Math 403 Chapter 20: Extension Fields

1. **Introduction:** The idea of the final few chapters is to dig a bit deeper into fields, specifically the idea that if a field F is contained inside a field E that things may happen in $E[x]$ that cannot happen in $F[x]$. For example $\mathbb{R} \subseteq \mathbb{C}$ and if we take $p(x) = x^2 + 4 \in \mathbb{R}[x]$ this does not factor in $\mathbb{R}[x]$ but does factor in $\mathbb{C}[x]$.

2. **An Extension Field with a Root - Part 1**

   (a) **Introduction:** First we'll take a look at the question of taking a polynomial $p(x) \in F[x]$ which is irreducible over F and finding a "larger" field in which $p(x)$ has a root, meaning a linear factor. We then go on to look at what that larger field must look like.

   (b) **Definition:** A field E is an *extension field* of a field F if F is a subfield of E.
   Example: An example of a field extension is $\mathbb{Q} \subseteq \mathbb{R}$. Another is $\mathbb{R} \subseteq \mathbb{C}$.

   (c) **Important Note:** We'll use the term "extension field" somewhat liberally when F is not necessarily directly contained in E but rather is isomorphic to a subfield of E. For example $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field and although $\mathbb{R}$ is not really a subfield (or even a subset) of $\mathbb{R}[x]/\langle x^2+1\rangle$ we can treat it as such by noting that

$$\mathbb{R} = \{\alpha \mid \alpha \in \mathbb{R}\} \approx \{\alpha + \langle x^2+1\rangle \mid \alpha \in \mathbb{R}\} \subseteq \mathbb{R}[x]/\langle x^2+1\rangle$$

(d) **Theorem (Fundamental Theorem of Field Theory):** Let F be a field and $f(x) \in F[x]$ be a nonconstant polynomial. Then there is an extension field of F in which $f(x)$ has a root.

Proof: Since $F[x]$ is a UFD we can factor $f(x)$ into irreducible factors. Write $f(x) = p(x)q(x)$ where $p(x)$ is an irreducible factor. We claim that $F[x]/\langle p(x)\rangle$ is an extension field with the desired property.

Since $p(x)$ is irreducible we know from a previous theorem that $\langle p(x)\rangle$ is maximal and $F[x]/\langle p(x)\rangle$ is a field.

The mapping $F \to F[x]/\langle p(x)\rangle$ given by $\alpha \mapsto \alpha + \langle p(x)\rangle$ is 1-1 because $\alpha + \langle p(x)\rangle = \beta + \langle p(x)\rangle$ implies $p(x)\Big|(\beta - \alpha)$ implies $\beta - \alpha = 0$ and operation preserving (by construction). and therefore yields an isomorphism of F to a subfield of $F[x]/\langle p(x)\rangle$.

In this way we can think of $F[x]/\langle p(x)\rangle$ as an extension field of F.

To show that $f(x)$ has a root in $F[x]/\langle p(x)\rangle$ observe that since $p(x)$ is a polyomial we have

$$\begin{aligned} f\left(x + \langle p(x)\rangle\right) &= p\left(x + \langle p(x)\rangle\right) q\left(x + \langle p(x)\rangle\right) \\ &= \left(p(x) + \langle p(x)\rangle\right) q\left(x + \langle p(x)\rangle\right) \\ &= \left(0 + \langle p(x)\rangle\right) q\left(x + \langle p(x)\rangle\right) \\ &= 0 + \langle p(x)\rangle \end{aligned}$$

$\mathcal{QED}$

Example: Consider $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. Since $f(x)$ itself is irreducible over $\mathbb{Q}$ we know that $f(x)$ has a root in the extension field $\mathbb{Q}[x]/\left\langle x^2 + 1\right\rangle$.

Example: Consider $f(x) = x^4 + 8x^2 + 15 \in \mathbb{Q}[x]$. Since $f(x) = (x^2 + 3)(x^2 + 5)$ each of which is irreducible over $\mathbb{Q}$ we know that $f(x)$ has a root in each of the extension fields $\mathbb{Q}[x]/\left\langle x^2 + 3\right\rangle$ and $\mathbb{Q}[x]/\left\langle x^2 + 5\right\rangle$.

Example: Consider $f(x) = x^5 + 2x^2 + 2x + 2 \in \mathbb{Z}_3[x]$. Since $f(x) = (x^2 + 1)(x^3 + 2x + 2)$ each of which is irreducible over $\mathbb{Z}_3$ (by the Degree 2/3 Test) we know that $f(x)$ has a root in each of the extension fields $\mathbb{Z}_3[x]/\left\langle x^2 + 1\right\rangle$ (a field with 9 elements) and $\mathbb{Z}_3[x]/\left\langle x^3 + 2x + 2\right\rangle$ (a field with 27 elements).

3. **An Extension Field with a Root - Part 2**

(a) **Introduction:** So the Fundamental Theorem of Field Theory states that we can always extend a field in order to pick up a root, but as we've seen this is not the only way. For example when we started with $x^2+1 \in \mathbb{Q}[x]$ we could simply have used the extension field $\mathbb{Q}[i]$. Would this have been different in a meaningful sense?

(b) **Definition:** Suppose E is an extension field of F and $a_1, ..., a_n \in E$. Denote by $F(a_1, ..., a_n)$ the smallest subfield of E containing both F and all of the a_i.
Example: We know that $\mathbb{R}$ is an extension field of $\mathbb{Q}$ and $\sqrt{2} \in \mathbb{R}$. We can then create $\mathbb{Q}(\sqrt{2})$ as the smallest subfield of $\mathbb{R}$ containing both $\mathbb{Q}$ and $\sqrt{2}$.

(c) **Theorem:** Let F be a field and $p(x) \in F[x]$ be irreducible over F. Suppose a is a root of $p(x)$ in some extension E of F. Then we have:

i. $F[x]/\langle p(x)\rangle \approx F(a)$

ii. Every element in $F(a)$ can be uniquely expressed in the form

$$c_{n-1}a^{n-1} + ... + c_1 a + c_0 \quad \text{with} c_i \in F$$

Note: This theorem basically states that extending the field via the Fundamental Theorem and extending the field by taking the smallest subfield approach yield isomorphic results. However the latter requires that we have an extension field with our root a in it to begin with.
Example: For example $x^2+2 \in \mathbb{R}[x]$ is irreducible over $\mathbb{R}$. Observe that $\sqrt{-2}$ is a root of x^2+2 in the $\mathbb{C}$, an extension field of $\mathbb{R}$. Then we get:

$$\mathbb{R}[x]/\left\langle x^2+2\right\rangle \approx F(\sqrt{-2})$$

And elements in $F(\sqrt{-2})$ can be expressed uniquely in the form:

$$c_1\sqrt{-2} + c_0 \quad \text{with} c_1, c_0 \in \mathbb{R}$$

Proof:

i. Define $\phi : F[x] \to F(a)$ by $\phi(f(x)) = f(a)$, then ϕ is a ring homomorphism and by the First Isomorphism Theorem we have:

$$F[x]/\text{Ker}\phi \approx \phi(F[x])$$

We claim that $\text{Ker}\phi = \langle p(x)\rangle$. Since $\phi(p(x)) = p(a) = 0$ we know $\langle p(x)\rangle \subseteq \text{Ker}\phi$ and since $\langle p(x)\rangle$ is maximal (since $p(x)$ is irreducible over F) and $1 \notin \text{Ker}\phi$ (since $\phi(1) = 1 \neq 0$) we know that $\text{Ker}\phi \neq F[x]$ and hence $\text{Ker}\phi = \langle p(x)\rangle$. So far this proves:

$$F[x]/\text{Ker}\left\langle p(x)\right\rangle \approx \phi(F[x])$$

Next we must show that $\phi(F[x]) = F(a)$.
By the definition of ϕ we know $\phi(F[x]) \subseteq F(a)$ so we'll show that $\phi(F[x])$ is a field which contains F and a and then since $F(a)$ is minimal we are done.

- $\phi(F[x])$ is a field because the quotient ring is a field by the previous theorem.
- $F \subseteq \phi(F[x])$ because for any $\alpha \in F$ we have $\phi(\alpha) = \alpha$ and $a \in \phi(F[x])$ because $\phi(x) = a$.

ii. The second result follows from the fact that the elements in $F[x]/\langle p(x)\rangle$ can be expressed uniquely in the form

$$c_{n-1}x^{n-1} + ... + c_0 + \langle p(x)\rangle$$

with $c_i \in F$ as we have seen in several examples and the isomorphism ϕ above maps such an element to $c_{n-1}a^{n-1} + ... + c_0$.

$\mathcal{QED}$

Example: Given $f(x) = x^2 + 2 \in \mathbb{Q}[x]$ and irreducible over $\mathbb{Q}$ we know that $\sqrt{-2} \in \mathbb{C}$, an extension field of $\mathbb{Q}$, and therefore:

$$\mathbb{Q}(\sqrt{-2}) \approx \mathbb{Q}[x]/\langle x^2 + 2 \rangle$$

and moreover:

$$\mathbb{Q}(\sqrt{-2}) = \left\{ c_1\sqrt{-2} + c_0 \,|\, c_i \in \mathbb{Q} \right\}$$

Example: Given $f(x) = x^3 - 5 \in \mathbb{Q}[x]$ and irreducible over $\mathbb{Q}$ we know that $\sqrt[3]{5} \in \mathbb{R}$, an extension field of $\mathbb{Q}$, and therefore:

$$\mathbb{Q}(\sqrt[3]{5}) \approx \mathbb{Q}[x]/\langle x^3 - 5 \rangle$$

and moreover:

$$\mathbb{Q}(\sqrt[3]{5}) = \left\{ c_2(\sqrt[3]{5})^2 + c_1(\sqrt[3]{5}) + c_0 \,|\, c_i \in \mathbb{Q} \right\}$$

Example: We can't always play this game since we have to know about an extension field already in order to build $F(a)$. For example $f(x) = x^5 + 2x^2 + 2x + 2 \in \mathbb{Z}_3[x]$ is irreducible over $\mathbb{Z}_3$ but other than using the quotient field approach we have no knowledge about any other extension field $\mathbb{Z}_3 \subseteq E$ in which there is a root $a \in E$ with which to construct $\mathbb{Z}_3(a)$

Note: In general $F(a, b) = F(a)(b)$, so for example $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ which is then the field of expressions of the form:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{ (a\sqrt{2} + b)\sqrt{3} + (c\sqrt{2} + d) \,|\, a, b, c, d \in \mathbb{Q} \right\}$$

which may be rewritten as:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{ a\sqrt{6} + b\sqrt{3} + c\sqrt{2} + d \,|\, a, b, c, d \in \mathbb{Q} \right\}$$

(d) **Corollary:** Let F be a field and $p(x) \in F[x]$ be irreducible over F. If b is a root of $p(x)$ in some extension E_1 of F and if a is a root of $p(x)$ in some extension E_2 of F then $F(a) \approx F(b)$.

Proof: Follows immediately since $F(a) \approx F[x]/\langle p(x) \rangle \approx F(b)$. $\mathcal{QED}$

4. **Splitting and Splitting Fields**

(a) **Introduction:** By the Fundamental Theorem of Field Theory we know that given $p(x) \in F[x]$ which is irreducible over F we can extend F to a field extension E to pick up a root, and hence a linear factor, we might wonder about extending F so that it picks up all roots and so $p(x)$ factors completely into linears.

(b) **Definition:** Let E be an extension field of F and let $f(x) \in F[x]$ be a nonconstant polynomial. We say that $f(x)$ *splits in* E if there are elements $a \in F$ and $a_1, ..., a_n \in E$ such that:

$$f(x) = a(x - a_1)...(x - a_n)$$

Note: The $a \in F$ is just there to basically say we can factor out the leading coefficient first. Almost always we'll deal with polynomials in which the leading coefficient is 1.

Note: The phrase "splits in E" is standard but confusing. A better phrase might be "splits in $E[x]$" or "splits over E".

(c) **Definition:** Given a field F and a polynomial $f(x) \in F[x]$, an extension field E of F is a *splitting field for* $f(x)$ *over* F if $f(x)$ splits in E does not split in any proper subfield of E containing F.

Note: The basic idea is that a splitting field is an extension field into which the polynomial splits but it does not split in a smaller subfield.

Example: The polynomial $x^2 - 2 \in \mathbb{Q}[x]$ splits in $\mathbb{C}$ since $x^2 = (x + \sqrt{2})(x - \sqrt{2})$ and both $(x + \sqrt{2}), (x - \sqrt{2}) \in \mathbb{C}[x]$. Of course it splits in $\mathbb{R}$ as well, and also in $\mathbb{Q}(\sqrt{2})$. In fact since the extension must contain the roots we know by definition that $\mathbb{Q}(\sqrt{2})$ is the smallest such extension field and is therefore a splitting field.

Note: Splitting fields are not necessarily unique. We know $\mathbb{Q}(\sqrt{2}) \approx \mathbb{Q}[x]/\langle x^2 - 2 \rangle$ and so $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$ is also a splitting field for $x^2 - 2$ over $\mathbb{Q}$. However this is a different (yet isomorphic) field extension than $\mathbb{Q}(\sqrt{2})$.

(d) **Theorem (Existence of Splitting Fields):** Let F be a field and $f(x) \in F[x]$ be a nonconstant polynomial. Then there exists a splitting field E of $f(x)$ over F.
Note: We'll assume $f(x)$ has leading coefficient 1, if not, just factor the leading coefficient first and deal with the rest.
Proof: By induction on the degree of $f(x)$. If the degree of $f(x)$ is 1 then $f(x)$ is linear and $f(x)$ is already split into one term. Suppose the statement is true for all polynomials of degree less than the degree of $f(x)$. By the Fundamental Theorem of Field Theory there is an extension field E of F in which $f(x)$ has a root, hence we get a linear term and so $f(x) = (x - a_1)g(x)$ where $a_1 \in E$ and $g(x) \in E[x]$. By the induction hypothesis then we have an extension field K of E in which $g(x)$ splits as $g(x) = (x - a_2)...(x - a_n)$ and so we see that $f(x)$ splits over K as well, since $f(x) = (x - a_1)(x - a_2)...(x - a_n)$. This K may not be a splitting field however we can obtain a splitting field by simply taking $F(a_1, ..., a_n)$. $\mathcal{QED}$

(e) **Theorem (Uniqueness of Splitting Fields up to Isomorphism):** Let F be a field and $f(x) \in F[x]$. Then any two splitting fields of $f(x)$ over F are isomorphic.
Before proving this, two lemmas:
Lemma: Suppose $\phi : F_1 \to F_2$ is a field isomorphism. Let $p(x) \in F_1[x]$ be irreducible over F_1 and suppose a_1 is a root of $p(x)$ in an extension field of F_1 and suppose a_2 is a root of $\phi(p(x))$ in an extension field of F_2. Then we can extend ϕ to an isomorphism from $F_1(a_1)$ to $F_2(a_2)$ which takes a_1 to a_2.
Proof: Since $p(x)$ is irreducible over F_1 we know that $\phi(p(x))$ is irreducible over F_2. The mapping:

$$\psi : F_1[x]/\langle p(x)\rangle \to F_2[x]/\langle \phi(p(x))\rangle$$

defined by

$$\psi\left(f(x) + \langle p(x)\rangle\right) = \phi(f(x)) + \langle \phi(p(x))\rangle$$

is a field isomorphism (check!) so then consider that we have a compound field isomorphism:

$$F_1(a_1) \to F_1[x]/\langle p(x)\rangle \to F_2[x]/\langle \phi(p(x))\rangle \to F_2(a_2)$$

where the first and third isomorphisms result from the Fundamental Theorem of Field Theory. Note that:

$$a_1 \mapsto x + \langle p(x)\rangle \mapsto \phi(x) + \langle \phi(p(x))\rangle \mapsto a_2$$

and note that for $\alpha \in F_1$ that:

$$\alpha \mapsto \alpha + \langle p(x)\rangle \mapsto \phi(\alpha) + \langle \phi(p(x))\rangle \mapsto \phi(\alpha)$$

$\mathcal{QED}$
Lemma: Suppose $\phi : F_1 \to F_2$ is a field isomorphism. Let $f(x) \in F_1[x]$. Suppose E_1 is a splitting field for $f(x)$ over F_1 and if E_2 is a splitting field for $\phi(f(x))$ over F_2. Then we can extend ϕ to an isomorphism from E_1 to E_2.
Proof: We induct on the degree of $f(x)$ by taking irreducible factors of $p(x)$ and using the previous lemma to extend E_1 progressively to pick up all the roots. Details omitted. $\mathcal{QED}$
Proof of Theorem: Follows immediately from the previous lemma using $F_1 = F_2 = F$ and letting ϕ be the identity. $\mathcal{QED}$

Example: In the case of $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ and irreducible over $\mathbb{Q}$ we know about two splitting fields, those being $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}[x]/\langle x^2 - 2\rangle$, and we already know that those are isomorphic. This theorem states that any others would also need to be isomorphic.

Example: Consider $f(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ which is irreducible over $\mathbb{Z}_3$.

Consider:

- The set:
$$\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$$
is in fact an extension field of $\mathbb{Z}_3$ (can you show it's a field?). In this field $f(x)$ splits since $x^2+1 = (x+i)(x+2i)$ and $(x+i), (x+2i) \in \mathbb{Z}_3[i][x]$. (Note that $\mathbb{Z}_3[i][x]$ means polynomials with coefficients in $\mathbb{Z}_3[i]$.) In fact there is no smaller subfield of $\mathbb{Z}_3[i]$ containing $\mathbb{Z}_3$ in which $f(x)$ splits (can you show this?) and so $\mathbb{Z}_3[i]$ is a splitting field for $f(x)$ over $\mathbb{Z}_3$.
- By the FTOFT $f(x)$ has a root, hence a linear factor, hence splits, in the extension field:
$$\mathbb{Z}_3[x]/\langle x^2 + 1\rangle = \left\{a + bx + \langle x^2 + 1\rangle \mid a, b \in \mathbb{Z}_3\right\}$$
In fact there is no smaller subfield of $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ containing (an isomorphic copy of) $\mathbb{Z}_3$ in which $f(x)$ splits and so $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ is a splitting field for $f(x)$ over $\mathbb{Z}_3$.
$$\mathbb{Z}_3[i] \approx \mathbb{Z}_3[x]/\langle x^2 + 1\rangle$$

Note: We can't write $\mathbb{Z}_3(i)$ to begin with because this requires us to start with an extension field of $\mathbb{Z}_3$ which contains i, and there is no obvious choice. However now that we know that $\mathbb{Z}_3[i]$ is an extension field of $\mathbb{Z}_3$ containing i then we can write $\mathbb{Z}_3(i)$ with this context.