We were proving:

**Theorem.** Suppose $F$ is a field and $f(x) \in F[x]$ is an irreducible polynomial. Then

1. \exists a field $E$ and an injective ring homomorphism $i : F \to E$ s.t.
   - (1-a) for some $\alpha \in E$, $i(f)(\alpha) = 0$.
     - ($f(x)$ has a zero in $E$.)
   - (1-b) $E = \mathbb{Q} \alpha + \mathbb{Q}(\alpha) \alpha + \ldots + \mathbb{Q}(\alpha) \alpha^{n-1}$ | $\alpha_0, ..., \alpha_{n-1} \in \mathbb{F}$

   where $n = \deg f$.

2. If $E'$ is a field and $i' : F \to E'$ is an injective ring homomorphism that satisfy (1-a) and (1-b),

   then $\exists \phi : E \cong E'$ s.t. $\phi(i(\alpha)) = i'(\alpha)$

   for any $\alpha \in F$.

And based on the discussion that we had, we will use $F[x]/\langle f(x) \rangle$. 
Proof of theorem (1) Since $f(x)$ is irreducible in $\mathbb{F}[x]$ and $\mathbb{F}[x]$ is a PID, $\langle f(x) \rangle$ is a maximal ideal. Hence $E := \mathbb{F}[x]/\langle f(x) \rangle$ is a field. Let $\iota: F \to \mathbb{F}[x]/\langle f(x) \rangle$, $\iota(c) = c + \langle f(x) \rangle$.

Clearly $\iota$ is a ring homomorphism.

Claim $\iota$ is injective.

Proof of claim. $\iota(c) = 0 \Rightarrow c + \langle f(x) \rangle = 0 + \langle f(x) \rangle$

$\Rightarrow c \in \langle f(x) \rangle$

Since $\langle f(x) \rangle$ is a proper ideal, $\langle f(x) \rangle \cap F = \{0\}$.
\[c = 0.\]

Let $\alpha := \chi + \langle f(x) \rangle$, and $\bar{f}(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0$.

Claim $\iota(\bar{f}) (\alpha) = 0$.

Proof of claim. $\iota(\bar{f}) (\alpha) = \iota(c_n) (\chi + I) + \iota(c_{n-1}) (\chi + I)^{n-1} + \ldots + \iota(c_0)$

$= (c_n + I) (\chi + I) + \ldots + (c_1 + I) (\chi + I) + C_0 + I$ (where $I = \langle f(x) \rangle$)

$= (c_n \chi^n + \ldots + c_1 \chi + C_0) + I = f(x) + I = 0 + I$.

By long division, for any polynomial $p(x)$, $\exists! q(x), r(x) \in \mathbb{F}[x], p(x) = f(x) q(x) + r(x)$ and $\deg r < \deg f = n$. 

\[ \Rightarrow \quad \rho(x) + I = \frac{\rho(x)q(x) + r(x)I}{\lambda^n I} \]

Since \( \deg r < n \), \( \exists! \quad a_0, \ldots, a_{n-1} \in F \) s.t.

\[ r(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \] ; and so

\[ \rho(x) + I = (a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}) + I \]

\[ = (a_0 + I) + (a_1 + I)(x + I) + \ldots + (a_{n-1} + I)(x + I)^{n-1} \]

\[ = i(a_0) + i(a_1) x + \ldots + i(a_{n-1}) x^{n-1}. \]

(2) Let \( \phi : F[x] \to E' \), \( \phi(x) = \rho(x) \). Then \( \rho(x) \in \ker \phi \). Since \( \rho(x) \) is irreducible, \( \ker \phi = \langle \rho(x) \rangle \). And so by the 1st isomorphism theorem, \( F[x]/\langle \rho(x) \rangle \cong \text{Im } \phi \).

\[ \rho(x) + \langle \rho(x) \rangle \mapsto \phi(x) \]

Since \( E' \) satisfies (1-b), \( \text{Im } \phi = E' \). This implies

\[ F[x]/\langle \rho(x) \rangle \cong E' \]

and claim follows. \( \blacksquare \)
Proposition. Suppose \( f(x) \in \mathbb{Z}_p[x] \) is an irreducible poly.
of degree \( n \). Then \( E := \mathbb{Z}_p[x]/\langle f(x) \rangle \) is a field of order \( p^n \).

\[ \text{Proof. Let } E := \mathbb{Z}_p[x]/\langle f(x) \rangle. \text{ Since } \mathbb{Z}_p[x] \text{ is a PID and } \langle f(x) \rangle \text{ is irr., } \langle f(x) \rangle \text{ is a maximal ideal of } \mathbb{Z}_p[x]. \]

Hence \( E := \mathbb{Z}_p[x]/\langle f(x) \rangle \) is a field.

Claim 1. \( E = \langle \sum a_i x^i, i \in \mathbb{Z}_p \rangle + \langle f(x) \rangle \mid a_i \in \mathbb{Z}_p \).

\[ \text{Proof of claim. Any element of } E \text{ is of the form } g(x) + \langle f(x) \rangle. \]

By long division, \( \exists g(x), r(x) \) st. \( g(x) = q(x)f(x) + r(x) \)
and \( \deg r < n. \) Hence \( g(x) + \langle f(x) \rangle = r(x) + q(x)f(x) + \langle f(x) \rangle \)
\[ = r(x) + \langle f(x) \rangle \in \text{RHS}. \]

Clearly \( \text{RHS} \subseteq \text{LHS} \) and claim follows.

Claim 2. \( (a_0, \ldots, a_{n-1}) \in \mathbb{Z}_p^n \mapsto (a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}) + \langle f(x) \rangle \)

is a bijection from \( \mathbb{Z}_p^n \) to \( E \).

\[ \text{Proof. The 1st claim implies } \theta \text{ is surjective. So it is enough to show } \theta \text{ is injective. Suppose } \theta(a_0, \ldots, a_{n-1}) = \theta(a_0', \ldots, a_{n-1}'). \]
Lecture 24: Finite fields

Friday, June 1, 2018 11:25 AM

\[ a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + \langle f(x) \rangle = a'_0 + a'_1 x + \cdots + a'_{n-1} x^{n-1} + \langle f(x) \rangle \]

And so \((a_0-a'_0) + (a_1-a'_1) x + \cdots + (a_{n-1}-a'_{n-1}) x^{n-1} = f(x) g(x)\)

\[ \Rightarrow \deg f + \deg g = \deg \text{ of LHS} < n \]

\[ \Rightarrow \deg g < 0 \Rightarrow \deg g = -\infty \quad \text{and} \quad g = 0 \]

\[ \Rightarrow \text{LHS} = 0 \quad \Rightarrow \quad a_0 = a'_0, \; a_1 = a'_1, \ldots, a_{n-1} = a'_{n-1}; \]

this implies \(\Theta\) is injective.

Hence \(|E| = |\mathbb{Z}_p^n| = p^n\).

**Warning.** \(E\) is **NOT** \(\mathbb{Z}_p^n\) as a ring. \(\mathbb{Z}_p^n\) has many zero-divisors if \(n > 1\), but \(E\) is a field.