Fild Theory

S. William

1 Basic Concepts

A field extension E/F just means a field E and a subfield F, like the ring extension. In fact field extension (**Fxt**) can be regarded as a sub-category of ring extension (**Rxt**). The field extension lies at the heart of field theory, and is crucial to many other algebraic domains. $F(S)$ denotes the minimal field containing a (finite) set S and the field E. The elements in $F(S)$ are called rational functions of F, since they have the form $\frac{f}{g}$ where $f, g \in F[S]$. Hence $F(S) = \mathrm{Frac}(F[S])$. Similarly, we have the field of formal power series denoted with $F((S)) = \mathrm{Frac}(F[[S]])$. This field is actually the ring of Laurent series over the field E.

Consider field extension E/F. A simple extension field of F is $F(x)$ the minimal subfield of F containing E and $x \in E$. Such extensions are also called simple extensions.

Definition 1.1 *In the field extension E/F, $\alpha \in E$ is an algebraic element if α is a root of a (non-zero) polynomial $f(x) \in F[x]$. Otherwise it is a transcendental element. E/F is an algebraic extension if all elements in E are algebraic elements. Otherwise it is transcendental extension.*

For an algebraic element $\alpha \neq 0$, there exist an ideal of $F[x]$ consists of polynomials that $f(\alpha) = 0$ named annihilation polynomials of α. The ideal must be $I_\alpha = (p(x))$ where the monic polynomial $p(x)$ is named minimal polynomial sometimes denoted as $\mathrm{irr}_E(a)$. Obviously, $p(x)$ is unique and irreducible. In ring extension, we do not have such polynomial necessarily.

Theorem 1.1 *If α is an algebraic element of E/F, then $F(\alpha) = F[\alpha] \simeq F[x]/(p(x))$ where $p(x)$ is the minimal polynomial of α, else if it is a transcendental element, then $F(\alpha) = \mathrm{Frac}(F[\alpha]) \simeq F(x)$.*

Proof. Let assignment map $\phi(f(x)) = f(\alpha)$ that is a homomorphism from $F[x]$ to $F[\alpha]$. $\square$

A field with no nontrivial algebraic extensions is called algebraically closed. An example is the field $\mathbb{C}$ of complex numbers. Every field has an algebraic extension which is algebraically closed (called its algebraic closure), for example $\mathbb{C}/\mathbb{R}$. (see the integral closure in ring theory)

Now we show the basic theorem for simply algebraic extension.

Theorem 1.2 (Simply algebraic extension I) *Given a field F, and $p(x) \in F[x]$ is an n-monic irreducible polynomial. Let quotient ring $E = K[x]/(p(x))$ that is indeed a field and $\alpha = x + (p(x))$. We have that*

1) algebraic extension $E/F = F(\alpha)/F$,

2) $p(x)$ is the minimal polynomial of α and $(p(x))$ consists of the annihilation polynomials of α,

3) E is regarded as a F-vector space with dimension n.

Example 1.1 $\mathbb{C} = \mathbb{R}[x]/(x^2+1), \mathbb{C}/\mathbb{R}$. *Denoting $x + (x^2+1)$ with i, we have $\mathbb{C} = R(i)$.*

The following result can be regarded as the inverse of Theorem 1.2.

Theorem 1.3 (Simply algebraic extension II) *Given a field extension E/F and an algebraic element α, namely $F(\alpha)/F$ is an algebraic extension, then*

1) there exists a minimal polynomial $p(x)$ (uniquely) of α as mentioned above,

2) if β is another root of $p(x)$, then there exists an isomorphism $\theta : F(\alpha) \to F(\beta)$ preserving K and mapping α to β.

2 Splitting Field

Before we introduce the splitting fields, we show the following basic result due to Kronecker.

Theorem 2.1 (Kronecker theorem) *If F is a field and $f(x) \in F[x]$, then there is a field extension E/F that $f(x)$ can be written as the product of the linear polynomials of $E[x]$.*

Definition 2.1 *Given field extension E/F and $f(x) \neq 0 \in F[x]$. $f(x)$ is split on E, if*

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), a \neq 0,$$

where $\alpha_1, \alpha_2, \cdots, \alpha_n \in E$. A subfield K of E is the splitting field of $f(x)$, if it is the minimal subfield of E where $f(x)$ is split.

Theorem 2.1 says there exists a splitting field for any $f(x) \in F[x]$, denoted as $F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are the root of $f(x)$. The splitting field for a set of polynomials is defined in the expected way. It can be shown that such splitting fields exist and are unique up to isomorphism. When we analyse a polynomial $f(x)$ on a field F, we usually give the splitting field at first.