Algebraic Curves by William Fulton

Algebraic Preliminaries

slideshow by
William M. Faucette

University of West Georgia

Outline

1. Fundamental Definitions

Table of Contents

1 Fundamental Definitions

Fundamental Definitions

When we speak of a **ring**, we shall always mean a commutative ring with a multiplicative identity.

A **ring homomorphism** from one ring to another must take the multiplicative identity of the first ring to that of the second.

A **domain**, or integral domain, is a ring (with at least two elements) in which the cancellation law holds.

A **field** is a domain in which every nonzero element is a unit, i.e. has a multiplicative inverse.

Fundamental Definitions

The letter $\mathbb{Z}$ will denote the domain of integers, while $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ will denote the fields of rational, real, and complex numbers, respectively.

Fundamental Definitions

Any domain R has a quotient field K, which is a field containing R as a **subring**, and any element in K may be written (not necessarily uniquely) as a ratio of two elements of R.

Any one-to-one ring homomorphism from R to a field L extends uniquely to a ring homomorphism from K to L.

Any ring homomorphism from a field to a nonzero ring is one-to-one.

Fundamental Definitions

For any ring R, $R[X]$ denotes the ring of polynomials with coefficients in R.

The **degree** of a nonzero polynomial $\sum a_i X^i$ is the largest integer d such that $a_d \neq 0$; the polynomial is **monic** if $a_d = 1$.

Fundamental Definitions

The ring of polynomials in n variables over R is written $R[X_1, \ldots, X_n]$.

We often write $R[X, Y]$ or $R[X, Y, Z]$ when $n = 2$ or 3.

The monomials in $R[X_1, \ldots, X_n]$ are the polynomials $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$, i_j nonnegative integers; the degree of the monomial is $i_1 + \cdots + i_n$. Every $F \in R[X_1, \ldots, X_n]$ has a unique expression $F = \sum a_{(i)} X^{(i)}$, where the $X^{(i)}$ are the monomials, $a_{(i)} \in R$.

Fundamental Definitions

We call F **homogeneous**, or a **form**, of degree d, if all coefficients $a_{(i)}$ are zero except for monomials of degree d.

Any polynomial F has a unique expression $F = F_0 + F_1 + \cdots + F_d$, where F_i is a form of degree i; if $F_d \neq 0$, d is the **degree** of F, written $\deg(F)$.

The terms F_0, F_1, F_2, ... are called the **constant, linear, quadratic**, ... terms of F; F is **constant** if $F = F_0$.

The zero polynomial is allowed to have any degree.

If R is a domain, $\deg(FG) = \deg(F) + \deg(G)$.

Fundamental Definitions

The ring R is a subring of $R[X_1, \ldots, X_n]$, and $R[X_1, \ldots, X_n]$ is characterized by the following property: if φ is a ring homomorphism from R to a ring S, and $s_1, \ldots, s_n$ are elements in S, then there is a unique extension of φ to a ring homomorphism $\widetilde{\varphi}$ from $R[X_1, \ldots, X_n]$ to S such that $\widetilde{\varphi}(X_i) = s_i$, for $1 \leq i \leq n$. The image of F under $\widetilde{\varphi}$ is written $F(s_1, \ldots, s_n)$.

The ring $R[X_1, \ldots, X_n]$ is canonically **isomorphic** to $R[X_1, \ldots, X_{n-1}][X_n]$.

Fundamental Definitions

An element a in a ring R is **irreducible** if it is not a unit or zero, and for any factorization $a = bc$, $b, c \in R$, either b or c is a unit. A domain R is a **unique factorization domain**, written UFD, if every nonzero element in R can be factored uniquely, up to units and the ordering of the factors, into irreducible elements.

Fundamental Definitions

If R is a UFD with quotient field K, then (by Gauss) any irreducible element $F \in R[X]$ remains irreducible when considered in $K[X]$; it follows that if F and G are polynomials in $R[X]$ with no common factors in $R[X]$, they have no common factors in $K[X]$.

Fundamental Definitions

If R is a UFD, then $R[X]$ is also a UFD. Consequently $k[X_1, \ldots, X_n]$ is a UFD for any field k. The quotient field of $k[X_1, \ldots, X_n]$ is written $k(X_1, \ldots, X_n)$, and is called the **field of rational functions** in n variables over k.

Fundamental Definitions

If $\varphi : R \to S$ is a ring homomorphism, the set $\varphi^{-1}(0)$ of elements mapped to zero is the **kernel** of φ, written $\mathrm{Ker}(\varphi)$. It is an **ideal** in R. An ideal I in a ring R is **proper** if $I \neq R$. A proper ideal is **maximal** if it is not contained in any larger proper ideal. A **prime** ideal is an ideal I such that whenever $ab \in I$, either $a \in I$ or $b \in I$.

Fundamental Definitions

A set S of elements of a ring R **generates** an ideal $I = \{\sum a_i s_i \mid s_i \in S, a_i \in R\}$. An ideal is **finitely generated** if it is generated by a finite set $S = \{f_1, \ldots, f_n\}$; we then write $I = (f_1, \ldots f_n)$.

An ideal is **principal** if it is generated by one element. A domain in which every ideal is principal is called a **principal ideal domain**, written PID. The ring of integers $\mathbb{Z}$ and the ring of polynomials $k[X]$ in one variable over a field k are examples of PID's.

Every PID is a UFD. A principal ideal $I = (a)$ in a UFD is prime if and only if a is irreducible (or zero).

Fundamental Definitions

Let I be an ideal in a ring R. The **residue class ring** of R modulo I is written R/I; it is the set of equivalence classes of elements in R under the equivalence relation: $a \sim b$ if $a - b \in I$. The equivalence class containing a may be called the I-residue of a; it is often denoted by $\overline{a}$.

The classes R/I form a ring in such a way that the mapping $\pi : R \to R/I$ taking each element to its I-residue is a ring homomorphism.

The ring R/I is characterized by the following property: if $\varphi : R \to S$ is a ring homomorphism to a ring S, and $\varphi(I) = 0$, then there is a unique ring homomorphism $\overline{\varphi} : R/I \to S$ such that $\varphi = \overline{\varphi} \circ \pi$.

A proper ideal I in R is prime if and only if R/I is a domain, and maximal if and only if R/I is a field. Every maximal ideal is prime.

Fundamental Definitions

Let k be a field, I a proper ideal in $k[X_1, \ldots, X_n]$. The canonical homomorphism π from $k[X_1, \ldots, X_n]$ to $k[X_1, \ldots, X_n]/I$ restricts to a ring homomorphism from k to $k[X_1, \ldots, X_n]/I$. We thus regard k as a subring of $k[X_1, \ldots, X_n]/I$; in particular $k[X_1, \ldots, X_n]/I$ is a vector space over k.

Fundamental Definitions

Let R be a domain. The **characteristic** of R, $\operatorname{char}(R)$, is the smallest integer p such that $1 + \cdots + 1$ (p times)$= 0$, if such a p exists; otherwise $\operatorname{char}(R) = 0$. If $\varphi : \mathbb{Z} \to R$ is the unique ring homomorphism from $\mathbb{Z}$ to R, then $\operatorname{Ker}(\varphi) = (p)$, so $\operatorname{char}(R)$ is a prime number or zero.

Fundamental Definitions

If R is a ring, $a \in R$, $F \in R[X]$, and a is a *root* of F, then $F = (X - a)G$ for a unique $G \in R[X]$. A field k is **algebraically closed** if any nonconstant $F \in k[X]$ has a root. It follows that $F = \mu \prod (X - \lambda_i)^{e_i}$, $\mu, \lambda_i \in k$, where the λ_i are the distinct roots of F, and e_i is the **multiplicity** of λ_i. A polynomial of degree d has d roots in k, counting multiplicities. The field $\mathbb{C}$ of complex numbers is an algebraically closed field.

Fundamental Definitions

Let R be any ring. The **derivative** of a polynomial $F = \sum a_i X^i \in R[X]$ is defined to be $\sum i a_i X^{i-1}$, and is written either $\frac{\partial F}{\partial X}$ or F_X.

If $F \in R[X_1, \ldots, X_n]$, $\frac{\partial F}{\partial X_i} = F_{X_i}$ is defined by considering F as a polynomial in X_i with coefficients in $R[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$.

Fundamental Definitions

The following rules are easily verified:

1. $(aF + bG)_X = aF_X + bG_X$, a, $b \in R$.
2. $F_X = 0$ if F is a constant.
3. $(FG)_X = F_X G + FG_X$, and $(F^n)_X = nF^{n-1}F_X$.
4. If $G_1, \ldots, G_n \in R[X]$, and $F \in R[X_1, \ldots, X_n]$, then

$$F(G_1, \ldots, G_n)_X = \sum_{i=1}^{n} F_{X_i}(G_1, \ldots, G_n)(G_i)_X.$$

5. $F_{X_i X_j} = F_{X_j X_i}$, where we have written $F_{X_i X_j}$ for $(F_{X_i})_{X_j}$.
6. (*Euler's Theorem*) If F is a form of degree m in $R[X_1, \ldots, X_n]$, then

$$mF = \sum_{i=1}^{n} X_i F_{X_i}.$$