An Almost Algebraic Proof of The Fundamental Theorem of Algebra

David Kamali

February 2021

Abstract

By the results of the Sylow theorems, algebraic extension theorems and Galois theory, we shall prove the fundamental theorem of algebra, which states that the set of complex numbers is algebraically closed. This process of abstraction will provide an almost algebraic proof of the theorem, and thereby supply us with a tool in solving many questions within the field of mathematics.

Acknowledgement

I should like to convey my most profound gratitude to everyone who played a role in my academic studies.

Firstly, I thank God for giving me the strength to complete my studies.

Secondly, I should like to personally thank Kjell Elfström for his outstanding guidance and unwavering patience during the process of completing the thesis.

At last, I would like to honour my mentors, Lennart and Carolina Torebring, for their confidence in me through this journey.

Ask the former generation
and find out what their ancestors learned,
for we were born only yesterday and know nothing,
and our days on earth are but a shadow.
Job 8:8-9

Contents

1 Introduction

Have you ever considered why not try to find a non-constant polynomial with coefficients in $\mathscr{C}$ that has no complex roots? The fact is that there exists none. Every polynomial over the complex numbers must have a complex root, and this thesis, by the help of the Sylow theorems, the primitive element theorem, and the fundamental theorem of Galois theory will provide an almost algebraic proof for this argument.

This thesis serves as an unofficial extract of Serge Lang's *Algebra* [4] and the second edition of Thomas W. Hungerford's *Abstract Algebra: An Introduction* [3]. All definitions, lemmas, theorems, corollaries, remarks and proofs are from these two sources, subject to reformulation and change of title and change of symbols.

In the upcoming sections, we shall state and prove all the important tools needed for proving the main theorem of this thesis. We shall state the Sylow theorems, discuss field extension and what we mean by an algebraic field extension, normal extension and separability, and further discuss the Galois group and state and prove the fundamental theorem of Galois theory.

1.1 The History of the Fundamental Theorem of Algebra

During eighteenth century, when mathematicians had not yet made up their minds about complex numbers, there was an ongoing discussion whether it is possible to factor every polynomial into factors of degree one or two. Polynomials of degree two and three had already been solved, and even a polynomial of degree 4 seemed to be solvable but no one knew any general formula regarding solving the polynomials of degree 5 or higher. Euler believed that it was possible to do so, but he lacked a proof. In 1746, d'Almbert did the first serious attempt to prove that it is possible to factor every polynomials into terms of one degree by proving the existence of complex roots directly. It was Gauss that came up with his first proof in 1797, which was based on polynomial equations of any degree. He continued to work on the problem and concluded his fourth and last proof in 1849, mentioning that Cayley had also given a proof. Thereafter, mathematician continued to work on the problem and came up with different methods of proving the theorem [2].

2 Sylow Theorems

Published in 1872, the following theorems and their given proofs are the work of the Norwegian mathematician, Ludwig Sylow, who generalized the work of Cauchy, and hence provided the most useful tools in finite group theory [1].

We divide these theorems into three sections for the simplicity of the reader.

However, before stating and proving these theorems, the following tools are needed.

Definition 2.1 Let G be a group, and $x, y \in G$. We say that x is **conjugate** to y if $\exists a \in G$ such that $y = a^{-1}xa$.

Definition 2.2 The **conjugacy class** of an element $x \in G$ is the set of all elements $a^{-1}xa$, where $a \in G$.

$$\mathrm{ccl}(x) = \{a^{-1}xa : a \in G\}.$$

Remark 2.3 Let G be a group. By $S \leq G$, we mean that S is a subgroup of G. Moreover, we define $N \lhd G$ to denote that N is a normal subgroup of G.

Definition 2.4 Let G be a group, and $x \in G$. The **centralizer** of x, denoted by $C(x)$, is the set that includes all the elements of G that commute with x. In other words:

$$C(x) = \{b \in G : bx = xb\}.$$

Lemma 2.5 The centralizer of x is a subgroup of G.

Proof

1. $C(x)$ contains the identity element e since $xe = ex$.
2. $C(x)$ is closed under multiplication since if $a, b \in C(x)$ we have:

$$x(ab) = (xa)b = (ax)b = a(xb) = a(bx) = (ab)x.$$

3. If $y \in C(x)$ then $y^{-1} \in C(x)$ since

$$\begin{aligned} yx = xy &\implies y^{-1}yx = y^{-1}xy \\ &\implies x = y^{-1}xy \\ &\implies xy^{-1} = y^{-1}xyy^{-1} \\ &\implies xy^{-1} = y^{-1}x. \end{aligned}$$

Thus proving that $C(x)$ is a subgroup of G. ■

Definition 2.6 Let G be a group. Then we denote the centre of G by $Z(G)$ which is defined by

$$Z(G) = \{x \in G : xa = ax \text{ for all a} \in G\}.$$

Lemma 2.7 Let G be a finite group, and $x \in G$. Then $|\operatorname{ccl}(x)| = [G : C(x)]$, and therefore $|\operatorname{ccl}(x)|$ divides $|G|$.

Proof Let $a, b \in G$. Then:

$$\begin{aligned} a^{-1}xa = b^{-1}xb &\iff x = ab^{-1}xba^{-1} \\ &\iff x = (ba^{-1})^{-1}x(ba^{-1}) \\ &\iff (ba^{-1})x = x(ba^{-1}) \\ &\iff (ba^{-1}) \in C(x) \\ &\iff C(x)a = C(x)b. \end{aligned}$$

By this we have established a bijection from $\operatorname{ccl}(x)$ to the set of cosets of $C(x)$ and this conclude the proof. ■

Remark 2.8 Let G be a finite group, and let $c_1, c_2, \ldots, c_t$ be the distinct conjugacy classes of G. Then $G = c_1 \cup c_2 \cup \cdots \cup c_t$, where the distinct conjugacy classes are mutually disjoint. Since distinct conjugacy classes are mutually disjoint, we have:

$$|G| = |(c_1 \cup c_2 \cup \cdots \cup c_t)| = |c_1| + |c_2| + \cdots + |c_t|. \tag{1}$$

Here the $|c_i|$ represent the number of elements in the conjugacy class c_i. Now, if we choose an arbitarty element in each conjugacy class, $x_i \in c_i$, then c_i consists of all the conjugates of x_i. Hence, by Lemma 2.7, $|c_i|$ is the same as $[G : C(x_i)]$ which is a divisor of $|G|$. So (1) turns into the following equation:

$$|G| = [G : C(x_1)] + [G : C(x_2)] + \cdots + [G : C(x_t)]\,. \tag{2}$$

Let $x, y \in G$. Then $yx = xy$ if and only if $x^{-1}yx = y$. This means that y is in the centre of G if and only if y has only itself as conjugate. Therefore, $Z(G)$ is the union of all the conjugacy classes of G that contain a single element. Hence we can write the following equation:

$$|G| = |Z(G)| + |c_1| + |c_2| + \cdots + |c_k|. \tag{3}$$

Note that $c_1, c_2, \ldots, c_k$ are all distinct conjugacy classes of G that contain more than one element. The order of each of them also divides the order of G. Equations (1), (2), and (3) are called **class equations** of the group G.

Lemma 2.9 (Cauchy's theorem for abelian groups) Let G be a finite abelian group and p a prime that divides the order of G. Then there exists an $x \in G$ such that $|x| = p$.

Proof Let $|G| = k$. We shall prove this theorem using the induction principles.

For the base case $k = 2$, we assume $|G| = 2$, and $p \mid |G|$, then $p = 2$. Let $x \in G, x \neq e$. Since $|G|$ is finite, we have that $|x| \mid |G|$ thus $|x| = 2$.

We now assume that the statement holds for $k = n - 1$, hence all abelian groups of order $n - 1$ have an element of order p, where p is prime and divides $n - 1$.

We now shall prove the statement for $k = n$. Let $|G| = n$, and let $x \in G$, $x \neq e$. Since the order of x is positive, it is a product of some prime t, thus $|x| = tr$. Choose $y = x^r$, hence $|y| = t$. We have now the following cases:

1. $t = p$, hence $|y| = p$ which proves the theorem.

2. $t \neq p$, we then introduce the cyclic normal (since G is abelian) subgroup $H = \langle y \rangle$, where $|H| = t$. We also form the quotient group G/H, then have

$$\begin{aligned} p \mid |G| &\implies p \mid |G/H||H| \\ &\implies p \mid |G/H|t \\ &\implies p \mid |G/H|, \end{aligned}$$

   and since $|G/H| = \frac{n}{t} \leq n$ by induction hypothesis we have an element Hz in G/H of order p.

   We have $Hz^p = (Hz)^p = He$ which indicates that $z^p \in H$. We can see that $(z^p)^t = e = (z)^{pt}$ which indicates that $|z| \mid pt$.

   Then:

   (a) If $|z| = 1$, then $|Hz| = 1$ which is a contradiction.

   (b) If $|z| = t$, then $Hz^t = (Hz)^t = He$, and since $|Hz| = p$ in G/H, we get that $p \mid t$ which is a contradiction.

   (c) If $|z| = p$, then the theorem is proved.

   (d) If $|z| = pt$, then $|z^t| = p$ which proves our theorem. ■

Definition 2.10 Let G be a group, with a fixed subgroup H, and let A and B be two arbitrary subsets of G. We say that A is ***H*-conjugate** to B if $\exists k \in H$ such that

$$B = k^{-1}Ak = \{k^{-1}ak : a \in A\}$$

Note that if $H = G$, we simplify the above expression by stating that A is conjugate to B.

Definition 2.11 A ***p*-group** is a group of order $p^k, k \in \mathbf{N}$ and p a prime. Let G be a group of finite order, and H a subgroup of G. We call H a ***p*-Sylow subgroup** if $|H| = p^n$, where p^n is the highest power of p dividing the order of G. The existence of H is clear because of the first Sylow theorem.

Definition 2.12 Let S be a subgroup of a group G. By the **normalizer** of S, we mean the set $N(S)$, such that:

$$N(S) = \{x \in G : x^{-1}Sx = S\}.$$

Lemma 2.13 Let S be a subgroup of a group G. Then:

1. $N(S)$ is a subgroup of a group G.
2. S is a normal subgroup of $N(S)$.

Proof Part 1:

1. $e^{-1}Se = S$ and hence $e \in N(S)$.
2. Let $x, y \in N(S)$. We then have:

$$\begin{aligned}(xy)^{-1}S(xy) &= y^{-1}x^{-1}Sxy \\ &= y^{-1}x^{-1}xSy \\ &= y^{-1}Sy \\ &= y^{-1}yS \\ &= S.\end{aligned}$$

   Hence $xy \in N(S)$.

3. Let $x \in N(S)$. We then have:

$$\begin{aligned}x^{-1}Sx = S &\implies Sx = xS \\ &\implies x^{-1}S = Sx^{-1}.\end{aligned}$$

   Hence $x^{-1} \in N(S)$.

Therefore, $N(S)$ is a subgroup of G.

Part 2: S is a normal subgroup of $N(S)$ by the definition of $N(S)$. ■

Lemma 2.14 Let S and T be subgroups of a finite group G, and let k be the number of elements in the equivalence class of T under S-conjugacy. Then $k = [S : S \cap N(T)]$ and $k \mid |S|$.

Proof Let U denote the intersection $S \cap N(T)$, and let $a, b \in S$. We then have:

$$\begin{aligned} a^{-1}Ta = b^{-1}Tb &\iff T = ab^{-1}Tba^{-1} \\ &\iff T = (ba^{-1})^{-1}T(ba^{-1}) \\ &\iff (ba^{-1})T = T(ba^{-1}) \\ &\iff (ba^{-1}) \in U \\ &\iff Ua = Ub, \end{aligned}$$

which provides a one-to-one correspondence between the elements of the equivalence class of T and the set of cosets of U in S. This proves that $k = [S : S \cap N(T)]$. By Lagrange's theorem, we can see that

$$|S| = [S : U]\,|U| = k|U|.$$

Hence $k \mid |S|$ which is what we wanted. ■

Lemma 2.15 Let G be a finite group, and let H be a p-Sylow subgroup of G. Also, let $g \in G$. If $|g| = p^k$ for some integer k and $g^{-1}Hg = H$. Then $g \in H$.

Proof By Lemma 2.13, H is a normal subgroup of $N(H)$. We thus introduce the quotient group $N(H)/H$. We can see that $g \in N(H)$. Since $|g| = p^k$, we have that $|Hg| = p^m$ in $N(H)/H$. Denote by C the cyclic group generated by Hg, i.e. $C = \langle Hg \rangle$, hence $|C| = p^m$. Let S be a subgroup of $N(H)$, such that $H \subseteq S$ and $C = S/H$. Counting orders, we have:

$$\begin{aligned} |C| = \frac{|S|}{|H|} &\implies |S| = |C||H| \\ &\implies |S| = p^m p^n \\ &\implies |S| = p^{m+n}. \end{aligned}$$

But as stated, H is a p-Sylow subgroup of G, and $H \subseteq S$, hence $H = S$ and therefore, $n + m = n$, where n is an integer and the highest exponent p can have. Thus $m = 0$. Hence C is the identity subgroup which implies $C = \langle He \rangle = \langle Hg \rangle \implies Hg = He \implies g \in H$. ■

Theorem 2.16 (First Sylow theorem) Let G be a finite group, and let p be a prime number. If p^m divides the order of G, then G has a subgroup of order p^m.

Proof We prove this theorem by the principle of induction on the order of G. Let $|G| = k$. If $k = 1$, and since every group is a subgroup of itself, then $|G| = 1 = p^0$.

Assume that the theorem holds for all $k \leq s - 1$. We are to prove that it holds for $k = s$. Let $|G| = s$. From Remark 2.8, we get that

$$|G| = |Z(G)| + [G : C(x_1)] + [G : C(x_2)] + \cdots + [G : C(x_r)]\,,$$

where $[G : C(x_i)] > 1$, $|G| > |C(x_i)|$, and $|Z(G)| \geq 1$.

Assume there exists an index j such that $p \nmid [G : C(x_j)]$. By Lagrange's theorem, $|G| = |C(x_j)| \cdot [G : C(x_j)]$, by assumption $p^m \mid |G|$, and we see that p^m must divide $|C(x_j)|$. Hence, by induction hypothesis $C(x_j)$ and thus G contains a subgroup of order p^m.

Assume that $p \mid [G : C(x_i)]$ for every i, and thus $p \mid |Z(G)|$. We know that $Z(G)$ is an abelian group, and therefore by Lemma 2.9, $Z(G)$ must contain an element t of order p. Let $N = \langle t \rangle$, a normal subgroup of G generated by the element t. Given that $|N| = p$, and by creating the quotient group G/N, we see that $|G/N| = \frac{|G|}{|N|} = \frac{|G|}{p}$. Therefore, the order of the quotient group G/N is less than $|G|$ and divisible by p^{m-1}. Let P be a subgroup of G/N of order p^{m-1} according to induction hypothesis. Then we can find a subgroup H such that $N \subseteq H$ and thus $P = H/N$. By Lagrange's theorem we get:

$$|H| = |H/N| \cdot |N| = |P| \cdot |N| = p^{m-1} \cdot p = p^m.$$

Hence G has a subgroup H of order p^m. ■

Theorem 2.17 (Second Sylow theorem) Let G be a group and H and S both p-Sylow subgroups of G. Then H and S are conjugate. That is, there exists an element $g \in G$, such that $H = g^{-1}Sg$.

Proof Let $|G| = p^n q$, and p, q relatively prime. Since S is a p-Sylow subgroup, $|S| = p^n$. Let $S = S_1, S_2, \dots, S_k$ be the distinct conjugates of S in G. By Lemma 2.14, $k = [G : N(S)]$. Note that k and p are relatively prime. We shall prove that the p-Sylow subgroup H is conjugate to S, or in other words, $H = S_i$ for some $S_i \in M$. We shall look at H-conjugacy to prove this theorem.

Since each S_i is a conjugate of S_1, and conjugacy is transitive, every conjugate of S_i in G is also a conjugate of S_1. In other words, every conjugate of S_i is some S_j. Also, the equivalence class of S_i under H-conjugacy contains only various S_j. So the set $M = \{S_1, S_2, \dots, S_k\}$ of all conjugates of S is a union of distinct equivalence classes under H-conjugacy. By Lemma 2.14, the number of subgroups in equivalence class of each $S_i \in M$, is a power of p, because the number of subgroups that are H-conjugate to S_i is $[H : H \cap N(S_i)]$ which also divides $|H| = p^n$. Therefore, $k = |M|$ is a sum of powers of p (the number of subgroups in equivalence class of each $S_i \in M$). Hence, we get:

$$k = \sum_{n=1}^{k} p^{w_n}.$$

But k and p are relatively prime. Thus one of the exponent of p must be zero. Let $w_i = 0$. We get $p^{w_i} = p^0 = 1$. This means that for some $S_i \in M$, we have $x^{-1}S_i x = S_i$ for every $x \in H$, i.e. it is an equivalence class by itself. Therefore, by Lemma 2.15, we have that $x \in S_i$ for all such x, so that $H \subseteq S_i$. We know that, by assumption, both S_i and H are p-Sylow subgroups, therefore they have the same order. Hence $H = S_i$ which is what we wanted to show. ■

Theorem 2.18 (Third Sylow theorem) Let G be a finite group. The total number of p-Sylow subgroups of G is $\equiv 1 \bmod p$.

Proof Let $M = \{S_1, S_2, \dots, S_k\}$ be the set of all p-Sylow subgroups of G. By Theorem 2.17, all elements of M are conjugate to S_1. Let $H = S_i$, for some $S_i \in M$. We now look at the relation of H-conjugacy.

H is the only H-conjugate of H. By the proof of Theorem 2.17, the class containing H is the only equivalence class with a single subgroup. Again, by the proof of Theorem 2.17, M is the union of distinct equivalence classes, and the number of subgroups in each class is a power of p. Just one of these classes contains H, and the rest have a positive power of p as the number of their subgroups. Thus k, the number of p-Sylow subgroups of G, is the sum of 1 and different positive powers of p. Hence

$$k = 1 + \sum_{n=1}^{k-1} p^{w_n} = 1 + qp$$

for some $q \in \mathbf{Z}^+$. Thus $k \equiv 1 \bmod p$. ■

Theorem 2.19 Let G be a finite p-group. Then G is solvable, i.e. it has an abelian tower with the trivial subgroup as the first element. If $|G| > 1$, then G has a non-trivial centre.

Proof The first part follows from the second, since if G has centre $Z(G)$, and we have an abelian tower for $G/Z(G)$ by induction, we can lift it to G to prove that G is solvable. To prove the second part, by using (3), we have:

$$|G| = |Z(G)| + |c_1| + |c_2| + \cdots + |c_k|,$$

where $c_1, c_2, \ldots, c_k$ are all distinct conjugacy classes of G that contain more than one element. Then $p \mid |G|$ and also $p \mid |c_i|$ for every i. Thus p divides the order of the centre of G, as was to be proved. ■

Corollary 2.20 Let G be a p-group where $|G| \neq 1$. Then there exists a sequence of subgroups

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that G_i is normal in G and G_{i+1}/G_i is a cyclic group of order p.

Proof Since $Z(G)$, the centre of G, is a non-trivial centre, there exists an element $a \neq e$ in $Z(G)$ such that $|a| = p$. Let S be the cyclic subgroup generated by a. By induction, if $G \neq S$, we can find a sequence of subgroups as above in the factor group G/S. Taking the inverse image of this tower in G gives us the sequence we wanted to show in G. ■

3 The Theorems of Algebraic Extension

In this chapter, we shall lay the foundation of field extension and algebraic field extension that are closely related to the roots of algebraic equations.

3.1 Algebraic Extension

Definition 3.1 Let E and F be fields such that $F \subseteq E$. We then say that E is an **extension field** of F, and we denote it by E/F.

Remark 3.2 If we view E as a vector space over F, we shall say that if the dimension of E is finite, then E is a **finite extension** of F. Otherwise, if the dimension of E is infinite, then E is an **infinite extension** of F.

Definition 3.3 Let E be a finite extension of F. By $[E : F]$ we mean the dimension of E over F.

Theorem 3.4 Let F be a field, and let E/F and S/F both be finite extensions. If $\phi : E \to S$ is an isomorphism such that $\phi(w) = w$ for every $w \in F$, then $[E : F] = [S : F]$.

Proof Let $[E : F] = k$, and by considering E as a vector space over F, let the elements $a_1, \ldots, a_k \in E$ form a basis for E over F. If we prove that $\phi(a_1), \ldots, \phi(a_k)$ form a basis for S over F, then we prove the theorem. We proceed as follows:

Let $b \in S$. We can see that $b = \phi(a)$ for some $a \in E$, since ϕ is an isomorphism. We then, for some elements $t_1, \ldots, t_k \in F$, have:

$$\begin{aligned} a = t_1a_1 + \cdots + t_ka_k &\implies b = \phi(a) = \phi(t_1a_1 + \cdots + t_ka_k) \\ &\implies b = \phi(t_1a_1) + \cdots + \phi(t_ka_k) \\ &\implies b = \phi(t_1)\phi(a_1) + \cdots + \phi(t_k)\phi(a_k). \end{aligned}$$

By assumption, $\phi(w) = w$ for every $w \in F$, so

$$b = t_1\phi(a_1) + \cdots + t_k\phi(a_k),$$

thus the elements $\phi(a_1), \ldots, \phi(a_k)$ span S.
Now suppose

$$w_1\phi(a_1) + \cdots + w_k\phi(a_k) = 0,$$

for $w_1, \ldots, w_k \in F$. If we show that $w_1 = \cdots = w_k = 0$, we prove that $\phi(a_1), \ldots, \phi(a_k)$ are linearly independent.

To do so, we have

$$\begin{aligned}\phi(w_1a_1 + \cdots + w_ka_k) &= \phi(w_1a_1) + \cdots + \phi(w_ka_k)\\ &= w_1\phi(a_1) + \cdots + w_k\phi(a_k)\\ &= 0.\end{aligned}$$

Since ϕ is injective, we have

$$w_1a_1 + \cdots + w_ka_k = 0.$$

We know by assumption that the elements $a_1, \ldots, a_k$ form a basis, thus they are linearly independent which leads to $w_1 = \cdots = w_k = 0$. Hence $\phi(a_1), \ldots, \phi(a_k)$ form a basis for S over F. ■

Definition 3.5 Let E be an extension field of F, and let a be an element in E. We say that a is **algebraic** over F if there exists a non-zero polynomial $f(x) \in F[x]$ of n degree $(n \geqslant 1)$ such that

$$f(a) = 0.$$

Definition 3.6 Let E be an extension field of F. E is said to be an **algebraic extension** of F if every element of E is algebraic over F.

Theorem 3.7 Let E/F be an extension, and let $a \in E$ be an algebraic element over F. Then there exists a unique monic irreducible polynomial $m(x) \in F[x]$ with a as a root. Also, if a is a root of $h(x) \in F[x]$, then $m(x) \mid h(x)$.

Proof Let A be the set of all non-zero polynomials in $F[x]$ that have a as a root. Then $A \neq \varnothing$ since a is algebraic over F. The degrees of the elements in A are non-negative integers, which by the well-ordering principle must have a smallest element k. Let $m(x) \in F[x]$ with $\deg(m(x)) = k$. Every non-zero constant multiple of $m(x)$ has degree k and has a as a root. So without loss of generality, we choose $m(x)$ to be monic.

To prove that $m(x)$ is irreducible, we assume the opposite. Let $m(x)$ be reducible. Then there are polynomials $w(x)$ and $z(x)$ such that $m(x) = w(x)z(x)$, where $\deg(w(x)) < k$ and $\deg(z(x)) < k$. Therefore, $m(a) = w(a)z(a) = 0$ in E. Because E is a field, $w(a) = 0$ or $z(a) = 0$ which means that either $w(x) \in A$ or $z(x) \in A$. This contradicts the fact that $\deg(m(x)) = k$ is the smallest degree. Hence $m(x)$ is irreducible.

We shall prove that $m(x)$ divides every $h(x)$ in A. By the division algorithm, we have

$$h(x) = m(x)s(x) + r(x), \tag{4}$$

where $\deg(r(x)) < k$ or $r(x) = 0$. Both $m(x), h(x) \in A$, therefore, $h(a) = m(a) = 0$. Thus from (4), we get

$$r(a) = h(a) - m(a)s(a) = 0.$$

Thus a is a root of $r(x)$. The polynomial $r(x)$ must be zero, for if not, then $r(x) \in A$ which is a contradiction. So $r(x) = 0$, and hence (4) becomes

$$h(x) = m(x)s(x).$$

Hence $m(x)$ divides every element in A.

To prove that $m(x)$ is unique, let $f(x) \in A$ be a monic irreducible polynomial. Then $m(x) \mid f(x)$. Since both $m(x)$ and $f(x)$ are irreducible and non-constant, we must have $f(x) = Cm(x)$, with $C \in F$. Since both $m(x)$ and $f(x)$ are monic by assumption, $C = 1$. Thus $f(x) = m(x)$, which proves that $m(x)$ is unique. ■

Definition 3.8 Let E be an extension field of F. If a is an algebraic element in E, then the non-zero monic polynomial of the lowest degree $m(x) \in F[x]$ such that $m(a) = 0$ is called **the irreducible polynomial** of a over F. We denote this polynomial by **Irr $(\boldsymbol{a}, \boldsymbol{F}, \boldsymbol{x})$**.

Theorem 3.9 Let E be a finite extension of F. Then E is an algebraic extension of F.

Proof Since E is a finite extension of F, the dimension of E is finite. Let $\dim(E) = n$. Now consider an element $a \in E$. Then the set $1 = a^0, a^1, \ldots, a^n$ has $n + 1$ elements, and therefore must be linearly dependent in E. Hence we have:

$$c_0 + c_1 a^1 + \cdots + c_n a^n = 0$$

for some (not all zero) c_i. Define the polynomial $f(x) \in F[x]$ as follows:

$$f(x) = c_0 + c_1 x^1 + \cdots + c_n x^n.$$

We then have that $f(a) = 0$, which means that $a \in E$ is algebraic over F. Thus E is an algebraic extension of F. ■

Theorem 3.10 Let E be a finite extension of I and let I be a finite extension of F, i.e. $(F \subseteq I \subseteq E)$. Then we have:

$$[E : F] = [E : I][I : F].$$

Proof The theorem suggests that if $\{a_i\}$ is a basis for I/F, and if $\{b_j\}$ is a basis for E/I then $\{a_i b_j\}$ is a basis for E/F (for $i \in K = \{1, 2, \ldots, k\}$ and $j \in L = \{1, 2, \ldots, l\}$).

Assume that $w \in E$. Then the theorem suggests that there exist elements $x_j \in I$, such that

$$w = \sum_{j=1}^{l} x_j b_j.$$

Also, for each $j \in K$, there exist elements $y_{ij} \in F$, such that

$$x_j = \sum_{i=1}^{k} y_{ij} a_i.$$

When we combine these two sums, we have:

$$w = \sum_{j=1}^{l} \left(\sum_{i=1}^{k} y_{ij} a_i \right) b_j.$$

This proves that the element $w \in E$ is generated by elements $a_i b_j$ in E/F. Thus we only need to prove that these elements are linearly independent. To prove linear independence, we assume that

$$\sum_{j=1}^{l}\left(\sum_{i=1}^{k} y_{ij} a_i\right) b_j = 0.$$

Since the elements b_j form a basis for E, we get, for each j,

$$\sum_{i=1}^{k} y_{ij} a_i = 0,$$

and since the elements a_i form a basis for I, we get $y_{ij} = 0$ which proves its linear independency. ■

Remark 3.11 The dimension of E over F is finite if and only if the dimension of E over I and the dimension of I over F are both finite.

Definition 3.12 Let E be an extension of F. Consider the element $a \in E$. The smallest subfield containing both F and a is called a **simple extension** of F and is denoted by $F(a)$.

Not that the elements of the simple extension $F(a)$ are of the form $\frac{h(a)}{k(a)}$ where $k(a) \neq 0$ and both $h(x), k(x) \in F[x]$.

Definition 3.13 Let $\{E_i\}_{1 \leq i \leq n}$ be a sequence of extension fields, such that:

$$E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n.$$

Such a sequence is said to be a **tower** of fields.

Definition 3.14 Let E be an extension of F and let $a_1, a_2, \ldots, a_n \in E$. We construct $F(a_1, a_2, \ldots, a_n)$ as the smallest subfield of E containing F and all the elements $a_1, a_2, \ldots, a_n$. $E = F(a_1, a_2, \ldots, a_n)$ is thus said to be a **finitely generated extension** of F, that is generated by the elements $a_1, a_2, \ldots, a_n$.

Theorem 3.15 Let a be algebraic over F, and let $m(x) = \mathrm{Irr}(a, F, x)$. Then:

1. $F(a) = F[a]$
2. $F(a) \cong F[x]/(m(x))$
3. $F(a)$ is a finite extension of F.
4. $[F(a) : F]$ is equal to the degree of $\mathrm{Irr}(a, F, x)$.

Proof Let $m(x) = \mathrm{Irr}(a, F, x)$ have degree n and assume that $f(x) \in F[x]$ does not have a as a root.

Since $f(a) \neq 0$, $m(x) \nmid f(x)$ and therefore we get

$$m(x)s(x) + f(x)t(x) = 1.$$

By substituting $x = a$, we see that

$$f(a)t(a) = 1,$$

which means that $f(a)$ has an inverse in $F[a]$, namely $t(a)$. So $F[a]$ is a field, and thus $F[a] = F(a)$.

Since $a \in F(a)$, and $F(a)$ is a field, all the powers of a must be contained in $F(a)$. Also, since $F(a)$ contains F, it must contain all the elements of the form $c_0 + c_1a + \cdots + c_ka^k$ with $c_i \in F$. In other words, $f(a) \in F(a)$ for every $f(x) \in F[x]$. Consider the map $\phi : F[x] \to F(a)$ given by $\phi(f(x)) = f(a)$. It is a ring homomorphism with $\mathrm{Ker}(\phi)$ containing all polynomials in $F[x]$ which have a as a root. By Theorem 3.7, $\mathrm{Ker}(\phi)$ is the principal ideal $(m(x))$. By the help of the first isomorphism theorem, we can see that $F[x]/(m(x)) \cong \mathrm{Im}(\phi)$ under the map that sends congruence class $[f(x)]$ to $f(a)$. Since $m(x)$ is irreducible, $F[x]/(m(x))$ and thus $\mathrm{Im}\,(\phi)$ are fields. $\phi(x) = a$ and every constant polynomial $c(x)$ is mapped to $c(x)$ by ϕ, so $\mathrm{Im}\,(\phi)$ is a subfield of $F(a)$ that contains both F and a. But $F(a)$ is the smallest subfield containing both F and a, hence $\mathrm{Im}\,(\phi) = F(a) \cong F[x]/(m(x))$.

Let $\deg(m(x)) = n$, and consider the set of powers of a, $A = \{1, a, a^2, \ldots, a^{n-1}\}$. The elements of A are linearly independent over F. We prove this statement by contradiction. Assume that the elements of A are not linearly independent. Let

$$c_0 + c_1a + \cdots + c_{n-1}a^{n-1} = 0$$

with $c_i \in F$ and not all $c_i = 0$. Now let

$$t(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}.$$

We can see that $t(x) \neq 0$ and $t(a) = 0$. This means that $m(x) \mid t(x)$ but this is a contradiction, hence the elements of A must be linearly independent.

Now assume $f(a) \in F[a]$. We have

$$f(x) = g(x)m(x) + p(x)$$

where $g(x), p(x) \in F[x]$ and $\deg(p(x)) < n$, and so we have

$$f(a) = g(a)m(a) + p(a) = p(a).$$

This means that the elements of A form a basis for $F[a]$ over F. Hence $[F(a) : F] = n$. ∎

Corollary 3.16 Let $\phi : E \to K$ be an isomorphism of fields. Let a be an algebraic element in some extension field of E with minimal polynomial $m(x) \in E[x]$, and let b be an algebraic element in some extension field of K with $\phi(m)(x) \in K[x]$ as its minimal polynomial. Then ϕ extends to an isomorphism of fields $\bar{\phi} : E(a) \to K(b)$, such that $\bar{\phi}(a) = b$ and $\bar{\phi}(t) = \phi(t)$ for every $t \in E$.

Proof We can extend ϕ to an ring isomorphism $E[x] \to K[x]$. Now we define the two following maps:

$$\eta : K[x]/(\phi(m)(x)) \to K(b)$$
$$\delta : K[x] \to K[x]/(\phi(m)(x)),$$

where $\eta([h(x)]) = h(b)$ and $\delta(h(x)) = [h(x)]$. The existence of such a map η is shown in the proof of Theorem 3.15.

Consider the following composition:

$$E[x] \xrightarrow{\phi} K[x] \xrightarrow{\delta} K[x]/(\phi(m)(x) \xrightarrow{\eta} K(b)$$

$$f(x) \mapsto \phi(f)(x) \mapsto [\phi(f)(x)] \mapsto \phi(f(b)).$$

Since the three maps ϕ, η and δ are surjective, so is the composite function, and its kernel contains all the functions $r(x) \in E[x]$ such that $\phi(r(b)) = 0$. By assumption η is an isomorphism. Therefore $\phi(r(b)) = 0$ if and only if $[\phi(r)(x)]$ is the zero class in $K[x]/\phi(m)(x)$. In other words, $\phi(r(b)) = 0$ if and only if $\phi(r)(x)$ is a multiple of $\phi(m)(x)$. But if $\phi(r)(x) = s(x)\phi(m)(x)$, then we shall have

$$\phi^{-1}(\phi(r))(x) = \phi^{-1}(s)(x)\phi^{-1}(\phi(m))(x) \implies r(x) = \phi^{-1}(s)(x)m(x).$$

Thus the kernel of the composite function is the principal ideal $(m(x))$ in $E[x]$. Hence by the first isomorphism theorem $E[x]/(m(x)) \cong K(b)$.

Define the map γ:

$$\gamma : E[x]/(m(x)) \to K(b)$$

such that $\gamma([f(x)]) = \phi(f(b))$. Let $t \in E$. Note that we have

$$\gamma([x]) = b$$

$$\gamma([t]) = \phi(t).$$

Let ϕ^* be the defined isomorphism in Theorem 3.15. We have

$$\begin{array}{rr} E[x]/(m(x)) \xrightarrow{\gamma} K(b) & E[x]/(m(x)) \xrightarrow{\phi^*} E(a) \\ [f(x)] \mapsto \phi(f(b)) & [f(x)] \mapsto f(b) \\ [t] \mapsto \phi(t) & [t] \mapsto t. \end{array}$$

The composite function $\gamma \circ (\phi^*)^{-1} : E(a) \to K(b)$ is an isomorphism that extends ϕ, and also $(\gamma \circ (\phi^*)^{-1})(a) = b$. ■

Definition 3.17 Let F be a field and let E/F and K/F be two different extension fields. Let also L be a field that contains E and K. The smallest subfield of L that contains both E and K is said to be the **compositum** of E and K in L. We denote this compositum by EK.

The compositum EK is defined only if E and K are contained in some field L.

Remark 3.18 In the above definition, if E is finitely generated over F, then EK is finitely generated over K. E.g.

$$E = F(a_1, a_2, \ldots, a_n) \subseteq L \text{ and } F \subseteq K \subseteq L \implies EK = K(a_1, a_2, \ldots, a_n).$$

The compositum EK is called the **lifting** of E to K.

Remark 3.19 Let E be an extension field of F, and let a be algebraic over F. Suppose that E and $F(a)$ are two subfields of a larger field L. Then a is also an algebraic over E.

A consequence of this is that if we have the tower fields

$$F \subseteq F(a_1) \subseteq F(a_1, a_2) \subseteq \cdots \subseteq F(a_1, a_2, \ldots, a_n)$$

where the elements in the set $\{a_1, a_2, \ldots, a_n\}$ are all algebraic over F, then a_{k+1} is algebraic over $F(a_1, a_2, \ldots, a_k)$ leading to the fact that every step of the tower being an algebraic extension of its former step.

Theorem 3.20 Let E/F be finite. Then E/F is a finitely generated extension.

Proof Since E/F be finite, E has a basis $A = \{a_1, a_2, \dots, a_n\}$. It is clear that E is the smallest subfield of E containing F and the elements of A. Hence $E = F(a_1, a_2, \dots, a_n)$. ■

Theorem 3.21 If $E = F(a_1, a_2, \dots, a_n)$ and the elements in the set $\{a_1, a_2, \dots, a_n\}$ are all algebraic over F, then E/F is a finite algebraic extension.

Proof Based on the assumption, we can form the following tower fields

$$F \subseteq F(a_1) \subseteq F(a_1, a_2), \subseteq \cdots \subseteq F(a_1, a_2, \dots, a_n) = E.$$

We can see that E is generated by one algebraic element at each step (from left to right) and is therefore, by Theorem 3.15, finite. Then by Remark 3.11, E/F is finite, and thus by Theorem 3.9, E is an algebraic extension of F. ■

Definition 3.22 Let Γ be a class of extension fields E/F. Assume the following conditions hold for Γ:

1. Suppose $F \subseteq I \subseteq E$. Then
$$E/F \in \Gamma \iff I/F \in \Gamma \text{ and } E/I \in \Gamma.$$
2. Suppose $E/F \in \Gamma$ and K/F is an extension field and both E and K are contained in some field. Then $EK/K \in \Gamma$.
3. Suppose $E/F, K/F \in \Gamma$, and both $E, K \subseteq L$ for a larger field L. Then $EK/F \in \Gamma$.

Then we shall say that Γ is **distinguished**.

3.2 Algebraic Closure and Splitting Field

Definition 3.23 Let E be an extension field of F. An ***F*-automorphism** of E is an isomorphism $\phi : E \to E$ such that $\phi(a) = a$ for every $a \in F$.

Remark 3.24 Let E/F be an extension. Let the function ϕ be an injective homomorphism of F to E:

$$\phi : F \to E.$$

Then ϕ generates an isomorphism of F with the image of F, namely $\phi(F)$.

Lemma 3.25 Let E/F be an algebraic extension, and let $\phi : E \to E$ be an injective homomorphism of E into E over F. Then ϕ is an automorphism.

Proof By assumption, ϕ is injective. We thus need to prove that it is surjective. Let $t \in E$ be any element, and let $m(x) = \mathrm{Irr}(t, F, x)$. Consider I to be the subfield of E that is generated by all the roots of $m(x)$ that lie in E. Then I is finitely generated which indicates that I/F is a finite extension. Also we see that $\phi : I \to I$, since it maps a root of $m(x)$ to a root of $m(x)$. Because ϕ produces the identity on F, we consider ϕ to be an F-homomorphism, and since ϕ is injective, the image of I is a subspace of I with dimension $[I : F]$, thus $\phi(I) = I$.

We have assumed that $t \in I$, therefore we can see $t \in \phi(I)$, which proves that ϕ is surjective too. Hence ϕ is an automorphism. ■

Remark 3.26 Let E and I be two extensions of the field F, where both E and I are subfields of the field L. We create the ring $E[I]$ which has elements of the form

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n,$$

where $x_i \in E$ and $y_i \in I$. Then EI is the quotient field of this ring, with elements of the form

$$\frac{x_1y_1 + x_2y_2 + \cdots + x_ny_n}{x_1'y_1' + x_2'y_2' + \cdots + x_k'y_k'}.$$

Lemma 3.27 Let F_1/K and F_2/K be two extension fields, and let both F_1 and F_2 be subfields of a larger field F. Yet again let $\phi : F \to L$ be an injective homomorphism, where L is some field. Then $\phi(F_1F_2) = \phi(F_1)\phi(F_2)$.

Proof We consider the element

$$\frac{x_1y_1 + x_2y_2 + \cdots + x_ny_n}{x_1'y_1' + x_2'y_2' + \cdots + x_k'y_k'} \in F_1F_2.$$

We then have:

$$\begin{aligned}\phi\left(\frac{x_1y_1 + x_2y_2 + \cdots + x_ny_n}{x_1'y_1' + x_2'y_2' + \cdots + x_k'y_k'}\right) &= \frac{\phi(x_1y_1) + \phi(x_2y_2) + \cdots + \phi(x_ny_n)}{\phi(x_1'y_1') + \phi(x_2'y_2') + \cdots + \phi(x_k'y_k')} \\ &= \frac{\phi(x_1)\phi(y_1) + \phi(x_2)\phi(y_2) + \cdots + \phi(x_n)\phi(y_n)}{\phi(x_1')\phi(y_1') + \phi(x_2')\phi(y_2') + \cdots + \phi(x_k')\phi(y_k')}.\end{aligned}$$

Hence the image of an element of $\phi(F_1F_2)$ is an element in $\phi(F_1)\phi(F_2)$, which proves that $\phi(F_1F_2) = \phi(F_1)\phi(F_2)$. ■

Remark 3.28 Let $p(x)$ be an irreducible polynomial in $F[x]$, where F is a field, and consider the canonical map

$$\phi : F[x] \to F[x]/(p(x)).$$

Then ϕ induces a homomorphism on F, and its kernel is 0 since every element in F except 0 has an inverse, and generates the unit ideal, and 1 does not belong to the kernel. We now let $\gamma = \phi(x)$ which is the class of x modulo $p(x)$. Then we have:

$$\phi(p)(\gamma) = \phi(p)(\phi(x)) = \phi(p(x)) = 0.$$

Thus γ is a root of $\phi(p)$, and therefore algebraic over the field $\phi(F)$. Hence $\phi(F)[\gamma]$ is an extension field of $\phi(F)$ in which $\phi(p)$ is a root.

Note that the remark above motives that for a field F, there exists an extension E that contains a root of a polynomial of degree greater than zero in $F[x]$.

Definition 3.29 A field E is said to be **algebraically closed** if every non-constant polynomial in $E[x]$ has a root in E. If E/F is an algebraic extension and E is algebraically closed, then E is said to be an **algebraic closure** of F. We shall frequently denote it by $\bar{E}$.

Lemma 3.30 If E/F is algebraic, then $|E| \leq \max(|F|, |\mathbf{N}|)$.

Proof If F is infinite, then $|F[x]| = |F|$, and otherwise $F[x]$ is countable. ■

Theorem 3.31 Let F be a field. Then F has an algebraic closure.

Proof Let S be a set containing F with $|S| > \max(|F|, |\mathbf{N}|)$. Let A be the set of all fields $E = (T, +_T, \cdot_T)$ such that $T \subseteq S$ and E is an algebraic extension of F. Order A by $E_1 \leq E_2$ if E_2 is a field extension of E_1. If $E_i = (T_i, +_i, \cdot_i)$ is any chain in A, then $E = (T, +, \cdot) \in A$ where $T = \bigcup_i T_i$, $+ = \bigcup_i +_i$ and $\cdot = \bigcup_i \cdot_i$. Hence, by Zorn's lemma, A has a maximal element E, which is an algebraic extension of F. We show that E is algebraically closed by contradiction. Assume that there is a non-constant polynomial in $E[x]$ without roots in E. Then there is also such an irreducible polynomial $p(x) \in E[x]$. By Remark 3.28, there exists a field L and an injective homomorphism $\phi : E \to L$ such that $\phi(p)(x)$ has a root $\gamma \in L$. Then $\phi(E)(\gamma)$ is an algebraic extension of $\phi(E)$ in which $\phi(p)(x)$ is a root. By Lemma 3.30,

$$|\phi(E)(\gamma)| \leq \max(|\phi(E)|, |\mathbf{N}|) = \max(|E|, |\mathbf{N}|) \leq \max(|F|, |\mathbf{N}|) < |S|.$$

We can therefore, extend ϕ to a bijection $\phi : K \to \phi(E)(\gamma)$ where $E \subseteq K \subseteq S$. If we define the structure of K by

$$w + z = \phi^{-1}(\phi(w) + \phi(z)), \quad wz = \phi^{-1}(\phi(w)\phi(z))$$

for $w, z \in K$, then $K \in A$. Since $p(\phi^{-1}(\gamma)) = \phi^{-1}(p(\gamma)) = \phi^{-1}(0) = 0$, we have $\phi^{-1}(\gamma) \notin E$. Hence, E is a proper subfield of $E(\phi^{-1}(\gamma))$, contradicting the maximality of E. ■

Theorem 3.32 Let F be a field, and let $\phi : F \to L$ be an injective homomorphism of F into an algebraically closed field L. Let also $E = F(a)$ be generated by one element where a is algebraic over F, and $p(x) = \mathrm{Irr}(a, F, x)$. Then:

1. The number of possible extension of ϕ to $F(a)$ is less than or equal to the number of roots of $p(x)$.

2. The number of possible extension of ϕ to $F(a)$ is equal to the number of distinct roots of $p(x)$.

Proof Let $b \in L$ be a root of $\phi(p)(x)$. If $h(x) \in F[x]$, then $h(a) \in F[a]$. We can then define an extension of ϕ by mapping $f(a)$ to $\phi(f)(b)$. This is well defined regardless of what polynomial $h(x)$ we choose. Indeed, let $k(x) \in F[x]$ such that $k(a) = h(a)$. Then $(k-h)(a) = 0$, whence $p(x) \mid (k(x) - h(x))$. Thus $\phi(p)(x) \mid (\phi(k)(x) - \phi(h)(x))$ and $\phi(k)(b) = \phi(h)(b)$. Clearly, the defined map is a homomorphism that induces ϕ on F, and it is an extension of ϕ to $F(a)$. ■

Definition 3.33 Let F be a field, and let $f(x)$ be a non-constant polynomial such that $f(x) \in F[x]$. Assume that E is an extension of F such that $f(x)$ splits into linear factors in E, that is one can write $f(x)$ in E as follows:

$$f(x) = c(x - a_1)(x - a_2) \cdots (x - a_n)$$

with $a_1, a_2, \ldots, a_n \in E$, and also that $E = F(a_1, a_2, \ldots, a_n)$ is generated by all the roots of $f(x)$. Then E is said to be a **splitting field**.

Theorem 3.34 Let F be a field, and let $g(x) \in F[x]$ be a non-constant polynomial where $\deg(g(x)) = k$. Then there exists a splitting field E of $g(x)$ over F such that $[E : F] \leq k!$.

Proof We shall prove this statement using the principle of induction on k.

Let $k = 1$. Then the splitting field of $f(x)$ is F itself and $[F : F] = 1 = 1!$.

Assume that the statement holds for $k = n - 1$. Let $k = n$. Since F is a field, $f(x)$ is a product of irreducible polynomials in $F[x]$. We can therefore write

$$f(x) = p(x)g(x),$$

where $p(x)$ is a monic irreducible factor of $f(x)$. If a is a root of $p(x)$, then by Theorem 3.31 there exists an extension, namely $F(a)$ such that $a \in F(a)$. Moreover, $p(x)$ is the minimal polynomial of a. Thus by Theorem 3.15, $[F(a) : F] = \deg(p(x)) \leq \deg(f(x)) = n$. The factor theorem states that $f(x) = (x - a)h(x)$ with $\deg(h(x)) = n - 1$. Therefore by the induction hypothesis there exists a splitting field $E/F(a)$ of $h(x)$ such that $[E : F(a)] \leq (n - 1)!$. We can write

$$h(x) = c(x - t_1)(x - t_2)\dots(x - t_{n-1}),$$

and since $f(x) = (x - a)h(x)$, we have

$$f(x) = c(x - a)(x - t_1)(x - t_2)\dots(x - t_{n-1}).$$

Therefore

$$E = F(a)(t_1, \dots, t_{n-1}) = F(a, t_1, \dots, t_{n-1}),$$

which proves that E is a splitting field of $f(x)$ over F such that

$$[E : F] = [E : F(a)][F(a) : F] \leq (n - 1)!n = n!. \ ■$$

Theorem 3.35 Let F and L be two fields, and let $\phi : F \to L$ be an isomorphism of fields. Also, let $f(x) \in F[x]$ be a non-constant polynomial, where its image $\phi(f)(x) \in L[x]$. If E is a splitting field of $f(x)$ over F, and S and splitting field of $\phi(f)(x)$ over L, then ϕ extends to an isomorphism $E \cong S$, or the two extensions E/F and S/L are isomorphic. In other words, any two splitting fields E and S of a polynomial $f(x) \in F[x]$ are isomorphic.

Proof We shall prove this theorem by the help of principle of induction on the degree of $f(x)$. Let $\deg(f(x)) = 1$. Then by the definition of a splitting field $f(x) = c(x - a)$ in $E[x]$, and $E = F(a)$. But by the assumption $f(x) = cx - ca$ is in $F[x]$, so we must have $c, ca \in F$. Hence, $a = c^{-1}ca$ is also in F. Therefore, $E = F(a) = F$. Since ϕ extends to an isomorphism $F[x] \cong L[x]$, $\phi(f(x))$ also has degree 1. The similar argument proves that $L = S$.

Assume that the statement holds for polynomials of degree $n - 1$, and let $\deg(f(x)) = n$. Since $f(x)$ has a monic irreducible factor $m(x) \in F[x]$, and ϕ extends to an isomorphism $F[x] \cong L[x]$, $\phi(m)(x)$ is a monic irreducible factor of $\phi(f)(x)$ in $L[x]$. We know that E contains all the roots of $m(x)$ since every root of $m(x)$ is a root of $f(x)$ as well. By a similar argument, L contains all the roots of $\phi(m)(x)$. Let $a \in E$ be a root of $m(x)$ and let $b \in S$ be a root of $\phi(m(x))$. Then by Corollary 3.16, ϕ extends to an isomorphism $F(a) \to L(b)$ that maps a to b. We have the following situation:

$$\begin{gathered} F \subseteq F(a) \subseteq E \\ L \subseteq L(b) \subseteq S \\ F(a) \xrightarrow{\cong} L(b) \\ F \xrightarrow{\phi} L. \end{gathered}$$

Since we have begun writing images of polynomials as we have:

$$\begin{aligned} \phi(f)(x) &= (x - \phi(a))\phi(h)(x) \\ &= (x - b)\phi(h)(x). \end{aligned}$$

So $f(x)$ splits over E, therefore we let $f(x) = c(x-a)(x-a_2)\dots(x-a_n)$. But $f(x) = (x-a)h(x)$, thus $h(x) = c(x-a_2)\dots(x-a_n)$. The smallest subfield that contains all the roots of $h(x)$ and the field $F(a)$ is indeed $F(a, a_2, \dots, a_n) = E$. Therefore E is the splitting field of $h(x)$ over $F(a)$. By a similar argument, S is a splitting field of $\phi(h(x))$ over $L(b)$. We see that $\deg(h(x)) = n-1$, hence the induction hypothesis implies that the isomorphism $F(a) \cong L(b)$ can be extended to an isomorphism $E \cong S$, which is what we are looking for. ■

Remark 3.36 If F and L are equal, and $\phi : L \to L$, then the above theorem states that any two splitting fields of $f(x)$ are isomorphic.

3.3 Normal and Separable Extension

Definition 3.37 Let F be a field, and let E be an algebraic extension of F. E is said to be **normal** if an irreducible polynomial in $F[x]$ has one root in E, then it has all its roots in E, i.e it splits over E.

Let E/F be an algebraic extension and let

$$\phi : F \to L$$

be an injective homomorphism of F in an algebraically closed field L. We shall consider extensions of ϕ to E. These extensions of ϕ map E on a subfield of L which is algebraic over $\phi(F)$. Thus, for simplicity, we shall assume that L is algebraic over $\phi(F)$ and hence is equal to an algebraic closure of $\phi(F)$.

Let S_ϕ be the set of extensions of ϕ to injective homomorphisms of E in L. Assume that M is another algebraically closed field, and let $\psi : F \to M$ be an injective homomorphism. Then there exists an isomorphism $\chi : L \to M$ extending the map $\psi \circ \phi^{-1}$ applied to the field $\phi(F)$.

Let S_ψ be the set of injective homomorphism of E in M extending ψ, and let $\phi^* \in S_\phi$ be an extension of ϕ to an injective homomorphism of E in L. Then $\chi \circ \phi^*$ is an extension of ψ to an injective homomorphism of E into M. This is because we have

$$\chi \circ \phi^* = \psi \circ \phi^{-1} \circ \phi = \psi.$$

Thus χ induces a mapping from S_ϕ to S_ψ, and the inverse mapping is induced by χ^{-1}. Hence S_ϕ and S_ψ are in bijection under the mapping

$$\phi^* \mapsto \chi \circ \phi^*.$$

Particularly, the cardinality of S_ϕ and S_ψ is the same, and only depends on the extension E/F.

Definition 3.38 We shall call this this cardinality the **separable degree** of E/F and denote it by

$$[E : F]_s.$$

Theorem 3.39 Let $K \subseteq F \subseteq L$ be a tower of fields. Then

$$[L : K]_s = [L : F]_s[F : K]_s.$$

Also, if L is finite over K, then $[L : K]_s$ is finite and

$$[L : K]_s \leq [L : K].$$

The separable degree is at most equal to the degree.

Proof Let $\phi : K \to M$ be an injective homomorphism of K in an algebraically closed field M. If $\{\phi_i\}_{i\in I}$ is the family of distinct extensions of ϕ to F, and $\{\psi_{ij}\}$ is the family of distinct extensions of ϕ_i to E, then by what we saw before, each ϕ_i has precisely $[L : F]_s$ extensions to injective homomorphisms of L in M. The set of injective homomorphisms $\{\psi_{ij}\}$ contains precisely

$$[L : F]_s[F : K]_s$$

elements. Any injective homomorphism of L into M over ϕ must be one of the ψ_{ij}, and thus we have multiplicity in towers.

Now assume that L/K is finite. Then we can obtain L as the following tower of extensions:

$$K \subseteq K(a_1) \subseteq K(a_1, a_2) \subseteq \cdots \subseteq K(a_1, \ldots, a_n) = L.$$

If we define inductively $F_{w+1} = F_w(a_{w+1})$, then by Theorem 3.32 we have

$$[F_w(a_{w+1}) : F]_s \leq [F_w(a_{w+1}) : F].$$

Hence the inequality is true for every step of the tower, and by multiplicity it follows that the inequality is true for the extension L/K, which is what we wanted. ■

Corollary 3.40 Let $K \subseteq F \subseteq L$ be a tower of fields, and let L/K be finite. The equality

$$[L : K]_s = [L : K]$$

holds if and only if the corresponding equality holds in each step of the tower, that is for L/F and F/K.

Proof We know that $[L : K] = [L : F][F : K]$. By Theorem 3.39,

$$[L : K]_s = [L : F]_s[F : K]_s.$$

Hence, if $[L : K]_s = [L : K]$, then

$$[L : F]_s[F : K]_s = [L : F][F : K].$$

By Theorem 3.39, we have $[L : F]_s \leq [L : F]$ and $[F : K]_s \leq [F : K]$. Thus $[L : F]_s = [L : F]$ and $[F : K]_s = [F : K]$.

Conversely, if $[L : F]_s = [L : F]$ and $[F : K]_s = [F : K]$, then it follows immediately from Theorem 3.39 that

$$[L : K]_s = [L : F]_s[F : K]_s = [L : F][F : K] = [L : K]. ■$$

Definition 3.41 Let F be a field, and let E be an extension of F.

1. A non-zero polynomial $f(x) \in F[x]$ is said to be **separable** if it has no repeated roots in any splitting fields, i.e. it only has distinct roots. $f(x)$ is said to be **inseparable** if it is not separable.

2. An element $a \in E$ is said to be **separable over F** if a is algebraic over F, and its minimal polynomial in $F[x]$ is separable.

3. E is said to be an **separable extension** if all its elements are separable over F.

Definition 3.42 Let $f(x) \in F[x]$ be the following polynomial:

$$f(x) = k_0 + k_1x^1 + k_2x^2 + \cdots + k_nx^n$$

The **derivative** of $f(x)$, namely $f'(x)$, is defined as follows:

$$f'(x) = k_1 + 2k_2x^1 + 3k_3x^2 + \cdots + nk_nx^{n-1}.$$

Note that if $F = \mathbf{R}$ in the above definition, then the derivative is the usual derivative in calculus, but here the definition is purely algebraic and can be used on any polynomials over any field.

Remark 3.43 Let $f(x), h(x) \in F[x]$ and $c \in F$. We then have the following properties:

1. $(f(x) + h(x))' = f(x)' + h(x)'$.
2. $(f(x)h(x))' = f'(x)h(x) + f(x)h'(x)$.
3. $(cf(x)' = cf'(x)$.

Theorem 3.44 The field E is a finite-dimensional, normal extension of F if and only if E is a splitting field over the field F of some polynomial $h(x) \in F[x]$.

Proof Part 1: Assume that E/F is finite dimensional and normal, and by viewing E as a vector space, let $w_1, \ldots, w_n$ be a basis. We can write $E = F(w_1, \ldots, w_n)$. Let $m_i(x)$ be the associated minimal polynomial of the root w_i, as w_i is algebraic over F. By normality, $m_i(x)$ splits over E. Then $h(x)$, which is $\prod_{i=1}^n m_i(x)$, splits over E. Therefore, E is the splitting field of $h(x)$.

Part 2: Let E be the splitting field over the field F of a polynomial $h(x) \in F[x]$. Then if $w_1, \ldots, w_n$ are the roots of $h(x)$, we can write $E = F(w_1, \ldots, w_n)$. Thus by Theorem 3.21, $[E : F]$ is finite. Let $m(x) = \mathrm{Irr}(z, F, x)$, where $z \in E$. Now consider $m(x) \in E[x]$ and let S be the splitting field of $m(x)$ over E. Then we have $F \subseteq E \subseteq S$. We shall show that every root of $m(x)$ in S is actually in E, which proves that $m(x)$ splits over E.

Let $t \in S$ be a root of $m(x)$, and $t \neq z$. By Corollary 3.16, there exists an isomorphism $F(z) \cong F(t)$ that maps every element of F to itself and z to t. Consider $E(t)$ which is a subfield of S ($E \subseteq E(t) \subseteq S$). Then we have

$$F \subseteq F(z) \subseteq E$$

$$F \subseteq F(t) \subseteq E(t),$$

we can see that $E(t)$ is a splitting field of $h(x)$ over $F(t)$ because

$$E(t) = F(w_1, \ldots, w_n)(t) = F(w_1, \ldots, w_n, t) = F(t)(w_1, \ldots, w_n).$$

Also, we know that $z \in E$ and E/F is a splitting field of $h(x)$, hence E is a splitting field of $h(x)$ over $F(z)$, too. So by Theorem 3.35 the isomorphism $E \to E(t)$ is an extended isomorphism of $F(z) \cong F(t)$, that maps z to t and every element of F to itself. Thus by Theorem 3.4, $[E : F] = [E(t) : F]$. In the tower field $F \subseteq E \subseteq E(t)$, by Theorem 3.15, $[E(t) : E]$ is finite, and as we stated before $[E : F]$ is also finite. Hence by Theorem 3.10 we have

$$[E : F] = [E(t) : F] = [E(t) : E][E : F] \implies 1 = [E(t) : E],$$

which indicates that $E(t) = E$, and this means that $t \in E$. Thus every root of the polynomial $m(x)$ in S is in E and $m(x)$ splits over E. Therefore E/F is normal. ■

Lemma 3.45 Let F be a field, and let $f(x) \in F[x]$. $f(x)$ is separable if $f(x)$ and $f'(x)$ are relatively prime.

Proof We shall prove this lemma by contradiction. Let E be the field such that $f(x)$ splits over it, and suppose that $f(x)$ is not separable. Then $f(x)$ must have a repeated root $a \in E$. Hence, for some polynomial $h(x) \in E[x]$, we can write

$$f(x) = (x-a)^2 h(x).$$

By taking the derivative, we have

$$f'(x) = (x-a)^2 h'(x) + 2(x-a)h(x).$$

We can see that a is a root of $f'(x)$ too since $f'(a) = 0h'(a) + 0h(a) = 0$. If then $m(x) \in F[x]$ is the minimal polynomial of a, then $m(x)$ is a non-constant polynomial such that $m(x) \mid f(x)$, and $m(x) \mid f'(x)$. But this is a contradiction since $f(x), f'(x)$ were relatively prime. Hence $f(x)$ must be separable. ■

Definition 3.46 Let E be an extension field of F, and let I be a field such that $F \subseteq I \subseteq E$. Then we name I an **intermediate field** of extension.

Definition 3.47 Let F be a field. We shall say that F has **characteristic 0** if $m1_F \neq 0_F$ for all positive integers m.

Theorem 3.48 Let F be a field of characteristic 0. We have:

1. Every irreducible polynomial $f(x) \in F[x]$ is separable.
2. Every algebraic extension E/F is a separable extension.

Proof Part 1: Let $f(x) \in F[x]$ be a non-constant irreducible polynomial, so that

$$f(x) = c_n x^n + \cdots + c_1 t + c_0,$$

where $c_n \neq 0, n \geq 1$. Then

$$f'(x) = nc_n x^{n-1} + \cdots + c_1,$$

where $nc_n \neq 0$. Therefore $f'(x)$ is a non-zero polynomial where $\deg(f'(x)) < \deg(f(x))$. So $f(x), f'(x)$ are relatively prime. Thus by Lemma 3.45, $f(x)$ is separable.

Part 2: The same argument holds for the minimal polynomial of each $a \in E$, so they are separable, which means that E is separable. ■

Theorem 3.49 (Primitive element theorem) Let F be a field and let E/F be a finite extension. There exists an element $a \in E$ such that $E = F(a)$ if and only if there exist only a finite number of intermediate fields I, i.e. $F \subseteq I \subseteq E$. If E is an separable extension of F, then such an element a exists.

Proof If F is finite, then the multiplicative group of E is generated by one element a, and the theorem is proved in this case. We therefore assume that F is infinite. Since the statement is an if and only if statement, we shall prove both parts.

Firstly, let there be only a finite number of intermediate fields. Let $a, b \in E$. Let c range over the elements of F. Then we only have a finite number of fields of the type $F(a + bc)$. This means that for some $c_1, c_2 \in F$, where $c_1 \neq c_2$, we have:

$$F(a + bc_1) = F(a + bc_2).$$

Since $a + bc_1$ and $a + bc_2$ are in the same field, so are the elements $c_1 - c_2$, $b(c_1 - c_2)$, b, and also a. Therefore $F(a, b)$ can be generated by only one element. By the principle of induction, if $E = F(a_1, \dots, a_k)$, then we can find $c_2, \dots, c_k \in F$ such that $E = F(\gamma)$, and $\gamma = a_1 + a_2c_2 + \cdots + a_{k-1}c_{k-1} + a_kc_k$.

Secondly, let $E = F(a)$ for some $a \in E$, and let $p(x) = \mathrm{Irr}(a, F, x)$. Let I be an intermediate field, $F \subseteq I \subseteq E$, and let $m_I(x) = \mathrm{Irr}(a, I, x)$. This means that $m_I(x) \mid p(x)$. Unique factorisation holds in $E[x]$, so any monic polynomial in $E[x]$ that divides $p(x)$ can be written as $\prod_{i=1}^{k}(x - a_i)$, where a_i's are roots of $p(x)$. Hence there exist only a finite number of these monic polynomials. So we can arrange a mapping

$$\psi : I \to \mathrm{Irr}(a, I, x) = m_I(x).$$

Let I^* be a subfield of I that is generated by coefficients of $m_I(x)$. Then the coefficients of $m_I(x)$ are in I^* and $m_I(x)$ is irreducible over I^* since it is irreducible over I. Hence the degree of a over I^* is equal to the degree of a over I. Thus $I = I^*$, which indicates that our field I is uniquely determined by its associated polynomial $m_I(x)$, and our map ψ is therefore injective, which proves that there are finite number of I's since there are finite number of $m_I(x)$'s.

Without loss of generality, let $E = F(a, b)$, where a, b are separable over F. Let $\phi_1, \dots, \phi_k$ be the distinct injective homomorphisms of $F(a, b)$ in $\bar{F}$ over F. Construct $f(x)$ such that

$$f(x) = \prod_{i \neq j}(\phi_i(a) + \phi_i(b)x - \phi_j(a) - \phi_j(b)x).$$

Then $f(x)$ is not the zero-polynomial, so there exists an element $c \in F$, such that $f(c) \neq 0$. Then the elements $\phi_i(a+bc)$ are all distinct for $i = 1, 2, \dots, k$. This means that $[F(a+bc) : F]$ is at least k. But $[F(a, b) : F] = k$, hence $F(a, b) = F(a + bc)$ which proves the statement. ■

Remark 3.50 The element a is said to be a **primitive element** of E if $E = F(a)$.

4 Galois Theory

The following results, are based on the work of Évariste Galois, a young French mathematician, who made great discoveries in the theory of polynomial equations. He was killed in a duel, but the night before his death, he wrote a letter to Auguste Chevalier, in which he mentioned the connection between groups and polynomial equations [5](page 14). Years after his death, many developments were made based on his works, which will be stated in this chapter. These developments are strong tools needed to prove the final result.

4.1 Galois Group

Definition 4.1 Let E be an extension field of F. The **Galois group** of E over F, denoted by **G(E/F)**, is the set of all F-automorphisms of E.

Lemma 4.2 Let again E be an extension field of F. Then $G(E/F)$ is a group under the composition of functions operation.

Proof Let $i : E \to E$ be the identity map. Since i is an automorphism and $i \in G(E/F)$, $G(E/F)$ is non-empty. Let $\phi, \psi \in G(E/F)$. Then for $\phi \circ \psi$ we have:

1. $(\phi \circ \psi)(x) = (\phi \circ \psi)(y) \implies \phi(\psi(x)) = \phi(\psi(y)) \implies \phi(x) = \phi(y) \implies x = y.$

2. Let $w \in E$. Then by surjectivity of ψ, there is a $y \in E$ such that $w = \psi(y)$, and by surjectivity of ϕ there is an $x \in E$ such that $y = \phi(x)$. Hence $w = (\psi \circ \phi)(x)$.

3. Since ϕ, ψ are homomorphisms, we have

$$(\psi \circ \phi)(x + y) = \psi(\phi(x + y)) = \psi(\phi(x)) + \psi(\phi(y)) = (\psi \circ \phi)(x) + (\psi \circ \phi)(y).$$

   We can prove $(\psi \circ \phi)(xy) = (\psi \circ \phi)(x)(\psi \circ \phi)(y)$ in a similar way.

4. For each $a \in F$, we have that $(\phi \circ \psi)(a) = \phi(\psi(a)) = \phi(a) = a$.

Therefore, $\phi \circ \psi$ is an automorphism and $\phi \circ \psi \in G(E/F)$, and $G(E/F)$ is closed. Let $\phi \in G(E/F)$. Then for ϕ^{-1} we have:

$$\phi(\phi^{-1}(x) + \phi^{-1}(y)) = \phi(\phi^{-1}(x)) + \phi(\phi^{-1}(y)) = x + y.$$

Hence

$$\phi^{-1}(x) + \phi^{-1}(y) = \phi^{-1}(x + y).$$

Moreover,

$$\phi(\phi^{-1}(x)\phi^{-1}(y)) = \phi(\phi^{-1}(x))\phi(\phi^{-1}(y)) = xy.$$

Hence

$$\phi^{-1}(x)\phi^{-1}(y) = \phi^{-1}(xy).$$

For each $a \in F$, we have that $\phi^{-1}(a) = \phi^{-1}(\phi(a)) = a$. Hence ϕ^{-1} is an automorphism and $\phi^{-1} \in G(E/F)$, an thereby we have proved that $G(E/F)$ is a group. ■

Lemma 4.3 Let E be an extension field of F, and let $f(x)$ be a polynomial with coefficients in F. Let $w \in E$ be a root of $f(x)$ and $\phi \in G(E/F)$. Then $\phi(w)$ is also a root of $f(x)$.

Proof Without loss of generality, assume that $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. By assumption $f(w) = 0_F$ and so we have:

$$\begin{aligned} f(\phi(w)) &= a_0 + a_1(\phi(w)) + a_2(\phi(w))^2 + \cdots + a_n(\phi(w))^n \\ &= \phi(a_0) + \phi(a_1)(\phi(w)) + \phi(a_2)(\phi(w))^2 + \cdots + \phi(a_n)(\phi(w))^n \\ &= \phi(a_0 + a_1w + a_2w^2 + \cdots + a_nw^n) \\ &= \phi(f(w)) \\ &= \phi(0_F) \\ &= 0_F. \end{aligned}$$

Hence $\phi(w)$ is also a root of $f(x)$. ■

Lemma 4.4 Let E be the splitting field of some polynomial over F, and let w, z be elements in E. Then there exists an ϕ in the Galois group of E over F such that $\phi(w) = z$ if and only if w and z have the same minimal polynomial in $F[x]$.

Proof Let $w, z \in E$ have the same minimal polynomial. Then by Corollary 3.16, there exists an isomorphism $\phi : F(w) \to F(z)$, such that $\phi(w) = z$, and ϕ fixes F elementwise. Since E is a splitting field of some polynomial $f(x)$ over F, then E is a splitting field of $f(x)$ over $F(w)$ and also $F(z)$. Therefore, ϕ extends to an F-automorphism of E (which we also denote by ϕ) by Theorem 3.35. This means that $\phi \in G(E/F)$ and $\phi(w) = z$. The converse is an immediate consequence of Lemma 4.3. ■

Theorem 4.5 Let $E = F(a_1, \ldots, a_n)$ be an algebraic extension field of F. If $\phi, \psi \in G(E/F)$ and $\phi(a_i) = \psi(a_i)$ for each $i \in \{1, 2, \ldots, n\}$, then $\phi = \psi$. This means that an automorphism in $G(E/F)$ is completely determined by its action on $a_1, \ldots, a_n$.

Proof Let $\gamma = \psi^{-1} \circ \phi \in G(E/F)$. We shall prove that γ is the same as the identity map ι. By definition, $\phi(a_i) = \psi(a_i)$ for every i, hence

$$\gamma(a_i) = (\psi^{-1} \circ \phi)(a_i) = \psi^{-1}(\phi(a_i)) = \psi^{-1}(\psi(a_i)) = (\psi^{-1} \circ \psi)(a_i) = \iota(a_i) = a_i.$$

Let $k \in F(a_1)$. By the proof of Theorem 3.15, there exist $c_i \in F$ such that

$$k = c_0 + c_1 a_1 + \cdots + c_{m-1} a_1^{m-1},$$

where m is the degree of the minimal polynomial of a_1. Since γ is a homomorphism that fixes every element of F including a_1, we have

$$\begin{aligned}\gamma(k) &= \gamma(c_0 + c_1 a_1 + \cdots + c_{m-1} a_1^{m-1}) \\ &= \gamma(c_0) + \gamma(c_1 a_1) + \cdots + \gamma(c_{m-1} a_1^{m-1}) \\ &= c_0 + c_1 a_1 + \cdots + c_{m-1} a_1^{m-1}.\end{aligned}$$

Therefore, $\gamma(k) = k$ for every $k \in F(a_1)$. The same argument holds to show that $\gamma(k) = k$ for every $k \in F(a_1)(a_2) = F(a_1, a_2)$. After repeating this process a finite number of times, we have $\gamma(k) = k$ for every $k \in F(a_1, a_2, \ldots, a_n) = E$, that is, $\gamma = \iota = \psi^{-1} \circ \phi$. Thus,

$$\psi = \psi \circ \iota = \psi \circ (\psi^{-1} \circ \phi) = (\psi \circ \psi^{-1}) \circ \phi = \iota \circ \phi = \phi. \blacksquare$$

Theorem 4.6 Let E be an extension field of F. Assume S is a subgroup of the Galois group of E over F, and let

$$I_S = \{a \in E : \phi(a) = a \text{ for every } \phi \in S\}.$$

Then I_S is an intermediate field of extension.

Proof We shall show that I_S is a subfield of E and that F is a subfield of I_S.

1. The assumption, $S \leq G(E/F)$ gives us that for every $\phi \in S$ and every $x \in F$ we have $\phi(x) = x$ and this proves that F is a subfield of I_S.

2. Let $x, y, z \in I_S, z \neq 0$ and $\phi \in S$. Then we have

   (a) $0, 1 \in I_S$ because $\phi(0) = 0$ and $\phi(1) = 1$ for every automorphism.

   (b) $\phi(x + y) = \phi(x) + \phi(y) = x + y$ and $\phi(xy) = \phi(x)\phi(y) = xy$. Thus I_S is closed under addition and multiplication.

   (c) $\phi(-z) = -\phi(z) = -z \implies -z \in I_S$

   (d) $\phi(z^{-1}) = \phi(z)^{-1} = z^{-1} \implies z^{-1} \in I_S$

   Thus proving that I_S is a subfield of E. ■

Note that we define I_S to be **fixed field** of the subgroup S.

4.2 Galois Extension

Lemma 4.7 Let E be a finite-dimensional extension of F. Let $S \leq G(E/F)$ and I its fixed field. Then E is a simple, separable and normal extension of I.

Proof Since E is a finite extension, every element $t \in E$ is algebraic over F, and hence algebraic over I. By Lemma 4.3, every $\phi \in S$ must map t to some root of its minimal polynomial $m(x) \in I[x]$. We see that the images of t of the automorphisms in S is finite. Let M denote the set containing all the images of t under automorphism in S:

$$M = \{t = t_1, t_2, \ldots, t_k\}.$$

Let $\phi, \psi \in S$, and let $t_i = \psi(t)$. Then $\phi(t_i) = (\phi \circ \psi)(t)$. Since $\phi \circ \psi \in S$, $\phi(t_i) \in M$ because it is an image of t. We also know that ϕ is injective. Therefore we must have k distinct images of t, namely $\phi(t_1), \phi(t_2), \ldots, \phi(t_k)$, and not necessarily in the same order as $t_1, t_2, \ldots, t_k$. We can see that ϕ permutes $t_1, t_2, \ldots, t_k$. Define $f(x)$ to be:

$$f(x) = \prod_{i=1}^{k}(x - t_i).$$

$f(x)$ is separable, because all t_i's are distinct. We shall prove that $f(x) \in I[x]$:

Let again $\phi \in S$. Then by applying ϕ to the both sides of equation, we get:

$$\phi(f)(x) = \prod_{i=1}^{k}(x - \phi(t_i)).$$

But since ϕ permutes $t_1, t_2, \ldots, t_k$, by rearranging we have:

$$\phi(f)(x) = \prod_{i=1}^{k}(x - \phi(t_i)) = \prod_{i=1}^{k}(x - t_i) = f(x).$$

This means that every automorphism $\phi \in S$ maps the coefficients of the separable polynomial $f(x)$ to themselves. This shows that the coefficients of $f(x)$ are in I, the fixed field of S, thus $f(x) \in I[x]$.

We know $t \in E$, and we see that $t = t_1$ is a root of $f(X) \in I[x]$, which indicates that t is separable over I, which leads to E being a separable extension of I.

We also know by assumption that $[E : F]$ is finite. Then $[E : I][I : F]$ is also finite, hence $[E : I]$ is finite. Therefore, by Theorem 3.49, $E = I(t)$ for some $t \in E$, hence $f(x)$ splits over E. Then E is a splitting field of $f(x)$ over I, and by Theorem 3.44, E/I is normal. ■

Theorem 4.8 Let E be a finite-dimensional extension of F. Assume that $S \leq G(E/F)$ and let I be its fixed field. Then $S = G(E/I)$ and $|S| = [E : I]$.

Proof We know, by Lemma 4.7, that $E = I(t)$ for some $t \in E$. Let $m(x)$ denote the minimal polynomial of t over E, and let $\deg(m(x)) = n$. Then by Theorem 3.15, $[E : I] = n$. Since by Lemma 4.3 and Theorem 4.5, distinct automorphisms of $G(E/I)$ map t to distinct roots of $m(x)$, the number of distinct automorphims on $G(E/I)$ is at most n. By the definition of fixed field I, we have:

$$S \subseteq G(E/I) \implies |S| \leq |G(E/I)| \leq [E : I] = n.$$

Let $f(x)$ be as in the proof of Lemma 4.7. In other words:

$$f(x) = \prod_{i=1}^{k}(x - t_i),$$

where $t_1, t_2, \ldots, t_k$ are all the images of t under an automorphism in S, and k is the number of distinct images of t under S. Then S contains at least as many automorphisms as k.

$t = t_1$ is a root of $f(x)$, hence $m(x) \mid f(x)$. Hence we have:

$$\deg(m(x)) = [E : I] = n \leq \deg(f(x)) = k \leq |S|.$$

By joining the two above inequalities, we have:

$$|S| \leq |G(E/I)| \leq [E : I] \leq |S| \implies |S| = |G(E/I)| = [E : I].$$

Hence, we have $S = G(E/I)$. ■

Definition 4.9 Let E be a finite-dimensional, normal and separable extension field of F. Then we say that E **is Galois over** F. We sometimes say that E is a **Galois extension** of F.

Remark 4.10 By Theorem 3.44, a Galois extension is a splitting field.

Lemma 4.11 Let E be a Galois extension field of F, let I be an intermediate field, and denote by $G(E/I)$ the Galois group of E over I. Then I is the fixed field of $G(E/I)$.

Proof Denote the fixed field of $G(E/I)$ by $\tilde{I}$. By definition $I \subseteq \tilde{I}$. We shall prove that $\tilde{I} \subseteq I$ by a contrapositive proof: $t \notin I \implies t \notin \tilde{I}$.

Let $t \notin I$. E is an algebraic extension of the intermediate field I, since E is a Galois extension of I. Therefore, t is algebraic over I with $m(x)$ as its minimal polynomial. we can see that $\deg(m(x)) \geq 2$, because if $\deg(m(x)) = 1$, then $t \in I$ which is a contradiction.

The roots of $m(x)$ are distinct, and both lie in E (by separability and normality). Now let s be a root of $m(x)$ such that $s \neq t$. By Lemma 4.4, there exists an automorphism $\phi \in G(E/I)$ such that $\phi(t) = s$, which means that there exists an automorphism that moves t, and hence $t \notin \tilde{I}$.

This proves that if $t \in \tilde{I}$, then $t \in I$. Hence $\tilde{I} \subseteq I$, and thus $I = \tilde{I}$. ■

Remark 4.12 Let I and J be intermediate fields. If $G(E/I) = G(E/J)$, then by Lemma 4.11, both I and J are the fixed fields of the same group, thus resulting in $I = J$.

4.3 The Fundamental Theorem of Galois Theory

Lemma 4.13 Let E/F be normal but also finite. Let I be an intermediate field, such that I/F is normal. Then there exists a surjective homomorphism of groups $\pi : G(E/F) \to G(I/F)$ such that $\mathrm{Ker}(\pi) = G(E/I)$.

Proof Assume that $\phi \in G(E/F)$, and let $a \in I$. Then a is algebraic over F. Let $m(x)$ denote its minimal polynomial. We know that I/F is normal, thus $m(x)$ splits in $I[x]$, so all the roots of $m(x)$ are contained in I. Since, by Lemma 4.3, $\phi(a)$ is also a root of $m(x)$, we have $\phi(a) \in I$. Therefore, $\phi(I) \subseteq I$ for every $\phi \in G(E/F)$, so the restriction of ϕ to I, which we denote by $\phi \mid I$, is an F-automorphism, $I \cong \phi(I)$. By Theorem 3.4, $[I : F] = [\phi(I) : F]$, but we also have $[I : F] = [I : \phi(I)][\phi(I) : F]$ because $F \subseteq \phi(I) \subseteq I$. Thus $[I : \phi(I)] = 1$, which means that $I = \phi(I)$, so $\phi \mid I$ is actually an automorphism in $G(I/F)$.

Construct the function $\pi : G(E/F) \to G(I/F)$ to be $\pi(\phi) = \phi \mid I$. It is clear that π is a homomorphism of groups whose kernel consists of the automorphisms of E whose restriction to I is the identity map, that is $\text{Ker}(\pi) = G(E/I)$.

To prove surjectivity, we do as follows: By Theorem 3.44, we know that E is a splitting field over F, and hence E is a splitting field of the same polynomial over I. Consequently, by Theorem 3.35, every $\psi \in G(I/F)$ can be extended to an F-automorphism $\phi \in G(E/F)$. So $\phi \mid I = \psi$, which means that $\pi(\phi) = \psi$. Hence π is surjective. ■

Theorem 4.14 Let E be a Galois extension field of F. Let L be the set that contains all the intermediate fields of extension, and let S be the set that contains all subgroups of the Galois group $G(E/F)$. Then we have:

Part 1: There is a bijection between L and S assigning every intermediate field I to the subgroup $G(E/I)$. Also

$$|G(E/I)| = [E : I]$$

and

$$[I : F] = [G(E/F) : G(E/I)].$$

Part 2: An intermediate field I is a normal extension of F if and only if $G(E/I) \triangleleft G(E/F)$, and in that case, $G(E/F)/G(E/I) \cong G(I/F)$.

Proof Part 1: The existence of a bijection between L and S assigning every intermediate field I to the subgroup $G(E/I)$ is an immediate consequence of Theorem 4.8 and Remark 4.12. Moreover, by Theorem 4.8 and Lemma 4.11, each intermediate field I is the fixed field of $G(E/I)$, and $[E : I] = |G(E/I)|$. Thus if $I = F$, then $[E : F] = |G(E/F)|$. We then, by considering Lagrange's theorem and Theorem 3.10, have:

1. $|G(E/I)|[G(E/F) : G(E/I)] = |G(E/F)|$,
2. $[E : I][I : F] = [E : F] = |G(E/F)|$,

which implies that:

$$[E : I][I : F] = |G(E/I)|[G(E/F) : G(E/I)] \implies [I : F] = [G(E/F) : G(E/I)]$$

which is what we wanted to prove.

Part 2: Assume that $G(E/I) \triangleleft G(E/F)$. Let $m(x) = \text{Irr}(w, F, x)$, with $w \in I$. We shall now prove that $m(x)$ splits in $I[x]$. We can see that $m(x)$ splits over $E[x]$ since E/F is a normal extension. Therefore it is only necessary to show that each root $z \in E$ of $m(x)$ is indeed in I.

By Lemma 4.4, there exists an automorphism $\phi \in G(E/I)$ such that $\phi(w) = z$. Let $\psi \in G(E/I)$. By normality, there exists a $\xi \in G(E/I)$ such that:

$$\psi \circ \phi = \phi \circ \xi.$$

We know that $w \in I$. Then

$$\psi(z) = \psi(\phi(w)) = \phi(\xi(w)) = \phi(w) = z.$$

This means that z is fixed by every element $\psi \in G(E/I)$, and thus must be an element in I which is the fixed field of $G(E/I)$.

On the other hand, assume I/F is normal. Then by Part 1, $[I : F]$ is finite. By Lemma 4.13, there exists a surjective homomorphism $\pi : G(E/F) \to G(I/F)$ such that $ker(\pi) = G(E/I)$, which indicates that $G(E/I) \lhd G(E/F)$. Hence by the first isomorphism theorem, we have:

$$G(E/F)/G(E/I) \cong G(I/F). \blacksquare$$

5 The Final Proof

We now have the necessary tools for proving the fundamental theorem of algebra. We shall take into consideration the two following facts from analysis:

1. By the theorem of the square root, every positive element in $\mathbf{R}$ is a square.
2. By the consequence of the intermediate value theorem, every polynomial $f(x) \in \mathbf{R}[x]$ of odd degree has a root in $\mathbf{R}$.

We shall also note that by considering $i = \sqrt{-1}$, every element of the extension $\mathscr{C}$ has a square root. Let $a + bi \in \mathscr{C}$, with $a, b \in \mathbf{R}$. We can now define $x + yi$ such that:

$$a + bi = (x + yi)^2$$

where

$$x^2 = \frac{a + \sqrt{a^2 + b^2}}{2} \quad \text{and} \quad y^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}.$$

Theorem 5.1 The field of complex numbers $\mathscr{C}$ is algebraically closed.

Proof We shall prove this theorem using an almost algebraic proof. We know that $\mathbf{R}$ has characteristic 0. Therefore, by Theorem 3.48, every algebraic extension of $\mathbf{R}$ is separable. Every finite extension of $\mathscr{C}$ is contained in an extension E which is finite and Galois over $\mathbf{R}$. We shall show that $E = \mathscr{C}$.

Let $G = G(E/R)$. Let H be a 2-Sylow subgroup of G and choose F to be its fixed field, that is $F = \{r \in E : \phi(r) = r \text{ for every } \phi \in H\}$. Knowing that $[F : \mathbf{R}]$ is odd, and by considering the primitive element theorem, we can find an element $a \in F$ such that $F = \mathbf{R}(a)$. Then a is the root of an irreducible polynomial $p(x) \in \mathbf{R}[x]$ of odd degree. This is possible only if $\deg(p(x)) = 1$. Hence G is indeed equal to H, and G is a 2-group.

We know that E is a normal, finite-dimensional and separable extension field of $\mathscr{C}$, hence by definition, E is a Galois extension of $\mathscr{C}$. Let $G_1 = G(E/\mathscr{C})$. Then G_1 is a 2-group. Assume that G_1 is not a trivial group, then by Corollary 2.20, G_1 has a subgroup G_2 of index 2. Thus by Theorem 4.14, there exists an intermediate field I (the fixed field of G_2), such that the degree of I over $\mathscr{C}$ is 2. In other words, I is a quadratic extension, but knowing that every element in $\mathscr{C}$ has a square root gives us the fact that $\mathscr{C}$ has no extensions of degree 2, and this contradicts our assumption. Therefore, G_1 is the trivial 2-group and $|G_1| = 1$. Hence $[E : \mathscr{C}] = 1$, thus $E = \mathscr{C}$. $\blacksquare$

5.1 Conclusion

We have proved that the set of complex number is algebraically closed, which means that every polynomial in $\mathscr{C}[x]$ has a root in $\mathscr{C}$. Then as a consequent of this theorem, by knowing that $\mathscr{C}$ is an splitting field, we see that every polynomial of degree n has exactly n roots. This provides us a strong tool for the further studies in the field of mathematics.

References

[1] J. O'Connor, E. F. Robertson, *Peter Ludwig Mejdell Sylow*, www.mathshistory.st-andrews.ac.uk/Biographies/Sylow/, University of St Andrews, Scotland, (2014) [Accessed 11 Nov 2020]

[2] J. Gray, *A History of Abstract Algebra*,Springer Nature Switzerland AG, eBook, (2018)

[3] T. W. Hungerford, *Abstract Algebra: An Introduction*, Second Edition, Cengage Learning, (1997)

[4] S. Lang, *Algebra*, Addison-Wesley Publishing Company, INC, (1965)

[5] I. Stewart, *Galois Theory*,Fourth Edition, Taylor and Francis Group, eBook, (2015)