In the previous lecture we proved:

**Theorem.** If \( f(x) \in \mathbb{Z}_p[x] \) is irreducible of degree \( n \), then \( E := \mathbb{Z}_p[x] / \langle f(x) \rangle \) is a field of order \( p^n \).

An important property of a finite field of order \( p^n \) is the following:

**Lemma.** Suppose \( E \) is a field and \( |E| = q \). Then

\[
\forall \alpha \in E, \quad \alpha^q = \alpha.
\]

**Proof.** If \( \alpha = 0 \), then \( \alpha^q = 0 = \alpha \). If \( \alpha \neq 0 \), then \( \alpha \in U(E) \).

By Lagrange's theorem \( |U(E)| = q-1 \); and so \( \alpha^{q-1} = 1 \Rightarrow \alpha^q = \alpha \). 

**Theorem.** Suppose \( E \) is a finite field and \( |E| = q \). Then

\[
\prod_{\alpha \in E} (x - \alpha) = x^q - x.
\]

**Proof.** By the previous lemma, \( \forall \alpha \in E \) is a zero of \( x^q - x \). And so \( \exists g(x) \in \mathbb{Z}_p[x], \quad x^q - x = g(x) \prod_{\alpha \in E} (x - \alpha) \).

Comparing degrees we get \( q = \deg g + |E| = \deg g + q \).
And so \( \deg g = 0 \). This means \( g(x) = c \in \mathbb{E} \setminus \mathbb{F} \).

Comparing the leading coefficients, we deduce that \( c = 1 \) and the claim follows.

We will come back to this theorem later. For now let's go back to zeros of polynomials. So far we have found a field extension that contains a zero of an irreducible polynomial. Can we find a field extension that contains all the zeros of an arbitrary positive degree polynomial?

**Def.** Suppose \( \mathbb{F} \) is a field, \( f(x) \in \mathbb{F}[x] \) has positive degree; \( \mathbb{E} \) is called a splitting field of \( f \) over \( \mathbb{F} \) if

1. \( \mathbb{E} \) is a field, \( \mathbb{E} \supseteq \mathbb{F} \); that means \( i \) is an injective ring homomorphism.

2. \( \exists \alpha_1, \ldots, \alpha_n \in \mathbb{E} \), \( f(x) = c (x-\alpha_1) \cdots (x-\alpha_n) \) \( c \in \mathbb{E} \)

3. \( \mathbb{E} \) is the smallest field that contains \( i(\mathbb{F}) \) and \( \alpha_1, \ldots, \alpha_n \).
Ex. \( \mathbb{Q} \sqrt{2} \) is a splitting field of \( x^2 - 2 \) over \( \mathbb{Q} \).

Solution. \( \mathbb{Q} \leftarrow \mathbb{Q} \sqrt{2} \) 
\[ a \rightarrow a \]

\[ x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}) \]

If a ring contains \( \mathbb{Q} \) as a subring and \( \sqrt{2} \), then
\[
\forall a, b \in \mathbb{Q}, \ a + b\sqrt{2} \text{ is in that ring. Hence } \mathbb{Q} \sqrt{2} \text{ is the smallest subring of } \mathbb{Q} \sqrt{2} \text{ that contains } \mathbb{Q} \text{ and } \sqrt{2}.
\]

Ex. Find a splitting field of \( x^3 - 2 \) over \( \mathbb{Q} \).

Solution. A splitting field \( E \) of \( x^3 - 2 \) over \( \mathbb{Q} \) contains zeros of \( x^3 - 2 \). Let's start with finding zeros of this polynomial in \( \mathbb{C} \).

If a complex number \( z \) is a zero of \( x^3 - 2 \), then
\[ z^3 = 2. \]
Using polar coordinates and Euler's formula, we have
\[ z = r e^{i\theta} \text{ where } r = |z| \text{ and } \theta = \arg(z). \]
Hence
\[
(r e^{i\theta})^3 = 2 \text{ implies } r^3 = 2 \text{ and } e^{3i\theta} = 1. \text{ And so } r = \sqrt[3]{2} \text{ and } 3\theta = 2k\pi \text{ for some } k \in \mathbb{Z}. \text{ Hence }
\]

\[
\cos \theta = \frac{\sqrt[3]{2}}{2} \quad \text{and} \quad \sin \theta = \frac{\sqrt[3]{2}}{2}.
\]
Recall from complex numbers:

If \( z \in \mathbb{C} \) and \( z^n = 1 \), then \( |z^n| = 1 \) implies \( |z| = 1 \). And so \( z \) is on the unit circle. If the argument of \( z \) is \( \theta \), then multiplying \( z \) is just rotation by angle \( \theta \) about the origin. So \( z^n = 1 \) means after \( n \) times rotation we get back to 1. Therefore \( n \theta = 2k \pi \) for some \( k \in \mathbb{Z} \). Hence we get \( n \) possible values \( 1, \zeta, \zeta^2, \ldots, \zeta^{n-1} \) where \( \zeta = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right) \).

And so \( y^n - 1 = (y - 1)(y - \zeta)(y - \zeta^2) \ldots (y - \zeta^{n-1}) \).

Hence \( 3\sqrt{2}, 3\sqrt{2} \zeta, 3\sqrt{2} \zeta^2 \) are zeros of \( x^3 - 2 \) where \( \zeta = e^{\frac{2\pi i}{3}} = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i \frac{\sqrt{3}}{2} \). So a splitting field of \( x^3 - 2 \) over \( \mathbb{Q} \) is \( \mathbb{Q}[3\sqrt{2}, 3\sqrt{2} \zeta, 3\sqrt{2} \zeta^2] \) which is the smallest subfield of \( \mathbb{C} \) that contains \( \mathbb{Q}, 3\sqrt{2}, 3\sqrt{2} \zeta, \) and \( 3\sqrt{2} \zeta^2 \). Then \( \zeta = 3\sqrt{2} \zeta/3\sqrt{2} \) is in this field; and so
\[ \zeta \in \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[3]{2} \zeta^2]. \] Hence \( \mathbb{Q}[\sqrt{2}, \zeta] \subseteq \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2} \zeta, \sqrt[3]{2} \zeta^2]. \)

Clearly \( \sqrt{2}, \sqrt[3]{2}, \sqrt[3]{2} \zeta^2 \in \mathbb{Q}([\sqrt{2}, \zeta]). \) So \( \mathbb{Q}([\sqrt{2}, \zeta]) \) is a splitting field of \( x^3 - 2 \) over \( \mathbb{Q}. \)

**Theorem.** Suppose \( F \) is a field and \( f(x) \in F[x] \) has positive degree. Then \( f(x) \) has a splitting field over \( F. \)

**Proof.** We proceed by induction on \( \deg(f). \)

**Base.** If \( \deg(f) = 1, \) then \( f(x) = a_1 x + a_0 \) and \( a_1 \in F \setminus \{0\}. \)

Hence \( f(x) = a_1 (x + a_0/a_1), \) \( a_0 \neq 0 \in F; \) and so \( F \) is a splitting field of \( f(x) \) over \( F. \)

**Induction Step.** \( F[x] \) is a UFD. So \( f(x) = \prod_{i=1}^{m} p_i(x) \) where \( p_i(x) \) is irreducible in \( F[x]. \) Hence \( \exists F \xrightarrow{\iota} \overline{F} \) and \( \alpha \in \overline{F} \) s.t. \( \iota(p_1)(\alpha) = 0. \) (Hence \( \iota(f)(\alpha) = 0 \)) and \( \overline{F} \) is the smallest ring that contains \( \alpha \) and \( \iota(F). \) Therefore by the factor theorem, \( \exists \overline{f}(x) \in \overline{F}[x] \) s.t. \( \deg \overline{f} = \deg f - 1 \) and \( \overline{f}(x) = (x-\alpha) \overline{f}(x). \) Now by the induction hypothesis,
We go over this part of argument in the next lecture.

Hence it should be $E$ and claim follows.

And so it contains $\bar{i}(\bar{f}(F))$ and $\bar{i}(a)$.

A subfield of $E$ that contains $\bar{i}(\bar{f}(F))$ and $\bar{i}(a)$.

Consider, $\bar{i}$ induces $\bar{i}$ in $\bar{E}$.

The smallest subfield of $E$ that contains $\bar{i}(\bar{f}(F))$ and $a_1, \ldots, a_n$. For some $c \in \bar{F}$.

If a field $E$ and $\bar{i}$ isomorphic over $\bar{F}$, that means $\bar{i}(\bar{f}(F)) = \bar{c}$. 

$E$ has a splitting field over $\bar{F}$, that means $\bar{f}(F) = (x-a_1) \cdots (x-a_n)$ for some $c \in \bar{F}$.