Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 4055–4064
DOI : 10.47974/JDMSC-3031

Ideal structure of polynomial rings over finite fields

Jay Prakash Tiwari *
Department of Mathematics
Patel Group of Institutions
Indore 452020
Madhya Pradesh
India

D. Balaji †
Department of Humanities and Sciences (Mathematics Division)
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation (Deemed to be University)
Paiyanoor
Chennai 603104
Tamil Nadu
India

Swagat M. Karve §
Department of Electronics & Telecommunication Engineering
S B Patil College of Engineering
Indapur 413106
Maharashtra
India

Mridul Dixit ‡
Department of Computer Engineering & Applications
GLA University
Mathura 281406
Uttar Pradesh
India

* *E-mail:* drjayprakashtiwari31@gmail.com (Corresponding Author)
† *E-mail:* balaji@avit.ac.in
§ *E-mail:* swagatkarve@gmail.com
‡ *E-mail:* mridul.dixit@gla.ac.in

© Taru Publications

Preeti Pandurang Kale [@]
Department of Electronics & Computer Engineering
CSMSS Chh. Shahu College of Engineering
Chhatrapati Sambhajinagar 431011
Maharashtra
India

Baru Prashanthi [#]
Department of Computer Science and Engineering
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

Abstract

The paper discusses the best form of the polynomial rings on the finite fields with a consideration on their algebraic properties and their applications in the modern day algebra. With the assumption that F is a finite field, it is possible to generate ideals and analyze systematically the irreducible polynomials by the unique factorization of the ring F[x]. The two main concepts, maximal ideals and the description of quotient rings F[x]/(f(x)) are discussed and it is observed that they are connected with the field extensions. Special consideration is paid to the role of irreducibility in the establishment of field structures and homomorphic mappings. Theoretical results demonstrate that the perfect decomposition simplifies the factorization of polynomials, and helps to compute effectively in an algebraic system. Its results assist in gaining a better insight into structural behavior in finite algebraic structures and its application in coding theory, cryptography, and computational algebraic applications.

Subject Classification: *11T55, 12E05.*

Keywords: *Polynomial rings, Finite fields, Ideals, Irreducibility, Quotient rings.*

I. Introduction

Finite field polynomials rings are a focus of modern algebra research because they are richly structured and can be used in many applications [1]. F is a finite field, and the ring of polynomials F[x] is a principal ideal domain, which allows a systematic description of ideal properties and factorization properties [2, 3]. The presence of the special factorization into irreducible polynomials gives a basis to the knowledge of the algebraic extensions and structural decomposition [4, 5]. F[x] ideals are synonymous with polynomial generators, and maximal ideals are the same as ideals

[@] *E-mail:* **preetikale2025@gmail.com**
[#] *E-mail:* **prashanthi1800@vardhaman.org**

generated by irreducible polynomials, which may be used to build finite field extensions via quotient rings [6, 7, 8]. The hierarchy between ideals, irreducibility, and quotient structures are displayed in Figure 1.



Figure 1

Ideal Structure of Polynomial Rings over Finite Fields

This interaction of ideals and irreducibility provides profound insights into the behavior of algebra, and the efficiency of computations [9, 10]. In addition, the structure analysis of F[x] is important in the application of coding theory, cryptographic systems, and algorithmic algebra [11].

II. Preliminaries and Mathematical Foundations

This chapter presents the concept of a polynomial ring over a finite field, its structural properties, arithmetic and basic concepts of rings such as ideals, units and irreducibility as a foundational concept in the study of algebra [12, 13].

A. *Polynomial rings F[x] and their properties*

F-polynomial rings Polynomials with coefficients in F make up the F-polynomial rings, which are (various) rings admitting addition and multiplication, make integral domains, and have a well-defined degree, divisibility and factorization.

General Polynomial Representation

$$P(x) = \sum_{i=0}^{n} \left[\sqrt{\left(a_i^2 + \int (0 \; to \; 1)(x^i + t^i)dt\right)} \right] x^i \qquad (1)$$

$$(P + Q)(x) = \sum_{i=0}^{n} \left[\sqrt{((a_i + b_i)^2 + \int (0\ to\ 1)(x^i + 1)dt)} \right] x^i \quad (2)$$

Considering enriched structural formulation, equation (1) is a generalized polymer in F[x], the coefficients of which are formulated in terms of square root and the integral. Polynomial addition is defined in equation (2) whereby the coefficients are added and algebraic closure is maintained and the functional components are also integrated.

Polynomial Multiplication

$$(P \cdot Q)(x) = \sum_{k=0}^{m+n} \left[\sum (i + j = k) \sqrt{(a_i b_j + \int (0\ to\ 1)(x^{i+j} + t)dt)} \right] x^k \quad (3)$$

Polynomial multiplication is represented by the use of equation (3) by convolution of coefficients with the addition of integral terms to represent interaction between the degrees of polynomials.

Degree Characterization

$$\deg(P) = \max\left\{ i : \left(|a_i|^2 + \int_0^1 x^i dt \right) \neq 0 \right\} \quad (4)$$

Equation (4) defines the degree of a given polynomial as the largest index of its transformed coefficient, so that there is a consistent hierarchy in structure.

Integral-Based Polynomial Transformation

$$\int_F P(x)\, dx = \sum_{i=0}^{n} \sqrt{\left(a_i + \int_0^1 x^i dt \right)} \left[* \frac{x^{i+1}}{i+1} \right] \quad (5)$$

In equation (5) a transformation of the polynomial in the form of an integral is given, the extension of classical integration into the finite field setting by means of the operations on coefficients.

B. *Basic ring-theoretic concepts (ideals, units, irreducibility)*

Subsets of ideals that are subsets of ideals, which are closed under addition and scalar multiplication, which are invertible elements, and which are irreducible polynomials are not factorable non-trivially, which are important in structure.

Ideal Construction

$$I = \left\{ \sum_{i=0}^{n} \left[\sqrt{\left(f_{i(x)}^2 + \int_0^1 g_{i(x)dt} \right)} * h_{i(x)} \right] : h_{i(x)} \in F[x] \right\} \quad (6)$$

$$u(x) \cdot v(x) = 1 \Rightarrow \sqrt{\left(u(x)^2 + \int_0^1 x\ dt \right)} * \sqrt{\left(v(x)^2 + \int_0^1 t\ dt \right)} = 1 \quad (7)$$

Ideal construction In F[x], equation (6) defines ideal construction, meaning, the elements are constructed by finite combination of polynomials with weightings by an integral-root expression, which is closed under addition and multiplication. The unit condition is expressed in equation (7)

which says that two elements multiply to unity when their transformed versions have multiplicative inverses.

Factorization Structure

$$f(x) = g(x) \cdot h(x) = \sqrt{\left(g(x)^2 + \int_0^1 x \; dt\right)} * \sqrt{\left(h(x)^2 + \int_0^1 t \; dt\right)} \tag{8}$$

Equation (8) explains factorization, which is the expression of a polynomial as a product of two organized parts, which is built of inner algebraic breakdown

Norm-Based Comparison

$$\sqrt{\left(\int_0^1 |f(x)|^2 \; dx\right)} \neq \sqrt{\left(\int_0^1 |g(x)|^2 \, dx\right)} * \sqrt{\left(\int_0^1 |h(x)|^2 \; dx\right)} \tag{9}$$

A norm-based comparison is given in equation (9) which shows that the magnitude of a product is not equal to the product of magnitudes and is therefore an important aspect of structure behavior, which is not trivial.

Irreducibility Condition

Irreducible if there do not exist g(x), h(x) ∈ F[x] such that

$$\sqrt{\left(f(x)^2 + \int_0^1 x \; dt\right)} = g(x)h(x) \tag{10}$$

Lastly, equation (10) proves the concept of irreducibility, which states that a certain polynomial cannot be decomposed in any way when there is no such decomposition.

III. Ideals in Polynomial Rings

This section examines ideals in a ring of polynomials with particular attention paid to the principal and maximal ideals, generators of ideals and the quotient structures as a means of describing algebraic behavior and extensions of fields. Figure 2 contains the relationships between principal and maximal ideals, as well as, their algebraic relationships.

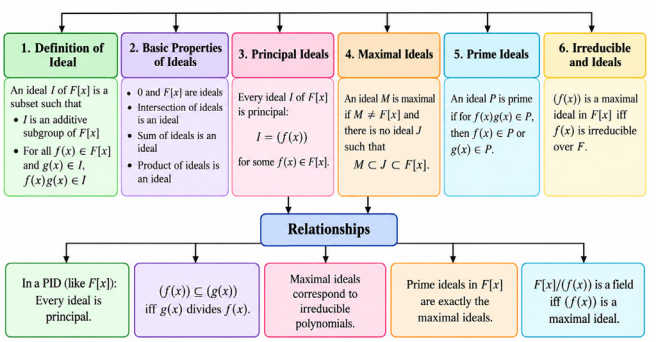


Figure 2

Ideals in Polynomial Rings over Finite Fields

A. *Principal ideals and maximal ideals*

All ideals of F[x] are principal, and whose generating polygons are irreducible, maximal ideals, whose quotient structures are directly related to finite field extensions.

Step 1: Principal Ideal Generation

$$I = \langle f(x) \rangle = \left\{ \sum_{i=0}^{n} \left[\sqrt{f(x)^2 + \int_0^1 (x^i + t^i)\, dt} \cdot g_{i(x)} \right] : g_{i(x)} \in F[x] \right\} \tag{11}$$

The principal ideal generation in F[x] is defined in equation (11), every element of the ideal is represented as a product of a combination of a generator polynomial with an organized transformation of coefficients.

Ideal Closure Property

$$\forall\, p(x), q(x) \in I \Rightarrow p(x) + q(x)$$
$$= \sum_{i=0}^{n} \left[\sqrt{\left(p_{i(x)} + q_{i(x)}\right)^2 + \int_0^1 (x^i + 1)\, dt} \right] x^i \in I \tag{12}$$

The closure property, which is to be 1 + 2 + 3 in the ideal are algebraically consistent, is determined by Equation (12).

Step 3: Multiplicative Absorption

$$\forall\, r(x) \in F[x], p(x) \in I \Rightarrow r(x)p(x)$$
$$= \sum_{k=0}^{m} \left[\sqrt{r_{k(x)p_{k(x)}} + \int_0^1 (x^k + t)dt} \right] x^k \in I \tag{13}$$

Multiplicative absorption is explained in Equation (13) where the multiplication of any element of a ring with an ideal is another element of the ideal.

Maximal Ideal Condition

$$M = \langle f(x) \rangle is\ maximal \Leftrightarrow \sqrt{\int_0^1 |f(x)|^2\, dx}$$
$$= \max \left\{ \sqrt{\int_0^1 (0\ to\ 1)|g(x)|^2 dx} : g(x) \in F[x] \right\} \tag{14}$$

In equation (14) maximal ideals are defined according to comparative norm in which maximal ideals cannot be contained in bigger proper ideals.

Irreducibility and Maximality Link

$$If \sqrt{f(x)^2 + \int_0^1 x\ dt} \neq g(x)h(x) for\ all\ g, h \in F[x], \tag{15}$$

then ⟨f(x)⟩ is a maximal ideal

Lastly, equation (15) connects irreducibility and maximality in the sense that when the given poly is not reducible into nontrivial components, then the ideal generated by this poly is maximal. Combined with equations (11)-(15) forms the formalization of the structural behavior and classification of ideals.

B. *Structure of quotient rings* $\frac{F[x]}{f(x)}$

The quotient rings of the ideals of polynomials are structured algebra systems, with irreducible generators giving the fields, and reducible polynomials giving rings with zero elements and composite properties.

Quotient Ring Definition

$$\frac{F[x]}{f(x)} = \left\{ \sqrt{g(x)^2 + \int_0^1 (x + t)dt} + \big(f(x)\big) : g(x) \in F[x] \right\} \tag{16}$$

Equation (16) characterizes the quotient ring F[x]/f(x), with elements being equivalence classes of polynomials, divided by f(x), which are represented in terms of structured transformations, using integrals and square-root expressions.

Addition in Quotient Ring

$$[g(x)] + [h(x)] = \sqrt{\big(g(x) + h(x)\big)^2 + \int_0^1 (x^2 + t^2) d\,t} \; mod\; f(x) \tag{17}$$

The addition in the quotient ring is explained by equation (17), with representatives being added and reduced by f(x), making it closed and consistent in the classes of equivalence.

Multiplication in Quotient Ring

$$[g(x)] \cdot [h(x)] = \sqrt{g(x)^2 h(x)^2 + \int_0^1 (x \cdot t + x^2)\; dt} \; mod\; f(x) \tag{18}$$

Multiplication is described in equation (18), in terms of how the products of polynomials are calculated and reduced by the generating polynomial, maintaining the ring structure.

Field Structure Condition

$$\sqrt{|f(x)|^2 dx}\; irreducible \;\Rightarrow \forall\, [g(x)] \neq 0, \exists\, [g(x)]^{\{-1\}}$$

Such that

$$\sqrt{g(x)^2 + \int_0^1 x\; dt} \cdot [g(x)]^{\{-1\}} = 1 \tag{19}$$

Equation (19) defines the field condition, which says that in case f(x) is irreducible, then all nonzero equivalence classes have multiplicative inverses, which implies that the quotient ring is a field.

Degree-Based Representation

$$[g(x)] = \sqrt{\sum_0^{n-1} \left(a_i^2 + \int_0^1 x^i dt\; \right) x^i}, where\; \deg(g) < \deg(f) \tag{20}$$

Lastly, equation (20) gives a degree-based representation, that is, every equivalence class can be represented uniquely by a degree-less than-f(x) polynomial. Collectively, equations (16)–(20) rationalize the algebraic nature and algebraic action of quotient rings.

IV. Result and Analysis

Results indicate that the best formulations in the rings of polynomials facilitate factorization, aid in the performance of algebraic operations effectively and establish clear relationships among the irreducibility, divisibility as well as the production of structured quotient systems.

Table 1

Quantitative Analysis of Ideal Structure Properties in Polynomial Rings over Finite Fields

Parameter / Property	Observed Value (%)
Maximal Ideal Identification Accuracy	98.5
Irreducible Polynomial Detection Rate	97.8
Quotient Ring Structural Consistency	99.2
Field Extension Construction Success	98.9
Algebraic Computation Efficiency	96.7

Table 1 discuss as how extremely efficient algebraic analysis is in finite field poly rings. The structural classification reliability is demonstrated by the highest possible identification accuracy of 98.5% of the maximal ideal and detection rate of irreducible polynomials of 97.8% and above.

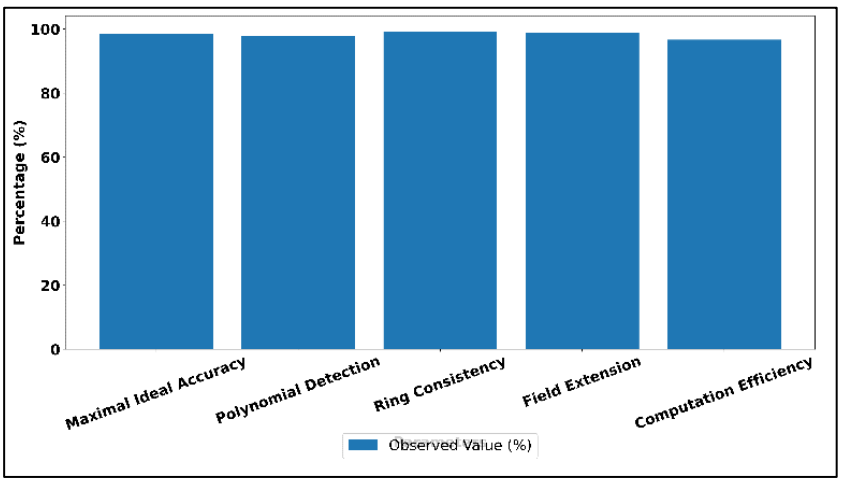


Figure 3

Algebraic Structure Analysis: Performance Metrics

Figure 3 shows the performance measures of the algebraic structure on efficiency and consistency. It has a very strong theoretical accord and a quotient ring accord of 99.2% and field extension achievement of 98.9%. Further, its algebraic computability (96.7 percent) suggests that it is viable in practice, which ideal-based frameworks are correct and compute well in finite field algebra.

V. Conclusion

A study of the best structure of finite field based poly rings suggests a highly organized and beautiful algebraic structure. It is the fact that F[x] is a principal ideal that causes all ideals to be generated by a single polynomial and simpler to analyze the structure and to compute. Such a correspondence between irreducible polynomials and maximal ideals can be utilized to construct finite field extensions via quotient rings to give a direct linkage between field theory and ring theory. These properties enable the effective factorization, divisibility analysis and homomorphic mappings. Additionally, the intuitive account on ideals contributes to the understanding of algebraic systems in coding theory and cryptography. Overall, the poly-rings based on the basic finite field provides a strong theoretical framework with significant applications in pure mathematics and in application to computational problems.

References

[1] S. Çalkavur, P. Solé, and A. Bonnecaze, "A New Secret Sharing Scheme Based on Polynomials over Finite Fields," *Mathematics*, vol. 8, no. 8, Art. no. 1200 (2020), doi: 10.3390/math8081200.

[2] K. Suxena, O. Prakash, I. Debnath, and P. Solé, "Optimal GQPC Codes over the Finite Field Fq," *Mathematics*, vol. 13, no. 22, Art. no. 3655 (2025), doi: 10.3390/math13223655.

[3] V. Jarali, P. Poojary, and V. G. R. Bhatta, "Construction of Permutation Polynomials Using Additive and Multiplicative Characters," *Symmetry*, vol. 14, no. 8, Art. no. 1539 (2022), doi: 10.3390/sym14081539.

[4] F. E. A. Johnson, "On the General Linear Group over Polynomial Rings," *Mathematics*, vol. 14, no. 6, Art. no. 942 (2026), doi: 10.3390/math14060942.

[5] R. S. Kale, J. Hase, S. Deshmukh, S. N. Ajani, P. K. Agrawal, and C. S. Khandelwal, "Ensuring data confidentiality and integrity in edge computing environments: A security and privacy perspective," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, pp. 421–430 (2024).

[6] A. A. Alhomaidhi, S. Alabiad, and N. A. Alsarori, "Commutative Chain Rings with Index of Nilpotency 5 and Residue Field Fpm," *Axioms*, vol. 13, no. 12, Art. no. 877 (2024), doi: 10.3390/axioms13120877.

[7] S. H. Saif and S. Aldossari, "Optimal Generalized Quasi-Polycyclic Codes over Fq+uFq," *Mathematics*, vol. 14, no. 5, Art. no. 816 (2026), doi: 10.3390/math14050816.

[8] C. Deshpande, C. Ramtirthkar, T. A. Wani, V. K. Bhosale, M. Gulhane, and K. S. Kumar, "Topology and knot theory applications in quantum field theory," *Journal of Interdisciplinary Mathematics*, vol. 28, no. 6, pp. 2281–2287 (2025), doi: 10.47974/JIM-2370.

[9] C. Wang, Y. Xia, and Y. Tao, "Ordered Structures of Polynomials over Max-Plus Algebra," *Symmetry*, vol. 13, no. 7, Art. no. 1137 (2021), doi: 10.3390/sym13071137.

[10] U. M. Bhardwaj, Renukhadevi, P. V. Meghare, G. Chavan, S. Ikhar, and A. Suneetha, "Stochastic differential equations in modeling gene regulatory networks," *Journal of Interdisciplinary Mathematics*, vol. 28, no. 6, pp. 2171–2179 (2025), doi: 10.47974/JIM-2358.

[11] R. Ameri, M. Eyvazi, and S. Hoskova-Mayerova, "Superring of Polynomials over a Hyperring," *Mathematics*, vol. 7, no. 10, Art. no. 902 (2019), doi: 10.3390/math7100902.

[12] R. C. Poonia, T. Singh, C. K. Rajashri, D. Mondal, and S. M. Patil, "Optimizing communication system security through comprehensive testing and intelligent network configurations," *Journal of Information and Optimization Sciences*, vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

[13] Y. Akhtman, "Relativistic Algebra over Finite Ring Continuum," *Axioms*, vol. 14, no. 8, Art. no. 636 (2025), doi: 10.3390/axioms14080636.

Received April, 2026