Peer Reviewed Referred
and
UGC Listed Journal
(Journal No. 40776)

AN INTERNATIONAL MULTIDISCIPLINARY
QUARTERLY RESEARCH JOURNAL
ISSN 2277-5730

AJANTA

Volume-VII, Issue-III
English Part - I
July - September - 2018

IMPACT FACTOR / INDEXING
2018 - 5.5
www.sjifactor.com

AJANTA PRAKASHAN

ENGLISH CONTENTS PART - I

VOLUME - VII, ISSUE - III–JULY - SEPTEMBER - 2018
AJANTA - ISSN 2277 - 5730 -IMPACT FACTOR - 5.5 (www.sjifactor.com)

9. Applications of Unique Factorization

SyedaFarra Fatima Nahri
Milliya Arts, Science and Management Science College, Beed.

Abstract

We are most familiar with the concept of polynomials with integer coefficients, rational coefficients , real coefficients and we are drilled in factoring them. In this paper our focus is on polynomials which are elements of certain ring ,and factoring of these polynomials.

Key Words : Ring,polynomials,integral domain, field,irreducible,reducible

Firstly introduced some definitions.

Zero Divisors : If R is acommutative ring, then $a \neq 0 \in R$ is said to be zero divisor if there exists $a,b \in R$, $b \neq 0$, such that ab=0

Integral domain :A commutative ring is an integral domain if it has no zero divisors.

The ring of integers is an example of integral domain.the ring Z_p of integers modulo p (p is prime) is an integral domain,but the ring Z_n of integers modulo n is not an integral domain when n is not prime.

Division ring :Aring is said to be a division ring if its non zero elements form a group under multiplication.

Field : A field is a commutative division ring, that is acommutative ring with a unity is called a field if every non-zero element have multiplicative inverse. We note down some results.

- Every field is an integral domain.
- A finite integral domain is a field.
- If p is a prime number then Z_p,thering of integers modulo p, is a field.

We are most familiar with the concept of polynomials with integer coefficients, rational coefficients , real coefficients and we are drilled in factoring them. Now we interested in polynomials will simply be elements of certain ring.introduced polynomials with coefficients from Z_n .All of these sets of polynomials are rings.

Polynomial ring : Let R be a commutative ring. The set of symbols

$R[x]=\{a_0+a_1x+\ldots\ldots+a_{n-1}x^{n-1}+a_nx^n \mid a_i \in R$, and n is non-negative integer$\}$ is called a ring of polynomials over R in the indeterminate x.

If $p(x)=a_0+a_1x+......+a_mx^m$ and $q(x)=b_0+b_1x+......+b_nx^n$ are in R[x] then p(x)=q(x) if and only if thier corresponding coefficient are equal. $p(x)+q(x)=c_0+c_1x+......+c_tx^t$ where for each i, $c_i=a_i+b_i$ and . $p(x).q(x)=c_0+c_1x+......+c_kx^k$ where $c_t=a_tb_0+a_{t-1}b_1+a_{t-2}b_2 ...+a_0b^t$

If $f(x)=a_0+a_1x+......+a_{n-1}x^{n-1}+a_nx^n \neq 0$ and leading term $a_n\neq 0$,then degree of f(x) is n, it is written as degf(x)=n.

Properties of R carry over R[x]

- If Dis integral domain then the polynomial ring D[x] is also an integral domain.
- Division Algorithm : Given two polynomials f(x) and $g(x) \neq 0$ in F[x] (f(x) is an integral domain), then their exists two polynomials t(x) [quotient] and r(x) [remainder] in F[x] such that f(x)=t(x)g(x)+r(x) where r(x)=0 or degr(x)<degr(x).

When the ring of coefficients of a polynomial ring is a field,we can use the long division process to determine the quotient and remainder.

The Remainder Theorem :If f(x)∈F[x] and a∈F, for any field F,then f(a)is the remainder when f(x) is divided by x-a.

Factor Theorem :If f(x)∈F[x] and a∈F, for a field F,then (x-a) dividesf(x) iff f(a)=0 i.e. remainder is zero.

If f(x) is a polynomial in F[x] for an arbitrary field F and f(c)=0 for an element c∈ F, then f(c) is called azero of f(x). If f(c) is a zero of the polynomial f(x) then c is a root of the equation f(x)=0, which is a solution of the equation.

A polynomial of degree n over a field has at most n zeros counting multiplicity.This is not true for arbitrary polynomial rings.For example, the polynomial$x^2 + 3x + 2$ has four zeros in Z_6 .lagrange was the first to prove it for polynomials in $Z_p[x]$.

To discuss factorization of polynomials, first introduce the polynomial analog of a prime integer.

Irreducible polynomial, Reducible polynomial : A polynomial p(x) in F[x] is said to be irreducible over integral domain F if whenever p(x)=a(x)b(x) with a(x) , b(x) ∈ F[x],then one of a(x) or b(x) has degree 0 (i.e. ,is a constant). A non zero , nonunit element of F[x] that is not irreducible over F is called reducible over F.

The polynomial x^2+1 is irreducible over the real field but not over the complex field, since $(x^2+1)=(x+i)(x-i)$ where $i^2= -1$

The polynomial x^2+1 is irreducible over Z_3 but reducible over Z_5.

Reducibility test for degree 2 and 3 : Let F be a field. If f(x)∈F[x] and deg f(x)= 2 or 3, then f(x) is reducible over F iff f(x) has a zero in F.

This test is particularly easy to use when the field is Z_p, since in this case, we can check reducibility of f(x) by simply testing to see if f(a)=0 for a=0, 1, 2,......p-1

Mod p irreducibility test : Let p be a prime and suppose that f(x)∈ Z[x] with deg f(x)≥1. Let $\bar{f}(x)$ be the polynomial in $Z_p[x]$ obtained from f(x) by reducing all the coefficients of f(x) modulo p. If $\bar{f}(x)$ is irreducible over Z_p and deg$\bar{f}(x)$=deg f(x), then f(x) is irreducible over Q.

Example: Let $f(x) = 21x^3 - 3x^2 + 2x + 9$. Then over Z_2, we have $\bar{f}(x) = x^3 + x^2 + 1$ and,since$\bar{f}(0)$=1 and $\bar{f}(1) = 1$, we see that $\bar{f}(x)$ is irreducible over Z_2. Thus f(x) is irreducible over Q.

Eisenstein's Criterion : Let $f(x)=a_0+a_1x+......+a_{n-1}x^{n-1}+a_nx^n$ ∈Z[x]. If there is a prime p such that $p/a_{n-1},............p/a_0$ but p does not divides a_n and p^2 does not divides a_0 , then f(x) is irreducible over Q.

Unique Factorization in Z[x]: Every polynomial in Z[x] that is not the zero polynomial or a unit in Z[x] can be written in the form $b_1b_2 \dots\dots b_s p_1(x)p_2(x) \dots\dots p_m(x)$,where the b's are irreducible polynomials of degree 0, and the $p_i(x)$'s areirreducible polynomials of positive degree. Furthermore, if

$$b_1b_2 \dots\dots b_s p_1(x)p_2(x) \dots\dots p_m(x) = c_1c_2 \dots\dots c_t q_1(x)q_2(x) \dots\dots q_n(x),$$

Wherethe b's and c's are irreducible polynomials of degree zero, and the $p(x)$'s , $q(x)$'s are irreducible polynomials of positive degree, then s=t, m=n, and, afterrenumbering the c's and $q(x)$'s, we have $b_i = \pm c_i$, for i=1,.......,s; and $p_i(x) = \pm q_i(x)$ for i=1,........,m.

Weird Dice is an application of Unique factorization : consider an ordinary pair of dice whose faces are labelled 1 through 6 . The probability of rolling a sum of 7 is6/36, the probability of rolling a sum of 6 is 5/36, and so on. In a 1978 issue of Scientific American ,Martin Gardner remarked that if one were to label the six faces of one cube with integers 1, 2, 2, 3, 3, 4 and the six faces of another cube with the integers 1, 3, 4, 5, 6, 8, then the probability of obtaining any particular sum with these dice is the same as the probability of rolling that sum with ordinary dice.in this we utilizethe fact that Z[x]has the unique factorization property.

Conclusion

Factorization of polynomials in Z[x] is interesting and helpful in solving mathematical games also.

References

1. Topics in Algebra by I.N. Herstein
2. A textbook of Abstract Algebra by S.K.D.Dubey,Gunjeshwar Shukla, V.S. Chubey
3. Contemporary Abstract Algebra by Joseph A. Gallian