Thm. Let $E \supset F$ be an extension field, and suppose $\alpha \in E$ is algebraic over F. Then there is a unique irreducible, monic polynomial $p(x)$ of smallest degree for which α is a root, and if α is a root of $f(x) \in F[x]$, then $p(x) \mid f(x)$.

Def. The unique irreducible, monic polynomial guaranteed above is called the minimal polynomial for $\alpha \in E$ over F.

The degree of α = degree of its min. polynomial.

Ex. The only elts of $E \supset F$ with degree 1 are the elements of F.

The minimal polynomial for $i \in \mathbb{C}$ over $\mathbb{Q}$ is x^2+1, so i has degree 2 over $\mathbb{Q}$.

Prop. Let $E \supset F$ be a field extension, with $\alpha \in E$ algebraic over F. Then

$$F(\alpha) \cong F[x]/\langle p(x) \rangle,$$

where $p(x)$ is the minimal polynomial of α over F.

Example/Exercise. $\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}$

(Proof.) Consider $\Phi_\alpha : F[x] \longrightarrow E$

$f(x) \longmapsto f(\alpha)$

Check: $\Phi_\alpha(F[x]) = F(\alpha) \subset E$

Also, $\ker \Phi_\alpha = \{f(x) \in F[x] \mid f(\alpha) = 0\} = \langle p(x) \rangle$.

So F.I.T:

$$F(\alpha) = \Phi_\alpha(F[x]) \cong F[x] / \ker \Phi_\alpha = F[x] / \langle p(x) \rangle. \quad \blacksquare$$

Linear algebra tools

If $E \supset F$ is an extension field, then E is a vector space over F.

The next theorem says

simple extension $\Longrightarrow$ finite-dimensional vector space

Thm. Let $E = F(\alpha)$ be a simple extension of F, with α algebraic over F of degree n. Then

$$\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$$

forms a basis for E over F.

(Proof.)

Linear independence: exercise using fact that α is not a root of any polynomial of deg $< n$.

Span: We NTS that $F(\alpha) = V$, where V is the v.s. over F spanned by $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$.

Let $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + x^n$ be the min. poly. for α.

Then

$$0 = p(\alpha) = a_0 + a_1 \alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n,$$

so

$$\alpha^n = -\overset{1}{a_0} - a_1 \overset{\alpha}{}\alpha - \overset{\alpha^2}{\cdots} - a_{n-1}\overset{\alpha^{n-1}}{\alpha^{n-1}} \in V.$$

Notice:

$$\begin{aligned}
\alpha^{n+1} &= \alpha \cdot \alpha^n \\
&= -a_0 \alpha - a_1 \alpha^2 - \cdots - a_{n-2}\alpha^{n-1} - a_{n-1}\alpha^n \\
&= -a_0 \alpha - a_1 \alpha^2 - \cdots - a_{n-2}\alpha^{n-1} \\
&\qquad - a_{n-1}\left(-a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}\right) \\
&\in V.
\end{aligned}$$

Similarly, $\alpha^m \in V$, for all $m \geq n$.

Now any $\beta \in E = F(\alpha)$ can be written as

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_m\alpha^m,$$

for some $b_0, b_1, \ldots, b_m \in F$. Since each α^k is in V, so is β. ∎

Def. If $E \supset F$ has dimension $n < \infty$ over F as a vector space, then we call E a finite extension of degree n over F and we write $[E:F] = n$.

Thm. If $E \supset F$ and $K \supset E$ are finite extensions, then $K \supset F$ is a finite extension, and

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

Thm Let $E \supset F$ be an extension field. Then TFAE:

1. E is a finite extension of F.
2. $\exists$ algebraic elements $\alpha_1, \ldots, \alpha_n \in E$ s.t. $$E = F(\alpha_1, \ldots, \alpha_n)$$
3. $\exists$ a sequence of fields $$E = F(\alpha_1, \ldots, \alpha_n) \supset F(\alpha_1, \ldots, \alpha_{n-1}) \supset \cdots \supset F(\alpha_1) \supset F,$$ where each $F(\alpha_1, \ldots, \alpha_k)$ is algebraic over $F(\alpha_1, \ldots, \alpha_{k-1})$.

Splitting fields

Def. Let F be a field, $p(x) \in F[x]$ with $\deg p(x) \geq 1$.
We say that $p(x)$ splits over an extension field $E \supset F$ if
$\exists\, \alpha_1, \ldots, \alpha_n \in E$ s.t.

$$p(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

for some $a \in F$. If $p(x)$ splits over E and

$$E = F(\alpha_1, \ldots, \alpha_n),$$

then E is a splitting field of $p(x)$.

Ex. $p(x) = (x^2-2)(x^2-6) \in \mathbb{Q}[x]$

$\mathbb{Q}(\sqrt{2})$ contains a root, but $p(x)$ doesn't split

$\mathbb{Q}(\sqrt{2}, \sqrt{6})$ is a splitting field

$\mathbb{C} \supset \mathbb{Q}$ is not a splitting field, even though $p(x)$ splits

Thm. Every nonconstant polynomial with coefficients in a field F admits a splitting field over F.

(Proof.) Induction on $\deg p(x)$, with $p(x) \in F[x]$.

Base case: $\deg p(x) = 1 \Rightarrow$ let $E = F$.

Inductive hypothesis: $n := \deg p(x)$, and every polynomial of degree $< n$ admits a splitting field

§ $p(x)$ is irreducible.

Then $\exists\ K \supset F$ s.t. $\alpha_1 \in K$ is a root of $p(x)$.

So $p(x) = (x-\alpha_1)\, q(x) \in K[x]$.

$\deg q(x) = n-1 \Rightarrow E \supset K$ is a splitting field for $q(x)$.

$\Rightarrow E \supset F$ is a splitting field for $p(x)$.

If $p(x)$ is not irreducible, write

$$p(x) = p_1(x)\, p_2(x) \cdots p_k(x),$$

with $\deg p_i(x) \geq 1$.

I.H. $\Rightarrow p_1(x)$ admits S.F. $K_1 \supset F$

$\Rightarrow p_2(x)$ admits S.F. $K_2 \supset K_1$

$\Rightarrow \cdots \Rightarrow p_k$ admits S.F. $K_k \supset K_{k-1}$

$$K_k = E \supset F.$$

∎