MATH 817: INTRODUCTION TO MODERN ALGEBRA I FALL 2025

JACK JEFFRIES

Contents

Introduction

These are the lecture notes and class materials for Math 817 Introduction to Modern Algebra I in Fall 2025. This is the first of a two part course on groups, rings, modules, and fields. In this first half, we will discuss group theory, including group actions, and introduce rings. A major goal of this course is to prepare graduate students for the PhD qualifying exam in algebra. The lecture notes draw heavily on Eloísa Grifo's notes from Fall 2024:

https://eloisagrifo.github.io/Teaching/algebra.pdf

which in turn draw from earlier lecture notes of Mark Walker and Alexandra Seceleanu. The impatient reader can go there to read ahead. The textbook

Abstract Algebra by Dummit and Foote

is a good resource covering similar material at a similar level.

1. Lecture of Monday, August 25

This class has four major topics: Groups, Rings, Modules, and Fields. Let us begin with group theory.

A group is a basic algebraic structure that is found in many objects we might otherwise care about, but has enough structure that we can deduce general statements and theorems.

Definitions and first examples.

Definition 1.1. A **binary operation** on a set S is a function $S \times S \to S$. If the binary operation is denoted by $\cdot$, we write $x \cdot y$ for the image of (x, y) under the binary operation $\cdot$.

Remark 1.2. We often write xy instead of $x \cdot y$ if the operation is clear from context.

Remark 1.3. We say that that a set S is closed under the operation $\cdot$ when we want to emphasize that for any $x, y \in S$ the result xy of the operation is an element of S. But note that closure is really part of the definition of a binary operation on a set, and it is implicitly assumed whenever we consider such an operation.

Definition 1.4. A **group** is a set G equipped with a binary operation $\cdot$ on G called the **group multiplication**, satisfying the following properties:

- **Associativity**: For every $x, y, z \in G$, we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- **Identity element**: There exists $e \in G$ such that $e \cdot x = x \cdot e = x$ for all $x \in G$.
- **Inverses**: For each $x \in G$, there is an element $y \in G$ such that $xy = e = yx$.

The element e is called the **identity element** or simply **identity** of the group. For each element $x \in G$, an element $y \in G$ such that $xy = e = yx$ is called an **inverse** of x. We may write that $(G, \cdot)$ is a group to mean that G is a group with the operation "$\cdot$".

The **order** of the group G is the number of elements in the underlying set.

Example 1.5. Fix a positive integer n, and let

$$\mathrm{GL}_n(\mathbb{R}) := \{\text{invertible } n \times n \text{ matrices with entries in } \mathbb{R}\}.$$

An invertible matrix is one that has a two-sided (multiplicative) inverse. This is called the **general linear group** of size n matrices with entries in $\mathbb{R}$. This is a group: multiplication of matrices is associative, there is an identity element given by the identity matrix, and every element has an inverse by definition.

Vaguely, the definition of group is motivated by the idea that a collection of functions from set to itself that preserves some extra structure naturally satisfies the three axioms: for example, the general linear group consists of functions from the vector space $\mathbb{R}^n$ to itself that preserve the linearity structure.

Remark 1.6. Although a group is the set *and* the operation, we will usually refer to the group by only naming the underlying set, G.

Remark 1.7. A set G equipped with an associative binary operation is a **semigroup**; if a semigroup also has an identity element, it is a **monoid**.

While *we will not be discussing semigroups nor monoids that are not groups in this class*, they can be useful and interesting objects. We will however include some fun facts about monoids in the remarks. In particular, there will be no monoids whatsoever in the qualifying exam.

Lemma 1.8. *For any group G, we have the following properties:*

(1) The identity is unique: there exists a unique $e \in G$ with $ex = x = xe$ for all $x \in G$.
(2) Inverses are unique: for each $x \in G$, there exists a unique $y \in G$ such that $xy = e = yx$.

Proof. Suppose e and e' are two identity elements; that is, assume e and e' satisfy $ex = x = xe$ and $e'x = x = xe'$ for all $x \in G$. Then

$$e = ee' = e'.$$

Now given $x \in G$, suppose y and z are two inverses for x, meaning that $yx = xy = e$ and $zx = xz = e$. Then

$$\begin{aligned} z &= ez && \text{since } e \text{ is the identity} \\ &= (yx)z && \text{since } y \text{ is an inverse for } x \\ &= y(xz) && \text{by associativity} \\ &= ye && \text{since } z \text{ is an inverse for } x \\ &= y && \text{since } e \text{ is the identity.} \end{aligned}$$

□

Remark 1.9. Note that our proof of Lemma 1.8 also applies to show that the identity element of a monoid is unique, since we did not use the existence of inverses in the proof of part (1).

Given a group G, we can refer to *the* identity of G. Similarly, given an element $x \in G$, we can refer to *the* inverse of x.

Notation 1.10. Given an element x in a group G, we write x^{-1} to denote its unique inverse.

Remark 1.11. In a monoid G with identity e, an element x might have a **left inverse**, which is an element y satisfying $yx = e$. Similarly, x might have a **right inverse**, which is an element z satisfying $xz = e$. An element in a monoid might have several distinct right inverses, or several distinct left inverses, but if it has both a left and a right inverse, then it has a unique left inverse and a unique right inverse, and those elements coincide. This follows from a careful analysis of the proof of part (2) of Lemma 1.8.

Exercise 1.12. Give an example of a monoid M and an element in M that has a left inverse but not a right inverse.

Definition 1.13. Let G be a group, $x \in G$, and $n \geqslant 1$ be an integer. We write x^n to denote the element obtained by multiplying x with itself n times:

$$x^n := \underbrace{x \cdots x}_{n \text{ times}}.$$

Exercise 1.14 (Properties of group elements). Let G be a group and let $x, y, z, a_1, \ldots, a_n \in G$. Show that the following properties hold:

(1) If $xy = xz$, then $y = z$.
(2) If $yx = zx$, then $y = z$.
(3) $(x^{-1})^{-1} = x$.
(4) $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.
(5) $(x^{-1}yx)^n = x^{-1}y^n x$ for any integer $n \geqslant 1$.
(6) $(x^{-1})^n = (x^n)^{-1}$.

Notation 1.15. Given a group G, an element $x \in G$, and a positive integer n, we write $x^{-n} := (x^n)^{-1}$.

Note that by Exercise 1.14, $x^{-n} = (x^{-1})^n$.

Exercise 1.16. Let G be a group and consider $x \in G$. Show that $x^a x^b = x^{a+b}$.

Definition 1.17. A group G is **abelian** if the group multiplication $\cdot$ is commutative, meaning that $x \cdot y = y \cdot x$ for all $x, y \in G$.

Often, but not always, the group operation for an abelian group is written as "+" instead of "$\cdot$". In this case, the identity element is usually written as 0 and the inverse of an element x is written as $-x$.

Example 1.18.

(1) The **trivial group** is the group with a single element $\{e\}$. This is an abelian group.
(2) The pairs $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are abelian groups.
(3) For any n, let $\mathbb{Z}/n$ denote the integers modulo n. Then $(\mathbb{Z}/n, +)$ is an abelian group where $+$ denotes addition modulo n.
(4) For any field F, such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Z}/p$ for a prime p, the set $F^\times := F \setminus \{0\}$ is an abelian group under multiplication. We will later formally define what a field is, but these fields might already be familiar to you.

Example 1.19. Let F be any field. If you are not yet familiar with fields, the real or complex numbers are excellent examples. Consider a positive integer n, and let

$$\mathrm{GL}_n(F) := \{\text{invertible } n \times n \text{ matrices with entries in } F\}.$$

An invertible matrix is one that has a two-sided (multiplicative) inverse. It turns out that if an $n \times n$ matrix M has a left inverse N then that inverse N is automatically a right inverse too, and vice-versa; this is a consequence of a more general fact we mentioned in Remark 1.11.

It it not hard to see that $\mathrm{GL}_n(F)$ is a nonabelian group under matrix multiplication. Note that $(\mathrm{GL}_1(F), \cdot)$ is simply $(F^\times, \cdot)$.

Even if the group is not abelian, the set of elements that commute with every other element is particularly important.

Definition 1.20. Let G be a group. The **center** of G is the set

$$\mathrm{Z}(G) := \{x \in G \mid xy = yx \text{ for all } y \in G\}.$$

Remark 1.21. Note that the center of any group always includes the identity. Whenever $\mathrm{Z}(G) = \{e_G\}$, we say that the center of G is trivial.

Remark 1.22. Note that G is abelian if and only if $\mathrm{Z}(G) = G$.

One might describe a group by giving a presentation.

Informal definition 1.23. A **presentation** for a group is a way to specify a group in the following format:

$$G = \langle \text{ set of generators } \mid \text{ set of relations } \rangle.$$

A set S is said to **generate** or be a **set of generators** for G if every element of the group can be expressed in some way as a product of finitely many of the elements of S and their inverses (with repetitions allowed). A **relation** is an identity satisfied by some expressions involving the generators and their inverses. We usually record just enough relations so that every valid equation involving the generators is a consequence of those listed here and the axioms of a group.

Remark 1.24. We can only take products of finitely many of our generators and their inverses because we do not have a way to make sense of infinite products.

Note, however, that the set of generators and the set of relations are allowed to be infinite.

Example 1.25. The group $\mathbb{Z}$ has one generator, the element 1, which satisfies no relations.

Example 1.26. The following is a presentation for the group $\mathbb{Z}/n$ of integers modulo n:

$$\mathbb{Z}/n = \langle x \mid x^n = e \rangle.$$

Definition 1.27. A group G is called **cyclic** if it is generated by a single element. A group G is **finitely generated** if it is generated by finitely many elements.

Example 1.28. We saw above that $\mathbb{Z}$ and $\mathbb{Z}/n$ are cyclic groups.

Exercise 1.29. Prove that every cyclic group is abelian.

Exercise 1.30. Prove that $(\mathbb{Q}, +)$ and $\mathrm{GL}_2(\mathbb{Z}_2)$ are not cyclic groups.

In general, given a presentation, it is very difficult to prove certain expressions are not actually equal to each other. In fact,

> There is no algorithm that, given any group presentation as an input, can decide whether the group is actually the trivial group with just one element.

and perhaps more strikingly

> There exist a presentation with finitely many generators and finitely many relations such that whether or not the group is actually the trivial group with just one element is *independent of the standard axioms of mathematics*!