1 Extension Fields

We now talk about extension fields.

1.1 Definition of an Extension Field

Definition 1.1: Extension Field

A field E is an **extension field** of a field F if $F \subseteq E$ and F is a field under the same operations as E.

Remark: Note that we say that F is a subfield of E. Alternatively, we can now say that E is a extension field of F.

1.1.1 Example 1: Extension Fields of the Rational Numbers

Consider $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \cong \mathbb{R}[x]/\langle x^2+1\rangle$. We call these the extension field of the rational numbers.

1.1.2 Example 2: Quadratic Extension Fields

Consider $Q \subseteq \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \cong \mathbb{Q}[x]/\langle x^2 - 2\rangle$.

1.1.3 Example 3: Extensions of Finite Fields

Consider $\mathbb{F}_3 \subseteq \mathbb{F}_3[i] \cong \mathbb{F}_3[x]/\langle x^2+1\rangle$.

1.2 Fundamental Theorem of Field Extensions

Theorem 1.1: Fundamental Theorem of Field Extensions

Let F be a field, and $f(x) \in F[x]$. Then, there exists an extension field E of F in which $f(x)$ has a zero.

Remarks:

- The complex numbers is a field extension of the real numbers in which the polynomial x^2+1 has a root.
- $\mathbb{Q}[\sqrt{2}]$ is a field extension of $\mathbb{Q}$ in which x^2-2 has a root.
- $\mathbb{F}_3[i]$ is a field extension of $\mathbb{F}_3$ in which x^2+1 has a root.

Note: The extension is not just $F[x]/\langle f(x)\rangle$. This is because if $f(x)$ is reducible, then $F[x]/\langle f(x)\rangle$ is not a field.
Fact: Every polynomial $f(x) \in \mathbb{C}[x]$ of degree > 0 has a root in the complex numbers, known as *algebraic closure*.

Proof. $F[x]$ is a UFD, so choose an irreducible polynomial $p(x) \in F[x]$ with $\deg p(x) > 0$ such that $p(x)|f(x)$. Then, $F[x]/\langle p(x)\rangle$ is a field. Now, we show that this is an extension field. Consider the mapping

$$\varphi : F \mapsto E$$

sending

$$a \mapsto a + \langle p(x)\rangle$$

This is clearly injective by $\langle p(x)\rangle$ having no non-zero constants. Additionally, the kernal is trivial. So, by the First Isomorphism Theorem, $F \cong \varphi(F) \subseteq E$.

Now, let $x + \langle p(x) \rangle \in E$. If $f(x) = a_n x^n + \dots + a_0$, then

$$\begin{aligned} f(x + \langle p(x) \rangle) &= a_n (x + \langle p(x) \rangle)^n + \dots + a_1 (x + \langle p(x) \rangle) + a_0 \\ &= a_n (x^n + \langle p(x) \rangle) + \dots \\ &= a_n x^n + \dots + a_1 x + a_0 + \langle p(x) \rangle \\ &= f(x) + \langle p(x) \rangle \end{aligned}$$

But, because $p(x) | f(x)$, this implies that $f(x) \in \langle p(x) \rangle$. This further implies that

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

so, we are done. $\square$

1.2.1 Example 1: Polynomial

Consider the polynomial $x^4 + x^3 + x + 2 \in \mathbb{F}_3[x]$. We can factor this into the polynomial

$$(x^2 + 1)(x^2 + x + 2)$$

This is contained in the fields $\mathbb{F}_3[x]/\langle x^2 + 1 \rangle$ or $\mathbb{F}_3[x]/\langle x^2 + x + 2 \rangle$.

1.2.2 Example 2: Polynomial

Consider the polynomial $3x^8 + 2x^6 + 4x + 14 \in \mathbb{Q}[x]$. This is irreducible by Eisenstein's criterion. So, we have the extension field

$$\mathbb{Q} \subseteq \mathbb{Q}[x]/\langle 3x^8 + 2x^6 + 4x + 14 \rangle$$

which has a root of $f(x)$.

1.3 More on Extension Fields

Definition 1.2

Let E be an extension field of F, and let $\alpha_1, \alpha_2, \dots, \alpha_n \in E$. Then, we define $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ to be the smallest subfield of E containing $F, \alpha_1, \alpha_2, \dots, \alpha_n$.

Theorem 1.2

Let E be an extension field of F, $\alpha \in E$ which is a root of the irreducible polynomial $p(x) \in F[x]$. Then,

$$F(\alpha) \cong F[x]/\langle p(x) \rangle$$

Proof. Consider the homomorphism

$$\varphi : F[x] \mapsto E$$

defined by

$$f(x) \mapsto f(\alpha)$$

We make the claim that $\ker \varphi = \langle p(x) \rangle$. We note that $\varphi(p(x)) = p(\alpha) = 0$ by definition. This implies that

$$\langle p(x) \rangle \subseteq \ker \varphi \neq F[x]$$

We note that $\langle p(x) \rangle$ is maximal. This implies that $\ker \varphi = \langle p(x) \rangle$.

The First Isomorphism Theorem says that $F[x]/\langle p(x) \rangle \cong \operatorname{im} \varphi \subseteq E$. We now make the claim that

$\operatorname{im}\varphi = F(\alpha)$. To see this, we note that

$$\alpha = \varphi(x) \implies \alpha \in \operatorname{im}\varphi$$

but if $a \in F$ is constant, then

$$a = \varphi(a) \implies F \subseteq \operatorname{im}\varphi$$

By the First Isomorphism Theorem, $\operatorname{im}\varphi$ is a field. This implies that

$$F(\alpha) \subseteq \operatorname{im}\varphi$$

To show the other side, take some $y \in \operatorname{im}\varphi$. Then, this means taht

$$y = \varphi(a_n x^n + \cdots + a_1 x + a_0) = a_n \alpha^n + \cdots + a_1 \alpha + a_0$$

We know that $\alpha \in F(\alpha)$ and $F \subseteq F(\alpha) \implies a_0, a_1, \ldots, a_n \in F(\alpha)$. This implies that $y \in F(\alpha)$ by closure, implying that $\operatorname{im}\varphi \subseteq F(\alpha)$. $\square$

1.3.1 Example 1

Consider $\mathbb{Q}\left(5^{\frac{1}{4}}\right)$. We know that the polynomial $x^4 - 5$ has the root $5^{\frac{1}{4}}$. By Eisenstein's criterion, this polynomial is irreducible. So

$$\mathbb{Q}\left(5^{\frac{1}{4}}\right) \cong \mathbb{Q}[x]/\langle x^4 - 5\rangle$$

where we can define the isomorphism by

$$5^{\frac{1}{4}} \mapsto x + \langle x^4 - 5\rangle$$

We note that $\mathbb{Q}[x]/\langle x^4 - 5\rangle$ is 4-dimensional. The basis is given by

$$\left\{1, x, x^2, x^3\right\}$$

So, it follows that

$$\mathbb{Q}[x]/\langle x^4 - 5\rangle = \left\{a + bx + cx^2 + dx^3 + \langle x^4 - 5\rangle \mid a, b, c, d \in \mathbb{Q}\right\}$$

But, we can map this to

$$\left\{a + b5^{\frac{1}{4}} + c5^{\frac{2}{4}} + d5^{\frac{3}{4}}\right\}$$