An Introduction to Proof-based Mathematics

Harvard/MIT ESP: Summer HSSP
Isabel Vogt

Class 3: Further Group Properties

Class Objectives

- Cayley Tables
- Permutations
- Symmetry Groups
- Group Order
- Order of an Element
- Cyclic Groups

1. **Group Order**

   The **order of a group** $\{G, *\}$ is the number elements in G, sometimes represented by $n(G)$

   For an **infinite group**, the order of the groups is infinite.

   A **finite group** necessarily has finite order.

   What concept from sets is related to this idea in groups?

2. **Order on an Element**

   The **order of an element** $a \in G$ is the smallest positive integer m such that $a^m = e$, where e is the identity element of the group.

   Note: here a^m is used to represent repeated combination using the binary operation $*$ defined upon the group. Written out for $m = 3$ this is: $a * a * a$.

   This intuitively means the number of times you must combine an element with itself to get back to the identity element.

   What is the order of the identity element?

   Given the group $\{0, 1, 2\}$ under $+_3$, give the oder of every element in the group.

3. **Cyclic Groups**

Consider the group $\{\mathbb{Z}_7\ 0, \times_7\}$.

Draw the Cayley table for this group:

What is the order of each element:

- $1 =$
- $2 =$
- $3 =$
- $4 =$
- $5 =$
- $6 =$

What is the order of the group? Do you notice anything about the order of the elements and the group?

Let $3 = g$, what is:

- $g^1 =$
- $g^2 =$
- $g^3 =$
- $g^4 =$
- $g^5 =$
- $g^6 =$

Rewrite the set $\{1, 2, 3, 4, 5, 6\}$ in terms of g.

What you have discovered is a **generator** of a **cyclic group**!

A group $\{G, *\}$ is said to be **cyclic** if $\exists g \in G$ such that $\forall x \in G, x = g^m$ for some $m \in \mathbb{Z}$. g is said to be a **generator** of the group.

Note, the generator is not necessarily unique. In the example on the previous page, 5 was also a generator for the group.

RTP $\forall n \in \mathbb{Z}^+$, $\{\mathbb{Z}_n, +_n\}$ is a cyclic group.

RTP Given a finite group $\{G, *\}$ with order n, and an element $a \in G$ with order n, G is cyclic.

RTP All cyclic groups are Abelian

RTP For all $n \in \mathbb{Z}^+$, there is a cyclic group of order n