ABSTRACT ALGEBRA II
AUTOMORPHISMS & GALOIS THEORY

MARIO L. GUTIERREZ ABED

Automorphisms of Fields

Definition. *Let E be an algebraic extension of a field F. Two elements $\alpha, \beta \in E$ are* **conjugate** *over F if* $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$*, that is, if α and β are zeroes of the same irreducible polynomial over F.* ★

Remark: The concept of conjugate elements just defined conforms with the classic idea of *conjugate complex numbers* if we understand that by conjugate complex numbers we mean numbers that are conjugate over $\mathbb{R}$. If $a, b \in \mathbb{R}$ and $b \neq 0$, then the conjugate complex numbers $a + bi$ and $a - bi$ are both zeroes of $x^2 - 2ax + a^2 + b^2$, which is irreducible in $\mathbb{R}[x]$.

Theorem (The Conjugation Isomorphisms). *Let F be a field, and let α and β be algebraic over F with* $\deg(\alpha, F) = n$*. Then the map $\psi_{\alpha,\beta}\colon F(\alpha) \to F(\beta)$ defined by*

$$\psi_{\alpha,\beta}(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1} \quad \text{for } c_i \in F$$

is an isomorphism of $F(\alpha)$ onto $F(\beta)$ if and only if α and β are conjugate over F.

Proof. See page $416 - 417$, *Fraleigh's*. □

Corollary 1. *Let α be algebraic over a field F. Every isomorphism ψ mapping $F(\alpha)$ onto a subfield of $\bar{F}$ such that $\psi(a) = a$ for $a \in F$ maps α onto a conjugate β of α over F. Conversely, for each conjugate β of α over F, there exists exactly one isomorphism $\psi_{\alpha,\beta}$ of $F(\alpha)$ onto a subfield of $\bar{F}$ mapping α onto β and mapping each $a \in F$ onto itself.*

Corollary 2. *Let $f(x) \in \mathbb{R}[x]$. If $f(a+bi) = 0$ for $(a+bi) \in \mathbb{C}$, where $a, b \in \mathbb{R}$, then $f(a-bi) = 0$ as well. (Loosely speaking, complex zeroes of polynomials with real coefficients occur in conjugate pairs.)*

Example 1: Consider $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. The zeroes of $\operatorname{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ are $\sqrt{2}$ and $-\sqrt{2}$; hence $\sqrt{2}$ and $-\sqrt{2}$ are conjugate over $\mathbb{Q}$. According to the above theorem, the map $\psi_{\sqrt{2},-\sqrt{2}}\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ defined by

$$\psi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$$

is an isomorphism of $\mathbb{Q}(\sqrt{2})$ onto itself. ▲

Remark: As illustrated in the preceding example, a field may have a nontrivial isomorphism onto itself. Such maps, known as **automorphisms**, will be of utmost importance in the work that follows.

Example: Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The map $\sigma\colon E \to E$ defined by

$$\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

for $a, b, c, d \in \mathbb{Q}$, is an automorphism of E; it is the conjugation isomorphism $\psi_{\sqrt{3},-\sqrt{3}}$ of E onto itself if we view E as $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$. We see that σ leaves $\mathbb{Q}(\sqrt{2})$ fixed. ▲

If $\{\sigma_i \mid i \in I\}$ is a collection of automorphisms of a field E, the elements of E about which $\{\sigma_i \mid i \in I\}$ gives the least information are those $a \in E$ left fixed by every σ_i for $i \in I$. The following theorem contains almost all that can be said about these fixed elements of E:

Theorem 1. *Let $\{\sigma_i \mid i \in I\}$ be a collection of automorphisms of a field E. Then the set*

$$E_{\{\sigma_i\}} = \{a \in E \mid \sigma_i(a) = a \ \ \forall\, i \in I\}$$

forms a subfield of E.

Proof. See page 419, *Fraleigh's*. □

Definition. *The field $E_{\{\sigma_i\}}$ defined on the preceding theorem is called the* ***fixed field*** *of $\{\sigma_i \mid i \in I\}$. (Obviously, for a single automorphism σ, we shall refer to $E_{\{\sigma\}}$ as the fixed field of σ.)* ★

Example: Consider the automorphism $\psi_{\sqrt{2},-\sqrt{2}}$ given on *Example 1* above. For $a, b \in \mathbb{Q}$, we have

$$\psi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2},$$

and $a + b\sqrt{2} = a - b\sqrt{2}$ if and only if $b = 0$. Thus the fixed field of $\psi_{\sqrt{2},-\sqrt{2}}$ is $\mathbb{Q}$. ▲

Remark: Note that an automorphism of a field E is in particular an injective mapping of E onto E, that is, a permutation of E. If σ and τ are automorphisms of E, then the permutation $\sigma\tau$ is again an automorphism of E, since, in general, compositions of homomorphisms again yield homomorphisms. This is how group theory comes into play on our present work:

Theorem 2. *The set of all automorphisms of a field E is a group under function composition. (This group is denoted as $\mathrm{Aut}(E)$.)*

Theorem 3. *Let E be a field and let F be a subfield of E. Then the set*

$$G(E/F) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma(a) = a \ \ \forall\, a \in F\}$$

forms a subgroup of $\mathrm{Aut}(E)$. Furthermore, $F \leq E_{G(E/F)}$, where

$$E_{G(E/F)} = \{a \in E \mid \sigma(a) = a \ \ \forall\, \sigma \in G(E/F)\}.$$

Remark 1: The group $G(E/F)$ is called the group of automorphisms of E leaving F fixed, or, more briefly, the ***group of** E **over** F*.

Remark 2: Do not think of E/F in the notation of $G(E/F)$ as denoting a quotient space of some sort, but rather as meaning that E is an extension field of the field F. This notation is unfortunately quite inconvenient but it's pretty standard. (so deal with it! ☺)

The ideas contained in theorems 1-3 above are illustrated in the following example. We urge you to study this example carefully:

Example 2: Consider the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. *Example 1* from our notes on *Extension Fields* shows that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$. If we view $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as $(\mathbb{Q}(\sqrt{3}))(\sqrt{2})$, then the conjugation isomorphism $\psi_{\sqrt{2},-\sqrt{2}}$ defined by

$$\psi_{\sqrt{2},-\sqrt{2}}(a+b\sqrt{2}) = a - b\sqrt{2}$$

for $a, b \in \mathbb{Q}(\sqrt{3})$ is an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ having $\mathbb{Q}(\sqrt{3})$ as a fixed field. Similarly, we have the automorphism $\psi_{\sqrt{3},-\sqrt{3}}$ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, having $\mathbb{Q}(\sqrt{2})$ as the fixed field.

Since the product of two automorphisms is itself an automorphism, we can consider $\psi_{\sqrt{2},-\sqrt{2}}\,\psi_{\sqrt{3},-\sqrt{3}}$, which moves both $\sqrt{2}$ and $\sqrt{3}$, that is, leaves neither number fixed.

Now let

$$\begin{aligned} \iota &= \text{The identity automorphism}, \\ \sigma_1 &= \psi_{\sqrt{2},-\sqrt{2}}, \\ \sigma_2 &= \psi_{\sqrt{3},-\sqrt{3}}, \\ \sigma_3 &= \psi_{\sqrt{2},-\sqrt{2}}\,\psi_{\sqrt{3},-\sqrt{-3}}. \end{aligned}$$

The group of all automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has a fixed field, by *Theorem 1*. This fixed field must contain $\mathbb{Q}$, since every automorphism of a field leaves 1 and hence the prime subfield fixed. A basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.
Since

$$\sigma_1(\sqrt{2}) = -\sqrt{2}, \qquad \sigma_1(\sqrt{6}) = -\sqrt{6}, \qquad \text{and} \qquad \sigma_2(\sqrt{3}) = -\sqrt{3},$$

we see that $\mathbb{Q}$ is exactly the fixed field of $G = \{\iota, \sigma_1, \sigma_2, \sigma_3\}$. It is readily checked that G is a group under automorphism multiplication (function composition). For instance, we have

$$\sigma_1\sigma_3 = \psi_{\sqrt{2},-\sqrt{2}}(\psi_{\sqrt{2},-\sqrt{2}}\,\psi_{\sqrt{3},-\sqrt{3}}) = \psi_{\sqrt{3},-\sqrt{3}} = \sigma_2.$$

The group table for G is given below:

	ι	σ_1	σ_2	σ_3
ι	ι	σ_1	σ_2	σ_3
σ_1	σ_1	ι	σ_3	σ_2
σ_2	σ_2	σ_3	ι	σ_1
σ_3	σ_3	σ_2	σ_1	ι

The group G is isomorphic to the Klein-4 group. We can show that G is the full group $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, because every automorphism τ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ maps $\sqrt{2}$ onto either $\pm\sqrt{2}$, by *Corollary 1*. Similarly, τ maps $\sqrt{3}$ onto either $\pm\sqrt{3}$. But since $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ leaving $\mathbb{Q}$ fixed is determined by its values on $\sqrt{2}$ and $\sqrt{3}$. Now ι, σ_1, σ_2, and σ_3 give all possible combinations of values on $\sqrt{2}$ and $\sqrt{3}$, and hence they are all possible automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Note that $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ has order 4, and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. This is no accident, but rather an instance of a general situation, as we shall see later. ▲

Theorem (The Frobenius Automorphism). *Let F be a finite field of characteristic p. Then the map $\sigma_p \colon F \to F$ defined by $\sigma_p(a) = a^p$ for $a \in F$ is an automorphism, known as the* ***Frobenius automorphism****, of F. Also, $F_{\{\sigma_p\}} \simeq \mathbb{Z}_p$.*

Remark: Freshmen in college sometimes make the error of saying that $(a+b)^n = a^n + b^n$. This theorem shows us that this *freshman's dream* $(a+b)^p = a^p + b^p$ is actually valid in a field F of characteristic p.

Definition. *Let E be a finite extension of a field F. Then the number of isomorphisms of E onto a subfield of $\bar{F}$ leaving F fixed is known as the* ***index*** *of E over F, denoted as $\{E : F\}$.* ★

Remark 1: A result that can be easily proven is that if $F \leq E \leq K$, where K is a finite extension field of the field F, then we have that $\{K : F\} = \{K : E\}\{E : F\}$.

Remark 2: Another result is that $\{F(\alpha) : F\} =$ the number of distinct zeroes of $\mathrm{irr}(\alpha, F)$.

Splitting Fields

Definition. *Let F be a field with algebraic closure $\bar{F}$. Let $\{f_i(x) \mid i \in I\}$ be a collection of polynomials in $F[x]$. Then a field $E \leq \bar{F}$ is said to be the* ***splitting field*** *of $\{f_i(x) \mid i \in I\}$ over F if E is the smallest subfield of $\bar{F}$ containing F and all zeroes in $\bar{F}$ of each of the $f_i(x)$. Generally we say that a field $K \leq \bar{F}$ is a* ***splitting field*** *over F if it is the splitting field of some set of polynomials in $F[x]$.* ★

A more concise definition of a splitting field (which will become more apparent once you read some of the results below) is given as follows:

Definition. *Let F be a field and $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a nonconstant polynomial in $F[x]$. Then an extension field E of F is said to be the* ***splitting field*** *of $p(x)$ if there exists elements $\alpha_1, \ldots, \alpha_n$ in E such that*

$$E = F(\alpha_1, \ldots, \alpha_n)$$

and

$$p(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n).$$

★

Example: We see that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field of $\{x^2 - 2, x^2 - 3\}$ and also of $\{x^4 - 5x^2 + 6\}$. ▲

Theorem. *A field E, where $F \leq E \leq \bar{F}$, is a splitting field over F if and only if every automorphism of $\bar{F}$ leaving F fixed maps E onto itself and thus induces an automorphism of E leaving F fixed.*

Proof. See page $432 - 433$, *Fraleigh's*. □

Definition. *Let E be an extension field of a field F. A polynomial $f(x) \in F[x]$* ***splits*** *in E if it factors into a product of linear factors in $E[x]$.* ★

Example: The polynomial $x^4 - 5x^2 + 6$ in $\mathbb{Q}[x]$ splits in the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ into $(x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$. ▲

Example: Let $p(x) = x^4 + 2x^2 - 8$ in $\mathbb{Q}[x]$. Then $p(x)$ has irreducible factors $x^2 - 2$ and $x^2 + 4$ in $\mathbb{Q}[x]$. Therefore, the field $\mathbb{Q}(\sqrt{2}, i)$ is the splitting field for $p(x)$:

$$\begin{aligned} p(x) &= (x^2 - 2)(x^2 + 4) \\ &= (x + \sqrt{2})(x - \sqrt{2})(x + 2i)(x - 2i). \end{aligned} \qquad ▲$$

Example: Let $p(x) = x^2 + 3$ in $\mathbb{Q}[x]$. Then $p(x)$ factors as $x^2 + 3 = (x - \sqrt{3}i)(x + \sqrt{3}i)$. Thus we have that $\mathbb{Q}(\sqrt{3}i)$ is the splitting field for $p(x)$ over $\mathbb{Q}$, which is of degree 2 over $\mathbb{Q}$, i.e. $[\mathbb{Q}(\sqrt{3}i) : \mathbb{Q}] = 2$. ▲

Example: Let $p(x) = x^4 - 1$ in $\mathbb{Q}[x]$. Then $p(x)$ factors as $x^4 - 1 = (x^2 + 1)(x^2 - 1) = (x - i)(x + i)(x - 1)(x + 1)$. Thus we have that $\mathbb{Q}(i)$ is the splitting field for $p(x)$ over $\mathbb{Q}$, which is of degree 2 over $\mathbb{Q}$, i.e. $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. ▲

Example: Let $p(x) = (x^2 - 2)(x^2 - 3)$ in $\mathbb{Q}[x]$. Then $p(x)$ factors as $(x^2 - 2)(x^2 - 3) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$. Thus we have that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field for $p(x)$ over $\mathbb{Q}$, which is of degree 4 over $\mathbb{Q}$, i.e.

$$\underbrace{[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]}_{4} = \underbrace{[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})]}_{2} \underbrace{[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]}_{2}.$$

▲

Corollary. *If $E \leq \bar{F}$ is a splitting field over F, then every irreducible polynomial in $F[x]$ having a zero in E splits in E.*

Corollary 3. *If $E \leq \bar{F}$ is a splitting field over F, then every isomorphic mapping of E onto a subfield of $\bar{F}$ leaving F fixed is actually an automorphism of E. In particular, if E is a splitting field of finite degree over F, then*

$$\{E : F\} = |G(E/F)|.$$

Example: Observe that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $\{x^2 - 2, x^2 - 3\}$ over $\mathbb{Q}$. On *Example 2* we showed that the mappings ι, σ_1, σ_2, and σ_3 are all automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ leaving $\mathbb{Q}$ fixed. (Actually, since every automorphism of a field must leave the prime subfield fixed, we see that these are the only automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.)
Then we have

$$\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\} = |G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = 4,$$

illustrating *Corollary 3*. ▲

Note: We wish to determine conditions under which

$$|G(E/F)| = \{E : F\} = [E : F]$$

for finite extensions E of F. We will show later on that this equation always holds when E is a splitting field over a field F of characteristic 0 or when F is a finite field. This equation however need not be true when F is an infinite field of characteristic $p \neq 0$.

<u>Example</u>: Consider the real cube root of 2, $\sqrt[3]{2}$. Now x^3-2 does not split in $\mathbb{Q}(\sqrt[3]{2})$, for $\mathbb{Q}(\sqrt[3]{2}) < \mathbb{R}$ and only one zero of x^3-2 is real. Thus x^3-2 factors in $(\mathbb{Q}(\sqrt[3]{2}))[x]$ into a linear factor of $x-\sqrt[3]{2}$ and an irreducible quadratic factor. The splitting field E of x^3-2 over $\mathbb{Q}$ is therefore of degree 2 over $\mathbb{Q}(\sqrt[3]{2})$. Then

$$[E:\mathbb{Q}] = [E:\mathbb{Q}(\sqrt[3]{2})]\,[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = (2)(3) = 6.$$

We have shown that the splitting field over $\mathbb{Q}$ of x^3-2 is of degree 6 over $\mathbb{Q}$.

We can verify by cubing that

$$\sqrt[3]{2}\frac{-1+i\sqrt{3}}{2} \qquad \text{and} \qquad \sqrt[3]{2}\frac{-1-i\sqrt{3}}{2}$$

are the other zeroes of x^3-2 in $\mathbb{C}$. Thus the splitting field E of x^3-2 over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. (Note that this is NOT the same field as $\mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$, which is of degree 12 over $\mathbb{Q}$.) ▲

Separable Extensions

Definition. *Let $f(x) \in F[x]$. An element $\alpha \in \bar{F}$ such that $f(\alpha) = 0$ is a zero of $f(x)$ of **multiplicity** ν if ν is the greatest integer such that $(x-\alpha)^\nu$ is a factor of $f(x)$ in $\bar{F}[x]$.* ★

Theorem. *Let $f(x)$ be irreducible in $F[x]$. Then all zeroes of $f(x)$ in $\bar{F}$ have the same multiplicity.*

Theorem. *If E is a finite extension of F, then $\{E:F\}$ divides $[E:F]$.*

Definition. *A finite extension E of F is said to be a **separable extension** of F if $\{E:F\} = [E:F]$. An element $\alpha \in \bar{F}$ is **separable** over F if $F(\alpha)$ is a separable extension of F. An irreducible polynomial $f(x) \in F[x]$ is **separable** over F if every zero of $f(x)$ in $\bar{F}$ is separable over F.* ★

Here's an alternate definition:

Definition. *Let F be a field. A polynomial $f(x) \in F[x]$ of degree n is said to be **separable** if it has n distinct roots in the splitting field of $f(x)$. That is, $f(x)$ is separable when it factors into distinct linear factors over the splitting field of $f(x)$. An extension E of F is said to be a **separable extension** of F if every element in E is a root of a separable polynomial in $F[x]$.* ★

<u>Example</u>: The field $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is separable over $\mathbb{Q}$ since, as we saw on a previous example, $\{E:\mathbb{Q}\} = 4 = [E:\mathbb{Q}]$. ▲

<u>Example</u>: The polynomial x^2-2 is separable over $\mathbb{Q}$, since it factors as $(x-\sqrt{2})(x+\sqrt{2})$. In fact, $\mathbb{Q}(\sqrt{2})$ is a separable extension of $\mathbb{Q}$:

Let $\alpha = a+b\sqrt{2}$ be an element of $\mathbb{Q}(\sqrt{2})$. If $b=0$, then α is a root of the separable polynomial

$$x^2 - 2ax + a^2 - 2b^2 = (x-(a+b\sqrt{2}))(x-(a-b\sqrt{2}))$$

▲

Fortunately, we have an easy way to determine separability of polynomials, as stated on the following theorem:

Theorem. *Let F be a field and $f(x) \in F[x]$. Then $f(x)$ is separable if and only if $f(x)$ and $f'(x)$ are relatively prime, i.e. if and only if* $\gcd(f(x), f'(x)) = 1$.

<u>*Note*</u>: We know that $\{F(\alpha) : F\}$ is the number of distinct zeroes of $\mathrm{irr}(\alpha, F)$. Also the multiplicity of α in $\mathrm{irr}(\alpha, F)$ is the same as the multiplicity of each conjugate of α over F. Thus, α is separable over F if and only if $\mathrm{irr}(\alpha, F)$ has all the zeroes of multiplicity 1. This tells us that an irreducible polynomial $f(x) \in F[x]$ is separable over F if and only if $f(x)$ has all zeroes of multiplicity 1.

Theorem. *If K is a finite extension of E and E is a finite extension of F, that is, if $F \leq E \leq K$, then K is separable over F if and only if K is separable over E and E is separable over F.*

Corollary. *If E is a finite extension of F, then E is separable over F if and only if each $\alpha \in E$ is separable over F.*

Definition. *A field is said to be* ***perfect*** *if every finite extension is a separable extension.* ★

Theorem. *Every field of characteristic* 0 *is perfect.*

Theorem. *Every finite field is perfect.*

Theorem (The Primitive Element Theorem). *Let E be a finite separable extension of a field F. Then there exists $\alpha \in E$ such that $E = F(\alpha)$.*[1] *That is, a finite separable extension of a field is a simple extension.*

Corollary. *A finite extension of a field of characteristic* 0 *is a simple extension.*

<u>*Remark*</u>: We see that the only "bad" case where a finite extension may not be simple is a finite extension of an infinite field of characteristic $p \neq 0$.

[1] Such an element α is known as a **primitive element**.

Galois Theory

We start by recalling the main results we have developed and should have well in mind:

1. Let $F \leq E \leq \bar{F}, \alpha \in E$, and let β be a conjugate of α over F, that is, $\mathrm{irr}(\alpha, F)$ has β as a zero also. Then there is an isomorphism $\psi_{\alpha,\beta}$ mapping $F(\alpha)$ onto $F(\beta)$ that leaves F fixed and maps α onto β.
2. If $F \leq E \leq \bar{F}$ and $\alpha \in E$, then an automorphism σ of $\bar{F}$ that leaves F fixed *must* map α onto some conjugate of α over F.
3. If $F \leq E$, the collection of all automorphisms of E leaving F fixed forms a group $G(E/F)$. For any subset S of $G(E/F)$, the set of all elements of E left fixed by all elements of S is a field E_S. Also, $F \leq E_{G(E/F)}$.
4. A field E, $F \leq E \leq \bar{F}$, is a splitting field over F if and only if every isomorphism of E onto a subfield of $\bar{F}$ leaving F fixed is an automorphism of E. If E is a finite extension and a splitting field over F, then $|G(E/F)| = \{E : F\}$.
5. If E is a finite extension of F, then $\{E : F\}$ divides $[E : F]$. If E is also separable over F, then $\{E : F\} = [E : F]$. Also, E is separable over F if and only if $\mathrm{irr}(\alpha, F)$ has all zeros of multiplicity 1 for every $\alpha \in E$.
6. If E is a finite extension of F and is a separable splitting field over F, then $|G(E/F)| = \{E : F\} = [E : F]$.

Definition. *A finite extension K of F is said to be a* ***finite normal extension*** *of F if K is a separable splitting field over F.* ★

Theorem. *Let K be a finite normal extension of F, and let E be an extension of F, where $F \leq E \leq K \leq \bar{F}$. Then K is a finite normal extension of E, and $G(K/E)$ is precisely the subgroup of $G(K/F)$ consisting of all those automorphisms that leave E fixed. Moreover, two automorphisms $\sigma, \tau \in G(K/F)$ induce the same isomorphism of E onto a subfield of $\bar{F}$ if and only if they are in the same left coset of $G(K/E)$ in $G(K/F)$.*

Definition. *If K is a finite normal extension of a field F, then $G(K/F)$ is called the* ***Galois group*** *of K over F.* ★

Theorem 4 (Main Theorem of Galois Theory). *Let K be a finite normal extension of a field F, with Galois group $G(K/F)$. For a field E, where $F \leq E \leq K$, let $\lambda(E)$ be the subgroup of $G(K/F)$ leaving E fixed. Then λ is a one-to-one map of the set of all such intermediate fields E onto the set of all subgroups of $G(K/F)$.*

The following properties hold for λ:

1) $\lambda(E) = G(K/E)$.
2) $E = K_{G(K/E)} = K_{\lambda(E)}$.
3) *For $H \leq G(K/F)$, we have $\lambda(E_H) = H$.*
4) $[K : E] = |\lambda(E)|$ *and* $[E : F] = (G(K/F) : \lambda(E))$, *the number of left cosets of $\lambda(E)$ in $G(K/F)$.*

5) *E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. When $\lambda(E)$ is a normal subgroup of $G(K/F)$, we have*

$$G(E/F) \simeq G(K/F)/G(K/E).$$

6) *The diagram of subgroups of $G(K/F)$ is the inverted diagram of intermediate fields of K over F.*