Recall: Given $E \supset F$ and an algebraic element $\alpha \in E$, $F(\alpha) \cong F[x]/\langle p(x) \rangle$, where $p(x)$ is the minimal polynomial for α.

If $\deg p(x) = 1$, what is $F[x]/\langle p(x) \rangle$?

F.

$F[x]/\langle x-\alpha \rangle$ = "$F[x]$, but set $x-\alpha = 0$"

= "$F[x]$, but set $x = \alpha$"

i.e., $\phi_\alpha : F[x] \longrightarrow F$. $\ker \phi_\alpha = \langle x-\alpha \rangle$

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

Thm. Suppose $E = F(\alpha)$ is a simple extension of F, and that $\alpha \in E$ is algebraic over F with degree n. Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ forms a basis for E over F.

(Proof.) Let $V \subseteq E$ denote the F-vector space over F spanned by $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

If $p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ is the min. polynomial for α, then

$$p(\alpha) = 0 \Rightarrow \alpha^n = -a_0 - a_1\alpha - a_2\alpha^2 - \cdots - a_{n-1}\alpha^{n-1}.$$

So $\alpha^n \in V$.

Then $\alpha^{n+1} = \alpha \cdot \alpha^n = \alpha(-a_0 - a_1\alpha - a_2\alpha^2 - \cdots - a_{n-1}\alpha^{n-1})$

$$= -a_0\alpha - a_1\alpha^2 - \cdots - a_{n-1}\alpha^n$$

is a linear combo of elements in $V \Rightarrow \alpha^{n+1} \in V$.

Similarly, $\alpha^m \in V$, for any $m \geq 0$.

Finally, pick $\beta \in E = F(\alpha)$. We know that

$$F(\alpha) = \Phi_\alpha(F[x]),$$

so $\beta = \Phi_\alpha(b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m)$

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

for some $b_0 + b_1 x + \cdots + b_m x^m \in F[x]$.

Linear combo of elts of $V \Rightarrow$ in V.

So $V = E$.

$\S$ $\exists$ $c_0, c_1, \ldots, c_{n-1} \in F$ s.t.

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0.$$

$\S$ $c_0, c_1, \ldots, c_{n-1}$ are not all zero.

Then

$$c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in F[x]$$

has α as a root. $\therefore$ divisible by $p(x)$.

But $\deg p(x) = n$, so we have a contradiction.

$\therefore$ $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ linearly indep. ∎

Def. We call $E \supset F$ a **finite extension of degree n over F** if E is a vector space of dimension n over F. Write $[E:F] = n$.

Ex ① $\mathbb{R} \supset \mathbb{Q}$ is a field extension of infinite degree. (In fact, uncountable.)

② $\mathbb{C} \supset \mathbb{R}$ is a field extension of degree 2.
$\{1, i\}$ is a basis.
$\mathbb{C} \cong \mathbb{R}[x]/\langle x^2+1 \rangle$

Thm. If $E \supset F$ and $K \supset E$ are finite field extensions, then
$$[K:F] = [K:E] \cdot [E:F].$$

Thm. Let $E \supset F$ be a field extension.
Then TFAE:
① E is a finite extension of F;
② $\exists$ a finite # of algebraic elements $\alpha_1, \ldots, \alpha_n \in E$ s.t.
$E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$;
③ $\exists$ a sequence of simple field extensions
$E = F(\alpha_1, \ldots, \alpha_n) \supset F(\alpha_1, \ldots, \alpha_{n-1}) \supset \cdots \supset F(\alpha_1) \supset F$,
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 and let $p(x) \in F[x]$ have degree $n \geq 1$. We say that $p(x)$ splits over an extension $E \supset F$ if $\exists\ \alpha_1, \alpha_2, \ldots, \alpha_n \in E$ and $c \in F$ s.t.
$$p(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

If $p(x)$ splits over E and $E = F(\alpha_1, \ldots, \alpha_n)$, then E is a splitting field for $p(x)$.

Ex ① $p(x) = 3x^2 + 3$ splits over $\mathbb{C}$, since

$$p(x) = 3(x-i)(x+i).$$

But $\mathbb{C}$ is not a splitting field for $p(x)$ over $\mathbb{Q}$.
But $\mathbb{C}$ is a splitting field for $p(x)$ as an extension of $\mathbb{R}$.

② $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ contains a root of

$$p(x) = (x^2-2)(x^2-6),$$

but $p(x)$ doesn't split.
The splitting field for $p(x)$ over $\mathbb{Q}$ is
$\mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Thm. Every nonconstant polynomial with coefficients in a field admits a splitting field.
(Proof.) We'll use induction on $\deg p(x) = n \geq 1$.

Base: $n = 1 \Rightarrow p(x) = \alpha x - \beta$, with $\alpha, \beta \in F$

$$= \alpha(x - \beta/\alpha),$$

so $p(x)$ splits over F.

Inductive hypothesis: Every polynomial in $F[x]$ of degree $1 \leq k < n$ admits a splitting field.

If $p(x)$ is not irreducible, we can find splitting fields for each of its irreducible factors and then a common extension of all of these is

a splitting field for $p(x)$.
So assume $p(x)$ is irred.

F.T.F.T.: $\exists\ K \supset F$ s.t. $p(x)$ has a root $\alpha \in K$.

Then

$$p(x) = (x-\alpha)\, q(x) \in K[x],$$

for some $q(x) \in K[x]$. $\deg q(x) = n-1$, so I.H. gives a splitting field $E \supset K$ for $q(x)$. So $E \supset F$ is a splitting field for $p(x)$.

∎