Last time

Minimal polynomials

Thm If \( a \) is algebraic over a field \( F \), then there is a unique monic irreducible polynomial \( p(x) \in F[x] \) such that \( p(a) = 0 \).

In fact, if \( f(x) \in F[x] \) is such that \( f(a) = 0 \), then \( p(x) \) divides \( f(x) \) in \( F[x] \).

Def: The polynomial \( p(x) \) is called the minimal polynomial for \( a \) over \( F \).

Ex
- The minimal polynomial for \( \sqrt{2} \) over \( \mathbb{Q} \) is \( x^2 - 2 \)
- The minimal polynomial for \( \sqrt{2} \) over \( \mathbb{R} \) is \( x - \sqrt{2} \)
- The min. poly. for \( i \) over \( \mathbb{R} \) is \( x^2 + 1 \)
- The min. poly. for \( i \) over \( \mathbb{C} \) is \( x - i \)

Def: Let \( E \) be an extension field of \( F \). If \( E \) has
Let \( E \) be an extension field of \( F \). If \( E \) has dimension \( n \) as an \( F \)-vector space, we write \([E:F]=n\) and say \( E \) has degree \( n \) over \( F \).

**Example**

If \( F \) is a field, \( p(x) \in F[x] \) is irreducible of degree \( n \), and \( a \) is a zero of \( p \) in some extension field of \( F \), then \([F(a):F]=n\).

**Example**

- \( \mathbb{Q}(i) \) has dimension 2 as a \( \mathbb{Q} \)-vector space
- \( \mathbb{R} \) has dimension 1 as a \( \mathbb{Q}(i) \)-vector space

**Going:** \( K \supseteq E \supseteq F \)

\([K:E]=m \implies [K:F]=mn\)

\([E:F]=n\)

**Theorem:** If \( E \) is a finite extension of \( F \), then \( E \) is an algebraic extension of \( F \).

**Proof:** Suppose \([E:F]=n\) and \( a \in E \). Then \([1, a, a^2, \ldots, a^n]\) is linearly dependent over \( F \).
\[ \{ 1, u, u^2, \ldots, u^n \} \text{ is linearly dependent over } \mathbb{F}. \]

\[ \Rightarrow \exists c_0, c_1, \ldots, c_n \in \mathbb{F} \text{ such that } c_0 + c_1 a + c_2 a^2 + \ldots + c_n a^n = 0. \]

\[ \Rightarrow a \text{ is a zero of } f(x) = c_n x^n + \ldots + c_0 \in \mathbb{F}[x]. \]

\[ \Rightarrow \text{Aside: } \mathbb{Q}(\alpha) = \{ a + b \alpha : a, b \in \mathbb{Q} \} \]

\[ \Rightarrow \{ 1, \alpha \} \text{ is a basis for } \mathbb{Q}(\alpha) \text{ over } \mathbb{Q}. \]

\[ \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2. \]

\[ \cdot \mathbb{Q}(\alpha) = \mathbb{Q}[x] / \langle x^2 + 1 \rangle \]

We proved, in general, that

\[ \frac{\mathbb{F}[x]}{\langle f(x) \rangle} \text{ is a } \mathbb{F} \text{ vector space of dimension } \deg(f) = n. \]

We checked

\[ 1 + \langle f(x) \rangle, x + \langle f(x) \rangle, \ldots, x^{n-1} + \langle f(x) \rangle \]

is a basis of \( \frac{\mathbb{F}[x]}{\langle f(x) \rangle} \).

\[ \cdot \text{If } \mathbb{F} \text{ is a field, it is always true that } \mathbb{F} \text{ has dimension 1 as an } \mathbb{F} \text{ vector space.} \]

For example \( \{ a \alpha \} \) is a basis, if \( a \in \mathbb{F}, a \neq 0. \)
Thm: Let $K$ be a finite extension of the field $E$, and let $E$ be a finite extension of the field $F$. Then $K$ is a finite extension of $F$ and

$$[K:F] = [K:E][E:F].$$


Let $\{x_1, \ldots, x_n\}$ be a basis for $K$ over $E$ and $\{y_1, \ldots, y_m\}$ be a basis for $E$ over $F$.

Suffices to prove: $\{y_j x_i : 1 \leq j \leq m, 1 \leq i \leq n\}$ is a basis for $K$ over $F$.

Spanning: Suppose $a \in K$. Then $\exists b_1, \ldots, b_n \in E$ such that

$$a = b_1 x_1 + \ldots + b_n x_n.$$ 

For each $b_i$, $\exists c_{i1}, c_{i2}, \ldots, c_{im} \in F$ such that

$$b_i = c_{i1} y_1 + c_{i2} y_2 + \ldots + c_{im} y_m$$

$$a = \sum_{i=1}^{n} b_i x_i = \sum_{i=1}^{n} \left( \sum_{j=1}^{m} c_{ij} y_j \right) x_i = \sum_{1 \leq j \leq m} \left[ \sum_{1 \leq i \leq n} c_{ij} y_j x_i \right].$$

$\{y_j x_i : 1 \leq j \leq m, 1 \leq i \leq n\}$ is a basis for $K$ over $F$. 

$K = \frac{\text{basis for } K/F}{n}$.
\[ K \supseteq \{ x_1, \ldots, x_n \} \text{ basis for } K/E \]
\[ E \supseteq \{ y_1, \ldots, y_m \} \text{ basis for } E/F \]
\[ F = \sum_{i,j} c_{ij} \]

**Independence**

Suppose \( \exists c_{ij} \in F \) such that \( \sum_{i,j} c_{ij} y_j x_i = 0 \).

Then \( \sum_{i=1}^n \left( \sum_{j=1}^m c_{ij} y_j \right) x_i = 0 \).

By the fact that the \( x_i \)'s are linearly independent over \( E \),
\[ \sum_{j=1}^m c_{ij} y_j = 0 \text{ for each } i. \]

By the fact that the \( y_j \) are linearly independent over \( F \),
\[ c_{ij} = 0 \text{ } \forall i,j. \]

**Notation:** Write \( E \mid m F \) if \( E \) is an extension field of \( F \) of degree \( m \).
So just proved: 
\[
\begin{align*}
K & \\
\subseteq & \\
\cap & \\
\cong & \\
\text{mn} & \\
E & \\
\subseteq & \\
\text{im} & \\
F & \\
\end{align*}
\]

\textbf{Proof:} Suppose \( F \) is a field, \( K \) some extension field of \( F \), and \( a \in K \) algebraic over \( F \). If \( E \subseteq K \) is another extension field of \( F \), then

\[
\frac{[E(a) : E]}{[E(a) : E]} \leq \frac{[F(a) : F]}{[F(a) : F]}
\]

\textbf{Pf:} Because \( a \) is algebraic over \( F \), it is clearly also algebraic over \( E \). We know

\[
F(a) = F[x] / \langle p(x) \rangle \quad \text{where } p \text{ is the minimal polynomial of } a \text{ over } F.
\]

\[
E(a) = E[x] / \langle q(x) \rangle \quad \text{where } q \text{ is the minimal polynomial of } a \text{ over } E.
\]
where \( q \) is the minimal polynomial of \( a \) over \( E \).

Because \( p(a) = 0 \), \( p(x) \in E[x] \subseteq F[x] \), we get that \( q(x) \) divides \( p(x) \) in \( E[x] \). Thus \( \deg(q) \leq \deg(p) \).

So

\[
[E(a) : E] = \deg(q) \leq \deg(p) = [F(a) : F].
\]

**Example**

```
\[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) = K\]
```

```
\[
\begin{array}{ccc}
\mathbb{Q}(\sqrt[3]{2}) & 12 & \mathbb{Q}(\sqrt[4]{3}) \\
3 & \downarrow & 4 \\
\mathbb{Q} & & \mathbb{Q} \\
\end{array}
\]
```

**Hence:**

\[
[K: \mathbb{Q}] = [K: \mathbb{Q}(\sqrt[4]{3})][\mathbb{Q}(\sqrt[4]{3}): \mathbb{Q}]
\]

\[
= 4 \left[ K: \mathbb{Q} \right] \quad \Rightarrow \quad 12 \mid [K: \mathbb{Q}]
\]

Similarly,

\[
3 \mid [K: \mathbb{Q}]
\]

On the other hand:

\[
[K: \mathbb{Q}] \leq 12
\]

\[
= [K: \mathbb{Q}] = 12
\]