Example Show that $\alpha = \sqrt{9+4\sqrt{2}}$ is alg. over $\mathbb{Q}$.
Find the min degree of the polynomial $p(x)$ s.t. $p(\alpha)=0$.

Let $x = \sqrt{9+4\sqrt{2}} = \alpha$

$x^2 = 9+4\sqrt{2}$

$x^2-9 = 4\sqrt{2}$

$(x^2-9)^2 = 32$

Let $p(x) = (x^2-9)^2 - 32 \Rightarrow p(\alpha) = 0$.

$p(x) = x^4 - 18x^2 + 49$

Is this min degree? Can we factor?

Rational root test: roots are $\pm 1, \pm 7$

7 does not work.

-7 does not work

No linear factors.

$$\begin{array}{r} 2401 \\ -\ 882 \\ \hline 1519 \end{array}$$

$$\begin{array}{r} 18 \\ 49 \end{array}$$

Rational root test: Given $p(x) \in \mathbb{Z}[x]$

$$p(x) = a_0 + a_1 x + \cdots + a_k x^k .$$

If $p(x)$ has a rational root $\frac{r}{s}$, then

$$\frac{r}{s} = \frac{\pm(\text{factor of } a_0)}{\pm(\text{factor of } a_k)} .$$

Now we check possible 2nd degree factors:

Suppose: $x^4 - 18x^2 + 49 = (x^2 + ax + b)(x^2 + cx + d)$

$= x^4 + (a+c)x^3 + (b + ac + d)x^2$

$+ (bc + ad)x + bd$

$a + c = 0 \Rightarrow c = -a$

$b + ac + d = -18 = b - a^2 + d$

$bc + ad = 0 = -ab + ad = 0$

$a(-b + d) = 0$

$bd = 49$

$b = d.$

Note if $a = c = 0$

$(x^2 + b)(x^2 + d)$

$= x^4 + (b+d)x^2 + bd$

λ : -18, μ : 49

doesn't work

$2b - a^2 = -18$

$b^2 = 49 \qquad b = \pm 7 = d$

$\pm 14 - a^2 = -18$

$b = -7 = d, \; a = \pm 2$

$b = 7 = d, \; a^2 = 32$ ✗

$\Rightarrow (x^2 + 2x - 7)(x^2 - 2x - 7)$

$= x^4 + (-7 - 4 - 7)x^2 + 49.$ ✓

-18

$x = \sqrt{9 + 4\sqrt{2}}$ satisfies $(x^2 + 2x - 7)(x^2 - 2x - 7) = 0$

So it must be a root of one of these

$x^2 = 9 + 4\sqrt{2}$

$2x = 2\sqrt{9+4\sqrt{2}}$

$9 + 4\sqrt{2} - 2\underbrace{\sqrt{9+4\sqrt{2}}}_{a+b\sqrt{2}} - 7 \stackrel{?}{=} 0$

$(a+b\sqrt{2})^2 = 9 + 4\sqrt{2}$

$a^2 + 2b^2 + 2ab\sqrt{2}$

$2ab = 4$

$a^2 + 2b^2 = 9$

$a = 1, b = 2$

$= 9 + 4\sqrt{2} - 2(1 + 2\sqrt{2}) \to$

$= 9 - 2 - 7 + (4-4)\sqrt{2} = 0$ ✓

∴ $x^2 - 2x - 7$ is the min polynomial of $\sqrt{9+4\sqrt{2}} = 1 + 2\sqrt{2}$.

Thm Let F be a field, $F \leq E$, extension field. Suppose that $\alpha \in E$. Consider $\phi_\alpha : F[x] \to E$, $f(x) \mapsto f(\alpha)$. (evaluation homomorphism)

Then α is transcendental $\iff \phi_\alpha$ is 1-1.

Proof. $\ker(\phi_\alpha) = \{f(x) \in F[x] : f(\alpha) = 0\}$

$= \{0\} \iff \alpha$ is transcendental.

We already showed:

Thm If F is a field, E an ext. field of F, $\alpha \in E$ is algebraic over F. Then $\exists$ irreducible poly $p(x)$ s.t. $p(\alpha)=0$, and p is unique up to a constant factor. It is also the polynomial of minimal degree s.t. $p(\alpha)=0$.

If $f(x) \in F[x]$ is any polynomial such that $f(\alpha)=0$, then $p(x) \mid f(x)$.

Pf: $(\ker \phi_\alpha) \neq \{0\}$ is an ideal in $F[x]$,

So $\ker \phi_\alpha = \langle p(x) \rangle$ for some $p(x) \in F[x]$.
(because $F[x]$ is a PID.)

$\therefore$ If $f(\alpha)=0 \iff f(x) \in \ker \phi_\alpha \iff f(x) = c(x)\,p(x)$ for some $c(x)$.

Irreducibility: if $p(x) = r(x)\,s(x)$, and $p(\alpha) = r(\alpha)\,s(\alpha) = 0$.

$\therefore$ $r(\alpha)$ or $s(\alpha) = 0$ ← since deg $p(x)$ is minimal, $r(x)$ or $s(x)$ must be a constant. ☑

Sp $r(\alpha)=0$
$r(x) = c(x)\,p(x)$.
$s(x) = \cdots$

We set the $p(x)$ with leading coefficient 1 (so it is unique) to be the $\mathrm{irr}(\alpha, F)$

"the irreducible poly of α over f" = "min. poly of α over F".

Simple Extensions: F field, E extension field, $\alpha \in E$

we will define $F(\alpha)$ ← minimal field extension of F that contains α.

"F adjoin α"

Cases: ① If α is algebraic over F, then

$\ker \phi_\alpha = \langle \text{irr}(\alpha, F) \rangle$

$\Rightarrow F[x] / \langle \text{irr}(\alpha, F) \rangle \cong \text{im}\,\phi_\alpha \subseteq E$

($\text{im}\,\phi_\alpha$ is a field)

Contains F ——

$\therefore \alpha$ is alg. over F

$\Rightarrow F(\alpha) = \phi_\alpha(F[x]) \subseteq E$.

② If α is transcendental over F, then $\phi_\alpha : F[x] \to E$ is 1-1.

$\phi_\alpha(F[x])$ is an integral domain. (but not a field)

$\cong F[\alpha]$, an integral domain.

$= \{ c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_k\alpha^k : k \in \mathbb{N} \cup \{0\},\ c_j \in F\ \forall j \}$

Take $F(\alpha)$ to be the field of quotients of $F[\alpha]$, i.e.

$F(\alpha) = \{$rational functions of α with coefficients in $F\}$.

↑ This is a field.

This $F(\alpha)$ is called a simple extension.