



Sets, Relations and Groups

Contents

Assessment statements	1214
1 Sets	1215
1.1 Basic set properties	1216
1.2 Venn diagrams	1217
1.3 Subset	1219
1.4 The power set	1221
1.5 Operations on sets	1222
1.6 Set differences	1225
1.7 Summary of set properties	1227
2 Relations and Functions	1234
2.1 Relations	1234
2.2 Functions	1246
3 Groups I	1264
3.1 Binary operations	1264
3.2 Groups	1273
3.3 Permutations	1286
4 Groups II	1302
4.1 Introduction	1302
4.2 Subgroups	1304
4.3 Cyclic groups	1310
4.4 Homomorphism and isomorphism	1315
Answers	1329



Sets, Relations and Groups



Assessment statements

- 8.1 Finite and infinite sets.
Subsets.
Operations on sets; union; intersection; complement; set difference; symmetric difference.
De Morgan's laws; distributive, associative and commutative laws (for union and intersection).
- 8.2 Ordered pairs: the Cartesian product of two sets.
Relations; equivalence relations; equivalence classes.
- 8.3 Functions: injections; surjections; bijections.
Composition of functions and inverse functions.
- 8.4 Binary operations. Operation tables (Cayley tables).
- 8.5 Binary operations with associative, distributive and commutative properties.
- 8.6 The identity element e .
The inverse a^{-1} of an element a .
Proof that left-cancellation and right-cancellation by an element a hold, provided that a has an inverse.
Proofs of the uniqueness of the identity and inverse elements.
- 8.7 The definition of a group $\{G, *\}$.
The operation table of group is a Latin square but the converse is false. Abelian groups.
- 8.8 Examples of groups:
 - $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ and \mathbb{C} under addition
 - integers under addition modulo n
 - non-zero integers under multiplication, modulo p , where p is prime
 - symmetries of plane figures including equilateral triangles and rectangles
 - invertible functions under composition of functions.
- 8.9 The order of a group element and the order of a group.
Cyclic groups. Generators.
Proof that all cyclic groups are Abelian.
- 8.10 Permutations under composition of permutations.
Cycle notation for permutations.
Result that every permutation can be written as a composition of disjoint cycles.
The order of a combination of cycles.
- 8.11 Subgroups, proper subgroups.
Use and proof of subgroup tests.
Lagrange's theorem.
Use and proof of the result that the order of a finite group is divisible by the order of any element. (Corollary to Lagrange's theorem.)
Definition and examples of left and right cosets of a subgroup of a group.
- 8.12 Definition of a group homomorphism.
Definition of the kernel of a homomorphism.
Proof that the kernel and the range of a homomorphism are subgroups.
Proof of homomorphism properties for identities and inverses.
Isomorphism of groups.
The order of an element is unchanged by an isomorphism.



Sets



Review

We will start this option by reviewing and extending your knowledge of set theory. Many of the concepts you have already seen in the book. We will begin with a few definitions.

Definitions are essential in any subject matter because they help precision in discussion. However, if we try to define any term, we will be using other words which are defined using still other words that are not defined, and so on. That is why, in mathematics, like any other subject, new structures start with some terms that are ‘understood’ but are not defined.

A set is an **undefined** term in set theory. It is understood to be a ‘*well-defined*’ collection of items or objects. Usually, the items in a set share some property. Any item that has the property is said to be a member (or an element) of the set and any item that does not have the property is not a member of the set.

Notation

We usually use capital letters to denote sets and the symbol \in to denote membership in a set. Thus, $x \in A$ means that object x is an element or a member of set A , and $y \notin A$ means that item y is not a member or element of set A . Also, when we list the elements of a set, or when we describe it by a rule, we use braces to indicate the set, as you will see in the following example.

Let A be the set of numbers on the sides of a normal die. Then we can define the set A by either listing its elements:

$$A = \{1, 2, 3, 4, 5, 6\}$$

or by stating a rule:

$$A = \{x \mid x = \text{a number on a six-sided die}\}.$$

(This is read as ‘the set of x such that x is a number on a six-sided die’ or any equivalent property.)

Notice that 5 is an element of A , and that is why we write

$$5 \in A$$

while 7 is not a member and we write

$$7 \notin A.$$



This is also called ‘set-builder’ notation.

1.1

Basic set properties

What do we mean by a *well-defined* collection? When we define a set by a rule or by listing its elements, then **well defined** means that we should always be able to make a clear decision whether any object is, or is not, an element of the set.

For example, if we define set B as the set of the first 10 positive integers, i.e.

$$B = \{x \mid x \text{ is one of the first 10 positive integers}\}, \text{ or } B = \{1, 2, \dots, 9, 10\}$$

then, given any number, we can always say whether it is an element of B or not.

$$\text{So, } 2.999 \notin B \text{ while } 3 \in B.$$

If we define $C = \{y \mid y \text{ is one of 10 integers}\}$, can we say that $3 \in C$? The answer is no. 3 may or may not be an element of C . So, B is a well-defined collection and hence it is a set, and C is not well defined and hence it is not a set.

When we discuss objects we always have the set of all possible objects that we call the **universal set** and we denote it by U . A set that contains no element is called an **empty set** and it is denoted by \emptyset or simply $\{\}$.

Note: Here is a list of sets that you already know but are mentioned here as a refresher.

\mathbb{N} The set of natural numbers and zero, $\{0, 1, 2, 3, \dots\}$.

\mathbb{Z} The set of integers, $\{\dots, -2, -1, 0, 1, 2, \dots\}$.

\mathbb{Z}^+ The set of positive integers, $\{1, 2, 3, \dots\}$.

\mathbb{Q} The set of rational numbers.

\mathbb{Q}^+ The set of positive rational numbers.

\mathbb{R} The set of real numbers.

\mathbb{R}^+ The set of positive real numbers.

\mathbb{C} The set of complex numbers.

Note: In many sources you may find a slight difference in the definition of these sets. Frequently we have

\mathbb{N} The set of natural numbers, $\{1, 2, 3, \dots\}$, while

\mathbb{W} The set of natural numbers and zero, $\{0, 1, 2, 3, \dots\}$.

Some sets can be defined using a rule:

\mathbb{Q} (the set of rational numbers) can be defined as

$$\mathbb{Q} = \left\{ x \mid x = \frac{a}{b}, a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}.$$

\mathbb{Q}^+ (the set of positive rational numbers) can be defined as

$$\mathbb{Q}^+ = \{ x \mid x \in \mathbb{Q}, x > 0 \}.$$

\mathbb{C} (the set of complex numbers) can also be defined as

$$\mathbb{C} = \{ x + iy \mid x, y \in \mathbb{R}, i^2 = -1 \}.$$

Some properties

- 1 No ordering is required for the elements of a set, thus $\{1, 2, 3, 4, 5, 6\}$ and $\{5, 1, 3, 2, 6, 4\}$ are the same set.
- 2 Each element of a set is listed only once; it is superfluous to list it again. Therefore, the set $\{1, 1, 2, 3, 4, 4, 5, 6\}$ is actually the set $\{1, 2, 3, 4, 5, 6\}$.
- 3 Two sets A and B are equal and we write $A = B$ if and only if they have the same elements.
For example, $\{1, 1, 2, 3\} = \{1, 2, 3\} = \{x \mid x \in \mathbb{Z}^+, x < 4\}$; or $A = B$, where $A = \{y \mid y = a + b, a, b \in \{1, 2, 3\}\}$ and $B = \{2, 3, 4, 5, 6\}$.
- 4 If there are exactly n distinct elements in a set A , where $n \in \mathbb{N}$, we say that A is a **finite** set and that n is the **cardinality** of A (the number of elements). Sometimes the number of elements is denoted by $|A|$ and sometimes as $n(A)$. If a set is not finite, then it is **infinite**.

For example, $A = \{1, 2, 3, 4, 5, 6\}$ is a finite set with $|A| = 6$, while \mathbb{N} is an infinite set.

Example 1

List the elements of the following sets:

- a) $A = \{x \in \mathbb{Z}^+ \mid -2 \leq x \leq 7\}$ b) $B = \{x \in \mathbb{Z} \mid x^2 < 16\}$
c) $C = \{x \in \mathbb{Q} \mid 3x^2 + 7x + 2 = 0\}$

Solution

- a) $A = \{1, 2, 3, 4, 5, 6, 7\}$ b) $B = \{0, \pm 1, \pm 2, \pm 3\}$ c) $C = \left\{-2, -\frac{1}{3}\right\}$



In many proofs, in this option or in other situations, when the statement is 'p if and only if q', denoted by $p \text{ iff } q$, or $p \Leftrightarrow q$ then we need to prove that p implies q , **and** q implies p , i.e. $p \Rightarrow q$ and $q \Rightarrow p$. We will sometimes denote the situation by (\Rightarrow) and (\Leftarrow) .



In proofs, we usually show that two sets are equal if elements from one set are also elements from the other set and vice versa. Thus, we write

$$(A = B) \Leftrightarrow ((\forall x \in A \Rightarrow x \in B) \text{ and } (\forall y \in B \Rightarrow y \in A)).$$

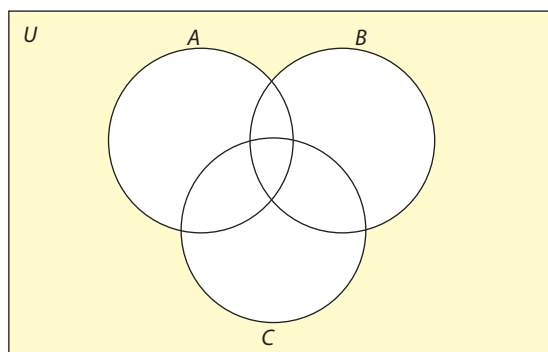
Here, we are borrowing a symbol that is used in logic to represent frequently used clauses such as 'for all elements from one set...', namely ' \forall '. So, if we want to say, 'for every integer, x , $x^2 \geq 0$ ', we write:

$$\forall x \in \mathbb{Z}, x^2 \geq 0.$$

Another quantifier that we may use in our discussion is the symbol for existence. So, if we want to say 'there is at least one element in A that is not in B ', then we write: $\exists x \in A$ such that $x \notin B$.

1.2 Venn diagrams

Sets can also be represented graphically using Venn diagrams. In Venn diagrams the universal set U is usually represented by a rectangle. Inside this rectangle, circles (or other 'closed' curves) can be used to represent sets.



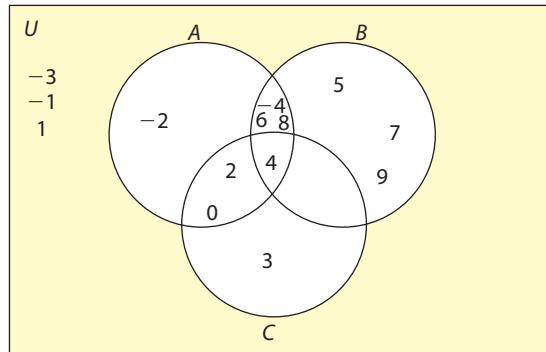
Venn diagrams are often used to indicate relationships between sets. We will show how a Venn diagram can be used in the following example.

Example 2

Given the universal set $U = \{x \in \mathbb{Z} \mid -4 \leq x \leq 9\}$, use a Venn diagram to show the following sets: $A = \{x \in U \mid x \text{ is even}\}$, $B = \{x \in U \mid |x| > 3\}$ and $C = \{x \in U \mid x^4 - 9x^3 + 26x^2 - 24x = 0\}$.

Solution

$A = \{-4, -2, 0, 2, 4, 6, 8\}$, $B = \{-4, 4, 5, 6, 7, 8, 9\}$, $C = \{0, 2, 3, 4\}$



Example 3

Write down the following sets in set-builder notation:

- the set of all even integers
- the set of all odd integers
- the set of all integers divisible by 5
- the set of all integers that have a remainder of 4 when divided by 7
- the set of all integers that have a remainder of l when divided by a prime number p where $l < p$.

Solution

- $A = \{2k \mid k \in \mathbb{Z}\}$
- $B = \{2k - 1 \mid k \in \mathbb{Z}\}$
- $C = \{5k \mid k \in \mathbb{Z}\}$
- $D = \{7k + 4 \mid k \in \mathbb{Z}\}$
- $E = \{pk + l \mid k \in \mathbb{Z}\}, 0 \leq l < p$



Example 4

Let M be the set $\{1, \{2, 3\}, 2, \emptyset\}$.

- a) Find the number of elements of M .
- b) Is $2 \in M$?
- c) Is $3 \in M$?
- d) Is $\{2, 3\} \in M$?
- e) Is $\{\emptyset\} = \emptyset$?

Solution

- a) 4
- b) Yes.
- c) No. $3 \in \{2, 3\}$ which is a member of M itself.
- d) Yes.
- e) No. $\{\emptyset\}$ is a set that contains the empty set as its only element, so it is not empty!

1.3 Subset

Definition 1

A set A is a **subset** of a set B , and we write $A \subseteq B$, if and only if every element of A is also an element of B . That means that the set A could be equal to the set B as well.

Formally, this means that for every x , if $x \in A$, then $x \in B$, or symbolically

$$A \subseteq B \Leftrightarrow \text{for every } x \in A \Rightarrow x \in B$$

From the above definition, we can develop a method for showing that a set A is not a subset of a set B by observing that if $A \not\subseteq B$, then there is at least one $x \in A$ which is not in B . Notice here that if A is not a proper subset of B , it obviously cannot be a subset of B .

All the following statements are true.

- ✓ $\{x, y\} \subseteq \{x, y, z\}$
- ✓ $\{x, y\} \subset \{x, y, z\}$
- ✓ $\{x, y\} \subseteq \{x, \{x, y\}, y, z\}$
- ✓ $\{x, y\} \in \{x, \{x, y\}, y, z\}$
- ✓ $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Theorem 1

For any set A , $A \subseteq U$, $A \subseteq A$, and $\emptyset \subseteq A$.



In many cases, we can abbreviate 'for every ...' by using the 'universal quantifier \forall ' instead. So for the subset definition, we would restate it as:

$$A \subseteq B \Leftrightarrow \forall x \in A \Rightarrow x \in B$$

If $A \subseteq B$, but $A \neq B$, then A is called a **proper subset** of B and we write $A \subset B$.



When $A \subseteq B$, it is also common to say 'A is contained in B', or 'B is a **superset** of A', and we write $B \supseteq A$.

Proof

- Since U is the universal set, it contains all elements, and hence it contains all elements that are in A .
- If $x \in A$ then $x \in A$, so $A \subseteq A$.
- The proof that $\emptyset \subseteq A$ can be done by contradiction. $\emptyset \subseteq A$ is a statement that is either true or false. Suppose it is false, that is, $\emptyset \not\subseteq A$, this means that not every $x \in \emptyset$ implies that $x \in A$, i.e. we can find some $x \in \emptyset$ such that $x \notin A$. This cannot be true because there is no $x \in \emptyset$ in the first place. So, our assumption that $\emptyset \not\subseteq A$ leads to a contradiction and hence cannot be true. Therefore, it has to be false, and $\emptyset \subseteq A$.

Equal sets revisited

With the definition of a subset, we can develop a new way of looking at equal sets.

By definition, A and B are equal if they have the same elements, i.e. every element of A is an element of B and every element of B is an element of A . Thus, we can now say

$A = B$ if and only if $A \subseteq B$ and $B \subseteq A$, or equivalently in symbolic form

$$A = B \Leftrightarrow A \subseteq B \text{ and } B \subseteq A.$$

Please notice here that the statement above makes two claims:

$$(\Rightarrow) \quad \text{If } A = B, \Rightarrow A \subseteq B \text{ and } B \subseteq A.$$

$$(\Leftarrow) \quad \text{If } A \subseteq B \text{ and } B \subseteq A, \Rightarrow A = B.$$

Each of the following statements is true.

$$\checkmark \quad \{\emptyset\} \in \{\{\emptyset\}\}$$

$$\checkmark \quad \emptyset \subseteq \{\{\emptyset\}\}$$

$$\checkmark \quad \{\emptyset\} \not\subseteq \{\{\emptyset\}\}$$

$$\checkmark \quad \{x\} \in \{\{x\}, y, z\}$$

$$\checkmark \quad \{x\} \subset \{x, y, z\}$$

$$\checkmark \quad \{x\} \not\subset \{\{x\}, y, z\}$$

$$\checkmark \quad \emptyset \subseteq \{a, b, \emptyset\}$$

$$\checkmark \quad \emptyset \in \{a, b, \emptyset\}$$

$$\checkmark \quad \{\emptyset\} \notin \{a, b, \emptyset\}$$

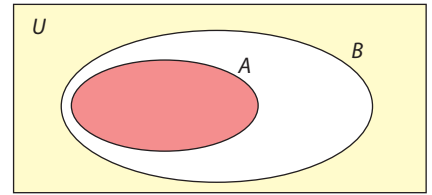


Venn diagrams for subsets

You can use Venn diagrams to show that one set is a subset of the other. Since, by definition, $A \subseteq B$ implies that every element of A is also an element of B , thus it is obvious that the Venn diagram for A is a part of the diagram for B .

Note: This diagram helps us understand the logic behind ‘proof by using contra-positive’ argument.

If A represents a proposition and B another one, then we can say that $A \Rightarrow B$; this is so because every element of A is automatically inside B . The contra-positive means that $\neg B \Rightarrow \neg A$. That is, if an element is not in B , it obviously cannot be in A .



\neg is a negation symbol.
' \neg ' is read as 'not'.



The power set

Definition 2

The **power set** of a set A , denoted as $\mathcal{P}(A)$, is the set of all subsets of A . Symbolically, this is written as

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}.$$

Example 5

Find the power set of $A = \{1, 2, 3\}$.

Solution

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$$

Note: Notice here that $|A| = 3$ and $|\mathcal{P}(A)| = 8 = 2^3$. This is a surprising but true result.

Theorem 2

Let A be a set with n elements, $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

Proof

In order to find $|\mathcal{P}(A)|$, we need to know how many subsets A has. Other than \emptyset and A itself, the subsets of A have 1, 2, 3, ..., or $n - 1$, elements each.

Recall from Chapter 4 of the textbook, that the number of subsets of size r that a set has, also known as combination of r elements out of n elements, is the binomial coefficient $\binom{n}{r}$. Thus,

$$|\mathcal{P}(A)| = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n}, \text{ where } \binom{n}{0} \text{ is the number of}$$

subsets with zero elements, i.e. \emptyset , and $\binom{n}{n}$ is the number of subsets with n elements, i.e. A .

However, applying the binomial theorem, we know that

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = (1+1)^n, \text{ and therefore } |\mathcal{P}(A)| = 2^n.$$

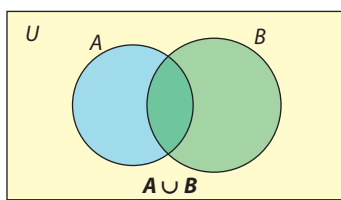
1.5

Operations on sets

Union and intersection

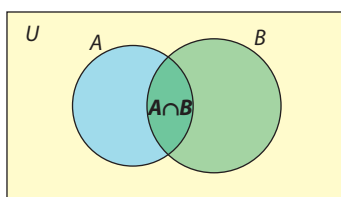
- If A and B are two sets of a universal set U , then **union** of A and B , written as $A \cup B$, is the set of elements that belong to A , or B , or *both*. Symbolically, this is written as

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}.$$



- If A and B are two sets of a universal set U , then **intersection** of A and B , written as $A \cap B$, is the set of elements that belong to *both A and B*. Symbolically, this is written as

$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}.$$



For example, if $A = \{x, y, z\}$ and $B = \{m, x, n, y\}$, then

$$A \cup B = \{m, n, x, y, z\} \text{ and } A \cap B = \{x, y\}.$$

Also,

$$A \cup \emptyset = A$$

$$A \cup U = U$$

$$A \cap U = A$$

$$A \cap \emptyset = \emptyset.$$

If $A \cap B = \emptyset$, then A and B are said to be **disjoint** sets.



The proof of each of the above is left as an exercise for you.



Some properties of union and intersection

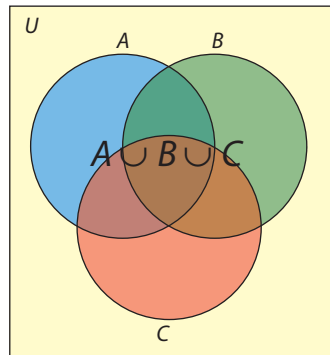
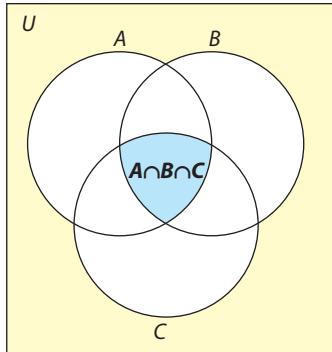
- Union of sets is associative.

$$A \cup (B \cup C) = (A \cup B) \cup C$$

Sometimes we write only $A \cup B \cup C$ as there is no need for parenthesis.

- Intersection of sets is associative.

$$A \cap (B \cap C) = (A \cap B) \cap C$$

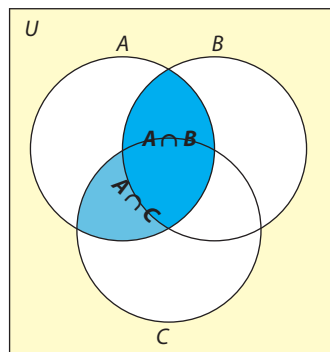
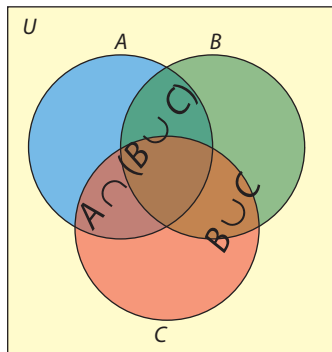


Also here sometimes we write only $A \cap B \cap C$ as there is no need for parenthesis.

- Sometimes the union and intersection of sets can be utilized by several sets. It is helpful for you to get acquainted with two notations:
 - The union of n sets $A_1, A_2, A_3, \dots, A_n$ can be written as $\bigcup_{i=1}^n A_i$.
 - The intersection of n sets $A_1, A_2, A_3, \dots, A_n$ can be written as $\bigcap_{i=1}^n A_i$.

Distributive properties

- Intersection is distributive over union.



$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Venn diagrams are helpful tools in understanding some set properties, but they are not proofs. For a property like this one, a formal proof is required and presented overleaf.

To show that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, we need to show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

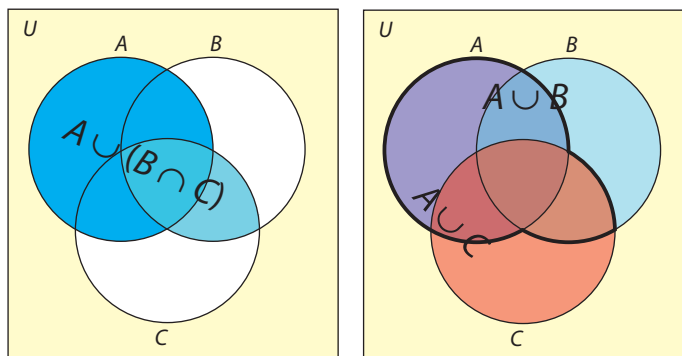
For all $x \in A \cap (B \cup C)$, $x \in A$ and $x \in B \cup C$. Since $x \in B \cup C$, then $x \in B$ or $x \in C$. Now, if $x \in B$, then $x \in A \cap B$, or, if $x \in C$, then $x \in A \cap C$. Thus we have shown that $x \in A \cap B$ or $x \in A \cap C$. This by definition means that $x \in (A \cap B) \cup (A \cap C)$. This completes the first part of the proof.

Now for every $x \in (A \cap B) \cup (A \cap C)$, $x \in (A \cap B)$ or $x \in (A \cap C)$. This means that $x \in A$ and $x \in B$ or $x \in A$ and $x \in C$. In both cases, x is an element of A and an element of either B or C , thus an element of $B \cup C$. Therefore, x belongs to both A and $B \cup C$, i.e. it belongs to $A \cap (B \cup C)$.

This completes the proof.

- Union is distributive over intersection.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$



To show that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, we need to show that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ and $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

For all $x \in A \cup (B \cap C)$, then $x \in A$ or $x \in B \cap C$. Since $x \in B \cap C$, then $x \in B$ and $x \in C$. Now, if $x \in B$, then $x \in A \cup B$, and, if $x \in C$, then $x \in A \cup C$. Thus we have shown that $x \in A \cup B$ and $x \in A \cup C$. This by definition means that $x \in (A \cup B) \cap (A \cup C)$. This completes the first part of the proof.

Now for every $x \in (A \cup B) \cap (A \cup C)$, $x \in (A \cup B)$ and $x \in (A \cup C)$. This means that $x \in A$ or $x \in B$ and $x \in A$ or $x \in C$. In both cases, if x is an element of A then it is an element of the union of A with any set, including $B \cap C$; and if x is not an element of A , then it must be an element of B and C , thus an element of $B \cap C$. Therefore, x belongs to A or $B \cap C$, i.e. it belongs to $A \cup (B \cap C)$.

This completes the proof.

- Union and intersection of sets are commutative operations.
 - $A \cup B = B \cup A$
 - $A \cap B = B \cap A$



Example 6

Given that $A = \{2, 4, 6, 8, 10, 12\}$, $B = \{3, 6, 9, 12\}$ and $C = \{2, 3, 5, 7, 11, 13, 17, 19, 23\}$ find the following sets:

- a) $A \cup B$ b) $C \cap (A \cup B)$ c) $C \cup (A \cap B)$

Solution

a) $A \cup B = \{2, 3, 4, 6, 8, 9, 10, 12\}$

b) $C \cap (A \cup B) = \{2, 3\}$

Notice here that

$$C \cap A = \{2\}, C \cap B = \{3\} \Rightarrow (C \cap A) \cup (C \cap B) = \{2, 3\}.$$

c) $C \cup (A \cap B) = \{2, 3, 5, 6, 7, 11, 12, 13, 17, 19, 23\}$ and

$$C \cup B = \{2, 3, 5, 6, 7, 9, 11, 12, 13, 17, 19, 23\}$$

$$\Rightarrow (C \cup A) \cap (C \cup B) = \{2, 3, 5, 6, 7, 11, 12, 13, 17, 19, 23\}.$$

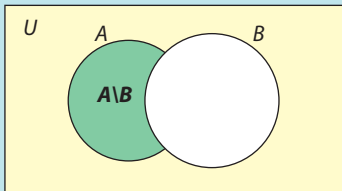
1.6

Set differences

Definition 3

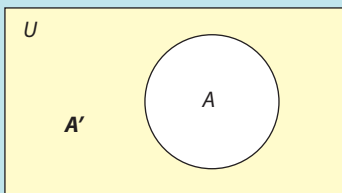
For any two sets A and B , the **difference** between set A and set B , denoted by $A \setminus B$ is the set of elements of A which are not in B . Symbolically,

$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}.$$



For any set A , the **complement** of A , denoted by A' , is the set of all elements in the universal set that are not in A .

$$A' = \{x \mid x \in U \text{ and } x \notin A\}$$



From the definitions left, it becomes obvious that

$$A \cap A' = \emptyset, \text{ or } A \cup A' = U.$$

Note: If we start with the definition of difference, then the complement can be understood as $A' = U \setminus A$, and if we start with the definition of complement then the difference can be understood as $A \setminus B = A \cap B'$.

Symmetric difference

The symmetric difference of two sets A and B , denoted by $A \Delta B$, is the set of all elements in A or in B but *not* in both.

There are several ways of interpreting this difference:

$$A \Delta B = \{x | x \in (A \cup B) \text{ and } x \notin (A \cap B)\}$$

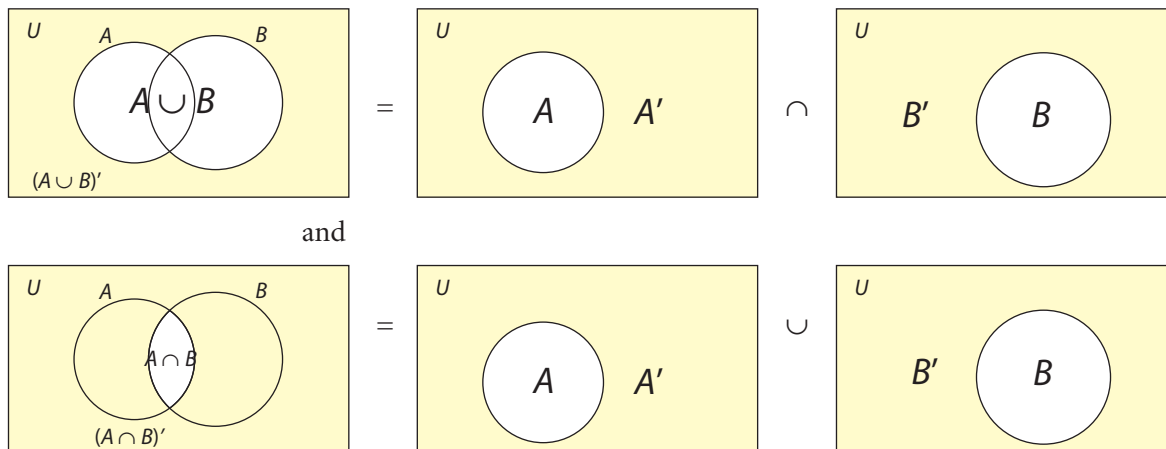
$$A \Delta B = (A \cup B) \setminus (A \cap B)$$

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

De Morgan's laws

For any two sets A and B , the following two statements are true:

- $(A \cup B)' = A' \cap B'$, and
- $(A \cap B)' = A' \cup B'$.



Proof (Optional – not required by IBO)

$$x \in (A \cup B)' \Rightarrow x \notin (A \cup B) \Rightarrow x \notin A \text{ and } x \notin B$$

(because if $x \in A$ then $x \in A \cup B$ which cannot be true here; similarly for B)

$$\Rightarrow x \in A' \text{ and } x \in B' \Rightarrow x \in A' \cap B', \text{ and thus}$$

$$(A \cup B)' \subseteq A' \cap B'.$$

Also,

$$x \in A' \cap B' \Rightarrow x \notin A \text{ and } x \notin B \Rightarrow x \notin (A \cup B)$$

(because if $x \in A$ then $x \notin A'$, or if $x \in B$ then $x \notin B'$, which cannot be true here)

$$\Rightarrow x \in (A \cup B)', \text{ and thus}$$

$$A' \cap B' \subseteq (A \cup B)'.$$

This completes the proof.

The proof of the second part of De Morgan's rule is left as an exercise for you.

1.7 Summary of set properties

(Proofs of some of these properties may have been presented before, are obvious, or left as an exercise.)

1 Commutativity of union and intersection

$$A \cup B = B \cup A; A \cap B = B \cap A$$

2 Associativity of union and intersection

$$(A \cup B) \cup C = A \cup (B \cup C); (A \cap B) \cap C = A \cap (B \cap C)$$

3 Distributive properties

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C);$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

4 Special cases

$$A \cup \emptyset = A; A \cap \emptyset = \emptyset$$

$$A \cap U = A; A \cup U = U$$

$$A \cup A = A; A \cap A = A$$

$$A \cup (A \cap B) = A; A \cap (A \cup B) = A$$

$$(A')' = A; A \cap A' = \emptyset; A \cup A' = U$$

$$U' = \emptyset; \emptyset' = U$$

Example 7

Simplify the following expressions:

a) $(A \cap B') \cap (A' \cap B)$

b) $(A \cup B') \cup (B \cup C') \cup (C \cup A')$

c) $A \cap (A' \cup B)$

d) $(A' \cup A)' \cup (A' \cup B)' \cap (A' \cup C)'$

Solution

$$\begin{aligned} \text{a) } (A \cap B') \cap (A' \cap B) &= A \cap B' \cap A' \cap B = A \cap A' \cap B' \cap B \\ &= (A \cap A') \cap (B' \cap B) = \emptyset \cap \emptyset = \emptyset \end{aligned}$$

$$\begin{aligned} \text{b) } (A \cup B') \cup (B \cup C') \cup (C \cup A') &= A \cup B' \cup B \cup C' \cup C \cup A' \\ &= A \cup A' \cup B \cup B' \cup C \cup C' \\ &= (A \cup A') \cup (B \cup B') \cup (C \cup C') \\ &= U \cup U \cup U = U \end{aligned}$$

$$\text{c) } A \cap (A' \cup B) = (A \cap A') \cup (A \cap B) = \emptyset \cup (A \cap B) = A \cap B$$

$$\begin{aligned} \text{d) } (A' \cup A)' \cup (A' \cup B)' \cap (A' \cup C)' &= U' \cup (A \cap B') \cap (A \cap C') \\ &= \emptyset \cup (A \cap B' \cap A \cap C') = A \cap B' \cap C' \\ &= A \cap (B \cup C)' \end{aligned}$$

Example 8

De Morgan's laws work for three or more sets. Show the following formulae to be true:

- a) $(A \cup B \cup C)' = A' \cap B' \cap C'$
- b) $(A \cap B \cap C)' = A' \cup B' \cup C'$
- c) $\left(\bigcup_{i=1}^n A_i\right)' = \bigcap_{i=1}^n A'_i, n \in \mathbb{Z}^+$
- d) $\left(\bigcap_{i=1}^n A_i\right)' = \bigcup_{i=1}^n A'_i, n \in \mathbb{Z}^+$

Solution

- a) $(A \cup B \cup C)' = ((A \cup B) \cup C)' = (A \cup B)' \cap C' = A' \cap B' \cap C'$
- b) $(A \cap B \cap C)' = ((A \cap B) \cap C)' = (A \cap B)' \cup C' = A' \cup B' \cup C'$
- c) To prove this formula we need to use the method of mathematical induction.

(i) Basis step:

$$n = 1 \Rightarrow A'_1 = A'_1$$

(ii) Inductive step:

We assume that the formula to be true for $n = k$, i.e.

$$\left(\bigcup_{i=1}^k A_i\right)' = \bigcap_{i=1}^k A'_i.$$

Now, we need show that the formula is true for $n = k + 1$.

$$\begin{aligned} \left(\bigcup_{i=1}^{k+1} A_i\right)' &= \left(\left(\bigcup_{i=1}^k A_i\right) \cup A_{k+1}\right)' = \left(\bigcup_{i=1}^k A_i\right)' \cap A'_{k+1} \\ &= \left(\bigcap_{i=1}^k A'_i\right) \cap A'_{k+1} = \bigcap_{i=1}^{k+1} A'_i \end{aligned}$$

(iii) Conclusion:

The formula is true for $n = 1$ and from the assumption that it is true for $n = k$ we have shown that it is true for $n = k + 1$. Therefore, we can deduce that the formula is for all $n \in \mathbb{Z}^+$.

- d) In a similar manner to c), the proof is straightforward and is left for you to practise.

Example 9

Given the sets A , B and C show the following identities:

- a) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
- b) $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$
- c) $(A \setminus B) \setminus C = A \setminus (B \cup C)$



Solution

- a) $A \setminus (B \cup C) = A \cap (B \cup C)' = A \cap B' \cap C'$
 $= (A \cap B') \cap (A \cap C') = (A \setminus B) \cap (A \setminus C)$
- b) $(A \cap B) \setminus C = (A \cap B) \cap C'$
 $= (A \cap C') \cap (B \cap C') = (A \setminus C) \cap (B \setminus C)$
- c) $(A \setminus B) \setminus C = (A \cap B') \cap C' = A \cap (B' \cap C')$
 $= A \cap (B \cup C)' = A \setminus (B \cup C)$

Exercise 1

1 Determine which sets are equal.

- a** $A = \{3, 6, 7\}, B = \{6, 7, 3\}$ **b** $A = \{x \in \mathbb{Z} \mid x^2 = 8\}, B = \{y \in \mathbb{Z}^+ \mid y = 2\sqrt{2}\}$
c $A = \{2\}, B = \{x \in \mathbb{N} \mid x^2 = 4\}$ **d** $A = \{-2, \emptyset, 2\}, B = \{x \in \mathbb{Z} \mid x^2 = 4\}$

2 $U = \{1, 2, 3, 4, 5, 6\}, A = \{1, 2, 3, 4\}, B = \{3, 4, 5\}$, and $C = \{1, 4, 5\}$. Find

- a** $A \cap (B \cup C)$ **b** $(A \cap B) \cup (A \cap C)$
c $(A \cup B)'$ **d** $A' \cup B'$
e $A' \cap B'$ **f** $A \setminus (B \cap C)$
g $A \Delta B$

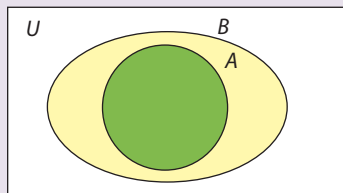
3 Determine whether each of the following statements is true. Justify your response by stating a property/theorem that supports your argument.

- a** $\sqrt{2} \in \mathbb{Q}$ **b** $(\sqrt{-1})^2 \in \mathbb{Z}$
c $\{2\} \subseteq \{2\}$ **d** $\{a\} \subset \{a, b\}, a \neq b$
e $\mathbb{Z}^+ \subset \mathbb{Q}$ **f** $\{3, a, b, c\} = \{3, a, b, 3, c, b\}$
g $\{a, e\} \cup \{e, f\} \cup \{g, h\} = \{a, e, f, g, h\}$
h Let $a, b \in \mathbb{R}$, and $a < b$, then $[a, b] \cap \{a, b\} = \{a\} \cup \{b\}$.
i Let $a, b \in \mathbb{R}$, and $a < b$, $[a, b] \setminus \{a, b\} = \{a, b\}$.

4 Let $A = \{a, \{2, a\}, \{4\}, \{\{2, 4\}\}, 4\}$. Determine which of the statements below are true and which are false.

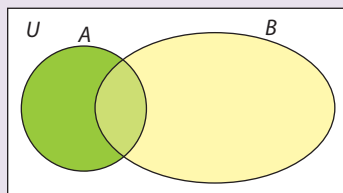
- a** $a \in A$ **b** $\{a\} \notin A$ **c** $\{2, a\} \subseteq A$
d $\{\{4\}, 4\} \subseteq A$ **e** $\{2, 4\} \in A$ **f** $\{\{2, 4\}\} \subseteq A$
g $\{\{2, a\}\} \subseteq A$ **h** $\{2, a\} \notin A$ **i** $\emptyset \subseteq A$

5 For each question part, copy the Venn diagram and shade the required region.



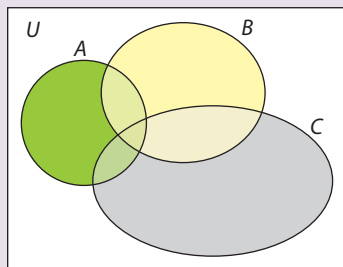
- a** $A \cap B$ **b** $A \cup B$ **c** $(A \cup B) \setminus (A \cap B)$
d $(A \cap B)'$ **e** $A \cap B'$ **f** $A' \cup B$

6 For each question part, copy the Venn diagram and shade the required region.



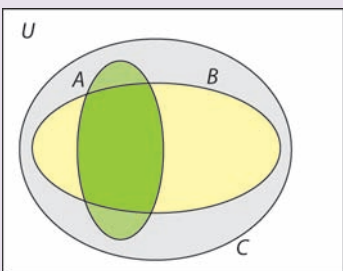
- a** $A \cap B$ **b** $A \cup B$ **c** $(A \cup B) \setminus (A \cap B)$
d $(A \cap B)'$ **e** $A \cap B'$ **f** $A' \cup B$
g $A \Delta B$

7 Three sets A , B and C are given. For each question part, copy the Venn diagram and shade the required region.



- a** $A \cap B'$ **b** $C' \cap B'$ **c** $B \cup (C \setminus A)$
d $(A \cup B)' \setminus C$ **e** $(A \cup B)' \setminus C$ **f** $(A \cap B)' \setminus C$
g $(A \cup B) \cap C'$

8 Three sets A , B and C are given. For each question part, copy the Venn diagram and shade the required region.

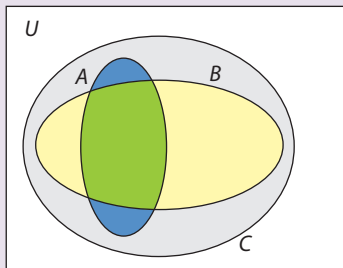


- a** $A \cap B'$ **b** $C' \cap B'$ **c** $B \cup (C \setminus A)$ **d** $(A \cup B)' \setminus C$
e $(A \cup B)' \setminus C$ **f** $(A \cap B)' \setminus C$ **g** $(A \cup B) \cap C'$

9 Let $A = \{a \mid a \in \mathbb{Z} \text{ and } a^4 - a^2 = 0\}$ and $B = \{b \mid b \in \mathbb{Z}^+ \text{ and } b = a^2\}$. Find

- a** $A \setminus B$ **b** $B \setminus A$ **c** $A \cap B$ **d** $\mathcal{P}(A)$

10 Write an expression that describes the region shaded in blue.



11 In a class, 84 students are preparing for their IB exams. 56 study maths at HL, 60 study English at HL, and 10 do not study either of these two courses. How many students study both maths HL and English HL?

12 A and B are subsets of U .

$$n(U) = 30, n(A \cup B) = 21, n(A \setminus B) = 10, n(B \setminus A) = 5.$$

Find $n(B \cap A)'$.

13 We define $M_r \subseteq \mathbb{Z}^+$ for every $r \in \mathbb{N}$ by: $M_r = \{x \in \mathbb{Z}^+ \mid r \mid x\}$.

List the elements of each of the following sets.

- a** M_1 **b** M_2'
c $M_2 \cap M_3$ **d** $M_6 \setminus M_3$

14 What can you conclude if $A \cap B = A \cup B$? Justify your response.

15 Prove each of the following (all sets are subsets of a universal set U):

- a** $(P \cup Q) \setminus (P \cap R) = P \cap (Q \setminus R)$ **b** $(P \cup Q) \setminus (P \cap Q) = (P \setminus Q) \cup (Q \setminus P)$
c $M \times (N \cup P) = (M \times N) \cup (M \times P)$ **d** $(A' \cup B)' \cup (A \cap B) = A$
e $(A' \cup B) \cap (A \cup B) = B$ **f** $A \cup (B \cap A')' = (A' \cap B)'$
g $P \Delta Q = (P \cup Q) \cap (P \cap Q)'$ **h** $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
i $[(A' \cup B) \cap (A \cup B')] = (A \cap B)' \cap (A \cup B)$
j $(A' \cap B) \cup C' = (A \cap C)' \cap (B' \cap C)'$
k $[(A \cap B) \cup (A' \cap B')] = (A \cup B) \cap (A' \cup B')$
l $(A \setminus B) \cap (B \setminus A) = (A \cup B) \setminus (A \cap B)$

16 A set A has n elements. A also has 21 subsets of size $(n - 2)$ each.

Find the number of subsets of A .

17 Prove each of the following (all sets are subsets of a universal set U):

- a** $A \cup B = A \Leftrightarrow B \subset A$ **b** $A \cap B = A \Leftrightarrow A \subset B$
c $A' \cup B = U \Leftrightarrow A \subset B$ **d** $A' \cap B = \emptyset \Leftrightarrow B \subset A$
e $A \subset B \Leftrightarrow B' \subset A'$

18 Let A and B be two non-empty subsets of a universal set U .

- a** Show that $A \subseteq B \Rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$.
- b** What is (\emptyset) ? $\mathcal{P}(\mathcal{P}(\emptyset))$?
- c** What relation is there between $\mathcal{P}(A \cap B)$ and $\mathcal{P}(A) \cap \mathcal{P}(B)$? Justify your response.
- d** What relation is there between $\mathcal{P}(A \cup B)$ and $\mathcal{P}(A) \cup \mathcal{P}(B)$? Justify your response.

19 Find the following unions and intersections. Justify your work.

- a** $\bigcup_{n \in \mathbb{N}} [n, n+1[$
- b** $\bigcap_{n \in \mathbb{Z}^+} \left[-\frac{1}{n}, 0\right]$
- c** $\bigcup_{n \in \mathbb{Z}^+} \left[\frac{1}{n}, 2 + \frac{1}{n}\right]$
- d** $\bigcap_{n \in \mathbb{Z}^+} \left[\frac{1}{n}, 2 + \frac{1}{n}\right]$

20 If A and B are finite sets, determine whether $|A \cup B| = |A| + |B|$.

21 Prove each of the following, given that A , B and C are three non-empty sets of a universal set U .

- a** If $A \subseteq B$, then $A \cup C \subseteq B \cup C$.
- b** If $A \subseteq B$, then $A \cap C \subseteq B \cap C$.
- c** $A \subseteq B$, iff $A \cap B = A$.
- d** If $A \subseteq B$, then $B \setminus A \cup A = B$.
- e** $A \setminus B \subseteq A$
- f** $A \cup (B \setminus A) = A \cup B$
- g** $A \subseteq B' \Leftrightarrow A \cap B = \emptyset$
- h** $A \setminus B \subseteq B \Leftrightarrow A \subseteq B$

22 Let A and B be two sets. Consider the following conjectures and prove those that are true and give a counter example for each one that is not true.

- a** $(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$
- b** $(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$
- c** $(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$
- d** $(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$
- e** $(A \cap B) \subseteq \mathcal{P}(A \cup B)$



Practice questions 1

- 1 $A - B$ is the set of all elements that belong to A but not to B .
 - a Use Venn diagrams to verify that $(A - B) \cup (B - A) = (A \cap B) - (A \cap B)$.
 - b Use De Morgan's laws to prove that $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$.
- 2 Let A and B be two non-empty sets, and $A - B$ be the set of all elements of A which are not in B . Draw Venn diagrams for $A - B$ and $B - A$ and determine if $B \cap (A - B) = B \cap (B - A)$.
- 3 Let X be a set containing n elements (where n is a positive integer). Show that the set of all subsets of X contains 2^n elements.
- 4
 - a Use a Venn diagram to show that $(A \cup B)' = A' \cap B'$.
 - b Prove that $[(A' \cup B) \cap (A \cup B')] = (A \cap B)' \cap (A \cup B)$.
- 5 The difference, $A - B$, of two sets A and B is defined as the set of all elements of A which do not belong to B .
 - a Show by means of a Venn diagram that $A - B = A \cap B'$.
 - b Using set algebra, prove that $A - (B \cup C) = (A - B) \cap (A - C)$.
- 6 Use Venn diagrams to show that
 - a $A \cup (B \cap A') = A \cup B'$
 - b $((A \cap B)' \cup B)' = \emptyset$.
- 7 Let A and B be subsets of the set U and let $C = A \cap B$, $D = A' \cup B$ and $E = A \cup B$.
 - a Draw separate Venn diagrams to represent the sets C , D and E .
 - b Using De Morgan's laws, show that $A = D' \cup C$.
 - c Prove that $B = D \cap E$.
- 8 Prove for sets A , B and C that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
- 9 For each $n \in \mathbb{Z}^+$, a subset of \mathbb{Z}^+ is defined by $S_n = \{x \in \mathbb{Z}^+ \mid n \text{ divides } x\}$.
 - a Express in simplest terms the membership of the following sets:
 - i S_1
 - ii S_2'
 - iii $S_2 \cap S_3$
 - iv $S_6 \setminus S_3$
 - b Prove that $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.
- 10 Prove that $(A \cup B) \setminus (A \cap C) = A \cap (B \setminus C)$ where A , B and C are three subsets of the universal set U .

Questions 1–10 © International Baccalaureate Organization



Relations and Functions

Please note:

The syllabus removed matrix examples from this option. Hence, they will not appear on exam papers. However, we will still use matrices in this book as examples to deepen your understanding of several concepts. Some questions (from old exam papers) may still contain matrices. These questions can be omitted if your teacher chooses to do so.

2.1 Relations

The Cartesian product

Definition 1

Let A and B be two subsets of U . The **Cartesian product** of A and B , denoted as $A \times B$, is defined by

$$A \times B = \{(x, y) | x \in A \text{ and } y \in B\}.$$

From the definition above, we can interpret the Cartesian product as the set of all *ordered* pairs whose first component is a member of A and second component is a member of B .

Example 1

Let $A = \{a, b\}$ and $B = \{1, 2, 3\}$. Find $A \times B$, $B \times A$, and $A \times A$.

Solution

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

$$B \times A = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$

Notice here that $A \times B \neq B \times A$.

$$A \times A = \{(a, a), (a, b), (b, a), (b, b)\}$$

Often, we are interested in the Cartesian product of a set with itself (as in the last question in Example 1) $A \times A$, which will be denoted by A^2 . In general, we use A^n to include all ordered n -tuples (x_1, x_2, \dots, x_n) of members of set A .

Note: You may have seen by now that the Cartesian plane you use in graphing is called \mathbb{R}^2 since it is a Cartesian product of \mathbb{R} with itself:

$$\mathbb{R}^2 = \{(x, y) | x, y \in \mathbb{R}\}$$



The 3D space coordinate system is also known as \mathbb{R}^3 :

$$\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$$

Example 2

A, B and C are subsets of U . Show that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Solution

Since this is a Cartesian product, then elements of $A \times (B \cup C)$ are of the form (x, y) .

Let $(x, y) \in A \times (B \cup C)$, then

$$x \in A \text{ and } y \in (B \cup C) \Rightarrow y \in B \text{ or } y \in C.$$

We know that $x \in A$ regardless of y , so, when $y \in B$, then we have $x \in A$ and $y \in B$, i.e. $(x, y) \in (A \times B)$; or when $y \in C$, then we have $x \in A$ and $y \in C$, i.e. $(x, y) \in (A \times C)$.

Thus, $(x, y) \in (A \times B)$ or $(x, y) \in (A \times C)$, and hence $(x, y) \in ((A \times B) \cup (A \times C))$. This proves that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.

Let $(x, y) \in ((A \times B) \cup (A \times C))$, then

$$(x, y) \in (A \times B) \text{ or } (x, y) \in (A \times C); \text{ hence,}$$

when $(x, y) \in (A \times B)$ then $x \in A$ and $y \in B$, or when $(x, y) \in (A \times C)$ then $x \in A$ and $y \in C$.

This in turn means that $x \in A$ and $y \in B$ or $y \in C$, and hence $y \in (B \cup C)$, thus

$$(x, y) \in A \times (B \cup C) \text{ and hence } (A \times B) \cup (A \times C) \subseteq A \times (B \cup C).$$

Therefore, $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Relations

If A and B are sets, as we defined earlier, the Cartesian product of A and B is the set

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}.$$

There are occasions when we are interested in only a part of $A \times B$. Take, for example, the set A to be the set of last year's HL maths students at your school,

$$A = \{\text{Marco, Roberto, Franz, George, Jin, Mara, ...}\},$$

and B the set of natural numbers \mathbb{N} . We may be interested in the scores that these students have on their IB exam, so we are interested in

$$\mathcal{R} = \{(x, y) \mid x \in A, y \in B, \text{ student } x \text{ has score } y\}.$$

For example, (Roberto, 7), (Franz, 3) and (Mara, 5) are elements of \mathcal{R} .

Generally, a relation is defined by a rule or description rather than by listing its ordered pairs.

Definition 2

Given two sets M and N , a relation \mathcal{R} from M to N is a subset of $M \times N$.



In some sources, M is called the **domain** of the relation and N is the **range**.



Sometimes \mathcal{R} is called a binary relation. Also, if we are given n sets M_1, M_2, \dots, M_n , then an n -ary relation on $M_1 \times M_2 \times \dots \times M_n$ is a subset of the Cartesian product $M_1 \times M_2 \times \dots \times M_n$. If $M = N$ then \mathcal{R} is a relation on set M and of course is a subset of $M \times M$.

Notation

There are several ways of writing a relation, two of which we state here.

- If \mathcal{R} is a relation, then the following are equivalent descriptions:
 $(x, y) \in \mathcal{R} \leftrightarrow x\mathcal{R}y$.

Let $A = \{3, 4, 5\}$ and $B = \{2, 4, 6\}$. Let \mathcal{R} , a relation from A to B , be defined by the rule:

$$x\mathcal{R}y \leftrightarrow x + y \text{ is a multiple of } 3.$$

We can write $3\mathcal{R}6$, or equivalently $(3, 6) \in \mathcal{R}$; $4\mathcal{R}2$, or equivalently $(4, 2) \in \mathcal{R}$, but we *cannot* write $(5, 2)$, $4\mathcal{R}6$, $(4\mathcal{R}6)$, etc.

- Let $\mathcal{T} = \left\{ (x, y) \mid x, y \in \mathbb{Z}^+, \frac{x}{y} \in \mathbb{Z}^+ \right\}$. This is a relation from \mathbb{Z}^+ to \mathbb{Z}^+ .
 This can also be written as $x\mathcal{T}y$. So $15\mathcal{T}3$, but $3\not\mathcal{T}15$.

Equivalence relations

Our major goal in this part is to discover particular properties of relations on a set. Thus, all the work in this part will involve subsets of $M \times M$ for some set M .

- $\mathcal{S} = \{(a, b) \in \mathbb{N}^2 \mid ab \geq 0\}$ is a reflexive relation on \mathbb{N} since $aa = a^2 \geq 0$ for any number $a \in \mathbb{N}$.
- $\mathcal{W} = \left\{ (x, y) \mid x, y \in (\mathbb{Z} \setminus \{0\}), \text{ and } \frac{x}{y} \in \mathbb{Z} \right\}$ is a reflexive relation since $\frac{x}{x} = 1 \in \mathbb{Z}$ for any non-zero integer x .
- $\mathcal{F} = \{(x, y) \mid x, y \in \mathbb{R} \text{ and } x - y > 2\}$ is not reflexive since $x - x = 0 \not> 2$.

Definition 4

A relation \mathcal{R} on a set M is **symmetric** if and only if for all $x, y \in M$,

$$(x, y) \in \mathcal{R} \Rightarrow (y, x) \in \mathcal{R},$$

or equivalently

$$x\mathcal{R}y \Rightarrow y\mathcal{R}x \text{ for all } x, y \in M.$$

- $\mathcal{S} = \{(a, b) \in \mathbb{N}^2 \mid ab \geq 0\}$ is symmetric since $ab \geq 0 \Leftrightarrow a \geq 0 \text{ and } b \geq 0$, or $a \leq 0 \text{ and } b \leq 0 \Leftrightarrow ba \geq 0$, i.e. $a\mathcal{S}b \Rightarrow b\mathcal{S}a$, or $(a, b) \in \mathcal{S} \Rightarrow (b, a) \in \mathcal{S}$.
- $\mathcal{P} = \{(a, b) \in \mathbb{R}^2 \mid a - b = 0\}$ is symmetric since $a - b = 0 \Rightarrow b - a = 0$, i.e. $(a, b) \in \mathcal{P} \Rightarrow (b, a) \in \mathcal{P}$ or $a\mathcal{P}b \Rightarrow b\mathcal{P}a$.

Definition 3

A relation \mathcal{R} on a set M is

reflexive if and only if $(x, x) \in \mathcal{R}$,
 or equivalently $x\mathcal{R}x$ for all $x \in M$.



- $\mathcal{R} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 4\}$ is symmetric since addition over the set of real numbers is commutative, then $x^2 + y^2 = 4 \Rightarrow y^2 + x^2 = 4$ which implies that $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
- $\rho = \{(x, y) \in \mathbb{R}^2 \mid x^2 - y^2 = 4\}$ is not symmetric since $x\rho y \Rightarrow x^2 - y^2 = 4 \Rightarrow y^2 - x^2 = -4 \not\Rightarrow y\rho x$; equivalently we may also write ' $\Rightarrow y\not\rho x$ '.

Example 3

A relation \mathcal{P} on a set $M = \{0, 1, 2, 3, 4\}$ is given below. Determine whether it is reflexive or symmetric.

$$\mathcal{P} = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 1), (2, 2), (2, 3), (3, 3), (4, 3), (4, 4)\}$$

Solution

\mathcal{P} is reflexive since for every element x in M , $x\mathcal{P}x - (0, 0), (1, 1)$, etc.

\mathcal{P} is not symmetric since there is at least one case where $x\mathcal{P}y$ but $y\not\mathcal{P}x - (2, 3) \in \mathcal{P}$ but $(3, 2) \notin \mathcal{P}$.

Definition 5

A relation \mathcal{R} on a set M is **antisymmetric** if and only if for all $x, y \in M$,

$$(x, y) \in \mathcal{R} \text{ and } (y, x) \in \mathcal{R} \Rightarrow x = y,$$

or equivalently,

$$\text{for all } x, y \in M, x\mathcal{R}y \text{ and } y\mathcal{R}x \Rightarrow x = y.$$

A relation $\rho = \{(x, y) \in \mathbb{R}^2 \mid x \geq y\}$ is antisymmetric since

$(x, y) \in \rho \Rightarrow x \geq y$ and $(y, x) \in \rho \Rightarrow y \geq x$, which can only be true if $x = y$.

Example 4

Is the relation \mathcal{P} in Example 3 antisymmetric?

Solution

We have $(0, 1) \in \mathcal{P}$ and $(1, 0) \in \mathcal{P}$, but obviously $0 \neq 1$, so the relation is not antisymmetric.



Notice here that this relation is not symmetric and is not antisymmetric. This is to show that antisymmetric does not mean 'not symmetric'.

Definition 6

A relation \mathcal{R} on a set M is **transitive** if and only if for all $x, y, z \in M$,

$$(x, y) \in \mathcal{R} \text{ and } (y, z) \in \mathcal{R} \Rightarrow (x, z) \in \mathcal{R} \text{ or equivalently,}$$

$$\text{for all } x, y, z \in M, x\mathcal{R}y \text{ and } y\mathcal{R}z \Rightarrow x\mathcal{R}z.$$

- A relation $\mathcal{T} = \{(x, y) \in \mathbb{R}^2 \mid x \geq y\}$ is transitive since
 $(x, y) \in \mathcal{T} \Rightarrow x \geq y$ and $(y, z) \in \mathcal{T} \Rightarrow y \geq z$, which leads to the conclusion
 that $x \geq z$, i.e. $(x, z) \in \mathcal{T}$.

Example 5

M is the power set of a set A . Consider the following relation on this set:

$$\mathcal{S} = \{(X, Y) \mid X, Y \in M, \text{ and } X \subseteq Y\}.$$

Is \mathcal{S} reflexive, symmetric, antisymmetric, or transitive?

Solution

Since $(X, X) \in \mathcal{S}$, i.e. $X \subseteq X$, then \mathcal{S} is reflexive.

Since $(X, Y) \in \mathcal{S} \Rightarrow X \subseteq Y \not\Rightarrow Y \subseteq X$, then \mathcal{S} is not symmetric.

Since $(X, Y) \in \mathcal{S}$ and $(Y, X) \in \mathcal{S} \Rightarrow X \subseteq Y$ and $Y \subseteq X \Rightarrow X = Y$, then \mathcal{S} is antisymmetric.

Since $(X, Y) \in \mathcal{S}$ and $(Y, Z) \in \mathcal{S} \Rightarrow X \subseteq Y$ and $Y \subseteq Z \Rightarrow X \subseteq Z$, which means that $(X, Z) \in \mathcal{S}$, then \mathcal{S} is transitive.

Example 6

Consider the relation $\mathcal{W} = \{(x, y) \mid x, y \in (\mathbb{Z} \setminus \{0\}), \text{ and } \frac{x}{y} \in \mathbb{Z}\}$. Is this relation reflexive, symmetric, or transitive?

Solution

It has been shown on page 1236 that \mathcal{W} is reflexive.

$(6, 3) \in \mathcal{W}$ because $\frac{6}{3} = 2 \in \mathbb{Z} \setminus \{0\}$, but $\frac{3}{6} = \frac{1}{2} \notin \mathbb{Z} \setminus \{0\} \Rightarrow (3, 6) \notin \mathcal{W}$, so

\mathcal{W} is not symmetric.

$(x, y) \in \mathcal{W}$ and $(y, z) \in \mathcal{W} \Rightarrow \frac{x}{y} = n$ and $\frac{y}{z} = m$, where m and n are non-negative integers, thus

$\frac{x}{z} = \frac{x}{y} \cdot \frac{y}{z} = nm$ is also a non-negative integer and hence $(x, z) \in \mathcal{W}$ and

\mathcal{W} is therefore transitive.

Example 7

Consider the relation \mathcal{P} on a set $M = \{1, 2, 3, 4\}$ given below. Determine whether it is transitive.

$$\mathcal{P} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 3), (3, 3)\}$$

Solution

\mathcal{P} is not transitive since $(2, 1)$ and $(1, 2)$ belong to \mathcal{P} but $(2, 2)$ does not.

Definition 7

A relation \mathcal{R} on a set M is called an **equivalence** relation if it is reflexive, symmetric and transitive.

Note: To prove a relation \mathcal{R} is an equivalence relation, you will need to prove \mathcal{R} to be

Reflexive: $x\mathcal{R}x$ for all $x \in M$.

Symmetric: for any $x, y \in M$, and if $x\mathcal{R}y$, then $y\mathcal{R}x$.

Transitive: for any $x, y, z \in M$, if $x\mathcal{R}y$ and $y\mathcal{R}z$, then $x\mathcal{R}z$.

Consider the following relation over the set of integers, \mathbb{Z} :

$\mathcal{R} = \{(x, y) \in \mathbb{Z}^2 \mid x - y \text{ is a multiple of } 5\}$, i.e. $x\mathcal{R}y \Rightarrow x - y = 5k$ where $k \in \mathbb{Z}$.

\mathcal{R} is reflexive since $x\mathcal{R}x \Rightarrow x - x = 0$, which is a multiple of 5.

\mathcal{R} is symmetric since $x\mathcal{R}y \Rightarrow x - y = 5k \Rightarrow y - x = -5k$, which is also a multiple of 5.

\mathcal{R} is transitive since $x\mathcal{R}y$ and $y\mathcal{R}z \Rightarrow x - y = 5k_1$ and $y - z = 5k_2$
 $\Rightarrow x - z = (x - y) + (y - z) = 5(k_1 + k_2)$ is also a multiple of 5.

Therefore, \mathcal{R} is an equivalence relation.

Example 8

Consider the relation $\mathcal{W} = \left\{ (x, y) \mid x, y \in (\mathbb{Z} \setminus \{0\}), \text{ and } \frac{x}{y} \in \mathbb{Z} \right\}$. Is \mathcal{W} an equivalence relation?

Solution

We have shown above (Example 6) that \mathcal{W} is reflexive and transitive, but not symmetric, and hence it is not an equivalence relation.

Example 9

Consider the set of triangles, \mathcal{T} , in a plane and define a relation, denoted by \approx , on this set by

$\approx = \{(X, Y) \in \mathcal{T}^2 \mid X \text{ is similar to } Y\}$. Is \approx an equivalence relation?

Solution

To answer the question you need to recall the definition of similar triangles. One definition states that two triangles are similar if and only if their angles are congruent.

$X \approx X$ is obvious since the angles of a triangle are congruent to themselves.

If $X \approx Y$, then the angles of Y are naturally congruent to those of X , and hence $Y \approx X$.

If $X \approx Y$ and $Y \approx Z$, then the angles of X are also congruent to those of Z , and hence $X \approx Z$.

Therefore, \approx is an equivalence relation.

Example 10 (Extremely important)

We define the relation called **congruence modulo 5**, denoted by \equiv , on the set of integers \mathbb{Z} by

$$a \equiv b \pmod{5} \text{ if and only if } 5 \text{ divides } (a - b), \text{ i.e. } 5 \mid (a - b).$$

Is \equiv an equivalence relation?

Solution

Reflexive: $a \equiv a \pmod{5}$ since $5 \mid (a - a)$, i.e. since $a - a = 0$ is a multiple of 5.

Symmetric: If $a \equiv b \pmod{5}$, then $(a - b)$ is a multiple of 5, i.e. $a - b = 5k$, where $k \in \mathbb{Z}$, thus $b - a = 5(-k)$. This in turn means that $b - a$ is a multiple of 5 since $-k \in \mathbb{Z}$, and hence $5 \mid (b - a)$ and $b \equiv a \pmod{5}$.

Transitive: If $a \equiv b \pmod{5}$ and $b \equiv c \pmod{5}$, then $5 \mid (a - b)$ and $5 \mid (b - c)$, thus $a - b = 5k_1$ and $b - c = 5k_2$. Adding these two equations gives us $a - b + b - c = a - c = 5k_1 + 5k_2 = 5(k_1 + k_2)$, and hence $5 \mid (a - c)$, and therefore $a \equiv c \pmod{5}$.

Therefore, we can conclude that congruence modulo 5 is an equivalence relation over the set of integers.

Equivalence classes

Example 10 is an instance of congruence modulo m , where m is any integer. A full discussion of congruence modulo m will appear later. Because of its significance, some important characteristics are worth studying. One question we can ask is: If we claim that $x \equiv a \pmod{5}$ for a given integer a , is x a unique number or are there several such numbers?

Let us take $a = 0$, then the relation is $x \equiv 0 \pmod{5}$. This implies that x can be 5, 10, ..., $5k$ for an integer k .

This set of numbers $\{\dots, -5, 0, 5, 10, \dots\}$ is called the **congruence class of 0 modulo 5**, and is denoted by $[0]$. So,

$p \mid q$ means that q is a multiple of p .



There are other ways of defining congruence, and we will discuss them later in this publication.





$$[0] = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{5}\} = \{x \in \mathbb{Z} \mid 5 \mid (x - 0)\} = \{x \in \mathbb{Z} \mid 5 \mid x\}$$

$$= \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 5\} = \{\dots, -5, 0, 5, 10, \dots\}.$$

Let us now take $a = 1$, then

$$[1] = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{5}\} = \{x \in \mathbb{Z} \mid 5 \mid (x - 1)\}$$

$$= \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 5 \text{ plus } 1\} = \{\dots, -9, -4, 1, 6, 11, \dots\}.$$

Similarly,

$$[2] = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{5}\} = \{x \in \mathbb{Z} \mid 5 \mid (x - 2)\}$$

$$= \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 5 \text{ plus } 2\} = \{\dots, -8, -3, 2, 7, 12, \dots\}$$

$$[3] = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{5}\} = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 5 \text{ plus } 3\}$$

$$= \{\dots, -7, -2, 3, 8, 13, \dots\}$$

$$[4] = \{x \in \mathbb{Z} \mid x \equiv 4 \pmod{5}\} = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 5 \text{ plus } 4\}$$

$$= \{\dots, -6, -1, 4, 9, 14, \dots\}$$

$$[5] = \{x \in \mathbb{Z} \mid x \equiv 5 \pmod{5}\} = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 5 \text{ plus } 5\}$$

$$= \{\dots, -5, 0, 5, 10, 15, \dots\}.$$

We notice here that there is no need for $[5]$ and we discover that $[0] = [5]$. Such classes like $[0]$, $[1]$, etc., are in general called **equivalence classes**.

Definition 8

If \mathcal{R} is an equivalence relation on a set A for $a \in A$, the set $[a] = \{x \in A \mid x \mathcal{R} a\}$ of elements of A which are equivalent to a is called **the equivalence class of a with respect to \mathcal{R}** , or **the \mathcal{R} -equivalence class of a** .

Example 11

Let \mathcal{R} be the relation on set \mathbb{Z} defined by

$$\mathcal{R} = \{(a, b) \in \mathbb{Z}^2 \mid a - b \text{ is even}\}.$$

Show that \mathcal{R} is an equivalence relation and find the equivalence classes.

Solution

Reflexive: $a \mathcal{R} a$, since $a - a = 0$ is even.

Symmetric: $a \mathcal{R} b \Rightarrow a - b \text{ is even} \Rightarrow b - a \text{ is even} \Rightarrow b \mathcal{R} a$.

Transitive: $a \mathcal{R} b \Rightarrow a - b \text{ is even}, b \mathcal{R} c \Rightarrow b - c \text{ is even}$
 $\Rightarrow a - b + b - c = a - c \text{ is even} \Rightarrow a \mathcal{R} c$.

The equivalence classes are

$$[0] = \{\dots, -2, 0, 2, \dots\} \text{ and } [1] = \{\dots, -3, -1, 1, 3, \dots\}.$$

Example 12

Let \mathcal{D} be the relation on the set of all differentiable functions from \mathbb{R} to \mathbb{R} defined by

$$\mathcal{D} = \{(f, g) \in \mathbb{R}^2 \mid f'(x) = g'(x) \text{ for all } x \in \mathbb{R}\}.$$

Show that \mathcal{D} is an equivalence relation and describe the equivalence classes.

Solution

Reflexive: $f\mathcal{D}f$ since $f'(x) = f'(x)$.

Symmetric: If $f\mathcal{D}g$, then $f'(x) = g'(x) \Rightarrow g'(x) = f'(x) \Rightarrow g\mathcal{D}f$.

Transitive: If $f\mathcal{D}g$ and $g\mathcal{D}h$, then

$$\begin{aligned} f'(x) &= g'(x) \text{ and } g'(x) = h'(x) \Rightarrow f'(x) = h'(x) \\ &\Rightarrow f\mathcal{D}h. \end{aligned}$$

The equivalence class for a function f , $[f]$, is the set of all functions that differ from f by a constant, i.e. $[f] = \{g \in \mathbb{R} \mid g = f + C\}$, i.e. all anti-derivatives of $f'(x)$.

For example, $[x^3] = \{x^3 + C, \text{ where } C \text{ is an arbitrary real constant}\}$.

Theorem 1

If \mathcal{R} is an equivalence relation on a set A , then any two equivalence classes $[a]$ and $[b]$ are either disjoint, or if they have any element in common then they must be equal. Stated differently, all three statements below are equivalent.

$$1 \quad a\mathcal{R}b \qquad 2 \quad [a] = [b] \qquad 3 \quad [a] \cap [b] \neq \emptyset$$

Proof

- 1 If $a\mathcal{R}b$, now let $c \in [a] \Rightarrow c\mathcal{R}a$, but $a\mathcal{R}b$, and by transitive property, $c\mathcal{R}b \Rightarrow c \in [b]$, and hence $[a] \subseteq [b]$. Similarly, $[b] \subseteq [a]$, and therefore $[a] = [b]$. This means that (1) implies (2).
- 2 If $[a] = [b]$, then obviously $[a] \cap [b] \neq \emptyset$ as $[a]$ is non-empty because it is reflexive. This means that (2) implies (3).
- 3 If $[a] \cap [b] \neq \emptyset$, then there is at least an element $c \in [a] \cap [b]$. Now, $c \in [a] \Rightarrow c\mathcal{R}a$, and $c \in [b] \Rightarrow c\mathcal{R}b$, and hence by using symmetric and transitive properties we get $a\mathcal{R}b$. This means that (3) implies (1).

Since (1) implies (2), (2) implies (3), and (3) implies (1), the statements must be equivalent.

In the follow-up discussion to Example 10, we observed that $[5] = [0]$. One reason is that $0\mathcal{R}5$.

We are now in a position to investigate how an equivalence relation on a set A 'induces' a **partition** of set A .

The theorem right leads us to the conclusion that $[a] \neq [b]$ if and only if $[a] \cap [b] = \emptyset$, i.e. $[a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset$, and $[a] \cap [b] = \emptyset \Rightarrow [a] \neq [b]$.



Definition 9

A **partition** of a set A is a collection of non-empty, disjoint subsets of A that are mutually exhaustive.

This means that the union of these subsets is the set A itself. A sample partition of a set A is shown below.

In general symbolic terms, a partition of a set A is a collection of n non-empty subsets of A such that

$$A_i \cap A_j = \emptyset, \text{ for all } i \neq j, \text{ and } \bigcup_{i=1}^n A_i = A.$$

The last definition leads us to a very important theorem concerning equivalence relationships. We know that if a relation \mathcal{R} is defined over a set A then the equivalence classes $[a_i]$ defined have the following properties:

$$[a_i] \neq \emptyset$$

$$\bigcup_{i=1}^n [a_i] = A$$

$$[a_i] \cap [a_j] = \emptyset, \text{ for all } i \neq j.$$

This shows us that the equivalence relation created a partition of the set A whose subsets are the equivalence classes.

Theorem 2

If \mathcal{R} is an equivalence relation on a set A , then the equivalence classes of \mathcal{R} induce a partition of set A .

Proof

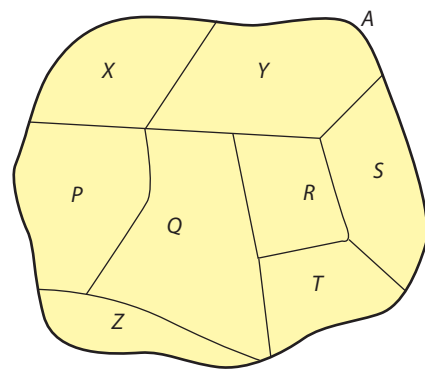
We need to prove two statements.

- 1 The equivalence classes form a partition of set A , and
 - 2 A partition of set A forms an equivalence relation on set A .
- 1 This has been shown above depending on Theorem 1 and the definition of an equivalence class.
 - 2 Suppose you have a partition containing n subsets of set A : $\{A_i \mid A_i \subseteq A \text{ for all } i \leq n\}$. Define a relation \mathcal{R} on A such that $x\mathcal{R}y$ if x and y belong to the same subset of A .

\mathcal{R} is reflexive since $x\mathcal{R}x$ for every $x \in A$, since x is in the same subset as itself!

\mathcal{R} is symmetric since if $x\mathcal{R}y$ then x and y belong to the same subset of A . In that case obviously y and x belong to the same subset of A .

\mathcal{R} is transitive since $x\mathcal{R}y$ and $y\mathcal{R}z$ imply that x and y belong to the same subset, say M , and y and z belong to the same subset N , and since y belongs to both subsets M and N , which are members of a partition and cannot have any element in common unless they are equal, then $M = N$ and therefore x and z are in the same subset.



Therefore, we have shown that the equivalence classes form a partition, and a partition generates an equivalence relation and hence we can say that equivalence classes of \mathcal{R} induce a partition of set A .

Example 13

Consider the congruence classes modulo 5 we generated in Example 10. Show that they form a partition of the set of integers.

Solution

Recall that the classes so created are: $[0]$, $[1]$, $[2]$, $[3]$ and $[4]$.

It is clear that $[a] \cap [b] = \emptyset$, unless $[a] = [b]$.

$$[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}$$

and hence the set of congruence classes mod 5 creates a partition of \mathbb{Z} .

Example 14

Consider the set $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and the following set $S = \{\{1, 4\}, \{6, 8, 2\}, \{3, 5\}, \{7\}\}$. Show that S is a partition of A .

Solution

Every element of S is non-empty.

All elements are mutually disjoint.

The union of all elements is A .

Therefore S is a partition of A .

Congruence (General)

So far you have seen some examples involving congruence for specific values. In this section we will discuss congruence in more general terms. This topic is important for this option as well as for the Discrete Mathematics option.

Definition 10

Let m be a positive integer. If a and b are integers, we say that a is congruent to b modulo m if $m \mid (a - b)$.

If a is congruent to b modulo m , then we write $a \equiv b \pmod{m}$. If a is not congruent to b modulo m , then we write $a \not\equiv b \pmod{m}$. The integer m is called the **modulus of congruence**.

- We have $24 \equiv 4 \pmod{5}$, since $5 \mid (24 - 4)$. Similarly $5 \equiv -11 \pmod{8}$, since $8 \mid (5 - (-11))$. On the other hand, $4 \not\equiv 17 \pmod{2}$ since $(4 - 17)$ is not divisible by 2.



Note: If $a, b \in \mathbb{Z}$, then $a \equiv b \pmod{m}$ for some positive integer m if and only if there exists an integer k such that $a = b + km$, since $m \mid (a - b)$ if and only if $a - b = km$ for some $k \in \mathbb{Z}$. So, we can summarize this result by stating:

Given a positive integer m and an integer b , integers which are congruent to b modulo m are obtained by adding an integer multiple of m to b .

As an illustration, let $m = 2$ and $b = 0$. Then the integers congruent to 0 modulo 2 are given by $a = 0 + 2k$, $k \in \mathbb{Z}$, i.e. $\{\dots, -4, -2, 0, 2, 4, \dots\}$. If $b = 1$, then the collection of all integers congruent to 1 are $\{\dots, -3, -1, 1, 3, \dots\}$. We can observe that these two classes of integers are distinct and each one is associated to a remainder when we divide an arbitrary integer n by 2.

This discussion leads us to the following important theorem which explains the structure of congruence classes slightly more fully than we have done so far.

Theorem 3

If $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when we divide them by m .

Proof

(\Rightarrow) Let $a \equiv b \pmod{m}$. Then, by definition $m \mid (a - b)$.

Now, by the division algorithm, if we divide a by m , then we can find q_1 and r_1 such that

$$a = m \cdot q_1 + r_1, 0 \leq r_1 < m$$

and similarly, if we divide b by m , then we can find q_2 and r_2 such that

$$b = m \cdot q_2 + r_2, 0 \leq r_2 < m.$$

So, we now have

$$a - b = (m \cdot q_1 + r_1) - (m \cdot q_2 + r_2) = m(q_1 - q_2) + (r_1 - r_2).$$

However, $m \mid (a - b)$, and so m must divide the right-hand side, $m(q_1 - q_2) + (r_1 - r_2)$.

This leads to the fact that m must divide $(r_1 - r_2)$ too. But

$$0 \leq r_1 < m \text{ and } 0 \leq r_2 < m, \text{ and so } (r_1 - r_2) \text{ cannot divide } m \text{ unless } r_1 - r_2 = 0, \text{ i.e. } r_1 = r_2.$$

Therefore, a and b leave the same remainder when we divide them by m .

(\Leftarrow) Let a and b leave the same remainder when we divide them by m .

Then we have

$$a = m \cdot q_1 + r \text{ and } b = m \cdot q_2 + r, \text{ and consequently}$$

$$a - b = m(q_1 - q_2), \text{ which means that } m \mid (a - b) \text{ and therefore } a \equiv b \pmod{m}.$$

The two previous theorems enable us to generalize the structure of congruence classes modulo m .

Since any two integers that leave the same remainder when divided by m , then the remainder itself will represent the equivalence class. This is so because if a leaves a remainder r when divided by m , then as we showed before:

$$a = m \cdot q_1 + r \Rightarrow a - r = m \cdot q_1 \\ \Rightarrow m \mid (a - r) \Rightarrow a \equiv r \pmod{m}.$$

Also, since $r < m$, then it takes on all the values $\{0, 1, 2, 3, \dots, m - 1\}$, and hence the congruence classes modulo m are $[0], [1], \dots, [m - 1]$.

In some books, these classes are also called **residue classes mod m** .

Theorem 4

Let $m \in \mathbb{Z}^+$. Then congruence modulo m is an equivalence relation.

Proof

- Reflexive property:** $a \equiv a \pmod{m}$ since $m \mid (a - a)$ for all $a \in \mathbb{Z}$.
- Symmetric property:** Suppose $a \equiv b \pmod{m}$. Then there is an integer k such that $a - b = km$. Hence, $b - a = (-k)m$ and $m \mid (b - a)$ [$-k$ is also an integer]. Thus $b \equiv a \pmod{m}$.
- Transitive property:** If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m \mid (a - b)$ and $m \mid (b - c)$. Hence, $m \mid ((a - b) + (b - c))$, i.e. $m \mid (a - c)$ and $a \equiv c \pmod{m}$.

Example 15

List the congruence classes mod 7.

Solution

Since the possible remainders when dividing by 7 are 0, 1, 2, ..., 6, then the congruence classes are:

$$[0] = \{\dots, -7, 0, 7, 14, \dots\}$$

$$[1] = \{\dots, -6, 1, 8, 15, \dots\}$$

\vdots

$$[6] = \{\dots, -1, 6, 13, 20, \dots\}$$

If f is a function from A to B , we also write $f: A \rightarrow B$; if $x \in A$, we also write $f: x \mapsto y$, where $y \in B$. (Notice the difference in symbols \rightarrow between sets and \mapsto between elements!)

In many instances, a function is also called a mapping (or simply map) from A to B . So, we say f is a mapping from A to B , or f maps x to $y = f(x)$.

2.2 Functions

The **function** concept has been discussed comprehensively in Chapter 2 of the HL book. We will present you here with a brief review of what you have seen there and a small number of bits and pieces that are not compulsory in the core part but essential for this option.

Definition 11

If A and B are non-empty sets, a **function from A to B** is a relation f from A to B such that for all $x \in A$, there is a *unique* element $y \in B$ with $(x, y) \in f$.

The set A is the **domain** of the function f and the set B is the **codomain** of f . If $(x, y) \in f$, we write $y = f(x)$ and say that y is the **image** of x under f or the value of f at x , and we also say that x is **mapped** to $y = f(x)$ by the function f . Several other notations are used such as: x is called the **input**, or **preimage**, and y is the **output**.

Definition 12

If f is a function from A to B , then the **subset** of B defined by

$$\{f(a) \mid a \in A\}$$

is called the **image** of A and is denoted by $f(A)$. This is to say that the image of A is the subset of B that consists of the images of all elements of A .

Additionally, if $f(A) = B$, then B is called the **range** of the function f . That is, if every element of B is an image of some element in A , then B is the range of f .

Example 16

Decide whether each of the following relations is a function. If the relation is a function, state its codomain and range.

- a) $A = \{1, 2, 3\}$, $B = \{3, 4, 5, 6\}$, and $g = \{(1, 5), (2, 4), (3, 3)\}$
- b) $A = \{1, 2, 3\}$, $B = \{3, 4, 5, 6\}$, and $h = \{(1, 5), (2, 4), (3, 3), (2, 6)\}$
- c) $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2 + 1$
- d) $g: \mathbb{R} \rightarrow [1, \infty[$ defined by $g(x) = x^2 + 1$

Solution

- a) This is a function. Codomain is $\{3, 4, 5, 6\}$ and range is $\{3, 4, 5\}$.
- b) This is not a function as 2 does not have a *unique* image.
- c) This is a function. Codomain is \mathbb{R} and range is $[1, \infty[$.
- d) This is a function. Codomain = range = $[1, \infty[$.

Definition 13

A function $f: A \rightarrow B$ is a **surjection** if and only if for every $y \in B$, there is at least an $x \in A$ such that $f(x) = y$.

Example 17

Consider each of the following and decide which of them is surjective.

- a) $A = \{1, 2, 3\}$, $B = \{3, 4, 5, 6\}$, and $g = \{(1, 5), (2, 4), (3, 3)\}$
- b) $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2 + 1$
- c) $g: \mathbb{R} \rightarrow [1, \infty[$ defined by $g(x) = x^2 + 1$



So, the range is always a subset of the codomain: $f(A) \subseteq B$. That is, they are also equal in numerous cases. This is why several mathematicians only talk about range and do not mention codomain.



The function is also called **surjective** or **onto**.

The definition left is equivalent to saying that $f(A) = B$, i.e. the range is equal to the codomain!



Since every element of B must be an image for *at least* an element of A , then the number of elements of A , $n(A) = |A|$ must at least be the same as $n(B)$, i.e. if f is surjective, then $|A| \geq |B|$.

Solution

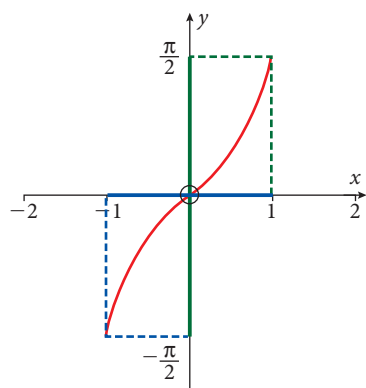
- a) g is not onto since $6 \in B$ but there is no $x \in A$ such that $g(x) = 6$.
- b) f is not surjective, since every $y < 1$ in B does not have an x in A such that $f(x) = y$.
- c) g is a surjection, since the range and codomain are equal.

Example 18

Consider whether the function $[-1, 1] \rightarrow \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ defined by $f(x) = \arcsin x$ is a surjection.

Solution

Take any number $y \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$. By definition, there is a sine value for each angle in the interval $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$, i.e. there is an $x \in [-1, 1]$ such that $\sin y = x$, which implies that $y = \arcsin x$. Thus f is a surjection. You see that from the graph of $f(x) = \arcsin x$ (left) where it is clear that the codomain and range are the same.

**Definition 14**

A function $f: A \rightarrow B$ is an **injection** if and only if for any $x_1, x_2 \in A$, $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$. (Distinct inputs of f produce distinct outputs.)



The function is also called **injective**, **into**, or **1-1 (one-to-one)**.

The above definition is equivalent to saying:

- For any $x_1, x_2 \in A$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. (Contra-positive of the basic definition and the one used frequently to prove functions are 1-1.)
- For every element y of the range $f(A)$ there is *exactly one* $x \in A$ such that $f(x) = y$. (For every output, there is *exactly one* input.)
- For every element y of the codomain there is *at most one* $x \in A$ such that $f(x) = y$. (For every output, there is *at most one* input.)

Note: Since *for every output, there is at most one input*, we can conclude that if f is injective, then every element in A must have an image in B , and hence $n(A) \leq n(B)$ or $|A| \leq |B|$.

Example 19

Consider each of the following and decide which of them is injective.

- a) $A = \{1, 2, 3\}$, $B = \{3, 4, 5, 6\}$, and $g = \{(1, 5), (2, 4), (3, 3)\}$

- b) $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2 + 1$
 c) $g: [0, \infty[\rightarrow [1, \infty[$ defined by $g(x) = x^2 + 1$

Solution

- a) g is an injection since $1, 2, 3 \in A$ all have different images in B .
 b) f is not an injection since $f(-1) = 2 = f(1)$.
 c) g is an injection, since the domain consists of non-negative real numbers only, then
 $f(x_1) = f(x_2) \Rightarrow x_1^2 + 1 = x_2^2 + 1 \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1 = x_2$.

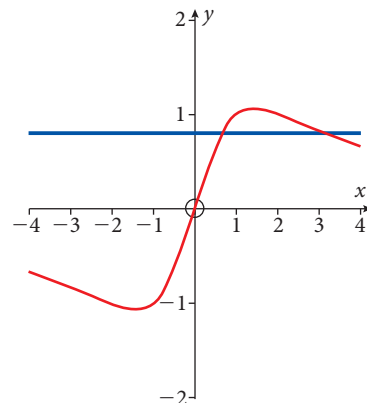
Example 20

Determine whether the function $g(x): \mathbb{R} \rightarrow \mathbb{R}$ defined by $g(x) = \frac{3x}{x^2 + 2}$ is one-to-one.

Solution

$$\begin{aligned} g(x_1) = g(x_2) &\Rightarrow \frac{3x_1}{x_1^2 + 2} = \frac{3x_2}{x_2^2 + 2} \Rightarrow 3x_1(x_2^2 + 2) = 3x_2(x_1^2 + 2) \\ &\Rightarrow 3x_1x_2^2 + 6x_1 - 3x_2x_1^2 - 6x_2 = 0 \\ &\Rightarrow 3x_1(2 - x_1x_2) + 3x_2(x_1x_2 - 2) = 0 \\ &\Rightarrow (2 - x_1x_2)(3x_1 - 3x_2) = 0 \Rightarrow \text{either } x_2 = \frac{2}{x_1} \text{ or } x_1 = x_2 \end{aligned}$$

Since $g(x_1) = g(x_2) \not\Rightarrow x_1 = x_2$, the function is not an injection. Notice how the horizontal line intersects the graph of the function at two points, pointing to the fact that different input values do not necessarily have different output values.



Definition 15

A function $f: A \rightarrow B$ which is an **injection** as well as a **surjection** is a **bijection** from A to B .



The function is also called **1-1 correspondence** between A and B .



Since the bijection is a surjection, then $|A| \geq |B|$, and it is an injection, then $|A| \leq |B|$; therefore in this case we should have $|A| = |B|$.

Example 21

Consider whether the function $[-1, 1] \rightarrow \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ defined by $f(x) = \arcsin x$ is a bijection.

Solution

You have seen in Example 18 that this function is a surjection. We need to show that it is also an injection.

You may recall from your study of trigonometric functions that by restricting the range of this function to the interval $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$, the following result is apparent.

$$f(x_1) = f(x_2) \Rightarrow \arcsin x_1 = \arcsin x_2 \Rightarrow x_1 = x_2$$

Therefore the function is a bijection. You can also observe that it is a bijection by noticing that on its graph (page 1248) the horizontal lines can intersect this function at one point, implying that for every y in the range there is exactly one x in the domain.

Example 22

Consider the function $h: \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $h(n) = n^3 + n$. Is this function a bijection?

Solution

We need to show that the function is injective and surjective.

Injection: Consider $n_1, n_2 \in \mathbb{Z}$

$$\begin{aligned} h(n_1) = h(n_2) &\Rightarrow n_1^3 + n_1 = n_2^3 + n_2 \Rightarrow n_1^3 - n_2^3 = n_2 - n_1 \\ &\Rightarrow (n_1 - n_2)(n_1^2 + n_1n_2 + n_2^2) = n_2 - n_1 \end{aligned}$$

Now, if $n_2 \neq n_1$ then $n_1^2 + n_1n_2 + n_2^2 = -1$. However, we have the following situations:

$n_1n_2 > 0$, then $n_1^2 + n_1n_2 + n_2^2 > 0$, or

$n_1n_2 < 0$, then either $|n_1| > |n_2| \Rightarrow n_1^2 + n_1n_2 > 0$ or

$|n_2| > |n_1| \Rightarrow n_2^2 + n_1n_2 > 0$ and hence, in both cases,

$n_1^2 + n_1n_2 + n_2^2 > 0$; therefore the only option is for $n_2 = n_1$.

Surjection: If h is surjective then given an element m in \mathbb{Z} , there should be n in \mathbb{Z} such that $m = h(n) = n^3 + n$. However, $n^3 + n = n(n^2 + 1)$ is always even whatever the value of n is. Since if n is odd, then $n = 2k + 1$ for some integer k , and $n^3 + n = (2k + 1)(4k^2 + 4k + 2)$, which is the product of an odd number by an even number and is therefore even. Similarly, when n is even, this product is even. This means all the odd numbers in the codomain are not images of numbers in the domain. So, h is not surjective and hence it is not a bijection.

(Take $m = 3$, then it should be possible to write 3 as the sum of an integer and its cube. That is not possible.)

Example 23

Consider the function $h: \mathbb{R} \rightarrow \mathbb{R}$ defined by $h(x) = x^3 + x$. Is this function a bijection?

Solution

We need to show that the function is injective and surjective.

Injection: Similar to Example 22.

Surjection: If h is surjective then given an element y in \mathbb{R} , there should be x in \mathbb{R} such that $y = h(x) = x^3 + x$. From your calculus chapters, you know that this function is increasing, and hence the horizontal line at y will intersect the graph at one point. Hence, there is always an x in the domain to correspond to every y in the codomain, and therefore it is surjective.

Thus h is a bijection from \mathbb{R} to \mathbb{R} .

Example 24

Consider the function $i_A: A \rightarrow A$ defined by $i_A(x) = x$ for every $x \in A$. Show that function i_A is a bijection.

Solution

Since for every $x \in A$ there is an $x \in A$ such that $i_A(x) = x$, then i_A is a surjection.

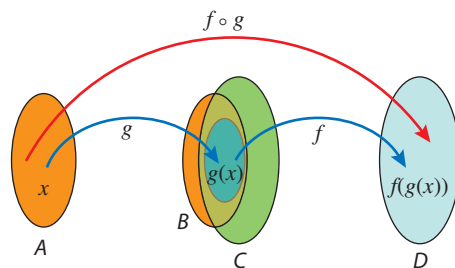
Since $i_A(x_1) = i_A(x_2) \Rightarrow x_1 = x_2$, then i_A is an injection. Thus i_A is a bijection.



i_A is known as the **identity function** on A since it maps every element in A to itself.

Composition of functions

You may recall from the book that if the *outputs* of a function g are used as inputs of a function f , we are forming the **composition** of f with g . For this composition to be possible, the outputs of g must be elements of the domain of f , i.e. the range of g must be a subset of the domain of f .



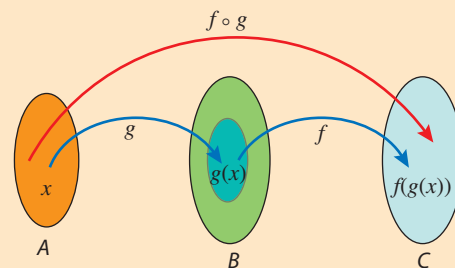
Definition 16

If $g: A \rightarrow B$ and $f: C \rightarrow D$ are functions from their respective domains, A and C , to their respective codomains, B and D respectively, and if $g(A) \subseteq C$, then the **composition** of f and g is the function

$$f \circ g: A \rightarrow D \text{ defined by } f \circ g(x) = f(g(x)).$$



In many cases, the codomain of the first function, B , does not have to be different from the domain of the second function C . Thus, you will have $g: A \rightarrow B$, $f: B \rightarrow C$ and $f \circ g: A \rightarrow C$ for example.



Note: Stated differently, suppose $g: A \rightarrow B$ and $f: C \rightarrow D$ are functions. Then for any $x \in A$, $g(x)$ is a member of $g(A)$ which is a subset of B . If $g(A)$ is also a subset of C , and we apply the function f to this value $g(x)$, the result is $f(g(x))$, a member of D . Thus, taking an arbitrary element x of A , applying the function g , then applying the function f to $g(x)$ is the same as associating a unique element of D with x , i.e. we have created a function $A \rightarrow D$, called the **composition function** of f and g and denoted by $f \circ g$. Notice that with this notation, even though g is applied first, it appears second in the expression $f \circ g$.

Example 25

Let $g: [2, \infty[\rightarrow \mathbb{R}$ defined by $g(x) = x^2 - 2$, and

$f: [1, \infty[\rightarrow \mathbb{R}$ defined by $f(x) = \sqrt{2x + 2}$. If possible, find $f \circ g$. Also, if possible, find $g \circ f$.

Solution

Since the domain of f is $[1, \infty[$, the range of g must be a subset of this set. The range of g is $[2, \infty[$ too, and hence a subset of $[1, \infty[$, so we can find the composition.

$f \circ g: [2, \infty[\rightarrow \mathbb{R}$ defined by

$$f \circ g(x) = f(g(x)) = f(x^2 - 2) = \sqrt{2(x^2 - 2) + 2} = \sqrt{2x^2 - 2}.$$

The range of f is $[2, \infty[$ which is a subset of the domain of g , $[2, \infty[$, and thus

$g \circ f: [1, \infty[\rightarrow \infty[$ defined by

$$g \circ f(x) = g(f(x)) = g(\sqrt{2x + 2}) = (\sqrt{2x + 2})^2 - 2 = 2x.$$

Note: In Example 25, you have seen that

$f \circ g(x) = \sqrt{2x^2 - 2} \neq g \circ f(x) = 2x$, i.e. composition of functions is **not commutative** (it is *not necessarily true* that $f \circ g = g \circ f$).

Example 26

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^2 + 1$ and $g: \mathbb{R} \rightarrow \mathbb{R}$ be defined by $g(x) = |x - 3|$. Find

a) $f \circ g(2)$

b) $g \circ f(2)$

c) $f \circ g(1)$

d) $g \circ f(1)$

Solution

a) $f \circ g(2) = f(12 - 3) = f(1) = 2$

b) $g \circ f(2) = g(2^2 + 1) = g(5) = 2$

c) $f \circ g(1) = f(11 - 3) = f(2) = 5$

d) $g \circ f(1) = g(1^2 + 1) = g(2) = 1$

Notice here how in one case $f \circ g(x) = g \circ f(x)$ and in another $f \circ g(x) \neq g \circ f(x)$.

Example 27

Let $g: A \rightarrow B$ and $f: B \rightarrow C$ be two bijections. Show that $f \circ g$ is also a bijection.

Solution

To show that $f \circ g$ is a bijection, we need to show that it is surjective as well as injective.

Surjection: Recall that $f \circ g: A \rightarrow C$, so we must take a value $z \in C$ and show that it has a preimage $x \in A$ under $f \circ g$. Now, because f is surjective, then there is an element y in B such that $f(y) = z$. Also, because g is surjective, there is an element x in A such that $g(x) = y$. Thus,

$$f \circ g(x) = f(g(x)) = f(y) = z$$

and therefore $f \circ g$ is a surjection.

Injection: Assume that $f \circ g(x_1) = f \circ g(x_2) \Rightarrow f(g(x_1)) = f(g(x_2))$, but f is an injection, so

$$g(x_1) = g(x_2). \text{ Now, } g \text{ is also an injection, and hence}$$

$$g(x_1) = g(x_2) \Rightarrow x_1 = x_2. \text{ Therefore,}$$

$$f \circ g(x_1) = f \circ g(x_2) \Rightarrow x_1 = x_2, \text{ and } f \circ g \text{ is an injection.}$$

The result follows.



Composition of functions is an associative operation.

That is, given $h: A \rightarrow B$, $g: B \rightarrow C$, and $f: C \rightarrow D$, then

$(f \circ g) \circ h = f \circ (g \circ h)$. To show that this is true, we can consider any element x in the domain of the composition, which is A , then

$$(f \circ g) \circ h(x) = (f \circ g)(h(x)) = f(g(h(x))) \text{ by definition of composition.}$$

Also,

$$f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x))) \text{ by definition too.}$$

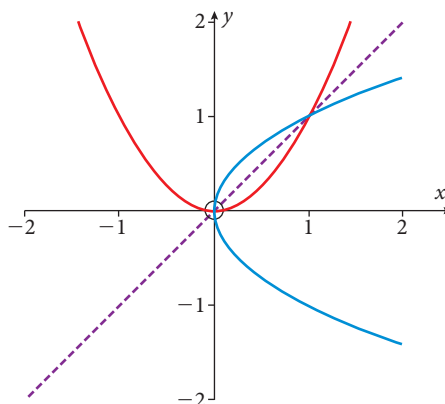
Therefore, $(f \circ g) \circ h = f \circ (g \circ h)$.

Inverse functions

Every relation \mathcal{R} from set A to set B has an inverse relation \mathcal{R}^{-1} from B to A formed by interchanging the order of the pairs in the relation \mathcal{R} :

$$\mathcal{R}^{-1} = \{(y, x) \in B \times A \mid (x, y) \in A \times B\} \Leftrightarrow y\mathcal{R}^{-1}x \text{ if and only if } x\mathcal{R}y.$$

Note: Recall that for relations over \mathbb{R} , interchanging the order of the pairs interchanges the horizontal and vertical coordinates of the points on the graphs of these relations. The result will be that graphs of relations and their inverses are reflections of each other with respect to the line $y = x$ (called the ‘first bisector’ or ‘identity line’).



Since functions are also relations, then each function has an inverse relation. The inverse relation of a function f may or may not be a function itself. If the inverse of a function is a function itself, then we call it the inverse function of f and denote it by f^{-1} .

Example 28

Consider the function f from $\{1, 2, 3, 4\}$ to $\{5, 6, 7\}$ defined by

$$f = \{(1, 5), (2, 5), (3, 6), (4, 7)\}.$$

- Find the inverse f^{-1} .
- Find the inverse of f^{-1} , that is find $(f^{-1})^{-1}$.

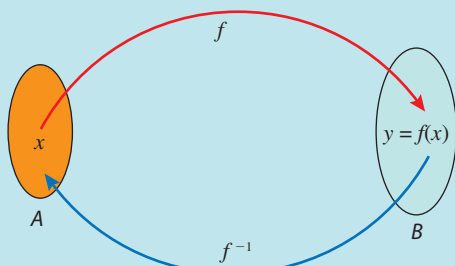
Solution

a) $f^{-1} = \{(5, 1), (5, 2), (6, 3), (7, 4)\}$. Notice here that the inverse f^{-1} is not a function itself.

b) $(f^{-1})^{-1} = \{(1, 5), (2, 5), (3, 6), (4, 7)\} = \{(1, 5), (2, 5), (3, 6), (4, 7)\} = f$.

Definition 17

Let $f: A \rightarrow B$ be a **bijection**. The inverse function of f is the function that assigns to an element $y \in B$ the unique element $x \in A$ such that $f(x) = y$.



The inverse function of f is denoted by f^{-1} . Thus,
 $f^{-1}(y) = x$ when $f(x) = y$.

Note: Why does the function have to be a bijection in order to have an inverse function?

For f^{-1} to be a function, all elements in its domain, which is B , must have an image each. Hence, every $y \in B$ should be associated with some $x \in A$, and hence f is a surjection.

If f were not an injection, then there exists at least two elements x_1 and x_2 in A that have the same image $y \in B$. This means that for f^{-1} , there is an element $y \in B$ that is assigned two images x_1 and x_2 in A , implying that f^{-1} is not a function.

Theorem 5

If f is a function from A to B , the inverse relation f^{-1} is a function from B to A if and only if f is a bijection.

In general, when we are dealing with inverse functions it is customary to say ‘the function has an inverse’, or ‘the function is invertible’ to mean that the function has an inverse and that the inverse is a function.

The above discussion leads us to a very important property of inverse functions. Let us consider a function $f: A \rightarrow B$ and its inverse $f^{-1}: B \rightarrow A$. Then,

$$f \circ f^{-1}(y) = f(f^{-1}(y)) = f(x) = y \Rightarrow f \circ f^{-1} = i_B.$$

Also,

$$f^{-1} \circ f(x) = f^{-1}(f(x)) = f^{-1}(y) = x \Rightarrow f^{-1} \circ f = i_A.$$

This observation provides us with a method to test whether two functions are inverses of each other.

Example 29

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = 4x^3$. Find the inverse of this function and check its correctness.

Solution

You have learned how to find the inverse of a function in Chapter 2 of the HL book. Recall that you switch the domain and range variables and solve the resulting equation for x .

$$f^{-1}(x) = \sqrt[3]{\frac{x}{4}}$$

To check our answer, we perform the composition as suggested in the note above.

$$f \circ f^{-1}(x) = f\left(\sqrt[3]{\frac{x}{4}}\right) = 4\left(\sqrt[3]{\frac{x}{4}}\right)^3 = 4 \cdot \frac{x}{4} = x, \text{ also}$$

$$f^{-1} \circ f(x) = f^{-1}(4x^3) = \sqrt[3]{\frac{4x^3}{4}} = \sqrt[3]{x^3} = x$$

Example 30

Show that the functions $f: \mathbb{R} \rightarrow]-2, \infty[$ and $h:]-2, \infty[\rightarrow \mathbb{R}$ defined by

$$f(x) = 5^{2x} - 2 \text{ and } h(x) = \frac{1}{2} \log_5(x+2)$$

are inverses of each other.

Solution

For any $x \in \mathbb{R}$,

$$h \circ f(x) = h(5^{2x} - 2) = \frac{1}{2} \log_5((5^{2x} - 2) + 2) = \frac{1}{2} \log_5(5^{2x}) = \frac{1}{2} \cdot 2x = x.$$

Also for any $x \in]-2, \infty[$,

$$f \circ h(x) = f\left(\frac{1}{2} \log_5(x+2)\right) = 5^{2\left(\frac{1}{2} \log_5(x+2)\right)} - 2 = 5^{\log_5(x+2)} - 2 = x + 2 - 2 = x.$$

Therefore f and h are inverses.

Example 31

If $f: A \rightarrow B$ and $g: B \rightarrow C$ are two invertible functions, show that

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Solution

To state the question differently, we can say that we need to show that $f^{-1} \circ g^{-1}$ is the inverse of $g \circ f$.

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ i_B \circ g^{-1} = g \circ g^{-1} = i_C$$

Also,

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ i_B \circ f = f^{-1} \circ f = i_A.$$

Therefore $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, i.e. the inverse of the composition of two functions is the composition of their inverses in reverse order!

Exercise 2

- 1 Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, and $C = \{x, y, z\}$. Find
- $A \times (B \cup C)$
 - $A \times (B \cap C)$
 - $A \times (B \setminus C)$
 - $(A \times B) \cup (A \times C)$
 - $(A \times B) \cap (A \times C)$
 - $(A \times B) \cap (A \times C')$
- b Which of the above expressions are equal?
- 2 Which of the following relations are equivalence relations on the given set?
- $\mathbb{R}, x \mathcal{R} y \Leftrightarrow x = y \text{ or } x = -y$
 - $\mathbb{Z}, x \mathcal{R} y \Leftrightarrow xy = 0$
 - $\mathbb{R}, x \mathcal{R} y \Leftrightarrow x^2 + x = y^2 + y$
 - $\mathbb{Z}^+, x \mathcal{R} y \Leftrightarrow xy \text{ is a square}$
 - $\mathbb{R} \times \mathbb{R}, (x, y) \mathcal{R} (a, b) \Leftrightarrow x^2 + y^2 = a^2 + b^2$
- 3 In the previous problem, describe the equivalence classes for those relations that are equivalence relations.
- 4 Let $A = \{1, 2, 3, 4, 5, 6\}$ and let $f: A \rightarrow A$ be a function defined by
- $$f(x) = \begin{cases} x+1, & \text{if } x \neq 6 \\ 1, & \text{if } x = 6 \end{cases}$$
- Find $f(3)$, $f \circ f(3)$, and $f(f(2))$.
 - Find a preimage of 4.
 - Show that f is a bijection.
- 5 Let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
- Define a relation \mathcal{R} on S by
- $$A \mathcal{R} B \Leftrightarrow |A| = |B|.$$
- Determine whether \mathcal{R} is an equivalence relation. If yes, describe the partition it induces on S . If not, justify why not.
- Define a relation \mathcal{X} on S by
- $$A \mathcal{X} B \Leftrightarrow |A| \neq |B|.$$
- Determine whether \mathcal{X} is an equivalence relation. If yes, describe the partition it induces on S . If not, justify why not.
- 6 Let $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ be defined by $f(x)$ for all $x \in \mathbb{Z}^+$ in each of the cases below. Determine if f is an injection, a surjection, or both. Justify your answer.
- $f(x) = x + 1$
 - $f(x) = 2x$
 - $f(x) = x^2$
 - $f(1) = 1, f(x) = x - 1 \text{ for } x > 1$

7 Let $f: x \mapsto 3x + 4$.

- a** Is $f: \mathbb{R} \rightarrow \mathbb{R}$ a bijection? Justify.
- b** Is $f: \mathbb{N} \rightarrow \mathbb{N}$ a bijection? Justify.
- c** Is $f: \mathbb{Q} \rightarrow \mathbb{Q}$ a bijection? Justify.

8 Let E and F be two finite sets such that $|E| = m$ and $|F| = n$. In each of the following give some indication why you believe your conclusion to be correct.

- a** Determine the number of functions from E into F .
- b** If $m \leq n$, determine the number of injections of E into F .
- c** If $m = n$, determine the number of surjections of E into F .

9 Consider the two functions f and g from \mathbb{Z} into \mathbb{Z} defined by

$$f(x) = 2x - 1 \text{ and } g(x) = x^2 + 1.$$

- a** Is f an injection? a surjection?
- b** Is g an injection? a surjection?
- c** If $A = [-4, 2]$ and $B = [0, 3]$, find
 - i** $A \cup B, A \cap B$
 - ii** $f(A \cup B), f(A) \cup f(B), f(A \cap B), f(A) \cap f(B)$
 - iii** $g(A \cup B), g(A) \cup g(B), g(A \cap B), g(A) \cap g(B)$

10 Consider the function $f: \mathbb{N} \rightarrow \mathbb{N}$ defined by

$$x \mapsto \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ \frac{x+1}{2} & \text{if } x \text{ is odd} \end{cases}$$

Is f an injection? a surjection?

11 Let the two functions f and g be from A into A . Show that

- a** if $f \circ g$ is a surjection, then f is a surjection.
- b** if $f \circ g$ is an injection, then g is an injection.

12 Consider the set $A = \{a, b, c\}$ and define the function $f: A \rightarrow A$ such that

$$f(a) = b, f(b) = c, \text{ and } f(c) = a.$$

- a** Show that f is a bijection from A into A .
- b** Calculate $f \circ f(a)$, $f \circ f(b)$, and $f \circ f(c)$.
- c** Determine $f \circ f \circ f$. What are the inverse functions of f and of $f \circ f$?

13 Let A and B be two subsets of a universal set U . Let \mathcal{R} be an equivalence relation defined on the elements of B . You are also given a function $f: A \rightarrow B$.

Define a relation \mathcal{S} in A such that $\forall x, y \in A, x\mathcal{S}y$ iff $f(x)\mathcal{R}f(y)$. Determine if \mathcal{S} is an equivalence relation in A .



14 Define a relation \mathcal{S} on \mathbb{R}^2 by: $(x_1, y_1)\mathcal{S}(x_2, y_2) \Leftrightarrow x_1^2 + y_1^2 = x_2^2 + y_2^2$.

- a** Show that \mathcal{S} is an equivalence relation.
- b** Describe the partition that this relation induces on the Cartesian plane, and give the equivalence class for $(1, 2)$.

15 The function $h: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is defined by $h: (a, b) \mapsto (2b - a, a + b)$.

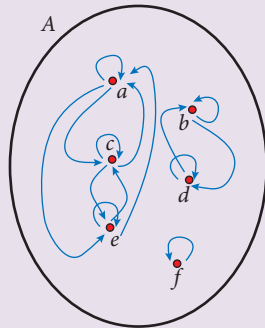
Determine whether h is injective, surjective, or both. If it has an inverse function find the inverse, and if does not have one, justify why not.

16 The relation \mathcal{R} is defined over $\mathbb{Z} \times \mathbb{Z}^+$ by: $(x_1, y_1)\mathcal{R}(x_2, y_2) \Leftrightarrow x_1 y_2 = y_1 x_2$.

Show that \mathcal{R} is an equivalence relation and describe the partition it induces.

17 A relation \mathcal{S} on set $A \{a, b, c, d, e, f\}$ is defined by the 'arrow diagram' below. (When there is an arrow from one element to the other then the elements are related, for example $a\mathcal{S}c$.)

Determine whether the relation is an equivalence relation, and if it is, describe the partition it induces on A .



18 Let $A = \{x \mid x \in \mathbb{N} \text{ and } 0 < x < 11\}$.

The relation \mathcal{R} is defined on A by:

$$x\mathcal{R}y \Leftrightarrow x^2 \equiv y^2 \pmod{5}.$$

Show that \mathcal{R} is an equivalence relation on A , and write down all the equivalence classes.

19 Determine which of the following functions with domain and codomain \mathbb{R} is a bijection. Justify your answer.

- a** $f(x) = 3x^2 + 1$
- b** $g(x) = 2x^3 + 1$
- c** $h(x) = \frac{3x^2 + 1}{x^2 + 2}$

20 If $f: A \rightarrow B$ is a bijection, and if $h: B \rightarrow C$ is a bijection, show that $h \circ f$ is also a bijection. Justify your response completely.

21 A relation ϕ is defined over the set of natural numbers by

$$\phi = \{(x, y) \mid x, y \in \mathbb{N} \text{ and } 3^x \equiv 3^y \pmod{10}\}.$$

- a** Show that ϕ is an equivalence relation.
- b** Find the equivalence classes.
- c** Find the smallest possible value for $3^{101} \pmod{10}$.

22 Consider the function $h: \mathbb{Z} \rightarrow \mathbb{Z}$ defined by

$$h(n) = 7n + 6.$$

Determine whether h is

- a** injective
- b** surjective.

In both cases, justify your response.

23 Consider the function $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by

$$f(x, y) = (x + 3y, 2x - 5y).$$

Show that the function is bijective and find its inverse.

24 Let f and g be two mappings from a set A to A . Show that

- a** if $f \circ g$ is a surjection, then f is a surjection.
- b** if $f \circ g$ is an injection, then g is an injection.

25 Let $A = \{x \mid x \in \mathbb{Z}, x > 1\}$. A relation \mathcal{R} is defined on A by

$$x\mathcal{R}y \Leftrightarrow \gcd(x, y) > 1.$$

Show that the relation is reflexive, symmetric, but NOT transitive.

26 The function $f: \mathbb{R} \rightarrow \mathbb{R}$ is defined by

$$f(x) = e^{\cos x} + 1.$$

- a**
 - i** Find the range, R , of f .
 - ii** Show that the function is not an injection. Justify.
 - iii** Determine, with reasons, whether the function is a surjection.
- b** We now restrict the function as follows:
 $f: [0, k] \rightarrow R, k > 0.$
 - i** Find the largest value of k for which the restricted function is a bijection.
 - ii** Find an inverse for this restricted function.

27 Let $U = \{4, 8, 12, 16, 20, 24, 28, 32, 36\}$. A relation \mathcal{S} is defined on U by

$$x\mathcal{S}y \Leftrightarrow x^2 \equiv y^2 \pmod{7}.$$

- a** Show that \mathcal{S} is an equivalence relation.
- b** Find the partition of U induced by \mathcal{S} on U .

- 28** The relation \mathcal{S} is represented by the table below. A '1' entry means that the element in the left column is related to the element in the top row; for example, $c\mathcal{S}d$. A zero entry implies that the two elements are not related, so $c\not\mathcal{S}e$.

Show that \mathcal{S} is an equivalence relation and find all equivalence classes.

\mathcal{S}	a	b	c	d	e	f	g	h	i
a	1	0	0	0	0	1	0	1	0
b	0	1	0	0	1	0	0	0	1
c	0	0	1	1	0	0	0	0	0
d	0	0	1	1	0	0	0	0	0
e	0	1	0	0	1	0	0	0	1
f	1	0	0	0	0	1	0	1	0
g	0	0	0	0	0	0	1	0	0
h	1	0	0	0	0	1	0	1	0
i	0	1	0	0	1	0	0	0	1

- 29** The function h is defined by

$$h: \mathbb{R}^2 \rightarrow \mathbb{R}^2 \text{ such that } h: (x, y) \mapsto (2x + 3y, y + 2x).$$

Show that h must have an inverse, and find that inverse, h^{-1} .

- 30** Determine whether the function g defined below is injective, surjective, or both. Justify your response.

$$g: (\mathbb{R}^+)^2 \rightarrow (\mathbb{R}^+)^2, \text{ where } g(x, y) = (2x + y, 2xy)$$

- 31** A relation \mathcal{R} is defined over \mathbb{N} by: $x\mathcal{R}y \Leftrightarrow x^2 \equiv y^2 \pmod{5}$.

- Show that \mathcal{R} is an equivalence relation.
- Find the partition of \mathbb{N} induced by \mathcal{R} on \mathbb{N} .

- 32 a** Show that the mapping $f: \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R}$ defined by

$$f(x) = \frac{2x+5}{x-1}$$

is an injection.

- Find the value of a so that the function $f: \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R} \setminus \{a\}$ becomes a bijection.

- 33** Consider a function $f: E \rightarrow F$. Let $A, B \subseteq E$ such that $A \cap B \neq \emptyset$. Show that

- $A \subset B \Rightarrow f(A) \subset f(B)$
- $f(A \cup B) = f(A) \cup f(B)$
- $f(A \cap B) \subset f(A) \cap f(B)$
- f is an injection $\Rightarrow f(A \cap B) = f(A) \cap f(B)$

- 34** If \cong is an equivalence relation on a set A , prove each of the following.

- If $a, b \in A$ such that $a \not\cong b$, then $[a] \cap [b] = \emptyset$.
- If $a, b, c, d \in A$ such that $c \in [a]$, $d \in [b]$, and $[a] \neq [b]$, then $c \not\cong d$.

Practice questions 2

- 1** Let $S = \{(x, y) \mid x, y \in \mathbb{R}\}$, and let $(a, b), (c, d) \in S$. Define the relation Δ on S as follows:

$$(a, b) \Delta (c, d) \Leftrightarrow a^2 + b^2 = c^2 + d^2.$$

- a** Show that Δ is an equivalence relation.
 - b** Find all ordered pairs (x, y) where $(x, y) \Delta (1, 2)$.
 - c** Describe the partition created by this relation on the (x, y) plane.
- 2** Consider the set $\mathbb{Z} \times \mathbb{Z}^+$. Let R be the relation defined by the following:
For (a, b) and (c, d) in $\mathbb{Z} \times \mathbb{Z}^+$, $(a, b) R (c, d)$ if and only if $ad = bc$, where ab is the product of the two numbers a and b .
- a** Prove that R is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^+$.
 - b** Show how R partitions $\mathbb{Z} \times \mathbb{Z}^+$, and describe the equivalence classes.
- 3** Let Y be the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
Define the relation R on Y by $aRb \Leftrightarrow a^2 - b^2 \equiv 0 \pmod{5}$, where $a, b \in Y$.
- a** Show that R is an equivalence relation.
 - b i** What is meant by 'the equivalence class containing a '?
 - ii** Write down all the equivalence classes.
- 4** The relation R is defined on the non-negative integers a, b such that aRb if and only if $7^a \equiv 7^b \pmod{10}$.
- a** Show that R is an equivalence relation.
 - b** By considering powers of 7, identify the equivalence classes.
 - c** Find the value of $7^{503} \pmod{10}$.
- 5** Consider the functions f and g , defined by
 $f: \mathbb{Z} \rightarrow \mathbb{Z}$ where $f(n) = 5n + 4$, and
 $g: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ where $g(x, y) = (x + 2y, 3x - 5y)$.
- a** Explain whether the function f is
 - i** injective
 - ii** surjective.
 - b** Explain whether the function g is
 - i** injective
 - ii** surjective.
 - c** Find the inverse of g .
 - d** Consider any functions $f: A \rightarrow B$ and $g: B \rightarrow C$. Given that $g \circ f: A \rightarrow C$ is surjective, show that g is surjective.
- 6** Let $S = \{\text{integers greater than } 1\}$. The relation R is defined on S by
 $mRn \Leftrightarrow \gcd(m, n) > 1$, for $m, n \in S$.
- a** Show that R is reflexive.
 - b** Show that R is symmetric.
 - c** Show using a counterexample that R is not transitive.



- 7** Let $a, b \in \mathbb{Z}^+$ and define $aRb \Leftrightarrow a^2 \equiv b^2 \pmod{3}$.
- a** Show that R is an equivalence relation.
 - b** Find all the equivalence classes.
- 8** We define the relation $(x, y) R (p, q)$ if and only if $x^2 - y^2 = p^2 - q^2$ where $(x, y), (p, q) \in \mathbb{R}^2$. Prove that R is an equivalence relation on \mathbb{R}^2 . Describe geometrically the equivalence class of $(1, 1)$.
- 9** Let $F(x) = x^2 - |x - 2|$.
- a** The function f is defined by
 $f:]-\infty, 1] \rightarrow \mathbb{R}$, where $f(x) = F(x)$.
Find the range of f and determine whether it is an injection.
 - b** The function g is defined by
 $g: [1, \infty[\rightarrow [0, \infty[$, where $g(x) = F(x)$.
Show that g has an inverse and find this inverse.
- 10** The relation R is defined on ordered pairs by
 $(a, b)R(c, d)$ if and only if $ad = bc$ where $a, b, c, d \in \mathbb{R}^+$.
- a** Show that R is an equivalence relation.
 - b** Describe, geometrically, the equivalence classes.

Questions 1–10 © International Baccalaureate Organization



Groups I

3.1 Binary operations

Operations on pairs of elements of sets arise in many contexts. In the set of integers, examples of such operations include the addition, subtraction, or multiplication of integers. In the set of 3×3 matrices, addition and multiplication of matrices are also operations. In such cases we speak of a **binary operation**. In general, a **binary operation** on a set A , denoted by any symbol of your choice, Δ for example, is a rule which assigns to each ordered pair of elements a and b from A a *uniquely* defined third element c and we write $a \Delta b = c$. Usually, we have a condition that c must also be an element of A ; otherwise the operation is not called a binary operation.

Definition 1

A **binary operation** on a set A is a function from $A \times A$ into A . Thus a binary operation is a rule $*$ which assigns to every ordered pair $(a, b) \in A \times A$ exactly one element $c \in A$; this element is denoted by

$$a * b = c.$$

There are two, very important, points which *must* be checked to determine whether an operation is a binary operation on set A :

- The rule for the operation must be **well defined**: it must assign to every ordered pair (a, b) *exactly* one element c .
- The second condition is that the element c is an element of A . This is called the **closure** property. It is very important to know that there are a few sources (among which is the IB) that do not include closure as a condition for an operation to be a binary operation. So, in exams, you may be required to test the closure property separately. In the following examples, we will indicate whether you need to check closure.

Typical examples of binary operations are addition and multiplication over the set of real numbers, since when we add two real numbers we get another real number, the same for multiplication.

Example 1

Decide whether each operation is binary and whether each set is closed under the given operation.

- a) The set of integers \mathbb{Z} under subtraction.
- b) The set of positive integers \mathbb{Z}^+ and division.

c) The set of 2×2 matrices with real coefficients

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}, \text{ and matrix addition.}$$

Solution

- a) Since the difference between two integers is a unique integer, the operation is a binary one and the set is closed under subtraction.
- b) Since the quotient of any two positive integers is a unique real number, the operation is binary. However, the quotient $\frac{a}{b}$ is not always a positive integer and hence \mathbb{Z}^+ is not closed under division. (Please note here that in most books the operation is not considered a binary operation because the set is not closed under it.)

c) Take two arbitrary 2×2 matrices with real coefficients

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and } \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

Now since each entry in $\begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$ is real and unique for

this sum the operation is binary. And since the resulting matrix is also an element of the set of 2×2 matrices with real coefficients, then it is closed under this operation. (Please note here too that the operation is considered binary because the result is a unique member of the set of real 2×2 matrices.)

Properties of binary operations

Definition 2

A binary operation $*$ on a set G is **associative** if and only if for all $a, b, c \in G$,

$$a * (b * c) = (a * b) * c.$$

A binary operation $*$ on a set G is **commutative** if and only if for all $a, b \in G$,

$$a * b = b * a.$$

A binary operation $*$ on a set G is **distributive** over another binary operation Δ if and only if for all $a, b, c \in G$,

$$a * (b \Delta c) = (a * b) \Delta (a * c).$$

Example 2

Decide whether subtraction in the set of integers \mathbb{Z} is associative or commutative.

Solution

Since $a - (b - c) = (a - b) + c \neq (a - b) - c$, the operation is not associative.

Also, $a - b \neq b - a$, except for $a = b = 0$, so the operation is not commutative.

Example 3

Decide whether the operation of intersection over the power set of a given set A is associative or commutative. Additionally, check if the operation of intersection is distributive over the union operation.

Solution

- Associativity: Let X , Y , and Z be subsets of A .

For all $a \in X \cap (Y \cap Z) \Leftrightarrow a \in X$ and $a \in (Y \cap Z) \Leftrightarrow a \in X$ and $a \in Y$ and $a \in Z$

$\Leftrightarrow (a \in X$ and $a \in Y)$ and $a \in Z \Leftrightarrow a \in (X \cap Y) \cap Z$. Therefore,

$$X \cap (Y \cap Z) = (X \cap Y) \cap Z.$$

- Commutativity: If $a \in (X \cap Y) \Leftrightarrow a \in X$ and $a \in Y \Leftrightarrow a \in Y$ and $a \in X \Leftrightarrow a \in (Y \cap X)$. Therefore,

$X \cap Y = Y \cap X$ and the operation is commutative.

- We proved in Chapter 1 that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Therefore, the operation ‘intersection’ is distributive over the operation ‘union’.

Example 4

Decide whether matrix addition over the set of 2×2 matrices with real coefficients is associative and commutative.

Solution

- Associativity: Let $M_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$ represent members of the set of 2×2 matrices with real coefficients, i.e.

$$M_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, M_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}, \dots$$

$$\begin{aligned} M_1 + (M_2 + M_3) &= M_1 + \begin{pmatrix} a_2 + a_3 & b_2 + b_3 \\ c_2 + c_3 & d_2 + d_3 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 + a_3 & b_1 + b_2 + b_3 \\ c_1 + c_2 + c_3 & d_1 + d_2 + d_3 \end{pmatrix} \\ &= \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix} + \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} = (M_1 + M_2) + M_3 \end{aligned}$$

- Commutativity:

$$M_1 + M_2 = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix} = \begin{pmatrix} a_2 + a_1 & b_2 + b_1 \\ c_2 + c_1 & d_2 + d_1 \end{pmatrix} = M_2 + M_1$$

Operation (Cayley) tables

If S is a small finite set, it is often convenient to define the binary operation on S by means of a table, which is constructed as follows:

All the elements of the set S are written across the top row of the table and also vertically, in the same order down the leftmost column of the table, as shown. The element corresponding to $c * b$, for example, is at the intersection of the row containing c with the column containing b .

*	a	b	c	...
a				
b				
c		$c * b$		
\vdots				

Such operation tables are also called **Cayley tables**, after the British mathematician Arthur Cayley.

These tables have what is called the **Latin square property** (see page 1273).

Example 5

A binary operation Δ is defined over the set $S = \{m, n, r, s\}$ using the table below.

Show that the set is closed under this operation, decide whether it is commutative, and check on particular instances of associativity using n, r , and s .

Δ	m	n	r	s
m	m	n	r	s
n	n	r	s	m
r	r	s	m	n
s	s	m	n	r



Sometimes, even if the operation itself is not commutative, you may still have some elements that are 'commutable'. For example, consider the following operation defined over \mathbb{Z}^+

$$a \circ b = a^b$$

In general $a \circ b \neq b \circ a$; for example

$$2 \circ 5 = 2^5 = 32 \neq 5 \circ 2 = 5^2 = 25,$$

however

$$2 \circ 4 = 2^4 = 16 = 4 \circ 2 = 4^2 = 16.$$

When a set with a binary operation is given by a Cayley's table then the operation is commutative if and only if equal elements appear in all positions that are symmetrically placed relative to the main diagonal. That is, to check whether an operation defined by a Cayley's table is commutative, simply draw the main diagonal, and see if the table is symmetric about it. For example, the operation Δ defined by the table above is commutative.



Solution

- Since all elements in the table are elements of set S , S is closed under Δ .
- Since for all possible choices such as $n \Delta r = s = r \Delta n$, or $s \Delta r = n = r \Delta s$, etc. the operation is commutative.
- Consider $(n \Delta r) \Delta s = s \Delta s = r$, and $n \Delta (r \Delta s) = n \Delta n = r$; therefore, $(n \Delta r) \Delta s = n \Delta (r \Delta s)$.

However, if we have to decide whether the operation is associative we have to consider all possible combinations, which is a very tedious task.

Example 6

Is the binary operation on \mathbb{R} defined by $a * b = a + b - 1$ commutative? Is it associative?

Solution

- Since $a * b = a + b - 1$ and $b * a = b + a - 1 = a + b - 1 = a * b$, then the operation is commutative.
- $(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + b + c - 2$, and $a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2$; therefore $*$ is associative.

Example 7

Is the binary operation on \mathbb{R} defined by $a * b = ab + 1$ commutative? Is it associative?

Solution

- Since $a * b = ab + 1$ and $b * a = ba + 1 = ab + 1 = a * b$, then the operation is commutative.
- $(a * b) * c = (ab + 1) * c = (ab + 1)c + 1 = abc + c + 1$, and $a * (b * c) = a * (bc + 1) = a(bc + 1) + 1 = abc + a + 1 \neq abc + c + 1$; therefore $*$ is not associative.

In some cases, you may find that associative behaviour holds for some elements of the set in question. However, we can only claim the associativity to hold if it does so for every element.



The identity element

In general, if we have a set S with a binary operation Δ on that set, then an element e of S is called a **left-identity** if $e \Delta a = a$ for every a in S . Similarly, it is called a **right-identity** if $a \Delta e = a$. e is called an **identity** if it is both a **left-** and a **right-identity**. This is given formally in the following definition.

Definition 3

An element e in a set S is an **identity element** (or **identity**) for an operation Δ defined over S if

$$e \Delta a = a \Delta e = a$$

for every element $a \in S$.



An element e is an identity if it leaves every element unchanged.

Theorem 1

If an operation \circ admits a left-identity e_1 and a right-identity e_2 , then these two identities are equal.



Theorem 1 means that there is a unique identity element i.e. there is one and only one identity element.

Proof

If we consider the left-identity e_1 , then $e_1 \circ e_2 = e_2$. However, if we consider the right-identity e_2 , then $e_1 \circ e_2 = e_1$. Thus $e_1 = e_2$ since they are both equal to $e_1 \circ e_2$.

- Addition over the integers has 0 as the identity element:

$$\text{For all } a \in \mathbb{Z}, a + 0 = 0 + a = a.$$

- Multiplication over the set of non-zero integers has 1 as the identity element:

$$\text{For all } a \in \mathbb{Z} \setminus \{0\}, a \times 1 = a \text{ or } 1 \times a = a.$$

- The set A is the identity element for the operation of intersection over the power set of A :

$$\text{If } B \subseteq A, \text{ then } A \cap B = B \cap A = B.$$

- The empty set, \emptyset , is the identity for the operation of union over the power set of A :

$$\text{If } B \subseteq A, \text{ then } \emptyset \cup B = B \cup \emptyset = B.$$

- If we consider the set of real numbers and define the operation $*$ by $a * b = a^b$, then 1 is a right-identity only since $a * 1 = a^1 = a$, but $1 * a = 1^a \neq a$, so 1 is not a left-identity.

- The set of 2×2 matrices with real coefficients

$$M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\} \text{ under matrix multiplication}$$

has $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ as an identity element since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

- The binary operation on \mathbb{R} defined by $a * b = a + b - 13$ has 13 as an identity:

$$a * 13 = a + 13 - 13 = a, \text{ and } 13 * a = 13 + a - 13 = a.$$



Notation

It is convenient when possible, to write ab when we mean $a \circ b$.

Theorem 2

If a binary operation $*$ on a set S admits an identity element e , then this element is unique.

Proof

Since e is an identity element, then for *any* $x \in S$:

$$x * e = e * x = x \quad (1)$$

Assume that there is at least another different identity element e' , then for *any* $x \in S$:

$$x * e' = e' * x = x \quad (2)$$

Now, since (1) is true for *any* $x \in S$, it has to be true for $x = e'$, and thus:

$$x * e = e * x = x \Rightarrow e' * e = e * e' = e' \quad (3)$$

Also, since (2) is true for *any* $x \in S$, it has to be true for $x = e$, and thus:

$$x * e' = e' * x = x \Rightarrow e * e' = e' * e = e \quad (4)$$

By comparing (3) and (4) we notice that $e * e' = e'$ and $e * e' = e$, and hence $e = e'$.

Therefore, our assumption of the existence of an identity element other than e is false and we can conclude that the identity element e is unique.

- The binary operation on \mathbb{Z} defined by $a * b = ab + 1$ has no identity.

Assume e is an identity, then $a * e = ae + 1 = a \Rightarrow e = \frac{a-1}{a}$ which is not unique! Also, consider the case of $a = 1$, then $e = 0$, but $a * 0 = 0 + 1 \neq a$. So, this operation has no identity element.

The inverse element

In general, if we have a set S with a binary operation Δ on that set, then an element a of S has a **left-inverse** a' if $a' \Delta a = e$. Similarly, a has a **right-inverse** a'' if $a \Delta a'' = a$. An element that is both a **left-** and a **right-inverse** is called an **inverse** and we denote it by a^{-1} . This is formally given in the following definition.

Definition 4

An element a^{-1} in a set S is an **inverse element** (or **inverse**) for an operation Δ defined over S if

$$a^{-1} \Delta a = a \Delta a^{-1} = e$$

for any element $a \in S$.

Theorem 3

If, for an associative operation \circ , an element a admits a left-inverse a' and a right-inverse a'' , then these two inverses are equal.

Proof

$$a' \circ a \circ a'' = (a' \circ a) \circ a'' = e \circ a'' = a'', \text{ also}$$

$$a' \circ a \circ a'' = a' \circ (a \circ a'') = a' \circ e = a', \text{ and therefore } a' = a''.$$

- The set of integers \mathbb{Z} under addition admits for each element an inverse; namely, for every $a \in \mathbb{Z}$, $-a$ is the inverse since $a + (-a) = (-a) + a = 0$.
- The set of non-negative real numbers under multiplication admits an inverse for each element; namely, for every $a \in \mathbb{R} \setminus \{0\}$, $\frac{1}{a}$ is the inverse since $a \times \frac{1}{a} = \frac{1}{a} \times a = 1$.
- The set of invertible 2×2 matrices with real coefficients

$$GL_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}$$

under matrix multiplication admits an inverse

$$\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} \text{ for each of its members since}$$

$$\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Theorem 4

If an operation $*$ defined on a set S has an identity element e , then every invertible element admits a *unique* inverse.

Proof

Let us take any invertible element $a \in S$. Assume that there is no unique inverse for a , then we can say that there are at least two inverses for a . Let the inverses of a be a_1 and a_2 .

By definition:

$$a * a_1 = a_1 * a = e \tag{1}$$

$$a * a_2 = a_2 * a = e \tag{2}$$

By comparing (1) and (2), we can write

$$a * a_1 = a_1 * a = e = a * a_2 = a_2 * a, \text{ which implies that}$$

$a * a_1 = e = a_2 * a$, and hence a_1 and a_2 are the right- and left-inverses of a which should be equal by Theorem 3.

Therefore, our assumption that there are at least two different inverses for a is false, and a admits a unique inverse, which we will denote here by a^{-1} .

Example 8

Consider the operation $*$ on the set of integers defined by $a * b = a + b - 13$. Does each element have an inverse?

Solution

Let a be an integer. Let b be a right-inverse of a . Recall that the identity for this operation is 13. Then $a * b = 13$. That is, $a + b - 13 = 13$. Solving for b we find $b = -a + 26$. This is also a left-inverse of a since $(-a + 26) * a = -a + 26 + a - 13 = 13$.

Cancellation laws

Theorem 5

Let $*$ be a binary operation that is defined on a non-empty set S with an identity element e and an inverse element a^{-1} for each element $a \in S$. The left and right cancellation laws hold, i.e.

if $a * b = a * c$, then $b = c$; and if $b * a = c * a$ then $b = c$.

Proof

Suppose $a * b = a * c$, and let a^{-1} be the inverse of a . Now operating with a^{-1} from the left we have

$$\begin{aligned} a^{-1} * (a * b) &= a^{-1} * (a * c) \Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c \\ &\Rightarrow e * b = e * c \Rightarrow b = c; \text{ this is the left cancellation law.} \end{aligned}$$

Similarly, if $b * a = c * a$ we operate with a^{-1} from the right, and we have

$$(b * a) * a^{-1} = (c * a) * a^{-1} \Rightarrow b * e = c * e \Rightarrow b = c \text{ (details are left for you as an exercise).}$$

Definition 5

Let G be a non-empty set together with a binary operation $*$ that assigns to each ordered pair $(a, b) \in G^2$ an element denoted by $a * b$ ¹. We say G is a **group** under this operation if the following four properties are satisfied. We usually write $(G, *)$ or $\{G, *\}$ to denote a group with an operation.

1. **Closure:** The set G is closed under this operation, i.e. $a * b \in G$.
2. **Associativity:** The operation is associative, i.e. $(a * b) * c = a * (b * c)$ for all a, b, c in G .
3. **Identity:** There is an element e in G , such that $a * e = e * a = a$ for all a in G . e is the identity element for the group under this operation.
4. **Inverses:** For each element a in G , there is an element b in G such that $a * b = b * a = e$. b is the inverse of a and every so often denoted by a^{-1} . (Notice that if b is the inverse of a , then a is the inverse of b . Therefore, we can say that the inverse of the inverse is the original element itself $(a^{-1})^{-1} = a$.)

¹ We usually consider that $a * b \in G$ by definition of a binary operation, but the IB syllabus does not define a binary operation to have this closure property. So, we will follow the syllabus in this publication and list the closure property separately.

If a group has the property that $a * b = b * a$, for every pair of elements a and b , we say the group is **Abelian** or **commutative**. A group is **non-Abelian** if there is at least one pair of elements a and b for which $a * b \neq b * a$.

A group G is said to be **finite** (or of **finite order**) if it has a finite (restricted) number of elements. In this case, the number of elements in G is called the **order** of G and is denoted by $|G|$. A group with infinitely many elements is said to have **infinite order**, or is **infinite**.

- \mathbb{Z} , \mathbb{Q} , and \mathbb{R} are all groups under ordinary addition. The identity is 0 and the inverse of a is $-a$. These are **infinite groups**.

Theorem 6 (Latin square property)

This property states that for all elements a and b in a group $(G, *)$, there exists a unique element c such that $a * c = b$.

Proof

Existence: Let $c = a^{-1} * b$.

Since $a^{-1} \in G$ and $b \in G$, then by closure $a^{-1} * b \in G$, and

$$a * c = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b \text{ and so } c \text{ exists and it satisfies } a * c = b.$$

Uniqueness: Let d be another element such that $a * d = b$.

$$d = e * d = (a^{-1} * a) * d = a^{-1} * (a * d) = a^{-1} * b = c$$

We can prove, in a similar manner, that there exists a unique element g such that $g * a = b$.



The converse of Theorem 6 is not true, i.e. if for all elements a and b , there exists a unique element c such that $a * c = b$, it does not necessarily follow that the set under that operation is a group.

The Latin square property gets its name from the fact that for a finite group $(G, *)$, it is possible to draw a Cayley table, which gives the element $a * b$ in the row corresponding to a and the column corresponding to b . This table will be a Latin square, a square display in which each possible value for a cell appears exactly once in each row, and exactly once in each column.

The set $\{1, -1, i, -i\}$ where $i^2 = -1$, is a group under complex multiplication.

Cayley's table is a good tool to use to check this group.

\times	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Notice here that each element appears in the table, once every row and once every column, implying that the set is closed under multiplication and that the operation gives a unique element for every pair.

The row corresponding to 1 yields the same values as the top row, implying that 1 is the identity. This is confirmed by observing that the column corresponding to 1 is also the same.

1 appears in every row and column, implying that every element has an inverse. We will assume that multiplication of complex numbers is known to be associative. Finally, the table is symmetric around its main diagonal, and that is why it is an Abelian group. This group is **finite**.

In Cayley tables for **groups**, the following are true:

- 1 All entries must belong to the members of the group indicating closure.
- 2 Every entry appears exactly once in every column and every row. If a binary operation is well defined, then if $a * b = c$, then c is unique.
- 3 The identity element must appear in every row and column. Since every element has an inverse, then, for example, $a * a^{-1} = e$, implying that it is in the a -row and in the a^{-1} -row, and since the inverse is unique, then e appears only once in each.

Examples of groups

- (\mathbb{Z}, \times) is not a group. It satisfies closure, identity, and associativity. However, not every element $a \in \mathbb{Z}$ has an inverse. For example, there is no integer b such that $3b = 1$.
- (\mathbb{Q}^+, \times) is an Abelian group. The product of any two rational numbers is a rational number, so closure is satisfied; the identity is 1, which is a rational number, and every positive rational number a has an inverse $\frac{1}{a}$. Also, for every ordered pair $a \times b = b \times a$. The group is infinite.

- The set of 2×2 matrices with real coefficients

$$M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\} \text{ under matrix addition, } (M_2, +) \text{ is an}$$

Abelian group. It is closed since the sum of any two 2×2 matrices is a

2×2 matrix, the identity is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and for every matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

the inverse is $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$. Addition of matrices is associative and therefore associativity is assumed. Also, as addition is commutative the group is Abelian. This group is infinite.

- The set of invertible 2×2 matrices with real coefficients

$$GL_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\} \text{ under matrix multiplication, } (GL_2, \cdot).$$

We have discussed this set in the discussion following Theorem 3, where

we showed that it has an identity and every element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has an

$$\text{inverse } \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}. \text{ Since the elements are matrices, we can}$$

assume that associativity of matrix multiplication holds here. We have not shown that the set is closed under multiplication yet. To show closure, we need to show that if we multiply two non-singular matrices, the answer should also be non-singular. Recall that for a matrix A to be non-singular, the determinant $(ad - bc)$ must be different from zero. Also, we need to recall that $\det(AB) = \det(A)\det(B)$, and if A and B are non-singular, their determinants are different from zero and hence $\det(AB) \neq 0$, which implies that AB is a member of GL_2 , and closure is satisfied.

Therefore, (GL_2, \cdot) is a group. However, it is non-Abelian because multiplication of matrices is not commutative.

Theorem 7

If a and b are elements of a group $(G, *)$, then

- 1 $(a^{-1})^{-1} = a$
- 2 $(a * b)^{-1} = b^{-1} * a^{-1}$

Proof

- 1 Since for every element a in G there is an inverse a^{-1} , such that $a * a^{-1} = a^{-1} * a = e$. Consider a^{-1} as an element in G , and hence $a^{-1} * a = a * a^{-1} = e$ implying that the inverse of a^{-1} is a , i.e. $(a^{-1})^{-1} = a$.



Please remember that for examinations starting 2014, questions containing matrices will not appear in official exam papers. Matrices are included here to explain certain concepts.

- 2 We proved beforehand that the inverse of an element is unique.
 $(a * b)(b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$ using associativity, thus
 $(a * b)(b^{-1} * a^{-1}) = a * e * a^{-1} = a * a^{-1} = e$; similarly
 $(b^{-1} * a^{-1})(a * b) = b^{-1} * e * b = b^{-1} * b = e$.
Hence, $b^{-1} * a^{-1}$ is the unique inverse of $a * b$.

Example 9

Consider the set of invertible 2×2 matrices with real coefficients

$$SL_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } ad - bc = 1 \right\} \text{ under matrix multiplication, } (SL_2, \cdot).$$

- a) Show that (SL_2, \cdot) is a group.
b) If $A = \begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix}$ and $B = \begin{pmatrix} 4 & 5 \\ 7 & 9 \end{pmatrix}$ are elements of this group, find $(A \cdot B)^{-1}$, $A^{-1} \cdot B^{-1}$, and $B^{-1} \cdot A^{-1}$.

Solution

- a) The set is closed under matrix multiplication because for any two members A and B , AB (we will use AB to represent $A \cdot B$) will also be in the same set.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \Rightarrow AB = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}, \text{ and}$$

since $\det(AB) = \det(A)\det(B)$, then $\det(AB) = 1 \times 1 = 1$ and AB is a member of this set. (You can also show that $\det(AB) = 1$ directly. With some algebra, you can write $\det(AB) = ad(eh - fg) + bc(fg - eh)$, but $eh - fg = 1$, and so $\det(AB) = ad - bc = 1$.)

The identity element $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is a member of the set.

Moreover, every element has an inverse in the set.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \text{ with } \det(A^{-1}) = da - cb = 1.$$

And associativity is assumed.

$$\begin{aligned} \text{b) } A &= \begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix}, B = \begin{pmatrix} 4 & 5 \\ 7 & 9 \end{pmatrix} \Rightarrow AB = \begin{pmatrix} 61 & 78 \\ 43 & 55 \end{pmatrix} \\ &\Rightarrow (AB)^{-1} = \begin{pmatrix} 55 & -78 \\ -43 & 61 \end{pmatrix}; \text{ also } A^{-1} = \begin{pmatrix} 5 & -7 \\ -2 & 3 \end{pmatrix}, B^{-1} = \begin{pmatrix} 9 & -5 \\ -7 & 4 \end{pmatrix} \\ &\Rightarrow A^{-1}B^{-1} = \begin{pmatrix} 94 & -53 \\ -39 & 22 \end{pmatrix} \text{ and } B^{-1}A^{-1} = \begin{pmatrix} 55 & -78 \\ -43 & 61 \end{pmatrix} \end{aligned}$$

Notice here that this example demonstrates Theorem 7.2 above.

Notation

- 1 Since the binary operation in a group is an associative operation, the convention is to write $a * b * c$ instead of $(a * b) * c$ or $a * (b * c)$.
- 2 It is also the convention to write $\underbrace{a * a * \dots * a}_{r \text{ times}}$ as a^r , and we interpret this 'exponent' as the binary operation '*' applied r times. Hence, the laws of exponents such as a^{r+s} are also interpreted similarly, '*' applied r times and s times, i.e. $a^{r+s} = a^r * a^s$; and finally, $(a^r)^s = \underbrace{a^r * a^r * \dots * a^r}_{s \text{ times}} = a^{rs}$.
- 3 We also define $a^0 = e$, and $a^{-r} = \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{r \text{ times}}$.

Congruence revisited

In the previous chapter we defined congruence classes modulo m (*residue classes mod m*) and concluded that they partition the set of integers into m classes $[0], [1], \dots, [m-1]$.

We define a congruence class as follows:

Definition 6

Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. The **congruence class of a modulo n** (denoted by $[a]$) is the set of all integers that are congruent to a modulo n , that is,

$$[a] = \{x \mid x \in \mathbb{Z} \text{ and } x \equiv a \pmod{n}\}.$$

Note: To say that $x \equiv a \pmod{n}$ means that $n \mid (x - a)$ or $x - a = kn$ for some integer k , or equivalently $x = a + kn$. Thus, a practical way of expressing a congruence class is

$$[a] = \{x \mid x \equiv a \pmod{n}\} = \{x \mid x = a + kn, k \in \mathbb{Z}\}, \text{ or in other words } [a] = \{a + kn \mid k \in \mathbb{Z}\}.$$

In congruence modulo 7, we have

$$\begin{aligned} [4] &= \{4 + 7k \mid k \in \mathbb{Z}\} = \{4, 4 \pm 7, 4 \pm 14, 4 \pm 21, \dots\} \\ &= \{\dots, -17, -10, -3, 4, 11, 18, 25, \dots\} \\ [-3] &= \{-3 + 7k \mid k \in \mathbb{Z}\} = \{-3, -3 \pm 7, -3 \pm 14, -3 \pm 21, \dots\} \\ &= \{\dots, -24, -17, -10, -3, 4, 11, 18, \dots\} \end{aligned}$$

We observe that $[-3] = [4]$, which should not be surprising because we know that $-3 \equiv 4 \pmod{7}$. This is an example of the following theorem.

Theorem 8

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

Proof

(\Rightarrow): Letting $a \equiv b \pmod{n}$, we show that $[a] \subseteq [b]$ first. Let $c \in [a]$, then $c \equiv a \pmod{n}$, but $a \equiv b \pmod{n}$; thus, by the transitive property, $c \equiv b \pmod{n}$ and $c \in [b]$ and therefore $[a] \subseteq [b]$.

Similarly we can show that $[b] \subseteq [a]$, and hence $[a] = [b]$.

(\Leftarrow): Assume $[a] = [b]$.

Now $a \in [a]$ and hence $a \in [b]$ implying that $a \equiv b \pmod{n}$.

Note: We can use Theorem 8 to show that two congruence classes modulo n are either equal or disjoint.

If they are disjoint, there is nothing to prove. If they are not disjoint, then there is at least $x \in [a] \cap [b]$, which in turn means that $x \equiv a \pmod{n}$ and $x \equiv b \pmod{n}$. Thus, $a \equiv b \pmod{n}$ by transitive and symmetric properties, and $[a] = [b]$ by Theorem 6.

Theorem 9

There are precisely n different congruence classes modulo n , $[0]$, $[1]$, $[2]$, \dots , $[n-1]$.

Proof

(*Outline only*) Recall from the previous chapter that any integer $a \equiv r \pmod{n}$, where r is the remainder when dividing a by n . Hence, for all integers $[a] = [r]$. Since r must be non-negative and less than n , then the possible values are $0, 1, 2, \dots, n-1$.

Definition 7

The set of all congruence classes modulo n is denoted by $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$.
(It is read as 'Z mod n'.)

For example, $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$.

Theorem 10

Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ imply the following:

- 1 $a + c \equiv b + d \pmod{m}$
- 2 $a - c \equiv b - d \pmod{m}$
- 3 $ac \equiv bd \pmod{m}$

Proof

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $m \mid (a - b)$ and $m \mid (c - d)$. These imply that $m \mid ((a - b) + (c - d))$. But this is the same as $m \mid ((a + c) - (b + d))$. This proves (1). Proof of (2) is similar. To prove (3), note that $m \mid (a - b) \Rightarrow m \mid c(a - b)$ and $m \mid (c - d) \Rightarrow m \mid b(c - d)$. Thus $m \mid (c(a - b) + b(c - d))$, which is the same as $m \mid (ac - bd)$. This completes the proof.

Note: Theorem 10 can be applied to a simpler case too, which we state overleaf without proof.



If $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, such that $a \equiv b \pmod{m}$, then the following hold:

- 1 $a + c \equiv b + c \pmod{m}$
- 2 $a - c \equiv b - c \pmod{m}$
- 3 $ac \equiv bc \pmod{m}$

Example 10

Apply the previous theorems to $23 \equiv 7 \pmod{8}$ using your own choice of numbers.

Solution

Let us consider adding 5 to both sides, i.e.

$$23 + 5 \equiv 7 + 5 \pmod{8} \Rightarrow 28 \equiv 12 \pmod{8}$$

Subtract 9:

$$23 - 9 \equiv 7 - 9 \pmod{8} \Rightarrow 14 \equiv -2 \pmod{8}$$

Multiply by 2:

$$23 \times 2 \equiv 7 \times 2 \pmod{8} \Rightarrow 46 \equiv 14 \pmod{8}$$

Does the converse of the previous theorem work?

For (1) and (2), the answer is obviously yes:

$$a + c \equiv b + c \pmod{m} \Rightarrow a + c - c \equiv b + c - c \pmod{m} \Rightarrow a \equiv b \pmod{m}$$

and

$$a - c \equiv b - c \pmod{m} \Rightarrow a - c + c \equiv b - c + c \pmod{m} \Rightarrow a \equiv b \pmod{m}$$

For (3), let us take an example:

$33 \equiv 12 \pmod{7} \Leftrightarrow 3 \times 11 \equiv 3 \times 4 \pmod{7}$. Cancel the 3 from both sides and you have

$$11 \equiv 4 \pmod{7}, \text{ which is true!}$$

However,

$$52 \equiv 12 \pmod{8} \Leftrightarrow 13 \times 4 \equiv 3 \times 4 \pmod{8} \text{ but } 13 \not\equiv 3 \pmod{8}.$$

In fact if c and m are relatively prime, then $ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$.

$$63 \equiv 15 \pmod{8} \Leftrightarrow 21 \times 3 \equiv 5 \times 3 \pmod{8} \text{ and } 21 \equiv 5 \pmod{8}$$

Theorem 11

If $[a] = [b]$, and $[c] = [d]$ in \mathbb{Z}_n , then

$$[a + c] = [b + d], \text{ and } [ac] = [bd].$$

Proof

$[a] = [b] \Rightarrow a \equiv b \pmod{n}$, and $[c] = [d] \Rightarrow c \equiv d \pmod{n}$, and hence by Theorem 8 $a + c \equiv b + d \pmod{n}$, and $ac \equiv bd \pmod{n}$; and hence by Theorem 8 $[a + c] = [b + d]$, and $[ac] = [bd]$.

Now we can define two new operations on the set \mathbb{Z}_n .

Definition 8

Addition and multiplication in \mathbb{Z}_n are defined by

$$[a] + [c] = [a + c] \text{ and } [a][c] = [ac].$$

Notation (1)

For convenience, and as long as it is clear from the context that we are in modulo n mode, we will use the symbol $+$ for addition modulo n . For multiplication modulo n , we will place the numbers next to each other rather than use symbols, so ab will mean $a \times b$.

In many sources, you will find that authors choose to attach the mod to the operation symbol such as $+_n$ for addition modulo n and \times_n for multiplication modulo n .

Example 11

In \mathbb{Z}_7 , perform the following operations:

$$[5] + [3], [4][6]$$

Solution

$$[5] + [3] = [5 + 3] = [8] = [1] \text{ since } [8] = [1 + 7] = [1]$$

$$[4][6] = [4 \cdot 6] = [24] = [3] \text{ since } [24] = [3 + 21]$$

Notation (2)

So far, we have been using $[a]$ to represent classes in \mathbb{Z}_n . However, whenever the context is clear that we are dealing with \mathbb{Z}_n , we will replace the class notation ' $[a]$ ' with a . In \mathbb{Z}_7 for instance we write 5 to indicate $[5]$ and we might say $5 + 4 = 2$ since we mean the classes and not the numbers themselves.



For example, here are the Cayley tables for addition in \mathbb{Z}_5 and multiplication in \mathbb{Z}_5 .

+	0	1	2	3	4	\times	0	1	2	3	4
0	0	1	2	3	4	0	0	0	0	0	0
1	1	2	3	4	0	1	0	1	2	3	4
2	2	3	4	0	1	2	0	2	4	1	3
3	3	4	0	1	2	3	0	3	1	4	2
4	4	0	1	2	3	4	0	4	3	2	1

Example 12

Determine whether $(\mathbb{Z}_6, +)$ is a group.

Solution

A Cayley table will be helpful in this exercise.

Closure has been discussed before. However, it is apparent from the table that all elements are members of \mathbb{Z}_6 , so the set is closed under addition modulo 6.

The identity element is also clear – it is 0.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Since 0 appears in every row and every column, then every element has its inverse. For example, the inverse of 2 is 4 and 3 is its own inverse.

Since we defined the addition of residue classes through addition of integers, the operation can be assumed to be associative.

Hence $(\mathbb{Z}_6, +)$ is a group.

Moreover, the operation is commutative and the group is an Abelian group.

Example 13

Determine whether the set $\{1, 3, 7, 9\}$ in \mathbb{Z}_{10} with multiplication modulo 10 is a group.

Solution

Again a Cayley table is helpful.

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

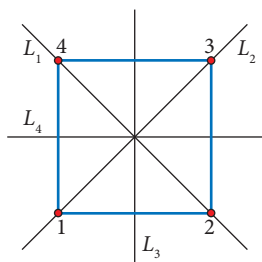
The set is closed under multiplication modulo 10.

Associativity is assumed.

The identity element is 1 since $1 \times a = a$ for all a in this set. This is clear from the table as the first row and the first column demonstrate that multiplying by 1 left the elements untouched.

1 and 9 are their own inverses, 7 is the inverse of 3 and vice versa.

The group is also Abelian.

Extended examples of groups**Symmetries of a square**

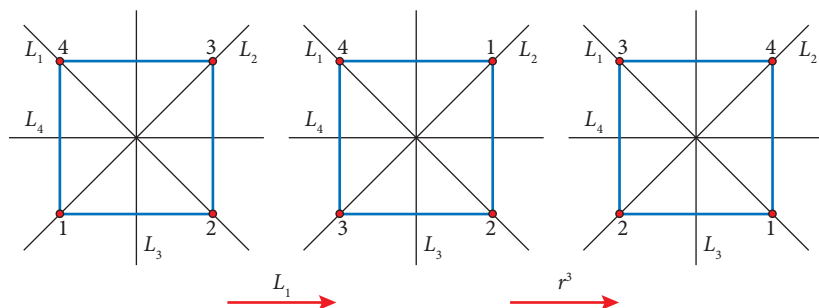
A square can be rotated counterclockwise through certain angles or reflected about certain lines, and it will end up with its original appearance. The corners, however, would have been moved. Rotation is centred at the centre of the square and the lines of reflection are the two lines through the diagonals, L_1 and L_2 , and the two lines through the vertical axis of symmetry, L_3 , and the horizontal axis, L_4 . Rotation is through multiples of 90° : $e = R_0$, $r = R_{90}$, $r^2 = R_{180}$, or $r^3 = R_{270}$. Notice that $R_{360} = R_0$.

The table right gives the results of performing any of these 'symmetries'.

Symmetry	Before	\rightarrow	After
e	4 3	$\xrightarrow{R_0}$	4 3
	1 2		1 2
r	4 3	$\xrightarrow{R_{90}}$	3 2
	1 2		4 1
r^2	4 3	$\xrightarrow{R_{180}}$	2 1
	1 2		3 4
r^3	4 3	$\xrightarrow{R_{270}}$	1 4
	1 2		2 3
L_1	4 3	$\xrightarrow{L_1}$	4 1
	1 2		3 2
L_2	4 3	$\xrightarrow{L_2}$	2 3
	1 2		1 4
L_3	4 3	$\xrightarrow{L_3}$	3 4
	1 2		2 1
L_4	4 3	$\xrightarrow{L_4}$	1 2
	1 2		4 3



These rotations and reflections are known as the **symmetries of a square**. If a reflection or rotation is followed by another reflection or rotation, the result can be one of the eight symmetries listed. For example, if L_1 is followed by r^3 , the result is equivalent to L_3 , i.e. $r^3 \circ L_1 = L_3$. See figure below.



We call the set of symmetries $D_4 = \{e, r, r^2, r^3, L_1, L_2, L_3, L_4\}$. The operation we are using in this set is composition of transformations, \circ . Cayley's table for all possible compositions of these transformations is given below. Notice that all the entries in the table are members of D_4 . This verifies the closure property for this set.

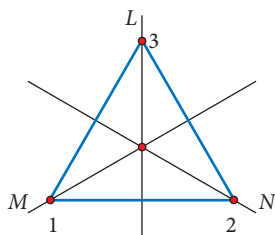
The composition of transformations is associative. Take, for example, $(rL_1)r^2$; this is r^2 followed by (rL_1) , which in turn is L_1 followed by r , that is, the whole composition is r^2 followed by L_1 followed by r , which means rL_1r^2 . We can argue similarly about $r(L_1r^2)$ and arrive at rL_1r^2 . So, the operation is associative.

\circ	e	r	r^2	r^3	L_1	L_2	L_3	L_4
e	e	r	r^2	r^3	L_1	L_2	L_3	L_4
r	r	r^2	r^3	e	L_4	L_3	L_1	L_2
r^2	r^2	r^3	e	r	L_2	L_1	L_4	L_3
r^3	r^3	e	r	r^2	L_3	L_4	L_2	L_1
L_1	L_1	L_3	L_2	L_4	e	r^2	r	r^3
L_2	L_2	L_4	L_1	L_3	r^2	e	r^3	r
L_3	L_3	L_2	L_4	L_1	r^3	r	e	r^2
L_4	L_4	L_1	L_3	L_2	r	r^3	r^2	e

Clearly e , which in essence is doing nothing, is the identity and as is apparent from the table, every element has an inverse since e appears in every row and column. For example, the inverse of r is r^3 and vice versa, while each L_i is its own inverse.

Therefore (D_4, \circ) is a group. Notice that $L_1r = L_3$ while $rL_1 = L_4$ and so the group is not Abelian. Non-commutativity can also be seen by observing that the table is not symmetric about the main diagonal.

Symmetries of an equilateral triangle

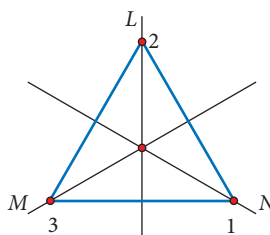


Another example of groups is the set of ‘symmetries’ in an equilateral triangle. There are three rotations, $I = R_0$, $R = R_{120}$, and $R^2 = R_{240}$, about the centroid, and there are three reflections around the lines through the three medians L , M , and N . We number the vertices as 1, 2, 3, so that you can discover what each transformation does.

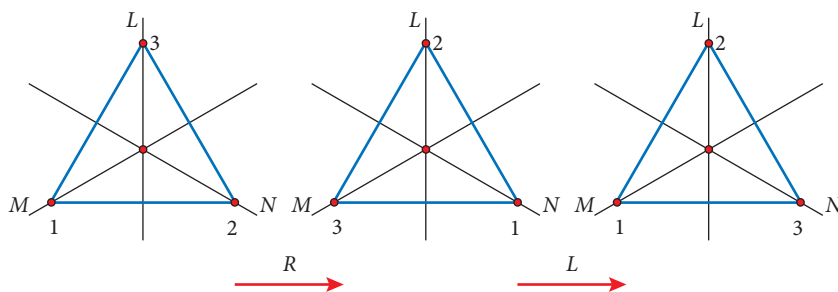
I does not change anything as expected.

R , for example, rotates the triangle around its centroid through an angle of 120° and so it takes 1 to the position taken by 2, 2 to the position of 3, and 3 to the position of 1 as shown in the diagram.

R^2 rotates the triangle through 240° . L reflects the triangle about its median L exchanging vertices 1 and 2 but keeping 3 untouched.



The composition of transformations can be looked at in a similar manner to the symmetries of the square and so the transformation LR is a rotation of 120° followed by a reflection in L , and so it is in essence a reflection in N and consequently we have $LR = N$. See figure below. (Remember that LR means that R is first, followed by L .)



Cayley's table below shows all possible compositions.

\circ	I	R	R^2	L	M	N
I	I	R	R^2	L	M	N
R	R	R^2	I	N	L	M
R^2	R^2	I	R	M	N	L
L	L	M	N	I	R	R^2
M	M	N	L	R^2	I	R
N	N	L	M	R	R^2	I

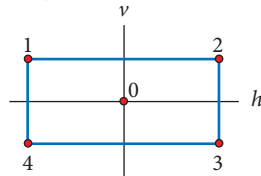


The set of six symmetries of the equilateral triangle with the operation of composition \circ , (D, \circ) forms a group. Here is why.

The elements of the table are all members of the set and hence it is closed. Obviously, I is the identity element. The identity transformation I is included in every row and column and hence every element has an inverse. And associativity is assumed in the composition of transformations.

Notice, however, that $ML = R \neq LM = R^2$, and hence it is not Abelian. (Also, the table is not symmetric about the main diagonal.)

Symmetries of a rectangle



The last example of symmetries concerns the set of symmetries of a rectangle. Similar to what we have done with the square and triangle, we will label the vertices of the rectangle with integers and observe the outcome of each symmetry transformation.

There are two reflections in the rectangle, one about its horizontal axis of symmetry, h , and one about its vertical axis, v . There is one rotation of 180° counterclockwise around its centre, r . Obviously, there is the identity symmetry, e . In total therefore, we only have four symmetries for the rectangle, e, r, h , and v . The group of symmetries for the rectangle is then $(\{e, r, h, v\}, \circ)$.

The table right gives the outcomes of these transformations.

Take rh for example; h results in $\begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$, and when followed by r we get $\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$ which is nothing but the outcome of v . Cayley's table for this group is given below.

\circ	e	r	h	v
e	e	r	h	v
r	r	e	v	h
h	h	v	e	r
v	v	h	r	e

Symmetry	Before	\rightarrow	After
e	$\begin{matrix} 1 & 2 \\ 4 & 3 \end{matrix}$	$\xrightarrow{R_0}$	$\begin{matrix} 1 & 2 \\ 4 & 3 \end{matrix}$
r	$\begin{matrix} 1 & 2 \\ 4 & 3 \end{matrix}$	$\xrightarrow{R_{180}}$	$\begin{matrix} 3 & 4 \\ 2 & 1 \end{matrix}$
h	$\begin{matrix} 1 & 2 \\ 4 & 3 \end{matrix}$	\xrightarrow{h}	$\begin{matrix} 4 & 3 \\ 1 & 2 \end{matrix}$
v	$\begin{matrix} 1 & 2 \\ 4 & 3 \end{matrix}$	\xrightarrow{v}	$\begin{matrix} 2 & 1 \\ 3 & 4 \end{matrix}$

Notice that, similar to the other cases before, the set is closed under the composition operation, an identity element exists, the operation is associative, and each element has its inverse. As you see above, the identity appears in every row and column, and each element is its own inverse. You notice that in this case, the entries are symmetric about the main diagonal, and hence the operation is commutative. Therefore, this group is an Abelian group.

3.3

Permutations

Unfortunately, the convention used here is not universal. In some resources you will find that, in permutations, contrary to the traditional function composition, the operation is done 'left to right', i.e. $\alpha\beta$.



In this section, we study certain groups of functions, called *permutation groups*, from set S to itself. Although groups of permutations of any non-empty set S exist, we will focus on the case where S is finite, $|S| = n$.

Definition 9

If S is a set, then a **permutation** on S is a bijection $\alpha: S \rightarrow S$. The set of all permutations on a set S is denoted by S_n . If $\alpha, \beta \in S_n$, we simplify the notation by writing $\alpha\beta$ for $\alpha \circ \beta$, and $\alpha\beta$ is referred to as the *product* of α and β rather than α composed with β .

In Chapter 2, we learned that if two functions are bijective, then their composition is also bijective, so the product of permutations is a binary operation on S_n by definition 9, because if α and β are two such permutations, then $\alpha\beta$ will also be a permutation and hence we are assigning for the ordered pair (α, β) an element $\alpha\beta \in S_n$. Moreover, since $\alpha\beta \in S_n$ the set is closed under this operation. Also, since $\alpha: S \rightarrow S$ is a bijection, then $\alpha^{-1}: S \rightarrow S$ exists and is a bijection and hence $\alpha^{-1} \in S_n$. If we let e be the identity function on S , then the following hold:

- 1 If $\alpha, \beta \in S_n$, then $\alpha\beta \in S_n$.
- 2 If $\alpha, \beta, \gamma \in S_n$, then $\alpha(\beta\gamma) = (\alpha\beta)\gamma$. Associativity of composition of bijections.
- 3 The identity function e is in S_n .
- 4 If $\alpha \in S_n$ then $\alpha^{-1} \in S_n$.

This shows that S_n is a group under the binary operation of function composition. This is known as the **permutation group** on S . Also, since we are focusing on finite sets, and if S has n elements, then S_n is the **symmetric group** on n elements.

For example, consider the set $S = \{a_1, a_2, a_3, a_4, a_5\}$ and define the permutation $\alpha \in S_5$ by

$\alpha(a_1) = a_5, \alpha(a_2) = a_1, \alpha(a_3) = a_2, \alpha(a_4) = a_4, \alpha(a_5) = a_3$. That is, we have the following correspondence:

$$a_1 \mapsto a_5, a_2 \mapsto a_1, a_3 \mapsto a_2, a_4 \mapsto a_4, a_5 \mapsto a_3.$$

This can be simplified by using only the subscripts, i.e.

$$\alpha(1) = 5, \alpha(2) = 1, \alpha(3) = 2, \alpha(4) = 4, \alpha(5) = 3. \text{ Or}$$

$$1 \mapsto 5, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 4, 5 \mapsto 3.$$

So, nothing is lost by using this simplification, and since this process can be done for any permutation in S_n , then S can be replaced by $\{1, 2, 3, 4, 5\}$ or in general $S = \{a_1, a_2, a_3, a_4, \dots, a_n\}$ can be replaced by $\{1, 2, 3, 4, \dots, n\}$.

For example, when you have a list of items to sort, you are essentially faced with the problem of finding a permutation of the objects that will put them in order after the permutation.



If we consider permutations of n objects, there are $n!$ of them. To understand this, first think through where object number 1 ends up. There are n possibilities for that. After the outcome of object 1 is determined, there are only $n - 1$ possible outcomes for object number 2. Thus, there are $n(n - 1)(n - 2) \dots 3 \cdot 2 \cdot 1 = n!$ permutations of a set of n objects.

For example, if we consider all possible rearrangements of the set $\{1, 2, 3\}$, there are $3! = 6$ of them. They are listed in the table below.

1	$1 \rightarrow 1$	$2 \rightarrow 2$	$3 \rightarrow 3$
2	$1 \rightarrow 2$	$2 \rightarrow 1$	$3 \rightarrow 3$
3	$1 \rightarrow 3$	$2 \rightarrow 2$	$3 \rightarrow 1$
4	$1 \rightarrow 1$	$2 \rightarrow 3$	$3 \rightarrow 2$
5	$1 \rightarrow 2$	$2 \rightarrow 3$	$3 \rightarrow 1$
6	$1 \rightarrow 3$	$2 \rightarrow 1$	$3 \rightarrow 2$

Here is one way to think about permutations (using permutations of three objects as an example). Imagine that there are three boxes labelled 1, 2, and 3. Initially, each contains a paper chip labelled with the same number: box 1 contains chip 1, and so on. A permutation is a rearrangement of the chips but in such a way that when you're done there is still only a single chip in each box.

In the table above, the notation $i \rightarrow j$ indicates that whatever was in box i moves to the box labelled j . So to apply permutation number 4 above means to take whatever chip is in box 2 and move it to box 3, to leave the contents of box 1 alone, and to take the chip from box 3 and put it into box 2. In other words, permutation number 4 above tells us to swap the contents of boxes 2 and 3.

The notation $i \rightarrow j$ is somewhat cumbersome to use, especially when the number of permutations is large. Below are the two possibilities for notation that we use in this book.

Notation

Two-row notation (array notation)

When we are investigating the permutation of objects in five boxes, we can write the permutation as

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

This indicates that the contents of box 1 move to box 5, the chip in box 2 moves to box 1, the chip in box 3 moves to box 2, box 4 is unchanged, and the chip in box 5 moves to box 3.

The benefit of this notation is that it is very easy to discover where everything goes.

This notation indicates that each member of the first row is mapped onto the corresponding member in the second row (directly beneath it).

Product (composition) of permutations

This notation is used to find the product of any two permutations in the following manner:

In S_5 , let $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$, then the product $\alpha\beta$ is the composition of α and β interpreted in the usual manner – β first, followed by α . So, for example,

$$\alpha\beta(1) = \alpha(5) = 3 \text{ and } \alpha\beta(3) = \alpha(2) = 1, \text{ etc.}$$

This process is done directly in the two-row notation.

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

Note that $\alpha\beta \neq \beta\alpha$. S_5 is therefore not Abelian. This can be generalized for S_n .

Note: The identity element of S_n is written in **two-row** notation as

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

This notation helps you find the inverse of each permutation. To find the inverse of any permutation read from the bottom row to the top row rather than top to bottom – so if 3 appears below 2 in a permutation α then 2 must appear below 3 in α^{-1} . Thus if

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \text{ then}$$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

The shortcoming of the 2-row notation is that it requires writing down each number twice. Since the top row can always be put in order, however, there is no real need to write it, so simply listing the second row is sufficient (assuming there is an obvious way to put the boxes in order).

Cycle notation

We can write the example above as (1 5 3 2).

This indicates that the contents of box 1 move to box 5, the contents of box 5 to box 3, the contents of box 3 to box 2, and the contents of box 2 back moves back into box 1. The system is called **cycle notation** since the contents of the boxes in parentheses move in a cycle: 1 to 5, 5 to 3, 3 to 2, and 2 back to 1. Notice that 4 does not appear as the contents of box 4 were unchanged! However, you can also write the above permutation as $(1\ 5\ 3\ 2)(4)$.

Permutations that do not move any items are often written as (1) .

Some permutations have more than one cycle. For example, the cycle notation for the permutation corresponding to:

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

is

$$(1\ 3)(2\ 5)$$

There are two cycles: 1 to 3 and 3 moves back to 1, while the other cycle takes 2 to 5 and 5 back to 2.

In cycle notation, it is not convenient to have duplicate elements in the various cycles that make up the permutation, so something like $(2\ 3)(2\ 5)$ is not usual. In such cases, the ‘product’ is simplified to give $(2\ 5\ 3)$.

As another example for notation, consider the permutation $(1\ 3\ 5)(2\ 7\ 6)$ of the numbers $\{1, 2, \dots, 7\}$. Again, notice that 4 is not included here, as it stays fixed. However, if you want, you can clarify its position by writing $(1\ 3\ 5)(2\ 7\ 6)(4)$.

Note also that the ordering does not matter as long as each item to be permuted appears only once, and that you can list a cycle starting with any member of it. All of the following specify precisely the same permutation:

$$(1\ 4\ 6)(3\ 5\ 9\ 7\ 8); (1\ 4\ 6)(5\ 9\ 7\ 8\ 3); (4\ 6\ 1)(9\ 7\ 8\ 3\ 5)\dots$$

Product of permutations using cycle notation

Let us take α and β from the example above.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}; \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$

Written in cycle notation they are

$$\alpha = (1\ 5\ 3\ 2) \text{ and } \beta = (1\ 5)(2\ 4\ 3)$$

Now for $\alpha\beta$, as we know from composition of functions, β must be applied first. 1 goes to 5, and 5 in α goes to 3, so we have so far $(1\ 3\dots)$

Now 3 in β goes to 2, but 2 in α goes to 1, and so 3 in the composition must go to 1. This closes the first part of the new cycle. So it is $(1\ 3)$. Next in β is 2, which goes to 4, followed by 4 in α , which is fixed. Thus, we have



Another possible form of the cycle notation is $(1, 5, 3, 2)$. This form may be helpful when we have 10 or more elements.



Notice also that $(1\ 3\ 5)(2\ 7\ 6)$ or $(2\ 7\ 6)(1\ 3\ 5)$ are equivalent, i.e. the product of ‘disjoint’ permutations is commutative.

(2 4). Hence, our final result will be (1 3)(2 4) which is the same result as above when written in two-row notation.

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

Similarly for $\beta\alpha$ we have: 1 goes to 5 in α and 5 goes to 1 in β and hence 1 goes to 1 in the composition, and so it is fixed. Next, 5 in α goes to 3 and 3 in β goes to 2, so we have so far (5 2...). However, 2 in α goes to 1 and 1 in β goes to 5 and so 2 goes to 5 in the composition, closing this part too, i.e. (2 5). Next in α we have 3, which goes to 2, but 2 in β goes to 4, and so 2 goes to 4 in the composition. Hence, we have (3 4...) in the composition. Knowing that 4 is fixed in α and 4 goes to 3 in β closes this part too and we have (3 4). Thus $\beta\alpha = (2 5)(3 4)$, which is the same result as above:

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

Example 14

Now try (1 3 4 2)(3 6 4 5)(1 6 2 3). Remember that we read from right to left!

Solution

$1 \rightarrow 6, 6 \rightarrow 4, 4 \rightarrow 2$, so $1 \rightarrow 2$

$2 \rightarrow 3, 3 \rightarrow 6, 6 \rightarrow 6$, so $2 \rightarrow 6$

$6 \rightarrow 2, 2 \rightarrow 2, 2 \rightarrow 1$, so $6 \rightarrow 1$, and this cycle closes, (1 2 6).

Next, we take the smallest number left in (1 6 2 3), 3.

$3 \rightarrow 1, 1 \rightarrow 1, 1 \rightarrow 3$, so $3 \rightarrow 3$, and 3 is fixed here.

$4 \rightarrow 4, 4 \rightarrow 5, 5 \rightarrow 5$, so $4 \rightarrow 5$

$5 \rightarrow 5, 5 \rightarrow 3, 3 \rightarrow 4$, and so $5 \rightarrow 4$, and this cycle closes too as (4 5).

Therefore, the product is:

$$(1 2 6)(4 5).$$

In 2-row notation, this could have been done in two stages:

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

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

This is the same product as above.

Example 15

If $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}$, show that $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$ is the inverse of α .

Solution

If $\gamma = \alpha^{-1}$, then their product must be e .

$$\alpha\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e.$$

Inverse of a permutation

Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 6 & 7 & 8 & 3 & 4 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 8 & 1 & 4 & 5 & 6 \end{pmatrix}$

Take the product $\alpha\beta$:

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = e$$

You can verify that this is true. It is also clear that

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = e$$

This is obviously an indication that α and β are inverses of each other.

Comparing the two permutations, you can see clearly that in order to get the inverse of a permutation, you simply swap the two rows and rearrange the top row in numerical order!

In cycle notation, to find the inverse of a permutation, list the numbers in reverse order. For example α , written in cycle notation is $\alpha = (1\ 5\ 7\ 3)(4\ 6\ 8)$ and hence $\alpha^{-1} = (8\ 6\ 4)(3\ 7\ 5\ 1)$ which is β !

Inverse of a permutation

To find the inverse of a permutation α , we can use one of the two forms:

- If α is in the array form, then swap row 1 with row 2, then rearrange the new row 1 in numerical order.
- If α is in cycle form, write the representation of α down in reverse order. That is, reverse the order in which the numbers appear in each cycle as well as the order of the cycles themselves.

Example 16

Find the inverse of $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$.

Solution

First swap rows.

$$\alpha^{-1} = \begin{pmatrix} 3 & 1 & 2 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

We now arrange the top row.

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

In cycle notation, $\alpha = (1\ 3\ 2)(4\ 5)$.

Hence, $\alpha^{-1} = (2\ 3\ 1)(5\ 4) = (1\ 2\ 3)(4\ 5)$, which is the same as above.

Inverse of a product of permutations

Since, as we have seen above, a permutation is a function, therefore it also obeys function rules.

Theorem 12

If α and β are two permutations defined on a set S , then $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$.

Proof

The proof follows from basic function rules.

$$\begin{aligned} (\alpha\beta)(\beta^{-1}\alpha^{-1}) &= \alpha(\beta\beta^{-1})\alpha^{-1} \text{ associativity of composition} \\ &= \alpha e \alpha^{-1} = \alpha\alpha^{-1} = e, \text{ also} \end{aligned}$$

$$(\beta^{-1}\alpha^{-1})(\alpha\beta) = \beta^{-1}(\alpha^{-1}\alpha)\beta = e$$

Thus, $\beta^{-1}\alpha^{-1}$ is the inverse of $\alpha\beta$

Order of a permutation

Composing (multiplying) different permutations leads to the question of composing a permutation with itself. For a permutation α , taking its product with itself $\alpha\alpha$ can be written as α^2 . In fact, the product of α with itself n -times is written as α^n .

Take for example the permutation

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

A few 'powers' of α are:

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

$$\alpha^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

$$\alpha^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$$

$$\alpha^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

As a result of the property above, the **cancellation law** for permutation multiplication is valid. That is

$$\alpha\beta = \alpha\gamma \Leftrightarrow \beta = \gamma$$

The proof is straightforward: you multiply (from left) both sides of the equation by α^{-1} .

$$\alpha^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e$$

Definition

For any permutation α , there exists a positive integer n such that $\alpha^n = e$. The smallest number n is called the order of the permutation.

In the previous example, the order of α is 6. We write $\text{ord}(\alpha) = 6$

Example

Consider the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$ as shown above earlier. Write it in cycle notation.

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

Notice here that we have a 2-cycle and a 3-cycle, while the order of the permutation is 6. This is a demonstration of the following theorem.

Theorem (Proof not included)

The order of a permutation written in disjoint cycle form is the *least common multiple of the lengths of the cycles*.

Example

Consider the permutation $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 4 & 3 & 8 & 1 & 2 \end{pmatrix}$ Write it in cycle notation, and verify that its order is 12.

The cycle notation for β is $(1\ 5\ 3\ 7)(2\ 6\ 8)$. 4 is fixed.

Since the length of the first cycle is 4 and the length of the second cycle is 3, then the order of β is 12.

$$\beta = (1\ 5\ 3\ 7)(2\ 6\ 8) \Rightarrow \beta^2 = (1\ 5\ 3\ 7)^2(2\ 6\ 8)^2 = (1\ 3)(5\ 7)(2\ 8\ 6)$$

$$\beta^3 = [(1\ 5\ 3\ 7)(2\ 6\ 8)] [(1\ 3)(5\ 7)(2\ 8\ 6)] = (1\ 7\ 3\ 5)$$

$$\beta^4 = [(1\ 5\ 3\ 7)(2\ 6\ 8)] [(1\ 7\ 3\ 5)] = (2\ 6\ 8)$$

$$\beta^8 = (2\ 6\ 8)(2\ 6\ 8) = (2\ 8\ 6)$$

Finally, $\beta^{12} = (2\ 8\ 6)(2\ 6\ 8) = e$.

Summary of properties of permutations

Here are some properties of permutations. Some have been discussed earlier and some are stated without formal proof.

- 1 Every permutation can be written as a product of disjoint cycles.

- 2 Disjoint cycles commute. That is, If $\alpha, \beta \in S_n$ and have no numbers in \mathbb{Z}_n that are moved by both α and β then $\alpha\beta = \beta\alpha$. In other words, if the disjoint cycle form of α has no number in common with the disjoint cycle form of β , then α and β commute.
- 3 Since a permutation is a bijective mapping (injective and surjective function) and the product is a composition of function, then the product of permutations is associative. That is $\alpha(\beta\gamma) = (\alpha\beta)\gamma$, and thus we simply write $\alpha\beta\gamma$ for the product!
- 4 $|S_n| = n!$ That is, there are $n!$ different permutations for a set of size n .
- 5 The identity permutation is $e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$. Its cycle form is (1) and when it is multiplied by any element of S_n the result is that element itself. Thus,

$$e\alpha = \alpha e = \alpha \text{ for every } \alpha \in S_n.$$
- 6 Every $\alpha \in S_n$ has an inverse α^{-1} such that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$.
- 7 Permutation composition (multiplication) is not necessarily commutative.
- 8 The **cancellation law** for permutation multiplication is valid. That is $\alpha\beta = \alpha\gamma \Leftrightarrow \beta = \gamma$.

Example 17

Show that the number of elements in S_n is $n!$. (This is also the **order** of S_n .)

Solution

Any member of S_n is of the form

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ - & - & - & - & \cdots & - \end{pmatrix}.$$

The number of elements in S_n is equal to the number of different ways we can place the numbers 1, 2, 3, ..., n in the blanks of the second row. This is nothing but the number of permutations of n objects and hence it is $n!$. Permutation of objects without replacement has been covered in the core part of your course.

Example 18

Consider S_3 , the symmetric group on 3 elements. Draw a Cayley table and verify that it is a group.

Solution

There are $3!$ elements for the set S_3 . Let us use p_i to represent the different elements. For example,



$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ and } p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Here is a Cayley table for this group under function composition.

\circ	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_5	p_6	p_3	p_4
p_3	p_3	p_4	p_1	p_2	p_6	p_5
p_4	p_4	p_3	p_6	p_5	p_1	p_2
p_5	p_5	p_6	p_2	p_1	p_4	p_3
p_6	p_6	p_5	p_4	p_3	p_2	p_1

Notice that p_1 is the identity, since it leaves the other permutations ‘untouched’ when it is composed with each. Since p_1 appears in every row and column, then we can say that there is an inverse for each element.

Associativity is assumed. Also, since the table is not symmetric about the main diagonal, we notice that the group is not Abelian.

Example 19

Let G be the set of functions $\{f, g, h, i, j, k\}$ defined below with the binary operation of function composition.

The functions are defined from $\mathbb{R} \setminus \{0, 1\}$ to $\mathbb{R} \setminus \{0, 1\}$.

$$f(x) = \frac{1}{1-x}, g(x) = \frac{x-1}{x}, h(x) = \frac{1}{x}, i(x) = x, j(x) = 1-x, k(x) = \frac{x}{x-1}.$$

Is (G, \circ) a group?

Solution

$$f(g(x)) = \frac{1}{1 - \frac{x-1}{x}} = \frac{x}{1} = x = i(x); f(h(x)) = \frac{1}{1 - \frac{1}{x}} = \frac{x}{x-1} = k(x);$$

$$f(j(x)) = \frac{1}{1 - (1-x)} = \frac{1}{x} = h(x); f(k(x)) = \frac{1}{1 - \frac{x}{x-1}} = \frac{x-1}{-1} = 1-x = j(x)$$

Similarly, we can find the rest of the results. Here is the Cayley table for this group.

\circ	i	f	g	h	j	k
i	i	f	g	h	j	k
f	f	g	i	k	h	j
g	g	i	f	j	k	h
h	h	j	k	i	f	g
j	j	k	h	g	i	f
k	k	h	j	f	g	i

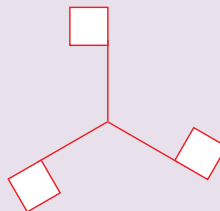
- The set is closed under composition.
- i is the identity element.
- Each element has an inverse as i appears in every row and column.
- Composition is associative.

The group is not Abelian as $g \circ h = j \neq h \circ g = k$.

Note: Try to see how this group is similar to S_3 . One way is to set up some correspondence between the elements of this group and those of S_3 . For example, $i \leftrightarrow p_1$, etc. We will leave that as an exercise for you.

Exercise 3

- 1 Suppose rotations of the figure (below) of $0, \frac{2\pi}{3}$, and $\frac{4\pi}{3}$ are denoted by 0, 2, and 4 respectively.



- Show that the set $\{0, 2, 4\}$ forms a group under the operation of transformation composition.
 - Construct a Cayley table for the group.
 - Is this an Abelian group?
- 2 Let the operation \boxtimes be defined by $x \boxtimes y = xy^2$ over \mathbb{Z} .
- Find the value of
 - $3 \boxtimes 5$
 - $5 \boxtimes 3$
 - $2 \boxtimes 2$
 - $0 \boxtimes -4$
 - $1 \boxtimes 3$
 - $3 \boxtimes 1$
 - $2 \boxtimes (3 \boxtimes 4)$
 - $(2 \boxtimes 3) \boxtimes 4$
 - Is $x \boxtimes y = y \boxtimes x$ for all values? If not, for what values?
 - Is $(x \boxtimes y) \boxtimes z = x \boxtimes (y \boxtimes z)$?

- 3** Show that addition modulo n is commutative and associative.
- 4** Find and set up a Cayley table for 'symmetries' in a rhombus.
- 5** Consider a set $A = \{a, b\}$. Let $M(A)$ be the set containing the following mappings on the elements of A :
- $$p(a) = a, p(b) = a; r(a) = a, r(b) = b; s(a) = b, s(b) = a; t(a) = b, t(b) = b.$$
- a** Construct a Cayley table for composition ' \circ ' as an operation on $M(A) = \{p, r, s, t\}$.
- b** Which is the identity element? Why?
- c** Is \circ commutative as an operation on $M(A)$?
- d** Which elements of $M(A)$ are invertible?
- e** Is $(M(A), \circ)$ a group?
- 6** Consider a set $A = \{a, b, c\}$. Let $M(A)$ be the set containing the following mappings on the elements of A :
- $$p(a) = a, p(b) = b, p(c) = c; r(a) = b, r(b) = a, r(c) = c; s(a) = a, s(b) = a, s(c) = a; t(a) = b, t(b) = b, t(c) = b.$$
- a** Construct a Cayley table for composition ' \circ ' as an operation on $M(A) = \{p, r, s, t\}$.
- b** Which is the identity element? Why?
- c** Is \circ commutative as an operation on $M(A)$?
- d** Which elements of $M(A)$ are invertible?
- e** Is $(M(A), \circ)$ a group?

In questions 7–14, decide whether the given set forms a group under the given operation. If it does, describe the group, and if it does not, justify.

- 7** $\{-1, 1\}$ and multiplication.
- 8** $\{-1, 0, 1\}$ and addition.
- 9** $\{n \mid n = 10k \text{ where } k \in \mathbb{Z}\}$ and addition.
- 10** $\{x = 2^m \mid m \in \mathbb{Z}\}$ and multiplication.
- 11** $\{x = 2^m 3^n \mid m, n \in \mathbb{Z}\}$ and multiplication.
- 12** M , the set of all mappings from \mathbb{R} to \mathbb{R} . Define the operation of addition $f + g$ for any mappings $f, g \in M$, by
- $$(f + g)(x) = f(x) + g(x) \quad \forall x \in \mathbb{R}.$$
- 13** $\mathbb{R} \setminus \{-1\}$, where the operation $*$ is defined by
- $$a * b = a + b + ab.$$
- 14** $\{x \mid x = a + b\sqrt{2}\}$, where a and b are both rational numbers not both 0. The operation is ordinary multiplication.
- 15** Show that if a and b are in the same group $(G, *)$, then the equation $a * x = b$ has exactly one solution.
- 16** Let $(M, *)$ be a group with the rule that $\forall a, b \in M, a^2 * b^2 = (a * b)^2$. Show that $(M, *)$ is Abelian.

- 17** S_4 is the group of permutations of 4 elements under the operation of function composition.
- Find the order of the group and justify your answer.
 - List all the elements of the group and construct a Cayley table for the operation.
 - Show that the group is not Abelian.
- 18** Let M be the set of matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $a, b, c \in \mathbb{R}$ and $a \neq 0$ and $c \neq 0$.
- Prove that M is a group under matrix multiplication.
 - Show that this group is not Abelian.
 - Consider the case where $a = c = 1$. Let N be the set of such matrices. Show that N under matrix multiplication is an Abelian group.
- 19** Consider the set $M = \{1, 3, 9, 11\}$ under multiplication modulo 16. Denote this multiplication simply by \times .
- Show that $3 \times (9 \times 11) = (3 \times 9) \times 11$.
 - Show that (M, \times) is a group.
 - Is this a cyclic group? If yes, find all generators.
- 20** Complete the following table in a way that makes the operation commutative.

\circ	a	b	c	d
a	a	b		d
b		c		
c	c	d	a	b
d		a		c

Is the set $\{a, b, c, d\}$ an Abelian group under this operation?

- 21** Complete the following table in a way that makes the set $\{w, x, y, z\}$ an Abelian group under the operation given by the table.

\circ	w	x	y	z
w	y			x
x	z	w		
y				
z				w

- 22** Prove that the set of 2×2 matrices with real coefficients is an Abelian group under matrix addition.

23 Let $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

Compute each of the following:

- $b \circ a$
- $a \circ b$
- a^{-1}
- b^{-1}
- $b^{-1} \circ a^{-1}$
- $a^{-1} \circ b^{-1}$
- $(b \circ a)^{-1}$
- $(a \circ b)^{-1}$

- 24** Repeat question 23 using

$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$.

25 Let $E = \{x \mid x = 2k, k \in \mathbb{Z}\}$ and consider the binary operation \odot defined by

$$\forall (a, b), (c, d) \in \mathbb{Z} \times E, (a, b) \odot (c, d) = (a + c, b + d).$$

Prove that $(\mathbb{Z} \times E, \odot)$ is an Abelian group.

26 Let $(A, *)$ be an Abelian group with identity element e . Define on A a new binary operation \odot defined by

$$a \odot b = a * b * c, \forall a, b \in A \text{ and } c \text{ is a specific element of } A \text{ distinct from } e.$$

Show that (A, \odot) is an Abelian group.

27 Consider the group $(G, *)$ with identity element e . Define a relation, \mathcal{R} , on the elements of G :

$$\text{If } a, b \in G, \text{ then } b \mathcal{R} a, \text{ if } \exists x \in G \text{ such that } b = x * a * x^{-1}.$$

a Show that \mathcal{R} is an equivalence relation.

b For a given element a , consider the function $f: G \rightarrow G$, such that

$$f(x) = a^{-1} * x * a.$$

Show that f is a bijection.

28 $(G, *)$ is a group such that $\forall x \in G, x * x = e$. Show that $(G, *)$ is Abelian.

29 $(G, *)$ is a group such that $\forall x, y \in G, (x * y)^2 = x^2 * y^2$. Show that $(G, *)$ is Abelian.

30 $(G, *)$ is a group such that $\forall x, y \in G, (x * y)^{-1} = x^{-1} * y^{-1}$. Show that $(G, *)$ is Abelian.

31 A teacher was typing a paper in which he wanted to include a list of 9 integers that form a group under multiplication modulo 91. Inadvertently he left out one of the integers and his list appeared with the following 8 numbers:

1, 9, 16, 22, 53, 74, 79, 81

Which integer was left out?

32 Find $\alpha\beta$ and $\beta\alpha$ when

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}.$$

33 If $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$.

a Find α^2 , α^4 , and α^6 .

b Write α in cycle notation.

c Find the inverse of α and verify your answer by multiplication of the two permutations.

34 Consider the following three permutations.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 7 & 1 & 5 & 8 & 2 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

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

Write each permutation in cycle form, and find each of the following.

a $\alpha\beta$

b $\alpha\beta\gamma$

c β^{-1}

d $(\beta\gamma)^{-1}$

e $\gamma^{-1}\beta^{-1}$

f $\alpha^{-1}\gamma\alpha$

g $\text{ord}(\gamma)$

h $\text{ord}(\alpha^{-1}\gamma\alpha)$

35 Change to cycle notation.

a $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 7 & 4 & 5 & 6 & 3 & 1 & 2 & 10 & 9 \end{pmatrix}$

b $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 9 & 11 & 4 & 8 & 15 & 5 & 3 & 7 & 2 & 6 & 1 & 12 & 13 & 14 \end{pmatrix}$

36 Change the cycle notation of the S_9 members given below into two-row notation.

a (1 3 5 7 9)

b (1 5 2)(3 4)(7 8 9)

c (1 7 4 6)(3 5 9 8)

Practice questions 3

1 Show that the set $H = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a = \pm 1, \text{ and } b \in \mathbb{Z} \right\}$ forms a group under matrix multiplication.

(You may assume that matrix multiplication is associative.)

2 a Prove that the set of matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

where $a, b, c \in \mathbb{R}$, is a group under matrix multiplication.

b Show that this group is Abelian if and only if there exists a real constant k such that $c = ka$.

3 The binary operation $a * b$ is defined by $a * b = \frac{ab}{a+b}$, where $a, b \in \mathbb{Z}^+$.

a Prove that $*$ is associative.

b Show that this binary operation does not have an identity element.

4 Let the matrix T be defined by $\begin{pmatrix} x & x+2 \\ x-5 & -x \end{pmatrix}$ such that $\det T = 1$.

a i Show that the equation for x is $2x^2 - 3x - 9 = 0$.

ii The solutions of this equation are a and b , where $a > b$.

Find a and b .

b Let A be the matrix where $x = 3$.

i Find A^2 .

ii Assuming that matrix multiplication is associative, find the smallest group of 2×2 matrices which contains A , showing clearly that this is a group.

5 The set $S = \{a, b, c, d\}$ forms a group under each of two operations $\#$ and $*$, as shown in the following group tables.

#	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

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



a Copy and complete the second table.

b Solve the following equations for x .

i $(b \# x) * c = d$

ii $(a * (x \# b)) * c = b$

6 Consider the group (H, \bullet) with identity element e .

a For $x, y \in H$, show that $(x \bullet y)^{-1} = y^{-1} \bullet x^{-1}$.

b Given $x, y \in H$, the relation R is defined as follows:

$xRy \Leftrightarrow$ there exists $z \in H$ such that $x = z \bullet y \bullet z^{-1}$.

Determine whether or not R is an equivalence relation.

7 The permutations p_1 and p_2 of the integers $\{1, 2, 3, 4, 5\}$ are given by

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \text{ and } p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}.$$

a Find the order of p_1 .

b i Find $p_2 p_1$, the composite permutation p_1 followed by p_2 .

ii Determine whether or not p_1 and p_2 commute under composition of permutations.

c Find $(p_1^2 p_2)^{-1}$.

8 a and b are elements of the group G whose binary operation is multiplication.

a Use mathematical induction to prove that $(bab^{-1})^n = ba^n b^{-1}$, for all $n \in \mathbb{Z}^+$.

b Show that $(bab^{-1})^{-1} = ba^{-1}b^{-1}$.

c Use parts **a** and **b** to show that $(bab^{-1})^n = ba^n b^{-1}$ for all negative integers n .

9 The binary operation $*$ is defined for $a, b \in \mathbb{Z}^+$ by

$$a * b = a + b - 2.$$

a Determine whether or not $*$ is

i closed

ii commutative

iii associative.

b i Find the identity element.

ii Find the set of positive integers having an inverse under $*$.

10 a The relation aRb is defined on $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ if and only if ab is the square of a positive integer.

i Show that R is an equivalence relation.

ii Find the equivalence classes of R that contain more than one element.

b Given the group $(G, *)$, a subgroup $(H, *)$ and $a, b \in G$, we define $a \sim b$ if and only if $ab^{-1} \in H$. Show that \sim is an equivalence relation.

Groups II

4.1 Introduction

In this chapter, we will discuss further properties of groups along with subgroups and relations among groups.

Definition 1

An element a in a group $(G, *)$ is said to have a **finite order** if $a^m = e$ for some $m \in \mathbb{Z}^+$. In such cases, the **order of the element a** , denoted by $|a|$, is the **smallest** positive integer n such that $a^n = e$. An element a is said to have **infinite order** if $a^m \neq e$ for **every** $m \in \mathbb{Z}^+$.

Example

- In the group $(\mathbb{R} \setminus \{0\}, \times)$, 3 has **infinite order** because $3^m \neq 1$ for **every** $m \in \mathbb{Z}^+$.
- In the group $\{1, -1, i, -i\}$ where $i^2 = -1$, under complex multiplication, the order of i is 4 because $i^4 = 1$, and the order of (-1) is 2 since $(-1)^2 = 1$. Obviously the order of 1 is 1.

- In the group $SL_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } ad - bc = 1 \right\}$,

described in Chapter 3, the element $A = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$

has order 12 because 12 is the smallest positive integer where

$$A^{12} = \left(\begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} \right)^{12} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2. \text{ So, we can write } |A| = 12.$$

- In the additive group $(\mathbb{Z}_6, +)$ the element 2 has order 3 because $2 + 2 + 2 = 0$, while $|5| = 6$ since $5 + 5 + 5 + 5 + 5 + 5 = 0$.
- In the group $\{1, 3, 7, 9\}$ in \mathbb{Z}_{10} with multiplication modulo 10, $|3| = 4$ since $3^4 = 1$ and $|9| = 2$.



Notice in the example above that the order of the identity is always 1. For example, $\left| \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right| = 1$. Also, notice in the fifth instance of the example, $3^8 = 1$, $3^{12} = 1$, etc. and $9^4 = 1$, $9^6 = 1$, etc. These are manifestations of the following theorem.

Theorem 1

Let a be an element in a Group (G, \cdot) , then:

- 1 If a has a *finite order* n , then $a^m = e$ if and only if $n \mid m$, i.e. m is a multiple of n .
- 2 $a^p = a^q$ if and only if $p \equiv q \pmod{n}$.
- 3 If a has infinite order, then all a^i (i is an integer) are different. (This means $a^i \neq a^j$ when $i \neq j$.)

Proof

- 1 If $n \mid m$, then we can write $m = kn$ for some integer k , and hence $a^m = a^{kn} = (a^n)^k = e^k = e$.

Conversely, if $a^m = e$, then by the division algorithm, $m = nq + r$ with $0 \leq r < n$, thus

$$a^m = a^{nq+r} = a^{nq} a^r = (a^n)^q a^r = e a^r = a^r = e,$$

but since n is the order of a , it is by definition the smallest integer with $a^n = e$. Hence, with $r < n$, $a^r = e$ is only possible if $r = 0$, and therefore $m = nq + 0$, i.e. $n \mid m$.

- 2 If $a^p = a^q$, then $a^p a^{-q} = a^q a^{-q} \Rightarrow a^{p-q} = a^0 = e$. By (1) $a^{p-q} = e$ is only possible if $n \mid (p - q)$, thus $p \equiv q \pmod{n}$ by definition of congruence modulo n .
- 3 We show this with indirect proof: suppose not all a^i are different, then there will be at least two values, x and y , with $x > y$ (you can also use $x < y$), such that

$$a^x = a^y \text{ which implies that } a^{x-y} = e \text{ (using (2) above).}$$

This in turn implies that $x \equiv y \pmod{n} \Rightarrow n$ is the order of the element, but the element has infinite order, which is a contradiction and therefore $a^x \neq a^y$.

Note: As a result of Theorem 1, we can conclude the following:

- 1 If $|a| = n$, and $n = kr$ with $r > 0$, then $|a^r| = k$.
- 2 If $a^x = a^y$ with $x \neq y$, then a must have a **finite order**.

Example

In the SL_2 group in the previous example, we used $A = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$ and showed that $|A| = 12$.

Now, $B = A^4 = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$. Now,

$$B^3 = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \text{ which verifies (1) above.}$$

The order of group elements has several uses in the following sections.

4.2**Subgroups**

You may have noticed from examples or exercises that some groups are subsets of others with the same binary operation. The group SL_2 under matrix multiplication is a subset of the group GL_2 under matrix multiplication. The following definition describes this phenomenon.

Definition 2

If a non-empty subset H of a group G is itself a group under the binary operation of G , we call H a **subgroup** of G . If $H \subset G$ then H is a **proper subgroup** of G . If $H \subseteq G$, then H is a subgroup of G .

Every group has at least two **subgroups**, $(\{e\}, *)$ and $(G, *)$ itself. $(\{e\}, *)$ is usually called the **trivial subgroup**, and the rest of the subgroups are **non-trivial**. Aside from these two subgroups, all other subgroups are **proper**.

The **notation** for a subgroup can be the same as subsets, and thus the context of the discussion will determine whether $H \subseteq G$ refers to a subset or a group.

Example

Let G be the group $\{0, 1, 2, 3, 4, 5, 6, 7\}$ under addition modulo 8. We will rearrange the elements in a Cayley table so that the subgroups will become apparent. Here is the table:

+	0	2	4	6	1	3	5	7
0	0	2	4	6	1	3	5	7
2	2	4	6	0	3	5	7	1
4	4	6	0	2	5	7	1	3
6	6	0	2	4	7	1	3	5
1	1	3	5	7	2	4	6	0
3	3	5	7	1	4	6	0	2
5	5	7	1	3	6	0	2	4
7	7	1	3	5	0	2	4	6

This group, as you notice, has two non-trivial subgroups: $A = \{0, 2, 4, 6\}$ and $B = \{0, 4\}$. B is a subgroup of A too.

Example

Consider the group of symmetries of the square (D_4, \circ) which we developed in Chapter 3. Looking at the Cayley table, it is clear that rotations with the identity constitute a subgroup, while the reflections with the identity do not constitute a subgroup. Notice here that the subgroup of rotations consists of ‘powers’ of r . That is, the group is made up of $\{e = r^0, r, r^2, r^3\}$. Such a subgroup is called a *cyclic*¹ subgroup of D_4 generated by r .

\circ	e	r	r^2	r^3	L_1	L_2	L_3	L_4
e	e	r	r^2	r^3	L_1	L_2	L_3	L_4
r	r	r^2	r^3	e	L_4	L_3	L_1	L_2
r^2	r^2	r^3	e	r	L_2	L_1	L_4	L_3
r^3	r^3	e	r	r^2	L_3	L_4	L_2	L_1
L_1	L_1	L_3	L_2	L_4	e	r^2	r	r^3
L_2	L_2	L_4	L_1	L_3	r^2	e	r^3	r
L_3	L_3	L_2	L_4	L_1	r^3	r	e	r^2
L_4	L_4	L_1	L_3	L_2	r	r^3	r^2	e

Theorem 2

For any group $(G, *)$, if $x \in G$, then the subset of G , X defined by $X = \{x^k \mid k \in \mathbb{Z}\}$, is a subgroup of G and is known as the **cyclic subgroup** generated by x . x is also called the **generator** of this subgroup. This will be proved after the subgroup tests.

¹ Cyclic groups are discussed later in the chapter (page 1310).

Subgroup tests

When deciding whether a subset H of a group G is a subgroup of G , we do not need to apply the definition and verify the group axioms. There are a few theorems that will simplify the process.

Note: For the rest of this chapter, we will not be using any specific symbols to denote the operation. So for two elements a and b , we will write ab when we mean $a * b$.

Theorem 3

Let G be a group and H a non-empty subset of G . Then, H is a subgroup of G iff $ab^{-1} \in H$ whenever $a, b \in H$.

Proof

- If H is a subgroup of G : If $a, b \in H$, then b has an inverse $b^{-1} \in H$ by definition of a group, and since H is closed under the binary operation $ab^{-1} \in H$.
- Conversely, suppose that H is a non-empty subset of G where $ab^{-1} \in H$, whenever $a, b \in H$.
 - Let $a = b$, then whenever $a, b \in H$ and $ab^{-1} = aa^{-1} = e \in H$ and the identity axiom is verified.
 - Now, $e, a \in H$, and hence $ea^{-1} = a^{-1} \in H$, and the inverse axiom is verified.
 - Now, since H includes inverses, when $a, b \in H$, then $a, b^{-1} \in H$, and hence $a(b^{-1})^{-1} = ab \in H$. So the closure axiom is verified.
 - Associativity is inherited from G .

Therefore, the set H is a subgroup of G .

Example 1

A group (M, Δ) has identity element i . N is a subset of M defined by

$$N = \{x \in M \mid x \Delta m = m \Delta x, \text{ for all } m \in M\}.$$

Show that N is a subgroup of M .

Solution

Let $a, b \in N$. We need to show that $a \Delta b^{-1} \in N$, i.e. we need to show that for all $m \in M$,

$$(a \Delta b^{-1}) \Delta m = m \Delta (a \Delta b^{-1}).$$

Now, let us first show that if $b \in N$ then $b^{-1} \in N$.



Since i is an element of M , then

$$\begin{aligned}
 m \Delta i &= i \Delta m \Rightarrow m \Delta (b \Delta b^{-1}) = (b \Delta b^{-1}) \Delta m && \text{Identity axiom} \\
 \Rightarrow (m \Delta b) \Delta b^{-1} &= b \Delta (b^{-1} \Delta m) && \text{Associativity} \\
 \Rightarrow (b \Delta m) \Delta b^{-1} &= b \Delta (b^{-1} \Delta m) && \text{Since } b \in N \\
 \Rightarrow b \Delta (m \Delta b^{-1}) &= b \Delta (b^{-1} \Delta m) && \text{Associativity} \\
 \Rightarrow m \Delta b^{-1} &= b^{-1} \Delta m && \text{Left cancellation} \\
 \text{thus } b^{-1} &\in N && \text{Definition of } N
 \end{aligned}$$

Now, since $a, b \in N \Rightarrow b^{-1} \in N$ and $m \Delta b^{-1} = b^{-1} \Delta m$, then

$$\begin{aligned}
 (a \Delta b^{-1}) \Delta m &= a \Delta (b^{-1} \Delta m) = a \Delta (m \Delta b^{-1}) = (a \Delta m) \Delta b^{-1} \\
 &= (m \Delta a) \Delta b^{-1} = m \Delta (a \Delta b^{-1}),
 \end{aligned}$$

which proves that whenever $a, b \in N$, then $a \Delta b^{-1} \in N$, and by Theorem 3, N is a subgroup of M .

Note: This proof will be done differently after the next theorem.

Theorem 4

Let G be a group and H a non-empty subset of G . Then, H is a subgroup of G if

- 1 $ab \in H$ whenever $a, b \in H$ (closure), and
- 2 $a^{-1} \in H$ whenever $a \in H$ (inverse).

Proof

- If H is a subgroup of G , it follows immediately, by definition, that the conditions are met.
- Conversely, if (1) and (2) hold, and $a, b \in H$, then by (2), $b^{-1} \in H$, and hence by (1) $ab^{-1} \in H$. Thus by Theorem 3, H is a subgroup of G .

Note: The importance of this theorem is that it reduces the number of characteristics we need to verify into two only.

Example 2

A group (M, Δ) has identity element i . N is a subset of M defined by

$$N = \{x \in M \mid x \Delta m = m \Delta x, \text{ for all } m \in M\}.$$

Show that N is a subgroup of M .

Solution

Let $a, b \in N$. We need to show that

- a) $a \Delta b \in N$ whenever $a, b \in N$, and
- b) $a^{-1} \in N$ whenever $a \in N$.

a) Since $a, b \in N$, then $a \Delta m = m \Delta a$, and $b \Delta m = m \Delta b$. We need to show that

$$(a \Delta b) \Delta m = m \Delta (a \Delta b).$$

Now,

$$\begin{aligned} (a \Delta b) \Delta m &= a \Delta (b \Delta m) = a \Delta (m \Delta b) = (a \Delta m) \Delta b \\ &= (m \Delta a) \Delta b = m \Delta (a \Delta b). \end{aligned}$$

b) This has been proved in Example 2.

When dealing with finite groups, it is simpler to use the following theorem.

Theorem 5 (Finite subgroup test)

Let G be a group and H a *finite* non-empty subset of G . Then, H is a subgroup of G if H is closed under the operation of G .

Proof

This theorem is a special case of Theorem 4 applied to a finite subset of G . In essence it says that H is a subgroup of G if $ab \in H$ whenever $a, b \in H$.

Since the closure axiom has been proved by Theorem 4, we need only verify that under this condition $a^{-1} \in H$ whenever $a \in H$.

Now, if $a = e$, then $a^{-1} = a \in H$ and we are done. If $a \neq e$, and since H is finite, then a has an order n . Also, since H is closed, then all positive powers of a are in H . Not all these powers are different because n is finite and hence for any power $r > n$ there should be a power $s < n$ such that $a^{r-s} = e$, and since $a \neq e$, then $r - s > 1$. Thus $a^{r-s} = a \cdot a^{r-s-1} = e$, which implies that $a^{r-s-1} = a^{-1}$. But $r - s - 1 = m$, which is some positive integer implying that $a^{r-s-1} = a^m$ is a positive power of a and hence it has to be in H . So, we showed that whenever $a \in H$, then $a^{-1} \in H$, and that completes the proof.

Example 3

Show that the set $\{1, 3, 4, 5, 9\}$ under multiplication modulo 11 (\times_{11}) is a subgroup of $(\mathbb{Z}_{11} \setminus \{0\}, \times_{11})$.

Solution

Since the group is finite, it is enough to show the subset closed under this operation. There are 10 multiplications (rather than 25) to check:

$$3 \times_{11} 4 = 1, 3 \times_{11} 5 = 4, 3 \times_{11} 9 = 5, 4 \times_{11} 5 = 9, 4 \times_{11} 9 = 3,$$

$$5 \times_{11} 9 = 1, 3^2 = 9, 4^2 = 5, 5^2 = 3, 9^2 = 4.$$



Theorem 2 – proof

Recall that the claim is that subset X defined by $X = \{x^k \mid k \in \mathbb{Z}\}$ is a subgroup of G . (The **cyclic subgroup** generated by x . x is also called the **generator** of this subgroup.)

Since $x \in X$, then X is non-empty. Now, let $x^i, x^j \in X$. Then $i - j \in \mathbb{Z}$ and hence $x^{i-j} \in X$ by definition of X . This in turn means that $x^{i-j} = x^i x^{-j} = x^i (x^j)^{-1} \in X$; thus, letting $a = x^i$ and $b = x^j \Rightarrow ab^{-1} \in X$, whenever $a, b \in X$, and by Theorem 3, X is a subgroup of G .

The following example is a demonstration of the validity of this theorem.

Example

- Consider the group of symmetries in an equilateral triangle (D, \circ) discussed in the previous chapter. Here is a reproduction of its Cayley table.

\circ	I	R	R^2	L	M	N
I	I	R	R^2	L	M	N
R	R	R^2	I	N	L	M
R^2	R^2	I	R	M	N	L
L	L	M	N	I	R	R^2
M	M	N	L	R^2	I	R
N	N	L	M	R	R^2	I

Notice how R generates a cyclic subgroup of (D, \circ) .

- Consider the group $(\mathbb{Z}_5 \setminus \{0\}, \times)$. The group elements are $\{1, 2, 3, 4\}$. Take 2 for example.

$2^2 = 4$, $2^3 = 3$, $2^4 = 1$, and hence 2 is a generator of a cyclic subgroup of $(\mathbb{Z}_5 \setminus \{0\}, \times)$. It is actually the group itself.

Example

Consider the group $(\mathbb{Z}_{11} \setminus \{0\}, \times)$. The group elements are $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Consider the element 3: $3^2 = 9$, $3^3 = 5$, $3^4 = 4$, $3^5 = 1$, and thus 3 generates a cyclic subgroup $\{1, 3, 4, 5, 9\}$ of the original group. The order of 3 in the group is 5, and so is the order of this subgroup. Notice that the order of this subgroup divides the order of the group itself, which is 10. 4, 5, or 9, will also generate this subgroup.

If you consider 2 or 6, you will see that they generate the whole group itself.

The previous example introduces us to the definition of **cyclic groups** in Section 4.3.

The centre of a group (Optional)

The **centre** of a group G is the subset $C(G)$ of all elements that commute with every element of G :

$$C(G) = \{a \in G : ag = ga \text{ for all } g \in G\}$$

Theorem

For a group G the centre $C(G)$ is a subgroup of G .

Proof

Since e , the identity element commutes with all elements in G , it is an element of C according to the definition.

Also, if $a, b \in C(G)$, then for any $g \in G$, $(ab)g = a(bg)$ by associativity.

Thus, $(ab)g = a(bg) = a(gb)$ since $b \in C(G)$.

Therefore, $(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$.

So $ab \in C(G)$.

Also, since $a \in C(G) \Rightarrow ag = ga \Rightarrow a^{-1}aga^{-1} = a^{-1}gaa^{-1} \Rightarrow ga^{-1} = a^{-1}g$.

Hence, $a^{-1} \in C(G)$.

Therefore, $C(G)$ is a subgroup of G by Theorem 4.

4.3

Cyclic groups

Definition 3

A group G is called **cyclic** if there is an element $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\}$. a is called a generator of G . Notice from the previous example that a generator is not unique. For instance, 2 and 6 are two of the generators of $(\mathbb{Z}_{11} \setminus \{0\}, \times)$.

Note: It is important to remember that in all cases, the identity element can be understood as $a^0 = e$, thus e is a member of every cyclic group too, but it cannot generate the groups except the trivial subgroup.

Theorem 6

All cyclic groups are Abelian.

Proof

If G is a cyclic group and x is a generator of order n , consider any two elements a and b in G . Since G is cyclic and generated by x , then there exists two integers r and s such that $a = x^r$ and $b = x^s$.



Now, $ab = x^r x^s = x^{r+s} = x^{s+r} = x^s x^r = ba$, and the group is Abelian.

Example

$(\mathbb{Z}, +)$ is cyclic. 1 is a generator. When the operation is addition, then 1^n is interpreted as $\underbrace{1 + 1 + \dots + 1}_{n \text{ terms}}$.

- $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$, $n \geq 1$ is a cyclic group under addition modulo n .
1 is a generator. $-1 = n-1$ is also a generator.
- $\mathbb{Z}_8 = \{0, 1, 2, \dots, 7\}$ is a specific example of such cyclic groups under addition modulo 8. 1, 3, 5, and 7 are generators.
 $3^8 = 3^0 = 0$, $3^3 = 3 + 3 + 3 = 1$, $3^6 = 2$, $3^1 = 3$, $3^4 = 3 + 3 + 3 + 3 = 4$,
 $3^7 = 5$, $3^2 = 3 + 3 = 6$, $3^5 = 7$.
- $A = \{1, 3, 7, 9\}$ under multiplication modulo 10 is cyclic with 3 and 7 as generators: $\{3^0, 3^1, 3^3, 3^2\}$; $\{7^0, 7^3, 7^1, 7^2\}$.
- Now consider the group $\{1, 3, 5, 7\}$ under multiplication modulo 8.
We leave it for you to verify that this is a group. However, we will show you here that it is not cyclic. If it were cyclic, then we should be able to generate it with at least one of the elements, 1, 3, 5, or 7. However, 1, being the identity, does not generate it, and neither does 3 (since $3^2 = 1 \Rightarrow |3| = 2$), nor 5 ($|5| = 2$), nor 7 ($|7| = 2$).

Theorem 7 (Lagrange's theorem)

If H is a subgroup of a finite group G , then the order of H divides the order of G . That is, $|G|$ is a multiple of $|H|$.

Example

You have seen that the group $(\mathbb{Z}_{11} \setminus \{0\}, \times)$ with elements $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ has a subgroup $H = \{1, 3, 4, 5, 9\}$ whose order is 5. We also pointed out that the order 5 divides the order of the whole group, 10. This is a demonstration of Lagrange's theorem.

Example

In the group of symmetries of the square, (D_4, \circ) , we notice that the group $\{e, r, r^2, r^3\}$ is a subgroup. The order of the group is 8 and the order of the subgroup is 4.

Proof

To understand the proof, we need to introduce another concept, that of a coset.

Cosets

Consider H , a subgroup of a group G . Define a relation \circ_H on G in the following manner:

$$a \circ_H b \Leftrightarrow a^{-1}b \in H$$

Stated differently, this relation means that $a \circ_H b$ iff $a^{-1}b = h$ for some $h \in H$. This can also be interpreted as saying $a \circ_H b$ iff $b = ah$ for some $h \in H$.

The last interpretation of the relationship gives rise to the following theorem.

Theorem

If H is a subgroup of G , then the relation $a \circ_H b$ is an equivalence relation on G .

Proof

To show that this relation is an equivalence relation, we need to show that it is reflexive, symmetric and transitive.

Reflexive: $a \circ_H a$ since $a^{-1}a = e \in H$ because H is a subgroup of G .

Symmetric: If $a \circ_H b \Leftrightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H \Rightarrow b^{-1}a \in H \Rightarrow b \circ_H a$.

Transitive: If $a \circ_H b$ and $b \circ_H c \Leftrightarrow a^{-1}b \in H$ and $b^{-1}c \in H \Rightarrow (a^{-1}b)(b^{-1}c) = a^{-1}c \in H \Rightarrow a \circ_H c$.

This discussion gives rise to the following results.

Definition: Left coset

If H is a subgroup of G , and a any element in G then the left coset of H in G determined by a is the set $aH = \{ax \mid x \in H\}$. (We can define a right coset in a similar manner but we will only focus on left cosets for our purposes here.)

Example: Coset (1)

Let $G = (\mathbb{Z}_{11} \setminus \{0\}, \times)$ and $H = \{1, 3, 4, 5, 9\}$. The left cosets of H are:

$1H = H$, $3H = \{3, 9, 1, 4, 5\}$, this is also H , and so are $4H$, $5H$, and $9H$.

$2H = \{2, 6, 8, 10, 7\}$, $6H = \{6, 7, 2, 8, 10\}$, also equal to $2H$, and so are $8H$, $10H$, and $7H$.

So, we have 2 left cosets for this group. Notice that both cosets have the same order, namely 5, and that the order of the group is $10 = 5 \times 2$, and that once two cosets have an element in common, then they are equal, and finally, the union of the cosets is the group G itself.

Example: Coset (2)

Let G be the set of functions $\{f, g, h, i, j, k\}$ defined on page 1296 of Chapter 3. We reproduce its Cayley table here for reference.

Since \circ_H as defined is an equivalence relation, it gives rise to equivalence classes.

$a \circ_H b$ iff $b = ah$ for some $h \in H \Rightarrow$ the equivalence class $[a]$ can be defined as

$$[a] = \{b : b = ah, h \in H\}.$$



\circ	i	f	g	h	j	k
i	i	f	g	h	j	k
f	f	g	i	k	h	j
g	g	i	f	j	k	h
h	h	j	k	i	f	g
j	j	k	h	g	i	f
k	k	h	j	f	g	i

Notice that it has a subgroup $\{i, h\}$, which we will consider as H .

The cosets are

$$\begin{aligned} iH &= H, fH = \{f, k\}, gH = \{g, j\}, hH = \{h, i\} = H, jH = \{j, g\} = gH, \\ kH &= \{k, f\} = fH. \end{aligned}$$

Here we have 3 left cosets. Also notice that the cosets have the same order, namely 2, and that the order of the group is $6 = 2 \times 3$, and that once two cosets have an element in common, then they are equal, and the union of the cosets is the group G itself.

The two examples point to the following theorem.

Theorem: Lagrange

Let H be a subgroup of a group G .

- 1 H is a left coset of itself.
- 2 For every element a in G , $a \in aH$, i.e. a is a member of its own left coset.
- 3 $\bigcup_{a \in G} aH = G$. That is, G is the union of the left cosets of H .
- 4 Any two left cosets of H are either equal or disjoint ($aH = bH$, or $aH \cap bH = \emptyset$).
- 5 All left cosets have the same order, namely $|H|$.

Proof

- 1 $H = eH$
- 2 Since $e \in H$, $ae = a \in aH$.
- 3 Obviously $aH \subseteq G$ for all a because of the closure axiom.

And for every $a \in G$, we showed in (2) that $a \in aH$, which is a subset of

$$\bigcup_{a \in G} aH, \text{ and thus}$$

$$G \subseteq \bigcup_{a \in G} aH. \text{ Therefore } \bigcup_{a \in G} aH = G.$$

- 4 Assume that $aH \cap bH \neq \emptyset$, thus we have at least an $x \in aH \cap bH$. Hence, because $x \in aH$ then

$x = ah_1$ for some $h_1 \in H$ by definition. Similarly, $x = bh_2$ for some $h_2 \in H$. This implies that

$x = ah_1 = bh_2$, which in turn implies that $a = bh_2(h_1)^{-1}$. Now for any $h \in H$, $ah \in aH$, but

$ah = bh_2(h_1)^{-1}h \in bH$ since $h_2(h_1)^{-1}h \in H$ by closure, and therefore $aH \subseteq bH$. A similar argument shows that $bH \subseteq aH$, and thus $aH = bH$.

- 5 Define a function $f: H \rightarrow aH$ by $f(h) = ah$. By definition of aH , any of its elements can be written as $f(h) = ah$, and hence f is surjective. Additionally, $f(h_1) = f(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$ (left cancellation), and the function is injective. Thus, f is bijective and its domain and range must have the same order.

One of the conclusions we can draw from the theorem above is that the different cosets corresponding to H form a partition of G .

Now, we can prove Lagrange's theorem:

Let S_1, S_2, \dots, S_k be the different cosets created by H . Since these cosets form a partition of G , then

$$G = \bigcup_{i=1}^k S_i = S_1 \cup S_2 \cup \dots \cup S_k, \text{ and because these cosets are disjoint}$$

$$|G| = \underbrace{|S_1| + |S_2| + \dots + |S_k|}_{k \text{ times}} = \underbrace{|H| + |H| + \dots + |H|}_{k \text{ times}} = k |H|.$$

Theorem 8

(Corollary to Lagrange's theorem)

Let G be a finite group, and x any element of G , then $|G|$ is a multiple of the order of x .

Proof

Recall from Theorem 2 that x generates a cyclic subgroup of G , which we denoted by $X = \{x^k \mid k \in \mathbb{Z}\}$, and using Lagrange's theorem, the order of G is a multiple of the order of X , which is the order of the element x itself.

Example 4

Show that if the order of a group G is a prime number, then the group is cyclic.

Solution

Let $|G| = n$ where n is a prime number.

Let x be any non-identity element in G , and by Theorem 2, it has an order k . But by Lagrange corollary, k must divide n which is not possible, and therefore $k = n$. Hence, G is a cyclic group generated by x .



Example 5

Consider \mathbb{Z}_{12} , the group of integers modulo 12 under addition and the subgroup $H = \{0, 3, 6, 9\}$. What are the left cosets?

Solution

The left cosets are

$0H = \{0, 3, 6, 9\}$. $3H$, $6H$, and $9H$ are all the same.

$1H = \{1, 4, 7, 10\} = 4H, 7H, 10H$ are all the same.

$2H = \{2, 5, 8, 11\} = 5H, 8H, 11H$ are all the same.



Homomorphism and isomorphism

The set of natural numbers as historically known is $\mathbb{N} = \{1, 2, 3, \dots\}$. If we wanted to write it in different notation, Roman for example, then we have $\mathbb{N} = \{I, II, III, \dots\}$. The two look different, but mathematically they are considered the same. The idea that eases the differences in names and notations is **isomorphism**. Isomorphism allows us to look at different groups as being equal regardless of the different appearances. For example, consider the subgroup A of S_3 represented by the table below and the group \mathbb{Z}_3 under addition modulo 3. A consists of the following 3 permutations:

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Here are the tables.

\circ	i	α	β	$+$	0	1	2
i	i	α	β	0	0	1	2
α	α	β	i	1	1	2	0
β	β	i	α	2	2	0	1

As we said, the first group members are permutations and the operation is composition, while the second group's elements are congruence classes and the operation is addition modulo 3. However, close inspection shows us that they are alike. If we think of setting up a correspondence between the elements of the two groups as follows

$$i \leftrightarrow 0, \alpha \leftrightarrow 1, \beta \leftrightarrow 2,$$

then knowing one table of operations will enable us to fill the other one without performing the operation in question. That is, knowing the addition table and using this correspondence we can fill the first table without performing any composition of permutations.

Here is the definition of isomorphism that makes this possible.

Definition 4

Let G be a group with operation $*$, $(G, *)$, and let H be a group with operation Δ , (H, Δ) .

- 1 A **homomorphism** of G into H is a mapping $f: G \rightarrow H$ such that

$$f(a * b) = f(a) \Delta f(b)$$

for every $a, b \in G$. G and H are said to be **homomorphic**.

- 2 An **isomorphism** of G into H is a bijective mapping $f: G \rightarrow H$ such that

$$f(a * b) = f(a) \Delta f(b)$$

for every $a, b \in G$.

G and H are said to be **isomorphic**. Notation differs among mathematicians. We will use $G \cong H$ to denote that the groups are isomorphic.

Notice here that an isomorphism is a homomorphism that is also bijective.

Example

Let k be an integer, and let $f: \mathbb{Z} \rightarrow \mathbb{Z}$ be a function defined by

$$f(n) = kn$$

f is a homomorphism from the group $(\mathbb{Z}, +)$ to itself, since

$$f(n_1 + n_2) = k(n_1 + n_2) = kn_1 + kn_2 = f(n_1) + f(n_2)$$

for all integers n_1 and n_2 .

Example

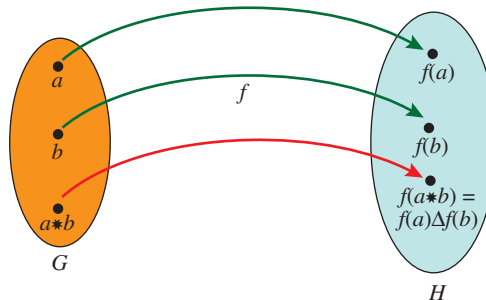
Let $g: \mathbb{Z} \rightarrow \mathbb{R}^+$ be defined by $g(x) = a^x$ where a is a positive real number, and consider the groups $(\mathbb{Z}, +)$ of integers under addition and (\mathbb{R}^+, \times) of positive real numbers under multiplication.

g is a homomorphism from $(\mathbb{Z}, +)$ to (\mathbb{R}^+, \times) .

For all integers x and y

$$g(x + y) = a^{x+y} = a^x \times a^y = g(x) \times g(y).$$

Note: Isomorphism is sometimes said to *preserve* the operation. It makes no difference whether we first operate in G and then apply f , or if we apply f first and then operate in H . See below.



For example, in the correspondence between Arabic notation and Roman notation, we get the same result if we add $2 + 3 = 5$ and then translate that



into Roman notation, $5 \rightarrow V$, or translate first, $2 \rightarrow II$ and $3 \rightarrow III$, and then add: $II + III = V$.

Since f is a bijection, then f^{-1} is also a bijection and it describes an isomorphism from H to G .

Example

Consider the example of the isomorphism described in the introduction to this section between the subgroup of S_3 and \mathbb{Z}_3 .

The correspondence described, $i \leftrightarrow 0$, $\alpha \leftrightarrow 1$, $\beta \leftrightarrow 2$, defines the isomorphism between the two groups. Call the mapping g , then

$$g(i) = 0, g(\alpha) = 1, \text{ and } g(\beta) = 2.$$

Then, for example,

$$g(\alpha \circ \beta) = g(i) = 0,$$

and

$$g(\alpha) + g(\beta) = 1 + 2 = 0;$$

thus

$$g(\alpha \circ \beta) = g(\alpha) + g(\beta).$$

You will need to check nine operations if you were to verify the definition for the whole operation. These are the entries in the Cayley table. In general, you need to check n^2 equations if G and H were finite of order n each.

Example

Consider the function $f: \mathbb{R}^+ \rightarrow \mathbb{R}$ defined by $f(x) = \ln x$ for each $x \in \mathbb{R}^+$.

\mathbb{R}^+ is a group with multiplication as the operation, \mathbb{R} is a group with addition as the operation, and f is a bijection from \mathbb{R}^+ into \mathbb{R} because it has an inverse $f^{-1}: \mathbb{R} \rightarrow \mathbb{R}^+$ defined by $f^{-1}(x) = e^x$. The mapping is an isomorphism because

$$f(xy) = \ln(xy) = \ln(x) + \ln(y) = f(x) + f(y) \text{ for all } x, y \in \mathbb{R}^+.$$

Theorem 9

Let G be a group with operation $*$, $(G, *)$, and let H be a group with operation Δ , (H, Δ) . If G and H are homomorphic with $f: G \rightarrow H$ as their homomorphism, then:

- 1 $f(e_G) = e_H$
- 2 $f(a^{-1}) = (f(a))^{-1}$, for each $a \in G$.
- 3 $f(a^n) = (f(a))^n$, for each $a \in G$ and each $n \in \mathbb{Z}$.

Proof

- 1 $e_G * e_G = e_G \Rightarrow f(e_G * e_G) = f(e_G) \Rightarrow f(e_G) \Delta f(e_G) = f(e_G)$,
but since $f(e_G) \in H$, then $f(e_G) = f(e_G) \Delta e_H$ as e_H is the identity in H ;
thus $f(e_G) \Delta f(e_G) = f(e_G) \Delta e_H \Rightarrow f(e_G) = e_H$ by left cancellation.
- 2 $f(a * a^{-1}) = f(a) \Delta f(a^{-1})$, and $f(a * a^{-1}) = f(e_G) = e_H$
 $\Rightarrow f(a) \Delta f(a^{-1}) = e_H$ but
 $f(a), (f(a))^{-1} \in H \Rightarrow f(a) \Delta (f(a))^{-1} = e_H \Rightarrow$
 $f(a) \Delta f(a^{-1}) = f(a) \Delta (f(a))^{-1} \Rightarrow f(a^{-1}) = (f(a))^{-1}$ by left cancellation.
- 3 We can use mathematical induction to prove this. We will prove it here for $n \geq 0$ and leave $n < 0$ as an exercise giving you a hint, $a^{-n} = (a^{-1})^n$.
The case $n = 0$ is obvious as $n = 0 \Rightarrow f(a^0) = (f(a))^0 \Rightarrow f(e_G) = e_H$ and also $n = 1$ is more obvious.
Now assume $f(a^k) = (f(a))^k$, then
 $f(a^{k+1}) = f(a^k * a) = f(a^k) \Delta f(a) = (f(a))^k \Delta f(a) = (f(a))^{k+1}$.
Therefore, $f(a^n) = (f(a))^n$ is true for all integers by the principle of mathematical induction.

The following theorem will provide you with a few properties that are helpful in dealing with group relationships.

Theorem 10

Let G be a group with operation $*$, $(G, *)$, and let H be a group with operation Δ , (H, Δ) . If $G \cong H$ with $f: G \rightarrow H$ as their isomorphism and G is Abelian, then H is Abelian.

Proof

Consider any two elements $x, y \in H$, then since f is a bijection, there are two elements $a, b \in G$ such that $f(a) = x$ and $f(b) = y$.

Now,

$$x \Delta y = f(a) \Delta f(b) = f(a * b) = f(b * a) = f(b) \Delta f(a) = y \Delta x.$$

Thus H is Abelian.

Note: If two groups are isomorphic, then they must have the same order since their isomorphism is a bijection. This provides you with a convenient way of showing that two groups are not isomorphic. If $|G| \neq |H|$, then G and H cannot be isomorphic.

Two groups that are **isomorphic** are considered to be 'the same' in the sense that any group-theoretic claim about one is also true for the other. For example, if one is cyclic or Abelian, then the other is cyclic or Abelian.



Here is a list of properties you can use in your proofs to quickly determine if two groups are not isomorphic:

G and H are groups, and $G \cong H$.

- 1 $|G| = |H|$
- 2 If G is Abelian, then H is Abelian.
- 3 If G is cyclic, then H is cyclic.
- 4 If G has a subgroup of order n , then H has a subgroup of order n ($n \in \mathbb{Z}^+$).
- 5 If G has an element of order n , then H has an element of order n .

(1) and (2) were discussed earlier. We will outline a proof for (3) here leaving the rest as exercises.

If G is cyclic, then there exists an element $a \in G$ which generates G , i.e. if the order of G is n , then it can be described as $\{a^0, a, a^2, \dots, a^n\}$. Since $G \cong H$, Theorem 9(3) and the fact that f is a bijection enable us to say that there is $b \in H$, such that $b = f(a)$ and $f(a^k) = (f(a))^k = b^k$ for all $k \leq n$. Hence, H can be described as $\{b^0, b, b^2, \dots, b^n\}$, and therefore is cyclic with b as a generator.

Example

The previous example gave you an example of an isomorphism. Here is an extension to look at the properties too.

Recall that $\ln(ab) = \ln a + \ln b$. The logarithmic function is an example to show you that the operations in the two isomorphic groups can be quite different.

Additionally, you can really see how all the properties mentioned earlier are clearly demonstrated by the logarithmic function. For example, the identity for multiplication is 1 as you know, $f(1) = \ln(1) = 0$, which is the identity for addition. Also, if a is a positive real number, then $\frac{1}{a}$ is its inverse. If you find $f\left(\frac{1}{a}\right) = \ln \frac{1}{a} = -\ln a = -f(a)$, so the image of the inverse is the inverse of the image!

Example 6

Consider the function $g(x): (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \times)$ defined by $g(x) = 2^x$. Show that this is an isomorphism from $(\mathbb{R}, +)$ to (\mathbb{R}^+, \times) .

Solution

- We need to show that the function is an injection:
Suppose that $2^x = 2^y$, then $\log_2 2^x = \log_2 2^y \Rightarrow x = y$.

Summary

Note: Isomorphism is a special case of what is called **group homomorphism**. Homomorphism is defined as:

Let G be a group with operation $*$, $(G, *)$, and let H be a group with operation Δ , (H, Δ) . A **homomorphism** of G into H is a mapping $f: G \rightarrow H$ such that

$$f(a * b) = f(a) \Delta f(b)$$

for every $a, b \in G$.
 G and H are said to be **homomorphic**.

The difference between homomorphism and isomorphism is that isomorphism requires the mapping to be a bijection while homomorphism does not.

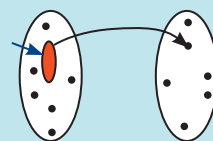
- To prove that it is a surjection, we need to show that for any positive real number y , we can find some real number x such that $g(x) = y$, i.e. $2^x = y$. Solving this equation for x gives us $x = \log_2 y$.
- To prove ‘operation-preservation’ we see that

$$g(x + y) = 2^{x+y} = 2^x \cdot 2^y = g(x) g(y).$$

Therefore, the function is an isomorphism between $(\mathbb{R}, +)$ and (\mathbb{R}^+, \times) .

Definition

If $f: G \rightarrow H$ is a group homomorphism, then the set $K = \{x \in G \mid f(x) = e_H\}$ is the **kernel** of f . The set K is often denoted by $\ker f$.



Theorem: $\ker f$ is a subgroup

If $f: G \rightarrow H$ is a group homomorphism, then $\ker f = \{x \in G \mid f(x) = e_H\}$ with the group G operation is a subgroup of G .

Proof

Since $f(e_G) = e_H$, $e_G \in \ker f$ and thus $\ker f \neq \emptyset$. Also, if $x, y \in \ker f$, then $f(x) = f(y) = e_H$. Hence, by Theorem 9, $f(y^{-1}) = (f(y))^{-1} = e_H^{-1} = e_H$, and so $y^{-1} \in \ker f$.

Since f is a homomorphism, $f(xy^{-1}) = f(x)f(y^{-1}) = e_H e_H = e_H$.

So $xy^{-1} \in \ker f$.

Hence, by Theorem 3, $\ker f$ is a subgroup of G .

In the earlier discussion, we stated that a homomorphism between two groups does not need to be a bijection. Hence, if $f: G \rightarrow H$ is a group homomorphism, then f is not necessarily surjective. Thus the range of f is a subset of H and not necessarily equal to it. The following theorem helps characterize the range of a group homomorphism.

Theorem: Range of f is a subgroup

If $f: G \rightarrow H$ is a group homomorphism, then the range of f is a subgroup of H under group H operation.

Proof

Since $e_G \in G$, then $G \neq \emptyset$. If $x \in G$, then $f(x) \in f(G)$ and so $f(G) \neq \emptyset$. $f(G)$ is the range of f .

Let $f(x), f(y) \in f(G)$ where $x, y \in G$. Since $x, y \in G$, then $xy^{-1} \in G$ and so $f(xy^{-1}) \in f(G)$.

Since f is a homomorphism, $f(xy^{-1}) = f(x)f(y^{-1}) \in f(G)$ and also $f(y^{-1}) = (f(y))^{-1}$.

Since whenever $f(x), f(y) \in f(G)$, then $f(x)(f(y))^{-1} \in f(G)$.

Therefore, by Theorem 3, $f(G)$ is a subgroup of H .

Remember that Theorem 3 states: Let G be a group and H a non-empty subset of G . Then, H is a subgroup of G iff $ab^{-1} \in H$ whenever $a, b \in H$.





Example 7

Let (G, \times) be the multiplicative group of nonzero rational numbers and H the set of rational numbers different from 1. Define the binary operation $*$ on H by

$$x * y = x + y - xy.$$

- a) Show that $(H, *)$ is a group.
 b) Let $f: G \rightarrow H$ be defined by $f(x) = 1 - x$. Show that f is a group homomorphism.

Solution

- a) If x, y are rational numbers different from 1, then $x + y - xy$ must also be a rational number different to 1. Otherwise, if $x + y - xy = 1$, then

$$x - xy = 1 - y \rightarrow x = \frac{1 - y}{1 - y} = 1, \text{ which is a contradiction.}$$

So, the set H is closed under $*$.

Let the identity element be e .

Hence,

$$x * e = e * x = x + e - xe = x \Rightarrow e(1 - x) = 0$$

Since $x \neq 1$, then $e = 0$.

So, the identity element is 0.

Now, if y is the inverse of x , then

$$x * y = x + y - xy = 0 \Rightarrow y = \frac{x}{x - 1}$$

This is a rational number as it has a non-zero denominator and is different from 1. ($y = 1$ will lead to a contradiction; $0 = -1$)

So, every element has an inverse.

The associativity of the operation is left as an exercise:

$$(x * y) * z = x * (y * z) = x + y + z - xy - xz - yz + xyz$$

Therefore $(H, *)$ is a group.

- b) Let $x, y \in G$, then

$$f(xy) = 1 - xy; f(x) = 1 - x; f(y) = 1 - y;$$

$$f(x) * f(y) = 1 - x + 1 - y - (1 - x)(1 - y) = 1 - xy$$

Hence, $f(xy) = f(x) * f(y)$ and the function f is a homomorphism.

Example 8

Consider the following two groups:

\mathbb{R} under addition

\mathbb{C}_1 of complex numbers z with $|z| = 1$ under multiplication

Let $f: \mathbb{R} \rightarrow \mathbb{C}_1$ be the map defined by $f(x) = e^{2\pi ix}$.

Show that this is a homomorphism and find its kernel.

Solution

$$f(x + y) = e^{2\pi i(x+y)} = e^{(2\pi ix + 2\pi iy)} = e^{2\pi ix} e^{2\pi iy} = f(x)f(y)$$

Hence, f is a homomorphism.

To find $\ker f$, we look for all $x \in \mathbb{R}$ such that $f(x) = e_{\mathbb{C}} = 1$ in this case,

$e^{2\pi ix} = 1 \Rightarrow 2\pi x$ must be a multiple of 2π . So, x must be an integer.

Therefore $\ker f = \mathbb{Z}$.

Example 9

Consider the group SL of 2×2 invertible matrices under matrix multiplication and the group of non-zero real Numbers $\mathbb{R} \setminus \{0\}$ under multiplication.

Define $f: SL \rightarrow \mathbb{R} \setminus \{0\}$ in the following manner.

If $A \in SL$, then $f(A) = \det A$.

Show that f is a homomorphism and find its kernel

Solution

$$f(AB) = \det(AB) = \det A \cdot \det B = f(A)f(B)$$

Hence, f is a homomorphism.

To find $\ker f$, we look for all $A \in SL$, such that $f(A) = 1$,

So, A is any 2×2 matrix where $\det A = 1$. Thus $\ker f$ is SL_2 defined in the previous chapter.

Exercise 4

Note: In several questions, we will refer to the binary operation between two elements a and b by simply writing ab . This is done for convenience purposes and it does not mean that the operation is the usual multiplication of real numbers.

- 1 Show that $(\mathbb{Z}_5 \setminus \{0\}, \times)$ is isomorphic to $(\mathbb{Z}_4, +)$.
- 2 Consider the set $M = \{[1], [3], [5], [9], [11], [13]\}$ under the operation \times , where \times is multiplication modulo 14. (You may assume properties of multiplication modulo n in this problem.)
 - a Show that $(5 \times 11) \times 3 = 5 \times (11 \times 3)$.
 - b Show that (M, \times) is a cyclic group and find all its generators.
 - c Find all non-trivial proper subgroups of this group.



- 3 a** $(\{e, x, x^2, x^3, x^4\}, \odot)$ is a cyclic group of order 5. Which elements generate the group?
- b** $(\{e, x, x^2, x^3, x^4, x^5\}, \odot)$ is a cyclic group of order 6. Which elements generate the group?
- c** Repeat part **b** for groups of order 7, 10, 15, and 20. How many generators does each have? Can you generalize?
- 4** Consider the group $S = \{I, R, R^2, L, M, N\}$ of symmetries of an equilateral triangle under transformation composition, \circ .
- a** Find the cyclic subgroup each of R, R^2 , or L generates.
- b** Is (S, \circ) cyclic? Justify your answer.

- 5** Let $U(n)$ be the set of integers less than n and relatively prime to n under multiplication modulo n .

For each group below, find the order of the group and the order of each of its elements. In each case explain how the order of the element is related to the order of the group.

- a** $(\mathbb{Z}_{12}, +_{12})$ **b** $(U(10), \cdot_{10})$ **c** $(U(12), \cdot_{12})$
- d** $(U(20), \cdot_{20})$ **e** D_4 (symmetries of the square)
- 6** Compute the orders of the following groups (all operations are modulo n):
- a** $U(3), U(4), U(12)$ **b** $U(5), U(7), U(35)$
- c** $U(4), U(5), U(20)$ **d** $U(3), U(5), U(15)$

Make a conjecture about the relationship among $|U(m)|$, $|U(n)|$, and $|U(mn)|$.

Now compute $|U(4)|$, $|U(10)|$, and $|U(40)|$. Do you need to adjust your conjecture?

- 7** Let $(G, *)$ be a group and $a \in G$. If $a^2 \neq e$ and $a^6 = e$, show that $a^4 \neq e$ and $a^5 \neq e$. What could be the order of a ?
- 8** Let (G, \cdot) be a group. Let $a \in G$ such that $|a| = 6$. Find $|a^2|$, $|a^3|$, $|a^4|$, and $|a^5|$. If $b \in G$ is such that $|b| = 9$, find $|b^i|$ for $i = 2, 3, \dots, 8$.
- 9** Consider the group $(\mathbb{Z}_{11} \setminus \{0\}, \times_{11})$.
- a** Find the cyclic group each of 2, 3, 4, 6, or 10 generates.
- b** Is $(\mathbb{Z}_{11} \setminus \{0\}, \times_{11})$ cyclic? Justify your answer.
- 10** You are given the operation table for a set of 7 members.

	a	b	c	d	e	f	g
a	a	b	c	d	e	f	g
b	b	c	a	e	f	g	d
c	c	a	b	f	g	d	e
d	d	e	f	g	a	b	c
e	e	f	g	a	d	c	b
f	f	g	d	b	c	e	a
g	g	d	e	c	b	a	f

- a** Show that $\{a, b, c\}$ form a group.
- b** Show that the whole set cannot form a group.
- 11** Consider a group (M, Δ) .
- a** If $x \in M$ has order 12, show that there is an element of M of order 3.
- b** If $|M| = 12$, show that (M, Δ) has a cyclic subgroup of order 2, 3, 4, or 6.
- 12** Show that a group with order p , where p is a prime number, must be cyclic.
- 13** A regular pentagon has 5 rotation symmetries I : R , which rotates the pentagon through an angle of 72° , R^2 , an angle of 144° , R^3 , an angle of 216° , and R^4 , an angle of 288° .
- Show that this group under composition of rotations is cyclic and that it is isomorphic to $(\mathbb{Z}_5, +)$.
- 14** Consider the set $N = \{1, 3, 5, 7, 9, 11, 13, 15\}$ under multiplication modulo 16. Denote this multiplication simply by \times .
- a** Show that $3 \times (9 \times 11) = (3 \times 9) \times 11$.
- b** Show that (N, \times) is a group.
- c** Does N have any subgroups? What order should they be? Find all of them.
- d** Is this a cyclic group? If yes, find all generators.
- 15** Consider a group (G, \circ) with an identity element i .
- a** $x \in G$ has order n . What should the order of x^{-1} be? Justify your answer.
- b** For $x, y, z \in (G, \circ)$, prove that $y = z^{-1}xz \Rightarrow y^n = z^{-1}x^n z$ for $n \in \mathbb{Z}^+$. (Hint: Use mathematical induction.)
- 16** Consider a group (G, \bullet) with identity element e .
- Consider also the set $H \subset G$ whose elements commute with all the elements of G , i.e.
- $$H = \{x \in G \mid \forall a \in G, ax = xa\}.$$
- Show that (H, \bullet) is a subgroup of (G, \bullet) .
- 17** A group (G, \cdot) is generated by two elements x and y subject only to the relations (every element of the group can be expressed as some product of x 's and y 's)
- $$x^3 = y^2 = (xy)^2 = 1.$$
- a** List the different elements of the group.
- b** List all the subgroups of this group.
- 18** A group (G, \cdot) is generated by two elements x and y subject only to the relations
- $$x^3 = y^2 = (xy)^3 = 1.$$
- a** List 12 different elements of the group.
- b** List all the subgroups of this group.
- 19** Let Q be the group (under matrix multiplication) generated by the complex matrices
- $$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \text{ where } i^2 = -1.$$
- Show that Q is a non-Abelian group of order 8.



- 20** Let T be the group (under matrix multiplication) generated by the real matrices

$$u = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } v = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Show that T is a non-Abelian group of order 8.

- 21** Let D be the group (under matrix multiplication) generated by the complex matrices

$$x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } b = \begin{pmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & e^{-\frac{2\pi i}{3}} \end{pmatrix}, \text{ where } i^2 = -1.$$

Show that D is a non-Abelian group of order 6.

- 22** If H and K are subgroups of a group $(G, *)$, then $H \cap K$ is also a subgroup of G .

Is the same true for $H \cup K$? Justify.

- 23** Let $(G, *)$ be a group, and $a, b, c \in G$. Show that the equation $a * x * c = b$ has a *unique* solution in G .

- 24** Find all subgroups of $\{\mathbb{Z}_7 \setminus \{0\}, \times_7\}$, of $(\{1, 3, 5, 7\}, \times_8)$, of $(\{1, 2, 4, 7, 8, 11, 13, 14\}, \times_{15})$.

- 25** Show that the group of matrices of the form

$$\begin{pmatrix} x & 0 \\ y & 1 \end{pmatrix}, x \neq 0$$

is a subgroup of the group (GL_2, \cdot) of real 2×2 invertible matrices.

- 26** Determine the cyclic subgroups of the group (GL_2, \cdot) of real 2×2 invertible matrices generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

- 27** Prove that every subgroup of a cyclic group is cyclic. Show, by a counterexample, that the converse of this theorem is not true.

- 28** Let $(G, *)$ be a group, and $a \in G$ has infinite order. Show that $a^i = a^j$ if and only if $i = j$. That is, no two distinct powers of a are equal (integral exponents).

- 29** (Optional) Show that the determinant of a matrix defines a homomorphism from the group of 2×2 non-singular real matrices under matrix multiplication to the group of non-zero real numbers under normal multiplication.

- 30** Show that the group M of 2×2 matrices described below under matrix multiplication and the group of symmetries of the equilateral triangle are isomorphic.

$$M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}, \right. \\ \left. \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \right\}$$

- 31** Show that the group $(\{1, -1, i, -i\}, \times)$ is isomorphic to $(\mathbb{Z}_4, +)$.
- 32** Let G be a group with some operation and a is some *fixed* element of G . Show that the mapping h defined by
- $$h(x) = a x a^{-1}, \forall x \in G$$
- is an isomorphism from G into itself.
- 33** Consider the set $\{4, 8, 12, 16\}$. Show that this set is a cyclic group under multiplication modulo 20. Find its generators.
- 34** Consider the set $\{7, 35, 49, 77\}$. Show that this set is a group under multiplication modulo 84. Is this a cyclic group?
- 35** Let $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and $H = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$.
Show that $(G, +)$ and $(H, +)$ are isomorphic.
- 36** Consider the function $f: \mathbb{R}^+ \rightarrow \mathbb{R}$ defined by $f(x) = \ln(x)$.
Show that f is a homomorphism from the group of positive real numbers under multiplication to the group of real numbers under addition. Find its kernel.
- 37** Consider the absolute value function from the group of all non-zero real numbers (under multiplication) into the group of positive real numbers (under multiplication).
Show that it is a homomorphism and find its kernel.
- 38** Let $P[x]$ denote the group of all polynomials with real coefficients under addition. Define the mapping φ that assigns to every function its derivative, i.e.
for every $f \in P[x]$, $\varphi: P[x] \rightarrow P[x]$ such that $\varphi(f) = f'$.
Show that it is a homomorphism and find its kernel.

Practice questions 4

- 1 a** Define an isomorphism between two groups (G, \circ) and (H, \bullet) .
- b** Let e and e' be the identity elements of groups G and H respectively.
Let f be an isomorphism between these two groups. Prove that $f(e) = e'$.
- c** Prove that an isomorphism maps a finite cyclic group onto another finite cyclic group.
- 2 a** Let f_1, f_2, f_3, f_4 be functions defined on $\mathbb{Q} - \{0\}$, the set of rational numbers excluding zero, such that $f_1(z) = z$, $f_2(z) = -z$, $f_3(z) = \frac{1}{z}$, and $f_4(z) = -\frac{1}{z}$, where $z \in \mathbb{Q} - \{0\}$.
Let $T = \{f_1, f_2, f_3, f_4\}$. Define \circ as the composition of functions, i.e.
 $(f_1 \circ f_2)(z) = f_1(f_2(z))$. Prove that (T, \circ) is an Abelian group.
- b** Let $G = \{1, 3, 5, 7\}$ and (G, \diamond) be the multiplicative group under the binary operation \diamond , multiplication modulo 8. Prove that the two groups (T, \circ) and (G, \diamond) are isomorphic.

3 Let $S = \{x \mid x = a + b\sqrt{2}; a, b \in \mathbb{Q}, a^2 - 2b^2 \neq 0\}$.

- a Prove that S is a group under multiplication, \times , of numbers.
- b For $x = a + b\sqrt{2}$, define $f(x) = a - b\sqrt{2}$. Prove that f is an isomorphism from (S, \times) onto (S, \times) .

4 a In any group, show that if the elements x , y , and xy have order 2, then $xy = yx$.

b Show that the inverse of each element in a group is unique.

c Let G be a group. Show that the correspondence $x \leftrightarrow x^{-1}$ is an isomorphism from G onto G if and only if G is **Abelian**.

5 Let (S, \circ) be the group of all permutations of four elements a, b, c, d . The permutation that maps a onto c , b onto d , c onto a and d onto b is represented

by $\begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}$.

The identity element is represented by $\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$.

Note that AB denotes the permutation obtained when permutation B is followed by permutation A .

a Find the inverse of the permutation $\begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix}$.

b Find a subgroup of S of order 2.

c Find a subgroup of S of order 4, showing that it is a subgroup of S .

6 Let $S = \{f, g, h, j\}$ be the set of functions defined by

$$f(x) = x, g(x) = -x, h(x) = \frac{1}{x}, j(x) = -\frac{1}{x}, \text{ where } x \neq 0.$$

a Construct the operation table for the group $\{S, \circ\}$, where \circ is the composition of functions.

b The following are the operation tables for the groups $\{0, 1, 2, 3\}$ under addition modulo 4, and $\{1, 2, 3, 4\}$ under multiplication modulo 5.

+	0	1	2	3	\times	1	2	3	4
0	0	1	2	3	1	1	2	3	4
1	1	2	3	0	2	2	4	1	3
2	2	3	0	1	3	3	1	4	2
3	3	0	1	2	4	4	3	2	1

By comparing the elements in the two tables given plus the table constructed in part a, find which groups are isomorphic. Give reasons for your answers. State clearly the corresponding elements.

7 The group (G, \times) has a subgroup (H, \times) . The relation R is defined on G ($xRy \Leftrightarrow (x^{-1}y \in H)$, for $x, y \in G$).

a Show that R is an equivalence relation.

b Given that $G = \{e, p, p^2, q, pq, p^2q\}$, where e is the identity element, $p^3 = q^2 = e$, and $qp = p^2q$, prove that $qp^2 = pq$.

c Given also that $H = \{e, p^2q\}$, find the equivalence class with respect to R which contains pq .

8 a Find $\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

b Let G be the set of matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ for } a, b \in \mathbb{R}.$$

Show that G is an Abelian group under matrix multiplication.

c Let F be the group of real ordered pairs under addition defined by

$$(a, b) + (c, d) = (a + c, b + d).$$

Show that G is isomorphic to F .

9 a Show that the set S of numbers of the form $2^m \times 3^n$, where $m, n \in \mathbb{Z}$, forms a group $\{S, \times\}$ under multiplication.

b Show that $\{S, \times\}$ is isomorphic to the group of complex numbers $m + ni$ under addition, where $m, n \in \mathbb{Z}$.

10 a Draw the Cayley table for the set of integers $G = \{0, 1, 2, 3, 4, 5\}$ under addition modulo 6, $+_6$.

b Show that $\{G, +_6\}$ is a group.

c Find the order of each element.

d Show that $\{G, +_6\}$ is cyclic and state its generators.

e Find a subgroup with three elements.

f Find the other proper subgroups of $\{G, +_6\}$.

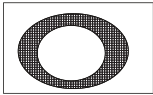
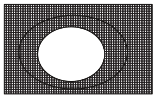
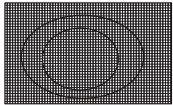
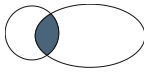
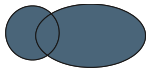
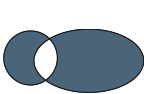
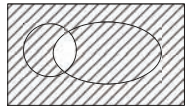
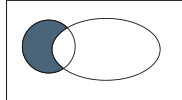
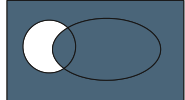
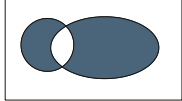
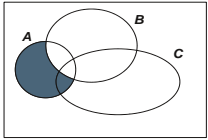
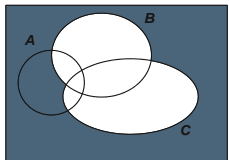
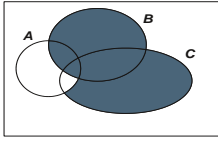
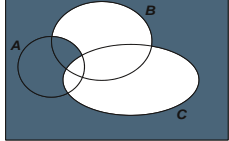
Questions 1–10 © International Baccalaureate Organization

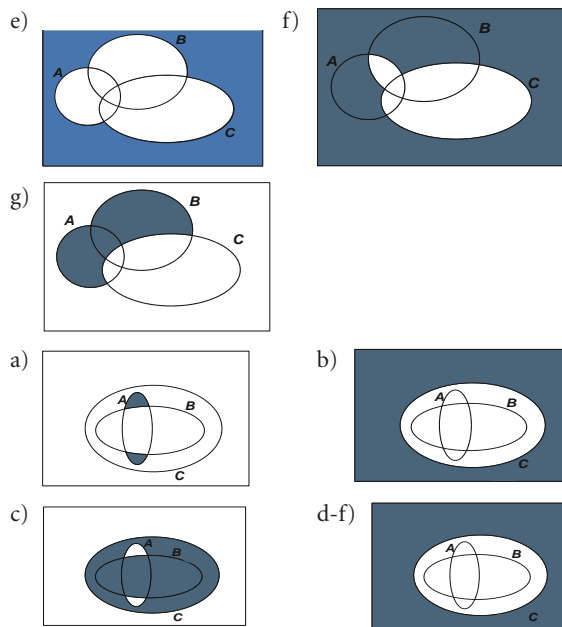


Answers

Chapter 1

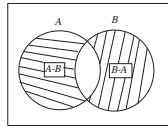
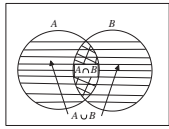
Exercise 1

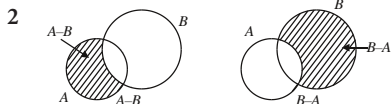
- 1 a) Equal b) Equal
c) Equal d) Not equal
- 2 a) $\{1, 3, 4\}$ b) $\{1, 3, 4\}$ c) $\{6\}$
d) $\{1, 2, 5, 6\}$ e) $\{6\}$ f) $\{1, 2, 3\}$
g) $\{1, 2, 5\}$
- 3 a) False b) True c) True
d) True e) True f) True
g) True h) True i) True
- 4 a) True b) True c) False
d) True e) False f) False
g) True h) False i) True
- 5 a) A b) B
c)  d) 
e) \emptyset f) 
- 6 a)  b) 
c)  d) 
e)  f) 
g) 
- 7 a)  b) 
c)  d) 



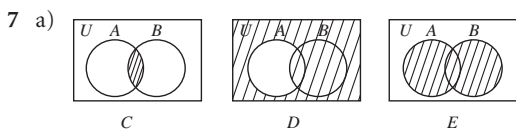
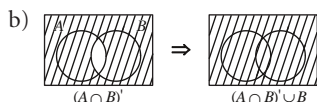
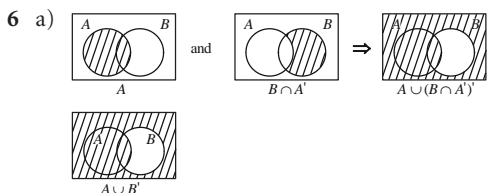
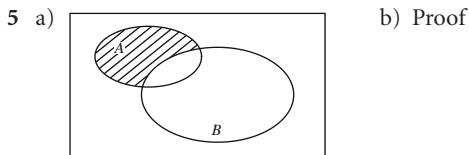
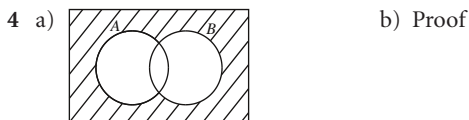
- g) \emptyset
- 9 a) $\{-1\}$ b) \emptyset c) $\{0, 1\}$
d) $\mathcal{P}(A) = \{\emptyset, \{0\}, \{-1\}, \{1\}, \{0, -1\}, \{0, 1\}, \{-1, 1\}, \{0, -1, 1\}\}$
- 10 $A \cap B'$ or $A \cap (C \setminus B)$
- 11 42
- 12 24
- 13 a) \mathbb{Z}^+ b) $\{1, 3, 5, \dots\}$ c) M_6 d) \emptyset
- 14 $A = B$
- 15 a-l) Proof
- 16 128
- 17 a-e) Proof
- 18 a) Proof
b) $\{\emptyset\}; \{\emptyset, \{\emptyset\}\}$
c) $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$
d) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$
- 19 a) $[0, \infty[$ b) \emptyset c) $[1, 3[$ d) $]0, 2]$
- 20 $|A \cup B| \neq |A| + |B|$
- 21 a-h) Proof
- 22 a-e) Proof

Practice questions 1

- 1 a)  
b) Proof



3 Proof



b-c) Proof

8 Proof

- 9 a) (i) $S_1 = \{x \in \mathbb{Z}^+ \mid 1 \text{ divides } x\}$
 $= 1, 2, 3, \dots = \mathbb{Z}^+$
(ii) $S_2 = \{x \in \mathbb{Z}^+ \mid 2 \text{ divides } x\}$
 $= 2, 4, 6, \dots$
Hence, $S_2' = 1, 3, 5, \dots$
(iii) $S_3 = \{x \in \mathbb{Z}^+ \mid 3 \text{ divides } x\}$
 $= 3, 6, 9, \dots$
Hence, $S_2 \cap S_3 = 6, 12, 18, \dots$
(iv) $S_6 = \{x \in \mathbb{Z}^+ \mid 6 \text{ divides } x\}$
 $= 6, 12, 18, \dots$
Hence, $S_6 \setminus S_3 = S_6 \cap S_3' = \emptyset$.

b) Proof

10 Proof

(vi) $A \times B$

b) i and iv; ii, iii, v, and vi

2 a, c, d, e

3 a) Points on the lines $y = x$ and $y = -x$ are symmetric with respect to the x - and y -axes. For example, $(2, 2)$, $(2, -2)$, $(-2, -2)$ and $(-2, 2)$.

c) Numbers of the form n and $-n - 1$.

d) Every complete square and its positive factors.

e) Concentric circles with O as centre.

4 a) 4, 5, 4

b) 3

c) Proof

5 a) \mathcal{R} is an equivalence relation. Classes are: $\{1\}$, $\{2\}$, ..., $\{9\}$.

b) \mathcal{X} is not an equivalence relation since it is not reflexive.

6 a) Injection

b) Injection

c) Injection

d) Surjection

7 a) Yes

b) No

c) Yes

8 a) nm

b) $\frac{n!}{(n-m)!}$

c) $n!$

9 a) Yes; no

b) No; no

c) (i) $[-4, 3]$, $[0, 2]$

(ii) $[-9, 5]$, $[-9, 5]$, $[-1, 3]$, $[-1, 3]$

(iii) $[1, 17]$, $[1, 17]$, $[1, 5]$, $[1, 10]$

10 No; yes

11 a-b) Proof

12 a) $f(a) \neq f(b) \neq f(c)$

b) c, a, b

c) Identity; $f^{-1} = f \circ f$

13 \mathcal{S} is an equivalence relation.

14 a) Proof

b) Concentric circles with centre at the origin. All points on the circle with radius $\sqrt{5}$.

15 Both. $h^{-1} : (a, b) \mapsto \left(\frac{2b-a}{3}, \frac{a+b}{3} \right)$.

16 Proof

17 \mathcal{S} is an equivalence relation; $\{\{a, c, e\}, \{b, d\}, f\}$

18 $\{\{1, 4, 6, 9, 11\}, \{2, 3\}, \{5, 10\}, \{7, 8\}\}$

19 a) Not a bijection

b) Bijection

c) Not a bijection

20 Proof

21 a) Proof

b) $\{\{0, 4, 8\}, \{1, 5, 9\}, \{2, 6\}, \{3, 7\}\}$

c) 3

22 a) Injective

b) Not surjective

23 $f^{-1}(x, y) = \left(\frac{5x+3y}{11}, \frac{2x-y}{11} \right)$

24 a-b) Proof

25 Proof

26 a) (i) $R = \left\{ \frac{e+1}{e}, e+1 \right\}$

(ii) Proof

(iii) Not a surjection

b) (i) $k = \pi$

(ii) $f^{-1}(x) = \arccos(\ln(x-1))$

27 a) Proof

b) $\{\{4, 24, 32\}, \{8, 20, 36\}, \{12, 16\}, 28\}$

Chapter 2

Exercise 2

- 1 a) (i) $\{(1, a), (1, b), \dots, (2, c), (1, x), \dots, (3, z)\}$
(ii) \emptyset
(iii) \emptyset
(iv) $\{(1, a), (1, b), \dots, (2, c), (1, x), \dots, (3, z)\}$
(v) \emptyset



28 Proof

29 $h^{-1}(x, y) \mapsto \left(\frac{3y-x}{4}, \frac{x-y}{2} \right)$

30 Neither

31 a) Proof

b) $\{5k, \{1+5k, 4+5k\}, \{2+5k, 3+5k\}\}, k \in \mathbb{N}$

32 a) Proof

b) $a = 2$

33 a-d) Proof

34 a-b) Proof

Practice questions 2

1 a) Proof

b) This is the set of ordered pairs (x, y) such that $x^2 + y^2 = 5$.

c) The partition is the set of all concentric circles in the plane with the origin as the centre.

2 a) Proof

b) The classes are those pairs (a, b) and (c, d) with $\frac{a}{b} = \frac{c}{d}$.

The elements are on the same line going through the origin.

3 a) Proof

b) (i) Student explanation

(ii) $\{5, 10\}, \{1, 4, 6, 9\}, \{2, 3, 7, 8\}$

4 a) Proof

b) $\{0, 4, 8, \dots\}, \{1, 5, 9, \dots\}, \{2, 6, 10, \dots\}, \{3, 7, 11, \dots\}$

c) 3

5 a) (i-ii) f is injective but not surjective.

b) (i-ii) g is injective and surjective.

c) $g^{-1}(x, y) = \left(\frac{5x+2y}{11}, \frac{3x-y}{11} \right)$

d) Proof

6 a-c) Proof

7 a) Proof

b) $3n-2; 3n-1; 3n; n \in \mathbb{Z}^+$

8 The equivalence class of $(1, 1)$ is a pair of straight lines through the origin with slopes ± 1 .

9 a) Range is $\left[-\frac{9}{4}, \infty \right)$; not an injection

b) $g^{-1}(x) = \sqrt{x + \frac{9}{4}} - \frac{1}{2}$ on $[0, 4]$

10 a) Proof

b) The equivalence classes are points lying, in the first quadrant, on straight lines through the origin.

c) No

3 Proof

4 e is the identity, s is the reflection with respect to the smaller diagonal, and l with respect to the larger diagonal, and r is a rotation of 180° .

$$\begin{array}{c|cccc} \circ & e & r & s & l \\ e & e & r & s & l \\ r & r & e & l & s \\ s & s & l & e & r \\ l & l & s & r & e \end{array}$$

5 a) \circ $\begin{array}{c|cccc} p & p & r & s & t \\ p & p & p & p & p \\ r & p & r & s & t \\ s & t & s & r & p \\ t & t & t & t & t \end{array}$ b) r is the identity.

$$\begin{array}{c|cccc} \circ & p & r & s & t \\ p & p & p & p & p \\ r & p & r & s & t \\ s & t & s & r & p \\ t & t & t & t & t \end{array}$$

c) No

d) r, s

e) No

6 a) \circ $\begin{array}{c|cccc} p & p & r & s & t \\ p & p & r & s & t \\ r & r & p & t & s \\ s & s & s & s & s \\ t & t & t & t & t \end{array}$ b) p is the identity.

$$\begin{array}{c|cccc} \circ & p & r & s & t \\ p & p & r & s & t \\ r & r & p & t & s \\ s & s & s & s & s \\ t & t & t & t & t \end{array}$$

c) No

d) p, r

e) No

7 A group with identity 1 and each element is self-inverse.

8 Not a group: $1+1=2 \notin \{-1, 0, 1\}$.

9 A group with identity 0 and inverse defined by $(10k)^{-1} = -10k$.

10 A group with identity 1 and inverse defined by $(2^m)^{-1} = 2^{-m}$.

11 A group with identity 1 and inverse defined by $(2^m 3^n)^{-1} = 2^{-m} 3^{-n}$.

12 A group with identity $f(x) = 0$ and inverse defined by $f^{-1}(x) = -f(x)$.

13 A group with identity 0 and inverse defined by $a^{-1} = -\frac{a}{a+1}$.

14 A group with identity 1 and inverse defined by $(a+b\sqrt{2})^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$.

15 Proof

16 Proof

17 a) 24

b) If we let $1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$,

$b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$, $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$, ..., then the table will

look like this:

$$\begin{array}{c|cccc} \circ & 1 & a & b & c \\ 1 & 1 & a & b & c \\ a & a & 1 & c & b \\ b & b & d & 1 & f \\ c & c & f & a & d \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

c) For example: $a \circ b = c \neq b \circ a = d$

18 a-c) Proof

Chapter 3

Exercise 3

1 a) Proof

b) \circ $\begin{array}{c|ccc} 0 & 0 & 2 & 4 \\ 0 & 0 & 2 & 4 \\ 2 & 2 & 4 & 0 \\ 4 & 4 & 0 & 2 \end{array}$

c) Yes

2 a) (i) 75

(ii) 45

(iii) 8

(iv) 0

(v) 9

(vi) 3

(vii) 4608

(viii) 288

b) No; $x = 0, y = 0$, or $x = y$

19 a–b) Proof

$$\begin{array}{c|cccc}
 \circ & a & b & c & d \\
 \hline
 a & a & b & c & d \\
 b & b & c & d & a \\
 c & c & d & a & b \\
 d & d & a & b & c
 \end{array}$$

c) Yes; 3, 11

$$\begin{array}{c|cccc}
 \infty & w & x & y & z \\
 \hline
 w & y & z & w & x \\
 x & z & w & x & y \\
 y & w & x & y & z \\
 z & x & y & z & w
 \end{array}$$

22 Proof

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 Proof

26 Proof

27 a–b) Proof

28 Proof

29 Proof

30 Proof

31 29

32 $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}, \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$

33 a) $\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}, \alpha^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$

and $\alpha^6 = e$.

b) (13)(245)

c) $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$, and $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$.

34 a) $\alpha = (1365)(2478), \beta = (18)(27)(36)(45), \gamma = (15)(247)(36)$

b) $\alpha\beta = (1283574)$

c) $\alpha\beta\gamma = (1783652)$

d) $\beta^{-1} = (18)(27)(36)(45) = \beta$

e) $(\beta\gamma)^{-1} = (18524)$

f) $\gamma^{-1}\beta^{-1} = (18524)$

g) $\alpha^{-1}\gamma\alpha = (13)(248)(56)$

h) $\text{ord}(\gamma) = 6$

i) $\text{ord}(\alpha^{-1}\gamma\alpha) = 6$

35 a) (1, 8, 2, 7)(3, 4, 5, 6)(9, 10)

b) (1, 10, 2, 9, 7, 5, 8, 3, 11, 6, 15, 14, 13, 12)

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

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

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

Practice questions 3

1 Proof

2 a–b) Proof

3 a–b) Proof

4 a (i) Proof

(ii) $a = 3, b = -\frac{3}{2}$

b (i) $A = \begin{pmatrix} 3 & 5 \\ -2 & -3 \end{pmatrix} \Rightarrow A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

(ii) $\{A, A^2, A^3, I\}$

5 a) $\begin{array}{c|cccc} * & a & b & c & d \\ \hline a & b & c & d & a \\ b & c & d & a & b \\ c & d & a & b & c \\ d & a & b & c & d \end{array}$

b) (i) $x = d$

(ii) $x = a$

6 a) Proof

b) R is an equivalence relation.

7 a) 6

b) (i) $p_2p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}$

(ii) They do not commute.

c) $(p_1^2p_2)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$

8 a–c) Proof

9 a) (i) Not closed (ii) Commutative

(iii) Not associative

b) (i) $e = 2$ (ii) $\{1, 2, 3\}$

10 a) (i) Proof

(ii) $\{2, 8\}, \{1, 4, 9\}$

b) Proof

Chapter 4

Exercise 4

- 1 Proof
- 2 a-b) Proof c) $\{1, 13\}, \{1, 9, 11\}$
- 3 a) $\{x, x^2, x^3, x^4\}$
b) $\{x, x^5\}$
c) 7 has 6 generators, 10 has 3, 15 has 8, and 20 has 8. The number of generators is the number of numbers less than or equal to the group order and is relatively prime to it.
- 4 a) $\{I, R, R^2\}, \{I, L\}$ b) No
- 5 a) 12, $([1], 12)$, $([2], 6)$, $([3], 4)$, $([4], 3)$, $([5], 12)$, $([6], 2)$, $([7], 12)$, $([8], 3)$, $([9], 3)$, $([10], 6)$, $([11], 12)$. Factors of 12.
b) 4, $([3], 4)$, $([7], 4)$, $([9], 2)$. Factors of 4.
c) 4, $([5], 2)$, $([7], 2)$, $([11], 2)$. Factors of 4.
d) 8, $([3], 4)$, $([7], 4)$, $([9], 2)$, $([11], 2)$, $([13], 4)$, $([17], 4)$, $([19], 2)$. Factors of 8.
e) 8, $(r, 4)$, $(r^2, 2)$, $(r^3, 4)$, $(L_1, 2)$, $(L_2, 2)$, $(L_3, 2)$, $(L_4, 2)$. Factors of 8.
- 6 a) $(U(3), 2)$, $(U(4), 2)$, $(U(12), 4)$
b) $(U(5), 4)$, $(U(7), 6)$, $(U(35), 24)$
c) $(U(4), 2)$, $(U(5), 4)$, $(U(20), 8)$
d) $(U(3), 2)$, $(U(5), 4)$, $(U(15), 8)$
 $|U(mn)| = |U(m)| \cdot |U(n)|$; $(U(4), 2)$, $(U(10), 4)$, $(U(40), 16)$;
 $|U(mn)| = |U(m)| \cdot |U(n)|$ iff m and n are relatively prime.
- 7 3 or 6
- 8 $|a^2| = 3$, $|a^3| = 2$, $|a^4| = 3$, $|a^5| = 6$.
 $|b^2| = 9$, $|b^3| = 3$, $|b^4| = 9$, $|b^5| = 9$, $|b^6| = 3$, $|b^7| = 9$, $|b^8| = 9$.
- 9 a) 2 and 6 generate $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$; 3 and 4 generate $\{1, 3, 4, 5, 9\}$; 10 generates $\{1, 10\}$.
b) Yes
- 10 a-b) Proof
- 11 a-b) Proof
- 12 Proof
- 13 Proof
- 14 a-b) Proof
c) Yes; 2 or 4; $\{1, 7\}$, $\{1, 9\}$, $\{1, 11\}$, $\{1, 15\}$, $\{1, 3, 9, 11\}$, $\{1, 5, 9, 13\}$
d) No
- 15 a) n
b) Proof
- 16 Proof
- 17 a) $\{1, x, x^2, y, xy, x^2y\}$
b) $\{1, y\}$, $\{1, xy\}$, $\{1, x^2y\}$, $\{1, x, x^2\}$
- 18 a) $1, x, x^2, y, xy, yx, x^2y, yxy, x^2yx, xyx^2$
b) $\{1\}$, $\{1, y\}$, $\{1, x^2yx\}$, $\{1, xyx^2\}$, $\{1, x, x^2\}$, $\{1, xy, yx^2\}$, $\{1, yx, x^2y\}$, $\{1, yxy, yxy\}$
- 19 Proof
- 20 Proof
- 21 Proof
- 22 No. Only if $H \subseteq K$ or $K \subseteq H$.
- 23 Proof

- 24 $\{1, 2, 4\}$, $\{1, 6\}$; $\{1, 3\}$, $\{1, 5\}$, $\{1, 7\}$; $\{1, 4\}$, $\{1, 11\}$, $\{1, 14\}$, $\{1, 2, 4, 8\}$, $\{1, 4, 7, 13\}$
- 25 Proof
- 26 $\left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, k \in \mathbb{N} \right\}, \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$
- 27 Proof
- 28 Proof
- 29 Proof
- 30 Proof
- 31 Proof
- 32 Proof
- 33 Generators: 8, 12
- 34 Not cyclic
- 35 Proof
- 36 If $x, y \in \mathbb{R}^+$ then $\ln(xy) = \ln x + \ln y$, thus f is a homomorphism. Since $f(x) = 0$ then $x = 1$, therefore $\ker f = \{1\}$.
- 37 If $x, y \in \mathbb{R} \setminus \{0\}$ then $|xy| = |x| |y|$, thus f is a homomorphism. Since $f(x) = 1$ then $x = \pm 1$, therefore $\ker f = \{-1, 1\}$.
- 38 If $f, g \in P[x]$, then $\varphi(f + g) = (f(x) + g(x))' = f'(x) + g'(x)$, thus φ is a homomorphism.
 $\varphi(f) = 0 \Rightarrow f'(x) = 0 \Rightarrow f$ must be a constant. Hence $\ker \varphi$ is the set of all constant functions with real coefficients.

Practice questions 4

- 1 a-c) Proof
- 2 a-b) Proof
- 3 a-b) Proof
- 4 a-c) Proof
- 5 a) $\begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$
b) For example: $\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}; \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}$
c) $\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}; \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}; \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}; \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}$
- 6 a)

$\begin{matrix} & f & g & h & j \\ f & f & g & h & j \\ g & g & f & j & h \\ h & h & j & f & g \\ j & j & h & g & f \end{matrix}$	$\begin{matrix} & f & g & h & j \\ f & f & g & h & j \\ g & g & f & j & h \\ h & h & j & f & g \\ j & j & h & g & f \end{matrix}$
---	---

b) $+_4$ is isomorphic with x_5 . Corresponding elements are: $0 \leftrightarrow 1$, $1 \leftrightarrow 2$, $2 \leftrightarrow 4$, $3 \leftrightarrow 3$; or $0 \leftrightarrow 1$, $1 \leftrightarrow 3$, $2 \leftrightarrow 4$, $3 \leftrightarrow 2$.
- 7 a-b) Proof c) $\{p^2, pq\}$
- 8 a) $\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & -b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
b) Proof c) Proof
- 9 a-b) Proof

10 a)

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

b) Proof

c)

Number	0	1	2	3	4	5
Order	1	6	3	2	3	6

d) Generators: 1 and 5

e) $\{0, 2, 4\}$

f) $\{0\}, \{0, 3\}$