Lecture 20

08 April 2024 14:08

From last time:

$m, n \in \mathbb{Z}$

$$y + i = (m + ni)^3$$

$$= m^3 + 3m^2ni - 3mn^2 - n^3i$$

$$= \underbrace{(m^3 - 3mn^2)}_{y} + i\underbrace{(3m^2n - n^3)}_{1}.$$

So $1 = n(3m^2 - n^2)$

$\Rightarrow$ Either $n = 1$ and $3m^2 - n^2 = 1$

$3m^2 - 1 = 1$

$3m^2 = 2$ ← no solution

or $n = -1$ and $3m^2 - n^2 = -1$

$3m^2 - 1 = -1$

$3m^2 = 0$

$m = 0.$

only solution

$\Rightarrow$ $y = m^3 - 3mn^2 = 0$

and $x = y^2 + 1 = 1$

only solution

and $x = y^2 + 1 = 1$ ← only solution

//

Back to examinable content:

Thm: Suppose F is a field, and $f \in F[x]$ is irreducible.

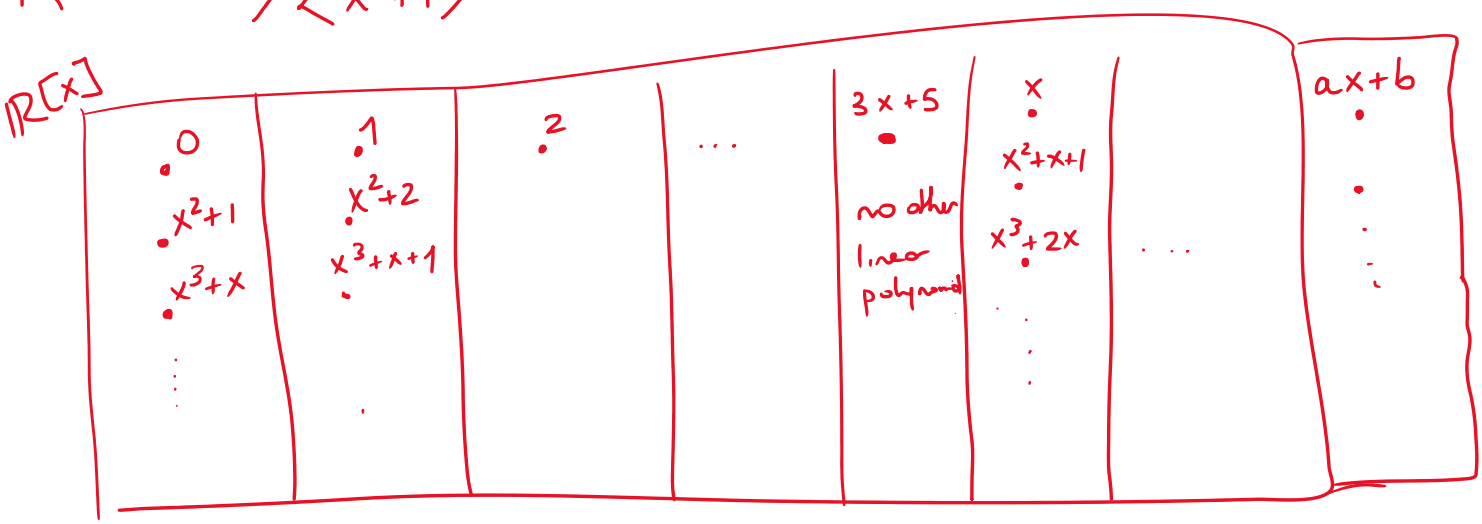
Then $K := F[x]/\langle f \rangle$ is a field extension of F (it contains F).

and the element $\alpha := [x]$ is a root of f.

//

Example: $F = \mathbb{R}$ $\quad f = x^2 + 1 \in \mathbb{R}[x]$ irreducible

$K = \mathbb{R}[x]/\langle x^2+1 \rangle$



$[x^6+1] = [-x^4+1]$ because $(x^6+1)-(-x^4+1)$

$= x^6 + x^4$

$= x^4(x^2+1)$

$[-x^4+1] = [x^2+1]$ because $(-x^4+1)-(x^2+1)$

$\|$ $= -x^4 - x^2$

$[0x+0]$ $= -x^2(x^2+1) \in \langle f \rangle$

We are using that $[x^2+1] = [0]$

So $[x^2] = [-1]$.

Proposition. Suppose $\deg(f) = n$.

- Every coset in $K = F[x]/\langle f \rangle$ has a unique representative of the form

$$[a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0]$$

$\|$

$$(a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0)$$

Proof: Suppose $[g]$ is any coset of $F[x]/\langle f \rangle$. By the long division algorithm, we can write $g = f \cdot q + r$ where

$r = 0$ or $\deg(r) < \deg(f)$.

But then $g - r = f \cdot q \in \langle f \rangle$

so $[g] = [r]$ and r has the form $[a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x^1 + a_0]$.

This representative is unique because, if $[r_1] = [r_2]$ and $\deg(r_1) < n$, $\deg(r_2) < n$

then $r_1 - r_2 \in \langle f \rangle$. So the only

$r_1 - r_2$: $\deg < n$; $\langle f \rangle$: $\deg = n$

possibility is $r_1 - r_2 = 0 \implies r_1 = r_2$. ∎

- Example: $F = \mathbb{R}$ $\quad f = x^2+1 \in \mathbb{R}[x]$

$K = \mathbb{R}[x]/\langle x^2+1 \rangle$ is a field extension of $\mathbb{R}$, $\alpha = [x]$ satisfies $\alpha^2 + 1 = 0$, and every coset can be written as

$$a \cdot \alpha + b. \quad (= [ax+b])$$

So $K \cong \mathbb{C}$.

Example: $F = \mathbb{Q}$ $\quad f = x^3 - 2 \in \mathbb{Q}[x]$ is irreducible.

(since $f = g \cdot h$ implies one factor is of degree 1, so f would have a root in $\mathbb{Q}$).

$K = \mathbb{Q}[x]/\langle x^3-2 \rangle$ is a field,

$\mathbb{Q}[x]$ satisfies $\alpha^3 - 2 = 0$,

The element $\alpha = [x]$ satisfies $\alpha^3 - 2 = 0$,

and every element of K can be written as $a\alpha^2 + b\alpha + c$. with $a, b, c \in \mathbb{Q}$.

In other words,

$$K \cong \mathbb{Q}[\sqrt[3]{2}] = \left\{ c + b\sqrt[3]{2} + a\sqrt[3]{4} \mid a,b,c \in \mathbb{Q} \right\}$$

Finite field of 4 elements:

Take $F = \mathbb{Z}_2 = \{0, 1\}$. Take $\mathbb{Z}_2[x]$

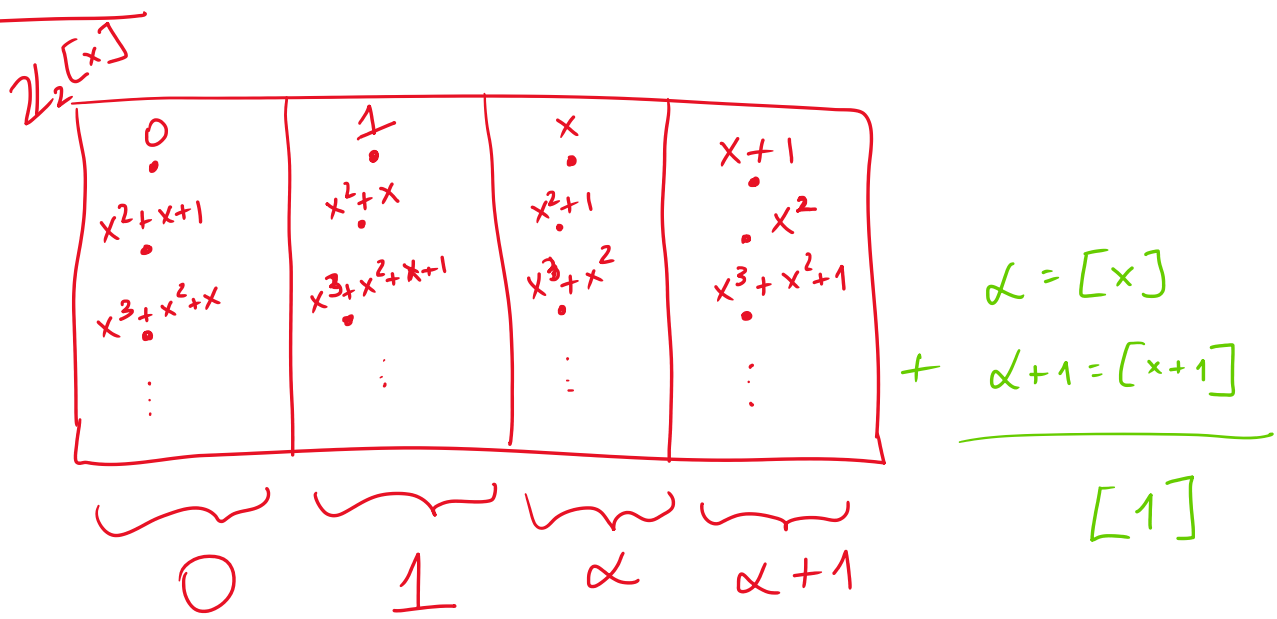
$$\left(x^8 + x^5 + x + 1 \right)$$

Let $f = x^2 + x + 1$. This is irreducible because it has <u>degree 2</u> and it has no roots.

$K = \mathbb{Z}_2[x] / \langle x^2 + x + 1 \rangle$ is a field,

The element $\alpha = [x]$ satisfies $\alpha^2 + \alpha + 1 = 0$ and every element of K can be written uniquely as $a \cdot \alpha + b$ with $a, b \in \mathbb{Z}_2$.

Picture:



$$\alpha^2 + \alpha + 1 = 0$$
$$\alpha^2 = \alpha + 1$$

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

·	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$$(\alpha+1)^2 = \alpha^2+\alpha+\alpha+1$$
$$= \alpha^2+1$$
$$= \alpha+1+1$$
$$= \alpha$$

- Rings with 4 elements.

$\mathbb{Z}_4$ $\quad$ $\mathbb{F}_4$ $\quad$ $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$

↳ the field of 4 elements

$\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$ — isomorphic

---

- Using the same techniques: $F = \mathbb{Z}_p$

and $f \in \mathbb{Z}_p[x]$ irreducible of degree n,

$K = \mathbb{Z}_p[x]/\langle f \rangle$ is a field

where every element can be written uniquely as

$$a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \dots + a_1 x + a_0. \qquad a_i \in \mathbb{Z}_p$$

total of p^n elements.

This is the field with p^n elements.

<u>Thm</u>: Any field has to have p^n elements for a prime p and an integer n.
And there is only one field (up to isomorphism) with p^n elements.