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.

Solution:

(a) Let $H = FG$, where F is a form of degree r and G is a form of degree s. Note that since F and G are forms, we know that $F = F_r$, where F_r is the form with degree r, and $G = G_s$, where G_s is the form with degree s.

[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.

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 $K = \text{Frac}(R)$, 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 $c = u_1c'$ and $d = u_2d'$.

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 $\langle a \rangle \subseteq \langle b \rangle$, 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) Note that if $F(a_1, \dots, a_n) = 0$, then $(x_i - a_i) \mid F(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n)$. Thus, we have

$$F(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n) = (x_i - a_i)\underbrace{g(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n)}_{G_i}.$$

This yields

$$F(x_1, \dots, x_n) = \sum_{i=1}^{n}(x_i - a_i)G_i.$$

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.

Let $F \in k[x_1, \dots, x_n] \cong k[x_1, \dots, x_{n-1}][x_n]$.

In the base case with $n = 1$, we know that there are finitely many roots in $\mathbb{A}^1(k)$, so we have the base case. If $n \geqslant 2$, then we write $F = \sum G_i x_n^i$. We know that since F is nonzero, then there is at least one nonzero G_i. We showed in Exercise 1.4 that there is some $a_1, \dots, a_{n-1} \in k$ such that $G_i(a_1, \dots, a_{n-1}) \neq 0$. Thus, $F(a_1, \dots, a_{n-1}, x_n)$ is not the zero polynomial, meaning there are finitely many roots, and thus infinitely many non-roots.

Thus, there are infinitely many $a_1, \dots, a_n \in k$ with $a_1, \dots, a_n \neq 0$.

We write $F = \sum G_i x_n^i$. We know that if all the G_i are constant, then we have a single-variable polynomial in x_n, and any choice of $a_1, \dots, a_{n-1} \in k$ provide other elements of $V(F)$. We assume that there is some G_i that is a nonconstant polynomial in $x_1, \dots, x_{n-1}$.

Since G_i is nonzero, we may use the previous paragraph to state that G_i has infinitely many non-roots, and for each choice of those $a_1, \dots, a_{n-1}$, we have a polynomial in x_n. This polynomial has a root, meaning there are infinitely many roots.

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 $(b_1, \dots, b_m) \in W$.

Solution (A Real Solution)**:** We have that V and W are defined by $\{F_1, \dots, F_r\}$ and $\{G_1, \dots, G_s\}$ for some polynomials. We define $V \times W$ to be the algebraic set defined by the polynomials in $\{F_1, \dots, F_r, G_1, \dots, G_s\}$ that are constant with respect to the other variables.

The Ideal of a Set of Points

Definition. If $X \subseteq \mathbb{A}^n(k)$, then the polynomials that vanish on X form an ideal in $k[x_1, \dots, x_n]$, called the ideal of X, or I(X).

$$I(X) := \{F \in k[x_1, \dots, x_n] \mid F(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in X\}.$$

The following hold.

- If $X \subseteq Y$, then $I(X) \supseteq I(Y)$.
- We have $I(\emptyset) = k[x_1, \dots, x_n]$, $I(\mathbb{A}^n(k)) = \langle 0 \rangle$ if k is infinite, and $I(\{(a_1, \dots, a_n)\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ for $a_1, \dots, a_n \in k$.
- We have $I(V(S)) \supseteq S$ for any set S of polynomials, and $V(I(X)) \supseteq X$ for any set X of points.
- We have $V(I(V(S))) = V(S)$ for any set of polynomials S, and $I(V(I(X))) = I(X)$ for any set X of points. If V is an algebraic set, $V = V(I(V))$ and if I is the ideal of an algebraic set, then $I = I(V(I))$.

Definition. If I is any ideal in a ring R, we define the radical of I, written $\text{rad}(I) = \{a^n \mid a \in I \text{ for some } n > 0\}$. We have that rad(I) is an ideal containing I. An ideal I is called a radical ideal if $I = \text{rad}(I)$.

- We have I(X) is a radical ideal for any $X \subseteq \mathbb{A}^n(k)$.

Exercise (Exercise 1.16)**:** Let V and W be algebraic sets in $\mathbb{A}^n(k)$. Show that $V = W$ if and only if $I(V) = I(W)$.

Solution: Let $V = W$. Then, if $F \in I(V)$, then $F = 0$ on W, so $F \in I(W)$, and vice versa.

Suppose $I(V) = I(W)$. We know that $V(I(V)) = V$ and $V(I(W)) = W$. Thus, if $(a_1, \dots, a_n) \in V$, we know that for all $F \in I(W)$, that $F(a_1, \dots, a_n) = 0$ as $F \in I(V)$, meaning $(a_1, \dots, a_n) \in V(I(W)) = W$. By symmetry, we have $V = W$.

Exercise (Exercise 1.17)**:**

(a) Let V be an algebraic set in $\mathbb{A}^n(k)$ and $P \in \mathbb{A}^n(k)$ not a point in V. Show that there is a polynomial $F \in k[x_1, \dots, x_n]$ such that $F(Q) = 0$ for all $Q \in V$ but $F(P) = 1$.

(b) Let $P_1, \dots, P_r$ e distinct points in $\mathbb{A}^n(k)$ not in an algebraic set V. Show that there are polynomials $F_1, \dots, F_r \in I(V)$ such that $F_i(P_j) = \delta_{ij}$.

(c) With $P_1, \dots, P_r$ and V as in (b), and $a_{ij} \in k$ for $1 \leqslant i, j \leqslant r$, show that there are $G_i \in I(V)$ such that $G_i(P_j) = a_{ij}$ for all i and j.

Solution:

(a) We know that there is some $F \in I(V)$ such that $F(P) \neq 0$. Letting $a = F(P)$, we have that $\frac{1}{a}F(P) = 1$.

(b) We find $F_i \in I(V \cup \{P_{-i}\})$, where $\{P_{-i}\} = \{P_1, \dots, P_r\} \setminus \{P_i\}$. Applying (a) to F_i, we get that $F_i(P_i) = 1$ and $F_i(P_j) = 0$ for $j \neq i$. By symmetry, this holds for $F_1, \dots, F_r$.

(c) With $P_1, \dots, P_r$ and V as in (b), find $F_1, \dots, F_r$ as in (b). Then, $G_i = \sum_j a_{ij} F_j$ yields our desired outcome.

Exercise (Exercise 1.18)**:** Let I be an ideal in a ring R. If $a^n \in I$ and $b^m \in I$, show that $(a+b)^{n+m} \in I$. Show that rad(I) is a (radical) ideal. Show that any prime ideal is radical.

Solution:

- Applying binomial theorem, we have

$$\begin{aligned}(a+b)^{n+m} &= \sum_{k=0}^{n+m} \binom{n+m}{k} a^{n+m-k} b^k \\ &\in I,\end{aligned}$$

  where $a^0 = b^0 := 1$.

- We have $I \subseteq \text{rad}(I)$, since we can take $n = 1$. If $a, b \in \text{rad}(I)$, we know that there is some n such that $a^n, b^m \in I$, so by the same logic as above, $(a-b)^{n+m} \in I$, meaning $a - b \in \text{rad}(I)$. Now, if $a \in \text{rad}(I)$ and $x \in R$, then we have that $a^n \in I$ for some n, meaning $x^n a^n \in I$ as I is an ideal, so $(xa)^n \in I$, so $xa \in \operatorname{rad}(I)$, so $\operatorname{rad}(I)$ is an ideal.

- Let I be prime, and let $a \in \operatorname{rad}(I)$. Then, $a^n \in I$ for some $n > 0$, meaning $(a)\left(a^{n-1}\right) \in I$. Then, either $a \in I$, or $a^{n-1} \in I$, so by the implicit inductive hypothesis, we have $a \in I$, so $\operatorname{rad}(I) \subseteq I$, so $\operatorname{rad}(I) = I$.

Exercise (Exercise 1.20)**:** Show that for any ideal I in $k[x_1, \dots, x_n]$, $V(I) = V(\operatorname{rad}(I))$, and $\operatorname{rad}(I) \subseteq I(V(I))$.

Solution:

- Clearly, $V(\operatorname{rad}(I)) \subseteq V(I)$ because $I \subseteq \operatorname{rad}(I)$. We know that if $P \in V(I)$, then there is some polynomial $F \in I$ such that $F(P) = 0$.

Exercise (Exercise 1.21)**:** Show that any $I = \langle x_1 - a_1, \dots, x_n - a_n \rangle \subseteq k[x_1, \dots, x_n]$ is a maximal ideal, and that the natural homomorphism from k to $k[x_1, \dots, x_n]/I$ is an isomorphism.

Solution: Note that $\langle x_1 - a_1, \dots, x_n - a_n \rangle \subseteq k[x_1, \dots, x_n]$ is isomorphic to $\langle x_1, \dots, x_n \rangle \subseteq k[x_1 + a_1, \dots, x_n + a_n]$, $k[x_1, \dots, x_n]/I \cong k$.

The Hilbert Basis Theorem

Earlier, we allowed any algebraic set $V(S)$ to be defined by an arbitrary set $\{F_i\}_{i \in I} \subseteq k[x_1, \dots, x_n]$. However, the Hilbert Basis Theorem will show that a finite number will do.

Theorem: Every algebraic set is the intersection of a finite number of hypersurfaces.

Proof. We know that $V(I)$ is the algebraic set for some $I \subseteq k[x_1, \dots, x_n]$. It is enough to show that I is finitely generated, as if $I = \langle F_1, \dots, F_n \rangle$, then $V(I) = V(F_1) \cap \dots \cap V(F_n)$. □

Now, to prove this, we need to show that any arbitrary ideal $I \subseteq k[x_1, \dots, x_n]$ is finitely generated. This is where the Hilbert Basis Theorem comes into play.

Definition. If R is a commutative ring, with identity, we say R is Noetherian if every ideal of R is finitely generated.

Note that all PIDs are Noetherian.

Now, we may state and prove the Hilbert Basis Theorem.

Theorem (Hilbert Basis Theorem)**:** If R is a Noetherian ring, then $R[x_1, \dots, x_n]$ is a Noetherian ring.

Proof. Since $R[x_1, \dots, x_n]$ is canonically isomorphic to $R[x_1, \dots, x_{n-1}][x_n]$. The theorem will follow by induction if we can prove that $R[x]$ is Noetherian whenever R is Noetherian.

Let $I \subseteq R[x]$ be an ideal. We wish to find a finite set of generators for I.

Let $F = a_d x^d + \cdots a_1 x + a_0 \in R[x]$ with $a_d \neq 0$. We call a_d the leading coefficient of F. Let J be the set of leading coefficients of polynomials in I. Then, $J \subseteq R$ is an ideal, so there are polynomials $F_1, \dots, F_r \in I$ whose leading coefficients generate J.

Select N larger than the degree of each F_i. For each $m \leqslant N$, let J_m be the ideal in R consisting of all leading coefficients of polynomials $F \in I$ with $\deg(F) \leqslant m$. Let $\left\{F_{m_j}\right\}$ be the finite set of polynomials in I with degree $\leqslant m$ such that their leading coefficients generate J_m. Let I' be the ideal generated by F_i and F_{m_j} for each i, m_j. It is enough to show that $I = I'$.

Suppose $I' \subsetneq I$. Let G be an element of I of minimal degree such that $G \notin I'$. If $\deg(G) > N$, then we may find Q_i such that $\sum Q_i F_i$ and G have the same leading term. However, this means $\deg(G - \sum Q_i F_i) < \deg(G)$, so $G - \sum Q_i F_i \in I'$, meaning $G \in I'$. Similarly, if $\deg(G) = m \leqslant N$, then we may lower the degree by subtracting $\sum Q_j F_{m_j}$ for some Q_j. □

Exercise (Exercise 1.22)**:** Let I be an ideal in a ring R, $\pi\colon R \to R/I$ the canonical projection.

(a) Show that for every ideal $J' \subseteq R/I$, that $\pi^{-1}(J') = J$ is an ideal of R containing I. Furthermore, show that for every ideal $J \subseteq R$, that $\pi(J) = J'$ is an ideal of R/I. This establishes a natural correspondence between ideals of R/I and ideals of R that contain I.

(b) Show that J' is a radical ideal if and only if J is radical. Similarly, show this for J prime and maximal.

(c) Show that J' is finitely generated if J is. Conclude that R/I is Noetherian if R is Noetherian. Thus, we get that $k[x_1, \dots, x_n]/I$ is Noetherian for any ideal $I \subseteq k[x_1, \dots, x_n]$ by the Hilbert Basis Theorem.

Solution:

(a) We know that $I \subseteq \pi^{-1}(J')$, as $I = \pi^{-1}(0 + I) \subseteq \pi^{-1}(J')$. Notice that, if $a, b \in \pi^{-1}(J')$ and $r \in R$, then $a + I, b + I \in J'$ and $r + I \in R/I$. Then, $a - b + I \in J'$, so $a - b \in \pi^{-1}(J')$, and $ra + I \in J'$, so $ra \in \pi^{-1}(J')$, so $\pi^{-1}(J')$ is an ideal of R.

Now, let $a + I, b + I \in \pi(J)$. Then, we know that there exist $c_1, c_2 \in J$ such that $a - c_1, b - c_2 \in I$. Thus, $(a - b) + (c_2 - c_1) \in I$. Since we have $c_2 - c_1 \in J$ as J is an ideal, so $\pi(a - b) = \pi(c_2 - c_1)$, and $(a - b) + I \in \pi(J)$. Now, let $a + I \in \pi(J)$, and let $r + I \in R/I$. Then, there exist $c_1 \in R$, $c_2 \in J$ such that $r - c_1 \in I$ and $a - c_2 \in I$, meaning that $\pi(c_1 c_2) = \pi(ra) = ra + I \in \pi(J)$.

(b) Let J be maximal. Then, $R/J \cong (R/I)/(\pi(J))$, is a field, meaning $\pi(J) \subseteq R/I$ is also maximal. This gives both directions.

Similarly, if J is prime, then $R/J \cong (R/I)/(\pi(J))$ is an integral domain, so $\pi(J) \subseteq R/I$ is also an integral domain. This gives both directions.

Let J be a radical ideal. Then, $J = \bigcap \left\{\mathfrak{p} \;\middle|\; J \subseteq \mathfrak{p}, \mathfrak{p} \text{ is prime}\right\}$. We know that for all $\mathfrak{p}$, $\pi(\mathfrak{p}) \subseteq R/I$ is prime. We know that $\pi(J) \subseteq \pi(\mathfrak{p})$ if and only if $J \subseteq \mathfrak{p}$, so $\pi(J) = \bigcap \left\{\pi(\mathfrak{p}) \;\middle|\; J \subseteq \mathfrak{p}, \mathfrak{p} \text{ is prime}\right\}$. In the reverse direction, we se that if $a \in \pi^{-1}(J)$, then $a + I \in J$, so $a^n + I \in J$ for some $n \in \mathbb{N}$, so $a^n \in \pi^{-1}(J)$, so $\pi^{-1}(J)$ is a radical ideal.

(c) Letting $\langle a_1, \dots, a_n \rangle = J$, then we know that $\langle \pi(a_1), \dots, \pi(a_n) \rangle = \pi(J)$. Thus, $\pi(J)$ is finitely generated.

Since R is an ideal, if R is Noetherian, then R/I is Noetherian, so by the Hilbert Basis Theorem, any ring of the form $k[x_1, \dots, x_n]/I$ is Noetherian.

Irreducible Components of an Algebraic Set

An algebraic set can be the union of several smaller algebraic sets. If $V \subseteq \mathbb{A}^n$ is such that $V = V_1 \cup V_2$, where V_1, V_2 are algebraic sets and $V_i \neq V$ for each i, then we say V is reducible. Else, we say V is irreducible.

Proposition: An algebraic set V is irreducible if and only if $I(V)$ is prime.

Proof. If $I(V)$ is not prime, then we have $F_1 F_2 \in I(V)$ with $F_i \notin I(V)$. Then, $V = (V \cap V(F_1)) \cup (V \cap V(F_2))$, with $V \cap V(F_i) \subsetneq V$, meaning V is irreducible.

If $V = V_1 \cup V_2$ with $V_i \subsetneq V$, then $I(V_i) \supsetneq I(V)$. Let $F_i \in I(V_i)$ with $F_i \notin I(V)$. Then, $F_1 F_2 \in I(V)$, so $I(V)$ is not prime. □

Now, we want to show that an algebraic set is a finite union of irreducible algebraic sets. To see this, we need to show an equivalent definition of a Noetherian ring.

Lemma: Let $\mathcal{I}$ be a nonempty collection of ideals in a Noetherian ring R. Then, $\mathcal{I}$ has a maximal member.

Proof. We will choose an ideal from each subset of $\mathcal{I}$. Letting I_0 be the chosen ideal for $\mathcal{I}$ itself, we let $\mathcal{I}_1 = \{I \in \mathcal{I} \mid I \supsetneq I_0\}$, with I_1 as the chosen ideal of $\mathcal{I}_1$. Continuing, we define

$$\mathcal{I}_j = \left\{I \in \mathcal{I} \;\middle|\; I \supsetneq I_{j-1}\right\},$$

and select $I_j \in \mathcal{I}_j$. It suffices to show that some $\mathcal{I}_n$ is empty.

Define $I = \bigcup_{n=0}^{\infty} I_n$ to be an ideal of R, and let $F_1, \dots, F_r$ be generators of I. We must have $F_i \in I_n$ for all i if n is sufficient large. Then, $I_n = I$, meaning $I_{n+1} = I_n$, which is a contradiction. □

Effectively, we have shown that every Noetherian ring satisfies the ascending chain condition on its ideals.

It follows that any collection of algebraic sets $\{V_\alpha\}$ in $\mathbb{A}^n(k)$ has a minimal element, by selecting the maximal member of $\{I(V_\alpha)\}$.

Theorem: Let V be an algebraic set in $\mathbb{A}^n(k)$. Then, there rae unique irreducible algebraic sets $V_1, \dots, V_m$ such that $V = V_1 \cup \cdots \cup V_m$, and $V_i \not\subseteq V_j$ for all $i \neq j$.

Proof. Let $\mathcal{I}$ be the set of algebraic sets in $\mathbb{A}^n(k)$ such that V is not the union of a finite number of irreducible algebraic sets. We wish to show that $\mathcal{I}$ is empty.

If not, let V be a minimal member of $\mathcal{I}$. Since $V \in \mathcal{I}$, V is not irreducible, so $V = V_1 \cup V_2$ with $V_i \subsetneq V$, meaning $V_i \notin \mathcal{I}$, so $V_i = V_{i,1} \cup \cdots V_{i,m_i}$, with $V_{i,j}$ irreducible. However, $V = \bigcup_{i,j} V_{i,j}$, which is a finite union.

Thus, any algebraic set V may be written as $V = V_1 \cup \cdots \cup V_m$ with V_i irreducible. To obtain the second condition, we may discard any V_i with $V_i \subseteq V_j$ with $i \neq j$.

To show uniqueness, let $V = W_1 \cup \cdots \cup W_m$ be another decomposition. Then, $V_i = \bigcup_j (W_j \cap V_i)$, so $V_i \subseteq W_{j(i)}$ for some $j(i)$. Similarly, $W_{j(i)} \subseteq V_k$ for some k. However, this means $V_i \subseteq V_k$, so $i = k$, so $V_i = W_{j(i)}$. Likewise, $W_j = V_{i(j)}$ for some $i(j)$. □

We call V_i the irreducible components of V, and $V = V_1 \cup \cdots \cup V_m$ is the decomposition of V into irreducible components.

Exercise (Exercise 1.25)**:**

(a) Show that $V\left(y - x^2\right) \subseteq \mathbb{A}^2(\mathbb{C})$ is irreducible; in fact, $I\left(V\left(y - x^2\right)\right) = \left\langle y - x^2\right\rangle$.

(b) Decompose $V\left(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3\right) \subseteq \mathbb{A}^2(\mathbb{C})$ into irreducible components.

Solution:

(a) Suppose there exists $g \in \mathbb{C}[x, y]$ such that $g | y - x^2$, meaning there exists $f \in \mathbb{C}[x, y]$ such that $fg = y - x^2$. Since $y - x^2$ has degree in y equal to 1, one of either f or g has degree in y equal to zero.

Therefore, without loss of generality, $f \in \mathbb{C}[x]$. Then, $g = yh_1 + h_2$, where $h_1, h_2 \in \mathbb{C}[x]$. Note that $h_1 \neq 0$, then $fg = fyh_1 + fh_2 = yfh_1 + fh_2$; since $fh_1 \neq 0$, we must have $fh_1 = 1$, so f is constant, so g is some constant multiple of $y - x^2$, so $y - x^2$ is irreducible. Thus, $\left\langle y - x^2\right\rangle$ is maximal, hence prime, so $I\left(V\left(y - x^2\right)\right) = \left\langle y - x^2\right\rangle$.

(b) Factoring, we see that both polynomials vanish whenever $y^2 + x = 0$. Finding all pairs, we get

$$\begin{aligned} V &= V\left(y^2 - x, y^2 + x\right) \cup V\left(y^2 - x, y - x\right) \cup \cdots \\ &= V\left(y^2 + x\right) \cup V(x - 1, y - 1) \cup V(x - 1, y + 1). \end{aligned}$$

Solution:

(a) Let $g \in I(V)$. Then,

$$g(x, y) = f_0(x) + \left(y - x^2\right) f_1(x, y),$$

wherein we order $y > x$ and do polynomial long division over y. This yields $f_0(x) = 0$ for all x, so that $I(V)$ is prime.

Exercise (Exercise 1.29)**:** Show that $\mathbb{A}^n(k)$ is irreducible if k is infinite.

Solution: We know that any polynomial that vanishes on $\mathbb{A}^n(k)$ is the zero polynomial, and $k[x_1, \dots, x_n]$ is an integral domain, so $\langle 0\rangle \subseteq k[x_1, \dots, x_n]$ is a prime ideal.

Algebraic Subsets of the Plane

We focus on the affine plane, $\mathbb{A}^2(k)$, and find its algebraic subsets.

It is enough to look at the irreducible algebraic subsets.

Exercise (Exercise 1.30)**:** Let $k = \mathbb{R}$.

(a) Show that $I\left(V\left(x^2 + y^2 + 1\right)\right) = \langle 1\rangle$.

(b) Show that every algebraic subset of $\mathbb{A}^2(\mathbb{R})$ is equal to $V(F)$ for some $F \in \mathbb{R}[x, y]$.

Solution:

(a) Since $x^2 + y^2 + 1 = 0$ if and only if $x^2 + y^2 = -1$, which means $V\left(x^2 + y^2 + 1\right) = \emptyset$. Thus, $I\left(V\left(x^2 + y^2 + 1\right)\right) = \mathbb{R}[x, y] = \langle 1\rangle$.

(b)

Exercise (Exercise 1.31)**:**

(a) Find the irreducible components of $V\left(y^2 - xy - x^2y + x^3\right)$ in $\mathbb{A}^2(\mathbb{R})$, and in $\mathbb{A}^2(\mathbb{C})$.

(b) Do the same for $V\left(y^2 - x\left(x^2 - 1\right)\right)$, and for $V\left(x^3 + x - x^2y - y\right)$.

Hilbert's Nullstellensatz

Given an algebraic set V, we have a criterion for determining whether or not V is irreducible. However, we do not have a way to describe V in terms of the set that defines V. This is what the Nullstellensatz, or zero locus theorem, will tell us.

We assume throughout this section that k is algebraically closed.

Theorem (Weak Nullstellensatz)**:** If I is a proper ideal in $k[x_1, \dots, x_n]$, then $V(I) \neq \emptyset$.

Proof. We may assume that I is a maximal ideal, as $J \supseteq I$ is maximal and $V(J) \subseteq V(I)$.

Thus, $L = k[x_1, \dots, x_n]/I$ is a field, and k is a subfield of L.

Suppose we knew that $k = L$. For each i, there is $a_i \in k$ such that $x_i - a_i \in I$. However, $\langle x_1 - a_1, \dots, x_n - a_n\rangle$ is a maximal ideal. Thus, $I = \langle x_1 - a_1, \dots, x_n - a_n\rangle$, and $V(I) = \{(a_1, \dots, a_n)\} \neq \emptyset$. □

Now, we have reduced the problem to showing that if an algebraically closed field k is a subfield of a field L, and there is a ring homomorphism of $k[x_1, \dots, x_n]$ onto L that is the identity on k, then $k = L$.

Theorem (Hilbert's Nullstellensatz)**:** Let I be an ideal in $k[x_1, \dots, x_n]$ with k algebraically closed. Then, $I(V(I)) = \operatorname{rad}(I)$.

Remark: In concrete terms, if $F_1, \dots, F_r, G$ are in $k[x_1, \dots, x_n]$, and G vanishes wherever $F_1, \dots, F_r$ vanish, then there is some equation $G^N = A_1F_1 + \cdots A_rF_r$ for some $N > 0$ and $A_i \in k[x_1, \dots, x_n]$.

Proof. We can see that $\operatorname{rad}(I) \subseteq I(V(I))$. Now, let G be in the ideal $I(V(F_1, \dots, F_r))$, where $F_i \in k[x_1, \dots, x_n]$. Let $J = \langle F_1, \dots, F_r, x_{n+1}G - 1\rangle \subseteq k[x_1, \dots, x_n, x_{n+1}]$.

Then, $V(J) \subseteq \mathbb{A}^{n+1}(k)$ is empty, since G vanishes wherever all the G_i are zero. Applying the weak Nullstellensatz to J, we have $1 \in J$, so there is an equation $1 = \sum A_i(x_1, \dots, x_{n+1})F_i + B(x_1, \dots, x_{n+1})(x_{n+1}G - 1)$. Now, let $y = 1/x_{n+1}$, and multiply the equation by a high power of y such that $y^N = \sum C_i(x_1, \dots, x_n, y)F_i + D(x_1, \dots, x_n, y)(g - y)$ in $k[x_1, \dots, x_n, y]$. Now, substituting G for y, we obtain our desired result. □

Corollary: If I i a radical ideal in $k[x_1, \dots, x_n]$, then $I(V(I)) = I$. Thus, there is a one-to-one correspondence between radical ideals and algebraic sets.

Corollary: If I is a prime ideal, then $V(I)$ is irreducible. Thus, there is a one-to-one correspondence between prime ideals and irreducible algebraic sets. The maximal ideals correspond to points.

Corollary: Let F be a nonconstant polynomial in $k[x_1, \dots, x_n]$, and $F = F_1^{n_1} \cdots F_r^{n_r}$ is a decomposition into irreducible factors. Then, $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ is the decomposition of $V(F)$ into irreducible components, and $I(V(F)) = \langle F_1, \dots, F_r \rangle$. There is a one-to-one correspondence between irreducible polynomials $F \in k[x_1, \dots, x_n]$ and irreducible hypersurfaces in $\mathbb{A}^n(k)$.

Corollary: Let I be an ideal in $k[x_1, \dots, x_n]$. Then, $V(I)$ is a finite set if and only if $k[x_1, \dots, x_n]/I$ is a finite-dimensional vector space over k. If so, the number of points in $V(I)$ is at most $\dim_k(k[x_1, \dots, x_n]/I)$.

Proof. Let $P_1, \dots, P_r \in V(I)$. Let $F_1, \dots, F_r \in k[x_1, \dots, x_n]$ such that $F_i(P_j) = \delta_{ij}$. Let $\overline{F_i}$ be the residue of F_i in $k[x_1, \dots, x_n]/I$.

If $\sum \lambda_i \overline{F_i} = 0$, where $\lambda_i \in k$, then $\sum \lambda_i F_i \in I$, so that $\lambda_j = \left(\sum \lambda_i F_i\right)\left(P_j\right) = 0$, meaning the $\overline{F_i}$ are linearly independent over k, and $\dim_k(k[x_1, \dots, x_n]/I)$.

Now, conversely, if $V(I) = \{P_1, \dots, P_r\}$ is finite, let $P_i = (a_{i1}, \dots, a_{in})$, and define F_j by $F_j = \prod_{i=1}^{r}\left(x_i - a_{ij}\right)$ for $j = 1, \dots, n$.

Then, $F_j \in I(V(I))$, so $F_j^N \in I$ for some $N > 0$, and we may take N large enough such that N works for all F_j. Taking residues in I, we have $\overline{F_j}^N = 0$, so that $\overline{x_j}^{rN}$ is a k-linear combination of $\overline{1}, \overline{x_j}, \dots, \overline{x_j}^{rN-1}$. Thus, by induction, $\overline{x_j}^s$ is a k-linear combination of $1, \overline{x_j}, \dots, \overline{x_j}^{rN-1}$ for all s, so the set $\left\{\overline{x_1}^{m_1} \dots \overline{x_n}^{m_n} \mid m_i < rN\right\}$ generates $k[x_1, \dots, x_n]/I$ as a k-vector space. □

Exercise (Exercise 1.33)**:**

(a) Decompose $V\left(x^2 + y^2 - 1, x^2 - z^2 - 1\right) \subseteq \mathbb{A}^3(\mathbb{C})$ into irreducible components.

(b) Let $V = \left\{\left(t, t^2, t^3\right) \in \mathbb{A}^3(\mathbb{C}) \;\middle|\; t \in \mathbb{C}\right\}$. Find $I(V)$ and show that V is irreducible.

Solution:

(a) We have that $x^2 = 1 - y^2$, so that $1 - y^2 - z^2 - 1 = 0$, and $y = \pm iz$. Thus, $V\left(x^2 + y^2 - 1, x^2 - z^2 - 1\right) = V\left(x^2 + y^2 - 1, y + iz\right) \cup V\left(x^2 + y^2 - 1, y - iz\right)$. We want to show that these are irreducible sets. Let $I_2 = \left\langle x^2 + y^2 - 1, y + iz\right\rangle$, $I_3 = \left\langle x^2 + y^2 - 1, y - iz\right\rangle$, and $I_1 = \left\langle x^2 + y^2 - 1, x^2 - z^2 - 1\right\rangle$.

By the Third Isomorphism Theorem,

$$\begin{aligned} \mathbb{C}[x, y, z]/I_{2,3} &\cong (\mathbb{C}[x, y, z]/\langle y \pm iz\rangle)/\left(\left\langle x^2 + y^2 - 1, y \pm iz\right\rangle/\langle y \pm iz\rangle\right) \\ &\cong \mathbb{C}[x, y]/\left\langle x^2 + y^2 - 1\right\rangle. \end{aligned}$$

To show that I_2 is prime, we show that $\mathbb{C}[x, y]/\left\langle x^2 + y^2 - 1\right\rangle$ is an integral domain.

Note that $\mathbb{C}[x, y] = \mathbb{C}[x + iy, x - iy] := \mathbb{C}[a, b]$. Then,

$$\begin{aligned} \mathbb{C}[x, y]/\left\langle x^2 + y^2 - 1\right\rangle &\cong \mathbb{C}[a, b]/\langle ab - 1\rangle \\ &\cong (\mathbb{C}[a])[b]/\langle ab - 1\rangle. \end{aligned}$$

Since $ab - 1$ is a degree 1 polynomial in $(\mathbb{C}[a])[b]$, we have $ab - 1$ is irreducible, so that $\langle ab - 1\rangle$ is prime, as $(\mathbb{C}[a])[b]$ is a unique factorization domain.

(b) We have $I(V) = \left\langle x^2 - y, x^3 - z\right\rangle$. To show that this is irreducible, consider the surjective homomorphism $\varphi\colon \mathbb{C}[x, y, z] \to \mathbb{C}[t]$, given by $f(x, y, z) \mapsto f\left(t, t^2, t^3\right)$. This has kernel $I(V)$, so that $\mathbb{C}[x, y, z]/I(V) \cong \mathbb{C}[t]$, and $I(V)$ is prime, so V is irreducible.

Exercise (Exercise 1.36)**:** Let $I = \left\langle y^2 - x^2, y^2 + x^2 \right\rangle \subseteq \mathbb{C}[x, y]$. Find $V(I)$ and $\dim_{\mathbb{C}}(\mathbb{C}[x, y]/I)$.

Solution: We see that I is generated by $\langle (y - x)(y + x), (y - ix)(y + ix) \rangle$. This gives $\{(0, 0)\}$ as $V(I)$.

Note that we have $y^2 + x^2 + I \cong 0$ and $y^2 - x^2 + I \cong 0$, so $x^2 \cong 0$ and $y^2 \cong 0$, meaning the basis for $\dim_{\mathbb{C}}(\mathbb{C}[x, y]/I)$ is $\{1, x, y, xy\}$.

Exercise (Exercise 1.37)**:** Let K be any field, $F \in K[x]$ a polynomial of degree $n > 0$.

Show that the residues $\overline{1}, \overline{x}, \dots, \overline{x}^{n-1}$ form a basis for $K[x]/\langle F \rangle$ over K.

Solution: Without loss of generality, we may assume F is monic, meaning that $x^n = -\left(a_{n-1}x^{n-1} + \cdots + a_1 x + a_0\right)$, meaning that $\overline{x}^n \in \operatorname{span}\left\{\overline{1}, \overline{x}, \dots, \overline{x}^{n-1}\right\}$. Thus, we know that the set $\left\{\overline{1}, \overline{x}, \dots, \overline{x}^{n-1}\right\}$ is spanning for $K[x]/\langle F \rangle$.

To show that this set is linearly independent in $K[x]/\langle F \rangle$, we suppose $gF = s_0\overline{1} + s_1\overline{x} + \cdots + s_{n-1}\overline{x}^{n-1}$. Then $g = 0$ by polynomial long division.

Exercise (Exercise 1.38)**:** Let $R = k[x_1, \dots, x_n]$ with k algebraically closed. Let $V = V(I)$. Show that there is a natural one-to-one correspondence between algebraic subsets of V and radical ideals in $k[x_1, \dots, x_n]/I$, and that irreducible algebraic sets (points) correspond to prime ideals (maximal ideals).

Solution: This follows from the correspondence in Exercise 1.22.

Modules and Finiteness

Definition. Let R be a ring. An R-module is a commutative group M with a scalar multiplication $R \times M \to M$ satisfying

(i) $(a + b)m = am + bm$ for $a, b \in R$, $m \in M$;

(ii) $a(m + n) = am + an$ for $a \in R$, $m, n \in M$;

(iii) $(ab)m = a(bm)$ for $a, b \in R$, $m \in M$;

(iv) $1_R m = m$ for $m \in M$, where 1_R is the multiplicative unit for R.

Example.

(1) A $\mathbb{Z}$-module is an abelian group.

(2) If R is a field, an R-module is an R-vector space.

(3) The multiplication in R makes any ideal of R into an R-module.

(4) If $\varphi \colon R \to S$ is a ring homomorphism, we define $r \cdot s$ by the equation $r \cdot s := \varphi(r)s$, which makes S into an R-module. If R is a subring of S, then S is an R-module.

Definition. A subgroup N of an R-module M is called a submodule if $am \in N$ for all $a \in R$ and $m \in N$.

If S is a set of elements of an R-module M, the submodule generated by S is defined to be

$$\left\{\sum r_i s_i \;\middle|\; r_i \in R, s_i \in S\right\};$$

it is the smallest submodule of M that contains S. If $S = \{s_1, \dots, s_n\}$ is finite, the submodule generated by S is denoted $\sum Rs_i$.

The module M is said to be finitely generated if $M = \sum Rs_i$ for some $s_1, \dots, s_n \in M$.

Definition. Let R be a subring of S.

(a) We say S is module-finite over R if S is finitely generated as an R-module. If S and R are fields, then we denote the dimension of S over R by $[R : S]$.

(b) Let $v_1, \dots, v_n \in S$, and $\varphi \colon R[x_1, \dots, x_n] \to S$ be the ring homomorphism taking x_i to v_i. The image of φ is written $R[v_1, \dots, v_n]$, which is a subring of S containing R and $v_1, \dots, v_n$.

Explicitly, we write

$$R[v_1, \dots, v_n] = \left\{ \sum a_{(i)} v_1^{i_1} \cdots v_n^{i_n} \;\middle|\; a_{(i)} \in R \right\}.$$

The ring S is ring-finite over R if $S = R[v_1, \dots, v_n]$ for some $v_1, \dots, v_n \in S$.

(c) Suppose $R = K$ and $S = L$ are fields. If $v_1, \dots, v_n \in L$ and $K(v_1, \dots, v_n)$ is the quotient field of $K[v_1, \dots, v_n]$. Consider $K(v_1, \dots, v_n) \subseteq L$ as a subfield, which is the smallest subfield of L containing K and $v_1, \dots, v_n$.

We say L is a finitely generated extension of K if $L = K(v_1, \dots, v_n)$ for some $v_1, \dots, v_n \in L$.

Exercise (Exercise 1.41)**:** If S is module-finite over R, then S is ring-finite over R.

Solution: Let S be module-finite. Then, $v \in S$ can be expressed as $v = r_1 s_1 + \cdots + r_n s_n$, so that $v \in R[s_1, \dots, s_n]$. Thus, $S \subseteq R[s_1, \dots, s_n]$. Since $r \in R$ and $s_1, \dots, s_n \in S$, we have that $R[s_1, \dots, s_n] \subseteq S$, and S is ring-finite over R.

Exercise (Exercise 1.43)**:** If L is ring-finite over K, where L and K are fields, then L is a finitely generated field extension of K.

Solution: Let L be ring-finite over K, where L and K are fields. Then, $L = K[v_1, \dots, v_n]$. For each $v_i \in K[v_1, \dots, v_n]$, we have that $v_i^{-1} \in K[v_1, \dots, v_n]$, so $L = K(v_1, \dots, v_n)$.

Exercise (Exercise 1.44)**:** Show that $L = K(x)$ is a finitely generated field extension of K, but L is not ring-finite over K.

Solution: Suppose toward contradiction that $K(x) = L = K\left[\frac{f_1}{g_1}, \dots, \frac{f_n}{g_n}\right]$.

Then, for all $h \in L$, we have that

$$\frac{1}{h} = \sum_i b_{(i)} \frac{f_1^{j_1} \cdots f_n^{j_n}}{g_1^{i_1} \cdots g_n^{i_n}},$$

meaning that

$$\frac{g_1^{i_1} \cdots g_n^{i_n}}{h} \in L[x].$$

However, since there are infinitely many irreducible monic polynomials in $L[x]$, choose h to not be equal to any of these.

Exercise (Exercise 1.45)**:** Let R be a subring of S, S a subring of T.

(a) If $S = \sum R v_i$ and $T = \sum S w_j$, then $T = \sum R v_i w_j$.

(b) If $S = R[v_1, \dots, v_n]$ and $T = S[w_1, \dots, w_m]$, show that $T = R[v_1, \dots, v_n, w_1, \dots, w_m]$.

(c) If R, S, T are fields, and $S = R(v_1, \dots, v_n)$, $T = S(w_1, \dots, w_m)$, show that $T = R(v_1, \dots, v_n, w_1, \dots, w_m)$.

Thus, each of the three finiteness conditions is a transitive relation.

Integral Elements

Definition. Let R be a subring of a ring S. An element $v \in S$ is said to be integral over R if there is a monic polynomial $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$ such that $f(v) = 0$.

If R and S are fields, then we say v is algebraic over R if v is integral over R.

Proposition: Let R be a subring of an integral domain S, with $v \in S$. The following are equivalent:

(i) v is integral over R;

(ii) $R[v]$ is module-finite over R;

(iii) there is a subring R' of S containing $R[v]$ that is module-finite over R.

Proof. If $0 = v^n + a_{n-1}v^{n-1} + \cdots + a_1 v + a_0 = 0$, then $v^n \in \sum_{i=0}^{n-1} Rv^i$, so $v^m \in \sum_{i=0}^{n-1} Rv^i$ for all m, so $R[v] = \sum_{i=0}^{n-1} Rv^i$.

Now, to show (ii) implies (iii), all we need to is take $R' = R[v]$.

To show (iii) implies (i), we let $R' = \sum_{i=1}^{n} Rw_i$, so that $vw_i = \sum_{j=1}^{n} a_{ij}w_j$ for some $a_{ij} \in R$. Then,

$$\sum_{j=1}^{n} \left(\delta_{ij}v - a_{ij}\right)w_j = 0$$

for all i, where δ_{ij} is the Kronecker delta function.

If we consider these equations in the quotient field of S, then $(w_1, \dots, w_n)$ is a nontrivial solution, so

$$\det\left(\delta_{ij}v - a_{ij}\right) = 0.$$

Since v only appears on the diagonal of this matrix, we have the form $0 = v^n + a_{n-1}v^{n-1} + \cdots + a_1 v + a_0$, where $a_i \in R$. Thus, v is integral over R. □

Corollary: The set of elements of S that are integral over R is a subring of S containing R.

Proof. If a, b are integral over R, then b is integral over $R[a] \supseteq R$, so $R[a, b]$ is module-finite over R, and $a \pm b, ab \in R[a, b]$, so they are integral over R. □

Exercise (Exercise 1.46)**:** Let R be a subring of S, S a subring of an integral domain T. If S is integral over R, and T is integral over S, show that T is integral over R.

Solution: Let $z \in T$. Then, $z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0$, where each $a_i \in S$. Note that we have $\left\{1, z, \dots, z^{n-1}\right\}$ as a basis for $R[a_0, \dots, a_{n-1}][z]$, so that $R[a_0, \dots, a_{n-1}][z] \subseteq T$ is module-finite over R. This ring contains the subring $R[z]$, so T is integral over R by part (3) of the proposition.

Exercise (Exercise 1.47)**:** Suppose S is an integral domain that is ring-finite over R. Show that S is module-finite over R if and only if S is integral over R.

Solution: Let S be ring-finite over R, so $S = R[a_1, \dots, a_n]$.

If S is integral over R, then for any $z \in S$, there is some polynomial $z^n + r_{n-1}z^{n-1} + \cdots + r_1 z + r_0 = 0$. Therefore, $\left\{1, z, \dots, z^{n-1}\right\}$ serves as a basis for $R[z] \subseteq S$ for any $z \in S$. However, this applies for each $a_1, \dots, a_n$, so S is finitely generated as a module over R.

If S is module-finite over R, then for any $v \in S$, $R[v] \subseteq R[a_1, \dots, a_n][v] = R[a_1, \dots, a_n, v] = S$, so $R[v]$ is module-finite over S, so S is integral over R.

Exercise (Exercise 1.48)**:** Let L be a field, k an algebraically closed subfield of L.

(a) Show that any element of L that is algebraic over k is in k.

(b) An algebraically closed field has no module-finite field extensions except itself.

Solution:

(a) If $z \in L$ is algebraic over k, then $z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0$, where $a_{n-1}, \dots, a_0 \in k$. However, since k is algebraically closed, this means $z \in k$, as z is a root of the polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

(b) We know that z is integral over k if and only if $k[z]$ is module-finite over k. However, since every integral/algebraic element over an algebraically closed field is in the field, there cannot be any module-finite extensions over k.

Exercise (Exercise 1.49)**:** Let K be any field, $L = K(x)$.

(a) Show that any element of L that is integral over $K[x]$ is in $K[x]$.

(b) Show that there is no nonzero element $F \in K[x]$ such that for every $z \in L$, $F^n z$ is integral over $K[x]$ for some $n > 0$.

Exercise (Exercise 1.50)**:** Let K be a subfield of L.

(a) Show that the set of elements of L that are algebraic over K is a subfield of L containing K.

(b) Suppose L is module-finite over K and R is a ring such that $K \subseteq R \subseteq L$. Show that R is a field.

Solution:

(a) Let a, b be algebraic over K. Then, $K(a, b)$ is module-finite over K, so $K(a, b)$ is an algebraic extension of K. Therefore, since $a + b, ab, a^{-1} \in K(a, b)$, all such elements algebraic over K, and K is trivially algebraic over K. Thus, the set of elements in L that are algebraic over K forms a subfield of L.

(b) Let $K \subseteq R \subseteq L$. Now, since L is module-finite over K, L is ring-finite over K, so R is ring-finite over K. Now, since $R \subseteq L$, R is module-finite over L, so for any $v \in R$, there is a polynomial such that

$$v^n + b_{n-1}v^{n-1} + \cdots + b_1 v + b_0 = 0.$$

Now, if $b_0 \neq 0$, we have

$$v\left(v^{n-1} + b_{n-1}v^{n-2} + \cdots + b_1\right) = -b_0,$$

meaning that

$$v\left(\frac{-1}{b_0}\left(v^{n-1} + b_{n-1}v^{n-2} + \cdots + b_1\right)\right) = 1,$$

and v has an inverse in R.

Field Extensions

Let K be a subfield of L, and suppose $L = K(v)$ for some $v \in L$. Let $\varphi\colon K[x] \to L$ be the homomorphism mapping $x \mapsto v$. Let $\ker(\varphi) = \langle f \rangle$ for some $f \in k[x]$. Then, $k[x]/\langle f \rangle \cong K[v]$, so $\langle f \rangle$ is prime.

We may consider two cases.

In the first case, if $f = 0$, then $K[v] \cong K[x]$, so $K(v) = L$ is isomorphic to $k(X)$, and thus L is not ring-finite or module-finite over K.

In the second case, if $f \neq 0$, then we may assume f is monic, meaning $\langle f \rangle$ is monic, and f is irreducible, so $\langle f \rangle$ is maximal, and $K[v]$ is a field. Thus, $K[v] = K(v)$, and $f(v) = 0$. Therefore, v is algebraic over K, and $L = K[v]$ is module-finite over K.

To finish the proof of the Nullstellensatz, we must prove that if a field L is a ring-finite extension of an algebraically closed field k, then $L = k$.

Thus, it is enough to show that L is module-finite over k — we already know that any ring-finite extensions are already module-finite. Now, we will show that this is always true, proving the Nullstellensatz.

Proposition: If L is ring-finite over a subfield K, then L is module-finite over K.

Proof. Let $L = K[v_1, \ldots, v_n]$. The case for $n = 1$ is taken care of by above, so we assume the result holds for all extensions generated by $n - 1$ elements. Let $K_1 = K(v_1)$; by induction, $L = K_1[v_2, \ldots, v_n]$ is module-finite over K_1. Assume towards contradiction that v_1 is not algebraic over K.

Each v_i satisfies an equation $v_i^{n_i} + a_{i,n_i-1}v_i^{n_i-1} + \cdots = 0$, where $a_{ij} \in K_1$. Letting $a \in K[v_1]$ — a multiple of the denominators of a_{ij} — we have equations $(av_i)^{n_i} + aa_{i,n_i-1}(av_i)^{n_i-1} + \cdots = 0$.

Therefore, for any $z \in L$, there is some N such that $a^N z$ is integral over $K[v_1]$. This must hold for all $z \in K(v_1)$; however, since $K(v_1)$ is isomorphic to the field of rational functions in one variable over K, this is impossible. □

Exercise (Exercise 1.51)**:** Let K be a field, $F \in K[x]$ an irreducible monic polynomial of degree $n > 0$.

(a) Show that $L = K[x]/\langle F \rangle$ is a field, and if $\overline{x}$ is the residue of x in L, then $F(\overline{x}) = 0$.

(b) Suppose L' is a field extension of K, $y \in L'$ such that $F(y) = 0$. Show that the homomorphism from $K[x]$ to L' that takes x to y induces an isomorphism of L with $K(y)$.

(c) With L' and y as in (b), suppose $G \in K[x]$ with $G(y) = 0$. Show that F divides G.

(d) Show that $F = (x - \overline{x})f_1$, where $f_1 \in L[x]$.

Solution:

(a) Let $L = K[X]/\langle F \rangle$, $x = X + \langle F \rangle$. Then, $F(x) = F(X + \langle X \rangle) = (X + \langle F \rangle)^n + \cdots + a_1(X + \langle F \rangle) + a_0 = F(X) + \langle F \rangle = 0 + \langle F \rangle$.

(b) Let $\varphi\colon K[X] \to L'$ map $X \mapsto Y$. By the first isomorphism theorem, since $F(y) = 0$ and F is irreducible, $\ker \varphi = \langle F \rangle$, so $K[X]/\langle F \rangle = K(y)$.

(c) Since $G \in \ker(\varphi)$, and F is irreducible, we have $G = FQ$ for some polynomial Q.

(d) This problem statement is too confusing.

Exercise (Exercise 1.52)**:** Let K be a field, $F \in K[x]$.

Show that there is a field L containing K such that $F = \prod_{i=1}^{n}(x - x_i) \in L[x]$.

Solution: Suppose this is the case for a polynomial of degree $\leqslant n$. Now, if F is a polynomial of degree $n + 1$ in $K[X]$. We may find $(X - x_i)$ such that $F = (X - x_i)F_1$ with $F_1 \in K[X]$. Splitting F_1, we obtain $F = \prod_{i=1}^{n+1}(X - x_i)$.

Exercise (Exercise 1.53)**:** Suppose K is a field of characteristic zero, F an irreducible monic polynomial in $K[x]$ of degree $n > 0$, and let L be the splitting field of F. Show that the x_i are distinct.

Solution: See Algebra II Notes regarding splitting fields over characteristic 0 fields.

Exercise (Exercise 1.54)**:** Let R be an integral domain with quotient field K, L a finite algebraic extension of K.

(a) For any $v \in L$, show that there is a nonzero $a \in R$ such that av is integral over R.

(b) Show that there is a basis $v_1, \dots, v_n$ for L over K such that each v_i is integral over R.

Affine Varieties

From now on, k is a fixed algebraically closed field, with affine algebraic sets in $\mathbb{A}^n = \mathbb{A}^n(k)$. Irreducible affine algebraic sets are called *affine varieties*.

All rings and fields contain k as a subring, with all homomorphisms of rings $\varphi\colon R \to S$ fixing k. We call affine varieties "varieties" this section since we are not dealing with other types of varieties yet.

Coordinate Rings

Let $V \subseteq \mathbb{A}^n$ be a nonempty variety. Then, $I(V)$ is prime in $k[x_1, \dots, x_n]$, meaning $k[x_1, \dots, x_n]/I(V)$ is an integral domain.

Definition. Let $\Gamma(V) := k[x_1, \dots, x_n]/I(V)$. Then, we call $\Gamma(V)$ the *coordinate ring* of V.

If V is any nonempty set, $\mathcal{F}(V, k)$ consists of all functions from V to k with pointwise operations. We identify k with the subring of $\mathcal{F}(V, k)$ consisting of constants.

Definition. If $V \subseteq \mathbb{A}^n$ is a variety, a function $f \in \mathcal{F}(V, k)$ is called a *polynomial function* if there exists a polynomial $F \in k[x_1, \dots, x_n]$ such that $f(a_1, \dots, a_n) = F(a_1, \dots, a_n)$ for all $(a_1, \dots, a_n) \in V$.

The polynomial functions form a subring of $\mathcal{F}(V, k)$ containing k. Two polynomials determine the same function if $(F - G)(a_1, \dots, a_n) = 0$ for all $(a_1, \dots, a_n) \in V$.

We may identify $\Gamma(V)$ with the subring of $\mathcal{F}(V, k)$ consisting of all the polynomial functions on $\mathcal{F}(V, k)$.

Exercise (Exercise 2.1)**:** Show that the map that associates to each $F \in k[x_1, \dots, x_n]$ a polynomial function in $\mathcal{F}(V, k)$ is a ring homomorphism whose kernel is $I(V)$.

Solution: The map $\varphi\colon k[x_1, \dots, x_n] \to \mathcal{F}(V, k)$ sends to zero functions all the polynomials that are identically zero on V, which is equal to $I(V)$.

Exercise (Exercise 2.2)**:** Let $V \subseteq \mathbb{A}^n$ be a variety. A subvariety of V is a variety $W \subseteq \mathbb{A}^n$ that is contained in V. Show that there is a natural one-to-one correspondence between algebraic subsets (resp. subvarieties, points) and radical ideals (resp. prime ideals, maximal ideals) in $\Gamma(V)$.

Solution: We know that: algebraic subsets of V correspond to radical ideals in $I(V)$; subvarieties of V correspond to prime ideals in $I(V)$; points in V correspond to maximal ideals in $I(V)$. Since radical ideals, prime ideals, and maximal ideals are preserved under quotients, we see that they correspond to the same objects in $\Gamma(V)$.

Exercise (Exercise 2.3)**:** Let W be a subvariety of V, and let $I_V(W)$ be the ideal of $\Gamma(V)$ corresponding to W.

(a) Show that every polynomial function on V restricts to a polynomial function on W.

(b) Show that the map $\varphi\colon \Gamma(V) \to \Gamma(W)$ defined in part (a) is a surjective homomorphism with kernel $I_V(W)$, so $\Gamma(W)$ is isomorphic to $\Gamma(V)/I_V(W)$.

Solution:

(a) If $f\colon V \to k$ is a polynomial map, then by defining $f|_W\colon W \to k$.

(b) Let $\varphi\colon \Gamma(V) \to \Gamma(W)$ be the map defined by $\varphi([f]) = [f|_W]$; the kernel of this map consists of all polynomials $F \in k[x_1, \dots, x_n]$ such that $F|_W = 0$, which is precisely $I_V(W)$.

Exercise (Exercise 2.4)**:** Let $V \subseteq \mathbb{A}^n$ be a nonempty variety. Show that the following are equivalent:

(i) V is a point;

(ii) $\Gamma(V) = k$;

(iii) $\dim_k(\Gamma(V)) < \infty$.

Solution: If V is a point, then $V = (a_1, \dots, a_n)$ is the zero of $P = s_1(x_1 - a_1) + \cdots + s_n(x_n - a_n)$, so $I(V) = \langle P \rangle$. Since $k[x_1, \dots, x_n] \cong k[x_1 - a_1, \dots, x_n - a_n]$ (by a translation), we have

$$\begin{aligned}\Gamma(V) &= k[x_1, \dots, x_n]/\langle x_1 - a_1, \dots, x_n - a_n \rangle \\ &= k[x_1 - a_1, \dots, x_n - a_n]/\langle x_1 - a_1, \dots, x_n - a_n \rangle \\ &= k.\end{aligned}$$

Since k is a dimension 1 k-vector space, this implies (iii).

If $\dim_k(\Gamma(V)) < \infty$, then $\Gamma(V)$ is a finite-dimensional k-algebra, meaning it is an Artinian ring, hence has Krull dimension zero. Thus, $\left\langle \overline{0} \right\rangle \subseteq \Gamma(V)$ is prime and is not contained in any other prime ideals, meaning $I(V)$ is maximal, hence V is a point.

Polynomial Maps

Definition. Let $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ be varieties. A map $\varphi\colon V \to W$ is called a polynomial map if there are polynomials $T_1, \dots, T_m \in k[x_1, \dots, x_m]$ such that $\varphi(a_1, \dots, a_n) = (T(a_1, \dots, a_n), \dots, T_m(a_1, \dots, a_n))$ for all $(a_1, \dots, a_n) \in V$.

Any map $\varphi\colon V \to W$ induces a homomorphism $\widetilde{\varphi}\colon \mathcal{F}(W, k) \to \mathcal{F}(V, k)$ by $\widetilde{\varphi}(f) = f \circ \varphi$.

If φ is a polynomial map, then $\widetilde{\varphi}(\Gamma(W)) \subseteq \Gamma(V)$, so $\widetilde{\varphi}$ restricts to a homomorphism, also written $\widetilde{\varphi}$, from $\Gamma(W)$ to $\Gamma(V)$. If $f \in \Gamma(W)$ is the $I(W)$ residue of F, then $\widetilde{\varphi}(f) = f \circ \varphi$ is the $I(V)$ residue of the polynomial $F(T_1, \dots, T_m)$.

If $V = \mathbb{A}^n$, $W = \mathbb{A}^m$, and $T_1, \dots, T_m \in k[x_1, \dots, x_n]$ determine a polynomial map $T\colon \mathbb{A}^n \to \mathbb{A}^m$, then the T_i are uniquely determined by T, so we usually write $T = (T_1, \dots, T_m)$.

Proposition: Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine varieties. There is a natural one to one correspondence between polynomial maps $\varphi\colon V \to W$ and homomorphisms $\widetilde{\varphi}\colon \Gamma(W) \to \Gamma(V)$. Any such φ is the restriction of a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$.

Proof. Let $\alpha\colon \Gamma(W) \to \Gamma(V)$ be a homomorphism. Set $T_i \in k[x_1, \dots, x_n]$ such that $\alpha(\overline{x_i}) = \overline{T_i}$, where the residue of x_i is taken in $I(W)$ and the residue of T_i is taken in $I(V)$. Then, $T = (T_1, \dots, T_m)$ is a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$ that induces $\widetilde{T}\colon k[x_1, \dots, x_m] \to k[x_1, \dots, x_n]$. Note that $\widetilde{T}(I(W)) \subseteq I(V)$ by construction, so $T(V) \subseteq W$, and T restricts to a polynomial map $\varphi\colon V \to W$. Now, on $\Gamma(W)$, we have

$$\begin{aligned}\widetilde{\varphi}(f)(\overline{x_1}, \dots, \overline{x_n}) &= f \circ \varphi(x_1, \dots, x_n)\\ &= (T_1, \dots, T_m)(x_1, \dots, x_n),\end{aligned}$$

so $\widetilde{\varphi} = \alpha$. □

Definition. A polynomial map $\varphi\colon V \to W$ is an isomorphism if there is a polynomial map $\psi\colon W \to V$ such that $\psi = \varphi^{-1}$.

Two affine varieties are isomorphic if and only if their coordinate rings are isomorphic.

Exercise (Exercise 2.6)**:** Let $\varphi\colon V \to W$ and $\psi\colon W \to Z$ be polynomial maps. Show that $\widetilde{\psi \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\psi}$. Show that the composition of polynomial maps is a polynomial map.

Solution: Let $f \in \mathcal{F}(V, k)$ be a polynomial function. Then,

$$\begin{aligned}\widetilde{\psi \circ \varphi}(f) &= f \circ (\psi \circ \varphi)\\ &= (f \circ \psi) \circ \varphi\\ &= \widetilde{\varphi} \circ \widetilde{\psi}(f).\end{aligned}$$

A polynomial map $\varphi\colon V \to W$ is defined by polynomials $T_1, \dots, T_m$; similarly, a polynomial map $\psi\colon W \to Z$ is defined by polynomials $S_1, \dots, S_r$; since the composition of two polynomials is another polynomial, the composition of their respective maps is also a polynomial map.

Exercise (Exercise 2.7)**:** Let $\varphi\colon V \to W$ be a polynomial map, and X an algebraic subset of W. Then, $\varphi^{-1}(X)$ is an algebraic subset of V. If $\varphi^{-1}(X)$ is irreducible and X is contained in the image of φ, show that X is irreducible.

Solution: Let $\varphi\colon V \to W$ be a polynomial map, and let X be an algebraic subset of W, with corresponding radical ideal I in $\Gamma(W)$. There is a homomorphism of coordinate rings, $\widetilde{\varphi}\colon \Gamma(W) \to \Gamma(V)$, and since the homomorphic image of a radical ideal is a radical ideal, the corresponding radical ideal $\widetilde{\varphi}(I) \subseteq \Gamma(V)$ corresponds to $\varphi^{-1}(X)$.

Now, if $\varphi^{-1}(X)$ is irreducible, then there is a corresponding prime ideal $\mathfrak{p} \subseteq \Gamma(V)$. Taking inverse images, $\widetilde{\varphi}^{-1} \circ \widetilde{\varphi}(\mathfrak{p})$ corresponds to $\varphi \circ \varphi^{-1}(X)$. If $X \subseteq \varphi \circ \varphi^{-1}(X) \subseteq X$, then $\mathfrak{p} \subseteq \widetilde{\varphi}^{-1} \circ \widetilde{\varphi}(\mathfrak{p}) \subseteq \mathfrak{p}$, meaning that X has corresponding prime ideal $\widetilde{\varphi}^{-1}(\mathfrak{p})$, and X is irreducible.

Exercise (Exercise 2.8)**:**

(a) Show that $\left\{\left(t, t^2, t^3\right) \in \mathbb{A}^3(k) \,\middle|\, t \in k\right\}$ is an affine variety.

(b) Show that $V\left(xz - y^2, yz - x^3, x^2 - x^2y\right) \subseteq \mathbb{A}^2(\mathbb{C})$ is a variety.

Solution:

(a) The set $S = \left\{\left(t, t^2, t^3\right) \in \mathbb{A}^3(k) \,\middle|\, t \in k\right\}$ has $I(S) = \left\langle x^2 - y, x^3 - z\right\rangle \subseteq k[x, y, z]$. From Exercise 1.33 (b), we have that

$$k[x,y,z]/I(S) \cong k[t],$$

given by the surjective ring homomorphism $f(x,y,z) \mapsto f\left(t,t^2,t^3\right)$. Since $k[t]$ is an integral domain, this means $I(S)$ is prime, so S is a variety.

(b) Using the hint, we know that $V = V\left(\left\langle y^3 - x^4, z^3 - x^5, z^4 - y^5\right\rangle\right)$, with algebraic set of $\left\{\left(t^3,t^4,t^5\right) \,\middle|\, t \in k\right\}$. This means we have a map $\varphi\colon \mathbb{A}^1(\mathbb{C}) \to V$ by taking $t \mapsto \left(t^3,t^4,t^5\right)$. This map is bijective, so the induced homomorphism $\varphi\colon \Gamma(V) \to \Gamma\left(\mathbb{A}^1(\mathbb{C})\right)$ is an isomorphism. Since $\Gamma\left(\mathbb{A}^1(\mathbb{C})\right) = \mathbb{C}[x]$ is an integral domain, so too is $\Gamma(V)$, so $I(V)$ is prime, and V is a variety.

Exercise (Exercise 2.9)**:** Let $\varphi\colon V \to W$ be a polynomial map of affine varieties, with $V' \subseteq V$ and $W' \subseteq W$ subvarieties. Suppose $\varphi(V') \subseteq W'$.

(a) Show that $\widetilde{\varphi}(I_W(W')) \subseteq I_V(V')$.

(b) Show that the restriction of φ gives a polynomial map from V' to W'.

Solution:

(a) Let $\overline{x_i}$ be the image of x_i in $\Gamma(V)$, and let $\overline{y_i}$ be the image of y_i in $\Gamma(W)$, where

$$\begin{aligned}\Gamma(V) &= k[x_1,\dots,x_m]/I(V)\\ \Gamma(W) &= k[y_1,\dots,y_n]/I(W).\end{aligned}$$

Let $f(\overline{y}_1,\dots,\overline{y}_n) \in I_W(W')$, meaning $f(a_1,\dots,a_n) = 0$ for all $(a_1,\dots,a_n) \in W'$. Let $(b_1,\dots,b_m) \in V'$. Then,

$$\begin{aligned}\widetilde{\varphi}(f)(b_1,\dots,b_m) &= f(\varphi(b_1,\dots,b_m))\\ &= 0,\end{aligned}$$

where we use the fact that $\varphi(V') \subseteq W'$. Thus, $\varphi(b_1,\dots,b_n) \in W'$, and $\widetilde{\varphi}(I_W(W')) \subseteq I_V(V')$.

(b) Using Exercise 2.3 and the duality relation, we notice that $\widetilde{\varphi}\colon \Gamma(W') \to \Gamma(V')$ is a homomorphism, so we use the proposition to determine that $\varphi|_{V'}$ is a polynomial map.

Exercise (Exercise 2.10)**:** Show that the projection map $P\colon \mathbb{A}^n \to \mathbb{A}^r$, where $n \geqslant r$, defined by $P(a_1,\dots,a_n) = (a_1,\dots,a_r)$ is a polynomial map.

Solution: Define $T_1,\dots,T_r$ to be identity.

Exercise (Exercise 2.12)**:**

(a) Let $\varphi\colon \mathbb{A}^1 \to V = V\left(y^2 - x^3\right) \subseteq \mathbb{A}^2$ be defined by $\varphi(t) = \left(t^2,t^3\right)$. Show that, although φ is an injective polynomial map, φ is not an isomorphism.

(b) Let $\varphi\colon \mathbb{A}^1 \to V = V\left(\left\langle y^2 - x^2(x+1)\right\rangle\right)$ be defined by $\varphi\left(t^2-1, t\left(t^2-1\right)\right)$. Show that φ is one-to-one and onto except that $\varphi(\pm 1) = (0,0)$.

Solution:

(a)

Coordinate Changes

If $T = (T_1,\dots,T_m)$ is a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$, and F is a polynomial in $k[x_1,\dots,x_m]$, we let $F^T = \widetilde{T}(F) = F(T_1,\dots,T_m)$.

For ideals I and algebraic sets V in $\mathbb{A}^m$, I^T is the ideal in $k[x_1,\dots,x_m]$ generated by $\left\{F^T \,\middle|\, F \in I\right\}$, and V^T denotes $T^{-1}(V) = V\left(I^T\right)$, where $I = I(V)$. If V is the hypersurface of F, then V^T is the hypersurface of F^T if F^T is not constant.

A *change of coordinates* on $\mathbb{A}^n$ is a polynomial map $T\colon \mathbb{A}^n \to \mathbb{A}^n$ such that each T_i is a polynomial of degree 1 and T is bijective. If $T_i = \sum a_{ij}x_j + a_{i0}$, then $T = T'' \circ T'$, where T' is a linear map and T'' is a translation. Since translations are invertible, it follows that T is bijective if and only if T' is invertible.

If T and U are affine changes of coordinates on $\mathbb{A}^n$, then so are $T \circ U$ and T^{-1}; in other words, T is an automorphism of the variety $\mathbb{A}^n$.

Exercise (Exercise 2.14)**:** A set $V \subseteq \mathbb{A}^n(k)$ is called a linear subvariety of $\mathbb{A}^n(k)$ if $V = V(\langle F_1, \dots, F_r\rangle)$, where the F_i are polynomials of degree 1.

(a) Show that if T is an affine change of coordinates on $\mathbb{A}^n$, then V^T is also a linear subvariety of $\mathbb{A}^n(k)$.

(b) If $V \neq \emptyset$ is a linear subvariety, show that there is an affine change of coordinates T of $\mathbb{A}^n$ such that $V^T = V(x_{m+1}, \dots, x_n)$

(c) Show that the m that appears in part (b) is independent of the choice of T. It is called the dimension of V.

Solution:

(a) If T is an affine change of coordinates, then each T_i is of the form $T_i = \sum a_{ij}x_j + a_{i0}$. Considering $F_i^T = F_i(T_1, \dots, T_i)$, we must have each F_i as a function of exactly one T_i. Since each T_i is also a polynomial of degree 1, $V^T = T^{-1}(V)$ is a variety generated by a family of polynomials of degree 1, so V^T is a linear subvariety.

(b) Let $V = V(F_1)$ for some degree 1 polynomial $F = \sum a_ix_i + a_0$. Define $T = (T_1, \dots, T_m)$. We may take T_m by defining

$$\begin{aligned} T_m(x_n) &= -\frac{a_0}{a_n} - \frac{a_1}{a_n}x_1 - \frac{a_2}{a_n}\cdots + \frac{1}{a_n}x_m \\ T_m(x_i) &= x_i. && i \leqslant n-1 \end{aligned}$$

Then, $F_1 \circ T = x_m$, so $V^T = V(x_m)$.

For the inductive step, we take $V = V(F_1, \dots, F_r, F_{r+1})$, and suppose T is defined for $V(F_1, \dots, F_r)$. Then, we may define

$$\begin{aligned} V^T &= T^{-1}(V(F_1, \dots, F_r)) \cap T^{-1}(F_{r+1}) \\ &= V(x_{m+1}, \dots, x_n) \cap T^{-1}(F_{r+1}), \end{aligned}$$

and we may set T to be such that $T^{-1}(V(F_{r+1})) = V(x_m)$, satisfying the inductive step.

(c) Suppose there were a change of coordinates $T = (T_1, \dots, T_n)$ such that $V(x_{m+1}, \dots, n)^T = V(x_{s+1}, \dots, x_n)$, where $s < m$. Then, by definition,

$$T^{-1}(V(x_{m+1}, \dots, x_n)) = V(x_{s+1}, \dots, x_n),$$

meaning that, since affine transformations are bijective,

$$T(V(x_{s+1}, \dots, x_n)) = V(x_{m+1}, \dots, x_n).$$

This means that any polynomial in $x_{s+1}, \dots, x_n$ yields a polynomial exclusively in $x_{m+1}, \dots, x_n$; this means that at least one of the affine transformations in $T_1, \dots, T_n$ yields 0 by the pigeonhole principle, so the transformations in $T_1, \dots, T_n$ are not independent.

Exercise (Exercise 2.15)**:** Let $P = (a_1, \dots, a_n)$ and $Q = (b_1, \dots, b_n)$ be distinct points in $\mathbb{A}^n$. The line through P, Q is defined by $\{a_1 + t(b_1 - a_1), \dots, a_n + t(b_n - a_n) \mid t \in k\}$.

(a) Show that if L is defined through P and Q, and T is an affine change of coordinates, then $T(L)$ is the line through $T(P)$ and $T(Q)$.

(b) Show that a line is a linear subvariety of dimension 1, and that any linear subvariety of dimension 1 is the line through any two of its points.

(c) Show that, in $\mathbb{A}^2$, a line is the same thing as a hyperplane.

(d) Let $P, P' \in \mathbb{A}^2$, L_1, L_2 be two distinct lines through P, and L_1', L_2' distinct lines through P'. Show that there is an affine change of coordinates of $\mathbb{A}^2$ such that $T(P) = P'$ and $T(L_i) = L_i'$.

Local Rings

Let V be a nonempty variety in $\mathbb{A}^n$, and let $\Gamma(V)$ be its coordinate ring. We may define the quotient field on $\Gamma(V)$, giving the *field of rational functions* on V, written $k(V)$.

If f is a rational function on V, and $P \in V$, we say f is defined at P if for some $a, b \in \Gamma(V)$, $f = \frac{a}{b}$, and $b(P) \neq 0$. If $\Gamma(V)$ is a unique factorization domain, there is an essentially unique representation $f = a/b$ with a, b having no common factors.

Example. If $V = V(xw - yz) \subseteq \mathbb{A}^4(k)$, then $\Gamma(V) = k[x, y, z, w]/\langle xw - yz\rangle$. Letting $\overline{x}, \overline{y}, \overline{z}, \overline{w}$ represent the residues, we have $\frac{\overline{x}}{\overline{y}} = \frac{\overline{z}}{\overline{w}} = f \in k(V)$ is defined at $p(x, y, z, w)$ whenever y or w are not equal to 0.

Letting $P \in V$, we define $\mathcal{O}_P(V)$ to be the set of rational functions on V that are defined at P. It turns out that $\mathcal{O}_P(V)$ defines a subring of $k(V)$ containing $\Gamma(V)$, which we call the *local ring* of V at P.

The set of points $P \in V$ where a rational function is not defined is called the pole set of f.

Proposition:

(1) The pole set of a rational function is an algebraic subset of V.

(2)
$$\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(V).$$

Proof. Suppose $V \subseteq \mathbb{A}^n$. Let $\overline{G}$ be the residue of $G \in k[x_1, \dots, x_n]$ in $\Gamma(V)$. Let $f \in k(V)$, and let

$$J_f = \left\{G \;\middle|\; \overline{G}f \in \Gamma(V)\right\}.$$

Note that J_f is an ideal containing $I(V)$, and points of $V(J_f)$ are those points where f is not defined.

Now, if $f \in \bigcap_{P \in V} \mathcal{O}_P(V)$, $V(J_f) = \emptyset$, so $1 \in J_f$ by the Nullstellensatz, meaning $f \in \Gamma(V)$. $\square$

Let $f \in \mathcal{O}_P(V)$. We can define the value of f at P, written $f(P)$, to be $a(P)/b(P)$. The ideal

$$\mathfrak{m}_P(V) = \{f \in \mathcal{O}_P(V) \mid f(P) = 0\}$$

is called the *maximal ideal* of V at P. It is the kernel of the evaluation homomorphism $f \mapsto f(P)$ onto k, so $\mathcal{O}_P(V)/\mathfrak{m}_P(V)$ is isomorphic to k.

In particular, note that all elements of $\mathcal{O}_P(V)$ that are not in $\mathfrak{m}_P(V)$ are units.

Lemma: The following conditions on a ring R are equivalent.

(1) The set of non-units in R forms an ideal.

(2) R has a unique maximal ideal that contains every proper ideal of R.

Proof. Let $\mathfrak{m} = \{\text{non-units of } R\}$. Every proper ideal of R is contained in $\mathfrak{m}$. $\square$

A ring that satisfies these conditions is known as a local ring. The units are those elements not belonging to the maximal ideal.

Proposition: $\mathcal{O}_P(V)$ is a Noetherian local integral domain.

Proof. We only need to show that every ideal I of $\mathcal{O}_P(V)$ is finitely generated. Since $\Gamma(V)$ is Noetherian, we may choose generators $f_1, \dots, f_r$ for the ideal $I \cap \Gamma(V)$ of $\Gamma(V)$. We claim that $f_1, \dots, f_r$ generate I in $\mathcal{O}_P(V)$. If $f \in I \subseteq \mathcal{O}_P(V)$, there is a $b \in \Gamma(V)$ with $b(P) \neq 0$ and $bf \in \Gamma(V)$. Then, $bf \in \Gamma(V) \cap I$, so $bf = \sum a_i f_i$ for some $a_i \in \Gamma(V)$, meaning $f = \sum (a_i/b) f_i$ as desired. $\square$

Exercise (Exercise 2.17)**:** Let $V = V\left(y^2 - x^2(x+1)\right)$, and $\overline{x}, \overline{y}$ residues in $\Gamma(V)$. Let $z = \frac{\overline{y}}{\overline{x}}$. Find the pole sets of z and z^2.

Solution: We start by verifying the pole sets for z^2. Taking z^2, we have

$$\begin{aligned} z^2 &= \frac{\overline{y}^2}{\overline{x}^2} \\ &= \frac{\overline{x}^2(\overline{x}+1)}{\overline{x}^2} \\ &= \overline{x}+1, \end{aligned}$$

meaning z^2 has no poles.

Now, since $z = \frac{\overline{y}}{\overline{x}}$, the only possible poles are points (a, b) where $a = 0$. However, if $P \in V$ and $a = 0$, we must have $b^2 = 0$, so $b = 0$. Therefore, the only possible pole is where $P = (0, 0)$. However, we must verify that this is indeed a pole.

Suppose z is defined at $(0, 0)$, so we may write $z = \frac{f(\overline{x},\overline{y})}{g(\overline{x},\overline{y})}$, for some $f, g \in \Gamma(V)$ with $g(0, 0) \neq 0$. Since $\overline{y}^2 = \overline{x}^2(\overline{x}+1)$, we may write $g(\overline{x}, \overline{y}) = g_0(\overline{x}) + \overline{y}g_1(\overline{x})$ (any other factors of $\overline{y}$ can be rewritten in terms of $\overline{x}$), and similarly writing $f(\overline{x}, \overline{y}) = f_0(\overline{x}) + \overline{y}f_1(\overline{x})$. Therefore,

$$\frac{\overline{y}}{\overline{x}} = \frac{f_0(\overline{x}) + \overline{y}f_1(\overline{x})}{g_0(\overline{x}) + \overline{y}g_1(\overline{x})},$$

so

$$\overline{y}(g_0(\overline{x}) + \overline{y}g_1(\overline{x})) = \overline{x}(f_0(\overline{x}) + \overline{y}f_1(\overline{x})).$$

Writing $\overline{y}^2 = \overline{x}^2(\overline{x}+1)$, we get

$$g_0(\overline{x})\overline{y}g_1(\overline{x})\left(\overline{x}^2(\overline{x}+1)\right) = f_0(\overline{x})\overline{x} + \overline{xy}f_1(\overline{x}),$$

so that $g_0(\overline{x}) = \overline{x}f_1(\overline{x})$, and $g_0 = 0$. Therefore, $g(0, 0) = g_0(0) + 0 \cdot g_1(0) = 0$, which is a contradiction.

Exercise (Exercise 2.18)**:** Let $\mathcal{O}_P(V)$ be the local ring of a variety V at point P. Show that there is a natural one-to-one correspondence between the prime ideals in $\mathcal{O}_P(V)$ and the subvarieties of V that pass through P.

Solution: Let I be prime in $\mathcal{O}_P(V)$. Then, $I \cap \Gamma(V) \subsetneq \Gamma(V)$ is prime, so $I \cap \Gamma(V)$ corresponds to a unique subvariety of V. Specifically, since $I \subsetneq \mathcal{O}_P(V)$ is an ideal, it is contained in $\mathfrak{m}_P$, so f is zero at P, meaning the subvariety corresponding to $I \cap \Gamma(V)$ passes through P.

Exercise (Exercise 2.21)**:** Let $\varphi\colon V \to W$ be a polynomial map of affine varieties, $\widetilde{\phi}\colon \Gamma(W) \to \Gamma(V)$ the induced map of coordinate rings.

Suppose $P \in V$, $\varphi(P) = Q$. Show that $\widetilde{\varphi}$ extends uniquely to a ring homomorphism $\overline{\varphi}\colon \mathcal{O}_Q(W) \to \mathcal{O}_P(V)$. Show that $\overline{\varphi}\left(\mathfrak{m}_Q(W)\right) \subseteq \mathfrak{m}_P(V)$.

Solution: Let $f = a/b \in \mathcal{O}_Q(W)$ be in reduced form. Define

$$\begin{aligned} \overline{\varphi}(f) &= (a \circ \varphi)/(b \circ \varphi) \\ &= \widetilde{\varphi}(a)/\widetilde{\varphi}(b). \end{aligned}$$

Since $\widetilde{\varphi}$ is unique, and f is written in its unique reduced form, this gives a unique map $\overline{\varphi}\colon \mathcal{O}_Q(W) \to \mathcal{O}_P(V)$.

Exercise (Exercise 2.22)**:** Let $T\colon \mathbb{A}^n \to \mathbb{A}^n$ be an affine change of coordinates, with $T(P) = Q$. Show that $\widetilde{T}\colon \mathcal{O}_Q(\mathbb{A}^n) \to \mathcal{O}_P(\mathbb{A}^n)$ is an isomorphism. Show that $\widetilde{T}$ induces an isomorphism from $\mathcal{O}_Q(V)$ to $\mathcal{O}_P\left(V^T\right)$ if $P \in V^T$ for any subvariety $V \subseteq \mathbb{A}^n$.

Solution: If T is an affine change of coordinates, then T is a bijective affine (hence polynomial) map, so the map $\widetilde{T}\colon \mathcal{O}_Q(\mathbb{A}^n) \to \mathcal{O}_P(\mathbb{A}^n)$ is a homomorphism. Suppose $\widetilde{T}\left(\frac{a}{b}\right) = 0$. Then, for all $t \in \mathbb{A}^n$, $a(T(t)) = 0$. Since T is an isomorphism, for all $s \in \mathbb{A}^n$, $s = T(t)$, for some $t \in \mathbb{A}^n$, meaning that for all $s \in \mathbb{A}^n$, $f(s) = 0$, so $\frac{f}{g} = 0$.

Let $\frac{a}{b} \in \mathcal{O}_P(\mathbb{A}^n)$. Define $\frac{s}{t} \in \mathcal{O}_Q(\mathbb{A}^n)$ by

$$\frac{s}{t} = \frac{a\left(T^{-1}\right)}{b\left(T^{-1}\right)}.$$

Since T is an isomorphism, we know that T^{-1} exists, and since $T^{-1}(Q) = P$, then $t(Q) \neq 0$, so $\widetilde{T}\left(\frac{s}{t}\right) = \frac{a}{b}$, meaning $\widetilde{T}$ is an isomorphism.

To show that $\widetilde{T}$ restricts to an isomorphism of $\mathcal{O}_Q(V)$ to $\mathcal{O}_P\left(V^T\right)$, we need to show that $\widetilde{T}(\mathcal{O}_Q(V)) = \mathcal{O}_P\left(V^T\right)$. This can be seen by taking $a, b \in \Gamma(V)$ with $b(Q) \neq 0$, and using our definition of V^T to find

$$\widetilde{T}\left(\frac{a}{b}\right) = \frac{a(T)}{b(T)}.$$

Here, $\widetilde{T}$ is defined at $P \in V^T$ if $b(T)\left(T^{-1}(T(P))\right) = b(T(P)) = b(Q) \neq 0$, so $\widetilde{T}(\mathcal{O}_Q(V)) = \mathcal{O}_P\left(V^T\right)$.

Discrete Valuation Rings

Proposition: Let R be an integral domain that is not a field. The following are equivalent:

(1) R is a local, Noetherian, and the maximal ideal is principal;

(2) there is an irreducible element $t \in R$ such that every nonzero $z \in R$ may be written uniquely in the form $z = ut^n$ for some unit $u \in R$ and n a nonnegative integer.

Proof. Assume (1). Let $\mathfrak{m}$ be the maximal ideal, and t a generator for $\mathfrak{m}$. Suppose $ut^n = vt^m$ with u, v units and $n \geqslant m$. Then, $ut^{n-m} = v$ is a unit, so $n = m$ and $u = v$. Thus, any expression of z is unique.

To show that z has an expression, we may assume $z = z_1 t$ for some $z_1 \in R$. If z_1 is a unit, we are done. Then, we assume $z_1 = z_2 t$, so that we have a sequence $(z_k)_k$, where $z_k = z_{k+1}t$. Since R is Noetherian, the chain of ideals $\langle z_1 \rangle \subseteq \langle z_2 \rangle \subseteq \cdots$ has a maximal member, so $\langle z_n \rangle = \langle z_{n+1} \rangle$ for some n. Thus, $z_{n+1} = vz_n$ for some $v \in R$, and $z_n = vtz_n$, and $vt = 1_R$, but t is not a unit.

Assume (2). We note that $\mathfrak{m} = \langle t \rangle$ is the set of non-units, and that the only ideals in R are the principal ideals, $\langle t^n \rangle$ for some nonnegative integer, meaning R is a principal ideal domain. □

Any ring that satisfies these conditions is called a *discrete valuation ring*, which we call a DVR. The element t is known as a uniformizing parameter for R, and any other uniformizing parameter is of the form ut for some unit $u \in R$.

If K is the field of fractions for R, then for fixed t, a nonzero element $z \in K$ has an expression $z = ut^n$ for a unit u and $n \in \mathbb{Z}$. The exponent n is called the *order* of z, which we write $\operatorname{ord}(z)$. We define $\operatorname{ord}(0) = \infty$.

Exercise (Exercise 2.23)**:** Show that the order function on K is independent of the choice of uniformizing parameter.

Solution: Since all uniformizing parameters are of the form vt for some unit v of R, we have that

$$\begin{aligned} z &= u(vt)^n \\ &= (uv^n)t^n \\ &= vt^n, \end{aligned}$$

since the units form a group. Thus, the order of z is independent of the choice of uniformizing parameter.

Exercise (Exercise 2.24)**:** Let $V = \mathbb{A}^1$, $\Gamma(V) = k[x]$, $K = k(x)$.

(a) For each $a \in k = V$, show that $\mathcal{O}_a(V)$ is a DVR with uniformizing parameter $t = X - a$.

(b) Show that

$$\mathcal{O}_\infty := \left\{f/g \in k(x) \,\middle|\, \deg(g) \geqslant \deg(f)\right\}$$

is a DVR with uniformizing parameter $t = 1/x$.

Solution:

(a) Any element of the maximal ideal of $\mathcal{O}_a(V)$ is zero at a, meaning that we are able to use long division to factor out $(x-a)$ from $\frac{p}{q} \in \mathfrak{m}_a$. Thus, $(x-a)$ is a uniformizing parameter for $\mathcal{O}_a(V)$, meaning $\mathcal{O}_a(V)$ is a DVR.

(b) If $\deg(g) \geqslant \deg(f)$, then we are able to factor out x^n from both f and g such that

$$\frac{f}{g} = \frac{f^*}{x^k(g^*)}$$

for some $f^*, g^* \in k(x)$ and $k \geqslant 0$. Thus, $\frac{1}{x}$ is a uniformizing parameter for $\mathcal{O}_\infty$.

Exercise (Exercise 2.26)**:** Let R be a DVR with fraction field K, and $\mathfrak{m}$ the maximal ideal of R.

(a) Show that if $z \in K$ and $z \notin R$, then $z^{-1} \in \mathfrak{m}$.

(b) Suppose $R \subseteq S \subseteq K$, and S is also a DVR. Suppose the maximal ideal of S contains $\mathfrak{m}$. Show that $S = R$.

Solution:

(a) Let $z \in K$ with $z \notin R$. Then, $z = ut^n$ with $n < 0$ (as if $n \geqslant 0$, z would be in R). Thus, $z^{-1} = u^{-1}t^{-n} \in R$.

(b) Let $x \in S$, and write $x = ut^n$ for some $n \in \mathbb{Z}$ and $t \in R$ such that $\langle t \rangle = \mathfrak{m}$. Let $\langle s \rangle = \mathfrak{n}$. We may write $t = vs^m$ for some $m \geqslant 0$ and unit $v \in S$. Therefore, $x = uv^m s^{mn}$. Therefore, $mn \geqslant 0$. If $m = 0$, then t is a unit, so $t \notin \mathfrak{n}$, which is a contradiction. Else, if $m > 0$, then $n > 0$, meaning $x \in R$.

Exercise: An order function on a field K is a function from K onto $\mathbb{Z} \cup \{\infty\}$ such that

(i) $\varphi(a) = \infty$ if and only if $a = 0$;

(ii) $\varphi(ab) = \varphi(a) + \varphi(b)$;

(iii) $\varphi(a+b) \geqslant \min(\varphi(a), \varphi(b))$.

Show that $R = \{z \in K \mid \varphi(z) \geqslant 0\}$ is a DVR with maximal ideal $\mathfrak{m} = \{z \mid \varphi(z) > 0\}$, and quotient field K. Conversely, show that if R is a DVR with quotient field K, then the function $\operatorname{ord}\colon K \to \mathbb{Z} \cup \{\infty\}$ is an order function on K.

Exercise (Exercise 2.29)**:** Let R be a DVR with quotient field K, and ord is the order function on K.

(a) If $\operatorname{ord}(a) < \operatorname{ord}(b)$, show that $\operatorname{ord}(a+b) = \operatorname{ord}(a)$.

(b) If $a_1, \dots, a_n \in K$, and for some i, $\operatorname{ord}(a_i) < \operatorname{ord}\left(a_j\right)$ for all $j \neq i$, then $a_1 + \cdots + a_n \neq 0$.

Exercise (Exercise 2.30)**:** Let R be a DVR with maximal ideal $\mathfrak{m}$ and fraction field K. Suppose a field k is a subring of R, and that the composition $k \hookrightarrow R \to R/\mathfrak{m}$ is an isomorphism of k with $R/\mathfrak{m}$. Verify the following assertions.

(a) For any $z \in R$, there is a unique $\lambda \in k$ such that $z - \lambda \in \mathfrak{m}$.

(b) Let t be a uniformizing parameter for R, with $z \in R$. Then, for any $n \geqslant 0$, there are unique $\lambda_0, \lambda_1, \dots, \lambda_n \in k$ and $z_n \in R$ such that $z = \lambda_0 + \lambda_n t + \cdots + \lambda_n t^n + z_n t^{n+1}$.

Forms

Let R be an integral domain. If $F \in R[x_1, \dots, x_{n+1}]$ is a form, then we define $F_* \in F[x_1, \dots, x_n]$ by taking $F_* = F(x_1, \dots, x_n, 1)$.

Conversely, for any polynomial $f \in R[x_1, \dots, x_n]$ of degree d, we write $f = f_0 + f_1 + \cdots + f_d$ into forms, and define $f^* \in R[x_1, \dots, x_{n+1}]$ to be

$$f^* = x_{n+1}^d f(x_1/x_{n+1}, \dots, x_n/x_{n+1}).$$

Then, f^* is a form of degree d.

Exercise (Exercise 2.35)**:**

(a) Show that there $d+1$ monomials of degree d in $R[x,y]$, and $\frac{(d+1)(d+2)}{2}$ monomials of degree d in $R[x,y,z]$.
(b) Let $V(d,n)$ be the forms of degree d in $k[x_1,\dots,x_n]$ for some field k. Show that $V(d,n)$ is a vector space over k, and that the monomials of degree d form a basis.
(c) Let $L_1, L_2, \dots$ and $M_1, M_2, \dots$ be sequences of nonzero linear forms in $k[x,y]$. Assume $L_i \neq \lambda M_j$ for all i,j and for any $\lambda \in k$. Let $A_{ij} = L_1L_2\cdots L_iM_1M_2\cdots M_j$ for all $i,j \geqslant 0$, where $A_{00} = 1$. Show that $\left\{A_{ij} \mid i+j = d\right\}$ forms a basis for $V(d,2)$.

Solution:

(a)
(b)
(c) We induct on d. Clearly, A_{00} is a basis for k.

Now, suppose

$$c_0A_{0d} + c_1A_{1,d-1} + \cdots + c_dA_{d0} = 0.$$

Factoring, we have

$$c_0A_{0d} + c_dA_{d0} + M_1L_1\left(c_1\frac{A_{1,d-1}}{M_1L_1} + \cdots + c_{d-1}\frac{A_{d-1,1}}{M_1L_1}\right) = 0.$$

By the induction hypothesis, the expression in parentheses must be zero, as as neither A_{d0} nor A_{0d} have factors of the form M_1L_1. Therefore,

$$c_0M_1\cdots M_d + c_dL_1\cdots L_d = 0.$$

Since $k[x,y]$ is a unique factorization domain, it cannot be the case that $L_1\cdots L_d = tM_1\cdots M_d$ by the assumption on L_i and M_j.

Direct Products

If $R_1,\dots,R_n$ are rings, the Cartesian product $R_1\times\cdots\times R_n$ is made into a ring by taking pointwise addition and pointwise multiplication.

This ring is known as the direct product of $R_1,\dots,R_n$, written $\prod_{i=1}^n R_i$. The natural projection maps $\pi_i\colon \prod_{j=1}^n R_j \to R_i$, given by $(a_1,\dots,a_n)\mapsto a_i$ are ring homomorphism.

The direct product is characterized by the following universal property: given any ring R and family of ring homomorphisms $\varphi_i\colon R\to R_i$, there is a unique ring homomorphism $\varphi\colon R\to\prod_{i=1}^n R_i$ such that $\pi_i\circ\varphi = \varphi_i$.

In particular, if a field k is a subring of each R_i, we may regard k as a subring of the product.

Operations with Ideals

Let I, J be ideals of R. The ideal generated by $\{ab \mid a\in I, b\in J\}$ is denoted IJ. Similarly, for ideals $I_1,\dots,I_n$, we denote the ideal $I_1\cdots I_n$ to be the ideal generated by $\{a_1a_2\cdots a_n \mid a_i\in I_i\}$, and I^n as $I\cdots I$ n times.

If I is generated by $a_1,\dots,a_n$, then I^n is generated by

$$\left\{a_1^{i_1}\cdots a_r^{i_r} \;\middle|\; \sum_j i_j = n\right\}.$$

Furthermore,

$$R = I^0 \supseteq I^1 \supseteq I^2 \supseteq \cdots.$$

Example. If $R = k[x_1, \dots, x_r]$, with $I = \langle x_1, \dots, x_r \rangle$. Then, I^n is generated by monomials of degree n, meaning there are polynomials with no terms with degree less than n in I^n. Furthermore, the residues of the monomials of degree $< n$ form a basis for $k[x_1, \dots, x_r]/I^n$ over k.

Now, if $R \subseteq S$ is a subring, then IS is the ideal of S generated by the elements of I. Note that $I^n S = (IS)^n$.

If I, J are ideals in R, then $I + J = \{a + b \mid a \in I, b \in J\}$ is an ideal, and is the smallest ideal containing both I and J.

Two ideals I, J are called comaximal if $I + J = R$.

Lemma: Let I, J be ideals. Then,

(1) $IJ \subseteq I \cap J$;

(2) for comaximal I, J, $IJ = I \cap J$.

Proof.

(1) Definition.

(2) If $I + J = R$, then

$$\begin{aligned} I \cap J &= (I \cap J)R \\ &= (I \cap J)(I + J) \\ &= (I \cap J)I + (I \cap J)J \\ &\subseteq JI + IJ \\ &= IJ. \end{aligned}$$

□

Exercise (Exercise 2.39)**:** Prove the following relations among ideals I_i, J in a ring R:

(a) $(I_1 + I_2)J = I_1 J + I_2 J$;

(b) $(I_1 \cdots I_N)^n = I_1^n \cdots I_N^n$.

Solution:

(a) Elements of $I_1 + I_2$ are of the form $a_1 + a_2$ for $a_1 \in I_1$, $a_2 \in I_2$, meaning elements of $(I_1 + I_2)J$ are of the form $(a_1 + a_2)b$ for some $b \in J$, or $a_1 b + a_2 b$, so $(I_1 + I_2)J \subseteq I_1 J + I_2 J$.

Now, elements of $I_1 J + I_2 J$ are of the form $a_1 b_1 + a_2 b_2$ for some $b_1, b_2 \in J$, $a_1 \in I_1$, and $a_2 \in I_2$. However, since $I_1, I_2, I_1 + I_2$ are ideals, $I_1 J + I_2 J \subseteq (I_1 + I_2)J$.

Exercise (Exercise 2.40)**:**

(a) Suppose I and J are comaximal ideals in R. Show that $I + J^2 = R$. Show that I^m and J^n are comaximal for all m, n.

(b) Suppose that $I_1, \dots, I_N$ are ideals in R, and $I_i, J_i = \bigcap_{j \neq i} I_i$ are comaximal for all i. Show that $I_1^n \cap \cdots \cap I_N^n = (I_1 \cdots I_N)^n = (I_1 \cap \cdots \cap I_N)^n$ for all n.

Solution:

(a) Let $I + J = R$, so that there exist $a \in I$, $b \in J$ such that $a + b = 1_R$. Squaring, we have

$$1_R = a^2 + 2ab + b^2.$$

Since $a^2 + 2ab \in I$ and $b^2 \in J^2$, we have $R \subseteq I + J^2$.

In a similar manner, we may exponentiate $(a+b)^n$ and $(a+b)^m$ to get that J is comaximal with I^n and J^m is comaximal with I. Therefore, I^n is comaximal with J^m.

Exercise (Exercise 2.41)**:** Let I, J be ideals in a ring R. Suppose I is finitely generated and $I \subseteq \operatorname{rad}(J)$. Show that $I^n \subseteq J$ for some n.

Solution: Find the maximum j such that $a_i^j \in J$, where a_i are the generators of of I. Call this value j_0. Of the m generators of I, we set $n := mj_0$. By the pigeonhole principle, at least one of the generators of I must have its power taken by j_0, so that $I^n \subseteq J$.

Exercise:

(a) Let $I \subseteq J$ be ideals in a ring R. Show that there is a natural ring homomorphism from R/I onto R/J.

(b) Let I be an ideal in a ring R, R a subring of S. Show that there is a natural ring homomorphism from R/I to S/IS.

Solution:

(a) We map $a + I \mapsto a + J$.

(b) We map $a + I \mapsto a + IS$.

Exercise (Exercise 2.43)**:** Let $P = (0, \dots, 0) \in \mathbb{A}^n$, and $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^n)$, with $\mathfrak{m} = \mathfrak{m}_P(\mathbb{A}^n)$. Let $I \subseteq k[x_1, \dots, x_n]$ be the ideal generated by $x_1, \dots, x_n$. Show that $I\mathcal{O} = \mathfrak{m}$, so $I^r\mathcal{O} = \mathfrak{m}^r$ for all r.

Solution: The ideal I consists of all polynomials in $k[x_1, \dots, x_n]$ that do not contain a constant term; thus, $I\mathcal{O}$ consists of all rational functions defined at $(0, \dots, 0)$ without a constant term. All these functions evaluate to 0 at $(0, \dots, 0)$, so $I\mathcal{O} \subseteq \mathfrak{m}$. Moreover, since any element of $\mathfrak{m}$ necessarily does not have a constant term, $\mathfrak{m} \subseteq I\mathcal{O}$, meaning that $\mathfrak{m} = I\mathcal{O}$.

Ideals with a Finite Number of Zeros

We will relate local questions (related to the local rings of some finite algebraic variety) to global questions (related to the coordinate rings).

Proposition: Let I be an ideal in $k[x_1, \dots, x_n]$, and let $V(I) = \{P_1, \dots, P_N\}$ be finite. Let $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbb{A}^n)$.

Then, there is a natural isomorphism from $k[x_1, \dots, x_n]/I$ with $\prod_{i=1}^n \mathcal{O}_i/I\mathcal{O}_i$.

Proof. Let $I_i = I(\{P_i\})$. Let $R = k[x_1, \dots, x_n]/I$, and let $R_i = \mathcal{O}_i/I\mathcal{O}_i$. The natural homomorphisms φ_i from R to R_i induce a homomorphism φ from R to $\prod_{i=1}^n R_i$.

By the Nullstellensatz, $\operatorname{rad}(I) = \bigcap_{i=1}^n I_i$, so $\left(\bigcap I_i\right)^d \subseteq I$ for some d. □