Theorem:

Let F be a field and $p(x) \in F[x]$ be a nonconstant irreducible polynomial

Let $n = \deg(P[x])$. Let $I = \langle P(x) \rangle$

Then $F[x]/I = \{(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) + I \mid a_0, a_1, \ldots, a_{n-1} \in F\}$

moreover if

$(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) + I = (b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}) + I$

then $a_0 = b_0,\ a_1 = b_1, \ldots, a_{n-1} = b_{n-1}$.

Proof: Let $f(x) + I \in F[x]/I$ where $f(x) \in F[x]$

By the division algorithm we can find $q(x), r(x) \in F[x]$

where $f(x) = q(x)\,p(x) + r(x)$

and either $\underline{r(x) = 0}$ or $\underline{\deg(r) < \deg(P) = n}$

so, $f(x) - r(x) = q(x)\,p(x) \in I$

Then $f(x) + I = \underbrace{r(x)}_{\deg < n} + I$

so, $f(x) + I$ can be written in the form

$$\underbrace{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}}_{r(x)} + I$$

suppose $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + I = b_0 + b_1 x + \cdots b_{n-1}x^{n-1} + I$

so $(a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1} + I = \underbrace{0 + I}_{I}$

Let $h(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1}$

Then $h(x) \in I$

so, $\underbrace{h(x)}_{\text{degree} \le n-1} = \underbrace{P(x)}_{\text{degree} = n} z(x)$ where $z(x) \in F[x]$

This can only happen when $z(x)$ is the zero polynomial.

$I = \langle P(x) \rangle$

$n = \deg(P)$

$a + I = b + I$ iff $a - b \in I$

so, $h(x)$ is the zero polynomial

Thus $(a_0-b_0)+(a_1-b_1)x+\cdots+(a_{n-1}-b_{n-1})x^{n-1}=0$

so $a_0-b_0=0, \ldots, a_{n-1}-b_{n-1}=0$

so $a_0=b_0, \ldots, a_{n-1}=b_{n-1}$ $\blacksquare$

Ex: $F[x]=\mathbb{Z}_3[x]$, $P(x)=x^2+\bar{1}$, $I=\langle x^2+\bar{1}\rangle$

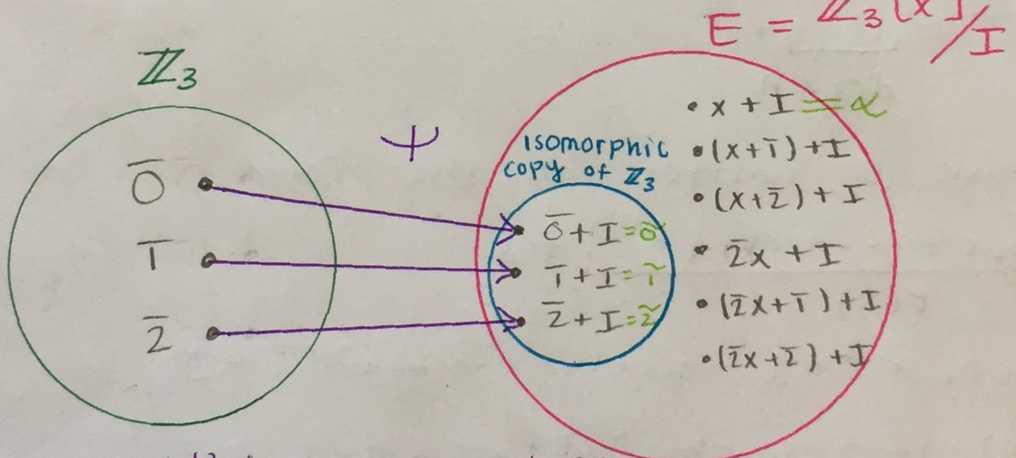
$E=\mathbb{Z}_3[x]/I=\{\bar{0}+I, \bar{1}+I, \bar{2}+I, x+I, (x+\bar{1})+I,$
$(x+\bar{2})+I, \bar{2}x+I, (\bar{2}x+\bar{1})+I, (\bar{2}x+\bar{2})+I\}$
$=\{(a_0+a_1x)+I \mid a_0,a_1\in\mathbb{Z}_3\}$

E is a field because p(X) is irreducible and non constant

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

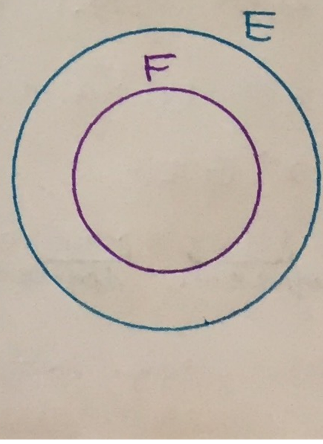
$x^2+I=-\bar{1}+I=\bar{2}+I$

we can think of $\mathbb{Z}_3$ as living inside of E. That is, there is an isomorphic copy of $\mathbb{Z}_3$ inside of E. Here is how you get it.



ψ is an isomorphism

Def: Let E and F be fields with $F\subseteq E$ then we say that E is an extension field of F



P.2 4/27

In $\mathbb{Z}_3$, $P(x) = x^2 + \bar{1}$ has no root

Move $P(x)$ to $\tilde{p}(t) = t^2 + \tilde{1} \in E[t]$ in the E land

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

$= \underbrace{(x^2+\bar{1})}_{P(x)} + I = \bar{0} + I = \tilde{0}$

$P(x) \in I$

So, E has an element whose square is $-\bar{1} + I$

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

$= (\bar{4}x^2 + I) + (\bar{1}+I)$

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

α and β both solve $t^2 + \tilde{1} = 0$

$t^2 + \tilde{1} = (t-\alpha)(t-\beta)$

$\Rightarrow (t-\alpha)(t-\beta) = (t-(x+I))(t-(\bar{2}x+I))$

$= t^2 + (\underbrace{(x+\bar{2}x)}_{\bar{3}x=\bar{0}} + I)t + \underbrace{(\bar{2}x^2+I)}$

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

$= (\bar{2}+I)(\bar{2}+I) = \bar{4} + I$

$= \bar{1} + I$

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

$= \bar{2} + I$

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

$= t^2 + \tilde{1}$

Lemma:

Let F be a field and let $I = \langle p(x) \rangle$ where $p(x)$ is not a constant, ie $\deg(p) \geq 1$

The function $\psi : F \to F[x]/I$

given by $\psi(c) = c + I$

is an isomorphism between F and $\tilde{F} = \mathrm{im}(\psi) = \{ c + I \mid c \in F \}$