Polynomial Rings Over Fields II

Kevin James

Proposition

The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proposition

Let $g(x)$ be a nonconstant polynomial in $F[x]$ and let

$$g(x) = f_1(x)^{e_1} f_2(x)^{e_2} \dots f_k(x)^{e_k}$$

be the factorization of $g(x)$ in $F[x]$, where the f_i are distinct. Then we have the following isomorphism of rings.

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{e_1}) \times \cdots \times F[x]/(f_k(x)^{e_k})$$

Proposition

If the polynomial $f(x)$ has roots $\alpha_1, \ldots, \alpha_k$ in F (not necessarily distinct), then $f(x)$ is divisible by $(x - \alpha_1) \ldots (x - \alpha_k)$. In particular, a polynomial of degree n over a field F has at most n roots in F, even counted with multiplicity.

Proposition

A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field the multiplicative group $F^\times$ of nonzero elements of F is a cyclic group.

Corollary

Let p be a prime. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Corollary

Let $2 \leq n \in \mathbb{Z}$ with $n = p_1^{a_1} \dots p_k^{a_k}$ where the p_i are distinct primes. We have the following isomorphisms of groups.

1. $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \cdots \times \left(\mathbb{Z}/p_k^{a_k}\mathbb{Z}\right)^\times$.
2. $(\mathbb{Z}/2^a\mathbb{Z})^\times \cong Z_2 \times Z_{2^{a-2}}$ *if* $a \geq 2$.
3. $(\mathbb{Z}/p^a\mathbb{Z})^\times \cong Z_{p^{a-1}(p-1)}$.