Content:

Question	If $E \subsetneq K$, is $[E:F] < [K:F]$? Yes.
Example	$\sqrt{3} + \sqrt{5}$ is algebraic over $\mathbb{Q}$.
Example	Construct a field of order 8.
Example	To solve $f(x) = x^2 + 1 \in \mathbb{R}[x]$, we made up i.
Theorem	Kronecker's Theorem. If F is a field and $f(x) \in F[x]$ such that $f(x)$ is not constant, then there is an extension, E of F, that contains a root of $f(x)$.
Example	$\mathbb{R}(i) \cong \mathbb{R}[x]/(x^2 + 1)$
Corollary	(Also Kronecker's) If F is a field and $f(x) \in F[x]$ is nonconstant, then there is an extension E of F in which f can be factored as a product of linear polynomials.
Example	$f(x) = x^4 - 1 \in \mathbb{R}[x]$. Then $f(x) = (x + 1)(x - 1)(x + i)(x - i)$ in $\mathbb{C}[x]$.
Example	$f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Then $f(x) = (x + \sqrt{2})(x - \sqrt{2}) \in \mathbb{Q}[x]$.
Definition	splits; splitting field
Proposition	If F is a field and $f \in F[x]$ is nonconstant, then a splitting field of f exists.

Question If $E \subsetneq K$ and all extensions are finite, is $[E:F] < [K:F]$? Yes.

Proof:

Claim: $[K:E] = 1 \Rightarrow K = E$.

Assume $[K:E] = 1$.

Then $\exists\ v \in K$ such that $\{v\}$ is a basis for K over E.

We know $1 \in K$, so $1 = cv$ for some $c \in E$.

So $v = c^{-1} \in E$.

Since $K = \{cv \mid c \in E\}$, then $K \subseteq E$.

And since K is an extension of E (i.e. $E \subseteq K$),

then we have $E = K$.

$\therefore E \subsetneq K \Rightarrow [K:E] > 1$

As previously proven (lecture notes 3/15/10)

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

So then $[K:F] > 1 \bullet [E:F]$.

Recall $[E:F] < \infty \Rightarrow E$ is algebraic over F.

Example $\sqrt{3}+\sqrt{5}$ is algebraic over $\mathbb{Q}$.

Proof:
We could find a polynomial over Q with $\sqrt{3}+\sqrt{5}$ as a root.
Or…
First note that
(1) $\mathbb{Q}(\sqrt{3},\sqrt{5}) = [\mathbb{Q}(\sqrt{3})](\sqrt{5})$ (i.e. $\mathbb{Q}(\sqrt{3},\sqrt{5})$ is an extension of $\mathbb{Q}(\sqrt{5})$).
(2) Recall from Lecture Notes 3/10/10 (If E/F is an extension, $a \in E$ where a is algebraic over F, $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root, deg $p(x) = n$, then (1) every element in $F(a)$ can be expressed uniquely as $c_0 + c_1a + \cdots + c_na^n$ where $c_i \in F$; and (2) $[F(a):F] = n$.), so
$f(x) = x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{5})[x]$ and $f(\sqrt{3}) = 0$, gives us
$[\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{5})] \le 2$.
Also $g(x) = x^2 - 5$ is irreducible in $\mathbb{Q}[x]$ and $g(\sqrt{5}) = 0$ gives us
$[\mathbb{Q}(\sqrt{5}):\mathbb{Q}] = 2$.
(3) We have shown previously (Lecture Notes 3/10/10) that
$\mathbb{Q}(\sqrt{3}+\sqrt{5}) = \mathbb{Q}(\sqrt{3},\sqrt{5})$.
So now we have
$[\mathbb{Q}(\sqrt{3}+\sqrt{5}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}):\mathbb{Q}] \le 4$.
$\therefore$ $[\mathbb{Q}(\sqrt{3}+\sqrt{5}):\mathbb{Q}]$ is finite, hence $\sqrt{3}+\sqrt{5}$ is algebraic over $\mathbb{Q}$.

Example Construct a field of order 8.

$\mathbb{Z}_2[x]/(x^3 + x + 1)$ is a field of order 8.

Proof:
Recall
(1) Vector Space HW #9 (If $[V:\mathbb{Z}_p] = n$, then $|V| = p^n$.)
(2) Lecture Notes 3/10/10 (If E/F is an extension, $a \in E$ where a is algebraic over F, $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root, deg $p(x) = n$, then (1) every element in $F(a)$ can be expressed uniquely as $c_0 + c_1a + \cdots + c_na^n$ where $c_i \in F$; and (2) $[F(a):F] = n$.)
(3) By Theorem LN 3/10/10 (If E/F is an extension, $a \in E$, and a is algebraic over F, then $F(a) \cong F[x](p(x))$ where $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root.)
Since $8 = 2^3$, then we are looking for a field V such that $|V| = 2^3$.
By (1), if $[V:\mathbb{Z}_2] = 3$, then $|V| = 8$.
If $V = \mathbb{Z}_p$ for some prime p, then by (2) $[\mathbb{Z}_p(a):\mathbb{Z}_p] = n$ if a is a root of an irreducible polynomial $f(x)$ of degree n in $\mathbb{Z}_p[x]$.
And by (3) $\mathbb{Z}_p[x]/(f(x)) \cong \mathbb{Z}_p(a)$, which is a field of order p^n (by (2)).
Since $x^3 + x + 1$ and $x^3 + x^2 + 1$ are both irreducible in $\mathbb{Z}_2[x]$ we can use either one. Cardan's formula will give us a root to either polynomial. Let's just choose one and call it α.
Then $\mathbb{Z}_2[x]/(x^3 + x + 1) \cong \mathbb{Z}_2(\alpha)$, a field of order 8.

Example To solve $f(x) = x^2 + 1 \in \mathbb{R}[x]$, we made up i.

$$\mathbb{R}(i) \cong \mathbb{R}[x]/(x^2 + 1)$$
$$\cup|$$
$$\mathbb{R} \cong \mathbb{R}'$$

Theorem Kronecker's Theorem. Let F be a field and $f(x) \in F[x]$ such that $f(x)$ is not constant. Then there is an extension, E of F, that contains a root of $f(x)$.

Proof:
Actually, we will construct an extension field E' (we'll still call it E) of a field F' that is isomorphic to F.
Let F be a field. Let f be a nonconstant polynomial in $F[x]$.
If f is not irreducible, we can look at one of its irreducible factors. So we may assume f is irreducible.
Let $E = F[x]/(f(x))$. We know E is a field as f is irreducible over F.
Let $F' = \{c + (f(x)) \mid c \in F\}$.
Then $F' \subseteq E$ as $F \subseteq F[x]$ and $E = \{c(x) + (f(x)) | c(x) \in F[x]\}$.
Define $\varphi: F \to F'$ by $\varphi(a) = a + (f(x))$ $\forall$ $a \in F$.
To show φ is a homomorphism, let $a, b \in F$ and note that
$\varphi(a) + \varphi(b) = a + (f(x)) + b + (f(x)) = a + b + (f(x)) = \varphi(a + b)$, and
$\varphi(a)\varphi(b) = (a + (f(x)))(b + (f(x))) = ab + (f(x)) = \varphi(ab)$.
To show φ is injective, let $a, b \in F$ such that $\varphi(a) = \varphi(b)$.
Then $a + (f(x)) = b + (f(x))$. Thus $a - b \in (f(x))$. Since $a - b \in F$, then $\deg(a - b) = 0$ in $F[x]$ and we know $\deg f(x) \geq 1$ as $f(x)$ is nonconstant.
Consequently, $a - b = 0$, or $a = b$.
To show φ is surjective, let $w \in F'$. Then $w = c + (f(x))$ for some $c \in F$.
Thus $\varphi(c) = w$. And we have that φ is a bijection.
And so we have $F' \cong F$.
We can induce an isomorphism $\overline{\varphi}: F[x] \cong F'[x]$ by
$\overline{\varphi}(c_0 + c_1x + c_2x^2 + \cdots + c_nx^n) = \varphi(c_0) + \varphi(c_1)x + \varphi(c_2)x^2 \cdots \varphi(c_n)x^n$.
Denote $\overline{\varphi}(f(x))$ as $\overline{f}(x)$.
Let $\alpha = x + (f(x))$. If $f(x) = c_0 + c_1x + \cdots + c_nx^n$, then
$\overline{f}(x) = c_0 + (f(x)) + (c_1 + (f(x)))x + \cdots (c_n + (f(x)))x^n \in F'[x]$.
Claim: α is a root of $\overline{f}(x)$.

$$\begin{aligned}\overline{f}(\alpha) &= c_0 + (f(x)) + (c_1 + (f(x)))\alpha + \cdots (c_n + (f(x)))\alpha^n \\ &= c_0 + (f(x)) + (c_1 + (f(x)))(x + (f(x))) + \cdots (c_n + (f(x)))(x + (f(x)))^n. \\ &= c_0 + c_1x + \cdots + c_nx^n + (f(x)). \\ &= 0 + (f(x)). \\ &= 0_E.\end{aligned}$$

$\therefore$ $\overline{f}(x)$ has a root α in E, hence E is an extension of F (actually F', an isomorphic copy of F) that has a root of $f(x)$.

Example $\mathbb{R}(i) \cong \mathbb{R}[x]/(x^2 + 1)$

Let $i = x + (x^2 + 1)$. Then we have $f(x) = 1 + x^2$ and applying the isomorphism as defined in the preceding proof, we have

$\overline{f}(x) = 1 + (x^2 + 1) + [1 + (x^2 + 1)]x^2$. So

$\overline{f}(i) = 1 + (x^2 + 1) + [1 + (x^2 + 1)][x + (x^2 + 1)]^2$

$= 1 + (x^2 + 1) + [1 + (x^2 + 1)][x^2 + (x^2 + 1)]$

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

$= 1 + x^2 + (x^2 + 1) = 0.$

Corollary (Also Kronecker's) Let F be a field and $f(x) \in F[x]$ a nonconstant polynomial. Then there is an extension E of F with f a product of linear polynomials in $E[x]$.

Proof:

We will induct on deg $f(x)$. If deg $f(x) = 1$, then $f(x)$ is a linear polynomial. Hence $f(x) = a(x - c)$ for some $a, c \in F$, and this is a product of linear factors in $F[x]$.

Assume deg $f > 1$ and that any polynomial of degree less than deg f is a product of linear factors in some $E'[x]$ where E' is an extension of F.

Since F is a field, then $F[x]$ is a UFD, hence we can write $f(x) = p(x)g(x)$, where $p(x)$ is irreducible. By Kronecker's Theorem, there is a field E that contains a, a root of p.

Hence, in $E[x]$, we have $p(x) = (x - a)h(x)$ and so $f(x) = (x - a)h(x)g(x)$.

By our induction hypothesis, there is a field E' such that $F \subseteq E \subseteq E'$, where $h(x)g(x)$ is a product of linear factors in $E'[x]$, and hence $f(x)$ is a product of linear factors in $E'[x]$.

Example

$f(x) = x^4 - 1 \in \mathbb{R}[x].$

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

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

$= (x + 1)(x - 1)(x + i)(x - i)$ in $\mathbb{C}[x]$.

So $f(x)$ does not split over $\mathbb{R}$, but $f(x)$ does split over $\mathbb{C}$.

Example

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

$= (x + \sqrt{2})(x - \sqrt{2}) \in \mathbb{R}[x].$

So $f(x)$ does not split over $\mathbb{Q}$, but $f(x)$ does split over $\mathbb{R}$.

Definition If E/F is an extension and $f \in F[x]$, then

(1) We say $f(x)$ *splits* over E if f can be factored into linear polynomials over E.

(2) We say E is a *splitting field* of f if f splits over E and f does not split over any proper subfield of E.

Proposition If F is a field and $f \in F[x]$ is nonconstant, then a splitting field of f exists.

Proof:
By Kronecker's Theorem, there is a field E containing F such that $f(x) = a(x - c_1)(x - c_2)\cdots(x - c_n) \in E[x]$.
Claim: $F(c_1, \ldots, c_n)$ is a splitting field for f.

We first show f splits over $F(c_1, \ldots, c_n)$.
Since $c_1, \ldots, c_n \in F(c_1, \ldots, c_n)$, then $x - c_i \in F(c_1, \ldots, c_n)[x]$.
Thus, $f(x) = a(x - c_1)(x - c_2)\cdots(x - c_n) \in F(c_1, \ldots, c_n)[x]$.
$\therefore$ f splits over $F(c_1, \ldots, c_n)$.

And lastly, we show $F(c_1, \ldots, c_n)$ is the smallest field in which f splits.
Let K be a field in which f splits. Then $c_1, c_2, \ldots, c_n \in K$ (by Proposition 3.24) and $F \subseteq K$ as K is an extension of F. Since $F(c_1, \ldots, c_n)$ is the smallest field containing $c_1, c_2, \ldots, c_n$ and F (by definition), then $F(c_1, \ldots, c_n) \subseteq$ K.
$\therefore$ $F(c_1, \ldots, c_n)$ is a splitting field of f.