(1) x^3-5 is irreducible over $\mathbb{Q}$ by Eisenstein with $p=5$. Thus, (x^3-5) is maximal

So, $K = \mathbb{Q}[x]/(x^3-5)$ is a field. And also K is an integral domain since fields are integral domains.

$$K = \{a+bx+cx^2+I \mid a,b,c \in \mathbb{Q}\}$$

and

$$I = (x^3-5)$$

(2) $25 = 5^2 = p^2$

We need a degree 2 irreducible poly. over $\mathbb{Z}_5$.

Consider $p(x) = x^2 + \bar{2}$.

Note that

$p(\bar{0}) = \bar{2} \neq \bar{0}$

$p(\bar{1}) = \bar{1}^2 + \bar{2} = \bar{3} \neq \bar{0}$

$p(\bar{2}) = \bar{2}^2 + \bar{2} = \bar{6} = \bar{1} \neq \bar{0}$

$p(\bar{3}) = \bar{3}^2 + \bar{2} = \bar{11} = \bar{1} \neq \bar{0}$

$p(\bar{4}) = \bar{4}^2 + \bar{2} = \bar{18} = \bar{3} \neq \bar{0}$

So, p is irreducible over $\mathbb{Z}_5$ since it has

no roots in $\mathbb{Z}_5$
and its degree 2.

So,

$$K = \mathbb{Z}_5[x]/(x^2+\bar{2})$$

is a field.

The elements are

$$K = \{(a+bx)+I \mid a,b \in \mathbb{Z}_5\}$$

and $I = (x^2+\bar{2})$.

K has 25 elements.

(3) $\alpha = \sqrt{3+\sqrt{6}}$.

So, $\alpha^2 = 3+\sqrt{6}$.

Thus, $\alpha^2 - 3 = \sqrt{6}$.

Hence $(\alpha^2-3)^2 = 6$.

Thus, $\alpha^4 - 6\alpha^2 + 3 = 0$.

Let $p(x) = x^4 - 6x^2 + 3$.

Then p is irreducible over $\mathbb{Q}$ using Eistenstein with $p=3$. And $p(\alpha)=0$.

Since p is monic, irreducible and $p(\alpha)=0$ we have $p(x) = \min_{\alpha,\mathbb{Q}}(x)$. ↗

So,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(m_{\alpha, \mathbb{Q}}(x))$$
$$= 4.$$

Thus,

$$\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 + d\alpha^3 / q, b, c, d \in \mathbb{Q}\}$$

(A) Suppose that

$ux = ab$ where $a, b \in R$.

we must show either a or b is a unit of R.

Since u is a unit, u^{-1} exists in R.

Then, $x = (u^{-1}a)b$.

Since x is irreducible

either $u^{-1}a$ or b

is a unit in R.

If b is a unit we are done.

(B) Suppose $u^{-1}a = v$ is a unit of R.

Then $a = uv$ is a unit

since $(uv)^{-1} = u^{-1}v^{-1}$.

So we have shown that if $ux = ab$ where $a, b \in R$, then either a is a unit or b is a unit. Hence ux is irreducible in R.

(B)

(⇒) Suppose $K = F$. Then a basis for K over F is $\{1\}$, since $K = \{f \cdot 1 \mid f \in F\}$.

So, $[K : F] = 1$.

(⇐) Suppose $[K : F] = 1$. Then there is a basis for K over F of size 1. Let $\beta = \{k\}$ where $k \in K$, and

$$K = \{f \cdot k \mid f \in F\}.$$

Clearly $F \subseteq K$ since this is given.

Why is $K \subseteq F$? (2)

Note that since $1 \in K$ we have $1 = fk$ where $f \in F$, $f \neq 0$.

So, $k = f^{-1}1 = f^{-1} \in F$.

Thus,

$$K = \{fk \mid f \in F\} \subseteq F$$

(f in F, k in F)

So, $K = F$.

(c) $F \subseteq K$, $[K:F] = n$.

$f(x) \in F[x]$ is irreducible of degree m.

Let $\gcd(n, m) = 1$.

(a) Contrapositives

Suppose that f has a root in K, Let α be such a root.

Then $F(\alpha) \subseteq K$

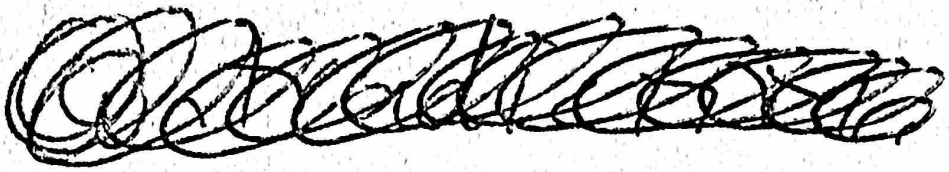
and

$$n = [K:F] = [K:F(\alpha)][F(\alpha):F]$$

$$= [K:F(\alpha)] \cdot m$$

So, $m \mid n$. (2)

Thus, $\gcd(m,n) \geq m > 1$.



(b) Is the converse true?
Ie, if f has no root in k then $\gcd(m,n)=1$?

$\mathbb{Q}(\sqrt[n]{2}) = k$

$| \; 2 = n$

$\mathbb{Q}$

$m=2$

$f(x) = x^2 + 1$

f has no root in k but $\gcd(2,2) = 2 > 1$

$\pm\lambda$ are the roots of f