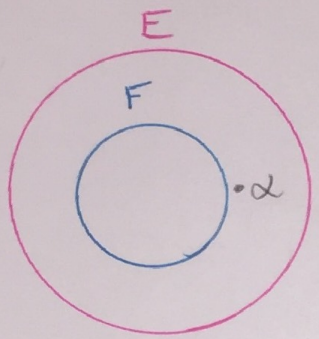
Kronecker's Theorem

Let F be a field and let $p(x) \in F[x]$ be a nonconstant irreducible polynomial over F. Then there exists an extension field E of F and $\alpha \in E$ with $p(\alpha) = 0$.



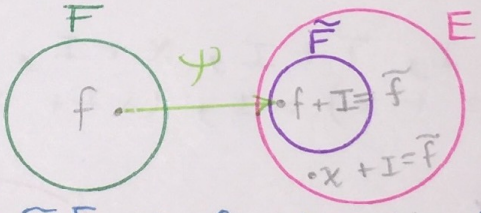
Note: If $p(c) = 0$ where $c \in F$, then p would be reducible over F

Proof: by division alg., if $p(c) = 0$ with $c \in F$, then $p(x) = (x-c)q(x) + r(x)$ with $q(x), r(x) \in F[x]$ and $r(x) =$ const. poly.
Then $0 = p(c) = (c-c)q(c) + r(x) = r(x)$
so, $r(x)$ is the zero poly. since its constant.
so, $p(x) = (x-c)q(x)$ where $q(x) \in F[x]$ ☑

Proof: Let $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$
Let $I = \langle p(x) \rangle$
Let $E = F[x]/I$

E is a field since p is nonconstant and irreducible
Let $\tilde{F} = \{f + I \mid f \in F\}$

* write $\tilde{f}$ for $f + I$ and $\tilde{x}$ for $x + I$



$\tilde{F} \cong F$ as fields via the isomorphism

$\psi: F \to \tilde{F}$ given by $\psi(f) = f + I$

Move p over to the land of E.
Let $\tilde{p}(t) = \tilde{a}_0 + \tilde{a}_1t + \cdots + \tilde{a}_nt^n \in \tilde{F}[t]$
we now show that $\tilde{x}$ is a root of $\tilde{p}(t)$
we have that

$$\tilde{p}(\tilde{x}) = \tilde{a}_0 + \tilde{a}_1\tilde{x} + a_2\tilde{x}^2 + \cdots + \tilde{a}_n x^n$$
$$= (a_0+I) + (a_1+I)(x+I) + (a_2+I)\underbrace{(x+I)^2}_{x^2+I} + \cdots + (a_n+I)\underbrace{(x+I)^n}_{x^n+I}$$
$$= \underbrace{(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)}_{p(x) \in I} + I = 0 + I = \tilde{0}.$$

☑

Ex: Let's make a finite field of size $8 = 2^3$

we need an irreducible poly in $\mathbb{Z}_2[x]$ of degree 3.

Consider $f(x) = x^3 + x + \bar{1}$

since $\deg(f) \leq 3$, we can test if f has roots in $\mathbb{Z}_2$ to see if it's irreducible or not

$$f(\bar{0}) = \bar{0}^3 + \bar{0} + \bar{1} = \bar{1} \neq \bar{0}$$
$$f(\bar{1}) = \bar{1}^3 + \bar{1} + \bar{1} = \bar{1} \neq \bar{0}$$

f has no roots in $\mathbb{Z}_3$ since $\deg(f) \leq 3$ we know that f is irreducible

$\mathbb{Z}_p$ is a finite field of size p when p is prime (1)

Finite Field Recipe (2)

How to make a finite field of size p^n where p is prime, $n \geq 2$

- Find an irreducible poly $f(x) \in \mathbb{Z}_p[x]$ of degree n
- Let $E = \mathbb{Z}_p[x] / \langle f(x) \rangle$
- Then $|E| = p^n$ and E is a field

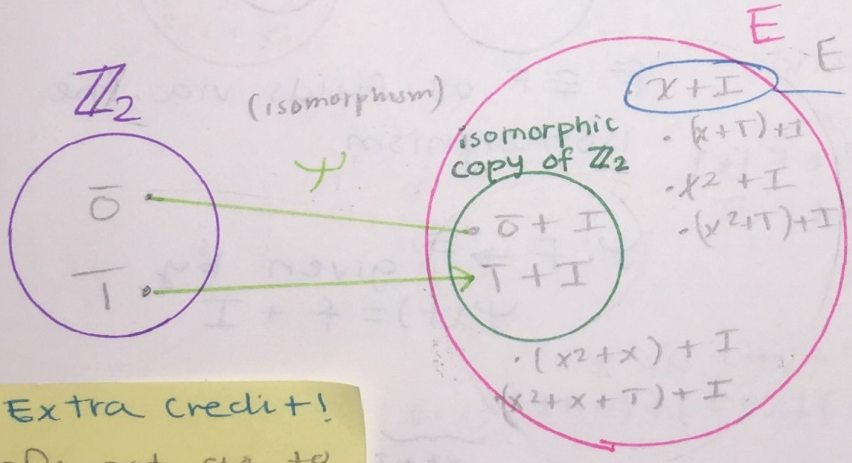
since $f(x) = x^3 + x + \bar{1}$ is irreducible over $\mathbb{Z}_2$, then $I = \langle x^3 + x + \bar{1} \rangle$ is maximal in $\mathbb{Z}_2[x]$

so $E = \mathbb{Z}_2[x]/I$ is a field.

and

$$E = \{(a_0 + a_1 x + a_2 x^2) + I \mid a_0, a_1, a_2 \in \mathbb{Z}_2\}$$

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



$x + I = \alpha$ (from Kroneckers thm) i.e. α solves

$$\tilde{f}(t) = t^3 + t + \tilde{1}$$

$\tilde{1} = \bar{1} + I$

$$\tilde{f}(t) = (t - \alpha)(\text{quadratic in } E(t))$$

Extra credit!

- Do not go to the event mentioned in class! ☺

How to calculate in E

$f(x) = x^3 + x + \bar{1}$, $I = \langle f(x) \rangle$

so $(x^3 + x + \bar{1}) + I = 0 + I$ ← just keep the highest power on the left side

so, $x^3 + I = (-x - \bar{1}) + I$

$\Rightarrow x^3 + I = (x + \bar{1}) + I$

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

Example: (calculations)

$[(\bar{1} + x) + I][(x + x^2) + I]$ } these two are inverses of eachother since their product $= \bar{1} + I$

$= (x + x^2 + x^2 + x^3) + I$

↙ $\bar{0}$

$= (x + \bar{2}x^2 + x^3) + I$

↑ $x^3 + I = (x + \bar{1}) + I$

$= (x + x + \bar{1}) + I = \bar{1} + I$ ← mult. identity in E

$2x = \bar{0}$

Thursday Week 14 May 4, 2017

May the fourth be With you.

Theorem: (Eisenstein Criterion)

Let p be a prime in $\mathbb{Z}$

Suppose that

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$ and $a_n \neq 0$

Suppose further

(1) p does not divide a_n

(2) p divides a_i for $i = 0, 1, 2, \ldots, n-1$ and

(3) p^2 does not divide a_0

Then $f(x)$ is irreducible over $\mathbb{Q}$

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

$p \nmid a_n$ $\quad p \mid a_{n-1}$ $\quad p \mid a_{n-2}$ $\quad p \mid a_1$ $\quad p \mid a_0$ $\quad p^2 \nmid a_0$

Ex: Let $f(x) = 7x^{100} + 9x^5 + 15x^2 + 12$ $\leftarrow 3^2 \nmid 12$

$p = 3$ $\quad 3 \nmid 7$ $\quad 3 \mid 9$ $\quad 3 \mid 15$ $\quad 3 \mid 12$

By Eisenstein, f is irreducible over $\mathbb{Q}$

Ex: (constructing $\mathbb{C}$ from $\mathbb{R}$)

Let $f(x) = x^2 + 1$

since f has no roots in $\mathbb{R}$ and $\deg(f) = 2$, we know that f is irreducible over $\mathbb{R}$.

{ * If $x^2 + 1 = 0$ then $x^2 = -1$ which can't happen for any $x \in \mathbb{R}$.

Let $I = \langle x^2 + 1 \rangle$ in $\mathbb{R}[x]$

Then I is maximal since $x^2 + 1$ is irreducible over $\mathbb{R}$ so, $E = \mathbb{R}[x]/I$ is a field.

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

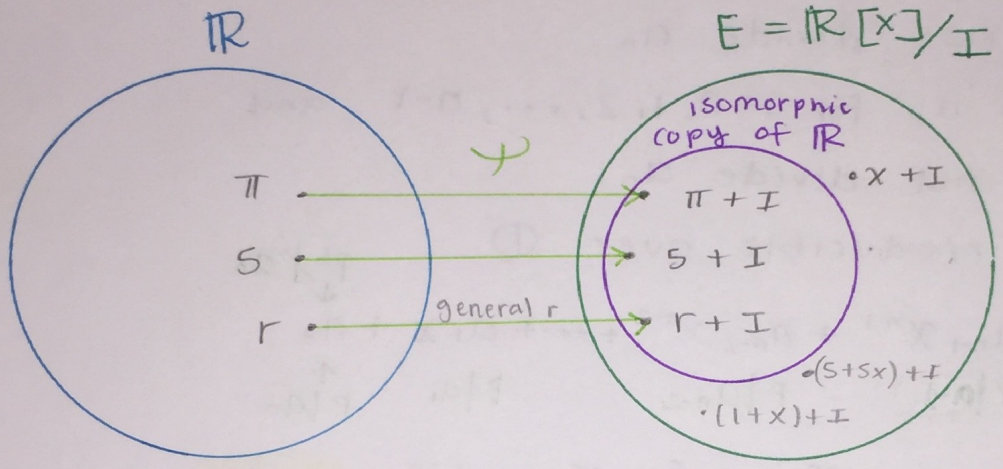
Also, $(x^2+1) + I = 0 + I$

$x^2 + 1 \in I$

so $x^2 + I = -1 + I$

so, $(x+I)^2 = -1 + I$

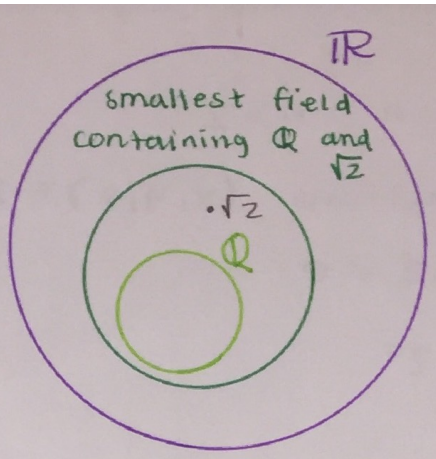
so $x + I$ acts like $i = \sqrt{-1}$



- ψ is an isomorphism between $\mathbb{R}$ and $im(\psi) = \psi(\mathbb{R})$ where $\psi(r) = r + I$
- E is isomorphic to $\mathbb{C}$

  $(a+bx) + I \longleftrightarrow a + bi$ (this is an isomorphism)

We will make this field



Ex: Let $f(x) = x^2 - 2$

$p = 2$ $\quad x^2 - 2$

$2 \nmid 1 \quad 2 \nmid (-2) \quad 2^2 \nmid (-2)$ } so, f is irreducible over $\mathbb{Q}$ by Eisenstein.

Let $I = \langle x^2 - 2 \rangle$

Then I is maximal in $\mathbb{Q}[x]$

so, $E = \mathbb{Q}[x]/I$ is a field.

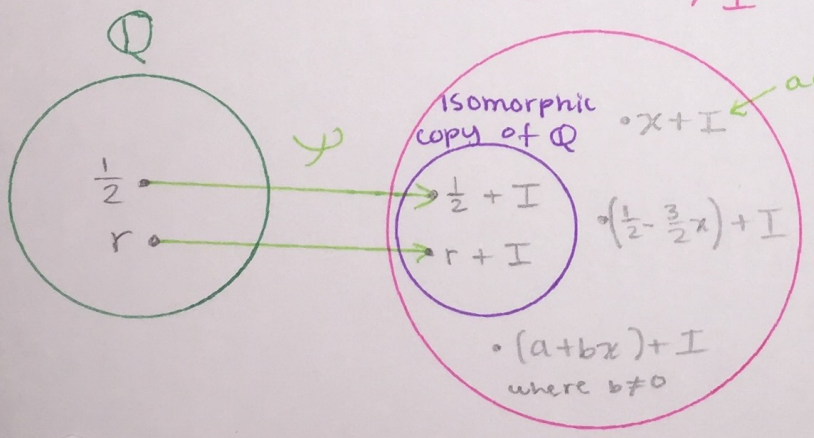
$$E = \{(a+bx) + I \mid a, b \in \mathbb{Q}\}$$

$(x^2-2) + I = 0 + I \rightarrow x^2 + I = 2 + I$

$x^2 - 2 \in I$

$(x+I)^2 = 2 + I$ ← so $x+I$ acts like $\sqrt{2}$

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



$\psi(r) = r + I$

$\psi : \mathbb{Q} \rightarrow E$

Simplification

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$

"$\mathbb{Q}$ adjoin $\sqrt{2}$"

E is isomorphic to $\mathbb{Q}(\sqrt{2})$

$E \longleftrightarrow \mathbb{Q}(\sqrt{2})$

$(a+bx)+I \longleftrightarrow a + b\sqrt{2}$

$x^n + y^n = z^n$, $n > 2$

has no solutions $(x, y, z) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$

where $xyz \neq 0$

$x^3 + y^3 = z^3$