

A Fundamental Theorem for Polynomials

Theorem: Every monic polynomial factors uniquely into a product of powers of irreducible monic polynomials.

Proof: Every monic polynomial factors into a product of powers of irreducible polynomials, and after dividing through by leading coefficients, we may assume these irreducible polynomials are all monic.

Suppose a monic polynomial has two such factorizations:

$$P_1(X)^{\alpha_1} P_2(X)^{\alpha_2} \cdots P_n(X)^{\alpha_n} = Q_1(X)^{\beta_1} Q_2(X)^{\beta_2} \cdots Q_m(X)^{\beta_m}.$$

By Euclid's lemma, each $P_i(X)$ divides some $Q_j(X)$ and vice-versa. But since they are all monic and irreducible, this would mean each $P_i(X)$ is equal to some $Q_j(X)$ and vice-versa.

The following generic result is valid in any situation where you have the usual properties of addition and multiplication, the product of two non-zero elements is not zero, and an analogous version of Theorem 1.1.4 holds.

Generic Fundamental Theorem of Factoring: Every non-zero non-unit factors into a product of irreducible elements and units. Moreover, up to multiplication by units, the irreducible elements are unique.