Section 29: Introduction to Extension Fields

Goal: The results in this section will allow us to prove that every nonconstant polynomial has a zero.

Def: A field E is an *extension field* of a field F if $F \leq E$.

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:
$f(x)$ 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 E.T.S that there exists an extension field of F that contains a root of $p(x)$. We can get our required extension field by noting that, since $\langle p(x)\rangle$ is a maximal ideal in $F[x]$, $F[x]/\langle p(x)\rangle$ must be a field. To show that F is a subfield of $E = F[x]/\langle p(x)\rangle$, we construct the following map, $\psi : F \to E$ via

$$\psi(a) = a + \langle p(x)\rangle$$

for $a \in F$. ψ is 1-1 since $\psi(a) = \psi(b)$ implies that $a - b \in \langle p(x)\rangle$ and since $a, b \in F$, $a - b = 0$ and $a = b$. ψ is a homomorphism that maps F 1-1 onto a subfield of $F[x]/\langle p(x)\rangle$. the existence of this subfield shows that E is an extension field of F.
Now we need to show that E contains a zero of $p(x)$. Let $\alpha = x + \langle p(x)\rangle \in E$. We can use the evaluation homomorphism $\phi_a : F[x] \to E$ at α, plugging into the polynomial $p(x)$.

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

Since x is a representative of the coset $\alpha = x + \langle p(x)\rangle$, we can rewrite our evaluation as

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

$$= p(x) + \langle p(x)\rangle = \langle p(x)\rangle = 0$$

Therefore, we have found an element α in an extension field E of F such that $p(\alpha) = 0$. ■

Proof Synopsis: The proof of Kronecker's Theorem comes in two parts. The first, and more challenging part, involves constructing an extension field based off that fact that our polynomial is irreducible in the original field. In the second part, we chose an element in our extension field such that our polynomial evaluates to the ideal generated by $p(x)$, which is the zero in the extension field, but also in our original field.

Classical Example: Take $F = \mathbb{R}$ and $f(x) = x^2 + 1$. $\mathbb{R}$ is a subfield of $\mathbb{R}[x]/\langle x^2 + 1\rangle$. Now choose an α,

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

We can now plug this into $f(x)$, keeping in mind that we are working in the field $\mathbb{R}[x]/\langle x^2 + 1\rangle$.

$$f(\alpha) = \alpha^2 + 1 = (x + \langle x^2 + 1\rangle)^2 + (1 + \langle x^2 + 1\rangle)$$
$$= (x^2 + 1) + \langle x^2 + 1\rangle = \langle x^2 + 1\rangle = 0$$

You may recognize the field $\mathbb{R}[x]/\langle x^2 + 1\rangle$ as $\mathbb{C}$.

Def: An element α of an extension field E of a field F is *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 *transcendental* over F.

Example: i is algebraic over $\mathbb{Q}$, while π and e are transcendental over $\mathbb{Q}$.

Note: In number theory, an element of $\mathbb{C}$ that is algebraic over $\mathbb{Q}$ is an algebraic number. A transcendental number is an element of $\mathbb{C}$ that is transcendental over $\mathbb{Q}$.

Thm. Let E be an extension field of a field F and let $\alpha \in E$. Let $\phi_\alpha : F[x] \to E$ 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 a 1-1 map.

Note: This theorem basically says that a number is transcendental over a field if and only if the number can be plugged into every polynomial and only be zero when the number itself is zero.

Thm. Let E be an extension field of 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 $f(x) \in F[x]$, with $f(x) \neq 0$, then $p(x)$ divides $f(x)$.

Note: This theorem says that all polynomials with a certain root are constructed from a base irreducible polynomial. For example, $x^2 - 8x + 15$ is constructed from $x - 3$ and $x - 5$.

Def: A *monic* polynomial is a polynomial where the coefficient of the highest power of x is 1.

Def: Let E be an extension field of a field F, and let $\alpha \in E$ be algebraic over F. The unique monic polynomial $p(x)$ having the property from the last theorem is the *irreducible polynomial* for α over F. and is denoted by $irr(\alpha, F)$. The degree of $irr(\alpha, F)$ is the *degree* of α over F, denoted $deg(\alpha, F)$.

Note: An element that is transcendental over a field behaves as though it were an indeterminate over the field.

Def: An extension field E of a field F is a *simple extension* of F if $E = F(\alpha)$ for some $\alpha \in E$, and where $F(\alpha)$ is the smallest subfield of E containing both F and α.

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

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

where the b_i are in F.

Note: This theorem states that every element of the simple extension $F(\alpha)$ is a polynomial in α.

Constructing the Complex Numbers: Recall that $\mathbb{R}[x]/\langle x^2 + 1\rangle$ is an extension field of $\mathbb{R}$. If $\alpha = x + \langle x^2 + 1\rangle$, then $\mathbb{R}(\alpha) = \mathbb{R}[x]/\langle x^2 + 1\rangle$. By the last theorem, we know that all elements of this field must be of the form $a + b\alpha$ for $a, b \in \mathbb{R}$. But we also know that α is the root of $x^2 + 1$, i.e. $\alpha^2 + 1 = 0$. Another may to say this is $\alpha = \sqrt{-1}$, which means that $\alpha = i$.

Selected Exercises

27. Let E be an extension field of a field F and let $\alpha \in E$ be algebraic over F. The polynomial $irr(\alpha, F)$ is sometimes referred to as the *minimal polynomial* for α over F. Why is this designation appropriate?

Answers:
The name is fitting because it is the simplest polynomial that has α as a root.

29. Let E be an extension field of F, and let $\alpha, \beta \in E$. Suppose α is transcendental over F, but algebraic over $F(\beta)$. Show that β is algebraic over $F(\alpha)$.

Proof:
Goal: $f(\beta) = 0$ for some nonzero $f \in F(\alpha)[x]$.
Given: $f(\alpha) = 0$ for $f(x) \in F[x]$ iff $\alpha = 0$, $f(\alpha) = 0$ for some $f(x) \in F(\beta)[x]$.
We can write an element of $F(\beta)[x]$ as $p(x) = a_0 + a_1x + \cdots + a_nx^n$ where each $a_i \in F(\beta)$ has the form $a_i = \frac{f(\beta)}{g(\beta)}$ where $f(x), g(x) \in F[x]$.
Therefore, $p(x) = \frac{f_0(\beta)}{g_0(\beta)} + \frac{f_1(\beta)}{g_1(\beta)}x + \cdots + \frac{f_n(\beta)}{g_n(\beta)}x^n$.
Since we know that α is algebraic over $F(\beta)$,

$$p(\alpha) = \frac{f_0(\beta)}{g_0(\beta)} + \frac{f_1(\beta)}{g_1(\beta)}\alpha + \cdots + \frac{f_n(\beta)}{g_n(\beta)}\alpha^n = 0$$

Multiply both sides by $\Pi_{i=0}^{n} g_i(\beta)$

$$f_0(\beta) + f_1(\beta)\alpha + \cdots + f_n(\beta)\alpha^n = 0$$

We can rewrite this polynomial in α as a polynomial with coefficients in $F(\alpha)$, therefore β is algebraic over $F(\alpha)$. ■

30. Let E be an extension field of a finite field F, where F has q elements. Let $\alpha \in E$ be algebraic over F of degree N. Prove that $F(\alpha)$ has q^n elements.