TOPICS IN ALGEBRA: FIELD EXTENSIONS AND GALOIS THEORY

PHIL MAYER

1. Extension Fields

Consider the polynomial $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Based on our discussion of unique factorization, we know that $x^2 - 2$ is irreducible over $\mathbb{Q}[x]$, but suppose we extend our field of possible coefficients to $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. We can then factor $f(x)$ into a product of linear terms in $\mathbb{Q}(\sqrt{2})$: $f(x) = (x - \sqrt{2})(x + \sqrt{2})$. Some preliminaries for the theory of field extensions are as follows.

Definition 1.1. E is an **extension field** of a field F if and only if $F \leq E$ (F is a subfield of E). Furthermore, E is a **simple extension** of F if and only if $E = F(\alpha)$ for some α.

Some common examples of extension fields include $\mathbb{Z}\sqrt{d}$ and $\mathbb{C} = \mathbb{R}(i)$. While some extension fields may initially appear to not be simple, as multiple extensions like $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, they may actually end up being simple. For example, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Definition 1.2. Let $\alpha \in E$, where E is an extension field of F. We say that α is **algebraic** over F if and only if α is a root of some function $f(x) \in F[x]$. Otherwise, α is said to be **transcendental** over F. Therefore, α is transcendental over F if and only if α is not algebraic over F.

For example, π and e are transcendental over $\mathbb{Q}$, yet algebraic over $\mathbb{R}$ since the functions $f(x) = x - \pi$ and $g(x) = x - e$ are in $\mathbb{R}[x]$. Yet not all real numbers are transcendental over $\mathbb{Q}$, for example. If we consider $\alpha = \sqrt{5}$, we see that α is a root of the function $x^2 - 5 \in \mathbb{Q}[x]$. As another example, if $\alpha = \sqrt{2} + \sqrt{3}$, then:

$$\alpha - \sqrt{2} = \sqrt{3} \implies 0 = \alpha^2 - 2\sqrt{2}\alpha - 1 \notin \mathbb{Q}[x]$$
$$\text{But } 0 = \alpha^4 - 10\alpha^2 + 1 \in \mathbb{Q}[x]$$

So α can be a root of a polynomial of degree 4 at the lowest over $\mathbb{Q}[x]$.

Now again consider $\mathbb{Q}(\sqrt{5})$. Notice that $\forall r \in \mathbb{Q}(\sqrt{5})$, $r = a + b\alpha = a + b\sqrt{5}$. Similarly, for all elements r in the field $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, would end up looking like $r = a + b\alpha + c\alpha^2 + d\alpha^3$ for $\alpha = \sqrt{2}+\sqrt{3}$. As we can see, the elements of our field start looking like vectors, written as linear combinations of basis vectors! For example, recall that in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, $\alpha^4 = 10\alpha^2 - 1$. So α^4 can be thought of as a linear combination of basis elements $\{1, \alpha, \alpha^2, \alpha^3\}$. Let's begin formalizing some of these ideas.

Theorem 1.3. *Suppose α is algebraic over F. Let $p(x)$ be the monic polynomial of smallest degree of which α is a root. Then $p(x)$ is irreducible over F and if $f(\alpha) = 0$, then $p(x) \mid f(x)$.*

Definition 1.4. We say that $p(x)$ (as defined in the previous theorem) is the **irreducible polynomial for α over F**. We denote it $\text{irr}(\alpha, F)$. The **degree of α over F** is given by $\deg(\alpha, F) = \deg(\text{irr}(\alpha, F))$.

Let's prove the theorem using this information. Our approach will be to use the division algorithm for polynomials.

Proof. First, suppose $p(x) \in F[x]$ is reducible.
Then it can be written $p(x) = f(x)g(x)$ for functions $f, g \in F[x]$.
Plug in $x = \alpha$. Then $p(\alpha) = 0 = f(\alpha) \cdot g(\alpha) \implies$ either $f(\alpha) = 0$ or $g(\alpha) = 0$.
But contradiction: $p(x)$ is the polynomial of least degree for which α is a root.
So $p(x)$ is irreducible over F.
Now suppose that α is a root of some function $h(x) \in F[x]$.
Then divide h by p: $h(x) = p(x)q(x) + r(x)$ where $0 < \deg(r) < \deg(p)$ or $r(x) = 0$.
Plugging in α, we see $h(\alpha) = 0 = p(\alpha)q(\alpha) + r(\alpha)$.
But $p(\alpha) = 0$, so $0 = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha) \implies r(\alpha) = 0$.
So $p(x) \mid h(x)$. □

To apply the theorem and definition to our previous example, we see that $\text{irr}(\alpha, \mathbb{Q}) = x^4 - 10x^2 + 1$ and $\deg(\alpha, \mathbb{Q}) = 4$. Let's do another example. Suppose we want to find the roots of the polynomial $f(x) = x^2 + x + 1$. Over $\mathbb{Z}_2$, we can plug in $x = 0$ and $x = 1$ to quickly see that $f(x)$ is irreducible. Yet suppose α is a root of the polynomial in some extension field $\mathbb{Z}_2(\alpha)$. Then just like in our other extension fields, elements in $\mathbb{Z}_2(\alpha)$ look like $a + b\alpha$ where $a, b \in \mathbb{Z}_2$. Since there are only two possibilities for a, b in this case, we can describe the extension field fully as the following set:

$$\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}$$

If we divide the linear term $(x - \alpha)$ into $f(x)$, we get the quotient $x + (1 + \alpha)$. So we have found a root of the function $f(x) = x^2 + x + 1$ in some field, namely $\mathbb{Z}_2(\alpha)$. To summarize, we have the following important theorem:

Theorem 1.5. *Let $F[x]$ be a ring of polynomials. If $f(x) \in F[x]$, then there exists an extension field E with $F \leq E$ where $f(x)$ has a root in E.*

2. Extension Fields as Vector Spaces

As mentioned in the last section, we can think of elements in an extension field as linear combinations of basis elements. The following theorem summarizes this idea.

Theorem 2.1. *Suppose α is algebraic over F and consider $E = F(\alpha)$. Then any $\beta \in E$ can be written uniquely as:*

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

where $a_i \in F$.

So if we have some power of α higher than $n-1$, we can rewrite it as a linear combination of lower powers of α. To prove this theorem, we need to prove both existence and uniqueness.

Proof. Since α is algebraic over F, α is a root of some irreducible, monic polynomial $p(x) = c_0 + c_1x + \cdots + x^n$ choosing $c_i \in F$ appropriately.
So $c_0 + c_1\alpha + \cdots + \alpha^n = 0$, or rearranged $\alpha^n = -c_{n-1}\alpha^{n-1} - \cdots - c_0$.
But suppose β is not written uniquely.
Then renaming the c_i from before to a_i, we know:

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

But then $\beta - \beta = 0$, so we have:

$$(a_0 - b_0) + (a_1 + b_1)\alpha + \cdots + (a_{n-1} + b_{n-1})\alpha^{n-1}$$

Where at least one coefficient has $a_i - b_i \neq 0$.
So β is a linear combination of $\{1, \alpha, \cdots, \alpha^{n-1}\}$ and α is therefore a root of some polynomial of degree less than n. □

So we can view any extension field $F(\alpha)$ as a vector space with dimension $\dim(F(\alpha)) = \deg(\text{irr}(\alpha, F))$. For example, consider the polynomial $x^4 - 6x^2 + 3$ over $\mathbb{Q}$. If we take $\alpha = \sqrt{3 - \sqrt{6}}$, then $\alpha^4 = 6\alpha^2 + 3 \implies \deg(\text{irr}(\alpha, \mathbb{Q})) = 4$. So we can take the set $\{1, \alpha, \alpha^2, \alpha^3\}$ to be a basis for $\mathbb{Q}(\alpha)$. If we instead work in the field $\mathbb{Q}(\sqrt{6})$, we instead have $\text{irr}(\alpha, \mathbb{Q}(\sqrt{6}) = x^2 - 3 + \sqrt{6}$ since $\alpha^2 = 3 - \sqrt{6} \in \mathbb{Q}(\sqrt{6})$. So our basis might instead look like $\{1, \alpha\}$ in order to generate all of $\mathbb{Q}(\alpha)$. The following theorem summarizes these ideas.

Theorem 2.2. *If $\deg(\alpha, F) = n$, then $F(\alpha)$ is a vector space with dimension n over F with basis $\{1, \alpha, \cdots, \alpha^{n-1}\}$. Furthermore, if $\beta \in F(\alpha)$, then β is algebraic over F and $\deg(\beta, F) \leq n$.*

Proof. Since $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, then any element in $F(\alpha)$ with degree (of α) greater than n can be rewritten as a linear combination of $\{1, \alpha, \cdots, \alpha^{n-1}\}$.
Suppose $\beta \in F(\alpha)$.

Then we have $n+1$ elements in the set $\{1, \beta, \cdots, \beta^n\}$, but our vector space has n elements.
So clearly the set is linearly dependent.
Then $b_n\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_0 = 0$ with at least one $b_i = 0$.
Therefore β is a root of some polynomial $f(x) \in F[x]$ so β is algebraic over F.
Furthermore, $\deg(f) \leq n$. □

3. Field Extensions Continued

Definition 3.1. E is an **algebraic extension** of F if and only if every element in E is algebraic over F.

Definition 3.2. E is a **finite extension** of F if and only if E is a finite-dimensional vector space over F.

So consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p})$ for each prime p. This is an infinite-dimensional vector space, and thus is not a finite extension of $\mathbb{Q}$. It is an algebraic extension, however, since we can square all elements and eventually get rational numbers. It turns out that if a field extension is finite, then it will be algebraic.

Theorem 3.3. *If E is a finite extension of F, then E is an algebraic extension of F.*

Proof. Suppose E over F is finite.
Then $[E : F] = n$, the dimension of E as a vector space.
Pick $\beta \in E$ and consider $1, \beta, \cdots, \beta^n$.
Then we have $n + 1$ elements and our vector space is n-dimensional.
So $1, \beta, \cdots, \beta^n$ are linearly dependent.
Then $a_0 + a_1\beta + \cdots + a_n\beta^n = 0$ with at least one $a_i \neq 0, a_i \in F$.
Then β is a root of $a_0 + a_1x + \cdots + a_nx^n$, so β is algebraic over F. □

The following theorem also illustrates another behavior of field extensions. If we have a "tower" of fields, then we can compute the dimension of the greatest extension from the smaller ones as follows.

Definition 3.4. Let E be a finite extension field of F. Then $[E : F] = \dim(E/F) = \deg(E/F)$.

Theorem 3.5. *If $F \leq E \leq K$, then $[K : F] = [K : E][E : F]$.*

Proof. Suppose $\{\vec{v}_i\}_{i=1}^n$ is a basis for K over E and $\{\vec{w}_j\}_{j=1}^m$ is a basis for E over F.
Then $[K : E] = n$ and $[E : F] = m$.
Now consider $\{\vec{v}_i\vec{w}_j\}$. We want to show this is a basis for K over F.
To show this is a generating set, pick $\alpha \in K$. We want to show α is a linear combination of $\vec{v}_i, \vec{w}_j$.
We can then write α as:

$$\alpha = \sum_{i=1}^n a_i\vec{v}_i$$

where $a_i \in E$ and E is a vector space over F.
But we can write each a_i as:

$$a_i = \sum_{j=1}^m b_{ij}\vec{w}_j \forall a_i$$

where $b_{ij} \in F$. We can then combine these two equations to see see:

$$\alpha = \sum_{i=1}^{n} \sum_{j=1}^{m} b_{ij} \vec{w}_j \vec{v}_i$$

Therefore $\{\vec{v}_i \vec{w}_j\}$ generates all of K. The proof for linear independence is left out, but can be shown relatively easily. □

We can also extend this theorem to the more general case where we have a taller "tower" of fields.

Corollary 3.6. Suppose $F_1 \leq F_2 \leq \cdots \leq F_n$. Then $[F_n : F_1]$ is given by:

$$[F_n : F_1] = \prod_{i=0}^{n-2} [F_{n-i} : F_{n-i-1}]$$

This can be proven relatively easily by mathematical induction. Since we now have products, we can also ask about divisibility.

Corollary 3.7. Suppose $\beta \in F(\alpha)$. Then $[F(\beta) : F] \mid [F(\alpha) : F]$.

Proof. Using the previous theorems, we know $[F(\alpha) : F] = [F(\alpha) : F(\beta)][F(\beta) : F]$ since $F \leq F(\beta) \leq F(\alpha)$. □

Finally, to move onto the next topic we need to introduce one more idea.

Definition 3.8. A field is said to be **algebraically closed** if and only if we cannot algebraically extend it. So, if F is closed, then any polynomial with coefficients in F has a root in $F[x]$.

It is implicit in this definition, then, that the only irreducible polynomials in an algebraically closed field $F[x]$ are linear, and any polynomial with higher degree (with coefficients in F) factors into a product of linear terms. The standard example is $\mathbb{C}$.

4. Constructions

To do constructions, we start with a unit line segment. The length of the line segment, regardless of its exact measure, will then be used to construct other numbers on the plane. For example, from the unit segment we get the point $(1, 0)$. We can then use a compass to get the points $(2, 0)$ and $(-1, 0)$, as well as points with y-coordinates like $(0, 1)$ and $(0, -1)$. Given lines of length α and $\beta \neq 0$, we can get $\frac{\alpha}{\beta}$ by constructing similar triangles.

Definition 4.1. A number α is constructable if and only if a line segment of $\mid \alpha \mid$ can be constructed from the unit segment in a finite number of steps.

The easily constructable numbers are the rationals, but we can also create field extensions of $\mathbb{Q}$ by adding square roots, done by intersecting lines with circles. Overall, it is clear then that the set of constructable numbers is a field, always a subfield of $\mathbb{R}$.

Theorem 4.2. *If γ is a constructable number, then there is a finite sequence of constructable $\alpha_1, \alpha_2, \cdots, \alpha_n$ with $\alpha_i = \gamma$ for some $i \in \mathbb{N}$ with $1 \leq i \leq n$ where $[\mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n) : \mathbb{Q}] = 2^n$, and so $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^r$ for some $r \in \mathbb{N}$.*

Now since $\gamma \in \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n)$, then $2^n = [\mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n) : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n) : \mathbb{Q}(\gamma)][\mathbb{Q}(\gamma) : \mathbb{Q}]$ where $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^r$. So $\mathbb{Q}(\gamma) \subset \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_n)$. We can now use these facts to prove some historically important theorems.

Theorem 4.3. *You cannot double a cube. For example, starting with a cube of volume 1, you cannot construct a cube of volume 2.*

Proof. Assume for contradiction that we can.
Then for a cube of volume 2, each of its side lengths are $\sqrt[3]{2}$.
But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $3 \neq 2^r$ for any $r \in \mathbb{Z}$, so contradiction.

□

Theorem 4.4. *You cannot square a circle. So, for example, given a circle of radius 1, we cannot construct a square that also has area π.*

Proof. Assume that in general, we can square a circle. Then consider a circle with radius 1.
Since the circle has area π, the square would need side lengths $\sqrt{\pi}$.
But $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$, which implies $\sqrt{\pi} \neq 2^r$ for any $r \in \mathbb{Z}$, so contradiction.

□

Theorem 4.5. *You cannot trisect an angle.*

Proof. Assume you can trisect $\theta = 60°$. Then we need to construct $\phi = 20°$.
Now you can show that ϕ is constructable if and only if a line segment of $\cos(\phi)$ is constructable.

But recall $\cos(3\phi) = 4\cos^3(\phi) - 3\cos(\phi)$ and $\cos(3\phi) = \cos(60^\circ) = \frac{1}{2}$.
So $\cos(3\phi) = \frac{1}{2} = 4\alpha^3 - 3\alpha$ for some α.
Then α is a root of the polynomial $8x^3 - 6x - 1$, which is irreducible over $\mathbb{Q}$.
But $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 \neq 2^r$ for any $r \in \mathbb{Z}$. So contradiction. □

5. Galois Theory

The next concept that we will explore is the relationship between field extensions (particularly, in relation to roots of polynomials) and groups of automorphisms. This will allow us to prove the insolvability of quintic polynomials in general, and more.

Definition 5.1. Recall that f is an **isomorphism** from F to F' if and only if f is one-to-one, onto, and $\forall a, b \in F, f(ab) = f(a)f(b)$ and $f(a+b) = f(a) + f(b)$.

Definition 5.2. f is an **automorphism** if and only if f is an isomorphism from F to F, itself.

We also need to rigorously define the idea of two field elements being conjugates. In previous courses in algebra and calculus, we saw that expressions like $x + \sqrt{2}$ could often by simplified by multiplying by their conjugate. In this case, $x + \sqrt{2}$'s conjugate is $x - \sqrt{2}$, but recall that we also talked about conjugates of complex numbers. The two ideas can be related by the following definition.

Definition 5.3. α and β are said to be **conjugates** if and only if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$.

For example, consider $\sqrt{17}$ and $-\sqrt{17}$ over $\mathbb{Q}$. These two numbers are conjugate since $\operatorname{irr}(\pm\sqrt{17}, F) = x^2 - 17$. Conversely, consider the function $f(x) = x^2 + x + 1$ over $\mathbb{Z}_2$. Since $\alpha, \alpha + 1 \in \mathbb{Z}_2(\alpha)$ are both roots, they are conjugates over $\mathbb{Z}_2$.

Now consider the polynomial $g(x) = x^3 - 5$ over $\mathbb{Q}$. Clearly, $\alpha = \sqrt[3]{5}$ is a real root, but the other two roots are complex. It turns out that for:

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

which is called a primitive cube root of 1, the other roots are $\omega\sqrt[3]{5}$ and $\omega^2\sqrt[3]{5}$. This result can be derived by factoring $g(x)$ into $(x - \alpha)(x^2 + \alpha x + \alpha^2)$ then applying the quadratic formula to the second factor. So by the above definitions, $\alpha, \omega\alpha$, and $\omega^2\alpha$ are all conjugates over $\mathbb{Q}$ since they share the same irreducible polynomial over $\mathbb{Q}$, namely $g(x)$. You could construct a tower of fields here, building up from $\mathbb{Q}$ to $\mathbb{Q}(\alpha$ and $\mathbb{Q}(\omega)$ up to $\mathbb{Q}(\alpha, \omega)$. The extension degrees and bases would be $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ with basis $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$, $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = 2$ since ω is a root of $x^2 + \alpha x + \alpha^2$ with basis $\{1, \omega\}$, and $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6$.

To begin tying these concepts into the discussion of automorphisms, consider the following theorem.

Theorem 5.4 (The Conjugation Isomorphisms)**.** *Suppose α, β are algebraic over F with $\deg(\alpha, F) = n$. Take $\phi : F(\alpha) \to F(\beta)$ defined by $\phi(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}$. Then ϕ is an isomorphism if and only if α is conjugate to β (i.e. $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$). Elements in F are left fixed and there exists exactly one such isomorphism for each β conjugate to α, leaving F fixed.*

So ultimately, our field isomorphisms send conjugates in one field to conjugates in another field. This means that automorphisms bring conjugates to conjugates in the same field. Interestingly, this idea is a direct analog to linear transformations; we might describe the behavior of a linear transformation by showing its action on basis vectors. For example, $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ by $id : \sqrt{2} \to \sqrt{2}$ and $\sigma_1 : \sqrt{2} \to \sqrt{2}$ fully describes two field isomorphisms (in fact, automorphisms in this case). As another example, we might consider $g : \mathbb{Q}(\sqrt[3]{5}) \to \mathbb{Q}(\omega\sqrt[3]{5})$ by $\sqrt[3]{5} \to \omega\sqrt[3]{5}$, or in other words $g(a + b\sqrt[3]{5} + c\sqrt[3]{25}) = a + b\omega\sqrt[3]{5} + c\omega\sqrt[3]{25}$. This example is not an automorphism since it sends elements from one field to a different field, despite acting on “basis” elements.

Definition 5.5. Let $\sigma : F \to F$ be an automorphism. We say $a \in F$ is **left fixed** by σ if and only if $\sigma(a) = a$. We can denote the set of all elements left fixed by σ as F_σ, called the **fixed field** of σ. Furthermore, given a set of automorphisms $\sigma_i : F \to F$, we say that $a \in F$ is left fixed by $\{\sigma_i\}$ if and only if $\forall i, \sigma_i(a) = a$, and we can denote the set of such elements $F_{\{\sigma_i\}}$.

Theorem 5.6. *If $F \leq E$, then $E_{\{\sigma_i\}} \leq E$ (i.e. $E_{\{\sigma_i\}}$ is a subfield of E).*

Proof. Suppose $F \leq E$ and $\forall i \in I, \sigma_i : E \to E$ is an automorphism.
Then $E_{\{\sigma_i\}} \neq \varnothing$ since $F \leq E_{\{\sigma_i\}}$.
Now let $a, b \in E_{\{\sigma_i\}}$.
Then $\sigma(a + b) = \sigma(a) + \sigma(b) = a + b$ since σ is an automorphism.
Similarly, $\sigma(ab) = \sigma(a) \cdot \sigma(b) = ab$.
$\therefore E_{\{\sigma_i\}}$ is a subfield of E. □

We can now begin to discuss the group structures involved.

Theorem 5.7. *Suppose $F \leq E$. Then the set of automorphisms of E is a group under function composition.*

Proof. Now clearly the set of all automorphisms of E is a subset of S_E, the set of permutations on E.
So let σ_1 and σ_2 be automorphisms of E.
Then $\sigma_1 \circ \sigma_2$ is an automorphism because both are automorphisms.
We also know that the identity permutation, $id = \iota$, is an automorphism as well since $\forall a \in E, \iota(a) = a$.
Finally, since σ_1 is a permutation, then σ_1^{-1} exists and is an automorphism as well, since σ_1 is an automorphism.
$\therefore$ the set of automorphisms of E is a group. □

Theorem 5.8. *Suppose $F \leq E$. Then the set of all automorphisms of E leaving F fixed is a subgroup of all automorphisms of E. We denote it by $G(E/F)$ and refer to this group as the **Galois group** of E over F.*

Proof. Let $\sigma, \tau \in G(E/F)$.
Then if we let $a \in F$, $\sigma(\tau(a)) = \sigma(a) = a \implies \sigma \circ \tau \in G(E/F)$.
Furthermore, $id = \iota$ has $\iota(a) = a$, so $\iota \in G(E/F)$.
Finally if $\sigma(a) = a$, then $\sigma^{-1}(a) = a$ so $\sigma^{-1} \in G(E/F)$.
$\therefore G(E/F)$ is a subgroup of the set of all automorphisms of E. □

For example, suppose we have a tower of fields with $\mathbb{Q}(\sqrt{7}, \sqrt{11})$ on top with $[\mathbb{Q}(\sqrt{7}, \sqrt{11}) : rationals] = 4$ and both $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{11})$ one level below each with extension degree 2 over $\mathbb{Q}$. Now consider $G(\mathbb{Q}(\sqrt{7})/\mathbb{Q}) = \{id, \sigma_1 : \sqrt{7} \to -\sqrt{7}\}$. Then if we consider the set of all automorphisms of $\mathbb{Q}(\sqrt{7}, \sqrt{11})$ over $\mathbb{Q}$, we have:

$$G(\mathbb{Q}(\sqrt{7}, \sqrt{11})/\mathbb{Q}) = \{\iota = id, \tau_1 : \sqrt{7} \to -\sqrt{7}, \sqrt{11} \to \sqrt{11}, \tau_2, \tau_3\}$$

Interestingly, we can view τ_1 as an extension of σ_1 since it performs the same action on $\mathbb{Q}(\sqrt{7})$. This serves to motivate the following theorem:

Theorem 5.9 (Isomorphism Extension Theorem)**.** *Suppose $\sigma : F \to F'$ is an isomorphism. Then if E is an extension field of F, then $\exists \tau : E \to E'$ such that $\forall a \in F, \tau(a) = \sigma(a)$.*

To continue the previous example (defining $\tau_2 : \sqrt{7} \to \sqrt{7}, \sqrt{11} \to -\sqrt{11}$ and $\tau_3 : \sqrt{7} \to -\sqrt{7}, \sqrt{11} \to -\sqrt{11}$), τ_2 and τ_3 can also be seen as extensions of $\sigma_2 : \sqrt{11} \to -\sqrt{11}$. Looking from $\mathbb{Q}(\sqrt{7}, \sqrt{11})$ over $\mathbb{Q}$, all of these isomorphisms are actually automorphisms, each an extension of the identity.

Theorem 5.10. *The number of extensions of σ from F to F depends only on E and F; not on σ.*

Definition 5.11. We can denote the **index of E over F** as $\{E : F\}$, the number of isomorphisms from E to E' leaving all F fixed, or equivalently, the number of extensions of $\sigma : F \to F'$ bringing E to E'.

Theorem 5.12. *Let $F \leq E \leq K$. Then $\{K : F\} = \{K : E\}\{E : F\}$.*

Finally, one of the last concepts we'll need is being able to say for certain where (in what field) the roots of a polynomial are, and whether or not any roots are repeated.

Definition 5.13. We say that E is a **splitting field** of $p(x)$ over F if and only if E is the smallest field containing F and all the roots of $p(x)$. Furthermore, if E is a splitting field of F, then every irreducible polynomial $p(x) \in F[x]$ splits in E (so all of its roots are in E).

Theorem 5.14. *If E is a splitting field of finite degree over F, then $\{E : F\} = |G(E/F)|$.*

Definition 5.15. Let $F \leq E$. Then E is **separable** over F if and only if $[E : F] = \{E : F\}$.

Theorem 5.16. *K is separable over F if and only if K is separable over E and E is separable over F. Additionally, an irreducible polynomial $p(x)$ is separable over F if and only if it has no repeated roots.*

Now with the following definition, we can establish the main theorem in Galois theory.

Definition 5.17. K is a **normal extension** of F if and only if K is a separable splitting field over F.

Theorem 5.18 (Main Theorem of Galois Theory)**.** *Let K be a finite, normal extension field of F with Galois group $G(K/F)$ (in class, our condition was K is a splitting field of F). Then for a field E with $F \leq E \leq K$, let $\lambda(E)$ be the subgroup of $G(K/F)$ leaving E fixed. Then:*

1. $\lambda(E) = G(K/E)$
2. $[K : E] = |\lambda(E)| = \{K : E\}$
3. *E is a normal subgroup of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. When this is true, $G(E/F) \simeq G(K/F)G(K/E)$*
4. *The tower of fields for a field extension and the group diagram for the Galois groups are similar, but flipped.*

Finally, we can address the problem of the insolvability of the quintic.

Definition 5.19. $p(x) \in \mathbb{Q}[x]$ is **solvable by radicals** if and only if $G(K/\mathbb{Q})$ is a solvable group where K is the splitting field of $p(x)$.

Definition 5.20. G is **solvable** if and only if we can construct a sequence of H_i such that $id \leq H_1 \leq \cdots \leq G$ where each H_i is normal in G and H_i/H_{i-1} is abelian.

Theorem 5.21. *There exists a polynomial $p(x) \in \mathbb{Q}[x]$ with $\deg(p(x)) = 5$ such that $G(K/\mathbb{Q}) \simeq S_5$, which is not solvable by radicals.*