Field and Galois Theory

Swayam Chube

October 23, 2022

Abstract

I find myself struggling with Field Theory and especially Galois Theory. These are some notes that I took while attempting to overcome my inability to comprehend the same.

Contents

Part I

Review

Chapter 1

Rings

Definition 1.1. A ring $R = (R, +, \cdot)$ is a non-empty set R with two binary operations $+$ (called addition) and $\cdot$ (called multiplication) with the following properties:

1. $(R, +)$ is an Abelian group
2. $(R, \cdot)$ is a monoid
3. The multiplication operation distributes over addition, that is, $a \cdot (b + c) = a \cdot b + a \cdot c$

Commutative Rings are those in which multiplication is commutative. We denote the additive identity by 0.

Definition 1.2 (Integral Domain). A commutative ring with unity is called an *integral domain* if

$$ab = 0 \Longleftrightarrow a = 0 \text{ or } b = 0$$

That is, an integral domain does not have any zero divisors. Sometimes we call integral domains just *domains*.

Definition 1.3 (Unit). An invertible element of a ring with unity is said to be a unit. That is, $u \in R$ is a unit if there is $v \in R$ such that $uv = 1$.

The set of all units in a ring with unity forms a group, generally denoted by either R^* or $R^\times$.

Definition 1.4 (Ideal). A subring A of a ring R is said to be an *ideal* of R if for every $r \in R$ and every $a \in A$ both $ra, ar \in A$.

Lemma 1.5. Let $S = \{a_1, \ldots, a_n\}$ be a finite subset of a commutative ring R with unity. Then the set

$$I = \{r_1 a_1 + \cdots + r_n a_n \mid r_1, \ldots, r_n \in R\}$$

is the smallest ideal of R containing A.

Proof. Straightforward. ■

We define the ideal generated by S to be the smallest ideal in R containing S, denoted by $\langle S \rangle$. A principle ideal is of the form $\langle a \rangle$ for some $a \in R$.

Theorem 1.6. Let R be a ring and let A be a subring of R. The set of cosets $\{r + A \mid r \in R\}$ is a ring under the operations $(s + A) + (t + A) = (s + t) + A$ and $(s + A) \cdot (t + A) = st + A$ if and only if A is an ideal of R.

Proof. TODO: Add in later ■

Definition 1.7 (Prime Ideal, Maximal Ideal). A *prime ideal* A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$. A *maximal ideal* of a commutative ring R is a proper ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

Theorem 1.8. Let R be a commutative ring with unity and A be an ideal of R. Then R/A is an integral domain if and only if A is prime.

Proof. Suppose R/A is an integral domain. Indeed, we have

$$\begin{aligned} st \in A &\Rightarrow st + A = 0 \\ &\Rightarrow (s + A)(t + A) = 0 \\ &\Rightarrow s + A = 0 \vee t + A = 0 \\ &\Rightarrow s \in A \vee t \in A \end{aligned}$$

and thus A is prime.

Conversely, if A is prime, then

$$\begin{aligned}(s+A)(t+A)=0 &\Rightarrow st+A=0\\ &\Rightarrow st\in A\\ &\Rightarrow s\in A\vee t\in A\\ &\Rightarrow s+A=0\vee t+A=0\end{aligned}$$

and thus R/A is a domain. ■

Theorem 1.9. Let R be a commutative ring with unity and A be an ideal of R. Then R/A is a field if and only if A is maximal.

Proof. Suppose R/A is a field and B be an ideal of R containing A. Let $b\in B\backslash A$. By definition, there is $c\in R$ such that $bc+A=(b+A)(c+A)=1+A$, or equivalently, $1-bc\in A$. But since $bc\in B$, $1\in B$ implying that $B=R$. Therefore, A is maximal.

Conversely, suppose A is maximal. It suffices to show that for all $a\notin A$, $a+A$ has an inverse. This immediately implies that R/A is both a domain and a field. Let $a\notin A$. Then, consider the ideal generated by $\langle A,a\rangle$, which properly subsumes A and thus must be equal to R. As a result, $1\in\langle A,a\rangle$ and thus, $1-ra\in A$ for some $r\in R$, implying that $r+A$ is an inverse of $a+A$ in R/A. ■

Corollary. Every maximal ideal is a prime ideal.

Definition 1.10 (Ring Homomorphism). A *ring homomorphism* $\phi:R\to S$ is a mapping from R to S that preserves the two ring operations; that is, for all $a,b\in R$

$$\phi(a+b)=\phi(a)+\phi(b)\qquad\phi(ab)=\phi(a)\phi(b)$$

The *kernel* of a ring homomorphism is defined as

$$\ker\phi=\{r\in R\mid\phi(r)=0\}$$

Theorem 1.11. Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/\ker\phi$ to $\phi(R)$ given by $r + \ker\phi \mapsto \phi(r)$ is an isomorphism. Equivalently, $R/\ker\phi \cong \phi(R)$.

Proof. Obviously, if $a, b \in \ker\phi$, then $\phi(a-b) = \phi(a) - \phi(b) = 0$ and thus $\ker\phi$ is a subring. Further, for any $r \in R$, $\phi(rs) = \phi(r)\phi(s) = 0$ for all $s \in \ker\phi$, implying that $\ker\phi$ is an ideal.

Consider now the map $\psi : R/\ker\phi \to \phi(R)$, given by $r\ker\phi \mapsto \phi(r)$. The kernel of this homomorphism is obviously trivial and it is therefore injective. Thus, it is an isomorphism. ■

Definition 1.12 (Characteristic of a Ring). The *characteristic* of a ring R is the least positive integer n such that $nx = 0$ for all $x \in R$. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\mathrm{char}(R)$.

Lemma 1.13. The characteristic of a domain is 0 or prime.

Proof. Let $st = n = \mathrm{char}(R) > 0$. Then,

$$(s \cdot 1)(t \cdot 1) = (st) \cdot 1 = 0$$

implying $s = n$ or $t = n$ and thus n is prime. ■

It is important to note that finite characteristic does not imply that the ring is finite. Consider $\mathbb{Z}_p[x]$ for example.

Definition 1.14 (Principal Ideal Domain). A *principal ideal domain* is an integral domain R in which every ideal has the form $\langle a \rangle$.

Definition 1.15 (Polynomial Ring). Let R be a commutative ring. The set of formal symbols

$$R[x] = \{a_n x^n + \cdots + a_0 \mid a_i \in R,\ n \in \mathbb{N}_0\}$$

is called the *ring of polynomials* over R in the indeterminate x with addition and multiplication defined using obviousness.

Lemma 1.16. If R is an integral domain, then so is $R[x]$.

Proof. Straightforward. ■

Theorem 1.17 (Division Algorithm). Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$.

Proof. Existence is simple induction and uniqueness is another simple degree argument. ■

Corollary. Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$. Thus, if $f(a) = 0$, then $x - a$ is a factor of $f(x)$.

Theorem 1.18. Let F be a field. Then $F[x]$ is a principal ideal domain.

Proof. Let A be an ideal in $F[x]$ and $g(x) \in A$ be a polynomial of minimum degree. Then, $\langle g(x) \rangle \subseteq A$. Conversely, let $f(x) \in A$, then $f(x) = q(x)g(x) + r(x)$, implying that $r(x) = 0$ lest $\deg r < \deg g$, contradicting the minimality of $\deg g$. Thus, $A \subseteq \langle g(x) \rangle$ and we are done. ■

Theorem 1.19. Let F be a field and $0 \neq p(x) \in F[x]$ have degree $n \geq 0$. Then p has at most n zeros in F counting multiplicity.

Proof. The proof is by induction on n. For $n = 0$, the conclusion is trivial. Now suppose $n > 0$. If p has no roots in F then we are trivially done. Suppose $x = a$ is a root of p, then $p(x) = (x - a)q(x)$ due to the factor theorem, and we are done due to the induction hypothesis. ■

Definition 1.20 (Associates, Irreducibles, Primes). Elements a and b of an integral domain R are called associates if $a = ub$ for some unit $u \in R$. A nonzero element a of R is called an *irreducible* if a is not a unit and whenever $b, c \in R$ with $a = bc$ then b or c is a unit. A nonzero element a of R is called a *prime* if a is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Theorem 1.21. In an integral domain, every prime is irreducible.

Proof. Let R be an integral domain and $p \in R$ be a prime with $p = ab$. Then, $p \mid ab$ and thus $p \mid a$ or $p \mid b$. Without loss of generality, let $p \mid a$ and $a = pa'$, consequently, $a'b = 1$ implying that b is a unit. ■

Theorem 1.22. In a principal ideal domain, an element is prime if and only if it is irreducible.

Proof. Since a principal ideal domain is implicitly an integral domain, each prime is irreducible. Conversely, let $a \in R$ be irreducible and $a \mid bc$. Then, consider the ideal $\langle a, b\rangle$ which must be of the form $\langle d\rangle$ for some $d \in R$. Thus, there is $r \in R$ such that $a = dr$, consequently, one of d or r must be a unit. Suppose d is a unit. Then $\langle d\rangle = R$ and thus $1 = ax + by$, implying $c = cax + ay$, i.e. $a \mid c$. On the other hand, if r is a unit, then $\langle a\rangle = \langle d\rangle$, and thus $b \in \langle d\rangle = \langle a\rangle$ i.e. $a \mid b$. This completes the proof. ■

Definition 1.23 (Unique Factorization Domain). An integral domain D is a unique factorization domain if

1. every nonzero element of R that is not a unit can be written as a product of irreducibles of R
2. the factorization into irreducibles is unique up to associates and the order in which the factors appear.

Lemma 1.24. In a principal ideal domain, any strictly increasing chain of ideals $I_1 \subsetneq I_2 \subsetneq \cdots$ must be finite in length.

Proof. Let $I = \bigcup_{i=1}^{\infty} I_i$. Obviously I is an ideal of R. As a result, there is $a \in R$ such that $I = \langle a \rangle$. Let $k = \arg\min_{i \in \mathbb{N}} a \in I_i$. Then, it is obvious that $I_{k+1} = I_k$. This finishes the proof. ■

Theorem 1.25. Every principal ideal domain is a unique factorization domain.

Proof. Let R be a principal ideal domain. First, we shall establish that every non-unit in R has at least one irreducible factor. Let $a_0 \in R$ be a non-unit. If a_0 is irreducible, we are done. If not, then we may write $a_0 = b_1 a_1$ where neither b_1 nor a_1 is a unit. If a_1 is irreducible, we are done, if not, then repeat. We now have an ascending chain of ideals $\langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \cdots$ and therefore must terminate. As a result, there is some k such that a_k is irreducible. This gives the desired conclusion.

Using a similar chain argument, one can show that every element can be written as a product of irreducibles. It remains to show uniqueness up to associates. This part of the proof proceeds by induction on r, the number of primes in the factorization of the element. For irreducibles, $r = 1$, since each irreducible is a prime in a PID, thus the base case is trivial. Suppose $r > 1$ and

$$a = p_1 \dots p_r = q_1 \dots q_s$$

Since $p_1 \mid q_1 \dots q_s$, it must divide one of the q_i's. Without loss of generality, suppose $p_1 \mid q_1$. Then there is a unit u such that $q_1 = up_1$. We are now left with $p_2 \dots p_r = uq_2 \dots q_s$, and applying the induction hypothesis, we are done. ■

Corollary. Let F be a field. Then $F[x]$ is a unique factorization domain.

Note that a field is trivially a UFD since every element is a unit.

TODO: Place this

Lemma 1.26. Let R be a commutative ring with unity and $I \subseteq R$ be an ideal (in this case it is implicitly two sided). Then there is a maximal ideal $\mathfrak{m}$ containing I that is proper in R.

Proof. Define the poset $(P, \subseteq)$ where

$$P = \{A \mid I \subseteq A \subsetneq R,\ A \text{ is an ideal}\}$$

Let C be any chain in P and define $U_C = \bigcup_{c \in C} c$. By construction, one can show that U_C is an ideal in R and must contain I. To see that U_C is proper, simply note that $1 \notin c$ for all $c \in C$ and thus $1 \notin U_C$. Further, for all $c \in C$, $c \subseteq U_C$. We have shown that each chain has a maximal element, in this case U_C and therefore due to Zorn's Lemma, there is $\mathfrak{m} \in P$ that is maximal and it is obvious that $\mathfrak{m}$ is a maximal ideal. ■

Note that it is known that the above lemma is **equivalent** to the Axiom of Choice.

Chapter 2

Fields

Definition 2.1 (Field). A *field* is an integral domain where every non-zero element is a unit.

Definition 2.2 (Prime Subfield). The *prime subfield* of a field F is the subfield of F generated by the multiplicative identity 1_F of F. It is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

Definition 2.3 (Extension Field). A field E is an *extension field* of a field F if there is a monomorphism of fields $\phi : F \hookrightarrow E$.

Theorem 2.4 (Fundamental Theorem of Field Theory). Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there is an extension field E of F in which f has a zero.

Proof. Consider the field $E = F[x]/\langle p(x)\rangle$ with the monomorphism $\phi : F \hookrightarrow F[x]/\langle p(x)\rangle$ given by $\phi(a) = a$. One immediately notes that $p(x + \langle p(x)\rangle) = 0$. ■

While we are at it, note the following lemma

Lemma 2.5. Let F and F' be fields, then the homomorphism of fields $\phi : F \to F'$ is either trivial or a monomorphism.

Proof. F has no proper ideals. ■

Definition 2.6 (Degree of an Extension). Let L be an extension field of a field K. Then, there is a basis of L over K. The size of this basis is the *degree* of the extension. The degree may be infinite.

Theorem 2.7. Let $L : K$ and $M : L$ be field extensions. Then,

$$[M : L][L : K] = [M : K]$$

Proof. TODO: Add in later ■

Definition 2.8. Suppose L is a field and K is a subfield. Let $S \subseteq L$. Then, we denote by $K(S)$, the **subfield of L generated over K by S**. If $S = \{a_1, \ldots, a_n\}$ is finite, then we denote this field by $K(a_1, \ldots, a_n)$.

Theorem 2.9. Let L be a field, let K be a subfield and let $\alpha \in L$. Then either:

1. $K(\alpha)$ is isomorphic to $K(x)$, the field of all rational forms with coefficients in K; or

2. there exists a unique monic irreducible polynomial $m \in K[x]$ such that

   (a) for all $f \in K[x]$, $f(\alpha) = 0$ if and only if $m \mid f$

   (b) the field $K(\alpha)$ coincides with $K[\alpha]$, the ring of all polynomials in α with coefficients in K; and

   (c) $[K[\alpha] : K] = \partial m$

Proof. Suppose there is no non-zero polynomial f in $K[x]$ such that $f(\alpha) = 0$. Then, consider the function $\psi : K(x) \to K(\alpha)$ given by $\psi(f/g) = f(\alpha)/g(\alpha)$. One notes that the denominator must always be non-zero. This mapping is indeed well defined,

$$\begin{aligned}\psi(f/g) = \psi(p/q) &\Leftrightarrow f(\alpha)q(\alpha) - p(\alpha)g(\alpha) \in L \\ &\Leftrightarrow fq - pg = 0 \\ &\Leftrightarrow f/g = p/q\end{aligned}$$

The fact that ψ is a homomorphism is just a routine computation. It is also surjective and therefore must be an isomorphism. (Recall that a homomorphism between fields must be trivial or a monomorphism).

Now suppose there is a non-zero polynomial g of minimum degree such that $g(\alpha) = 0$. Let $m = g/a$ where a is the leading coefficient of g. Let $f \in K[x]$ such that $f(\alpha) = 0$. Then, $f(x) = q(x)m(x) + r(x)$ with $r = 0$ or $\deg r < \deg m$. Therefore, $r = 0$, lest $r(\alpha) = 0$ with $\deg r < \deg m$, a contradiction to the minimality of $\deg m$. Uniqueness and irreducibility are both obvious due to similar minimality arguments.

Now consider $f(\alpha)/g(\alpha) \in K(\alpha)$, where $g(\alpha) \neq 0$ and $\gcd(f(x), g(x)) \in K^\times$. Then there exist polynomials $a, b \in K[x]$ such that $ag + bm = 1$ and thus $a(\alpha)g(\alpha) = 1$. Consequently, $f(\alpha)/g(\alpha) = a(\alpha)f(\alpha) \in K[\alpha]$.

Finally, note that $\{1, \alpha, \dots, \alpha^{\deg m - 1}\}$ is a linearly independent set and spans $K[\alpha]$. This finishes the proof. ■

2.1 Algebraic Extensions

Definition 2.10 (Algebraic). If α has a minimal polynomial over$K$, we say that α is *algebraic* over K and that $K[\alpha] = K(\alpha)$ is a *simple* algebraic extension of K. Otherwise α is said to be *transcendental* over K.

Theorem 2.11. Let $K(\alpha)$ be a simple transcendental extension of a field K. Then the degree of $K(\alpha)$ over K is infinite.

Definition 2.12 (Algebraic Extension). An extension L of K is said to be an *algebraic extension* if every element of L is algebraic over K. Otherwise L is a *transcendental extension*.

Lemma 2.13. Every finite extension is algebraic.

Proof. Let L be a finite extension of K, with $[L : K] = n$. Then $\{1, \alpha, \dots, \alpha^n\}$ is linearly dependent. ■

One notes that the converse is not necessarily true. For example, $\mathbb{C}$ is an infinite algebraic extension of $\mathbb{R}$.

Corollary. Let $L : K$ and $M : L$ be field extensions and let $\alpha \in M$. If α is algebraic over K then it is also algebraic over L.

Theorem 2.14. Let L be a field, K be a subfield, and let $\alpha \in L$ be algebraic over K with minimal polynomial $m \in K[x]$. Then, $K(\alpha) = K[\alpha] \cong K[x]/\langle m(x)\rangle$.

Recall from the Fundamental Theorem of Field Theory that any irreducible polynomial in a field has a root in an extension field. This gives rise to the following theorem:

Theorem 2.15. Let L be a field and K be a subfield of L. Let $m \in K[x]$ be a monic, irreducible polynomial and $\alpha \in L$ be a zero of m. Then, $K(\alpha) = K[\alpha] \cong K[x]/\langle m(x)\rangle$.

Proof. Consider the mapping $\psi : K[x]/\langle m(x)\rangle \to K[\alpha]$ that maps $x + \langle m(x)\rangle \mapsto \alpha$. The kernel of this isomorphism is obviously $\langle m(x)\rangle$ due to a preceeding theorem. As a result, we have a monomorphism of fields. Conversely, for any $\beta \in K[\alpha]$, there is a polynomial $f \in K[x]$ such that $\beta = f(\alpha)$, therefore establishing surjection. Thus, we have an isomorphism of fields. ■

Corollary. Let L be a field, K a subfield and $m \in K[x]$ be a monic irreducible polynomial. Let $\alpha, \beta \in L$ be zeros of m. Then, $K(\alpha) = K[\alpha] \cong K[\beta] = K(\beta)$. Furthermore, this isomorphism fixes every element of K.

The above corollary can be generalized to give the following result:

Theorem 2.16. Let L and L' be fields with isomorphic subfields K and K' under the isomorphism φ with the canonical extension $\widetilde{\varphi} : K[x] \to K'[x]$. Let $f \in K[x]$ be irreducible and $\widetilde{f} = \widetilde{\varphi}(f)$. Let $\alpha \in L$ be a zero of f and $\alpha' \in L'$ be a zero of $\widetilde{f}$. Then there is an isomorphism $\psi : K[\alpha] \to K'[\alpha']$ that takes α to α' and agrees with φ on K.

Proof. It suffices to show that $K[x]/\langle f(x)\rangle \cong K'[x]\langle \widetilde{f}(x)\rangle$. Consider the map $\phi : K[x]/\langle f(x)\rangle \to K'[x]/\langle \widetilde{f}(x)\rangle$ given by $\phi(p(x) + \langle f(x)\rangle) = \widetilde{p}(x) + \langle \widetilde{f}(x)\rangle$. It is routine to check that this is indeed an isomorphism. ■

2.2 Algebraic Closure

Definition 2.17. A field F is said to be *algebtaically closed* if every polynoimal of positive degree has a root in F

Theorem 2.18. Let k be a field. Then there is an algebraically closed field K containing k.

Proof. Define the set $S = \{x_f \mid f \in k[x],\ \deg f \geq 1\}$. Let I be the ideal I in $k[S]$ generated by $\{f(x_f) \mid f \in k[x],\ \deg f \geq 1\}$. First, we shall show that I is proper. Suppose not, then there are polynomials $g_1, \dots, g_n \in k[S]$ such that $1 = \sum_{i=1}^{n} g_i f_i(x_{f_i})$. Note that the polynomials $\{g_i\}$ contain only finitely many distinct indeterminates from S. Let us use the shorthand x_i for x_{f_i}. Let the indeterminates in g_i and f_i cumulatively be $\{x_1, \dots, x_n, x_{n+1}, \dots, x_m\}$. Let E be an extension field containing $\alpha_1, \dots, \alpha_n$ such that $f_i(\alpha_i) = 0$ for all $1 \leq i \leq n$. Now substituting $x_i = \alpha_i$ for all $1 \leq i \leq n$ and $x_j = 0$ for all $n+1 \leq j \leq m$, we have a contradiction.

Now, let $\mathfrak{m}$ be a maximal ideal of $k[S]$ containing I. Obviously $k[S]/\mathfrak{m}$ is a field containing k and $x_f + \mathfrak{m}$ is a root of $f(x)$, thus every polynomial in $k[x]$ has a root in $K_1 = k[S]/\mathfrak{m}$. Now repeat this process indefinitely. Define $K = \bigcup_{i=1}^{\infty} K_i$. Note that K is a field. Further, if $f(x) \in K[x]$, then $f(x) \in K_n[x]$ for some n and has a root in $K_{n+1} \subseteq K$. This finishes the proof. ■

Corollary. Let F be a field. Then there is a field $K \supseteq F$ such that K is algebraically closed and K is algebraic over F.

Proof. Let L be an algebraically closed field containing F and consider

$$K = \{\alpha \in L \mid [F(\alpha) : F] < \infty\}$$

■

Theorem 2.19. Let k be a field and E, an algebraic extension of k. Let $\sigma : E \to E$ be a k-embedding. Then, σ is an automorphism.

Proof. It suffices to show that σ is surjective. Let $\alpha \in E$ and $p(x) = m_\alpha(x) \in k[x]$ and E' be the subfield of E generated by all the roots of $p(x)$ in E. It is obvious that σ takes the roots of p to other roots of p. Therefore, $\sigma(E') \subseteq E'$. Furthermore, if $\alpha_1, \ldots, \alpha_n$ is a basis for E' over E, then $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ is a basis for $\sigma(E')$ over E and both have the same dimension. Hence, $\sigma(E') = E'$, consequently, $\alpha \in \sigma(E)$. This completes the proof. ■

Definition 2.20 (Algebraic Closure). Let k be a field. Then K is said to be an algebraic closure of k if K is algebraically closed and K/k is algebraic.

We shall show that the algebraic closure of a field is unique upto isomorphism but there may be multiple algebraically closed fields containing k. For example, $\mathbb{A}$ and $\mathbb{C}$ are two algebraically closed fields containing $\mathbb{Q}$.

Corollary. Let k be a field. Then there is an algebraically closed extension of k that is algebraic over k.

Proof. Let L be an algebraically closed field containing k. Consider the algebraic subfield of L over k. ■

Lemma 2.21. Let k be a field and $\sigma : k \to L$ be a homomorphism of fields (also known as an embedding) where L is algebraically closed. Then there is an extension of σ that is an embedding of $k(\alpha)$ into L when α is algebraic over k.

Proof. Since α is algebraic over k, $k(\alpha) = k[\alpha]$. Therefore, for all $x \in k(\alpha)$, there is $f(X) \in k[X]$ such that $x = f(\alpha)$. Let β be any root of m_α^σ in L. Define $\overline{\sigma} : k(\alpha) \to k^\sigma(\beta)$ such that $f(\alpha) \mapsto f^\sigma(\beta)$. To see that this is well defined, note that if $f(\alpha) = g(\alpha)$, then $f(X) - g(X) = m_\alpha(X)q(X)$. As a result,

$$f(\beta) - g(\beta) = m_\alpha^\sigma(\beta)q^\sigma(\beta) = 0$$

this completes the proof. ■

Theorem 2.22 (Extension Theorem). Let k be a field and E an algebraic extension of k, and there exists an extension of σ to an embedding of E in L. If E is algebraically closed and L is algebraic over k^σ, then any such extension of σ is an isomorphism of E onto L.

Proof. Let S be the set of all pairs (F, τ) where F is a subfield of E containing k, and τ is an extension of σ to an embedding of F in L. Note that S is nonempty since $(k, \sigma) \in S$. Let $\{(F_i, \tau_i)\}_{i \in I}$ be a chain in $(S, \leqq)$ where $(F, \tau) \leqq (F', \tau')$ if $F \subseteq F'$ and $\tau'|_F = \tau$. Let $F = \bigcup_{i \in I} F_i$ and define τ on F to be equal to τ_i on some F_i. Obviously, F is a field and (F, τ) is an upper bound for the chain. Then, using Zorn's Lemma, there is a maximal element $(K, \lambda) \in S$ where λ is an extension of σ. We shall now show that $K = E$. Supopse not, then there is $\alpha \in E$ such that $\alpha \notin K$. But due to the previous theorem, there is an extension of λ to $K(\alpha)$. This proves the first part of the theorem.

Finally, if E is algebraically closed, then so is E^σ, further, L is algebraic over E^σ. As a result, $L = E^\sigma$ and σ is an isomorphism. ■

Corollary. Let k be a field and E, E' be algebraic and algebraically closed extensions of k. Then there is an isomorphism $\sigma : E \to E'$.

Theorem 2.23. Let K be a splitting field of the polynomial $f(X) \in k[X]$. If E is another splitting field of K, then there is an isomorphism $\sigma : E \to K$ inducing the identity on k. If $k \subseteq K \subseteq k^a$ where k^a is an algebraic closure of k, then ay embbedding of E in k^a inducing the identity on k must be an isomorphism of E onto K.

Proof. Let K^a be the algebraic closure of K. Then, K^a is algebraic over k and further, is algebraically closed. Then, due to a preceeding theorem, we may extend this to an embedding $\sigma : E \to K^a$ which induces an identity on K. We shall now show that σ is an isomorphism. It suffices to show that σ is surjective since injectivity is implicit.

Over E, we have the factorization $f(X) = (X - \beta_1) \cdots (X - \beta_n)$. Then, $f^\sigma(X) = c(X - \sigma\beta_1) \cdots (X - \sigma\beta_n)$. But since we have a unique factorization in $K^a[X]$, we must have that α_i are a permutation of $\sigma\beta_i$. Therefore, $\sigma\beta_i \in K$ for all i and therefore, $\sigma E \subseteq K$. But since $K = k(\alpha_1, \ldots, \alpha_n) = k(\sigma\beta_1, \ldots, \sigma\beta_n)$, we have that $K \subseteq \sigma E$ and therefore, $K = \sigma E$. ■

2.3 Splitting Fields

Definition 2.24 (Splitting Field). Let L be a field, K a subfield of L and $f \in K[x]$. We say that an extension $M \subseteq L$ of K is a splitting field for f over K if

1. f splits completely over M
2. f does not split completely over any subfield E such that $K \subseteq E \subsetneq M$.

It is obvious from definition, if $f(x) = a(x - a_1) \cdots (x - a_n)$ in some extension L of K, then the splitting field for f is given by $F(a_1, \dots, a_n)$.

The next theorem establishes the existence of splitting fields

Theorem 2.25. Let K be a field and $f \in K[x]$ be nonconstant. Then there exists a splitting field L for $f(x)$ over K

Proof. Straightforward induction. ■

Theorem 2.26. Let K and K' be fields and let $\varphi : K \to K'$ be an isomorphism with the canonical extension $\widetilde{\varphi} : K[x] \to K'[x]$ and let L, L' be splitting fields of f over K and $\widetilde{\varphi}(f)$ over K'. Then there is an isomorphism $\phi : L \to L'$ that agrees with φ on K.

Proof. Induct on $\deg f$. The base case is trivial. Now suppose $\deg f > 1$ and let $p(x)$ be an irreducible factor of f over K and let $a \in L$ be a zero of $p(x)$. Similarly, let $b \in L'$ be a root of $\widetilde{\varphi}(p)$. Due to a preceeding theorem, there is an isomorphism $\alpha : K(a) \to K'(b)$ that agrees with φ on K. Let us now write $f(x) = (x - a)g(x)$ where $g \in K(a)[x]$ and therefore, $\alpha(g) \in K'(b)[x]$. We already know that L is a splitting field for g and L' for $\alpha(g)$. Due to the inductive hypothesis, there is an isomorphism $\phi : L \to L'$ that agrees with α on $K(a)$ and thus with φ on K. This finishes the proof. ■

Corollary. Let K be a field and $f(x) \in K[x]$. Then any two splitting fields of $f(x)$ over K are isomorphic.

Proof. In the previous theorem, take $K = K'$. ■

2.4 Finite Fields

Definition 2.27. A field K of characteristic p is called perfect if $K^p = K$.

Theorem 2.28. Any finite field F has prime power cardinality. Let F be a field of cardinality p^n where p is a prime and n is a positive integer. Then F is unique upto isomorphism.

Proof. The first fact follows from Cauchy's Theorem on the additive subgroup of F. To show the existence of a field of cardinality p^n, consider the splitting field of the polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Let K be the splitting field. I claim that for all $a \in K$, $f(a) = 0$. First note that K must have characteristic p. Let α, β be two roots of f in K, then it is easy to show that $(\alpha - \beta)$ and $\alpha^{-1}\beta$ must be roots of f in K, thus the roots of $f(x)$ form a field. Further, note that $D_x f(x) = p^n x^{p^n - 1} - 1 = -1$ and thus does not share any root with $f(x)$. This implies that the roots of f are distinct in K. As a result, the K is the field composed of roots of $f(x)$. Thus K has size p^n.

Let K be any field of cardinality p^n. Then, for all non-zero elements $x \in K \backslash \{0\}$, we must have $x^{p^n - 1} = 1$ and thus $x^{p^n} - x = 0$ for all $x \in K$. And thus K is isomorphic the field of roots for the polynomial $x^{p^n} - x$, immediately implying that all such fields are isomorphic since splitting fields are unique upto isomorphism. ■

Such fields are denoted by $\mathrm{GF}(p^n)$, the Galois Field of order p^n.

Theorem 2.29. Every finite field is perfect.

Proof. Consider the map $\mathrm{GF}(p^n) \xrightarrow{\phi} \mathrm{GF}(p^n)$. Using the fact that $\operatorname{char} \mathrm{GF}(p^n) = p$, it is not hard to show that ϕ is a homomorphism of fields. Further, for all $a \in \mathrm{GF}(p^n)$, we have that $a = (a^{p^{n-1}})^p$ and thus ϕ is surjective, implying that ϕ is an automorphism and thus finite fields are perfect. ■

The map ϕ is known as the Frobenius Automorphism.

2.5 Normal Extensions

Definition 2.30 (Normal Extension). An algebraic extension E/F is called a *normal extension* if whenever $f(x) \in F[x]$, is irreducible and has a root in E, then $f(x)$ splits into linear factors in $E[x]$.

As an example, we note that each extension of degree 2 is normal. First, note that since $[E : F]$ is finite, it is algebraic. Indeed, let $f(x)$ be an irreducible polynomial with some root $\alpha \in E$. If $\alpha \in F$, then $f(x)$ is linear and the conclusion is trivial. If $\alpha \in E \backslash F$, then $1, \alpha, \alpha^2$ are not linearly independent, as a result, $f(x)$ must have degree 2 and withoutl loss of generality, let f be monic. Then, we may write $f(x) = (x - \alpha)(x - \beta)$ for some $\beta \in E$. As a result, f splits in E and E is a normal extension of F.

Definition 2.31 (F-embedding). Let K and E be fields with a common subfield F. Then an F-embedding from K to E is an injective homomorphism $\sigma : K \hookrightarrow E$ such that $\sigma(x) = x$ for all $x \in F$.

Theorem 2.32. Let E/F be an algebraic extension such that $E \subseteq \overline{F}$. Then the following are equivalent:

1. Every embedding of K in k^a over k induces an automorphsim of K
2. K is the splitting field of a family of polynomials in $k[X]$
3. Every irreducible polynomial of $k[X]$ which has a root in K splits into linear factors in K

Proof.

1. Let $\alpha \in K$ and $p(x)$ be the minimal polynomial. There is an isomorphism $k(\alpha) \to k(\beta)$ that fixes k. This is an embedding of $k(\alpha)$ in k^a and therefore can be extended to an embeddingd of K in k^a. But due to the hypothesis, this must be an automorphism of K, therefore, $\beta \in K$ and $p(x)$ splits in $K[X]$. In conclusion, K is the splitting field of the collection of polynomials $m_\alpha(x) \in k[X]$ where $\alpha \in K$. Note that we have also shown that if $p(x)$ is irreducible and has a root in K, then it splits in K. This shows that $(1) \implies (2) \wedge (3)$.

2. Now suppose K is the splitting field of the collection of polynomials $\{f_i\}_{i\in I}$. Let α and σ be an embedding of K in k^a. Let $\alpha \in K$. Let $\alpha \in K$ be the root of

some polynomial $f_i \in K[x]$, then $\sigma\alpha$ is also a root of the same polynomial and therefore, an element of K. As a result, $\sigma K \subseteq K$. We have shown previously that every such embedding must be an automorphism of K. This shows that $(2) \implies (1)$.

3. Now it suffices to show that $(3) \implies (1)$. Let $\alpha \in K$, then there is an irreducible polynomial $p(x) \in k[x]$ for α. Obviously, $\sigma\alpha$ is also a root of p and due to the hypothesis of (3), we know that $\sigma\alpha \in K$, therefore, $\sigma K \subseteq K$, which immediately implies that σ is an automorphism.

■

Theorem 2.33. Normal extensions remain normal under lifting. If $k \subseteq E \subseteq K$ and K is normal over k, then K is normal over E. If K_1 and K_2 are normal over k, and are contained in some field L, then K_1K_2 is normal over k and so is $K_1 \cap K_2$.

Proof. I have no idea what a lifting is.

Let σ be an embedding of K over E, then it is also an embedding of K over k and is therefore an automorphism of K. It now follows that K is normal over E.

Let σ be an embedding of K_1K_2 in k^a over k. As a result, $\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2) = K_1K_2$ since the restriction of σ to K_1 and K_2 are both embeddings over k. Therefore, it follows that σ is an automorhism and K_1K_2 is normal over k.

Similarly, let $p(x) \in k[x]$ have a root in $K_1 \cap K_2$, then it has all roots in K_1 and all roots in K_2 and therefore in $K_1 \cap K_2$. This completes the proof. ■

Theorem 2.34. Let E/k be a finite extension. Let $\sigma_1, \dots, \sigma_n$ be the distinct embeddings of E in E^a, then the extension

$$K = (\sigma_1 E) \cdots (\sigma_n E)$$

is the smallest normal extension of k containing E.

Proof. It is obvious that $E \subseteq K$. Then, for any embedding τ of K in E^a over k, the restriction of $\tau \circ \sigma_i$ is also an embedding of E in E^a. Therefore, $(\tau\sigma_i)_{i \in [n]}$ is a permutation of $(\sigma_i)_{i \in [n]}$. Thus, $\tau(K) \subseteq K$ and is an automorphism.

Let L/k be a normal extension and τ be an embedding of L in E^a. The restriction of τ to E must be one of the σ_i's, therefore, L must contain $\sigma_i E$ and hence the compositum $(\sigma_1 E) \cdots (\sigma_n E)$. ■

2.6 Separable Extensions

Let E/F be an algebraic extension, L be an algebraicaly closed field and $\sigma : F \to L$ be an embedding of F such that L is algebraic over σF, therefore is equal to the algebraic closure of σF, which is unique up to isomorphism.

Let S_σ be the set of extensions of σ to an embedding of E in L. Now, let L' be an algebraically closed field and $\tau : F \to L'$ be an embedding such that $L'/\tau F$ is an algebraic extension. We shall now show that S_σ and S_τ are in bijection.

Due to preceeding results, we know that L and L' are isomorphic. Let $\lambda : L \to L'$ be a field isomorphism which extends the map $\tau \circ \sigma^{-1}$ on the field σF. Now, for all $\sigma^* \in S_\sigma$, we know that $\lambda \circ \sigma^*$ is an extension of τ to an embedding of E into L'. It is not hard to see that $\lambda \circ \sigma^*$ is an extension of τ, therefore, λ induces a bijection from S_σ to S_τ, and they have the same cardinality.

Definition 2.35 (Separable Degree). The cardinality of S_σ is denoted by $[E : F]_s$ and called the *separable degree* of E over F.

Theorem 2.36. Let $k \subseteq F \subseteq E$ be a tower. Then

$$[E : k]_s = [E : F]_s[F : k]_s$$

Furthermore, if E is finite over k, then $[E : k]_s$ is finite and $[E : k]_s \leq [E : k]$.

Proof. Let $\sigma : k \to L$ be an embedding of k in an algebraically closed field L. Let $\{\sigma_i\}_{i\in I}$ be the family of distinct extensions of σ to F and for each i, let $\{\tau_{ij}\}$ be the family of distinct extensions of σ_i to E. Note that τ_{ij} contains precisely $[E : F]_s[F : k]_s$ elements. Moreover, the restriction of any embedding of E into L to F is one of the σ_i's and therefore the embedding must be one of the τ_{ij}'s and we have the desired conclusion.

Since E/k is finite, we have a tower of fields as follows:

$$k \subseteq k(\alpha_1) \subseteq k(\alpha_1, \alpha_2) \subseteq \cdots \subseteq k(\alpha_1, \dots, \alpha_n) = E$$

Recall that for any field K, the number of extensions of an embedding of K into an algebraically closed field L to $K(\alpha)$ is equal to the number of distinct roots of the minimal polynomial of α over $K[X]$.

As a result, we have $[K(\alpha) : K]_s \leq [K(\alpha) : K]$ and working inductively, we have the desired conclusion. ■

It is important to note that in the last part of the previous proof, the equality holds if and only if the equality holds at each step in the tower, that is, if and only if the minimal polynomial for α_i has distinct roots.

Definition 2.37 (Separable). Let E/k be a finite extension. Then E is said to be *separable* over k if $[E:k]_s = [E:k]$. An element α algebraic over k is said to be separable over k if $k(\alpha)$ is separable over k. A polynomial $f(X) \in k[X]$ is called separable if it has no multiple roots.

Theorem 2.38. Let E be a finite extension of k. Then E is separable over k if and only if each element of E is separable over k.

Proof. Suppose E is separable over k and $\alpha \in E$. Then we have a tower of finite extensions $k \subseteq k(\alpha) \subseteq E$. Due to a conclusion we made through the proof of the previous theorem, we must have $[k(\alpha):k]_s = [k(\alpha):k]$. Therefore, α is separable over k.

Conversely, suppose each element of E is separable over k. Let $E = k(\alpha_1, \dots, \alpha_n)$. Then, we have the following tower:

$$k \subseteq k(\alpha_1) \subseteq \cdots \subseteq k(\alpha_1, \dots, \alpha_n) = E$$

We shall inductively show $[k(\alpha_1, \dots, \alpha_i):k]_s = [k(\alpha_1, \dots, \alpha_i):k]$. The base case with $i = 1$ is trivial. Now, we have that

$$[k(\alpha_1, \dots, \alpha_i) : k(\alpha_1, \dots, \alpha_{i-1})]_s = [k(\alpha_1, \dots, \alpha_i):k]_s / [k(\alpha_1, \dots, \alpha_{i-1}):k]_s$$

But since α_i is separable over k, it must be the case that α_i is separable over $k(\alpha_1, \dots, \alpha_{i-1})$, therefore, $k(\alpha_1, \dots, \alpha_i)/k$ is separable. This completes the proof. ■

Theorem 2.39. Let E/k be a finite separable extension and $K \supseteq E \supseteq k$ be the smallest normal extension of k containing E. Then K/k is separable.

Proof. Follows from the fact that the compositum of separable extensions is separable. ■

Definition 2.40 (Infinite Separability). Let E be an arbitrary algebraic extension of k. We say E is *separable* over k if every finitely generated subextension is separable over k.

Definition 2.41. The compositum of all separable extensions of k in a given algebraic closure k^a is a separable extension, which is denoted by k^s, and called the *separable closure* of k.

As a matter of terminology, if E is an algebraic extension of k, and σ any embeding of E in k over $k<$ then we call σE a conjugate of E in k^a.

Corollary. Let E/k be finite. Then the smallest normal extension of k containing E is the compositum of all the conjugates of E in E^a.

Definition 2.42. Let α be algebraic over k. If $\sigma_1, \dots, \sigma_r$ are the distincts embeddings of $k(\alpha)$ in k^a over k, then we call $\sigma_1\alpha, \dots, \sigma_r\alpha$ the *conjugates* of α in k^a. Note that these elements are simpy the distinct roots of the irreducible polynomial of α over k.

Theorem 2.43 (Primitive Element Theorem). Let E/k be finite. There exists an element $\alpha \in E$ such that $E = k(\alpha)$ if and only if there exists only a finite number of fields F such that $k \subseteq F \subseteq E$. If E/k is finite separable, then there exists such an element α.

Proof. If k is finite, then we know that the multiplicative group of E is cyclic, which will therefore also generate E over k. Henceforth, suppose k is infinite.

Suppose now that there are only finitely many intermediate fields. Consider $k(\alpha + c\beta)$ for $c \in K$. Obviously this properly contains k and due to the Pigeon Hole Principle, there must be $c_1 \neq c_2 \in k$ such that $k(\alpha + c_1\beta) = k(\alpha + c_2\beta)$. As a result, $\beta = (c_1 - c_2)^{-1}(\alpha + c_1\beta - (\alpha + c_2\beta)) \in k(\alpha + c_1\beta)$. Thus, α is also in that field. Hence, we see that $k(\alpha, \beta) = k(\alpha + c_1\beta)$. Proceeding inductively, we have the desired conclusion.

Conversely, suppose $E = k(\alpha)$. Let $f(x) = m_\alpha(x) \in k[x]$ be the minimal polynomial for α over k. Let F be an intermediate field. Then $g(x) = m_\alpha(x) \in F[x]$ divides $f(x)$. Let $\alpha_1, \dots, \alpha_n$ be the roots of f in an algebraic closure k^a containing

E. Then $g(x)$ is a monic polynomial with leading coefficient 1, dividing $f(x)$ and is equal to a product of a subset of factors $(x - \alpha_i)$. Therefore, we may have only a finite number of intermediate fields.

We shall show the statement about separable extensions using induction. Let $E = k(\alpha, \beta)$ be a separable extension. Let $\sigma_1, \dots, \sigma_n$ be the distinct embeddings of $k(\alpha, \beta)$ in k^a over k. Consider the polynomial:

$$P(x) = \prod_{i \neq j} \left((\sigma_i\beta - \sigma_j\beta)x + (\sigma_i\alpha - \sigma_j\alpha) \right)$$

Since we may never have both $\sigma_i\alpha = \sigma_j\alpha$ and $\sigma_i\alpha = \sigma_j\alpha$, $P(x)$ is a non-zero polynomial. Therefore, there is $c \in k(\alpha, \beta)$ such that $P(c) \neq 0$. As a result, the elements $\sigma_i(\alpha + c\beta)$ are all distinct. Hence, σ_i's are a subset of the embeddings of $k(\alpha + c\beta)$ over k in k^a, consequently,

$$n \leq [k(\alpha + c\beta) : k]_s \leq [k(\alpha + c\beta) : k] \leq [k(\alpha, \beta) : k] = n$$

and we have the desired conclusion. ■

Definition 2.44. If E/k is algebraic and there is $\alpha \in E$ such that $E = k(\alpha)$, then α is a *primitive element* of E over k.

Part II

Galois Theory

Chapter 3

Galois Theory

Definition 3.1 (Galois Extension, Galois Group). An algebraic extension K of a field k is called *Galois* if it is normal and separable. The group of k-automorphisms of K over k is called the *Galois Group* and is denoted by $\mathrm{Gal}(K/k)$.

The fundamental theorem of Galois theory is the following:

Theorem 3.2 (FTGT). Let K be a finite Galois extension of k, with Galois group G. There is a bijection between the set of subfields E of K containing k, and the set of subgroups H of G, given by $E = K^H$. The field E is Galois over k if and only if H is normal in G, and if that is the case, then the map $\sigma \mapsto \sigma\mid_E$ induces an isomorphism of G/H onto the Galois group of E over k.

Theorem 3.3. Let K be a Galois extension of k. Let $G = \mathrm{Gal}(K/k)$. Then $k = K^G$. If F is an intermediate field, $k \subseteq F \subseteq K$, then K is Galois over F. The map $F \mapsto \mathrm{Gal}(K/F)$ from the set of intermediate fieldws into the set of subgroups of G is injective.

Proof. Let $\alpha \in K^G$. Let $\sigma : k(\alpha) \to K^a$ be a k-embedding. We know that there is an extension of σ to a k-embedding. Since K/k is normal, σ must be an automorphism of K fixing k and therefore, an element of G. This implies that σ fixes α. We have now shown that any embedding of $k(\alpha)$ in K over k must fix α, therefore, $[k(\alpha) : k]_s = 1$, but since α is separable over k, we must have $k(\alpha) = k$. Equivalently, $k = K^G$.

Since K/k is normal, so is K/F. Similarly, since K/k is separable, so is K/F, therefore, K/F is Galois.

Suppose two fields F and F' map to the same group H, which is a subgroup of G. Then, due to the first part, $F = K^H = F'$, establishing injectivity. ■

Definition 3.4 (Associated, Belongs). Let K/k be a Galois extension. Then for any intermediate subfield, $k \subseteq F \subseteq K$, we define the subgroup $\text{Gal}(K/F)$ to be *associated* with F and similarly, we say that a subgroup H of G *belongs* to an intermediate field F if $H = \text{Gal}(K/F)$.

Lemma 3.5. Let E/k be algebraic separable. Suppose there is an integer $n \geq 1$ such that every element $\alpha \in E$ is of degree at most n over k. Then E is finite over k and $[E : k] \leq n$.

Proof. Let $\alpha \in E$ have maximal degree over k. We shall show that $k(\alpha) = E$. Suppose not, then there is $\beta \in E$ such that $\beta \notin k(\alpha)$. Then, due to the primitive element theorem, there is $\gamma \in E$ such that $k(\gamma) = k(\alpha, \beta)$. But we would then have that $[k(\gamma) : k] \geq [k(\alpha, \beta) : k] > [k(\alpha) : k]$, a contradiction. This completes the proof. ■

Theorem 3.6 (Artin). Let K be a field and let G be a group of automorphisms of K, of order n. Let $k = K^G$ be the fixed field. Then K is a finite Galois extension of k and its Galois group is G. Further, we have $[K : k] = n$.

Proof. Let $\alpha \in K$ and $\sigma_1, \dots, \sigma_r$ be a maximal set of elements of G such that $\sigma_1\alpha, \dots, \sigma_r\alpha$ are distinct. Then, if $\tau \in G$, then $(\tau\sigma_1\alpha, \dots, \tau\sigma_r\alpha)$ is a permutation of $(\sigma_1\alpha, \dots, \sigma_r\alpha)$, lest we contradict the maximality of r. Hence, α is a root of

$$f(x) = \prod_{i=1}^{r}(x - \sigma_i\alpha)$$

further, for any $\tau \in G$, $f^\tau = f$ due to our previous conclusion. As a result, $f(x) \in k[x]$. Furthermore, f is separable. Now, since every element $\alpha \in K$ is a root of a separable polynomial of degree at most n wit hcoefficients in k, we have that K/k is finite separable extension of degree at most k due to the previous lemma. Now, since the minimal polynomial for α also splits in K, K/k is also normal and therefore Galois. Recall that the order of $\text{Gal}(K/k)$ has order at most $[K : k] \leq n$. This implies that $|G| = |\text{Gal}(K/k)|$, equivalently, $G = \text{Gal}(K/k)$. ■

Corollary. Let K be a inite Galois extension of k and let G be its Galois group. Then every subgroup of G belongs to some subfield F such that $k \subseteq F \subseteq K$.

Proof. Let H be a subgroup of G and let $F = K^H$. Due to Artin, K/F is Galois with group H. ■

The discussion till now establishes the first half of the Fundamental Theorem of Galois Theory.

Lemma 3.7. Let K/k be Galois and $\lambda : K \to K'$ be an isomorphism. Let $G = \operatorname{Gal}(K/k)$ and $G' = \operatorname{Gal}(\lambda K/\lambda k)$. Then, $G \cong G'$ under the mapping $\phi : \sigma \mapsto \lambda\sigma\lambda^{-1}$.

Proof. Obviously, ϕ is a group homomorphism but is also invertible and therefore, an isomorphism. ■

Theorem 3.8. Let K/k be Galois with group G. Let F be a subfield, $k \subseteq F \subseteq K$, and let $H = \operatorname{Gal}(K/F)$. Then F/k is normal (and therefore Galois) if and only if $H \trianglelefteq G$. If F/k is normal, then the restriction map $\sigma \mapsto \sigma\mid_F$ is an epimorphism of G onto $\operatorname{Gal}(F/k)$, whose kernel is H. Therefore, $\operatorname{Gal}(F/k) \cong G/H$.

Proof. Suppose F/k is normal (and therefore Galois) and $G' = \operatorname{Gal}(F/k)$. Then, the mapping $\theta : G \to G'$ given by $\sigma \mapsto \sigma\mid_F$. The kernel of this homomorphism is H and therefore is normal in G. Furthermore, any element $\tau \in G'$ extends to an embedding of K in k^a which must be an automorphism of K, since K/k is normal, as a result, the restriction map is surjective. This proves the first half of the first statement and the last statement.

Now suppose F/k is not normal, then there is an embedding λ of F in K over k which is not an automorphism of F. But due to the Extension Theorem, we may extend this to an embedding of K over k in k^a, which would also be an automorphism of K since K/k is normal. But note that the Galois groups $\operatorname{Gal}(K/\lambda F)$ and $\operatorname{Gal}(K/F)$ are conjugate and belong to distinct subfields, hence cannot be equal. Therefore, H is not normal in G. ■

This concludes the proof of the Fundamental Theorem of Galois Theory.