MATH 113 Notes

Professor: Forte Shinko

Neo Lee

Spring 2024

Contents

Chapter 1

Motivation

1.1 Abstraction

We have two very similar theorems, and turns out they can be generalized into one single property, hence the abstraction. This is the idea of abstraction, and it is the core of modern mathematics.

Theorem 1.1 Prime factorization

Every integer $n > 1$ can be uniquely factorized as a product of primes.

Theorem 1.2 Fundamental theorem of algebra in $\mathbb{R}$

Every polynomial $p(x)$ of degree $n > 0$ with real coefficients can be factorized into a product of linear and quadratic polynomials with real coefficients.

It turns out that these two theorems are very similar, and we can describe them with one single property, namely the unique factorization domain (UFD).

Corollary 1.1 Generalization as UFD

1. $(\mathbb{Z}, +, \cdot)$ is a UFD.
2. $(\mathbb{R}[x], +, \cdot)$ is a UFD.

With abstraction, we can also prove theorems in a more general setting and sometimes apply generalized theorems to specific cases to get an easier proof.

Theorem 1.3 Fermat's little theorem

If p is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

Proof: Apply Lagrange's theorem to the group $(\mathbb{Z}/p\mathbb{Z}, \cdot)$. 😊

Note:

This proof using abstracted theorem is much easier than the original proof in traditional number theory.

Chapter 2

Group Theory

2.1 Lecture 1

Definition 2.1: Binary operation

A binary operation on a set S is a funtion from $S \times S$ to S.

Example 2.1 (Addition on $\mathbb{Z}$)

We can define addition on $\mathbb{Z}$ as a binary operation, since for any $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$.

Wrong Concept 2.1: Non-examples of binary operation

1. Subtraction on $\mathbb{N}$ is not a binary operation. Consider the case $a = 1, b = 2$, then $a - b = -1 \notin \mathbb{N}$.
2. Division on $\mathbb{R}$ is not a binary operation. Division by zero is not defined on $\mathbb{R}$. Hence, division is not a binary operation from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$.

2.2 Lecture 2

Some examples of binary operations:

Example 2.2 (The midpoint operation on $\mathbb{R}^2$)

$$T(\vec{a}, \vec{b}) = \frac{1}{2}(\vec{a} + \vec{b}).$$

Example 2.3 (The set of functions from $\mathbb{R}$ to $\mathbb{R}$)

Some examples are $x^2, \sin x$. The set of functions from $\mathbb{R}$ to $\mathbb{R}$ has a binary operation of composition, taking (f, g) to $f \circ g$.

Note:

For convenience, we typically write composition by $fg = f \circ g$.

Example 2.4 (Cross product)

Cross product is a binary operation on $\mathbb{R}^3$.

Wrong Concept 2.2: Dot product is not a binary operation

Dot product is not a binary operation on $\mathbb{R}^3$, since the result of dot product is a scalar, which is not in $\mathbb{R}^3$. In particular *dot prodcut*: $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$.

Definition 2.2: Matrix of $n \times n$

Denote $\mathcal{M}_n(\mathbb{F})$ to be the set of $n \times n$ matrices over $\mathbb{F}$.

Example 2.5 ($\mathcal{M}_n(\mathbb{F})$ has two common binary operations)

Namely addition and multiplication on matrices.

Example 2.6 (Power set of $\mathbb{R}$)

The power set of $\mathbb{R}$ has union and intersection as binary operations.

Note:

$\{1, 2, 3\} \cup \{\pi, e\} = \{1, 2, 3, \pi, e\}$ is in the power set of $\mathbb{R}$.

Definition 2.3: Monus operation

Consider the monus operation defined by $(x, y) \mapsto \max(x - y, 0)$.

Definition 2.4: Multiplication table (aka Cayley table)

Try to do the Cayley table on the set $\{0, 1, 2, 3\}$ with the monus operation.

Note:

You can also define a binary opeartion by simply listing out the Cayley table. Hence, a binary operation on $\{0, 1, 2, 3\}$ is just any way to fill the 4×4 grid. So binary operation is actually not that unique.

Note:

In this class, we typically talk about sets equipped with binary operations. For example, we talk abou the set $\mathbb{Z}$ equipped with addition $(\mathbb{Z}, +)$ or even with multiplication as well $(\mathbb{Z}, +, \cdot)$.

Definition 2.5: Monoid

A monoid is a set M equipped with a binary operation $\cdot$ such that

1. **Associativity:** $\cdot$ is associative, i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in M$.
2. **Existence of identity:** There exists an identity element $e \in M$ such that $e \cdot a = a \cdot e = a$ for all $a \in M$.

Definition 2.6: Group

A group is a set G equipped with a binary operation $\cdot$ such that

1. **Associativity:** $\cdot$ is associative, i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
2. **Existence of identity:** There exists an identity element $e \in G$ such that $e \cdot a = a \cdot e = a$ for all $a \in G$.
3. **Existence of inverse:** For every $a \in G$, there exists an inverse $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Note:

- We typically denote a group by $(G, \cdot)$, but sometimes we omit the binary operation $\cdot$ if it is clear from the context.
- Group is an extension of monoid, since every group is a monoid, but not every monoid is a group.

2.3 Lecture 3

Example 2.7 ($(\mathcal{M}_n(\mathbb{R}), \cdot)$ is a monoid but not group)

Matrix multiplication is associative, and the identity matrix I_n is the identity element. However, not every matrix has an inverse (is invertible).

Example 2.8 (S^S is a monoid)

Let S be a set. Then S^S is the set of all functions from S to S. The binary operation is composition, i.e. $(f, g) \mapsto f \circ g$. The identity element is the identity function id_S. Obviously, composition is associative. However, depending on the set S not all functions necessarily have an inverse.

Proposition 2.1 Unique identity

A binary operation can have at most one identity element.

Proof: Suppose e_1 and e_2 are both identity elements. Then $e_1 = e_1 \cdot e_2 = e_2$. 😄

Definition 2.7: Identity

Since we have shown that identity is unique, it make sense to denote the identity element of a group G by e_G or simply e if it is clear from the context.

Definition 2.8: Power of zero is identity

For any $a \in G$, we define $a^0 = e$.

Example 2.9 ($(\mathbb{Z}, \cdot)$ is not a group)

The only invertible elements are ± 1.

Example 2.10 (Integer mod n)

Let $n \in \mathbb{Z}^+$, define the set of integers mod n by $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$. $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group but $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is not a group because consider $0 \in \mathbb{Z}/n\mathbb{Z}$, then $0 \cdot a = 0$ for all $a \in \mathbb{Z}/n\mathbb{Z}$, so 0 does not have an inverse.

2.4 Lecture 4

Definition 2.9: Unit group of monoid M

Let M be a monoid, then denote $M^\times$ to be the unit group (group of units) of M, where it is the set of all invertible elements of M, which is a group under the binary operation of M.

Note:

We call the invertible element of a monoid the unit element.

Note:

We infer the group $\mathbb{Q}^\times$ as $(\mathbb{Q}, \cdot)^\times$ instead of $(Q, +)^\times$ because $(\mathbb{Q}, +)$ is automatically a group, which we denote as the group $\mathbb{Q}$anyways.

Proposition 2.2 Unique inverse

Let M be a monoid, and a, b be inversitible. Then ab is invertible and $(ab)^{-1} = b^{-1}a^{-1}$.

Example 2.11 (Integer matrix)

Consider the monoid $(\mathcal{M}_n(\mathbb{Z}), \cdot)$. Then the unit group is $(\mathcal{M}_n(\mathbb{Z}), \cdot)^\times$, which we denote as $\mathrm{GL}_n(\mathbb{Z})$, called the general linear group of degree n over $\mathbb{Z}$. In other words, it's all the invertible $n \times n$ matrices with integer entries.

Note:

A matrix $A \in \mathcal{M}_n(\mathbb{Z})$ is invertible if and only if $\det A \in \mathbb{Z}$ is invertible as an element of the monoid $(\mathbb{Z}, \cdot)$, i.e. $\det A = \pm 1$.

Definition 2.10: Symmetric group

Let X be a set and consider the monoid $(X^X, \circ)$, the set of all functions from $X \to X$ under composition. Then the unit group $(X^X, \circ)^\times$ is called the symmetric group on X and is denoted by $\mathrm{Sym}(X)$ or S_X.

Note:

In other words, the symmetric group on X is the set of all bijections from X to X.

Example 2.12 ($\mathrm{Sym}(\mathbb{R})$)

Define the function $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 2x + 1$. Then $f \in \mathrm{Sym}(\mathbb{R})$.

Proof: From elementary algebra, we know that f is bijective. In particular

$$f^{-1} = g : x \mapsto \frac{x-1}{2}.$$

It is easy to see that $g \circ f = f \circ g = e$. ☺

Chapter 3

Starting a new chapter

3.1 Demo of commands

Definition 3.1: Some defintion

yap

Question 1: Some question

yap

Solution

Some proof: yap 😄

Note:

Some note

Theorem 3.1 Some theorem

yap

Wrong Concept 3.1: Some wrong concept

yap

Lemma 3.1 Some lemma

yap

Proposition 3.1 Some proposition

yap

Example 3.1 (Some example)

yap

Claim 3.1 Some claim

yap

Corollary 3.1 Some corollary

yap

Some unlabeled theorem

This is a new paragraph

Algorithm 1: Some algorithm

Input: input
Output: output
`/* This is a comment */`

```
1  This is first line ;                                  // This is also a comment
2  if x > 5 then
3  |  do nothing
4  else if x < 5 then
5  |  do nothing
6  else
7  |  do nothing
8  end
9  while x == 5 do
10 |  still do nothing
11 end
12 foreach x = 1 : 5 do
13 |  do nothing
14 end
15 return return nothing
```