INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in July 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

Study Of Special Irreducible Normal Polynomials

Anju Bala, Research Scholar, Dept. of Mathematics, Shri JJT University, Jhunjhunu Rajasthan
Dr. Vishwajeet S. Goswami, Research Guide, Dept. of Mathematics, Shri JJT University, Jhunjhunu Rajasthan

ABSTRACT

This study paper brings out the understanding of special irreducible polynomials. We will also try to uncover known results on irreducible normal polynomials and Root polynomials over arbitrary fields. We will also try to find out some of the irreducible polynomials that exist. When we talk of irreducibility, it is also something that we can consider when we talk about prime numbers that cannot be further factored. It may not be wrong to say that factoring polynomials and bringing irreducibility is used in forming Algorithms in Computer Algebra systems or CAS.

The questions that move around Integers or Integer space can be then understood when answers can be found when questions are made about the Numbers in a Finite Field. We can focus on concepts like explicit root polynomials for third-degree normal Polynomials of a cyclic nature over a field of characteristic 2 is resulted.

KEYWORDS: Reducible Polynomial, Irreducible Polynomial, Normal Polynomial, Root Polynomial, Finite Field, Eisenstein Criterion

INTRODUCTION

The study of Finite Fields implies a key part in theories like Abstract Algebra and Cryptography. A polynomial is considered normal in every residue class of modulo p when there is exactly one integer polynomial with coefficients ≥ 0 and ≤ p-1. A polynomial is then simplified by factorization and merging coefficients of the same degree of terms and can be called reducible.

When we talk of a finite field, it is a field that can contain finite number of elements. Finite field is a set of which the Multiplication, Addition and Subtraction and division are performed and that can satisfy certain basic rules. In 1850, Eisenstein firstly understood the existence of normal bases for finite fields and was further validated by Schönemann for the case of Fp and then by Hensel in 1888 for arbitrary fields. These then form the base where the applications are seen in faster computations in coding theory and Cryptography.

Irreducible Polynomials are with coefficients in an integral domain $\mathbb{R}$, if the product of the two polynomials have their coefficients in $\mathbb{R}$. It can also be considered that an irreducible polynomial is an irreducible element in the rings of polynomials over $\mathbb{R}$. We call a polynomial as irreducible if it cannot be further factored into polynomials with coefficients in the same domain that they do not have a negative degree. It is not easy to check whether an irreducible polynomial is normal polynomial.

REVIEW

It can be understood that a normal polynomial can be factored and stand reducible in domain set. There are two things to note that for a normal polynomial to be irreducible we need to check for the prime coefficient. Take, for instance, 7 as a prime element in the field of $\mathbb{Z}$. Because 7 cannot be further factored into a product of much smaller numbers in $\mathbb{Z}$. Similarly, $x^2 + 3$ is prime in $\mathbb{Q}$ $[x]$. Because $x^2 + 3$ cannot be further factored into a product of polynomials of a lower degree in $\mathbb{Q}$ $[x]$. Reducibility is limited to the fact that the polynomial will have a prime constant.

A unitary polynomial (a polynomial with a coefficient equal to 1) *f (x)* from F [x] is called normal over F if its roots are all rationally expressed over F through any root of the polynomial f (x).

Let a degree *f (x)* equal to *n* be greater than two and F be a formally real field. In this case, H. Kleiman proved the following theorem:

The normal polynomial $f = x^n + \sum_{j=0}^{n-1} \square a_{(n-1)-j} x^{(n-1)-j}$ with coefficients in a formally real field F is uniquely determined by the set S= {M, a^n - 2}, where M is the set of root polynomials for *f* (*x*). In addition, the set M contains at least one nonlinear polynomial, if $n > 2$. If the set M contains a root polynomial of degree two, then the normal polynomial $f(x)$ is uniquely determined by the set M.

Let $\Phi_n(x)$ be a circular polynomial of order n, $n>6$, therefore, the degree of the polynomial $\Phi_n(x)$ is greater than or equal to 4.

OBJECTIVES

There exist many tests that understand the reducibility of a polynomial. We can go through the different tests that are considered for irreducibility. There are some of the tests that we go through depend on the degree of the polynomial that is being tested. While some of the tests may seem simple, some of the tests also depend on the domain at the polynomial is carried in $\mathbb{Q}[x]$ for rational numbers, $\mathbb{R}[x]$ for Real Numbers and $\mathbb{Z}_n[x]$ for set of integers of mod n.

METHODOLOGY AND HYPOTHESES

We can understand that a polynomial is reducible only when we understand where we find its roots. It gives a basic idea that if the given polynomial is reducible, it provides a constraint on where the roots belong.

A monic polynomial with prime constant coefficient p is reducible. We may find one of its irreducible factors has a constant term which may be positive or negative p and the rest have a constant term positive or negative 1.

One of the methods for polynomials over $\mathbb{Z}$ is to use complex analysis to say something about the location of the roots. You can probably apply Rouche's theorem; for here is how Perron's criterion is proven, which cites that a monic polynomial $x_n+a_n-1x_n-1+\ldots+a_0$ with integer coefficients is irreducible if $|a_n-1|>1+|a_n-2|+\ldots+|a_0|$ and $a_0\neq0$.

Eisenstein's criterion

Eisenstein's criterion goes to prove that a polynomial with integer coefficients is considered irreducible. It cannot be written as a product of two polynomials of smaller degree with integer coefficients. Sometimes you may not find it applied to most polynomials, but it is good to prove it is efficient for showing examples of certain polynomials which are irreducible.

$p(x) = a_n x^n + a_{(n-1)}\, x^{(n-1)} + \ldots + a_1\, x + a_0$

$a_i \in \mathbb{Z}$ for all $i = 0, \ldots, n$ and $a_n \neq 0$ which means that the degree of $p(x)$ is n is irreducible if some prime number p divides all coefficients $a_0, \ldots, a_{n-1},$ but not all leading coefficient a_n and, moreover, p^2 does not divide the constant term a_0

This can be considered sufficient if not a necessary condition. Let us consider the polynomial $x^2 +1$ which is irreducible but it does, in no way, fulfill the above property, since no prime number can divide 1. We can however change or substitute $x +1$ for x can produce the polynomial $x^2 + x + 2$ which can be seen to fulfill the Eisenstien criterion (with $p = 2$) and describes the polynomial as irreducible.

Hilbert's criterion

A popular German mathematician named David Hilbert provided a theory in which he stated that for any finite set of irreducible polynomials which is in any finite number of variables which do have Rational coefficients can allow specialized subset that seems proper for the variables to Rational numbers in a way that all polynomials are proved irreducible.

Let f_1 $(X_1, \ldots, X_r, Y_1, \ldots., Y_5), \ldots, f_n$ $(X_1, \ldots, X_r, Y_1, \ldots, Y_5)$ be irreducible polynomials in a ring $\mathbb{Q}(X_1, \ldots, X_r)$ $[Y_1, \ldots., Y_8]$

Then there exists an r-tuple of rational numbers $(a_1, \ldots, a_r)$ such that f_1 $(a_1, \ldots, a_r, Y_1, \ldots., Y_8), \ldots, f_n$ $(a_1, \ldots, a_r, Y_1, \ldots., Y_8)$ are irreducible in the ring $\mathbb{Q}(Y_1, \ldots, Y_r)$

We derive from this theorem that there can be many r-tuples which are infinite. In fact, the set for irreducible specials, called the Hilbert set, is large in many cases. For example, this set here Zariski dense in $\mathbb{Q}^r$. The assertion proves right even if we require $(a_1, \ldots, a_r)$ to be pure integers.

Brute Force Method

Brute Force method goes on to prove with an intuitive, direct, and straightforward technique where we try to enumerate all the possible ways or solutions. It can show that the polynomial is irreducible by showing that any of polynomials that may be factors, could not be factors.
Let us consider: $x^4 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$
Consider that the polynomial is treated as f (x). We need to find out that f (x) can be factored as g (x) x h (x) where g (x) and h (x) have a lower degree than 4, so the degree of the polynomial test is 4 where the degree of g (x) is less than 4 and the degree of h (x) is less than 4. It is not enough to factor out a constant, for example, we build factor it into real polynomials that both have. When we have f (x) factor of g (x) x h (x), the degree of f (x) would be equal to the degree of g (x) and the degree of h (x). Multiplication of polynomial causes the degrees to be added together. Since we know that the sum of the degrees of the factored Polynomial is 4 the degrees of g (x) and h (x) will be less than or equal to 4. The degree of the polynomial is always supposed to be greater than 0. The possible outcomes can be 1 + 3 or 3 + 1 or 2 + 2. One factor must be 1 or 2. Our next step is to check if f (x) has the degree 1 or degree 2 factor.
Degree 1 Polynomials: x, $x + 1$
Degree 2 Polynomials: $x^2 + x + 1$, $x^2 + 1$, $x^2 + x$, x^2
We will be left with constant 1 every time we try to reduce f (x) with the given possibilities. Hence none of the degree of polynomials will further reduce it proving that the given polynomial of $f(x)$ is irreducible.
We can test to check for irreducibility is to check for roots or Element or Field to be a root. Finite Field here could represent $\mathbb{Q}[x]$ for rational numbers, $\mathbb{R}[x]$ for Real Numbers and $\mathbb{Z}p[x]$ for set of integers where p is a prime number. We need to prove that if the root can be placed in the polynomial whether the polynomial in question can be reduced. Now f (x) $\in$ F[x] has a root $a \in$ F mean that f (a) = 0 and that x – a is a factor of f (x). We need to find out that f (x) $\in$ F[x] has a root in F then f (x) will be reducible. This cannot be said in the reverse manner as the meaning does not hold true. If we have a root then the polynomial is reducible.
Let us consider $x^4 + 2x^3 + 3x + 1$ is reducible in $\mathbb{Z}_5[x]$. We can prove the reducibility by finding the root. $\mathbb{Z}_5$ has only 5 elements Z5 = {0, 1, 2, 3, 4}.
Trial can be arranged for the polynomial to achieve that 3 is the root of f (x).
Proving that $(x - 3)$ is a non-trivial factor of f (x) and that it is reducible.

SCOPE

This part of Abstract Algebra, along with the theory of finite fields and polynomials over finite fields are used for making systems for protecting information with encryption and decryption. They have been used for cyclic redundant codes which utilize polynomials over fields F_p.
Again, we need to understand that finite fields are a set with a finite number of elements, so we can perform all the arithmetic operations. Finite fields are limited with respect to the said arithmetic operations For any two elements of the field $a,b \in$ Fp. So if any operations are performed, the resulting element $c \in$ Fp. The calculations are made with modulo p that belongs to both the finite field and is a prime number.
We reiterate that a scope for irreducible polynomials is that if you find it irreducible in one field say Z, you may find it reducible in say $\mathbb{Q}$. The search for irreducible polynomials is difficult to compute a problem, especially over fields of large dimensions.

LIMITATIONS

Root Test:
We can test to check for irreducibility is checking for roots or element or a Field to be a root. Finite Fields here could represent $\mathbb{Q}[x]$ for rational numbers, $\mathbb{R}[x]$ for Real Numbers and $\mathbb{Z}p[x]$ for set of integers where p is a prime number. We need to prove that if the root can be placed in the polynomial whether the polynomial in question can be reduced. Now f (x) $\in$ F[x] has a root $a \in$ F mean that f (a) = 0 and that $x - a$ is a factor of f (x). We need to find out that f (x)

$\in \mathrm{F}[x]$ has a root in F then $f(x)$ will be reducible. This cannot be said in the reverse manner as the meaning does not hold true. If we have a root then the polynomial is reducible.
Let us consider $x^4 + 2x^3 + 3x + 1$ is reducible in $\mathbb{Z}_5[x]$. We can prove the reducibility by finding the root. $\mathbb{Z}_5$ has only 5 elements $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
Trial can be arranged for the polynomial to achieve that 3 is the root of f (x)
Proving that (x -3) is a non-trivial factor of f (x) and that it is reducible.
Similarly, if a polynomial has no roots, we cannot determine that it is irreducible.

Consider the polynomial $x^4 + 5x^2 + 4 \in \mathbb{R}[x]$ it may not have roots in $\mathbb{R}$ but can be reducible to $(x^2 + 1)(x^2 + 4)$.
However, irreducibility tests are like the above only move to check the whether the polynomial is found to be irreducible in the said domain in which they are arranged. We cannot conversely imply that the if the test fail to prove the irreducibility can be then termed to be reducible.
Take example of the Eisenstein Criterion test that is used in some important use cases to prove the irreducibility with little work. We derive that it is not applicable to all polynomials with $\mathbb{Z}$ coefficients that are irreducible over the field of $\mathbb{Q}$.

CONCLUSION

This article attempted to explain certain concepts and the properties of irreducible polynomials. Generally, we also find it in the Galois theory. We also attempted to look at it from an algebraic point of view and from the point of view of mathematics and applied theory in cryptography. This paper also finds an extensive search of finite fields. We reiterate that one method of finding the irreducibility of a polynomial does not prove it cannot be reducible in another domain. We can find both a theoretical and a practical usability of irreducibility theory considering the various aspects that showcase its applicability and the importance of it.

REFERENCE

G. Eisenstein, Lehrätze, J. Reine Angew. Math., 39 (1850), pp. 180-182
T. Schönemann, Über einige von Herrn Dr. Eisenstein aufgestellte Lehrätze, Irredutible congruenzen betreffend
K. Hensel, Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor
J. Reine Angew. Math., 103 (1888), pp. 230-237, Math., 40 (1850), pp. 185-187
R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, Cambridge, UK, 1994.
V. V. Prasolov, Mnogochleny, M.: MTSNMO, 2003, pp. 58-72. [in Russian]
N. Koblitz, Algebraic aspects of Cryptography, Springer-Verlag,
Berlin, Heidelberg, 1998. -217 p
Eisenstein's Irreducibility Criterion. Brilliant.org
D. Hilbert, "Uber die Irreducibilitat ganzer rationaler Functionen mit ganzzahligen Coefficienten", J. reine angew. Math. 110 (1892) 104–129.
Lang (1997) p.41, p.42
H. Kleiman, ‘’Methods for polynomials and related theorems’’, Monatshefte fur Mathematik, vol. 73, 1969, pp. 63 - 68
Lang, Serge (1997). Survey of Diophantine Geometry. Springer-Verlag. ISBN 3-540-61223-8. Zbl 0869.11051.
J. P. Serre, Lectures on The Mordell-Weil Theorem, Vieweg, 1989.
M. D. Fried and M. Jarden, Field Arithmetic, Springer-Verlag, Berlin, 2005.
H. Völklein, Groups as Galois Groups, Cambridge University Press, 1996.
G. Malle and B. H. Matzat, Inverse Galois Theory, Springer, 1999.
U. Turusbekova, “Finding irreducible polynomials of a special type”, Bulletin of Kazakh National Technical University, 2019, vol. 6 (136), pp. 691-696
Irreducible Polynomials by James Hamblin