1 Extension Fields

We continue our discussion on extension fields.

1.1 More on Extension Fields

Corollary 1.1

If $\alpha, \beta \in E$, which are both roots of an irreducible polynomial $p(x) \in F[x]$, then $F(\alpha) \cong F(\beta)$.

Proof. We know that $F(\alpha) \cong F[x]/\langle p(x)\rangle \cong F(\beta)$. So, we're done. $\square$

1.1.1 Example 1: Polynomials

Consider $x^3 - 2 \in \mathbb{Q}[x]$. By Eisenstein's criterion, this is irreducible. Although there are no roots in $\mathbb{Q}$, we can find roots in other places. In particular, looking at the complex and real numbers, we know that a root is $\sqrt[3]{2}$. Now,

$$(x^3 - 2) = (x - \sqrt[2]{3})q(x)$$

where $q(x)$ is quadratic. The other roots, then, are

$$\left(\frac{-1+\sqrt{-3}}{2}\right)\sqrt[3]{2}, \left(\frac{-1-\sqrt{-3}}{2}\right)\sqrt[3]{2}$$

If we let $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$, then we know that $\zeta_3 \in \mathbb{C}$ such that

$$(\zeta_3)^3 = 1$$

We have

$$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\zeta_3\sqrt[3]{2}) \cong \mathbb{Q}(\zeta_3^2\sqrt[3]{2})$$

Now, notice that

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b2^{\frac{1}{3}} + c2^{\frac{2}{3}} \mid a, b, c \in \mathbb{Q}\} \subseteq \mathbb{R}$$
$$\mathbb{Q}(\zeta_3\sqrt[3]{2}) = \{a + b\zeta_3 2^{\frac{1}{3}} + c\zeta_3 2^{\frac{2}{3}} \mid a, b, c \in \mathbb{Q}\} \not\subseteq \mathbb{R}$$

1.1.2 Example 2: Pi

Consider $\pi \in \mathbb{R}$, and suppose we look at $\mathbb{Q}(\pi)$. We note that π is not a root of *any* nonzero polynomial in $\mathbb{Q}[x]$. This kind of number is called *transcendental* over $\mathbb{Q}$.

1.2 Splitting Field

Definition 1.1: Splitting Field

Let E be an extension field of F, and let $f(x) \in F[x]$. We say that $f(x)$ *splits* in E if

$$f(x) = a(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$$

for $a \in F$, $\alpha_i \in E$ for $1 \leq i \leq n$. We call E a **splitting field** for $f(x)$ over F if $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Theorem 1.1

Let F be a field and $f(x) \in F[x]$ a nonconstant polynomial. Then, there exists a splitting field for $f(x)$ over $F[x]$.

Proof. We use induction on the degree of $f(x)$.

- Base Case: For $\deg f(x) = 1$, we have $f(x) = ax + b$. A polynomial of degree 1 will have one root; in this case, it's $-\frac{b}{a}$. So, this should already be split. So,

$$f(x) = ax + b = a\left(x - \left(-\frac{b}{a}\right)\right)$$

  splits in F.

- Inductive Step: Suppose that if $\deg g(x) = n - 1$, then $g(x)$ has a splitting field over F. Suppose $\deg f(x) = n$. There exists a field extension E in which $f(x)$ has a root $\alpha \in E$. This implies that

$$f(x) = (x - \alpha)g(x)$$

  for $g(x) \in E[x]$. By the inductive hypothesis, there exists a splitting field K for $g(x)$ over E. This implies that, for $a \in E$, $\alpha_1, \ldots, \alpha_n \in K$ and so

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) = ax^n + \ldots$$

  but $a \in F$. Thus, $f(x)$ splits in K. So, $F(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq K$ is a splitting field.

So, we are done. □

1.2.1 Example 1: Polynomials

$x^3 - 2$ does not split over $\mathbb{Q}$ because it's irreducible. It does not split over $\mathbb{Q}(\sqrt[3]{2})$ because it does not contain the other two roots.

A splitting field is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2})$. This is the same thing as writing $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. This is because

- They both contain $\mathbb{Q}$.
- They both contain $\sqrt[3]{2}$.
- Since $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ contains both $\sqrt[3]{2}$ and ζ_3, and since it's a field, it must be closed under multiplication.

1.3 Even More on Extension Fields

Theorem 1.2

Let F be a field, $p(x) \in F[x]$ a irreducible polynomial, and an isomorphism

$$\varphi : F \mapsto F'$$

Then, if α is a root of $p(x)$ and β is a root $\varphi(p(x))$, then $F(\alpha) \cong F'(\beta)$.

Proof.

$$F(\alpha) \xrightarrow{\sim} F[x]/\langle p(x)\rangle \xrightarrow{\varphi} F'[x]/\langle \varphi(p(x))\rangle \xrightarrow{\sim} F'(\beta)$$

So

$$\varphi(a_n x^n + \cdots + a_0 + \langle p(x)\rangle) = \varphi(a_n)x^n + \cdots + \varphi(a_0) + \langle \varphi(p(x))\rangle$$

And we are done. □

Theorem 1.3

Let $\varphi : F \mapsto F'$ be an isomorphism of fields, $f(x) \in F[x]$. If E is a splitting field for $f(x)$ over F and E' is a splitting field for $\varphi(f(x))$ over F', then there is an isomorphism $E \cong E'$ that agrees with φ on F.

Corollary 1.2

Any two splitting fields of $f(x) \in F[x]$ over F are isomorphic.

Proof. Let $F' = F$. We can define $\varphi : F \mapsto F$ the identity function by $a \mapsto a$. THen, we can apply the theorem. □