Abstract Algebra Lecture Notes

Simon Xiang

Lecture notes for the Fall 2021 graduate section of Abstract Algebra (Math 380C) at UT Austin, taught by Dr. Raskin. These notes were taken live in class (and so they may contain many errors). Source files: https://git.simonxiang.xyz/math_notes/files.html

Contents

1 August 25, 2021

Welcome to the first day of class! This is how Dr. Raskin thinks about algebra– in some way abstract algebra is a set of organizational tools that teaches you how to break up a question or pose a question, or reduce it to a simpler case. There was a tradition to classify all sorts of finite algebraic structures, eg finite dim Lie algebras or Lie rings or some binary operation, etc. Studying geometry or showing there are no solutions are more interesting aspects of algebra.

We'll start with finite group theory, then move on to ring theory. We'll follow *Dummit and Foote*, as well as lecture notes from Gaitsgory's Math 122 taught at Harvard. The formalism of group theory is somewhat abstract, because it's an organizational tool. What is group theory? In life, there are various ways of symmetry, eg reflections ($\mathbb{Z}/2$ symmetry, where actions of $\mathbb{Z}/2$ preserve the structure). Another $\mathbb{Z}/2$ symmetry is rotations, and so these two different types of symmetry are the "same". Group theory abstracts this idea of G symmetries by realizing $\mathbb{Z}/2$ as a group.

1.1 Group theory

Definition 1.1. A **group** G consists of a set G and a map $m\colon G \times G \to G$, $(g,h) \mapsto g \cdot h$ (multiplication) such that

(a) the multiplication is associative, eg for all g_1, g_2, g_3, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$,

(b) there exists some $1 \in G$ such that $1 \cdot g = g \cdot 1 = g$ for all $g \in G$,

(c) for all $g \in G$ there exists some $g^{-1} \in G$ such that

We say that 1 is the identity and g^{-1} is the inverse for g.

Lemma 1.1. *Identity elements are unique.*

Proof. Suppose $1, \widetilde{1} \in G$ are both identity elements. Then

$$\widetilde{1} = 1 \cdot \widetilde{1} = 1. \qquad \boxtimes$$

Lemma 1.2. *Inverses are unique.*

Proof. Suppose $g \in G$ with inverses g^{-1} and $\widetilde{g^{-1}}$. Then

$$g^{-1} = g^{-1} \cdot 1 = g^{-1} \cdot (g \cdot \widetilde{g^{-1}}) = (g^{-1} \cdot g) \cdot \widetilde{g^{-1}} = 1 \cdot \widetilde{g^{-1}} = \widetilde{g^{-1}}. \qquad \boxtimes$$

Example 1.1. Here are some examples of groups.

- Suppose $\mathbb{R}^\times \subseteq \mathbb{R}$ is the set of non-zero real numbers. Then $(\mathbb{R}^\times, \cdot)$ is a group. Some variants include $(\mathbb{R}^{>0}, \cdot)$, $(\{-1, 1\}, \cdot)$, and $(\mathbb{Q}^\times, \cdot)$ which are all groups.

- $(\mathbb{R}, \cdot)$ is not a group because 0 has no inverse. However, $(\mathbb{R}, +)$ is a group with unit 0, and the inverse of some $x \in \mathbb{R}$ is $-x$. Sometimes we write groups additively where it makes more sense.

- The **symmetric group on n letters**, denoted S_n, is the set of maps

$$S_n = \{\sigma \colon \{1, \cdots, n\} \xrightarrow{\cong} \{1, \cdots, n\}\}$$

  where multiplication is just composition and the identity element is the identity morphism. Since each σ is a bijection, we have a unique inverse map σ^{-1} which is the multiplicative inverse for σ.

  You can think of groups as subgroups of S_n (leading to Cayley's theorem), for example a reflection is a shuffling of infinitely many points in $\mathbb{R}^2$ around some axis.

2 August 27, 2021