ABSTRACT ALGEBRA II
EXTENSION FIELDS

MARIO L. GUTIERREZ ABED

Introduction to Extension Fields

Definition. *A field E is called an **extension field** of a field F if $F \leq E$.* ★

The following important theorem shows that every nonconstant polynomial has a zero:

Theorem (Kronecker's Theorem). *Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.*

Proof. By *Theorem 23.20*[1], $f(x)$ has a factorization in $F[x]$ into polynomials that are irreducible over F. Let $p(x)$ be an irreducible polynomial in such a factorization. It is clearly sufficient to find an extension field E of F containing an element α such that $p(\alpha) = 0$.

Take the maximal ideal $\langle p(x) \rangle$ in $F[x]$, so that $F[x]/\langle p(x) \rangle$ is a field (we know this from a previous theorem). We claim that F can be identified with a subfield of $F[x]/\langle p(x) \rangle$ in a natural way by use of the map $\psi \colon F \to F[x]/\langle p(x) \rangle$ given by

$$\psi(a) = a + \langle p(x) \rangle \qquad \text{for } a \in F.$$

Notice that this map is injective:

$$\begin{aligned} &\psi(a) = \psi(b) \\ &\Longrightarrow a + \langle p(x) \rangle = b + \langle p(x) \rangle \qquad \text{for some } a, b \in F \\ &\Longrightarrow (a - b) \in \langle p(x) \rangle, \end{aligned}$$

so $a - b$ must be a multiple of the polynomial $p(x)$, which is of degree ≥ 1. Now $a, b \in F \Longrightarrow a - b \in F$. Thus we must have $a - b = 0 \Longrightarrow a = b$.

We defined addition and multiplication in $F[x]/\langle p(x) \rangle$ by choosing any representatives, so we may choose $a \in (a + \langle p(x) \rangle)$. Thus ψ is a homomorphism that maps F injectively onto a subfield of $F[x]/\langle p(x) \rangle$. We identify F with $\{a + \langle p(x) \rangle \mid a \in F\}$ by means of this map ψ. Thus we shall view $E = F[x]/\langle p(x) \rangle$ as an extension field of F. Hence we have manufactured our desired extension field E of F, and all that remains for us to show is that E contains a zero of $p(x)$:

Let us set

$$\alpha = x + \langle p(x) \rangle,$$

so $\alpha \in E$. Consider the evaluation homomorphism $\phi_\alpha \colon F[x] \to E$. If $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, where $a_i \in F$, then we have

$$\phi_\alpha(p(x)) = a_0 + a_1(x + \langle p(x) \rangle) + \cdots + a_n(x + \langle p(x) \rangle)^n$$

[1] Here's *Theorem 23.20* for reference:
If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique expect for order and for unit (that is, nonzero constant) in F.

in $E = F[x]/\langle p(x)\rangle$. But we can compute in $F[x]/\langle p(x)\rangle$ by choosing representatives, and x is a representative of the coset $\alpha = x + \langle p(x)\rangle$. Therefore,

$$\begin{aligned} p(\alpha) &= (a_0 + a_1 x + \cdots + a_n x^n) + \langle p(x)\rangle \\ &= p(x) + \langle p(x)\rangle = \langle p(x)\rangle = 0 \end{aligned}$$

in $F[x]/\langle p(x)\rangle$. We have thus found an element $\alpha \in E = F[x]/\langle p(x)\rangle$ such that $p(\alpha) = 0$, and therefore $f(\alpha) = 0$. □

We now illustrate the construction involved in the proof to the above theorem by an example:

Example: Let $F = \mathbb{R}$, and let $f(x) = x^2 + 1$, which is well known to have no zeroes in $\mathbb{R}$ and thus is irreducible over $\mathbb{R}$. This in turn implies that $\langle x^2 + 1\rangle$ is a maximal ideal in $\mathbb{R}[x]$, so $\mathbb{R}[x]/\langle x^2 + 1\rangle$ is a field. Now identifying $r \in \mathbb{R}$ with $r + \langle x^2 + 1\rangle \in \mathbb{R}[x]/\langle x^2 + 1\rangle$, we can view $\mathbb{R}$ as a subfield of $E = \mathbb{R}[x]/\langle x^2 + 1\rangle$. Let

$$\alpha = x + \langle x^2 + 1\rangle.$$

Computing in $\mathbb{R}[x]/\langle x^2 + 1\rangle$, we find

$$\begin{aligned} \alpha^2 + 1 &= (x + \langle x^2 + 1\rangle)^2 + (1 + \langle x^2 + 1\rangle) \\ &= (x^2 + 1) + \langle x^2 + 1\rangle = 0. \end{aligned}$$

Thus α is a zero of $x^2 + 1$. ▲

Remark: As you may have noticed from the above example, it turns out that $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$.

Definition. *An element α of an extension field E of a field F is said to be* ***algebraic*** *over F if $f(\alpha) = 0$ for some nonzero $f(x) \in F[x]$. If α is not algebraic over F, then α is said to be* ***transcendental*** *over F.* ★

Example: It is easy to see that the real number $\sqrt{1 + \sqrt{3}}$ is algebraic over $\mathbb{Q}$. For if $\alpha = \sqrt{1 + \sqrt{3}}$, then

$$\begin{aligned} \alpha^2 &= 1 + \sqrt{3} \\ \implies \alpha^2 - 1 &= \sqrt{3} \\ \implies (\alpha^2 - 1)^2 &= 3 \\ \implies \alpha^4 - 2\alpha^2 - 2 &= 0, \end{aligned}$$

so α is a zero of $x^4 - 2x^2 - 2$, which is in $\mathbb{Q}[x]$. ▲

Theorem 1. *Let E be an extension field of a field F and let $\alpha \in E$. Let $\phi_\alpha \colon F[x] \to E$ be the evaluation homomorphism of $F[x]$ into E such that $\phi_\alpha(a) = a$ for $a \in F$ and $\phi_\alpha(x) = \alpha$. Then α is transcendental over F if and only if ϕ_α gives an isomorphism of $F[x]$ with a subdomain of E, that is, if and only if ϕ_α is an injective map.*

Proof. Note that

$$\begin{aligned} \alpha \text{ is transcendental over } F &\iff f(\alpha) \neq 0 && \text{for all nonzero } f(x) \in F[x] \\ &\iff \phi_\alpha(f(x)) \neq 0 && \text{for all nonzero } f(x) \in F[x] \\ &\iff \ker(\phi_\alpha) = \{0\} \\ &\iff \phi_\alpha \text{ is injective.} \end{aligned}$$

□

<u>*Note*</u>: Consider the extension field $\mathbb{R}$ of $\mathbb{Q}$. We know that $\sqrt{2}$ is algebraic over $\mathbb{Q}$, being a zero of $x^2 - 2$. Of course, $\sqrt{2}$ is also a zero of $x^3 - 2x$ and of $x^4 - 3x^2 + 2 = (x^2 - 2)(x^2 - 1)$. Both of these polynomials having $\sqrt{2}$ as a zero were multiples of $x^2 - 2$. The next theorem shows that this is an illustration of a general situation. This theorem plays a central role in our later work:

Theorem 2. *Let E be an extension field of a field F and let $\alpha \in E$, where α is algebraic over F. Then there is an irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. This irreducible polynomial $p(x)$ is uniquely determined up to a constant factor in F and is a polynomial of minimal degree ≥ 1 in $F[x]$ having α as a zero. If $f(\alpha) = 0$ for $f(x) \in F[x]$, then $p(x)$ divides $f(x)$.*

Proof. See page 269, *Fraleigh*'s. □

Definition. *Let E be an extension field of a field F, and let $\alpha \in E$ be algebraic over F. The unique polynomial $p(x)$ having the property described in* Theorem 2 *above, is called the* ***irreducible polynomial for** α **over** F and will be denoted by* $\mathrm{irr}(\alpha, F)$. *The degree of* $\mathrm{irr}(\alpha, F)$ *is the* ***degree of** α **over** F, denoted by* $\deg(\alpha, F)$. ★

<u>*Remark*</u>: Note for instance that $\mathrm{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, with $\deg(\sqrt{2}, \mathbb{Q}) = 2$.

<u>*Example*</u>: Referring back to a previous example, we see that for $\alpha = \sqrt{1 + \sqrt{3}} \in \mathbb{R}$, α is a zero of $x^4 - 2x^2 - 2$, which is in $\mathbb{Q}[x]$. Since $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$ (this is true by Eisenstein with $p = 2$ for instance), we see that

$$\mathrm{irr}(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2.$$

Thus $\sqrt{1 + \sqrt{3}}$ is algebraic of degree 4 over $\mathbb{Q}$. ▲

<u>*Note*</u>: Consider the following two cases:

- **(Case I)** Suppose α is algebraic over F. Then the kernel of the evaluation homomorphism ϕ_α is $\langle \mathrm{irr}(\alpha, F) \rangle$, and by a previous theorem we have that $\langle \mathrm{irr}(\alpha, F) \rangle$ is a maximal ideal of $F[x]$. Therefore $F[x]/\langle \mathrm{irr}(\alpha, F) \rangle$ is a field and is isomorphic to the image $\phi_\alpha[F[x]] \in E$. This subfield $\phi_\alpha[F[x]]$ of E is then the smallest subfield of E containing F and α. We shall denote this field by $F(\alpha)$.
- **(Case II)** Suppose α is transcendental over F. Then by *Theorem* 1 above, ϕ_α gives an isomorphism of $F[x]$ with a subdomain of E. Thus in this case $\phi_\alpha[F[x]]$ is not a field but an integral domain, which we shall denote by $F[\alpha]$. Now by a previous corollary, E contains a field of quotients of $F[\alpha]$, which is thus the smallest subfield of E containing F and α. As in *Case I* above, we denote this field by $F(\alpha)$.

Definition. *An extension field E of a field F is a* ***simple extension*** *of F if $E = F(\alpha)$ for some nonzero $\alpha \in E$.* ★

Note: The next theorem gives us some insight into the nature of the field $F(\alpha)$ in the case where α is algebraic over F:

Theorem. *Let E be a simple extension $F(\alpha)$ of a field F, and let α be algebraic over F. Let the degree of $\operatorname{irr}(\alpha, F)$ be $n \geq 1$. Then every element β of $E = F(\alpha)$ can be uniquely expressed in the form*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

where the b_i's are in F.

Proof. See page 270, *Fraleigh*'s. □

<u>*Note*</u>: We can use the above theorem to show that indeed $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$. As we saw in a previous example, we can view $\mathbb{R}[x]/\langle x^2+1\rangle$ as an extension field of $\mathbb{R}$. Let

$$\alpha = x + \langle x^2+1\rangle.$$

Then $\mathbb{R}(\alpha) = \mathbb{R}[x]/\langle x^2+1\rangle$ and consists of all elements of the form $a + b\alpha$ for $a, b \in \mathbb{R}$, by the above theorem. But since $\alpha^2 + 1 = 0$, we see that α plays the role of $i \in \mathbb{C}$, and $a + b\alpha$ plays the role of $(a + bi) \in \mathbb{C}$. Thus $\mathbb{R}(\alpha) \cong \mathbb{C}$. *This is the elegant algebraic way to construct $\mathbb{C}$ from $\mathbb{R}$.*

Theorem. *Let E be an extension field of a field F, and let $\alpha \in E$ be algebraic over F. If $\deg(\alpha, F) = n$, then $F(\alpha)$ is an n-dimensional vector space over F with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Furthermore, every element $\beta \in F(\alpha)$ is algebraic over F, and $\deg(\beta, F) \leq \deg(\alpha, F)$.*

Proof. See page 280, *Fraleigh*'s. □

Algebraic Extensions

Definition. *An extension field E of a field F is called an* ***algebraic extension*** *of F if every element in E is algebraic over F.* ★

Definition. *If an extension field E of a field F is of finite dimension n as a vector space over F, then E is a* ***finite extension of degree*** *n* ***over*** *F. We shall let $[E : F]$ be the degree n of E over F.* ★

<u>*Remark*</u>: Note that to say that a field E is a finite extension of a field F <u>does not</u> mean that E is a finite field. It just asserts that E is a finite-dimensional vector space over F, i.e. that $[E : F]$ is finite.

Theorem. *A finite extension field E of a field F is an algebraic extension of F.*

Proof. See page 283, *Fraleigh*'s. □

Theorem 3. *If E is a finite extension field of a field F, and K is a finite extension field of E, then K is a finite extension of F, and furthermore*

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

Proof. See page 284, *Fraleigh*'s. □

Corollary 1. *If F_i is a field for $i = 1, \dots, r$ and F_{i+1} is a finite extension of F_i, then F_r is a finite extension of F_1, and*

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1].$$

Corollary 2. *If E is an extension field of F, $\alpha \in E$ is algebraic over F, and $\beta \in F(\alpha)$, then* $\deg(\beta, F)$ *divides* $\deg(\alpha, F)$.

The following example illustrates a type of argument one often makes using *Theorem 3* or its corollaries:

Example: By *Corollary 2*, there is no element of $\mathbb{Q}(\sqrt{2})$ that is a zero of $x^3 - 2$. Note that $\deg(\sqrt{2}, \mathbb{Q}) = 2$, while a zero of $x^3 - 2$ is of degree 3 over $\mathbb{Q}$, but 3 does not divide 2. ▲

Example 1: Consider $\mathbb{Q}(\sqrt{2})$. By a previous result we know that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. We can easily see that $\sqrt{2} + \sqrt{3}$ is a zero of the polynomial $p(x) = x^4 - 10x^2 + 1$:

To see this, note that

$$\begin{aligned}
\alpha = \sqrt{2} + \sqrt{3} &\implies \alpha^2 = (\sqrt{2} + \sqrt{3})^2 \\
&\implies \alpha^2 = 2 + 2\sqrt{2}\sqrt{3} + 3 \\
&\implies (\alpha^2 - 5)^2 = (2\sqrt{2}\sqrt{3})^2 \\
&\implies \alpha^4 - 10\alpha^2 + 25 = 4 \cdot 3 \cdot 2 \\
&\implies \alpha^4 - 10\alpha^2 + 1 = 0.
\end{aligned}$$

Now, by applying the same method as in *Example 1* from our notes on *Rings & Fields*, we can easily see that $p(x)$ is irreducible in $\mathbb{Q}[x]$. Thus,

$$\operatorname{irr}(\sqrt{2} + \sqrt{3}, \mathbb{Q}) = x^4 - 10x^2 + 1 \qquad \implies \qquad [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4.$$

As a result we have that $(\sqrt{2} + \sqrt{3}) \notin \mathbb{Q}(\sqrt{2})$, and thus $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Consequently, $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$. we also have that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. ▲

Theorem. *Let E be an algebraic extension of a field F. Then there exists a finite number of elements $\alpha_1, \dots, \alpha_n$ in E such that $E = F(\alpha_1, \dots, \alpha_n)$ if and only if E is a finite-dimensional vector space over F, that is, if and only if E is a finite extension of F.*

Proof. See page 286, *Fraleigh*'s. □