Abstract Algebra - an Introduction to Group Theory.

1 Some Introductory concepts

1.1 Introduction

Abstract algebra concerns itself with the study of algebraic structures.
Structure exists in all the mathematics we use, however you have probably happily done arithmetic without worrying about the fact you are using a binary operation that may also be commutative and associative. In this unit you will learn about how a group structure can be imposed on many different systems to often give the same results.

As you work through this text you will find many examples of what is being described. Also you will find rules expressed in a general mathematical form without giving a specific example. You should always endeavour to add your own examples in order to deepen your understanding. *If you cannot add your own example - ask one of the tutors for help.*

1. 2 Sets

Structure can be added to sets. Some of the sets we use will be familiar, others may seem more esoteric!
Some familiar infinite sets

N	=	{natural numbers}	=	{1, 2, 3, 4,5 ,6, 7, 8, ...}
Z	=	{integers}	=	{..... ,–4, –3, –2, –1, 0, 1, 2, 3, 4, 5, ...}
Q	=	{rational numbers}	=	$\{a/b : a, b \in \mathbf{Z} \text{ and } b \neq 0\}$ *note* **Q** *stands for quotient*
R	=	{real numbers}	=	
C	=	{complex numbers}	=	$\{a + ib : a, b \in \mathbf{R} \text{ and } i = \sqrt{-1}\}$

Examples of sets containing different mathematical objects:

$$A = \left\{ \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix} \right\}$$

$$B = \left\{ \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix} \right\}$$

C = {ate, tea, eta, tae, aet, eat}
D = {the different ways of putting on a sweater}
= {correctly, inside out, back to front, inside out and back to front}.

1.3 Binary Operations

Informally:

We use binary operations all the time. Simplistically a binary operation combines two objects from some set to produce a third unique object.

For example:

$6 + 5 = 11$

$2 \times 7 = 14$

$\begin{pmatrix}2\\3\end{pmatrix} + \begin{pmatrix}5\\6\end{pmatrix} = \begin{pmatrix}7\\9\end{pmatrix}$

$(2 - 3i)(4+ i) = (11 - 10i)$ *where the operation is multiplication of complex numbers.*

$2^3 = 8$ *2 is raised to the power 3, the operation is called exponentiation.*

In each of the above examples two objects combine to give a unique third object.

Formally:

Suppose A is a set. We say that * is a *binary operation on the set A* if * is a rule by which two elements of A are combined to give a unique element of some set B.

Definition

A *binary operation* * on a set A is a function from A x A $\rightarrow$ B

We will write the result of combining a_1 and a_2 as $a_1 * a_2$.

(We recall that A x A is the set of all ordered pairs (a_1, a_2) consisting of two elements from A. Thus $\mathbf{R} \times \mathbf{R} = \mathbf{R}^2 = \{ (r_1, r_2) : r_1 \in \mathbf{R}, r_2 \in \mathbf{R} \}$ and may be thought of as the real plane).

As we can see from the previous examples most of our familiar operations on real numbers (e.g. addition, subtraction, multiplication) are binary operations as for example addition is a rule that takes two real numbers and returns the single number which we call a + b. We usually will use * to denote a binary operation unless there is some other obvious symbol such as + in the case of addition.

Further Examples

Some less obvious binary operations defined on the set of real numbers

$a * b = (a^2 + b^2)^{1/2}$ *eg* 3*4 = ..., 3 * 8 = ...

$a * b$ = the highest common factor of a and b *eg* 4 * 6 = ..., 6 * 7 = ...

The binary operation $\cap$ (intersection) defined on all the subsets of some universal set Ω

$A \cap B$ where $A, B \subseteq \Omega$

Well defined

In order for an operation to be a binary operation on some set it must be well defined, in other words it has to be possible to apply the binary operation to every pair of elements in the set.

Division is well defined on the set A = {1, 2, 3, 4, 5} since $a \div b$ is defined for all $a, b \in$ A. Thus division **is** a binary operation on set A.

Division is not well defined on the set B = {0, 1, 2, 3, 4, 5} since $a \div b$ is not defined when $b = 0$. Thus division **is not** a binary operation on set B.

Closure

Definition: A binary operation $* : A \times A \rightarrow B$ is said to be **closed** if $B \subseteq A$. ie if $a_1 * a_2 \in A$ for all $a_1, a_2 \in A$.

Informally we could think of this as a self-contained system - the result of applying the binary operation to each pair of elements from set A is always a member of the set A.

For example

The addition of natural numbers is **closed**, ie $a + b \in \mathbf{N}$, for all $a, b \in \mathbf{N}$.

Division defined on set A above ($A = \{1, 2, 3, 4\ 5\}$) is **not closed**, since $1 \div 2 = 0.5 \notin A$

*Remember to prove something is **not** true, you only need one counter example to establish this, whereas if something is true it must be true in every possible case, so we would express this in general terms.*

Exercise 1.3

1. Which of the following are binary operations?

   a) Multiplication of 2x2 matrices with real entries,
   b) Multiplication of 2x3 matrices with real entries,
   c) Addition of 2x2 matrices with real entries,
   d) Addition of 2x3 matrices with real entries,
   e) Forming the determinant of AB when A and B are two 2x2 matrices,
   f) Subtraction on the set of all integers,
   g) Division on the set of all integers excluding 0,
   h) Exponentiation on the set of natural numbers,
   i) Exponentiation on the set of integers,
   j) Finding the Lowest Common Multiple for a pair of natural numbers,
   k) Addition of complex numbers.

2. In each case where you have found a binary operation in 1, decide whether or not the operation is closed.

3. The following give the results of applying a binary operation to the set $\mathbf{Q} - \{0\}$, ie the set of rational numbers, excluding zero. Try to write down a formula for the result, in the form $a * b =$

   a) $5*2 = 8$, $4*7 = 12$, $8*6 = 15$
   b) $5*2 = 10/7$, $4*7 = 28/11$, $8*6 = 48/14 = 24/7$
   c) $5*2 = 17$, $4*7 = 39$, $8*6 = 62$

4. Establish whether the following binary operations are i) well-defined and ii) closed, on **Z**, **Q**, **R** respectively.

   a) $a * b = (a - b)/(a + b)$
   b) $a * b = ab + a$
   c) $a * b = \sqrt{(a^2 + b^2)}$
   d) $a * b = |a - b|$

1.4 Commutative and Associative Laws

Commutative Law :

A binary operation on a set A is commutative if $a * b = b * a$ for all $a, b \in A$.

Example 1.4.1

$a + b = b + a$, for all $a, b \in \mathbf{N}$, ie addition of natural numbers is **commutative**

Example 1.4.2

Consider $a * b = (a - b)/(a + b)$, for all $a, b \in \mathbf{Q}$,
$4*7 = -3/11$ and $7*4 = 3/11$, ie $4*7 \neq 7*4$, so * is **not commutative**.

Associative Law :

A binary operation on set A is associative if $a*(b*c) = (a*b)*c$ for all $a, b, c \in A$.

This is like punctuation in mathematics . It addresses the question of the need for brackets. Does an expression mean the same with or without brackets?
Which of the operations $+, -, \times, \div$ are associative?

Example 1.4.3

When $a * b = a$ (ie the first mentioned number) is defined on **N**
Then $a*(b*c) = a*b = a$ and $(a*b)*c = a*c = a$, so * is **associative**.

Example 1.4.4

When $a * b = ab + 1$ for all $a, b \in \mathbf{N}$
Then $a*(b*c) = a*(bc + 1) = a(bc + 1) + 1 = abc + a + 1$
and $(a*b)*c = (ab + 1)*c = (ab + 1)c + 1 = abc + c + 1$, so * is **not associative**

1.5 Identity

Definition : If a set A has a binary operation *, and there is a fixed element e of A such that $x*e = x$ and $e*x = x$ for all $x \in A$, then e is called an identity. *(We will later establish that if we have a group the identity is unique)*

As some binary operations are **not** commutative it is important that an identity has the same effect whether it is to the left or right of the binary operator. Basically an identity is an element which when combined with any element of the set leaves that element unchanged.

Example 1.5.1

$1 \times a = a$ and $a \times 1 = a$, for all $a \in \mathbf{R}$, so 1 is the identity for multiplication on the set of real numbers.

Example 1.5.2

$0 + a = a$ and $a + 0 = a$, for all $a \in \mathbf{Z}$, so 0 is the identity for addition on the set of integers.

Example 1.5.3

$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ and $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ so $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ is the identity for multiplication on the set of 2×2 matrices with real entries.

Example 1.5.4

$A \cap \Omega = A$ and $\Omega \cap A = A$, for all A where $A \subseteq \Omega$, so Ω is the identity for the binary operation intersection on the set of all subsets of Ω. (*Where Ω is the universal set*)

Not all binary operations defined on sets will give rise to an identity.

Example 1.5.5

Consider $a * b = ab + 1$ defined on the set of integers.
If there exists an identity e then $a * e = a$, so $ae + 1 = a$

$$ae = a - 1$$
$$e = (a - 1)/a = 1 - 1/a \notin \mathbf{Z}$$

Even if we changed the set on which the binary operation is defined to $\mathbf{R} - \{0\}$, e would still not be an identity as it is dependent on a.

1.6 Inverse

Definition : If a set A has a binary operation *, and an identity element e, and if for each and every element a of A, there can be found an element b such that $a * b = e$ and $b * a = e$ then b is called the inverse of a.

Example 1.6.1

$a + (-a) = 0$ and $(-a) + a = 0$ so $-a$ is the inverse of a under addition defined on the set of real numbers.

Example 1.6.2

$$\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\begin{pmatrix}1/a & 0\\ 0 & 1/a\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \text{ and } \begin{pmatrix}1/a & 0\\ 0 & 1/a\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

so $\begin{pmatrix}1/a & 0\\ 0 & 1/a\end{pmatrix}$ is the inverse of $\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}$ under matrix multiplication on the set of 2×2 diagonal matrices with equal real entries

Do all 2×2 matrices with real entries have an inverse?

If not give an example of a 2×2 matrix without an inverse.

Exercise 1.6

1. Using Ex 1.3 No 1
   In each case where you found a binary operation decide whether the operation is
   i) commutative ii) associative

2. For the following binary operations defined on **R**, decide whether the operations are
   i) commutative ii) associative

   a) $a*b = \min(a, b)$ ie the result of the binary operation is the least value
   b) $a*b = \dfrac{a+b}{ab}$
   c) $a*b = b$ ie the last mentioned
   d) $a*b = |a - b|$
   e) $a*b = \sqrt{(a^2 + b^2)}$

3. Find, if it exists, the identity element for each of the binary operations in question 2

4. For each of the binary operations in Question 2, which did have an identity element, find out if
   there is an inverse for every element w.r.t. the particular binary operation.

5. What is the identity of the binary operation $\cup$ defined on the set of subsets of some universal set. Does every subset have an inverse w.r.t. $\cup$.

6. A binary operation * is defined on **Z** by $a*b = a + b + ab$ for all $a, b \in \mathbf{Z}$
   Prove that * satisfies the associative law. Find the identity with respect to *. Does every element have an inverse with respect to * ?