Definition. Let $E/F$ be a field extension. $\alpha \in E$ is called algebraic over $F$ if $\alpha$ is a zero of a polynomial $f(x) \in F[x] \setminus \{0\}$. Otherwise $\alpha$ is called transcendental over $F$.

Theorem. Suppose $E/F$ is a field extension, and $\alpha \in E$ is algebraic over $F$. Then

1. There exists a monic polynomial $m_{\alpha,\infty} \in F[x]$ such that for $f(x) \in F[x]$,
   $$f(\alpha) = 0 \iff m_{\alpha,\infty} | f(\alpha).$$

2. $m_{\alpha,\infty}$ is irreducible in $F[x]$.

3. $F[x]/\langle m_{\alpha,\infty} \rangle \cong F[\alpha] := \{ \sum_{i=0}^{\infty} a_i \alpha^i \mid a_i \in F \}$; and $F[\alpha]$ is a field.

4. $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an $F$-basis of $F[\alpha]$ where $d = \deg m_{\alpha}$; and so
   $$\dim_F F[\alpha] = \deg m_{\alpha}.$$ 

Before we get to proof of the above theorem, let’s point out that if $E/F$ is a field extension, then $E$ can be viewed as an $F$-vector space. The dimension $\dim_F E$ of $E$ as an $F$-vector space is denoted by $[E:F]$, and sometimes called the degree of the field extension $E/F$. 
Proof. Let \( \phi_\alpha : F[x] \to E \) be the evaluation at \( \alpha \). We have seen that \( \phi_\alpha \) is a ring homomorphism. And so \( F[x]/\ker \phi_\alpha \cong \text{Im} \phi_\alpha \).

Since \( F[x] \) is a PID and \( \ker \phi_\alpha \neq 0 \) (\( \alpha \) is algebraic), \( \exists \) monic polynomial such that \( \ker \phi_\alpha = \langle m_\alpha(x) \rangle \).

And so \( p(\alpha) = 0 \iff p(x) \in \ker \phi_\alpha \iff m_\alpha(x) \mid p(x) \).

\( \text{Im} \phi_\alpha = F[x]/\langle m_\alpha(x) \rangle \to E \); and so it is an integral domain. Hence \( \langle m_\alpha(x) \rangle \in \text{Spec}(F[x]) \setminus \{0\} \). Since \( F[x] \) is a PID, we deduce that \( \langle m_\alpha(x) \rangle \) is a maximal ideal. Therefore \( m_\alpha(x) \) is irreducible in \( F[x] \) and \( F[x]/\langle m_\alpha(x) \rangle \cong F[\alpha] \) is a field.

For any \( p(x) \in F[x] \), let \( q(x) \) and \( r(x) \) be the quotient and remainder of \( p(x) \) divided by \( m_\alpha(x) \). So we have \( p(\alpha) = q(\alpha) m_\alpha(\alpha) + r(\alpha) = r(\alpha) \) and \( \deg r < \deg m_\alpha \). This implies \( F[\alpha] = \langle a_0 + a_1 \alpha + \ldots + a_{d-1} \alpha^{d-1} \mid a_i \in F \rangle \); and so \( F[\alpha] \) is the \( F \)-span of \( 1, \alpha, \ldots, \alpha^{d-1} \), and \( \dim_F F[\alpha] \leq \deg m_\alpha \).

Claim. \( 1, \alpha, \ldots, \alpha^{d-1} \) are linearly independent over \( F \).
Lecture 22: Minimal polynomial

Monday, February 26, 2018 8:10 AM

Proof of claim. If not, \( c_0 + c_1 \alpha + \ldots + c_{d-1} \alpha^{d-1} = 0 \) for some \((c_0, \ldots, c_{d-1}) \in \mathbb{F}^d \setminus \mathbb{F} \alpha^{d-1} \). Hence \( p(\alpha) = 0 \) where \( p(x) = \sum_{i=0}^{d-1} c_i x^i \); this implies \( m_\alpha(\alpha) \mid p(\alpha) \). From this we deduce either \( p = 0 \) or \( \deg m_\alpha \leq \deg p \), which is a contradiction. ■

Definition. \( m_\alpha(\alpha) \in \mathbb{F}[x] \) in the previous theorem is called the minimal polynomial of \( \alpha \) over \( \mathbb{F} \).

Observation. Suppose \( E/\mathbb{F} \) is a field extension, and \( \alpha \in E \) is algebraic over \( \mathbb{F} \).

If \( p(x) \in \mathbb{F}[x] \) is irreducible and \( p(\alpha) = 0 \), then \( p(x) = c m_\alpha(x) \) for some \( c \in \mathbb{F}^* \).

Proof. \( m_\alpha(\alpha) \mid p(\alpha) \) and \( p(x) \) is irreducible \( \implies p(x) = c m_\alpha(x) \) for some \( c \in \mathbb{F}^* \). ■

Proposition. Let \( \mathbb{F} \) be a field and suppose \( p(x) \in \mathbb{F}[x] \) is irreducible.

Then \( \exists \) a field extension \( E \) of \( \mathbb{F} \) and \( \alpha \in E \) such that

1. \( m_\alpha(\alpha) = c p(x) \),
2. \( E = F(x) \).

Proof. Since \( p(x) \) is irreducible, \( \langle p(x) \rangle \) is a maximal ideal of \( \mathbb{F}[x] \).

Hence \( E = \mathbb{F}[x]/\langle p(x) \rangle \) is a field. Since \( \mathbb{F} \cap \langle p(x) \rangle = 0 \), \( F \rightarrow E \).

Let \( \alpha := x + \langle p(x) \rangle \in E \). Then \( p(\alpha) = 0 \) and
Lecture 22: Towards splitting field

Monday, February 26, 2018  8:26 AM

$f(x) = 0 \iff f(x) \in \langle p(x) \rangle$. Therefore if the leading coeff.

of $p$ is $c$, then $m_p(x) = c \cdot p(x)$. And clearly we have $E = F[x]$.

We can continue this process and get a field $E = F[x_1, \ldots, x_d]$ such that $p(x) = (x - \alpha_1) \cdots (x - \alpha_d)$. Next we will show that this field is essentially unique.

**Lemma.** Suppose $\phi : F \to F'$ is an isomorphism. Then

1. $\phi$ can be extended to an isomorphism $\phi : F[x] \to F'[x]$,

\[\phi \left( \sum_{i=0}^{n} a_i x^i \right) = \sum_{i=0}^{n} \phi(a_i) x^i.\]

2. Let $p(x)$ be an irred. polynomial in $F[x]$. Then $\phi(p(x))$ is irreducible in $F'[x]$.

3. Suppose $E/F$ and $E'/F'$ are field extensions, $\alpha \in E$ is a

zero of $p(x)$, and $\alpha' \in E'$ is a zero of $\phi(p(x))$. Then

\[\exists! \ \theta : F[x] \sim F'[x'] \text{ s.t.} \begin{cases}
\phi |_F = \theta |_F \\
\phi(\alpha) = \alpha'
\end{cases}
\]
Lecture 22: Towards splitting field

Monday, February 26, 2018  8:37 AM

Page 5

pp. Parts (1) and (2) are clear. Based on the first two parts
we get that \( F[x]/\langle p(x) \rangle \) and \( F[x]/\langle \phi(p(x)) \rangle \)
are isomorphic fields. Using evaluation maps we get that

\[
\begin{align*}
\text{\(F\langle x+j\rangle/\langle j+\phi(p(x))\rangle\)} & \xrightarrow{\phi} \text{\(F\langle x+j\rangle/\langle \phi(p(x))\rangle\)} \\
\text{\(F\langle j\rangle/\langle j+p(x)\rangle\)} & \xrightarrow{\phi} \text{\(F\langle j\rangle/\langle \phi(p(x))\rangle\)}
\end{align*}
\]

A field does not have non-trivial ideal. And so
any non-zero homomorphism is an injection.

And clearly the restriction to \( F \) is \( \phi. \)

**Def.** Let \( f \in F[x] \). A field extension \( E/F \) is called the splitting field of \( f \) if

1. \( f \) can be written as a product of degree 1 polynomials in \( E[x] \),
2. \( f \in E' \subseteq E \), then \( f \) cannot be written as a product of degree 1 polynomials in \( E'[x] \).

This is equivalent to say \( \exists \alpha_1, \ldots, \alpha_n \in E \) st.

1. \( f(x) = c \prod (x-\alpha_1)(x-\alpha_2) \cdots (x-\alpha_n) \)
2. \( E = F(\alpha_1, \ldots, \alpha_n) \)

\( \text{subfield generated by } F \) and \( \alpha_1, \alpha_2, \ldots, \alpha_n \).
Lemma. Let \( f(x) \in F[x]\backslash F \). Then there is a splitting field of \( f(x) \) over \( F \).

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

Let \( \phi(x) \) be an irreducible factor of \( f(x) \). Then by a propo.

\( \exists \) a field extension \( E_1 = F[\alpha_1] \) such that \( \phi(\alpha_1) = 0 \); and so

\( f(x) = (x - \alpha_1) \phi_1(x) \) for some \( \phi_1(x) \in E_1[x] \) and \( \deg \phi_1 = \deg f - 1 \).

By the induction hypothesis \( \phi_1 \) has a splitting field \( E \) over \( E_1 \).

And so \( \exists \alpha_2, ..., \alpha_n \in E \) st. (1) \( \phi_1(x) = c(x - \alpha_2)(x - \alpha_3)...(x - \alpha_n) \)

(2) \( E = E_1(\alpha_2, ..., \alpha_n) \).

And so \( f(x) = c(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)...(x - \alpha_n) \) and

\( E = F(\alpha_1, \alpha_2, ..., \alpha_n) \).

So \( E \) is the splitting field of \( f(x) \) over \( F \).

Theorem. Suppose \( \phi: F \to F' \) is an isomorphism of fields \( F \)

and \( F' \). We extend \( \phi \) to an isomorphism \( \phi: F[x] \to F'[x] \).

Let \( f(x) \in F[x] \backslash F \). Suppose \( E \) is a splitting field of \( f(x) \) over
F and E' is a splitting field of \( \phi(\alpha)(\sigma) \) over F'. Then there is an isomorphism \( \phi : E \cong E' \) such that \( \phi|_F = \phi \).

\[ \begin{array}{ccc}
E & \xrightarrow{\phi} & E' \\
\downarrow 2 & & \downarrow 2 \\
F & \xrightarrow{\sigma} & F'
\end{array} \]

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

If all the irreducible factors of \( f \) are of degree 1, then \( \phi(\alpha)(\sigma) = c \Pi (x-\alpha_i) \) for \( c, \alpha_i \in F \). And so \( \phi(f(\alpha)) = \phi(\alpha)(\sigma) \Pi (x-\phi(\alpha_i)) \). Hence \( E=F \) and \( E'=F' \). And \( \phi = \phi \) works.

Suppose \( \phi(\alpha)(\sigma) \) is an irreducible factor of \( f(\alpha) \) and \( \deg p \geq 2 \).

Then \( \phi(\alpha)(\sigma) \) is an irreducible factor of \( \phi(f(\alpha)) \). Since \( E \) is an splitting field of \( f(\alpha) \) over \( F \) and \( \phi(\alpha)(\sigma) \mid f(\alpha) \), \( \exists \alpha_1 \in E \) s.t. \( p(\alpha_1) = 0 \). Similarly \( \exists \alpha'_1 \in E' \) s.t. \( \phi(p)(\alpha'_1) = 0 \). So by a lemma proved earlier, \( \exists \phi_1 : F[\alpha_1] \cong F[\alpha'_1], \phi_1|_F = \phi \), and \( \phi_1(\alpha_1) = \alpha'_1 \).

And so \( \phi(\alpha) = (x-\alpha_1) \phi_1(\alpha) \) and

\[
\phi(f(\alpha)) = \phi_1(f(\alpha)) = \phi_1(x-\alpha_1) \phi_1(\phi_1(\alpha))(x) = (x-\alpha'_1)(\phi_1(\alpha))(x)
\]

\[ \begin{array}{ccc}
F[\alpha_1] & \xrightarrow{\phi_1} & F[\alpha'_1] \\
\downarrow 1 & & \downarrow 1 \\
F & \xrightarrow{\sigma} & F'
\end{array} \]
Claim. $E$ is the splitting field of $f_1(x)$ over $F[x_1]$. 

**Proof.** \( \exists \alpha_1, \ldots, \alpha_n \in E, \ f_1(x) = c_1 (x-\alpha_1) (x-\alpha_2) \cdots (x-\alpha_n) \) and \( E = F(\alpha_1, \alpha_2, \ldots, \alpha_n) \).

And so \( f_1(x) = c_1 (x-\alpha_2) (x-\alpha_3) \cdots (x-\alpha_n) \) and \( E = F(\alpha_1) (\alpha_2, \ldots, \alpha_n) = (F[x_1]) (\alpha_2, \ldots, \alpha_n) \). \( \Box \)

Claim. $E'$ is the splitting field of $f_1(x)\phi$ over $F[x_1]$. 

**Proof.** is similar to the previous claim \( f_1(x) = (x-\alpha_1) \phi(f_1) \).

So by the induction hypothesis, \( \exists \phi : E \cong E' \) s.t.

\[
\begin{array}{ccc}
E & \xrightarrow{\sim} & E' \\
\downarrow \phi & & \downarrow \phi' \\
F[x_1] & \xrightarrow{\sim} & F[x_1] \\
\downarrow \phi_1 & & \downarrow \phi_1' \\
F & \xrightarrow{\sim} & F'
\end{array}
\]

And the claim follows. \( \Box \)

Corollary. If $E$ and $E'$ are two splitting fields of $f(x)$ over $F$, then \( \exists \phi : E \cong E' \) s.t. \( \phi|_F = \text{id}_F \).