Thm: Suppose K/F is a field extension and $\alpha \in K$ is algebraic over F, and that α has degree n. Then $[F(\alpha):F] = n$ and $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is an F-basis for $F(\alpha)$.

Pf: First, $\deg f_\alpha = n \Rightarrow \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is F-lin. ind.

$\Rightarrow [F(\alpha):F] \geq n$.

Next, $V = \{a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1} : a_i \in F\}$ is closed under:

i) Subtraction ✓

ii) Multiplication, by the division algorithm. ✓

Suppose $g_1, g_2 \in F[x]$, $\deg < n$.

- If $\deg g_1 + \deg g_2 < n$ then $g_1(\alpha) g_2(\alpha) \in V$. ✓

- If $\deg g_1 + \deg g_2 \geq n$ then write $g_1 g_2 = p(x) f_\alpha(x) + r(x)$, where $r(x) = 0$ or $\deg r < n$.

Then $g_1(\alpha)\, g_2(\alpha) = p(\alpha) \underbrace{f_\alpha(\alpha)}_{= 0} + r(\alpha)$

$= r(\alpha) \in V$.

· Taking inverses:

Suppose $g(x) \in F[x] \setminus \{0\}$, $\deg g < n$.

Write $1 = u(x) g(x) + v(x) f_\alpha(x)$, (Bezout's lemma for $F[x]$)

and w.L.O.G., assume (by div. alg.) that $\deg u < n$.

Then $1 = u(\alpha) g(\alpha) \Rightarrow u(\alpha) = g(\alpha)^{-1}$ (and $u(\alpha) \in V$).

Therefore, V is a field which contains α, and

$[V:F] \leq n \Rightarrow V = F(\alpha)$ and $[F(\alpha):F] = n$. ∎

Sandbox:

1a) What is $\mathbb{F}_3(\sqrt{2})$?

Natural to think of this as the smallest extension of $\mathbb{F}_3$ where x^2-2 has a root.

Q1) Is x^2-2 irred. over $\mathbb{F}_3$?

Yes, because it is a degree 2 poly. w/ no roots.

$\left(\begin{array}{c} f(x) = x^2-2 \\ f(0) = -2, \\ f(\pm 1) = -1 \end{array} \right)$

So $\mathbb{F}_3(\sqrt{2}) \cong \mathbb{F}_3[x]/(x^2-2)$,

(field)

and $[\mathbb{F}_3(\sqrt{2}):\mathbb{F}_3] = 2$.

1b) What is $\mathbb{F}_7(\sqrt{2})$?

Be careful: $x^2-2=(x-3)(x+3)$, so "$\sqrt{2}$" $\in \mathbb{F}_7$,

and $\mathbb{F}_7(\sqrt{2})=\mathbb{F}_7$.

Thm (Kronecker ++): Suppose F is a field, $f \in F[x]$ is irred. of degree n, and α is a root of f in some extension of F. Then:

i) $F(\alpha) \cong F[x]/(f)$

ii) The map $g+(f) \mapsto g(\alpha)$ from $F[x]/(f) \to F(\alpha)$ is an isomorphism, and

iii) $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is an F-basis for $F(\alpha)$.

Similarly: If F is a field, $h \in F[x]$ is irred, $\deg h = n$ then $[F[x]/(h) : F] = n$ and

$\{1, x, x^2, \dots, x^{n-1}\}$ is an F-basis for $F[x]/(h)$.