UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG

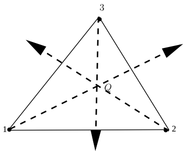
SCHOOL OF
MATHEMATICS

ABTRACT MATHEMATICS

MATH2015

PART 1: ELEMENTARY ALGEBRA, Chapters 1-5

PART 2: ELEMENTARY GROUP THEORY, Chapters 6-8



NAME:

STUDENT NUMBER:

Phone Number:

Prof E.G. Mphako-Banda and Ms C. Mennen
School of Mathematics
University of the Witwatersrand

Contents

Chapter 1

FINITE,COUNTABLE AND UNCOUNTABLE SETS

1.1 ELEMENTS AND MEMBERSHIP

The word *set* is fundamental in all mathematics today, from elementary school to research mathematics. We think of a set as a *collection of objects* with the objects being *members or elements of* the set, or belonging to the set. This concept of a set is supported by intuition and vision and relies on our mutual understanding of the words and symbols used in the description. As such, a set may be classed as a *common notion.*

1.1.1 Definition: *empty, non-empty, finite and infinite sets*

A set is a collection of elements that may be given by listing or by specifying a property. It may contain no elements, that is, it may be *empty*; have a *finite* number of elements; or have an *infinite* number of elements. If a set has elements, it is said to be *non-empty.* Two set are *equal* if they have identical memberships. We use the following notation: If X is any set then $x \in X$ means x is and element or member of the set X, and $x \notin X$ means that x is not a member of the set X.

1.1.2 Listing and set builder notation

We introduce a notation for sets. Let $A = \{1, 2, 3, 4, 5\}$. Here the elements of A are listed. We may write $A = \{x \in \mathbb{Z} \mid 1 \leq x \leq 5\}$. This is the *set-builder* notation for the set A. More generally if $p(x)$ is any statement about the elements x of a known set U, $\{x \in U \mid p(x)\}$ is the set of all elements in U for which $p(x)$ is true. e.g.$U = \mathbb{Z}$, and $p(x)$ is the statement that x lies between 1 and 5. It not always possible to write a set as a list and/or in set builder notation.

1.1.3 Notation

We use capital letters such as A to represent sets, lower case letters such as a to represent elements and $\in$ and $\notin$ for an element of and not an element of respectively.

1.2 ORDER OF A SET

Let $|A|$ be the number of elements in set A. We call this number the *order*, *size*, or *cardinality* of the set A. Hence ; $|A| = 0 \iff A = \emptyset$, $|A| = 1 \iff A$ is a singleton set, $|A|$ is finite if and only if A is a *finite set.* $|A| = \infty$ implies that A is an *infinite set.*

1.3 SUBSETS

If A and B are sets we say A is *contained* in B if every element of A is an element of B. We say A is a *subset* of B and write $A \subseteq B$, or $B \supseteq A$.

1.3.1 Special sets

1. $\emptyset$ represents the set with no elements, that is the *empty set.*
   E.g. $\{x \in \mathbb{Z} \mid x^2 + 1 = 0\} = \emptyset$. Note that $\emptyset \subseteq A$ for all sets A (the empty set $\emptyset$ is a subset of any set A) . Further note that $\{x \in \mathbb{C} \mid x^2 + 1 = 0\} = \{i, -i\} \neq \emptyset$.

2. A set with only one element is called a *singleton set.* E.g. $A = \{\emptyset\}$, $A = \{\ a\}$, or $A = \{x \in \mathbb{R}^+ \mid x^2 - 1 = 0\} = \{1\}$ are singleton sets.

3. The universal set U, the set of all elements in a larger set where all sets under discussion are subsets.

1.4 PROPERTIES OF SETS

The following results hold of sets:

1. If $A \subseteq B$ but $A \neq B$, then A is a *proper subset* of B. That is $A \subset B$. We may also write $A \subsetneqq B$. So A is a subset of itself but **not** a proper subset of itself. The emptyset $\emptyset$ is a proper subset of all non empty sets, but not a proper subset of itself. The empty set is referred to as the *trivial subset* of a non empty set.

2. If A and B are subsets and $A \subseteq B$ and $B \subseteq A$ then $A = B$. Certainly, if $A = B$ then $A \subseteq B$ and $B \subseteq A$. This principle is useful because it produces a method of showing that two sets are the same. That is, to show $A \subseteq B$ we must establish that;
   $\forall x \in A, \quad x \in A \Rightarrow x \in B$. To show $A = B$ we must establish that
   $\forall x, \quad x \in A \iff x \in B$.

1.5 CONSTRUCTING NEW SETS FROM OLD SETS

1. If X is a subset of U then $X' = \{x \in U \mid x \notin X\}$ and is called the *complement* of X in U.

2. If X and Y are subsets of U, then the *union* of X and Y,
   $X \cup Y = \{x \in U \mid x \in X \text{ or } x \in Y\}$.

3. If X and Y are subsets of U, then the *intersection* of X and Y, $X \cap Y = \{x \in U \mid x \in X \text{ and } x \in Y\}$.

4. $X - Y = X \backslash Y = \{x \in U \mid x \in X \text{ and } x \notin Y\}$ is called the *difference between* X and Y.

5. $X \Delta Y = (X - Y) \cup (Y - X)$ is called the *symmetric difference* between X and Y.

6. It is often necessary to form unions and intersections of large classes of sets. Let $\{X_i\}$ be an entirely arbitrary class of sets indexed by a set I of subscripts. Then

$$\bigcup_{i \in I} X_i = \{x \in U \mid x \in X_i \text{ for at least one } \quad i \in I\}$$

and

$$\bigcap_{i \in I} X_i = \{x \in U \mid x \in X_i \text{ for all } \quad i \in I\}.$$

7. For X and Y non-empty sets, $X \times Y = \{(x, y) \mid x \in X, \quad y \in Y\}$ is called the *direct (Cartesian)* product of sets X and Y. This definition of the product of two sets extends easily to the product of n sets, for n any positive integer. If $X_1, X_2, X_3, \cdots, X_n$ are non-empty sets, then their product $X_1 \times X_2 \times X_3 \times \cdots \times X_n$ is the set of all *ordered n-tuples* $(x_1, x_2, x_3, \cdots, x_n)$ where $x_i \in X_i$, for each subscript i.

8. Suppose X is any set. Then the *power set of* X, denoted by $\mathcal{P}(X)$, is the set of all subsets of X. That is: $\mathcal{P}(X) = \{A \mid A \subseteq X\}$. Thus X and $\emptyset$ are in the power set of set X. If X is a finite set with n elements then $|\mathcal{P}(X)| = 2^n$.

9. If X is a non-empty set, a family or collection Σ of subsets of X is a partition of X, with the elements in Σ called cells, if

   (i) no cell $X_i \in \Sigma$ is empty. That is $X_i \neq \emptyset$ for all $X_i \in \Sigma$.

   (ii) the cells are pair-wise disjoint. That is : $X_i \cap X_j = \emptyset$ for all X_i and X_j in the partition Σ.

   (iii) every element of X belongs to some cell. That is: If $x \in X$ then $x \in X_i$ for some $X_i \in \Sigma$. By (ii) above x will belong to exactly one cell in the partition. We can write X as the union of the cells in the partition as follows: $X = \bigcup_{X_i \in \Sigma} X_i$.

1.6 TUTORIAL

(1) In each case describe A in the notation $A = \{x \mid P(x)\}$.

   (a) A is the set of multiples of 5.

   (b) A is the set of all integers between $-\frac{1}{2}$ and $\frac{9}{2}$.

(2) Describe each of the following sets by listing their elements.

   (a) $\{x \in \mathbb{Z}^+ \mid x^2 = 16\}$.

(b) $\{x = 2m + 3 \mid m \in \mathbb{Z}, 1 \leq x \leq 6\}$.

(c) $\{x \in \mathbb{Z} \mid 0 < x < 100\}$.

(d) $\left\{\frac{1}{2n-1} \mid n \in \mathbb{Z}^+\right\}$.

(3) If possible, list the elements in the following sets, and find the order of the sets.

(a) $\{n \in \mathbb{N} \mid n^3 \text{ is odd }\}$.

(b) $\{x \in \mathbb{R} \mid x^3 + 3x^2 - x - 3 = 0\}$.

(c) $\{x \in \mathbb{Q} \mid x^2 = 2\}$.

(d) $\{x \in \mathbb{Z} \mid x^2 \leq 4\}$.

(e) $\{x \in \mathbb{R} \mid |x| \leq 1\}$.

(f) $\{z \in \mathbb{C}| \mid |z| \leq 1\}$.

(4) Let $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3\}$ and $C = \{2, 4\}$. Find all sets X satisfying each pair of conditions.

(a) $X \subseteq B$ and $X \subseteq C$.

(b) $X \subseteq B$ and $X \not\subseteq C$.

(5) (a) Suppose A, B, C are sets such that $A \subseteq B$ and $B \subseteq C$. Explain why $A \subseteq C$.

(b) Suppose that $A \subseteq B$ and $B \subset C$. Explain why $A \subset C$ but $A \neq C$.

Chapter 2

THE INTEGERS

2.1 WELL-ORDERING AXIOM

Every non-empty set of positive integers has a *smallest member*.

2.2 DIVISION ALGORITHM

Let n and $d \geq 1$ be integers. There exists uniquely determined integers q and r such that $n = qd + r$ and $0 \leq r < d$. q and r are called *quotient* and *remainder* respectively.

2.2.1 Definition: divisor

If n and d are integers, d is called a divisor of n if $n = qd$ for some integer q. We write $d \mid n$.

2.2.2 Theorem

Let m, n and d denote integers.

1. $n \mid n \quad \forall n$.
2. If $d \mid m$ and $m \mid n$, then $d \mid n$.
3. If $d \mid n$ and $n \mid d$ then $d = \pm n$.
4. If $d \mid n$ and $d \mid m$ then $d \mid (xn + ym)$ for all integers x and y. We call $xn + ym$ a *linear combination* of m and n.

2.2.3 Definition: greatest common divisor

If m and n are integers, not both zero, an integer d is called the *greatest common divisor* of m and n, written $\gcd(m, n)$ if

(i) $d \geq 1$,

(ii) $d \mid m$ and $d \mid n$,

(iii) if $k \mid m$ and $k \mid n$, then $k \mid d$.

2.2.4 Theorem

Let m and n be integers, not both zero. Then $d = \gcd(m.n)$ exists and $d = xn + ym$ for some integers x and y.

2.3 EUCLIDEAN ALGORITHIM

2.3.1 Examples

1. If $m = qn + r$ show that $\gcd(m, n) = \gcd(n, r)$.
2. Find $\gcd(78, 30)$ and express it as a linear combination of 78 and 30.
3. Find $\gcd(41, 12)$ and express it as a linear combination of 41 and 12.

2.3.2 Note on algorithm

The Euclidean Algorithm procedure works as follows. For integers m and n not both zero, we use the division algorithm repeatedly: $m = q_1 n + r_1, n = q_2 r_1 + r_2, r_1 = q_3 r_2 + r_3, \cdots\cdots$ At each stage we divide the divisor at the previous stage by the remainder, so that the remainders form a decreasing sequence of non-negative integers:

$$n > r_1 > r_2 > r_3 > \cdots \geq 0.$$

Clearly, we must encounter a remainder of 0 (in at most n steps). If r_t denotes the last non-zero remainder, the last two equations are $r_{t-2} = q_t r_{t-1} + r_t$ and $r_{t-1} = q_{t+1} r_t + 0$. Now, repeated applications give; $\gcd(m, n) = \gcd(n, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{t-1}, r_t) = r_t$. Hence $\gcd(m, n)$ is the last non-zero remainder. Moreover we can express $\gcd(m, n) = r_t$ as a linear combination of m and n by eliminating the remainders $r_{t-1}, r_{t-2}, r_{t-3}, \cdots$, successively from these equations.

2.4 RELATIVELY PRIME

2.4.1 Definition: relatively prime

Two integers m and n are called *relatively prime* if $\gcd(m, n) = 1$.

2.4.2 Theorem

Let m and n be integers, not both zero. Then m and n are relatively prime if and only if $1 = xm + yn$ for some integers x and y.

2.4.3 Corollary

If m and n are integers and $\gcd(m, n) = d$, then $\dfrac{m}{d}$ and $\dfrac{n}{d}$ are relatively prime.

2.4.4 Theorem

Let m and n be relatively prime integers.

(i) If $m \mid k$ and $n \mid k$, then $mn \mid k$.

(ii) If $m \mid kn$ for some k, then $m \mid k$.

2.5 PRIME NUMBERS

2.5.1 Definition: prime

An integer p is a *prime number* if

(i) $p \geq 2$ and

(ii) if $d \mid p$ and $d > 0$, then $d = 1$ or $d = p$.

2.5.2 Theorem: Euclid's Lemma

Let p denote a prime.

(i) If $p \mid mn$ where m and n are integers, then $p \mid m$ or $p \mid n$.

(ii) If $p \mid m_1 m_2 m_3 ....m_k$ where each m_i is an integer, then $p \mid m_i$ for some i.

2.5.3 Theorem: Prime Factorisation Theorem

(i) Every integer $n \geq 2$ is the product of one or more primes.

(ii) The factorisation is unique up to the order of the factors. In fact $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, where the p_i are distinct primes $n_i \geq 1$ for all i. Then the positive divisors of n are the integers of the form $d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$, where $0 \leq d_r \leq n_i$ holds for i.

2.5.4 Definition: greatest common divisor, the least common multiple

Let $n_1, n_2, \cdots, n_r$ be positive integers.

(i) The greatest common divisor of these integers, denoted $\gcd(n_1, n_2, \cdots, n_r)$, is the positive common divisor that is a multiple of every common divisor.

(ii) The least common multiple of these integers, denoted by $\operatorname{lcm}(n_1, n_2, \cdots, n_r)$, is the positive common multiple that is a divisor of every common multiple.

2.5.5 Examples

1. Find $\gcd(4, 6, 10)$ and $\operatorname{lcm}(4, 6, 10)$.

2. Find $\gcd(12, 20, 18)$ and $\operatorname{lcm}(12, 20, 18)$.

3. Find $\gcd(63, 60, 245)$ and $\operatorname{lcm}(63, 60, 245)$.

2.5.6 TUTORIAL

1. In each case compute the $\gcd(m, n)$ and express it as a linear combination of m and n.

   (a) $m = 72, \quad n = 42.$

   (b) $m = 327, \quad n = 54.$

   (c) $m = 377, \quad n = 29.$

   (d) $m = 72, \quad n = -175.$

2. If $m \geq 1$, show that $m \mid n$ if and only if $\gcd(m, n) = m$.

3. Let m and n be integers and let $d = \gcd(m, n)$.

   (a) Show that $\dfrac{m}{d}$ and $\dfrac{n}{d}$ are relatively prime.

   (b) If $k \mid d$, show that $\gcd\left(\dfrac{m}{k}, \dfrac{n}{k}\right) = \dfrac{d}{k}$.

4. If $\gcd(m, n) = 1$, and $k \mid m$, show that $\gcd(k, n) = 1$.

5. Show that $\gcd(km, kn) = k \gcd(m, n)$.

6. Suppose p is an integer with the following property: If m and n are integers and $p \mid mn$, either $p \mid m$ or $p \mid n$. Show that p must be a prime.

7. Let p be a prime. If n is an integer, show that either $p \mid n$ or $\gcd(p, n) = 1$.

8. If $\gcd(m, p) = 1$ and p is prime, show that $\gcd(m, p^k) = 1$ for all $k \geq 1$.

9. If $m \geq 1$ and $n \geq 1$ are relatively prime integers and mn is the square of an integer, show that both m and n are squares of integers. Is this result true if $\gcd(m, n) \neq 1$?

Chapter 3

EQUIVALENCE RELATIONS

3.1 EQUIVALENCE RELATIONS

3.1.1 Definition: equivalence relation

A relation $\approx$ on a set A is an *equivalence relation* if it satisfies the following conditions, where a, b, and c denote elements of A:

(i) $a \approx a$ for all a in A. (reflexive property)

(ii) If $a \approx b$ then $b \approx a$. (symmetric property)

(iii) If $a \approx b$ and $b \approx c$ then $a \approx c$. (transitive property)

We say a is *equivalent or congruent* to b if $a \approx b$.
In order to define an equivalence relation we need (1) a SET and (2) a RULE that satisfies the above three conditions (reflexive, symmetric and transitive properties) .

3.1.2 Definition: equivalence class

Let $\approx$ be an equivalence on a set A. Given $a \in A$, the *equivalence class* $[a]$ or $\bar{a}$ of a is defined to be the set of all elements in A that are equivalent to a. That is; $[a] = \{x \in A \mid x \approx a\}$. The equivalence class $[a]$ is said to be *generated* by a.

3.1.3 Examples

1. Equality on any set A. $[a] = \{a\}$ for all $a \in A$.

2. Parallelism on the set of straight lines.

3. If X and Y are subsets of U, a finite set, write $X \approx Y$ if $|X| = |Y|$. $[X]$ consists of all sets with the same number of elements as X.

4. If m and n are integers, write $a \approx b$ if $a-b$ is even. Then there are only two equivalence classes, $[0]$ of all even numbers and $[1]$ of all odd numbers.

5. On $\mathbb{Q}$ define $\approx$ as follows: $\dfrac{a}{b} \approx \dfrac{c}{d}$ if and only if $ad = bc$ where $b, d \neq 0$ and $a, b, c, d \in \mathbb{Z}$. Then the equivalence class of any rational $\dfrac{a}{b}$ is all rational numbers that can be reduced by cancellation of common factors to $\dfrac{a}{b}$.

3.2 PARTITIONS

3.2.1 Theorem

Let $\approx$ be an equivalence on a set A and let a and b be elements in A. Then

1. $a \in [a]$ for every $a \in A$.
2. $[a] = [b]$ if and only if $a \approx b$.
3. If $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$.
4. If $a \in C$, where C is any equivalence class then $C = [a]$. That is, an equivalence class can be named using any of its members.

Hence the family Σ of equivalence classes form a partition of the set A. We may write $A_{\approx} = \Sigma$.

3.2.2 Definition: transversal

Let $A_{\approx} = \Sigma$ be the set of disjoint, distinct equivalence classes of A under $\approx$. Let T be a set consisting of exactly one element from each equivalence class. The set T is called a *Transversal* to A under $\approx$

3.2.3 Exercise

Let $\approx$ be defined on $\mathbb{Z}^+$ by: $x \approx y$ if and only if x and y have the same number of digits. Then $\approx$ be defined on $\mathbb{Z}^+$ is an equivalence relation. Find $\mathbb{Z}^+_{\approx}$ and a transversal for this relation.

3.3 TUTORIAL

1. In each case decide whether the given $\approx$ is an equivalence on A. Give reasons for your answers. If it is an equivalence, describe the equivalence classes.

   (a) $A = \{-2, -1, 0, 1, 2\}$; $\quad a \approx b$ means that $a^3 - a = b^3 - b$.

   (b) $A = \{x \in \mathbb{R} \mid x > 0\}$; $\quad x \approx y$ means $xy = 1$.

   (c) $A = \mathbb{N}$; $\quad a \approx b$ means that $b = ka$ for some integer k.

   (d) $A = \mathbb{R} \times \mathbb{R}$; $(x, y) \approx (x_1, y_1)$ means that $y - 3x = y_1 - 3x_1$.

2. Let $U = \{1, 2, 3\}$ and $A = U \times U$. In each case show that $\approx$ is an equivalence relation on A and find $A_{\approx} = \Sigma$.

(a) $(a, b) \approx (a_1, b_1)$ if $a + b = a_1 + b_1$.

(b) $(a, b) \approx (a_1, b_1)$ if $a = a_1$.

Chapter 4

CONGRUENCES AND THE INTEGERS MODULO n

4.1 CONGRUENCE MODULO n

4.1.1 Definition: congruent modulo n

Let $n \geq 2$ be an integer. Then integers a and b are said to be congruent modulo n if $n \mid (a - b)$. In this case we write $a \equiv b(modn)$ and refer to n as the modulus.

4.1.2 Theorem

Congruence modulo n is an equivalence on $\mathbb{Z}$ the integers. That is:

(i) $a \equiv a \pmod{n}$ for every $a \in \mathbb{Z}$,

(ii) if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$,

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

4.1.3 Definition: residue class

The equivalence class $[a]$ is called the residue class of a modulo n and may also be denoted by $\overline{a}$.

4.1.4 Theorem

Given $n \geq 2$, $[a] = [b]$ if and only if $a \equiv b \pmod{n}$.

4.2 INTEGERS MODULO n

4.2.1 Definition: integer modulo n

The set $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$ of all residue classes modulo n is called the set of integers modulo n, where $\overline{a} = [a]$ for $a = 0, 1, 2, \cdots, n-1$.

4.2.2 Theorem

If $n \geq 2$ and $a \in \mathbb{Z}$, then $[a] = [r]$ or $\overline{a} = \overline{r}$ for some integer r where $0 \leq r < n$. Moreover the residue classes $\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}$ modulo n are distinct; that is $|\mathbb{Z}_n| = n$.

4.2.3 Examples

1. Locate $\overline{48}$ and $\overline{-16}$ in $\mathbb{Z}_7$.
2. If a is an odd integer, show that $\overline{a} = \overline{1}$ or $\overline{a} = \overline{3}$ in $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.
3. In $\mathbb{Z}_n$, show that $\overline{a} = \overline{0}$ if and only if $n \mid a$.
4. Compute in $\mathbb{Z}_6$, $\overline{3} + \overline{5}$ and $\overline{3}.\overline{5}$.

4.2.4 Theorem

Let $n \geq 2$ be a fixed modulus and let a, b and c denote arbitrary integers. Then the following hold in $\mathbb{Z}_n$.

(i) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ and $\overline{a}\overline{b} = \overline{b}\overline{a}$.

(ii) $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$ and $\overline{a}(\overline{b}\overline{c}) = (\overline{a}\overline{b})\overline{c}$.

(iii) $\overline{a} + \overline{0} = \overline{a}$ and $\overline{a}\overline{1} = \overline{a}$.

(iv) $\overline{a} + \overline{-a} = \overline{0}$.

(v) $\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{ac}$.

4.2.5 Examples

1. What is the remainder when 4^{119} is divided by 9?
2. **Casting out Nines.** Show that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

4.2.6 Theorem

Let a and n be integers with $n \geq 2$. Then $\overline{a}$ has an inverse in $\mathbb{Z}_n$ if and only if a and n are relatively prime.

4.2.7 Examples

1. Find the inverse of $\overline{16}$ in $\mathbb{Z}_{35}$ and use it to solve $\overline{16}x = \overline{9}$ in $\mathbb{Z}_{35}$.
2. Find the elements of $\mathbb{Z}_9$ that have inverses.

4.2.8 Theorem

The following are equivalent for $n \geq 2$.

(i) Every element $\overline{a} \neq \overline{0}$ in $\mathbb{Z}_n$ has an inverse.

(ii) If $\overline{ab} = \overline{0}$ in $\mathbb{Z}_n$, then either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.

(iii) n is prime.

4.2.9 Example

Write down the multiplication table for $\mathbb{Z}_5$.

4.2.10 Notation

When working in $\mathbb{Z}_n$, we frequently write the residue class $\overline{a}$ simply as a.

4.3 TUTORIAL

1. Find all integers $k \geq 2$ such that:

   (a) $-3 \equiv 7 \pmod{k}$

   (b) $3 \equiv k^2 \pmod{k}$

   (c) $5 \equiv k \pmod{k^2}$

2. If $a \equiv b \pmod{n}$ and $m \mid n$, show that $a \equiv b \pmod{m}$.

3. Find the remainder when

   (a) 10^{515} divided by 7

   (b) 7^{348} divided by 11.

4. If $p \neq 2, 3$ is prime, show that $\overline{p} = \overline{1}$ or $\overline{p} = \overline{5}$ in $\mathbb{Z}_6$.

5. (a) If $\overline{a}$ and $\overline{b}$ both have inverses in $\mathbb{Z}_n$, show that the same is true for $\overline{ab}$.

   (b) If $\overline{a_1}, \overline{a_2}, \cdots, \overline{a_m}$ have inverses in $\mathbb{Z}_n$, show that the same is true of $\overline{a_1 a_2 \cdots a_m}$.

6. (a) If $\overline{ab} = 0$ in $\mathbb{Z}_n$, and $\gcd(a, n) = 1$, show that $\overline{b} = \overline{0}$.

   (b) Show that $\overline{a}$ is invertible in $\mathbb{Z}_n$ if and only if $\overline{ab} = 0$ implies that $\overline{b} = \overline{0}$.

7. Show that the following conditions on an integer $n \geq 2$ are equivalent.

   (a) $\overline{a}^2 = \overline{0}$ in $\mathbb{Z}_n$, implies that $\overline{a} = \overline{0}$.

   (b) n is square free (that is, a product of distinct primes).

8. Show that the following conditions on an integer $n \geq 2$ are equivalent.

   (a) If $\overline{a}$ is in $\mathbb{Z}_n$, then either $\overline{a}$ is invertible in $\mathbb{Z}_n$ or $\overline{a^k} = \overline{0}$, for some $k \geq 1$.

   (b) n is a power of a prime.

Chapter 5

MAPPINGS (FUNCTIONS) AND BINARY OPERATIONS

5.1 DOMAIN, CODOMAIN, RANGE AND GRAPHS OF MAPPINGS

5.1.1 Definition: Mappings, domain, range, graph

Let A and B be non empty sets.

1. A *mapping* or *function* $\alpha : A \to B$ is a rule that assigns to every element a of A exactly one element $\alpha(a)$ of B. This property is described as the ***well defined*** or ***function*** property of a rule. We will refer to a rule being well defined or a mapping.

2. A is called the domain of the mapping α written $D(\alpha)$.

3. $\alpha(a)$ is called the image of element a.

4. $\alpha(A) = \{\alpha(a)|a \in A\} = Im(\alpha)$ is called the *range* or *image* of mapping α. $Im(\alpha)$ is a subset of B.

5. Graph of G is $G(\alpha) = \{(a,b)|a \in A, b \in B \text{ and } b \in \alpha(a)\} = \{(a, \alpha(a))|a \in A\}$.

6. If $A = S \times S$ and $B = S$ then the mapping is a binary operation on S.

The process of defining or creating a (well defined) mapping α consist of two parts.

(i) Specifying the *domain* A and the *co-domain* B of α.

(ii) Specifying *exactly one* element $\alpha(a)$ for each a in A.

That is, we must specify the *domain*, the *co-domain* and the *well defined action.*

Note that when we say there is a mapping we will assume it describes a well defined action. If we are defining a rule we need to prove that we have a well defined action to call it a function or mapping.

In algebra we usually use Greek lower case letters, $\alpha, \beta, \cdots, \theta, \eta$ to represent mappings (functions) that are usually just called maps or mappings. That is $\alpha : A \to B$ is a mapping with domain A and co-domain B.

5.1.2 Examples

1. $\alpha : \mathbb{Z} \to \mathbb{Z}$ defined by $\alpha(x) = 2x$ for integer x.

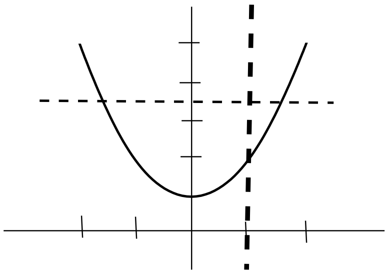
2. $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(x) = x^2$ for all x in $\mathbb{R}$.

3. Let T be the non empty set of real numbers and let $S = T \times T$. Define $\alpha : S \to T$ by $\alpha(t_1, t_2) = t_1$. This mapping is called the *projection* of $T \times T$ onto its first component. This is a binary operation.

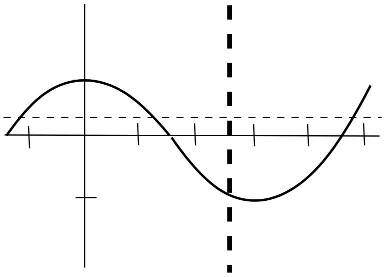
4. Let T be the non empty set of real numbers and let $S = T \times T$. Define $\alpha : S \to T$ by $\alpha(t_1, t_2) = t_1 + t_2$. Similarly define $\alpha : S \to T$ by $\alpha(t_1, t_2) = t_1 t_2$. Both these mappings are binary operations.

5.1.3 Test for a mapping or a function

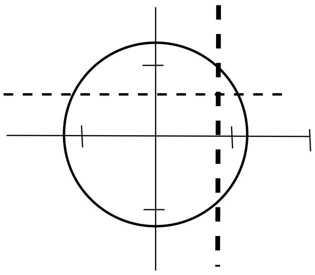
Let a, $b \in A$. We need to prove that if $a = b$ then $\alpha(a) = \alpha(b)$. This is the *algebraic process* equivalent to the vertical line test in the plane $\mathbb{R}^2$. This geometric test is useful for finding counter examples when α is not a function and $D(\alpha) = \mathbb{R}$ and $Im(\alpha) = \mathbb{R}$.



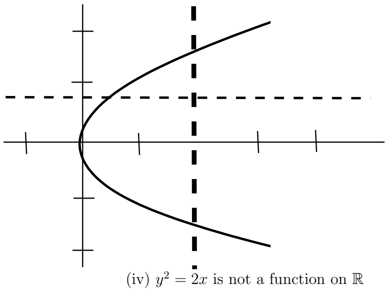
(i) $\alpha(x) = x^2 + 1$ is a function on $\mathbb{R}$



(ii) $\alpha(x) = \cos x$ is a function on $\mathbb{R}$



(iii) $\alpha(x) = \pm\sqrt{1 - x^2}$ is not a function on $\mathbb{R}$



(iv) $y^2 = 2x$ is not a function on $\mathbb{R}$

5.2 PROPERTIES OF MAPPINGS - COMPOSITIONS AND BIJECTIONS

5.2.1 Definition

1. $\alpha : A \to B$ and $\beta : A \to B$ are *equal* if and only if $\alpha(a) = \beta(a)$ **for each** $a \in A$.

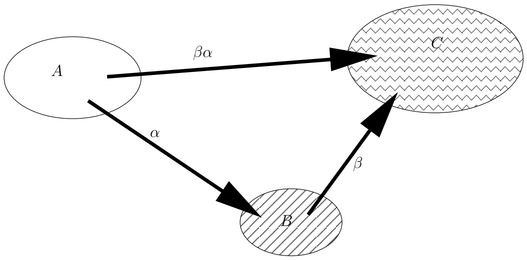
2. $\alpha : A \to B$ is called the *identity mapping* if $\alpha(a) = a$ for each a in A and is denoted by 1_A. Obviously $A \subseteq B$ in this case.

3. $\alpha : A \to B$ is said to be *injective* or *one-to one* if $\alpha(a) = \alpha(b)$ implies that $a = b$. To algebraically show that α is a one-to-one mapping or injective: Let $\alpha(a) = \alpha(b)$ and prove that $a = b$. That is $\alpha(a) = \alpha(b) \Rightarrow a = b$. This *algebraic process* is equivalent to the *horizontal line test* in the plane $\mathbb{R}^2$. The geometric test is useful in finding counter examples when a mapping is not one-to-one and $D(\alpha) = \mathbb{R}$ and $Im(\alpha) = \mathbb{R}$.

4. $\alpha : A \to B$ is *onto* or *surjective* if for each $b \in B$ we can find $a \in A$ such that $\alpha(a) = b$. That is $B = Im(\alpha)$. Algebraically, show that for each (any) $b \in B$, $\exists a \in A$ such that $\alpha(a) = b$.

5. A map that is both injective and surjective is called a *bijection.*

6. Given $\alpha : A \to B$ and $\beta : B \to C$, then the *composition mapping* $\beta\alpha : A \to C$ is defined by $\beta\alpha(a) = \beta(\alpha(a))$ for all $a \in A$.



7. Associative property hold for composition of maps: That is $\alpha(\beta\delta) = (\alpha\beta)\delta$.

8. If $\alpha : A \to B$ is a mapping , a mapping $\beta : B \to A$ is called *inverse* of α if $\beta\alpha = 1_A$ and $\alpha\beta = 1_B$. We say the mapping α is *invertible.* We note that $\boxed{\beta(b) = a \text{ if and only if } \alpha(a) = b.}$ We show that if such a mapping β exists it is *unique* and we can write it as α^{-1}.

9. If there exists a bijection from set A onto set B , we say A and B are in *one-to-one correspondence* or are *numerically equivalent.*

5.2.2 Examples

1. Equality
   $\alpha(x) = x^2 + x + 1$ and $\beta(x) = (x-1)(x+2) + 3$ are equal mappings.

2. Injective mappings

   (i) $\alpha : \mathbb{N} \to \mathbb{N}$ defined by $\alpha(n) = 2n + 1$ is one-to-one since if $2n + 1 = 2m + 1$ then $n = m$.

   (ii) $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(n) = n^2 + 1$ for all $n \in \mathbb{R}$ is not one-to-one since we see:

   $$\alpha(n) = \alpha(m) \Rightarrow n^2 + 1 = m^2 + 1 \Rightarrow n^2 = m^2 \Rightarrow n = \pm m.$$

   It would be one to one if the domain and co domain were $\mathbb{N}$.

   (iii) $\alpha : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ with $\alpha(a, b) = ab$ is not injective as as $\alpha(2, 3) = 6$ and $\alpha(1, 6) = 6$ but $(2, 3) \neq (1, 6)$.

3. Surjective mappings

   (i) $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(x) = 2x - 5$ is onto since
   $y = 2x - 5 \Rightarrow x = \dfrac{y+5}{2} \in \mathbb{R}$.

   (ii) $\alpha : \mathbb{N} \to \mathbb{N}$ defined by $\alpha(n) = 2n + 1$ is not onto since no even integer is in $Im(\alpha)$.

   (iii) $\alpha : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ with $\alpha(a, b) = ab$ is surjective as $x \in \mathbb{R} \Rightarrow x = \alpha(x, 1)$ where $(x, 1) \in \mathbb{R} \times \mathbb{R}$.

4. Bijections

   (i) The identity map $1_A : A \to A$ is a bijection.

   (ii) $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(x) = 2x - 5$ is both one-to-one and onto.

   (iii) $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(x) = \sin x$ is not a bijection since is not a bijection since it is not one-to-one or onto R.

   (iv) $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(x) = \tan x$ is not a bijection since it is not one-to-one but is onto .

   (v) $\alpha : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ with $\alpha(a, b) = ab$ is not a bijection since it is not injective.

5. Numerically equivalent
   $\alpha : A \to B$ is a bijection and if A and B are both finite, then $|A| = |B|$.

6. Composition

   (i) If $\alpha : A \to A$ and $1_A : A \to A$ then $\alpha 1_A = 1_A \alpha$. If $\alpha : A \to B$ then $1_B \alpha = \alpha$ and $\alpha 1_A = \alpha$ where $1_B : B \to B$.

   (ii) $\alpha : \mathbb{R} \to \mathbb{R}$ and $\beta : \mathbb{R} \to \mathbb{R}$ be defined by $\alpha(x) = x + 1$ and $\beta(x) = x^2$ for all x in $\mathbb{R}$. $\beta\alpha : \mathbb{R} \to \mathbb{R}$ and $\beta\alpha(x) = \beta(x + 1 = (x + 1)^2$ while $\alpha\beta : \mathbb{R} \to \mathbb{R}$ and $\alpha\beta(x) = \alpha(x^2) = x^2 + 1$ so $\beta\alpha \neq \alpha\beta$.

5.3 PROPERTIES OF THE INVERSES OF MAPPINGS

5.3.1 Theorem

Let $\alpha : A \to B$ and $\beta : B \to C$ denote mappings

(i) $1_A : A \to A$ is invertible and $(1_A)^{-1} = 1_A$

(ii) If α is invertible, then α^{-1} is unique and is invertible with $(\alpha^{-1})^{-1} = \alpha$

(iii) If α and β are both invertible, then $\beta\alpha$ is invertible and $(\beta\alpha)^{-1} = \alpha^{-1}\beta^{-1}$.

5.3.2 Theorem: Invertibility Theorem

A mapping $\alpha : A \to B$ is invertible if and only if it is a bijection. Thus if $\alpha : A \to B$ is a bijection then α^{-1} exists as a mapping from B to A and this inverse is unique. Further if a mapping is invertible then it is a bijection.

5.4 TUTORIAL

1. In each case determine whether α is a mapping (it has a well defined action).

   (a) $\alpha : \mathbb{N} \to \mathbb{N}$ defined by $\alpha(n) = -n$ for all $n \in \mathbb{N}$.

   (b) $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(x) = \sqrt{x}$ for all $x \in \mathbb{R}$.

   (c) $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(xy) = (x, y)$ for all x and y in $\mathbb{R}$.

2. In each case state whether the mapping is onto (surjective), one-to-one (injective), and/or bijective. Justify your answers.

   (a) $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(x) = 3 - 4x$.

   (b) $\alpha : \mathbb{N} \to \mathbb{N}$ defined by $\alpha(n) = \begin{cases} \frac{n+1}{2} & \text{if } n \text{ is odd} \\ \frac{n}{2} & \text{if } n \text{ is even} \end{cases}$.

   (c) $\alpha : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ defined by $\alpha(x) = (x + 1, x - 1)$.

   (d) $\alpha : A \to A \times B$ defined by $\alpha(a) = (a, b_0)$ where $b_0 \in B$ is fixed and $A \neq \emptyset$.

3. Let $A \overset{\alpha}{\to} B \overset{\beta}{\to} C$ be mappings.

   (a) If $\beta\alpha$ is onto, show that β is onto.

   (b) If $\beta\alpha$ is one-to-one and α is onto, show that β is one-to-one.

   (c) If $\beta\alpha$ is onto and β is one-to one, show that α is onto.

4. (a) For $\alpha : A \to A$, show that $\alpha^2 = \alpha$ if and only if $\alpha(x) = x$ for all $x \in \alpha(A)$.

   (b) If $\alpha : A \to A$ with $\alpha^2 = \alpha$, then show α is onto if and only if α is one-to-one.

5. In each case verify that α^{-1} exists and describe its action.

   (a) $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(x) = ax + b$, where $0 \neq a \in \mathbb{R}$ and $b \in \mathbb{R}$.

(b) $\alpha : A \times B \to B \times A$ defined by $\alpha(a,b) = (b,a)$.

6. Let $A \overset{\alpha}{\to} B \overset{\beta}{\to} C$ satisfy $\beta\alpha = 1_A$. If either α is onto or β is one-to-one, show that each is invertible and that each is the inverse of the other.

7. Let $A \overset{\alpha}{\to} B \overset{\beta}{\to} C$ satisfy $\beta\alpha = 1_A$. If A and B are finite sets with $|A| = |B|$, show that $\alpha\beta = 1_B$, $\alpha = \beta^{-1}$ and $\beta = \alpha^{-1}$. (Compare your answer to the solution in Ex above.)

Chapter 6

THE GROUP CONCEPT

The notion of a *Group* is one of the most unifying ideas in mathematics. It draws together a wide variety of mathematical objects for which a notion of combination or product exists.

6.1 GROUPS

6.1.1 Definition: group

Formally, a *group* G is defined to be a *set* with an *associative binary operation* $\star$, called *product* that is *closed;* a specific *unique* element, called *identity* (*neutral element* or *unity*) and written e (or 1) ; and with the property that for each g in G there is an element called the *inverse* of g and written $g.^{-1}$. We write $\langle G, \star \rangle$ as the group. That is, written mathematically we have: $\langle G, \star \rangle$ is a group if for all g, g_1, g_2, g_3 in G,

1. $g_1 \star g_2 \in G$, **Closed**
2. $g_1 \star (g_2 \star g_3) = (g_1 \star g_2) \star g_3$ **Associatve**
3. $g \star e = e \star g = g$ **Identity**
4. $g^{-1} \star g = g \star g^{-1} = e$ **iNverses**

6.1.2 Definition: abelian

A group G is *Abelian* or *Commutative* if $a \star b = b \star a$ for each $a, b \in G$. (A B E L) **Note that the C in CAIN does not stand for commutative.**

6.2 BINARY OPERATIONS $\star$: MAPS FROM $S \times S$ to S

6.2.1 Definition: binary operation $\star$

A *binary operation* $\star$ on set S is a *mapping* (function) that assigns to each *ordered pair* (a, b) of elements of S (or $(a, b) \in S \times S$) some *unique* element of S.

That is $\star : S \times S \to S$ and is a mapping or function. We write $a \star b$ for $\star(a, b)$ or just ab. The definition of a mapping was completely explored in Chapter 5.

6.2.2 commutative, associative and distributive binary maps

Suppose a binary operation $\star$ is defined on a set S.

1. If the domain of $\star$ is $S \times S$ and the co-domain of $\star$ is S, we say that S is *closed* under the operation $\star$.

2. The operation must be a function. That is if $(a,b) = (a',b')$ then $a \star b = a' \star b'$. This is a mathematical way of saying that there is a *unique* element $ab \in S$ associated with the ordered pair $(a,b) \in S \times S$.

3. In general in a group $a \star b \neq b \star a$. That is the binary operation is not necessarily commutative. The operation is *commutative* if $a \star b = b \star a$ for all $a, b \in S$.

4. The operation is *associative* if $(a \star b) \star c = a \star (b \star c)$ for $a, b, c \in S$. All groups have an associative binary operation.

5. An element e in S is called the *Unity, Neutral element* or *Identity* for the operation $\star$ if $a \star e = e \star a = a$ for all a in S. All groups have a unique identity.

6. An element a in S is said to be a *Unit* in S or is *Invertible* in S under $\star$ if we can find an *inverse* for a in S. That is, there is $b \in S$ such that $a \star b = b \star a = e$, where e is unity in S. In a group all elements are invertible and hence are units.

6.2.3 Examples

1. If $\star$ is ordinary addition on $\mathbb{Z}$, $\mathbb{R}$ or $\mathbb{C}$ then unity $e = 0$. Thus $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{C}, + \rangle$ are abelian groups.

2. If $\star$ is ordinary multiplication on $\mathbb{Z}$, $\mathbb{R}$ or $\mathbb{C}$ then unity $e = 1.$. But the units of $\mathbb{Z}$ under multiplication are 1 and -1. While $\mathbb{Z}$, $\mathbb{R}$ or $\mathbb{C}$ are not groups under multiplication, $\mathbb{R} \backslash \{0\}$ and $\mathbb{C} \backslash \{0\}$ are groups under multiplication. BUT $\mathbb{Z} \backslash \{0\}$ is *not* a group under multiplication.

3. In $\mathcal{P}(U) = \{X \mid X \subseteq U\}$, $\emptyset$ the empty set is unity under Δ, the symmetric difference. Under intersection $\cap$, unity is the whole set U.

4. In $\mathcal{P}(U) = \{X \mid X \subseteq U\}$ under Δ, each element is its own inverse. The elements in $\mathcal{P}(U)$ do not have inverses under intersection, $\cap$.

5. Let $M = \{f : X \to X \mid f \text{ is a mapping}\}$. Then M is closed under the composition of mappings. This example can only be explored after careful consideration of mappings.

6. Symmetries (isometries of the plane) of figures such as isosceles triangles, squares and regular polygons form groups.

7. The set $M_n(\mathbb{R})$ or $M_n(\mathbb{C})$ of $n \times n$ matrices over the reals $\mathbb{R}$ or the complex numbers $\mathbb{C}$ are closed under both *addition* and *multiplication*, but are not groups under multiplication.

6.3 GROUP PROPERTIES

6.3.1 Proposition

Let G be a group. Then

1. If e is unity then $e^{-1} = e$.
2. If $a \in G$ then the inverse of a is unique. We write this unique element as a^{-1}. Further we have that $(a^{-1})^{-1} = a$.
3. If a and b are in G then so is $a \star b$ and $(a \star b)^{-1} = b^{-1} \star a^{-1}$.
4. If $a_1, a_2, \cdots, a_n$ are units so is $a_1 \star a_2 \star \cdots \star a_n$ and $(a_1 \star a_2 \star \cdots \star a_n)^{-1} = a_n^{-1} \star \cdots \star a_2^{-1} \star a_1^{-1}$.
5. If a is a unit so is a^n for any $n \in \mathbb{Z}$ where $a^0 = e$, and $(a^{-1})^n = (a^{-1})^n$.

6.3.2 Notation

1. We usually write $\star$ as a multiplicative operation, and write $a \star b$ as just ab. Similarly we may denote e by 1 if the underlying binary operation is multiplicative and the inverse of a by a^{-1} and $a \star a \star a \star \cdots \star a = aaa \cdots a = a^n$ for a multiplied by itself n times for $n \in \mathbb{Z}^+$ and $a^r \star a^s = a^{r+s}$ for any integers r and s.
2. If the operation $\star$ is addition $+$, then $e = 0$ and $a^{-1} = -a$ and $a \star a \star a \star \cdots \star a = a + a + a + \cdots + a = na$ for a added to itself n times for $n \in \mathbb{Z}^+$.

6.3.3 Proposition: cancellation laws

Let g, h and f be in group G, then

(i) If $gh = gf$, then $h = f$.

(ii) If $hg = fg$, then $h = f$.

6.3.4 Proposition

Let h and g be in G then

(i) The equation $gx = h$ has a unique solution $x = g^{-1}h$ in G.

(ii) The equation $xg = h$ has a unique solution $x = hg^{-1}$.

6.3.5 Definition: subgroup

A non-empty subset H of G is a *subgroup* of G, if H itself forms a group under the same operation as G. We may write $H \leq G$. Each group has two subgroups. $H = \{e\}$, called the *trivial subgroup* and $H = G$ called the *improper subgroup*. Other subgroups are called *proper subgroups* of G. Here we write $H < G$.

6.3.6 Theorem

Let H be a non empty subset of G. Then H is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$.

6.3.7 Definition: order

The *order* or *cardinality* of a group written $|G|$, is the number of elements in G. The *order* of an element g in G is the smallest positive integer n such that $g^n = e$. The order may be finite of infinite.

6.4 CAYLEY TABLES

Small finite groups can be displayed on a Cayley Table or a Multiplication Table. If $M = \{e, a, b, c\}$, consider the binary operation shown in the Cayley Table below. The elements of M appear across the top of the table and down the left of the table in the same order.

M	e	a	b	c
e	e	a	b	c
a	a	a	b	e
b	b	b	c	c
c	c	e	c	e

In the first table we can see that

- e is the unity in the set since the first row and column of the table repeat the elements of M in their order.
- The binary operation is commutative seen by the symmetry of the table.
- The binary operation is not associative $(ab)c = bc = c$ but $a(bc) = ac = e$.
- Thus this set M is not a group.

M	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

In the second table we can see that

- M is an abelian group.

M	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

In the third table we can see that

- M is an abelian group.

To check if the set presented in the Cayley table is a group:

1. The body of the table must contain ONLY the listed elements and each element of the set must appear exactly once in each row and column. This indicates that the binary operation is *closed.*
2. There must be exactly one row and exactly one column in the table that are the same as the leading row and column. This will tell you which element is the *unity element.*
3. Unity must appear exactly once in each row and column linking an element to its *inverse.*
4. The table symmetrical about the main diagonal signifies an *abelian structure.*

6.5 TUTORIAL

1. In each case, a binary operation $\star$ is given on a set M. Decide whether it is closed, commutative, associative, whether a unity exists, and find the units (if there is unity).

   (a) $M = \mathbb{Z}, a \star b = a - b$.

   (b) $M = \mathbb{R}, a \star b = a + b - ab$.

   (c) $M = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ and $(x, y, z) \star (x', y', z') = (xx', xy' + yz', zz')$.

2. We call a set M which has an associative binary operation and a unity a *Monoid.*

   (i) If u is invertible in monoid M, show that $au = bu$ in M implies that $a = b$.

   (ii) If M is a finite monoid and $au = bu$ in M implies that $a = b$, show that u is invertible in M.

3. Let u and v be invertible in the monoid M.

   (i) If $u^{-1} = v^{-1}$, show that $u = v$.

   (ii) If $a \in M$ and $ua = au$, show that $u^{-1}a = au^{-1}$.

(iii) If $uv = vu$, show that $u^{-1}v^{-1} = v^{-1}u^{-1}$.

4. Show that $\langle \mathbb{R} \backslash \{1\}, \star \rangle$ is a group where $a \star b = ab + a + b$. . Explain why $\langle \mathbb{R}, \star \rangle$ is not a group.

5. Let G be a group and let $g, h, k \in G$.

   (i) Show that if $ghg = gkg$ then $h = k$.

   (ii) Give an example or explain why it is not always true that if $hgh = kgk$ then $h = k$.

6. Let G be the set of all ordered pairs (a, b) where a and $b \neq 0$ are real numbers. Define $\bigoplus$ on G as:

$$(a_1, b_1) \bigoplus (a_2, b_2) = (a_1 + b_1 a_2, b_1 b_2).$$

   (i) Compute $(2, -1) \bigoplus (3, 1)$; $(2, -1) \bigoplus (2, -1)$; $(1, 2) \bigoplus \left(\frac{-1}{4}, \frac{1}{2} \right)$.

   (ii) Show that G is a group under $\bigoplus$. Is G abelian?

7. Let G be the set of all ordered pairs (a, b) where a is a non zero real number and $b = \pm 1$. Define $\bigotimes$ on G as:

$$(a_1, b_1) \bigotimes (a_2, b_2) = \left(a_1 a_2^{b_1}, b_1 b_2 \right).$$

   (i) Compute $(2, -1) \bigotimes (3, 1)$; $(2, -1) \bigotimes (2, -1)$; $(1, 2) \bigotimes \left(\frac{-1}{4}, \frac{1}{2} \right)$.

   (ii) Show that G is a group under $\bigotimes$. Is G abelian?

   (iii) Which elements of G are their own inverses?

8. Let G be a group such that every element is it own inverse. What is $(ab)^{-1}$? Show that G is an abelian group.

Chapter 7

GROUPS OF PERMUTATIONS

7.1 PERMUTATIONS

7.1.1 Definition: permutation

If X is a nonempty set, a *permutation* of X is a bijection $\alpha : X \to X$. That is, a permutation is a *one-to-one* function from X onto X.

7.2 SYMMETRY GROUPS

7.2.1 Definition: symmetric group

If X is a non-empty set, the *symmetric group* on X, denoted by S_X, is the set of all permutations on X under the operation of composition of mappings. If $|X| = n$ then we may write $S_X = S_n$.

7.2.2 Example

Let $X = \{1, 2, 3\}$.
$S_X = \{\alpha | \alpha : X \to X \text{ a bijection}\} = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$

$$\alpha_1 : 1 \to 1; 2 \to 2; 3 \to 3. \quad \alpha_2 : 1 \to 2; 2 \to 3; 3 \to 1. \quad \alpha_3 : 1 \to 3; 2 \to 1; 3 \to 2. \text{Rotations}$$

$$\alpha_4 : 1 \to 1; 2 \to 3; 3 \to 2. \quad \alpha_5 : 1 \to 2; 2 \to 1; 3 \to 3. \quad \alpha_6 : 1 \to 3; 2 \to 2; 3 \to 1. \text{Reflections}$$

We note that if we call $\alpha_1 = e$, the *unity mapping* or the *identity permutation,* and denote $\alpha_2 = \rho$ and $\alpha_4 = R$ then the following relationships hold.

$$\boxed{\rho^2 R = R\rho; \qquad \rho^3 = e; \qquad R^2 = e.}$$

In fact $S_X = S_3$ and S_3 can be represented as $\{e, \rho, \rho^2, R, \rho R, \rho^2 R\}$ and the multiplication or Cayley table is as follows:

Each element is a unit with $e^{-1} = e$, $\rho^{-1} = \rho^2$, $(\rho^2)^{-1} = \rho$, $R^{-1} = R$, $(\rho R)^{-1} = \rho R$, $(\rho^2 R)^{-1} = \rho^2 R$. We also note that the operation is associative but not commutative, since $\rho R \neq R\rho$. Let $H = \{e, R\}$, $K = \{e, \rho, \rho^2\}$, and $J = \{e, \rho R\}$. These sets are also closed under composition of mappings with tables as follows.

0	e	ρ	ρ^2	R	ρR	$\rho^2 R$
e	e	ρ	ρ^2	R	ρR	$\rho^2 R$
ρ	ρ	ρ^2	e	ρR	$\rho^2 R$	R
ρ^2	ρ^2	e	ρ	$\rho^2 R$	R	ρR
R	R	$\rho^2 R$	ρR	e	ρ^2	ρ
ρR	ρR	R	$\rho^2 R$	ρ	e	ρ^2
$\rho^2 R$	$\rho^2 R$	ρR	R	ρ^2	ρ	e

H	e	R
e	e	R
R	R	e

K	e	ρ	ρ^2
e	e	ρ	ρ^2
ρ	ρ	ρ^2	e
ρ^2	ρ^2	e	ρ

J	e	ρR
e	e	ρR
ρR	ρR	e

7.2.3 Note

1. We introduce a notation for the display of a permutation.
   Say $X = \{1, 2, 3, \cdots, n\}$ and $\alpha : X \to X$ is a permutation. Then
   $\alpha : \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$. In the above example we will then be able to write:
   $\rho R = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. The product $\rho(\rho R) = \rho^2 R = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ can be seen as a movement $1 \to 2$ and then $2 \to 3$ using ρR and then ρ. $\rho R \rho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.
   Here we use ρ first and then ρR.

2. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ be in S_4.
   Then $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$.

3. We can use this notation to write down the inverse of each element.
   Say $\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$ then $\delta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 3 & 4 & 5 \end{pmatrix}$ by reading from the second line of the array δ to the first.

4. S_n is called the *symmetric group of* n *elements* or degree n. We note that $|S_n| = n!$. That is $|S_3| = 6 = 3!$ the number of permutations of three objects taken three at a time. Similarly $|S_4| = 4! = 24$.

7.3 FIXED AND MOVED ELEMENTS

7.3.1 Definition: fixed, moved, disjoint

Let $X = \{1, 2, 3, \cdots, n\}$ and $\alpha \in S_n$.

1. An element $k \in X$ is *fixed* by α if $\alpha(k) = k$. We may just write αk for $\alpha(k)$.
2. If $\alpha(k) \neq k$ then we say that k is *moved* by α.
3. Two permutations α and β are *disjoint* if no element of X is moved by both α and β. That is the set of elements moved by α is disjoint from the set of elements moved by β.

7.3.2 Examples

1. $e \in S_n$ is the only permutation that fixes all the elements while $\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$ fixes none of the elements. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ fixes 1 and 4.
2. Let $\sigma \in S_n$. On $X = \{1, 2, 3, \cdots, n\}$ define the equivalence $a \equiv b$ if $b = \sigma^r(a)$ for some $r \in \mathbb{Z}$. We assume that $\sigma^0 = e$. The equivalence class of $a = [a] = \{\sigma^r(a) | r \in \mathbb{Z}\}$. This is called the *orbit* of a under σ. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$ then $\sigma(1) = 3$, $\sigma^2(1) = \sigma(3) = 4$, $\sigma^3(1) = \sigma(4) = 5$, $\sigma^4(1) = \sigma(5) = 6$, $\sigma^5(1) = \sigma(6) = 2$, $\sigma^6(1) = \sigma(2) = 1$. Therefore the orbit of $1 = [1] = \{1, 2, 3, 4, 5, 6\}$. We in fact see a *cycle* being produced. That is $(1 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 2 \rightarrow 1)$ or more briefly $(1 \quad 3 \quad 4 \quad 5 \quad 6 \quad 2)$.
3. In S_5 let $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$. On $X = \{1, 2, 3, \cdots, n\}$ define the equivalence $a \equiv b$ if $b = \tau^r(a)$ for some $r \in \mathbb{Z}$. $\tau(1) = 3$, $\tau^2(1) = \tau(3) = 5$, $\tau^3(1) = \tau(5) = 1$. So $[1] = \{1, 3, 5\}$ forming the cycle $(1 \quad 3 \quad 5)$. $[2] = \{2\}$ and $[4] = \{4\}$.

7.4 CYCLE DECOMPOSITION

7.4.1 Definition: cycles, length of cycles

Let $X = \{1, 2, 3, \cdots, n\}$ and let $k_1, k_2, \cdots, k_r$ be distinct elements in X.

1. Then the *Cycle* $\sigma = (k_1 \quad k_2 \quad \cdots \quad k_r)$ is the permutation in S_n defined by $\sigma(k_i) = k_{i+1}$ if $1 \leq i \leq r - 1$, $\sigma(k_r) = k_1$ and $\sigma(k) = k$ if $k \notin \{k_1, k_2, \cdots, k_r\}$.
2. We say that σ has length r and refer to σ as an r-cycle. In example 2 above σ is a 6-cycle, while in example 3 , τ is a 3-cycle.

7.4.2 Lemma

Let $M_\sigma = \{x \in X | \sigma(x) \neq x\}$. So if x in X is moved by σ, then σx is also moved by σ. So if $x \in M_\sigma$ then $\sigma x \in M_\sigma$.

7.4.3 Theorem

If σ and τ in S_n are disjoint, then $\sigma\tau = \tau\sigma$.

7.4.4 Cycle representation and multiplication

1. The permutation $\sigma = (1 \quad 4 \quad 2 \quad 3)$ in S_4 can be written in other ways using cycle notation. $\sigma = (1 \quad 4 \quad 2 \quad 3) = (4 \quad 2 \quad 3 \quad 1) = (2 \quad 3 \quad 1 \quad 4) = (3 \quad 1 \quad 4 \quad 2)$.

2. Given $\sigma = (1 \quad 2 \quad 4)$ in S_4 will fix 3, while in S_5 will fix 3 and 5.

3. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 10 & 4 & 2 & 5 & 9 & 8 \end{pmatrix}$. We see 4 different equivalence classes or orbits under the relation $a \equiv b$, if $b = \sigma^r(a)$ for some $r \in \mathbb{Z}$. on the set
   $X = \{1, 2, 3, \cdots, 10\}$. $[1] = \{1, 3, 7, 2\}$ producing the cycle $(1 \quad 3 \quad 7 \quad 2) : [4] = \{4, 6\}$ with cycle $(4 \quad 6)$; $[5] = \{5, 10, 8\}$ making cycle $(5 \quad 10 \quad 8)$ and $[9] = \{9\}$ and the trivial cycle (9). Being equivalence classes the sets are disjoint and hence they produce disjoint cycles (permutations).
   So $\sigma = (1 \quad 3 \quad 7 \quad 2)(5 \quad 10 \quad 8)(4 \quad 6)(9)$ or just $(1 \quad 3 \quad 7 \quad 2)(5 \quad 10 \quad 8)(4 \quad 6)$.

4. We see that if permutations σ and τ are disjoint then they commute. That $\sigma\tau = \tau\sigma$. In fact if σ is an m-cycle and τ is an n-cycle and σ and τ are disjoint then the order of the products $\sigma\tau$ or $\tau\sigma$ is nm.

5. If cycles σ and τ are not disjoint then their product can be written as a product of disjoint cycles.
   Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} = (1 \quad 3 \quad 5 \quad 2)$
   and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} = (2 \quad 3 \quad 5 \quad 4)$
   then $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} = (1 \quad 3 \quad 2 \quad 5 \quad 4)$.
   We can multiply the cycles directly according to the rule of always beginning at the extreme right and moving back till the end of the given product. That is: $(1 \quad 3 \quad 5 \quad 2)(2 \quad 3 \quad 5 \quad 4) = (1 \quad 3 \quad 2 \quad 5 \quad 4)$.

7.4.5 Theorem

If σ is an r-cycle, then σ^{-1} is also an r-cycle. In fact if $\sigma = (k_1 \quad k_2 \quad \cdots \quad k_r)$ then $\sigma^{-1} = (k_r \quad k_{r-1} \quad \cdots \quad k_1)$.

7.4.6 Theorem: Cycle Decomposition Theorem

If $\sigma \neq e$ is in S_n, then σ is the product of one or more disjoint cycles of length at least 2. It can be proved that this factorisation is unique up to the order of the factors.

7.4.7 Example

List the elements of S_4, each factorises into disjoint cycles. There are $4! = 24$
e; $(1 \quad 2)$; $(1 \quad 2 \quad 3)$; $(1 \quad 3 \quad 2)$; $(1 \quad 2)(3 \quad 4)$; $(1 \quad 2 \quad 3 \quad 4)(1 \quad 3)$;
$(1 \quad 2 \quad 4)$; $(1 \quad 4 \quad 2)$; $(1 \quad 3)(2 \quad 4)$; $(1 \quad 2 \quad 4 \quad 3)$ etc.
These are the types of decomposition.

7.5 CYCLIC STRUCTURE

7.5.1 Definition: cyclic structure

We note that the permutations can be classified according to following notion. Two permutations have the same *cyclic structure* if, when they are factored into disjoint cycles, they have the same number of cycles of each length.

7.5.2 Definition: transposition

A cycle of length 2 is called a transposition.

7.5.3 Note

(i) If δ is a transposition, then $\delta = (m \quad n)$ for m, n in X. Certainly $\delta^2 = e$ and so $\delta^{-1} = \delta$

(ii) Let $\sigma = (1 \quad 2)(3 \quad 4)$. $\sigma^2 = e$ and so $\sigma^{-1} = \sigma$, but σ is not a transposition.

(iii) We can write $(1 \quad 2 \quad 3 \quad 4 \quad 5)$ as the product of transpositions.

$$(1 \quad 2 \quad 3 \quad 4 \quad 5) = (1 \quad 5)(1 \quad 4)(1 \quad 3)(1 \quad 2).$$

That is $1 \to 2$; $2 \to 1 \to 3$; $3 \to 1 \to 4$; $4 \to 1 \to 5$; $5 \to 1$.
We always move from the right transposition to the left, looking for an appearance of the digit. If it does not occur then we have found the final destination.

7.5.4 Theorem

Every cycle of length $r > 1$ is a product of $r - 1$ transpositions.
In fact $(k_1 \quad k_2 \quad \cdots \quad k_{r-1} \quad k_r) = (k_1 \quad k_r)(k_1 \quad k_{r-1}) \quad \cdots \quad (k_1 \quad k_3)(k_1 \quad k_2)$.

7.5.5 Lemma

Let $\gamma_1 \neq \gamma_2$ be transpositions. If γ_1 moves k, transpositions δ_1 and λ_2 exist such that $\gamma_2\gamma_1 = \lambda_2\delta_1$, where δ_1 fixes k and λ_2 moves k.

7.5.6 Lemma

If the identity permutation e can be written as a product of $n \geq 3$ transpositions, then it can be written as a product of $n - 2$ transpositions.

7.5.7 Theorem: Parity Theorem

If a permutation σ has two factorisations

$$\sigma = \gamma_n\gamma_{n-1}\cdots\gamma_2\gamma_1 = \rho_m\rho_{m-1}\cdots\rho_2\rho_1$$

where each γ_i and ρ_j is a transposition, then both m and n are even or both are odd.

7.6 ORDER OF A PERMUTATION

7.6.1 Definition: order

1. An element α of S_n has *order* $r > 0$ if $\alpha^r = e$, and no smaller positive power of α is e.
2. The *order* of a k cycle is k. (see Tutorial)
3. The *order of the product of disjoint cycles* is the lcm of the orders of the cycles. (see Tutorial)

7.7 CONJUGATION OF PERMUTATIONS

7.7.1 Definition: conjugate permutations

Two permutations σ and τ in S_n are *conjugate* in S_n if we can find $\gamma \in S_n$ such that $\gamma\sigma\gamma^{-1} = \tau$ and $\gamma^{-1}\tau\gamma = \sigma$.

7.7.2 Proposition

Let σ and τ be permutations in S_n where σ has a decomposition as follows:
$\sigma = (a_1 \quad a_2 \quad \cdots \quad a_{k_1})(b_1 \quad b_2 \quad \cdots \quad b_{k_2})\cdots$ then $\tau\sigma\tau^{-1}$ has cyclic decomposition
$\tau\sigma\tau^{-1} = (\tau(a_1) \quad \tau(a_2) \quad \cdots \quad \tau(a_{k_1}))(\tau(b_1) \quad \tau(b_2) \quad \cdots \quad \tau(b_{k_2}))\cdots$
That is to find $\tau\sigma\tau^{-1}$ apply τ directly to the entries in σ.

7.7.3 Proposition

Two permutations σ and τ in S_n are conjugate in S_n if and only if they have the same cyclic structure.
To find $\gamma \in S_n$ such that $\gamma\sigma\gamma^{-1} = \tau$, line up σ and τ one beneath the other, with corresponding cycles. $\gamma \in S_n$ is the mapping that maps row of σ to the row of τ.

7.7.4 Proposition

On S_n define $\equiv$ as follows: $\sigma \equiv \tau$ if and only if σ and τ are conjugate in S_n. Then $\equiv$ is an equivalence relation on S_n. The equivalence classes of S_n under $\equiv$ partition S_n into sets of distinct cyclic structure.

7.8 THE ALTERNATING GROUP

7.8.1 Definition: even and odd permutations, alternating group, parity

1. A permutation σ is called *even* or *odd*, according it can be written in some way as a product of an even or odd number of transpositions.
2. The set of all even permutations in S_n is denoted by A_n and is called the *Alternating Group of degree n.*
3. We refer to this eveness or oddness of the permutation as its *parity.*

7.8.2 Example

Determine the parity of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 6 & 1 & 7 & 8 & 2 & 9 & 3 \end{pmatrix}$.

$$\begin{aligned} \sigma &= (1 \quad 5 \quad 7 \quad 2 \quad 4)(3 \quad 6 \quad 8 \quad 9) \\ &= (1 \quad 4)(1 \quad 2)(1 \quad 7)(1 \quad 5)(3 \quad 9)(3 \quad 8)(3 \quad 6). \end{aligned}$$

There are 7 transpositions in this factorisation and the permutation is odd.

7.8.3 Theorem

If $n \geq 2$, the set A_n has the following properties.

1. e is in A_n and if σ and τ are in A_n then so are σ^{-1}, τ^{-1} and $\sigma\tau$.
2. $|A_n| = \frac{1}{2}n!$

7.9 CYCLE STRUCTURE OF S_4 AND S_5

1. $|S_4| = 4! = 24$. Let A_4 be the set of even permutation and B_4 be the set of odd permutation in S_4. Then $|A_4| = |B_4| = 12$.

Type of Equivalence Classes Modulo in S_4	No. of elements in the class	Order of each element in the class	Parity of elements in each class
$[e] = [(1)(2)(3)(4)]$	1	1	even
$[(1 \quad 2)]$	$\frac{4.3}{2} = 6$	2	odd
$[(1 \quad 2)(3 \quad 4)]$	$\frac{1}{2}\left\{\frac{4.3}{2}\frac{2.1}{2}\right\} = 3$	2	even
$[(1 \quad 2 \quad 3)]$	$\frac{4.3.2}{3} = 8$	3	even
$[(1 \quad 2 \quad 3 \quad 4)]$	$\frac{4.3.2.1}{4} = 6$	4	odd

2. $|S_5| = 5! = 120$ $|A_5| = |B_5| = 60$.

Type of Equivalence Classes Modulo in S_5	No. of elements in the class	Order of each element in the class	Parity of elements in each class
$[e] = [(1)(2)(3)(4)(5)]$	1	1	even
$[(1 \quad 2)]$	$\frac{5.4}{2} = 10$	2	odd
$[(1 \quad 2)(3 \quad 4)]$	$\frac{1}{2}\left\{\frac{5.4}{2}\frac{3.2}{2}\right\} = 15$	2	even
$[(1 \quad 2 \quad 3)]$	$\frac{5.4.3}{3} = 20$	3	even
$[(1 \quad 2 \quad 3 \quad 4)]$	$\frac{5.4.3.2}{4} = 30$	4	odd
$[(1 \quad 2)(3 \quad 4 \quad 5)]$	$\frac{5.4}{2}\frac{3.2.1}{3} = 20$	6	odd
$[(1 \quad 2 \quad 3 \quad 4 \quad 5)]$	$\frac{5.4.3.2.1}{5} = 24$	5	even

7.10 TUTORIAL

1. Compute the indicated product involving the permutations in S_6.
   $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$ $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$ $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$

   (a) $\tau\sigma$ (b) $\tau^2\sigma$ (c) $\mu\sigma^2$ (d) $\sigma^{-2}\tau$ (e) $\sigma^{-1}\tau\sigma$

2. Let A be a set and let $\sigma \in S_A$. For a fixed $a \in A$, the set $[a] = \{\sigma^n(a) | n \in \mathbb{Z}\}$ is the orbit of a under σ. In the following find the orbit of 1 under the permutations: (a) σ (b) τ (c) μ (from question 1)

3. Find the number of elements in the set $\{\sigma \in S_4 | \sigma(3) = 3\}$.

4. Find the number of elements in the set $\{\sigma \in S_5 | \sigma(2) = 5\}$.

5. Find the orbits of the following permutations.

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

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

   (c) $\sigma : \mathbb{Z} \to \mathbb{Z}$ where $\sigma(n) = n + 2$.

6. Compute the following products of cycles in S_8.

   (a) $(1\ \ 4\ \ 5)(7\ \ 8)(2\ \ 5\ \ 7)$

   (b) $(1\ \ 3\ \ 2\ \ 7)(4\ \ 8\ \ 6)$

   (c) $(1\ \ 2)(4\ \ 7\ \ 8)(2\ \ 1)(7\ \ 2\ \ 8\ \ 1\ \ 5)$

7. Show that the following defines an equivalence relation on S_3.
   For $\alpha, \beta \in S_3$, we say $\alpha \equiv \beta$ if $\alpha\beta^{-1} \in H$. Show that the equivalence classes are $H = \{e, R\}$, $H\rho = \{\rho, \rho^2 R\}$, $H\rho^2 = \{\rho^2, \rho R\}$. Similarly equivalences replacing H with K or J can be defined.

8. Express the following as a product of disjoint cycles, and then as a product of transpositions. (a) $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1\end{pmatrix}$ (b) $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6\end{pmatrix}$.

9. Which of the permutations in S_3 are even permutations? Make the table for the alternating group A_3.

10. An element a of S_8 has order $r > 0$ if $a^r = e$, the identity permutation, and no smaller positive power of a is e.

    (a) What is the order of the cycle $(1\ \ 4\ \ 5\ \ 7)$?

    (b) State a theorem suggested by part (a).

    (c) What is the order of $\sigma = (4\ \ 5)(2\ \ 3\ \ 7)$, and of $\tau = (1\ \ 4)(3\ \ 5\ \ 7\ \ 8)$?

    (d) State a theorem suggested by (c).

    (e) In S_n prove that the order of an r-cycle is r.

11. Prove that

    $$(1\ \ 2\ \ 3\cdots\ \ r) = (2\ \ 3\ \ 4\cdots r\ \ 1) = (3\ \ 4\ \ 5\cdots r\ \ 1\ \ 2) = \cdots = (r\ \ 1\ \ 2\cdots r{-}1).$$

    Conclude that there are exactly r such notations for this cycle.

12. Exhibit two 2-cycles whose product is a 3-cycle.

13. Let α and β be r- cycles in S_x. If there is an x_0 in X such that (i) both α and β move x_0 and (ii) $\alpha^t(x_0) = \beta^t(x_0)$ for all integers t, then $\alpha = \beta$.
    (Hint: If α is an r-cycle and $0 \leq j \leq r$, then $\alpha^j(i_1) = (i_{1+j})$.

14. Let $\alpha = (1\ \ 2)(3\ \ 4\ \ 5)(6\ \ 7\ \ 8\ \ 9)$ and $\beta = (1\ \ 3\ \ 5\ \ 7)(2\ \ 4\ \ 6\ \ 8)$. Find $\beta\alpha\beta^{-1}$ and $\alpha\beta\alpha^{-1}$.

15. Given $\sigma = (1\ \ 2)(3\ \ 4\ \ 5)(6\ \ 7\ \ 8\ \ 9)$ and $\delta = (1\ \ 3)(4\ \ 9\ \ 5)(2\ \ 6\ \ 7\ \ 8)$. Find β such that $\delta = \beta\sigma\beta^{-1}$.

16. Let $\alpha = \beta_1\beta_2\beta_3\cdots\beta_m$, where the β_i are disjoint r_i-cycles. Prove that the order of α is the $lcm\{r_1, r_2, \cdots, r_m\}$.

17. An r-cycle is even if and only if r is odd.

18. If $n \geq 2$, then A_n is generated by 3-cycles. [Hint: $(i \quad j)(j \quad k) = (i \quad j \quad k)$ and $(i \quad j)(k \quad m) = (i \quad j)(j \quad k)(j \quad k)(k \quad m)$] .

19. Prove that S_n can be generated by $(1 \quad 2), (1 \quad 3), (1 \quad 4), ...(1 \quad n)$.

20. Make a table for the cyclic structure of S_5.

21. Show that conjugacy in S_n is an equivalence relation on S_n. (See Appendix 1)

Chapter 8

MOTIONS OF SYMMETRY

8.0.1 RIGID MOTIONS OF REGULAR POLYHEDRA

8.0.2 Definition: figure, edges, vertices, faces

Group Theory began with the study of groups inside the symmetric group S_n. In this section we discuss some of these groups that arise from the symmetries of geometric figures. *By a figure* we mean a finite set of points called *vertices*, some pairs of which are joined by straight lines or *edges.* These edges may bound a *face* of the plane figure or a body in space.

8.1 MOTION OF SYMMETRY

8.1.1 Definition: motion of symmetry

A *motion* or *symmetry* of a geometric figure is a permutation of its vertices (edges or faces) that can be realized by a rigid motion in space. The motion of symmetry *preserves distance* between the vertices (edges or faces) it permutes. Each rigid motion is a permutation (bijection) of n objects, BUT not all permutations may be realised as rigid motions of a plane figure or a body in space.

8.1.2 Definition:axes of symmetry, rotations and reflections

1. Given two motions σ and τ of a figure, the *composite* $\sigma\tau$ is also a motion obtained by first doing τ and then σ. Similarly σ^{-1} is a motion achieved by *reversing the motion* σ. Finally, the identity permutation e is a motion , that is no *movement* at all.

2. The *axes of symmetry* are lines around which the geometric figure is symmetrical. That is, for every point P there is another point P' such that the perpendiculars from the points to a line of symmetry are equal of length and coincident. In a geometric body lines of symmetry may run from

$$\left.\begin{array}{c}\text{Vertex}\\ \text{Midpoint of Edge}\\ \text{Centre of Face}\end{array}\right\}\overset{\text{to}}{\Longleftrightarrow}\left\{\begin{array}{c}\text{Vertex}\\ \text{Midpoint of Edge}\\ \text{Centre of Face}\end{array}\right.$$

3. A rotation (in $\mathbb{R}^3$-space) about a plane line of symmetry, through π radians, is called a *reflection in the line of symmetry.* Points that lie on the line or axis of symmetry are pointwise invariant (not moved) under the motion, but a motion about an axis from the midpoint of an edge will leave that edge invariant but will interchange the endpoints of that edge. That is the edge is invariant but not pointwise. A motion about an axis to the midpoint of a face will rotate the vertices of the face. Again the face is invariant but not pointwise under the rigid motion.

4. A rotation about a *point* (in $\mathbb{R}^2$ or $\mathbb{R}^3$) in the plane through angle is a *rotation.* If the plane figure is regular (all sides the same length) then this angle $\theta = \dfrac{2\pi}{n}$ radians, where n is the number of vertices of the figure. This point is at the intersection of the lines of symmetry of the body and is called the *centre* of the body.

8.1.3 The group of symmetry of a non-square rectangle

Vertices 1, 2, 3, 4, and sides a, b, c, d where $|a| = |c|$ and $|b| = |d|$
There are two axes of symmetry and one point of rotation:
The axes run from the midpoint of a to midpoint of c (horizontal axis) , midpoint of b to midpoint of d (vertical axis). The point of rotation is at the intersection of the axes of symmetry(centre of the face)

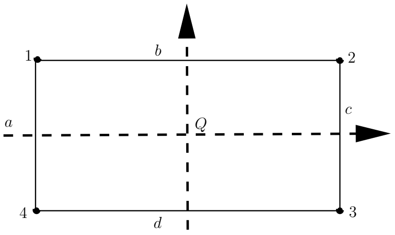


Figure 8.1: Axes of symmetry for the rectangle

The motions $(1 \quad 2)(3 \quad 4)$ and $(1 \quad 4)(2 \quad 3)$ result from rotating or reflecting the rectangle π radians about the vertical and horizontal axes of symmetry, respectively. The composite of these is $(1 \quad 3)(2 \quad 4)$, which is the motion obtained by a rotation of π radians in the plane of the rectangle about point Q.
Hence $G = \{e, (1 \quad 2)(3 \quad 4), (1 \quad 4)(2 \quad 3), (1 \quad 3)(2 \quad 4)\} = \{e, a, b, c\}$. We note that
$e^2 = a^2 = b^2 = c^2 = e$. This group of four elements is called the *Klein Group.*

8.1.4 The group of motions of an equilateral triangle

Vertices 1, 2, 3, and edges a, b, c.

Axes of symmetry run from each vertex to the midpoint of the opposite sides. Point of rotation lies at their intersection in the plane. The motions $\sigma = (1 \quad 2 \quad 3)$ and $\sigma^2 = (1 \quad 3 \quad 2)$ are achieved by clockwise rotations of $\dfrac{2\pi}{3}$ radians and $\dfrac{4\pi}{3}$ radians about Q,

M	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

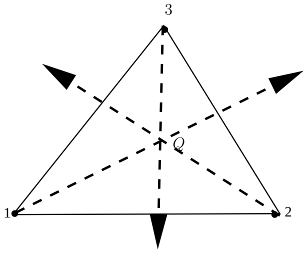


Figure 8.2: Axes of symmetry for the equilateral triangle

respectively. In addition $\tau = (2 \quad 3)$ is realised by rotating the triangle π radians about the line through the vertex 1 and the midpoint of the opposite side. Similarly $(1 \quad 3)$ and $(1 \quad 2)$ are motions, so the group is in fact $S_3 = \{e, (1 \quad 2 \quad 3), (1 \quad 3 \quad 2), (1 \quad 2), (1 \quad 3), (2 \quad 3)\}$.

8.1.5 The group of motions of the square

Vertices 1, 2, 3, 4 and edges a, b, c, d.

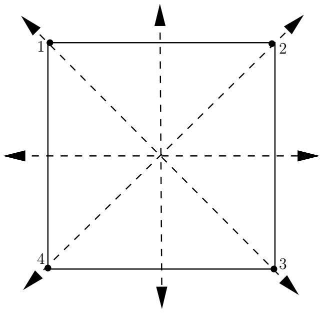


Figure 8.3: Axes of symmetry for the square

There are 4 axes of symmetry: From vertex 1 to vertex 3, from vertex 2 to vertex 4, and from midpoint a to midpoint c, from midpoint b to midpoint d. Rotational symmetry about the point of intersection of these axes, through $\frac{2\pi}{4} = \frac{\pi}{2}$, $2\left(\frac{2\pi}{4}\right) = \frac{4\pi}{2} = \pi$ and

$3\left(\dfrac{2\pi}{4}\right) = \dfrac{3\pi}{2}$ radians. The group of motions is denoted by D_4, the regular polygon with 4 vertices, and is called the *Octic Group* (has 8 elements) and is the group of rigid motions of a square. Let $\rho_0 = e$ be the identity . $\mu_1 = (1 \quad 2)(3 \quad 4)$ and $\mu_2 = (1 \quad 4)(2 \quad 3)$ be the mirror images in perpendicular bisectors of the sides; and $\delta_1 = (1 \quad 3)$ and $\delta_2 = (2 \quad 4)$ be the diagonal flips. We note that the motions are not commutative.

D_4	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	$\rho1$	ρ_2	ρ_0

Table 8.1: Multiplication Table for D_4

$$\{\rho_0\} \subset \{\rho_0, \mu_1\} \subset \{\rho_0, \rho_2, \mu_1, \mu_2\} \subset D_4; \qquad D_4 \subset S_4$$

8.1.6 The group of motions of a regular polygon

The Dihedral group D_n, the group of motions of a regular n-gon, for $n \geq 3$. The group of motions of the n-gon are of two types:

1. $\sigma = (1 \quad 2 \quad 3 \quad 4 \quad \cdots \quad n)$; the clockwise rotation of $\dfrac{2\pi}{n}$ radians about the centre of the figure.
2. $\tau = (1 \quad n-1)(2 \quad n-2)(3 \quad n-3)\cdots$ the rotation of π radians about a line through the vertex n and the centre of the figure.

If n is odd, then τ fixes only one vertex n, whereas if $n = 2m$, then τ fixes n and m.

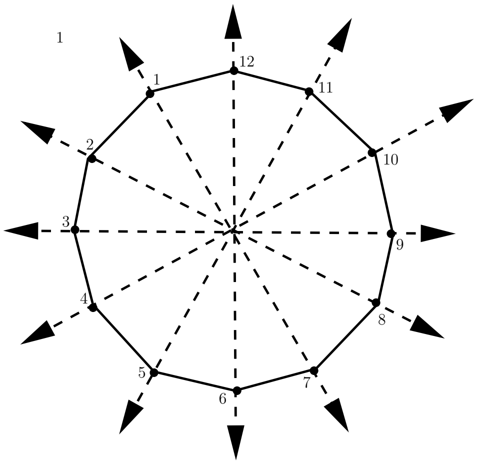


Figure 8.4: Axes of symmetry of the 12-gon (D_{12})

8.2 TUTORIAL

1. Find the group of motions of the diamond shown in Figure 8.5(a) with all edges and the vertical diagonal, of length 1.

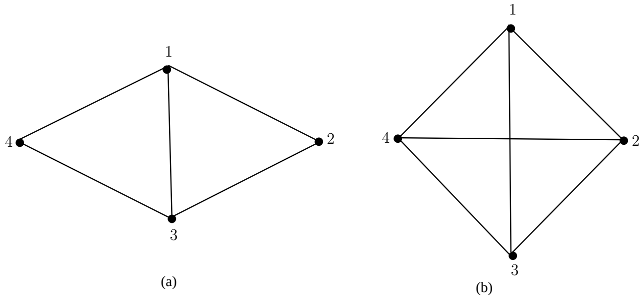


Figure 8.5:

2. Find the group of motions of the diamond shown in Figure 8.5(b) with both the diagonals, of length 1.

REFERENCES

1. Introduction to Abstract Algebra W. Keith Nicholson, Pringle, Weber and Schmidt - Kent Publ. Co.

2. Guide to Abstract Algebra, Carol Whitehead, Palgrave Mathematical Guides, Macmillan.

3. Algebra and Geometry, A F Beardon, Cambridge Univ. press, 2005

4. Glimpses of Algebra and Geometry, G Toth, Springer, 1997.

5. Naive Lie Theory, J Stillwell, Springer, 2008

6. The Geometry of Discrete Groups, A F Beardon, Springer, 1983.

7. Groups, C R Jordan & D A Jordan, Hodder Headline Group, 1994.