Lecture 14: More on Fields

Lecture: Sujata Ghosh *Scribe: Shramana Dey*

1 Topics for this lecture

In this lecture, we shall talk about the following

1. Homomorphism from $\mathbb{Z}$ to some Ring
2. Characteristics of a Field
3. Size of Finite Field
4. Integral Domain

2 Homomorphism from $\mathbb{Z}$ to a Ring (R)

Let's discuss about homomorphisms from $\mathbb{Z}$ to some Ring R.
Consider a homomorphism $f : \mathbb{Z} \to R$.
What is $Ker\ f$?
-Suppose, $R = 0_R$ then $Ker\ f = \mathbb{Z}$.
-Suppose, $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ then $Ker\ f = 0$. [*Note:* The Homomorphism preserves the additive and multiplicative identity. A homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ will take 1 to 1. In general, a homomorphism from $\mathbb{Z}$ to R will take 1 to 1_R.]
-Suppose, $R = \mathbb{Z}/n\mathbb{Z}$ then $Ker\ f = n\mathbb{Z}$.

2.1 What happens to $Ker\ f$ if R is a field?

Proposition 2.1 *If R is a field and $f : \mathbb{Z} \to R$ is a homomorphism, then $Ker\ f$ is either 0 or $p\mathbb{Z}$ for some prime p.*

Proof. Suppose, $Ker\ f \neq 0$. Now, $Ker\ f$ is an ideal of $\mathbb{Z}$. So, $Ker\ f = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. We need to show that n is prime. Suppose not! Then without loss of generality, we can write $n = a.b$ where $a, b \in \mathbb{Z}$.
Now, we have $f(n) = 0 \implies f(a.b) = 0 \implies f(a).f(b) = 0$.
Then either $f(a) = 0$ or $f(b) = 0$.
Suppose $f(a) \neq 0$. To show that $f(b) = 0$
Since, $f(a) \neq 0$, $(f(a))^{-1}$ exists as R is a field. So,
$f(a).f(b) = 0 \implies (f(a))^{-1}(f(a).f(b)) = 0 \implies f(b) = 0$
So, $a \in Ker\ f$ or $b \in Ker\ f$.
Then, $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$, that is either a is a multiple of n or b is a multiple of n, a contradiction. Thus, n is a prime number. This completes the proof. □

3 Characteristic of a Field

Let F be a field. Consider the homomorphism $f : \mathbb{Z} \to F$. Then, by the above result, we have $Ker\ f = \{0\}$ or $p\mathbb{Z}$, for some prime p. If $Ker\ f = \{0\}$, we say that the field F has characteristic 0. If $Ker\ f = p\mathbb{Z}$, then we say that the field F has characteristic p.

Examples:

-Fields with characteristic 0: $\mathbb{R}, \mathbb{Q}$

-Fields with characteristic p: $\mathbb{Z}/p\mathbb{Z}$

4 Size of a Finite Field

Proposition 4.1 *If F is a finite field then $|F| = p^n$ for some prime p and some positive integer n.*

Proof. Let F be a finite field. Consider, the homomorphism $f : \mathbb{Z} \to F$. Now, $Ker\ f \neq 0$, as $\mathbb{Z}$ is an infinite set and F is finite. So, $Ker\ f = p\mathbb{Z}$ for some prime p.
Now, consider a function $g : \mathbb{Z}/p\mathbb{Z} \to F$ defined as: $g(z + p\mathbb{Z}) = f(z)$

- Is g well-defined?

  Suppose, $z_1 + p\mathbb{Z} = z_2 + p\mathbb{Z}$

  Then, $z_1 - z_2 \in p\mathbb{Z}$

  Then, $f(z_1 - z_2) = 0_F$ (Since $p\mathbb{Z}$ is the kernel)

  Then, $f(z_1) = f(z_2)$

  So, $g(z_1 + p\mathbb{Z}) = g(z_2 + p\mathbb{Z})$

- Is g injective?

  Let $g(z_1 + p\mathbb{Z}) = g(z_2 + p\mathbb{Z})$

  Then, $f(z_1) = f(z_2)$

  Then, $z_1 - z_2 \in p\mathbb{Z}$

  Then, $z_1 + p\mathbb{Z} = z_2 + p\mathbb{Z}$.

- Is g a homomorphism?

  $g((z_1 + p\mathbb{Z}) + (z_2 + p\mathbb{Z}))$

  $= g((z_1 + z_2) + p\mathbb{Z})$

  $= f(z_1 + z_2)$

  $= f(z_1) + f(z_2)$

  $= g(z_1 + p\mathbb{Z}) + g(z_2 + p\mathbb{Z})$

  Also, $g((z_1 + p\mathbb{Z}).(z_2 + p\mathbb{Z}))$

  $= g((z_1.z_2) + p\mathbb{Z})$

  $= f(z_1.z_2)$

$$= f(z_1).f(z_2)$$
$$= g(z_1 + p\mathbb{Z}).g(z_2 + p\mathbb{Z})$$

Thus, g is an injective homomorphism from $\mathbb{Z}/p\mathbb{Z} \to F$. Then, $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to Image(g) in F. Then one can identify elements of $\mathbb{Z}/p\mathbb{Z}$ with elements of Image(g), and consider F to be a vector space over the field $\mathbb{Z}/p\mathbb{Z}$.
But F is a finite vector space in particular a finite-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. Let $dim(F) = n$. Then, any $v \in F$ can be written uniquely as $a_1v_1 + a_2v_2 + \cdots + a_nv_n$, where $a_i \in \mathbb{Z}/p\mathbb{Z}$ $\forall i$ and $\{v_1, v_2, \cdots, v_n\}$ is a basis on F over $\mathbb{Z}/p\mathbb{Z}$. This provides us with a bijection between F and $(\mathbb{Z}/p\mathbb{Z})^n$. But $|(\mathbb{Z}/p\mathbb{Z})^n| = p^n$. So, $|F| = p^n$.
This completes the proof. □

Definition: A **vector space** consists of a set V (elements of V are called **vectors**), a field $\mathbb{F}$ (elements of $\mathbb{F}$ are called **scalars**), and two operations

- An operation called *vector addition* that takes two vectors $v, w \in V$, and produces a third vector, written $v + w \in V$.
- An operation called *scalar multiplication* that takes a scalar $c \in \mathbb{F}$ and a vector $v \in V$, and produces a new vector, written $cv \in V$.

which satisfy the following conditions (called *axioms*).

1. Associativity of vector addition: $(u + v) + w = u + (v + w)$ for all $u, v, w \in V$.
2. Existence of a zero vector: There is a vector in V, written 0 and called the **zero vector**, which has the property that $u + 0 = u$ for all $u \in V$
3. Existence of negatives: For every $u \in V$, there is a vector in V, written $-u$ and called the **negative of** u, which has the property that $u + (-u) = 0$.
4. Associativity of multiplication: $(ab)u = a(bu)$ for any $a, b \in \mathbb{F}$ and $u \in V$.
5. Distributivity: $(a + b)u = au + bu$ and $a(u + v) = au + av$ for all $a, b \in \mathbb{F}$ and $u, v \in V$.
6. Unitarity: $1u = u$ for all $u \in V$.

5 Integral Domains

A commutative ring with identity is said to be an integral domain if for all $a, b \in R$, $a.b = 0$ implies either $a = 0$ or $b = 0$.
Examples:
-$\mathbb{Z}$
-any field
-$F[x]$, where F is a field -Consider $\mathbb{Z}/4\mathbb{Z}$ and consider $[2] \in \mathbb{Z}/4\mathbb{Z}$. Now, $[2] \neq [0]$, but $[2][2] = [0]$. Thus, $\mathbb{Z}/4\mathbb{Z}$ is *not* an integral domain.

Exercise Prove that any finite integral domain is a field.

Proposition 5.1 *Any finite integral domain is a field.*

Proof. To prove that any finite integral domain is a field, we need to show that every nonzero element has a multiplicative inverse.
Let D be a finite integral domain. Since D is finite, every nonzero element $a \in D$ generates a cyclic subgroup of $D^{\times}$, the group of units of D, under multiplication.
Now, consider an arbitrary nonzero element $a \in D$. We'll denote the cyclic subgroup generated by a as $\langle a \rangle$. Since D is an integral domain, $\langle a \rangle$ is closed under multiplication and contains the identity element 1.
Since D is finite, there exists a positive integer n such that $a^n = 1$, where 1 is the multiplicative identity of D. This means that a has an inverse, namely a^{n-1}, because $a \cdot a^{n-1} = a^{n-1} \cdot a = a^n = 1$.
Therefore, every nonzero element of D has a multiplicative inverse, and D is a field by definition.
This concluses the proof that any finite integral domain is a field. □

Proposition 5.2 *Any integral domain can be extended to a field.*

What does this result say?
If R is an integral domain, then there exists a field F such that there is an injective homomorphism $h : R \to F$. For example, The integral domain, $\mathbb{Z}$ can be extended to the field of rational numbers, $\mathbb{Q}$.
The proof is to be discussed in the next lecture.