Content:

Example	$\mathbb{Q}[i] = \mathbb{Q}(i)$.
Theorem	If E/F is an extension, $a \in E$, then $F[a] = F(a) \Leftrightarrow F[a]$ is a field.
Example	$\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.
Definition	algebraic, transcendental, algebraic extension, transcendental ext.
Proposition	π and e are transcendental over $\mathbb{Q}$.
Example	$\mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$
Example	π^2 is transcendental over $\mathbb{Q}$.
Example	$\mathbb{Q}(i)/\mathbb{Q}$ is an algebraic extension.
Theorem	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.
Question	Can we find $p(x)$ for $\sqrt{3} + \sqrt{5}$?
Corollary	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 $c_0 + c_1 a + \cdots + c_n a^n$ where $c_i \in F$. (2) $[F(a):F] = n$.

Announcement Field Extension, Part I: #11, 12 due Wednesday
#18, 19 due Monday

Example $F[\alpha] = \{c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n \mid c_i \in F, n \in \mathbb{N} \cup \{0\}\}$ so
$\mathbb{Q}[i] = \{ c_0 + c_1(i) + c_2(i)^2 + \cdots + c_n(i)^n \mid c_i \in F, n \in \mathbb{N} \cup \{0\}\}$

Example Prove $\mathbb{Q}[i] = \mathbb{Q}(i)$.

Proof:
We get $\mathbb{Q}[i] \subseteq \mathbb{Q}(i)$ for free.

To show the reverse containment, we could show
$z \in \mathbb{Q}(i) \Rightarrow z \in \mathbb{Q}[i]$. But this would take some work.
It is easier to just show $\mathbb{Q}[i]$ is a field.
Let $a + bi \in \mathbb{Q}[i]$ where $a + bi \neq 0$.
Then since $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \in \mathbb{Q}[i]$, and
$(a + bi)\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\right) = 1$, then every nonzero element
of $\mathbb{Q}[i]$ is a unit, hence $\mathbb{Q}[i]$ is a field.
Since $\mathbb{Q}(i)$ is the smallest field containing Q and i, and
$\mathbb{Q}[i]$ is "a" field containing Q and i, then $\mathbb{Q}(i) \subseteq \mathbb{Q}[i]$.
$\therefore \mathbb{Q}[i] = \mathbb{Q}(i)$.

Theorem If E/F is an extension, $a \in E$, then $F[a] = F(a) \Leftrightarrow F[a]$ is a field.
Proof: You do it.
$\Rightarrow$: Is immediate.
$\Leftarrow$: Just do what we did before.

Assume $F[a] = F(a)$. Then since $F(a)$ is a field, $F[a]$ is a field.

Conversely, assume $F[a]$ is a field.
We already know $F[a] \subseteq F(a)$ (Lecture Notes 3/8/10)
And now we have $F[a]$ is a field that contains F and a.
Since $F(a)$ is the smallest field containing F and a, then
$F(a) \subseteq F[a]$, consequently $F[a] = F(a)$.

Example $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.
Proof:
Since $\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$ and $\mathbb{Q} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$, then
$\mathbb{Q}(\sqrt{3} + \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$.
To show the reverse containment, notice that

$$(\sqrt{3} + \sqrt{5})\left(\frac{\sqrt{3} - \sqrt{5}}{-2}\right) = 1,$$

$$\Rightarrow -\frac{1}{2}\sqrt{3} + \frac{1}{2}\sqrt{5} = (\sqrt{3} + \sqrt{5})^{-1} \in \mathbb{Q}(\sqrt{3} + \sqrt{5})$$

$$\Rightarrow 2\left(-\frac{1}{2}\sqrt{3} + \frac{1}{2}\sqrt{5}\right) = -\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3} + \sqrt{5})$$

$$\Rightarrow 2\sqrt{5} = -\sqrt{3} + \sqrt{5} + \sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3} + \sqrt{5})$$

$$\Rightarrow \sqrt{5} = -\frac{1}{2}(2\sqrt{5}) \in \mathbb{Q}(\sqrt{3} + \sqrt{5})$$

$$\Rightarrow \sqrt{3} = (\sqrt{3} + \sqrt{5}) - \sqrt{5} \in \mathbb{Q}(\sqrt{3} + \sqrt{5}).$$

$\therefore \mathbb{Q}(\sqrt{3} + \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$, hence $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

Definition Let E/F be an extension and $a \in E$.
(1) a is *algebraic* over F is $\exists f(x) \in F[x]$ where $f(x) \neq 0$ and a is a root of $f(x)$.
(2) a is *transcendental* over F is no such $f(x)$ exists.
(3) E/F is an *algebraic extension* if all elements in E are algebraic over F.
(4) E/F is a *transcendental extension* otherwise.

Proposition π and e are transcendental over $\mathbb{Q}$.
Proof:
e is transcendental given by Lindemann, 1882.
π is transcendental given by Hermite, 1873.

Example $\mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$.

Proof:
By the theorem above, $\mathbb{Q}[\pi] = \mathbb{Q}(\pi)$ if $\mathbb{Q}[\pi]$ is a field.
Suppose $\mathbb{Q}[\pi]$ is a field, then $\pi^{-1} \in \mathbb{Q}[\pi]$, thus
$\mathbb{Q}[\pi]$ is a field $\Rightarrow \pi^{-1} \in \mathbb{Q}[\pi]$
$\Rightarrow \pi(c_0 + c_1\pi + \cdots + c_n\pi^n) = 1$
$\Rightarrow -1 + c_0\pi + c_1\pi^2 + \cdots + c_n\pi^{n+1} = 0$
$\Rightarrow f(\pi) = 0$ where $f(x) = -1 + c_0x + c_1x^2 + \cdots + c_nx^{n+1} \in \mathbb{Q}[x]$.
But we know π is transcendental over $\mathbb{Q}$, so this is a contradiction.
$\therefore \mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$.

Note If you have a polynomial with a as a root, you can construct an inverse. Start with $-1 + c_0x + c_1x^2 + \cdots + c_nx^{n+1} \in \mathbb{Q}[x]$ and work backwards to $a(c_0 + c_1a + \cdots + c_na^n) = 1$.

Example π^2 is transcendental over $\mathbb{Q}$.
Proof:
Suppose π^2 is algebraic over $\mathbb{Q}$.
Then $\exists f(x) = c_0 + c_1x + \cdots + c_nx^n \in \mathbb{Q}[x]$ such that
$0 = f(\pi^2) = c_0 + c_1\pi^2 + \cdots + c_n\pi^{2n}$.
If $g(x) = c_0 + c_1x^2 + c_2x^4 + \cdots + c_nx^{2n}$, then
$g(\pi) = c_0 + c_1\pi^2 + \cdots + c_n\pi^{2n} = 0$.
But π is transcendental over $\mathbb{Q}$, so this is a contradiction.
$\therefore \pi^2$ is transcendental over $\mathbb{Q}$.

Example $\mathbb{Q}(i)/\mathbb{Q}$ is an algebraic extension.

Proof:
$\mathbb{Q}(i)/\mathbb{Q}$ is an algebraic extension if every element of $\mathbb{Q}(i)$ is algebraic over $\mathbb{Q}$, so we just need to show $\forall\, a, b \in \mathbb{Q}$, $a + bi$ is algebraic over $\mathbb{Q}$.
Let $a, b \in \mathbb{Q}$ and let $f(x) = x^2 - 2ax + a^2 + b^2$.
Then $f(a + bi) = (a + bi)^2 - 2a(a + bi) + a^2 + b^2$
$= a^2 + 2abi - b^2 - 2a^2 - 2abi + a^2 + b^2 = 0$.
Thus, for any element $a + bi$ of $\mathbb{Q}(i)$, there is a nonzero polynomial $f(x) \in \mathbb{Q}[x]$ for which $f(a + bi) = 0$.

Theorem Let E/F is an extension and $a \in E$. If 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.

Proof:

Let $a \in E$ such that a is algebraic over F.

Define $\varphi_a: F[x] \to E$ by $\varphi_a(f(x)) = f(a)$. Then $\ker \varphi_a = (p(x))$ (hw).

Since a is algebraic over F, then $\exists\, f(x) \in F[x]$ where $f(x) \neq 0$ and a is a root of $f(x)$. Since F is a field, then $F[x]$ is a UFD, hence $f(x)$ can be factored into a product of irreducibles.

So we can write $f(x) = p_1(x)^{e1}\, p_2(x)^{e2} \cdots p_r(x)^{er}$ where $r \leq \deg f(x)$, $\deg p_i(x) < \deg f(x)$ and $p_i(x)$ are distinct irreducibles for all i such that $1 \leq i \leq r$. Thus, $\exists\, i$ such that $p_i(a)^{ei} = 0$

(otherwise $0 = f(a) = p_1(a)^{e1}\, p_2(a)^{e2} \cdots p_r(a)^{er} \neq 0$.)

Ignoring multiplicities, suppose $\exists\, j$ such that $p_j(x) \neq p_i(x)$ and $p_j(a) = p_i(a) = 0$. Without loss of generality, suppose $p_1(x)$ is an irreducible polynomial of least degree such that $p_1(a) = 0$.

And suppose $p_2(a) = 0$. Then $\exists\, q(x), r(x) \in F[x]$ such that $p_2(a) = p_1(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg p_1(x)$. Since $r(x) = p_2(x) - p_1(x)q(x)$, then $r(a) = p_2(a) - p_1(a)q(a) = 0 - 0 \bullet q(x) = 0$. But $p_1(x)$ is the polynomial of least degree such that $p_1(a) = 0$, so $r(x) = 0$. Hence $p_2(x) = p_1(x)q(x)$.

And since $p_2(x)$ is irreducible, then $q(x)$ is a unit.

Thus $p_2(x)$ and $p_1(x)$ are associates and $(p_2(x)) = (p_1(x))$.

Thus $\ker \varphi_a = \{f(x) \in F[x] \mid f(a) = 0\} = (p_1(x))$.

By the First Isomorphism Theorem, $F[x]/(p(x)) \cong \varphi_a(F[x])$.

Recall that $\varphi_a(F[x]) = F[a]$ (Lecture Notes 3/8/10).

Since F is a field, then $F[x]$ is a PID, hence

$p(x)$ is irreducible $\Rightarrow (p(x))$ is maximal.

Thus $F[x]/(p(x))$ is a field. So then $F[x]/(p(x)) \cong \varphi_a(F[x]) = F[a]$ gives us that $F[a]$ is a field. And $F[a]$ is a field $\Rightarrow F[a] = F(a)$ by the theorem above. $\therefore\ F(a) \cong F[x]/(p(x))$.

Example Can we find $p(x)$ for $\sqrt{3}+\sqrt{5}$?
By the theorem above, since $\sqrt{3}+\sqrt{5}$ is algebraic over $\mathbb{Q}$, then $\mathbb{Q}(\sqrt{3}+\sqrt{5}) \cong \mathbb{Q}[x]/(p(x))$ where $p(x)$ is irreducible in $\mathbb{Q}[x]$ and $p(\sqrt{3}+\sqrt{5}) = 0$.
To find $p(x)$, notice that $(\sqrt{3}+\sqrt{5})^2 = 8 + 2\sqrt{15} = 2(4+\sqrt{15})$.
And $(\sqrt{3}+\sqrt{5})^4 = (2(4+\sqrt{15}))^2 = 4(31+8\sqrt{15})$. So
$(\sqrt{3}+\sqrt{5})^4 - 16(\sqrt{3}+\sqrt{5})^2 + 4 = 4(31+8\sqrt{15}) - 16(2(4+\sqrt{15})) - 4$
$= 124 + 32\sqrt{15} - 128 - 32\sqrt{15} - 4 = 0$.
Thus $f(\sqrt{3}+\sqrt{5}) = 0$ if $f(x) = x^4 - 16x - 4$.
To show $f(x)$ is irreducible, note that $f(1) = -19$, $f(-1) = 13$, $f(2) = -20$, $f(-2) = 44$, $f(4) = 188$, $f(-4) = 316$. So $f(x)$ has no linear factors. Suppose $f(x) = (x^2 + ax + b)(x^2 + cx + d)$, then
$c + a = 0$; $d + ac + b = -16$; $ad + bc = 0$; $bd = -4$.
So $c = -a$, hence $d - a^2 + b = -16$; $ad - ab = 0$. Thus $d = b$.
And now we have $b^2 = -4$, a contradiction.
$\therefore f(x) \neq (x^2 + ax + b)(x^2 + cx + d)$ due to impossible restrictions on the coefficients. Thus $f(x)$ is the desired irreducible polynomial.

Note From this example, we have $\mathbb{Q}(\sqrt{3}+\sqrt{5}) \cong \mathbb{Q}[x]/(x^4 - 16x - 4)$.
In $\mathbb{Q}(\sqrt{3}+\sqrt{5})$, elements look like
$c_0 + c_1(\sqrt{3}+\sqrt{5}) + c_2(\sqrt{3}+\sqrt{5})^2 + c_3(\sqrt{3}+\sqrt{5})^3 + \cdots$.
In $\mathbb{Q}[x]/(x^4 - 16x - 4)$, elements look like
$g(x) + (x^4 - 16x - 4)$ where $g(x) = 0$ or $\deg g(x) < 4$
(i.e. $c_0 + c_1x + c_2x^2 + c_3x^3 + (x^4 - 16x - 4)$).
By the isomorphism we can conclude that all elements in $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ are linear combinations of 1, $\sqrt{3}+\sqrt{5}$, $(\sqrt{3}+\sqrt{5})^2$, and $(\sqrt{3}+\sqrt{5})^3$, hence $\{1, \sqrt{3}+\sqrt{5}, (\sqrt{3}+\sqrt{5})^2, (\sqrt{3}+\sqrt{5})^3\}$ is a basis for $\mathbb{Q}(\sqrt{3}+\sqrt{5})$.

Corollary Let E/F be an extension, $a \in E$ where a is algebraic over F. Let $p(x)$ be an irreducible polynomial in $F[x]$ such that a is a root. If deg $p(x) = n$, then

(1) every element in $F(a)$ can be expressed uniquely as $c_0 + c_1a + \cdots + c_na^{n-1}$ where $c_i \in F$.

Proof:
This follows from the fact that elements in $F[x]/(p(x))$ can be expressed uniquely as $f(x) + (p(x))$ where $f(x) = 0$ or deg $f(x) < n$.

By previous theorem, we have $F(a) \cong F[x]/(p(x))$.
Since $F(a)$ contains F and a, then by closure, every element in $F(a)$ can be expressed as $c_0 + c_1a + c_2a^2 \cdots$ where $c_i \in F$.
And since elements in $F[x]/(p(x))$ can be expressed uniquely as $f(x) + (p(x))$ where $f(x) = 0$ or deg $f(x) < n$, then by the isomorphism, φ_a: $F[x]/(p(x)) \to F(a)$ defined by $\varphi_a(f(x) + (p(x))) = f(a)$, we have every element in $F(a)$ can be expressed uniquely as $c_0 + c_1a + \cdots + c_na^{n-1}$ where $c_i \in F$.

(2) $[F(a):F] = n$.

Proof:
Since we have from (1) that every element in $F(a)$ can be expressed uniquely as $c_0 + c_1a + \cdots + c_na^n$ where $c_i \in F$, then
by Vector Space HW #8, $\{1, a, \ldots, a^{n-1}\}$ is a basis for $F(a)$ over F.
Thus $[F(a):F] = n$.