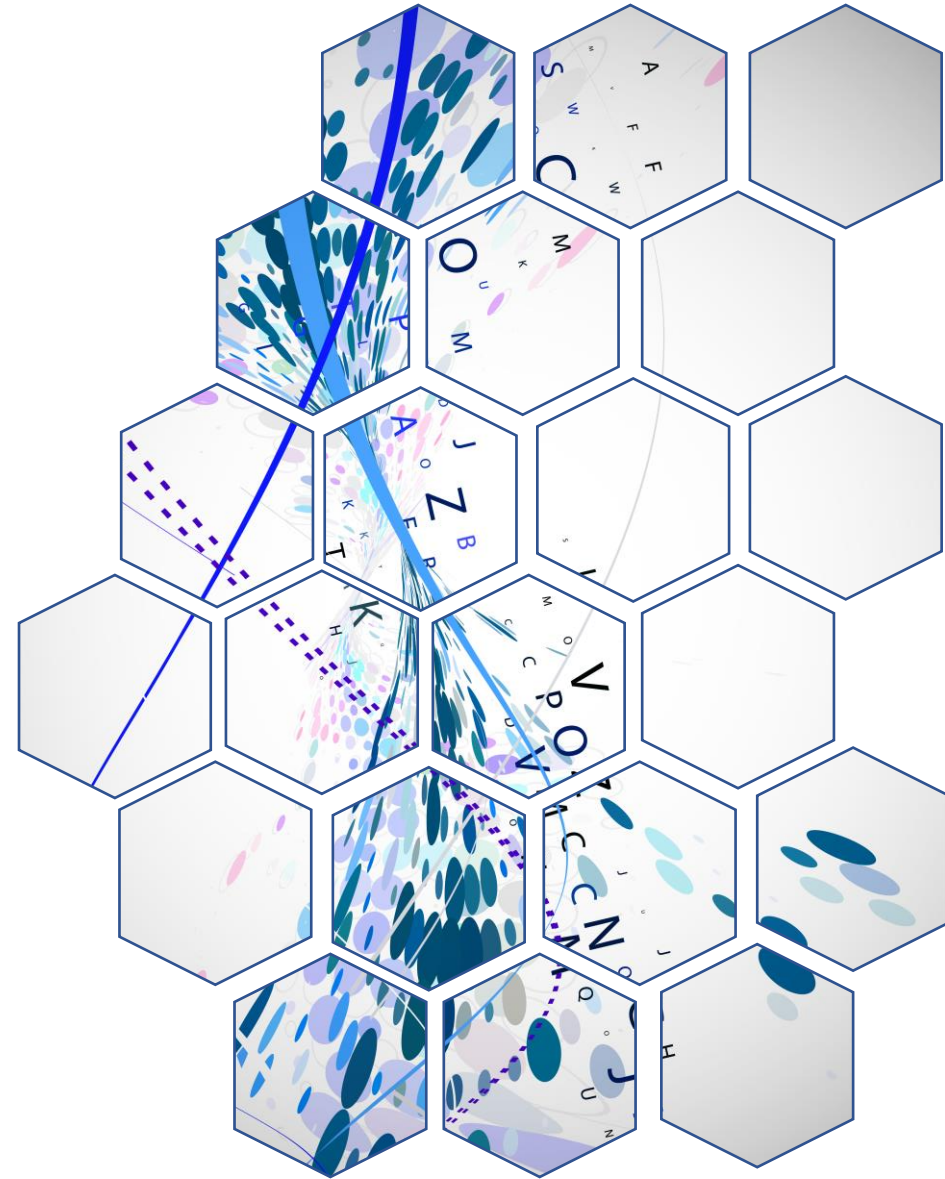


POLYNOMIAL

Abstract Algebra



Kh. Tahera Mehjabin
IT 23604

27th November 2024

OUTLINE :

- INTRODUCTION OF POLYNOMIALS
- TYPES OF POLYNOMIALS
- POLYNOMIAL RINGS
- IRREDUCIBLE POLYNOMIAL
- PSEUDO RANDOM GENERATOR FOR POLYNOMIAL
- POYNOMIAL PSEUDO-RANDOM NUMBER GENERATOR VIA CYCLIC PHASE



POLYNOMIALS :

- Polynomials are algebraic expressions that consist of variables and coefficients.
- Variables are also sometimes called indeterminates.
- We can perform arithmetic operations such as addition, subtraction, multiplication, and also positive integer exponents for polynomial expressions.

POLYNOMIALS

The diagram illustrates the components of the polynomial $5x^2 + 2y - 7$. The terms are color-coded: the first term $5x^2$ has a purple coefficient (5) and a blue exponent (2); the second term $2y$ has a purple coefficient (2) and a green variable (y); and the third term is a pink constant (7). Brackets and dashed lines connect the labels to the corresponding parts of the expression.

Coefficient
Exponent
Constant
Variable
Operator

$$5x^2 + 2y - 7$$

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 $3x^0$

Linear polynomial

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

Quadratic polynomial

Polynomials with 2 as the degree . Example :
 $8x^2 + 7y - 9$, $m^2 + mn - 6$

Cubic polynomial

Polynomials with 3 as the degree. Example : $3x^3$,
 $p^3 + pq + 7$

POLYNOMIAL RINGS

A polynomial ring or polynomial algebra is a ring formed from the set of polynomials in one or more indeterminates (traditionally also called variables) with coefficients in another ring, often a field.

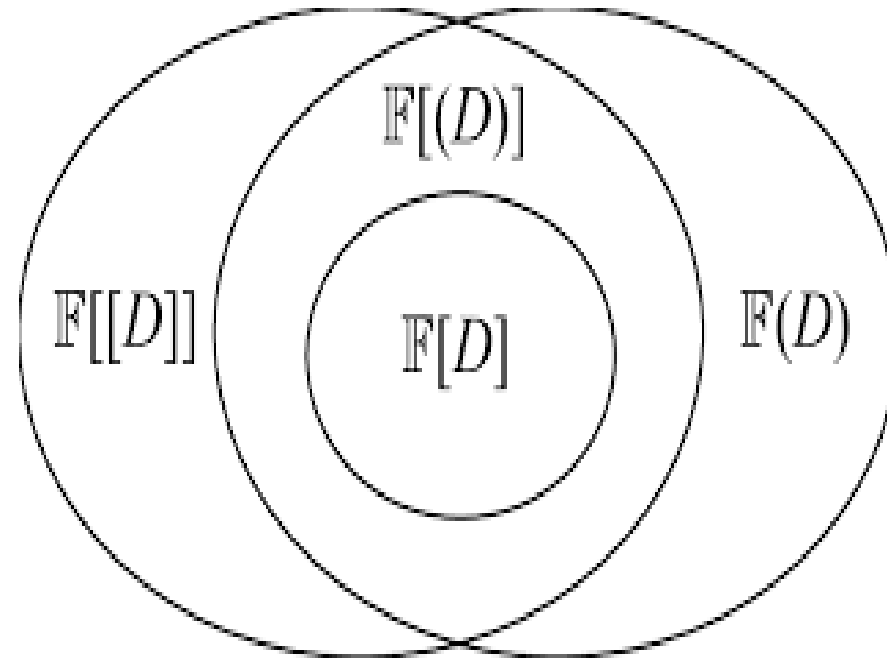


fig - Relationship among polynomial rings

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 $x^2 - 2 \in \mathbb{Q}[x]$ 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 .

POLYNOMIAL PSEUDO-RANDOM NUMBER GENERATOR VIA CYCLIC PHASE

Polynomials $f(x)$: $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n$; $f_i \in GF(p^n)$
are assigned to a Galois field $GF(0)$.

If a generic algebra $A(n)$ is defined in $GF(0)$ and modular arithmetic modulo p [12] is used, the algebraic field $Z(p)$ is the ring of quotients modulo the prime p (at least for the multiplication operator).

For example, addition of two polynomials in $GF(2)$ and $Z_3(2)$
modulo $(x^3 + x + 1)$ is: $f(x) = x^2 + 1$; $f_2(x) = x^2 + x$ $f(x) = \sum f_i(x)$
 $= f_1(x) + f_2(x) = x + 1$

This is the polynomial equation .

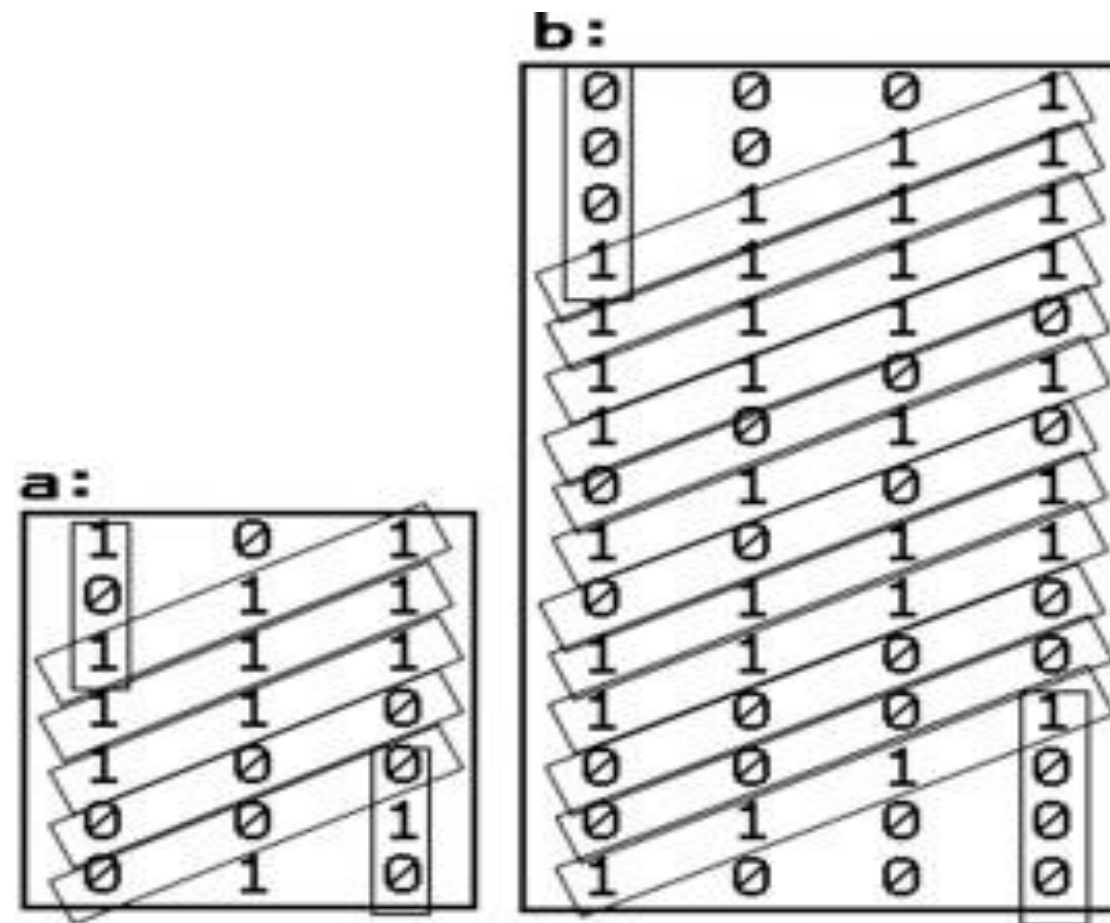


Figure : Pseudo random code generating