Last time

$\mathbb{F}$ a field, $\phi(x) \in \mathbb{F}[x]$

prime poly (ie cannot be written as $\phi(x) = a(x) \cdot b(x)$ w/ $\deg a, \deg b \geq 1$)

$$\rightarrow \mathbb{F}_{\phi(x)} = \left\{ r(x) = \sum_{i=0}^{k} a_i x^i \;\middle|\; \begin{array}{l} a_i \in \mathbb{F} \\ k < n \end{array} \right\}$$

"remainders of mod-ϕ arithmetic".

$\mathbb{F}_{\phi(x)}$ is a field w/ mod-ϕ addition and mult.

If $\#\mathbb{F} = t$, $\#\mathbb{F}_{\phi(x)} = t^n$

Example $\mathbb{F} = \mathbb{F}_2$ $\phi(x) = x^2 + x + 1$

ϕ is prime (over $\mathbb{F}_2$) since it has no roots

$$\rightarrow \mathbb{F}_{\phi(x)} = \left\{ r(x) = a_0 + a_1 x \;\middle|\; a_0, a_1 \in \mathbb{F}_2 \right\}$$

$$= \{ 0, 1, x, x+1 \}$$

($k < n \Rightarrow k \equiv k \mod n$)

+	0	1	x	x+1
0				
1				
x				1
x+1				

$\phi(x) = x^2 + x + 1$

Note $x^2 = -(x+1) \mod \phi$

$= x+1 \mod \phi$

$\Rightarrow$

$$x \cdot x = x+1$$

Similarly $x^3 = 1 \mod \phi$.

Def: A <u>ring</u> is a set R, w/ specified elements $0, 1 \in R$ and two binary op'n:

$$+ : R \times R \to R$$

$$\cdot : R \times R \to R$$

that satisfy all axioms of a field except (possibly) existence of mult. inverse.

Examples

1) $\mathbb{Z}$

$\to \mathbb{Z}_n$

$\mathbb{Z}_p = \mathbb{F}_p$

(2) $\mathbb{Z}_n$ w/ $+ \bmod$, $\cdot \bmod n$

(3) If $\mathbb{F}$ is a field

$\mathbb{F}[x]$ is a ring

Fields $\subseteq$ Rings $\subseteq$ Ab Group

(4) $\mathbb{F}$ a field, $\phi(x) \in \mathbb{F}[x]$

that is not prime

$\rightarrow \mathbb{F}_{\phi(x)}$ is not a field:

$\phi = a \cdot b$ $\deg \phi > \deg a, \deg b \geq 1$

$a, b \in \mathbb{F}_{\phi(x)}$

$a \cdot b = 0 \bmod \phi$

$\neq \quad \neq$

but $\mathbb{F}_{\phi(x)}$ is a ring.

Def: For rings R, S, a

ring homomorphism is a function

$f: R \to S$ s.th:

1) $f(0) = 0$, $f(1) = 1$

2) $f(a+b) = f(a) + f(b)$ $\forall a, b \in R$

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

3) $f(-a) = -f(a)$ $\forall a \in R$

$f(a^{-1}) = f(a)^{-1}$ $\forall$ of $a \in R$.

f is called an **iso** if it is bijective.

Rem: $f: R \to S$ is a ring iso iff $\exists$ a ring homomorphism $f^{-1}: S \to R$ s.th

$f^{-1} \circ f = id_R$

$f \circ f^{-1} = id_S$.

Notation We will denote

$\mathbb{F}_{\phi(x)}$ as $\mathbb{F}[x]/\phi(x)$

$\left(\mathbb{F}[x]/\langle \phi(x) \rangle \right)$

analogous to $\mathbb{Z}/n\mathbb{Z}$.

Consider a field $\mathbb{F}$ and a prime poly $\phi(x) \in \mathbb{F}[x]$.

If $\deg \phi = 1$

$$\mathbb{F}_{\phi(x)} = \mathbb{F}[x]/\phi(x) = \{ a_0 \mid a_0 \in \mathbb{F} \}$$

$$\cong \mathbb{F}$$

Suppose $\deg \phi > 1$.

$$\# \mathbb{F}[x]/\phi(x) = \# \mathbb{F}^{\deg \phi}$$

We can consider the ring homomorphism:

$$\pi : \mathbb{F}[x] \to \mathbb{F}[x]/\phi(x)$$

$$f(x) \longmapsto f(x) \bmod \phi(x)$$

$$f \cdot g \longmapsto f \cdot g \bmod \phi$$

$$\| \quad f \bmod \phi \cdot g \bmod \phi$$

$$f + g \bmod \phi = f \bmod \phi + g \bmod \phi$$

$$\left\{ r(x) = \sum_{i=0}^{k} a_i x^i \right\} = \mathbb{F}$$

$k < n$

$$\mathbb{F} \subseteq \mathbb{F}[x]/\phi(x) =: \mathbb{K}$$

as the set of constant remainder poly's.

Thus we can view ϕ as

a poly over $\mathbb{k}$

$\phi(x) = 0$

ie $\phi(X) \in \mathbb{k}[X]$

$\mathbb{k} = \{ a_0 + a_1 x + \dots + a_k x^k \mid a_0, \dots, a_k \in \mathbb{F} \}$

$$\mathbb{k}[X] = \{ r_0 + r_1 X + r_2 X^2 + \dots + r_m X^m \mid r_0, \dots, r_m \in \mathbb{F}(x), \deg r_i < n \}$$

$$= \{ r_0(x) + r_1(x) X + r_2(x) \cdot X^2 + \dots \}$$

$a_0, \dots, a_n \in \mathbb{F} \subseteq \mathbb{k}$

$\phi(x) = a_0 + a_1 x + \dots + a_n x^n$

$$\phi(X) = a_0 + a_1 X + \dots + a_n X^n$$

$$\pi : \mathbb{F}[x] \to \mathbb{F}[x] / \phi(x) =: \mathbb{k}$$

$\phi(X) \in \mathbb{k}[X]$ $\quad \pi(x) \in \mathbb{k}$

$$\phi(X)\Big|_{\pi(x)} = \phi(\pi(x))$$

$\pi(x) - x \cong$

$$= \phi(x) = 0 \in \mathbb{k}$$

ie $\pi(x)$ is a root

of $\phi(X)$

ie (in $\mathbb{k}[X]$)

$$\rightarrow \phi(X) = (X - \pi(x))\,\psi(X)$$

Example

$\mathbb{F} = \mathbb{R}$ $\quad \phi(x) = x^2 + 1$

$$\mathbb{R}[x]/\langle x^2+1 \rangle = \{ a_0 + a_1 x \mid a_0, a_1 \in \mathbb{R} \}$$

$$x \cdot x = -1 \mod \phi$$

$$(x^2 + 1 = 0 \mod \phi)$$

$$\mathbb{C} = \left\{ a_0 + a_1 i \;\middle|\; a_0, a_1 \in \mathbb{R} \right\}$$

Def: Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$. A splitting field of $f(x)$ over $\mathbb{F}$, is a field $\mathbb{F} \subseteq \mathbb{E}$ s.th when we view $f(x) \in \mathbb{E}[x]$, it decomposes into linear factors ie

$$f(x) = a \cdot (x - a_1) \cdot \ldots \cdot (x - a_n)$$

over $\mathbb{E}$, $(a, a_1, \ldots, a_n \in \mathbb{E})$

and $\mathbb{E}$ is minimal wrt this property

(ie if $\mathbb{F} \subseteq \mathbb{k}$ and

$f(x)$ decomposes into linear factors over $\mathbb{k}$, then $\mathbb{E} \subseteq \mathbb{k}$).

Example

$\mathbb{C}$ is a splitting field of $f(x) = x^2 + 1$ over $\mathbb{R}$: over $\mathbb{C}$

$$f(x) = (x - i)(x + i)$$

for minimality, if $\mathbb{R} \subseteq \mathbb{k}$ and $f(x)$ splits over $\mathbb{k}$, ie

$$f(x) = (x - i)(x + i)$$

then $i^2 + 1 = 0$

$(=)$ $i^2 = -1$

and since $\mathbb{k}$ is a field it must contain all expression of the form

$$a_0 + a_1 i \quad \text{for } a_0, a_1 \in \mathbb{R}$$

$\Rightarrow \mathbb{k}$ contains

$$\mathbb{C}$$

Proposition: Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$. Then there exists a splitting field of $f(x)$ over $\mathbb{F}$.

Proof: Let us decompose f into prime factors over $\mathbb{F}$.

$$f(x) = f_1(x) \cdot \ldots \cdot f_n(x)$$

$f(x) = f_1(x) \cdots f_k(x)$.

If $f_1, \ldots, f_k$ are all linear then $\mathbb{F}$ is a splitting field of f.

Otherwise, wlog, suppose $\deg f_1 > 1$.

Consider $\mathbb{F} \subseteq \mathbb{K}_1 = \mathbb{F}[x]/f_1(x)$

and we know that $f_1(x)$ has a root in $\mathbb{K}$, say $\alpha \in \mathbb{K}$ ($\pi(x) = \alpha$)

Thus $f_1(x) = (x - \alpha) \cdot g_1(x)$

for some $g_1(x) \in \mathbb{K}_1[x]$.

We can consider $f(x) \in \mathbb{K}_1[x]$

and as such, it has at least one linear factor

bcs

$$f(x) = f_1(x) \cdot \ldots \cdot f_k(x)$$

$$= (x - \alpha)\, g_1(x) \cdot f_2(x) \cdot \ldots \cdot f_k(x)$$

if $g_1(x)$ is not linear,

repeat the process

to get $\mathbb{F} \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2$.

Since f can have at most finite number of roots, this process terminats in $\mathbb{F} \subseteq \mathbb{K}$ s.t h

$$f(x) = \alpha \cdot (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$$

$$\alpha, \alpha_1, \ldots, \alpha_n \in \mathbb{K}.$$

For minimality, observe that $\mathbb{K}_1$ is the minimal

field containing $\mathbb{F}$ and α

so $\mathbb{K}$ would be

(by induction) the minimal

field containing $\mathbb{F}$ and

all the roots of $f(x)$.

Thus $\mathbb{K}$ is a splitting

field for f over $\mathbb{F}$. //