9.3.2025: Math 122 Lecture 1 Notes

Vasily Krylov

1 Motivating Groups with Numbers

We will spend the first half of the course studying *groups*, which are fundamental objects in math.

To ground the definition of a group, we begin with numbers: the *natural numbers* are the set of counting numbers

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

If we *add* any two natural numbers, we get another natural number, but we note that we *cannot* always subtract natural numbers to get another natural number. For example,

$$3 - 5 = -2 \notin \mathbb{N}.$$

So, we can extend natural numbers and consider the *integers*

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Unlike natural numbers, we can *add* and *subtract* integers to get another integer, but, in general, we cannot divide (i.e. $\frac{2}{3} \notin \mathbb{Z}$).

This can be extended even further, to the set of *rational numbers*

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \right\}.$$

This set is closed under addition, subtraction, multiplication and division.

However, in many situations in math, we want the “numbers" that we are dealing with to be “continuous." For example, if we take the number $\sqrt{2}$, we note that $\sqrt{2}$ is not a rational number (cannot be written as the ratio of two integers), but can be written as the limit of rational numbers, by taking the decimal representation $\sqrt{2} = 1.4142135\dots$ and truncating.

So, we can extend rational numbers to the set of *real numbers* $\mathbb{R}$, which can be viewed as the "limits" of rational numbers.

Finally, it is oftentimes very useful to extend the real numbers to the set of *complex numbers* $\mathbb{C}$ by adding the $i = \sqrt{-1}$.

One reason that we wish to extend the real numbers to the set of complex numbers is the Fundamental Theorem of Algebra, which states:

Fundamental Theorem of Algebra: Every non-zero degree n polynomial $p(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$ with complex coefficients $a_i \in \mathbb{C}$ has exactly n *complex* roots (counted with multiplicity) $b_1, \dots, b_n \in \mathbb{C}$, where we can rewrite our polynomial as

$$p(t) = (t - b_1) \dots (t - b_n).$$

Notably, this theorem does *not* hold over $\mathbb{R}$. For example, the polynomial $p(t) = t^2 + 1$ does not have real roots.

So, we have the different number systems

$$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}.$$

What do all of these have in common?

- For all numbers x, y, we can form $x + y$ also in that number system

The properties of this operation can be axiomatized to the notion of a *group.*

2 Defining Groups

Definition (group). A *group* is a set S together with a map $m : S \times S \to S$ that is called a "law of composition" (where we will write ab for $m(a, b)$) that satisfies *three* axioms:

1. *(identity)* There exists an element $e \in S$, called the *identity* such that $ae = ea = a$ for all $a \in S$.
2. *(inverse)* For any $a \in S$, there exists an *inverse* element $b \in S$ such that $ab = ba = e$.
3. *(associative law)* For all $a, b, c \in S$, we have

$$a(bc) = (ab)c.$$

If (S, m) only satisfies properties (1) and (3), then we call S a *monoid.* If $*(S, m)$ only satisfies (3), then we call it a *semigroup.*

Note: it took lots of time and thinking for people to get to these axioms!

2.1 Examples of Groups

- Note that $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all groups, where the law of composition m is defined such that $m(a, b) = a + b$, the identity is the element 0 and the inverse to a is $-a$.
- $\mathbb{N}$ is *NOT* a group ((2) fails) but $\mathbb{N}$ is a monoid
- Example of a semigroup which is not a monoid:

  $$\mathbb{Z}_{>0} = \{1, 2, 3, \dots, \}$$

  We can add elements, associativity holds, but there is no inverse and no identity.

3 First Properties of Groups

We now prove the following properties of groups using the axioms:

(a) The identity e is *unique*

(b) The inverse element of a is also *unique* (to be denoted a^{-1})

(c) For all $a, b \in S$, we have $(ab)^{-1} = b^{-1}a^{-1}$.

Proof of (a): Suppose that we have identity elements $e, e' \in S$. Then,

$$e = e \cdot e' = e'.$$

□

Proof of (b): Suppose that we have b, b' that are the inverse to a. We have

$$\begin{aligned}(b \cdot a) \cdot b' &= b \cdot (a \cdot b') \text{ by associativity} \\ e \cdot b' &= b \cdot e \\ b' &= b.\end{aligned}$$

□

Proof of (c): To prove (c), we need to check that $(b^{-1}a^{-1})(ab) = e$. Indeed,

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}(ab)) \\ &= b^{-1}((a^{-1}a)b) \\ &= b^{-1}(eb) \\ &= b^{-1}b \\ &= e.\end{aligned}$$

□

Exercise: Show that $(a^{-1})^{-1} = a$.

4 Why is the associativity axiom so important?

Note: When we write an expression like

$$2 + 3 + 1 + 10,$$

we do *not* specify the order in which we sum. So, we are implicitly using that the result does *not* depend on the order in which we sum.

This is a general (very important) fact about semigroups.

Claim: For all $a_1, \ldots, a_n \in S$, the product $a_1 a_2 \ldots a_n$ does *not* depend on the order in which we take it.

For example,

$$(a_1(a_2a_3))a_4 = a_1(a_2(a_3a_4)).$$

More formally...

Proposition: There is a unique way to define, for every $n \in \mathbb{Z}_{>0}$, a product of n elements $a_1, \ldots, a_n \in S$, denoted temporarily as $[a_1 \ldots a_n]$, with the following properties:

(i) $[a_1] = a_1$

(ii) $[a_1 a_2] = a_1 a_2$

(iii) For any $1 \leq i < n$, we have

$$[a_1 \dots a_n] = [a_1 \dots a_i][a_{i+1} \dots a_n].$$

Proof: We induct on n. It is easy to check that this holds for $n \leq 2$. Then, we suppose that the claim holds for products of Γ elements for $\Gamma \leq n-1$. We wish to define the product of n elements. Because this product must satisfy (iii) for $i = n-1$, we must define

$$[a_1 \dots a_n] := [a_1 \dots a_{n-1}][a_n].$$

To show that $[a_1 \dots a_n]$ is unique, it remains to check (iii) for $i < n-1$:

$$\begin{aligned}
[a_1 \dots a_n] &= [a_1 \dots a_{n-1}][a_n] \text{ by definition} \\
&= ([a_1 \dots a_i][a_{i+1} \dots a_{n-1}])\,[a_n] \text{ by the inductive hypothesis} \\
&= [a_1 \dots a_i]\,([a_{i+1} \dots a_{n-1}][a_n]) \text{ by associativity} \\
&= [a_1 \dots a_i][a_{i+1} \dots a_{n-1} a_n] \text{ by induction.}
\end{aligned}$$

□

5 More Examples of Groups

5.1 $\mathbb{Z}/n\mathbb{Z}$

We define $\mathbb{Z}/n\mathbb{Z}$ from $\mathbb{Z}$ as follows: The set

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}.$$

The law of composition

$$m : (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$$

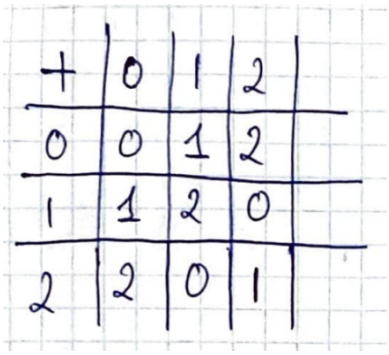
is defined as

$$m(a,b) = \begin{cases} a+b \text{ if } a+b \leq n-1 \\ a+b-n, \quad \text{otherwise,} \end{cases}$$

where $m(a,b)$ yields the remainder of $a+b$ under the division by n.

Exercise: Check that $(\mathbb{Z}/n\mathbb{Z}, m)$ is a *group*.

Example: When $n = 3$, $\mathbb{Z}/3\mathbb{Z} = \{0,1,2\}$ where we can make the table of how elements compose with eachother:



Note that this remains the same if we mirror across the main diagonal! That is, for all a, b, we have $a + b = b + a$.

Groups with this property are called *commutative* (or *abelian*). We will later see examples of non-commutative groups.

5.2 More examples of (commutative) groups

Of the groups we have introduced

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z},$$

we note that some have more structure than just addition $+$: they also have $\cdot$ (product). For example, for any $a, b \in \mathbb{Q}$ (or $\mathbb{Z}, \mathbb{R}, \mathbb{C}$, the product $a \cdot b \in \mathbb{Q}$, meaning that it is well-defined.

Exercise: The product $\cdot$ on $\mathbb{Z}$ defines a product on $\mathbb{Z}/n\mathbb{Z}$ as follows: for any $a, b \in \mathbb{Z}/n\mathbb{Z}$, we define $a \cdot b :=$ remainder of ab under division by n.

Note that

$$(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot), (\mathbb{Z}/n\mathbb{Z}, \cdot)$$

are *monoids*. They have an identity 1, but do not satisfy the inverse property of groups (0 does not have an inverse).

Can we construct groups out of them?

Yes! In general, if S is a monoid, we can consider the group $S^\times = \{a \in S \mid a \text{ invertible}\}$.

How this works in our example:

- $\mathbb{Z}^\times = \{\pm 1\}$, group consisting of two elements.
- $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ is a group under $\cdot$
- $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ is a group under $\cdot$
- $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ is a group under $\cdot$

What is $(\mathbb{Z}/n\mathbb{Z})^\times$?