

# GROUP THEORY

AMIN WITNO

## Preface

Written at Philadelphia University, Jordan for Math 342 and Math 442, these notes<sup>1</sup> were used first time in the Spring 2007 semester. They have since been revised<sup>2</sup> and shall be revised again as often as the author teaches the course. Outline notes are more like a revision. No student is expected to fully benefit from these notes unless they have regularly attended the lectures.

## 1 Introduction

By a *binary operation*  $\star$  on a set we mean a function taking each ordered pair  $a, b$  to another element in the set which shall be denoted by  $a \star b$ . The word *ordered* here means that in general  $a \star b \neq b \star a$ .

*Definition.* A *group*  $G$  is a set together with a binary operation  $\star$  on  $G$  which satisfies the following three axioms.

- 1) For every elements  $a, b, c \in G$ ,  $a \star (b \star c) = (a \star b) \star c$ .
- 2) There exists  $e \in G$  such that  $a = a \star e = e \star a$  hold for every element  $a \in G$ .
- 3) For each element  $a \in G$  there exists  $b \in G$  satisfying  $a \star b = b \star a = e$ .

*Remark.* Condition (1) in other words says that the operation  $\star$  is *associative*. An element  $e$  satisfying condition (2) is called an *identity element* of  $G$ . We shall soon see that a group has exactly one identity element. For (3) we call  $b$  an *inverse* of  $a$  in  $G$ . We shall also prove that every  $a \in G$  has a unique inverse.

*Example.* We give several examples of what a group might look like.

- 1) The set of integers  $\mathbb{Z}$  together with ordinary addition, which we know associative, is a group. The number  $e = 0$  is an identity element of  $\mathbb{Z}$  and an inverse of any integer  $a$  is  $-a$ .

Similarly also, under addition, the following sets each form a group: the rational numbers  $\mathbb{Q}$ , the real numbers  $\mathbb{R}$ , and the complex numbers  $\mathbb{C}$ . From now on we

---

<sup>1</sup>Copyrighted under a Creative Commons License

<sup>2</sup>Last Revision: 27-01-2009

shall simply say *the group*  $\mathbb{Z}$ , referring to the group of integers under addition; and likewise with the groups  $\mathbb{Q}$ ,  $\mathbb{R}$ , and  $\mathbb{C}$ .

- 2) The set of non-zero rational numbers  $\mathbb{Q}^*$  is a group under the usual multiplication. Its identity element is  $e = 1$  and each non-zero rational number  $a/b$  has inverse  $b/a$ . So do we have the groups  $\mathbb{R}^*$  and  $\mathbb{C}^*$  of non-zero numbers, respectively real and complex, under multiplication. However, note that  $\mathbb{Z}^*$ , the set of non-zero integers, is not a group under multiplication because, for instance, 2 has no inverse in it. (Explain!) Henceforth the groups  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$ , and  $\mathbb{C}^*$  are always understood under multiplication and with the number 0 discarded.
- 3) The set  $\{0\}$  under addition is a group where 0 is the identity and only element of  $G$ . Essentially this is the only kind of a group with one element, denoted by  $G = \{e\}$  and it is called the *trivial group*.
- 4) We can have a group with two elements,  $G = \{e, a\}$  where  $e$  is identity and where the binary operation is defined by  $a \star a = e$ . You can check that it does satisfy the three axioms of a group.
- 5) The set  $M(2, \mathbb{R})$  of  $2 \times 2$  matrices with real entries is a group under matrix addition. Can you identify the identity element and the inverse of  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{R})$ ?

Similarly the set  $M(n, S)$  of  $n \times n$  matrices over  $S$  under matrix addition forms a group, where  $S$  may be the set of integers, rationals, or complex numbers.

- 6) The set  $GL(2, \mathbb{R})$  of  $2 \times 2$  matrices with non-zero determinants is also a group under matrix multiplication. We know from linear algebra that matrix multiplication is associative. The identity element here is  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , and recall that having a non-zero determinant is equivalent to being invertible.

*Definition.* We call the binary operation  $\star$  *commutative* if  $a \star b = b \star a$  for all. In that case the group  $G$  is called *abelian*. The examples given above are all abelian groups, except the last one is non-abelian since matrix multiplication is not commutative.

**Proposition 1.1.** Let  $G$  be a group with a given binary operation.

- 1) There is exactly one identity element in  $G$ .
- 2) Each  $a \in G$  has a unique inverse in  $G$ .

*Proof.* Suppose there were two identity elements,  $e$  and  $f$ . Then  $e \star f = f$  since  $e$  is identity, while at the same time  $e \star f = e$  as  $f$  is identity. Hence  $e = f$ . This proves (1). For (2) assume  $a$  had two inverses  $b$  and  $c$ . Then  $a \star b = a \star c = e$ . Operate both sides by  $b$  from the left and then apply associativity to get

$$\begin{aligned} b \star (a \star b) &= b \star (a \star c) \\ (b \star a) \star b &= (b \star a) \star c \\ e \star b &= e \star c \\ b &= c \end{aligned}$$

This shows that  $a$  can have only one inverse. ▽

*Remark.* From now on we use the phrase *the* identity element, denoted by  $e$ , and *the* inverse of an element  $a$ , denoted by  $a^{-1}$ . Moreover for convenience we write  $ab$  instead of  $a \star b$ , unless sometimes when the operation is actually addition then we write  $a + b$  in order to avoid ambiguity. (Also, when using addition, it is better to keep the notation for inverse as  $-a$  instead of  $a^{-1}$ .) By associativity we may then write the product  $abc$  without ambiguity, which generalizes to any finite number of elements,  $a_1 a_2 a_3 \cdots a_n$ , without the necessity of brackets.

**Proposition 1.2.** For any elements of a group the following statements hold.

- 1)  $(a^{-1})^{-1} = a$
- 2)  $(ab)^{-1} = b^{-1}a^{-1}$
- 3)  $ab = ac$  implies  $b = c$
- 4)  $ba = ca$  implies  $b = c$

*Remark.* Properties (3) and (4) above are known by the name *left* and *right cancellation laws*, respectively. We should not assume that cancellation laws always apply unless we know that we are dealing with group elements. We have, for example,

$$\begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 4 & 8 \end{pmatrix}$$

seemingly contradicting (4). Can you account for this false counter-example?

**Theorem 1.3.** If  $G$  and  $H$  are two groups, with their respective binary operations, then the set  $G \times H = \{(g, h) \mid g \in G, h \in H\}$  is a group under the operation defined by  $(g, h)(g', h') = (gg', hh')$ . The name for this group is the *direct product* of  $G$  and  $H$ .

### Exercise 1

- 1) Prove Proposition 1.2.
- 2) Prove Theorem 1.3.
- 3) Let  $G$  be a group. Prove that  $G$  is abelian if and only if, for all the elements of  $G$ , any one of the following properties holds.
  - a)  $ab = ca$  implies  $b = c$
  - b)  $axb = cxd$  implies  $ab = cd$
  - c)  $(ab)^2 = a^2b^2$
  - d)  $(ab)^{-1} = a^{-1}b^{-1}$
- 4) Prove that if  $a^2 = e$  for every element  $a$  in a group  $G$  then  $G$  is abelian.

## 2 The Group $\mathbb{Z}_n$

This section is devoted to the presentation of a group with a finite number of elements, called the modular integers. We assume a knowledge from set theory concerning an equivalence relation and its equivalence classes.

*Definition.* Fix an integer  $n > 0$ . Define two integers  $a, b$  to be *congruent mod  $n$*  when  $a - b = nk$  for some integer  $k$ . We denote this relation by  $a \equiv b \pmod{n}$  and show that it is an equivalence relation over  $\mathbb{Z}$ :

- 1) *reflexive*:  $a \equiv a \pmod{n}$  since  $a - a = nk$  with  $k = 0$ .
- 2) *symmetric*:  $a \equiv b \pmod{n}$  implies  $b \equiv a \pmod{n}$  because  $a - b = nk$  implies  $b - a = nh$  with  $h = -k$ .
- 3) *transitive*:  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$  imply  $a \equiv c \pmod{n}$  because  $a - b = nk$  and  $b - c = nh$  imply  $a - c = a - b + b - c = nj$  with  $j = k + h$ .

Now let the equivalence classes under this relation be called *congruence classes*, where for each  $a \in \mathbb{Z}$  we denote its congruence class by

$$\begin{aligned} [a]_n &= \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} \\ &= \{b \in \mathbb{Z} \mid b - a = nk\} \\ &= \{nk + a \mid k \in \mathbb{Z}\} \end{aligned}$$

The following results follow from the fact about equivalence classes.

- 1)  $a \in [a]_n$  for each  $a \in \mathbb{Z}$ , and  $b \in [a]_n$  if and only if  $a \equiv b \pmod{n}$ .
- 2)  $[a]_n = [b]_n$  if and only if  $a \equiv b \pmod{n}$ .
- 3)  $[a]_n \cap [b]_n = \phi$  if and only if  $a \not\equiv b \pmod{n}$ .
- 4)  $\bigcup \{[a]_n \mid a \in \mathbb{Z}\} = \mathbb{Z}$ .

It also means that each integer belongs to exactly one congruence class, or that the congruence classes form a partition for the set  $\mathbb{Z}$ . Now we will be interested in knowing how many distinct congruence classes we have. For that we assume the following principle, called the *Division Algorithm*.

**Theorem 2.1** (The Division Algorithm in  $\mathbb{Z}$ ). Given two integers  $a$  and  $n > 0$  there exist integers  $q$  and  $r$  such that  $a = qn + r$  and  $0 \leq r < n$ .

This principle is really what we call the long division method of dividing an integer by another. For example dividing 47 by 5 gives us 9 (*quotient*) and *remainder* 2, hence  $47 = 9 \cdot 5 + 2$ . This remainder  $r$  clearly has to be smaller than the *divisor*  $n$ , else the long division process must continue. In particular  $r = 0$  if and only if  $a = nk$  for some  $k \in \mathbb{Z}$ , and  $a \equiv 0 \pmod{n}$ . More generally, following the above theorem, we have  $a \equiv r \pmod{n}$ .

**Proposition 2.2.** For a given  $n > 0$  there are exactly  $n$  congruence classes of  $\mathbb{Z}$  given by  $[0]_n, [1]_n, [2]_n, \dots, [n-1]_n$ .

*Proof.* By the Division Algorithm, each integer  $a$  belongs to one of these classes, hence there are at most  $n$  of them. To complete the proof we show that these  $n$  classes are all distinct. If it were not so then two of them, say  $0 \leq i < j \leq n-1$  satisfy the relation  $i \equiv j \pmod{n}$ , or  $j - i = nk$ , impossible as  $1 \leq j - i \leq n-1$ .  $\square$

*Definition.* The set of *modular integers*  $\mathbb{Z}_n$  is the set consisting of the  $n$  congruence classes under congruence mod  $n$ :

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$$

Next define a binary operation  $+$  on this set, called *addition mod  $n$* , by letting

$$[a]_n + [b]_n = [a + b]_n$$

We have to show first that this is well-defined, meaning that different choices of  $a, b$  for the same classes  $[a]_n, [b]_n$  should not yield a different sum. This follows since  $[a]_n = [a']_n$  and  $[b]_n = [b']_n$  imply  $a - a' = nk$  and  $b - b' = nh$  hence  $(a + b) - (a' + b') = n(k + h)$ , meaning that  $a + b \equiv a' + b' \pmod{n}$ , and therefore

$$[a']_n + [b']_n = [a' + b']_n = [a + b]_n = [a]_n + [b]_n$$

We are now ready to prove the main result.

**Theorem 2.3.** The set  $\mathbb{Z}_n$  is an abelian group under addition mod  $n$ .

*Proof.* The commutative property is inherited from the ordinary addition used in the definition. From the requirements to be a group, we verify:

- 1) For every three classes,  $[a]_n + ([b]_n + [c]_n) = [a]_n + [b + c]_n = [a + (b + c)]_n = [(a + b) + c]_n = [a + b]_n + [c]_n = ([a]_n + [b]_n) + [c]_n$ .
- 2) The identity element of  $\mathbb{Z}_n$  is  $[0]_n$  since  $[a]_n + [0]_n = [a + 0]_n = [a]_n$  for all  $[a]_n \in \mathbb{Z}_n$ .
- 3) For each  $[a]_n \in \mathbb{Z}_n$ , we have  $-[a]_n = [-a]_n$  since  $[a]_n + [-a]_n = [a - a]_n = [0]_n$ .  $\nabla$

*Remark.* From now on, we shall simplify the notations quite drastically. We write  $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$  to really mean that each element is a modular integer, that is a congruence class mod  $n$  (which is an infinite set of integers!). From now on let us agree that *the group  $\mathbb{Z}_n$*  refers to this group of modular integers under addition mod  $n$ .

*Example.* With  $n = 4$  we have  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$  where the addition mod 4 produces the following *multiplication table*—just a name, despite the fact that the operation here is addition! To avoid confusion, a multiplication table is better called a *Cayley table*.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

To avoid ambiguity, instead of writing  $2 + 3 = 1$  (which really means  $[2]_4 + [3]_4 = [5]_4$ ) we may sometimes write  $2 +_4 3 = 1$  or alternatively  $2 + 3 \equiv 1 \pmod{4}$ .

### 3 The Group $U_n$

We continue with the example of  $\mathbb{Z}_n$  but this time we introduce a different operation: *multiplication mod  $n$* . For  $[a]_n, [b]_n \in \mathbb{Z}_n$  we define  $[a]_n[b]_n = [ab]_n$ . As before we show first that this is well-defined. Let  $[a]_n = [a']_n$  and  $[b]_n = [b']_n$ . Then  $a = a' + nk$  and  $b = b' + nh$ , hence  $ab = a'b' + n(a'h + b'k + nkh)$ , that is  $ab \equiv a'b' \pmod{n}$ . Thus

$$[a']_n[b']_n = [a'b']_n = [ab]_n = [a]_n[b]_n$$

Once again we return to the simplified notation  $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$ . For example with  $n = 4$  we have  $2 \cdot 3 \equiv 2 \pmod{4}$ . The table of multiplication mod 4 is given below.

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

We can see that in general 1 acts as identity, however  $\mathbb{Z}_n$  can never be a group as 0 has no inverse since  $0a = 0$  for all  $a \in \mathbb{Z}_n$ . We proceed now to find a subset of  $\mathbb{Z}_n$  which does form a group under multiplication mod  $n$ .

*Definition.* Two integers  $m, n$  are said to be *relatively prime* when they have no common factors larger than 1. For example 12 and 25 are relatively prime, but 12 and 27 are not since they have a common factor of 3.

**Lemma 3.1.** The integers  $m, n$  are relatively prime if and only if  $mx + ny = 1$  for some integers  $x, y$ .

*Proof.* Let  $d$  be a common factor of  $m$  and  $n$ . This means that both  $m/d$  and  $n/d$  are integers, hence the quantity  $mx + ny$  is a multiple of  $d$  for any integers  $x, y$ . In particular if  $mx + ny = 1$  then  $d$  divides 1, hence  $d = \pm 1$  and  $m, n$  are relatively prime.

Conversely suppose  $m, n$  are relatively prime. Let  $L = \{mx + ny \mid x, y \in \mathbb{Z}\}$  and let  $c = mx_0 + ny_0$  be the least positive element in  $L$ . We claim that  $c$  divides  $m$ . To see why, use the Division Algorithm:  $m = qc + r$  with  $0 \leq r < c$ . Then  $r = m - qc = m - q(mx_0 + ny_0) = m(1 - qx_0) + n(-qy_0) \in L$ . This is impossible as  $c$  is supposedly the least, unless  $r = 0$ . By symmetry we conclude that  $c$  divides  $n$  as well. Being a common factor of  $m$  and  $n$ , then  $c = 1$ , hence  $mx_0 + ny_0 = 1$ .  $\nabla$

Note that  $n$  is relatively prime to  $m$  if and only if  $n$  is relatively prime to every integer  $a \in [m]_n$ . This is true since if  $a = nk + m$  then  $mx + ny = 1$  if and only if  $ax + n(y - kx) = 1$ .

**Corollary 3.2.** The integers  $m, n$  are relatively prime if and only if there exists an integer  $b$  such that  $mb \equiv 1 \pmod{n}$ , in which case  $b$  is also relatively prime to  $n$ .

*Proof.* Note that the equation  $mx + ny = 1$  is equivalent to  $[m]_n[x]_n = [1]_n$  in  $\mathbb{Z}_n$ .  $\nabla$

**Lemma 3.3.** Suppose  $n$  is relatively prime both to  $m$  and to  $m'$ . Then  $n$  is relatively prime to  $mm'$ .

*Proof.* Let  $mx + ny = 1$  and  $m'x' + ny' = 1$  for some integers  $x, y, x', y'$ . Multiply these two equations:

$$mm'(xx') + n(mxy' + m'x'y + nyy') = 1$$

and by the lemma this means  $mm'$  and  $n$  are relatively prime.  $\nabla$

*Definition.* Let  $U_n$  denote the subset of  $\mathbb{Z}_n$  consisting of the classes of  $m$  for which  $m$  is relatively prime to  $n$ . For example  $U_{10} = \{1, 3, 7, 9\}$ . We are now ready to show that this is the subset which forms a group under multiplication mod  $n$ .

**Theorem 3.4.** The set  $U_n$  is an abelian group under multiplication mod  $n$ .

*Proof.* The lemma shows that the product of two elements in  $U_n$  is again in  $U_n$ . Associativity and commutativity follow from those of ordinary multiplication used in the definition. The integer 1 is relatively prime to  $n$  and  $[1]_n$  is the identity element of  $U_n$ . Finally the lemma shows that each element of  $U_n$  has an inverse element.  $\nabla$

*Example.* The group  $U_{10} = \{1, 3, 7, 9\}$  has Cayley table given below.

$\times$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

*Remark.* The elements in  $\mathbb{Z}_n$  with a multiplicative inverse—those relatively prime to  $n$ —are otherwise called the *units* of  $\mathbb{Z}_n$ ; this reason yields the notation for  $U_n$ . Henceforth we simply say *the group*  $U_n$  to refer to this group of units in  $\mathbb{Z}_n$  where the operation is understood multiplication mod  $n$ .

**Lemma 3.5** (Euclid’s Lemma). If  $m, n$  are relatively prime and  $mk \equiv 0 \pmod{n}$  for some integer  $k$ , then  $k \equiv 0 \pmod{n}$ .

### Exercise 3

- 1) Find the inverse for each element in  $U_{11}$ .
- 2) Draw the Cayley table for  $U_{12}$ .
- 3) Prove the above Euclid’s lemma.
- 4) Suppose that  $m, n$  are relatively prime. Show that if  $k \equiv 0 \pmod{m}$  and  $k \equiv 0 \pmod{n}$  then  $k \equiv 0 \pmod{mn}$ .

## 4 Subgroups

*Definition.* A subset  $H$  of a group  $G$  is called a *subgroup* of  $G$  if  $H$  is itself a group under the same binary operation inherited from  $G$ .

*Example.* We illustrate the idea with several examples.

- 1) We know that the sets  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  are all groups under addition. In this case  $\mathbb{Z}$  is a subgroup of  $\mathbb{Q}$ , which is a subgroup of  $\mathbb{R}$ , which is a subgroup of  $\mathbb{C}$ .
- 2) The set  $\mathbb{Q}^*$  under multiplication is a group and a subgroup of  $\mathbb{R}^*$ . The subset  $\mathbb{Z}^*$  is not a subgroup of  $\mathbb{Q}^*$  because it is not a group under multiplication.
- 3) The subset  $2\mathbb{Z}$  of even numbers is a subgroup of  $\mathbb{Z}$  under addition. You can verify that adding two even numbers gives another even number, and that the three group axioms hold in  $2\mathbb{Z}$ .
- 4) The set  $\{1, -1\}$  forms a group under multiplication, so it is a subgroup of the group  $\mathbb{Q}^*$ . Although  $\{1, -1\}$  is also a subset  $\mathbb{Z}^*$ , it is not a subgroup of  $\mathbb{Z}^*$  because the latter is not a group under multiplication.
- 5) Every group is a subgroup of itself.
- 6) Every group has a *trivial subgroup* consisting of only the identity element  $\{e\}$ .
- 7) The subset  $U_n$  is not a subgroup of  $\mathbb{Z}_n$  even though both of them are groups, because they are defined with different binary operations.
- 8) The set  $M(2, \mathbb{Z})$  is a subgroup of  $M(2, \mathbb{R})$  under matrix addition.

- 9) The group  $GL(2, \mathbb{R})$  under matrix multiplication has a subgroup given by  $SL(2, \mathbb{R})$  consisting of  $2 \times 2$  matrices with determinant  $\pm 1$ .

**Lemma 4.1.** Let  $H$  be a subgroup of a group  $G$ .

- 1) The identity element of  $H$  is that of  $G$ .
- 2) For each  $a \in H$ , its inverse in  $H$  is the same  $a^{-1} \in G$ .

**Theorem 4.2.** A non-empty subset  $H$  of a group  $G$  is a subgroup if and only if  $ab^{-1} \in H$  whenever  $a, b \in H$ .

*Proof.* Necessity is clear. Suppose the required condition is satisfied in  $H$ . Associativity in  $H$  is inherited from  $G$ . There is at least one element  $a \in H$ , hence  $aa^{-1} = e \in H$ . This is the identity element in  $H$  according to the lemma. Also for each  $a \in H$  we have  $ea^{-1} = a^{-1} \in H$  and this is the inverse of  $a$  in  $H$  by the lemma. Last but not least we have to verify that  $a, b \in H$  implies  $ab \in H$ . But since  $b \in H$  implies  $b^{-1} \in H$  then  $a, b \in H$  implies  $a(b^{-1})^{-1} = ab \in H$ .  $\square$

*Example.* The set  $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$  under addition satisfies the Theorem since  $nk + (-nj) = n(k - j) \in n\mathbb{Z}$ . Thus  $n\mathbb{Z}$  is a subgroup of  $\mathbb{Z}$  under addition. We call the elements of  $n\mathbb{Z}$  *multiples* of  $n$ , that is, members of the congruence class  $[0]_n$ . In particular  $2\mathbb{Z}$  is the subgroup of even numbers under addition.

*Remark.* Theorem 4.2 is usually presented in the format of a two-step subgroup test:  $H$  is a subgroup if (1)  $a, b \in H$  implies  $ab \in H$  and (2)  $x \in H$  implies  $x^{-1} \in H$ .

**Proposition 4.3.** If  $H$  and  $K$  are subgroups of  $G$  then  $H \cap K$  is also a subgroup of  $G$ . More generally the intersection of any collection of subgroups is again a subgroup.

#### Exercise 4

- 1) Prove Lemma 4.1.
- 2) Let  $G$  be a group and  $H$  be a finite non-empty subset of  $G$ . Prove that  $H$  is a subgroup if  $ab \in H$  whenever  $a, b \in H$ .
- 3) Prove Proposition 4.3.
- 4) For any  $a \in G$ , the *centralizer* of  $a$  in  $G$  is defined by  $C(a) = \{x \in G \mid ax = xa\}$ . Show that  $C(a)$  is a subgroup of  $G$ , and conclude that the *center* of a group,  $Z(G) = \{x \in G \mid ax = xa \text{ for all } a \in G\}$  is also a subgroup of  $G$ , upon observing that  $Z(G) = \bigcap C(a)$  where the intersection is taken over all the elements  $a \in G$ .

## 5 Cyclic Groups

*Definition.* Suppose  $G$  is a group and  $a \in G$ . For each integer  $n > 0$  we define  $a^n$  recursively by  $a^1 = a$  and  $a^n = a^{n-1}a$ . In addition let  $a^0 = e$  and  $a^{-n} = (a^{-1})^n$ .

**Proposition 5.1.** The following statements hold, for every  $m, n \in \mathbb{Z}$ .

- 1)  $a^m a^n = a^{m+n} = a^n a^m$
- 2)  $a^{-n} = (a^{-1})^n = (a^n)^{-1}$
- 3)  $(a^m)^n = a^{mn} = (a^n)^m$

*Definition.* Let  $G$  be a group and  $a \in G$ . We define the set  $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$  and will prove that this set is a subgroup of  $G$  called the *cyclic subgroup generated by  $a$* .

**Theorem 5.2.** For any element  $a \in G$  the set  $\langle a \rangle$  is an abelian subgroup of  $G$ .

*Proof.* Elements of  $\langle a \rangle$  are of the form  $a^k$  for some  $k \in \mathbb{Z}$ . In particular  $a^0 = e \in \langle a \rangle$ . If  $a^j, a^k \in \langle a \rangle$  then  $a^j(a^k)^{-1} = a^j a^{-k} = a^{j-k} \in \langle a \rangle$ . Hence  $\langle a \rangle$  is a subgroup of  $G$  by Theorem 4.2. Commutativity is given by the proposition. (How?)  $\nabla$

*Remark.* Note that when the operation in  $G$  is addition, we write  $a^k = a + a + \cdots + a$  (with  $k$  terms) and so the notation  $a^k$  becomes  $ka$ . For example the subgroup  $2\mathbb{Z}$  of  $\mathbb{Z}$  under addition is really the cyclic subgroup generated by 2, and in general,  $n\mathbb{Z} = \langle n \rangle$ .

*Definition.* Let  $G$  be a group and  $a \in G$ . If  $\langle a \rangle = G$  then we call the group  $G$  *cyclic* and call  $a$  a *generator* of  $G$ . We have seen that a cyclic group is necessarily abelian but, of course, we do not expect all abelian groups to be cyclic.

*Example.* The group  $\mathbb{Z}$  under addition is a cyclic group generated by 1. Similarly  $\mathbb{Z}_n = \langle 1 \rangle$  for all  $n > 0$ , under addition mod  $n$ . Another example is  $U_5 = \{1, 2, 3, 4\}$  under multiplication mod 5, where 2 and 3 are both generators.

**Theorem 5.3.** Any subgroup of a cyclic group is again cyclic.

*Proof.* Let  $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$  and let  $H$  be a subgroup of  $G$ . If  $H = \{e\}$  then it is cyclic, trivially  $H = \langle e \rangle$ . Otherwise let  $n$  be the least positive integer for which  $a^n \in H$ . We claim that  $H = \langle a^n \rangle$ . Why? Clearly  $\langle a^n \rangle \subseteq H$ . Now for each  $a^m \in H$  we use the Division Algorithm to write  $m = qn + r$  with  $0 \leq r < n$ . Then  $a^{qn} = (a^n)^q \in H$  and  $a^m(a^{qn})^{-1} = a^{m-qn} = a^r \in H$ . But  $n$  being the least exponent, this is not possible unless  $r = 0$ . Hence  $a^m = a^{qn} = (a^n)^q \in \langle a^n \rangle$  and it follows that  $H = \langle a^n \rangle$ .  $\nabla$

*Example.* Since  $\mathbb{Z}$  is cyclic under addition, we conclude that all its subgroups are cyclic, hence of the form  $\langle n \rangle = n\mathbb{Z}$ . In other words, any subgroup of  $\mathbb{Z}$  under addition must be the group of multiples of some integer  $n$ . Moreover, as shown in the proof,  $n$  is the least positive integer in this subgroup. For example, knowing that the intersection of subgroups is again a subgroup, we have  $\langle 4 \rangle \cap \langle 6 \rangle = \langle 12 \rangle$  because 12 is the least positive multiple of both 4 and 6.

**Theorem 5.4.** As subgroups of  $\mathbb{Z}$ , if  $m, n$  are relatively prime then  $\langle m \rangle \cap \langle n \rangle = \langle mn \rangle$ .

*Proof.* Let  $\langle c \rangle = \langle m \rangle \cap \langle n \rangle$  where  $c$  is the least positive integer in this subgroup. Then by definition  $c = mk$  for some integer  $k$ , and at the same time also  $c$  is a multiple of  $n$ . But  $m, n$  relatively prime implies, by Euclid's Lemma, that  $k$  is multiple of  $n$ . Hence  $c$  is a multiple of  $mn$ . Being the least,  $c \leq |mn|$  so  $c = |mn|$  and  $\langle c \rangle = \langle mn \rangle$ .  $\nabla$

*Remark.* Unlike with  $\mathbb{Z}_n$ , the group  $U_n$  is not always cyclic. In number theory, a generator for  $U_n$ , if cyclic, is known by the name *primitive root*. It can be shown that primitive roots exist if and only if  $n = 1, 2, 4, p^k$ , or  $2p^k$  where  $p$  is any prime number larger than 2 and  $k$  is any positive integer. These are the only values for  $n$  for which  $U_n$  is a cyclic group. What is a prime number?

*Definition.* An integer  $p > 1$  is *prime* if it is not a multiple of any integer  $n$  in the range  $1 < n < p$ . The first few prime numbers are 2, 3, 5, 7, 11, 13, ... Note that a prime  $p$  is always relatively prime to all the numbers  $1, 2, 3, \dots, p-1$ , so  $U_p = \{1, 2, 3, \dots, p-1\}$ .

**Exercise 5**

- 1) Prove Proposition 5.1.
- 2) Find all the generators for the cyclic groups  $\mathbb{Z}_7$ ,  $\mathbb{Z}_8$ , and  $\mathbb{Z}_9$ .
- 3) Find all the generators for the groups  $U_7$ ,  $U_8$ , and  $U_9$ , if cyclic.
- 4) Suppose that  $G$  and  $H$  are both cyclic groups. Prove true or false:  $G \times H$  is cyclic.

**6 Cosets**

*Definition.* Let  $H$  be a subgroup of a group  $G$ . For elements  $a, b \in G$  define the relation  $a \sim b$  if and only if  $ab^{-1} \in H$ . Your job is to prove that this defines an equivalence relation on  $G$ . For example if  $G = \mathbb{Z}$  with addition and  $H = \langle n \rangle$  then  $a \sim b$  if and only if  $a - b \in \langle n \rangle = [0]_n$ . But this is the relation  $a \equiv b \pmod{n}$  we saw in Section 2.

*Definition.* We call the equivalence class of  $a \in G$  under this relation the *coset* of  $a$  in  $G$  with respect to the subgroup  $H$ , given by

$$\begin{aligned}
 Ha &= \{b \in G \mid b \sim a\} \\
 &= \{b \in G \mid ba^{-1} \in H\} \\
 &= \{b \in G \mid ba^{-1} = h, h \in H\} \\
 &= \{b \in G \mid b = ha, h \in H\} \\
 &= \{ha \mid h \in H\}
 \end{aligned}$$

Hence, for example, with the relation  $a \equiv b \pmod{n}$  on  $\mathbb{Z}$ , the cosets are the congruence classes mod  $n$ . From the properties of equivalence classes we conclude that these cosets form a partition for the group  $G$ . For one thing this means that every element  $a \in G$  belongs to exactly one coset. Other facts are recorded below.

**Proposition 6.1.** Let  $H$  be a subgroup of a group  $G$ . Let  $a, b \in G$ .

- 1)  $a \in Ha$  and, moreover,  $b \in Ha$  if and only if  $ab^{-1} \in H$ .
- 2)  $Ha = Hb$  if and only if  $ab^{-1} \in H$ . In particular  $Ha = H$  if and only if  $a \in H$ .
- 3)  $Ha \cap Hb = \phi$  if and only if  $ab^{-1} \notin H$ .
- 4)  $\bigcup \{Ha \mid a \in G\} = G$ .

*Definition.* How many different cosets are there? Denote this quantity by  $[G:H]$ , called the *index* of  $H$  in  $G$ , if it is finite, otherwise write  $[G:H] = \infty$ . Also denote the number of elements in  $G$  by  $|G|$  and call this quantity the *order* of  $G$ . We say the group  $G$  is *finite* or *infinite* depending on  $|G|$ , and for the latter case we write  $|G| = \infty$ .

**Lemma 6.2.** Let  $G$  be a group and  $H$  a subgroup. For each  $a \in G$ , we have  $|Ha| = |H|$ .

*Proof.* Each element in  $Ha$  is of the form  $ha$  for some  $h \in H$ . Moreover  $ha = h'a$  implies  $h = h'$  by the cancellation law. Hence either both  $|Ha|, |H|$  are infinite, or both finite and equal.  $\nabla$

*Definition.* An integer  $n \neq 0$  *divides*  $m$  if  $m = nk$  for some integer  $k$ . This is equivalent to having  $m$  a multiple of  $n$ , or  $m \in [0]_n = \langle n \rangle$  when  $n > 0$ . We also say, in this case, that  $m$  is *divisible* by  $n$ , or that  $n$  is a *divisor* or *factor* of  $m$ .

**Theorem 6.3** (Lagrange’s Theorem). The order of any subgroup  $H$  of a finite group  $G$  is a divisor of  $|G|$ . In particular  $|G|/|H| = [G:H]$ .

*Proof.* Let  $G$  be a finite group and  $H$  a subgroup of  $G$ . There can be only finitely many cosets in  $G$  with respect to  $H$ , say  $k = [G:H]$  of them. By the lemma we have  $|H|k = |G|$ , hence  $|H|$  divides  $|G|$ .  $\nabla$

**Corollary 6.4.** A group of prime order is cyclic, and furthermore any non-identity element is a generator.

*Proof.* Let  $G$  be a group such that  $|G| = p$ , a prime and let  $a \in G$ . By Lagrange’s Theorem the order of  $\langle a \rangle$  divides  $|G|$ . But  $|\langle a \rangle| \neq 1$  unless  $a = e$ , otherwise  $|\langle a \rangle| = p$  and so  $\langle a \rangle = G$ .  $\nabla$

*Definition.* Let  $G$  be a group and  $a \in G$ . The *order* of  $a$ , written  $|a|$ , is the least integer  $n > 0$  such that  $a^n = e$  if it exists, else let  $|a| = \infty$ . For example, modulo 5 we have  $2^2 \equiv 4$ ,  $2^3 \equiv 3$ ,  $2^4 \equiv 1$ ; hence  $|2| = 4$  in the group  $U_5$ .

**Lemma 6.5.** Let  $a$  be an element of a group  $G$ . Then  $|a| = |\langle a \rangle|$ .

*Proof.* Assume first  $|a| = n$  is finite. Let  $H = \{a, a^2, \dots, a^n = e\}$  and claim that  $\langle a \rangle = H$ . It suffices to show that all powers of  $a$  are represented here. Given  $a^m$  for any integer  $m$  we use the Division Algorithm to write  $m = qn + r$  where  $0 \leq r \leq n - 1$ . Then  $a^m = (a^n)^q a^r = a^r \in H$ .

Next we show that the elements  $a, a^2, \dots, a^n$  are all distinct. To see this, given  $a^j = a^k$  with  $1 \leq j < k \leq n$  implies  $a^{k-j} = e$ , impossible as  $0 < k - j < n$  and  $n$  is supposedly the least number with the property  $a^n = e$ .

Thus we conclude  $|a| = n = |H| = |\langle a \rangle|$ . As for the infinite case, note that if  $a^j = a^k$  then  $a^{j-k} = e$ . Thus  $|a| = \infty$  implies that the elements  $a, a^2, \dots$  are all distinct, and so  $\langle a \rangle$  will be infinite as well.  $\nabla$

**Corollary 6.6.** The order of any element of a finite group  $G$  is a divisor of  $|G|$ .

*Proof.* Let  $a \in G$  and  $H = \langle a \rangle$  in Lagrange’s theorem. Then  $|a| = |H|$  divides  $|G|$ .  $\nabla$

**Corollary 6.7.** Let  $G$  be a finite group and  $a \in G$ . Then  $a^{|G|} = e$ .

*Proof.* Let  $|a| = n$ , finite since  $G$  is. We know that  $|G| = nk$  for some integer  $k$ . Hence  $a^{|G|} = (a^n)^k = e^k = e$ .  $\nabla$

*Definition.* For every integer  $n > 1$  let  $\phi(n)$  denote the number of positive integers up to and relatively prime to  $n$ . In other word  $\phi(n) = |U_n|$ . For example  $\phi(10) = 4$  since  $U_{10} = \{1, 3, 7, 9\}$ .

If we let  $G = U_n$  in the last corollary then we derive the Euler’s theorem of number theory. If in addition  $n = p$ , a prime, then  $U_p = \{1, 2, \dots, p - 1\}$  and this is the special case Fermat’s little theorem.

**Theorem 6.8** (Euler’s Theorem). If  $a$  is relatively prime to a positive integer  $n$ , then  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

**Theorem 6.9** (Fermat’s Little Theorem). Let  $p$  be a prime not dividing  $a$ . Then  $a^{p-1} \equiv 1 \pmod{p}$ .

**Exercise 6**

- 1) Verify that the relation  $a \sim b$  if and only if  $ab^{-1} \in H$  is indeed an equivalence relation on the group  $G$ , where  $H$  is any subgroup of  $G$ .
- 2) Consider the subgroup  $H = \{\pm 1\}$  of the group  $G = \mathbb{Q}^*$ . Describe the cosets induced by the relation  $a \sim b$  if and only if  $ab^{-1} \in H$ .
- 3) Repeat the above exercise using  $G = U_{13}$  and  $H = \langle 3 \rangle$ .
- 4) Suppose that  $H$  and  $K$  are finite subgroups of  $G$  such that  $|H|$  and  $|K|$  are relatively prime. Show that  $H \cap K = \{e\}$ .

## 7 Finite Cyclic Groups

In this section we seek to identify the order of each element of a given finite cyclic group  $G$ . Since every subgroup of  $G$  is generated by one element, as  $G$  itself is, such knowledge will also lead to the classification of all the subgroups of  $G$ .

**Lemma 7.1.** Let  $a \in G$ , not assumed cyclic. Then  $a^k = e$  if and only if  $|a|$  divides  $k$ .

*Proof.* Let  $|a| = n$  and write  $k = qn + r$  with  $0 \leq r < n$ . We have  $a^k = (a^n)^q a^r = a^r$ . By the minimality of  $n$ , then  $a^k = e$  if and only if  $r = 0$ .  $\nabla$

*Definition.* The *greatest common divisor* of two integers  $m$  and  $n$ , written  $\gcd(m, n)$ , is the largest integer which divides both. This quantity always exists, unless  $m = n = 0$ , and is at least 1. In particular  $\gcd(m, n) = 1$  if and only if  $m, n$  are relatively prime.

**Theorem 7.2.** Suppose  $a \in G$ , not assumed cyclic, such that  $|a| = n$ . Then  $|a^m| = n / \gcd(m, n)$ .

*Proof.* Let  $|a^m| = k$ . Since  $\langle a^m \rangle$  is a subgroup of  $\langle a \rangle$ , Lagrange's theorem says that  $k$  divides  $n$ , so we write  $k = n/d$  for some  $d$ . This  $d$  must be the largest divisor of  $n$  such that  $(a^m)^{n/d} = e$ . Meanwhile, the lemma requires that  $|a| = n$  divide  $m(n/d) = mk$ . As  $n = dk$ , it follows that  $d$  must divide  $m$ . Thus  $d$  is the largest common divisor of  $m$  and  $n$  with condition that  $a^{mn/d} = e$ . This condition actually holds for any divisor of  $m$  because  $a^{mn/d} = (a^n)^{m/d} = e$ ; hence choosing  $d = \gcd(m, n)$  yields the minimal correct value of  $k$ , the order of  $a^m$ .  $\nabla$

**Corollary 7.3.** Suppose  $G = \langle a \rangle$ , of order  $n$ . Then  $G = \langle a^m \rangle$  if and only if  $m, n$  are relatively prime.

*Proof.*  $\langle a^m \rangle = \langle a \rangle$  if and only if  $|a^m| = |a| = n$ , if and only if  $\gcd(m, n) = 1$ .  $\nabla$

**Corollary 7.4.** Let  $m$  represent an integer as well as an element of  $\mathbb{Z}_n$ . Then  $m$  and  $n$  are relatively prime if and only if  $\mathbb{Z}_n = \langle m \rangle$ .

*Proof.* Simply let  $G = \mathbb{Z}_n = \langle 1 \rangle$  in the above corollary.  $\nabla$

*Example.* Consider  $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ . The elements relatively prime to 10 are 1, 3, 7, 9. For each of these we have

$$\begin{aligned} \langle 1 \rangle &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\} \\ \langle 3 \rangle &= \{3, 6, 9, 2, 5, 8, 1, 4, 7, 0\} \\ \langle 7 \rangle &= \{7, 4, 1, 8, 5, 2, 9, 6, 3, 0\} \\ \langle 9 \rangle &= \{9, 8, 7, 6, 5, 4, 3, 2, 1, 0\} \end{aligned}$$

Note that other elements do not generate the group, for instance  $\langle 4 \rangle = \{4, 8, 2, 6, 0\}$ .

**Lemma 7.5.** Distinct subgroups of a finite cyclic group have unequal orders.

*Proof.* Let  $G = \langle a \rangle$ , say of order  $n$ . We know that subgroups of  $G$  are of the form  $\langle a^k \rangle$ . Take two subgroups  $\langle a^k \rangle$  and  $\langle a^h \rangle$  of equal orders, and we will show that  $\langle a^k \rangle = \langle a^h \rangle$ . By the theorem,  $\gcd(k, n) = \gcd(h, n) = d$ . We may write  $dc = k$  for some integer  $c$ , hence  $a^k \in \langle a^d \rangle$ . But  $|a^d| = n/\gcd(d, n) = n/d = n/\gcd(k, n) = |a^k|$ , which implies that  $\langle a^k \rangle = \langle a^d \rangle$ . By a symmetrical argument we have  $\langle a^h \rangle = \langle a^d \rangle$ . Hence the two subgroups are one and the same.  $\square$

**Theorem 7.6.** Let  $G = \langle a \rangle$ , of order  $n$ . Including  $a$ , there are exactly  $\phi(n)$  generating elements of  $G$ . Moreover, for every positive divisor  $d$  of  $n$ , there exist exactly  $\phi(d)$  elements in  $G$  of order  $d$ .

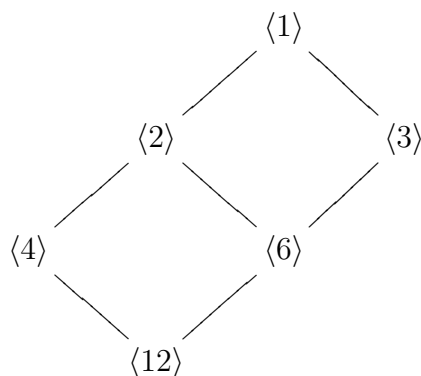
*Proof.* Write  $G = \{a, a^2, \dots, a^n = e\}$ . By Corollary 7.3,  $a^m$  generates  $G$  if and only if  $m \in U_n$ . Their number is given by  $|U_n| = \phi(n)$ . Now if  $d$  divides  $n$ , say  $dk = n$ , then  $|a^k| = n/k = d$ . By the preceding lemma, every element of order  $d$  is a generator of this subgroup  $\langle a^k \rangle$  of order  $d$ . By the same reasoning, there are  $\phi(d)$  such elements.  $\square$

*Remark.* Now by Corollary 6.6, every element in such  $G$  has order a divisor of  $n$ . The above theorem then yields a known identity of number theory involving the phi-function:  $\sum \phi(d) = n$ , where the sum is over all positive integers  $d$  that divide  $n$ .

**Theorem 7.7.** Let  $G$  be a cyclic group of order  $n$ . For every divisor  $d$  of  $n$  there is a unique subgroup of  $G$  of order  $d$ , and these are the only subgroups  $G$  can have.

*Proof.* This results from the last two assertions as well as Lagrange's theorem.  $\square$

*Example.* Since every subgroup of a cyclic group is again cyclic, all these results apply to any finite cyclic group  $G$  as well as all its subgroups and its sub-subgroups. The *subgroup lattice* is a way we can diagram these subgroup relations. The following is the subgroup lattice for the group  $\mathbb{Z}_{12}$ . Note that  $\langle 1 \rangle = \mathbb{Z}_{12}$  and that  $\langle 12 \rangle = \langle 0 \rangle = \{0\}$ .



### Exercise 7

- 1) Determine the order of every element in  $\mathbb{Z}_{24}$  and the subgroup it generates. Check your result against Theorem 7.6 and verify the identity  $\sum \phi(d) = n$ .
- 2) Draw the subgroup lattice for each of the groups  $\mathbb{Z}_{24}$ ,  $\mathbb{Z}_{25}$ ,  $\mathbb{Z}_{30}$ , and  $\mathbb{Z}_{36}$ .
- 3) The group  $U_{18}$  is cyclic. Count how many generators it has and draw its subgroup lattice as well.
- 4) Let  $G$  and  $H$  be finite cyclic groups such that  $|G|$  and  $|H|$  are relatively prime. Prove that  $G \times H$  is again cyclic.

## 8 Normal Subgroups

Had we defined the equivalence relation  $a \sim b$  to be  $b^{-1}a \in H$  then the coset of  $a$  would have looked different, given by  $aH = \{ah \mid h \in H\}$ , otherwise called the *left coset* of  $a$  in  $G$  with respect to the subgroup  $H$ . This is to distinguish it from the *right coset*  $Ha$  of the previous section. This differentiation would not have been needed if  $G$  were abelian, in which case  $aH = Ha$  for all  $a \in G$ , or if  $H$  were a normal subgroup, below.

*Definition.* Let  $G$  be a group. A subgroup  $N$  of  $G$  is called *normal* if  $aN = Na$  for every  $a \in G$ . Hence for abelian groups, all subgroups are normal, but the converse does not always hold. (See Exercise 13.1 for an example.)

**Proposition 8.1.** A subgroup  $N$  of  $G$  is normal if and only if  $ana^{-1} \in N$  for every  $a \in G$  and  $n \in N$ .

*Proof.* Suppose  $N$  is normal. Then  $an \in aN = Na$ , hence  $an = n'a$  for some  $n' \in N$ . It follows that  $ana^{-1} = n'aa^{-1} = n' \in N$ .

Conversely suppose  $ana^{-1} \in N$  for every  $a \in G$  and  $n \in N$ . Then

$$\begin{aligned} b \in Na &\leftrightarrow ab^{-1} \in N \\ &\leftrightarrow b^{-1}(ab^{-1})b \in N \\ &\leftrightarrow b^{-1}a \in N \\ &\leftrightarrow b \in aN \end{aligned}$$

which shows that  $Na = aN$ . ▽

*Definition.* For any subsets  $A, B$  of a group  $G$  we define the product  $AB = \{ab \mid a \in A, b \in B\}$ . In particular when  $B = \{b\}$  we write  $AB = Ab$ , which coincides with the notion of a (right) coset when  $A$  is a subgroup. Note that associativity in  $G$  implies that  $A(BC) = (AB)C$  for any three subsets  $A, B, C$ .

**Lemma 8.2.** Let  $N$  be a normal subgroup of  $G$ . Then for every  $a, b \in G$ ,

- 1)  $NN = N$
- 2)  $N(Na) = (Na)N = Na$
- 3)  $(Na)(Nb) = N(ab)$

*Proof.* We have  $NN = \bigcup\{Nn \mid n \in N\} = N$  since for any subgroup (not necessarily normal)  $Ha = H$  if and only if  $a \in H$ . Then  $(Na)(Nb) = N(aN)b = N(Na)b = (NN)(ab) = N(ab)$ . In particular with  $b = e$ ,  $(Na)N = Na$  and  $N(Na) = Na$ . ▽

*Definition.* With  $N$  a normal subgroup of  $G$ , we denote by  $G/N$  (read  $G \bmod N$ ) the set of all cosets in  $G$  with respect to this subgroup:  $G/N = \{Na \mid a \in G\}$ . We also introduce the operation  $(Na)(Nb) = N(ab)$  in this set, which will then become a group of order  $[G:N]$ . The group  $G/N$  is better known as the *quotient group* or *factor group* of  $G \bmod N$ .

**Theorem 8.3.** For any normal subgroup  $N$  of a group  $G$ , the set  $G/N$  forms a group under the operation  $(Na)(Nb) = N(ab)$  for every  $a, b \in G$ .

*Proof.* We show first that this operation is well-defined. Suppose that  $Na = Na_2$  and  $Nb = Nb_2$ . These are equivalent to having  $aa_2^{-1}, bb_2^{-1} \in N$ . Since  $N$  is normal, also  $c = a_2(bb_2^{-1})a_2^{-1} \in N$ . Hence  $aa_2^{-1}c = ab(a_2b_2)^{-1} \in N$ , meaning that  $(ab) \sim a_2b_2$  and so  $N(a)N(b) = N(ab) = N(a_2b_2) = N(a_2)N(b_2)$ . Now for the group axioms:

- 1) Associative:  $Na((Nb)(Nc)) = NaN(bc) = N(a(bc)) = N((ab)c) = N(ab)N(c) = (N(a)N(b))N(c)$ .
- 2) Identity: The identity element in  $G/N$  is  $N = Ne$ .
- 3) Inverse: For each element  $Na \in G/N$  its inverse is given by  $N(a^{-1})$ . ▽

*Example.* The group  $\mathbb{Z}$  under addition is abelian, hence all its subgroups are normal. Let  $N = \langle 2 \rangle$ , the subgroup of all even numbers. Then  $N + a = N$  for every  $a$  even. If  $a, b$  are both odd then  $a - b$  is even and belongs to  $N$ , hence  $N + a = N + b$ . Thus the quotient group  $\mathbb{Z}/\langle 2 \rangle = \{\langle 2 \rangle, \langle 2 \rangle + 1\} = \{e, o\}$  where  $e$  represents the coset of even numbers  $[0]_2$  and  $o$  the coset of odd numbers  $[1]_2$ . The Cayley table looks like this.

+	$e$	$o$
$e$	$e$	$o$
$o$	$o$	$e$

In the next section we will see that this group is essentially  $\mathbb{Z}_2$  in the sense of isomorphism. Also in general we will show that  $\mathbb{Z}/\langle n \rangle \approx \mathbb{Z}_n$ .

*Example.* We look at the group  $U_7$  and one of its subgroups,  $\langle 6 \rangle = \{1, 6\}$ . There are three cosets given by  $\langle 6 \rangle 1 = \langle 6 \rangle$ ,  $\langle 6 \rangle 2 = \{2, 5\}$ , and  $\langle 6 \rangle 3 = \{3, 4\}$ . These three form the factor group  $U_7/\langle 6 \rangle$  whose Cayley table, represented by 1,2,3, respectively, is provided below.

×	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Can you identify which familiar group this really is?

**Exercise 8**

- 1) Prove that the following subgroups are normal subgroups.
  - a)  $SL(2, \mathbb{R})$  of  $GL(2, \mathbb{R})$
  - b) the center  $Z(G)$  of  $G$
  - c) any subgroup of a cyclic group
  - d) any subgroup of index 2
- 2) Describe the factor group  $\mathbb{Z}_{12}/\langle 3 \rangle$  and draw its Cayley table. Similarly, do also for  $U_{13}/\langle 3 \rangle$ .
- 3) Show that the factor group of an abelian group is abelian. Is the factor group of a cyclic group cyclic?
- 4) Prove that the factor group  $G/Z(G)$  is never cyclic, unless it is trivial.

## 9 Group Isomorphisms

*Definition.* A function  $\theta : G \rightarrow G'$  between two groups is called a *homomorphism* if it satisfies  $\theta(ab) = \theta(a)\theta(b)$  for every  $a, b \in G$ . This condition says that  $\theta$  preserves the binary operation. Note that the operation  $\theta(a)\theta(b)$  is that of  $G'$ , which is not distinguishable from that of  $G$  in the notation but is not assumed the same. We also define the *range*  $\theta(G) = \{\theta(a) \mid a \in G\}$  and the *kernel*  $\ker(\theta) = \{a \in G \mid \theta(a) = e'\}$  where  $e'$  denotes the identity in  $G'$ .

*Example.* Let us illustrate this idea with a few examples.

- 1) Let  $\theta : \mathbb{Z} \rightarrow \mathbb{Z}_n$  be given by  $\theta(a) = [a]_n$ . This is a homomorphism as  $[a + b]_n = [a]_n + [b]_n$ . We have  $\ker(\theta) = n\mathbb{Z}$  and  $\theta(\mathbb{Z}) = \mathbb{Z}_n$ .
- 2) Let  $\theta : \mathbb{Z} \rightarrow \{\pm 1\}$  such that  $\theta(n) = (-1)^n$ . Then  $\theta(a+b) = (-1)^{a+b} = (-1)^a(-1)^b = \theta(a)\theta(b)$ , showing it is a homomorphism. Here  $\theta(\mathbb{Z}) = \{\pm 1\}$  and  $\ker(\theta) = \langle 2 \rangle$ .
- 3) Let  $\theta : \mathbb{R} \rightarrow \mathbb{R}^*$  where  $\theta(x) = e^x$ . We have  $e^{x+y} = e^x e^y$  hence it is a homomorphism, with  $\theta(\mathbb{R}) = (0, \infty)$  and  $\ker(\theta) = \{0\}$ .

**Proposition 9.1.** Let  $\theta : G \rightarrow G'$  be a homomorphism from a group  $G$  with identity  $e$  to another group  $G'$  with identity  $e'$ .

- 1)  $\theta(e) = e'$  and  $\theta(a^{-1}) = \theta(a)^{-1}$  for every  $a \in G$ .
- 2)  $\theta$  is one-to-one if and only if  $\ker(\theta) = \{e\}$ .
- 3)  $\theta(G)$  is a subgroup of  $G'$ .
- 4)  $\ker(\theta)$  is a normal subgroup of  $G$ .

*Definition.* A homomorphism  $\theta : G \rightarrow G'$  is called an *isomorphism* when it is one-to-one and onto, in which case we say that  $G$  and  $G'$  are *isomorphic*, written  $G \approx G'$ . The meaning of onto is, of course, that  $\theta(G) = G'$ .

Isomorphism really means that the two groups are essentially identical, except for the different labeling of the elements. For example we have seen there is only one group with 2 elements, namely  $G = \{e, a\}$  in which  $a^2 = e$ . We can see that  $G \approx \mathbb{Z}_2$  by identifying  $\theta(e) = 0$  and  $\theta(a) = 1$ . Another example is from Example (3) above, where the group  $\mathbb{R}$  under addition is isomorphic to the real interval  $(0, \infty)$  under multiplication, by way of the homomorphism function  $\theta(x) = e^x$ , or the inverse  $\theta^{-1}(y) = \ln y$ .

**Theorem 9.2.** Any finite cyclic group of order  $n$  is isomorphic to  $\mathbb{Z}_n$ . Any infinite cyclic group is isomorphic to  $\mathbb{Z}$ .

*Proof.* Let  $G = \langle a \rangle = \{a^0, a^1, a^2, \dots, a^{n-1}\}$  where  $a \in G$  is of order  $n$ . Let  $\theta : G \rightarrow \mathbb{Z}_n$  be given by  $\theta(a^k) = k = [k]_n$ . This is a homomorphism since  $\theta(a^k a^l) = \theta(a^{k+l}) = [k+l]_n = [k]_n + [l]_n = \theta(a^k) + \theta(a^l)$ . Moreover  $\theta$  is one-to-one as  $\theta(a^k) = [0]_n$  if and only if  $k = 0$  and  $a^k = e$ . Also  $\theta$  is clearly onto, proving the isomorphism  $G \approx \mathbb{Z}_n$ .

If on the other hand  $|a| = \infty$  then simply define  $\theta(a^k) = k \in \mathbb{Z}$ . By a very similar argument we show that  $\theta$  is an isomorphism and  $G \approx \mathbb{Z}$ . ▽

**Theorem 9.3** (The Fundamental Homomorphism Theorem). Let  $\theta : G \rightarrow G'$  be a homomorphism of groups. Then  $G/\ker(\theta) \approx \theta(G)$ .

*Proof.* We let  $H = \ker(\theta)$  and define the map  $\Theta : G/H \rightarrow \theta(G)$  according to the rule  $\Theta(Ha) = \theta(a)$ . This map is well-defined, for if  $Ha = Hb$  then  $ab^{-1} \in H$ , leading to  $e' = \theta(ab^{-1}) = \theta(a)\theta(b)^{-1}$  and thus  $\theta(a) = \theta(b)$ . It is also a homomorphism because

$$\Theta((Ha)(Hb)) = \Theta(H(ab)) = \theta(ab) = \theta(a)\theta(b) = \Theta(Ha)\Theta(Hb)$$

as  $\theta$  is. It is clear that  $\Theta$  is onto and furthermore, the fact that  $\theta(a) = \theta(b)$  implies  $Ha = Hb$  (How?) shows that it is one-to-one, hence an isomorphism.  $\nabla$

*Example.* The following are some examples of isomorphism between groups.

- 1) From Example (1) above,  $\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}_n$ .
- 2) In particular from Example (2),  $\mathbb{Z}/2\mathbb{Z} \approx \{\pm 1\} \approx \mathbb{Z}_2$ .
- 3) As a counter-example, we shall demonstrate why  $\mathbb{Z}_2 \times \mathbb{Z}_2$  is not isomorphic to  $\mathbb{Z}_4$ . Note that every element  $\alpha \in \mathbb{Z}_2 \times \mathbb{Z}_2$  meets the condition  $\alpha^2 = (0, 0)$ , the identity of this group. Therefore  $\theta(\alpha)^2 = 0 \in \mathbb{Z}_4$ —if  $\theta$  is a homomorphism. But then  $\theta$  is not onto since  $\mathbb{Z}_4$ , being cyclic, contains an element of order 4.

*Remark.* Generally speaking, an isomorphism preserves algebraic structures of the one group onto the other. Properties such as group order, being abelian or cyclic, existence of a particular subgroup, etc., must agree between the two isomorphic groups. In the example of  $\mathbb{Z}_2 \times \mathbb{Z}_2$  and  $\mathbb{Z}_4$ , the fact that one is cyclic and the other not is sufficient evidence that no isomorphism can exist between the two groups.

**Theorem 9.4** (Chinese Remainder Theorem). Suppose that  $m, n \in \mathbb{Z}$  are relatively prime. Then  $\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$ .

*Proof.* Let  $\theta : \mathbb{Z} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$  be defined by  $\theta(a) = (a, a) = ([a]_m, [a]_n)$ . The fact that  $[a + b] = [a] + [b]$  in each  $\mathbb{Z}_m$  and  $\mathbb{Z}_n$  makes this function an onto homomorphism. We have  $\ker(\theta) = \{a \in \mathbb{Z} \mid a \in [0]_m \cap [0]_n\} = \langle mn \rangle$  by Theorem 5.4. Hence  $\mathbb{Z}_m \times \mathbb{Z}_n \approx \theta(\mathbb{Z}) \approx \mathbb{Z}/\langle mn \rangle \approx \mathbb{Z}_{mn}$  by the fundamental homomorphism theorem.  $\nabla$

*Remark.* The Chinese remainder theorem belongs to number theory. For an illustration, this theorem implies that the congruence  $a \equiv b \pmod{12}$  is equivalent to the simultaneous pair  $a \equiv b \pmod{3}$  and  $a \equiv b \pmod{4}$ . It also means that the congruences  $x \equiv 5 \pmod{7}$  and  $x \equiv 8 \pmod{11}$  have a unique common solution in  $\mathbb{Z}_{77}$ .

**Corollary 9.5.** If  $m$  and  $n$  are relatively prime integers then  $\phi(mn) = \phi(m)\phi(n)$ .

*Proof.* Note that  $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$  is a unit element (that is, invertible under multiplication) if and only if  $a$  and  $b$  are, respectively, in  $\mathbb{Z}_m$  and  $\mathbb{Z}_n$ . (Why?) This says that we have  $\phi(m)\phi(n)$  such units. Looking at  $\mathbb{Z}_{mn}$  on the other hand, we know this number is equal to  $|U_{mn}| = \phi(mn)$ .  $\nabla$

### Exercise 9

- 1) Prove Proposition 9.1.
- 2) Let  $a \in G$  and  $\theta : G \rightarrow G$  be given by  $\theta(x) = axa^{-1}$  for every  $x \in G$ . Prove that  $\theta$  is an isomorphism; it is named the *inner automorphism* of  $G$  induced by  $a$ .
- 3) Show that  $U_8$  is isomorphic to  $U_{12}$  but not to  $U_{10}$ .
- 4) Rewrite carefully the proof of the fundamental homomorphism theorem without looking at your notes.

## 10 Finite Abelian Groups

The main thing of this section is the fundamental theorem of finite abelian groups, which classify all abelian groups of a given order. The proof of the theorem will be provided as a separate handout.

**Theorem 10.1** (The Fundamental Theorem of Finite Abelian Groups). Every finite abelian group is isomorphic to the direct product of cyclic groups.

Before putting this theorem into action, we need to borrow from number theory the fundamental theorem of arithmetic, which states that every positive integer  $n$  is a unique product of powers of distinct primes,  $n = \prod p_i^{k_i}$ . Note that powers of primes in such an expression are pairwise relatively prime:

*Definition.* The integers  $n_1, n_2, \dots, n_k$  are said to be *pairwise relatively prime* when they are relatively prime in pairs, that is,  $\gcd(n_i, n_j) = 1$  whenever  $i \neq j$ .

The Chinese remainder theorem can now be generalized in a natural way involving three or more copies of finite cyclic groups.

**Theorem 10.2** (Chinese Remainder Theorem). If the integers  $n_1, n_2, \dots, n_k$  are pairwise relatively prime then  $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k} \approx \mathbb{Z}_{n_1 n_2 \dots n_k}$ .

Hence, by the fundamental theorem, every finite abelian group is isomorphic to the direct product of cyclic groups of a prime power order. This knowledge enables us to classify with ease all abelian groups of a given order.

*Example.* Consider an abelian group of order  $400 = 2^4 \times 5^2$ . There are only 10 ways by which we can possibly have distinct prime powers whose product is 400, and each choice corresponds to a direct product in the following list.

$$\begin{array}{ll}
 \mathbb{Z}_{2^4} \times \mathbb{Z}_{5^2} & \mathbb{Z}_{2^4} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
 \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} & \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
 \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{5^2} & \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
 \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} & \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
 \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5
 \end{array}$$

It is not hard to verify that no two of these 10 groups are isomorphic to each other. Thus the number of distinct abelian groups of a prime order  $p^k$  is given by the  $p(k)$ , the number of distinct partitions of the positive integer  $k$ . For example,  $p(4) = 5$  since there are 5 ways we can partition the number 4, namely (a)  $4 = 4$ ; (b)  $4 = 3 + 1$ ; (c)  $4 = 2 + 2$ ; (d)  $4 = 2 + 1 + 1$ ; and (e)  $4 = 1 + 1 + 1 + 1$ .

Two immediate consequences of the fundamental theorem are worth mentioning, one of which is an independent theorem due to Cauchy. Be aware, however, that the genuine Cauchy’s theorem applies to finite groups in general, not just abelian groups. (See Corollary 13.2.)

**Corollary 10.3** (Cauchy’s Theorem). Let  $G$  be a finite abelian group of order divisible by  $p$ , a prime number. Then there exists an element of order  $p$  in  $G$ .

*Proof.* The prime  $p$  appears in the factorization of  $n = |G|$ , hence one of the cyclic groups, say the first, in the product is  $\mathbb{Z}_{p^k}$  with  $k \geq 1$ . Since  $p$  divides  $p^k$ , we have an element of order  $p$  in  $\mathbb{Z}_{p^k}$ , call it  $a$ . This gives us an element of the same order in  $G$ , corresponding to the element  $(a, 0, \dots, 0)$  in the direct product.  $\square$

**Corollary 10.4.** Suppose that  $G$  is an abelian group of order  $n$ , and that  $n$  has no repeated prime factors. Then  $G \approx \mathbb{Z}_n$  and hence it is cyclic.

*Proof.* Then  $G \approx \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$  and since all these primes are pairwise relatively prime, the result follows by the Chinese remainder theorem.  $\nabla$

### Exercise 10

- 1) List all the abelian groups of the specified order.
  - a) 25
  - b) 42
  - c) 100
  - d) 2400
- 2) Show why  $\mathbb{Z}_{p^2} \not\approx \mathbb{Z}_p \times \mathbb{Z}_p$ . Generalize your argument to proving that there are exactly  $p(k)$  non-isomorphic abelian groups of order  $p^k$ .
- 3) Let  $G$  be a finite abelian group of order divisible by  $d$ . Show that  $G$  has a subgroup of order  $d$ .
- 4) Following the factorization notation  $n = \prod p_i^{k_i}$ , prove that  $\phi(n) = \prod \phi(p_i^{k_i})$ . Show also that  $\phi(p^k) = p^k - p^{k-1}$  and apply these properties to evaluate  $\phi(3960000)$ .

## 11 Permutation Groups

*Definition.* A *permutation* on a set  $A$  means a function  $f : A \rightarrow A$  which is one-to-one and onto. If the set is given by  $A = \{1, 2, 3, \dots, n\}$  then let  $S_n$  denote the set of all permutations on  $A$ . It is not hard to see that  $|S_n| = n!$  and that it forms a group under function composition.<sup>3</sup> We call  $S_n$  the *symmetric group* of degree  $n$  and call any subgroup of  $S_n$  a *permutation group*.

**Theorem 11.1** (Cayley's Theorem). Every group is isomorphic to a permutation group.

*Sketch of proof.* For each  $a \in G$  we associate to it  $f_a : G \rightarrow G$  given by  $f_a(x) = ax$  for all  $x \in G$ . This function  $f_a$  is a permutation on  $G$ . The set  $G' = \{f_a \mid a \in G\}$  is then a group under composition. That  $G \approx G'$  can be established by showing that  $a \rightarrow f_a$  is indeed an isomorphism.  $\nabla$

*Remark.* If  $G$  is a finite group, according to Cayley's theorem,  $G$  is isomorphic to a subgroup of  $S_n$ , where  $n = |G|$ . In particular, there can be only finitely many groups, up to isomorphism, of a given finite order.

*Example.* Consider  $S_6$ , the set of  $6! = 720$  permutations on  $\{1, 2, 3, 4, 5, 6\}$ . An element of  $S_6$  may be written in *cyclic notation*, for instance  $(1, 2, 5)(3, 6)$ , which really means the function  $f$  given by

$$\begin{array}{lll} f(1) = 2 & f(2) = 5 & f(3) = 6 \\ f(4) = 4 & f(5) = 1 & f(6) = 3 \end{array}$$

---

<sup>3</sup>Recall from calculus concerning the composition of two functions  $f$  and  $g$  which is normally written  $g \circ f(x) = g(f(x))$ .

Note that 4 is missing in the notation; this is understood as  $f(4) = 4$ . In general, elements left unchanged by the permutation need not be included in the cyclic notation, except when writing the identity permutation:  $e = (1)$ . Following convention, composition is read from right to left, and it is generally non-commutative, for instance,

$$\begin{aligned}(1, 2, 5)(3, 6) \circ (4, 6, 2, 1) &= (1, 4, 3, 6, 5) \\ (4, 6, 2, 1) \circ (1, 2, 5)(3, 6) &= (2, 5, 4, 6, 3)\end{aligned}$$

*Definition.* The term *cycle* refers to each bracketed part in a cyclic notation. It is intuitively clear that every permutation can be represented by *disjoint* cycles, that is, where no two cycles have a common element. If a cycle has  $d$  elements in it, we call it a  $d$ -*cycle*.

For example, the permutation  $(1, 2, 5)(3, 6)$  is written in two disjoint cycles: the 3-cycle  $(1, 2, 5)$  and the 2-cycle  $(3, 6)$ . Note that it is not ambiguous to write  $(1, 2, 5)(3, 6)$  in place of the composition  $(1, 2, 5) \circ (3, 6)$ . Moreover,

**Proposition 11.2.** If  $f$  and  $g$  are two disjoint cycles then  $f \circ g = g \circ f$ .

**Proposition 11.3.** Every permutation is a product of 2-cycles. There is more than one way to express this product but the parity of the number of 2-cycles used is unique: always even or always odd.

*Proof.* Note, for example,  $(1, 2, 3, 4, 5, 6) = (1, 6)(1, 5)(1, 4)(1, 3)(1, 2)$  and generalize. To show that parity is unique, first prove that the identity  $e$  can only be written as a product of even 2-cycles. (Use induction.) Next observe that  $f^{-1} = f$  if  $f$  is a 2-cycle. Hence with 2-cycles, if  $f_1 f_2 \cdots f_s = g_1 g_2 \cdots g_t$  then  $f_1 f_2 \cdots f_s \circ g_t \cdots g_2 g_1 = e$ , and so  $s + t$  must be even—either both odd or both even.  $\nabla$

*Definition.* A permutation is called *even* or *odd* as it is the product of an even or odd number of 2-cycles. In particular, the even permutations form a subgroup of  $S_n$ , called the *alternating group* of degree  $n$  and is denoted by  $A_n$ .

**Theorem 11.4.**  $A_n$  is a subgroup of  $S_n$  of order  $n!/2$ .

*Proof.* Working with 2-cycles, it is clear that the composition of two even permutations is again even. Furthermore since every 2-cycle is self-inverse, the inverse of a permutation retains its parity. (Why?) Theorem 4.2 then implies that  $A_n$  is a subgroup.

What are now the cosets induced by  $A_n$ ?  $A_n e = A_n$  is one. What about  $A_n(1, 2)$ ? (The theorem assumes  $n \geq 2$ , else  $A_1 = S_1 = \{e\}$ .) Every odd permutation  $f$  belongs to  $A_n(1, 2)$  because  $f^{-1} \circ (1, 2)$  is even. These two cosets then make up all of  $S_n$ , hence  $A_n$  accounts for exactly half of the elements in  $S_n$ .  $\nabla$

### Exercise 11

- 1) Verify the claim that  $S_n$  is a group of order  $n!$  under composition of functions.
- 2) Determine the order of each element of  $S_n$  given below.
  - a)  $(2, 1, 5, 6, 4, 3)$
  - b)  $(2, 1, 5)(6, 4, 3)$
  - c)  $(2, 1, 5)(6, 4)$
  - d)  $(2, 1, 5)(6, 4)(3, 9, 7, 8)$
- 3) Show that  $S_n$  is non-abelian for all  $n \geq 3$ .
- 4) Prove that the alternating subgroup  $A_n$  is normal in  $S_n$ .

## 12 The Dihedral Groups

We consider another permutation group which arises in geometry, namely the group of symmetries on a regular polygon. Let's label the vertices of a regular  $n$ -gon by  $1, 2, \dots, n$ . There are  $n$  symmetries by rotation which correspond to  $n$  elements of  $S_n$ , namely  $R = (1, 2, 3, \dots, n)$ , the  $360^\circ/n$ -rotation; and  $R^2$ , the  $720^\circ/n$ -rotation; ... up to  $R^n = e$ , the  $360^\circ$ -rotation. Then there are also reflections along the  $n$  axes of symmetry, making a total of  $2n$  permutations which form a subgroup  $D_n$  of  $S_n$ .

*Example.* We illustrate with  $n = 4$ , a square. The four reflections are given by  $F_1 = (1, 4)(2, 3)$ ,  $F_2 = (2, 4)$ ,  $F_3 = (1, 2)(3, 4)$ ,  $F_4 = (1, 3)$ . The four rotations are  $R, R^2, R^3, R^4 = e$ , which correspond to  $90^\circ, 180^\circ, 270^\circ, 360^\circ$ , respectively. The Cayley table for  $D_4$  given below shows how the compositions work, remembering that they read right to left.

$\circ$	$R$	$R^2$	$R^3$	$e$	$F_1$	$F_2$	$F_3$	$F_4$
$R$	$R^2$	$R^3$	$e$	$R$	$F_2$	$F_3$	$F_4$	$F_1$
$R^2$	$R^3$	$e$	$R$	$R^2$	$F_3$	$F_4$	$F_1$	$F_2$
$R^3$	$e$	$R$	$R^2$	$R^3$	$F_4$	$F_1$	$F_2$	$F_3$
$e$	$R$	$R^2$	$R^3$	$e$	$F_1$	$F_2$	$F_3$	$F_4$
$F_1$	$F_4$	$F_3$	$F_2$	$F_1$	$e$	$R^3$	$R^2$	$R$
$F_2$	$F_1$	$F_4$	$F_3$	$F_2$	$R$	$e$	$R^3$	$R^2$
$F_3$	$F_2$	$F_1$	$F_4$	$F_3$	$R^2$	$R$	$e$	$R^3$
$F_4$	$F_3$	$F_2$	$F_1$	$F_4$	$R^3$	$R^2$	$R$	$e$

**Theorem 12.1.**  $D_n$  is a group under composition of functions.

*Proof.* As a finite subset of  $S_n$ , it suffices to show that  $D_n$  is closed under composition, meaning that  $f \circ g \in D_n$  whenever  $f, g \in D_n$ . This is left as an exercise.  $\square$

*Definition.* We call this permutation group  $D_n$  the *dihedral group* of degree  $n$ , and fix the notation  $D_n = \{R, R^2, \dots, R^n = e, F_1, F_2, \dots, F_n\}$  to represent the rotations and reflections, respectively. Since  $|D_n| = 2n$ , in particular we have  $D_3 = S_3$  but in general  $D_n$  is a proper subgroup of  $S_n$  and is non-abelian as  $S_n$  is.

**Theorem 12.2.** Let  $p$  denote a prime number larger than 2. Every group of order  $2p$  is isomorphic to either  $Z_{2p}$  (if abelian) or to  $D_p$  (if non-abelian).

*Proof.* The abelian case is given by Corollary 10.4. Assume  $G$  is a non-abelian group of order  $2p$ . A non-identity element in  $G$  must have order 2 or  $p$  (not  $2p$  or else  $G$  would be cyclic, hence abelian). Not all elements can have order 2, lest  $G$  would be abelian (Exercise 1.4) so let  $a \in G$  be chosen with  $|a| = p$ .

Thus  $G$  is partitioned into two cosets,  $\langle a \rangle$  and  $\langle a \rangle b$  for any element  $b \notin \langle a \rangle$ . Moreover  $|b| = 2$  for the following reason. If not then  $|b| = p$  and  $\langle a \rangle \cap \langle b \rangle = \{e\}$  since a non-trivial common element will generate both. But  $\langle a \rangle$  is normal in  $G$  (of index 2!) so  $\langle a \rangle b^2$  is identity in  $G/\langle a \rangle$ , that is,  $b^2 \in \langle a \rangle$ —a contradiction.

We have shown that any non-abelian group of order  $2p$  is necessarily of the form  $G = \{a, a^2, \dots, a^p = e, ab, a^2b, \dots, a^pb = b\}$ . To complete the proof, we next show that the binary operation on  $G$  is uniquely determined so that up to isomorphism there can be only one such group. Simply note that  $|ab| = 2$  since  $ab \notin \langle a \rangle$ , thus  $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}$ . This determines all products in  $G$  for they are of the form either  $a^i(a^j b^k) = a^{i+j} b^k$  or  $(a^i b)(a^j b^k) = a^i (ba^j) b^k = a^i (a^{-j} b) b^k = a^{i-j} b^{k+1}$ , where  $k = 0$  or 1.  $\square$

In the above proof we are shown two more facts about  $D_n$  which we shall state and prove again anyhow as follow.

**Proposition 12.3.** In any dihedral group, the composition of a rotation with a reflection, in either order, is a reflection.

*Proof.* The cyclic subgroup  $\langle R \rangle$  of  $D_n$  contains all the  $n$  rotations, and it generates two cosets—the other one being the set of all  $n$  reflections represented by  $\langle R \rangle F$ , or  $F \langle R \rangle$ , for any reflection  $F \in D_n$ .  $\nabla$

**Proposition 12.4.** If  $F \in D_n$  is a reflection then  $F \circ R = R^{n-1} \circ F$ .

*Proof.* Being a reflection,  $F \circ R$  is self-inverse, hence  $F \circ R = (F \circ R)^{-1} = R^{-1} \circ F$ .  $\nabla$

### Exercise 12

- 1) Draw the Cayley table for each  $D_3$  and  $D_5$ , clearly distinguishing between the rotations and the reflections.
- 2) Determine the order of each element in  $D_n$ .
- 3) Show that  $D_n$  is non-abelian for all  $n \geq 3$ .
- 4) In any dihedral group, prove that the composition of two reflections is a rotation.

## 13 Topics in Finite Groups

Many of the results concerning finite groups rely on the well-known Sylow theorems, some of which are stated without proof as follow.

**Theorem 13.1** (Sylow's Theorem). Suppose that  $|G| = p^k m$ , where  $p$  is a prime number not dividing  $m$ . Then  $G$  has a subgroup of order  $p^j$ , for each  $0 \leq j \leq k$ . Moreover, the number of subgroups of order  $p^k$  is a divisor of  $m$  in the congruence class  $[1]_p$  and in particular this subgroup is unique if and only if normal.

Note that Sylow's theorem supercedes that of Cauchy. We state Cauchy's theorem again next as a corollary, followed by another immediate consequence of Sylow's theorem.

**Corollary 13.2** (Cauchy's Theorem). Let  $G$  be a finite group of order divisible by  $p$ , a prime number. Then  $G$  has an element of order  $p$ .

*Proof.* It suffices if  $G$  has a subgroup of order  $p$ , because such subgroup is necessarily generated by an element of the same order. That is what Sylow's theorem says.  $\nabla$

**Corollary 13.3.** Let  $p < q$ , both prime numbers such that  $q \notin [1]_p$ . Then any group of order  $pq$  is isomorphic to  $\mathbb{Z}_{pq}$ .

*Proof.* Under the given conditions, Sylow's theorem says we have a unique, hence normal, subgroups of each order  $p$  and  $q$ , call them  $P$  and  $Q$ , respectively. Let  $a \in P$  and  $b \in Q$ . We will show that  $ab = ba$ . Being normal, they imply  $ba^{-1}b^{-1} \in P$  and  $aba^{-1} \in Q$ . Now let  $x = aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1}$ ; the first identity says  $x \in P$  and the second  $x \in Q$ , hence  $x$  belongs to  $P \cap Q$ , a subgroup whose order divides both  $p$  and  $q$ , so it is trivial. We conclude  $e = x = aba^{-1}b^{-1}$  and  $ab = ba$ .

Next, the map  $\theta : P \times Q \rightarrow G$  such that  $\theta(a, b) = ab$  is a homomorphism because, by what we have shown above,  $\theta((a, b)(c, d)) = acbd = abcd = \theta(a, b)\theta(c, d)$ . The kernel contains  $(a, b)$  for which  $ab = e$ , or  $a = b^{-1}$ . Again this would mean  $a \in P \cap Q$  and  $a = e = b$ . Hence  $\theta$  is one-to-one and, since  $G$  is finite, onto as well. This yields the isomorphism  $G \approx P \times Q \approx \mathbb{Z}_p \times \mathbb{Z}_q \approx \mathbb{Z}_{pq}$  by the Chinese remainder theorem.  $\nabla$

Efforts have been done in order to classify all finite groups of a given order, up to isomorphism. The next table displays all the groups of order up to 15. (There are 14 groups of order 16 and, to mention some of the extremes, 51 of order 32 and 267 of order 64.) As an additional tool, the following theorem is also a useful well-known fact in finite group theory.

**Theorem 13.4.** Every group of order  $p^2$ , where  $p$  is prime, is abelian.

$n$	Groups of order $n$ , up to isomorphism
1	$\mathbb{Z}_1$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6, S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4, Q_8$ (see Exercise 13.1)
9	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$
10	$\mathbb{Z}_{10}, D_5$
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12}, \mathbb{Z}_6 \times \mathbb{Z}_2, A_4, D_6, Q_{12}$ (see remark below)
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}, D_7$
15	$\mathbb{Z}_{15}$
⋮	
$p$	$\mathbb{Z}_p$
$2p$	$\mathbb{Z}_{2p}, D_p$
$p^2$	$\mathbb{Z}_{p^2}, \mathbb{Z}_p \times \mathbb{Z}_p$

*Remark.* The notation  $Q_{12} = \langle a, b \mid a^4 = b^3 = a^3bab = e \rangle$  stands for the group generated by two elements  $a, b$  under the given defining relations. Note that the last identity can be written  $ba = ab^2$ . You can check the Cayley table for the 12 elements of  $\{a^j b^k \mid 1 \leq j \leq 4, 1 \leq k \leq 3\}$  to see why this non-abelian group is neither  $A_4$  nor  $D_6$ .

*Definition.* A group  $G$  is *simple* if it has no normal subgroups other than  $\{e\}$  and  $G$  itself.

Simple groups are an important and difficult topic of finite group theory, closely connected to the study of polynomial equations. Roughly speaking, knowing a normal subgroup  $H$  of  $G$  enables one to study the smaller factor group  $G/H$ . Therefore, identifying finite simple groups will help in the classification problem of finite groups in general.

*Example.* There are no simple groups of order 20. Since  $20 = 4 \times 5$ , by Sylow's theorem any group  $G$  of order 20 has a subgroup of order 5. The number  $n$  of such subgroups divides 4 and belongs to the congruence class  $[1]_5$ . Only  $n = 1$  meets these conditions. Being unique, this subgroup of order 5 is normal, hence  $G$  is not simple.

We have seen in Corollary 6.4 that any group of prime order is simple and is essentially  $\mathbb{Z}_p$ —in fact too simple, as it has no non-trivial subgroups at all. We shall now demonstrate why there are no simple abelian groups other than these.

**Theorem 13.5.** Every simple abelian group is isomorphic to  $\mathbb{Z}_p$  for some prime  $p$ .

*Proof.* For abelian groups, all subgroups are normal, so  $G$  can be normal only if it has no proper subgroups. In particular  $\langle a \rangle = G$  for any non-identity element  $a \in G$ . And we know that the only cyclic groups with no proper subgroups are those of prime order.  $\square$

It has also been proved that there are no non-abelian simple groups of odd order, nor of order twice an odd number. On the other hand, a whole class of non-abelian simple groups of even order is given by the alternating groups.

**Theorem 13.6.** The alternating group  $A_n$  is simple if and only if  $n \geq 5$ .

### Exercise 13

1) The *quaternion group*  $Q_8 = \{\pm E, \pm I, \pm J, \pm K\}$  is a subgroup of  $SL(2, \mathbb{C})$ , where

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

- a) Draw the Cayley table to verify that  $Q_8$  is indeed a subgroup of  $SL(2, \mathbb{C})$ .
  - b) Determine the order of each element in  $Q_8$ .
  - c) Draw the subgroup lattice for  $Q_8$ , noting that it has 4 non-trivial subgroups.
  - d) Show that every subgroup of  $Q_8$  is normal, despite its being non-abelian.
- 2) Classify all groups of order below 100 to which Corollary 13.3 is applicable.
  - 3) Prove that there are only two groups of order 99.
  - 4) Prove that no simple group has order 30.

## To Learn More

Any one of the following textbooks is recommended for further reading and self-study.

1. Joseph A. Gallian, *Contemporary Abstract Algebra*, Sixth Edition 2006, Houghton Mifflin, ISBN 0618514717
2. John F. Humphreys, *A Course in Group Theory*, 1996, Oxford University Press, ISBN 0198534590
3. I. N. Herstein, *Topics in Algebra*, Second Edition 1975, Wiley, ISBN 0471010901
4. W. R. Scott, *Group Theory*, 1987, Dover Publications, ISBN 0486653773