polynomial ring over a field

Canonical name	PolynomialRingOverAField
Date of creation	2013-03-22 17:42:55
Last modified on	2013-03-22 17:42:55
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	14
Author	pahio (2872)
Entry type	Theorem
Classification	msc 13F07
Related topic	FieldAdjunction
Related topic	PolynomialRingOverIntegralDomain
Related topic	PolynomialRingWhichIsPID
Defines	coprime

Theorem. The polynomial ring over a field is a Euclidean domain.

Proof. Let $K[X]$ be the polynomial ring over a field K in the indeterminate X. Since K is an integral domain and any polynomial ring over integral domain is an integral domain, the ring $K[X]$ is an integral domain.

The degree $\nu(f)$, defined for every f in $K[X]$ except the zero polynomial, satisfies the requirements of a Euclidean valuation in $K[X]$. In fact, the degrees of polynomials are non-negative integers. If f and g belong to $K[X]$ and the latter of them is not the zero polynomial, then, as is well known, the long division f/g gives two unique polynomials q and r in $K[X]$ such that

$$f \;=\; qg+r,$$

where $\nu(r) < \nu(g)$ or r is the zero polynomial. The second property usually required for the Euclidean valuation, is justified by

$$\nu(fg) \;=\; \nu(f)+\nu(g) \;\geqq\; \nu(f).$$

The theorem implies, similarly as in the ring $\mathbb{Z}$ of the integers, that one can perform in $K[X]$ a Euclid's algorithm which yields a greatest common divisor of two polynomials. Performing several Euclid's algorithms one obtains a gcd of many polynomials; such a gcd is always in the same polynomial ring $K[X]$.

Let d be a greatest common divisor of certain polynomials. Then apparently also kd, where k is any non-zero element of K, is a gcd of the same polynomials. They do not have other gcd's than kd, for if d' is an arbitrary gcd of them, then

$$d' \mid d \quad \text{and} \quad d \mid d',$$

i.e. d and d' are associates in the ring $K[X]$ and thus d' is gotten from d by multiplication by an element of the field K. So we can write the

Corollary 1. The greatest common divisor of polynomials in the ring $K[X]$ is unique up to multiplication by a non-zero element of the field K. The `http://planetmath.org/Monic2`monic gcd of polynomials is unique.

If the monic gcd of two polynomials is 1, they may be called *coprime.*

Using the Euclid's algorithm as in $\mathbb{Z}$, one can prove the

Corollary 2. If f and g are two non-zero polynomials in $K[X]$, this ring contains such polynomials u and v that

$$\gcd(f,\, g) \;=\; uf+vg$$

and especially, if f and g are coprime, then u and v may be chosen such that $uf+vg = 1$.

Corollary 3. If a product of polynomials in $K[X]$ is divisible by an irreducible polynomial of $K[X]$, then at least one `http://planetmath.org/Product`factor of the product is divisible by the irreducible polynomial.

Corollary 4. A polynomial ring over a field is always a principal ideal domain.

Corollary 5. The factorisation of a non-zero polynomial, i.e. the of the polynomial as product of irreducible polynomials, is unique up to constant factors in each polynomial ring $K[X]$ over a field K containing the polynomial. Especially, $K[X]$ is a UFD.

Example. The factorisations of the trinomial X^4-X^2-2 into monic irreducible prime factors are
$(X^2-2)(X^2+1)$ in $\mathbb{Q}[X]$,
$(X^2-2)(X+i)(X-i)$ in $\mathbb{Q}(i)[X]$,
$(X+\sqrt{2})(X-\sqrt{2})(X^2+1)$ in $\mathbb{Q}(\sqrt{2})[X]$,
$(X+\sqrt{2})(X-\sqrt{2})(X+i)(X-i)$ in $\mathbb{Q}(\sqrt{2},\, i)[X]$.