

Introduction

Oh hey, it's another one of these independent studies. Me and a friend are going to be going through William Fulton's *Algebraic Curves*. It will be hard, it will be long, and it might not work out for me, but who cares.

Contents

Introduction	1
Affine Algebraic Sets	1
Algebraic Preliminaries	1

Affine Algebraic Sets

Algebraic Preliminaries

We will assume all rings are commutative with unity, where \mathbb{Z} is the integers, \mathbb{Q} is the rationals, \mathbb{R} is the reals, and \mathbb{C} is the complex numbers.

Any integral domain R has a quotient field K , which contains R as a subring, and any element in K may be written as a not necessarily unique 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 .

If R is a ring, then $R[x]$ is 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 $a_d = 1$.

The ring of polynomials in n variables over R is $R[x_1, \dots, x_n]$. We write $R[x, y]$ and $R[x, y, z]$ if $n = 2$ and 3 respectively. Monomials in $R[x_1, \dots, x_n]$ are of the form $x^{(i)} := x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, where i_j are nonnegative integers, and the degree of the monomial is $i_1 + \cdots + i_n$. Every $F \in R[x_1, \dots, x_n]$ has a unique expression $F = \sum a_{(i)} x^{(i)}$, where $x^{(i)}$ are monomials, and $a_{(i)} \in R$. We say F is homogeneous of degree d if all $a_{(i)}$ are zero except for monomials of degree d . The polynomial F is written as $F = F_0 + F_1 + \cdots + F_d$, where F_i is a form of degree i , and $d = \deg(F)$ for $F_d \neq 0$.

The ring R is a subring of $R[x_1, \dots, x_n]$, and the ring $R[x_1, \dots, x_n]$ is characterized by the following: if $\varphi: R \rightarrow S$ is a ring homomorphism, and s_1, \dots, s_n are elements in S , then there is a unique extension of φ to a ring homomorphism $\bar{\varphi}: R[x_1, \dots, x_n] \rightarrow S$ such that $\bar{\varphi}(x_i) = s_i$. The image of F under $\bar{\varphi}$ is written $F(s_1, \dots, s_n)$. The ring $R[x_1, \dots, x_n]$ is canonically isomorphic to $R[x_1, \dots, x_{n-1}][x_n]$.

An element $a \in R$ is called irreducible if it is not a unit or zero, and any factorization $a = bc$ with $b, c \in R$ is such that either b or c is a unit. A domain R is a unique factorization domain (UFD) if every nonzero element in R can be factored uniquely up to units and ordering.

If R is a UFD with quotient field K , then any irreducible element $F \in R[x]$ remains irreducible when considered in $K[x]$.

Theorem (Gauss's Lemma for \mathbb{Z}): If $F \in \mathbb{Z}[x]$ is a monic polynomial that is irreducible, then F is irreducible in $\mathbb{Q}[x]$.

If F and G are polynomials in $R[x]$ with no common factors in $R[x]$, then they have no common factors in $K[x]$.

If R is a UFD, then $R[x]$ is also a UFD, and consequently $k[x_1, \dots, x_n]$ is a UFD for any field k . The quotient field of $k[x_1, \dots, x_n]$ is written $k(x_1, \dots, x_n)$ is called the field of rational functions in n variables over k .

If $\varphi: R \rightarrow S$ is a ring homomorphism, $\ker(\varphi) := \varphi^{-1}(0)$. The kernel is an ideal in R . An ideal in R is proper if $I \neq R$, and a proper ideal is known as maximal if it is not contained in any larger proper ideal.^I An ideal \mathfrak{p} is prime if, whenever $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.^{II}

Let k be a field and I a proper ideal in $k[x_1, \dots, x_n]$. The canonical homomorphism π from $k[x_1, \dots, x_n]$ to $k[x_1, \dots, x_n]/I$ restricts to a ring homomorphism from k to $k[x_1, \dots, x_n]/I$. We regard k as a subring of $k[x_1, \dots, x_n]/I$, which is a vector space over k .

If R is an integral domain, then $\text{char}(R)$, the characteristic of R , is the smallest integer p such that

$$\underbrace{1 + 1 + \dots + 1}_{p \text{ times}} = 0.$$

If p exists, we say $\text{char}(R) = p$, else 0.

Note that if $\varphi: \mathbb{Z} \rightarrow R$ is the unique ring homomorphism from \mathbb{Z} to R ,^{III} then $\ker(\varphi) = \langle p \rangle$, so $\text{char}(R)$ is prime or 0.

If R is a ring, and $F \in R[x]$, and a is a root of F , then $F = (x - a)G$ for some unique polynomial $G \in R[x]$. A field k is algebraically closed if any nonconstant $F \in k[x]$ has a root.

Exercise (Exercise 1.1): Let R be an integral domain.

- (a) If F and G are forms of degree r and s respectively in $R[x_1, \dots, x_n]$, show that FG is a form of degree $r + s$.
- (b) Show that any factor of a form in $R[x_1, \dots, x_n]$ is also a form.

Exercise (Exercise 1.2): Let R be a UFD and K the quotient field of R . Show that every element $z \in K$ may be written as $z = a/b$, where $a, b \in R$ have no common factors. This representative is unique up to units of R .

Solution:

Exercise (Exercise 1.3): Let R be a principal ideal domain, and let P be a nonzero proper prime ideal in R .

- (a) Show that P is generated by an irreducible element.
- (b) Show that P is maximal.

Solution:

- (a) Since P is principal, we know that $P = \langle a \rangle$ for some $a \in R$. We know that a cannot be a unit, as otherwise $P = R$, contradicting the assumption that P is proper, and that $a \neq 0$ as P is not zero.

Suppose toward contradiction that $\langle a \rangle \subsetneq \langle b \rangle$ for some $b \in R$. Then, $a = bc$ for some $c \in R$. If $c \notin \langle a \rangle$, then since $\langle a \rangle$ is prime, we must have $b \in \langle a \rangle$, contradicting strict inclusion. Thus, $c \in \langle a \rangle$, so $c = at$ for some $t \in R$. Therefore, we have $a = abt$, so $bt = 1_R$, and $\langle b \rangle = R$.

- (b) Since R is a PID, and P is prime, we know that $P = \langle a \rangle$ is generated by an irreducible element. Thus, if $\langle a \rangle \subsetneq \langle b \rangle$, then $a = bc$ for some $c \in R$. Since we have unique factorization (as all PIDs are UFDs), and a is irreducible, this means either b or c is a unit. If b is a unit, then $\langle b \rangle = R$, and if c is a unit, then $\langle b \rangle = \langle a \rangle$. Thus, $\langle a \rangle$ is maximal.

Exercise (Exercise 1.4): Let k be an infinite field, $f \in k[x_1, \dots, x_n]$. Suppose $F(a_1, \dots, a_n) = 0$ for all $a_1, \dots, a_n \in k$. Show that $f = 0$.

Exercise (Exercise 1.5): Let k be any field. Show that there are an infinite number of irreducible monic polynomials in $k[x]$.

^IAlternatively, an ideal I is maximal if the quotient ring R/I is a field.

^{II}Alternatively, an ideal \mathfrak{p} is prime if R/\mathfrak{p} is an integral domain.

^{III}This is because \mathbb{Z} is initial in the category of rings. See Aluffi.

Solution: Suppose F_1, \dots, F_n were all the irreducible monic polynomials in $k[x]$. Consider the polynomial $P = F_1 F_2 \cdots F_n + 1$. We note that P is monic. We will show that P is irreducible.

Suppose toward contradiction that P were reducible. We know that $k[x]$ is a principal ideal domain, so $P \in \langle F_i \rangle$ for some irreducible monic F_i . However, we know that, for any F_i , $1 \leq i \leq n$, $P \nmid F_i$, as, applying the division algorithm to P , we get

$$P = (F_i) \prod_{j \neq i} F_j + 1,$$

where $r \neq 0$. Thus, P is not reducible and monic, so there are infinitely many irreducible monic polynomials in $k[x]$.

Exercise (Exercise 1.6): Show that any algebraically closed field is infinite.

Solution: Note that if k is any field, then there are infinitely many irreducible monic polynomials in $k[x]$. If k is algebraically closed, then $(x - a)$, for $a \in k$, is the only irreducible monic polynomial. Since there are infinitely many irreducible monic polynomials in $k[x]$, there are infinitely many $a \in k$ such that $(x - a)$ is irreducible in $k[x]$. Thus, k is infinite.

Exercise (Exercise 1.7): Let k be any field, and $F \in k[x_1, \dots, x_n]$, with $a_1, \dots, a_n \in k$.

(a) Show that

$$F = \sum \lambda_{(i)} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n},$$

where $\lambda_{(i)} \in k$.

(b) If $F(a_1, \dots, a_n) = 0$, show that $F = \sum_{i=1}^n (x_i - a_i) G_i$ for some not necessarily unique $G_i \in k[x_1, \dots, x_n]$.