Part VI. Extension Fields

Section VI.29. Introduction to Extension Fields

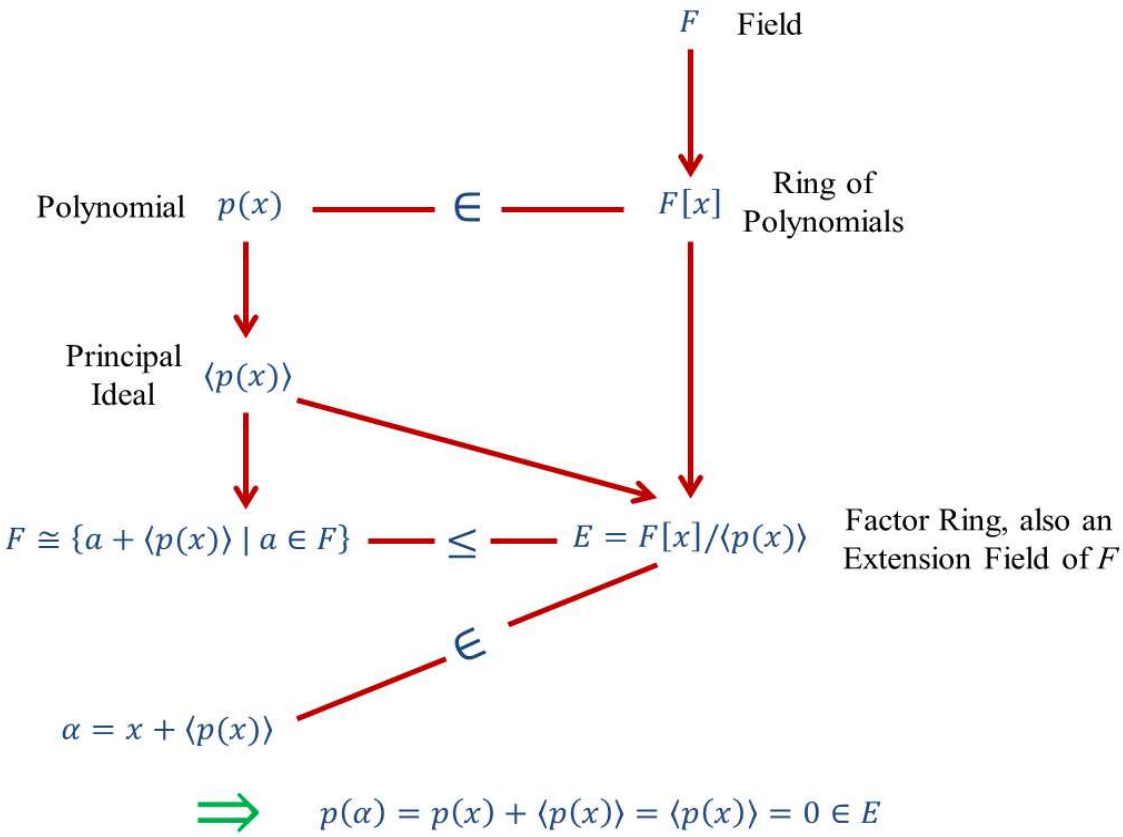
Note. In this section, we attain our "basic goal" and show that for any polynomial over a field F, there is an "extension field" E (that is, F is a subfield of E) such that the polynomial has a zero in E.

Definition 29.1. A field E is an *extension field* of field F if $F \leq E$ (that is, if F is a subfield of E).

Example. We can view $\mathbb{R}$ as an extension field of $\mathbb{Q}$ (we will see many fields "between" $\mathbb{Q}$ and $\mathbb{R}$) and $\mathbb{C}$ as an extension field of $\mathbb{R}$. Notice that $x^2 - 2 \in \mathbb{Q}[x]$ but $x^2 - 2$ has no zero in $\mathbb{Q}$. However, $x^2 - 2$ has two zeros in $\mathbb{R}$. Also, $x^2 + 1 \in \mathbb{R}[x]$ but $x^2 + 1$ has no zero in $\mathbb{R}$. however, $x^2 + 1$ has two zeros in $\mathbb{C}$. This foreshadows the following result (our "basic goal"). Considering the magnitude of the result, the proof is rather short. This is because we have lots of equipment at this stage! Joseph Gallian in his *Contemporary Abstract Algebra* (8th Edition, Brooks/Cole, 2013, page 360) calls the result the "Fundamental Theorem of Field Theory."

Theorem 29.3. Kronecker's Theorem (Basic Goal).
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 $f(\alpha) = 0$.

Note. A diagram of the proof of Kronecker's Theorem is:



Example 29.4. To further illustrate the proof of Kronecker's Theorem, let $F = \mathbb{R}$ and $f(x) = x^2 + 1 \in \mathbb{R}[x]$. Since f is irreducible over $\mathbb{R}$, then $\langle x^2 + 1 \rangle$ is a maximal ideal in $\mathbb{R}[x]$ by Theorem 27.25. So by Theorem 27.9, $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a field. As in the proof, we "identify" $r \in \mathbb{R}$ with $r + \langle x^2 + 1 \rangle \in \mathbb{R}[x]/\langle x^2 + 1 \rangle$, so we "view" $\mathbb{R}$ as a subfield of $\mathbb{R}[x]/\langle x^2 + 1 \rangle$, we have

$$f(\alpha) = \alpha^2 + 1 = (x + \langle x^2 + 1 \rangle)^2 + \underbrace{(1 + \langle x^2 + 1 \rangle)}_{\text{"identified" with } 1}$$

$$= x^2 + 1 + \langle x^2 + 1 \rangle = \langle x^2 + 1 \rangle = 0.$$

So α is a zero of $x^2 + 1$. At the end of this section we associate $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ with $\mathbb{C}$.

Example 29.5. Let $F = \mathbb{Q}$ and consider $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. Then $x^2 - 2$ and $x^2 - 3$ are irreducible in $\mathbb{Q}[x]$. So we know there is an extension field of $\mathbb{Q}$ containing a zero of $x^2 - 2$ and there exists *another* extension field of $\mathbb{Q}$ containing a zero of $x^2 - 3$. However, the construction (and the proof of Kronecker's Theorem which we gave) does not imply that there is a *single* field containing both a zero of $x^2 - 2$ and a zero of $x^2 - 3$.

Note. The "Kronecker" of "Kronecker's Theorem" is Leopold Kronecker (1823–1891) who was born in Poland and did most of his work in Germany.

He is well-known for the quote "God made the integers; all else is the work of man." Kronecker's philosophical view of math is that every object of mathematics should be constructible and constructed in a finite number of steps. In 1882 he published "Foundations of an Arithmetic Theory of Algebraic Numbers" in which he introduced the idea of an extension field created by adjoining a single element (a zero of a polynomial) to the field of rational numbers. Quoting from *A History of Abstract Algebra* by Israel Kleiner: "Kronecker rejected irrational numbers as

bona fide entities since they involve the mathematical infinite. For example, the algebraic number field $Q(\sqrt{2})$ was defined by Kronecker as the quotient field of the polynomial ring $Q[x]$ relative to the ideal generated by $x^2 - 2$, though he would have put it in terms of congruences rather than quotient rings. These ideas contain the germ of what came to be known as *Kronecker's Theorem*, namely that every polynomial over a field has a root in some extension field." Kronecker's rival in this "finitest" view was Richard Dedekind (1831–1916). Dedekind used an axiomatic approach, including an acceptance of the axiomatized infinite. Whereas Kronecker would start with the natural numbers, build the integers, the rationals, and then finite extensions of the rationals, Dedekind treats the real numbers as a complete ordered field from the start. Dedekind's version of completeness (and hence his approach to irrationals) is dealt with using "Dedekind cuts." A Dedekind cut of $\mathbb{R}$ is two nonempty sets $A, B \subset \mathbb{R}$ such that: $a < b$ for all $a \in A$ and $b \in B$, $A \cap B = \varnothing$, and $A \cup B = \mathbb{R}$. The claim (the "Axiom of Completeness" for $\mathbb{R}$) is that either A has a largest element or B has a smallest element. This can be stated in everyday language as the following. Suppose an airplane taxis down a runway and takes off. Is there a last point in time the plane is on the ground or a first point in time that the plane is off the ground? (The answer: There is a last point in time the plane is on the ground.) These are the ideas you will address early in our Analysis 1 (MATH 4217/5217) class.

Definition 29.6. 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.

Note. In the Analysis 1 (MATH 4217/5217) class, an *algebraic number* is a real number which is a zero of a polynomial in $\mathbb{Q}[x]$. A *transcendental number* is a real number which is not algebraic. There are an infinite number of algebraic numbers and an infinite number of transcendental numbers... *but*, surprisingly, there are *more* transcendental numbers then algebraic numbers. Example 29.8 claims that π and e are transcendental. Our book takes a slightly different definition of *algebraic number* and *transcendental number* and allows them to be complex.

Definition 29.11. 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 $\mathbb{Q}$.

Theorem 29.12. Let E be an extension field of 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 $\phi_\alpha(x) = \alpha$ (this is the usual evaluation homomorphism of Section 22). 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 one to one map.

Note. The following result will have application to the topic of algebraic field extensions in Section 31.

Theorem 29.13. 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 greater than or equal to 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 $f(x)$.

Definition 29.14. A polynomial is a *monic polynomial* if the coefficient of the highest power of x is 1. Let E be an extension field of field F. Let $\alpha \in E$ be algebraic over F. The unique monic polynomial $p(x)$ having the property described in Theorem 29.13 (in particular, $p(x)$ is irreducible) is the *irreducible polynomial for α over F*, denoted $\text{irr}(\alpha, F)$. The degree of $\text{irr}(\alpha, F)$ is the *degree of α over F*, denoted $\deg(\alpha, F)$.

Example 29.15. Of course, $\text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ and $\deg(\sqrt{2}, \mathbb{Q}) = 2$. In general, for $n \in \mathbb{N}$, $\text{irr}(\sqrt[n]{2}, \mathbb{Q}) = x^n - 2$ and $\deg(\sqrt[n]{2}, \mathbb{Q}) = n$. The text argues that $\text{irr}(\sqrt{1+\sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2$ and $\text{irr}(\sqrt{1+\sqrt{3}}, \mathbb{Q}) = 4$.

Note 29.1. Let E be an extension field of field F and let $\alpha \in E$. If α is algebraic over F, then by Theorem 29.13, there is $p(x) \in F[x]$ such that $p(x)$ is irreducible, $p(\alpha) = 0$ (or $\phi_\alpha(p) = 0$ where ϕ_α is the evaluation homomorphism) and for any polynomial $f(x)$ for which $f(\alpha) = 0$, we have that $p(x)$ divides $f(x)$. We know that $\text{irr}(\alpha, F)$ is a unique such $p(x)$, and so $\langle \text{irr}(\alpha, F) \rangle$ is precisely the collection of

all polynomials which are 0 when evaluated at α. That is, $\ker(\phi_\alpha) = \langle \text{irr}(\alpha, F)\rangle$. Since $\text{irr}(\alpha, F)$ is irreducible, then by Theorem 27.15 we have that $\langle \text{irr}(\alpha, F)\rangle$ is a maximal ideal of $F[x]$. So, by Theorem 27.9, $F[x]/\langle \text{irr}(\alpha, F)\rangle$ is a field. Since $\phi_\alpha : F[x] \to F$ is a ring homomorphism (Theorem 22.4) with kernel $\ker(\phi_\alpha) = \langle \text{irr}(\alpha, F)\rangle$, then by the Fundamental Homomorphism Theorem (Theorem 26.17), $\mu_\alpha : F[x]/\langle \text{irr}(\alpha, F)\rangle \to \phi_\alpha[F[x]]$ given by $\mu_\alpha(f(x)+\langle \text{irr}(\alpha, F)\rangle) = \phi_\alpha(f(x)) = f(\alpha)$ is an isomorphism, and so $F[x]/\langle \text{irr}(\alpha, F)\rangle$ is a field isomorphic to $\phi_\alpha[F[x]]$. Now $\phi_\alpha[F[x]]$ includes F as a subfield (the subfield of all "constant polynomials") and includes α (since $\phi_\alpha(x) = \alpha$). Since a field is closed under addition and multiplication, any field containing α must contain all linear combinations of powers of α (all these linear combinations are simply the set of all polynomials with constant term 0 evaluated at α). So, $\phi_\alpha[F[x]]$ is the smallest subfield of E containing both F and α. This is denoted $F(\alpha)$.

Note 29.2. Let E be an extension field of field F and let $\alpha \in E$. If α is transcendental over F then by Theorem 29.12, $\phi_\alpha : F[x] \to E$ is an isomorphism (i.e., ϕ_α is one to one) of $F[x]$ with a subdomain of E (i.e., a "sub-integral domain"). However, $\phi_\alpha[F[x]]$ is not a field ($\alpha^{-1} \notin \phi_\alpha[F[x]]$). Denoting $\phi_\alpha[F[x]]$ as $F[\alpha]$, Corollary 21.8 implies the field E contains a field of quotients of integral domain $F[\alpha]$. This field of quotients is then the smallest subfield of E containing both F and α (in the sense described in Section 21—see the first paragraph of Section 21 on page 190, and the first paragraph of page 195). This field of quotients is denoted $F(\alpha)$.

Definition 29.17. An extension field E of field F is a *simple extension* of F if $E = F(\alpha)$ for some $\alpha \in E$.

Example 29.16. We know (or accept) that π is transcendental over $\mathbb{Q}$. So by Note 29.1, the simple extension $\mathbb{Q}(\pi)$ is isomorphic the field $\mathbb{Q}(x)$ of rational functions over $\mathbb{Q}$ in indeterminate x (i.e., $\mathbb{Q}(x)$ is isomorphic to the field of quotients of $\mathbb{Q}[x]$). So when a simple extension of a field F is made using an element transcendental over F, the result is structurally equivalent to creating a field of quotients where the transcendental element "acts as" an indeterminate x.

Theorem 29.18. Let E be a simple extension $F(\alpha)$ of field F where α is algebraic over F. Let the degree of $\text{irr}(\alpha, F)$ be n (where $n \geq 1$). Then every element β of $E = F(\alpha)$ can be uniquely expressed in the form

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}$$

where each $b_i \in F$.

Note. The previous theorem should sort of remind you of a basis of a vector space. This is further explored in the next example and dealt with in detail in the next section.

Example. Algebraic Development of $\mathbb{C}$.

In Example 29.4, we claimed that we can associate $\mathbb{R}[x]/\langle x^2+1\rangle$ with $\mathbb{C}$. In that example, we have $\mathbb{R}[x]/\langle x^2+1\rangle$ as an extension field of $\mathbb{R}$. Let $\alpha = x + \langle x^2+1\rangle$. Then $R(\alpha) = \mathbb{R}[x]/\langle x^2+1\rangle$ by the definition of $F(\alpha)$ (see Note 29.1). Since $\text{irr}(\alpha, F) = x^2+1$ has degree $n = 2$, then every element of $F(\alpha)$ is of the form $a + b\alpha$ for $a, b \in \mathbb{R}$ by Theorem 29.18. Since $p(\alpha) = \alpha^2 + 1 = 0$, then this "$\alpha$" plays the same role as $i \in \mathbb{C}$. So, the extension field $R(\alpha)$ (or $R(i)$, if you like) is isomorphic to $\mathbb{C}$. The text calls this an "elegant algebraic way to construct $\mathbb{C}$ from $\mathbb{R}$."

Revised: 2/16/2013