &= \phi(3^i) + \phi(3^j). \end{aligned}$$

Hence,  $U(10) \approx \mathbb{Z}_4$  under  $\phi(3^k) = k \bmod 4$ .

2. Similarly,  $U(5) \approx \mathbb{Z}_4$ .

**Example 6.5.** There is no isomorphism from  $\mathbb{Q}$  under addition to  $\mathbb{Q}' = \mathbb{Q} \setminus \{0\}$  under multiplication. Since if  $\mathbb{Q} \approx \mathbb{Q}'$ , then there is an 1-1 and onto function s.t.  $\exists a \in \mathbb{Q} : \phi(a) = -1$ . But

$$-1 = \phi(a) = \phi\left(\frac{1}{2}a + \frac{1}{2}a\right) = \phi\left(\frac{a}{2}\right) \cdot \phi\left(\frac{a}{2}\right) = \left(\phi\left(\frac{a}{2}\right)\right)^2$$

and there is no  $x \in \mathbb{Q}' : x^2 = -1$ . Hence there is no isomorphism from  $\mathbb{Q}$  under addition to  $\mathbb{Q}'$  under multiplication.

**Example 6.6.** Let  $G = SL(2, \mathbb{R})$ , the group of  $2 \times 2$  matrices with determinant 1. Show that  $G \approx G$  under  $\phi_M(A) = MAM^{-1}, \forall A \in G, M$  is any  $2 \times 2$  matrix with determinant 1.

First, let  $A \in G$  be arbitrary, then

$$\det(\phi_M(A)) = \det(MAM^{-1}) = (\det M)(\det A)(\det M^{-1}) = 1 \cdot 1 \cdot 1 = 1.$$

Hence  $\phi_M : G \rightarrow G$ . Second, assume that  $\forall A, B \in G, \phi_M(A) = \phi_M(B)$ . Then

$$\begin{aligned} \phi_M(A) &= \phi_M(B), \\ MAM^{-1} &= MBM^{-1}, \\ M^{-1}MAM^{-1} &= M^{-1}MBM^{-1}, \\ 1 \cdot AM^{-1} &= 1 \cdot BM^{-1}, \\ AM^{-1}M &= BM^{-1}M, \\ A &= B. \end{aligned}$$

Hence,  $\forall A, B \in G, \phi_M(A) = \phi_M(B) \implies A = B$ . Next, let  $B \in G$  be arbitrary. WTS  $\exists A \in G : \phi(A) = MAM^{-1} = B$ . Notice that

$$\phi(A) = MAM^{-1} = B \implies A = M^{-1}BM.$$

Let  $A = M^{-1}BM \in G$ , then

$$\phi(A) = MAM^{-1} = M(M^{-1}BM)M^{-1} = B.$$

Hence  $\forall B \in G, \exists A \in G : \phi(A) = B$ . Finally,

$$\phi(AB) = MABM^{-1} = (MA)I(BM^{-1}) = (MAM^{-1})(MBM^{-1}) = \phi(A)\phi(B).$$

Hence  $G \approx G$  under  $\phi(A) = MAM^{-1}, A \in G$ .

## 6.2 Cayley's Theorem

**Theorem 6.1** (Cayley's Theorem). *Every group is isomorphic to a group of permutations.*

*Proof.* Let  $G$  be an arbitrary group. Then for every  $g \in G$ , define a function  $T_g : G \rightarrow G$  as

$$\forall x \in G, T_g(x) = gx.$$

WTS  $T_g$  is a permutation on the set of elements of  $G$ . Let  $x_1, x_2 \in G$  be arbitrary, assume that  $T_g(x_1) = T_g(x_2)$ . Then,

$$T_g(x_1) = T_g(x_2),$$

$$gx_1 = gx_2,$$

$$g^{-1}gx_1 = g^{-1}gx_2,$$

$$x_1 = x_2.$$

Hence  $\forall x_1, x_2 \in G, T_g(x_1) = T_g(x_2) \implies x_1 = x_2$  and  $T_g$  is 1-1.

Next, let  $y \in G$  be arbitrary. Notice that

$$T_g(x) = gx = y \implies x = g^{-1}y.$$

Since  $g^{-1}y \in G \implies x = g^{-1}y \in G$ , let  $x = g^{-1}y$ , it follows that

$$T_g(x) = gx = g(g^{-1}y) = y.$$

Hence  $\forall y \in G, \exists x \in G : T_g(x) = y$  and  $T_g$  is onto. Since  $T_g : G \rightarrow G$  is 1-1 and onto, by Definition 5.1,  $T_g$  is a permutation of the elements of  $G$ .

Let  $\overline{G} = \{T_g : g \in G\}$ . WTS  $\overline{G}$  is a group under function composition. First, let  $T_{g_1}, T_{g_2} \in \overline{G}, x \in G$  be arbitrary, then

$$\begin{aligned}(T_{g_1}T_{g_2})(x) &= T_{g_1}(T_{g_2}(x)) \\ &= T_{g_1}(g_2x) \\ &= g_1(g_2x) \\ &= (g_1g_2)(x) \\ &= T_{g_1g_2}(x) \in \overline{G}.\end{aligned}$$

Since  $\forall g_1, g_2 \in G, g_1g_2 \in G$ , it follows that  $T_{g_1g_2} \in \overline{G}$ . Hence  $\forall T_{g_1}, T_{g_2} \in \overline{G}, T_{g_1}T_{g_2} \in \overline{G}$  and  $\overline{G}$  is closed under function composition. Second, let  $T_{g_1}, T_{g_2}, T_{g_3} \in \overline{G}, x \in G$  be arbitrary, then

$$\begin{aligned}(T_{g_1}(T_{g_2}T_{g_3}))(x) &= T_{g_1}((T_{g_2}T_{g_3})(x)) & ((T_{g_1}T_{g_2})T_{g_3})(x) &= (T_{g_1}T_{g_2})(T_{g_3}(x)) \\ &= T_{g_1}(T_{g_2}(T_{g_3}(x))) & &= (T_{g_1}T_{g_2})(g_3x) \\ &= T_{g_1}(T_{g_2}(g_3x)) & &= T_{g_1}(T_{g_2}(g_3x)) \\ &= T_{g_1}(g_2g_3x) & &= T_{g_1}(g_2g_3x) \\ &= g_1g_2g_3x & &= g_1g_2g_3x.\end{aligned}$$

Hence  $\forall T_{g_1}, T_{g_2}, T_{g_3} \in \overline{G}, T_{g_1}(T_{g_2}T_{g_3}) = (T_{g_1}T_{g_2})T_{g_3}$  and  $T_g$  is associative under function composition. Next,  $e \in G \implies T_e \in \overline{G}$ . Let  $T_g \in \overline{G}, x \in G$  be arbitrary. Then,

$$(T_eT_g)(x) = T_e(T_g(x)) = T_e(gx) = egx = gx = T_g(x).$$

and

$$(T_gT_e)(x) = T_g(T_e(x)) = T_g(ex) = gex = gx = T_g(x).$$

Hence  $T_eT_g = T_gT_e = T_g$  and  $T_e$  is the identity element of  $\overline{G}$ . Finally,  $g, g^{-1} \in G \implies T_g, T_{g^{-1}} \in \overline{G}$ . So

$$(T_{g^{-1}}T_g)(x) = T_{g^{-1}}(T_g(x)) = T_{g^{-1}}(gx) = g^{-1}gx = ex = T_e(x).$$

and

$$(T_gT_{g^{-1}})(x) = T_g(T_{g^{-1}}(x)) = T_g(g^{-1}x) = gg^{-1}x = ex = T_e(x).$$

Hence  $T_{g^{-1}}T_g = T_gT_{g^{-1}} = T_e$  and  $T_{g^{-1}}$  is the inverse of  $T_g$ . Therefore,  $\overline{G}$  is a group under function composition.

Let  $\phi(g) = T_g, \forall g \in G$ , so  $\phi : G \rightarrow \overline{G}$ . WTS  $G \approx \overline{G}$  under  $\phi$ . First, assume that  $\forall g_1, g_2 \in G, T(g_1) = T(g_2)$ . Then,

$$\phi(g_1) = \phi(g_2) \implies T_{g_1} = T_{g_2}.$$

It follows that

$$\begin{aligned} T_{g_1}(x) &= T_{g_2}(x), x \in G, \\ g_1x &= g_2x, \\ g_1 &= g_2. \end{aligned}$$

Hence  $\forall g_1, g_2 \in G, T(g_1) = T(g_2) \implies g_1 = g_2$ . Next, by definition,

$$\overline{G} = \{T_g : g \in G\} \implies \forall T_g \in \overline{G}, \exists g \in G : \phi(g) = T_g.$$

Hence  $\overline{G}$  is onto. Finally,  $\phi(g_1g_2) = T_{g_1g_2}$  and

$$T_{g_1g_2}(x) = g_1g_2x = g_1T_{g_2}(x) = T_{g_1}(T_{g_2}(x)) = (T_{g_1}T_{g_2})(x).$$

Hence

$$\phi(g_1g_2) = T_{g_1g_2} = T_{g_1}T_{g_2} = \phi(g_1)\phi(g_2).$$

Therefore,  $G \approx \overline{G}$  under  $\phi$ . □

**Example 6.7.** For  $U(12) = \{1, 5, 7, 11\}$ , find  $\overline{U(12)}$ . Figure 6.4 shows the permutations of  $U(12)$  in array form. Figure 6.5 shows the Cayley tables for  $U(12)$  and  $\overline{U(12)}$ .

$$\begin{aligned} T_1 &= \begin{bmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{bmatrix}, & T_5 &= \begin{bmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{bmatrix}, \\ T_7 &= \begin{bmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{bmatrix}, & T_{11} &= \begin{bmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{bmatrix}. \end{aligned}$$

Figure 6.4: The permutations of  $U(12)$  in array form.

.

$U(12)$	1	5	7	11	$\overline{U(12)}$	$T_1$	$T_5$	$T_7$	$T_{11}$
1	1	5	7	11	$T_1$	$T_1$	$T_5$	$T_7$	$T_{11}$
5	5	1	11	7	$T_5$	$T_5$	$T_1$	$T_{11}$	$T_7$
7	7	11	1	5	$T_7$	$T_7$	$T_{11}$	$T_1$	$T_5$
11	11	7	5	1	$T_{11}$	$T_{11}$	$T_7$	$T_5$	$T_1$

Figure 6.5: The Cayley tables for  $U(12)$  and  $\overline{U(12)}$ .

### 6.3 Properties of Isomorphisms

**Theorem 6.2.** *Let  $\phi : G \rightarrow \overline{G}$  be an isomorphism. Then*

- (i)  $e \in G, \bar{e} \in \overline{G}, \phi(e) = \bar{e}$ .
- (ii)  $\forall n \in \mathbb{Z}, \forall a \in G, \phi(a^n) = (\phi(a))^n$ . In additive form,  $\phi(na) = n\phi(a)$ .
- (iii)  $\forall a, b \in G, ab = ba \iff \phi(a)\phi(b) = \phi(b)\phi(a)$ .
- (iv)  $G = \langle a \rangle \iff \overline{G} = \langle \phi(a) \rangle$ .
- (v)  $\forall a \in G, |a| = |\phi(a)|$ .
- (vi)  $k \in \mathbb{Z}, b \in G, x^k = b$  has the same number of solutions in  $G$  as the equation  $x^k = \phi(b)$  in  $\overline{G}$ .
- (vii) If  $G$  is finite, then  $G$  and  $\overline{G}$  have exactly the same number of elements of every order.

*Proof.* (i) Let  $e \in G, \bar{e} \in \overline{G}$ . Then,

$$\begin{aligned}\bar{e}\phi(e) &= \phi(ee) = \phi(e)\phi(e), \\ \bar{e}\phi(e)(\phi(e))^{-1} &= \phi(e)\phi(e)(\phi(e))^{-1}, \\ \bar{e} &= \phi(e).\end{aligned}$$

(ii) Let  $n \in \mathbb{Z}, a \in G$  be arbitrary. Then,

$$\phi(a^n) = \phi(\underbrace{aa \cdots a}_n) = \underbrace{\phi(a)\phi(a) \cdots \phi(a)}_n = (\phi(a))^n.$$

Hence  $\forall n \in \mathbb{Z}, \forall a \in G, \phi(a^n) = (\phi(a))^n$ .

(iii) Let  $a, b \in G$  be arbitrary.

( $\Rightarrow$ ) Assume that  $ab = ba$ . Then,

$$ab = ba \implies \phi(ab) = \phi(ba) \implies \phi(a)\phi(b) = \phi(b)\phi(a).$$

( $\Leftarrow$ ) Assume that  $\phi(ab) = \phi(ba)$ . Then,

$$\phi(ab) = \phi(ba) \implies ab = ba.$$

(iv) Let  $G = \langle a \rangle$ . By closure,  $\overline{G} = \langle \phi(a) \rangle$ . Since  $\phi$  is onto,  $\forall b \in \overline{G}, \exists a^k \in G : \phi(a^k) = b$ . Then, by Theorem 6.1 (ii),

$$b = \phi(a^k) = (\phi(a))^k \subseteq \langle \phi(a) \rangle.$$

Hence  $\overline{G} \subseteq \langle \phi(a) \rangle$  and  $\overline{G} = \langle \phi(a) \rangle$ .



(v) Let  $a \in G$  be arbitrary and let  $|a| = k$ . Then  $a^k = e$  and

$$\bar{e} = \phi(e) = \phi(a^k) = (\phi(a))^k.$$

So  $|\phi(a)| = t \leq k$ . Let  $t < k$ , then

$$\bar{e} = (\phi(a))^t = \phi(a^t) \implies a^t = e.$$

But this contradicts that  $|a| = k$ . Hence  $t = k$  and  $|a| = |\phi(a)|$ .

(vi) Let  $x^k = b \in G, x^k = \phi(b) \in \bar{G}, k \in \mathbb{Z}$ . Then,

$$x = b^{1/k} = (\phi(b))^{1/k} = \phi(b^{1/k}).$$

Hence the number of  $x : x = b^{1/k} \in G$  is the same as the number of  $x : x = \phi(b^{1/k}) \in \bar{G}$ .

(vii) Let  $G$  be finite. Since  $\phi$  is 1-1 and onto, and by Theorem 6.1 (ii),  $\forall a \in G, |a| = |\phi(a)|$ . Hence the number of  $a \in G : |a| = k$  is the same as the number of  $\phi(a) \in \bar{G} : |\phi(a)| = k$ .

□

**Theorem 6.3.** Let  $\phi : G \rightarrow \bar{G}$  be an isomorphism. Then

- (i)  $\phi^{-1} : \bar{G} \rightarrow G$  is an isomorphism.
- (ii)  $G$  is Abelian  $\iff \bar{G}$  is Abelian.
- (iii)  $G$  is cyclic  $\iff \bar{G}$  is cyclic.
- (iv)  $K \leq G \implies \phi(K) = \{\phi(k) : k \in K\} \leq \bar{G}$ .
- (v)  $\bar{K} \leq \bar{G} \implies \phi^{-1}(\bar{K}) = \{\phi^{-1}(\bar{k}) : \bar{k} \in \bar{K}\} \leq G$ .
- (vi) For the center  $Z(G)$ ,  $\phi(Z(G)) = Z(\bar{G})$ .

*Proof.* Let  $\phi : G \rightarrow \bar{G}$  be an isomorphism. Since  $\phi : G \rightarrow \bar{G}$  is 1-1 and onto, by Theorem 0.6,

$$\exists \phi^{-1} : \bar{G} \rightarrow G : \forall g \in G, \phi^{-1}(\phi(g)) = g \text{ and } \forall \bar{g} \in \bar{G}, \phi(\phi^{-1}(\bar{g})) = \bar{g}.$$

(i) First, assume that  $\forall \bar{a}, \bar{b} \in \bar{G}, \phi^{-1}(\bar{a}) = \phi^{-1}(\bar{b})$ , then

$$\begin{aligned} \phi^{-1}(\bar{a}) &= \phi^{-1}(\bar{b}), \\ \phi(\phi^{-1}(\bar{a})) &= \phi(\phi^{-1}(\bar{b})), \\ \bar{a} &= \bar{b}. \end{aligned}$$

Hence  $\forall \bar{a}, \bar{b} \in \bar{G}, \phi^{-1}(\bar{a}) = \phi^{-1}(\bar{b}) \implies \bar{a} = \bar{b}$ . Next, let  $a \in G$  be arbitrary, then

$$\begin{aligned}\phi(a) &= \bar{a} \in \bar{G}, \\ \phi^{-1}(\phi(a)) &= \phi^{-1}(\bar{a}), \\ a &= \phi^{-1}(\bar{a}).\end{aligned}$$

Hence  $\forall a \in G, \exists \bar{a} \in \bar{G} : \phi^{-1}(\bar{a}) = a$ . Finally, since  $\phi(ab) = \phi(a)\phi(b) = \bar{a}\bar{b}$ , it follows that

$$\phi^{-1}(\bar{a}\bar{b}) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(\bar{a})\phi^{-1}(\bar{b}).$$

Hence  $\phi^{-1} : \bar{G} \rightarrow G$  is an isomorphism.

(ii)  $(\implies)$  Let  $G$  be Abelian. So

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

Then,

$$\begin{aligned}\phi(ab) &= \phi(ba), \\ \phi(a)\phi(b) &= \phi(b)\phi(a), \\ \bar{a}\bar{b} &= \bar{b}\bar{a}, \bar{a}, \bar{b} \in \bar{G}.\end{aligned}$$

So  $G$  is Abelian  $\implies \bar{G}$  is Abelian.

$(\impliedby)$  Let  $\bar{G}$  be Abelian. So

$$\forall \bar{a}, \bar{b} \in \bar{G}, \bar{a}\bar{b} = \bar{b}\bar{a}.$$

Then,

$$\begin{aligned}\phi^{-1}(\bar{a}\bar{b}) &= \phi^{-1}(\bar{b}\bar{a}), \\ \phi^{-1}(\bar{a})\phi^{-1}(\bar{b}) &= \phi^{-1}(\bar{b})\phi^{-1}(\bar{a}), \\ ab &= ba, a, b \in G.\end{aligned}$$

So  $\bar{G}$  is Abelian  $\implies G$  is Abelian.

Hence,  $G$  is Abelian  $\iff \bar{G}$  is Abelian.

(iii)  $(\implies)$  Let  $G$  be cyclic. So  $\exists a \in G : G = \langle a \rangle$ . Let  $\phi(a) = \bar{a} \in \bar{G}$ , by closure,  $\langle \bar{a} \rangle \subseteq \bar{G}$ . Let  $\bar{b} \in \bar{G}$ , then

$$\exists b \in G : \phi(b) = \bar{b}.$$

Since

$$b \in \langle a \rangle \implies b = a^k, k \in \mathbb{Z},$$

it follows that

$$\bar{b} = \phi(b) = \phi(a^k) = (\phi(a))^k = \bar{a}^k \in \langle \bar{a} \rangle.$$

Hence  $\overline{G} \subseteq \langle \bar{a} \rangle$  and  $\overline{G} = \langle \bar{a} \rangle$ .

( $\Leftarrow$ ) Let  $\overline{G}$  be cyclic. So  $\exists \bar{a} \in \overline{G} : G = \langle \bar{a} \rangle$ . Let  $\phi^{-1}(\bar{a}) = a \in G$ , by closure,  $\langle a \rangle \subseteq G$ . Let  $b \in G$ , then

$$\exists \bar{b} \in \overline{G} : \phi^{-1}(\bar{b}) = b.$$

Since

$$\bar{b} \in \langle \bar{a} \rangle \implies \bar{b} = \bar{a}^k, k \in \mathbb{Z},$$

it follows that

$$b = \phi^{-1}(\bar{b}) = \phi^{-1}(\bar{a}^k) = (\phi^{-1}(\bar{a}))^k = a^k \in \langle a \rangle.$$

Hence,  $G \subseteq \langle a \rangle$  and  $G = \langle a \rangle$ .

(iv) Let  $K \leq G$  and  $\phi(K) = \{\phi(k) : k \in K\} \subseteq \overline{G}$ . Since  $K \leq G$ ,

$$e \in K \implies \phi(e) \in \phi(K).$$

Hence  $\phi(K) \neq \emptyset$ .

Let  $a, b \in K$  be arbitrary, then  $\phi(a), \phi(b) \in \phi(K)$  and  $\phi(a)\phi(b) = \phi(ab)$ . Since  $K \leq G$ ,  $\forall a, b \in K, ab \in K$ . It follows that

$$ab \in K \implies \phi(ab) \in \phi(K).$$

Hence  $\forall \phi(a), \phi(b) \in \phi(K), \phi(a)\phi(b) \in \phi(K)$ .

Let  $\phi(a) \in \phi(K)$  be arbitrary. Then  $(\phi(a))^{-1} = \phi(a^{-1})$ . Since  $K \leq G, a \in K \implies a^{-1} \in K$ . It follows that

$$a^{-1} \in K \implies \phi(a^{-1}) \in \phi(K).$$

Hence  $\forall \phi(a) \in \phi(K), (\phi(a))^{-1} \in \phi(K)$ .

Hence by Theorem 3.2,  $\phi(K) \leq \overline{G}$ .

(v) Let  $\overline{K} \leq \overline{G}$  and  $\phi^{-1}(\overline{K}) \in \{\phi^{-1}(\bar{k}) : \bar{k} \in \overline{K}\} \subseteq G$ . Since  $\overline{K} \leq \overline{G}$ ,

$$\bar{e} \in \overline{K} \implies \phi^{-1}(\bar{e}) \in \phi^{-1}(\overline{K}).$$

Hence  $\phi(\overline{K}) \neq \emptyset$ .

Let  $\phi^{-1}(\bar{a}), \phi^{-1}(\bar{b}) \in \phi^{-1}(\overline{K})$  be arbitrary. Then,  $\phi^{-1}(\bar{a})\phi^{-1}(\bar{b}) = \phi^{-1}(\bar{a}\bar{b})$ . Since  $\overline{K} \leq \overline{G}$ , it follows that

$$\bar{a}\bar{b} \in \overline{K} \implies \phi^{-1}(\bar{a}\bar{b}) \in \phi^{-1}(\overline{K}).$$

Hence  $\forall \phi^{-1}(\bar{a}), \phi^{-1}(\bar{b}) \in \phi^{-1}(\bar{K}), \phi^{-1}(\bar{a})\phi^{-1}(\bar{b}) \in \phi^{-1}(\bar{K})$ .

Let  $\phi^{-1}(\bar{a}) \in \phi^{-1}(\bar{K})$  be arbitrary. Then

$$(\phi^{-1}(\bar{a}))^{-1} = \phi^{-1}(\bar{a}^{-1}).$$

Since  $\bar{K} \leq \bar{G}$ , it follows that  $\forall \bar{a} \in \bar{K}, \bar{a}^{-1} \in \bar{K}$ , and

$$\bar{a}^{-1} \in \bar{K} \implies \phi^{-1}(\bar{a}^{-1}) \in \phi^{-1}(\bar{K})$$

Hence,  $\forall \phi^{-1}(\bar{a}) \in \phi^{-1}(\bar{K}), (\phi^{-1}(\bar{a}))^{-1} \in \phi^{-1}(\bar{K})$ .

Hence by Theorem 3.2,  $\phi^{-1}(\bar{K}) \leq G$ .

□

**Example 6.8.** Consider  $\mathbb{Z}_12, D_6, A_4$ . All three groups have order 12. Since the largest order of any element in the three are 12, 6, 3, respectively, no two are isomorphic. Alternatively, the number of elements of order 2 in each is 1, 7, 3.

**Example 6.9.**  $\mathbb{Q}$  under addition is not isomorphic to  $\mathbb{Q}' = \mathbb{Q} \setminus \{0\}$  under multiplication. Because  $\forall a \in \mathbb{Q}, a \neq e, |a| = \infty$ , since  $an = 0 \iff a = 0$ , but  $|-1| = 2$  in  $\mathbb{Q}'$ .

## 6.4 Automorphisms

**Definition 6.2.** An isomorphism  $G \approx G$  is an *automorphism* of  $G$ .

**Example 6.10.** The isomorphism  $SL(2, \mathbb{R}) \approx SL(2, \mathbb{R})$  in Example 6.6 is an automorphism of  $SL(2, \mathbb{R})$ .

**Example 6.11.** The function  $\phi : \mathbb{C} \rightarrow \mathbb{C}$  given by  $\phi(a + bi) = a - bi$  is an automorphism of  $(\mathbb{C}, +)$ . The restriction of  $\phi$  to  $\mathbb{C}^*$  is an automorphism of  $(\mathbb{C}^*, \cdot)$ .

**Example 6.12.** Let  $\mathbb{R}^2 = \{(a, b) : a, b \in \mathbb{R}\}$ . Then  $\phi(a, b) = (b, a)$  is an automorphism of  $\mathbb{R}^2$  under componentwise addition. Geometrically,  $\phi$  reflects each point in the plane across the line  $y = x$ . Generally, any reflection across a line passing through the origin or any rotation of the plane about the origin is an automorphism of  $\mathbb{R}^2$ .

**Definition 6.3.** Let  $G$  be a group, and let  $a \in G$ . The function  $\phi_a : \forall x \in G, \phi_a(x) = axa^{-1}$  is the inner automorphism of  $G$  induced by  $a$ .

**Example 6.13.** By Example 6.6,  $\phi_a$  is actually an automorphism of  $G$ .

**Example 6.14.** Figure 6.6 shows the inner automorphism of  $D_4$  induced by  $R_{90}$ .

$$\begin{array}{lcl}
x & \xrightarrow{\phi_{R_{90}}} & R_{90} x R_{90}^{-1} \\
\hline
R_0 & \rightarrow & R_{90} R_0 R_{90}^{-1} = R_0 \\
R_{90} & \rightarrow & R_{90} R_{90} R_{90}^{-1} = R_{90} \\
R_{180} & \rightarrow & R_{90} R_{180} R_{90}^{-1} = R_{180} \\
R_{270} & \rightarrow & R_{90} R_{270} R_{90}^{-1} = R_{270} \\
H & \rightarrow & R_{90} H R_{90}^{-1} = V \\
V & \rightarrow & R_{90} V R_{90}^{-1} = H \\
D & \rightarrow & R_{90} D R_{90}^{-1} = D' \\
D' & \rightarrow & R_{90} D' R_{90}^{-1} = D
\end{array}$$

Figure 6.6

**Definition 6.4.**  $Aut(G)$  is the set of all automorphisms of  $G$  and  $Inn(G)$  is the set of all inner automorphisms of  $G$ .

**Theorem 6.4.** Let  $G$  be a group. Then  $Aut(G)$  and  $Inn(G)$  are both groups under function composition.

*Proof.* Let  $G$  be a group, and let  $Aut(G) = \{\phi : G \rightarrow G \text{ s.t. } G \approx G\}$ ,  $Inn(G) = \{\phi_a : a \in G\}$ .

WTS  $Aut(G)$  is a group. First, let  $\phi_1, \phi_2 \in Aut(G), a \in G$  be arbitrary. Then,

$$(\phi_1 \phi_2)(a) = \phi_1(\phi_2(a)) = \phi_1(b) = c.$$

Since  $\phi_1, \phi_2$  are automorphisms of  $G$ , it follows that

$$b, c \in G \implies \phi_1 \phi_2 \in Aut(G).$$

Hence

$$\forall \phi_1, \phi_2 \in Aut(G), \phi_1 \phi_2 \in Aut(G)$$

and  $Aut(G)$  is closed under function composition. Second, by Theorem 0.6,

$$\forall \phi_1, \phi_2, \phi_3 \in Aut(G), \phi_1(\phi_2 \phi_3) = (\phi_1 \phi_2) \phi_3.$$

Third, let  $\phi_e(a) = a, \forall a \in G$ . WTS  $\phi_e \in Aut(G)$ . First, since  $\forall a \in G, \phi_e(a) = a$ , it follows that  $\phi_e : G \rightarrow G$ . Second, assume that  $\forall a, b \in G, \phi_e(a) = \phi_e(b)$ . Then,

$$\phi_e(a) = \phi_e(b) \implies a = b.$$

Hence  $\phi_e$  is 1-1. Third, since  $\forall a \in G, \exists a \in G : \phi(a) = a$ . Hence  $\phi_e$  is onto. Finally,

$$\phi_e(ab) = ab = \phi_e(a)\phi_e(b).$$

Hence,  $\phi_e$  is an automorphism of  $G$  and  $\phi_e \in \text{Aut}(G)$ . It follows that

$$(\phi\phi_e)(a) = \phi(\phi_e(a)) = \phi(a)$$

and

$$(\phi_e\phi)(a) = \phi_e(\phi(a)) = \phi(a).$$

Hence,

$$\exists \phi_e \in \text{Aut}(G) : \forall \phi \in \text{Aut}(G), \phi\phi_e = \phi_e\phi = \phi,$$

and  $\phi_e$  is the identity element of  $\text{Aut}(G)$ . Finally, since  $\forall \phi \in \text{Aut}(G), \phi : G \rightarrow G$  is an automorphism, by Theorem 6.3,  $\phi^{-1} : G \rightarrow G$  is an isomorphism and  $\phi^{-1} \in \text{Aut}(G)$ . By Theorem 0.6, since  $\phi$  is 1-1 and onto,

$$\forall a \in G, (\phi^{-1}\phi)(a) = a = \phi_e(a) \text{ and } (\phi\phi^{-1})(a) = a = \phi_e(a).$$

Hence,

$$\forall \phi \in \text{Aut}(G), \exists \phi^{-1} \in \text{Aut}(G) : \phi^{-1}\phi = \phi\phi^{-1} = \phi_e$$

and  $\phi^{-1}$  is a reverse of  $\phi$ . Therefore,  $\text{Aut}(G)$  is a group.

WTS  $\text{Inn}(G) = \{\phi_a : a \in G\}$  under function composition is a group. First, let  $\phi_a, \phi_b \in \text{Inn}(G), x \in G$  be arbitrary. Then,

$$\begin{aligned} (\phi_a\phi_b)(x) &= \phi_a(\phi_b(x)) \\ &= \phi_a(bxb^{-1}), \\ &= abxb^{-1}a^{-1} \\ &= (ab)x(ab)^{-1} \quad (\text{Theorem 2.4}) \\ &= \phi_{ab}(x). \end{aligned}$$

Since  $a, b \in G \implies ab \in G$ , it follows that  $\phi_{ab} \in \text{Inn}(G)$  and  $\text{Inn}(G)$  is closed under function composition. Second, By Theorem 0.6,

$$\phi_a(\phi_b\phi_c) = (\phi_a\phi_b)\phi_c.$$

Hence function composition is associative. Third, since  $e \in G \implies \phi_e \in \text{Inn}(G)$ , it follows that

$$(\phi_a\phi_e)(x) = \phi_a(\phi_e(x)) = \phi_a(exe^{-1}) = \phi_a(x)$$

and

$$(\phi_e\phi_a)(x) = \phi_e(\phi_a(x)) = \phi_e(axa^{-1}) = eaxa^{-1}e^{-1} = axa^{-1} = \phi_a(x).$$

Hence  $\phi_a\phi_e = \phi_e\phi_a = \phi_a$  and  $\phi_e$  is the identity element of  $\text{Inn}(G)$ . Finally, since  $a^{-1} \in G \implies \phi_{a^{-1}} \in \text{Inn}(G)$ , it follows that

$$\begin{aligned} (\phi_a\phi_{a^{-1}})(x) &= \phi_a(\phi_{a^{-1}}(x)) \\ &= \phi_a(a^{-1}x(a^{-1})^{-1}) \\ &= \phi_a(a^{-1}xa) \\ &= aa^{-1}xaa^{-1} \\ &= x = \phi_e(x) \end{aligned}$$

and

$$\begin{aligned} (\phi_{a^{-1}}\phi_a)(x) &= \phi_{a^{-1}}(\phi_a(x)) \\ &= \phi_{a^{-1}}(axa^{-1}) \\ &= a^{-1}axa^{-1}(a^{-1})^{-1} \\ &= a^{-1}axa^{-1}a \\ &= x = \phi_e(x). \end{aligned}$$

Hence  $\phi_a\phi_{a^{-1}} = \phi_{a^{-1}}\phi_a = \phi_e$  and  $\phi_{a^{-1}}$  is the reverse of  $\phi_a$ . Therefore,  $\text{Inn}(G)$  is a group under function composition.  $\square$

**Example 6.15.** To find  $\text{Inn}(D_4)$ , note that the list of inner automorphisms of  $D_4$  is  $\{\phi_{R_0}, \phi_{R_{90}}, \phi_{R_{180}}, \phi_{R_{270}}, \phi_H, \phi_V, \phi_D, \phi_{D'}\}$ . Since  $R_{180} \in Z(D_4) = \{a \in D_4 : \forall x \in D_4, ax = xa\}$ , it follows that

$$\phi_{R_{180}}(x) = R_{180}xR_{180}^{-1} = x,$$

so  $\phi_{R_{180}} = \phi_{R_0}$ . Also,

$$\phi_{R_{270}}(x) = R_{270}xR_{270}^{-1} = R_{90}R_{180}xR_{180}^{-1}R_{90}^{-1} = R_{90}xR_{90}^{-1} = \phi_{R_{90}}(x).$$

Similarly, since  $H = R_{180}V$  and  $D' = R_{180}D$ , it follows that

$$\phi_H = \phi_V, \phi_D = \phi_{D'}.$$

Hence the previous list can be pared down to  $\{\phi_{R_0}, \phi_{R_{90}}, \phi_H, \phi_D\}$ . WTS these are distinct.

**Example 6.16.** Compute  $\text{Aut}(\mathbb{Z}_{10})$ . Let  $\phi \in \text{Aut}(\mathbb{Z}_{10})$ . Since  $\phi$  is an automorphism of  $\mathbb{Z}_{10}$ , by Theorem 6.2 (ii) and (v),

$$\forall k \in \mathbb{Z}, \phi(k) = k\phi(1)$$

and

$$1 \in \mathbb{Z}_{10}, |\phi(1)| = |1| = 10.$$

So

$$\phi \in \text{Aut}(\mathbb{Z}_{10}) \implies |\phi(1)| = 10.$$

Define

$$\alpha_1(1) = 1, \quad \alpha_3(1) = 3, \quad \alpha_7(1) = 7, \quad \alpha_9(1) = 9.$$

Since

$$\begin{aligned} |\alpha_1(1)| &= |1| = 10, \\ |\alpha_3(1)| &= |3| = 10, \\ |\alpha_7(1)| &= |7| = 10, \\ |\alpha_9(1)| &= |9| = 10, \end{aligned}$$

it follows that

$$\alpha_1, \alpha_3, \alpha_7, \alpha_9 \in \text{Aut}(\mathbb{Z}_{10})$$

Since

$$\forall \phi \in \text{Aut}(\mathbb{Z}_{10}), (\alpha_1 \phi)(1) = \alpha_1(\phi(1)) = \phi(1)\alpha_1(1) = \phi(1)$$

and

$$(\phi \alpha_1)(1) = \phi(\alpha_1(1)) = \phi(1).$$

Hence  $\alpha_1$  is the identity element of  $\text{Aut}(\mathbb{Z}_{10})$ . Since

$$(\alpha_3 \alpha_7)(1) = \alpha_3(\alpha_7(1)) = \alpha_3(7) = 7\alpha_3(1) = 7 \cdot 3 \bmod 10 = 1$$

and

$$(\alpha_7 \alpha_3)(1) = \alpha_7(\alpha_3(1)) = \alpha_7(3) = 3\alpha_7(1) = 3 \cdot 7 \bmod 10 = 1,$$

it follows that  $\phi_7$  is the reverse of  $\phi_3$  and vice versa. The reverses of  $\phi_1$  and  $\phi_9$  are themselves. Since

$$\begin{aligned} \alpha_3(1) &= 3, \\ (\alpha_3 \alpha_3)(1) &= (\alpha_3)^2(1) = 3 \cdot 3 \bmod 10 = 9, \\ (\alpha_3)^3(1) &= 3 \cdot 3 \cdot 3 \bmod 10 = 7, \\ (\alpha_3)^4(1) &= 3^4 \bmod 10 = 1, \\ (\alpha_3)^5(1) &= 3^4 \bmod 10 = 3, \\ &\vdots \end{aligned}$$

it follows that  $\text{Aut}(\mathbb{Z}_{10}) = \langle \alpha_3 \rangle$  and  $\text{Aut}(\mathbb{Z}_{10})$  is cyclic. Figure 6.7 shows that  $\mathbb{Z}_{10} \approx U(10)$ .

**Theorem 6.5.**  $\forall n \in \mathbb{N}, \text{Aut}(\mathbb{Z}_n) \approx U(n)$ .

*Proof.* (Not covered in lectures) Let  $n \in \mathbb{N}$  be arbitrary. Let  $\phi \in \text{Aut}(\mathbb{Z}_n)$ . So  $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  is an automorphism. By Theorem 6.2 (ii),

$$\forall n \in \mathbb{Z}, \phi(n) = n\phi(1).$$



$U(10)$	1	3	7	9	$Aut(\mathbb{Z}_{10})$	$\alpha_1$	$\alpha_3$	$\alpha_7$	$\alpha_9$
1	1	3	7	9	$\alpha_1$	$\alpha_1$	$\alpha_3$	$\alpha_7$	$\alpha_9$
3	3	9	1	7	$\alpha_3$	$\alpha_3$	$\alpha_9$	$\alpha_1$	$\alpha_7$
7	7	1	9	3	$\alpha_7$	$\alpha_7$	$\alpha_1$	$\alpha_9$	$\alpha_3$
9	9	7	3	1	$\alpha_9$	$\alpha_9$	$\alpha_7$	$\alpha_3$	$\alpha_1$

Figure 6.7: The Cayley tables of  $\mathbb{Z}_{10}$  and  $U(10)$ .

Hence any automorphism  $\phi$  is determined by the value of  $\phi(1)$ . By Theorem 6.2 (v),

$$1 \in \mathbb{Z}_n, |\phi(1)| = |1| = n.$$

Let  $\alpha(1) = 1$ , then

$$|\alpha(1)| = |1| = n \implies \alpha \in \mathbb{Z}_n$$

and  $\alpha(1) = 1 \in U(n)$ . Let  $f : Aut(\mathbb{Z}_n) \rightarrow U(n)$  such that  $f(\phi) = \phi(1)$ .

First, assume that  $\forall \alpha, \beta \in Aut(\mathbb{Z}_n), f(\alpha) = f(\beta)$ . Then

$$f(\alpha) = f(\beta) \implies \alpha(1) = \beta(1).$$

It follows that

$$\forall k \in \mathbb{Z}, \alpha(k) = k\alpha(1) = k\beta(1) = \beta(k).$$

Hence  $f$  is 1-1. Next, let  $b \in U(10)$  be arbitrary and let  $\alpha(a) = ab \bmod n, \forall a \in \mathbb{Z}_n$ .  $\alpha$  is an automorphism of  $\mathbb{Z}_n$  and  $\alpha \in Aut(\mathbb{Z}_n)$ . Since

$$f(\alpha) = \alpha(1) = 1 \cdot b \bmod n = b \in U(n),$$

$f$  is onto. Finally, since

$$\begin{aligned} f(\alpha\beta) &= (\alpha\beta)(1) \\ &= \alpha(\beta(1)) \\ &= \beta(1)\alpha(1) \\ &= \alpha(1)\beta(1) \\ &= f(\alpha)f(\beta). \end{aligned}$$

Hence  $Aut(\mathbb{Z}_n) \approx U(n)$ . □

**Example 6.17.** Consider  $H \leq S_4$ ,

$$H = \{(1), (1234), (13)(24), (1432), (12)(34), (24), (14)(23), (13)\}.$$

One has the subgroups

$$(12)H(21) = \{(1), (1342), (14)(23), (1234), (12)(34), (14), (13)(24), (23)\}$$

and

$$(123)H(321) = \{(1), (1423), (12)(34), (1324), (14)(23), (34), (13)(24), (12)\}$$

of  $S_4$  that are isomorphic to  $H$ .

## 7 Cosets and Lagrange's Theorem

### 7.1 Properties of Cosets

**Definition 7.1.** Let  $G$  be a group and let  $H \leq G, H \neq \emptyset$ . For any  $a \in G$ ,

$$aH = \{ah : h \in H\}, \quad Ha = \{ha : h \in H\}, \quad aHa^{-1} = \{aha^{-1} : h \in H\}.$$

The set  $aH$  is the *left coset of  $H$  in  $G$  containing  $a$* ,  $Ha$  is the *right coset of  $H$  in  $G$  containing  $a$* . The element  $a$  is the *coset representative of  $aH$  or  $Ha$* . The number of elements in  $aH$  is  $|aH|$ , and the number of elements in  $Ha$  is  $|Ha|$ .

**Example 7.1.** Let  $G = S_3$  and  $H = \{(1), (13)\}$ . Then the left cosets of  $H$  in  $G$  are

$$\begin{aligned} (1)H &= H, \\ (12)H &= \{(12), (12)(13)\} = \{(12), (132)\} = (132)H, \\ (13)H &= \{(13), (1)\} = H, \\ (23)H &= \{(23), (23)(13)\} = \{(23), (123)\} = (123)H. \end{aligned}$$

**Example 7.2.** Let  $\alpha = \{R_0, R_{180}\} \leq D_4$ . Then

$$\begin{aligned} R_0\alpha &= \alpha, \\ R_{90}\alpha &= \{R_{90}, R_{270}\} = R_{270}\alpha, \\ R_{180}\alpha &= \{R_{180}, R_0\} = \alpha, \\ V\alpha &= \{V, H\} = H\alpha, \\ D\alpha &= \{D, D'\} = D\alpha. \end{aligned}$$

**Example 7.3.** Let  $H = \{0, 3, 6\} \leq \mathbb{Z}_9$  under addition. Then the left cosets of  $H$  in  $\mathbb{Z}_9$  are

$$\begin{aligned} 0 + H &= \{0 + 0, 0 + 3, 0 + 6\} = \{0, 3, 6\} = 3 + H = 6 + H, \\ 1 + H &= \{1, 4, 7\} = 4 + H = 7 + H, \\ 2 + H &= \{2, 5, 8\} = 5 + H = 8 + H. \end{aligned}$$

**Lemma 7.1.** Let  $G$  be a group,  $H \leq G$ , and  $a, b \in G$ . Then,

- (i)  $a \in aH$ .
- (ii)  $aH = H \iff a \in H$ .
- (iii)  $(ab)H = a(bH)$  and  $H(ab) = (Ha)b$ .
- (iv)  $aH = bH \iff a \in bH$ .
- (v)  $(aH = bH)$  or  $(aH \cap bH = \emptyset)$ ,
- (vi)  $aH = bH \iff a^{-1}b \in H$ .
- (vii)  $|aH| = |bH|$ .
- (viii)  $aH = Ha \iff H = aHa^{-1}$ .
- (ix)  $aH \leq G \iff a \in H$ .

*Proof.* Let  $G$  be a group,  $H \leq G$ , and  $a, b \in G$ .

(i) Since  $e \in H$ , it follows that  $a = ae \in aH$ .

(ii) ( $\Rightarrow$ ) Assume that  $aH = H$ . Then by Lemma 7.1 (i),

$$a \in aH = H.$$

( $\Leftarrow$ ) Assume that  $a \in H$ . Let  $ah \in aH$ , then

$$a \in H, h \in H \implies ah \in H.$$

Let  $h \in H$ . Since

$$a \in H \implies a^{-1} \in H,$$

it follows that  $a^{-1}h \in H$ . Then

$$h = eh = (aa^{-1})h = a(a^{-1}h) \in aH.$$

(iii) Let  $(ab)h \in (ab)H$ . Then

$$(ab)h = a(bh) \in a(bH) \implies (ab)H \subseteq a(bH).$$

Let  $a(bh) \in a(bH)$ . Then

$$a(bh) = (ab)h \in (ab)H \implies a(bH) \subseteq (ab)H.$$

Hence  $(ab)H = a(bH)$ .

Let  $h(ab) \in H(ab)$ . Then

$$h(ab) = (ha)b \in (Ha)b \implies H(ab) \subseteq (Ha)b.$$

Let  $(ha)b \in (Ha)b$ . Then

$$(ha)b = h(ab) \in H(ab) \implies (Ha)b \subseteq H(ab).$$

Hence  $H(ab) = (Ha)b$ .

(iv)  $(\implies)$  Assume that  $aH = bH$ . Then

$$a = ae \in aH = bH.$$

$(\impliedby)$  Assume that  $a \in bH$ . Then  $a = bh$  and by Lemma 7.1 (iii),

$$aH = (bh)H = b(hH).$$

Since  $h \in H$ , by Lemma 7.1 (ii),  $hH = H$  and hence

$$aH = b(hH) = bH.$$

(v) Assume that  $aH = bH$ . Then

$$aH \cap bH = aH = bH \neq \emptyset.$$

Assume that  $aH \cap bH = \emptyset$ . Then

$$\neg(\exists x : x \in aH, x \in bH) \implies aH \neq bH.$$

(vi)  $(\implies)$  Assume that  $aH = bH$ . Since

$$\begin{aligned} a(a^{-1}bH) &= b(a^{-1}bH), \\ bH &= ba^{-1}bH, \\ H &= a^{-1}bH, \\ aH &= bH, \end{aligned}$$

it follows that

$$aH = bH \iff a^{-1}bH = H.$$

By Lemma 7.1 (ii),

$$a^{-1}bH = H \iff a^{-1}b \in H.$$

$(\impliedby)$  Assume that  $a^{-1}b \in H$ . Then

$$a^{-1}bH = H \implies bH = aH.$$

(vii) Since  $|aH| = |H|$ ,  $|bH| = |H|$ , it follows that  $|aH| = |bH|$ .

(viii) ( $\Rightarrow$ ) Assume that  $aH = Ha$ . Then

$$\begin{aligned} aH &= Ha, \\ aHa^{-1} &= H. \end{aligned}$$

( $\Leftarrow$ ) Assume that  $H = aHa^{-1}$ . Then

$$\begin{aligned} H &= aHa^{-1}, \\ Ha &= aH. \end{aligned}$$

(ix) ( $\Rightarrow$ ) Assume that  $aH \leq G$ . Then

$$e \in aH, e = ee \in eH \implies aH \cap eH \neq \emptyset.$$

By Lemma 7.1 (v),  $aH = eH = H$ . By Lemma 7.1 (ii),

$$aH = H \iff a \in H.$$

( $\Leftarrow$ ) Assume that  $a \in H$ . By Lemma 7.1 (ii),

$$a \in H \iff aH = H \leq G.$$

□

**Example 7.4.** Find the cosets of  $H = \{1, 15\}$  in  $G = U(32) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$ .

$$\begin{aligned} 1H &= \{1, 15\} = 15H, \\ 3H &= \{3, 13\} = 13H, \\ 5H &= \{5, 11\} = 11H, \\ 7H &= \{7, 9\} = 9H, \\ 17H &= \{17, 31\} = 31H, \\ 19H &= \{19, 29\} = 29H, \\ 21H &= \{21, 27\} = 27H, \\ 23H &= \{23, 25\} = 25H. \end{aligned}$$

## 7.2 Lagrange's Theorem and Consequences

**Theorem 7.1** (Lagrange's Theorem). *Let  $G$  be a group,  $|G| = n$ . Then*

$$H \leq G \implies |H| \mid |G|.$$

*Moreover, the number of distinct left and right cosets of  $H$  in  $G$  is  $|G|/|H|$ .*

*Proof.* Let  $G$  be a group,  $|G| = n$ . Assume that  $H \leq G$ . Let  $a_1H, a_2H, \dots, a_rH$  be the distinct left cosets of  $H$  in  $G$ . Then,

$$\forall a \in G, \exists i \in \{1, 2, \dots, r\} : aH = a_iH.$$

By Lemma 7.1 (i),  $a \in aH$ . So

$$\forall a \in G, \exists i \in \{1, 2, \dots, r\} : a \in a_iH.$$

It follows that

$$G = a_1H \cup \dots \cup a_rH.$$

By Lemma 7.1 (v), this union is disjoint, so

$$|G| = |a_1H| + |a_2H| + \dots + |a_rH|.$$

Since

$$\forall i \in \{1, \dots, r\}, |a_iH| = |H|,$$

it follows that

$$\begin{aligned} |G| &= |a_1H| + |a_2H| + \dots + |a_rH| \\ &= \underbrace{|H| + \dots + |H|}_r \\ &= r|H|. \end{aligned}$$

Hence  $|H| \mid |G|$  and the number of distinct left and right cosets of  $H$  in  $G$  is  $r = |G|/|H|$ .  $\square$

**Definition 7.2.** The *index* of  $H \leq G$ , denoted by  $|G : H|$ , is the number of distinct left cosets of  $H$  in  $G$ .

**Corollary 7.1.1.**  $|G| = n, H \leq G \implies |G : H| = |G|/|H|$ .

**Corollary 7.1.2.**  $|G| = n \implies \forall a \in G, |a| \mid |G|$ .

*Proof.* Let  $G$  be a group and  $|G| = n$ . Let  $a \in G$  be arbitrary. By Theorem 3.4,  $\langle a \rangle \leq G$ . By Theorem 7.1,  $|\langle a \rangle| \mid |G|$ . Hence

$$\forall a \in G, |a| \mid |G|.$$

$\square$

**Corollary 7.1.3.**  $|G| = p, p \text{ is prime} \implies G \text{ is cyclic}$ .

*Proof.* Let  $G$  be a group and  $|G| = p$ ,  $p$  is prime. Let  $a \in G$  and  $a \neq e$ . Then, by Theorem 3.4,  $\langle a \rangle \leq G$ . By Theorem 7.1,  $|\langle a \rangle| \mid |G|$ . Since  $|G| = p$ , it follows that  $|\langle a \rangle| \in \{1, p\}$ . But

$$a \neq e \implies \langle a \rangle \neq 1.$$

Hence

$$|\langle a \rangle| = p = |G|, \langle a \rangle \leq G \implies G = \langle a \rangle.$$

□

**Corollary 7.1.4.**  $|G| = n, a \in G \implies a^{|G|} = e$ .

*Proof.* Let  $G$  be a group,  $|G| = n$ , and  $a \in G$ . By Corollary 7.1.2,  $|a| \mid |G|$ , so  $|G| = |a|k, k \in \mathbb{Z}$ . Then

$$a^{|G|} = a^{|a|k} = e^k = e.$$

□

**Corollary 7.1.5** (Fermat's Little Theorem).  $\forall a \in \mathbb{Z}, \forall p = \text{prime}, a^p \bmod p = a \bmod p$ .

*Proof.* Let  $a \in \mathbb{Z}$  and  $p$  is prime. By the division algorithm,

$$a = pm + r, 0 \leq r < p.$$

So  $a \bmod p = r$ . If  $r = 0$ , then  $a \bmod p = 0$  and  $a^p \bmod p = 0$ . If  $0 < r < p$ , let  $r \in U(p) = \{1, 2, \dots, p-1\}$  under multiplication modulo  $p$ . Then by Corollary 7.1.4,

$$r^{|U(p)|} = r^{p-1} = 1.$$

It follows that

$$r^{p-1} \bmod p = 1 \implies r^p \bmod p = r.$$

□

**Example 7.5.** The converse of Lagrange's Theorem is false. By Table 5.1,  $A_4$  has eight elements of order 3 ( $\alpha_5$  through  $\alpha_{12}$ ). Let  $H \leq A_4, |H| = 6$ . Let  $a \in A_4, |a| = 3$ . By Theorem 7.1,

$$|A_4 : H| = |A_4|/|H| = 12/6 = 2.$$

So at most two of the cosets  $H, aH, a^2H$  are distinct. But equality of any pair of these three implies that  $aH = H \implies a \in H$ . Thus,  $H : |H| = 6$  would have to contain all eight  $a \in A_4, |a| = 3$ , which is absurd.

**Theorem 7.2.** Let  $G$  be a group,  $H, K \leq G, |H| = m, |K| = n$ . Define the set  $HK = \{hk : h \in H, k \in K\}$ . Then  $|HK| = |H||K|/|H \cap K|$ .

*Proof.* Although the set  $HK$  has  $|H||K|$  products, there may be  $hk = h'k', h \neq h', k \neq k'$ . For every  $t \in H \cap K$ , the product  $hk = (ht)(t^{-1}k)$ , so each element in  $HK$  is represented by at least  $|H \cap K|$  products in  $HK$ . But

$$hk = h'k' \implies t = h^{-1}h' = kk'^{-1} \in H \cap K \implies h' = ht, k' = t^{-1}k.$$

Thus each element in  $HK$  is represented by exactly  $|H \cap K|$  products. So  $|HK| = |H||K|/|H \cap K|$ .  $\square$

**Example 7.6.** A group of order 75 can have at most one subgroup of order 25. Suppose  $H, K$  are two subgroups of order 25. Since

$$|H \cap K| \mid |H| = |H \cap K| \mid 25 \implies |H \cap K| \in \{1, 5\}.$$

It follows that

$$|HK| = |H||K|/|H \cap K| = 25 \cdot 25/|H \cap K| \in \{625, 125\}.$$

Hence

$$|H \cap K| = 25 \implies H = K.$$

**Theorem 7.3.** Let  $G$  be a group and  $p > 2$  is a prime. Then

$$|G| = 2p \implies G \approx \mathbb{Z}_{2p} \text{ or } G \approx D_p.$$

*Proof.* Let  $G$  be a group and  $p > 2$  is a prime. Let  $|G| = 2p$ . Assume that  $\forall a \in G, |a| \neq 2p$ . Since  $a \in G, a \neq e, \langle a \rangle \leq G$ , by the Lagrange's Theorem,

$$|G| = 2p, \langle a \rangle \leq G \implies |\langle a \rangle| \mid |G| \implies |a| \mid 2p.$$

Hence

$$\forall a \in G, a \neq e, |a| = 2 \text{ or } |a| = p.$$

If  $|a| = 2$ , then

$$\forall a, b \in G, ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

So  $G$  is Abelian. Then,  $\forall a, b \in G, a, b \neq e, a \neq b$ , the set  $\{e, a, b, ab\}$  is closed and hence is a subgroup of  $G$  of order 4. But this contradicts the Lagrange's Theorem since

$$|G| = 2p, H \leq G \implies |H| \mid |G| = 2p,$$

and 4 does not divide  $2p$ . Hence  $|a| = p$ .

Let  $b \in G : b \neq \langle a \rangle$  be arbitrary. Then by the Lagrange's Theorem and the assumption that  $\forall a \in G, |a| \neq 2p$ , one has  $|b| = 2$  or  $|b| = p$ . Since  $\langle a \rangle, \langle b \rangle \leq G, |\langle a \rangle| \neq \infty, |\langle b \rangle| \neq \infty$ , by Theorem 7.2,

$$|\langle a \rangle \cap \langle b \rangle| \mid |\langle a \rangle| = |a| = p.$$



So  $|\langle a \rangle \cap \langle b \rangle| = 1$  or  $|\langle a \rangle \cap \langle b \rangle| = p$ . Since  $\langle a \rangle \neq \langle b \rangle$  and  $e \in \langle a \rangle, e \in \langle b \rangle$ , it follows that  $|\langle a \rangle \cap \langle b \rangle| = 1$ . If  $|b| = p$ , then by Theorem 7.2,

$$|\langle a \rangle \langle b \rangle| = |\langle a \rangle| |\langle b \rangle| = p^2 > 2p = |G|,$$

which is impossible. Hence  $\forall b \in G, b \notin \langle a \rangle, |b| = 2$ .

Consider  $ab$ . Since  $ab \notin \langle a \rangle$ ,  $|ab| = 2$ . Then

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

This relation completely determines the multiplication table for  $G$ . For example,

$$\begin{aligned} a^3(ba^4) &= a^2(ab)a^4 \\ &= a^2(ba^{-1})a^4 \\ &= a(ab)a^3 \\ &= a(ba^{-1})a^3 \\ &= (ab)a^2 \\ &= (ba^{-1})a^2 \\ &= ba. \end{aligned}$$

Since the multiplication table for all noncyclic groups of order  $2p$  is uniquely determined by the relation  $ab = ba^{-1}$ , all noncyclic groups of order  $2p$  must be isomorphic to each other.  $\square$

### 7.3 An Application of Cosets to Permutation Groups

**Definition 7.3.** Let  $G$  be a group of permutation of a set  $S$ . The *stabilizer of  $i \in S$  in  $G$*  is

$$\text{stab}_G(i) = \{\phi \in G : \phi(i) = i\}.$$

Proof that  $\text{stab}_G(i) \leq G$ . Let  $G$  be a group of permutation of a set  $S$ , let

$$\text{stab}_G(i) = \{\phi \in G : \phi(i) = i\}, i \in S.$$

Let  $\phi_1, \phi_2 \in \text{stab}_G(i)$ , so  $\phi_1(i) = i, \phi_2(i) = i$ . It follows that

$$(\phi_1\phi_2)(i) = \phi_1(\phi_2(i)) = \phi_1(i) = i \implies \phi_1\phi_2 \in \text{stab}_G(i).$$

Let  $\phi \in \text{stab}_G(i)$ . Then

$$\phi(\phi^{-1}(i)) = (\phi\phi^{-1})(i) = \epsilon(i) = i \implies \phi^{-1}(i) = i.$$

It follows that  $\phi^{-1} \in \text{stab}_G(i)$ . Hence by the Two-step Subgroup Test,  $\text{stab}_G(i) \leq G$ .

**Definition 7.4.** Let  $G$  be a group of permutations of a set  $S$ . The *orbit* of  $i \in S$  under  $G$  is

$$\text{orb}_G(i) = \{\phi(i) : \phi \in G\}.$$

The number of elements in  $\text{orb}_G(i)$  is  $|\text{orb}_G(i)|$ .

**Example 7.7.** Let

$$G = \{(1), (132)(456)(78), (132)(465), (123)(456), (123)(456)(78), (78)\} \leq S_8.$$

Then,

$$\begin{aligned} \text{orb}_G(1) &= \{1, 3, 2\}, & \text{stab}_G(1) &= \{(1), (78)\}, \\ \text{orb}_G(2) &= \{2, 1, 3\}, & \text{stab}_G(2) &= \{(1), (78)\}, \\ \text{orb}_G(4) &= \{4, 6, 5\}, & \text{stab}_G(4) &= \{(1), (78)\}, \\ \text{orb}_G(7) &= \{7, 8\}, & \text{stab}_G(7) &= \{(1), (132)(465), (123)(456)\}. \end{aligned}$$

**Example 7.8.** Let  $D_4$  be a group of permutation of a square. Figure 7.1(a) and (b) show  $\text{orb}_{D_4}(p)$  and  $\text{orb}_{D_4}(q)$ , respectively. Furthermore,  $\text{stab}_{D_4}(p) = \{R_0, D\}$  and  $\text{stab}_{D_4}(q) = \{R_0\}$ .

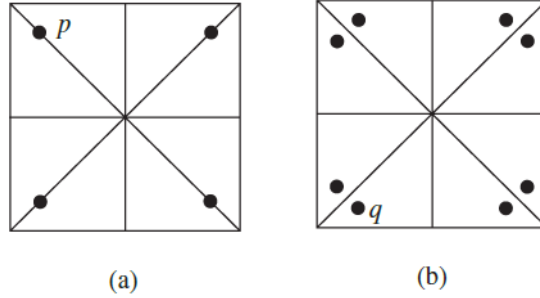


Figure 7.1: (a)  $\text{orb}_{D_4}(p)$ . (b)  $\text{orb}_{D_4}(q)$ .

**Theorem 7.4** (Orbit-Stabilizer Theorem). *Let  $G$  be a finite group of permutations of a set  $S$ . Then,*

$$i \in S, |G| = |\text{orb}_G(i)| |\text{stab}_G(i)|.$$

*Proof.* Let  $G$  be a group of permutation of a set  $S$  and  $|G| = n$ . By the Lagrange Theorem,

$$\text{stab}_G(i) \leq G \implies |\text{stab}_G(i)| \mid |G|, i \in S$$

and the number of distinct left cosets of  $stab_G(i)$  in  $G$ ,  $r = |G|/|stab_G(i)|$ .

Let

$$T : \{\phi stab_G(i) : \phi \in G\} \rightarrow orb_G(i) = \{\phi(i) : \phi \in G\}.$$

Assume that  $\alpha stab_G(i) = \beta stab_G(i)$ . Then by Lemma 7.1,

$$\alpha stab_G(i) = \beta stab_G(i) \iff \alpha^{-1}\beta \in stab_G(i).$$

It follows that

$$(\alpha^{-1}\beta)(i) = i \implies \alpha(i) = \alpha(\alpha^{-1}\beta(i)) = (\alpha\alpha^{-1}\beta)(i) = \beta(i).$$

Hence  $T$  is a well-defined function.

Assume that  $\alpha(i) = \beta(i)$ . Then  $(\alpha^{-1}\beta)(i) = i$  and it follows that by Lemma 7.1,

$$\alpha stab_G(i) = \beta stab_G(i) \iff \alpha^{-1}\beta \in stab_G(i).$$

Hence  $T$  is 1-1. Let  $j \in orb_G(i)$  be arbitrary. Since

$$\exists \alpha \in G : \alpha(i) = j,$$

it follows that

$$T(\alpha stab_G(i)) = \alpha(i) = j.$$

Hence  $T$  is onto  $orb_G(i)$ . Thus,

$$|orb_G(i)| = r = |G|/|stab_G(i)| \implies |G| = |orb_G(i)||stab_G(i)|.$$

□

## 7.4 The Rotation Group of a Cube and a Soccer Ball

**Theorem 7.5.** *The group of rotations of a cube is isomorphic to  $S_4$ .*

*Proof.*

□

## 8 External Direct Products

### 8.1 Definition and Examples

**Definition 8.1.** Let  $G_1, G_2, \dots, G_n$  be a finite collection of groups. The *external direct product* of  $G_1, G_2, \dots, G_n$  is

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \dots, g_n) : g_i \in G_i\},$$

where

$$(g_1, g_2, \dots, g_n)(g'_1, g'_2, \dots, g'_n) = (g_1g'_1, g_2g'_2, \dots, g_ng'_n).$$

Each  $g_i g'_i$  is performed with the operation of  $G_i$ . If each  $G_i$  is finite, then

$$|G_1 \oplus G_2 \oplus \cdots \oplus G_n| = |G_1||G_2| \cdots |G_n|.$$

Proof that  $G_1 \oplus \cdots \oplus G_n$  is a group. Since

$$(g_1, \dots, g_n)(g'_1, \dots, g'_n) = (g_1g'_1, \dots, g_ng'_n)$$

and  $g_1g'_1 \in G_1, \dots, g_ng'_n \in G_n$ , it follows that  $G_1 \oplus \cdots \oplus G_n$  is closed. Next, since

$$\begin{aligned} [(g_1, \dots, g_n)(g'_1, \dots, g'_n)](g''_1, \dots, g''_n) &= (g_1g'_1, \dots, g_ng'_n)(g''_1, \dots, g''_n) \\ &= [(g_1g'_1)g''_1, \dots, (g_ng'_n)g''_n] \\ &= [g_1(g'_1g''_1), \dots, g_n(g'_ng''_n)] \\ &= (g_1, \dots, g_n)(g'_1g''_1, \dots, g'_ng''_n) \\ &= (g_1, \dots, g_n)[(g'_1, \dots, g'_n)(g''_1, \dots, g''_n)], \end{aligned}$$

it follows that  $G_1 \oplus \cdots \oplus G_n$  is associative. Further, since

$$\begin{aligned} (e_1, \dots, e_n)(g_1, \dots, g_n) &= (e_1g_1, \dots, e_ng_n) \\ &= (g_1, \dots, g_n) \\ &= (g_1e_1, \dots, g_ne_n) \\ &= (g_1, \dots, g_n)(e_1, \dots, e_n), \end{aligned}$$

it follows that  $(e_1, \dots, e_n)$  is the identity element of  $G_1 \oplus \cdots \oplus G_n$ . Lastly, since

$$\begin{aligned} (g_1^{-1}, \dots, g_n^{-1})(g_1, \dots, g_n) &= (g_1^{-1}g_1, \dots, g_n^{-1}g_n) \\ &= (e_1, \dots, e_n) \\ &= (g_1g_1^{-1}, \dots, g_ng_n^{-1}) \\ &= (g_1, \dots, g_n)(g_1^{-1}, \dots, g_n^{-1}), \end{aligned}$$

it follows that  $(g_1^{-1}, \dots, g_n^{-1})$  is the reverse of  $(g_1, \dots, g_n)$ . Hence,  $G_1 \oplus \cdots \oplus G_n$  is a group.

**Example 8.1.** Consider  $U(8) = \{1, 3, 5, 7\}$ ,  $U(10) = \{1, 3, 7, 9\}$ . Then

$$\begin{aligned} U(8) \oplus U(10) = \{ & (1, 1), (1, 3), (1, 7), (1, 9), \\ & (3, 1), (3, 3), (3, 7), (3, 9), \\ & (5, 1), (5, 3), (5, 7), (5, 9), \\ & (7, 1), (7, 3), (7, 7), (7, 9) \}. \end{aligned}$$

The product  $(3, 7)(7, 9) = (3 \cdot 7 \bmod 8, 7 \cdot 9 \bmod 10) = (5, 3)$ .

**Example 8.2.** Consider  $\mathbb{Z}_2 = \{0, 1\}$  and  $\mathbb{Z}_3 = \{0, 1, 2\}$ . Then

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}.$$

Since

$$\begin{aligned} (0, 0)(0, 1) &= (0, 1) = (0, 1)(0, 0), \\ (0, 0)(0, 2) &= (0, 2) = (0, 2)(0, 0), \\ &\vdots \\ (1, 1)(1, 2) &= (0, 0) = (1, 2)(1, 1), \end{aligned}$$

it follows that  $\mathbb{Z}_2 \oplus \mathbb{Z}_3$  is an Abelian group of order 6. Since the operation in each component is addition,

$$\begin{aligned} (1, 1) &= (1, 1), \\ 2(1, 1) &= (0, 2), \\ 3(1, 1) &= (1, 0), \\ 4(1, 1) &= (0, 1), \\ 5(1, 1) &= (1, 2), \\ 6(1, 1) &= (0, 0). \end{aligned}$$

Hence  $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle (1, 1) \rangle$ . It follows that  $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_6$ .

**Example 8.3.** Let  $G$  be a group of order 4. By the Lagrange's Theorem,

$$|G| = 4, \langle a \rangle \leq G, a \in G \implies |\langle a \rangle| = |a| \mid |G| = 4.$$

So  $a \in G, a \in \{1, 2\}$ . Let  $a, b \in G, a \neq e, b \neq e, a \neq b$ . Then,  $ab \neq a, ab \neq b$ , and  $ab \neq e$ , otherwise  $a = b^{-1} = b$ . Thus  $G = \{e, a, b, ab\}$ . Since  $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ , the operation table is uniquely determined. Hence  $G \approx \mathbb{Z}_4$  or  $G \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

## 8.2 Properties of External Direct Products

**Theorem 8.1.**  $|(g_1, g_2, \dots, g_n)| = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$ .

*Proof.* Let  $s = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$  and  $t = |(g_1, g_2, \dots, g_n)|$ . Since  $s$  is a multiple of each  $|g_i|$ , by Theorem 4.1 (ii),

$$g_i^s = g_i^0 = e_i \iff |g_i| \mid (s - 0) = s.$$

It follows that

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

and  $t \leq s$ . On the other hand, since

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

by Theorem 4.1 (ii),

$$g_i^t = g_i^0 = e_i \iff |g_i| \mid (t - 0) = t.$$

So  $t$  is a common multiple of  $|g_1|, \dots, |g_n|$ . Since  $s = \text{lcm}(|g_1|, \dots, |g_n|)$ , it follows that  $s \leq t$ . Hence  $s = t$ .  $\square$

**Example 8.4.** Groups of order 100 include  $\mathbb{Z}_{100}, \mathbb{Z}_{25} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4, \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, D_{50}, D_{10} \oplus \mathbb{Z}_5, D_5 \oplus \mathbb{Z}_{10}, D_5 \oplus D_5$ .

**Example 8.5.** Find the number of elements of order 5 in  $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ .

By Theorem 8.1, the number of elements  $(a, b) \in \mathbb{Z}_{25} \oplus \mathbb{Z}_5$  of order 5 is the number of elements with the property

$$5 = |(a, b)| = \text{lcm}(|a|, |b|).$$

So either  $|a| = 5, |b| \in \{1, 5\}$  or  $|a| \in \{1, 5\}, |b| = 5$ .

**Case 1**  $|a| = 5, |b| \in \{1, 5\}$ , then since  $5, 10, 15, 20 \in \mathbb{Z}_{25}$  and

$$|5| = |10| = |15| = |20| = 5,$$

there are four choices for  $a$ . Since  $0, 1, 2, 3, 4 \in \mathbb{Z}_5$  and

$$\begin{aligned} |0| &= 1, \\ |1| &= |2| = |3| = |4| = 5, \end{aligned}$$

there are five choices for  $b$ . Hence there are  $4 \cdot 5 = 20$  elements of order 5. Namely,  $(5, 0), (5, 1), (5, 2), (5, 3), (5, 4), (10, 0), \dots, (20, 4)$ .

**Case 2**  $|a| = 1, |b| = 5$ , then there are one choice for  $a$  (namely,  $0 \in \mathbb{Z}_{25}$ ) and four choices for  $b$  (namely,  $\{1, 2, 3, 4\} \in \mathbb{Z}_5$ ). Hence there are  $1 \cdot 4 = 4$  elements of order 5. Namely,  $(0, 1), (0, 2), (0, 3), (0, 4)$ .

Hence there are  $20 + 4 = 24$  elements of order 5 in  $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ .

**Example 8.6.** Find the number of cyclic subgroups of order 10 in  $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$ .

By Theorem 8.1, this is the number of elements  $(a, b) \in \mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$  with the property

$$10 = |(a, b)| = \text{lcm}(|a|, |b|).$$

**Case 1**  $|a| = 10, |b| \in \{1, 5\}$ . By Theorem 4.4,

$$\mathbb{Z}_{100} = \langle 1 \rangle, |\mathbb{Z}_{100}| = 100, 10|100,$$

the number of elements  $a \in \mathbb{Z}_{100} : |a| = 10$  is  $\phi(10) = 4$ . Hence, there are four choices for  $a$ . Similarly,

$$\mathbb{Z}_{25} = \langle 1 \rangle, |\mathbb{Z}_{25}| = 25, 1|25, 5|25,$$

the number of elements  $b \in \mathbb{Z}_{25} : |b| = 1$  is  $\phi(1) = 1$  and  $|b| = 5$  is  $\phi(5) = 4$ . Hence there are  $1 + 4 = 5$  choices for  $b$ . So there are  $4 \cdot 5 = 20$  elements  $(a, b) \in \mathbb{Z}_{100} \oplus \mathbb{Z}_{25} : |(a, b)| = 10$ .

**Case 2**  $|a| = 2$  and  $|b| = 5$ . By Theorem 4.4,

$$\mathbb{Z}_{100} = \langle 1 \rangle, |\mathbb{Z}_{100}| = 100, 2|100,$$

the number of elements  $a \in \mathbb{Z}_{100} : |a| = 2$  is  $\phi(2) = 1$ . Similarly,

$$\mathbb{Z}_{25} = \langle 1 \rangle, |\mathbb{Z}_{25}| = 25, 5|25,$$

the number of elements  $b \in \mathbb{Z}_{25} : |b| = 5$  is  $\phi(5) = 4$ . Hence there are four choices for  $b$ . So there are  $1 \cdot 4 = 4$  elements  $(a, b) \in \mathbb{Z}_{100} \oplus \mathbb{Z}_{25} : |(a, b)| = 10$ .

Hence there are  $20 + 4 = 24$  elements  $(a, b) \in \mathbb{Z}_{100} \oplus \mathbb{Z}_{25} : |(a, b)| = 10$ . Since by Theorem 4.4,

$$|\langle (a, b) \rangle| = 10, 10|10,$$

there are  $\phi(10) = 4$  elements of order 10 in  $\langle (a, b) \rangle$ . Hence each cyclic subgroup of order 10 is generated by four elements of order 10. So there are totally  $24/4 = 6$  cyclic subgroups of order 10 in  $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$ .

**Theorem 8.2.** Let  $G, H$  be finite cyclic groups. Then

$$G \oplus H \text{ is cyclic} \iff \gcd(|G|, |H|) = 1.$$

*Proof.* Let  $G = \langle g \rangle, H = \langle h \rangle$ .

( $\Rightarrow$ ) Assume that  $G \oplus H$  is cyclic. So  $\exists (g, h) \in G \oplus H : G \oplus H = \langle (g, h) \rangle$ . Let  $|G| = m, |H| = n$ , so

$$|(g, h)| = |\langle (g, h) \rangle| = |G \oplus H| = mn.$$

Let  $\gcd(m, n) = d$ , since

$$(g, h)^{mn/d} = (g^{mn/d}, h^{mn/d}) = (g^m)^{n/d}, (h^n)^{m/d} = (e, e),$$

it follows that

$$|(g, h)| = mn \leq mn/d \implies d = 1.$$

Hence

$$\gcd(m, n) = d = 1 \implies |G| = m, |H| = n \text{ are relatively prime.}$$

( $\Leftarrow$ ) Assume that  $|G| = m, |H| = n$  are relatively prime. So  $\gcd(m, n) = 1$ . Then, by Theorem 8.1,

$$\begin{aligned} |\langle (g, h) \rangle| &= |(g, h)| = \text{lcm}(|g|, |h|) \\ &= \text{lcm}(|\langle g \rangle|, |\langle h \rangle|) \\ &= \text{lcm}(|G|, |H|) \\ &= mn \\ &= |G \oplus H|. \end{aligned}$$

Hence  $G \oplus H = \langle (g, h) \rangle$ . □

**Corollary 8.2.1.** *Let  $G_1, G_2, \dots, G_n$  be cyclic. Then  $G_1 \oplus G_2 \oplus \dots \oplus G_n$  is cyclic iff  $\gcd(|G_i|, |G_j|) = 1$  when  $i \neq j$ .*

**Corollary 8.2.2.** *Let  $m = n_1 n_2 \dots n_k$ . Then  $\mathbb{Z}_m \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_k}$  iff  $\gcd(n_i, n_j) = 1$  when  $i \neq j$ .*

### 8.3 The Group of Units Modulo $n$ as an External Direct Product

**Definition 8.2.** Let  $k \mid n$ . Then  $U_k(n) = \{x \in U(n) : x \bmod k = 1\}$ .

**Example 8.7.** Consider  $U_7(105) = \{1, 8, 22, 29, 43, 64, 71, 92\}$ .

Since  $U_k(n)$  is finite, and

$$1 \in U(n), 1 \bmod k = 1 \implies 1 \in U_k(n) \implies U_k(n) \neq \emptyset.$$

By Theorem 3.3, let  $a, b \in U_k(n)$ , so  $a, b \in U(n), ab \in U(n)$ . Then

$$a \bmod k = 1, b \bmod k = 1 \implies ab \bmod k = 1$$

and  $ab \in U_k(n)$ . Hence  $U_k(n) \leq U(n)$ .



**Theorem 8.3.** Let  $\gcd(s, t) = 1$ . Then

$$U(st) \approx U(s) \oplus U(t).$$

Moreover,

$$U_s(st) \approx U(t) \quad \text{and} \quad U_t(st) \approx U(s).$$

*Proof.* An isomorphism from  $U(st)$  to  $U(s) \oplus U(t)$  is  $x \rightarrow (x \bmod s, x \bmod t)$ . An isomorphism from  $U_s(st)$  to  $U(t)$  is  $x \rightarrow x \bmod t$ . An isomorphism from  $U_t(st)$  to  $U(s)$  is  $x \rightarrow x \bmod s$ .  $\square$

**Corollary 8.3.1.** Let  $m = n_1 n_2 \dots n_k$  and  $\gcd(n_i, n_j) = 1, i \neq j$ . Then,

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus \dots \oplus U(n_k).$$

## 9 Normal Subgroups and Factor Groups

### 9.1 Normal Subgroups

**Definition 9.1.** Let  $G$  be a group and  $H \leq G$ . Then  $H$  is a *normal* subgroup of  $G$  if  $\forall a \in G, aH = Ha$ . In symbols,

$$H \leq G, \forall a \in G, aH = Ha \implies H \triangleleft G.$$

If  $H \triangleleft G$ , then

$$\forall a \in G, h \in H, \exists h' \in H : ah = h'a.$$

Likewise,

$$\exists h'' \in H : ha = ah''.$$

It is possible that  $h' = h$  or  $h'' = h$ .

**Theorem 9.1** (Normal Subgroup Test). Let  $G$  be a group and  $H \leq G$ . Then

$$H \triangleleft G \iff \forall x \in G, xHx^{-1} \subseteq H.$$

*Proof.* Let  $G$  be a group and  $H \leq G$ .

( $\implies$ ) Assume that  $H \triangleleft G$ . So  $\forall a \in G, aH = Ha$ . Let  $x \in G$  be arbitrary and  $h \in H$ . Then

$$\exists h' \in H : xh = h'x \implies xhx^{-1} = h' \in H.$$

Hence  $\forall x \in G, xHx^{-1} \subseteq H$ .

( $\Leftarrow$ ) Assume that  $\forall x \in G, xHx^{-1} \subseteq H$ . Let  $x = a$ , then

$$aHa^{-1} \subseteq H \implies aH \subseteq Ha.$$

Let  $x = a^{-1}$ , then

$$a^{-1}H(a^{-1})^{-1} = a^{-1}Ha \subseteq H \implies Ha \subseteq aH.$$

Hence  $\forall x \in G, aH = Ha$  and  $H \triangleleft G$ .  $\square$

**Example 9.1.** Every subgroup of an Abelian group is normal. In this case,  $\forall a \in G, h \in H, ah = ha$ .

**Example 9.2.** The center  $Z(G) = \{a \in G : \forall x \in G, ax = xa\}$  is always normal. In this case,  $\forall a \in G, h \in Z(G), ah = ha$ .

**Example 9.3.** The alternating group  $A_n$  of even permutations is a normal subgroup of  $S_n$ . Note, for example, that for  $(1) \in S_n, (123) \in A_n, (12)(123) \neq (123)(12)$  but  $(12)(123) = (132)(12), (132) \in A_n$ .

**Example 9.4.** The subgroup of rotations in  $D_n$  is normal in  $D_n$ . For any rotation  $r$  and any reflection  $f$ ,  $fr = r^{-1}f$ , whereas for any rotations  $r, r', rr' = r'r$ .

**Example 9.5.** Let  $H \triangleleft G, K \leq G$ . Then  $HK = \{hk : h \in H, k \in K\} \leq G$ . First,  $e = ee \in HK$  and  $HK \neq \emptyset$ . Next, let  $a = h_1k_1, b = h_2k_2, h_1, h_2 \in H, k_1, k_2 \in K$  be arbitrary. Then

$$\begin{aligned} ab^{-1} &= (h_1k_1)(h_2k_2)^{-1} \\ &= h_1k_1k_2^{-1}h_2^{-1} \\ &= h_1(k_1k_2^{-1})h_2^{-1}. \end{aligned}$$

Since  $H \triangleleft G, h_2^{-1} \in H$ , and  $k_1k_2^{-1} \in K \subseteq G$ , it follows that

$$\exists h' \in H : (k_1k_2^{-1})h_2^{-1} = h'(k_1k_2^{-1})$$

and hence

$$ab^{-1} = h_1(k_1k_2^{-1})h_2^{-1} = h_1h'(k_1k_2^{-1}) \in HK.$$

Hence by Theorem 3.1,  $HK \leq G$ .

**Example 9.6.** The group  $SL(2, \mathbb{R})$  of  $2 \times 2$  matrices with determinant 1 is a normal subgroup of  $GL(2, \mathbb{R})$ , the group of  $2 \times 2$  matrices with nonzero determinant. To verify, by Theorem 9.1, let  $x \in GL(2, \mathbb{R}), h \in SL(2, \mathbb{R}) = H$ . Note that

$$(\det x)(\det h)(\det x)^{-1} = (\det x)(\det x)^{-1} = 1,$$

hence

$$xhx^{-1} \in H \implies xHx^{-1} \subseteq H.$$

**Example 9.7.** By Figure 5.5 for  $A_4$ ,  $H = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \triangleleft A_4$ , whereas  $K = \{\alpha_1, \alpha_5, \alpha_9\}$  is not a normal subgroup of  $A_4$ . To verify, let  $\beta \in A_4$ ,  $|\beta H \beta^{-1}| = 4$  and  $H$  is the only subgroup of  $A_4$  of order 4 since all other elements of  $A_4$  have order 3. Hence  $\beta H \beta^{-1} = H$ . In contrast,  $\alpha_2 \alpha_5 \alpha_2^{-1} = \alpha_7 \notin K$ , so  $\alpha_2 K \alpha_2^{-1} \not\subseteq K$ .

## 9.2 Factor Groups

**Theorem 9.2.** Let  $G$  be a group and  $H \triangleleft G$ . Then the set  $G/H = \{aH : a \in G\}$  is a group under the operation  $(aH)(bH) = abH$ . In this case,  $G/H$  is a factor group.

*Proof.* Let  $G$  be a group and  $H \triangleleft G$ . Consider the set  $G/H = \{aH : a \in G\}$  under the operation  $(aH)(bH) = abH$ .

First, let  $aH, bH \in G/H$  be arbitrary. Then  $(aH)(bH) = abH$ . Since  $a, b \in G$ ,  $ab \in G$ , it follows that  $abH \in G/H$  and  $G/H$  is closed under the operation. Second, let  $aH, bH, cH \in G/H$ , then

$$\begin{aligned} (aH)[(bH)(cH)] &= (aH)(bcH) = abcH, \\ [(aH)(bH)](cH) &= (abH)(cH) = abcH. \end{aligned}$$

Hence the operation is associative. Third, since  $e \in G \implies eH \in G/H$ , let  $aH \in G/H$  be arbitrary, then

$$(aH)(eH) = aeH = aH = eaH = (eH)(aH).$$

Hence  $eH \in G/H$  is the identity element. Finally, let  $a \in G$  be arbitrary, then since  $a^{-1} \in G$ , it follows that  $a^{-1}H \in G/H$  and

$$(aH)(a^{-1}H) = aa^{-1}H = eH = a^{-1}aH = (a^{-1}H)(aH).$$

Hence  $a^{-1}H$  is the reverse element of  $aH$ . Therefore,  $G/H$  is a group under the operation.  $\square$

**Example 9.8.** Let  $4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, \dots\}$ . Consider the four left cosets,

$$\begin{aligned} 0 + 4\mathbb{Z} &= \{\dots, -8, -4, 0, 4, 8, \dots\}, \\ 1 + 4\mathbb{Z} &= \{\dots, -7, -3, 1, 5, 9, \dots\}, \\ 2 + 4\mathbb{Z} &= \{\dots, -6, -2, 2, 6, 10, \dots\}, \\ 3 + 4\mathbb{Z} &= \{\dots, -5, -1, 3, 7, 11, \dots\}. \end{aligned}$$

These are the only left cosets of  $4\mathbb{Z}$ . Since if  $k \in \mathbb{Z}$ , then  $k = 4q + r$ ,  $0 \leq r < 4$ . Hence

$$k + 4\mathbb{Z} = r + 4q + 4\mathbb{Z} = r + 4\mathbb{Z}.$$

Figure 9.1 shows the Cayley table of  $\mathbb{Z}/4\mathbb{Z}$ . Hence,  $\mathbb{Z}/4\mathbb{Z} \approx \mathbb{Z}_4$ . More generally, for any  $n > 0$ , let  $n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$ , then  $\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}_n$ .

	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$
$0 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$
$1 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$
$2 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$
$3 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$

Figure 9.1: The Cayley table of  $\mathbb{Z}/4\mathbb{Z}$ .

**Example 9.9.** Let  $G = \mathbb{Z}_{18}$  and  $H = \langle 6 \rangle = \{6, 12, 0\}$ . Then since

$$\begin{aligned}
0 + H &= H = 6 + H = 12 + H, \\
1 + H &= \{1, 7, 13\} = 7 + H = 13 + H, \\
2 + H &= \{2, 8, 14\} = 8 + H = 14 + H, \\
3 + H &= \{3, 9, 15\} = 9 + H = 15 + H, \\
4 + H &= \{4, 10, 16\} = 10 + H = 16 + H, \\
5 + H &= \{5, 11, 17\} = 11 + H = 17 + H,
\end{aligned}$$

it follows that  $G/H = \{0 + H, 1 + H, 2 + H, 3 + H, 4 + H, 5 + H\}$ . Consider  $(5 + H) + (4 + H)$ ,

$$\begin{aligned}
(5 + H) + (4 + H) &= 5 + 4 + H \\
&= 9 + H \\
&= 3 + 6 + H \\
&= 3 + \{6, 12, 0\} \\
&= 3 + H.
\end{aligned}$$

**Example 9.10.** Let  $\mathfrak{K} = \{R_0, R_{180}\}$ , and consider the factor group of  $D_4$

$$D_4/\mathfrak{K} = \{\mathfrak{K}, R_{90}\mathfrak{K}, H\mathfrak{K}, D\mathfrak{K}\}.$$

Figure 9.2 shows the Cayley table for  $D_4/\mathfrak{K}$ .

$D_4/\mathfrak{K}$  provides a good opportunity to demonstrate how a factor group of  $G$  is related to  $G$  itself. Arrange the heading of the Cayley table for  $D_4$  in such a way that elements from the same coset of  $\mathfrak{K}$  are in adjacent columns as shown in Figure 9.3. Then, the multiplication table for  $D_4$  can be blocked off into boxes that are cosets of  $\mathfrak{K}$ , and the substitution that replaces a box containing the element  $x$  with the coset  $x\mathfrak{K}$  yields the Cayley table for  $D_4/\mathfrak{K}$ .

For example, when one passes from  $D_4$  to  $D_4/\mathfrak{K}$ , the box shown in Figure 9.4 in Figure 9.3 becomes the element  $H\mathfrak{K}$  in Figure 9.2. Similarly, the box shown in Figure 9.5 becomes the element  $D\mathfrak{K}$ , and so on.

In this way, one can see that the formation of a factor group  $G/H$  causes a systematic collapse of the elements of  $G$ . In particular, all the elements in the coset of  $H$  containing  $a$  collapse to the single group element  $aH$  in  $G/H$ .

	$\mathcal{H}$	$R_{90}\mathcal{H}$	$H\mathcal{H}$	$D\mathcal{H}$
$\mathcal{H}$	$\mathcal{H}$	$R_{90}\mathcal{H}$	$H\mathcal{H}$	$D\mathcal{H}$
$R_{90}\mathcal{H}$	$R_{90}\mathcal{H}$	$\mathcal{H}$	$D\mathcal{H}$	$H\mathcal{H}$
$H\mathcal{H}$	$H\mathcal{H}$	$D\mathcal{H}$	$\mathcal{H}$	$R_{90}\mathcal{H}$
$D\mathcal{H}$	$D\mathcal{H}$	$H\mathcal{H}$	$R_{90}\mathcal{H}$	$\mathcal{H}$

Figure 9.2

	$R_0$	$R_{180}$	$R_{90}$	$R_{270}$	$H$	$V$	$D$	$D'$
$R_0$	$R_0$	$R_{180}$	$R_{90}$	$R_{270}$	$H$	$V$	$D$	$D'$
$R_{180}$	$R_{180}$	$R_0$	$R_{270}$	$R_{90}$	$V$	$H$	$D'$	$D$
$R_{90}$	$R_{90}$	$R_{270}$	$R_{180}$	$R_0$	$D'$	$D$	$H$	$V$
$R_{270}$	$R_{270}$	$R_{90}$	$R_0$	$R_{180}$	$D$	$D'$	$V$	$H$
$H$	$H$	$V$	$D$	$D'$	$R_0$	$R_{180}$	$R_{90}$	$R_{270}$
$V$	$V$	$H$	$D'$	$D$	$R_{180}$	$R_0$	$R_{270}$	$R_{90}$
$D$	$D$	$D'$	$V$	$H$	$R_{270}$	$R_{90}$	$R_0$	$R_{180}$
$D'$	$D'$	$D$	$H$	$V$	$R_{90}$	$R_{270}$	$R_{180}$	$R_0$

Figure 9.3

$H$	$V$
$V$	$H$

Figure 9.4

$D$	$D'$
$D'$	$D$

Figure 9.5

**Example 9.11.** Let

$$G = U(32) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$$

and  $H = U_{16}(32) = \{1, 17\}$ . Since

$$\begin{aligned} 1H1^{-1} &= 1H1 = H \subseteq H \\ 3H3^{-1} &= 3H11 = \{3, 51\}11 = \{3, 19\}11 = \{33, 209\} = \{1, 17\} = H \subseteq H, \\ 5H5^{-1} &= 5H13 = \{5, 85\}13 = \{5, 21\}13 = \{65, 273\} = \{1, 17\} = H \subseteq H, \\ &\vdots \\ 31H31^{-1} &= 31H31 = \{31, 527\}31 = \{31, 15\}31 = \{961, 465\} = \{1, 17\} = H \subseteq H, \end{aligned}$$

hence by Theorem 9.1,  $H \triangleleft G$ . Since

$$\begin{aligned} 1H &= \{1, 17\}, \\ 3H &= \{3, 51\} = \{3, 19\}, \\ 5H &= \{5, 85\} = \{5, 21\}, \\ 7H &= \{7, 119\} = \{7, 23\}, \\ 9H &= \{9, 25\}, \\ 11H &= \{11, 27\}, \\ 13H &= \{13, 29\}, \\ 15H &= \{15, 31\}, \\ 17H &= \{17, 1\} = 1H, \\ &\vdots \\ 31H &= \{31, 15\} = 15H, \end{aligned}$$

it follows that  $G/H = \{1H, 3H, 5H, 7H, 9H, 11H, 13H, 15H\}$  with the operation  $(aH)(bH) = abH$  is a factor group and  $|G/H| = |G|/|H| = 16/2 = 8$ . Since

$$(1H)(kH) = kH = (kH)(1H), k \in \{1, 3, 5, \dots, 15\},$$

$(1H) \in G/H$  is the identity. Since

$$\begin{aligned} (3H)(5H) &= 15H = (5H)(3H), \\ (3H)(7H) &= 21H = \{21, 357\} = \{21, 5\} = 5H = (7H)(3H), \\ (7H)(9H) &= 63H = \{63, 1071\} = \{31, 15\} = 15H = (9H)(7H), \\ &\vdots \\ (aH)(bH) &= (bH)(aH) \in G/H, a, b \in \{1, 3, 5, \dots, 15\}, \end{aligned}$$

it follows that  $G/H$  is Abelian.

There are three possible Abelian groups of order 8, namely,

$$\begin{aligned}\mathbb{Z}_8 &= \{0, 1, \dots, 7\}, \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 &= \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1)\}, \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 &= \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), \\ &\quad (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}.\end{aligned}$$

Since

$$(3H)^4 = 81H = 1H \implies |3H| = 4,$$

it follows that  $G/H$  is not isomorphic to  $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$  since

$$\neg \exists a \in \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 : |a| = 4.$$

Since  $\mathbb{Z}_8 = \langle 3 \rangle$  and  $|\mathbb{Z}_8| = 8$ , by Theorem 4.4,

$$2 \mid 8, 2 \in \mathbb{N} \implies \text{number of } a \in \mathbb{Z}_8 : |a| = 2 \text{ is } \phi(2) = 1.$$

Since  $|7H| = 2$  and  $|9H| = 2$ , there is more than an element of order 2 and  $G/H$  is not isomorphic to  $\mathbb{Z}_8$ . Hence  $U(32)/U_{16}(32) \approx \mathbb{Z}_4 \oplus \mathbb{Z}_2$ , which is also isomorphic to  $U(16)$ .

**Example 9.12.** Let  $G = \mathbb{Z}_8 \oplus \mathbb{Z}_4 = \{(0, 0), (0, 1), (0, 2), (0, 3), \dots, (7, 2), (7, 3)\}$  and  $H = \langle (2, 2) \rangle$ . Since

$$\begin{array}{ll} 1(2, 2) = (2, 2), & 0(2, 2) = (0, 0) \\ 2(2, 2) = (4, 4) = (4, 0), & -1(2, 2) = (-2, -2) = (6, 2), \\ 3(2, 2) = (6, 6) = (6, 2), & -2(2, 2) = (-4, -4) = (4, 0), \\ 4(2, 2) = (8, 8) = (0, 0), & -3(2, 2) = (-6, -6) = (2, 2) \\ 5(2, 2) = (10, 10) = (2, 2), & -4(2, 2) = (-8, -8) = (0, 0), \\ \vdots & \vdots \end{array}$$

it follows that  $H = \langle (2, 2) \rangle = \{(2, 2), (4, 0), (6, 2), (0, 0)\}$ . Since

$$\begin{aligned}(0, 0)H(0, 0)^{-1} &= (0, 0)H(0, 0) = H \subseteq H, \\ (0, 1)H(0, 1)^{-1} &= (0, 1)H(0, 3) \\ &= \{(2, 3), (4, 1), (6, 3), (0, 1)\}(0, 3) \\ &= \{(2, 6), (4, 4), (6, 6), (0, 4)\} \\ &= \{(2, 2), (4, 0), (6, 2), (0, 0)\} = H \subseteq H, \\ &\vdots \\ (7, 3)H(7, 3)^{-1} &= (7, 3)H(1, 1) \\ &= \{(9, 5), (11, 3), (13, 5), (7, 3)\}(1, 1) \\ &= \{(1, 1), (3, 3), (5, 1), (7, 3)\}(1, 1) \\ &= \{(2, 2), (4, 4), (6, 2), (8, 4)\} \\ &= \{(2, 2), (4, 0), (6, 2), (0, 0)\} = H \subseteq H,\end{aligned}$$

by Theorem 9.1,  $H \triangleleft G$ . Hence  $G/H$  with the operation  $(aH)(bH) = abH$  is a factor group. Since

$$\begin{aligned}
(0,0)H &= \{(2,2), (4,0), (6,2), (0,0)\}, \\
(0,1)H &= \{(2,3), (4,1), (6,3), (0,1)\}, \\
(0,2)H &= \{(2,4), (4,2), (6,4), (0,2)\} = \{(2,0), (4,2), (6,0), (0,2)\}, \\
(0,3)H &= \{(2,5), (4,3), (6,5), (0,3)\} = \{(2,1), (4,3), (6,1), (0,3)\}, \\
(1,0)H &= \{(3,2), (5,0), (7,2), (1,0)\}, \\
(1,1)H &= \{(3,3), (5,1), (7,3), (1,1)\}, \\
(1,2)H &= \{(3,4), (5,2), (7,4), (2,2)\} = \{(3,0), (5,2), (7,0), (2,2)\}, \\
(1,3)H &= \{(3,5), (5,3), (7,5), (2,3)\} = \{(3,5), (5,3), (7,1), (2,3)\}, \\
(2,0)H &= \{(4,2), (6,0), (8,2), (2,0)\} = \{(4,2), (6,0), (0,2), (2,0)\} = (0,2)H, \\
(2,1)H &= \{(4,3), (6,1), (8,3), (2,1)\} = \{(4,3), (6,1), (0,3), (2,1)\} = (0,3)H, \\
&\vdots
\end{aligned}$$

it follows that

$$G/H = \{(0,0)H, (0,1)H, (0,2)H, (0,3)H, (1,0)H, (1,1)H, (1,2)H, (1,3)H\}$$

and  $|G/H| = 8$ . Hence  $G/H$  is isomorphic to one of  $\mathbb{Z}_8, \mathbb{Z}_4 \oplus \mathbb{Z}_2$  and  $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ . Since for any  $(a,b)H$ ,

$$((a,b)H)^4 = ((a,b)^4H) = ((4a, 4b)H) = \begin{cases} (4,0)H & , a \text{ is odd} \\ (0,0)H & , a \text{ is even} \end{cases}$$

and  $(0,0), (4,0) \in H$ , it follows that

$$((a,b)H)^4 = ((a,b)^4H) = ((4a, 4b)H) = H.$$

Hence  $\forall (a,b)H \in G/H, |(a,b)H| \leq 4$ . Since

$$((1,0)H)^2 = ((1,0)^2H) = (2,0)H \neq H,$$

it follows that  $|(1,0)H| = 4$ . Hence  $G/H$  is not isomorphic to  $\mathbb{Z}_8$  and  $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

### 9.3 Applications of Factor Groups

**Theorem 9.3.** *Let  $G$  be a group and let  $Z(G)$  be the center of  $G$ . Then*

$$G/Z(G) \text{ is cyclic} \implies G \text{ is Abelian.}$$

*Proof.* Let  $G$  be a group and let  $Z(G)$  be the center of  $G$ . Assume that  $G/Z(G)$  is cyclic. Since

$$Z(G) = \{a \in G : \forall x \in G, ax = xa\},$$



the factor group

$$G/Z(G) = \{gZ(G) : g \in G\}.$$

Since  $G/Z(G)$  is cyclic,

$$\exists gZ(G) \in G/Z(G) : G/Z(G) = \langle gZ(G) \rangle.$$

Let  $kZ(G) \in G/Z(G)$  arbitrary, then

$$\exists i \in \mathbb{Z} : (gZ(G))^i = kZ(G).$$

But

$$(gZ(G))^i = g^i Z(G) = kZ(G).$$

Since

$$Z(G) \leq G \implies e \in Z(G),$$

it follows that

$$k = ke = g^i a, a \in Z(G).$$

Let

$$C(g) = \{x \in G : xg = gx\}$$

be the center of  $g$ . Then since

$$\begin{aligned} g^i \in G, g^i g &= gg^i \implies g^i \in C(g), \\ a \in Z(G) \subseteq G, ag &= ga \implies a \in C(g), \end{aligned}$$

it follows that  $k = g^i a \in C(g)$ . Since  $k$  is arbitrary,

$$\forall k \in G, kg = gk.$$

Hence  $g \in Z(G)$  and by Lemma 7.1,

$$gZ(G) = Z(G) \implies G/Z(G) = \{gZ(G) = Z(G) : g \in G\} = \{Z(G)\}.$$

Hence  $g \in Z(G), \forall g \in G, gx = xg$ . □

**Theorem 9.4.** *Let  $G$  be a group. Then  $G/Z(G) \approx \text{Inn}(G)$ .*

*Proof.* Let  $G$  be a group. Let

$$G/Z(G) = \{gZ(G) : g \in G\}$$

and

$$\text{Inn}(G) = \{\phi_g(x) = gxg^{-1} : \forall x \in G, g \in G\}.$$

Let  $T(gZ(G)) = \phi_g(x)$ . First, let  $gZ(G), hZ(G) \in G/Z(G)$  be arbitrary. Assume that  $gZ(G) = hZ(G)$ . By Lemma 7.1 (vi),

$$gZ(G) = hZ(G) \iff h^{-1}g \in Z(G).$$

It follows that  $\forall x \in G, h^{-1}gx = xh^{-1}g$ . So

$$\begin{aligned} h^{-1}gx &= xh^{-1}g, \\ gxg^{-1} &= h x h^{-1}, \\ \phi_g(x) &= \phi_h(x). \end{aligned}$$

Hence  $T : gZ(G) \rightarrow \phi_g(x)$  is a function. Second, let assume that  $T(gZ(G)) = T(hZ(G))$ . Then

$$\begin{aligned} T(gZ(G)) &= T(hZ(G)), \\ \phi_g(x) &= \phi_h(x), \\ gxg^{-1} &= h x h^{-1}, \\ h^{-1}gx &= xh^{-1}g, \end{aligned}$$

it follows that  $h^{-1}g \in Z(G)$ . By Lemma 7.1 (vi),

$$gZ(G) = hZ(G) \iff h^{-1}g \in Z(G).$$

Hence  $T$  is one-to-one. Next, let  $\phi_g(x) \in Inn(G)$  be arbitrary. Since  $T$  is one-to-one, there exists an inverse function  $T^{-1}$  s.t.

$$\begin{aligned} T(gZ(G)) &= \phi_g(x), \\ gZ(G) &= T^{-1}(\phi_g(x)), \end{aligned}$$

it follows that

$$\exists gZ(G) \in G/Z(G) : T(gZ(G)) = T(T^{-1}(\phi_g(x))) = \phi_g(x).$$

Hence  $T$  is onto. Finally,

$$\begin{aligned} T(gZ(G)hZ(G)) &= T(ghZ(G)) \\ &= \phi_{gh}(x) \\ &= ghx(gh)^{-1} \\ &= ghxh^{-1}g \end{aligned}$$

and

$$\begin{aligned} T(gZ(G))T(hZ(G)) &= \phi_g\phi_h(x) \\ &= \phi_g(hxh^{-1}) \\ &= ghxh^{-1}g. \end{aligned}$$

Hence  $T$  conserves the operation. It follows that  $G/Z(G) \approx Inn(G)$ .  $\square$

**Example 9.13.**

**Theorem 9.5** (Cauchy's Theorem for Abelian Groups). *Let  $G$  be a finite Abelian group and let  $p$  be a prime,  $p \mid |G|$ . Then*

$$\exists g \in G : |g| = p.$$

*Proof.* Let  $G$  be a finite Abelian group and let  $p$  be a prime,  $p \mid |G|$ . If  $|G| = 2$ , then let  $p = 2$  and  $\exists g \in G : |g| = 2$ . Hence Theorem 9.5 is true.

If  $|G| \neq 2$ . By the Second Principle of Mathematical Induction, assume that Theorem 9.5 is true for all Abelian groups with orders less than  $|G|$ . Let  $x \in G$ ,  $|x| = m = qn$ ,  $q$  is prime, then  $|x^n| = q$ . Hence

$$\exists x^n \in G : |x^n| = q.$$

If  $q = p$ , then Theorem 9.5 is true. If  $q \neq p$ , since  $G$  is Abelian,

$$\langle x \rangle \leq G \implies \langle x \rangle \triangleleft G.$$

Hence

$$\overline{G} = G/\langle x \rangle = \{g\langle x \rangle : g \in G\}$$

with the operation  $(g\langle x \rangle)(h\langle x \rangle) = gh\langle x \rangle$  is a factor group. Since  $G$  is Abelian,  $g, h \in G$ ,  $gh = hg$ . It follows that

$$\begin{aligned} g\langle x \rangle, h\langle x \rangle \in \overline{G}, (g\langle x \rangle)(h\langle x \rangle) &= gh\langle x \rangle \\ &= hg\langle x \rangle \\ &= (h\langle x \rangle)(g\langle x \rangle). \end{aligned}$$

Hence  $\overline{G}$  is Abelian. Since

$$|\overline{G}| = |G/\langle x \rangle| = |G|/|\langle x \rangle| = |G|/q,$$

it follows that  $|\overline{G}| < |G|$ . Hence Theorem 9.5 is true for  $|\overline{G}|$ . So  $p \mid |\overline{G}|$  and

$$\exists y\langle x \rangle \in \overline{G} : |y\langle x \rangle| = p.$$

Since  $\langle x \rangle$  is the identity element of  $|\overline{G}|$ , it follows that  $(y\langle x \rangle)^p = y^p\langle x \rangle = \langle x \rangle$ . Hence  $y^p \in \langle x \rangle$ . If  $y^p = e$ , then Theorem 9.5 is true. If  $y^p \neq e$ , then  $|y^p| = q$  and  $|y^q| = p$ .  $\square$

**9.4 Internal Direct Products**

**Definition 9.2.** Let  $H, K \triangleleft G$ . If

$$G = HK = \{hk : h \in H, k \in K\}, \quad \text{and} \quad H \cap K = \{e\},$$

then  $G = H \times K$  is the *internal direct product* of  $H, K$ .

Figure 9.6 and 9.7 show the internal direct product and external direct product.

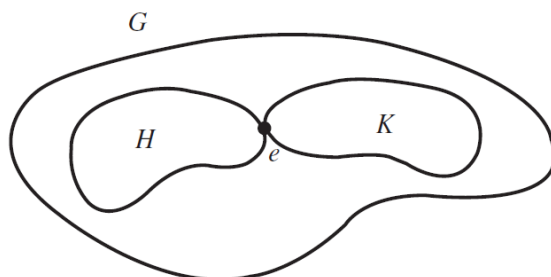


Figure 9.6: For the internal direct product,  $H, K$  must be subgroups of the same group.

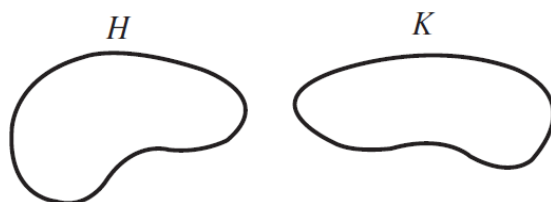


Figure 9.7: For the external direct product,  $H, K$  can be any groups.

**Example 9.14.** If  $s, t$  are relatively prime positive integers then  $U(st) = U_s(st) \times U_t(st)$ .

**Example 9.15.** In  $D_6$  let  $F \in D_6$  be some reflection and let  $R_k \in D_6$  be a rotation of  $k$  degrees. Then,

$$D_6 = \{R_0, R_{120}, R_{240}, F, R_{120}F, R_{240}F\} \times \{R_0, R_{180}\}.$$

**Definition 9.3.** Let  $H_1, H_2, \dots, H_n \triangleleft G$ . Then  $G$  is the *internal direct product* of  $H_1, H_2, \dots, H_n$ , denoted  $G = H_1 \times H_2 \times \dots \times H_n$ , if

1.  $G = H_1 H_2 \dots H_n = \{h_1 h_2 \dots h_n : h_i \in H_i\}$ ,
2.  $(H_1 H_2 \dots H_i) \cap H_{i+1} = \{e\}, i = 1, 2, \dots, n-1$ .

**Theorem 9.6.** Let  $G$  be a group. Then

$$G = H_1 \times H_2 \times \dots \times H_n \implies G \approx H_1 \oplus H_2 \oplus \dots \oplus H_n.$$

*Proof.* Let  $G$  be a group and assume that  $G = H_1 \times H_2 \times \cdots \times H_n$ . So  $H_1, H_2, \dots, H_n \triangleleft G$ ,

$$G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n : h_i \in H_i\},$$

and

$$(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\}, i = 1, 2, \dots, n-1.$$

Let  $h_i \in H_i, h_j \in H_j, i \neq j$ , then by Theorem 9.1,

$$H \triangleleft G \iff \forall x \in G, x H x^{-1} \subseteq H.$$

So

$$h_j h_i h_j^{-1} \in h_j H_i h_j^{-1} \subseteq H_i$$

and

$$h_i h_j h_i^{-1} \in h_i H_j h_i^{-1} \subseteq H_j.$$

It follows that

$$(h_i h_j h_i^{-1}) h_j^{-1} \in H_j h_j^{-1} = H_j$$

and

$$h_i (h_j h_i^{-1} h_j^{-1}) \in h_i H_i = H_i.$$

Hence,

$$h_i h_j h_i^{-1} h_j^{-1} \in H_i \cap H_j = \{e\} \implies h_i h_j h_i^{-1} h_j^{-1} = e \implies h_i h_j = h_j h_i.$$

Next, let  $g \in G$ ,

$$g = h_1 h_2 \cdots h_n \quad \text{and} \quad g = h'_1 h'_2 \cdots h'_n$$

where  $h_i, h'_i \in H_i, i = 1, \dots, n$ . Then, since  $h_i h_j = h_j h_i$ , it follows that

$$\begin{aligned} g &= g, \\ h_1 h_2 \cdots h_n &= h'_1 h'_2 \cdots h'_n, \\ h'_n h_n^{-1} &= (h'_1)^{-1} h_1 (h'_2)^{-1} h_2 \cdots (h'_{n-1})^{-1} h_{n-1}. \end{aligned}$$

Therefore

$$h'_n h_n^{-1} \in (H_1 H_2 \cdots H_{n-1}) \cap H_n = \{e\},$$

it follows that

$$h'_n h_n^{-1} = e \implies h'_n = h_n.$$

So

$$\begin{aligned} h_1 h_2 \cdots h_n &= h'_1 h'_2 \cdots h'_n, \\ h_1 h_2 \cdots h_{n-1} &= h'_1 h'_2 \cdots h'_n h_n^{-1}, \\ h_1 h_2 \cdots h_{n-1} &= h'_1 h'_2 \cdots h'_{n-1} e, \\ h_1 h_2 \cdots h_{n-1} &= h'_1 h'_2 \cdots h'_{n-1}. \end{aligned}$$

Repeating the steps,

$$h'_{n-1}h_{n-1}^{-1} = e \implies h'_{n-1} = h_{n-1}.$$

Continuing the process, eventually

$$h'_i = h_i, i = 1, \dots, n.$$

Define  $\phi : G \rightarrow H_1 \oplus H_2 \oplus \dots \oplus H_n$  by  $\phi(h_1h_2 \dots h_n) = (h_1, h_2, \dots, h_n)$ . First, assume that  $h_1h_2 \dots h_n, h'_1h'_2 \dots h'_n \in G, h_1h_2 \dots h_n = h'_1h'_2 \dots h'_n$ . Then

$$\begin{aligned} \phi(h_1h_2 \dots h_n) &= (h_1, h_2, \dots, h_n) \\ &= (h'_1, h'_2, \dots, h'_n) \\ &= \phi(h'_1h'_2 \dots h'_n). \end{aligned}$$

So  $\phi$  is a well-defined function. Second, assume that  $\phi(h_1h_2 \dots h_n) = \phi(h'_1h'_2 \dots h'_n)$ . Then since  $h'_i = h_i, i = 1, \dots, n$ , it follows that

$$h_1h_2 \dots h_n = h'_1h'_2 \dots h'_n.$$

Hence  $\phi$  is one-to-one. Third, let  $(h_1, h_2, \dots, h_n) \in H_1 \oplus \dots \oplus H_n$  be arbitrary. Since

$$\begin{aligned} \phi(h_1 \dots h_n) &= (h_1, \dots, h_n), \\ h_1 \dots h_n &= \phi^{-1}((h_1, \dots, h_n)). \end{aligned}$$

Let  $h_1 \dots h_n = \phi^{-1}((h_1, \dots, h_n))$ , it follows that

$$\phi(h_1 \dots h_n) = \phi(\phi^{-1}((h_1, \dots, h_n))) = (h_1, \dots, h_n).$$

Hence  $\phi$  is onto. Finally,

$$\begin{aligned} \phi((h_1 \dots h_n)(h'_1 \dots h'_n)) &= \phi(h_1h'_1 \dots h_nh'_n) \\ &= (h_1h'_1, \dots, h_nh'_n) \\ &= (h_1, \dots, h_n)(h'_1, \dots, h'_n) \\ &= \phi(h_1 \dots h_n)\phi(h'_1 \dots h'_n). \end{aligned}$$

Hence  $\phi$  preserves the operation. Therefore,  $G \approx H_1 \oplus \dots \oplus H_n$ . □

**Theorem 9.7.** *Let  $G$  be a group and  $p$  a prime. Then*

$$|G| = p^2 \implies G \approx \mathbb{Z}_{p^2} \quad \text{or} \quad G \approx \mathbb{Z}_p \oplus \mathbb{Z}_p.$$

*Proof.* □

**Corollary 9.7.1.** *Let  $G$  be a group and  $p$  a prime. Then*

$$|G| = p^2 \implies \forall a, b \in G, ab = ba.$$

## 10 Group Homomorphisms

**Definition 10.1.** A *homomorphism*  $\phi : G \rightarrow \overline{G}$  is a mapping that preserves the group operation; that is,  $\forall a, b \in G, \phi(ab) = \phi(a)\phi(b)$ .

**Definition 10.2.** The *kernel* of a homomorphism  $\phi$  from a group  $G$  to a group with identity  $e$  is the set  $\{x \in G : \phi(x) = e\}$ , denoted by  $\text{Ker } \phi$ . Moreover,  $\text{Ker } \phi \triangleleft G$ .

**Example 10.1.** Any isomorphism is a homomorphism that is also one-to-one and onto. The kernel of an isomorphism is the trivial subgroup.

**Example 10.2.** Let  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$  under multiplication.. Then the determinant mapping  $A \rightarrow \det A$  is a homomorphism from  $GL(2, \mathbb{R})$  to  $\mathbb{R}^*$ . The kernel of the determinant mapping is  $SL(2, \mathbb{R})$ .

**Example 10.3.** The mapping  $\phi : \mathbb{R}^* \rightarrow \mathbb{R}^*, \phi(x) = |x|$  is a homomorphism with  $\text{Ker } \phi = \{-1, 1\}$ .

**Example 10.4.** Let  $\mathbb{R}[x]$  be the group of all polynomials with real coefficients under addition. For  $f \in \mathbb{R}[x]$ , let  $f'$  be the derivative of  $f$ . Then  $\phi(f) = f'$  is a homomorphism  $\phi : \mathbb{R}[x] \rightarrow \mathbb{R}[x]$ .  $\text{Ker } \phi$  is the set of all constant polynomials.

**Example 10.5.** The mapping  $\mathbb{Z} \rightarrow \mathbb{Z}_n, \phi(m) = m \bmod n$ , is a homomorphism and  $\text{Ker } \phi = \langle n \rangle$ .

**Example 10.6.** The mapping  $\phi : \mathbb{R}^* \rightarrow \mathbb{R}^*, \phi(x) = x^2$ , under multiplication is a homomorphism, since  $a, b \in \mathbb{R}^*, \phi(ab) = (ab)^2 = a^2b^2 = \phi(a)\phi(b)$ .  $\text{Ker } \phi = \{-1, 1\}$ .

**Example 10.7.** The mapping  $\phi : \mathbb{R} \rightarrow \mathbb{R}, \phi(x) = x^2$  under addition is not a homomorphism, since  $a, b \in \mathbb{R}, \phi(a + b) = (a + b)^2 = a^2 + 2ab + b^2 \neq a^2 + b^2 = \phi(a) + \phi(b)$ .

## 10.1 Properties of Homomorphisms

**Theorem 10.1.** *Let  $\phi : G \rightarrow \overline{G}$  be a homomorphism, let  $g \in G$ . Then*

1.  $e \in G, \bar{e} \in \overline{G}, \phi(e) = \bar{e}$ .
2.  $\forall n \in \mathbb{Z}, \phi(g^n) = (\phi(g))^n$ .
3.  $|g| = n \implies |\phi(g)| \mid |g|$ .
4.  $\text{Ker } \phi \leq G$ .
5.  $\phi(a) = \phi(b) \iff a \text{Ker } \phi = b \text{Ker } \phi$ .
6.  $\phi(g) = \bar{g} \implies \phi^{-1}(\bar{g}) = \{x \in G : \phi(x) = \bar{g}\} = g \text{Ker } \phi$ . (!)

*Proof.* Let  $\phi : G \rightarrow \overline{G}$  be a homomorphism,  $g \in G$ .

1. Let  $e \in G, \bar{e} \in \overline{G}$ . Since  $\phi$  is OP,  $\phi(e) \in \overline{G}$ ,

$$\phi(g)\phi(e) = \phi(ge) = \phi(g) = \phi(eg) = \phi(e)\phi(g).$$

Hence  $\phi(e) = \bar{e}$ .

2. Let  $n \in \mathbb{Z}$  be arbitrary, since  $\phi$  is OP,

$$\phi(g^n) = \underbrace{\phi(g) \cdots \phi(g)}_n = (\phi(g))^n.$$

3. Let  $|g| = n$ , then

$$(\phi(g))^n = \phi(g^n) = \phi(e) = \bar{e}.$$

By Theorem 4.1(ii),

$$(\phi(g))^n = \bar{e} = (\phi(g))^0 \iff |\phi(g)| \mid (n - 0) = n.$$

4. Let  $\text{Ker } \phi = \{g \in G : \phi(g) = \bar{e}, g, g^{-1} \in \text{Ker } \phi\}$ , then

$$\phi(gg^{-1}) = \phi(e) = \bar{e} \implies gg^{-1} \in \text{Ker } \phi.$$

Hence by one-step subgroup test,  $\text{Ker } \phi \leq G$ .

5. ( $\Rightarrow$ ) Let  $\phi(a) = \phi(b)$ , then

$$\bar{e} = \phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}),$$

Hence  $ab^{-1} \in \text{Ker } \phi$ . Since by Theorem 10.1.4,  $\text{Ker } \phi \leq G$ , by Lemma 7.1.6,

$$ab^{-1} \in \text{Ker } \phi \iff a \text{Ker } \phi = b \text{Ker } \phi.$$



( $\Leftarrow$ ) Let  $a \text{ Ker } \phi = b \text{ Ker } \phi$ , then by Lemma 7.1.6,

$$ab^{-1} \in \text{Ker } \phi \iff a \text{ Ker } \phi = b \text{ Ker } \phi.$$

Hence,

$$\bar{e} = \phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} \implies \phi(a) = \phi(b).$$

Therefore,  $\phi(a) = \phi(b) \iff a \text{ Ker } \phi = b \text{ Ker } \phi$ .

6. Let  $\phi(g) = \bar{g}, \phi^{-1}(\bar{g}) = \{x \in G : \phi(x) = \bar{g}\}, g \text{ Ker } \phi = \{gx : \phi(x) = \bar{e}\}$ .  
Let  $x \in \phi^{-1}(\bar{g})$ , then

$$\phi(x) = \bar{g} = \phi(g).$$

By Theorem 10.1.5,

$$\phi(x) = \phi(g) \iff x \text{ Ker } \phi = g \text{ Ker } \phi.$$

Since  $\phi(e) = \bar{e} \implies e \in \text{Ker } \phi$ , it follows that

$$x = xe \in x \text{ Ker } \phi = g \text{ Ker } \phi.$$

Hence,  $\phi^{-1}(\bar{g}) \subseteq g \text{ Ker } \phi$ .

Let  $gx \in g \text{ Ker } \phi$ , then

$$\phi(gx) = \phi(g)\phi(x) = \bar{g}\bar{e} = \bar{g} \implies gx \in \phi^{-1}(\bar{g}).$$

Hence  $g \text{ Ker } \phi \subseteq \phi^{-1}(\bar{g})$ .

Therefore  $\phi^{-1}(\bar{g}) = g \text{ Ker } \phi$ .

□

**Theorem 10.2.** Let  $\phi : G \rightarrow \bar{G}$  be a homomorphism, let  $H \leq G$ . Then

1.  $\phi(H) = \{\phi(h) : h \in H\} \leq \bar{G}$ .
2.  $H$  is cyclic  $\implies \phi(H)$  is cyclic.
3.  $H$  is Abelian  $\implies \phi(H)$  is Abelian.
4.  $H \triangleleft G \implies \phi(H) \triangleleft \phi(G)$ .
5.  $|\text{Ker } \phi| = n \implies \phi : G \rightarrow \phi(G)$  is an  $n$ -to-1 mapping.
6.  $H$  is finite  $\implies |\phi(H)| \mid |H|$ .
7.  $\bar{K} \leq \bar{G} \implies \phi^{-1}(\bar{K}) = \{k \in G : \phi(k) \in \bar{K}\} \leq G$ .
8.  $\bar{K} \triangleleft \bar{G} \implies \phi^{-1}(\bar{K}) = \{k \in G : \phi(k) \in \bar{K}\} \triangleleft G$ .
9.  $\phi$  is onto and  $\text{Ker } \phi = \{e\} \implies \phi : G \rightarrow \bar{G}$  is an isomorphism.

*Proof.* Let  $\phi : G \rightarrow \overline{G}$  be a homomorphism, and  $H \leq G$ .

1. Let  $\phi(H) = \{\phi(h) : h \in H\} \subseteq \overline{G}$ . Let  $\phi(h_1), \phi(h_2) \in \phi(H)$ , then since  $\phi$  is OP,

$$\phi(h_1)(\phi(h_2))^{-1} = \phi(h_1)\phi(h_2^{-1}) = \phi(h_1h_2^{-1}).$$

Hence,

$$h_1h_2^{-1} \in H \implies \phi(h_1)(\phi(h_2))^{-1} = \phi(h_1h_2^{-1}) \in \phi(H).$$

By one-step subgroup test,  $\phi(H) \leq \overline{G}$ .

2. Let  $H = \langle h \rangle, h \in H$ , then  $x \in H, x = h^n, n \in \mathbb{Z}$ . Let  $\phi(x) \in \phi(H)$  be arbitrary, then

$$\phi(x) = \phi(h^n) = (\phi(h))^n.$$

Hence  $\phi(H) = \langle \phi(h) \rangle$ .

3. Let  $H$  be Abelian, then  $a, b \in H, ab = ba$ . Let  $\phi(a), \phi(b) \in \phi(H)$ , then

$$\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a).$$

Hence  $\phi(H)$  is Abelian.

4. Let  $H \triangleleft G$ , then by Theorem 9.1,

$$H \triangleleft G \iff g \in G, gHg^{-1} \subseteq H.$$

Let  $\phi(g) \in \phi(G), \phi(h) \in \phi(H)$ , then

$$\phi(g)\phi(h)(\phi(g))^{-1} = \phi(g)\phi(h)\phi(g^{-1}) = \phi(ghg^{-1}).$$

Since  $ghg^{-1} \in gHg^{-1} \subseteq H$ , by definition,  $\phi(ghg^{-1}) \in \phi(H)$ . Hence,

$$\phi(g)\phi(h)(\phi(g))^{-1} = \phi(ghg^{-1}) \in \phi(H) \implies \phi(g)\phi(H)(\phi(g))^{-1} \subseteq \phi(H)$$

Therefore by Theorem 9.1,

$$\phi(g)\phi(H)(\phi(g))^{-1} \subseteq \phi(H) \iff \phi(H) \triangleleft \phi(G).$$

5. Let  $|\text{Ker } \phi| = n, g \in G, \bar{g} \in \phi(G)$ . Then by Theorem 10.1.6,

$$\phi(g) = \bar{g} \implies \phi^{-1}(\bar{g}) = \{x \in G : \phi(x) = \bar{g}\} = g \text{Ker } \phi.$$

Hence,

$$|\text{ker } \phi| = n \implies |g \text{Ker } \phi| = n = |\phi^{-1}(\bar{g})|.$$

Therefore,

$$\bar{g} \in \phi(g), \exists x_1, \dots, x_n \in G : \phi(x_1) = \dots = \phi(x_n) = \bar{g}.$$

6. Let  $|H| = n$ . Let  $\phi_H : H \rightarrow \phi(H)$ , then  $\phi_H$  is a homomorphism. Since

$$H \leq G \implies e \in H \implies \phi(e) \in \phi(H),$$

therefore  $\text{Ker } \phi_H \neq \emptyset$ . Let  $|\text{Ker } \phi_H| = t$ , by Theorem 10.2.5,  $|\text{Ker } \phi_H| = t \implies \phi_H : H \rightarrow \phi(H)$  is  $t$ -to-1. Hence,

$$|\phi(H)| = |H|/t \implies |\phi(H)| \mid |H| = n.$$

7. Let  $\overline{K} \leq \overline{G}$  and  $\phi^{-1}(\overline{K}) = \{k \in G : \phi(k) \in \overline{K}\} \subseteq G$ . Since

$$e \in G, \phi(e) = \overline{e} \in \overline{K} \implies e \in \phi^{-1}(\overline{K}),$$

therefore  $\phi^{-1}(\overline{K}) \neq \emptyset$ . Let  $a, b \in \phi^{-1}(\overline{K})$ , then  $\phi(a), \phi(b) \in \overline{K}$ . Since  $\phi$  is OP,

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1}.$$

Since  $\overline{K} \leq \overline{G} \implies \phi(a)(\phi(b))^{-1} \in \overline{K}$ , therefore

$$\phi(ab^{-1}) = \phi(a)(\phi(b))^{-1} \in \overline{K} \implies ab^{-1} \in \phi^{-1}(\overline{K}).$$

Hence by one-step subgroup test,  $\phi^{-1}(\overline{K}) \leq G$ .

8. Let  $\overline{K} \triangleleft \overline{G}$  and  $\phi^{-1}(\overline{K}) = \{k \in G : \phi(k) \in \overline{K}\}$ . Let  $a \in \phi^{-1}(\overline{K}), g \in G$ . Then since  $\phi$  is OP,

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)\phi(a)(\phi(g))^{-1}.$$

Since  $\overline{K} \triangleleft \overline{G}$ , therefore  $\phi(g) \in \overline{G}, \phi(a) \in \overline{K}$ ,

$$\phi(g)\overline{K}(\phi(g))^{-1} \subseteq \overline{K} \implies \phi(g)\phi(a)(\phi(g))^{-1} \in \overline{K}.$$

Hence,

$$\phi(gag^{-1}) = \phi(g)\phi(a)(\phi(g))^{-1} \in \overline{K} \implies gag^{-1} \in \phi^{-1}(\overline{K}).$$

Therefore,  $g\phi^{-1}(\overline{K})g^{-1} \subseteq \phi^{-1}(\overline{K})$  and by Theorem 9.1,  $\phi^{-1}(\overline{K}) \triangleleft G$ .

9. Let  $\phi$  be onto and  $\text{ker } \phi = \{e\}$ . By Theorem 10.2.5,  $|\text{Ker } \phi| = 1 \implies \phi : G \rightarrow \overline{G}$  is 1-to-1. Since  $\phi$  is 1-to-1, onto, and OP, therefore  $\phi$  is an isomorphism.

□

**Corollary 10.2.1.** *Let  $\phi : G \rightarrow \overline{G}$  be a homomorphism. Then  $\text{Ker } \phi \triangleleft G$ .*

*Proof.* Let  $\phi : G \rightarrow \overline{G}$  be a homomorphism. By Theorem 10.1.4,  $\text{Ker } \phi \leq G$ . By Theorem 9.1, let  $g \in G, x \in \text{Ker } \phi$  be arbitrary, and  $gxg^{-1} \in g\text{Ker } \phi g^{-1}$ . Then

$$\begin{aligned}\phi(gxg^{-1}) &= \phi(g)\phi(x)\phi(g^{-1}) \\ &= \phi(g)\phi(x)(\phi(g))^{-1} \\ &= \phi(g)\bar{e}(\phi(g))^{-1} \\ &= \phi(g)(\phi(g))^{-1} \\ &= \bar{e}.\end{aligned}$$

Hence  $gxg^{-1} \in \text{Ker } \phi \implies g\text{Ker } \phi g^{-1} \subseteq \text{Ker } \phi$ . Therefore  $\text{Ker } \phi \triangleleft G$ .  $\square$

**Example 10.8.** Let  $\phi : \mathbb{C}^* \rightarrow \mathbb{C}^*, \phi(x) = x^4$  be a mapping. Since for  $x, y \in \mathbb{C}^*$ ,

$$\phi(xy) = (xy)^4 = x^4 y^4 = \phi(x)\phi(y),$$

$\phi$  is a homomorphism. Since

$$\text{Ker } \phi = \{x \in \mathbb{C}^* : \phi(x) = x^4 = 1\} = \{1, -1, i, -i\},$$

so, by Theorem 10.2.5,  $|\text{Ker } \phi| = 4 \implies \phi$  is a 4-to-1 mapping. To find all  $x \in \mathbb{C}^* : \phi(x) = 2$ , since  $\phi(\sqrt[4]{2}) = (\sqrt[4]{2})^4 = 2$ , by Theorem 10.1.6,

$$\phi^{-1}(2) = \{x \in \mathbb{C}^* : \phi(x) = 2\} = \sqrt[4]{2} \text{Ker } \phi = \{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i\}.$$

Finally, let  $H = \langle \cos 30^\circ + i \sin 30^\circ \rangle$ . By Theorem 10.1.3, Theorem 10.2.6, and DeMoivre's Theorem,

$$(r(\cos \theta + i \sin \theta))^n = r^n(\cos n\theta + i \sin n\theta).$$

$$|H| = 12, \phi(H) = \langle \cos 120^\circ + i \sin 120^\circ \rangle, \text{ and } |\phi(H)| = 3.$$

**Example 10.9.** Let  $\phi : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}, \phi(x) = 3x$  be a mapping. Since for  $a, b \in \mathbb{Z}_{12}$ ,

$$\phi(a + b) = 3(a + b) = 3a + 3b = \phi(a) + \phi(b),$$

$\phi$  is a homomorphism. Since for  $a \in \mathbb{Z}_{12}$ ,

$$\phi(a) = 3a = 0 \implies a = 0, 4, 8,$$

therefore  $\text{Ker } \phi = \{0, 4, 8\}$ . By Theorem 10.2.5,  $|\text{Ker } \phi| = 3 \implies \phi$  is a 3-to-1 mapping. Since  $\phi(2) = 6$ , by Theorem 10.1.6,

$$\phi^{-1}(6) = \{a \in \mathbb{Z}_{12} : \phi(a) = 6\} = 2 + \text{Ker } \phi = \{2, 6, 10\}.$$

By Theorem 10.2.2,  $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$  is cyclic  $\implies \phi(\langle 2 \rangle) = \{0, 6\}$  is cyclic. By Theorem 10.1.3,

$$|2| = 6 \implies |\phi(2)| = |6| = 2||2| = 6.$$

Let  $\overline{K} = \{0, 6\} \leq \mathbb{Z}_{12}$ , by Theorem 10.2.7,

$$\phi^{-1}(\overline{K}) = \{a \in \mathbb{Z}_{12} : \phi(a) \in \overline{K}\} \leq \mathbb{Z}_{12}.$$

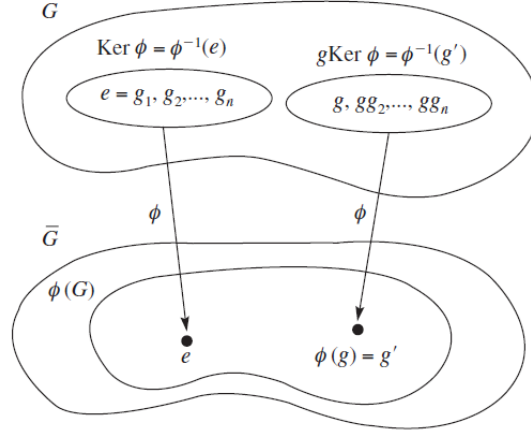


Figure 10.1

**Example 10.10.** Both  $\mathbb{Z}_{12}, \mathbb{Z}_{30}$  are cyclic. To determine all homomorphisms  $\phi : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{30}$ . Let  $1 \in \mathbb{Z}_{12}, \phi(1) = a$ , by Theorem 10.1.2,

$$x \in \mathbb{Z}_{12}, \phi(x) = x\phi(1) = xa.$$

By Lagrange's Theorem,

$$a \in \mathbb{Z}_{30}, |a| = |\langle a \rangle| \mid 30,$$

and by Theorem 10.1.3,

$$1 \in \mathbb{Z}_{12}, |1| = 12 \implies |\phi(1)| = |a| \mid 12.$$

Hence  $|a| \in \{1, 2, 3, 6\} \implies a = \{0, 15, 10, 20, 5, 25\}$ . Let  $\phi_n(1) = n$ , then  $\{\phi_0, \phi_{15}, \phi_{10}, \phi_{20}, \phi_5, \phi_{25}\}$  are all the homomorphisms from  $\mathbb{Z}_{12} \rightarrow \mathbb{Z}_{30}$ . For example, let  $a, b \in \mathbb{Z}_{12}$ , then

$$\phi_{15}(a + b) = (a + b)\phi_{15}(1) = (a + b)15 = 15a + 15b = \phi_{15}(a) + \phi_{15}(b).$$

**Example 10.11.** The mapping  $\phi : S_n \rightarrow \mathbb{Z}_2$  that takes an even permutation to 0 and an odd permutation to 1 is a homomorphism (Figure 10.2).

## 10.2 The First Isomorphism Theorem

**Theorem 10.3** (First Isomorphism Theorem). *Let  $\phi : G \rightarrow \bar{G}$  be a homomorphism. Then  $\psi : G/\text{Ker } \phi \rightarrow \phi(G), \psi(g\text{Ker } \phi) = \phi(g)$  is an isomorphism. In symbols,  $G/\text{Ker } \phi \approx \phi(G)$ .*

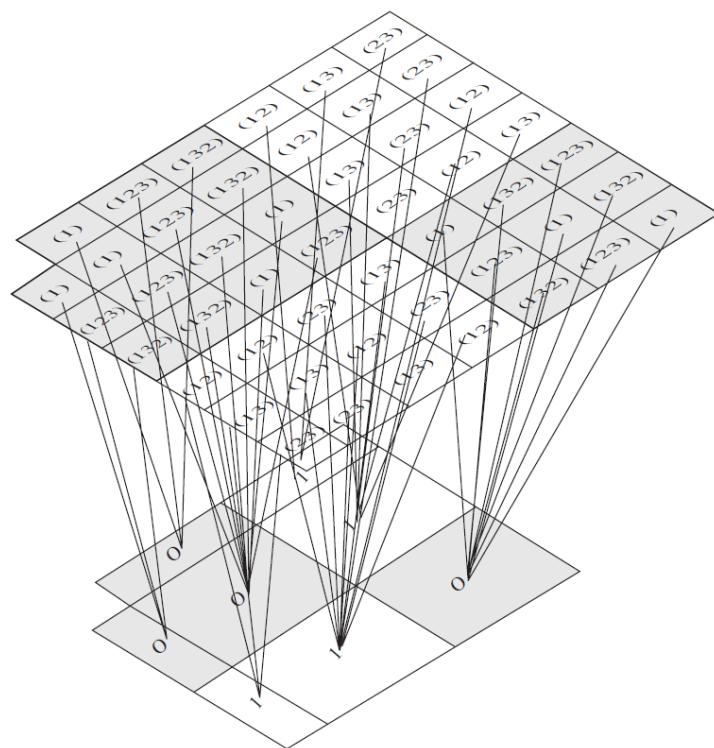


Figure 10.2: Homomorphism from  $S_3$  to  $Z_2$ .

*Proof.* Let  $\phi : G \rightarrow \overline{G}$  be a homomorphism. Let  $\psi : G/\text{Ker } \phi \rightarrow \phi(G), \psi(g \text{Ker } \phi) = \phi(g)$  be a mapping. Let  $a, b \in G$ , by Theorem 10.1.5,

$$\phi(a) = \phi(b) \iff a \text{Ker } \phi = b \text{Ker } \phi.$$

Hence  $\psi$  is well-defined and 1-to-1. Let  $\phi(g) \in \phi(G)$ , since

$$g \in G \implies \exists g \text{Ker } \phi \in G/\text{Ker } \phi : \psi(g \text{Ker } \phi) = \phi(g).$$

Hence  $\psi$  is onto. By Corollary 10.2.1,  $\text{Ker } \phi \triangleleft G$ , therefore by Theorem 9.2,  $G/\text{Ker } \phi$  under  $a \text{Ker } \phi \cdot b \text{Ker } \phi = ab \text{Ker } \phi$  is a factor group. Let  $a \text{Ker } \phi, b \text{Ker } \phi \in G/\text{Ker } \phi$ , then

$$\begin{aligned} \psi(a \text{Ker } \phi \cdot b \text{Ker } \phi) &= \psi(ab \text{Ker } \phi) \\ &= \phi(ab) \\ &= \phi(a)\phi(b) \\ &= \psi(a \text{Ker } \phi)\psi(b \text{Ker } \phi). \end{aligned}$$

Hence  $\psi$  is OP. Therefore  $\psi : G/\text{ker } \phi \rightarrow \phi(G)$  is an isomorphism and  $G/\text{ker } \phi \approx \phi(G)$ .  $\square$

**Corollary 10.3.1.** *Let  $G$  be a finite group. Then*

$$\phi : G \rightarrow \overline{G} \text{ is a homomorphism} \implies |\phi(G)| \mid |G|, |\overline{G}|.$$

*Proof.* Let  $\phi : G \rightarrow \overline{G}$  be a homomorphism. By Theorem 10.1.4,  $\text{Ker } \phi \leq G$ . By Lagrange's Theorem,

$$|G/\text{Ker } \phi| = |G|/|\text{Ker } \phi| \implies |G/\text{Ker } \phi| \mid |G|.$$

By Theorem 10.3,

$$G/\text{Ker } \phi \approx \phi(G) \implies |\phi(G)| = |G/\text{Ker } \phi| \mid |G|.$$

By Theorem 10.2.1,

$$G \leq G \implies \phi(G) \leq \overline{G}.$$

Hence by Lagrange's Theorem,

$$\phi(G) \leq \overline{G} \implies |\phi(G)| \mid |\overline{G}|.$$

Therefore,  $|\phi(G)| \mid |G|, |\overline{G}|$ .  $\square$

**Example 10.12.** Let  $\phi : D_4 \rightarrow D_4$  be a homomorphism given by Figure 10.3. Then  $\text{Ker } \phi = \{R_0, R_{180}\}$ . Let  $\psi : D_4/\text{Ker } \phi \rightarrow \phi(D_4), \psi(x \text{Ker } \phi) = \phi(x), x \in D_4$  be a mapping. So,

$$\begin{aligned} \psi(R_0 \text{Ker } \phi) &= \phi(R_0) = R_0 = \phi(R_{180}) = \psi(R_{180} \text{Ker } \phi), \\ \psi(R_{90} \text{Ker } \phi) &= \phi(R_{90}) = H = \phi(R_{270}) = \psi(R_{270} \text{Ker } \phi), \\ \psi(H \text{Ker } \phi) &= \phi(H) = R_{180} = \phi(V) = \psi(V \text{Ker } \phi), \\ \psi(D \text{Ker } \phi) &= \phi(D) = V = \phi(D') = \psi(D' \text{Ker } \phi). \end{aligned}$$

By Theorem 10.3,  $\psi(D_4/\text{Ker } \phi) \approx \phi(D_4)$ .

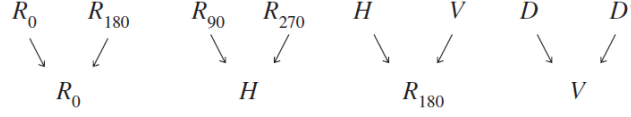


Figure 10.3

**Note 10.1.** Theorem 10.3 can be represented by Figure 10.4, where  $\gamma : G \rightarrow G/\text{Ker } \phi$ ,  $\gamma(g) = g \text{Ker } \phi$  is called the *natural mapping* from  $G$  to  $G/\text{Ker } \phi$ . By the proof of Theorem 10.3,  $\psi\gamma = \phi$ . In this case, Figure 10.4 is *commutative*.

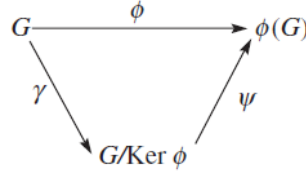


Figure 10.4

**Example 10.13.** Let  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ ,  $\phi(m) = m \bmod n$  be a homomorphism. Since  $a \in \mathbb{Z} : \phi(a) = a \bmod n = 0 \implies a \in \{0, n\}$ , therefore  $\text{Ker } \phi = \langle n \rangle = \{0, n\}$ . By Theorem 10.3,  $\mathbb{Z}/\text{Ker } \phi \approx \phi(\mathbb{Z}) = \mathbb{Z}_n$ .

**Example 10.14.** The warping function  $W$  maps each  $a \in \mathbb{R}$  to a point  $a$  radian from  $(1,0)$  on the unit circle centered at  $(0,0)$ . The positive reals in the counterclockwise direction, the negative reals in the clockwise direction, and  $W(0) = (1,0)$  (Figure 10.5).  $W$  is a homomorphism from  $\mathbb{R}$  under addition onto the circle group, the group of complex number of magnitude 1 under multiplication. From elementary trigonometry facts,

$$W(x) = \cos x + i \sin x,$$

$$W(x+y) = W(x)W(y).$$

Since  $W$  is periodic of period  $2\pi$ , therefore  $\text{Ker } W = \langle 2\pi \rangle$ . So, from the First Isomorphism Theorem,  $\mathbb{R}/\langle 2\pi \rangle \approx$  the circle group.

**Example 10.15.** Let  $H \leq G$ . The normalizer of  $H$  in  $G$  is  $N(H) = \{x \in G : xHx^{-1} = H\}$  and the centralizer of  $H$  in  $G$  is  $C(H) = \{x \in G : xhx^{-1} = h, h \in H\}$ . Let  $\psi : N(H) \rightarrow \text{Aut}(H)$ ,  $\psi(g) = \phi_g$ , where  $\phi_g(h) = ghg^{-1}$ ,  $h \in H$  is the inner automorphism of  $H$  induced by  $g$ . The mapping  $\psi$  is a homomorphism with  $\text{Ker } \psi = C(H)$ . So, by the First Isomorphism Theorem,

$$N(H)/\text{Ker } \psi = N(H)/C(H) \approx \psi(N(H)) \leq \text{Aut}(H).$$



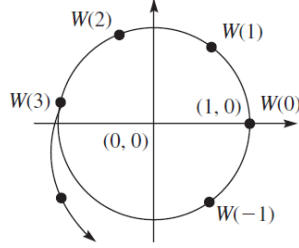


Figure 10.5

**Example 10.16.** Let  $|G| = 35$ . By Lagrange's Theorem,

$$g \in G, g \neq e, |g| = |\langle g \rangle| \mid |G| = 35.$$

Hence,  $|g| \in \{5, 7, 35\}$ . If  $\exists a \in G : |a| = 35$ , then  $G = \langle a \rangle$ . So assume that  $g \in G, a \neq e, |g| \in \{5, 7\}$ . But not all  $g \in G$  can have order 5, since  $g \in G : |g| = 5$  come 4 at a time ( $|x| = 5 \implies |x^2| = |x^3| = |x^4| = 5$ ) and 4 does not divide 34. Similarly, since 6 does not divide 34, not all  $g \in G$  can have order 7. Hence,  $G$  has elements of order 5 and 7. Since  $\exists g \in G : |g| = 7$ ,  $\exists H \leq G : |H| = 7$ . In fact,  $H$  is the only subgroup of  $G$  of order 7, since if  $K \leq H, |K| = 7$ , then

$$|HK| = |H||K|/|H \cap K| = 7 \cdot 7/1 = 49.$$

But this is impossible in a group of order 35. Since  $a \in G, aHa^{-1} \leq G, |aHa^{-1}| = 7$ , therefore  $H = aHa^{-1}$ . So,  $N(H) = G$ . Since  $H$  has prime order, it is cyclic and therefore Abelian. In particular,  $C(H)$  contains  $H$ . So,  $7 \mid |C(H)|$  and  $|C(H)| \mid 35$ . It follows that  $C(H) = G$  or  $C(H) = H$ . If  $C(H) = G$ , then an element  $x$  of order 35 can be obtained by letting  $x = hk$ , where  $h \in H, h \neq e$  and  $|k| = 5$ . If  $C(H) = H$ , then  $|C(H)| = 7$  and  $|N(H)/C(H)| = 35/7 = 5$ . However, 5 does not divide  $|Aut(H)| = |Aut(Z_7)| = 6$ . This contradiction shows that  $G$  is cyclic.

**Theorem 10.4** (Normal Subgroups Are Kernels). *Let  $\phi : G \rightarrow \overline{G}$  be a homomorphism. Then*

$$H \triangleleft G \implies H = \text{Ker } \phi.$$

*In particular, let  $\gamma : G \rightarrow G/N, \gamma(g) = gN$  be a homomorphism called the natural homomorphism from  $G$  to  $G/N$ . Then,*

$$N \triangleleft G \implies N = \text{Ker } \gamma.$$

*Proof.* Let  $\gamma : G \rightarrow G/N, \gamma(g) = gN$  be the natural homomorphism from  $G$  to  $G/N$ . Then,

$$\gamma(xy) = (xy)N = xNyN = \gamma(x)\gamma(y).$$

Moreover,

$$g \in \text{Ker } \gamma \iff gN = \gamma(g) = N.$$

By Lemma 7.1.2,

$$gN = N \iff g \in N.$$

Hence,

$$\text{Ker } \gamma \subseteq N, N \subseteq \text{Ker } \gamma \implies N = \text{Ker } \gamma.$$

□

## 11 Fundamental Theorem of Finite Abelian Groups

### 11.1 The Fundamental Theorem

**Theorem 11.1** (Fundamental Theorem of Finite Abelian Groups). *Let  $G$  be a finite Abelian group. Then*

$$G = H_1 \oplus H_2 \oplus \cdots \oplus H_k,$$

*where  $H_i$ 's are cyclic groups of order prime-power, i.e.  $|H_i| = p_i^{n_i}$ . Moreover, the number of  $H_i$  in the product and  $|H_i|$  are uniquely determined by  $G$ .*

**Note 11.1.** Let  $G$  be a finite Abelian group. Then by the Fundamental Theorem,

$$G = H_1 \oplus H_2 \oplus \cdots \oplus H_k,$$

where  $H_i$ 's are cyclic and  $|H_i| = p_i^{n_i}$ . Since a cyclic group of order  $n$  is isomorphic to  $\mathbb{Z}_n$ , therefore  $H_i \approx \mathbb{Z}_{p_i^{n_i}}$ . Hence,

$$G \approx \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}},$$

where  $p_i$ 's are not necessarily distinct primes and the prime-powers  $p_1^{n_1}, p_2^{n_2}, \dots, p_k^{n_k}$  are uniquely determined by  $G$ . Writing a group in this form is called *determining the isomorphism class of  $G$* .

### 11.2 The Isomorphism Classes of Abelian Groups

**Note 11.2.** The Fundamental Theorem can be used as an algorithm to construct all Abelian groups of any order. Consider Abelian groups  $G, |G| = p^k$ , where  $p$  is prime and  $k \leq 4$ . In general, there is one group of order  $p^k$  for each set of positive integers whose sum is  $k$  (such a set is called a *partition of  $k$* ); that is, if

$$k = n_1 + n_2 + \cdots + n_t,$$

where  $n_i$ 's are positive integers, then

$$\mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_t}}$$

Order of $G$	Partitions of $k$	Possible direct products for $G$
$p$	1	$Z_p$
$p^2$	2	$Z_{p^2}$
$p^3$	1 + 1	$Z_p \oplus Z_p$
	3	$Z_{p^3}$
	2 + 1	$Z_{p^2} \oplus Z_p$
$p^4$	1 + 1 + 1	$Z_p \oplus Z_p \oplus Z_p$
	4	$Z_{p^4}$
	3 + 1	$Z_{p^3} \oplus Z_p$
	2 + 2	$Z_{p^2} \oplus Z_{p^2}$
	2 + 1 + 1	$Z_{p^2} \oplus Z_p \oplus Z_p$
	1 + 1 + 1 + 1	$Z_p \oplus Z_p \oplus Z_p \oplus Z_p$

Figure 11.1

is an Abelian group of order  $p^k$  (Figure 11.1).

Furthermore, the uniqueness portion of the Fundamental Theorem guarantees that distinct partitions of  $k$  yield distinct isomorphism classes. Thus, for example,  $\mathbb{Z}_9 \oplus \mathbb{Z}_3$  is not isomorphic to  $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ . A reliable mnemonic for comparing external direct products is the cancellation property. If  $A$  is finite, then

$$A \oplus B \approx A \oplus C \iff B \approx C.$$

Thus  $\mathbb{Z}_4 \oplus \mathbb{Z}_4$  is not isomorphic to  $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$  since  $\mathbb{Z}_4$  is not isomorphic to  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

Now that one knows how to construct all the Abelian groups of prime power order, the next step is to construct all Abelian groups of a certain order  $n$ , where  $n$  has two or more distinct prime divisors. First, write  $n$  in prime-power decomposition form

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}.$$

Next, individually form all Abelian groups of order  $p_1^{n_1}$ , then  $p_2^{n_2}$ , and so on, as described earlier. Finally, form all possible external direct products of these groups. For example, let  $G$  be an Abelian group of order

$$n = 1176 = 2^3 \cdot 3 \cdot 7^2.$$

Then, for  $2^3$ , since

$$\begin{aligned} p = 2, k = 3 \\ &= 2 + 1 \\ &= 1 + 1 + 1, \end{aligned}$$

the possible isomorphism classes for Abelian groups of order  $2^3$  are

$$\begin{aligned}\mathbb{Z}_8, \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2, \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.\end{aligned}$$

For 3, since  $p = 3, k = 1$ , the only possible isomorphism class for Abelian groups of order 3 is  $\mathbb{Z}_3$ . For  $7^2$ , since

$$p = 7, k = 2 = 1 + 1,$$

the possible isomorphism classes for Abelian groups of order  $7^2$  are

$$\mathbb{Z}_{49}, \mathbb{Z}_7 \oplus \mathbb{Z}_7.$$

Hence, the complete list of the possible distinct isomorphism classes for  $G$  is

$$\begin{aligned}\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}, \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}, \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}, \\ \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7, \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7, \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7.\end{aligned}$$

To determine which of the preceding six isomorphism classes represents the structure of  $G$ , one can compare the orders of the elements of  $G$  with the orders of the elements in the six direct products, since by Theorem 6.2.7, two finite Abelian groups are isomorphic if and only if they have the same number of elements of each order. For example, if  $G$  has any elements of order 8, then  $G$  must be isomorphic to the first or fourth group above, since these are the only groups with elements of order 8. Then, check if  $G$  has any elements of order 49, since the first group above has elements of order 49, but the fourth group does not.

Consider some specific Abelian group  $G : |G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ , where  $p_i$ 's are distinct primes. One can express  $G$  as an internal direct product of cyclic groups of prime-power order. For simplicity, assume that  $G$  has  $2^n$  elements. First, compute the orders of all the elements of  $G$ . Second, select a element  $a_1 \in G$  of maximum order  $2^r$ . Then  $\langle a_1 \rangle$  is one of the factors in the desired internal direct product. If  $G \neq \langle a_1 \rangle$ , select an element  $a_2 \in G$  of maximum order  $2^s$  such that

$$s \leq n - r \text{ and } a_2, a_2^2, a_2^4, \dots, a_2^{2^{s-1}} \notin \langle a_1 \rangle.$$

Then  $\langle a_2 \rangle$  is a second direct factor. If  $n \neq r + s$ , select an element  $a_3 \in G$  of maximum order  $2^t$  such that  $t \leq n - r - s$  and

$$a_3, a_3^2, a_3^4, \dots, a_3^{2^{t-1}} \notin \langle a_1 \rangle \times \langle a_2 \rangle = \{a_1^i a_2^j : 0 \leq i < 2^r, 0 \leq j < 2^s\}.$$

Then  $\langle a_3 \rangle$  is another direct factor. Continue in this fashion until the internal direct product  $\langle a_1 \rangle \times \langle a_2 \rangle \times \langle a_3 \rangle \times \cdots$  has the same order as  $G$ .

The greedy algorithm for an Abelian Group  $G$  of order  $p^n$  is as follows:

1. Compute the orders of all the elements of  $G$ .
2. Select an  $a_1 \in G$  of maximum order and define  $G_1 = \langle a_1 \rangle$ . Set  $i = 1$ .
3. If  $|G| = |G_i|$ , stop. Otherwise, replace  $i$  by  $i + 1$ .
4. Select an  $a_i \in G$  of maximum order  $p^k$  such that  $p^k \leq |G|/|G_{i-1}|$  and  $a_i, a_i^p, a_i^{p^2}, \dots, a_i^{p^{k-1}} \notin G_{i-1}$ , and define  $G_i = G_{i-1} \times \langle a_i \rangle$ .
5. Return to step 3.

In the general case where  $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ , one simply use the algorithm to build up a direct product of order  $p_1^{n_1}$ , then another of order  $p_2^{n_2}$ , and so on. The direct product of all these pieces is the desired factorization of  $G$ .

**Example 11.1.** Let  $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$  under multiplication modulo 65. Since  $|G| = 16 = 2^4$ , the possible isomorphism classes for  $G$  are

$$\begin{array}{ll}
 k = 4, & \mathbb{Z}_{16}, \\
 = 3 + 1, & \mathbb{Z}_8 \oplus \mathbb{Z}_2, \\
 = 2 + 2, & \mathbb{Z}_4 \oplus \mathbb{Z}_4, \\
 = 2 + 1 + 1, & \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \\
 = 1 + 1 + 1 + 1, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.
 \end{array}$$

Figure 11.2 shows the orders of the elements of  $G$ .

Element	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
Order	1	4	4	2	4	4	4	4	4	4	4	4	2	4	4	2

Figure 11.2

From Figure 11.2, since  $G$  has no elements of order 16 and 8, and  $G$  only has three elements of order 2, it must be that either

$$G \approx \mathbb{Z}_4 \oplus \mathbb{Z}_4 \text{ or } G \approx \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Since  $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$  has a subgroup isomorphic to  $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ , it has more than three elements of order 2. Therefore, it must be that  $G \approx \mathbb{Z}_4 \oplus \mathbb{Z}_4$ .

To express  $G$  as an internal direct product, select an element of maximum order, say  $8 \in G$ . Then  $\langle 8 \rangle$  is a factor in the product. Next select a second element  $a \in G$  such that  $|a| = 4$  and

$$a, a^2 \notin \langle 8 \rangle = \{1, 8, 64, 57\}.$$

Since

$$12 \in G, |12| = 4, \langle 12 \rangle = \{12, 14, 38, 1\}$$

it follows that  $\langle 12 \rangle$  is the second factor in the product. Since

$$|\langle 8 \rangle \times \langle 12 \rangle| = 16 = |G|,$$

it follows that  $G = \langle 8 \rangle \times \langle 12 \rangle$ .

**Example 11.2.** Let

$$G = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, \\ 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\}$$

under multiplication modulo 135. Since  $|G| = 24 = 2^3 \cdot 3$ , the possible isomorphism classes for Abelian groups of order  $2^3$  are

$$\begin{aligned} k = 3, & & \mathbb{Z}_8, \\ = 2 + 1, & & \mathbb{Z}_4 \oplus \mathbb{Z}_2, \\ = 1 + 1 + 1, & & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2. \end{aligned}$$

The possible isomorphism class for Abelian groups of order 3 is  $\mathbb{Z}_3$ . Hence the possible isomorphism classes for  $G$  are

$$\begin{aligned} \mathbb{Z}_8 \oplus \mathbb{Z}_3 &\approx \mathbb{Z}_{24}, \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 &\approx \mathbb{Z}_{12} \oplus \mathbb{Z}_2, \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 &\approx \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2. \end{aligned}$$

Consider  $8 \in G$ . By direct calculations,  $8^6 = 109$  and  $8^{12} = 1$ . Since  $|8| = 12$ ,  $G$  is not isomorphic to  $\mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ . Since  $|109| = 2 = |134|$ ,  $G$  is not isomorphic to  $\mathbb{Z}_{24}$ . Hence  $G \approx \mathbb{Z}_{12} \oplus \mathbb{Z}_2$ , and  $G = \langle 8 \rangle \times \langle 134 \rangle$ .

**Note 11.3.** Rather than express an Abelian group as a direct product of cyclic groups of prime-power orders, it is often more convenient to combine the cyclic factors of relatively prime order to obtain a direct product of the form

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}, n_i \mid n_{i-1},$$

like in Example 11.2. For example,

$$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

would be written as

$$\mathbb{Z}_{180} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_2.$$

The greedy algorithm is easily adapted to accomplish this by replacing step 4 by 4': select an element  $a_i \in G$  of maximum order  $m$  such that  $m \leq |G|/|G_{i-1}|$  and  $a_i, a_i^2, \dots, a_i^{m-1} \notin G_{i-1}$ , and define  $G_i = G_{i-1} \times \langle a_i \rangle$ .

**Corollary 11.1.1.** *Let  $G$  be a finite Abelian group. Then,*

$$m \mid |G| \implies \exists H \leq G : |H| = m.$$

**Note 11.4.** Corollary 11.1.1 shows that the converse of Lagrange's Theorem is true for finite Abelian groups. Suppose  $G$  is Abelian,  $|G| = 72$ , and one wishes to produce a  $H \leq G, |H| = 12$ . By the Fundamental Theorem, since  $|G| = 72 = 2^3 3^2$ , the possible isomorphism classes for Abelian groups of order  $2^3$  and  $3^2$  are

$$\begin{array}{ll} k = 3, & \mathbb{Z}_8, \\ = 2 + 1, & \mathbb{Z}_4 \oplus \mathbb{Z}_2, \\ = 1 + 1 + 1, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2. \end{array}$$

and

$$\begin{array}{ll} k = 2, & \mathbb{Z}_9, \\ = 1 + 1, & \mathbb{Z}_3 \oplus \mathbb{Z}_3, \end{array}$$

respectively. Hence,  $G$  is isomorphic to one of the following groups,

$$\begin{array}{ll} \mathbb{Z}_8 \oplus \mathbb{Z}_9, & \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9, & \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3. \end{array}$$

By Corollary 11.1.1, since  $12 \mid 72$ , it follows that  $\mathbb{Z}_8 \oplus \mathbb{Z}_9 \approx \mathbb{Z}_{72}$  and  $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_{12} \oplus \mathbb{Z}_6$  have a subgroup of order 12. To construct a subgroup of order 12 in  $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$ , one simply pieces together all of  $\mathbb{Z}_4$  and the subgroup of order 3 in  $\mathbb{Z}_9$ ; that is,

$$\{(a, 0, b) : a \in \mathbb{Z}_4, b \in \{0, 3, 6\}\}.$$

An analogous procedure applies to the remaining cases and to any finite Abelian group.

### 11.3 Proof of the Fundamental Theorem

**Note 11.5.** The proof of the Fundamental Theorem is long and complex so it will be broke down into a series of lemmas.

**Lemma 11.1.** *Let  $G$  be a finite Abelian group,  $|G| = p^n m$ , where  $p$  is a prime,  $p \nmid m$ . Then  $G = H \times K$ , where  $H = \{x \in G : x^{p^n} = e\}$ ,  $K = \{x \in G : x^m = e\}$ . Moreover,  $|H| = p^n$ .*

*Proof.* Let  $G$  be a finite Abelian group,  $|G| = p^n m$ , where  $p$  is a prime,  $p \nmid m$ .  
Let  $H = \{x \in G : x^{p^n} = e\}$ ,  $K = \{x \in G : x^m = e\}$ .

By Definition 9.2,

$$H, K \triangleleft G, G = HK, H \cap K = \{e\} \implies G = H \times K.$$

By One-Step Subgroup Test,

$$H \subseteq G, a, b \in H, ab^{-1} \in H \implies H \leq G.$$

Let  $a, b \in H$  and  $c, d \in K$ . Then since  $G$  is Abelian,

$$\begin{aligned} (ab^{-1})^{p^n} &= a^{p^n} (b^{-1})^{p^n} \\ &= a^{p^n} (b^{p^n})^{-1} \\ &= ee^{-1} \\ &= e \\ \therefore ab^{-1} &\in H, \end{aligned}$$

and

$$\begin{aligned} (cd^{-1})^m &= c^m (d^{-1})^m \\ &= c^m (d^m)^{-1} \\ &= ee^{-1} \\ &= e \\ \therefore cd^{-1} &\in K. \end{aligned}$$

Hence,

$$ab^{-1} \in H, cd^{-1} \in K \implies H, K \leq G.$$

By Theorem 9.1,

$$H \leq G, \forall x \in G, xHx^{-1} \subseteq G \implies H \triangleleft G.$$

Let  $x \in G, h \in H, k \in K$ . Let  $xhx^{-1} \in xHx^{-1}, xkx^{-1} \in xKx^{-1}$ , then

$$\begin{aligned} (xhx^{-1})^{p^n} &= x^{p^n} h^{p^n} (x^{-1})^{p^n} \\ &= x^{p^n} h^{p^n} (x^{p^n})^{-1} \\ &= x^{p^n} e (x^{p^n})^{-1} \\ &= x^{p^n} (x^{p^n})^{-1} \\ &= e, \\ \therefore xhx^{-1} &\in H \implies xHx^{-1} \subseteq H, \end{aligned}$$



and

$$\begin{aligned}
(xkx^{-1})^m &= x^m k^m (x^{-1})^m \\
&= x^m k^m (x^m)^{-1} \\
&= x^m e (x^m)^{-1} \\
&= x^m (x^m)^{-1} \\
&= e, \\
\therefore xkx^{-1} \in K &\implies xKx^{-1} \subseteq K.
\end{aligned}$$

Hence,

$$H \triangleleft G, K \triangleleft G \iff \forall x \in G, xHx^{-1} \subseteq H, xKx^{-1} \subseteq K.$$

By Theorem 0.2,

$$\forall a, b \in \mathbb{Z}, a \neq 0, b \neq 0, \exists s, t \in \mathbb{Z} : \gcd(a, b) = as + bt.$$

Since  $p \nmid m$ ,

$$\gcd(m, p^n) = 1 = sm + tp^n, s, t \in \mathbb{Z}.$$

Let  $x \in G$ . Then

$$x = x^1 = x^{sm+tp^n} = x^{sm} x^{tp^n}.$$

By Corollary 7.1.4,

$$|G| = n, a \in G \implies a^{|G|} = e.$$

Since  $|G| = p^n m, x \in G$ , it follows that

$$\begin{aligned}
x^s \in G &\implies (x^{sm})^{p^n} = (x^s)^{p^n m} = e, \\
&\therefore x^{sm} \in H, \\
x^t \in G &\implies (x^{tp^n})^m = (x^t)^{p^n m} = e, \\
&\therefore x^{tp^n} \in K.
\end{aligned}$$

Hence,  $x \in HK \implies G \subseteq HK$ . Let  $hk \in HK, h \in H, k \in K$ . Then

$$h \in G, k \in G \implies hk \in G.$$

Hence,  $HK \subseteq G$  and therefore  $G = HK$ .

Let  $x \in H \cap K$ . By Corollary 4.1.2,

$$a \in G, a^k = e \iff |a| \mid k.$$

Since  $x \in H \cap K$ , it follows that  $x \in H, x \in K$  and

$$x^{p^n} = e, x^m = e \iff |x| \mid p^n, |x| \mid m.$$

Since  $1 = sp^n + tm$ , it follows that

$$|x| \mid 1 \implies |x| = 1.$$

Hence  $x = e$  and  $H \cap K = \{e\}$ . Therefore,  $G = H \times K$ .

By Theorem 7.2,

$$H, K \leq G \implies |HK| = |H||K|/|H \cap K|.$$

Hence

$$\begin{aligned} p^n m = |G| &= |HK| \\ &= |H||K|/|H \cap K| \\ &= |H||K|/1 \\ &= |H||K|. \end{aligned}$$

By Lemma 0.1,

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

It follows that

$$p \mid p^n m = |H||K| \implies p \mid |H| \text{ or } p \mid |K|.$$

If  $p \mid |K|$ , then by Theorem 9.5,

$$p \mid |G| \implies \exists x \in G : |x| = p.$$

Hence

$$p \mid |K| \implies \exists x \in K : |x| = p.$$

By Corollary 4.1.2,

$$x \in K, x^m = e \iff |x| = p \mid m.$$

But  $p \nmid m$ . Hence  $p \nmid |K| \implies p \mid |H|$ . Therefore  $|H| = p^n$ .  $\square$

**Note 11.6.** Given an Abelian group  $G$ ,  $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ , where  $p_i$ 's are distinct primes. Let  $G(p_i) = \{x \in G : x^{p_i^{n_i}} = e\}$ . Then by Lemma 11.1 and induction,

$$G = G(p_1) \times G(p_2) \times \cdots \times G(p_k), |G(p_i)| = p_i^{n_i}.$$

**Lemma 11.2.** Let  $G$  be an Abelian group,  $|G| = p^n$ . Then

$$a \in G \text{ is a maximal order element} \implies G = \langle a \rangle \times K, K \leq G.$$

*Proof.* Let  $G$  be an Abelian group,  $|G| = p^n$ .

By induction, let  $n = 1$ , then  $|G| = p$ . Let  $a \in G$  be a maximal order element. By Lagrange's Theorem,

$$\langle a \rangle \leq G \implies |a| = |\langle a \rangle| \mid |G| = p.$$

Hence  $|a| \in \{1, p\}$ . Since by definition,  $a$  is a maximal order element, therefore

$$|a| = p = |G| \implies G = \langle a \rangle = \langle a \rangle \times \langle e \rangle.$$

Hence the statement is true for  $n = 1$ . Next, assume that the statement is true for  $1 \leq k < n$ .

Let  $a \in G$  be the maximal order element,  $|a| = p^m$ . Then  $\forall x \in G, |x| = p^s \mid p^m, 1 \leq s \leq m$ . Therefore by Theorem 4.1.2,

$$x^{p^m} = x^{p^s} = e \iff p^s \mid (p^m - p^s).$$

Hence  $\forall x \in G, x^{p^m} = e$ . If  $G = \langle a \rangle$ , then  $G = \langle a \rangle \times \langle e \rangle, \langle e \rangle \leq G$ . The proof is completed. If  $G \neq \langle a \rangle$ . Let  $b \in G, b \notin \langle a \rangle$  be the smallest order element. By Theorem 4.2.2,

$$|b^p| = |b| / \gcd(|b|, p) = |b|/p.$$

By the manner in which  $b$  was chosen, it follows that  $b^p \in \langle a \rangle$ . (cont.) □

**Lemma 11.3.** *Let  $G$  be an Abelian group,  $|G| = p^n$ . Then*

$$G = H_1 \times H_2 \times \cdots \times H_k,$$

*where  $H_i$ 's are cyclic.*

**Note 11.7.** By Lemma 11.1 and Note 11.6,

$$G = G(p_1) \times G(p_2) \times \cdots \times G(p_k), |G(p_i)| = p_i^{n_i}.$$

By Lemma 11.3,

$$G(p_i) = H_1 \times H_2 \times \cdots \times H_k,$$

where  $H_i$ 's are cyclic. Hence  $G$  is an internal direct product of cyclic groups of prime order. Since

$$G(p_i) = \{x \in G : x^{p_i^{n_i}} = e\},$$

the groups  $G(p_i)$  are uniquely determined by  $G$ .

**Lemma 11.4.** *Let  $G$  be an Abelian group,  $|G| = p^n$ . If*

$$G = H_1 \times H_2 \times \cdots \times H_m \text{ and } G = K_1 \times K_2 \times \cdots \times K_n,$$

*where  $H_i, K_i$  are nontrivial cyclic subgroups with*

$$|H_1| \geq |H_2| \geq \cdots \geq |H_m| \text{ and } |K_1| \geq |K_2| \geq \cdots \geq |K_n|,$$

*then  $m = n$  and  $|H_i| = |K_i|$ .*

*Proof.* □

## 12 Introduction to Rings

### 12.1 Motivation and Definition

**Definition 12.1** (Ring). A *ring*  $R$  is a set with two binary operations, addition and multiplication, such that  $\forall a, b, c \in R$ :

1.  $a + b = b + a$ .
2.  $(a + b) + c = a + (b + c)$ .
3. There is an additive identity  $0 \in R : \forall a \in R, a + 0 = a$ .
4.  $\forall a \in R, \exists -a \in R : a + (-a) = 0$ .
5.  $a(bc) = (ab)c$ .
6.  $a(b + c) = ab + ac$  and  $(b + c)a = ba + ca$ .

**Note 12.1.** So,  $R$  is an Abelian group under addition, also having an associative multiplication that is left and right distributive over addition. Note that multiplication need not be commutative. If  $ab = ba$ , then  $R$  is *commutative*. Also,  $R$  need not have an identity under multiplication. If  $e \in R, e \neq 0 : \forall a \in R, ea = ae = a$ , then  $e$  is a *unity* (or *identity*). A nonzero element of a commutative ring with unity need not have a multiplicative inverse. When it does, it is a *unit* of the ring. Thus, if  $a^{-1} \in R$ , then  $a \in R$  is a unit.

Let  $a, b \in R, a \neq 0$ ,  $R$  is commutative. If  $\exists c \in R : b = ac$ , then  $a$  *divides*  $b$  (or  $a$  is a *factor* of  $b$ ) and  $a \mid b$ . If  $a$  does not divide  $b$ , then  $a \nmid b$ .

Recall that if  $a \in G$  under addition and  $n \in \mathbb{Z}^+$ ,  $na = a + a + \cdots + a$  ( $n$  summands). When dealing with rings, this notation can cause confusion, since one also use juxtaposition for the ring multiplication. When there is the potential for confusion, one will use  $n \cdot a = a + a + \cdots + a$  ( $n$  summands).

### 12.2 Examples of Rings

**Example 12.1.**  $\mathbb{Z}$  under addition and multiplication is a commutative ring with unity 1. The units of  $\mathbb{Z}$  are 1 and -1.

**Example 12.2.**  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  under addition and multiplication modulo  $n$  is a commutative ring with unity 1. The set of units is  $U(n)$ .

**Example 12.3.** The set  $\mathbb{Z}[x]$  of all polynomials in the variable  $x$  with integer coefficients under addition and multiplication is a commutative ring with unity  $f(x) = 1$ .

**Example 12.4.** The set  $M_2(\mathbb{Z})$  of  $2 \times 2$  matrices with integers entries is a noncommutative ring with unity  $I$ .

**Example 12.5.** The set  $2\mathbb{Z}$  of even integers under addition and multiplication is a commutative ring without unity.

**Example 12.6.** The set of all continuous real-valued functions of a real variable whose graphs pass through the point  $(1,0)$  is a commutative ring without unity under the operations of pointwise addition and multiplication, i.e.  $(f+g)(a) = f(a) + g(a)$  and  $(fg)(a) = f(a)g(a)$ .

**Example 12.7.** Let  $R_1, R_2, \dots, R_n$  be rings. These rings can be used to construct a new ring as follows. Let

$$R_1 \oplus R_2 \oplus \dots \oplus R_n = \{(a_1, a_2, \dots, a_n) : a_i \in R_i\}$$

and define

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

and

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_n).$$

Then  $R_1 \oplus R_2 \oplus \dots \oplus R_n$  is a ring called the *direct sum* of  $R_1, R_2, \dots, R_n$ .

### 12.3 Properties of Rings

**Note 12.2.**  $b - c$  denotes  $b + (-c)$ .

**Theorem 12.1** (Rules of Multiplication). *Let  $R$  be a ring,  $a, b, c \in R$ . Then*

1.  $a0 = 0a = 0$ .
2.  $a(-b) = (-a)b = -(ab)$ .
3.  $(-a)(-b) = ab$ .
4.  $a(b - c) = a(b + (-c)) = ab - ac$  and  $(b - c)a = (b + (-c))a = ba - ca$ .

*Futhermore, if  $R$  has a unity element 1, then*

5.  $(-1)a = -a$ .
6.  $(-1)(-1) = 1$ .

*Proof.* Let  $R$  be a ring,  $a, b, c \in R$ .

1. By Definition 12.1.6,

$$0 + a0 = a0 = a(0 + 0) = a0 + a0.$$

By cancellation,

$$\begin{aligned} 0 + a0 + (-a0) &= a0 + a0 + (-a0) \\ 0 &= a0. \end{aligned}$$

Similarly,

$$\begin{aligned} 0 + 0a &= 0a = (0 + 0)a = 0a + 0a \\ 0 + 0a + (-0a) &= 0a + 0a + (-0a) \\ 0 &= 0a. \end{aligned}$$

Hence,  $a0 = 0a = 0$ .

2. By Definition 12.1.6,

$$\begin{aligned} a(-b) + ab &= a(-b + b) = a0 = 0 \\ a(-b) + ab + (-ab) &= 0 + (-ab) \\ a(-b) &= -(ab). \end{aligned}$$

Similarly,

$$\begin{aligned} (-a)b + ab &= (-a + a)b = 0b = 0 \\ (-a)b + ab + (-ab) &= 0 + (-ab) \\ (-a)b &= -(ab). \end{aligned}$$

Hence,  $a(-b) = (-a)b = -(ab)$ .

3. By Definition 12.1.6 and Theorem 12.1.1,

$$\begin{aligned} (-a)(-b) + (-ab) &= -a(-b + b) = -a0 = 0 \\ (-a)(-b) + (-ab) + ab &= 0 + ab \\ (-a)(-b) + (-a + a)b &= ab \\ (-a)(-b) + (-a + a)b &= ab \\ (-a)(-b) + 0b &= ab \\ (-a)(-b) + 0 &= ab \\ \therefore (-a)(-b) &= ab. \end{aligned}$$

4. By Definition 12.1.6 and Theorem 12.1.2,

$$\begin{aligned} a(b - c) &= a(b + (-c)) \\ &= ab + a(-c) \\ &= ab - ac. \end{aligned}$$

Similarly,

$$\begin{aligned} (b - c)a &= (b + (-c))a \\ &= ba + (-c)a \\ &= ba - ca. \end{aligned}$$

Assume that  $1 \in R$ , then

5. By Theorem 12.1.2,  $(-1)a = -(1a) = -a$ .
6. By Theorem 12.1.3,  $(-1)(-1) = (1)(1) = 1$ .

□

**Theorem 12.2** (Uniqueness of the Unity and Inverses). *Let  $R$  be a ring. Then*

1.  *$R$  has a unity  $\implies$  it is unique.*
2.  *$a \in R, a^{-1} \in R \implies a^{-1} \in R$  is unique.*

*Proof.* Let  $R$  be a ring.

1. Assume that  $\exists e_1, e_2 \in R : e_1a = ae_2 = a$  and  $e_2a = ae_2 = a$ . Then

$$e_1e_2 = e_2e_1 = e_1 \text{ and } e_2e_1 = e_1e_2 = e_2.$$

Hence  $e_1 = e_2e_2 = e_2e_1 = e_2$ .

2. Assume that  $a \in R, \exists a_1, a_2 \in R : a_1a = aa_1 = e$  and  $a_2a = aa_2 = e$ . Then

$$\begin{array}{ll} a_1a = a_2a & aa_1 = aa_2 \\ a_1aa_1 = a_2aa_1 & a_1aa_1 = a_1aa_2 \\ a_1e = a_2e & ea_1 = ea_2 \\ a_1 = a_2, & a_1 = a_2. \end{array}$$

□

## 12.4 Subrings

**Definition 12.2** (Subring).  $S \subseteq R$  is a *subring of  $R$*  if  $S$  is a ring with the operations of  $R$ .

**Theorem 12.3** (Subring Test). *Let  $R$  be a ring,  $S \subseteq R, S \neq \emptyset$ . Then*

$$a, b \in S, a - b, ab \in S \implies S \text{ is a subring of } R.$$

*Proof.* Let  $R$  be a ring,  $S \subseteq R, S \neq \emptyset$ .

Assume that  $a, b \in S, a - b, ab \in S$ . Since  $R$  is a ring and  $S \subseteq R$ , by One-Step Subgroup test,

$$a, b \in S, a - b \in S \implies S \leq R.$$

So  $S$  is closed under addition,  $0 \in S$ , and  $\forall a \in S, \exists -a \in S : a + (-a) = 0$ . Hence addition is a binary operation in  $S$  and  $S$  fulfills property 1 to 4 in Definition 12.1.

Since  $S \subseteq R$  and  $a, b \in S, ab \in S$ , it follows that multiplication is a binary operation in  $S$  and  $S$  fulfills property 5 and 6 of Theorem 12.1.

Hence by Definition 12.1,  $S$  is a subring of  $R$ .  $\square$

**Example 12.8.**  $\{0\}$  and  $R$  are subrings of any ring  $R$ .

Since  $\{0\} \subseteq R, \{0\} \neq \emptyset, 0 - 0, 00 \in \{0\}$ , by Theorem 12.3,  $\{0\}$  is a subring of  $R$ .

Since  $R \subseteq R, 0 \in R \implies R \neq \emptyset, a, b \in R, a - b, ab \in R$ , by Theorem 12.3,  $R$  is a subring of  $R$ .

**Example 12.9.**  $\{0, 2, 4\}$  is a subring of the ring  $\mathbb{Z}_6$ .

Since  $\{0, 2, 4\} \subseteq \mathbb{Z}_6, \{0, 2, 4\}$ , and

$$\begin{aligned} 0 + 0 &= 2 + 4 = 4 + 2 = 0, & 0(0) &= 0(2) = 0(4) = 2(0) = 4(0) = 0, \\ 0 + 2 &= 2 + 0 = 4 + 4 = 2, & 2(2) &= 4(4) = 4, \\ 0 + 4 &= 2 + 2 = 4 + 0 = 4, & 2(4) &= 4(2) = 2, \end{aligned}$$

by Theorem 12.3,  $\{0, 2, 4\}$  is a subgroup of  $\mathbb{Z}_6$ .

Note that although 1 is the unity in  $\mathbb{Z}_6$ , 4 is the unity in  $\{0, 2, 4\}$ .

**Example 12.10.** For each  $n \in \mathbb{Z}^+$ , the set

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$$

is a subring of  $\mathbb{Z}$ .

Since  $n\mathbb{Z} \subseteq \mathbb{Z}, 0 \in n\mathbb{Z} \implies n\mathbb{Z} \neq \emptyset$ , and

$$a, b \in n\mathbb{Z}, a - b, ab \in n\mathbb{Z},$$

By Theorem 12.3,  $n\mathbb{Z}$  is a subring of  $\mathbb{Z}$ .

**Example 12.11.** The set of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

is a subring of  $\mathbb{C}$ .

Since  $\mathbb{Z}[i] \subseteq \mathbb{C}, 0 \in \mathbb{Z}[i] \implies \mathbb{Z}[i] \neq \emptyset$ , and since  $\mathbb{C}, \mathbb{Z}$  are rings,  $a + bi, c + di \in \mathbb{Z}[i]$ ,

$$(a + bi) + (c + di) = (a + b) + (c + d)i \in \mathbb{Z}[i],$$

and

$$\begin{aligned} (a + bi)(c + di) &= (a + bi)c + (a + bi)(di) \\ &= ac + bci + adi - bd \\ &= (ac - bd) + (ad + bc)i \in \mathbb{Z}[i], \end{aligned}$$

by Theorem 12.3,  $\mathbb{Z}[i]$  is a subring of  $\mathbb{C}$ .

**Example 12.12.** Let  $R$  be the ring of all real-valued functions of a single real variable under pointwise addition and multiplication. The subset  $S \subseteq R$  of functions whose graphs pass through the origin forms a subring of  $R$ .



**Example 12.13.** The set

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{Z} \right\}$$

is a subring of the ring of all  $2 \times 2$  matrices over  $\mathbb{Z}$ .

**Note 12.3.** The relationship between a ring and its various subrings can be depicted as a subring lattice diagram (Figure 12.1). In such a diagram, any ring is a subring of all the rings that it is connected to by one or more upward lines.

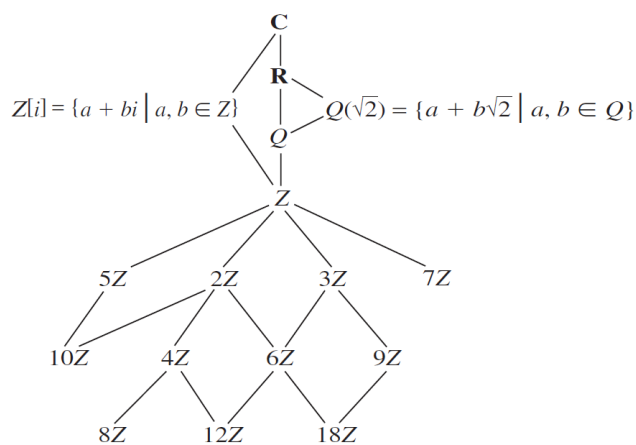


Figure 12.1