Introduction to Field Extension

Date: Mar 13 Made by Eric

In this note, $\mathbb{E}$ is always a field

Definition

Definition 1. *$\mathbb{E}$ is an **extension** of $\mathbb{F}$ if $\mathbb{F} \leq \mathbb{E}$*

Definition 2. *Let $\mathbb{F} \leq \mathbb{E}$ and $\alpha \in \mathbb{E}$*

*α is **algebraic over** $\mathbb{F}$ if there exists non-zero polynomial f in $\mathbb{F}[x]$ such that $f(\alpha) = 0$*

*α is **transcendental over** $\mathbb{F}$ if α is not algebraic over $\mathbb{F}$, more precisely, if $f(\alpha) = 0 \implies f = 0$*

Definition 3. *Let $\alpha \in \mathbb{C}$*

*α is an **algebraic number** if α is algebraic over $\mathbb{Q}$*

*α is an **transcendental number** is α is not an algebraic number*

Definition 4. *Let $f \in \mathbb{F}[x]$*

f is a monic polynomial if the leading coefficient is 1

Definition 5. *Let $\mathbb{F} \leq \mathbb{E}$, and let $\alpha \in \mathbb{E}$ be algebraic over $\mathbb{F}$*

*The **irreducible polynomial for** α **over** $\mathbb{F}$ is the unique monic irreducible polynomial f that satisfy $f(\alpha) = 0$*

$$irr(\alpha, \mathbb{F}) = f$$

*The **degree of** α **over** $\mathbb{F}$ is $deg(\ irr(\alpha, \mathbb{F}))$*

$$deg(\alpha, \mathbb{F}) = deg(\ irr(\alpha, \mathbb{F}))$$

Definition 6. *Let $\mathbb{F} \leq \mathbb{E}$, $\alpha \in \mathbb{E}$ be algebraic, and $\phi_\alpha : \mathbb{F}[x] \to \mathbb{E}$ be evaluation homomorphism*

$$\mathbb{F}(\alpha) = \phi_\alpha[\mathbb{F}[x]]$$

Definition 7. *Let $\mathbb{F} \leq \mathbb{E}$, $\alpha \in \mathbb{E}$ be transcendental, and $\phi_\alpha : \mathbb{F}[x] \to \mathbb{E}$*

$\mathbb{F}(\alpha)$ is the field of quotient expanded by $\phi_\alpha[\mathbb{F}[x]]$

Definition 8. *Let $\mathbb{F} \leq \mathbb{E}$*

*$\mathbb{E}$ is a **simple extension** of $\mathbb{F}$ if $\mathbb{E} = \mathbb{F}(\alpha)$ for some $\alpha \in \mathbb{E}$*

Theorems

Theorem 1. *Let $f \in \mathbb{F}[x]$*

There exists $\mathbb{E}$, an extension of $\mathbb{F}$, such that $\exists \alpha \in \mathbb{E}, f(\alpha) = 0$

Proof. Let $p \in \mathbb{F}[x]$ be an irreducible factor of f, such that p is of degree more than 1 **(If every irreducible factor of f is of degree less than or equal to 1, we can simply pick $\mathbb{F} = \mathbb{E}$ and pick any $(x - \alpha)$)**

Let $\mathbb{E} := \mathbb{F}[x]/\langle p(x) \rangle$

We now prove $\mathbb{F}$ is isomorphic to a subfield of $\mathbb{E}$

Let $\phi : \mathbb{F} \to \mathbb{E}$ be defined by $c \mapsto c + \langle p(x) \rangle$

$\phi(c + d) = ((c + d) + \langle p \rangle) = (c + \langle p \rangle) + (d + \langle p \rangle) = \phi(c) + \phi(d)$

$\phi(cd) = cd + \langle p \rangle = (c + \langle p \rangle)(d + \langle p \rangle) = \phi(c)\phi(d)$

$\phi(a) = \phi(b) \implies a + \langle p \rangle = b + \langle p \rangle \implies a - b \in \langle p \rangle \implies a = b$

$\forall \phi(r) \in \phi[\mathbb{F}], \phi(r^{-1})\phi(r) = 1$ **This guarantee that the image of ϕ is a field** (done)

We now prove $\exists \alpha \in \mathbb{E}, f(\alpha) = 0$

Let $\beta = x + \langle p \rangle$

$f(\beta) = f(x) + \langle p \rangle = \langle p \rangle$

Notice $\langle p \rangle$ is the additive identity in $\mathbb{E}$ (done)

■

Theorem 2. *Let $\mathbb{E}$ be an extension of $\mathbb{F}$ and let $\alpha \in \mathbb{E}$. Let $\phi_\alpha : \mathbb{F}[x] \to \mathbb{E}$ be the evaluation homomorphism of α*

α is transcendental over $\mathbb{F}$ if and only if ϕ_α is a monomorphism

Proof. $(\longrightarrow)$

$\phi_\alpha(f) = \phi_\alpha(g) \implies f(\alpha) = g(\alpha) \implies (f - g)(\alpha) = 0 \implies f - g = 0 \implies f = g$

$(\longleftarrow)$

$f(\alpha) = 0 \implies \phi_\alpha(f) = 0 \implies f = 0$ ■

Theorem 3. *Let $\mathbb{E}$ be an extension of $\mathbb{F}$, and pick $\alpha \in \mathbb{E}$ where α is algebraic over $\mathbb{F}$*

The smallest polynomial $p \in \mathbb{F}[x]$ that satisfy $p(\alpha) = 0$, is irreducible

Proof. Let $S = \{f \in \mathbb{F}[x] | f(\alpha) = 0\}$

We now prove S is an ideal of $\mathbb{F}[x]$

Let $g, h \in S$ and $r \in \mathbb{F}[x]$

$(g + h)(\alpha) = g(\alpha) + h(\alpha) = 0 \implies g + h \in S$

$0(\alpha) = 0 \implies 0 \in S$

$(-g)(\alpha) = -g(\alpha) = 0 \implies -g \in S$

$(gs)(\alpha) = g(\alpha)s(\alpha) = 0s(\alpha) = 0 \implies gs \in S$

$(sg)(\alpha) = s(\alpha)g(\alpha) = s(\alpha)0 = 0 \implies sg \in S$ (done)

We know $\mathbb{F}[x]$ contains only principal ideal, so we can pick a polynomial p that generate S and see that p is of smallest degree and is irreducible ■

Theorem 4. *Let $\mathbb{E} = \mathbb{F}(\alpha)$, where $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$. Let $\beta \in \mathbb{E}$, and let $n = deg(\alpha, \mathbb{F})$*

β can be uniquely expressed as $c_0\alpha^0 + c_1\alpha^1 + \cdots + c_{n-1}\alpha^{n-1}$ for some $\{c_0, \ldots, c_{n-1}\} \subseteq \mathbb{F}$

Proof. Let $\phi_\alpha : \mathbb{F}[x] \to \mathbb{E}$ be evaluation homomorphism

Because $\mathbb{E} = \mathbb{F}(\alpha)$ and α is algebraic over $\mathbb{F}$, so we know $\mathbb{E} \simeq \phi_\alpha[\mathbb{F}[x]]$

Because we know $\langle \text{ irr}(\alpha, \mathbb{F})\rangle$ is the kernel of $\phi_\alpha[\mathbb{F}[x]]$, so by First Isomorphism Theorem, we know $\mu : \mathbb{F}[x]/\langle \text{ irr}(\alpha, \mathbb{F})\rangle \to \mathbb{E}$ defined by $f + \langle \text{ irr }(\alpha, \mathbb{F})\rangle \mapsto \phi_\alpha(f)$ is an isomorphism

We now prove β can be expressed in such fashion

Because μ is an isomorphism, we know there exists $f + \langle \text{ irr}(\alpha, \mathbb{F})\rangle$ satisfy $\mu(f + \langle \text{ irr}(\alpha, \mathbb{F})\rangle) = \beta$

We fix such f

Do division algorithm on f with $\langle \text{ irr}(\alpha, \mathbb{F})\rangle$ to have $f = q \text{ irr}(\alpha, \mathbb{F}) + r$

Because $f - r = q \text{ irr}(\alpha, \mathbb{F}) \in \langle \text{ irr}(\alpha, \mathbb{F})\rangle$, we know $f + \langle \text{ irr}(\alpha, \mathbb{F})\rangle) = r + \langle \text{ irr}(\alpha, \mathbb{F})\rangle)$

Then we see $\beta = \mu(f + \langle \text{ irr}(\alpha, \mathbb{F})\rangle) = \mu(r + \langle \text{ irr}(\alpha, \mathbb{F})\rangle) = \phi_\alpha(r) = r(\alpha)$ where $deg(r) < deg(\alpha, \mathbb{F})$ (done)

We now prove uniqueness

Assume such expression is not unique

Let $\beta = d_0\alpha^0 + \cdots + d_{n-1}\alpha^{n-1}$ where d is another sequence of coefficients

$(c_0 - d_0)\alpha^0 + \cdots + (c_{n-1} - d_{n-1})\alpha^{n-1} = 0$ CaC to that $n = deg(\alpha, \mathbb{F})$ (done) ∎

Theorem 5. $\mathbb{R}(x + \langle x^2 + 1\rangle) \simeq \mathbb{C}$

Proof. Let $\phi : \mathbb{C} \to \mathbb{R}(x + \langle x^2 + 1\rangle)$ be defined by lifting $1 \mapsto 1 + \langle x^2 + 1\rangle$ and $i \mapsto x + \langle x^2 + 1\rangle$

$\phi(a + bi) + \phi(c + di) = [(a + bx) + \langle x^2 + 1\rangle] + [(c + dx) + \langle x^2 + 1\rangle] = [(a + c) + (b + d)x] + \langle x^2 + 1\rangle = \phi((a + bi) + (c + di))$

LEFT TO PROVE ∎

Summary

1. The spirit of simple extension $\mathbb{F}(\alpha)$ is to take all outputs of $\mathbb{F}$-coefficient polynomial with input x, as a field

2. All element in simple extension $\mathbb{F}(\alpha)$ can be expressed as a polynomial of α of degree less than $deg(\alpha, \mathbb{F})$

3. If α is algebraic over $\mathbb{F}$, $|\mathbb{F}(\alpha)| = |\mathbb{F}|^{deg(\alpha,\mathbb{F})}$. If α is transcendental over $\mathbb{F}$, $\mathbb{F}(\alpha) \geq \infty$

4. To have $|\mathbb{F}(\alpha)| = p^n$, construct irreducible $f \in \mathbb{Z}_p[x]$ such that $deg(f) = n$, and let α be a zero of f, then $|\mathbb{Z}_p(\alpha)| = p^n$

5. If α is algebraic over $\mathbb{F}$, then there is a set of coefficient in $\mathbb{F}$ that can assemble α back to 0