A brief exposition on the Primitive Element Theorem

Christian Lentz

Abstract

In this project, I will study and prove the Primitive Element Theorem (PET), including a brief exposition regarding the history of the theorem. Following this, I will consider problem 7 in Section 8.2 of [3]. Finally, I will extend this example to an illustrative discussion of Galois Theory and Algebraic Number Theory. In particular, Galois groups are often introduced as they naturally arise from the study of the roots of a single polynomial. Using this, we can make concrete statements regarding the solvability by radicals of polynomials based on the structure of their associated Galois groups. Conversely, given a finite Galois (i.e. normal and separable) extension $\mathbb{F}/\mathbb{K}$, my discussion will describe how the PET can be used to reduce the study of $\mathbf{Gal}(\mathbb{F}/\mathbb{K})$ to the study of a subset of the roots of a single polynomial over $\mathbb{K}$.

1 Introduction

The primitive element theorem is intimately connected to the development of Galois Theory. Indeed, the first formulation of the theorem appeared in Èvariste Glaois' first memoir of 1831, which was published in 1846. An english translation is available at [5]. However, Galois' formulation of the proof was incomplete, and restricted to splitting fields over $\mathbb{Q}$. The generalized formulation of the PET is due to German mathematician Ernst Steinitz [9], who published the proof in 1910 together with *Steinitz's Theorem*. Interestingly, Emil Artin's reformulation of Galois Theory in [2] does not require the notion of primitive elements.

2 Preliminaries

For the sake of expediting this exposition, we will take standard definitions and concepts in ring and field theory to be given, and will only provide background absolutely essential for stating and proving the PET. We will adopt standard convention by calling $\mathbb{F}$ the *extension* of a base field $\mathbb{K}$ and writing $\mathbb{F}/\mathbb{K}$ to denote the extension. Write $\mathbb{E} = \mathbb{K}(u_1, \ldots, u_n)$ to denote the smallest subfield of $\mathbb{F}$ that contains $\mathbb{K}$ and the elements $u_1, \ldots, u_n \in \mathbb{F}$. In words, $\mathbb{E}$ is the extension of $\mathbb{K}$ generated by $u_1, \ldots, u_n \in \mathbb{F}$. In the case that $\mathbb{E} = \mathbb{K}(u)$ for a single $u \in \mathbb{F}$ then $\mathbb{E}$ is called a *simple extension* of $\mathbb{K}$.

Definition 1 *(Algebraic Elements and Extensions). An element $u \in \mathbb{F}$ is called **algebraic over** $\mathbb{K}$ if there exists $f(x) \in \mathbb{K}[x]$ such that $f(u) = 0$. The extension $\mathbb{F}$ is called an **algebraic extension** of $\mathbb{K}$ if each $u \in \mathbb{F}$ is algebraic over $\mathbb{K}$.*

We have the following proposition, which which will be a foundational concept in the present work.

Proposition 1 *Let $u \in \mathbb{F}$ be algebraic over base field $\mathbb{K}$. Then there exists a unique monic and irreducible polynomial $p(x) \in \mathbb{K}[x]$ such that $p(u) = 0$, and we call $p(x)$ the **minimal polynomial** of u over $\mathbb{K}$.*

Proof. First, define the set

$$I = \{f(x) \in \mathbb{K}[x] : f(u) = 0\} \subset \mathbb{K}[x].$$

Observe that for any $f(x), g(x) \in I$ we have $f(u) + g(u) = 0$, implying that $f(x) + g(x) \in I$. Furthermore, for any additional polynomial $h(x) \in \mathbb{K}[x]$ we have $h(u)f(u) = h(u) \cdot 0 = 0$. So I is an ideal of $\mathbb{K}[x]$, which is a principal ideal domain (PID). Thus, I is principally generated and we can write $I = \langle p(x) \rangle$ for a nontrivial polynomial $p(x) \in \mathbb{K}[x]$ of minimal degree. Now, take $f(x), g(x) \in K[x]$. Since $\mathbb{K}[x]$ is a PID, it follows that anytime $f(x)g(x) \in I$, we must have $f(u) = 0$ or $g(u) = 0$, otherwise one of the two would be zero and a zero divisor. Thus, I must but a prime ideal of a PID, making it a maximal ideal of $\mathbb{K}[x]$. Appealing to proposition 5.3.9 of [3], then it must be the case that the factor ring $\mathbb{K}[x]/\langle p(x) \rangle$ is a field, which is true if, and only if, $p(x)$ is irreducible over $\mathbb{K}$. Finally, by taking $p(x)$ to be the unique monic generator of I, this completes the proof. □

In fact, by taking the elements of $\mathbb{F}$ as vectors and those in $\mathbb{K}$ as scalars, then $\mathbb{F}$ is in fact a vector space over $\mathbb{K}$. In particular, the vector addition axioms follow from the abelian structure of the group $(\mathbb{F}, +)$, and the scalar multiplication axioms follow from the fact that $\mathbb{K}$ is a subfield of $\mathbb{F}$. Write $[\mathbb{F} : \mathbb{K}]$ to denote the dimension of $\mathbb{F}$ as a vector space over $\mathbb{K}$, and in words say that this is the *degree* of $\mathbb{F}$ over $\mathbb{K}$. In the case that $[\mathbb{F} : \mathbb{K}]$ is finite, then $\mathbb{F}$ is called a *finite extension* of $\mathbb{K}$. Introducing this vector space perspective of extension fields allows the proofs of the following propositions to be a simple linear-algebraic exercises.

Proposition 2 *Let $u \in \mathbb{F}$ have a minimal polynomial $p(x) \in \mathbb{K}[x]$ such that* ***deg*** *$p(x) = n$. It follows that $[\mathbb{K}(u) : \mathbb{K}] = n$.*

Proposition 3 *Let $u \in \mathbb{F}$ where $\mathbb{F}$ is a finite extension of $\mathbb{K}$. Then u is algebraic over $\mathbb{K}$.*

Thus, any finite extension is indeed algebraic. The converse of Proposition 3 is also true, but we only need the above for our exposition. We require one more definition to state the PET.

Definition 2 *(Separable Elements and Extensions). A polynomial $f(x) \in \mathbb{K}[x]$ is called* ***separable*** *if its irreducible factors have only simple roots. An element $u \in \mathbb{K}$ that is algebraic over $\mathbb{F}$ is called separable when its minimum polynomial is separable. An algebraic extension field $\mathbb{F}$ of $\mathbb{K}$ is called* ***separable over*** *$\mathbb{K}$ if each of its elements is separable.*

Theorem 4 *(Primitive Element Theorem). Let $\mathbb{F}$ be a finite extension of $\mathbb{K}$. If $\mathbb{F}$ is separable over $\mathbb{K}$, then $\mathbb{F}/\mathbb{K}$ is a simple extension.*

Finally, to prove the special case of Theorem 4 in which $\mathbb{K}$ is finite, we will recall the following fact of finite field theory. See Section 6.5 of [3] for a proof.

Lemma 5 *Any finite subgroup of a the multiplicative group of a field is cyclic.*

3 Proving the PET

The proof outlined here will follow a standard pattern (c.f. [3, 7]). The case for finite $\mathbb{K}$ is handled easily via Lemma 5, although we will explicitly walk through this below. For the infinite case, assume that for $\alpha, \beta \in \mathbb{F}$ we have $\mathbb{F} = \mathbb{K}(\alpha, \beta)$. Following this assumption, we may utilize the fact that $\mathbb{F}/\mathbb{K}$ is a separable extension to observe that the minimum polynomials of u and v each have unique roots. Leveraging this fact, we construct a single primitive element for the extension. Note that this is enough to conclude the proof by observing that we can extend this result inductively by taking the above to be our base case and then writing

$$\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_r) = \mathbb{K}(\beta_m, \alpha_{m+1}, \ldots, \alpha_r) = \ldots$$

where β_m is a primitive element for the extension generated by adjoining $\alpha_1, \ldots, \alpha_m$. In other words, the field extension $\mathbb{K}(\beta_m, \alpha_{m+1}, \ldots, \alpha_r)$ is constructed via iteratively applying the base case, and eventually we are left with an extension generated by a single element, β_r.

3.1 Finite Fields

For now, take $\mathbb{K}$ to be finite and let $\mathbb{F}$ be a finite extension of $\mathbb{K}$ such that $|\mathbb{F}| = n + 1$. Thus, $\mathbb{F}$ is also finite and it follows from Lemma 5 that the units $\mathbb{F}^{\times}$ give a cyclic group $(\mathbb{F}^{\times}, \times) = \langle \alpha \rangle$ of order n under the multiplication on $\mathbb{F}$. To proceed, we will show that $\mathbb{F} = \mathbb{K}(\alpha)$ by showing that the subset relationship holds in either direction. The case for the zero element is trivial. Additionally, it follows by definition that $\mathbb{K}(\alpha)$ is the smallest subfield of $\mathbb{F}$ which contains the elements of $\mathbb{K}$ and α, so the only work here is to show that $\mathbb{F} \subseteq \mathbb{K}(\alpha)$. Suppose that $\gamma \in \mathbb{F}$. Then we can write $\gamma = \alpha^m$ for some $m \leqslant n$. But $\alpha \in \mathbb{K}(\alpha)$, so we must have $\gamma = \alpha^m \in \mathbb{K}(\alpha)$. Thus, $\mathbb{F} \subseteq \mathbb{K}(\alpha)$, which completes the proof for the finite case.

3.2 Infinite Fields

Let $\mathbb{F} = \mathbb{K}(\alpha, \beta)$ and $f(x), g(x) \in \mathbb{K}[x]$ the minimum polynomials for α and β with degrees m and n respectively. Additionally, let $\mathbb{E}$ be an extension of $\mathbb{F}$ such that $f(x), g(x)$ both split over $\mathbb{E}$. Since the extension $\mathbb{F}/\mathbb{K}$ is separable by assumption, then the roots $\alpha_1, \ldots, \alpha_m \in \mathbb{E}$ and $\beta_1, \ldots, \beta_n \in \mathbb{E}$ of, respectively, $f(x)$ and $g(x)$, are distinct. Note that we must have α as a root of $f(x)$ and β as a root of $g(x)$ by definition. Without loss of generality, we will assume that $\alpha_1 = \alpha$ and $\beta_1 = \beta$. Now define the linear function

$$\alpha_i + \beta_j x = \alpha + \beta x.$$

Observe that taking $j = 1$ will not admit unique solutions since it reduces the above to

$$\alpha_i - \alpha = (\beta - \beta)x = 0 \cdot x.$$

For instance, fix $x = 1$ and choose any $x \in \mathbb{E}$. On the other hand, by choosing $j \neq 1$, the above will admit a unique solution of the form

$$x = \frac{\alpha - \alpha_i}{\beta_j - \beta} \in \mathbb{E}.$$

Since $\mathbb{K}$ is infinite and there are finitely many α_i and β_j, there must exist $c \in \mathbb{K}$ such that $\alpha + \beta c \neq \alpha_i + \beta_j c$ for all i and each $j \neq 1$. Now consider the element $t = \alpha + \beta c \in \mathbb{E}$. It is immediate that $\mathbb{K}(t) \subseteq \mathbb{K}(\alpha, \beta)$ since $c \in \mathbb{K}$ and $\alpha, \beta \in \mathbb{K}(\alpha, \beta)$. Thus, it will be enough to conclude the proof by showing that $\mathbb{K}(\alpha, \beta) \subseteq \mathbb{K}(t)$.

To proceed, we define $h(x) = f(t - cx) \in \mathbb{K}(t)[x]$ and let $p(x)$ be the minimal polynomial of β over $\mathbb{K}(t)$. By construction, we have that

$$h(\beta) = f(\alpha + \beta c - \beta c) = f(\alpha) = 0.$$

Since $g(\beta) = 0$ by assumption as well and $p(x)$ has minimal degree, then it must be the case that $p(x)$ is a common divisor of both $h(x)$ and $g(x)$ over the field

$\mathbb{K}(t)$. However, we chose c such that $\alpha + \beta c \neq \alpha_i + \beta_j c$ unless $i = j = 1$. Thus, it follows that β is indeed the only root that $h(x)$ and $g(x)$ share over the extension $\mathbb{E}$ as well, implying that we have $\gcd(h(x), g(x)) = x - \beta$. But since $p(x)$ is a common divisor of the two over a subfield of $\mathbb{E}$, then it must also divide the two over $\mathbb{E}$. Thus, $p(x)$ can have degree no larger than that of the linear factor $x - \beta$. This implies that $\deg(p(x)) = 1$, so by Proposition 2 we have

$$[\mathbb{K}(t, \beta) : \mathbb{K}(t)] = 1 \Rightarrow \beta \in \mathbb{K}(t).$$

Finally, as $c \in \mathbb{K}$ then it follows that

$$c\beta \in \mathbb{K}(t) \Rightarrow t + c\beta = \alpha \in \mathbb{K}(t).$$

Hence, $\mathbb{K}(\alpha, \beta) \subseteq \mathbb{K}(t)$, which completes the proof.

3.3 A modified formulation

The statement of the PET can be relaxed as follows.

Claim 1 *Let $\mathbb{F} = \mathbb{K}(\alpha_1, \ldots, \alpha_r)$ be a finite extension of $\mathbb{K}$ and assume that α_i are separable over $\mathbb{K}$ for $i \neq 1$. Then $\mathbb{F}/\mathbb{K}$ is a finite extension.*

The distinction here is that we do not take α_1 to have a minimal polynomial that is separable, and hence we do not require that the extension field is separable either. This statement allows $\mathbb{F}$ to satisfy milder assumptions when compared to the form of the theorem previously stated. In particular, this recognizes that $\mathbb{K}(\alpha_1)$ is simple by definition, so we do not require the separability assumption for that single element.

4 Computing a primitive element

Although the proof of PET is not explicitly constructive, it does provide useful intuition for how to construct a primitive element. Extending the above result inductively, we see that a primitive element of the finite extension $\mathbb{F} = \mathbb{K}(\alpha_1, \ldots, \alpha_r)$ can be chosen to be a linear combination of the form $c_1\alpha_1 + \cdots + c_r\alpha_r$ for $c_i \in \mathbb{K}$. However, determining the c_i is not immediate (c.f. Example 1). As is noted in [6], if $\mathbb{F}$ is a Galois extension of $\mathbb{K}$, then an element of this form is primitive if each non-identity automorphism of $\mathbf{Gal}(\mathbb{F}/\mathbb{K})$ moves it.

Example 1 *For $\omega = (-1+\sqrt{3}\cdot i)/2$ being the primitive cubed root unity, then we have $\mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(\omega + \sqrt[3]{2})$.*

To show that the above claim holds, we can first start by noting that each extension over $\mathbb{Q}$ is of the same degree. Hence, by methods of linear algebra, we can see immediately the the two extension are, at very least, isomorphic as vector spaces over $\mathbb{Q}$. Computing the characteristic polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ we obtain

$$x = \sqrt[3]{2} \iff x^3 - 2 = 0,$$

which is irreducible via Eisenstein's Criterion. Similarly, for ω over $\mathbb{Q}(\sqrt[3]{2})$ we have

$$(-1 + \sqrt{3} \cdot i)/2 = x \iff \left(\frac{2x+1}{i}\right)^2 - 3 = 0.$$

Expanding, we obtain a minimal polynomial $-4x^2 - 4x - 4$ and a simple application of the quadratic formula reveals that its roots are $x = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$, which lie in $\mathbb{C}$. As both minimal polynomials are irreducible, then the tower law and Proposition 2 imply that

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

Hence, a basis for this vector space over $\mathbb{Q}$ is

$$\mathcal{B} = \{1, \omega, \sqrt[3]{2}, \omega\sqrt[3]{2}, \sqrt[3]{4}, \omega\sqrt[3]{4}\}.$$

On the other hand, determining a minimal polynomial for $\omega + \sqrt[3]{2}$ proceeds as follows by letting $x = \omega + \sqrt[3]{2}$ and writing:

$$\begin{aligned} x &= (-1 + \sqrt{3} \cdot i)/2 + \sqrt[3]{2} \\ x &= -\frac{1}{2} + \frac{\sqrt{3}}{2}i + \sqrt[3]{2} \\ 2 &= \left(x + \frac{1}{2} - \frac{\sqrt{3}}{2}i\right)^3 \end{aligned}$$

Expanding and collecting the single term with an irrational coefficient yields:

$$\begin{aligned} \frac{2}{3}x^3 + x^2 - x - 2 &= i\sqrt{3} \cdot (x+1)x \\ \left(\frac{2}{3}x^3 + x^2 - x - 2\right)^2 &= -3x^2(x+1)^2 \end{aligned}$$

While this is certainly not a nice closed form, it is enough to determine that

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

and since this extension is simple, we obtain a basis

$$\{(\omega + \sqrt[3]{2})^k\}_{k=0}^5.$$

It is enough to conclude by showing that these bases generate the exact same vector space. In particular, we can express each power of $\omega + \sqrt[3]{2}$ in terms of the basis $\mathcal{B}$. To do so, we compute

$$\begin{aligned} (\omega + \sqrt[3]{2})^0 &= 1 \\ (\omega + \sqrt[3]{2})^1 &= \omega + \sqrt[3]{2} \\ (\omega + \sqrt[3]{2})^2 &= 1 - \omega + 2\omega\sqrt[3]{2} + \sqrt[3]{4} \\ (\omega + \sqrt[3]{2})^3 &= 3 - \sqrt[3]{2} - 3\omega\sqrt[3]{2} + 3\omega\sqrt[3]{4} \\ (\omega + \sqrt[3]{2})^4 &= 9\omega + 6\sqrt[3]{2} - 6\sqrt[3]{4} - 6\omega\sqrt[3]{4} \\ (\omega + \sqrt[3]{2})^5 &= -21 - 21\omega + 15\omega\sqrt[3]{2} + 12\sqrt[3]{4} \end{aligned}$$

which yields a coefficient matrix

$$\begin{pmatrix} 1 & \cdot & -1 & 3 & \cdot & -21 \\ \cdot & 1 & -1 & \cdot & 9 & -21 \\ \cdot & 1 & \cdot & -1 & 6 & \cdot \\ \cdot & \cdot & 2 & -3 & \cdot & 15 \\ \cdot & \cdot & 1 & \cdot & -6 & 12 \\ \cdot & \cdot & \cdot & 3 & -6 & \cdot \end{pmatrix}$$

where powers of $\omega + \sqrt[3]{2}$ ascend with column index and elements of the basis $\mathcal{B}$ ascend with row index. This matrix is invertible. For instance, one can compute with code that its determinant is nonzero. This completes the proof of the claim.

5 Number Fields

In this course, our discussion of the topics addressed in this exposition were primarily employed for the development of Galois theory, and in particular to study the roots of polynomials with coefficients in $\mathbb{Q}$. However, it is natural to wonder whether this process can be reversed. In other words, given a finite Galois extension $\mathbb{F} = \mathbb{K}(\alpha_1, \ldots, \alpha_r)$ of $\mathbb{K}$, what information can one learn about $\mathbb{F}/\mathbb{K}$ using Galois Theory?

Indeed, the primary focus of Algebraic Number Theory [7, 8] is to study arithmetic in so-called **Number Fields**, or finite extensions of $\mathbb{Q}$. In fact, the PET provides a natural way to characterize number fields in terms of a single element and/or polynomial. For instance, taking the example from the previous section, Algebraic Number Theory provides tools to understand arithmetic in $\mathbb{Q}(\omega, \sqrt[3]{2})$ by understanding properties of the minimal polynomial of $t = \omega + \sqrt[3]{2}$. This works since t is guaranteed to be algebraic over $\mathbb{K}$ when the finite extension is Galois. Furthermore, it is natural to employ Galois Theory for this task since we have reduced the study of a Galois extension $\mathbb{F}/\mathbb{K}$ to the study of a single polynomial which has roots in $\mathbb{F}$.

6 Concluding Remarks

We have proven the PET for the case of finite and infinite fields. Following this, we exemplified how one may compute the primitive element of a finite extension. Finally, we motivated the foundational role that the PET plays in Algebraic Number Theory. The style file for this paper was modified from the Canadian Conference on Computation Geometry available at [1]. The style file for the associated presentation is due to Professor Lori Ziegelmeier of Macalester College. The content covered in this project was inspired from this summer research internship at MIT [4].

References

[1] Canadian conference on computation geometry. https://sites.google.com/view/cccgwads-2025/cccg-2025. Accessed: 2025-12-17.

[2] Emil Artin and Arthur Norton Milgram. *Galois theory*, volume 2. Courier Corporation, 1998.

[3] John A Beachy and William D Blair. *Abstract algebra*. Waveland Press, 2019.

[4] Xavier Choe and Garima Rastogi. Number fields and galois theory. https://math.mit.edu/research/highschool/primes/circle/documents/2021/Choe$_R$astogi.pdf.*Accessed* : $2025 - 12 - 07$.

[5] Évariste Galois and Peter M Neumann. *The mathematical writings of Évariste Galois*, volume 6. European mathematical society, 2011.

[6] James S. Milne. Fields and galois theory (v4.30), 2012. Available at www.jmilne.org/math/.

[7] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[8] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[9] Ernst Steinitz. Algebraische theorie der körper. 1910.