In the previous lecture we proved:

**Theorem.** Let $F$ be a field, and $p(x)$ be an irreducible polynomial in $F[x]$. Then there are a field $E$, an embedding $F \to E$, and $\alpha \in E$ such that $i(p)(\alpha) = 0$.

**Ex.** Let $f_0(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree $d$. Then there is a field extension $F \supseteq \mathbb{Z}_p$ which has a zero of $f_0$ and $|F| = p^d$.

**Solution.** By the previous theorem, $\exists$ a field extension $E \supseteq \mathbb{Z}_p$ and $\alpha \in E$ such that $f_0(\alpha) = 0$.

Let $\phi_\alpha : \mathbb{Z}_p[x] \to E$ be the evaluation at $\alpha$. Then

1. $\exists m_\alpha(x) \in \mathbb{Z}_p[x]$ which is irreducible and $\ker \phi_\alpha = \langle m_\alpha(x) \rangle$;

2. $\text{Im } \phi_\alpha$ is a field;

3. $\text{Im } \phi_\alpha = \{ c_0 + c_1\alpha + \ldots + c_{d-1}\alpha^{d-1} | c_i \in \mathbb{Z}_p \}$ where $d = \deg m_\alpha$.

As $f_0(\alpha) = 0$, $f_0(x) \in \ker \phi_\alpha$. So $\langle f_0(x) \rangle \subseteq \langle m_\alpha(x) \rangle$. Since $f_0(x)$
is irreducible $\langle f_0(x) \rangle$ is a maximal ideal. Therefore

$$\langle f_0(x) \rangle = \langle m_\alpha(x) \rangle ;$$

and $\frac{f_0(x)}{m_\alpha(x)}$, $m_\alpha(x) | f_0(x)$. Thus $\deg f_0 = \deg m_\alpha$.

And so $F = \mathbb{Z}_p \cdot \alpha + \cdots + \mathbb{Z}_p \cdot \alpha^{d-1} | c_i \in \mathbb{Z}_p$ is a field.

$$\begin{array}{c}
\text{Claim: } \mathbb{Z}_p^d \rightarrow F, (c_0, \ldots, c_{d-1}) \mapsto c_0 + c_1 \alpha + \cdots + c_{d-1} \alpha^{d-1} \\
\text{is a bijection.}
\end{array}$$

\underline{Proof of claim.} We already know that $l$ is surjective.

\underline{Why is it injective?}

$$l(c_0, \ldots, c_{d-1}) = l(c'_0, \ldots, c'_{d-1})$$

$$\Rightarrow c_0 + c_1 \alpha + \cdots + c_{d-1} \alpha^{d-1} = c'_0 + c'_1 \alpha + \cdots + c'_{d-1} \alpha^{d-1}$$

$$\Rightarrow (c_0 - c'_0) + (c_1 - c'_1) \alpha + \cdots + (c_{d-1} - c'_{d-1}) \alpha^{d-1} = 0$$

$$\Rightarrow (c_0 - c'_0) + (c_1 - c'_1) \alpha + \cdots + (c_{d-1} - c'_{d-1}) \alpha^{d-1} \in \ker \phi_d = \langle m_\alpha(x) \rangle$$

$$\Rightarrow m_\alpha(x) q(x) = (c_0 - c'_0) + (c_1 - c'_1) \alpha + \cdots + (c_{d-1} - c'_{d-1}) \alpha^{d-1}$$

for some $q(x) \in \mathbb{Z}_p [x]$.

$$\Rightarrow \deg m_\alpha + \deg q = \deg ((c_0 - c'_0) + \cdots + (c_{d-1} - c'_{d-1}) \alpha^{d-1})$$
So \( q(x) = 0 \); and so \((c_0 - c'_0) + (c_1 - c'_1) x + \ldots + (c_{d-1} - c'_{d-1}) x^{d-1} = 0\),

which implies \( c_0 = c'_0, \ c_1 = c'_1, \ldots, \) and \( c_{d-1} = c'_{d-1} \). And so

\[
(c_0, c_1, \ldots, c_{d-1}) = (c'_0, c'_1, \ldots, c'_{d-1}),
\]

which means \( \ell \) is injective.

Therefore \( |F| = |\mathbb{Z}_p^d| = p^d \).

**Ex. @** Show that \( x^3 - x + 1 \) is irreducible in \( \mathbb{Z}_3[x] \).

(1) Show that there is a field \( F \) such that \( |F| = 27 \).

**Solution.** @ A degree 3 polynomial in \( \mathbb{Z}_3[x] \) is irreducible if and only if it has no zero in \( \mathbb{Z}_3 \).

For \( a \in \mathbb{Z}_3 \), by Fermat's theorem, \( a^3 - a + 1 = a - a + 1 = 1 \).

So \( x^3 - x + 1 \) does not have a zero in \( \mathbb{Z}_3 \). And so \( x^3 - x + 1 \) is irreducible in \( \mathbb{Z}_3[x] \).

(1) By the previous example, there is a field \( F \) of order \( 3^{3} = 27 \).
Ex. Let $f(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree $d > 1$.

Suppose $\alpha$ is a zero of $f(x)$ in a field extension $E$ of $\mathbb{Z}_p$.

Then $\alpha^{(p^d)} = \alpha$.

Pf. By the previous examples we know $F = \mathbb{Z}_p[x]$ is a field of order $p^d$. So $\alpha \in U(F) = F^\times \setminus \{0\}$.

$U(F)$ is a group of order $p^d - 1$. So by Lagrange theorem $|U(F)| = 1$, which implies $\alpha^{(p^d-1)} = 1$; and therefore $\alpha^{(p^d)} = \alpha$. $\blacksquare$