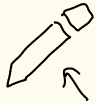
Math 5402

3/16/20

week 9

1. Test out chat box
   Test out un-muting and talking
   Test out annotate or  pencil

2. Canvas site
   for zoom stuff + class recordings

3. These notes I'll put
   on the website like normal

4. I graded the tests.
   I'm going to email
   them to you.

Theorem from last time

F is a field and $p(x) \in F[x]$ is non-constant & irreducible of degree n and let $K = F[x]/(p(x)) = F[x]/I$ where $I = (p(x))$. Then,

1. K is a field with a copy of F inside of K
2. $K = \{(a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}) + I \mid a_i \in F\}$
3. The elements $1 + I, x + I, x^2 + I, \dots, x^{n-1} + I$ form a basis for K over F.
4. $[K:F] = \deg_F(K) = n$

Note: Suppose we want to construct a finite field of size p^n where p is prime. Find an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree n. Then, letting $I = (f(x))$, then

$$K = \mathbb{Z}_p[x]/I = \{(a_0 + a_1 x + \dots + a_{n-1} x^{n-1}) + I \mid a_i \in \mathbb{Z}_p\}$$

The size of K is p^n.

Ex: Construct a finite field of size $4 = 2^2$.

$\boxed{\begin{array}{l} p=2 \\ n=2 \end{array}}$

Need irreducible poly in $\mathbb{Z}_2[x]$ of degree $n=2$.

Let $f(x) = x^2 + x + \bar{1}$

f is irreducible over $\mathbb{Z}_2$

Since $\deg(f) = 2$, we just need to show it has no roots in $\mathbb{Z}_2$.

$f(\bar{0}) = \bar{0}^2 + \bar{0} + \bar{1} = \bar{1} \neq \bar{0}$

$f(\bar{1}) = \bar{1}^2 + \bar{1} + \bar{1} = \bar{1} \neq \bar{0}$

So, f is irreducible over $\mathbb{Z}_2$.

In $\mathbb{Z}_2[x]$, let $I = (x^2 + x + \bar{1})$.

Let $K = \mathbb{Z}_2[x]/I$

$= \{\underbrace{(a_0 + a_1 x)}_{\text{go up to degree } n-1=1} + I \mid a_0, a_1 \in \mathbb{Z}_2\}$

$= \{\bar{0} + I, \bar{1} + I, x + I, (\bar{1} + x) + I\}$

$K = \{\bar{0}+I, \bar{1}+I, x+I, (\bar{1}+x)+I\}$

$I = (x^2+x+\bar{1})$

In particular, $(x^2+x+\bar{1})+I = \bar{0}+I$

So, $\boxed{x^2+I = (-x-\bar{1})+I = (x+\bar{1})+I}$ $(*)$

$-\bar{1} = \bar{1}$ in $\mathbb{Z}_2$

Example calculations:

$(x+I)+((\bar{1}+x)+I) = (\bar{1}+\bar{2}x)+I$

$= \bar{1}+I$

$\bar{2} = \bar{0}$

$[(\bar{1}+x)+I][(\bar{1}+x)+I] = (\bar{1}+\bar{2}x+x^2)+I$

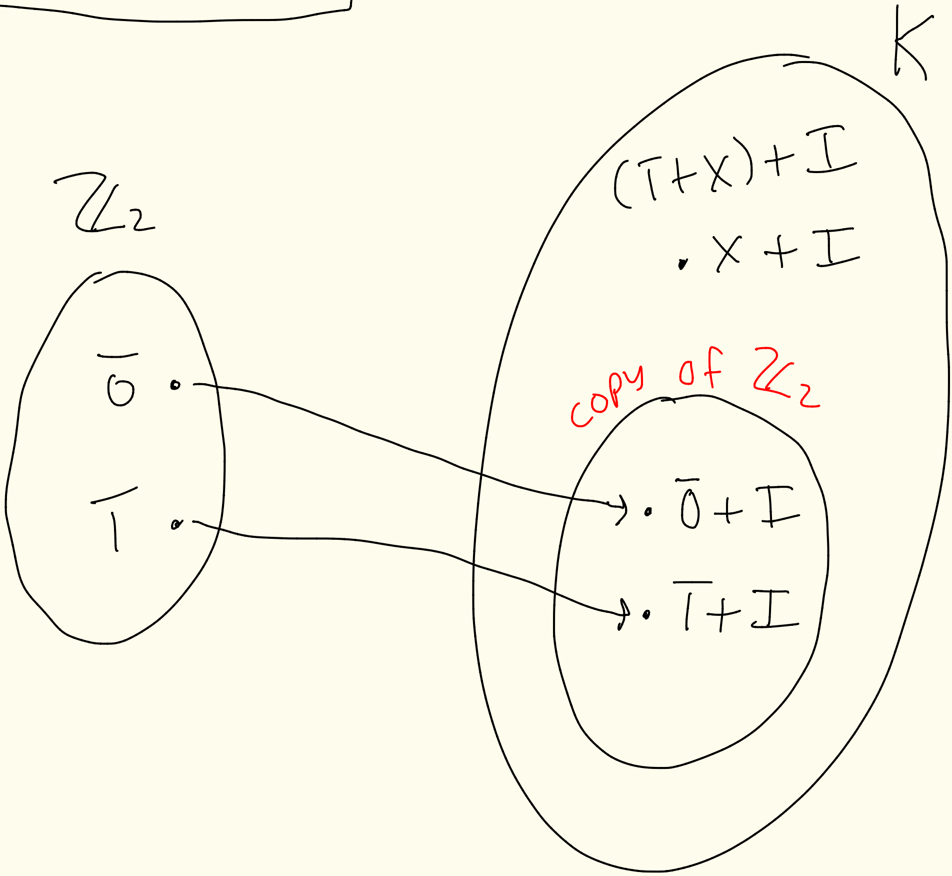
$= (\bar{1}+x^2)+I \underset{(*)}{=} (\bar{1}+x+\bar{1})+I$

$\bar{2} = \bar{0}$

$= x+I$

$K = \mathbb{Z}_2[x] / I \qquad I = (x^2 + x + 1)$

pg 4'



$x + I$ is a root of

$$p(t) = \underbrace{t^2 + t + (\bar{1} + I)}_{\text{here you can plug elements of } K \text{ into } p(t)}$$

<u>Ex</u>: Consider $p(x) = x^2 - 2$ in $\mathbb{Q}[x]$.

$p(x)$ is irreducible over $\mathbb{Q}$ since its of degree 2 and the only roots of $p(x)$ are $\pm\sqrt{2} \notin \mathbb{Q}$.

[You can also use Eisenstein's criteria.]

Let $I = (x^2 - 2)$ in $\mathbb{Q}[x]$.

Let $K = \mathbb{Q}[x]/I$.

Then $K = \{(a_0 + a_1 x) + I \mid a_0, a_1 \in \mathbb{Q}\}$

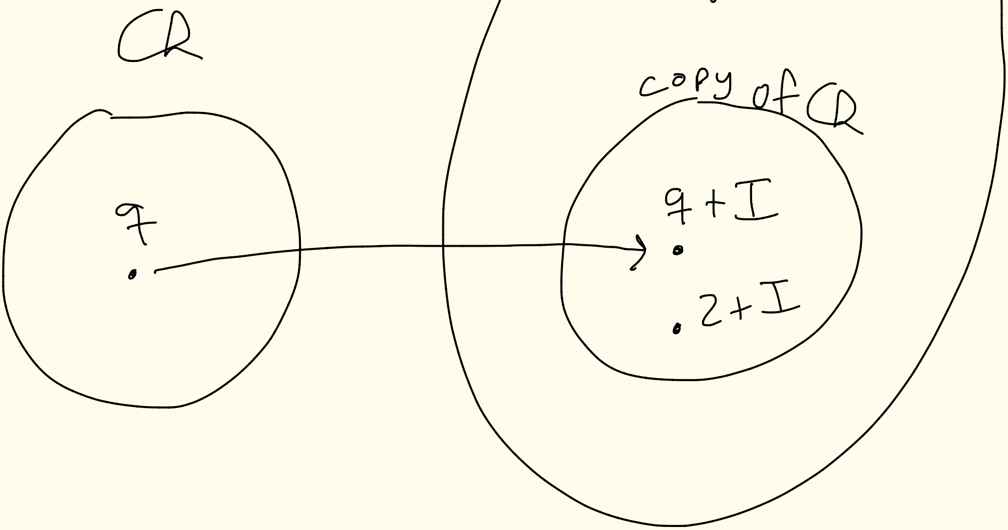
Also, $(x^2 - 2) + I = 0 + I$.

So, $x^2 + I = 2 + I$.

So, $x + I$ acts like "$\sqrt{2}$".

$x+I$ is a root of $p(t) = \underbrace{t^2-(2+I)}_{\boxed{t^2-2 \text{ moved into } K}}$

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



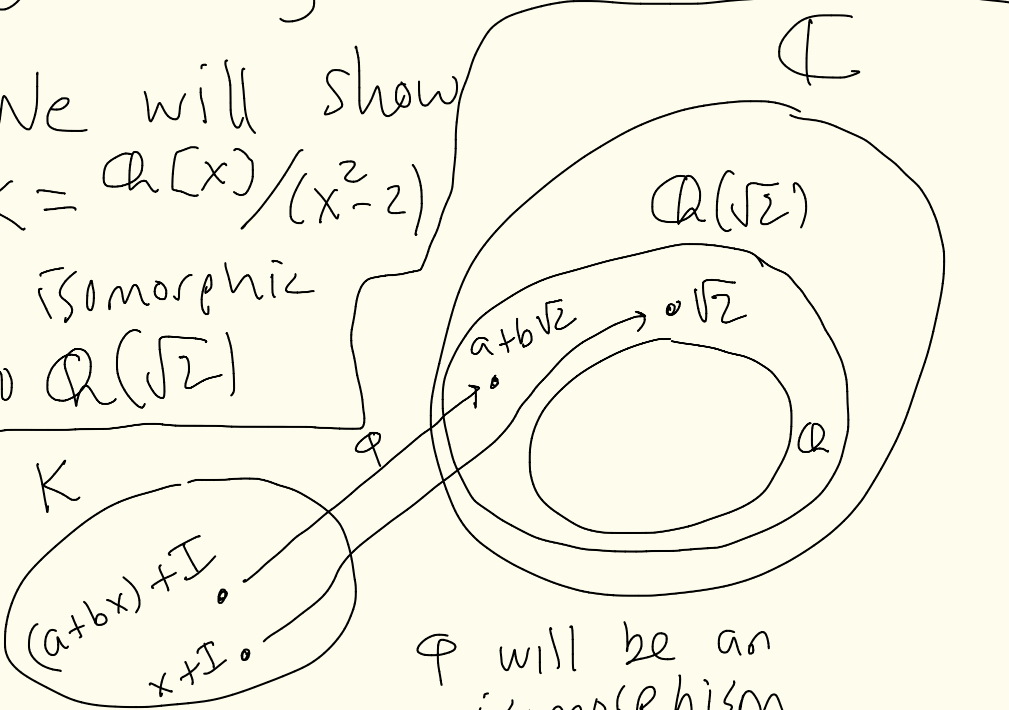
$$(x+I)^2 = x^2+I = 2+I$$

$$(-x+I)^2 = x^2+I = 2+I$$

Next time we will define $\underbrace{\mathbb{Q}(\sqrt{2})}_{\mathbb{Q} \text{ adjoin } \sqrt{2}}$

to be the smallest field containing $\mathbb{Q}$ and $\sqrt{2}$.

We will show $K = \mathbb{Q}[x]/(x^2-2)$ is isomorphic to $\mathbb{Q}(\sqrt{2})$



φ will be an isomorphism