THE FUNDAMENTAL THEOREM OF LINEAR MAPS

YUKI ZANG

Abstract. The primitive element theorem is an important theorem in field theory, a branch of abstract algebra. It focuses on finite-degree extensions and determines when such extensions are simple. In this paper, we will introduce necessary definitions and propositions, along with concrete examples, to build up toward the theorem. Briefly, the theorem states that a finite extension is simple if and only if there are finitely many intermediary fields between the original and the extended field.

1. Introduction

The primitive element theorem has fundamental importance in field theory and Galois theory. It helps characterizing finite degree extensions that can be generated by a single element, which is thus named as a primitive element. Meanwhile, such extensions are called simple extensions. The theorem facilitates our analysis on the structural properties of such fields.

The history of the Main Theorem dates back to 1831 when mathematician Évariste Galois first sketched a proof of the classical primitive element theorem. The theorem states as follows:

Theorem 1.1.

Every separable field extension of finite degree is simple.

The proof wasn't complete but could be easily finished by a theorem of Joseph-Louis Lagrange from 1771. Galois then extensively used the theorem for the development of Galois theory and fundamental theorem of Galois theory. Later in 1910, mathematician Ernst Steinitz proposed a modern version of the theorem, which he then named as the theorem of the intermediate fields. This is the Main Theorem we will focus on, and it states as follows:

Main Theorem. *Primitive Element Theorem(Steinitz,1910 [7]):*
Let F and K be arbitrary fields, and let K be an extension of F of finite degree. Then there exists an element $\alpha \in K$ such that $K = F(\alpha)$ if and only if there are finitely many fields L with $F \subseteq L \subseteq K$.

In fact, using the fundamental theorem of Galois theory, the latter theorem leads to the former. The theorem can be useful in implication as it determines when a 'generator' of a field exists. To better illustrate the theorem, we provide an example here:

Example 1.2. Let $F = \mathbb{R}$ and $K = \mathbb{C}$. Since every complex number can be uniquely expressed by $a + bi$ for $a, b \in \mathbb{R}$, we see that $(1, i)$ is a basis for $\mathbb{C}$ over $\mathbb{R}$, i.e. the dimension of $\mathbb{C}$ as a vector space over $\mathbb{R}$ is 2. Hence, there is no intermediary field between $\mathbb{R}$ and $\mathbb{C}$. By theorem, $\mathbb{C}$ is a simple extension. Indeed, $\mathbb{C} = \mathbb{R}(i)$, where $i \in \mathbb{C}$.

In this paper, we will give a proof of the Main Theorem and dig into possible applications. The structure of the paper is as follows. In Section 2 we give the definitions of extensions, extension degrees, and minimal polynomial, with examples. We also state necessary theorems, propositions, and lemmas. In Section 3 we elaborate on the proof of the Main Theorem. Finally, in Section 4, we focus on applications and some original examples.

Acknowledgements. I would like to thank professor Madeline Brandt for discussions and for insightful suggestions.

2. Background

We assume the reader is familiar with definitions of field and extension field as introduced in class as well as in [2, Chapter 20]. Throughout, it is expected that the reader has preliminary knowledge of abstract algebra.

Given a field F and an extension E over F. The primary theorem addresses the conditions under which F is considered a simple extension of E. Before investigating further, let's define terms and provide necessary building blocks.

Definition 2.1. Let E be an extension field of a field F and let $a \in E$. We call a *algebraic over* F if a is the zero of some nonzero polynomial in $F[x]$. Otherwise a is *transcendental over* F.

We now give one example to each type of the element.

Example 2.2. Let $F = \mathbb{Q}$ and $E = \mathbb{R}$. $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ as it is the zero of $x^2 - 2 \in \mathbb{Q}[x]$.

Example 2.3. Let $F = \mathbb{Q}$ and $E = \mathbb{C}$. π (Lindemann, 1882 [4]) and e (Hermite, 1873 [3]) are proved to be transcendental over $\mathbb{Q}$.

Definition 2.4. An extension E of F is called an *algebraic extension* of F if every element of E is algebraic over F. Otherwise, E is called a *transcendental extension* of F. Furthermore, E is called a *simple extension* of F if $\exists\ a \in E$ such that $E = F(a)$. Such a is a *primitive element* defined after the Main Theorem.

Example 2.5. $\mathbb{Q}(\sqrt{5}) = \{s + \sqrt{5}t | s, t \in \mathbb{Q}\}$ is an extension field, specifically a simple extension field, over $\mathbb{Q}$ as $\forall\ s + \sqrt{5}t$ is a zero of $x^2 - 2sx + s^2 - 5t^2 \in \mathbb{Q}[x]$. $\mathbb{R}$ and $\mathbb{C}$ are transcendental extensions of $\mathbb{Q}$.

Theorem 2.6 (as stated in Thm 21.2 [2]). *If a is algebraic over a field F, then there is a unique monic irreducible polynomial $p(x)$ in $F[x]$ such that $p(a) = 0$.*

Example 2.7. Following example 2.2, $p(x) = x^2 - 2 = 0$ for $x = \sqrt{2}$. $p(x)$ is unique by theorem 2.6.

Definition 2.8. Such polynomial mentioned in theorem 2.6 is the *minimal polynomial for a over* F.

Definition 2.9. Let E be an extension field of a field F. We say that E has degree n over F and write $[E : F] = n$ if E has dimension n as a vector space over F. If $[E : F]$ is finite, E is called a *finite extension* of F; otherwise, we say that E is an *infinite extension* of F.

Example 2.10. We first refer to a result stated in Thm 20.3 [2]:
Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F, then $F(a)$ is isomorphic to $F(x)/\langle p(x)\rangle$. Furthermore, if $deg\ p(x) = n$, then every member of $F(a)$ can be uniquely expressed in the form

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0,$$

where $c_0, c_1, \ldots, c_{n-1} \in F$.
Now, let a be algebraic over F. By theorem 2.6, there is a unique minimal polynomial for a over F. From the result above, we know that $\{1, a, \ldots, a^{n-1}\}$ is a basis for $F(a)$ over F. Thus, $[F(a) : F] = n$. On the other hand, $\mathbb{C}$ is an infinite extension of $\mathbb{Q}$.

Theorem 2.11 (as stated in Thm 21.4 [2]). *If E is a finite extension of F, then E is an algebraic extension of F.*

Proposition 2.12. *([8, p.18]) Suppose K/F is a finite-degree extension and F is finite. Then K is a simple extension of F.*

Theorem 2.13 (as stated in Thm 21.3 [2]). *Let a be algebraic over F, and let $p(x)$ be the minimal polynomial for a over F. If $f(x) \in F[x]$ and $f(a) = 0$, then $p(x)$ divides $f(x)$ in $F[x]$.*

Lemma 2.14 ([5]). *Let $m(x)$ be the minimal polynomial of α over F. Then $\deg_F(\alpha) = \deg(m(x)) = [F(\alpha) : F]$.*

3. Main Theorem

Now that we have introduced all necessary definitions and related theorems, we are ready to prove the Main Theorem.

Main Theorem. *Primitive Element Theorem (Steinitz, 1910 [7])*
Let F and K be arbitrary fields, and let K be an extension of F of finite degree. Then there exists an element $\alpha \in K$ such that $K = F(\alpha)$ if and only if there are finitely many fields L with $F \subseteq L \subseteq K$.

We follow the proof given in [6].

Proof. Let F be a field and K an extension over K such that $[K : F]$ is finite.

$\Rightarrow$:

Suppose $K = F(\alpha)$ for some $\alpha \in K$ and L is an intermediary field of K/F. K is a finite extension, so L is also a finite extension. By theorem 2.11, K, L are algebraic extensions. Therefore, by theorem 2.6, α has the minimal polynomial $m(x) \in F[x]$ and $m'(x) \in L[x]$. Now, $m'(x)$ is the minimal polynomial for α over L and $m(x) \in F[x] \subseteq L[x]$ with $m(\alpha) = 0$. By theorem 2.13, $m'(x) \mid m(x)$ in $L[x]$.

Now let L' be the field generated over F by the coefficients of $m'(x)$. Then $L' \subseteq L$, and the minimal polynomial for α over L' is still $m'(x)$. Therefore, by lemma 2.14,

$$[K : L] = \deg(m'(x)) = [K : L']$$

Together with $L' \subseteq L$, which we've shown above, this implies that $L' = L$. Now, every intermediary field is generated over F by the coefficients of some monic polynomial dividing $m(x)$. Since the polynomial $m(x)$ has only finitely many monic factors, we conclude that there can be only finitely many subfields of K containing F.

$\Leftarrow$

Suppose K/F has finite degree and finitely many intermediary fields. If F is finite, then by proposition 2.12, K is a simple extension of F. Thus, assume F (and hence also K) is infinite. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be a basis for K over F. Then $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$. We will demonstrate the implication via induction.

Base case: $K = F(\varepsilon)$ for $\varepsilon \in K$ is a simple extension by definition.
Inductive step: $\forall\ K = F(\alpha_1, \dots, \alpha_i, \beta, \gamma) : \exists \varepsilon \in K$ such that $K = F(\alpha_1, \dots, \alpha_i, \varepsilon)$
Assume $K' = F(\alpha_1, \dots, \alpha_i, \beta + x\gamma)$ for $\forall x \in F$: since F is infinite and there are only finitely many

intermediate fields, $\exists$ distinct $x, y \in F$ such that $F(\alpha_1, \ldots, \alpha_i, \beta + x\gamma) = F(\alpha_1, \ldots, \alpha_i, \beta + y\gamma)$. Call this field L. Then $L \subseteq F(\alpha_1, \ldots, \alpha_i, \beta, \gamma)$. Now $\beta + x\gamma, \beta + y\gamma \in L \Rightarrow (\beta + x\gamma) - (\beta + y\gamma) = (x - y)\gamma \in L$. As $x \neq y$, $x - y$ has its multiplicative inverse in L, so $\gamma = (x - y)^{-1}(x - y)\gamma \in L$. Clearly also, $\beta = (\beta + x\gamma) - x\gamma \in L$. Thus, $F(\alpha_1, \ldots, \alpha_i, \beta, \gamma) \subseteq L \Rightarrow L = F(\alpha_1, \ldots, \alpha_i, \beta, \gamma)$. Now letting $\varepsilon = \beta + x\gamma$, we see that

$$K' = F(\alpha_1, \ldots, \alpha_i, \varepsilon) = L = F(\alpha_1, \ldots, \alpha_i, \beta, \gamma) = K$$

Therefore, the theorem holds. □

4. Applications and Examples

The Main Theorem has implications in Algebraic Number Theory, Coding Theory and Cryptography, etc. It also helps with solving polynomials and is essential in Galois Theory. In addition, it gives birth to the following corollary:

Corollary 4.1 (as stated in Thm 21.6 [2]). *If F is a field of characteristic 0, and a and b are algebraic over F, then there is an element c in $F(a, b)$ such that $F(a, b) = F(c)$.*

We now see an example illustrating this result.

Original Example. Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ for $a, b \in \mathbb{Z}$, $a \neq b$. $\mathbb{Q}$ is a field of characteristic 0, and $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ is a field extension of degree 4, with $\{1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\}$ being the basis of the vector space. Meanwhile, consider $x^2 - a = 0$ and $x^2 - b = 0$. $\sqrt{a}, \sqrt{b}$ are algebraic over F. Then, by the corollary, there is an element c in $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ such that $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(c)$.
Claim that $c = \sqrt{a} + \sqrt{b}$. Then $\mathbb{Q}(c) \subseteq \mathbb{Q}(\sqrt{a}, \sqrt{b})$, and $c^2 = a + b + 2\sqrt{ab}$, $c^3 = a\sqrt{a} + 3b\sqrt{a} + 3a\sqrt{b} + b\sqrt{b}$. Solving the linear equations, we know that

$$\sqrt{a} = \frac{1}{2b - 2a}(c^3 - (3a + b)c)$$
$$\sqrt{b} = \frac{1}{2a - 2b}(c^3 - (a + 3b)c)$$

This further implies that $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \subseteq \mathbb{Q}(c)$, so $E = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

The following is an example for the finite field. Finite field has nonzero characteristic, so we refer to the Main Theorem.

Original Example. Let $F = GF(2) = \mathbb{Z}/2 = \{0, 1\}$ with addition and multiplication defined as follows:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Let $E = GF(8) = \mathbb{F}_2[x]/p(x) = \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$ with operations defined by addition/multiplication modulo $p(x)$, where $p(x) = x^3 + x + 1$ is an irreducible polynomial in $\mathbb{Z}_2[x]$. Readers may check on their own that this is indeed a field. Since E is finite, there must be finite number of intermediary fields between F and E. Now, by the Main Theorem, E is simple. Indeed, we claim that $E = F(x)$ because $\forall e \in GF(8) \setminus GF(2)$: e is a polynomial generated by only 1 and x.

Finally we provide a nonexample [1]. It fails because there are infinitely many intermediary fields.

Example 4.2. Consider $K = \mathbb{F}_p(x, y)$, the field of rational functions in x, y over the finite field with p elements, and the extension $L = K(x^{\frac{1}{p}}, y^{\frac{1}{p}})$. An infinite number of intermediary fields can be given by $K(ax^{\frac{1}{p}} + y^{\frac{1}{p}})$ for $\forall a \in K$. This can be proven true by contradiction. Suppose $L' = K(ax^{\frac{1}{p}} + y^{\frac{1}{p}}) = K(bx^{\frac{1}{p}} + y^{\frac{1}{p}})$ for $a, b \in K$ and $a \neq b$. Then, $(a-b)x^{\frac{1}{p}} \in L' \Rightarrow (a-b)^{-1}(a-b)x^{\frac{1}{p}} = x^{\frac{1}{p}} \in L'$, and also $y^{\frac{1}{p}} \in L$. Thus, $L' = K(x^{\frac{1}{p}}, y^{\frac{1}{p}}) = L$, so $ax^{\frac{1}{p}} + y^{\frac{1}{p}}$ is a primitive element, which can't be true.

Now by the Main Theorem, L can't be a simple extension. Indeed, L is an extension of degree p^2 over K, so if it were simple, there must exist an element of degree p^2. However, $\forall \alpha \in L$: $\alpha^p \in K$, i.e. there is no primitive element.

References

[1] https://math.stackexchange.com/questions/118830/a-problem-on-field-extension. Accessed: 2023-05-09.

[2] J. Gallian. 10650 Toebben Drive, Independence, KY 41051, 7th ed. 2010 edition.

[3] C. Hermite. *Œuvres de Charles Hermite: publiées sous les auspices de l'Académie des sciences*, volume 1. Gauthier-Villars, 1905.

[4] F. Lindemann. Über die zahl π. In *Pi: A Source Book*. 1882.

[5] U. of California Irvine. Extension fields. Accessed: 2023-05-09.

[6] PlanetMath. Proof of primitive element theorem, 2013. Accessed: 2023-05-05.

[7] E. Steinitz. Algebraische theorie der körper. 1910.

[8] N. University. Finite fields, primitive elements, and composite extensions. Accessed: 2023-05-10.

Department of Mathematics, Brown University, Providence, RI 02912
Email address: matianyu_zang@brown.edu