Last time:

Thm Let $F$ be a field and $f(x) \in F[x]$ of deg $\geq 1$. Then there is an extension field $E$ of $F$ in which $f(x)$ has a 0.

Def: Suppose $E$ and $F$ is an extension of fields, $f(x) \in F[x]$ has $\deg (f) \geq 1$. We say that $f(x)$ splits in $E$ if there are elements $a \in F$ and $a_1, \ldots, a_n \in E$ such that

$$f(x) = a(x-a_1)(x-a_2)\cdots(x-a_n)$$

in $E[x]$. We call $E$ a splitting field for $f(x)$ over $F$ if $E = F(a_1, \ldots, a_n)$.

Recall: If $F \subseteq E$ are fields, and $a_1, \ldots, a_n \in E$, $F(a_1, \ldots, a_n)$ denotes the smallest subfield of $E$ containing $F$ and $a_1, \ldots, a_n$. It is equal to the intersection of every subfield of $E$ that contains $F$ and $a_1, \ldots, a_n$.

Note that: If $C \subseteq E$, and $C$ contains $F$, $a_1, \ldots, a_n$, then
Note that: If \( C \subseteq E \), and \( C \) contains \( F \), \( a_1, \ldots, a_n \), then
\[
F(a_1, \ldots, a_n) \subseteq C.
\]

Then let \( F \) be a field, \( f(x) \in F[x] \) non-constant. Then there exists a splitting field \( E \) for \( f(x) \) over \( F \).

**Pf:** If \( \deg(f) = 1 \), then \( E = F \) splits \( f(x) \).

So, suppose \( \deg(f) > 1 \); we'll proceed by induction.

By Theorem, \( \exists \) an extension field \( L \) of \( F \) so that \( f \) has a zero in \( L \).

\[
\implies f(x) = (x-a_1)g(x) \in L[x]
\]

Since \( \deg(g) < \deg(f) \), \( \exists \) a field \( K \) containing \( L \) that splits \( g \).

\[
\implies f(x) = a_1(x-a_2) \cdots (x-a_n) \in K[x],
\]

with \( a_1 \in F \), \( a_2, a_3, \ldots, a_n \in K \).

Now, \( F(a_1, \ldots, a_n) \subseteq K \) is a splitting field of \( f \).

Note: \( F \subseteq L \subseteq K \)

\[
\uparrow
\]

\[
f \text{ has a zero } a_1,
\]

\[
g(x) \text{ splits in } K, \text{ where}
\]
Lemma  Suppose \( F \) is a field, \( E \supseteq F \), \( a_1, \ldots, a_n \in E \).

Then \( F(a_1, \ldots, a_n) = F(a_1, \ldots, a_{n-1})(a_n) \).

\textbf{Pf:} The LHS, i.e., \( F(a_1, \ldots, a_n) \), is the intersection of all subfields of \( E \) containing \( F \) and \( a_1, \ldots, a_n \). The RHS, i.e., \( F(a_1, \ldots, a_{n-1})(a_n) \), is one such field, so

\[ F(a_1, \ldots, a_n) \subseteq F(a_1, \ldots, a_{n-1})(a_n). \]

Conversely, by definition, \( F(a_1, \ldots, a_{n-1}) \subseteq F(a_1, \ldots, a_n) \).

Moreover, \( a_n \in F(a_1, \ldots, a_{n-1}) \). Thus

\[ F(a_1, \ldots, a_{n-1})(a_n) \subseteq F(a_1, \ldots, a_n). \]

Example  \( f(x) = x^4 - x^2 - 2 = (x^2-2)(x^2+1) \in \mathbb{Q}[x]. \)

A splitting field for \( f \) is

\( \mathbb{Q}(\sqrt{2}, i) \subseteq \mathbb{C} \) because

\[ (x^2-2)(x^2+1) = (x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i) \in \mathbb{C}[x]. \]

Additionally, \( \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})((i) = \{ \alpha + \beta i : \alpha, \beta \in \mathbb{Q}(\sqrt{2}) \}) \).
\[ \sum (a+bi+ci+di) \in \mathbb{C} \]

**Example** \( f(x) = x^2 + x + 2 \) in \( \mathbb{Z}/3\mathbb{Z}[x] \).

Let \( E = \mathbb{Z}/3\mathbb{Z}[x] / \langle x^2 + x + 2 \rangle \), and let \( \beta \in E \) denote the image of \( \alpha \).

- \( E \) is a field because \( x^2 + x + 2 \in \mathbb{Z}/3\mathbb{Z}[x] \) is irreducible.
- We claim that \( E \) is a splitting field for \( x^2 + x + 2 \).

By definition of \( \beta \), \( \beta^2 + \beta + 2 = 0 \) in \( E \).

\[ \Rightarrow \quad x^2 + x + 2 = (x - \beta) q(x) \quad \text{in} \quad E[x]. \]

To find \( q(x) \), use long division, obtain

\[ x^2 + x + 2 = (x - \beta)(x + \beta^2 + 1) \quad \text{in} \quad E[x]. \]

\[ \Rightarrow \quad E \text{ splits } x^2 + x + 2 \]

Moreover, \( E \) is a splitting field for \( x^2 + x + 2 \) over \( \mathbb{Z}/3\mathbb{Z} \) because \( \mathbb{Z}/3\mathbb{Z}(\beta) \subseteq E \) is all of \( E \).

This latter equality holds because every elt of \( E \) is of the form \( c_0 + c_1 \beta \) for some \( c_0, c_1 \in \mathbb{Z}/3\mathbb{Z} \).

**Recall:** If \( F \) is a field, \( f(x) \in F[x] \) degree \( n \), then every element of \( F[x]/f(x) \) is uniquely expressible in the
every element of \( \mathbb{F}(x) / \langle f(x) \rangle \) is uniquely expressible in the form \( c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + \langle f(x) \rangle \) with \( c_j \)'s \( \in \mathbb{F} \).

Another splitting field for \( x^2 + x + 2 \) over \( \mathbb{Z}_3 \mathbb{Z} \)

Let \( K = \mathbb{Z}_3 \mathbb{Z} (x) / \langle x^2 + 1 \rangle \) and \( \alpha \) the image of \( x \) in \( K \).

Then \( \alpha^2 + 1 = 0 \).

Have \( x^2 + x + 2 = (x - (1+\alpha))(x - (1-\alpha)) \) in \( K(x) \)

Indeed, \( \text{RHS is} \)

\[
\begin{aligned}
\left( 1 + \alpha + (1-\alpha) \right) x + (1+\alpha)(1-\alpha) \\
\left( 1 + \alpha + (1-\alpha) \right) x + (1-\alpha)(1+\alpha) \\
(1+\alpha)(1-\alpha) = 1 - \alpha^2 = 1 - (-1) = 2
\end{aligned}
\]

\( = x^2 - 2x + 2 = x^2 + x + 2 \) in \( \mathbb{Z}_3 \mathbb{Z} (x) \).

Thus, \( K \) splits \( f \), and by analogous argument to above,

\( K \) is a splitting field for \( f \) over \( \mathbb{Z}_3 \mathbb{Z} \).

We will later prove that all splitting fields over \( \mathbb{F} \) of some fixed polynomial \( f(x) \in \mathbb{F}(x) \) are isomorphic.
Field of fractions

**Summary:**
- Integral domain $D$.
- The field of fractions $\mathbb{F}(D)$ is a field $F$ that contains $D$ as a subring.
- **Key point:** In particular, every integral domain is contained in a field.

**How to construct $F$?**
- Consider $S = \mathbb{F}(a,b) : a, b \in D, b \neq 0$.
  (Think of $(a,b)$ as a fraction $a/b$).
- Precisely, put an equivalence relation on $S$ as
  
  $$(a,b) \sim (c,d) \text{ if } ad = bc \text{ in } D.$$ 

  Write $a/b$ for the equivalence class containing $(a,b)$.

  $F = \text{ the set of equivalence classes from } S.$