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. *An $\mathbb{F}$-**polynomial** is a polynomial in $\mathbb{F}[x]$*

Definition 3. *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, no nonzero $\mathbb{F}$-polynomial have root α*

Definition 4. *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 5. *Let $f \in \mathbb{F}[x]$*

f is a monic polynomial if the leading coefficient is 1

Definition 6. *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 $f \in \mathbb{F}[x]$ that satisfy $f(\alpha) = 0$*

Definition 7. *Let f be the irreducible polynomial for α over $\mathbb{F}$*

*We write $irr(\alpha, \mathbb{F}) = f$ and the **degree of** α **over** $\mathbb{F}$ $deg(\alpha, \mathbb{F}) = deg(f)$*

Definition 8. *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 9. *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 10. *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 $f \in \mathbb{F}[x]$, where f have roots less than $deg(f)$ in $\mathbb{F}$*

We can extend $\mathbb{F}$ to a field $\mathbb{E}$ such that f have more roots in $\mathbb{E}$

Proof. First notice that f have root β means exactly that $(x - \beta)$ appears in the factorization of f

Let $deg(f) = n$. Because f have roots less than $deg(f) \in \mathbb{F}$, we factorize f and we will see the result have at least a factor p that is of degree more than 1

Example: Let $f(x) = x^3 + 8x^2 + 21x + 14 = (x^2 + 7x + 14)(x + 1)$ f have only **one** root -1, and $deg(f) = 3$. $p(x)$ is the factor of degree 2

Fix such $p(x)$, and let $\mathbb{E} := \mathbb{F}[x]/\langle p(x)\rangle$

We now prove $\mathbb{F}$ is isomorphic to a subfield of $\mathbb{E}$, so $\mathbb{E} := \mathbb{F}[x]/\langle p(x)\rangle$

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 $\exists \alpha \in \mathbb{E} \setminus \mathbb{F}, f(\alpha) = 0$

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, with input x, of $\mathbb{F}$-coefficient polynomial 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 construct a field of cardinality 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. If α is transcendental, then there is not.

Exercises

29.

Let $\mathbb{E}$ be an extension of $\mathbb{F}$, and let $\alpha, \beta \in \mathbb{E}$. Suppose α is transcendental over $\mathbb{F}$ but algebraic over $\mathbb{F}(\beta)$

Show β is algebraic over $\mathbb{F}(\alpha)$

Proof. α is algebraic over $\mathbb{F}(\beta)$ implies that there exists a set of polynomial $\{f_0, \ldots, f_n\}$ in $\mathbb{F}[x]$ such that $f_n(\beta)\alpha^n + \cdots + f_0(\beta)\alpha^0 = 0$ where $f_n(\beta) \neq 0$

Suppose that among the set of polynomial $\{f_0, \ldots, f_n\}$, the one that is of the highest degree is of the degree m

Then we can rewrite $f_n(\beta)\alpha^n + \cdots + f_0(\beta)\alpha^0 = 0$ into the form

$$g_m(\alpha)\beta^m + \cdots + g_0(\alpha)\beta^0 = 0$$

Where $\{g_m, \ldots, g_0\}$ is a set of polynomial in $\mathbb{F}[x]$

Notice α is transcendental over $\mathbb{F}$, so we know $g_m(\alpha) \neq 0$

This shows that β is algebraic over $\mathbb{F}(\alpha)$ ■

30

Let $\mathbb{E}$ be an extension of $\mathbb{F}$, where $|\mathbb{F}| = q$. Let $\alpha \in \mathbb{E}$. Suppose $deg(\alpha, \mathbb{F}) = n$

Prove $|\mathbb{F}(\alpha)| = q^n$

Proof. Let $f : \mathbb{F}^n \to \mathbb{F}[\alpha]$ be defined by $(c_n, \ldots, c_1) \mapsto c_n\alpha^{n-1} + \cdots + c_1\alpha^0$

Notice every element β in $\mathbb{F}(\alpha)$ can be uniquely expressed in the form $\beta = c_n\alpha^{n-1} + \cdots + c_1\alpha^0$ where $c_i \in \mathbb{F}$, so we know f is bijective, which give us $|\mathbb{F}[\alpha]| = q^n$ ■

31.

(a) Show that there exists an irreducible polynomial of degree 3 in $\mathbb{Z}_3[x]$

(b) Show that there exists a finite field of 27 elements

Proof. **(a)** $x^3 + 2x + 1$ is an irreducible polynomial of degree 3

(b)

We know there exists an extension $\mathbb{E}$ for $\mathbb{F}$ such that $\mathbb{E}$ contain a zero α of $x^3 + 2x + 1$

Notice $deg(\alpha, \mathbb{F}) = 3$

By Exercises 30, we know $|\mathbb{Z}_3(\alpha)| = |\mathbb{Z}_3|^3 = 27$ ■

32

Consider the prime field $\mathbb{Z}_p$

(a) Show that, for $p \neq 2$, not every element in $\mathbb{Z}_p$ is a square of an element of $\mathbb{Z}_p$

(b) Show that there exists finite field of p^2 elements for every prime p in $\mathbb{Z}^+$

Proof. **(a)**

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be defined by $x \mapsto x^2$

Assume every element is a square of an element of $\mathbb{Z}_p$

We know f is onto, so we deduce f is one-to-one by counting

$f(1) = f(p-1)$ CaC

(b)

When p>2, pick an element a that is not a square of an element of $\mathbb{Z}_p$

Consider the polynomial $g(x) = x^2 - a \in \mathbb{Z}_p[x]$

Because g have no zeros in $\mathbb{Z}_p$, and $deg(g) = 2$, so g is irreducible

We know there exists an extension $\mathbb{E}$ of $\mathbb{Z}_p$ such that g have some zeros α in $\mathbb{E}$

$|\mathbb{Z}_p(\alpha)| = p^{deg(\alpha, \mathbb{Z}_p)} = p^{deg(g)} = p^2$

When $p = 2$, consider the polynomial $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$

Because f have no zeros in $\mathbb{Z}_2$, and $deg(f) = 2$, so f is irreducible

We know there exists an extension $\mathbb{E}$ of $\mathbb{Z}_2$ such that g have some zeros α in $\mathbb{E}$

$|\mathbb{Z}_2(\alpha)| = p^{deg(\alpha, \mathbb{Z}_2)} = 2^{deg(g)} = 2^2$

■

35.

Show that there exists a field of 8 elements; of 16 elements; of 25 elements

Proof. Consider $f = x^3 + x + 1 \in \mathbb{Z}_2[x]$

Let $\mathbb{E}$ be an extension of $\mathbb{Z}_2$ containing zeros α for f

$|\mathbb{Z}_2(\alpha)| = 8$

Consider $f = x^4 + x + 1 \in \mathbb{Z}_2[x]$

Let $\mathbb{E}$ be an extension of $\mathbb{Z}_2$ containing zeros α for f

$|\mathbb{Z}_2(\alpha)| = 16$

Consider $f = x^2 + 2 \in \mathbb{Z}_5[x]$

Let $\mathbb{E}$ be an extension of $\mathbb{Z}_5$ containing zeros α for f

$|\mathbb{Z}_5(\alpha)| = 25$

■

36.

Let $\mathbb{F}$ be a finite field of characteristic p. Show that every element of $\mathbb{F}$ is algebraic over the prime field $\{m \cdot 1 | m \in \mathbb{Z}\}$

Proof. Clearly 0 is algebraic over $\{m \cdot 1 | m \in \mathbb{Z}\}$

Let $\alpha \in \mathbb{F}^*$

Notice $\alpha^{|\mathbb{F}^*|} = 1$, since $\mathbb{F}^*$ is a group

Then $\alpha^{|\mathbb{F}^*|} - 1 = 0$, so α is algebraic over $\{m \cdot 1 | m \in \mathbb{Z}\}$ ■

37.

Show that every finite field $\mathbb{F}$ is of prime-power order

Proof. Let p be the characteristic of $\mathbb{F}$

$\{m \cdot 1 | m \in \mathbb{Z}\}$ is an additive subgroup of $\mathbb{F}$ of order p, so $|\mathbb{F}|$ is divided by p

Assume there exists another prime q that divides $|\mathbb{F}|$

Because $\langle \mathbb{F}, + \rangle$ is a group, by Sylow's First Theorem, we know there exists an element $x \in \mathbb{F}$ of order q in the additive group $\mathbb{F}$

Let $q = np + r$ where $r < p$

$r \cdot x = q \cdot x = 0$ CaC ■