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

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 $\varphi\colon R \to S$ is a ring homomorphism, and $s_1, \dots, x_n$ are elements in S, then there is a unique extension of φ to a ring homomorphism $\overline{\varphi}\colon R[x_1, \dots, x_n] \to S$ such that $\overline{\varphi}(x_i) = s_i$. The image of F under $\overline{\varphi}$ 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 $\varphi \colon R \to S$ 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 $\operatorname{char}(R)$, the characteristic of R, is the smallest integer p such that

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

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

Note that if $\varphi \colon \mathbb{Z} \to R$ is the unique ring homomorphism from $\mathbb{Z}$ to R,[III] then $\ker(\varphi) = \langle p \rangle$, so $\operatorname{char}(R)$ 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: Since $K = \operatorname{Frac}(R)$, we know that every $z \in K$ is of the form $z = \frac{a}{b}$. Since R a unique factorization domain, $\gcd(a, b)$ is unique and well-defined. Set $c \cdot \gcd(a, b) = a$ and $d \cdot \gcd(a, b) = b$. Then,

$$\begin{aligned} z &= \frac{a}{b} \\ &= \frac{c \cdot \gcd(a, b)}{d \cdot \gcd(a, b)} \\ &= \frac{c}{d}. \end{aligned}$$

We show that this is unique up to units. Suppose

$$\begin{aligned} z &= \frac{c}{d} \\ &= \frac{c'}{d'}. \end{aligned}$$

Then, by the properties of the field of fractions, we know that

$$c'd = cd',$$

and since R is a UFD, we know that $\gcd(c, d) = \gcd(c', d') = 1$, so $c = u_1 c'$ and $d = u_2 d'$.

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.

[I] Alternatively, an ideal I is maximal if the quotient ring R/M 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.

(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 $\langle a \rangle \subseteq \langle b \rangle$, 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 $k[x]$.

Solution: Suppose $F_1, \dots, F_n$ were all the irreducible monic polynomials in $k[x]$. Consider the polynomial $P = F_1F_2 \cdots F_n + 1$. 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, $1 \leqslant i \leqslant n$, $P \nmid F_i$, 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 polynoimals 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 $G_i \in k[x_1, \dots, x_n]$.

Solution:

(a) We let

$$G = F(x_1 + a_1, x_2 + a_2, \dots, x_n + a_n).$$

Then, since $G \in k[x_1, \dots, x_n]$, we have

$$G = \sum \lambda_{(i)} x_1^{i_1} \cdots x_n^{i_n}.$$

Then, we have

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

(b)

Affine Space and Algebraic Sets

Definition. If k is a field, then when we write $\mathbb{A}^n(k)$, or $\mathbb{A}^n$, to be the cartesian product of k with itself n times.

We call $\mathbb{A}^n(k)$ the affine n-space over k. Its elements are called points. We call $\mathbb{A}^1(k)$ the affine line and $\mathbb{A}^2(k)$ the affine plane.

Definition. If $F \in k[x_1, \dots, x_n]$, then $P = (a_1, \dots, a_n) \in \mathbb{A}^n(k)$ is called a zero of F if $F(P) = (a_1, \dots, a_n) = 0$.

If F is not constant, then the zeros of F are called the hypersurface defined by F, defined by $V(F)$. A hypersurface in $\mathbb{A}^2(k)$ is called an affine plane curve.

If F is a polynomial of degree 1, then $V(F)$ is called a hyperplane in $\mathbb{A}^n(k)$; if $n = 2$, then an affine hyperplane is a line.

Definition. If S is any set of polynomials in $k[x_1, \dots, x_n]$, then $V(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ for all } F \in S\}$. In other words, $V(S) = \bigcap_{F \in S} V(F)$. If $S = \{F_1, \dots, F_r\}$, we write $V(F_1, \dots, F_r)$.

A subset $X \subseteq \mathbb{A}^n(k)$ is an affine algebraic set (or algebraic set) if $X = V(S)$ for some S.

Proposition:

(1) If I is the ideal in $k[x_1, \dots, x_n]$ generated by S, then $V(S) = V(I)$; thus, every algebraic set is equal to $V(I)$ for some ideal I.

(2) If $\{I_\alpha\}$ is a collection of ideals, then $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$.

(3) If $I \subseteq J$, then $V(I) \supseteq V(J)$.

(4) For any polynomialsF, G, $V(FG) = V(F) \cup V(G)$. Furthermore, $V(I) \cup V(J) = V(\{FG \mid F \in I, G \in J\})$.

(5) We have that $V(0) = \mathbb{A}^n(k)$, $V(1) = \emptyset$, $V(x_1 - a_1, \dots, x_n - a_n) = \{(a_1, \dots, a_n)\}$ for $a_i \in k$. Thus, any finite subset of $\mathbb{A}^n(k)$ is an algebraic set.

Exercise (Exercise 1.8)**:** Show that the algebraic subsets of $\mathbb{A}^1(k)$ are just the finite subsets together with $\mathbb{A}^1(k)$ itself.

Solution: Since $k[x]$ is a principal ideal domain, we know that the zero set $V(S)$ for any $S \subseteq k[x]$ is of the form $V(\langle f \rangle) = V(f)$, where $f \in k[x]$. Since f is a polynomial, f has finitely many roots, so there are finitely many elements in the algebraic subset.

Additionally, since $0 \in k[x]$, we know that k is also an algebraic subset.

Exercise (Exercise 1.14)**:** Let F be a nonconstant polynomial in $k[x_1, \dots, x_n]$, where k is algebraically closed. Show that $\mathbb{A}^n(k) \setminus V(F)$ is infinite if $n \geqslant 1$ and that $V(F)$ is infinite if $n \geqslant 2$. Conclude that the complement of any proper algebraic set is infinite.

Solution: We know that k is infinite as k is algebraically closed.

Exercise (Exercise 1.15)**:** Let $V \subseteq \mathbb{A}^n(k)$ and $W \subseteq \mathbb{A}^m(k)$ be algebraic sets. Show that

$$V \times W = \{(a_1, \dots, a_n, b_1, \dots, b_m) \mid (a_1, \dots, a_n) \in V, (b_1, \dots, b_m) \in W\}$$

is an algebraic set in $\mathbb{A}^{n+m}(k)$. It is called the product of V and W.

Solution: Consider the set of polynomials in $k[x_1, \dots, x_n, x_{n+1}, \dots, x_{n+m}]$ given by $P = F(x_1, \dots, x_n) + G(x_{n+1}, \dots, x_m)$, where F is a polynomial in the ideal whose algebraic set is V and G is an ideal in the algebraic set whose ideal is W. Then, the collection of zeros are those of the form $(a_1, \dots, a_n, b_1, \dots, b_m)$, where $(a_1, \dots, a_n) \in V$ and $(b_1, \dots, b_m) \in W$.