1. Polynomial Rings

Recall that a **polynomial ring** in x over a field F, denoted $F[x]$, is the set of all finite polynomials $a_0 + a_1x + ... + a_nx^n$, where $a_0, ..., a_n$, also known as the coefficients of the polynomial, are in F. Let the **degree** of a polynomial be the highest power x^n with a nonzero coefficient. We see that this is a commutative ring with unit. In fact, $F[x]$ is a principal ideal domain: that is, if I is an ideal of $F[x]$, I can be generated by some element $a \in I$.

Define a polynomial $p(x)$ to be **irreducible** if it cannot be expressed as $p(x) = a(x)b(x)$ for non-unit polynomials $a(x)$ and $b(x)$. Then we see that $F[x]$ is also a **unique factorization domain**, or a domain where every nonzero element r can be written as a product of irreducibles $p_1...p_n$, unique up to a unit.

Theorem 1. *An ideal $((p(x))$ generated by a polynomial $p(x)$ is a maximal ideal if and only if $p(x)$ is irreducible in $F(x)$.*

This theorem is important because it tells us exactly what the maximal ideals of $F[x]$ are. If M is a maximal ideal of $F[x]$, $F[x]/M$ is a field. This field contains F (more precisely, it contains the field $\{a + M | a \in F\}$, which is isomorphic to F). This allows us to construct fields $F \subset K$, where K is called an **extension** of F. We would like to construct such fields K that allow a polynomial $p(x)$ to have **roots** in K.

Example 1. *$\mathbb{Q}(\sqrt{2})$ is an extension of the field $\mathbb{Q}$. The polynomial $x^2 + 2$ is irreducible in $\mathbb{Q}$, but in $\mathbb{Q}(\sqrt{2})$, it has the roots $\sqrt{2}$ and $-\sqrt{2}$.*

2. Field Extensions

Let $F \subset K$ be two fields. We call K an **extension** of F, and F a **subfield** of K. Note that K is in fact a vector space over F, because it satisfies the laws for addition and scalar multiplication. Because of this, $\dim_F(K)$ is well-defined. If $\dim_F(K)$ is finite, K is a **finite extension** of F, We will write $\dim_F(K)$ as $[K : F]$, called the **degree** of K over F.

Theorem 2. *Let $L \supset K \supset F$ be three fields such that both $[L : K]$ and $[K : F]$ are finite. Then L is a finite extension of F, and $[L : F] = [L : K][K : F]$.*

Now suppose K is a finite extension of F with degree n. Let $u \in K$. Then the elements $1, u, ..., u^n$ must be linearly dependent over F. This means that we can find $a_0, ..., a_n \in F$, not all zero, so that $a_0 + a_1u + ...a_nu^n = 0$.

Elements of a field extension satisfying this property are called **algebraic**, and if all elements of K are algebraic, we say that K is an **algebraic extension** of F. We have just seen that all finite extensions must be algebraic.

Note: The converse is not true. Can you find an example?

Example 2. *Consider $\mathbb{C} \supset \mathbb{Q}$. This is an infinite-dimensional extension. Numbers such as $\frac{1}{2}$, $1 + i$, $\sqrt{1 + \sqrt[3]{1 + \sqrt{2}}}$ are all algebraic over $\mathbb{Q}$. On the other hand, e and π are not algebraic; they are **transcendental**.*

If $a \in K$ is algebraic, let $p(x) \in F[x]$ be the monic polynomial of smallest degree such that $p(a) = 0$. We call $p(x)$ the **minimal polynomial** of a. Note that $p(x)$ is uniquely defined, as well as irreducible.

Theorem 3. *If a is algebraic and has a minimal polynomial of degree n, then $[F(a):F]=n$.*

If $p(x)$ is an irreducible polynomial in $F[x]$, then $M=((p(x))$ is a maximal ideal of $F[x]$. This means that $K=F[x]/M$ is a field that we can consider to be an extension of F. We note that $x+M$ is an element of K, and from calculations, we can see that this is in fact a root of $p(x)$. In fact, we claim that $[K:F]$ is actually a finite extension.

Exercise 1. *$[K:F]=n$, where n is the degree of $p(x)$.*

If $p(x)$ is a polynomial in $F[x]$, we say that $p(x)$ **splits** over K if $p(x)$ has a factorization into linear factors over $K[x]$. From the previous paragraph, we deduce that for every polynomial $p(x)$ in $F[x]$, there is some extension $K\supset F$, of degree at most $n!$, for which $p(x)$ splits over K. We call a minimal such extension a **splitting field** of $p(x)$ over F; this is unique up to isomorphism. A splitting field of a collection of polynomials may be called a **normal extension**; the reasoning behind this terminology should become more clear in the next section.

Example 3. *The splitting field for $(x^2-2)(x^2-3)$ is $\mathbb{Q}(\sqrt{2},\sqrt{3})$, a field of degree 4 over $\mathbb{Q}$.*

Example 4. *The splitting field of x^3-2 is* ***not*** *$\mathbb{Q}(\sqrt[3]{2})$, because the other roots of the polynomial, such as $\sqrt[3]{2}(\frac{-1+i\sqrt{3}}{2})$, are not in $\mathbb{Q}(\sqrt[3]{2})$. In fact, this splitting field is $\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})$, which has degree 6 over $\mathbb{Q}$.*

Example 5. *The splitting field of x^4+4 is $\mathbb{Q}(i)$, a field of degree 2 over $\mathbb{Q}$. Note that x^4+4 factors as $(x^2-2x+2)(x^2+2x+2)$.*

One may frequently draw diagrams for these fields, ordered by inclusion, to help visualize their relationships.

3. Galois Theory

Define a polynomial $f(x)$ over a field F to be **separable** if all of its roots are distinct (in a splitting field). Note that a polynomial has a multiple root if and only if the polynomial and its derivative are not relatively prime.

Exercise 2. *Deduce that an irreducible polynomial must be separable.*

Define a field K to be **separable** over F if every element of K is the root of a separable polynomial over F (note that it suffices to show that every minimal polynomial is separable).

Definition 1. *Let $K\supset F$ be a field extension. Define $Aut(K/F)$ to be the set of automorphisms of K that keep all elements of F fixed.*

We easily see that $Aut(K/F)$ is a subgroup of $Aut(K)$, where the group operation is composition. Now, we claim that

Theorem 4. *Any permutation σ in $Aut(K/F)$ permutes the roots of irreducible polynomials.*

Example 6. *In $K=\mathbb{Q}(\sqrt{2})$, the two automorphisms of $Aut(K/\mathbb{Q})$ are the identity map and the map $\sigma(a+b\sqrt{2})=a-b\sqrt{2}$.*

Example 7. *In $K = \mathbb{Q}(\sqrt[3]{2})$, we have $Aut(K/\mathbb{Q})$ is the trivial group, because any such automorphism must fix $\sqrt[3]{2}$ since the other two roots of $x^3 - 2 = 0$ are not in the field extension.*

Now, let $H \leq Aut(K)$ be a subgroup of $Aut(K)$. Then the collection L of elements of K fixed by all member of H is a subfield of K, and is called the **fixed field** of H. We note that this relation is **inclusion-reversing**; that is,

Theorem 5. *1) If $F_1 \subseteq F_2 \subseteq K$, then $Aut(K/F_2) \leq Aut(K/F_1)$.*
2) If $H_1 \leq H_2 \leq Aut(K)$ with fixed fields F_1 and F_2 respectively, then $F_2 \subseteq F_1$.

Let K/F be a finite extension. We say that K is **Galois** over F if $|Aut(K/F)| = [K : F]$, and we denote $Aut(K/F)$ by $Gal(K/F)$. We may show that this condition is equivalent to saying to K is the splitting field over F of some separable polynomial.

To show our final result, we will look at the duality of subgroups of the Galois group and the diagram of their corresponding fixed fields. For each of the examples we have given so far, we see that the diagrams of inclusion have a strong similarity, provided that one of them is flipped.

The Fundamental Theorem of Galois Theory states that this is not a coincidence - in fact, it holds for every Galois extension. We first have that

Theorem 6. *If G is a subgroup of $Aut(K)$ and F is its fixed field, then $[K : F] = |G|$.*

Thus, $|Aut(K/F)| \leq [K : F]$, and equality holds if and only if F is the fixed field of $Aut(K/F)$. Conversely, if G is a finite subgroup of $Aut(K)$ with fixed field F, then $Aut(K/F) = G$.

From this, we obtain the Fundamental Theorem of Galois Theory:

Theorem 7. *Let K/F be a Galois extension, and let $G = Gal(K/F)$. There is a natural bijection between subfields $E \supset F$ of K and subgroups H of G, given by $E \to \{\text{elements fixing } E\}$ and $H \to \{\text{fixed field of } H\}$.*

Essentially, this gives us that lattice of subfields of K containing F and the lattice of subgroups of G are dual posets.