Content:

Example	$[\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] = 3$; $[\mathbb{Q}(\sqrt{1+\sqrt{2}}): \mathbb{Q}] = 4$
Example	$f(x) = x^2 + x + 2 \in \mathbb{Z}[x]$, $a \in E$ where $E/\mathbb{Z}_3$ is an extension, then $a^3 = 2a$, and $a^{17} = a$.
Theorem	If E/F is an extension, $a \in E$, a is algebraic over F, then (1) $\exists!$ monic irreducible polynomial $p(x)$ such that a is a root; and (2) $p(x)$ is of minimal degree among all polynomials that have a as a root.
Definition	irr(a, F), min(a, F)
Theorem	If E/F is an extension, $a \in E$, then $[F(a):F] < \infty \Leftrightarrow a$ is algebraic over F.
Theorem	Let E/F be an extension then $[E:F] < \infty \Rightarrow E$ is algebraic over F.
Example	$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2},\ldots):\mathbb{Q}] = \infty$, but $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2},\ldots$ are algebraic elements.
Theorem	Let K/E be an extension and E/F be an extension. If $[K:E]$ and $[E:F]$ are both finite, then $[K:F] = [K:E][E:F]$.
Example	If E/F and K/F are extensions and $E \subseteq K$, then $[K:E] \geq [E:F]$.

Summary If a is algebraic over F, then we can figure out what elements in $F(a)$ look like.
We find $p(x)$, an irreducible polynomial in $F[x]$ such that $p(a) = 0$.
Since $F(a) \cong F[x]/(p(x))$, we know what elements in here look like.
If $[F(a):F] = \deg p(x) = n$, then
$c_0 + c_1 a + \cdots + c_n a^n$ is an arbitrary element in $F(a)$.

Example $[\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] = 3$

Proof:
Since $p(x) = x^3 - 2$ is irreducible (by rational root test), and $p(\sqrt[3]{2}) = 0$, then $[\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] = \deg(x^3 - 2) = 3$.

Example $[\mathbb{Q}(\sqrt{1+\sqrt{2}}): \mathbb{Q}] = 4$

Proof:
Since (*) $p(x) = x^4 - 2x - 1$ is irreducible
(as $p(x + 1) = x^4 + 4x^3 + 4x^2 - 2$ is an Eisenstein polynomial)
and $p(\sqrt{1+\sqrt{2}}) = 0$, then
$[\mathbb{Q}(\sqrt{1+\sqrt{2}}): \mathbb{Q}] = \deg(x^4 - 2x - 1) = 4$.
(*) We find $p(x) = x^4 - 2x - 1$ by noting that
$(\sqrt{1+\sqrt{2}})^2 = 1 + \sqrt{2}$ and
$(\sqrt{1+\sqrt{2}})^4 = 3 + 2\sqrt{2}$. Since
$3 + 2\sqrt{2} - 2(1 + \sqrt{2}) - 1 = 0$, then we have
$p(x) = x^4 - 2x - 1$ where $p(\sqrt{1+\sqrt{2}}) = 0$,

Example $f(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$, $a \in E$ where $E/\mathbb{Z}_3$ is an extension, and $f(a) = 0$, then $a^3 = 2a + 1$, and $a^{17} = a$.

Proof:
Since $f(x)$ is irreducible (Rational Root test) and $f(a) = 0$, then $[\mathbb{Z}_3(a): \mathbb{Z}_3] = 2$. Then elements in $\mathbb{Z}_3(a)$ look like $c_0 + c_1a$; $c_0, c_1 \in \mathbb{Z}_3$.
We know $a^2 \in \mathbb{Z}_3(a)$ and $a^2 + 2a + 2 = 0$. Thus $a^2 = -2a - 2 = a + 1$.
And $a^3 = a^2 \bullet a = (a + 1) \bullet a = a^2 + a = a + 1 + a = 2a + 1$.
For a^{17} we could continue the procedure above, or use group theory.
Since $|\mathbb{Z}_3(a)| = 3^2 = 9$, then $9b = 0$ $\forall$ $b \in \mathbb{Z}_3(a)$.
Since $|\mathbb{Z}_3(a)^*| = 8$, then $b^{8k} = 1$ $\forall$ $b \in \mathbb{Z}_3(a)^*$.
So $a^{17} = (a^8)^2a = a$.

Theorem If E/F is an extension, $a \in E$, a is algebraic over F, then
(1) $\exists!$ monic irreducible polynomial $p(x)$ such that a is a root; and
(2) $p(x)$ is of minimal degree among all polynomials that have a as a root.
(3) If $f(x) \in F[x]$ such that $f(a) = 0$, then $p(x) | f(x)$.

Proof:
Define $\varphi_a: F[x] \to E$ by $\varphi_a(f(x)) = f(a)$.
Since $F[x]$ is a PID and $\ker \varphi_a$ is an ideal, $\exists$ $g(x) \in F[x]$ such that $\ker \varphi_a = (g(x))$. Let $g(x) = c_0 + c_1x + \cdots + c_nx^n$. If we let $p(x) = c_n^{-1} \bullet g(x)$, then $p(x)$ is a monic associate of $g(x)$ as c_n^{-1} is a unit in F. So by Homework 1, Exercise #5(c), $(g(x)) = (p(x))$.
And we have also proven previously that $p(x)$ is of minimal degree in $(p(x))$. Since $\ker \varphi_a = \{f(x) \in F[x] | f(a) = 0\}$, then we have proven part (2) of the desired result.

Claim (1): $p(x)$ is irreducible.
Suppose it is not.
Then $\exists$ $h(x), k(x) \in F[x]$ such that $p(x) = h(x)k(x)$ and $\deg h, \deg k < n$.
Since $\ker \varphi_a = \{f(x) \in F[x] | f(a) = 0\}$ and $p(x)$ is of minimal degree, then $h(x) \notin \ker \varphi_a$, and $k(x) \notin \ker \varphi_a$.
But $0 = \varphi_a(f(x)) = \varphi_a(h(x)k(x)) = \varphi_a(h(x)) \bullet \varphi_a(k(x)) = h(a)k(a)$, a contradiction as $\varphi_a(h(x)), \varphi_a(k(x)) \in E$, a field, which has no zero divisors.

Claim (2): $p(x)$ is unique.
Suppose $q(x)$ is a monic irreducible polynomial such that $q(a) = 0$.
Then $p(x) | q(x)$ by definition of $(p(x))$. Note that this gives us part (3) of the desired result.
And $p(x) | q(x) \Rightarrow q(x) = p(x)j(x)$.
Since $p(x)$ and $q(x)$ are irreducible, then $j(x) \in F$.
Thus $\deg q(x) = \deg p(x)$. And since they are both monic, then $j(x) = 1$.
$\therefore$ $p(x)$ is unique. And this gives us part (1) of the desired result.

Definition If E/F is an extension, $a \in E$, a is algebraic over F, then the monic irreducible polynomial $p(x)$ such that a is a root is denoted as *irr(a, F)* or *min(a, F).* (Now that we have uniqueness, we can call it "the" monic irreducible polynomial for a or the minimal polynomial for a over F.)

Theorem If E/F is an extension, $a \in E$, then
$[F(a):F] < \infty \Leftrightarrow a$ is algebraic over F.

Proof:
$\Rightarrow$: Suppose $[F(a):F] < \infty$.
Then $[F(a):F] = n \in \mathbb{N}$.
By definition of $F(a)$, we know $\{1, a, \ldots, a^n\} \subseteq F(a)$.
Since $[F(a):F] = n$, then $\{1, a, \ldots, a^n\}$ is linearly dependent over F.
So there are $c_i \in F$, not all 0 such that $c_0 + c_1a + \cdots + c_na^n = 0$.
Thus, $f(x) = c_0 + c_1x + \cdots + c_nx^n$ is a non-zero polynomial in F[x] such that $f(a) = 0$.
$\therefore$ a is algebraic over F.

$\Leftarrow$: Assume a is algebraic over F.
By the theorem above, we know there is a monic irreducible polynomial $p(x)$ such that $p(a) = 0$.
And by the isomorphism $F(a) \cong F[x]/(p(x))$, we have
$[F(a):F] = \deg p(x) = n$.

Theorem Let E/F be an extension then
$[E:F] < \infty \Rightarrow E$ is algebraic over F.

Proof:
Suppose $[E:F] < \infty$. Then $[E:F] = n \in \mathbb{N}$.
Let $a \in E$ such that $a \notin F$.
By closure of the field E, we have $\{1, a, \ldots, a^n\} \subseteq E$.
Since $[E:F] = n$, then $\{1, a, \ldots, a^n\}$ is linearly dependent over F.
So there are $c_i \in F$, not all 0 such that $c_0 + c_1a + \cdots + c_na^n = 0$.
Thus, $f(x) = c_0 + c_1x + \cdots + c_nx^n$ is a non-zero polynomial in F[x] such that $f(a) = 0$.
$\therefore$ E is algebraic over F.

Example $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots):\mathbb{Q}] = \infty$, but
$\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots$ are algebraic elements.
This demonstrates that the converse of the above theorem is false.

Theorem Let K/E be an extension and E/F be an extension. If $[K:E]$ and $[E:F]$ are both finite, then $[K:F] = [K:E][E:F]$.

Proof:
Let $\{k_1, \ldots, k_n\}$ be a basis for K/E.
Let $\{b_1, \ldots, b_m\}$ be a basis for E/F.
Claim: $B = \{k_i b_j \mid 1 \le i \le n, 1 \le j \le m\}$ is a basis for K/F.
Note: If we prove this, we're done since $|B| = mn$.
Read this proof in the handout (Theorem 39)

Let $x \in K$. Then $x = d_1k_1 + d_2k_2 + \cdots + d_nk_n$ for some $d_i \in E$.
Also, each $d_i \in E$ can be written as $d_i = c_{i1}b_1 + + c_{i2}b_2 + \cdots + c_{im}b_m$ for some $c_{ij} \in F$. Substituting this linear combination for each d_i in the first equation, we get that x is a linear combination of elements of B. Thus, B spans K.

Now, suppose $\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}k_i b_j = 0$ for some $r_{ij} \in F$.

Then $\sum_{i=1}^{n}\left(\sum_{j=1}^{m} r_{ij}b_j\right)k_i = 0$ where $\sum_{j=1}^{m} r_{ij}b_j \in E$.

So since $\{k_1, \ldots, k_n\}$ is a basis for K/E (and thus linearly independent), we have $\sum_{j=1}^{m} r_{ij}b_j = 0$ for all i.

Thus, since $\{b_1, \ldots, b_m\}$ is a basis for E/F, we have $r_{ij} = 0$ for all j.
Thus, $r_{ij} = 0$ for all i and j.
$\therefore$ B is linearly independent over F, hence B is a basis for K/F,
So, $[K:F] = |B| = mn = [K:E][E:F]$.

Example If E/F and K/F are extensions and $E \subseteq K$, then $[K:E] \ge [E:F]$.

Proof (1):
By preceding theorem, we have $[K:F] = [K:E][E:F]$.
Since $[K:E] \ge 1$, then $[K:E] \ge [E:F]$.

Proof (2):
By exercise #6 in Vector Space Homework, we can extend the basis for E into a basis for K.