Math 403 Chapter 21: Algebraic Extensions

1. Introduction: Extension fields may be categorized several different ways. In this chapter we will look at some of these divisions.

2. Algebraic v Transcendental

(a) Definition: Given an extension field $E$ of $F$ and an element $a \in E$, we say that $a$ is **algebraic over $F$** if $a$ is the root of a polynomial in $F$. Otherwise we say it is **transcendental over $F$**.

   Note: The base field $F$ is important here. Often when people just say “transcendental” they mean over $\mathbb{Q}$ but that isn’t the only possibility.

   Example: $\sqrt{2} \in \mathbb{R} \supseteq \mathbb{Z}$ is algebraic over $\mathbb{Z}$ because it is a root of the polynomial $x^2 - 2 \in \mathbb{Z}[x]$.

   Example: $\sqrt{2} + \sqrt{3} \in \mathbb{R} \supseteq \mathbb{Z}$ is algebraic over $\mathbb{Z}$ because it is a root of the polynomial $x^4 - 4x^2 + 1 \in \mathbb{Z}[x]$.

   Example: $\pi \in \mathbb{R} \supseteq \mathbb{Z}$ is transcendental over $\mathbb{Z}$ because there is no polynomial in $\mathbb{Z}[x]$ for which $\pi$ is a root. This is hard to prove.

   Example: $\pi \in \mathbb{C} \supseteq \mathbb{R}$ is algebraic over $\mathbb{R}$ because it is a root of the polynomial $x - \pi \in \mathbb{R}[x]$.

(b) Definition: An extension field $E$ of $F$ is called an **algebraic extension of $F$** if every element of $E$ is algebraic over $F$. Otherwise we say it is a **transcendental extension of $F$**.

(c) Definition: An extension field of the form $F(a)$ is a simple extension of $F$.

3. Algebraic Extensions

(a) Introduction: Here we will focus specifically on a theorem related to algebraic extensions. It basically revisits something we know but from an opposite direction.

(b) Theorem: Let $E$ be an extension field of $F$ and let $a \in E$. If $a$ is algebraic over $F$ then $F(a) \approx F[x]/\langle p(x) \rangle$ where $p(x)$ is a polynomial in $F[x]$ of minimal degree for which $p(a) = 0$. In addition such a $p(x)$ will be irreducible over $F$.

   Note: This isomorphism arose earlier in the FTOFT but in that case we started with an irreducible polynomial and constructed an extension field in which a root existed whereas in this case we starting with an extension field that we know about and a root in that extension field and an irreducible polynomial emerges.

   Proof: If $a$ is algebraic over $F$ then define $\phi : F[x] \to F(a)$ by $\phi(f(x)) = f(a)$. By the First Isomorphism Theorem we know that

   $$F[x]/\text{Ker}\ \phi \approx \phi(F[x]) \subseteq F(a)$$

Since $a$ is algebraic over $F$ there are $f(x) \in F[x]$ with $f(a) = 0$ and so $\text{Ker}\ \phi \neq 0$. Thus we know that $\text{Ker}\ \phi$ is a nonzero ideal of $F[x]$ which can be written in the form $\langle p(x) \rangle$ (since $F[x]$ is a PID) where $p(x)$ is a polynomial of minimal degree in the ideal (previous theorem). Since $p(x)$ has minimal degree it must be irreducible since if we could reduce $p(x) = f(x)g(x)$ then $0 = p(a) = f(a)g(a)$ would imply a polynomial of lower degree for which $a$ were a root.

Now then since $p(x)$ is irreducible we know that $\langle p(x) \rangle$ is maximal (previous theorem) and hence $F[x]/\langle p(x) \rangle$ is a field (previous theorem) and since $F[x]/\langle p(x) \rangle \approx \phi(F[x])$ we know that $\phi(F[x])$ is a subfield of $F(a)$ containing both $F$ (since $\phi(c) = c$ for $c \in F$) and $a$ (since $\phi(x) = a$). But $F(a)$ is the smallest such subfield and so $\phi(F[x]) = F(a)$ and the result follows. 

QED
Example: Consider $\sqrt{2} \in \mathbb{R} \supseteq \mathbb{Q}$ is algebraic over rationals, since it’s a root of, among other things, $x^2 - 2 \in \mathbb{Q}[x]$, and so $\mathbb{Q}(\sqrt{2}) \approx F[x]/\langle p(x) \rangle$ where $p(x)$ is a polynomial in $\mathbb{Q}[x]$ of minimal degree which is irreducible over $\mathbb{Q}$. In fact we know that $\mathbb{Q}(\sqrt{2}) \approx F[x]/\langle x^2 - 2 \rangle$ but in this new theorem we started with $\sqrt{2}$ and the theorem proves the existence of the polynomial from the field extension rather than the other way around.

(c) Corollary: If $a \in E \supseteq F$ is algebraic over $F$ then there is a unique monic irreducible polynomial in $F[x]$ for which $a$ is a root.

Proof: If $p(x)$ is the polynomial arising in the previous proof then we can multiply by the multiplicative inverse of the leading coefficient to get a monic irreducible polynomial. To show it is unique suppose $p_1(x) \neq p_2(x)$ were both monic irreducible polynomials of minimal degree with $p_1(a) = p_2(a) = 0$. Then $(p_1 - p_2)(x)$ would be a nonzero polynomial of smaller degree for which $a$ is a root. Now then either $p_1 - p_2$ itself is irreducible or it has an irreducible factor which will also have $a$ as a root. Either way we have a nonzero polynomial of smaller degree for which $a$ is a root, a contradiction. $\square$

(d) Definition: The polynomial arising in the previous theorem is called the minimal polynomial for $a$ over $F$.

(e) Corollary: If $p(x)$ is the minimal polynomial for $a \in E \supseteq F$ over $F$ then for all $f(x) \in F[x]$ with $f(a) = 0$ we have $p(x) | f(x)$ in $F[x]$.

Proof: For any other $f(x) \in F[x]$ with $f(a) = 0$ we know that $f(x) \in \text{Ker } \phi = \langle p(x) \rangle$ with the $\phi$ from the theorem. Then $p(x) | f(x)$ by definition of $\langle p(x) \rangle$. $\square$

4. The Degree of an Extension

(a) Definition: Let $E$ be an extension field of $F$. We say that $E$ has degree $n$ over $F$ and write $[E : F] = n$ if $E$ has dimension $n$ as a vector space over $F$. If $[E : F]$ is finite we say that $E$ is a finite extension of $F$ and otherwise we say that $E$ is an infinite extension of $F$.

Note: Basically (haha) if we can find a set $B = \{b_1, ..., b_n\}$ taken from $E$ such that every element of $E$ can be written uniquely as a linear combination of elements of $B$ using coefficients in $E$ then $B$ is the basis and $[E : F] = n$ is the dimension.

Example: We have $[\mathbb{C} : \mathbb{R}] = 2$ since $\{1, i\}$ form a basis for $\mathbb{C}$ over reals because every element of $\mathbb{C}$ can be written in the form $a(1) + b(i)$ with $a, b \in \mathbb{R}$.

Example: We have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 3$ because elements in $\mathbb{Q}(\sqrt{2})$ have the unique form $c_0 + c_1 \sqrt{2} + a_2 (\sqrt{2})^2$ with $c_0, c_1, c_2 \in \mathbb{Q}$ by a previous theorem.

(b) Theorem: If $E$ is a finite extension of $F$ then each $a \in E$ is algebraic over $F$ and so $E$ is algebraic over $F$.

Proof: Suppose $[E : F] = n$ and $a \in E$. The set $\{1, a, ..., a^n\}$ contains more than $n$ elements and hence is linearly dependent over $F$, meaning there are constants $c_0, ..., c_n$ with $c_0 + c_1 a + ... + c_n a^n = 0$. Then $a$ is a root of $f(x) = c_0 + c_1 x + ... + c_n x^n$ and hence is algebraic. $\square$

Note: The converse is false, for example $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, ...)$ (forever!) is algebraic but not finite. Do you see why?

(c) Theorem: If we have finite field extensions $F \subseteq E \subseteq K$ then $[K : F] = [K : E][E : F]$.

Proof: Omit. The details are just icky and unenlightening and the basic idea can be captured with an example. $\square$

Example: Suppose we take $\mathbb{Q}$ and extend it to $\mathbb{Q}(\sqrt{2})$ have a degree 2 field extension with basis $\{1, \sqrt{2}\}$ in which all elements have the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$.

Suppose we then extend from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(\sqrt{2})(\sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. This is a degree 3 field extension with basis $\{1, \sqrt{5}, (\sqrt{5})^2\}$ in which all elements have the form $c + d\sqrt{5} + e(\sqrt{5})^2$ with $c, d, e \in \mathbb{Q}(\sqrt{2})$. 

Really then all elements in $Q(\sqrt{2}, \sqrt[3]{5})$ have the form:

$$c + d\sqrt{5} + e(\sqrt{5})^2 = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})\sqrt{5} + (a_3 + b_3\sqrt{2})(\sqrt{5})^2$$

$$= a_1 + b_1\sqrt{2} + a_2\sqrt{5} + b_2\sqrt{2}\sqrt{5} + a_3(\sqrt{5})^2 + b_3\sqrt{2}(\sqrt{5})^2$$

Thus $Q(\sqrt{2}, \sqrt[3]{5})$ is a degree 6 field extension of $Q$ with basis:

$$\{1, \sqrt{2}, \sqrt{5}, \sqrt{2}\sqrt{5}, (\sqrt{5})^2, \sqrt{2}(\sqrt{5})^2\}$$

Note that conceptually we could have extended it to $Q(\sqrt[3]{5})$ first, and this leads to the following diagram:

Note: The theorem can also inform us about what field extensions are possible and whether elements are or are not in field extensions.

Example: By the above example any field extension between $Q$ and $Q(\sqrt{2}, \sqrt[3]{5})$ must have degree over $Q$ which divides 6. This also tells us, for example, that $\sqrt[3]{7} \notin Q(\sqrt{2}, \sqrt[3]{5})$.

This is because if it were then we would have:

$$Q \subseteq Q(\sqrt[3]{7}) \subseteq Q(\sqrt{2}, \sqrt[3]{5})$$

and hence:

$$\left[Q(\sqrt{2}, \sqrt[3]{5}) : Q\right] = \left[Q(\sqrt[3]{7}) : Q(\sqrt{2}, \sqrt[3]{5})\right] \left[Q(\sqrt{2}, \sqrt[3]{5}) : Q\right]$$

However $4 \nmid 6$. 
5. Final Theorems

(a) **Theorem:** If $K$ is algebraic over $E$ and $E$ is algebraic over $F$ then $K$ is algebraic over $F$.

**Proof:** Let $a \in K$. Since $K$ is algebraic over $E$ there is some irreducible polynomial $p(x) = c_n x^n + \ldots + c_1 x + c_0$ with $c_i \in E$ such that $p(a) = 0$. Consider now the diagram:

\[
\begin{array}{c}
K \\
\downarrow \downarrow \\
F(c_0, c_1, \ldots, c_n, a) \quad E \\
\downarrow \\
F(c_0, c_1, \ldots, c_n) \\
\downarrow \\
\quad \vdots \\
\downarrow \\
F(c_0, c_1) \\
\downarrow \\
F(c_0) \\
\downarrow \\
F \\
\end{array}
\]

Since each $c_i$ is algebraic over $F$ each field extension up until the split is finite. Moreover the left branch is degree $n$ and so $a \in F(c_0, c_1, \ldots, c_n, a)$ which is a finite extension over $F$. Thus $a$ is algebraic over $F$. \(\Box\)

(b) **Theorem:** Let $E$ be an extension field of $F$. Then the set of all elements in $E$ which are algebraic over $F$ form a subfield of $E$.

**Proof:** Suppose $a, b \in E$ are algebraic over $F$ and $b \neq 0$. Consider that $[F(a, b) : F] = [F(a, b) : F(b)][F(b) : F]$ which is finite since $a, b$ are algebraic. Thus since $a + b, a - b, ab, a/b \in F(a, b)$ we know that all four are in a finite extension of $F$ and hence are algebraic over $F$. Thus the set of elements in $E$ which are algebraic over $F$ form a subfield of $E$. \(\Box\)