Lecture Notes
MTH223A

Yvette Fajardo-Lim, Ph.D.
Department of Mathematics and Statistics
De La Salle University - Manila

Contents

Chapter 1

Fundamental Concepts

This chapter introduces the fundamental concepts that are a prerequisite in studying abstract algebra.

1.1 Functions

The concept of a function is fundamental to nearly all areas of mathematics. The term mapping is also used for the concept of a function. The basic idea is to assign a rule of association between the elements of the first set and those of a second set. The association is to be such that for each element in the first set, there is one and only one associated element in the second set.

Definition 1.1. *Let X and Y be two nonempty sets. A* **mapping or a function** *f* **from** *X* **to** *Y is a rule denoted by $f : X \to Y$ which assigns to each element x of X a* **unique** *element y of Y. In this case, we write $y = f(x)$ to mean that the value of f at x is y. y is called the* **image** *of x and x is the* **pre-image** *of y under f. The set X is called the* **domain** *of f and Y the* **codomain** *of f. The* **range** *of f is the set $\{f(x)|x \in X\}$.*

The rule is usually given in the form of an equation, especially when the sets involved are infinite.

Example 1.1. The following equations define functions from $\mathbb{R}$ to $\mathbb{R}$.

1. Given $2x + y = 3$, then the function $y = 3 - 2x$ defines the number y to be $3 - 2x$. If $x = 2$ then $y = 3 - 2(2) = -1$. The domain is the set of allowable x-values, in this case, the set of all real numbers. The range, which consists of the resulting y-values is the also set of all real numbers.

2. The formula $y = x^2$ defines the number y to be the square of the number x. If $x = 5$, then $y = 5^2 = 25$. The domain is the set of all real numbers. The range is the set of nonnegative real numbers.

Definition 1.2. *A function f with domain D is said to be* **one-to-one** *or* **injective** *if whenever $f(x_1) = f(x_2)$ implies $x_1 = x_2$ for all $x_1, x_2 \in D$.*

Example 1.2. Let $f : \mathbb{R} \to \mathbb{R}$ and $f(x) = 3 - 2x$. To show that f is one-to-one, let $f(x_1) = f(x_2)$ then

$$\begin{aligned} 3 - 2x_1 &= 3 - 2x_2 \\ 3 - 2x_1 - 3 &= 3 - 2x_2 - 3 \\ -2x_1 &= -2x_2 \\ -2x_1\left(-\frac{1}{2}\right) &= -2x_2\left(-\frac{1}{2}\right) \\ x_1 &= x_2 \end{aligned}$$

Hence, f is injective.

Definition 1.3. *A function $f : X \to Y$ is said to be* **onto** *or* **surjective** *if $f(X) = Y$.*

Example 1.3. Again, let $f : \mathbb{R} \to \mathbb{R}$ and $f(x) = 3 - 2x$. To show that f is surjective, we choose an arbitrary element $y \in \mathbb{R}$. We have to find x such that $f(x) = y$.

$$\begin{aligned} 3 - 2x &= y \\ -2x &= y - 3 \\ x &= \frac{y-3}{-2} \in \mathbb{R} \end{aligned}$$

and

$$\begin{aligned} f(x) &= f\left(\frac{y-3}{-2}\right) \\ &= 3 - 2\left(\frac{y-3}{-2}\right) \\ &= 3 - \left(\frac{y-3}{-1}\right) \\ &= 3 - \left(\frac{-y+3}{1}\right) \\ &= 3 + y - 3 \\ &= y \end{aligned}$$

Hence, f is surjective.

Definition 1.4. *A function f is said to be* **bijective** *if it is both one-to-one and onto. A bijective function is also called a* **one-to-one correspondence**.

Example 1.4. From examples 1.2 and 1.2, the function $f(x) = 3 - 2x$ is a bijective function.

Definition 1.5. *Let $f : X \to Y$ and $g : Y \to Z$ be functions. The* **composition** *$f \circ g$ of f and g is the function from X to Z defined by the equation $(f \circ g)(x) = f(g(x))$ for all $x \in X$.*

Example 1.5. Let $f : \mathbb{R} \to \mathbb{R}$ and $f(x) = 3 - 2x$. Let $g : \mathbb{R} \to \mathbb{R}$ and $f(x) = x^2$.

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g(3-2x) \\ &= (3-2x)^2 \\ &= 9 - 12x + 4x^2\end{aligned}$$

and

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= f(x^2) \\ &= 3 - 2x^2\end{aligned}$$

Theorem 1.1. Properties of Functions
Given functions $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then

1. *$h \circ (g \circ f) = (h \circ g) \circ f$ (associativity)*
2. *If f and g are one-to-one, then $(g \circ f)$ is one-to-one.*
3. *If f and g are onto, then $(g \circ f)$ is onto.*
4. *If f is one-to-one and onto, then there is a function f^{-1} from B onto A such that $f^{-1}(f(a)) = a$ for all a in A and $f(f^{-1}(b)) = b$ for all b in B.*

Exercises.

1. For each of the following mappings $f : \mathbb{Z} \to \mathbb{Z}$ given below, determine if the mapping is injective, surjective, or bijective.

   (a) $f(x) = 2x$

   (b) $f(x) = \begin{cases} x & \text{if } x \text{ is even} \\ 2x - 1 & \text{if } x \text{ is odd} \end{cases}$

   (c) $f(x) = |x|$

   (d) $f(x) = \begin{cases} x & \text{if } x \text{ is even} \\ \dfrac{x-1}{2} & \text{if } x \text{ is odd} \end{cases}$

1.2 Divisibility of Integers

The integers $\mathbb{Z}$ comprise the natural numbers $\mathbb{N}$(or $\mathbb{Z}^+$), the number 0, and the negative integers, which we will denote by $\mathbb{Z}^-$. When an integer is divided by a second nonzero integer, the quotient may or may not be an integer. For instance, $\frac{24}{8} = 3$ is an integer while $\frac{17}{5} = 3.4$ is not. This observation leads to the following definition.

Definition 1.6. *An integer b is **divisible** by an integer $a \neq 0$ if there exists another integer c such that $b = ac$. In symbols, we write $a|b$ if b is divisible by a, and $a \not| b$ if b is not divisible by a.*

Example 1.6.

1. $3|12$ because there exists $c = 4$ such that $12 = 3 \cdot 4$.
2. $3 \not| 16$ because there is no $c \in \mathbb{Z}$ such that $16 = 3 \cdot c$.

Other terms for the divisibility property $a|b$ is that a is a divisor of b, and that b is a multiple of a.

Theorem 1.2.

1. *If $a|b$ then $a|bc$ for any integer c.*
2. *If $a|b$ and $b|c$ then $a|c$ for any integer c.*
3. *If $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers x and y.*
4. *If $a|b$ and $b|a$ then $a = \pm b$.*
5. *If $a|b$ and $a > 0, b > 0$ then $a \leq b$.*
6. *$a|b$ if and only if $ma|mb, m \neq 0$*

Illustration 1.1.

1. Since $11|66$ then theorem 1.2 part 1 tells us that $11|330$ because $330 = 66 \cdot 5$.
2. Since $11|66$ and $66|198$ then theorem 1.2 part 2 tells us that $11|198$.
3. Since $3|21$ and $3|33$ then theorem 1.2 part 3 tells us that
$$3|(5 \cdot 21 - 3 \cdot 33) = 105 - 99 = 6.$$
4. Since $7| - 7$ and $-7|7$ then theorem 1.2 part 4 tells us that $7 = -(-7)$.
5. Since $25|75$ then theorem 1.2 part 5 tells us that $25 < 75$.
6. Theorem 1.2 part 6 tells us that $8|64$ if and only if $16|128$.

Remark: If $a|b_i$ for $i = 1, 2, \ldots, n$ then $a|\sum_{i=1}^{n} b_i x_i$ for any integers $x_1, x_2, \ldots, x_n$. This is a generalization of theorem 1.2 part 3.

The next result is a formal statement of the outcome when any integer b is divided by any positive integer. For example, if 25 is divided by 7, the quotient is 3 and the remainder is 4. These numbers are related by the equality $25 = 7 \cdot 3 + 4$. In general, we have the following theorem.

Theorem 1.3. ***The Division Algorithm.*** *If a and b are integers with $a > 0$, there exist unique integers q and r such that $b = aq + r$.*

Illustration 1.2. If $a = 133$ and $b = 21$, then $q = 6$ and $r = 7$, since $133 = 21 \cdot 6 + 7$. Likewise, if $a = -50$ and $b = 8$, then $q = -7$ and $r = 6$ since $-50 = 8(-7) + 6$.

Definition 1.7. *The integer a is called a **common divisor** of the integers b and c if $a|b$ and $a|c$.*

Remarks:

1. If b and c are not both zero then they have only a finite number of common divisors since any nonzero integer has only a finite number of divisors.
2. If $b = 0$ and $c = 0$, then every integer $a \neq 0$ is a common divisor of b and c.

Example 1.7.

1. If $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$.
2. If $b = 0$ and $c = 0$, there are infinite number of common divisors.

Definition 1.8. *The positive integer a is said to be the **greatest common divisor** of b and c if*

1. *$a|b$ and $a|c$*
2. *$d|b$ and $d|c \Rightarrow d|a$*

We write (b, c) to denote the greatest common divisor of b and c.

Example 1.8. From example 1.7, if $b = 4$ and $c = 6$, the common divisors of b and c are $\pm 1, \pm 2$. Hence, $(4, 6) = 2$.

Remark: If $(b, c) = g$ then there exists integers x and y such that $g = bx + cy$.

Example 1.9. Since $(4, 6) = 2$ then $2 = 4 \cdot 2 + 6(-1)$ where $x = 2$ and $y = -1$.

The proof of the following theorem may be found from the book of Niven.

Theorem 1.4. *The greatest common divisor of b and c can be characterized in the following ways:*

1. *it is the least positive value of $bx + cy$ where x and y ranges over all integers;*
2. *it is the positive common divisor of b and c that is divisible by every common divisor.*

Definition 1.9. *If $(a, b) = 1$ then a and b are **relatively prime** and if $(a_1, a_2, \ldots, a_n) = 1$ then $a_1, a_2, \ldots, a_n$ are **relatively prime**.*

Note that If $(a, b) = 1$ then we can also say that a and b are coprime, or a is prime to b.

Example 1.10. $(2,5) = (3,5) = 1$ then 2, 3 and 5 are relatively prime.

Theorem 1.5. *If $c|ab$ and $(c,a) = 1$ then $c|b$.*

Illustration 1.3. $3|66$ where $(3,11) = 1$, then $3|6$.

Theorem 1.6. *The Euclidean Algorithm. Given integers b and $c > 0$, we make a repeated application of the division algorithm to obtain a series of equations,*

$$\begin{aligned} b &= cq_1 + r_1, \quad 0 < r_1 < c, \\ c &= r_1q_2 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2, \\ &\vdots \\ r_{j-2} &= r_{j-1}q_j + r_j, \quad 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_{j+1} + 0. \end{aligned}$$

Then $(b,c) = r_j$, the last nonzero remainder in the division process. Values of x and y in $(b,c) = bx + cy$ can be obtained by writing each r_i as a linear combination of b and c.

Example 1.11. Find (963,657).

$$\begin{aligned} 963 &= 657(1) + 306 && (1.1) \\ 657 &= 306(2) + 45 && (1.2) \\ 306 &= 45(6) + 36 && (1.3) \\ 45 &= 36(1) + 9 && (1.4) \\ 36 &= 9(4) + 0 && (1.5) \end{aligned}$$

Hence, (963,657)=9.

Example 1.12. Find x, y such that $9 = 963x + 657y$.

$$\begin{aligned} 9 &= 45 - 36 && \text{from equation } 1.4 \\ &= 45 - (306 - 45(6)) && \text{from equation } 1.3 \\ &= 45(7) - 306 \\ &= [657 - 306(2)](7) - 306 && \text{from equation } 1.2 \\ &= 657(7) - 306(15) \\ &= 657(7) - (963 - 657)(15) && \text{from equation } 1.1 \\ &= 963(-15) + 657(22) \end{aligned}$$

Hence, $x = -15$ and $y = 22$

Theorem 1.7. *If $p|ab$ where p is a prime, then $p|a$ or $p|b$. Generally, if $p|a_1a_2\ldots a_n$ then $p|a_i$ for some i.*

Illustration 1.4. $11|(2 \cdot 121)$ implies that $11|121$ since $(2,11) = 1$ and $5|(4 \cdot 9 \cdot 25)$ implies that $5|25$.

Exercises.

1. Find $(435, 377)$, and find x, y such that $(435, 377) = 435x + 377y$.
2. Find $(3553, 527)$, and find x, y such that $(3553, 527) = 3553x + 527y$.
3. Which of the integers $0, 1, \ldots, 10$ can be expressed in the form $12m + 20n$, where m, n are integers?
4. Give a proof by induction to show that each number in the sequence $12, 102, 1002, 10002, \ldots$, is divisible by 6.

1.3 Equivalence Relations and Modular Arithmetic

Let S be a non-empty set. A relation on S is a statement about pairs of elements of S, which may be true for some pairs and false for others. For example, if $S = \mathbb{R}$, the statement $a \leq b$ is true for some choices of a and b (e.g. $a = 1, b = 3$) and false for others (e.g. $a = 5, b = 2$); equally, if $S = \{$ Algebra students $\}$, the statement "a is in the same college as b" is true for some pairs and false for others.We usually use $\sim$ to stand for a relation, and we write "$a \sim b$ " to mean "a is related to b under the relation $\sim$", and "$a \not\sim b$ " to mean "a is not related to b under the relation $\sim$"; thus for the relation of "less than or equal to" on $\mathbb{R}$ we have $2 \sim 7$ and $6 \not\sim 3$.

Definition 1.10. *An **equivalence relation** $\sim$ on a set S is a relation that is:*

1. *Reflexive.*

   $a \sim a$ for all $a \in S$.

2. *Symmetric.*

   Whenever $a \sim b$, then $b \sim a$.

3. *Transitive.*

   If $a \sim b$ and $b \sim c$ then $a \sim c$.

*If a and b are related this way we say that they are **equivalent** under $\sim$. If $a \in S$, then the set of all elements of S that are equivalent to a is called the **equivalence class** of a denoted by $[a]$. In set notation,*

$$[a] = \{x \in S | x \sim a\}$$

Example 1.13.

1. Let $S = \{$ Algebra students $\}$, and let $a \sim b$ if a is in the same college as b. Clearly $\sim$ is reflexive since each Algebra student is in the same college as himself or herself. $\sim$ is also symmetric since if a is in the same college as b then b is in the same college as a. Lastly, $\sim$ is transitive since if a is in the same college as b, who is in the same college as c, then clearly a is in the same college as c. Therefore, $\sim$ is an equivalence relation on S. The equivalence class of a is the set of all Algebra students in the same college as a.

2. Let $S = \mathbb{R}$, and let $a \sim b$ if $a \leq b$.

   (a) Reflexive.
   $a \sim a$ for all $a \in S$ implies $a \leq a$. Hence, $\sim$ is reflexive.

   (b) Symmetric.
   If $a \sim b$, then $a \leq b$ but $b \geq a$. Thus, $\sim$ is not symmetric.

   (c) Transitive.
   If $a \sim b$ and $b \sim c$ then $a \leq b$ and $b \leq c$ which implies that $a \leq c$. Therefore, $\sim$ is transitive.

   Since $\sim$ is not symmetric, then $\sim$ is not an equivalence relation on S.

3. Let $S = \{(a, b)|a, b \in \mathbb{Z}^+\}$, and let $(a, b) \sim (c, d)$ if $a + d = b + c$.

   (a) Reflexive.
   $(a, b) \sim (a, b)$ for all $(a, b) \in S$ then $a + b = b + a$. Hence, $\sim$ is reflexive by the commutative property of addition.

   (b) Symmetric.
   If $(a, b) \sim (c, d)$, then $a + d = b + c$. But $b + c = c + b$ and $a + d = d + a$. Hence, $a+d = b+c = c+b = d+a$ which gives us $c+b = d+a$ and therefore $(c, d) \sim (a, b)$ which implies that $\sim$ is symmetric.

   (c) Transitive.
   If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ then $a + d = b + c$ and $c + f = d + e$. Hence,

$$\begin{aligned} (a+d)+(c+f) &= (b+c)+(d+e) \\ (a+d)+(c+f)-c-d &= (b+c)+(d+e)-c-d \\ a+f &= b+e \end{aligned}$$

   Therefore, $(a, b) \sim (e, f)$ and $\sim$ is transitive.

   Therefore $\sim$ is an equivalence relation on S.

   Under the relation $\sim$ in the set S, the equivalence classes are as follows:

$$\begin{aligned} [(1,1)] &= \{(a,b)|(a,b) \sim (1,1)\} \\ &= \{(a,b)|a+1 = b+1\} \\ &= \{(a,b)|a = b\} \\ &= \{(a,a)|a \in \mathbb{Z}^+\} \\ [(1,2)] &= \{(a,b)|(a,b) \sim (1,2)\} \\ &= \{(a,b)|a+2 = b+1\} \\ &= \{(a,b)|a+1 = b\} \\ &= \{(a,a+1)|a \in \mathbb{Z}^+\} \\ [(1,3)] &= \{(a,b)|(a,b) \sim (1,3)\} \end{aligned}$$

$$
\begin{aligned}
&= \{(a,b)|a+3=b+1\}\\
&= \{(a,b)|a+2=b\}\\
&= \{(a,a+2)|a\in\mathbb{Z}^+\}\\
&\vdots\\
[(1,n)] &= \{(a,b)|(a,b)\sim(1,n)\}\\
&= \{(a,b)|a+n=b+1\}\\
&= \{(a,b)|a+(n-1)=b\}\\
&= \{(a,a+(n-1))|a\in\mathbb{Z}^+\}\\
[(2,1)] &= \{(a,b)|(a,b)\sim(2,1)\}\\
&= \{(a,b)|a+1=b+2\}\\
&= \{(a,b)|a=b+1\}\\
&= \{(b+1,b)|b\in\mathbb{Z}^+\}\\
[(3,1)] &= \{(a,b)|(a,b)\sim(3,1)\}\\
&= \{(a,b)|a+1=b+3\}\\
&= \{(a,b)|a=b+2\}\\
&= \{(b+2,b)|b\in\mathbb{Z}^+\}\\
&\vdots\\
[(n,1)] &= \{(a,b)|(a,b)\sim(n,1)\}\\
&= \{(a,b)|a+1=b+n\}\\
&= \{(a,b)|a=b+(n-1)\}\\
&= \{(b+(n-1)),b|b\in\mathbb{Z}^+\}
\end{aligned}
$$

Definition 1.11. *Let S be a set. A family $S_i, i=1,\dots n$ of subsets of S is called a* ***partition*** *of S if the following are satisfied:*

1. $S_i \neq$ *for all* $i, i=1,\dots n$
2. $S_i \cap S_j =$ *for all* $i \neq j$
3. $\bigcup_{i=1}^{n} S_i = S$

Example 1.14. The equivalence classes in the examples above partition the set S. First, since $\sim$ is reflexive then $a \in [a]$, hence, each equivalence class is nonempty since each element a lies in at least one equivalence class. Secondly, assume that the equivalence classes $[a]$ and $[b]$ have non-empty intersection, then we must show that they are equal. Take $c \in [a] \cap [b]$; then $c \sim a$ and $c \sim b$, and by symmetry we have $a \sim c$, and then by transitivity $a \sim b$ (and $b \sim a$ by symmetry again). Now given $d \sim [a]$ we have $d \sim a$, so by transitivity $d \sim b$, giving $d \in [b]$, so $[a] \subseteq [b]$; similarly $[b] \subseteq [a]$, and so $[a] = [b]$ as required. Lastly, the union of all these equivalence classes is the set S.

Note that if $[a]$ is any equivalence class and b is any representative of $[a]$, then $[b] = [a]$ for $b \in [b]$, so the class containing b is unique, and must be the same class. Note also that the argument above uses all three properties of reflexivity, symmetry and transitivity; if we have a relation which does not have all of these properties we can define sets $[a]$ as above, but they will not break the set up into pieces in the same way. For example, in the "less than or equal to" relation the set of elements related to $a \in \mathbb{R}$ is the interval $(-\infty, a]$; any two such sets have non-empty intersection, but they are all distinct.

Remark: Any equivalence relation on S gives a partition of S and any partition gives rise to an equivalence relation by defining $a \sim b$ if and only if a and b belong to the same subset.

We will now apply the above discussion to the set of integers, $\mathbb{Z}$. We shall define a relation on $\mathbb{Z}$, show that it is an equivalence relation, and then consider the partition into equivalence classes.

Definition 1.12. *Let $n \in \mathbb{Z}^+$. Given $a, b \in Z$, a **is congruent to** b **modulo** n if a and b have the same remainder on division by n, or equivalently that $n|(a-b)$. We write*

$$a \equiv b(mod\ n)$$

to indicate that a is congruent to b modulo n.

Example 1.15.

1. $21 \equiv 9(\text{mod } 4)$ because $21 = (5)(4) + 1$ and $9 = (2)(4) + 1$ or equivalently $21 - 9 = 12 = (3)(4)$.
2. $15 \equiv 0(\text{mod } 5)$ because $15 - 0 = 15 = (3)(5)$.
3. $1 \equiv 16(\text{mod } 3)$ because $1 - 16 = -15 = (-5)(3)$.

This gives the relation of congruence modulo n on $\mathbb{Z}$, defined by $a \sim b$ if and only if a is congruent to b modulo n.

Theorem 1.8. *The relation congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

Since congruence modulo n is an equivalence relation on $\mathbb{Z}$ then we have to determine the equivalence classes, which we will call *congruence classes* in this case. First recall from Division Algorithm that given $a \in \mathbb{Z}$ we may divide by n to give a quotient and a remainder; i.e.,

$$a = qn + r, \qquad 0 \leq r < n.$$

Moreover, this expression is unique. Thus each element of $a \in \mathbb{Z}$ is congruent modulo n to exactly one of $0, 1, \ldots, n-1$; so the congruence classes are

$$[0], [1], \ldots, [n-1]$$

We set $\mathbb{Z}_n$ to be the set of these congruence classes. Hence there are n elements in $\mathbb{Z}_n$.

Example 1.16. If we take n=5, we obtain the following congruence classes:

$$\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}$$

We have $[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}$, and the intersection of any two of these classes is empty. Moreover if we take any other element $a \in \mathbb{Z}$, then $[a]$ is equal to one of the five classes listed; for example, $[9] = [4]$, since $9 \in [4]$. Thus $\mathbb{Z}_n = \{[0], [1], [2], [3], [4]\}$. For convenience, we will use $\mathbb{Z}_n = \{0, 1, 2, 3, 4\}$.

Exercises.

1. Determine if the relation described is an equivalence relation on the given set. For those that are equivalence relations, describe the equivalence classes: (*Fraleigh, 11-17, p.14*)
   (a) Let $S = \mathbb{Z}$, $a \sim b$ if $ab > 0$
   (b) Let $S = \mathbb{R}$, $a \sim b$ if $|a| = |b|$
   (c) Let $S = \mathbb{R}$, $a \sim b$ if $a \geq b$
   (d) Let $S = \mathbb{R}$, $a \sim b$ if $|x - y| \leq 3$
   (e) Let $S = \mathbb{Z}^+$, $a \sim b$ if a and b have the same number of digits in the usual base ten notation
   (f) Let $S = \mathbb{Z}^+$, $a \sim b$ if $a - b$ is divisible by 2
2. On the set $\{(a, b)\}$ of all ordered pairs of positive integers, define $(x_1, y_1) \sim (x_2, y_2)$ if and only if $x_1 y_2 = x_2 y_1$. Show that this defines an equivalence relation.
3. On the set of all $n \times n$ matrices over $\mathbb{R}$, define $A \sim B$ if and only if there exists an invertible matrix P such that $PAP^{-1} = B$. Check that $\sim$ defines an equivalence relation.

Chapter 2

Groups and Subgroups

An introduction to the theory of groups is presented in this chapter.

2.1 Binary Operations

We are familiar with the operations of addition, subtraction and multiplication on real numbers. These are examples of *binary operations*. When we speak of a binary operation on a set, we have in mind a process that combines two elements of the set to produce a third element of the set. This third element, the result of the operation on the first two must be unique. That is, there must be one and only one result from the combination. We make the following formal definition.

Definition 2.1. *Let G be a nonempty set. A* **binary operation *** *on G is a rule for combining two elements of G to produce another element of G; given $a, b \in G$ we write $a * b$ for the element produced by combining a with b. Thus, we can say that G is* **closed with respect to** $*$.

Example 2.1.

1. If $G = \mathbb{R}$, then $a * b = a + b$ defines a binary operation on G since $a + b \in \mathbb{R}$.
2. If $G = \mathbb{Z}$, then $a * b = ab$ defines a binary operation on G since $ab \in \mathbb{Z}$.
3. If $G = \mathbb{Z}^+$, then $a * b = a - b$ does not define a binary operation on G, because if $b \geq a$ then $a - b \notin \mathbb{Z}^+$. However, if we replace $\mathbb{Z}^+$ by $\mathbb{Z}$, then we do obtain a binary operation.
4. If $G = \mathbb{Z}$, then $a * b = \frac{a}{b}$ does not define a binary operation on G, because if b does not divide a exactly then $\frac{a}{b} \notin \mathbb{Z}$. If we set $G = \mathbb{Q}$ instead, we still do not have a binary operation, because if $b = 0$ then $\frac{a}{b}$ is not defined. However, if we set $\mathbb{Q}^* = \mathbb{Q} \backslash \{0\}$, then $\frac{a}{b}$ does define a binary operation on $\mathbb{Q}^*$.

Remarks: The important things to note are:

1. $a * b$ must be defined for all $a, b \in G$;
2. $a * b$ must itself be an element of G for all $a, b \in G$.

Exercises. Determine whether the given operations are binary operations or not.

1. $G = \mathbb{Z}^-, a * b = min(a, b)$
2. $G = \mathbb{R}^-, a * b = ab$
3. $G = \mathbb{Z}/\{-1\}, a * b = a + b + ab$
4. $G = \mathbb{R}^+, a * b = ab - 1$

e. $G = \mathbb{Z},\ a * b = a - b$

f. $G = \mathbb{Q},\ a * b = \dfrac{ab}{2}$

g. $G = \mathbb{Z}^+,\ a * b = a^b$

2.2 Groups: Definition and Examples

Definition 2.2. *A **semigroup** is a set G together with a binary operation * which is associative. That is, for all $a, b, c \in G, (a * b) * c = a * (b * c)$.*

Thus $*$ is associative if the position of brackets does not matter when three elements are combined.

Example 2.2.

1. Addition on the set $\mathbb{Z}$ is associative, since $(a+b)+c = a+(b+c)$ for all $a, b, c \in \mathbb{Z}$. Hence, $\mathbb{Z}$ under addition is a semigroup.
2. Multiplication on the set $\mathbb{Z}$ is associative, since $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{Z}$. Hence, $\mathbb{Z}$ under multiplication is a semigroup.
3. Subtraction on the set $\mathbb{Z}$ is not associative, e.g. $(3 - 2) - 1 = 1 - 1 = 0$ while $3 - (2 - 1) = 3 - 1 = 2$. This tells us that $\mathbb{Z}$ under subtraction is not a semigroup.

Definition 2.3. *A **monoid** is a semigroup $(G, *)$ if there exists an element e of G where $a * e = a = e * a$ for all $a \in G$; e is called an **identity element** of G.*

Thus an element is an identity if it leaves every element unchanged.

Example 2.3.

1. Addition on the set $\mathbb{Z}$ has identity 0 since $a + 0 = a = 0 + a$ for all $a \in \mathbb{Z}$. Hence, the semigroup $(\mathbb{Z}, +)$ is a monoid.
2. Multiplication on the set $\mathbb{Z}$ has identity 1, since $a1 = a = 1a$ for all $a \in \mathbb{Z}$. Hence, the semigroup $(\mathbb{Z}, \bullet)$ is a monoid.

Definition 2.4. *A **group** is a monoid $(G, *)$ if for all $a \in G$ there exists $a^{-1} \in G$ which satisfies the property $a * a^{-1} = e = a^{-1} * a$ for all $a \in G$; a^{-1} is called the **inverse element of** a.*

Thus an inverse of a is an element which when combined with it gives the identity.

Example 2.4.

1. For addition on $\mathbb{Z}$, the inverse of the element a is $-a$, since $a+(-a) = 0 = (-a)+a$. Hence, the monoid $(\mathbb{Z}, +)$ is a group.

2. For multiplication on $\mathbb{Z}$, the only elements having inverses are 1 and -1 and in each case the inverse is the element itself. Hence, the monoid $(\mathbb{Z}, \bullet)$ is not a group.

We may also consider other binary operations which are not as simple as the ones mentioned above.

Example 2.5.

1. The binary operation defined on $\mathbb{Z}$ by $a * b = a + b + 1$ is associative;

   $(a*b)*c = (a+b+1)*c = a+b+1+c+1 = a+b+c+2 = a*(b+1+c) = a*(b*c)$.

   The identity is -1, as $(-1) * a = -1 + a + 1 = a = a + (-1) + 1 = a * (-1)$ for all a and the element a has inverse $-a - 2$, as $a * (-a - 2) = a + (-a - 2) + 1 = -1 = (-a - 2) + a + 1 = (-a - 2) * a$.

2. The binary operation defined on $\mathbb{Z}$ by $a * b = 2a + 2b$ is not associative, e.g., $(1 * 2) * 3 = 6 * 3 = 18$ while $1 * (2 * 3) = 1 * 10 = 22$; it has no identity, because if $e * a = a$ then $2e + 2a = a$, which requires $2e = -a$, and no element e can satisfy this for all .

3. The binary operation defined on $\mathbb{Z}$ by $a * b = ab^2 + a + b$ is not associative, since $(1 * 2) * 1 = 7 * 1 = 15$ while $1 * (2 * 1) = 1 * 5 = 31$; however, it has identity 0, as $a * 0 = 0 + a + 0 = a$ and $0 * a = 0 + 0 + a = a$ for all $a \in \mathbb{Z}$.

Remarks: A group is a set together with an associative operation such that every element has an inverse and any pair of elements can be combined without going outside the set. This latter condition is called *closure*. To test if $(G, *)$ is a group, the following properties must be verified.

1. **Closure.** G is closed under $*$. That is, if $a, b \in G$ then $a * b \in G$;

2. **Associativity**. For all $a, b, c \in G, (a * b) * c = a * (b * c)$.;

3. **Identity**. There is an e such that $a * e = a = e * a$ for all $a \in G$;

4. **Inverses**. For all $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$.

Example 2.6.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups under addition.

2. $\mathbb{Q}\backslash\{0\}, \mathbb{R}\backslash\{0\}, \mathbb{C}\backslash\{0\}$ are groups under multiplication.

3. The set of bijections $X \to X$ (for any non-empty set X) is a group under composition of functions.

4. The set of invertible $n \times n$ matrices with real entries (for any $n > 1$) is a group under matrix multiplication.

Note also that there is no requirement that the binary operation be commutative.

Definition 2.5. *A group $(G, *)$ whose binary operation is commutative is called **abelian**. That is, $a * b = b * a$ for all $a, b \in G$.*

Example 2.7. Thus from example 2.6 above, (1) and (2) are abelian, while (3) and (4) are not (assuming that the set X in (3) has more than two elements). The set $\mathbb{Z}$ together with the binary operation $*$ defined by $a * b = a + b + 1$ from example 2.5(1) is an additional example of an abelian group.

Remark: If G is a finite group its **Cayley table** or **multiplication table** or **group table** can be formed. The rows and columns of the table are labeled by the elements, and the entry in row a and column b is the element $a * b$.

Example 2.8. The Cayley tables for $G = \{1, -1, i, -i\}$ under multiplication and $(Z_4, +)$ are as follows:

$\bullet$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	$-i$

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

Note that we may observe that each of these groups is abelian, because the table is symmetric about the main diagonal. We also notice that in the Cayley table of $(Z_4, +)$ each row is obtained from the one before by simply moving the first element to the end and sliding every other element along one place.

Remark: A Cayley table for a set G can be used to determine if $(G, *)$ is a group. Consider for example the set $G = \{\ a,\ b,\ c,\ d\ \}$ whose Cayley table is shown below:

*	a	b	c	d
a	b	c	b	a
b	a	c	b	d
c	c	b	a	d
d	d	a	c	b

Clearly, G is closed under $*$ since every entry in each row and column is an element of G. However, there is no identity element in G, since there is no row whose entries are exactly the same as the column headings, and no column whose entries are exactly the same as the row headings. Since there is no identity element, each element does not have an inverse either. Hence, G can not be a group and we need not check if the associative property holds.

Exercises.

1. Determine if the given set is a semigroup, a monoid, a group or none of these with respect to the operation *:
   (a) $G =$ set of all real numbers x such that $0 < x \leq 1$, $a * b = ab$
   (b) $G =$ set of all even integers, $a * b = a + b$
   (c) $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \text{ are even integers} \right\}, A * B = A + B$
   (d) $G =$ set of all quadratic polynomials in x with integer coefficients, $*$ is the usual multiplication of polynomials
   (e) $G = \{\ a + b\sqrt{2},\ a,\ b \in \mathbb{Z}^+\ \}$ where the binary operation is ordinary multiplication
   (f) $G = \mathbb{Z},\ a * b = a + ab$
   (g) $G = \mathbb{Z},\ a * b = a + ab + b$
2. Construct the multiplication table for $G_1 = \mathbb{Z}_7^*$ and $G_2 = \mathbb{Z}_9^*$. Use these tables to determine whether or not these sets are groups.

2.3 Elementary Properties of Groups

We begin with a comment on notation. If we are working in an arbitrary group, then we write e for the identity, and also we suppress the symbol for the binary operation and write simply ab for $a*b$. This "multiplicative notation" is used simply for convenience; it does not mean that the binary operation is necessarily multiplication. If however we are working in a particular group and there is an appropriate symbol for either the identity or the binary operation (such as "0" or "+", for instance), then we use it.

The following are consequences of our definition of a group.

Theorem 2.1. *(Uniqueness of the Identity Element): In a group G, the identity element is unique.*

Theorem 2.2. *(Uniqueness of the Inverse): If G is a group, then each element of G has a unique inverse.*

Recall that we write a^{-1} for the unique inverse of the element a; thus we have

$$aa^{-1} = e = a^{-1}a.$$

Note also that the inverse of a^{-1} is a. (In an additive group we write $-a$ instead of a^{-1}.)

Theorem 2.3. *(Uniqueness of Solutions): If G is a group and $a, b \in G$, then the equation $ax = b$ has the unique solution $x = a^{-1}b$; similarly the equation $xa = b$ has the unique solution $x = ba^{-1}$.*

Corollary 2.3.1. *(Cancelation Laws): If G is a group and $a, b, c \in G$ with $ab = ac$ or $ba = ca$, then $b = c$.*

We may express this result as saying that a group has left and right cancelation laws.

Corollary 2.3.2. *If G is a group with identity e, and $a, b \in G$ with $ab = e$, then $b = a^{-1}$ and $a = b^{-1}$.*

Thus if we are in a group and wish to check that b is the inverse of a, it suffices to check that $ab = e$; it must then also be true that $ba = e$.

Corollary 2.3.3. *Given an element a of a group G, as x runs through the elements of G, the elements ax are just the elements of G in some order, without repetitions; the same is true of the elements xa.*

This result implies that each row and column of the Cayley table of a finite group must contain each element exactly once. We have seen this in the two tables above in example 2.8; in fact it is sometimes possible to exploit this result if we are given an incomplete Cayley table. For example, consider the following:

$*$	v	w	x	y	z
v			w		
w	z				x
x		y			
y					
z					

Since $vx = w$ and $wz = x$, the identity cannot be v, x, w or z; so it must be y, and we may fill in the y row and column.

$*$	v	w	x	y	z
v			w	v	
w	z			w	x
x		y		x	
y	v	w	x	y	z
z				z	

Next vz cannot be w or v since they already occur in the v row, and it cannot be x or z either since they are in the z column ; so it must be y. Continuing thus eventually yields the full table:

$*$	v	w	x	y	z
v	x	z	w	v	y
w	z	v	y	w	x
x	w	y	z	x	v
y	v	w	x	y	z
z	y	x	v	z	w

To find the inverse of any element a of a finite group G in a Cayley table, all we have to do is find the row headed by a and move across this row until the identity element is found. The heading of the column containing this element is the inverse of a.

Theorem 2.4. *(Inverse of a Product): If a and b are elements of a group G, then*

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

Exercises. Answer the following exercises from Fraleigh:

1. *Exercise 22, p. 57:* Determine if the statement is true or false:
   (a) A group may have more than one identity element.
   (b) In a group, every linear equation has a solution.
   (c) Every finite group with at most three elements has a commutative operation.
   (d) If $a,\ b,\ c$ are fixed elements of a group G, then the equation
   $$a\ *x\ *\ b = c$$
   has a unique solution in G.
   (e) The empty set can be considered a group.
2. *Exercise 25, p. 58 :* If * is a binary operation on a set S, an element $x \in S$ is called an **idempotent** if $x\ *\ x = x$. Prove that a group G has exactly one idempotent.
3. *Exercise 31, p. 58:* Let G be a group and let $a,\ b \in G$. Show that $(a * b)^{-1} = a^{-1} * b^{-1}$ if and only if $a * b = b * a$.

2.4 Finite Groups

Definition 2.6. *If a group G has a finite number of elements, G is called a **finite group**, or a **group of finite order.** The number of elements in G is called the **order** of G, and is denoted by $|G|$ or by $o(G)$. If G does not have a finite number of elements, G is called an **infinite order** or a **group of infinite order**.*

Example 2.9.

1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are groups of infinite order.
2. $G = \{1, -1, i, -i\}$ under multiplication is a group of order 4.
3. $G = (Z_6, +)$ is a finite group of order 6.
4. The Klein 4-group with the group table below is of order 4.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

We may extend the associative law as follows. Since $(ab)c = a(bc)$ holds, we may write abc without ambiguity. If we consider expressions of length 4 rather than 3, there are five ways of inserting brackets:

$$((ab)c)d, (a(bc))d, (ab)(cd), a((bc)d), a(b(cd))$$

Of these the first and second are equal, as are the fourth and fifth; if we write $ab = f$, the first and third are $(fc)d$ and $f(cd)$, while setting $cd = g$ makes the third and fifth $(ab)g$ and $a(bg)$. Thus all five give the same element, so we may omit brackets here as well. In fact an easy induction argument shows that brackets may be omitted without ambiguity from an expression of any length; we shall tend to do this from now on.

One immediate consequence of this is the following definition.

Definition 2.7. *Let G be a group, $a \in G$ and $n \in \mathbb{Z}^+$. Then we write*

$$\begin{aligned} a^n &= a \cdot a \cdots a \ (n \text{ terms}) \\ a^0 &= e \\ a^{-n} &= (a^{-1})^n = (a^{-1}) \cdot (a^{-1}) \cdots (a^{-1}) \ (n \text{ terms}) \end{aligned}$$

*Then clearly $a^m \cdot a^n = a^{m+n}$ and $a^m \cdot a^{-n} = a^{m-n}$ and $(a^n)^{-1} = a^{-n}$. The elements a^n for $n \in \mathbb{Z}^+$ are called **powers** of a. In an additive group we write na instead of a^n, and call such elements **multiples** of a.*

Example 2.10. Let $G = (Z_4, +)$ and let $a = 3$. Then

$$\begin{aligned} 3^0 &= e = 0 \\ 3^1 &= 3 \\ 3^2 &= 3 + 3 = 2 \\ 3^3 &= 3 + 3 + 3 = 1 \\ 3^4 &= 3 + 3 + 3 + 3 = 0 \\ 3^{-3} &= (3^{-1})^3 = 1^3 = 1 + 1 + 1 = 3 \\ 3^2 + 3^2 &= 2 + 2 = 0 = 3^4 \\ 3^2 + 3^{-3} &= 2 + 3 = 1 = 3^{-1} \end{aligned}$$

Since G is an additive group, then $3^1 = (1)(3), 3^2 = (2)(3), 3^3 = (3)(3), 3^4 = (4)(3)$ which are multiples of 3.

Definition 2.8. *Let G be a group and let $a \in G$. The smallest positive integer n such that*

$$a^n = e$$

is called the **order** *of a. This is denoted by $|a|$ or by $o(a)$. If no such integer exists, then a is said to be of* **infinite order**.

Example 2.11.

1. Let $G = (Z_4, +)$. Then $e = 0$ and we have
   (a) $0^1 = 0$, so $o(0) = 1$
   (b) $1^1 = 1, 1^2 = 2, 1^3 = 3, 1^4 = 0$, so $o(1) = 4$
   (c) $2^1 = 2, 2^2 = 0$, and $o(2) = 2$
   (d) $3^1 = 3, 3^2 = 2, 3^3 = 1, 3^4 = 0$, and $o(3) = 4$
2. Given the Cayley table below, we have $e = y$.

$*$	v	w	x	y	z
v	x	z	w	v	y
w	z	v	y	w	x
x	w	y	z	x	v
y	v	w	x	y	z
z	y	x	v	z	w

   (a) $v^1 = v, v^2 = x, v^3 = w, v^4 = z, v^5 = y$, and $o(v) = 5$
   (b) $w^1 = w, w^2 = v, w^3 = z, w^4 = x, w^5 = y$, and $o(w) = 5$
   (c) $x^1 = x, x^2 = z, x^3 = v, x^4 = w, x^5 = y$, and $o(x) = 5$
   (d) $y^1 = y$, and $o(y) = 1$
   (e) $z^1 = z, z^2 = w, z^3 = x, z^4 = v, z^5 = y$, and $o(z) = 5$
3. Let $G = (\mathbb{R}^*, \bullet)$, so that $e = 1$. Then $o(1) = 1$. If $a \in \mathbb{R}^*$ and $a \neq 1$, then $a^n = aa \cdots a \neq 1$ for any positive integer n, so that $o(a) = +\infty$. This shows that in G, there is one element of order 1 and all the other elements are of infinite order.

We notice that the order of the element divides the order of the group if the group is finite. We will learn later why.

Exercises.

1. In each of the following, determine the order of the given element in the given group:
   (a) $G = Z_8, +, a = 2$
   (b) $G = (\mathbb{Q}^+, \bullet), a = -1$
   (c) $G = (\mathbb{Z}_7^*, \bullet), a = 5$

2.5 Subgroups

Among the nonempty subsets of a group G, there are some that form a group with respect to the binary operation $*$ that is defined in G. That is, a subset $H \subseteq G$ may be such that H is also a group with respect to $*$. Such a subset H is called a *subgroup* of G and we write $H \leq G$.

Definition 2.9. *Let G be a group with respect to the binary operation *. A nonempty subset H of G is called a* ***subgroup*** *of G if H forms a group with respect to the binary operation * that is defined in G.*

Example 2.12.

1. From example 2.6(1), $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are groups under addition. Hence, $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$ and both are subgroups of $(\mathbb{R}, +)$.

2. From example 2.6(2), $\mathbb{C}^*$ is a group under multplication, and $G = \{1, -1, i, -i\}$ is a subgroup of this group as shown in example 2.8.

3. Let $G = (Z_4, +)$ and let $H = \{0, 2\}$. Given the group table for $(H, +)$ as shown below, it is clear that H is a subgroup of G.

$+$	0	2
0	0	2
2	2	0

   Clearly, addition modulo 4 is a binary operation in H . Associativity is passed on from G to H, the identity element 0 is in H and the inverses of the elements of H are likewise in H, namely: $0^{-1} = 0,\ 2^{-1} = 2$.

   However, H under this binary operation is not a subgroup of $(\mathbb{Z}, +)$ since the binary operations are different.

4. Let $G = (Z_4, +)$ and let $H = \{1, 3\}$. Since $1 + 3 = 4 \notin H$, addition modulo 4 is **not** a binary operation in H. Thus, H is not a subgroup of G. Note that it is not necessary to check the other group properties once a property of groups is not satisfied by the subset.

Definition 2.10. *The subsets $H = \{e\}$ and $H = G$ are always subgroups of the group G. They are referred to as* ***trivial*** *subgroups and other subgroups of G are called* ***nontrivial****. If $H \neq G$, then H is a* ***proper subgroup*** *of G and we write $H < G$*

Example 2.13.

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$.

2. $G = (\{1, -1, i, -i\}, \bullet)$ is a nontrivial subgroup of $(\mathbb{C}^*, \bullet)$.

3. $H = (\{0, 2\}, +) < G = (Z_4, +)$.

Exercises. Determine if $H \leq G$.

1. $G = (\mathbb{Z}_6, +)$, $H = \{0, 2, 4\}$.
2. $G = (\mathbb{Z}_6, +)$, $H = \{1, 3, 5\}$.
3. $G = (\mathbb{Q}^+, \bullet)$, $H = \mathbb{Z}^+$.
4. $G = (\mathbb{C} = \{\ z = x+yi :\ x,\ y \in \mathbb{R},\ \ i^2 = -1\ \}, +), (a+bi)+(c+di) = (a+c)+(b+d)i$
   (a) $H = i\mathbb{R} = \{\ iy : y \in \mathbb{R}\ \}$
   (b) $H = \{\ z = x + yi :\ x,\ y \in \mathbb{Z}\ \}$

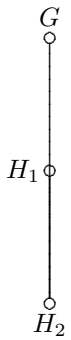
2.6 Subgroup Lattice

The relationship between the various subgroups of a group can be illustrated with a *subgroup lattice* of the group. This is a diagram that includes all the subgroups of the group and connects a subgroups H_i at one level to a subgroup H_k at a higher level with a sequence of line segments if and only if H_i is a proper subgroup of H_j.

Example 2.14.

1. Let $G = (\{1, -1, i, -i\}, \bullet)$. Then the subgroups of G are:
   (a) G
   (b) $H_1 = \{1, -1\}$
   (c) $H_2 = \{1\}$

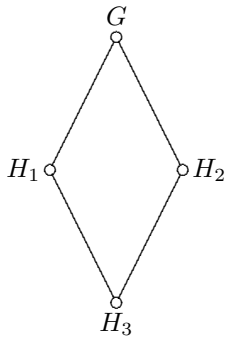
   Hence, $H_2 < H_1 < G$ and the subgroup lattice is



2. Let $G = (Z_6, +)$. Then the subgroups of G are:
   (a) G
   (b) $H_1 = \{0, 2, 4\}$
   (c) $H_2 = \{0, 3\}$

(d) $H_3 = \{0\}$

Hence, $H_3 < H_1 < G$ and $H_3 < H_2 < G$. The subgroup lattice is



Exercises. Construct the lattice diagram for each of the following graphs:

1. $G = (\mathbb{Z}_{15}, +)$
2. $G = (\mathbb{Z}_7^*, \bullet)$
3. $G =$ Klein-4 group

2.7 Tests for Subgroups

The following theorems will show if a subset of a group is a subgroup without verifying if all the properties of a group hold.

Theorem 2.5. *(Two-Step Test): A nonempty subset H of a group G is a subgroup of G if and only if*

1. *$a, b \in H$ implies that $ab \in H$.*
2. *$a \in H$ implies that $a^{-1} \in H$.*

Theorem 2.6. *(One-Step Test): A nonempty subset H of a group G is a subgroup of G if and only if for all $a, b \in H$, $ab^{-1} \in H$.*

Example 2.15.

1. Let G be an abelian group and $H = \{x \in G | x^2 = e\}$. Then $H \leq G$ as verified below.

   (a) *Two-Step Test.*

i. Let $x, y \in H$. Then $x^2 = e, y^2 = e$.

$$\begin{aligned} (xy)^2 &= (xy)(xy) \\ &= x(yx)y && \text{by associativity} \\ &= x(xy)y && \text{since } G \text{ is abelian} \\ &= x^2y^2 \\ &= e \end{aligned}$$

Hence, $xy \in H$.

ii. Let $x \in H$.

$$\begin{aligned} (x^{-1})^2 &= (x^2)^{-1} \\ &= e \end{aligned}$$

Then, $x^{-1} \in H$.

(b) *One-Step Test.* Let $x, y \in H$.

$$\begin{aligned} (xy^{-1})^2 &= (xy^{-1})(xy^{-1}) \\ &= x(y^{-1}x)y^{-1} && \text{by associativity} \\ &= x(xy^{-1})y^{-1} && \text{since } G \text{ is abelian} \\ &= x^2(y^{-1})^2 \\ &= e \end{aligned}$$

Therefore, $xy^{-1} \in H$.

However, only one test is needed to verify if H is a subgroup of G. The verification using the two tests are for illustration purposes only. The next example will use only one test.

2. We show that $4\mathbb{Z}$ is a subgroup of the additive group $\mathbb{Z}$ by the one-step test. Let $x, y \in 4\mathbb{Z}$, then $x = 4m, y = 4n$ where $m, n \in \mathbb{Z}$. Given $4n \in \mathbb{Z}$, then its inverse is $-4n = 4(-n)$. Hence, $4m + (-4n) = 4m + 4(-n) = 4(m - n) \in 4\mathbb{Z}$.

Our next result concerns the intersection of groups.

Theorem 2.7. *The intersection of any family of subgroups of G is itself a subgroup of G.*

Example 2.16. If $G = \mathbb{Z}$, the intersection of the subgroups $3\mathbb{Z}$ and $4\mathbb{Z}$ is the subgroup $12\mathbb{Z}$, since the numbers which are multiples of both 3 and 4 are the multiples of 12; the intersection of all subgroups $m\mathbb{Z}$ for $m \in \mathbb{Z}^+$ is the identity subgroup $\{0\}$, as no non-zero number is a multiple of all positive integers.

Exercises.

1. Use the one-step to determine if the following subsets H are subgroups of the given groups G:

(a) Let $G = (\{2^k : k \in \mathbb{Z})\}, \bullet$, $H = \{2^r : r \text{ is an even integer}\}$

(b) Let $G = (\mathbb{R}, +),\ H = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$

2. Use the two-step test to determine if the subsets H is a subgroup of the given group G:

(a) Let $G = (\mathbb{Z}, +)$, $H = 3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$

(b) Let H be a nonempty subset of a finite group G be closed under the binary operation Of G.

2.8 Centers and Centralizers

We begin with a definition concerning a pair of elements of G.

Definition 2.11. *If $g, h \in G$ and $gh = hg$, we say that g and h **commute** or **centralize** each other.*

Example 2.17.

1. In an abelian group any two elements commute.
2. In any group G, e commutes with every element of G.

Our first result in this section concerns powers of commuting elements.

Theorem 2.8. *If $g, h \in G$ commute then $gh^n = h^n g$ and $(gh)^n = g^n h^n$ for all $n \in \mathbb{Z}^+$.*

We now consider the set of all elements which commute with a given element of G.

Definition 2.12. *Given $g \in G$, the centralizer of g in G is the set $C(a) = \{x \in G | xg = gx\}$ of all elements of G which commute with g.*

If G is finite it is simple to read off $C(g)$ from the Cayley table; we simply compare entries in the g row and column, looking for ones which agree.

Example 2.18.

1. In any abelian group $G, C(a) = G$ for all $a \in G$.
2. Given the group table for $(G, *)$,

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	f	e	d	c
c	c	d	a	b	f	e
d	d	c	e	f	b	a
e	e	f	d	c	a	b
f	f	e	b	a	c	d

Then

(a) $C(a) = G$
(b) $C(b) = \{a, b\}$
(c) $C(c) = \{a, c\}$
(d) $C(d) = \{a, d, f\}$
(e) $C(e) = \{a, e\}$
(f) $C(f) = \{a, d, f\}$

We notice that all centralizers in these examples are subgroups of G; this is no accident, as our next result shows.

Theorem 2.9. *If $g \in G$ then $C(g)$ is a subgroup of G.*

Definition 2.13. *The centre $Z(G)$ of G is the intersection of all subgroups $C(g)$ as g runs through G.*

Example 2.19.

1. $Z(G) = G$ for any abelian group G since $C(a) = G$ for all $a \in G$.
2. From example 2.18, $Z(G) = \{a\}$

Remark: By theorem 6.3, we see that $Z(G)$ is also a subgroup of G; it consists of those elements which commute with every element of G. It is clear that G is abelian if and only if $Z(G) = G$.

Exercises. Determine $C(g)$ for all $g \in G$ and $Z(G)$ for each of the following groups:

1. $G = (\{1, -1, i, -i\}, \bullet)$
2. $G = (\mathbb{Z}_7^*, \bullet)$
3. Given the group table:

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	ab^2
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Chapter 3

Some Special Classes of Groups

3.1 Cyclic Groups

In this section we concentrate on the subgroup of G generated by a single element.

Definition 3.1. *Let $g \in G$, the elements of $< g >$ are the powers g^n of g for $n \in \mathbb{Z}$. Hence, the elements of $< g >$ are*

$$\ldots g^{-5}, g^{-4}, g^{-3}, g^{-2}, g^{-1}, g^0, g^1, g^2, g^3, g^4, g^5, \ldots$$

However, not all of these need be distinct.

Example 3.1. Let $G = (\mathbb{Z}_6, +)$. Then $< 2 >= \{2^0, 2^1, 2^2\} = \{0, 2, 4\}$, the power 2^3 is equal to 0, while $2^{-1} = 4$. Also, $< 4 >= \{4^0, 4^1, 4^2\} = \{0, 4, 2\}$. Hence, $< 2 >=< 4 >$.

We shall need to consider carefully the question of when two powers will be equal. We begin with a partial result.

Lemma 3.1. *Suppose $n \in \mathbb{Z}^+$ with $g^n = e$. If $s, t \in \mathbb{Z}$ with $s \equiv t (mod\ n)$, then $g^s = g^t$.*

We may now determine the distinct elements of $< g >$; we split into two cases according to whether this subgroup is finite or infinite.

Theorem 3.1. *Let $g \in G$*

1. *If $|g| = n < \infty$, then $< g >= \{e, g, g^2 \ldots, g^{n-1}\}$, and these elements are all distinct.*

2. *If $|g|$ is infinite, then all elements g^r for $r \in \mathbb{Z}$ are distinct.*

Definition 3.2. *A subgroup of G of the form $< g >$ for some $g \in G$ is called a **cyclic subgroup** of G. If there is an element $g \in G$ such that $G =< g >$, we say that G is a **cyclic group**; any element g with $< g >= G$ is called a **generator** of G.*

Thus G is cyclic if it is generated by a single element.

Example 3.2.

1. $(\mathbb{Z}_n, +)$ is cyclic, as it is generated by [1].
2. $(\mathbb{Z}, +)$ is cyclic, as it is generated by 1.
3. $(\mathbb{Q}, +)$ is not cyclic, as there is no $g \in \mathbb{Q}$ such that $\mathbb{Q}$ consists of the elements ng for $n \in \mathbb{Z}$.

Remark: A cyclic group is clearly abelian, because for all $r, s \in \mathbb{Z}$ we have

$$g^r \cdot g^s = g^{r+s} = g^{s+r} = g^s \cdot g^r.$$

Any group G has cyclic subgroups, since for each $g \in G$ we may take the cyclic subgroup $< g >$ of G. If in fact G itself is cyclic, we can say more.

Theorem 3.2. *Any subgroup of a cyclic group is cyclic.*

Example 3.3.

1. The subgroup $(4\mathbb{Z}, +)$ of the cyclic group $(\mathbb{Z}, +)$ is cyclic, since it is generated by 4.
2. The subgroup $(\{0, 2, 4\}, +)$, of the cyclic group $(\mathbb{Z}_6, +)$ is cyclic, since it is generated by 2. It is also generated by 4 as shown in example 3.1.

We now give a definition concerning the order of a cyclic subgroup.

Definition 3.3. *If $g \in G$, the* ***order*** *$o(g)$ of g is the order of the subgroup $< g >$ generated by g; if $< g >$ is infinite, we say that g has* ***infinite order****.*

Example 3.4.

1. If $G = (\mathbb{Z}_n, +)$ then $o(1) = n$, because $< 1 >= \{0, 1, 2, \ldots, n-1\} = G$.
2. If $G = (\mathbb{Z}, +)$ then any non-identity element has infinite order.
3. From example 2.11(2), since $< z >= \{y, z, w, x, v\} = G$ then $o(z) = 5 = o(G)$. Likewise, $o(v) = o(w) = o(x) = o(z) = 5$. Hence, G has 4 generators, v, w, x and z.
4. Given the group table below,

$*$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	f	e	d	c
c	c	d	a	b	f	e
d	d	c	e	f	b	a
e	e	f	d	c	a	b
f	f	e	b	a	c	d

the order of the elements are as follows:

g	a	b	c	d	e	f
$o(g)$	1	2	2	3	2	3

Remark: There are various things we may observe about element orders. First, as defined earlier, $o(g)$ is the least natural number n such that $g^n = e$ or is ∞ if there is no such n. Clearly $o(g) = 1$ if and only if $g = e$, while if $e \neq e$ then $o(g) = 2$ if and only if $g^2 = e$ which implies that $g^{-1} = g$. Also, $o(g^{-1}) = o(g)$, because any power of g^{-1} is a power of g and vice versa, so that $< g^{-1} >=< g >$. Finally, a finite group of order n is cyclic if and only if it has an element g with $o(g) = n$.

Example 3.5.

1. In $(\mathbb{Z}_6, +)$, 3 is its own inverse, and has order 2.
2. In $(\mathbb{Z}_5, +)$ the inverse of 1 is 4, with successive powers $4, 3, 2, 1, 0$, so $o(4) = 5 = 0(1)$
3. The group in example 3.4(4) is not cyclic, since it has no element of order 6.

In addition, we may now decide precisely when two powers of an element are equal.

Theorem 3.3. *Take $g \in G$ with $o(g) = n$; then $g^s = g^t$ if and only if $s \equiv t(mod\ n)$.*

In particular, we may see exactly which powers of an element are equal to the identity.

Corollary 3.3.1. *If $g \in G$, then $g^s = e$ if and only if $o(g)|s$.*

Exercises.

1. In each of the following, determine if the given group is cyclic or not. If it is cyclic, find at least one generator for G.
   (a) $G = (\{3^k : k \in \mathbb{Z}\}, \bullet)$
   (b) $G = (\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}, +)$
   (c) G is the group of exercise 3 of section 2.8
2. Determine the order of the given elements of the given groups:
   (a) $G = (\mathbb{Z}_1^* 1, \bullet),\ a = 2$
   (b) $G = (Z_{12}, +),\ a = 3, 6, 4, 7$
   (c) G G is the group of exercise 3 of section 2.8, a^2, ab
3. *Prove:* Let $G =< a >$ a finite cyclic group of order n. For any integer m, the subgroup generated by a^m is the same as the subgroup generated by a^d shere $d = (m, n)$.

3.2 Groups of Permutations

Let X be a finite set. Recall that a *permutation* of X is a bijective map from X to itself. Because the nature of the permutations of X depends only on the number of elements of X, rather than the particular elements themselves, we may as well assume that $X = \{1, 2, \ldots n\}$.

Definition 3.4. *The group of permutations of the set $\{1, 2, \ldots n\}$ is called the* ***symmetric group of degree n****, and is written S_n.*

An element $\sigma \in S_n$ may be written as $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$, where $a_i = \sigma(i)$ for $0 \leq i \leq n$. Since there are n choices for a_1, then $n-1$ choices for a_2 (as it must be different from a_1), then $n-2$ choices for a_3 and so on, we see that there are $n!$ different permutations of $\{1, 2, \ldots n\}$; thus S_n has $n!$ elements. There are also $n!$ different ways of writing a given permutation, since we may rearrange the columns in any order; for example, in S_3 we have

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \ldots$$

The composite of two permutations is defined by

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$$

The identity permutation is $\begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$, and the inverse of $\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$ is $\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ 1 & 2 & \ldots & n \end{pmatrix}$.

It is clear that S_1, the trivial group and S_2 are abelian; however, if $n \geq 3$ then S_n is non-abelian. To see this, let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \ldots & n \\ 2 & 1 & 3 & 4 \ldots & n \end{pmatrix}, \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \ldots & n \\ 1 & 3 & 2 & 4 \ldots & n \end{pmatrix}$$

so that σ simply interchanges 1 and 2, and π interchanges 2 and 3); then

$$\sigma\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \ldots & n \\ 3 & 1 & 2 & 4 \ldots & n \end{pmatrix}, \pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \ldots & n \\ 2 & 3 & 1 & 4 \ldots & n \end{pmatrix}$$

so that $\sigma\pi \neq \pi\sigma$.

We now consider a particular type of permutation.

Definition 3.5. *For any positive integer $r \leq n$, let $a_1, a_2, \ldots, a_r$ be distinct elements of the set $\{1, 2, \ldots n\}$. We denote by $(a_1\ a_2\ \ldots\ a_r)$ the permutation given by*

$$\sigma(a_i) = a_{i+1} \text{ for } 1 \leq i \leq r-1, \qquad \sigma(a_r) = a_1, \qquad \sigma(a) = a \text{ for } a \notin \{a_1, a_2, \ldots, a_r\}$$

We call $(a_1\ a_2\ \ldots\ a_r)$ a ***cycle of length r****, or an* ***r-cycle****.*

Example 3.6. *In the permutations above we have* $\sigma = (1\ 2), \pi = (2\ 3), \sigma\pi = (1\ 3\ 2)$ *and* $\pi\sigma = (1\ 2\ 3)$*; σ and $= \pi$ are 2-cycles, and $\sigma\pi$ and $\pi\sigma$ are 3-cycles.*

Remarks: There are several things to note about cycles.

1. An r-cycle can be written in r different ways, since
$$(a_1\ a_2\ \ldots\ a_r) = (a_2\ \ldots a_r\ a_1) = \ldots = (a_r\ a_1\ \ldots\ a_{r-1})$$
2. Any 1-cycle is simply the identity permutation.
3. We can multiply two cycles by 'feeding in' elements from the left in turn; for example, if $\sigma = (1\ 2\ 5)$ and $\pi = (2\ 3\ 4)$ then $\sigma\pi = (1\ 2\ 5)(2\ 3\ 1)$ maps
$$1 \to 2 \to 3, 3 \to 3 \to 4, 4 \to 4 \to 2, 2 \to 5 \to 5, 5 \to 1 \to 1$$
and so $\sigma\pi = (1\ 3\ 4\ 2\ 5)$.
4. The inverse of a cycle is obtained by simply writing its elements in reverse order; for example if π is as above then $\pi^{-1} = (4\ 3\ 2)$. We can check this by computing $(2\ 3\ 4)(4\ 3\ 2) = 1$.
5. The order of a cycle is simply given by its length, because applying $(a_1\ a_2\ \ldots\ a_r)$ successively maps
$$a_1 \to a_2 \to \ldots \to a_r \to a_1$$
for example,$(2\ 3\ 4)$ has order 3.
6. If $\sigma = (a_1\ a_2\ \ldots\ a_r)$ and $\pi = (b_1\ b_2\ \ldots\ b_r)$, where the sets $\{a_1, a_2, \ldots, a_r\}$ and $\{b_1, b_2, \ldots, b_r\}$ are disjoint, i.e., have empty intersection, then $\sigma\pi = \pi\sigma$; for example, if $\sigma = (4\ 5\ 6\ 7)$ and $\pi = (1\ 2\ 3)$ in S_8, then
$$\sigma\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 8 \end{pmatrix}$$
We can see this because the elements moved by σ and π are different, so it does not matter whether σ or π is performed first.

Now not all permutations are cycles; for example, the permutation
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 8 \end{pmatrix}$$
just obtained is not a cycle. However, we obtained this permutation as a product of two cycles which moved disjoint sets of points; this suggests how we may extend the idea of cycles to cover all permutations.

Definition 3.6. *Let $\sigma = (a_1\ a_2\ \ldots\ a_r)$ and $\pi = (b_1\ b_2\ \ldots\ b_r)$ be cycles of S_n. If the sets $\{a_1, a_2, \ldots, a_r\}$ and $\{b_1, b_2, \ldots, b_r\}$ are disjoint, we say that σ and π are* ***disjoint cycles****. This terminology is extended in the obvious way to sets of more than two cycles.*

For the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 8 \end{pmatrix}$ above, it is easy to recover the cycles (4 5 6 7) and (1 2 3) of which it is a product; in fact using (6), (1) and (2) above we may write

$$\alpha = (4\ 5\ 6\ 7)(1\ 2\ 3) = (1\ 2\ 3)(4\ 5\ 6\ 7) = (5\ 6\ 7\ 4)(1\ 2\ 3) = (4\ 5\ 6\ 7)(1\ 2\ 3)(8) = \ldots$$

The following theorem shows that the behavior observed in this example is typical.

Theorem 3.4. *Every permutation in S_n can be written as a product of disjoint cycles; moreover this expression is unique up to*

1. *the order in which the cycles occur,*
2. *the different ways of writing each cycle, and*
3. *the presence or absence of 1-cycles.*

Definition 3.7. *A permutation which is written as a product of disjoint cycles is said to be in **cycle notation**; if all 1-cycles are included, it is said to be in **full cycle notation**.*

Example 3.7. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 6 & 9 & 7 & 2 & 3 & 8 & 4 \end{pmatrix}$ and $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 6 & 1 & 7 & 4 & 9 & 2 & 5 \end{pmatrix}$; then the expressions for $\sigma, \pi, \sigma\pi$ and σ^{-1} in (full) cycle notation are as follows:

$$\begin{aligned} \sigma &= (2\ 5\ 7\ 3\ 6)(4\ 9)(= (2\ 5\ 7\ 3\ 6)(4\ 9)(1)(8) \text{ in full cycle notation}) \\ \pi &= (1\ 3\ 6\ 4)(2\ 8)(5\ 7\ 9) \\ \sigma\pi &= (2\ 5\ 7\ 3\ 6)(4\ 9)(1\ 3\ 6\ 4)(2\ 8)(5\ 7\ 9) = (1\ 3\ 4\ 5\ 9)(2\ 7\ 6\ 8) \\ \sigma^{-1} &= (6\ 3\ 7\ 5\ 2)(9\ 4) = (3\ 7\ 5\ 2\ 6)(4\ 9) \end{aligned}$$

It is easy to calculate the order of a permutation written in cycle notation.

Theorem 3.5. *If $\sigma = \alpha_1\alpha_2 \ldots \alpha_k$, where the α_i are disjoint cycles, then the order of σ is the least common multiple of the lengths of the cycles α_i.*

Example 3.8. If $\pi = (1\ 3\ 6\ 4)(2\ 8)(5\ 7\ 9)$ as above, then the order of π is the least common multiple of 4,3 and 2 which is 12.

To conclude this section we focus on the smallest non-trivial cycles.

Definition 3.8. *A 2-cycle is called a **transposition**.*

The following result gives some indication of the importance of transpositions.

Theorem 3.6. *If $n > 1$, every permutation in S_n can be written as a product of transpositions.*

Example 3.9. In S_8 we have $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix} = (1\ 4)(1\ 8)(1\ 7)(2\ 5)(2\ 3)$.

Notice that in this example the expression (1 4)(1 8)(1 7)(1 2)(1 2)(2 5)(2 3) gives the same permutation. In general there will be many ways of expressing a given permutation as a product of transpositions; the essential uniqueness of theorem 3.4 occurs because the cycles there are required to be disjoint. In the next section we will see what can be said about uniqueness of expression in terms of transpositions.

Exercises.

1. Determine the order of each of the following permutations:
   (a) $\sigma = (1\ 2\ 5)(6\ 8\ 3\ 4)$
   (b) $\sigma = (5\ 7\ 3)(8\ 1\ 2)(6\ 9)$
   (c) $\sigma = (3\ 1\ 4\ 2)(2\ 1\ 7)(5\ 7\ 3)$
2. Express each of the permutations below as a product of transpositions:
   (a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 8 & 4 & 2 & 1 & 6 & 3 \end{pmatrix}$
   (b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 7 & 1 & 5 & 3 & 4 \end{pmatrix}$

3.3 The Sign of a Permutation

Let $\sigma \in S_n$, and suppose that $\sigma = \alpha_1\alpha_2 \dots \alpha_k$ with the α_i disjoint cycles. Set

$$v(\sigma) = \sum_1^k (|\alpha_i| - 1)$$

where $|\alpha_i|$ denotes the length of the cycle α_i . Note that $v(\sigma)$ is well-defined because of the uniqueness in theorem 3.4, in particular, cycles of length 1 contribute 0 to the sum, and so may be ignored.

Example 3.10. If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 2 & 8 & 3 & 6 & 1 & 7 \end{pmatrix} = (1\ 4)(1\ 8)(1\ 7)(2\ 5)(2\ 3) = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$, then $v(\sigma) = 3 + 2 + 0 = 5$.

Note that because σ^{-1} has the same cycle lengths as σ , we have $v(\sigma^{-1}) = v(\sigma)$.

Example 3.11. If σ is as above, $\sigma^{-1} = (7\ 8\ 4\ 1)(3\ 5\ 2)(6)$, so $v(\sigma^{-1}) = 3 + 2 + 0 = 5$.

Clearly $v(\sigma) = 1$ if and only if σ is a transposition. In fact we may interpret $v(\sigma)$ as follows: if all possible 1-cycles are included in the expression $\sigma = \alpha_1\alpha_2 \dots \alpha_k$, then $\sum_1^k (|\alpha_i| - 1)$ is the number of entries in the domain minus the number of cycles ; thus $v(\sigma) = n - k$, i.e., $v(\sigma)$ is the difference between n and the number of cycles in the full cycle notation.

Example 3.12. If σ is as above, then $n = 8$ and $k = 3$, so $v(\sigma^{-1}) = 8 - 3 = 5$.

Now $v(\sigma)$ on its own is not particularly important, but it enables us to make the following definition.

Definition 3.9. *Given $\sigma \in S_n$, the **sign** of σ is defined by*

$$sign(\sigma) = (-1)^{v(\sigma)}$$

*Thus $sign(\sigma) = \pm 1$; if $sign(\sigma) = 1$ we call σ an **even permutation**, while if $sign(\sigma) = -1$ we call σ) an **odd permutation**.*

Example 3.13. Example. If $\sigma = (1\ 4\ 8\ 7)(2\ 5\ 3)(6)$ as above, we have $sign(\sigma) = (-1)^5 = -1$, and so σ is odd. Note that because $v(\sigma^{-1}) = v(\sigma)$, we have $sign(\sigma^{-1}) = sign(\sigma)$.

We now consider how the sign of a permutation is affected by multiplication by a transposition.

Lemma 3.2. *Let $\sigma \in S_n$, and take τ a transposition; then $sign(\tau\sigma) = -sign(\sigma)$.*

Example 3.14. Let $\sigma = (1\ 4\ 7\ 8)(2\ 5\ 3)$ as above, so that $sign(\sigma) = -1$. If $\tau = (4\ 5)$ then

$$\tau\sigma = (4\ 5)(1\ 4\ 7\ 8)(2\ 5\ 3) = (1\ 4\ 3\ 2\ 5\ 7\ 8); v(\tau\sigma) = 6; sign(\tau\sigma) = (-1)^6 = 1 = -sign(\sigma)$$

On the other hand, if $\tau = (4\ 8)$ then

$$\tau\sigma = (4\ 8)(1\ 4\ 7\ 8)(2\ 5\ 3) = (1\ 4\ 7)(2\ 5\ 3); v(\tau\sigma) = 4; sign(\tau\sigma) = (-1)^4 = 1 = -sign(\sigma)$$

Corollary 3.6.1. *If $\tau_1, \ldots \tau_r \in S_n$ are transpositions, then $sign(\tau_1\ \ldots\ \tau_r) = (-1)^r$.*

This shows what can be said about an expression for a given permutation as a product of transpositions: an even (respectively odd) permutation can only be written as a product of an even (respectively odd) number of transpositions.

Theorem 3.7. *Let $\sigma, \pi \in S_n$, then $sign(\sigma)sign(\pi) = sign(\sigma\pi)$.*

Example 3.15. *In S_8, let $\sigma = (1\ 4\ 8)(2\ 3\ 7)(5\ 6)$ and $\pi = (1\ 6)(3\ 7\ 8)(4\ 5)$; then*

$$\sigma\pi = (1\ 4\ 8)(2\ 3\ 7)(5\ 6)(1\ 6)(3\ 7\ 8)(4\ 5) = (1\ 5)(2\ 7)(3\ 8\ 6\ 4)$$

Here

$$\begin{aligned} v(\sigma) &= 2+2+1=5 \text{ so } sign(\sigma) = -1 \\ v(\pi) &= 1+2+1=4 \text{ so } sign(\pi) = 1 \\ v(\sigma\pi) &= 1+1+3=5 \text{ so } sign(\sigma\pi) = -1 \end{aligned}$$

Theorem 3.8. *The subgroup of S_n consisting of all the even permutations is called the **alternating group of degree** n, and is written A_n. The order of A_n is $\dfrac{n!}{2}$*

Exercises:

1. In each of the following, determine if each of the following permutations is odd or even.

   (a) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 7 & 2 & 4 & 6 \end{pmatrix}$

   (b) $\beta = (5\ 9\ 8\ 6\ 4\ 2)(1\ 8\ 7\ 6\ 5)$

   (c) $\gamma = (8\ 7\ 1\ 6)(4\ 5\ 2\ 9)$

   (d) $\delta = \sigma^2, \quad \sigma = (1\ 5\ 7\ 6)(3\ 4\ 2)$

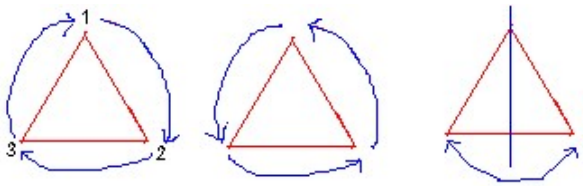
2. Explain why there is no permutation σ such that $\sigma^{-1}(3\ 1\ 5\ 8)\sigma = (2\ 5\ 7)$

3. Find all the elements of A_4.

3.4 Dihedral Groups

The **Dihedral groups** are the groups, D_n, of the possible symmetry operations on n-sided Regular Polygons.

The smallest n-sided regular polygon is the triangle, so we will start with D_3. A symmetry operation on a geometrical object is rotations and reflection that leaves the object in the same shape. This will, for a triangle, mean a rotation to the left or right by a third of a turn, or no rotation at all, or a reflection through any of its 'heights'. If we name the corners 1,2 and 3 we can see that this is the same as permutations of these corners.



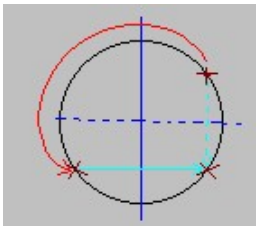
The first of the two rotations will move 1 to 2, 2 to 3 and 3 to 1, which is the cyclic permutation (1 2 3), the other rotation will be the cyclic rotation (1 3 2). The three reflections will exchange two corners and will be the same as the three possible cyclic permutation of three objects that exchange two objects, (1 2),(2 3) , and (1 3). Then we have left the 'do nothing' operation (1).

The symmetry group n-sided regular polygon will have one identity element, 'do nothing', $n-1$ rotational elements with rotations of 1 to $n-1$ of a $\frac{1}{n}$-turn. For polygons with an odd number of corners, there will be n reflectionss, one through each corner to the midpoint of the opposite edge. For polygons with an even number of sides, there will be $\frac{n}{2}$ reflections, with the axis through each opposite pair of corners, and $\frac{n}{2}$ through the midpoints of opposite edges, n in total. This means that the number of elements in

the symmetry group for a n-sided regular polygon will be $1 + n - 1 + n = 2n$, and this will be the order of this group. Hence, the order of the Dihedral group Dn is $2n$.

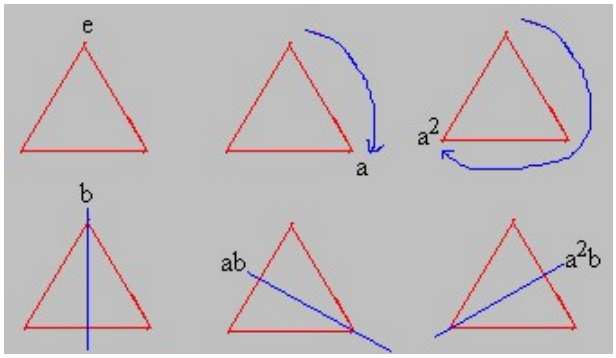
Is D_n really a group? By theorem 1.1, the composition of functions is associative. The inverse of a rotation will simply be a new rotation that together with the first one make a full turn. If the first one was by $\frac{p}{n}$ turn, then the new one need to be $\frac{n-p}{n}$ turn, together making $\frac{p}{n} + \frac{n-p}{n} = 1$ turn. The inverse of a reflection will simply be the reflection itself. The identity element will be the 'do nothing' operator.

Any reflection can be described using rotations and one reflection. We first rotate the point to a point opposite to the position where it should go, then we do the reflection.



All elements of a dihedral group can be described as $a^p b^r$, where p describes the angle, 0 to $n-1$, and r is a binary value, 0 or 1 (for no reflection or a reflection).

The elements of D3 would now be,



We can now write the group D_3 as,

$*$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

where

e = rotation through 0° about the centroid $= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)$

a = rotation through 120° about the centroid $= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$

a^2 = rotation through 240° about the centroid $= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$

b = reflection about the altitude through vertex 1 $= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$

ab = reflection about the altitude through vertex 2 $= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$

a^b = reflection about the altitude through vertex 3 $= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$

The order of a is n and the order of b is 2.

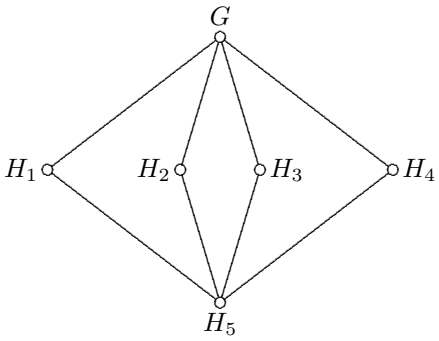
The subgroups of D_3 are as follows:

1. $G = \{e, a, a^2, b, ab, a^2b\}$
2. $H_1 = \{e, a, a^2\}$
3. $H_2 = \{e, a^2b\}$
4. $H_3 = \{e, ab\}$
5. $H_4 = \{e, b\}$
6. $H_5 = \{e\}$

Hence, we have

$$\begin{aligned} H_5 < \quad H_1 \quad < G \\ H_5 < \quad H_2 \quad < G \\ H_5 < \quad H_3 \quad < G \\ H_5 < \quad H_4 \quad < G \end{aligned}$$

and its subgroup lattice will be



What are the elements of D_n? Note that $ba = a^2b = a^{-1}b$. We can use this to be able to perform any operation. We have for example $aba = a(ba) = a(a^{-1}b) = aa^{-1}b = eb = b$.

We then get, for general dihedral groups, that,

$$a^p a^q = a^{(p+q)(mod\ n)},$$

because of the associativity of the subgroup $< a >$. We then get,

$$a^p ba^q = a^p(ba)a^{q-1} = a^p(a^{-1}b)a^{q-1} = a^{p-1}ba^{q-1} = a^{p-1-1}ba^{q-2} = \ldots = a^{(p-q)(mod\ n)}b,$$

and,

$$a^p ba^q b = a^{(p-q)(mod\ n)}bb = a^{(p-q)(mod\ n)}e = a^{(p-q)(mod\ n)}.$$

In general all elements of the dihedral groups will be of this form. Hence, the group table for D_4 can be obtained as below.

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	ab^2
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

A degenerate '2-sided Regular Polygon' would be a line segment. This would have one 'do nothing' operator, one rotate by 180° operator and two symmetric operators that would actually be the same as the ones we already got. This would make the total number of operators equal to two, not 4 as our rule states. There is thus no dihedral group of order 2 or less. We now define formally a what a dihedral group is.

Definition 3.10. *Let n be a positive integer, $n \geq 3$, D_n is called the* **dihedral group of order** $2n$ *under composition of symmetries.*

$$D_n = \{a^r b^s | r = 0, 1, \ldots, n-1, s = 0, 1\}$$

where

$$\begin{aligned} a^p a^q &= a^{(p+q)(mod\ n)} \\ a^p b a^q &= a^{(p-q)(mod\ n)} b \\ a^p b a^q b &= a^{(p-q)(mod\ n)}. \end{aligned}$$

Exercises.

1. Find $Z(D_3)$
2. Construct the lattice diagram for D_4.

Chapter 4

Lagrange's Theorem and Homomorphisms

4.1 Cosets

In this section we let G be a group and H a subgroup of G; we shall consider certain subsets of G determined by H.

Definition 4.1. *For any $g \in G$, the subset $Hg = \{hg | h \in H\}$ of G is called a **right coset** of H.*

Remarks: There are several things to note about this definition.

1. $g \in Hg$, since $g = eg$ and $e \in H$.

2. If H is finite, say $H = \{h_1, \ldots h_n\}$, then $Hg = \{h_1 g, \ldots, h_n g\}$ and these elements $h_i g$ are all distinct by the Cancelation Laws.

3. H is one of its right cosets, since $H = He$.

4. Although each element $g \in G$ gives a right coset Hg, there is no claim that we obtain a different right coset for each element, in fact as we shall see this only happens if $H = \{e\}$.

Example 4.1. Let $G = \mathbb{Z}$ and $H = 4\mathbb{Z}$. We have the following right cosets of H:

$$\begin{aligned} 4\mathbb{Z} + 0 &= \{4n | n \in \mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}, \\ 4\mathbb{Z} + 1 &= \{4n + 1 | n \in \mathbb{Z}\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}, \\ 4\mathbb{Z} + 2 &= \{4n + 2 | n \in \mathbb{Z}\} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}, \\ 4\mathbb{Z} + 3 &= \{4n + 3 | n \in \mathbb{Z}\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}. \end{aligned}$$

This accounts for all elements of $\mathbb{Z}$. Moreover, these are the only right cosets, e.g.

$$4\mathbb{Z}+4=\{4n+4|n\in\mathbb{Z}\}=\{\ldots,-4,0,4,8,12,\ldots\}=4\mathbb{Z}+0$$

In this example we see that the right cosets partition G; there must therefore be an equivalence relation giving rise to this partition. We recall that the equivalence relation concerned must be such that two elements of G are related if and only if they lie in the same subset; here we have

$$a \text{ and } b \text{ lie in the same right coset } \iff a\equiv b(mod\ 4)\iff 4|(a-b)\iff a-b\in 4\mathbb{Z}.$$

Now $-b$ is the inverse of b in the additive group $\mathbb{Z}$; so this suggests considering the relation defined by

$$a\sim b\iff ab^{-1}\in H.$$

Theorem 4.1. *If $H\leq G$, the relation $\sim$ defined on G by $a\sim b\iff ab^{-1}\in H$ is an equivalence relation; the equivalence class containing a is the right coset Ha.*

Thus from what we know about equivalence relations, we see that the right cosets of H do indeed partition G.

Example 4.2. Take $G=D_4$.

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	ab^2
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Take $H=\{e,b\}$. The right cosets of H are then

$$\begin{aligned}
He &= \{e,b\}=Hb\\
Ha &= \{a,ba\}=\{a,a^3b\}=Ha^3b\\
Ha^2 &= \{a^2,ba^2\}=\{a^2,a^2b\}=Ha^2b\\
Ha^3 &= \{a^3,ba^3\}=\{a^3,ab\}=Hab
\end{aligned}$$

Note that this bears out the general result shown earlier that if g is any representative of a given equivalence class C, then $[g]=C$.

So far we have considered only right cosets; however, in an exactly similar way we may define the left cosets of a subgroup H of G as the subsets of the form gH for $g\in G$. Their properties are analogous to those of right cosets; the left coset version of theorem

4.1 uses the element $a^{-1}b$ instead of $ab^{-}1$. Clearly, if G is abelian then left and right cosets are the same thing. However, in example 4.2 the left cosets of H are

$$\begin{aligned} eH &= \{e, b\} = bH \\ aH &= \{a, ab\} = abH \\ a^2H &= \{a^2, a^2b\} = a^2bH \\ a^3H &= \{a^3, a^3b\} = a^bH \end{aligned}$$

and so we see that in general left and right cosets may be different.

Exercises.

1. Find the left and the right cosets of the following subgroups:
   (a) $G = (Z_{12}, +),\ H =< 3 >$
   (b) $G = D_4,\ H =< a >$

4.2 Lagrange's Theorem

As an immediate consequence of theorem 4.1, we may prove one of the fundamental theorems of finite group theory, called Lagrange's theorem.

Theorem 4.2. *(Lagrange's Theorem) If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.*

Example 4.3.

1. D_4 $\{e, a, a^2, a^3\}$ and $\{e, b\}$, and $4|8, 2|8$.
2. $(\mathbb{Z}_6, +)$ has subgroups $\{0, 2, 4\}$ and $\{0, 3\}$, and $3|6, 2|6$.

Remarks: Note that we have also shown that the number of right cosets of H in G is $|G|/|H|$; we call this number the **index of H in G**, and write it as $|G : H|$. The rest of this section is devoted to consequences of Lagrange's theorem; we begin with the order of an element.

Corollary 4.2.1. *If $|G| = n$ and $g \in G$, then $o(g)|n$ and $g^n = e$.*

Example 4.4.

The elements of D_4 have orders 1, 2 and 4, each of which divides 8.

The elements of $(Z_6, +)$ have orders 1, 2, 3 and 6, each of which divides 6.

Our next result classifies at a stroke all groups of order n for infinitely many values n.

Corollary 4.2.2. *A group of prime order is cyclic, and has no proper non-trivial subgroups; any non-identity element generates the group.*

Example 4.5. The group in example 2.11(2) is cyclic since its order is 5.

Theorem 4.3. *If $H, K \leq G$ and $(|H|, |K|) = 1$, then $H \cap K = \{e\}$.*

Example 4.6. *If $G = (\mathbb{Z}_6, +)$ we may take $H = \{0, 2, 4\}$ and $K = \{0, 3\}$, then $|H| = 3, |K| = 2$ and $(3, 2) = 1$, and we do indeed have $H \cap K = \{0\}$.*

Exercises.

1. Find $G : H$ for the following given groups and subgroups.
   (a) $G = (Z, +), H = 3Z$
   (b) $G = (\{1, -, i, -i\}, \bullet), H = \{1, -1\}$
   (c) $G = D_4,\ H = \{e, a, a^2, a^3\}$
2. Determine if the statement is true or false (*Fraleigh, Exercise 15, p. 123)*
   (a) The number of left cosets of a subgroup of a finite group divides the order of the group.
   (b) Every group of prime order is abelian.
   (c) A subgroup of a group is a left coset of itself.
   (d) Every finite group contains an element of every order that divides the order of the group.
   (e) Only subgroups of finite groups can have left cosets.
3. Let G be a group, and let $a \in G$, with $o(a) = 30$. Let $H =< a >,\ \ K =< a^4 >$. How many distinct cosets does K have in H? Identify these cosets.
4. Let $g, h \in G$ with $gh = hg$. Show that if $o(g) = m$ and $o(h) = n$ with $(m, n) = 1$, then $o(gh) = mn$.

4.3 Homorphisms

In this section we consider maps between groups which "preserve structure".

Definition 4.2. *Let G and H be groups. A map $\phi : G \to H$ is called a **homomorphism** if*

$$\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in G.$$

*A homomorphism which is one-to-one is or injective called a **monomorphism**. If it is onto or surjective, then it is called an **epimorphism**. A homomorphism which is both one-to-one and onto or bijective is called an **isomorphism**. If there is an isomorphism $G \to H$, we say that G and H are **isomorphic**, and write $G \cong H$.*

Remarks: Two finite groups G and H are isomorphic if their Cayley tables have the same structure, it is only the names of the elements which are different. Hence, we can "replace" the elements of G by those of H which is a bijection , and as the element in row a and column b is ab, we need the element in row $\phi(a)$ and column $\phi(b)$ to be $\phi(ab)$. This is exactly the condition above.

Example 4.7.

1. The map $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by $\phi(n) = 2n$ for all $n \in \mathbb{Z}$ is a homomorphism, since

$$\phi(m + n) = 2(m + n) = 2m + 2n = \phi(m) + \phi(n)$$

for all $m, n \in \mathbb{Z}$.

If $m,\ n \in \mathbb{Z}$ such that $\phi(m) = 2m = 2n = \phi(n)$, then $m = n$ and hence ϕ is one-to-one. However, all odd integers have no pre-images under ϕ and hence ϕ is not onto.

2. The map $\phi : (\mathbb{R}^*, \bullet) \to (\mathbb{R}^*, \bullet)$ defined by $\phi(x) = x^2$ for all $x \in \mathbb{R}^*$ is a homomorphism, since

$$\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y)$$

for all $x, y \in \mathbb{R}^*$.

However, $\phi(-2) = 4 = \phi(2)$ which shows that ϕ is not one-to-one. It is also not onto since negative real numbers have no pre-images.

3. The map $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \bullet)$ defined by $\phi(x) = e^x$ for all $x \in \mathbb{R}$ is a homomorphism, since

$$\phi(x + y) = e^{(x+y)} = e^x e^y = \phi(x)\phi(y)$$

for all $x, y \in \mathbb{R}$.

If $x,\ y \in \mathbb{R}$ such that $\phi(x) = e^x = e^y = \phi(y)$, then $x = y$. Also, if $y \in \mathbb{R}^+$ then we can find $x = \ln y$ such that $e^x = y$. This means that ϕ is both one-to-one and onto and hence, ϕ is an isomorphism.

4. The map $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ defined by $\phi(r) = [r]$ for all $r \in \mathbb{Z}$ is a homomorphism, since

$$\phi(r + s) = [r + s] = [r] + [s] = \phi(r) + \phi(s)$$

for all $r, s \in \mathbb{R}^*$.

If $x,\ y \in \mathbb{Z},\ \ x \neq y$ such that $x = q_1 n + r,\ y = q_2 n + r$, then $\phi(x) = \phi(q_1 n + r) = r = \phi(y)$, which shows that ϕ is not one-to-one. On the other hand, if $r \in \mathbb{Z}_n$, then for all integer values of q, we have $x = qn + r \in \mathbb{Z}$ and $\phi(x) = \phi(qn + r) = r$, which means that ϕ is onto and therefore an epimorphism.

There are certain properties which any homomorphism possesses.

Theorem 4.4. *Let $\phi : G \to H$ be a homomorphism, then:*

1. $\phi(e_G) = e_H$;
2. $\phi(g^{-1}) = \phi(g)^{-1}$ *for all* $g \in G$. ;
3. $\phi(g^n) = \phi(g)^n$ *for all* $g \in G, n \in \mathbb{Z}^+$.

Remark: Note that if G and H are both additive groups, then (3) is written $\phi(ng) = n\phi(g)$.

Example 4.8.

1. Take $G = (\mathbb{R}^*, \bullet)$ and $H = (\mathbb{R}^*, \bullet)$ with the map $\phi : G \to H$ defined by $\phi(x) = x^2$ for all $x \in \mathbb{R}^*$: we have $e_G = 1$, and $\phi(1) = 1^2 = 1 = e_H$; the inverse of $x \in G$ is $\frac{1}{x}$, and $\phi\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)^2 = \frac{1}{x^2}$ which is the inverse of $x^2 = \phi(x)$; the nth power of x is x^n, and $\phi(x^n) = (x^n)^2 = x^2 n = (x^2)^n$, which is the nth power of $x^2 = \phi(x)$.
2. Take $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}^+, \bullet)$, with the map $\phi : G \to H$ defined by $\phi(x) = e^x$ for all $x\mathbb{R}$: we have $e_G = 0$, and $\phi(0) = e^0 = 1 = e_H$; the inverse of $x \in G$ is $-x$, and $\phi(-x) = e^{-x}$, which is the inverse of $e^x = \phi(x)$; the nth power of x is nx, and $\phi(nx) = e^{(nx)} = (e^x)^n$, which is the nth power of $e^x = \phi(x)$.

This result has an immediate consequence for orders of elements.

Corollary 4.4.1. *If G has finite order n and $\phi : G \to H$ is a homomorphism, then the order of $\phi(g)$ divides n; if ϕ is one-to-one, then the order of $\phi(g)$ equals n.*

In particular, if two groups are isomorphic they must have equal numbers of elements of any given order; this can sometimes be used to show that two groups are not isomorphic.

Example 4.9. Consider the multiplicative groups $\mathbb{R}^*$ and $\mathbb{R}^+$; the element -1 of $\mathbb{R}^*$ has order 2, whereas $\mathbb{R}^+$ has no such element, so they cannot be isomorphic.

Our next result concerns the composition of two homomorphisms.

Theorem 4.5. *If $\phi : G \to H$ and $\theta : H \to K$ are both homomorphisms, so is $\phi \circ \theta : G \to K$.*

In the case of an isomorphism we may consider its inverse.

Theorem 4.6. *If $\phi : G \to H$ is an isomorphism, so is $\phi^{-1} : H \to G$.*

Definition 4.3. *An isomorphism $\phi : G \to G$ is called an* ***automorphism*** *of G.*

Remark: Theorems 4.5 and 4.6 show that the set of automorphisms of G actually form a group.

We conclude this section by giving a result on cyclic groups being isomorphic.

Theorem 4.7. *Any two cyclic groups of the same order are isomorphic.*

Exercises. Determine if $\phi : G \to G'$ is a homomorphism. If it is, determine if it is an isomorphism.

1. $G = (\mathbb{Z}, +)$, $G' = (\mathbb{Z}_n, +)$, where n is a positive integer, $\phi(a) = r$ where $a = qn + r$, $0 \leq r < n$.
2. $G = G' = (\mathbb{R}^*, \bullet)$ and define $\phi : G \to G'$ by $\phi(x) = x^n$, where n is a positive integer.
3. $G = (\mathbb{R}, +)$, $G' = (\mathbb{Z}, +)$, $\phi(x) = \lfloor x \rfloor$.
4. $G = G' = (\mathbb{R}^*, \bullet$, $\phi(x) = |x|$
5. $G = (\mathbb{R}, +)$, $G' = (\mathbb{R}^*, \bullet)$, $\phi(x) = 2^x$

4.4 Kernel and Image of a Homomorphism

In this section we take an arbitrary homomorphism $\phi : G \to H$ and try to measure how far it is from being an isomorphism.

Definition 4.4. *Given a homomorphism $\phi : G \to H$, the **kernel** of ϕ is the subset $Ker\phi = \{g \in G | \phi(G) = e_H\}$ of G, while the image of ϕ is the subset $\phi(G) = \{\phi(g) | g \in G\}$ of H.*

Example 4.10.

1. If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is defined by $\phi(n) = 2n$ for all $n \in \mathbb{Z}$, then $Ker\phi = \{0\}$ and $\phi(G) = 2\mathbb{Z}$.
2. If $\phi : (\mathbb{R}^*, \bullet) \to (\mathbb{R}^*, \bullet)$ defined by $\phi(x) = x^2$ for all $x \in \mathbb{R}^*$, then $Ker\phi = \{-1, 1\}$ and $\phi(G) = \mathbb{R}^+$.
3. If $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \bullet)$ defined by $\phi(x) = e^x$ for all $x \in \mathbb{R}$, then $Ker\phi = \{0\}$ and $\phi(G) = \mathbb{R}^+$.
4. If $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ defined by $\phi(r) = [r]$ for all $r \in \mathbb{Z}$, then $Ker\phi = \{n\mathbb{Z}\}$ and $\phi(G) = \mathbb{Z}_n$.

It will be seen that in each of these examples the kernel and image are subgroups of G and H respectively; this is no accident.

Theorem 4.8. *If $\phi : G \to H$ is a homomorphism, then $Ker\phi \leq G$ and $\phi(G) \leq G$.*

Our next result concerns homomorphic images of cyclic groups.

Theorem 4.9. *If G is cyclic and $\phi : G \to H$ is a homomorphism, then $\phi(G)$ is also cyclic.*

It is clear that $\phi(G)$ gives a measure of how close ϕ is to being surjective; we may now show that $Ker\phi$ does the same thing for injectivity.

Theorem 4.10. *$\phi : G \to H$ is one-to-one if and only if $Ker\phi = \{e_G\}$.*

Thus if only one element of G maps to e_H, then only one element of G maps to each element of $\phi(G)$. Our next result generalizes this.

Theorem 4.11. *Let $\phi : G \to H$ be a homomorphism with $Ker\phi = K$, and take $g \in G$ and $h \in \phi(G)$; then the set $\{x \in G | \phi(x) = h\}$ equals the right coset Kg.*

Thus if $|Ker\phi| = m$, exactly m elements of G map to each element of $\phi(g)$.

Example 4.11. *Take the homomorphism $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_5, +)$ defined by $\phi(r) = [r]$ for all $r \in \mathbb{Z}$; then $Ker\phi = 5\mathbb{Z}$. If we take $g = 7$ then $h = \phi(g) = [7] = [2]$; the set of elements $x \in \mathbb{Z}$ with $\phi(x) = [2]$ is the right coset $5\mathbb{Z} + 2 = 5\mathbb{Z} + 7$.*

This result has a consequence applying to homomorphisms from finite groups.

Corollary 4.11.1. *Let $\phi : G \to H$ be a homomorphism, and suppose $|G| = n, |Ker\phi| = m, \phi(G) = r$; then $n = mr$.*

Thus $|\phi(G)|$ must divide both $|G|$ and $|H|$. This observation can sometimes be useful.

Example 4.12. *If $|G| = 16$ and $|H| = 9$, the only homomorphism $\phi : G \to H$ is the trivial map sending all elements of G to e_H since $|\phi(G)|$ must divide both 16 and 9, it must be 1, so $\phi(G) = e_H$.*

Exercises. Determine if ϕ is one-to-one by finding the kernel of each of the following homomorphisms.

1. $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_6, +)$, $\phi(x) = \phi(6q + r) = r$
2. $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \bullet)$, $\phi(x) = 2^x$.
3. $\phi : (\mathbb{R}^*, \bullet) \to (\mathbb{R}^+, \bullet)$, $\phi(x) = |x|$.
4. $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \bullet)$, $\phi(x) = 3^x$.

Chapter 5

Conjugacy

5.1 Conjugacy Classes

We begin with a definition concerning pairs of elements of G which at first sight may seem rather strange.

Definition 5.1. *If $a, b \in G$, we say that b is conjugate to a if there exists $x \in G$ with $b = x^{-1}ax$.*

Example 5.1.

1. In D_4 we have a^3 conjugate to a, since with $x = b$ we have $b^{-1}ab = bab = a^3bb = a^3$.
2. In any group G, the only element conjugate to the identity is itself, since for all $x \in G$ we have $x^{-1}ex = x^{-1}x = e$.

Our first result shows that this definition is not as strange as it may seem.

Theorem 5.1. *Conjugacy is an equivalence relation on G.*

Since we have an equivalence relation, we know that we have equivalence classes, and that they partition G.

Definition 5.2. *The equivalence classes for the relation of conjugacy are called **conjugacy classes** of G; we write $\mathbf{C}_g$ for the conjugacy class containing the element g.*

On the previous lesson, when we had an equivalence relation on G, we saw that all equivalence classes, the right cosets of the subgroup H, had the same size; this enabled us to prove an important result, the Lagrange's theorem. The two examples above immediately show that this is not the case here; we shall need to consider how to calculate the size of a given conjugacy class in due course.

We begin by noting that example (2) above shows that the conjugacy class $\mathbf{C}_e$ is simply $\{e\}$; we may determine which other elements of G form conjugacy classes on their own.

Theorem 5.2. *If $g \in G$ then $\mathbf{C}_g = \{g\}$ if and only if $g \in Z(G)$.*

As a result, we see that conjugacy is really only of interest in a non-abelian group.

Corollary 5.2.1. *G is abelian if and only if $\mathbf{C}_g = \{g\}$ for all $g \in G$.*

Our next results will show that conjugate elements have very similar properties. We begin by considering orders of conjugate elements.

Theorem 5.3. *If $g, h \in G$ and h is conjugate to g, then $o(h) = o(g)$.*

Example 5.2. In D_4 the elements a and $a^3$are conjugate, and each has order 4.

Remark: The converse need not be true, for example, in $\mathbb{Z}_4$ the elements [1] and [3] both have order 4, but they are not conjugate as the group is abelian. We next consider centralizers.

Theorem 5.4. *If $g, h \in G$ and $h = x^{-1}gx$, then $C_G(h) = x^{-1}C_G(g)x$.*

In particular, in a finite group conjugate elements have centralizers of the same size.

Example 5.3. If $G = D_4$ we have $b^{-1}ab = a3$, and $C_G(a) = \{e, a, a^2, a^3\} = C_G(a^3)$; thus $b^{-1}C_G(a)b = \{b^{-1}eb, b^{-1}ab, b^{-1}a^2b, b^{-1}a^3b\} = \{e, a^3, a^2, a\} = b^{-1}C_G(a^3)b$.

Example 5.4. We shall determine the conjugacy classes in $G = D_3$. We know that $\{e\}$ is one conjugacy class; we saw that $Z(G) = \{e\}$ from exercise (1) of section 3.4, so this is the only conjugacy class of order 1. Of the remaining elements, a and a^2 have order 3 while the rest have order 2; thus $\{a, a^2\}$ must be a conjugacy class, as must $\{b, ab, a^2b\}$ (otherwise there would be a class of order 1). To check this, note that $b^{-1}ab = bab = a2$ so that $a^2 \in \mathbf{C}_a$, while $(a2)^{-1}ba^2 = aba^2 = ba = a^2b$ and $a^{-1}ba = a^2ba = ab$ so that $a^2b, ab \in \mathbf{C}_b$. Thus we do indeed have three conjugacy classes $\mathbf{C}_e, \mathbf{C}_a$ and $\mathbf{C}_b$, of sizes 1, 2 and 3. Note that the centralizer sizes of representative elements are $|C_G(e)| = |G| = 6, |C_G(a)| = |\{e, a, a^2\}| = 3$ and $|C_G(b)| = |\{e, b\}| = 2$.

This example suggests the following expression for the size of a conjugacy class.

Theorem 5.5. *If g inG, then $|\mathbf{C}_g| = \dfrac{|G|}{C_G(g)}$.*

Example 5.5. Take $G = D_3$ and $g = b$, so that $C_G(g) = \{e, b\}$. We let x run through the elements of G, and compute the conjugate $x^{-1}gx$ and the right coset $C_G(g)x$. We obtain the following.

x	$x^{-1}gx$	$C_G(g)x$
e	b	$\{e, b\}$
b	b	$\{e, b\}$
a	ab	$\{a, a^2b\}$
a^2b	ab	$\{a, a^2b\}$
a^2	a^2b	$\{a^2, ab\}$
ab	a^2b	$\{a^2, ab\}$

Thus each distinct conjugate $x^{-1}gx$ corresponds to a distinct right coset $C_G(g)x$.

Exercises.

1. Find all the conjugacy classes of D_4.
2. Let H be a subgroup of a group G. For any x in G, define $x^{-1}Hx = \{x^{-1}hx | h \in H\}$. Prove that
   (a) $x^{-1}Hx \leq G$.
   (b) If H is cyclic, then $x^{-1}Hx$ is cyclic.
   (c) If H is abelian, then $x^{-1}Hx$ is abelian.

5.2 Normal Subgroups

In this section we consider a certain type of subgroup of a group G, defined in terms of conjugacy.

Definition 5.3. *The subgroup H of a group G is called a* ***normal subgroup*** *if $g^{-1}hg$ for all $h \in H$ and $g \in G$; we write $H \triangleleft G$ if this condition is satisfied.*

Example 5.6.
1. If $G = D_4$, then $H = \{e, b\}$ is not a normal subgroup, since $a^{-1}ba = a^3ba = a^2b \notin H$.
2. If $G = D_4$, then $H = \{e, a^2\}$ is a normal subgroup, since for all $g \in G$ we have $g^{-1}eg = e$ and $g^{-1}a^2g = a^2$, as $a^2 \in Z(G)$.

Remarks: Although this is at first sight a rather strange definition, we will see that it has some important consequences. The following facts are immediate.

1. Every subgroup of an abelian group is normal because if $gh = hg$ for any g and h then $g^{-1}hg = h$.
2. $\{e\}$ and G are normal subgroups of G.
3. $Z(G) \triangleleft G$ because if $h \in Z(G)$ then $g^{-1}hg = h$ for all $g \in G$.
4. A normal subgroup is a union of conjugacy classes of G.

The last of these observations can be useful, as the following examples show.

Example 5.7.

1. The conjugacy classes of D_3 are $\{e\}, \{a, a^2\}$, and $\{b, ab, a^2b\}$. If $H \triangleleft G$, then H must be a union of some of these, including $\mathbf{C}_e$; there are four possibilities:

$$\mathbf{C}_e, \quad \mathbf{C}_e \cup \mathbf{C}_a, \quad \mathbf{C}_e \cup \mathbf{C}_b, \quad \mathbf{C}_e \cup C_a \cup \mathbf{C}_b$$

   However, $|\mathbf{C}_e \cup \mathbf{C}_b| = 1 + 3 = 4$, which does not divide $|D6| = 6$, so this cannot be a subgroup; the remaining three are in fact all subgroups: we have $\mathbf{C}_e = \{e\}, \mathbf{C}_e \cup \mathbf{C}_a = \{e, a, a^2\}$ and $\mathbf{C}_e \cup C_a \cup \mathbf{C}_b$.

2. Suppose that we are given a group G of order 12 with four conjugacy classes, $\mathbf{C}_e, \mathbf{C}_a, \mathbf{C}_b$, and $\mathbf{C}_c$; we are told that $|C_G(a)| = 4$ and $C_G(b) = C_G(c)$, and are asked to show that G can only have one possible proper non-trivial normal subgroup. We identify the class sizes: $|\mathbf{C}_e| = 1$ since $\mathbf{C}_e = \{e\}$; $|\mathbf{C}_a| = \frac{12}{4} = 3$; and as $|\mathbf{C}_b| = |\mathbf{C}_c|$ and the sum of the class sizes is $|G| = 12$, we must have $|\mathbf{C}_b| = |\mathbf{C}_c| = 4$. The only possible combination of 1,3,4,4 including 1 which gives a factor of 12 other than 1 or 12 is 1+3=4; so the only possible proper non-trivial normal subgroup is $\mathbf{C}_e \cup \mathbf{C}_a$.

Our main result in this section gives some explanation of why a normal subgroup is defined as it is; the full picture will emerge in the final section.

Theorem 5.6. *If H is a subgroup of G, then $H \lhd G$ if and only if the left and right cosets of H in G are the same.*

Example 5.8. We saw that in D_4 the left and right cosets of the subgroup $H = \{e, b\}$ were different, so this gives another way of seeing that H is not a normal subgroup.

This result gives a convenient way of seeing in a particular case that a subgroup is normal.

Corollary 5.6.1. *If G is a finite group and H is a subgroup of index 2 in G so that $|H| = \frac{1}{2}|G|$, then $H \lhd G$.*

Example 5.9.

1. If $G = D_3$ then we have seen that $H = \{e, a, a^2\}$ is a normal subgroup of G, and its index in G is 2.

2. If $G = D_4$ then the subgroup $H = \{e, a, a^2, a^3\}$ is a normal subgroup, since its index in G is 2. We may see this directly as follows: clearly $g^{-1}hg \in H$ for all $g, h \in H$, so it suffices to consider $g \notin H$; then $g = a^i b, h = a^j$, and $g^{-1}hg = (a^i b)^{-1}a^j a^i b = b^{-1}(a^i)^{-1}a^j a^i b = b^{-1}(a^- i a^j a^i)b = b^{-1}a^j b = a^j \in H$

Exercises.

1. Determine if $H \lhd G$.

   (a) $G = (Z, +),\ H = 3Z$

   (b) $G = D_4, H = \{e, ab\}$

2. Show that $Z(G)$ is a normal subgroup of G, where G is any group and $Z(G)$ is the center of G.

3. If $H,\ K$ are normal subgroups of G, then $L = H \cap K$ is also a normal subgroup of G

5.3 Quotient Groups

In this final section we shall see that the main reason for the importance of normal subgroups concerns their relationship with homomorphisms.

Theorem 5.7. *If $\phi : G \to H$ is a homomorphism, then $Ker\phi \lhd G$.*

Thus every homomorphism from G gives a normal subgroup of G. In fact, the reverse is also true; to see this, we begin by recalling the construction of $\mathbb{Z}_n$. Given $n \in \mathbb{Z}^+$, we took the group $\mathbb{Z}$ and partitioned it into equivalence classes $[0], [1], \ldots [n-1]$. We then sought to define a binary operation on this set of equivalence classes by setting

$$[a] + [b] = [a + b] \text{ for all equivalence classes } [a], [b]$$

we had to be careful here, since we needed to check that this definition did not depend on the choice of representatives of the classes $[a]$ and $[b]$. Having done so, it was then easy to show that this made the set of equivalence classes into a group, which we called $\mathbb{Z}_n$. Now the equivalence class $[r]$ is just the right coset $n\mathbb{Z} + r$ of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$. This suggests that, given any group G and a subgroup H, we might try to generalize the above construction and turn the set of right cosets of H in G into a group, by defining a binary operation on the set of right cosets by

$$HxHy = Hxy \text{ for all right cosets } Hx, Hy$$

however, for this to work we must overcome the problem about choosing different representatives of right cosets. As typical elements of Hx and Hy are $h'x$ and hy for $h, h' \in H$, we need $h'xhy \in Hxy$, i.e., $h'xhy(xy)^{-1} \in H$; since

$$h'xhy(xy)^{-1} = h'xhyy^{-1}x - 1 = h'xhx^{-1},$$

and $h' \in H$, the condition required is that $xhx^{-1} \in H$ for all $h \in H$ and $x \in G$, which is exactly the requirement that H be a normal subgroup of G. Thus if $H \lhd G$, we can define a binary operation on the set of right cosets of H in G as above; in this case we call the set of cosets G/H. We may now prove that this binary operation does make G/H into a group, called the *quotient group* of G by H, and that there is a homomorphism, called the *natural map*, from G to G/H with kernel H.

Theorem 5.8. *If H is a normal subgroup of G, the set G/H of cosets of H in G is a group under the binary operation above; there is a homomorphism $\phi : G \to H$ defined by $\phi(g) = Hg$, and $ker\phi = H$.*

Example 5.10.

1. If $G = D_4$ and $H = \{e, b\}$, we know that H is not a normal subgroup of G; we cannot define a binary operation on the set of right cosets of H as above, as $Ha = \{a, a^3b\}, Ha^2 = \{a^2, a^2b\}$, but $aa^2 = a^3$ and $a^3ba^2b = a$ do not lie in the same right coset.

2. If $G = D_4$ and $H = \{e, a^2\}$, then we have seen that $H \lhd G$; thus we do have a group G/H. If we order the elements of G according to the cosets of H, the Cayley table of G naturally gives that of G/H; here we have $G/H \cong$ Klein 4-group.

G	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	ab^2
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

G/H	He	Ha	Hb	Hab
He	He	Ha	Hb	Hab
Ha	Ha	He	Hab	Hb
Hb	Hb	Hab	He	Ha
Hab	Hab	Hb	Ha	He

Note that the Cayley table of G only breaks into 'blocks' of cosets of H if H is normal.

We have thus shown that there is a close relationship between homomorphisms from G and normal subgroups of G, given by taking kernels. The next result may be seen as showing that this relationship is essentially (i.e., up to isomorphism) a bijection, in that the natural map is the only homomorphism having a given normal subgroup as its kernel.

Thus let $\phi : G \to G_1$ be any homomorphism; then $Ker\phi \lhd G$, so we may form the quotient group $G/Ker\phi \cong \phi(G)$. By corollary 4.11.1 we know that $|G/Ker\phi| = |\phi(G)|$ if G is finite; the fundamental homomorphism theorem states that in fact rather more is true.

Theorem 5.9. *(The Fundamental Theorem of Homomorphism) If $\phi : G \to G_1$ is a homomorphism, then $G/Ker\phi \cong \phi(G)$.*

Example 5.11. Let $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_4, +)$ be the homomorphism defined by

$$\phi(x) = \phi(4q + r) = r$$

Then $N = Ker\ \phi = \{4k + k \in Z\}$ and $G/N = \{N, N + 1, N + 2, N + 3\}$. The mapping ψ consists of the following: $N \mapsto 0,\ N + 1 \mapsto 1,\ N + 2 \mapsto 2,\ N + 3 \mapsto 3$. Clearly, ψ is an isomorphism. Moreover, ϕ is onto, so that $\phi(\mathbb{Z}) = \mathbb{Z}_4$. The group tables for $G/N = \mathbb{Z}/N$ and $G_1 = \mathbb{Z}_4$ are shown below:

$*$	N	$N+1$	$N+2$	$N+3$
N	N	$N+1$	$N+2$	$N+3$
$N+1$	$N+1$	$N+2$	$N+3$	N
$N+2$	$N+2$	$N+3$	N	$N+1$
$N+3$	$N+3$	N	$N+1$	$N+2$

$*$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Observe that each group table can be obtained from the other by replacing the entries in a table by the corresponding images or pre-images under the mapping ψ.

The fundamental homomorphism theorem is also known as the *First Isomorphism Theorem*. We also have the following isomorphism theorems. The proofs are omitted in these notes but you may refer to Fraleigh, pp. 229-230.

Theorem 5.10. *(Second Isomorphism Theorem) Let H be a subgroup of a group G and N be a normal subgroup of G. Then $HN/N \cong H/H \cap N$.*

Theorem 5.11. *Third Isomorphism Theorem) Let H and K be normal subgroups of a group G, with $K \leq H$. Then $G/H \cong (G/K)/(H/K)$.*

Example 5.12. *Let $G = \mathbb{Z},\ H = 5\mathbb{Z},\ K = 10\mathbb{Z}$, with respect to addition. Since G is abelian, every subgroup is normal, so $H,\ K$ are normal subgroups of G. We have*

$$\begin{aligned} G/H &= \mathbb{Z}/5\mathbb{Z} = \{\ H,\ H+1,\ H+2,\ H+3,\ H+4\ \} \cong \mathbb{Z}_5 \\ G/K &= \mathbb{Z}/10\mathbb{Z} = \{\ K,\ K+1, K+2,\ \ldots, K+9\ \} \cong \mathbb{Z}_{10} \\ H/K &= 5\mathbb{Z}/10\mathbb{Z} = \{K,\ K+5\ \} \cong \mathbb{Z}_2 \end{aligned}$$

On the other hand,

$$\begin{aligned} (G/K)/(H/K) &= \{H/K,\ H/K + (K+1),\ H/K + (K+2),\ H/K + (K+3), \\ &\quad H/K + (K+4)\ \} \cong \mathbb{Z}_5 \end{aligned}$$

which shows that

$$G/H \cong (G/K)/(H/K)$$

Exercises.

1. For the homomorphism $\phi : D_4 \to (\{1, -1\}, \bullet)$ defined by

$$\phi(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is a rotation} \\ -1 & \text{if } \alpha \text{ is a reflection} \end{cases}$$

   do the following:

   (a) Find $K = Ker\phi$

   (b) Construct the group tables for G/K and $\phi(G)$

   (c) Find the image of each element of G/K under the natural map ψ.

2. For each of the following, find the elements of $G/H,\ G/K,\ H/K$ and $(G/K)/(H/K)$. Construct the group tables for G/H and $(G/K)/(H/K)$ and identify the corresponding images of these two isomorphic factor groups.

   (a) $G = \mathbb{Z}, H = 3\mathbb{Z},\ K = 9\mathbb{Z}$

   (b) $G = Z_{24}, H =< 2 >,\ K =< 6 >$