Intro + lecture 1.1

About me: Andrew Kobin

ajkobin@emory.edu

Post-Doctoral Fellow

Office: MSC E425

Office Hours

Agenda:

- introductions
- syllabus
- quick tour of Canvas
- intro to rings

Introduction

Abstract algebra is in general concerned with different types of structure.

In Algebra I, we learned about groups: a set G is a group if it has a binary operation $\cdot : G \times G \to G$ which is associative, unital and has inverses.

The key questions we will continue to investigate are:

- What other structures can we define?

  (rings, fields, modules, vector spaces)

- How do different structures relate?

  (homomorphisms, functors)

- What do these additional structures reveal about the sets themselves?

Some of the most important examples of groups and rings are:

symmetries

integers

$\mathbb{Z}$

permutations

modular arithmetic

roots of polynomials

$$(x-1)(x^2+x+1)$$

$x=1$

$x=e^{2\pi i/3}$

$x=e^{4\pi i/3}$

polynomials

$$x^3-1 = (x-1)(x^2+x+1)$$

Motivating Example The integers $\mathbb{Z}$

have two binary operations:

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \qquad \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

$$(x, y) \mapsto x+y \qquad (x, y) \mapsto xy$$

As we saw in Algebra I, $(\mathbb{Z}, +)$ forms an abelian group:

- $(x+y)+z = x+(y+z)$
- $x + 0 = x = 0 + x$
- $x + (-x) = 0 = (-x) + x$
- $x + y = y + x$.

Is $(\mathbb{Z}, \cdot)$ also a group? Let's check:

- $(xy)z = x(yz)$ ✓

- $x1 = x = 1x$ ✓

- $xx^{-1} = 1 = x^{-1}x$ only if $x \neq 0$ ✗

Instead, we can consider the set of nonzero integers under multiplication,

$$\mathbb{Z}^{\times} = \{x \in \mathbb{Z} \mid x \neq 0\}.$$

$\boxed{\text{Proposition}}$ $(\mathbb{Z}^{\times}, \cdot)$ is an abelian group.

Exercise 1: Prove it for review.

So the set $\mathbb{Z}$ admits two binary operations, $+$ and $\cdot$, that determine group structures on $\mathbb{Z}$ and $\mathbb{Z}^\times$, resp.

They interact via the distributive property:

$$x(y+z) = xy + xz.$$

This says that $\mathbb{Z}$ is a **ring**.

for the French "anneau"

Def A **ring** is a set A equipped with two binary operations

$$+ : A \times A \to A \quad \text{and} \quad \cdot : A \times A \to A$$

satisfying :

(1) $(A, +)$ is an abelian group.

(2) For all $x, y, z \in A$, $(xy)z = x(yz)$.

(3) There exists an element $1 \in A$ such that $1x = x = x1$ for all $x \in A$.

(4) For all $x, y, z \in A$,

$$x(y+z) = xy + xz \quad \text{and} \quad (x+y)z = xz + yz.$$

In addition, A is called commutative if

(5) For all $x, y \in A$, $xy = yx$.

Exercise 2: Write out each part of axiom (1) to review the definition of group/abelian group.

Remarks: (i) Some people still call A a ring if it doesn't have $1 \in A^{\times}$, but we will always assume this is the case.

(e.g. $2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\}$)

(ii) Notice that not every $x \in A$ is

required to have a multiplicative inverse,

i.e. some $x^{-1} \in A$ with $xx^{-1} = 1 = x^{-1}x$.

In particular, $(A, \cdot)$ is not a group —

rather, it's a (multiplicative) monoid.

For comparison, $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$

is an additive monoid since no $n \in \mathbb{N}_0$

has an additive inverse $-n \in \mathbb{N}_0$.

$\boxed{\text{Prop}}$ The set of units in a ring A,

$A^\times = \{x \in A \mid xy = 1 = yx \text{ for some } y \in A\}$, is a group under $\cdot$. If A is commutative, then $A^\times$ is abelian.

Exercise 3: Prove it!

This gives us a new way of generating interesting examples of groups: start with a ring A and compute $A^\times$.

Next time: examples and properties of rings.