CHAPTER 3

Further Examples of Groups

In this section, we study more examples of groups. We first study the effect of multiplication on integers modulo n, where $n \in \mathbb{N}$. We then look at permutation groups, a very important class in the study of group theory. To conclude the section, we shall have a brief look at dihedral groups, which are motivated by geometric considerations.

3.1. The Groups $\mathbb{Z}_n^*$

Consider the set $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, together with multiplication modulo 8. Clearly, this does not form a group. To see this, it is clear that the only candidate for multiplicative identity is 1. It then follows that the elements $0, 2, 4, 6$ have no inverse.

Suppose now that we remove these "troublemakers", and consider instead the set $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, again with multiplication modulo 8. It is then not too difficult to see that we now have a group.

DEFINITION. We write $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : x \text{ has a multiplicative inverse in } \mathbb{Z}_n\}$ for every $n \in \mathbb{N}$ and $n \geqslant 2$.

PROPOSITION 3.1. *Suppose that $n \in \mathbb{N} \setminus \{1\}$. Then $x \in \mathbb{Z}_n^*$ if and only if the greatest common divisor $(x, n) = 1$.*

PROOF. It is well known that $(x, n) = 1$ if and only if there exist $y, m \in \mathbb{Z}$ such that $xy + nm = 1$ in $\mathbb{Z}$, if and only if there exists $y \in \mathbb{Z}$ such that $xy \equiv 1 \pmod{n}$, if and only if $x \in \mathbb{Z}_n^*$. ◯

EXAMPLES. (1) $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$.
(2) Suppose that $p \in \mathbb{N}$ is prime. Then $\mathbb{Z}_p^* = \{1, 2, ..., p-1\}$.

PROPOSITION 3.2. *Suppose that $n \in \mathbb{N} \setminus \{1\}$, and that $\cdot$ denotes multiplication modulo n. Then $(\mathbb{Z}_n^*, \cdot)$ is an abelian group.*

PROOF. (G4) is obvious from the definition of $\mathbb{Z}_n^*$. Also, (G1) holds, for if $x, y \in \mathbb{Z}_n^*$, then $y' \cdot x'$ is clearly the inverse of $x \cdot y$, so that $x \cdot y \in \mathbb{Z}_n^*$. (G2) follows from the associativity of multiplication modulo n. (G3) follows, as the element 1 is clearly in $\mathbb{Z}_n^*$. Finally (GA) follows from the commutativity of multiplication modulo n. ◯

3.2. Permutation Groups

Let X be a non-empty set. A permutation ϕ on X is a function $\phi : X \to X$ which is one-to-one and onto. Furthermore, if $x \in X$, we denote by $x\phi$ the image of x under the permutation ϕ.

It is not difficult to see that if $\phi : X \to X$ and $\psi : X \to X$ are both permutations on X, then $\phi\psi : X \to X$, defined by $x(\phi\psi) = (x\phi)\psi$ for every $x \in X$, *i.e.* ϕ followed by ψ, is also a permutation on X.

THEOREM 3.3. *Suppose that X is a non-empty set, and $\pi(X)$ denotes the set of all permutations on X. Then $\pi(X)$ forms a group.*

REMARK. We have omitted reference to the group operation, which is clearly composition of functions.

PROOF OF THEOREM 3.3. (G1) holds, for the composition of two one-to-one and onto functions from X to X is also a one-to-one and onto function from X to X. (G2) follows from the associativity of composition of functions. (G3) is satisfied, since the function $i : X \to X$, defined by $xi = x$ for every $x \in X$ is clearly a permutation. Finally, (G4) follows, for if $\phi : X \to X$ is one-to-one and onto, it is well known that an inverse function exists and that it is one-to-one and onto. ◯

We are interested in the special case when X is finite. Then we can assume, without loss of generality, that $X = \{1, 2, \ldots, n\}$, where $n \in \mathbb{N}$. We now let S_n denote the set of all permutations on the set $\{1, 2, \ldots, n\}$.

COROLLARY 3.4. *For every $n \in \mathbb{N}$, S_n forms a group.*

DEFINITION. For every $n \in \mathbb{N}$, the group S_n is called the symmetric group on n symbols.

PROPOSITION 3.5. *For every $n \in \mathbb{N}$, $|S_n| = n!$.*

PROOF. There are n choices for 1ϕ. For each such choice, there are $n - 1$ choices for 2ϕ. And so on. ◯

To represent particular elements of S_n, there are various notations. For example, we can use the notation

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ 1\phi & 2\phi & \ldots & n\phi \end{pmatrix}$$

to denote the permutation ϕ.

EXAMPLE. In S_4,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

denotes the permutation ϕ, where $1\phi = 2$, $2\phi = 4$, $3\phi = 1$ and $4\phi = 3$. On the other hand,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}. \tag{3.1}$$

We may also use the cycle notation. To illustrate this, we continue with the same example.

EXAMPLES. In S_4, the permutations

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

can be represented respectively by the cycles (1 2 4 3) and (1 3 4). Note that in the latter case, since the image of 2 is 2, it is not necessary to include this in the cycle. Furthermore, the information (3.1) can be represented in cycle notation by

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

We also say that the cycles (1 2 4 3), (1 3 4) and (1 2) have lengths 4, 3 and 2 respectively.

(2) In S_6, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$$

can be represented in cycle notation as (1 2 4 3)(5 6).

(3) In S_4, we have (1 2 4 3) = (1 2)(1 4)(1 3).

The last example motivated the following notion.

DEFINITION. Suppose that $n \in \mathbb{N}$. A permutation in S_n that interchanges two numbers among the elements of $\{1, 2, \ldots, n\}$ and leaves all the others unchanged is called a transposition.

REMARK. The following are obvious:

(1) A transposition can be represented by a 2-cycle.

(2) A transposition is its own inverse.

THEOREM 3.6. *Suppose that $n \in \mathbb{N}$.*

(i) *Every permutation in S_n can be written as a product of disjoint cycles. Furthermore, the order of the permutation is the least common multiple of the lengths of the disjoint cycles.*

(ii) *For every subset $\{x_1, x_2, \ldots, x_k\}$ of the set $\{1, 2, \ldots, n\}$, where the elements $x_1, x_2, \ldots, x_k$ are distinct, we have*

$$(x_1\ x_2\ \ldots\ x_k) = (x_1\ x_2)(x_1\ x_3)\ldots(x_1\ x_k);$$

in other words, every cycle can be written as a product of transpositions.

(iii) *Consequently, every permutation in S_n can be written as a product of transpositions.*

PROOF. (i) Let $\phi \in S_n$. Define a relation $\mathcal{R}$ on the set $\{1, 2, \ldots, n\}$ in the following way: For $x, y \in \{1, 2, \ldots, n\}$, we say that $x\mathcal{R}y$ if there exists $k \in \mathbb{Z}$ such that $y = x\phi^k$. It is not difficult to see that $\mathcal{R}$ is an equivalence relation on the set $\{1, 2, \ldots, n\}$. It follows that $\mathcal{R}$ partitions $\{1, 2, \ldots, n\}$ into a disjoint union $Y_1 \cup \ldots \cup Y_m$. For each $j = 1, 2, \ldots, m$, it is easy to see that $x\phi \in Y_j$ for every $x \in Y_j$. It follows that if we now define the function $\phi_j : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ by writing

$$x\phi_j = \begin{cases} x\phi, & \text{if } x \in Y_j, \\ x, & \text{if } x \notin Y_j, \end{cases}$$

then the function ϕ, restricted to Y_j, is a cycle that involves only the elements of Y_j. Furthermore, $\phi = \phi_1 \ldots \phi_m$, a product of disjoint cycles. Suppose now that for every $j = 1, 2, \ldots, m$, the order of ϕ_j is d_j. Let $D = d_1 \ldots d_m$. Then clearly $\phi^D = i$. It follows that the order of ϕ must be a divisor of D. Furthermore, since the different permutations ϕ_j permute elements in the different subsets Y_j of $\{1, 2, \ldots, n\}$, the order of ϕ must also be a multiple of each of $d_1, \ldots, d_m$. The smallest natural number that satisfies these requirements is clearly the least common multi ple of the numbers $d_1, \ldots, d_m$. Note now that the order of a cycle is its length.

(ii) can be checked easily.

(iii) follows on combining (i) and (ii). ◯

REMARK. The first part of Theorem 3.6(i) can also be proved in the following way. Let

$$B = \{j \in \{1, \ldots, n\} : j\phi \neq j\}.$$

If $B = \emptyset$, then the proof is complete. If $B \neq \emptyset$, let m be the smallest element in B. We now let $B_1 = \{m\phi^k : k \in \mathbb{Z}\}$ and $B_2 = \{1, \ldots, n\} \setminus B_1$. Define a permutation $\phi_1 : \{1, \ldots, n\} \to \{1, \ldots, n\}$ by writing

$$x\phi_1 = \begin{cases} x\phi, & \text{if } x \in B_1, \\ x, & \text{if } x \in B_2. \end{cases}$$

Also, define a permutation $\phi_2 : \{1, \ldots, n\} \to \{1, \ldots, n\}$ by writing

$$x\phi_2 = \begin{cases} x, & \text{if } x \in B_1, \\ x\phi, & \text{if } x \in B_2. \end{cases}$$

Then it is not difficult to see that $\phi = \phi_1\phi_2$, that ϕ_1 is a cycle that is disjoint from the permutation ϕ_2. We now repeat the argument on B_2, and note that since $\{1, \ldots, n\}$ is finite, this process must terminate after a finite number of repetitions.

EXAMPLE. In S_9, the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 5 & 1 & 7 & 8 & 4 & 9 & 6 \end{pmatrix}$$

can be written in cycle notation as (1 3 5 7 4)(6 8 9). By Theorem 3.6(ii), we have

$$(1\ 3\ 5\ 7\ 4) = (1\ 3)(1\ 5)(1\ 7)(1\ 4) \quad \text{and} \quad (6\ 8\ 9) = (6\ 8)(6\ 9).$$

Hence the permutation can be represented by (1 3)(1 5)(1 7)(1 4)(6 8)(6 9). Note now that the inverse of (1 3)(1 5)(1 7)(1 4) is (1 4)(1 7)(1 5)(1 3), and the inverse of (6 8)(6 9) is (6 9)(6 8). It is not difficult to see that the inverse of (1 3)(1 5)(1 7)(1 4)(6 8)(6 9) is (6 9)(6 8)(1 4)(1 7)(1 5)(1 3); in other words, the inverse of (1 3 5 7 4)(6 8 9) is (6 9 8)(1 4 7 5 3) = (9 8 6)(4 7 5 3 1). In view of Theorem 3.6(i), we also have that the order of the permutation is 15.

DEFINITION. Suppose that $n \in \mathbb{N}$ and $n \geqslant 2$. Then a permutation in S_n is said to be odd (resp. even) if it is representable as the product of an odd (resp. even) number of transpositions.

REMARKS. (1) It can be shown that no permutation can be simultaneously odd and even.
(2) Note that an odd permutation can have even order. Consider, for example, a transposition.

DEFINITION. Suppose that $n \in \mathbb{N}$ and $n \geqslant 2$. We denote by A_n the set of all even permutations in S_n.

THEOREM 3.7. *Suppose that $n \in \mathbb{N}$ and $n \geqslant 2$. Then*

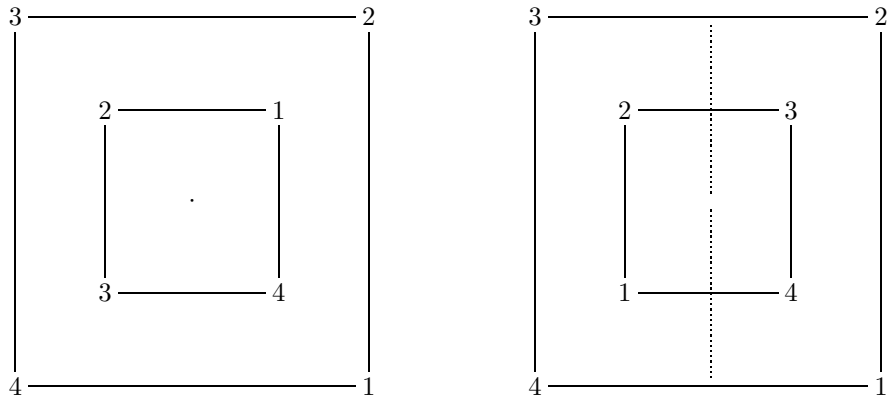
(i) *A_n is a subgroup of S_n; and*
(ii) *$|A_n| = n!/2$.*

PROOF. (i) Clearly A_n is non-empty, since the identity permutation i is obviously even. Suppose now that $\phi, \psi \in A_n$. Then clearly $\phi' \in A_n$. It follows that $\psi \circ \phi' = \phi'\psi \in A_n$. It now follows from Theorem 1E that A_n is a subgroup of S_n.
(ii) If $\phi \in A_n$, then clearly $\phi(1\ 2) \in S_n \setminus A_n$. Define $f : A_n \to (S_n \setminus A_n)$ by writing $f(\phi) = \phi(1\ 2)$ for every $\phi \in A_n$. It is not difficult to show that f is one-to-one and onto. The result follows. ◯

DEFINITION. For every $n \in \mathbb{N} \setminus \{1\}$, the group A_n is called the alternating group on n symbols.

3.3. Dihedral Groups

Suppose that we draw a square on a cardboard, carefully label the four corners $(1, 2, 3, 4)$, cut the square out, throw it in the air, and then put it back without looking. Then either the square can end up placed similarly as before, or some or all of its corners end up differently from before. The following are two examples. The picture on the left shows that the square has been rotated clockwise by 90°, while the picture on the right shows that the square has been flipped (reflected) about the vertical axis.



We can interpret the left hand picture as representing the permutation $(1\ 2\ 3\ 4)$ of S_4 and the right hand picture as representing the permutation $(1\ 4)(2\ 3)$ of S_4. Now write $\rho = (1\ 2\ 3\ 4)$ and $\phi_1 = (1\ 4)(2\ 3)$. We can also write $\phi_2 = (1\ 2)(3\ 4)$ for the reflection across the other axis. We can then easily check that the possibilities can be represented by the eight elements below:

$$\begin{array}{llll} i, & \rho = (1\ 2\ 3\ 4), & \rho^2 = (1\ 3)(2\ 4), & \rho^3 = (1\ 4\ 3\ 2), \\ \phi_1 = (1\ 4)(2\ 3), & \phi_1\rho = (2\ 4), & \phi_1\rho^2 = (1\ 2)(3\ 4), & \phi_1\rho^3 = (1\ 3). \end{array} \tag{3.2}$$

Note that we have, for example, $\phi_2 = (1\ 2)(3\ 4) = \phi_1\rho^2$.
Note also that the permutations like

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & \diamondsuit & \diamondsuit \end{pmatrix}$$

are impossible. The corner 2 is always next to the corner 1. Since the corner 1 ends up at position 1, the corner 2 can only end up at position 2 or 4, but not 3 which is diagonally opposite to 1.
We can check that the set

$$D_4 = \{i, \rho, \rho^2, \rho^3, \phi_1, \phi_1\rho, \phi_1\rho^2, \phi_1\rho^3\}$$

forms a proper subgroup of S_4. The group D_4 is called a dihedral group.

We can describe the dihedral group D_n for every $n \in \mathbb{N}$ with $n \geqslant 3$ in a similar way. We start with a regular n-gon and label the vertices 1 to n consecutively. We then write $\rho = (1\ 2\ \ldots\ n)$ and take ϕ to denote a fixed reflection. Then it can be proved that for every $n \geqslant 3$,

$$D_n = \{i, \rho, \rho^2, \ldots, \rho^{n-1}, \phi, \phi\rho, \phi\rho^2, \ldots, \phi\rho^{n-1}\}$$

is a subgroup of S_n. Note also that for every $n \in \mathbb{N}$ with $n \geqslant 3$, $|D_n| = 2n$ and $|S_n| = n!$. It follows that $D_3 = S_3$ and that for every $n \geqslant 4$, D_n is a proper subgroup of S_n.

Problems for Chapter 3

1. Construct the group table for $\mathbb{Z}_{30}^*$, and calculate the order of each of the elements.

2. For each of the following permutations in S_9, express the permutation as a product of disjoint cycles and calculate the order of the permutation. Furthermore, express each permutation as a product of transpositions, and state whether the permutation is odd or even.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 7 & 4 & 8 & 5 & 9 & 6 \end{pmatrix}$

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 5 & 1 & 2 & 8 & 9 & 3 & 7 \end{pmatrix}$

3. By expressing each of its elements as a product of disjoint cycles, find all the possible orders of elements of S_4.

4. By investigating all the possible cycle structures of its elements when expressed as products of disjoint cycles, find all the possible orders of elements of S_8.

5. Show that A_3 is cyclic.

6. Show that A_4 is not abelian and not cyclic. How about A_n for $n > 4$? Justify your assertion.

7. Suppose that $(G, *)$ is a group, and that $a \in G$. Define a function $\phi : G \to G$ by writing $x\phi = x * a$ for every $x \in G$. Prove that $\phi : G \to G$ is a permutation on G.

8. Describe the group D_6 in terms of permutations in S_6.