MAT157 Lecture 5 Notes

Anatoly Zavyalov

September 21, 2020

1 Back to field axioms

Looking at axioms P1-P9, the claim is that there is a **unique** field with two elements.

Let $F = \{0, 1\}$. Every field must have at least two elements, one that plays the role of $\mathbf{0}$, and one that plays the role of $\mathbf{1}$, and $\mathbf{0} \neq \mathbf{1}$.

We can use axioms to determine some values for addition and multiplication between the two elements in the field:

+	0	1
0	**0**	**1**
1	**1**	**0**

·	0	1
0	**0**	**0**
1	**0**	**1**

To find the value of $\mathbf{1} + \mathbf{1}$, we use axiom P3, which states that $\mathbf{1}$ must have an additive inverse **-1**.

We cannot have $\textbf{-1} = \mathbf{0}$, as that would give

$$\mathbf{1} = \mathbf{1} + \mathbf{0} = \mathbf{1} + (\textbf{-1}) = \mathbf{0}$$

This is a contradiction, meaning that $\textbf{-1} = \mathbf{1}$, which gives

$$\mathbf{1} + \mathbf{1} = \mathbf{1} + (\textbf{-1}) = 0.$$

The value of $\mathbf{0} \cdot \mathbf{0}$ cannot be $\mathbf{1}$, as that would give

$$\begin{aligned}
\mathbf{1} = \mathbf{0} \cdot \mathbf{0} &= \mathbf{0} \cdot (\mathbf{0} + \mathbf{0}) && \text{By P2} \\
&= \mathbf{0} \cdot \mathbf{0} + \mathbf{0} \cdot \mathbf{0} && \text{By P9} \\
&= \mathbf{1} + \mathbf{1} && \text{Since } \mathbf{0} \cdot \mathbf{0} = \mathbf{1} \\
&= \mathbf{0}
\end{aligned}$$

We also find that there is a unique field with 3 elements, such as $\{0, 1, \mathbf{x}\}$, with the following definitions for addition and multiplication:

+	0	1	x
0	**0**	**1**	**x**
1	**1**	**x**	**0**
x	**x**	**0**	**1**

·	0	1	x
0	**0**	**0**	**0**
1	**0**	**1**	**x**
x	**0**	**x**	**1**

There is also a unique field with 4 elements:

+	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

·	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

There is also a unique field with 5, 7, 8, 9, 11, 13 elements.

There is **no** field with 6, 10, 12 elements!

Fact

Given $q \in \mathbb{N}$, there exists a field F with q elements if and only if $q = p^m$ for some prime number p, and $m \in N$.

Furthermore, this field is **unique** (up to renaming of variables).

This field is denoted by F_q.

So there is

$$F_2, F_3, F_4, F_5, F_7, F_8, F_9, F_{11}, F_{13}...$$

2 Integers mod k

Let $\mathbb{Z}_k$ be a set of "symbols" $[a]_k$ where $a \in \mathbb{Z}$, with the convention that $[a]_k = [a']_k$ if a and a' differ by a multiple of k.

An other notation is $[a]_k = a \bmod k$.

Addition: $[a]_k + [b]_k = [a+b]_k$.

Multiplication: $[a]_k + [b] + k = [a \cdot b]_k$.

Fact: $\mathbb{Z}_k$ is a field if and only if $k = p$, where p is a prime number. For example, $\mathbb{Z}_4$ is **not** a field.

Thus $F_p = \mathbb{Z}_p$ for a prime p.

2.1 Example

$$[4]_5 \cdot [2]_5 = [4 \cdot 2]_5 = [8]_5 = [3]_5.$$

This can be written as

$$(4 \bmod 5) \cdot (2 \bmod 5) = 8 \bmod 5 = 3 \bmod 5.$$

2.1.1 Another fun example

What's the last digit of $1023 \cdot 577$? You obviously don't multiply it out, you just want to find

$$[1023 \cdot 577]_{10} = [1023]_{10} \cdot [577]_{10} = [3]_{10} \cdot [7]_{10} = [21]_{10} = [1]_{10}.$$

2.2 Example of an infinite field

$\mathbb{Q} = \{\frac{p}{q} | p \in \mathbb{Z}, q \in \mathbb{N}\}$ is a field. However, $\mathbb{N}, \mathbb{Z}$ are not.

2.3 Another example

$\mathbb{R}$ is a field. Suppose that $S \subseteq \mathbb{R}$ subset, closed under addition and multiplication, i.e.

$$a, b \in S \implies a + b \in S,$$
$$a, b \in S \implies a \cdot b \in S$$

Is S itself a field? The answer is **yes**, if it has properties:

- $\mathbf{0} \in S$
- $\mathbf{0} \in S$
- $a \in S, \implies -a \in S$
- $a \in S, a \neq 0 \implies a^{-1} \in S$