Proceedings of the 4th International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/108/2025.22648

A Method of Finding Irreducible Polynomials

Xiangyue Cheng

Kimball Union Academy, Meriden, USA
chengx25@kua.org

Abstract: This paper introduces a simplified approach to finding irreducible polynomials, a fundamental concept in abstract algebra crucial for understanding field and ring structures. Traditionally, identifying these polynomials involves complex computations or heuristic methods. Our study presents a straightforward method by constructing and proving the integrality of the polynomial roots, bridging advanced and elementary mathematical principles. The proposed method utilizes Vieta's formulas and roots of unity to systematically construct potential roots of an element's irreducible polynomial across various fields. We provide elementary proofs using induction and polynomial properties, demonstrating the method's effectiveness through examples in both rational and finite fields.

Keywords: Irreducible Polynomials, Abstract Algebra, Vieta's Formulas, Field Extensions

1. Introduction

In Michael Artin's classic textbook *Algebra*, he gives two ways of finding irreducible polynomials. One is to find a linear dependence relation of an element γ. If we can find a linear dependence relation $c_n\gamma^n + c_{n-1}\gamma^{n-1} + \cdots + c_1\gamma + c_0 = 0$, then function $c_nx^n + c_{n-1}x^{n-1} + \cdots + c_1 + c_0$ is the irreducible polynomial of γ. The second method is to "guess" the roots [1]. For example, given an element $\alpha = \sqrt{2} + \sqrt{3}$, we can guess the four roots of the irreducible polynomial are $\sqrt{2} + \sqrt{3}$, $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$, $-\sqrt{2} - \sqrt{3}$. Thus, the irreducible polynomial is $[x - (\sqrt{2} + \sqrt{3})][(x - (\sqrt{2} - \sqrt{3})][x - (-\sqrt{2} + \sqrt{3})][x - (-\sqrt{2} - \sqrt{3})] = x^4 - 10x^2 + 1$. Building upon these foundational methods, this paper aims to generalize and refine the technique of "guessing" roots to accommodate any linear combinations of roots such as $\sqrt[n_1]{m_1}, \sqrt[n_2]{m_2}, \cdots, \sqrt[n_k]{m_k}$, where n_k, m_k are positive integers. This generalization proposes a systematic method to not only predict but also verify all possible roots of the irreducible polynomial associated with complex algebraic combinations.

To extend the practicality of Artin's methods, this paper introduces an algebraic framework that leverages the properties of roots of unity and the symmetric nature of polynomials. By systematically constructing a set of potential roots and then proving their validity through algebraic manipulation and elementary proofs, we can apply this refined method to a broader class of elements. This approach not only simplifies the process of identifying irreducible polynomials but also enhances our understanding of their structural characteristics and their role in algebraic number theory and field extension studies.

This paper is structured to guide the reader through a progressive understanding of our methodology and findings. Initially, we review existing methods in the literature, grounding our approach within the broader field of algebra. We then describe our novel approach in detail,

DOI: 10.54254/2753-8818/108/2025.22648

illustrating the theoretical underpinnings and practical steps involved in constructing irreducible polynomials. Subsequent sections provide empirical validations through examples, discuss the broader implications of our findings, and conclude with a summary of the contributions and potential future directions for this line of research.

2. Literature review

An irreducible polynomial is defined as a polynomial that cannot be factored over a given field, meaning it cannot be expressed as a product of two or more non-constant polynomials within that field. For instance, $x^2 - 2$ is irreducible in the rational number field. Irreducible polynomials play a crucial role in number theory, particularly in constructing field extensions, generating prime numbers, and exploring algebraic properties of number systems [2].

The study of irreducible polynomials has evolved considerably, with numerous methods developed to identify them effectively. One classic approach is through algorithms based on number theory, as discussed by Shoup [3], who presented novel techniques for finding irreducible polynomials over finite fields. These methods often involve complex computations that rely on properties of finite fields, Galois theory, and probabilistic approaches to test irreducibility [4]. These algorithmic methods are foundational in computational algebra systems and have widespread applications in coding theory and cryptography [5].

Another approach to irreducibility involves leveraging properties of symmetric polynomials and field extensions. Michael Artin, in his book "Algebra," outlines a more elementary way of finding irreducible polynomials using linear dependence relations of an element and "guessing" the roots of the polynomials. Artin's approach, while not algorithmic, highlights the relationship between elementary algebraic manipulation and advanced algebraic structures, making the subject more accessible to learners of different levels. This paper builds on Artin's methods by generalizing the "guessing" approach into a more systematic framework applicable to broader classes of algebraic elements.

Vieta's formulas provide another key tool in identifying irreducible polynomials by establishing relationships between polynomial roots and coefficients. Vieta's formulas help determine the conditions under which a polynomial is irreducible by evaluating the integrality of constructed roots. Previous research has highlighted the significance of Vieta's relations in understanding symmetric functions and field properties [6]. Symmetric polynomials, as described by Macdonald [7], also play a crucial role in analyzing the structure of polynomials and their factorization, particularly in the context of field extensions. Moreover, Stewart explored various properties of field extensions and their relationship to the structure of polynomials, illustrating the theoretical importance of Vieta's formulas in understanding polynomial behavior [8].

3. Methodology

For any given element $\alpha = \sqrt[n_1]{m_1} + \sqrt[n_2]{m_2} + \cdots + \sqrt[n_k]{m_k}$, where n_k, m_k are positive integers, one root of the irreducible polynomial is the addition of one term from every following group:
$\{\sqrt[n_1]{m_1}, \sqrt[n_1]{m_1}\omega_1, \sqrt[n_1]{m_1}{\omega_1}^2, \cdots, \sqrt[n_1]{m_1}{\omega_1}^{n_1-1}\}, \{\sqrt[n_2]{m_2}, \sqrt[n_2]{m_2}\omega_2, \sqrt[n_2]{m_2}{\omega_2}^2, \cdots, \sqrt[n_2]{m_2}{\omega_2}^{n_2-1}\}$, $\{\sqrt[n_3]{m_3}, \sqrt[n_3]{m_3}\omega_3, \sqrt[n_3]{m_3}{\omega_3}^2, \cdots, \sqrt[n_3]{m_3}{\omega_3}^{n_3-1}\}, \cdots, \{\sqrt[n_k]{m_k}, \sqrt[n_k]{m_k}\omega_k, \sqrt[n_k]{m_k}{\omega_k}^2, \cdots, \sqrt[n_k]{m_k}{\omega_k}^{n_k-1}\}$, where $\omega_k \; is \; n_k - th \; roots \; of \; unity$. Therefore, using product rule, there are $n_1 n_2 \cdots n_k$ roots in total. For example, considering an element $\beta = \sqrt{2} + \sqrt[3]{3}$, all the roots are all possible addition of one term from $\{\sqrt{2}, -\sqrt{2}\}$ and one term from $\{\sqrt[3]{3}\omega, \sqrt[3]{3}\omega^2, \sqrt[3]{3}\}$, where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. There are $\{\sqrt{2} + \sqrt[3]{3}\omega, \sqrt{2} + \sqrt[3]{3}\omega^2, \sqrt{2} + \sqrt[3]{3}, -\sqrt{2} + \sqrt[3]{3}\omega, -\sqrt{2} + \sqrt[3]{3}\omega^2, -\sqrt{2} + \sqrt[3]{3}\}$, six roots in total.

DOI: 10.54254/2753-8818/108/2025.22648

Next, we are going to prove that every polynomial like that is integral which is required for an irreducible polynomial. Let's prove by induction. First, we can verify if the element $\alpha = \sqrt[n]{m}$ only has one term, them the irreducible polynomial is $x^n - m$. Then if the element $\alpha = \sqrt[n_1]{m_1} + \sqrt[n_2]{m_2}$, first substitute $y_1 = x - \sqrt[n_1]{m_1}, y_2 = x - \sqrt[n_1]{m_1}\omega, \cdots, y_{n_1} = x - \sqrt[n_1]{m_1}\omega^{n_1-1}$, where ω is n_1 -th roots of unity. Thus, the polynomial becomes $({y_1}^{n_2} - m_2)({y_2}^{n_2} - m_2)\cdots({y_{n_1}}^{n_2} - m_2)$. To prove this polynomial is integral, we need to use Vieta's Theorem.

4. Vieta's theorem

According to Vieta's formulas [9, 10], for a polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, there are n roots: $r_1, r_2, \cdots, r_n$. They satisfy the following relationship:

$$1.\quad \sum_{1\le j\le n} r_j = -\frac{a_{n-1}}{a_n}$$

$$2.\quad \sum_{1\le i<j\le n} r_j r_i = \frac{a_{n-2}}{a_n}$$

$$\vdots$$

$$n.\quad r_1 r_2 \cdots r_n = (-1)^n \frac{a_0}{a_n}$$

If left-hand side is degree of n, we denote the sum S_n. If we rise power of every element in S_n *to power m, then we denote it as* S_n^m. *For example,* $\sum_{1\le i<j\le n} {r_i}^2 {r_j}^2 = S_2^2$. We know that if $a_n = 1$, then if $a_0, a_1, \cdots, a_{n-1}$ are all integers, $S_1, S_2, \cdots, S_n$ are integers. I am going to use Vieta's Formulas to prove that $({y_1}^{n_2} - m_2)({y_2}^{n_2} - m_2)\cdots({y_{n_1}}^{n_2} - m_2)$ in the last section is integral with respect to x.

5. Results and discussion

We can expand the polynomial $({y_1}^{n_2} - m_2)({y_2}^{n_2} - m_2)\cdots({y_{n_1}}^{n_2} - m_2) = S_{n_1}^{n_2} - m_2 S_{n_1-1}^{n_2} + {m_2}^2 S_{n_1-2}^{n_2} - {m_2}^3 S_{n_1-3}^{n_2} + \cdots + (-1)^{n_1}{m_2}^{n_1}$. To begin with, I will first prove $S_1, S_2, \cdots, S_{n_1}$ are integral polynomials with respect to x.

Let's introduce another variable δ and form a polynomial $(\delta - y_1)(\delta - y_2)(\delta - y_3)\cdots(\delta - y_{n_1})$, in which δ is considered as variable and $y_1, y_2, \cdots y_{n_1}$ are considered as constant. Expanding the polynomial, we find it's equal to $\delta^{n_1} - S_1\delta^{n_1-1} + S_2\delta^{n_1-2} - \cdots + (-1)^{n_1}S_n$. Recall that we could substitute $y_1, y_2, \cdots, y_{n_1}$ with x, so we can also write the polynomial $(\delta - y_1)(\delta - y_2)(\delta - y_3)\cdots(\delta - y_{n_1})$ *as* $[(\delta - x) + \sqrt[n_1]{m_1}][(\delta - x) + \sqrt[n_1]{m_1}\omega]\cdots[(\delta - x) + \sqrt[n_1]{m_1}\omega^{n_1-1}] = (\delta - x)^{n_1} + m_1$. Clearly, $(\delta - x)^{n_1} + m_1$ is integral polynomial with respect to x, so does $(\delta - y_1)(\delta - y_2)(\delta - y_3)\cdots(\delta - y_{n_1})$. Therefore, every coefficient of $(\delta - y_1)(\delta - y_2)(\delta - y_3)\cdots(\delta - y_{n_1})$ is integral polynomial with respect to x, so $S_1, S_2, \cdots, S_{n_1}$ are integral polynomials with respect to x.

Furthermore, I am going to prove that S_n^m is integral polynomial with respect to x given that S_n is integral. It is trivial using Newton's Identities. Therefore, we prove that $({y_1}^{n_2} - m_2)({y_2}^{n_2} - m_2)\cdots({y_{n_1}}^{n_2} - m_2)$ is integral polynomial with respect to x. For element $\alpha = \sqrt[n_1]{m_1} + \sqrt[n_2]{m_2} + \sqrt[n_3]{m_3}$, we could separate the first two radicals with the third, so the irreducible polynomial becomes

$$(y - \sqrt[n_3]{m_3})(y - \sqrt[n_3]{m_3}\omega)\cdots(y - \sqrt[n_3]{m_3}\omega^{n_3-1}),$$

whereω *is* $n_3 - th$ *roots of unity and y is the irreducible polynomial of* $\sqrt[n_1]{m_1} + \sqrt[n_2]{m_2}$. The polynomial equals to $y^{n_3} - m_3$. Since we have proven that y is integral polynomial with respect to

DOI: 10.54254/2753-8818/108/2025.22648

x, $y^{n_3} - m_3$ is also integral polynomial with respect to x. Using the same substitution, we could further prove that all polynomials we found using the method of constructing the roots are integral. Therefore, we prove that using our method, we could find irreducible polynomial.

6. Conclusion

This paper introduced a generalized approach for finding irreducible polynomials by extending Michael Artin's methods, utilizing a combination of polynomial root construction, Vieta's formulas, and roots of unity. Our results showed that this approach effectively generates irreducible polynomials for a wide range of algebraic elements, simplifying the identification process and bridging the gap between advanced abstract algebra and elementary mathematical techniques. Through elementary proofs and practical examples, we demonstrated the method's validity and its potential applicability across rational and finite fields.

However, the approach has some limitations, particularly when dealing with high-degree polynomials or more intricate algebraic elements, where calculations become increasingly complex. Future work could focus on optimizing computational efficiency for implementation in automated systems, which would be beneficial for applications in cryptography and coding theory. Additionally, further research could explore adapting the method for non-linear combinations or more complex algebraic structures, enhancing its versatility and expanding its applicability to broader mathematical contexts.

References

[1] *Artin, M. (2012). Algebra (2nd ed.). China Machine Press.*
[2] *Murty, M. R. (2002). Prime Numbers and Irreducible Polynomials. The American Mathematical Monthly, 109(5), 452–458. https://doi.org/10.2307/2695645*
[3] *Shoup, V. (1990). New Algorithms for Finding Irreducible Polynomials Over Finite Fields. Mathematics of Computation, 54(189), p.435. doi:https://doi.org/10.2307/2008704.*
[4] *Cohen, H. (2000). A course in computational algebraic number theory. Berlin: Springer.*
[5] *von and Gerhard, J. (2013). Modern Computer Algebra. Cambridge University Press.*
[6] *Lang, S. (2002). Algebra. Graduate texts in mathematics. Springer Nature. doi:https://doi.org/10.1007/978-1-4613-0041-0.*
[7] *Macdonald, I. G. (1998). Symmetric functions and Hall polynomials. Oxford university press.*
[8] *Stewart, I. (2022). Galois Theory. doi:https://doi.org/10.1201/9781003213949.*
[9] *Vieta's formulas. (2024). Wikipedia. https://en.wikipedia.org/wiki/Vieta%27s_formulas*
[10] *Valahas, T. and Boukas, A. (2011) 'On Vieta's formulas and the determination of a set of positive integers by their sum and product', Australian Senior Mathematics Journal. Adelaide, South Australia, Australia: Australian Asso ciation of Mathematics Teachers Inc, 25(2), pp. 55–62. https://search.informit.org/doi/10.3316/informit.59339953 1083782.*