

Polynomial Rings

Polynomial Rings

1. Definition

- The set of all polynomials with coefficients from a ring R , denoted $R[x]$, forms a ring itself under polynomial addition and multiplication.

2. Degree of a Polynomial

- The highest power of x with a non-zero coefficient; important for understanding division and factorization.

3. Division Algorithm for Polynomials

- Similar to integer division: for polynomials $f(x)$ and $g(x)$ (g nonzero) over a field, there exist unique $q(x)$ and $r(x)$ such that $f(x) = q(x)g(x) + r(x)$, with degree of r less than degree of g .

4. Irreducible Polynomials

- Polynomials that cannot be factored into lower-degree polynomials over a given field, analogous to prime numbers in the integers.

5. Roots and Factorization

- A polynomial's roots relate directly to its factors: if a is a root, then $(x - a)$ is a factor.

6. Applications

- Polynomial rings underpin error-correcting codes, cryptographic systems, and the construction of finite fields used in computer science.