Abstract Algebra

Contents

1 Groups

1.1 Binary Operators

Definition. A **binary operation** on a set S is a function $f : S \times S \to S$.
They are usually denoted with infix operators, e.g.

$$s \cdot t, s * t, etc.$$

A binary operation, $*$ is always closed, i.e.

$$\forall s, t \in S : s * t \in S$$

Definition. A binary operation $*$ is

1. **Associative** if $a * (b * c) = (a * b) * c$
2. **Communative** if $a * b = b * a$

Example. $+$, $-$, $\times$ are binary operations in $\mathbb{R}$
A binary operation can also be defined by a table:

$*$	a	b
a	b	a
b	a	b

i.e. $a * b = b$, $a * b = a$
$b * a = a$, $b * b = b$
It is communative:

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

It is also associative (which takes some time to prove).

1.2 Groups

Definition. A **group** is a set G with a binary operator that $*$ satisfy

1. $\forall a, b, c : a * (b * c) = (a * b) * c$ (Associativity)
2. $\exists e \in G : \forall a \in G : e * a = a * e = a$ (Identity)
3. $\forall a \in G : \exists a' \in G : a * a' = a' * a = e$ (Inverse)

Definition. A group is **abelian** iff it is communtative.
Definition. The **order** of a group G, denoted by $|G|$,m is the number of elements in it.
A finite group is a group with finite order.
An infinite group is a group with infinite order.
Example. $\mathbb{Z}$ with addition is a group, as

1. Addition is associative
2. 0 is the identity
3. The inverse of any integer a is $-a$

Example. Define $*$ on the reals to be

$$a * b = a + b + 3$$

We shall show that this makes a group

1. $a * (b * c) = a * (b + c + 3) = a + (b + c + 3) + 3 = a + b + c + 6$
   $(a * b) * c = (a + b + 3) * c = (a + b + 3) + c + 3 = a + b + c + 6$
   Therefore it is associative.

2. Let e be the identity. Hence $e * a = a$, $e + a + 3 = a$, $e = -3$

3. For all A, there should be an inverse a'.

$$\begin{aligned} a * a' &= -3 \\ a + a' + 3 = -3 \\ a = -a - 6 \end{aligned}$$

   So there exists an invers for all a since subtraction (and negation) is well defined in the reals

Definition. $\mathbb{Z}_n$ is the group (and later ring) of integers modulo n, containing 1, 2, ... $n - 1$.
Operations are defined as the normal operations (addition or multiplication) with the answers modulo n
Example. $\mathbb{Z}_3$ is a group with the following table:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

2 Glossary of Definitions

Definition. A **binary operation** on a set S is a function $f : S \times S \to S$.
Definition. A binary operation $*$ is

1. **Associative** if $a * (b * c) = (a * b) * c$
2. **Communative** if $a * b = b * a$

Definition. A **group** is a set G with a binary operator that $*$ satisfy

1. $\forall a, b, c : a * (b * c) = (a * b) * c$ (Associativity)
2. $\exists e \in G : \forall a \in G : e * a = a * e = a$ (Identity)
3. $\forall a \in G : \exists a' \in G : a * a' = a' * a = e$ (Inverse)

or (in words)

1. For all a, b and c in G, $a * (b * c) = (a * b) * c$ (Associativity)
2. There exists an e in G, called the identity element, such that for all a, $e * a = a * e = a$ (Identity)
3. For any a, there is an inverse element, a', in G such that $a * a' = a' * a = e$ (Inverse)

Definition. A group is **abelian** iff it is communtative.
Definition. The **order** of a group G, denoted by $|G|$,m is the number of elements in it.
Definition. $\mathbb{Z}_n$ is the group (and later ring) of integers modulo n, containing 1, 2, ... $n - 1$.
Operations are defined as the normal operations (addition or multiplication) with the answers modulo n