3/9
Monday
Week 8

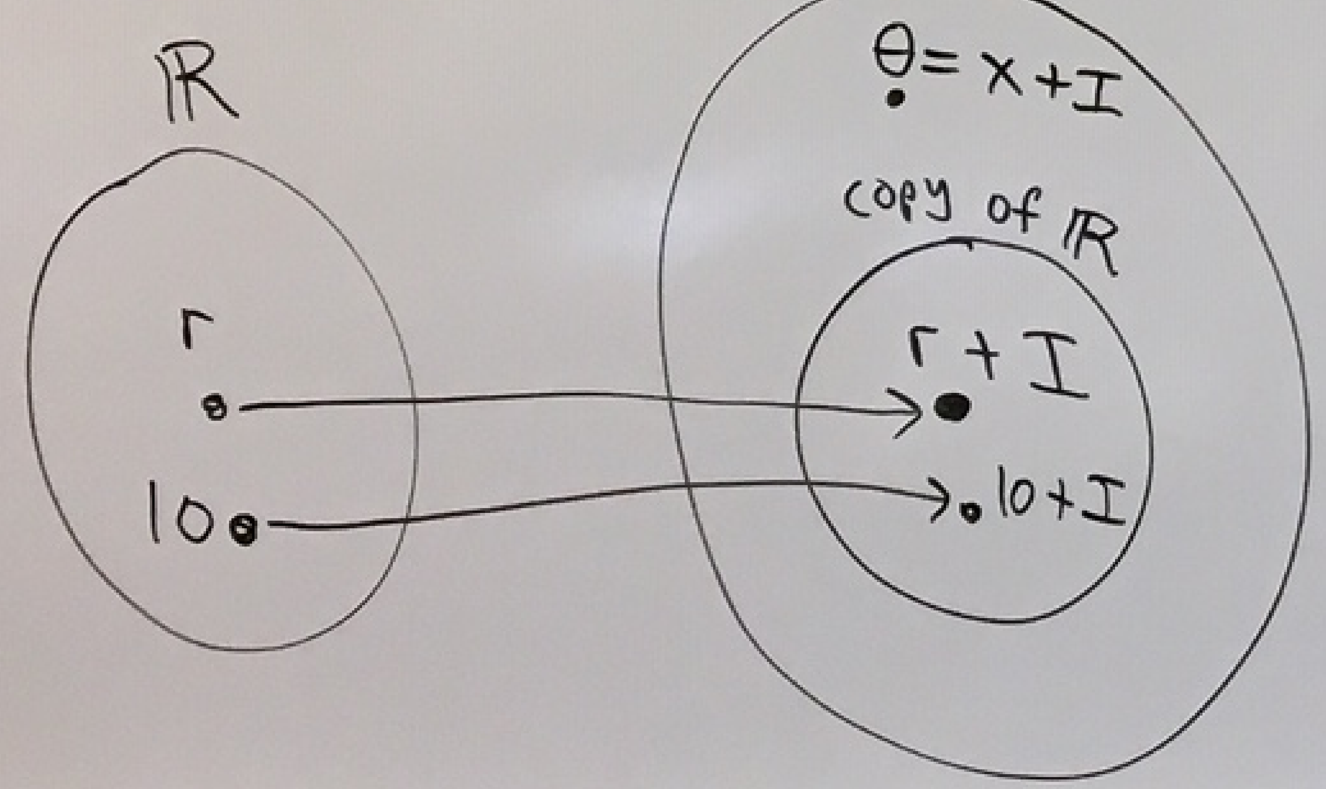
Theorem: Let F be a field and let $p(x) \in F[x]$ be non-constant and irreducible over F. Then there exists a field K containing as isomorphic copy of F in which $p(x)$ has a root.

Identifying F with the isomorphic copy shows that there exists an extension of F in which $p(x)$ has a root.

Ex from last time:

$F = \mathbb{R}$, $p(x) = x^2+1$

$K = \mathbb{R}[x]/I$



$I = (x^2+1)$
K is a field

$\theta^2 + (1+I)$
$= 0+I$

θ is a root of $p(x)$

Proo

wh

Sinc

So,

<u>proof:</u> Let

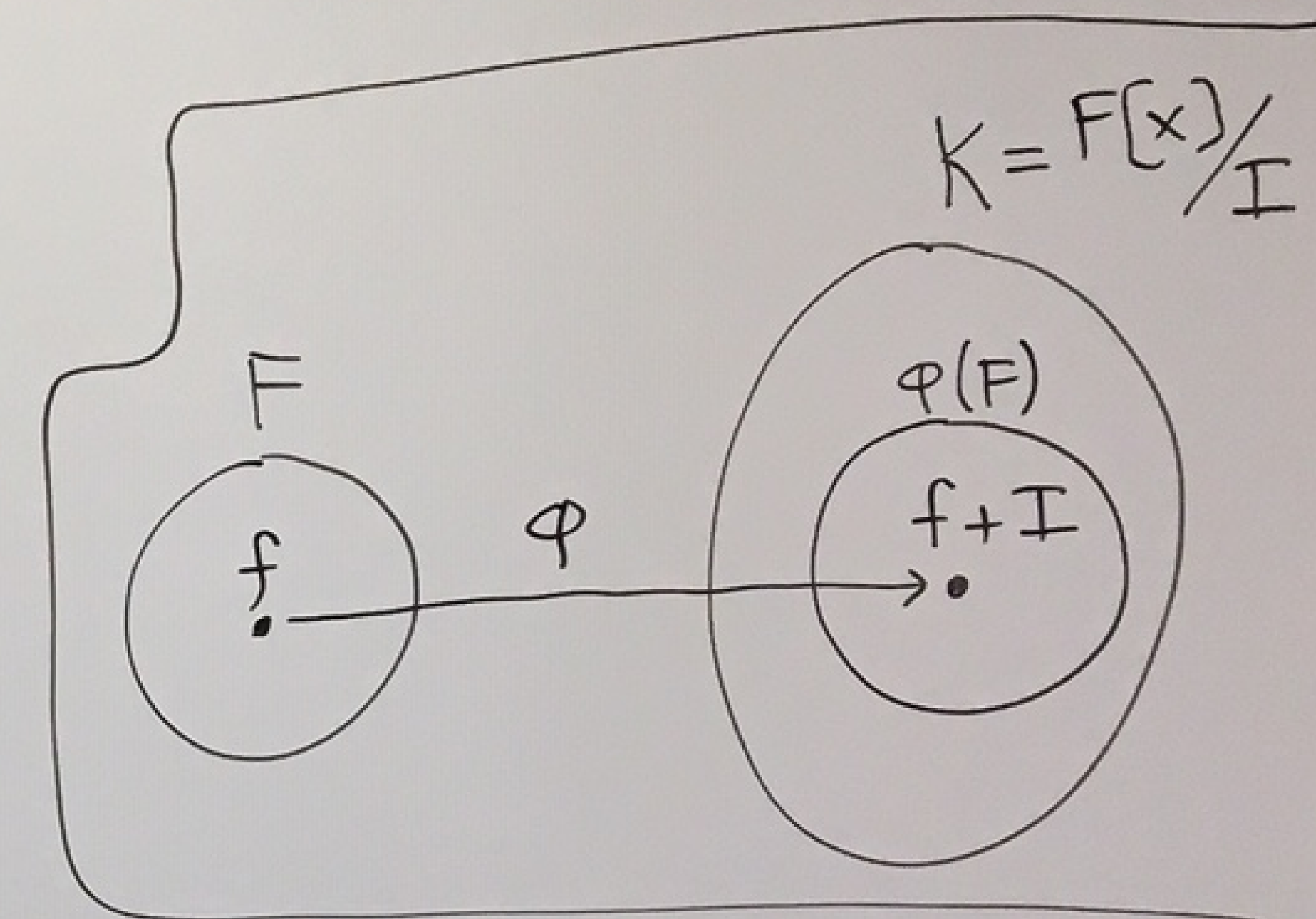
$$K = F[x]/I$$

where $I = (p(x)) = \{ p(x)f(x) \mid f(x) \in F[x] \}$.

Since $F[x]$ is a PID and $p(x)$ is irreducible, we have that $I = (p(x))$ is maximal.

So, K is a field.

Let's show there exists an isomorphic copy of F inside of K.



Define $\varphi : F \to K$ by $\varphi(f) = f + I$.

① φ is a homomorphism.

Let $f_1, f_2 \in F$. Then,

$$\begin{aligned}\varphi(f_1+f_2) &= (f_1+f_2)+I \\ &= (f_1+I)+(f_2+I) \\ &= \varphi(f_1)+\varphi(f_2).\end{aligned}$$

and $\varphi(f_1 f_2) = f_1 f_2 + I = (f_1+I)(f_2+I) = \varphi(f_1)\varphi(f_2)$

② φ is 1-1

Since $\ker(\varphi)$ is an ideal of F and F is a field, either $\ker(\varphi) = \{0\}$ or $\ker(\varphi) = F$.

Note that $\varphi(0) = 0 + I$ and $\varphi(1) = 1 + I$.

Also, $0 + I \neq 1 + I$ because if they were then $1 = 1 - 0 \in I$ and that would imply $1 = p(x)f(x)$ for some $f(x) \in F(x)$. That can't happen since $\deg(p(x)) \geq 1$ and so $\deg(p(x)f(x)) \geq 1$.

Since $\varphi(1) \neq 0 + I$, we have that $\ker(\varphi) \neq F$.

So, $\ker(\varphi) = \{0\}$.

Thus, φ is 1-1.

Recall φ is 1-1 iff $\ker(\varphi) = \{0\}$

Conclusion of ① & ②

Thus, F is isomorphic to $\varphi(F)$.

P(x

Le

H

b

S

S

Le

$p(x)$ has a root in K

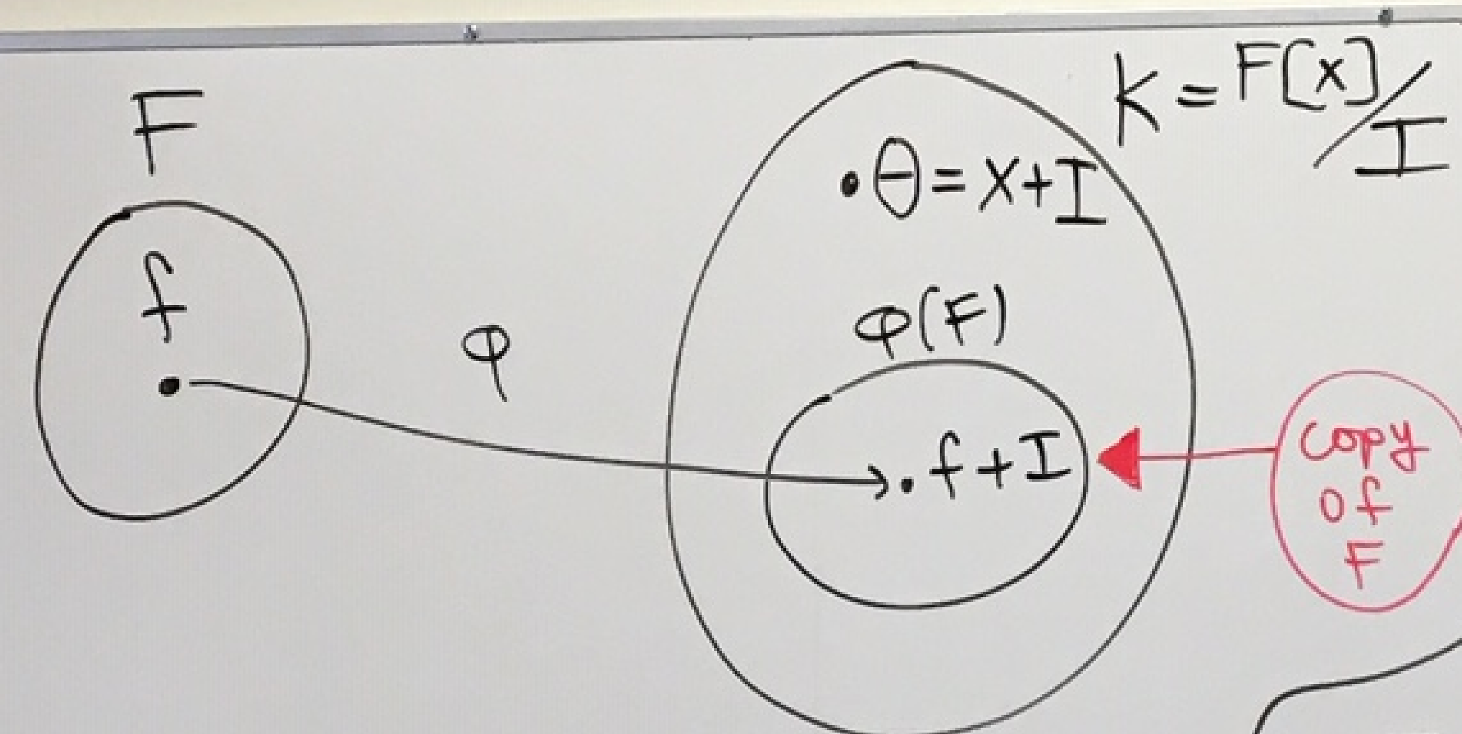
Let $\theta = x + I$.

Hence forth, given $f \in F$, denote $f + I$ by $\overline{f}$.

So, $\overline{f} = f + I$.

Suppose $p(t) = a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0$ where $a_i \in F$.

Lets "move" the coefficients of $p(t)$ over to $\varphi(F)$.



Let

$$\overline{p}(t) = \overline{a}_n t^n + \overline{a}_{n-1} t^{n-1} + \dots + \overline{a}_1 t + \overline{a}_0 .$$

Then,

$$\begin{aligned}
\overline{p}(\theta) &= \overline{a}_n \theta^n + \overline{a}_{n-1} \theta^{n-1} + \dots + \overline{a}_1 \theta + \overline{a}_0 \\
&= (a_n + I)(x+I)^n + (a_{n-1} + I)(x+I)^{n-1} + \dots + (a_1+I)(x+I) + (a_0+I) \\
&= (a_n + I)(x^n + I) + (a_{n-1} + I)(x^{n-1} + I) + \dots + (a_1+I)(x+I) + (a_0+I) \\
&= (a_n x^n + I) + (a_{n-1} x^{n-1} + I) + \dots + (a_1 x + I) + (a_0 + I) \\
&= (a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) + I \\
&= p(x) + I \underset{p(x) \in I}{=} 0 + I .
\end{aligned}$$

$\boxed{\text{The End}}$

$\boxed{\text{Example from last time}}$:

$F = \mathbb{R}$, $p(x) = x^2+1$

$I = (x^2+1)$

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

$$= \{ (a+bx) + I \mid a,b \in \mathbb{R} \}$$

I love fields!

<u>Theorem:</u> Let F be a field. Let $p(x) \in F[x]$ be a non-constant irreducible polynomial. Let $n = \deg(p(x))$. Let $K = F[x]/I$ where $I = (p(x))$.

Let $\theta = x + I$.

Then, $\bar{1}, \theta, \theta^2, \ldots, \theta^{n-1}$ is a basis for K over $\bar{F}$.

$\boxed{\bar{F} = \{ f+I \mid f \in F \} \text{ is the isomorphic copy of } F \text{ living in } K.}$

$\boxed{\bar{a} = a + I}$

Hence,

$$K = \{ \bar{a}_0 + \bar{a}_1\theta + \bar{a}_2\theta^2 + \cdots + \bar{a}_{n-1}\theta^{n-1} \mid a_i \in F \}$$

$$= \{ (a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}) + I \mid a_i \in F \}$$

Pr

D

w

proof: Let $a(x)+I \in K$ where $a(x) \in F[x]$.

Dividing $p(x)$ into $a(x)$ gives

$$a(x) = p(x)q(x) + r(x)$$

where $q(x), r(x) \in F[X]$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(p(x)) = n$.

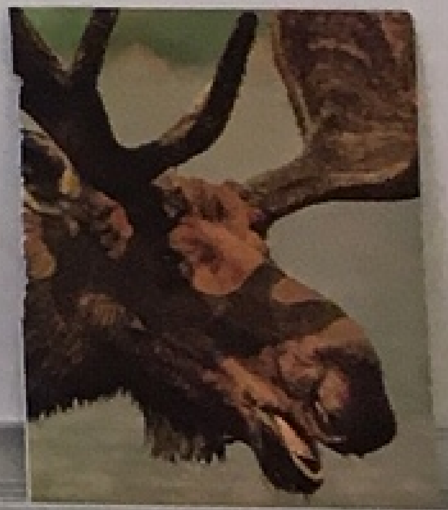
Since $a(x) - r(x) = p(x)q(x) \in I$, we have $a(x) + I = r(x) + I$.

So,

$$\bar{1} = 1 + I$$
$$\theta = x + I$$
$$\theta^2 = x^2 + I$$
$$\vdots$$
$$\theta^{n-1} = x^{n-1} + I$$

span K over $\bar{F}$.

So, $a(x)+I = r(x)+I \in \{(a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}) + I \mid a_i \in F\} = \{\bar{a}_0 + \bar{a}_1\theta + \bar{a}_2\theta^2 + \cdots + \bar{a}_{n-1}\theta^{n-1} \mid a_i \in F\}$



Suppose $\bar{1}, \theta, \theta^2, \dots, \theta^{n-1}$ were linearly dependent.

Then

$$\bar{a}_0 \bar{1} + \bar{a}_1 \theta + \bar{a}_2 \theta^2 + \dots + \overline{a_{n-1}}\, \theta^{n} = \bar{0}$$

for some $a_i \in F$ with not all $\bar{a}_i = \bar{0}$. $\leftarrow$ $\boxed{\bar{a}_i = \bar{0} \text{ iff } a_i = 0 \quad \bar{F} \text{ is isomorphic to } F}$

So,

$$(a_0 + a_1 x + \dots + a_{n-1} x^{n-1}) + I = 0 + I$$

where $a_i \in F$ and not all a_i are zero.

Then, $a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \in I$.

Then, $\underbrace{a_0 + a_1 x + \dots + a_{n-1} x^{n-1}}_{\boxed{\text{non-zero of degree} \leq n-1}} = p(x) f(x)$ where $f(x) \in F[x]$.

This can't happen since $\deg(p(x)) = n$.

Thus, $\bar{1}, \theta, \theta^2, \dots, \theta^{n-1}$ are linearly independent.

So, $\bar{1}, \theta, \theta^2, \dots, \theta^{n-1}$ is a basis for $K = F(x)/I$ over $\bar{F} \cong F$.

$\boxed{\text{QED}}$

I love this proof!