150A: Modern Algebra
Notes

Melissa Zhang
UC Davis

Winter 2024

Contents

These notes are for a course based on Artin's *Algebra*. As such, we generally follow the conventions in that book, but also introduce common terminology and vocabulary not used in the book.

Important terms are either *italicized* or **bolded**. In general, a bolded term indicates that I am introducing to you right now and that you should learn right now. An italicized term might just be an emphasis, or a term that we will seriously introduce later in the course.

1 Introduction to abstract algebra

In algebra, we use symbols to represent quantities, objects, relations, etc. This translates a specific problem into an abstract problem. We develop methods to solve this problem in more generality (i.e. abstractly, or algebraically) and then translate the solution back to the specific problem.

When I first saw algebra in middle school, this is the kind of problem I would solve:

Example 1.1. Tamara has 35 coins in nickels and quarters. In all, she has $4.15. How many of each type of coin does she have? [1]

Different subfields of algebra are used to solve different parts or types of problems.

Example 1.2. One of the nicest and most pervasive types of algebra is **linear algebra**:

- All relationships between variables are *linear*, as opposed to quadratic, exponential, non-algebraic, etc.
- We often simplify nonlinear problems using linear approximations, then obtain approximate solutions.
- *Matrix groups* are used *represent* more complicated abstract groups.

Example 1.3. *Modern* or *abstract* algebra is a more general term referring to all algebra beyond, say, solving single-variable equations or basic linear algebra. For example, topics in abstract algebra include

- algebraic structures: groups, rings, fields, lattices, representations, group actions, etc.

[1] from https://www.chilimath.com/lessons/algebra-word-problems/coin-word-problems/

- relations between them: homomorphisms, isomorphisms, sub- and quotient objects, products, etc.

Our course focuses on the most fundamental algebraic structure among those listed: groups. Below, we will discuss groups from two related points of view. This serves both as a bit of a review, as well as an overview of the structure of this course.

1.1 Groups by axiomatic definition

Definition 1.4. A **group** is a set G together with a **law of composition** $\circ$ that has the following properties:

- $\circ$ is associative: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$
- G contains an identity element $1 = 1_G$ such that $1 \circ a = a$ and $a \circ 1 = a$ for all $a \in G$.
- Every element $a \in G$ has an **inverse**, i.e. an element b such that $a \circ b = 1 = b \circ a$.

Other terms for *law of composition* include **group law**, **multiplication in the group**, **composition rule**, **group operation**, etc.

Exercise 1.5. (a) What happens if we drop the requirement that $a \circ 1 = a$ and just assume that $1 \circ a = a$?

(b) What happens if we drop the requirement that $b \circ a = 1$ and just assume that $a \circ b = 1$?

Remark 1.6. Note that commutativity of $\circ$ is not required in the definition of a group. A group where $\circ$ is indeed commutative, i.e. $a \circ b = b \circ a$ for all $a, b \in G$ is called a **commutative** or **abelian** (or **Abelian**) group.

To describe a group, we have to provide both the *underlying set* G and the composition rule $\circ$. So, we might write something like $(G, \circ)$ to be super clear, but just write G if it's clear what group we're talking about.

Also, we don't need to use the symbol $\circ$.

Exercise 1.7. Which of the following are groups? Why or why not?

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{Z}, -)$

(d) $(\mathbb{Z}, \cdot)$

(e) $(\mathbb{R}, +)$

(f) $(\mathbb{R}, \cdot)$

(g) $(\mathbb{R} - \{0\}, \cdot)$

(h) $(\mathbb{C}, +)$

(i) $(\mathbb{C}, \cdot)$

(j) $(\mathbb{C} - \{0\}, \cdot)$

(k) $(\mathbb{Q}, +)$

(l) $(\mathbb{Q}, \cdot)$

(m) $(\mathbb{Q} - \{0\}, \cdot)$

After doing this exercise, you might realize that $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are all very similar. This is because they are all **fields**, which are another type of algebraic structure that we will discuss in this course.

Example 1.8. Let $M_{2\times 2}\mathbb{R}$ denote the set of 2×2 matrices with real entries. This is a group under addition, but is *not* a group under matrix multiplication, because some matrices are not invertible (e.g. the zero matrix).

Example 1.9. The **general linear group** of 2×2 matrices is

$$GL_2(\mathbb{R}) = \{A \in M_{2\times 2}(\mathbb{R}) \mid \det A \neq 0\}.$$

By definition[2], everything in $GL_2(\mathbb{R})$ has a multiplicative inverse. Matrix multiplication is indeed associative. We write either I or I_2 for the identity matrix.

[2]review determinants if this isn't clear!