LECTURE 17

26.03.2024

How to construct fields containing p^2 elements, for any prime number p?

Before getting into this let us introduce the concept of irreducible polynomials, which we would use below:

- A polynomial $f(x)$ over a ring R is said to be irreducible if $f(x)$ cannot be expressed as a product, $g(x) \cdot h(x)$ of polynomials $g(x)$ and $h(x)$ whose degrees are ≥ 1.

Example:

$R = \mathbb{Z}/3\mathbb{Z}$: $f(x) = x^2 - 2 = [1] \cdot x^2 - [2]$.

Does $f(x)$ have any root in R?

NO $\left[[0]^2 = [0], \quad [1]^2 = [1], \quad [2]^2 = [1] \right]$

So, $f(x)$ is irreducible over $\mathbb{R}$ as $f(x)$ cannot be expressed as the product of $g(x)$ and $h(x)$ with degrees ≥ 1.

Let α be some root of $f(x)$. Then,

$$\boxed{\begin{aligned} \mathbb{Z}/3\mathbb{Z}[\alpha] &\cong \mathbb{Z}/3\mathbb{Z}[x] \big/ (x^2-2) \\ &\cong \mathbb{Z}/3\mathbb{Z} + \mathbb{Z}/3\mathbb{Z}\,\alpha \\ &\cong (\mathbb{Z}/3\mathbb{Z})^2 \quad [\text{as abelian groups}] \end{aligned}}$$

So, $\mathbb{Z}/3\mathbb{Z}[\alpha]$ contains 9 elements.

We have started off from a field $\mathbb{Z}/3\mathbb{Z}$ containing 3 elements and using an irreducible polynomial over $\mathbb{Z}/3\mathbb{Z}$, we have come up with a ring structure $\mathbb{Z}/3\mathbb{Z}[\alpha]$ containing

$3^2 = 9$ elements. If we can prove that $\mathbb{Z}/3\mathbb{Z}[\alpha]$ is a field, we get a field containing $3^2 = 9$ elements.

To achieve this, let us prove the following lemma.

Lemma. Let F be a field. Then, $F[x]/(f(x))$ is a field iff $f(x)$ is irreducible over F.

Proof: Let $F' = F[x]/(f(x))$. We have the following:

F' is a field

iff F' has only two ideal $\{0_{F'}\}$ and F'

iff $F[x]$ has only two ideals containing $(f(x))$, $(f(x))$ and $F[x]$. (Why?)

iff $(f(x))$ is a maximal ideal of $F[x]$.

iff there is no other $g(x)$ in $F[x]$ s.t. $g(x)$ divides $f(x)$ (Why?)

iff $f(x)$ is irreducible over F.

So, we have constructed a field containing $3^2 = 9$ elements, $\mathbb{Z}/3\mathbb{Z}[x] \big/ (x^2-2)$

Let us now generalize this idea to construct fields of order p^2, for any prime p.

- We consider the field $\mathbb{Z}/p\mathbb{Z}$ and try to find irreducible polynomials of degree 2 over $\mathbb{Z}/p\mathbb{Z}$.

Let us first consider $\mathbb{Z}/2\mathbb{Z}$.

Consider $f(x) = x^2 - 1$. Then, $f(x) = (x-1)(x+1)$, so, $f(x)$ will not work.

But consider $f(x) = x^2 + x + 1$, it is irreducible over $\mathbb{Z}/2\mathbb{Z}$.

So, the required field having $2^2 = 4$ elements is $\dfrac{\mathbb{Z}/2\mathbb{Z}\,[x]}{(x^2 + x + 1)}$

Let us consider primes $p > 2$.

Consider the polynomial $f(x) = x^2 - b$ and a prime $p > 2$. Now, $f(x)$ will be irreducible in $\mathbb{Z}/p\mathbb{Z}$ if b is not a square in $\mathbb{Z}/p\mathbb{Z}$. So, if we can ensure the existence of such a b in $\mathbb{Z}/p\mathbb{Z}$, $p > 2$, we are done.

We prove the following lemma.

Lemma: Let p be a prime number > 2. Then, there exists $b \in \mathbb{Z}/p\mathbb{Z}$, such that b is not a square.

Proof: Consider a function:

$$f : \mathbb{Z}/p\mathbb{Z} \setminus \{[0]\} \to \mathbb{Z}/p\mathbb{Z} \setminus \{[0]\},$$

$$f(g) = g^2.$$ Now,

$$\begin{aligned} f(g_1 \cdot g_2) &= (g_1 \cdot g_2)^2 \\ &= g_1^2 \cdot g_2^2 \\ &= f(g_1) \cdot f(g_2) \end{aligned}$$

So, f is a group homomorphism on $\mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}$.

It is enough to show that f is not a surjective map. We know that in this case, f is surjective iff

f is injective iff $\operatorname{Ker} f = \{[1]\}$. So, if we can show that $\operatorname{Ker} f \neq \{[1]\}$, we are done.

Now, $\operatorname{Ker} f = \left\{ [a] \in \mathbb{Z}/_{p}\mathbb{Z} \setminus \{[0]\} : a^2 \equiv 1 \pmod{p} \right\}$

We have, $a^2 \equiv 1 \pmod{p}$

$$\text{iff} \quad p \mid a^2 - 1$$

$$\text{iff} \quad p \mid (a+1)(a-1)$$

$$\text{iff} \quad p \mid (a+1) \quad \text{or} \quad p \mid (a-1)$$

$$\text{iff} \quad a \equiv -1 \pmod{p} \quad \text{or}, \quad a \equiv 1 \pmod{p}$$

Thus, $\operatorname{Ker} f = \{[1], [-1]\}$.

Hence, $\operatorname{Ker} f \neq \{[1]\}$

So, f is not surjective.

This completes the proof.

- Thus, we have a way to construct fields having p^2 elements for every prime p.

Prime fields

A field F is said to be prime if F has no proper subfield.

Example

$\mathbb{Z}/2\mathbb{Z}$

Lemma Consider any field F. Then,

(a) if F has characteristic 0, then F contains a subfield K s.t. $K \cong \mathbb{Q}$.

(b) if F has characteristic $p > 0$, then F contains a subfield K s.t. $K \cong \mathbb{Z}/p\mathbb{Z}$.

Proof: Let $f: \mathbb{Z} \to F$ defined by:

$$f(n) = \underbrace{1 + 1 - \cdots + 1}_{n \text{ times}}.$$

for all $n \in \mathbb{Z}$, 1 being the multiplicative identity of F. We have that, f is a homomorphism.

(a) Suppose the characteristic of F is 0.

Then $\operatorname{Ker} f = \{0\}$. So, f is injective.

Define $f^*: \mathbb{Q} \to F$ by:

$$f^*\left(\frac{a}{b}\right) = f(a)\left[f(b)\right]^{-1} \text{ for all } \frac{a}{b} \in \mathbb{Q}.$$

1. Is f^* injective?

$$f^*\left(\frac{a}{b}\right) = f^*\left(\frac{c}{d}\right)$$

$$\Rightarrow f(a)\left[f(b)\right]^{-1} = f(c)\left[f(d)\right]^{-1}$$

$$\Rightarrow \quad f(a)\,f(d) = f(b)\,f(c)$$

$$\Rightarrow \quad f(ad) = f(bc).$$

$$\Rightarrow \quad ad = bc.$$

$$\Rightarrow \quad a/b = c/d.$$

So, f^* is injective.

2. Is f^* a homomorphism?

$$- \quad f^*\left(\frac{a}{b} + \frac{c}{d}\right) = f^*\left(\frac{ad + bc}{bd}\right)$$

$$= f(ad + bc)\,[f(bd)]^{-1}$$

$$= \left(f(a)f(d) + f(b)f(c)\right)[f(b)]^{-1}[f(d)]^{-1}$$

$$= f(a)\,[f(b)]^{-1} + f(c)\,[f(d)]^{-1}$$

$$= f^*\left(\frac{a}{b}\right) + f^*\left(\frac{c}{d}\right)$$

$$
\begin{aligned}
\cdot\ f^*\left(\tfrac{a}{b}\cdot\tfrac{c}{d}\right) &= f^*\left(\frac{ac}{bd}\right) \\
&= f(ac)\,[f(bd)]^{-1} \\
&= f(a)\,f(c)\,[f(b)]^{-1}\,[f(d)]^{-1} \\
&= f(a)\,[f(b)]^{-1}\,f(c)\,[f(d)]^{-1} \\
&= f^*(a/b)\cdot f^*(c/d).
\end{aligned}
$$

Then, we have that f^* is an injective homomorphism from $\mathbb{Q}$ to F. So, $\mathbb{Q} \cong \text{Image}(f^*)$.

But $\text{Image}(f^*)$ is a subfield of F and we have our K s.t. $F \supseteq K \cong \mathbb{Q}$. This completes the proof.