Contents

1 Group theory

1.1 Introduction

1.1.1 Abstract algebra

Abstract algebra allows us to discuss properties of types of mathematical structures.

Rather than construct a specific object, and explore its properties, we can explore the properties of an abstract structure with certain definitions. We can then apply findings from this to an any structure which meets the definition.

1.1.1.1 Examples of abstract algebra

We explore:

- Groups
- Rings
- Fields
- Vector spaces
- Inner product spaces

1.1.2 Defining groups

1.1.2.1 Magma

A magma, or groupoid, is a set with a single binary operation.

These can be defined as an ordered pair $(s, \odot)$ where s is the set, and $\odot$ is the binary operation.

If a and b are in s, then $a \odot b$ is also in s.

The following are magmas:

Natural numbers and addition $n \times n$ matrices with determinants other than 0 Natural numbers above 0 and addition Integers and addition Rational numbers and division $\{-1, 1\}$ and multiplication

The following are not magmas:

- Natural numbers up to 10 and addition

1.1.2.2 Semigroup

A semigroup is a magma whose binary operation is associative.

The following are semigroups:

Natural numbers and addition $n \times n$ matrices with determinants other than 0 Natural numbers above 0 and addition Integers and addition

The following are not semigroups:

- $\{-1, 1\}$ and multiplication
- Rational numbers and division
- Natural numbers up to 10 and addition

1.1.2.3 Monoid

A monoid is a semigroup with an identity element

The following are monoids:

- Natural numbers and addition
- $n \times n$ matrices with determinants other than 0
- Integers and addition
- $\{-1, 1\}$ and multiplication

The following are not monoids:

- Natural numbers above 0 and addition
- Rational numbers and division
- Natural numbers up to 10 and addition

1.1.2.4 Group

A group is a monoid where there is an inverse operation for the binary operation.

The following are groups:

Integers and addition $n \times n$ matrices with determinants other than 0 $\{-1, 1\}$ and multiplication

The following are not groups:

Natural numbers above 0 and addition Rational numbers and division Natural numbers and addition Natural numbers up to 10 and addition

1.1.3 Subgroups

A subgroup of a group is a subset of a group, which also forms a group with the same element.

For example all even numbers are a subgroup of the addition group of integers.

1.1.4 Abelian groups

A commutative group, that is where $a \odot b = b \odot a$.

The following are abelian groups:

- Integers and addition
- $\{-1, 1\}$ and multiplication

The following are not abelian groups:

- Natural numbers above 0 and addition
- Rational numbers and division
- Natural numbers and addition
- Natural numbers up to 10 and addition
- $n \times n$ matrices with determinants other than 0

1.1.5 Group order

For finite groups, each element e has:

$e^n = I$

For some $n \in \mathbb{N}$

Where I is the identity element.

The order of the group is the smallest value of n such that that holds for all elements.

For example in the multiplicative group $G = \{-1, 1\}$ the order is 2.

Or:

$|G| = 2$

Additionally

$|-1| = 2$

$|1| = 1$

1.2 Creating groups

1.2.1 Permutations and the symmetric group

A permutation is defined as a bijection from a set to itself.

For a set of size n, the number of permutations is $n!$. This is because there are n possibilities for the first item, $n-1$ for the second and so on.

1.2.1.1 The symmetric group

The set of all permutations forms a group, the symmetric group. This forms a group because:

- There is an identity element

- Each combination of permutations is also in the group.
- Each permutation has an inverse in the group.

1.2.1.2 Permutation groups

A subgroup of the symmetric group is called a permutation group.

1.2.2 Morphism

Morphisms are functions which preserve the relationships between members of a set, and specified functions.

That is, if:

$a \odot b = c$

Then $f(x)$ is morphism if:

$f(a) \odot f(b) = f(a \odot b)$

Here we discuss morphisms in the context of groups, but we can define morphisms for sets with more than one function, for example with addition and multiplication.

Morphisms are also known as homomorphisms.

The following are morphisms of the additive group of integers.

Where we refer to c, $c \neq 0 \in \mathbb{I}$.

- $f(x) = 0$
- $f(x) = x$
- $f(x) = cx$
- Converting natural numbers to integers

The following are not morphisms

- $f(x) = x + 1$

1.2.2.1 Isomorphism

An isomorphism is a morphism which has an inverse.

This means the function is bijective.

The following are isomorphisms:

- $f(x) = x$
- $f(x) = cx$

- Converting natural numbers to integers

The following are not isomorphisms

- $f(x) = 0$
- $f(x) = x + 1$

1.2.2.2 Endomorphism

An endomorphism is one where the domain and codomain are the same.

The following are endomorphisms:

- $f(x) = 0$
- $f(x) = x$
- $f(x) = cx$

The following are not endomorphisms

- Converting natural numbers to integers
- $f(x) = x + 1$

1.2.2.3 Automorphism

An endomorphism which is also an isomorphism

The following are automorphisms:

- $f(x) = x$
- $f(x) = cx$

The following are not automorphisms

- $f(x) = 0$
- $f(x) = x + 1$
- Converting natural numbers to integers

1.2.2.4 Monomorphism

A morphism which is injective. That is:

$f(a) = f(b) \rightarrow a = b$

The following are monomorphisms:

- $f(x) = x$
- $f(x) = cx$

- Converting natural numbers to integers

The following are not monomorphisms:

- $f(x) = 0$
- $f(x) = x + 1$

1.2.3 Generating sets

We can define a group through a generating set and an operation.

And define the group as $G =< S >$

1.2.4 Finite groups

Consider the set of natural numbers and addition modulo 4. This forms a group containing:

$\{0, 1, 2, 3\}$

This can be written as Z_4 or more generally as Z_n, or Z/nZ.

1.3 Group operations

1.3.1 The group commutator

The group commutator is:

$[a, b] = a^{-1}b^{-1}ab$

If the group is abelian then $[a, b] = 0$. The group commutator is a measure of how non-abelian the group is.

This has the following properties:

Alternativity: $[A, A] = I$

1.3.2 The direct product of groups

If we have two groups G and H we can form new group $G \times H$.

For every $g \in G$ and $h \in H$ there is $(g, h) \in G \times H$.

The binary operation we have is:

$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1, h_2)$

1.4 Specifc groups

1.4.1 The trivial group

The trivial group is the group with just the identity member I.

1.4.2 The infinite cyclic group (Z)

1.4.2.1 The additive group of integers

1.4.2.2 Generating cyclic groups

We can generate a group with a single element, it is a cyclic group.

For example, we can define a group $G =< 1 >$ which gives us the additive group of integers.

1.4.2.3 Infinite cyclic groups are isomorphic to the additive group of integers

More generally, any infinite cyclic group is isomorphic to the additive group of integers.

Consider the multiplicative group of $< i >$.

This contains $\{1, -1, i, -i\}$.

This is also automorphic to the natural number and modulo addition group above.

We can define finite cyclic groups of size n using the generating element $z^{\frac{1}{n}}$. This is isomorphic to the general cyclic group C_n, and to Z/nZ.

1.4.2.4 Abelian cyclic groups

Cyclic groups are abelian.

1.4.3 The finite cyclic groups (C_n or Z_n)

1.4.4 The circle group T

The circle group, T, includes all complex numbers of magnitude 1.

1.5 Normal subgroups

1.5.1 Cosets and normal subgroups

A coset is defined between a group and a subgroup of the group.

For a group G, and its subgroup H:

- The left coset is $\{gH\}$
- The right coset is $\{Hg\}$

For $\forall g \in G$.

For abellian groups, the left and right cosets are the same.

The left and right cosets can also be the same, even if the group G is not abelian.

1.5.1.1 Normal subgroups

If the left and right cosets are the same then H is a normal subgroup.

1.5.1.2 Cosets divide a group.

Consider two left cosets, aH and bH, with a common element.

This means that $ah_i = bh_j$.

We can use this to get:

$a = bh_j h_i^{-1}$

$b = ah_i h_j^{-1}$

We know that:

$ah \in aH$

$bh \in bH$

So:

$bh_j h_i^{-1} h \in aH$

$ah_i h_j^{-1} h \in bH$

And so:

$bH \subset aH$

$aH \subset bH$

Therefore:

$aH = bH$

1.5.1.3 Example 1

Consider the group $\{-1, 1\}, \times$

For the subgroup $\{1\}, \times$, the left coset is $\{gH\} = \{1, -1\}$.

The right coset is the same.

1.5.1.4 Example 2

Consider the group of integers and addition: $(Z, +)$

For subgroup $(mZ, +)$, the left and right cosets are the same because the group is abelian.

The coset of the subgroup is the subgroup multiplied by each element in G.

This is mZ, $mZ + 1$, $mZ + 2$ and so on.

Once we reach $mZ + m$ this has looped, and is already a coset, so we only need the sets upto $mZ + m - 1$.

1.5.2 Quotient groups

We have a group G and a normal subgroup N.

We define a quotient group from this as G/N. This is the set of cosets from N.

1.5.3 Group extension

This defines a group G from a normal subgroup N and a quotient group Q.

1.6 Theorems

1.6.1 Cayley's theorem

Cayley's theorem states that every group G is isomorphic to a subgroup of the symmetric group acting on G.

Multiplication by a member of G is a bijective function, as for each g there is also a g^{-1}.

This means that multiplication of each member of G is a permutation, and so is a subset of the symmetric group on G.

1.6.2 Lagrange's theorem

Lagrange's theorem states that for any finite group G, the order of every subgroup is a divisor of the order of G.

Consider subset H. We know that all cosets are disjoint, and that the union of all cosets is G.

As cosets are the same size, we know that:

$|G| = m|H|$, where m is the number of cosets.

This means that if a group has order 10, a subgroup must have order 1, 2 5 or 10.

1.7 Group action

1.7.1 Group action

We have a group G and a set S.

We have a function $g.s$ which maps onto S such that:

- $I.s = s$
- $(gh).s = g(h.s)$