LECTURE 21

16.04.2024

A brief overview on finite fields

We will basically prove an existence result and a uniqueness result for finite fields.

Theorem (Existence): Let p be a prime number and n be a positive integer. Then there exists a field extension $F/\mathbb{Z}_p$ of degree n.

Proof: Consider the polynomial $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Let S be a splitting field of $f(x)$. Let a be a root of $f(x)$ in S.

Then, $f(x) = (x-a)^m g(x)$, where $m \geq 1$ and a is not a root of $g(x)$.

Let us consider $f'(x)$.

From $f(x) = x^{p^n} - x$, $f'(x) = -1$ (Check!)

From $f(x) = (x-a)^m g(x)$, $f'(x) =$

$$(x-a)^{m-1}\left[m\,g(x) + (x-a)\,g'(x)\right].$$

Then, we have that $m-1=0$, i.e., $m=1$.

This means that all the roots of $f(x)$ are distinct, that is, $f(x)$ has p^n distinct roots in S. Let F be the set of all these roots.

If we can show that F is a field, we are done. Let $a, b \in F$, with $b \neq 0$.

(i) We show that $a-b \in F$.

Now, $(a-b)^{p^n} = a^{p^n} - b^{p^n} = a-b$. So, $a-b \in F$.

(ii) We show that $ab^{-1} \in F$.

Now, $(ab^{-1})^{p^n} = a^{p^n}(b^{p^n})^{-1} = ab^{-1}$. So, $ab^{-1} \in F$.

Thus $F = S$ and also, we have

$[F : \mathbb{Z}_p] = n$ (Check!) .

This completes the proof.

<u>Theorem (Uniqueness)</u>. Any two finite fields containing p^n elements are isomorphic, where p is a prime number and n is a positive integer.

<u>Proof</u>: Consider the polynomial $x^{p^n} - x$ over $\mathbb{Z}_p$. Take any field F of characteristic p containing p^n elements. We consider the algebraic structure $(F \setminus \{0\}, \cdot)$. It is a commutative group of order $p^n - 1$. Then, for all $a \in F \setminus \{0\}$, $a^{p^n - 1} = 1$. So, $a^{p^n} = a$. Also, $0^{p^n} = 0$. Hence, F contains all roots of $x^{p^n} - x$, and hence contains a splitting field S of $x^{p^n} - x$. But F is exactly the

set of roots of $x^{p^n} - x$. Thus, $F = S$.

So, we have that any field of characteristic p containing p^n elements is a splitting field of $x^{p^n} - x$. Thus, any two such fields are isomorphic.

This completes the proof.

Example.

Consider the field $\mathbb{Z}_2$ and consider the polynomial $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$.

$f(x)$ is irreducible in $\mathbb{Z}_2[x]$.

Then, we can consider the field

$$F = \mathbb{Z}_2[x] / (x^3 + x + 1) = \mathbb{Z}_2(\lambda_1),$$ where,

λ_1 is a root of $x^3 + x + 1$ in F:

$x + (x^3 + x + 1)$.

$\mathbb{Z}_2(\lambda_1) = \mathbb{Z}_2[\lambda_1] = \{0, 1, \lambda_1, \lambda_1^2, 1+\lambda_1, 1+\lambda_1^2, \lambda_1+\lambda_1^2, 1+\lambda_1+\lambda_1^2\}$.

H.W. Write the addition table for $\mathbb{Z}_2(\lambda_1)$.

H.W. Considering $x^3+x+1 = (x+\lambda_1)\,g(x)$ find the roots of $g(x)$, say λ_2 and λ_3, and show that $\mathbb{Z}_2(\lambda_1, \lambda_2, \lambda_3) = \mathbb{Z}_2(\lambda_1)$, that is, $\mathbb{Z}_2(\lambda_1)$ is a splitting field of the polynomial x^3+x^2+1 over $\mathbb{Z}_2$.

H.W. Do the same study for the polynomial x^3+x^2+1 over $\mathbb{Z}_2$.