An Introduction to Proof-based Mathematics

Harvard/MIT ESP: Summer HSSP

Isabel Vogt

Class 2: Introduction to Groups

Class Objectives

- Binary Operations
- Groups Axioms
  - Closure
  - Associativity
  - Identity Element
  - Unique Inverse
- Abelian Groups
- Permutations
- Symmetry Groups

1. **Binary Operations on Sets**

A **binary operation** is some rule for combining two objects to get another object.

Some familiar binary operations are $+, \times, -, \div$, however another binary operation could be:

$$a * b = a + b(a - b)$$

What is 3*7?

We could also have a binary operation that combined two members of this class and output a "word" formed from the first two letters of their first names.

For example: If we call this binary operation $\otimes$, then Michael $\otimes$ Helen would be Mihe.

A binary operation defined on a set A means that one may combine the elements of A under that binary operation.

NOTE: this does not assume closure, ie that the result will also be an element of A!

A set X is **closed** under a certain binary operation $*$ if $\forall\ a, b \in X, a * b \in X$

This intuitively means that the set is self-contained to any combination of elements using the operation $*$

It is trapped!

Example:

Let A be the set $\{1, 2, 3, 4, 5\}$ and let $\diamond$ be defined by $a \diamond b = 2a - b$

What is $3 \diamond 2$?

What is $5 \diamond 2$?

Is this set A “closed” under the operation $\diamond$?

Would the set $\mathbb{N}$ be closed under the operation $\diamond$? Prove it or provide a counter example.

Would the set $\mathbb{Z}$ be closed under the operation $\diamond$? Prove it or provide a counter example.

2. **Associativity**

A binary operation $*$ is said to be **associative** if $\forall a, b,\ a * (b * c) = (a * b) * c$

This is the order of operations condition. If one may group the order of successively combining three elements in both ways and always get the result, the operation is associative.

Example:

Let $\star$ be defined on the set $\mathbb{Z}$ such that $\forall a, b \in \mathbb{Z}, a \star b = 2a + 3b$. Is this operation $\star$ associative?

Let $\ominus$ be defined on the set $\mathbb{Z}$ such that $\forall a, b \in \mathbb{Z}, a \ominus b = a + b + ab$. Is this operation $\ominus$ associative?

3. **Commutativity**

A binary operation $*$ is said to be **commutative** if $\forall a, b,\ a * b = b * a$

This is the order of combination condition. This is different than associativity in which the oder is in how one groups successive applications of the operator. Here the order of *elements* is reversed.

Example:

Let $\star$ be defined on the set $\mathbb{Z}$ such that $\forall a, b \in \mathbb{Z}, a \star b = 2a + 3b$. Is this operation $\star$ associative?

Let $\ominus$ be defined on the set $\mathbb{Z}$ such that $\forall a, b \in \mathbb{Z}, a \ominus b = a + b + ab$. Is this operation $\ominus$ associative?

4. **Identity Element**

For an operation $*$ defined on a set S, $e \in S$ is said to be an **identity element** if $\forall a \in S, a * e = a$

What is the identity element in $\mathbb{Z}$ for the operation $+$?

For $\times$?

It is important that the identity element be universal, i.e. there is one e in the S which is an identity for all elements in S.

This comes down to the difference between the statements:

$$\forall a \in S, \exists e \in S \mid a * e = a$$

and

$$\exists e \in S \mid \forall a \in S, a * e = a$$

Which one determines an identity element?

An identity element defined as such is **unique**, and we can prove this only from the definition!

RTP: An identity element for a set S must be unique.

5. **Inverse**

For a binary operation $*$ defined on a set S with an identity element $e \in S$, every element a is said to have an inverse if $\forall\ a \in S, \exists\ a^{-1} \in S$ such that $a * a^{-1} = e$

How is this definition different than the identity definition? Is the inverse for each $a \in S$ universal or particular to the element?

We can also prove that if under an associative binary operation $*$ on a set S, a has an inverse a^{-1}, then this inverse is unique.

RTP: Given an associative binary operation $*$ defined on a set S, if each element has an inverse, this inverse is unique.

6. The Group Axioms

A **Group** is a particular kind of set with a binary operation $*$ defined upon it which satisfies the following four axioms:

- G1. Closure: The set must be closed under the operation $*$
- G2. Associativity: The operation $*$ must be associative for all elements of G
- G3. Right Identity: $\exists e$ such that $\forall a \in G, a * e = a$
- G4. Right Inverse: $\forall a \in G, \exists a^{-1}$ such that $a * a^{-1} = e$

So a group is just a particular type of set associated with an operation. We can characterize some easy groups.

These axioms are special because the are **independent**; if we remove one, they no longer specify a group.

Do these axioms explicitly state that:

- $a * b = b * a$?
- the identity e is unique?
- the identity e is also a left identity: $e * a = a$?
- the inverse of a is unique?
- the right inverse of a is also its left inverse: if $a * b = e$ then $b * a = e$?

Many of these things are true, but we will have to prove them as theorems. Some we already have!

7. Model 1: The set G is the set of integers $\mathbb{Z}$. The operation is addition.
   Confirm that all the axioms are satisfied.

8. Model 2: The set G is the set of nonzero rational numbers $\mathbb{Q}$. The operation is multiplication.

   (a) Confirm that all the axioms are satisfied.

   (b) Why the restriction to "nonzero?"

   (c) Can you use the integers in place of the rational numbers and still have a group?

9. **Some Theorems**

RTP: The right inverse of an element a is also its left inverse

RTP: The right identity element e is also a left identity

RTP: Given a group G with operation $*$, If $b * a = c * a$, then $b = c$

10. **Abelian Group**

An **Abelian group** is a commutative group. The binary operation $*$ must be commutative for all elements of the group G

For example:

The group $\{\mathbb{Z}, +\}$ is an Abelian group. Can you prove this?

Note: Group notation is in the form { Set, operation}

So $\{\mathbb{Z}, +\}$ is the group made from the set containing the integers under the operation of $+$.

11. **Modular Arithmetic**

Modular arithmetic is going to become very important as we move into number theory, but it is also very prevalent in finite groups.

Modular arithmetic takes the infinite set of numbers on which we normally work, and shrinks it down to some finite set of n elements. Every number is then represented as the remainder that number yields upon division by n.

So say we are working with addition **modulo** 3. This is often referred to as addition (mod 3) or $+_3$.

Here the set of numbers on which we are working is $\{0, 1, 2\}$

All number which are multiples of 3 (ie the set $\{3n|n \in \mathbb{Z}\}$) are equal to 0 (mod 3)

All the numbers which have a reminder of 1 upon division by three can be represented as the set:
$\{1, 4, 7, 10, ...\}$ or $\{3n + 1|n \in \mathbb{Z}\}$ and are equal to 1 (mod 3)

All the numbers which have a reminder of 2 upon division by three can be represented as the set:
$\{2, 5, 8, 11, ...\}$ or $\{3n + 2|n \in \mathbb{Z}\}$ and are equal to 2 (mod 3)

We can think of this as clock arithmetic, where numbers wrap back around upon themselves.

Examples:

What is $4 +_5 3$?

What is 17 (mod 11)?

What is 7 + 8 (mod 13)?

Model 3: Show the set G is the set $\{$0,1, 2, 3$\}$ under addition modulo 4 ($+_5$) satisfies the group axioms.

12. **Cayley Tables**

A Cayley Table is a table of all combinations of elements in a set under a binary operation.

For example: the Cayley table for addition modulo 4 on the set {0,1,2,3} is:

RTP: If {G, *} is a group, then each element of G will appear once and only once in each row and column of the Cayley table.

13. **Symmetry Groups**

The symmetry group of the equilateral triangle

14. **Permuations**

A permutation is an invertible function whose domain and image are both the first n integers. It takes an integer as its argument and returns an integer as the function value. It is most easily represented in "cycle notation" by a symbol (for $n = 6$) like $f = (134)(26)(5)$. This is shorthand for

$f(1) = 3, f(3) = 4, f(4) = 1, f(2) = 6, f(6) = 2, f(5) = 5$. Usually a single-element cycle like (5) is omitted, and a permutation like (1)(2)(3)(4)(5)(6) that does nothing is symbolized by I.

If $g = (3625)$

- What is $g(6)$?
- What is $g(5)$?
- What is $g(4)$?

For $n = 3$ the product (23)(123) is equal to (13). Why?

- (123) takes 1 to 2, then (23) takes 2 to 3.
- (123) takes 2 to 3, then (23) takes 3 back to 2.
- (123) takes 3 to 1, then (23) leaves 1 alone.
- So the net effect of ba is to interchange 1 and 3.

Similarly, the product (13)(12) is equal to (123). Why?

- (12) takes 1 to 2, then (13) leaves 2 alone.
- (12) takes 2 to 1, then (13) takes 1 to 3.
- (12) leaves 3 alone, then (13) takes 3 to 1, .
- So the net effect is $1 \to 2 \to 3 \to 1$.

Calculate (123)(123).

Calculate (123)(132).

15. Model 4: The set G is the set of permutations of the first 3 integers. The operation is “multiplication” (successive performance) of permutations. We can place the numbers at the vertices of an equilateral triangle, with 1 at the lower left, 2 at the lower right, 3 at the top.

    (a) List the six permutations, and associate each with a symmetry operation of the triangle.

    (b) Confirm that the group axioms are satisfied.

    (c) Show that (12)(13) and (13)(12) are not equal. Is this a problem for the axioms?

16. Model 5: The set G is the set of symmetry operations of the regular hexagon. The operation is composition (successive performance) of operations. Each can be associated with a permutation of the first six integers.

    (a) Write the permutation that corresponds to a 60 degree counterclockwise rotation, and confirm that its square and its inverse are what you would expect geometrically.

    (b) What permutation corresponds to a 180 degree rotation about an axis through vertices 1 and 4? What is its inverse?

    (c) What symmetry operation corresponds to the permutation (14)(23)(56)?

17. **Challenge Problem**

You will investigate two groups:

$\{\{1,2,3,4\},\times_5\}$ and $\{\{0,1,2,3\},+_4\}$ and their similarities.

(a) Verify that both of these sets satisfy all the group axioms

(b) Write out the Cayley tables for both of these groups

(c) Is one or both groups Abelian?

(d) How do the two groups have a similar structure? If you call 1=a, 2=b, 3=c, 4=d in the first group, can you find a way to call 0,1,2,3 a,b,c,d (in some order) in the second group so that the Cayley tables are identical?