A Special Note: Galois Theory involves the study of arbitrary fields and fields can come in many different guises. However, throughout these notes we shall restrict ourselves to fields whose elements are complex numbers. That is, all of our fields $F$ (even when we forget to mention it!) will have $F \subset C$.

Galois Basics

**Definition 1** Let $F \subset K, K'$, all fields. We say $\sigma : K \to K'$ is an isomorphism over $F$ if

1. $\sigma$ is a bijection from $K$ to $K'$
2. $\sigma(a + b) = \sigma(a) + \sigma(b)$ for all $a, b \in K$
3. $\sigma(ab) = \sigma(a)\sigma(b)$ for all $a, b \in K$
4. $\sigma(c) = c$ for all $c \in F$

We say that the elements of $F$ are fixed by $\sigma$. Note, however, that it is acceptable that other elements (not in $F$) are also fixed by $\sigma$.

The most important case is when $K = K'$.

**Definition 2** Let $F \subset K$, both fields. We say $\sigma : K \to K$ is an automorphism of $K$ over $F$ if

1. $\sigma$ is a bijection from $K$ to itself
2. $\sigma(a + b) = \sigma(a) + \sigma(b)$ for all $a, b \in K$
3. $\sigma(ab) = \sigma(a)\sigma(b)$ for all $a, b \in K$
4. $\sigma(c) = c$ for all $c \in F$

Now we come to the object of study.

**Definition 3** Let $F \subset K$, both fields. We define the Galois Group of $K$ over $F$, denote $\Gamma(K : F)$ as follows. The elements are all of the automorphisms of $K$ over $F$. The group operation is concatenation. That is, given two automorphisms $\sigma, \tau$ we define their product $\sigma \tau$ by

$$(\sigma \tau)(a) = \tau(\sigma(a))$$  \hspace{1cm} (1)

We define the inverse $\sigma^{-1}$ by

$$(\sigma^{-1})(b) \text{ is that a such that } \sigma(a) = b$$  \hspace{1cm} (2)
Exercise: Show that \( \sigma \tau \in \Gamma(K : F) \). That is, given that \( \sigma, \tau \) satisfy the four properties above show that \( \sigma \tau \) also satisfies the four properties above.

Exercise: Show that \( \sigma^{-1} \in \Gamma(K : F) \). That is, given that \( \sigma \) satisfies the four properties above show that \( \sigma^{-1} \) also satisfies the four properties above.

Example: Consider \( \Gamma(C : \text{Re}) \), the automorphisms of the complex numbers \( C \) over the real numbers \( \text{Re} \). We claim that complex conjugation, defined by (for \( a, b \) real)

\[
\sigma(a + bi) = a - bi \tag{3}
\]
satisfies the four properties above. For example, the third property states that, setting

\[
(a + bi)(c + di) = e + fi
\]
one has

\[
(a - bi)(c - di) = e - fi \tag{4}
\]

Exercise: Check that \( \sigma \), as defined by (3) satisfies all four properties.

There is another element of \( \Gamma(C : \text{Re}) \). The identity! The map \( e : K \to K \) given by \( e(\alpha) = \alpha \) for all \( \alpha \in K \) is always an element of \( \Gamma(K : F) \).

**Theorem 0.1** The only elements of \( \Gamma(C : \text{Re}) \) are complex conjugation \( \sigma \) and the identity \( e \).

**Proof:** Let \( \tau \in \Gamma(C : \text{Re}) \) and consider \( \tau(i) \). As \( i^2 + 1 = 0 \)

\[
0 = \tau(0) = \tau(i^2 + 1) = \tau(i)^2 + 1 \tag{5}
\]

That is, denoting \( \tau(i) \) by \( z \), \( z \) must satisfy \( z^2 + 1 = 0 \). There are only two possibilities for \( z \), either \( z = i \) or \( z = -i \). Further, the value of \( z = \tau(i) \) determines the entire map \( \tau \). This is because any complex number \( \alpha \) can be written \( \alpha = a + bi \) with \( a, b \) real and so

\[
\tau(\alpha) = \tau(a) + \tau(b)\tau(i) = a + bz \tag{6}
\]
as \( \tau \) fixes all real numbers. When \( z = i \) we have \( \tau(\alpha) = \alpha \) so that \( \tau \) is the identity. When \( z = -i \) we have \( \tau(a + bi) = a - bi \) and so \( \tau \) is complex conjugation \( \sigma \).

We therefore have \( \Gamma(C : \text{Re}) = \{ e, \sigma \} \). The identity acts as the identity of the group and

\[
\sigma^2(a + bi) = \sigma(\sigma(a + bi)) = \sigma(a - bi) = a + bi \tag{7}
\]
so that \( \sigma^2 = e \). We have a group on two elements. We can further write

\[
\Gamma(C : \text{Re}) \cong (\mathbb{Z}_2, +) \tag{8}
\]
by mapping \( e \) to 0 and \( \sigma \) to 1.

**Caution:** An expression such as \( \sigma^3(\alpha) \) does not mean the cube of \( \sigma(\alpha) \) but rather the result of applying \( \sigma \) three times to \( \alpha \), in this case, \( \sigma(\sigma(\sigma(\alpha))) \).

To say, for example, that \( \sigma^3 = e \), would be to say that \( \sigma(\sigma(\sigma(\alpha))) = \alpha \) for all \( \alpha \).

The proof ideas in Theorem 0.1 can be greatly generalized.
Theorem 0.2 Let $F \subset K, K'$, all fields. Let $\sigma : K \rightarrow K'$ be an isomorphism over $F$ as given by Definition 1. Let $\alpha \in K$ and let $\alpha$ be a root of some $p(x) \in F[x]$. That is, we may write

$$p(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x]$$

with the coefficients in $F$. Set $\beta = \sigma(\alpha)$ Then $\beta$ is a root of $p(x)$.

Proof: As

$$0 = p(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

we apply $\sigma$ to both sides and (noting, critically, that as $a_i \in F$, $\sigma(a_i\alpha^i) = \sigma(a_i)\sigma(\alpha)^i = a_i\beta^i$)

$$0 = \sigma(0) = a_0 + a_1\beta + \ldots + a_n\beta^n$$

as desired.

Theorem 0.3 Let $F \subset K, K'$, all fields. Assume $K = F(\alpha_1, \ldots, \alpha_s)$. Let $\sigma : K \rightarrow K'$ be an isomorphism over $F$ as given by Definition 1. Then $\sigma$ is determined by the values of $\sigma(\alpha_1), \ldots, \sigma(\alpha_s)$.

Proof: For any monomial $\kappa = c\alpha_1^{m_1} \cdots \alpha_s^{m_s}$ with $c \in F$, the value of $\sigma(\kappa)$ is determined by

$$\sigma(\kappa) = c\sigma(\alpha_1)^{m_1} \cdots \sigma(\alpha_s)^{m_s}$$

Any polynomial $\lambda$ in $\alpha_1, \ldots, \alpha_s$ is the sum of monomials and hence $\sigma(\lambda)$ is determined. When $K$ is an extension of $F$ of finite dimension (which is pretty much all we look at) every $\lambda \in K$ is such a polynomial and so $\sigma$ is determined on $K$. But even in the general case every $\lambda \in K$ can be written as the quotient $\lambda = \lambda_1/\lambda_2$ of polynomials and hence $\sigma(\lambda) = \sigma(\lambda_1)/\sigma(\lambda_2)$ is still determined.

Here is a powerful consequence.

Theorem 0.4 Let $F \subset K$, both fields, and assume only that $[K : F]$ is finite. Then the Galois Group $\Gamma[K : F]$ (as given by Definition 3) is finite.

Proof: Suppose $n = [K : F]$. Write $K = F(\alpha_1, \ldots, \alpha_s)$ for some $\alpha_1, \ldots, \alpha_s$.

(While it might not be the most efficient, one way to do this is to take a basis $\alpha_1, \ldots, \alpha_n$ for $K$ over $F$.) Let $\sigma \in \Gamma[K : F]$ and set $\beta_i = \sigma(\alpha_i)$ for each $i$. Each $\alpha_i$ satisfies some polynomial $p_i(x) \in F[x]$ of degree at most $n$. From theorem 0.2, $\beta_i$ satisfies the same polynomial. But we know that a polynomial of degree at most $n$ can have at most $n$ roots so there are at most $n$ choices for $\beta_i$. These choices, from Theorem 0.3, determine $\sigma$ on all of $K$.

A Cautionary Note: Suppose that in Theorem 0.4 we have $K = F(\alpha_1, \ldots, \alpha_s)$. Each $\sigma(\alpha_i)$ must be one of a finite number of choices. However, not all choices necessarily give a good $\sigma$. For example, suppose we wrote $K = Q(\sqrt{2}, \sqrt{3}, \sqrt{6})$. For $\sigma \in \Gamma[K : Q]$ we must have $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$, $\sigma(\sqrt{6}) = \pm\sqrt{6}$. But we don’t get all eight choices. If, say, $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = +\sqrt{3}$, then we must have (as $\sigma$ sends products to products) $\sigma(\sqrt{6}) = -\sqrt{6}$.

Now we can give a wide class of examples for which the Galois Group is determined.
**Theorem 0.5** Let $F \subset K$, both fields, and assume that $K = F(\alpha)$. Let $p(x) \in F[x]$ be the minimal polynomial for $\alpha$. Suppose further that $\beta \in K$ is also a root of $p(x)$. Then there is an automorphism $\sigma$ of $K$ over $F$ with $\sigma(\alpha) = \beta$.

**Proof**: Set $n$ to be the degree of $p(x)$. Then

\[ K = \{a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1} : a_0, \ldots, a_{n-1} \in F\} \]

As $p(x)$ is a minimal polynomial for $\alpha$ it must be irreducible (over $F$) and hence it must be a minimal polynomial for $\beta$ as well. Thus $[F(\beta) : F] = n$. But as $\beta \in F(\alpha)$, $F(\beta) \subseteq F(\alpha)$. As the dimensions over $F$ are the same we deduce that $F(\beta) = K$. Thus we can write

\[ K = \{a_0 + a_1 \beta + \ldots + a_{n-1} \beta^{n-1} : a_0, \ldots, a_{n-1} \in F\} \]

We define $\sigma$ by

\[ \sigma(a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1}) = a_0 + a_1 \beta + \ldots + a_{n-1} \beta^{n-1} \]

The key point is that products are sent to products. Write $p(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$. In multiplying elements of the form $a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1}$ we use the reduction $\alpha^n = -b_{n-1} \alpha^{n-1} - \ldots - b_0$. As $\beta$ has the same minimal polynomial in multiplying elements of the form $a_0 + a_1 \beta + \ldots + a_{n-1} \beta^{n-1}$ we use the same reduction $\beta^n = -b_{n-1} \beta^{n-1} - \ldots - b_0$.

**Theorem 0.6** Let $F \subset K$, both fields, and assume that $K = F(\alpha)$. Let $p(x) \in F[x]$ be the minimal polynomial for $\alpha$. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s$ be all the roots of $p(x)$ Then the Galois Group $\Gamma[K : F]$ (as given by Definition 3) will have precisely $s$ elements $\sigma_1 = e, \sigma_2, \ldots, \sigma_s$.

**Proof**: As $K = F(\alpha)$, $\sigma$ is determined (Theorem 0.3) by $\sigma(\alpha)$ which must be (Theorem 0.2) one of $\alpha_1, \ldots, \alpha_s$. From Theorem 0.5 each of these give a valid $\sigma_i \in \Gamma[K : F]$. 

4