Notes on *Math H113: Abstract Algebra* lectures by Professor Edward Frenkel, Spring 2021

Jay Monga

January 28, 2021

Contents

1 Introduction **2**
- 1.1 First Look at Sets . . . 2
- 1.2 Groups . . . 2
  - 1.2.1 Galois Group . . . 2
  - 1.2.2 Braid Group . . . 3
- 1.3 Algebra vs Analysis . . . 3
- 1.4 Paradoxes . . . 3

2 Set Theory **4**
- 2.1 Recap . . . 4
- 2.2 Sets Continued . . . 4
  - 2.2.1 Functions . . . 4
- 2.3 Cardinality . . . 5

3 Groups **6**
- 3.1 Binary Operations . . . 6

4 Groups cont. **8**
- 4.1 Complex Numbers . . . 8
- 4.2 Formalized Groups . . . 8
  - 4.2.1 Important Results . . . 8

Lecture 1

Introduction

Welcome to Math H113: Honors Abstract Algebra! As opposed to Math 113: Abstract Algbra, H113 will proceed at a faster pace and cover more material. As a result, some material like the details of a proof or definition will be covered just enough to pique our curiousity but rich coverage left aside for independent study. In these notes, I will try to fill in some gaps of the coverage, and we'll see how this goes.

1.1 First Look at Sets

We start by providing a definition of algebra, the focus of this class.

Definition 1.1.1. Algebra is the study of sets with operations satisfying certain axioms.

But what even is a set? We can think of a set as just a colection of items. The idea seems simple enough, but leaving it this simple can cause us problems later down the road, as we will see. For now, we will leave it as that. We can see how the set is one of the basic building blocks of mathematics, and we can start to explore some interesting behavior that comes from defining special structure and operations on elements of a set. This leads to our discussion of groups.

1.2 Groups

Groups are the fundamental set in this class.

Definition 1.2.1. A **group** is the set of symmetries for a given object.

Consider a circle. We can define a group for this object by the set of all rotations of that circle by an angle modulo 2 π. Notice that applying two rotations is the same as applying the composition of the rotations, the 0 degree rotation composes with a rotation to produce the same rotation, and every rotation has an inverse rotation that will reset it to the 0 degree rotation. These three properties are what makes the set of all 2D rotations $SO(2)$ a group.
Let's now formalize our definition of a group

Definition 1.2.2. A **group** is the set G with an operation satisfying axioms of

1. $\forall x, yz \in G, x \cdot (y \cdot g) = (x \cdot y) \cdot g$ (Associativity)
2. $\exists e \in G$ s.t. $e \cdot g = g \cdot e = g, \forall g \in G$ (Identity element)
3. $\forall g \in G, \exists g'$ s.t. $g \cdot g' = g' \cdot g = e$ (Inverse element)

Now we can go through some examples! We already introduced $SO(2)$, which Prof. Frenkel brings up in the beginning of *Love and Math*, but there are other cool examples as well.

1.2.1 Galois Group

First, let's introduce the concept of a field.

Definition 1.2.3. A **field** is a set defined with two binary addition and multiplication operations that satisfy a set of axioms.

Figure 1.1: Insert circle diagram here

We will go more in detail later; these axioms are similar to the axioms of a vector space. Common fields include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
The Galois group can be seen as extending a field into a set of symmetries.
The Galois group is named after its discoverer Évariste Galois who tragically died in a duel at a young age. One interesting application of his work was for determining existence of solutions in terms of a radical for polynomials with degree greater than or equal to 5. This problem was significantly studied by the great mathematician Muhammad ibn Mūsā al-Khwārizmī 1000 years before Galois's time.
The word algorithm is derived from al-Khwārizmī and algebra, the topic of this class, comes from a book he wrote called al-jabr.

1.2.2 Braid Group

1.3 Algebra vs Analysis

1.4 Paradoxes

Lecture 2

Set Theory

2.1 Recap

Last lecture, we talked about

- Notion of a set
- Russel Paradox ($R = \{x | x \notin x\}$)
- ZFC axioms to solve carelessness in definition of a set that lead to logical inconsistencies like Russel Paradox
- It's hard to precisely define a set is, so to some extent we have to take some faith in that we understand them to be some agreeable object

As always, use Wikipedia or nLab to look up things you are interested in.

2.2 Sets Continued

As before, we look at sets as a collection of objects. Let's look at types of sets

- empty set: this is a unique set with no items denoted by $\emptyset$
- finite sets: sets with a finitely many elements
- functions: a specific type of relation between two sets, but can be seen as a set itself
- subset: a set that is a collection of some elements of another set (the integers are a subset of the real numbers)

Definition 2.2.1. Suppose A and B are two sets. A **function** $f : A \to B$ is a rule that assigns to every every element $a \in A$ an element (one and only one) of B, denoted $f(a)$

Definition 2.2.2. A function $f : A \to B$ has **domain** A and **codomain** B

2.2.1 Functions

Functions are pretty important to us, so we will dive deeper into them.

Example 2.2.1. In single-variable calculus, we consider functions $f : \mathbb{R} \to \mathbb{R}$

Example 2.2.2. Consider $A = \{a, b, c\}, B = \{x, y, z, w\}, f : A \to B$

- A valid f would be
  - $f(a) = x$
  - $f(b) = y$
  - $f(c) = z$
- An invalid f would
  1. $f(a) = x$
  2. $f(b) = y$
  3. $f(c) = z$
  4. $f(c) = w$

  since we see that c is getting mapped to two different elements z, w.

Function properties to be familiar with

- injective, or one-to-one
- surjective, or onto
- bijective, one-to-one and onto
- uniquness of inverse (prove through some algebra looking at $g' \circ f \circ g$)

Remember to read function composition from right to left, ie applying f first and then g is written as $g \circ f$.

2.3 Cardinality

With a notion of functions and their properties, we can start talking about set sizes.

Definition 2.3.1. A set A is **finite** if there exists a bijection with

Lecture 3

Groups

3.1 Binary Operations

Definition 3.1.1. A **binary operation** on a set S is a function

$$f : S \times S \to S$$

We will denote $f(a, b)$ as $a * b$ when it is clear what f is, or we are talking about some general f.

Definition 3.1.2. $*$ is called **commutative** if $\forall a, b \in S, a * b = b * a$

Definition 3.1.3. $*$ is called **associative** if

$$(a * b) * c = a * (b * c)$$

Remark 3.1.1. *If $*$ is associative, then $*$ defines an n-ary operation (function on n ordered arguments).*

Binary operations in general are not commutative or associative, but we can see that they give rise to interesting structure if they do hold.

Example 3.1.1. Consider the binary operation of $+$ on $\mathbb{N}$. We can trivially see that

- $+$ is commutative
- $+$ is associative

Example 3.1.2. Again consider $+$, but on $\mathbb{Z}^+$. We notice that the element 0 has a special property

$$\forall a \in \mathbb{Z}^+, a + 0 = 0 + a = a$$

Definition 3.1.4. An element e of a set S with a defined binary operation $*$ is called the **identity element** of S if

$$\forall a \in S, a * e = e * a = a$$

Lemma 3.1.1. *For binary structure $(S, *)$, an identity element in S, if it exists, must be unique.*

Proof. Uniquness proofs often follow the structure of assuming two seperate entities exist, and then proving that they must be the same entity. In this case, we assume we have two elements e, e' that satisfy the definition of identity element on binary structure $(S, *)$.

Let's consider the value of $e * e$. using the identity property of e, we have

$$e * e' = e'$$

But using the identity property of e', we must have

$$e * e' = e$$

These two equalities give us $e = e'$.

We can put this proof in one cute line as well

$$e' = e * e' = e$$

But be sure to explain your steps! □ □

Example 3.1.3. Consider the set of counterclockwise rotations by some angle φ. We define $+$ on this set as

$$x + y \mod 2\pi$$

Example 3.1.4. On $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ consider the $+$ operation with a special rule: for $C \in \mathbb{R}^+$, $x + y$ will take on the value of its remainder when divided by C. This is called addition modulo C. We can say $x \equiv y \mod C$ if $\exists n \in \mathbb{Z}$ s.t. $x = y + nC$

With our equivalence class established, we can say that

$$\tilde{x} \sim x', \tilde{y} \sim y' \implies \tilde{x} * \tilde{y} \sim x' + y'$$

Example 3.1.5. Consider the set of rotations of a sphere (known as $SO(3)$). We can consider each element of this set as a point on the sphere. In general, the operation of composing two rotations will not be commutative, but associative. This binary operation will also have an identity element.

Example 3.1.6. We will show that complex numbers give us an alternate, but equivalent, description of the symmetries of a circle. Recall the standard definitions of addition and multiplication for complex numbers.

Remark 3.1.2. $\mathbb{N}, \mathbb{Z}^+, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *have 2 natural operations:* $+$ *and* $\cdot$

Lecture 4

Groups cont.

4.1 Complex Numbers

- Complex numbers are commutative group under multiplication and addition
  - This property is sort of unique to groups isomorphic to $\mathbb{R}^2$
- When restricted to unit circle, group of complex numbers under multiplication isomorphic to residue classes of $\mathbb{Z}$ modulo 2π
  - Eulers formula
    - Algebra vs analysis discussion
    - Taylor series derivation
    - Another proof I missed I think

4.2 Formalized Groups

Definition 4.2.1. A **group** is a set S with an associative binary operation $*$ such that

(Closed under $*$) $* : S \times S \to S$

(Identity element) $\exists e \in S$ s.t. $\forall x \in S$, $e * x = x * e = x$

(Inverse element) $\forall x \in S$, $\exists x' \in S$ s.t. $x * x' = x' * x = e$

Example 4.2.1. Consider $M_{n\times n}$, the set of all $n \times n$ matrices with entires in $\mathbb{R}$. Is this a group under the binary operation of matrix multiplication?

- Axiom 1 holds since an $n \times n$ matrix times an $n \times n$ matrix

However, consider

$$GL_n\{\mathbb{R}\} = \{A \in M_{n\times n}(\mathbb{R}) \mid \det A \neq 0\}$$

which is the set of all invertible $n \times n$ matrices. This set will form a group.

It's now time to define the notion of a subgroup

Definition 4.2.2. A **subgroup** of a group G is a subset of G that also forms a group

Remark 4.2.1. *It's not enough for a subset of G to be closed under $*$ to be considered a subgroup, we need to check the other properties too. Conside $\mathbb{Z}^+$*

Definition 4.2.3. A **homomorphism** $h : G^{*G} \to H^{*H}$ is a function between two sets such that

$$h(g_1 *_G g_2) - h(g_1) *_H h(g_2)$$

Example 4.2.2. We just talked about a homomorphism from $G = SL_2(\mathbb{R})$ to H_+ (upper half plane of complex numbers)

4.2.1 Important Results

Assume we have some group structure $(G, *)$

Theorem 4.2.1.

$$a * b = a * c \implies b = c$$

Proof. We are guarenteed to have an inverse for a □

Theorem 4.2.2. *The equation*

$$a * x = b$$

has a unique solution

$$x = a' * b$$

Proof. □