MATH 3311, FALL 2025: LECTURE 39, DECEMBER 5

Video: `https://youtu.be/4SjN0MJaywA`

<u>Fields</u>

We now move on to a new topic, which we will briefly touch on this semester. We will return to it in much greater detail starting next semester.

Example 1. Consider $\mathbb{Z}/p\mathbb{Z}$: this is an additive abelian group, but it is also equipped with a multiplication operation such that $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})\backslash\{0\}$ is a *group* under multiplication. This means that one can do linear algebra as one is used to: Row reduction works because we can always 'divide' by non-zero entries.

Let us abstract the properties used for doing linear algebra in the following definition:

Definition 1. A **field** is a 5-tuple $(k, +, 0, \cdot, 1)$ where:

- $(k, +, 0)$ is an additive abelian group;
- $\cdot : k \times k \xrightarrow{(x,y)\mapsto x\cdot y} k$ is a binary operation;
- $1 \in k\backslash\{0\}$ is a non-zero element.

This data is required to satisfy the following properties:

(1) (Commutativity for $\cdot$) For all $x, y \in k$, we have $x \cdot y = y \cdot x$;
(2) (Associativity for $\cdot$) For all $x, y, z \in k$, we have $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
(3) (Identiy for $\cdot$) For all $x \in k$, we have $1 \cdot x = x \cdot 1 = x$;
(4) (Distributivity) For all $x, y, z \in k$, we have

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

(5) (Inverses for $\cdot$) If $x \in k^\times = k\backslash\{0\}$, then there exists $x^{-1} \in k$ such that $xx^{-1} = 1$.

Remark 1. The conditions (1), (2), (3) and (5) together imply that $(k^\times, \cdot, 1)$ is an *abelian* group.

Remark 2. If we drop condition (5), then what we have is called a **commutative ring**. An example of a tuple with this property is $(\mathbb{Z}, +, 0, \cdot, 1)$: Only $\pm 1 \in \mathbb{Z}\backslash\{0\}$ are invertible for $\cdot$.

Example 2. $(\mathbb{Q}, +, 0, \cdot, 1)$ is a field. As are $(\mathbb{R}, +, 0, \cdot, 1)$ and $(\mathbb{C}, +, 0, \cdot, 1)$.

Example 3. Example 1 shows that $(\mathbb{Z}/p\mathbb{Z}, +, 0, \cdot, 1)$ is a field when p is prime. We will denote his field by $\mathbb{F}_p$: the finite field with p elements.

Example 4 (Non-example). If n is not a prime, then $(\mathbb{Z}/n\mathbb{Z}, +, 0, \cdot, 1)$ is *not* a field, because the non-zero elements that are not prime to n are not invertible. This is however an example of a commutative ring.

Fact 1. If k is a field and $x \in k$, then $0 \cdot x = 0 = x \cdot 0$.

Proof. $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$.
Canceling $0 \cdot x$ from both sides now gives us the result. □

Fact 2. For $x \in k$, we have $(-1) \cdot x = -x$.

Proof. $x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1 + (-1)) \cdot x = 0 \cdot x = 0$.
This shows that x and $(-1) \cdot x$ are additive inverses. □

Remark 3. Remember that the element 1 is *not* literally the *number* 1. It is only the identity element for the $\cdot$ operation. Similarly, -1 is not literally negative one, but rather the additive inverse to the multiplicative identity. The above facts show that these abstract notions have familiar behaviors.

Observation 1. If $x, y \in k^\times$ are non-zero elements then $x \cdot y \neq 0$

Proof. This is because $k^\times$ is closed under multiplication. □

Example 5 (Non-example). If k_1 and k_2 are fields, then the direct product $k_1 \times k_2$ can be equipped with coordinatewise addition and multiplication. However, we have $(1,0)\cdot(0,1) = (1\cdot 0, 0\cdot 1) = (0,0)$. This shows that $k_1 \times k_2$ cannot be a field.

So how can we construct new fields if we direct products won't do? Before we try to answer this, let us look at the following nice example.

Example 6 (Fields of order 4). Suppose that k is a field of order 4. Write $1_k, 0_k$ for the multiplicative and additive identity elements. Then every element of the additive group k is killed by 4. In particular $4 \cdot 1_k = 0$[1]. But we can write this as

$$0 = (1_k + 1_k + 1_k + 1_k) = (1_k + 1_k)(1_k + 1_k) = (2 \cdot 1_k)(2 \cdot 1_k)$$

By Observation 1, this means that $2 \cdot 1_k = 0$. Now, for any element $x \in k$, we have

$$2 \cdot x = x + x = 1_k \cdot x + 1_k \cdot x = (1_k + 1_k) \cdot x = 0 \cdot x = 0.$$

Therefore, every element of k is killed by 2. That is, we have $x = -x$.

Now, let us write the elemnts of k as $\{0_k, 1_k, x, y\}$. Let us consider the element $x + 1_k$: A little thought shows that this has to be equal to y. Similarly, the element x^2 also has to be y. This shows that we have

$$x + 1 = x^2 \Leftrightarrow x^2 - x - 1 = 0 \Leftrightarrow x^2 + x + 1 = 0.$$

The last equivalence is because $a = -a$ for all $a \in k$.

[1]Here, 2 is not an element of the field, but is the actual integer. This is the usual scaling by integers in an additive abelian group.