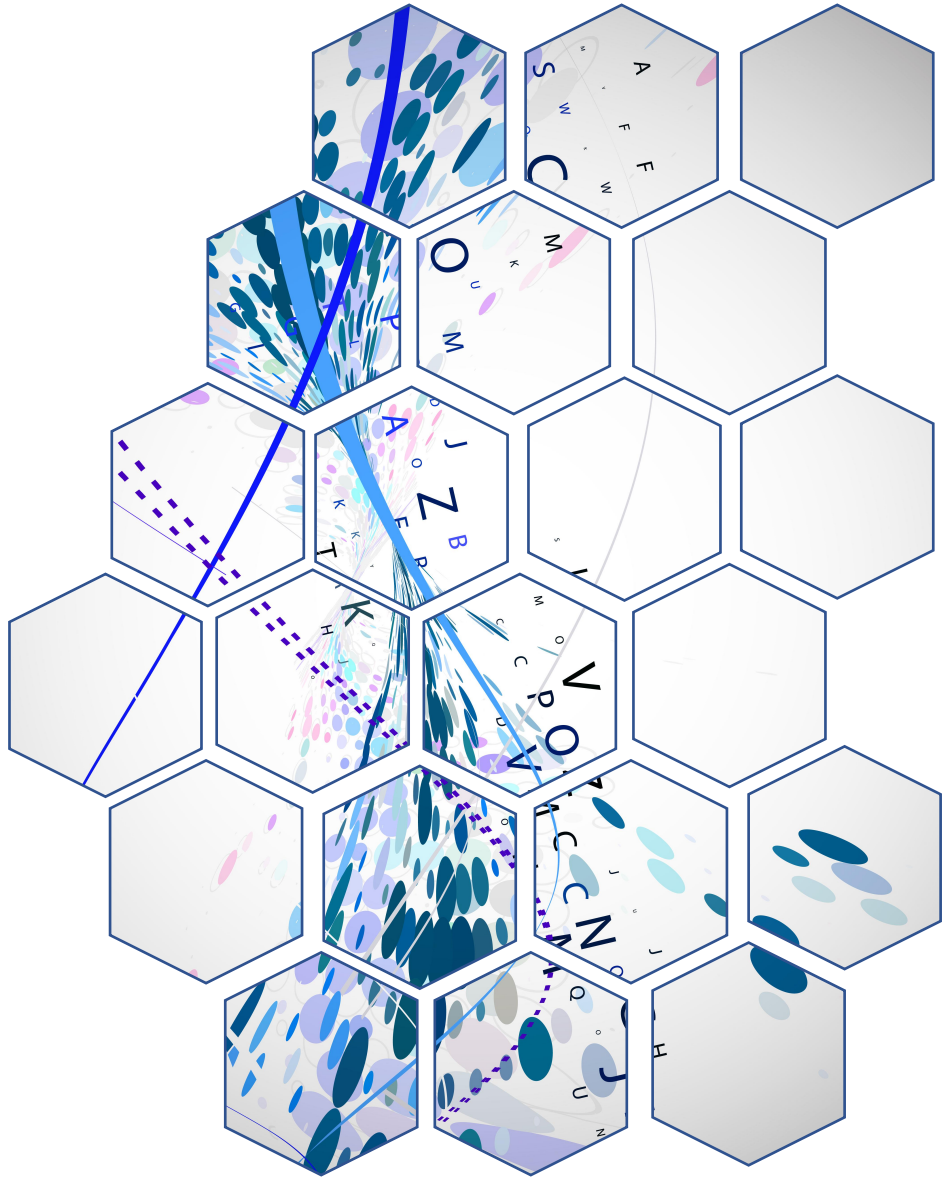
POLYNOMIAL

Abstract Algebra



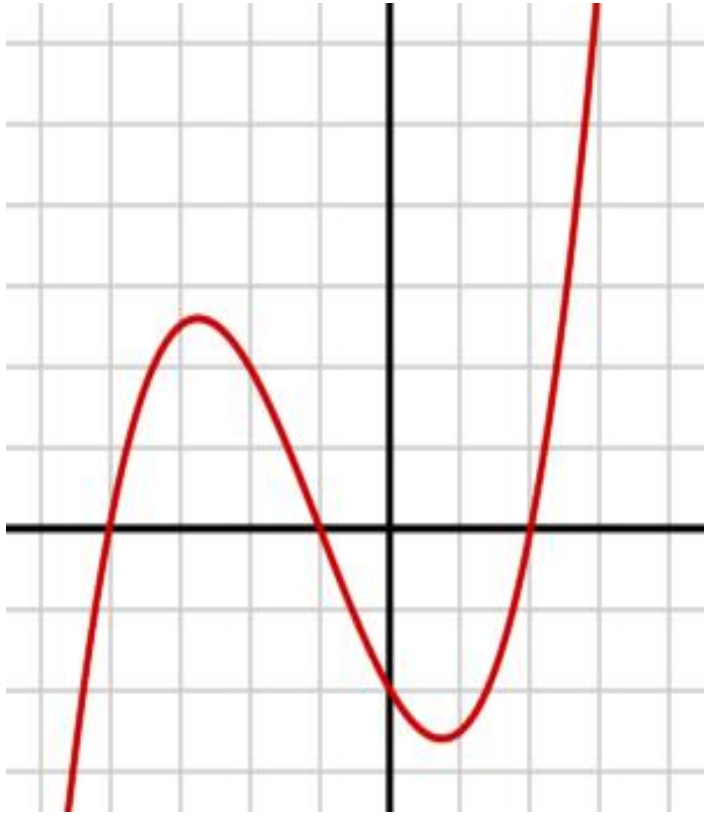
Submitted by

Kh. Tahera Mehjabin

IT 23604

27th November 2024

OUTLINE :

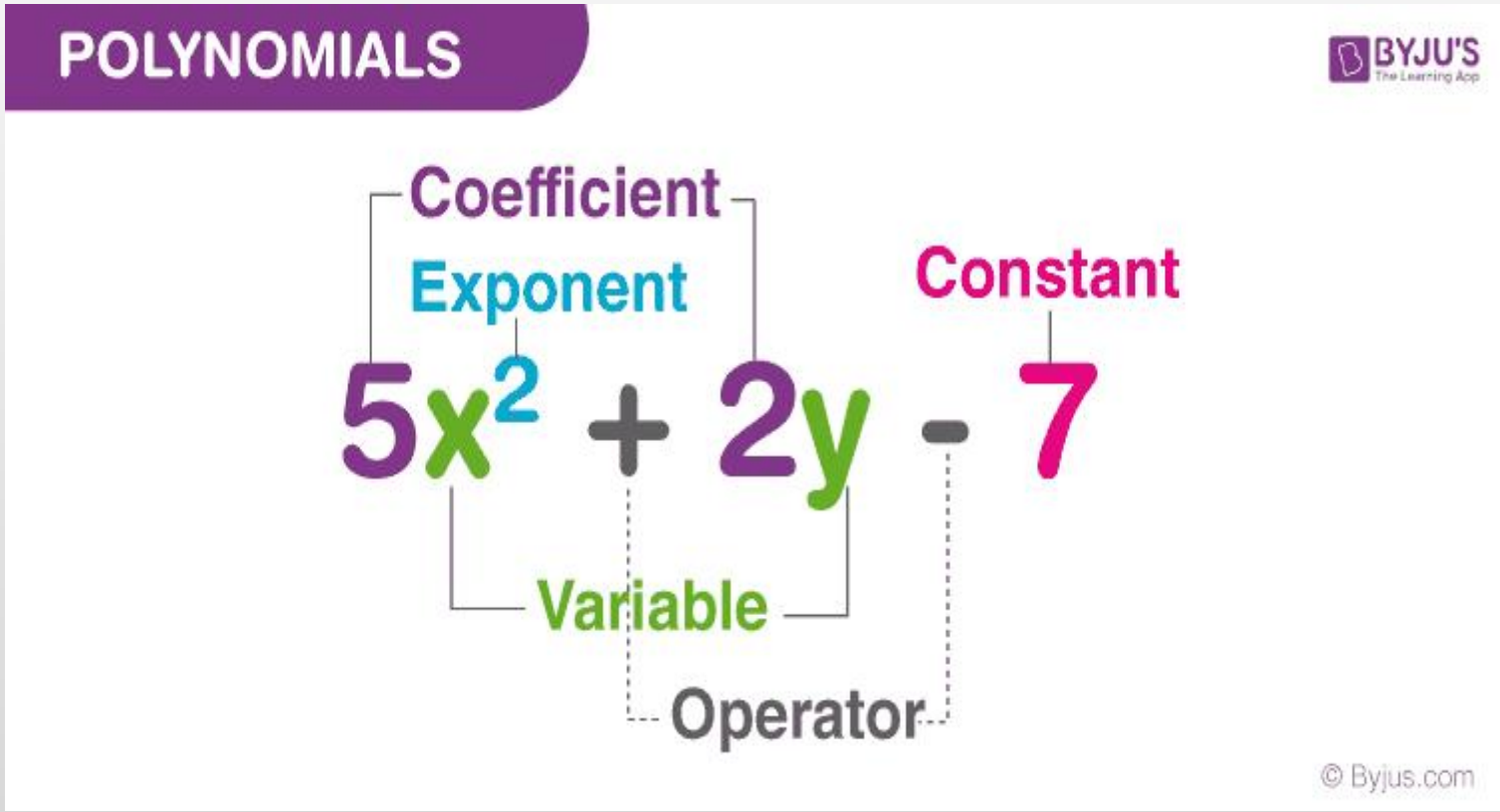


- INTRODUCTION OF POLYNOMIALS
- TYPES OF POLYNOMIALS
- DEGREES OF POLYNOMIAL
- POLYNOMIAL RINGS
- IRREDUCIBLE POLYNOMIAL
- PSEUDO RANDOM GENERATOR FOR POLYNOMIAL
- Applications of Polynomials in Abstract Algebra

POLYNOMIALS :

- Polynomials are algebraic expressions that consist of variables and coefficients.

- Addition, subtraction, multiplication, and also positive integer exponents can be perfomed for polynomial expressions.


POLYNOMIALS
BYJU'S
The Learning App
Coefficient
Exponent
Constant
5x² + 2y - 7
Variable
Operator
© Byjus.com

TYPES OF POLYNOMIALS

Monomials: A monomial is a polynomial expression that contains only one term. For example 4t, 21x, 2y, 9pq.

Binomials: A binomial is a polynomial with two, unlike terms. For example $3x + 4x^2$

Trinomial : A trinomial is a polynomial with three, unlike terms. For example, $3x + 5x^2 – 6x^3$ and $12pq + 4x^2 – 10$.

DEGREES OF POLYNOMIAL

Zero or constant polynomial

Polynomials with 0 degree. Example : 3 or 3x0

Linear polynomial

Polynomials with 1 as the degree. Example : x + y - 4, 5m + 7n, 2p

Quadratic polynomial

Polynomials with 2 as the degree . Example : 8x2 + 7y - 9, m2 + mn - 6

Cubic polynomial

Polynomials with 3 as the degree. Example : 3x3, p3 + pq + 7

POLYNOMIAL RINGS

A polynomial ring R[x] consists of polynomials where the coefficients come from a ring R.

Basic operations in polynomial rings:

- **Addition:** Combine like terms.
- **Multiplication:** Distribute terms and multiply coefficients.
- **Factorization:** Break down polynomials into irreducible factors.

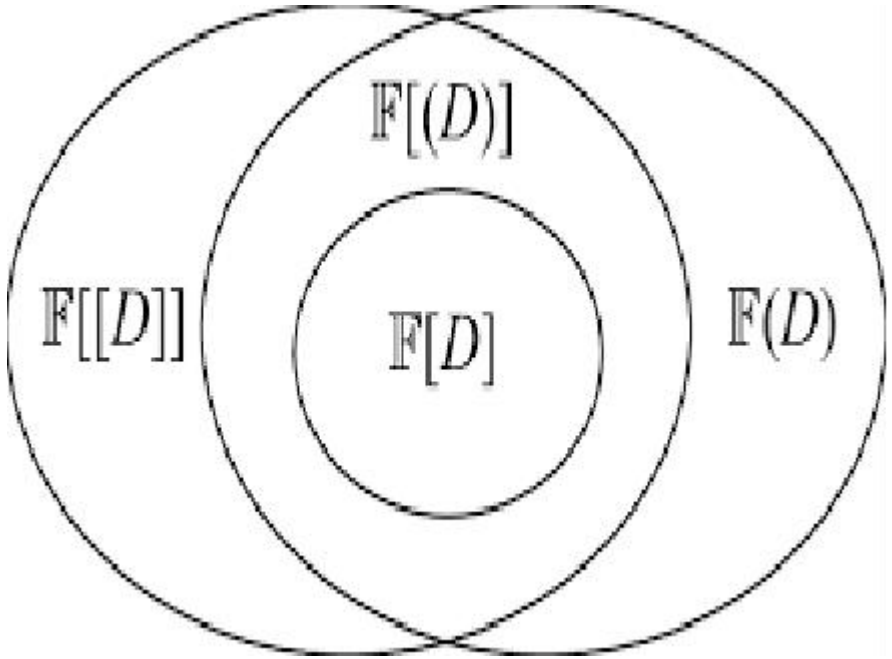


fig - Relationship among polynomial rings

IRREDUCIBLE POLYNOMIAL

- An irreducible polynomial is a polynomial that cannot be factored into the product of two non-constant polynomials.

- An irreducible polynomial is also called a prime polynomial.

The polynomial $x^2-2 \in Q[x]$ is irreducible since

Solution :

it cannot be factored any further over the rational numbers.

x^2+1 is irreducible over the real numbers.

PSEUDO RANDOM GENERATOR FOR POLYNOMIAL

- Pseudorandom generators for low-degree polynomials are a particular instance of a Pseudo Random Number Generator (PRNG)
- In statistical tests, the tests are considered as evaluations of low degree polynomials.
- Efficient procedure that maps a short truly random seed to a longer pseudorandom string .

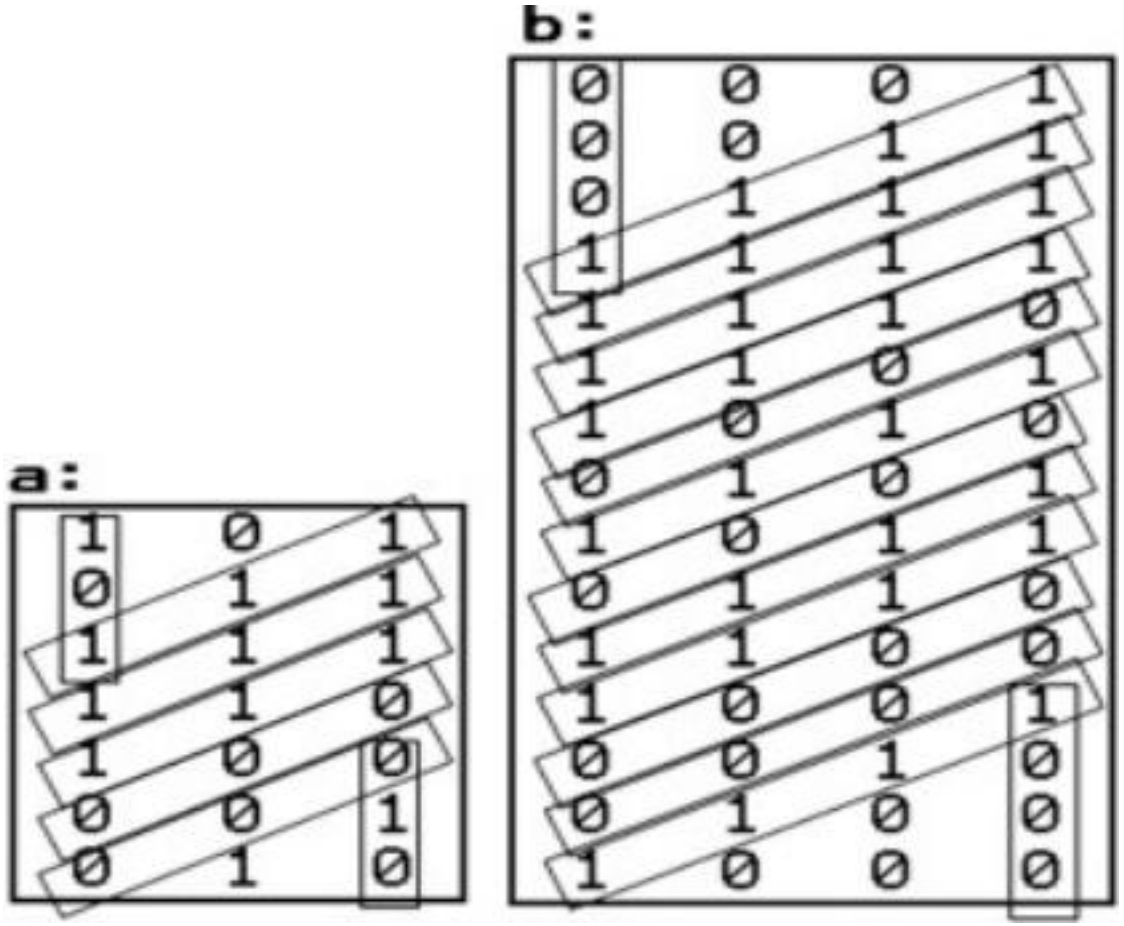


Figure : Pseudo random code generating

Applications of Polynomials in Abstract Algebra:

1. Coding Theory
2. Cryptography
3. Algebraic Geometry
4. Commutative Algebra

Reffenences ：

1. Abstract Algebra : Theory and Applications
Thomas W. Judson
2. Polynomial pseudo random number generator via cyclic phase
Angelo Marchi, Alfonso Del Giudice, Antonio Liverani
Faculty of Economics

THANK YOU