LECTURE 14

15.06.2024

We will now move on to discuss about homomorphisms from $\mathbb{Z}$ to some ring R, say.

Take a homomorphism $f: \mathbb{Z} \to R$.

What is $\ker f$?

- $R = \{0_R\}$. $\ker f = \mathbb{Z}$
- $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. $\ker f = \{0\}$

[Note that 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]

- $R = \mathbb{Z}/n\mathbb{Z}$. $\ker f = n\mathbb{Z}$.

Q. What happens to $\ker f$ if R is a field?

Proposition: 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 $n = a \cdot b$, $a, b \in \mathbb{Z}$

Now, we have $f(n) = 0$

$$\Rightarrow f(a \cdot b) = 0$$

$$\Rightarrow f(a) \cdot f(b) = 0$$

Then, either $f(a) = 0$ or $f(b) = 0$

[Suppose $f(a) \neq 0$. To show $f(b) = 0$.

Since $f(a) \neq 0$, $(f(a))^{-1}$ exists. So,

$f(a) \cdot f(b) = 0 \implies (f(a))^{-1}(f(a) \cdot f(b)) = 0$

$\implies f(b) = 0$]

So, $a \in \text{Ker } f$ or $b \in \text{Ker } f$.

Then, $a \in n\mathbb{Z}$ or $b \in \mathbb{Z}$, 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.

Characteristic of a field.

Let F be a field. Consider the homomorphism $f: \mathbb{Z} \to F$. Then, by the above result, we have:

$\text{Ker } f = \{0\}$ or $p\mathbb{Z}$, for some prime p.

If $\text{Ker } f = \{0\}$, we say that the field F has characteristic 0. If $\text{Ker } f = p\mathbb{Z}$,

then we say that the field F has characteristic p.

Examples

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

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

Size of finite fields.

Theorem: 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 $g: \frac{\mathbb{Z}}{p\mathbb{Z}} \to F$,

$g(z + p\mathbb{Z}) = f(z)$

① Is g well-defined? YES

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

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

Then, $f(z_1 - z_2) = 0_F$

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

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

② Is g injective? YES

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

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

Then, $f(z_1 - z_2) = 0_F$

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

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

③ Is g a homomorphism? YES

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

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

$$= f(z_1 + z_2)$$

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

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

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

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

$$= f(z_1 \cdot z_2)$$

$$= f(z_1) \cdot f(z_2)$$

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

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(γ), and consider F to be a vector space over the field $\mathbb{Z}/p\mathbb{Z}$. (Check!)

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 $a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$, where $a_i \in \mathbb{Z}/p\mathbb{Z}$ for all 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.

Integral domains

A commutative ring with identity R is said to be an integral domain if for all $a, b \in R$, $a \cdot b = 0$ 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 $[2] \cdot [2] = [0]$.

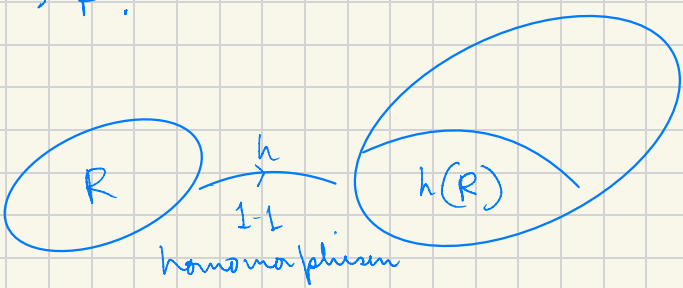
  Thus $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain.

H.W. Prove that any finite integral domain is a field

Theorem: 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 $h : R \to F$.



An example case

The integral domain, $\mathbb{Z}$ can be extended to the field of rational numbers, $\mathbb{Q}$.