Introduction

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

Contents

Introduction 1

Affine Algebraic Sets 1

Algebraic Preliminaries . . . 1
Affine Space and Algebraic Sets . . . 4
The Ideal of a Set of Points . . . 5
The Hilbert Basis Theorem . . . 7
Irreducible Components of an Algebraic Set . . . 8
Algebraic Subsets of the Plane . . . 9
Hilbert's Nullstellensatz . . . 10
Modules and Finiteness . . . 11
Integral Elements . . . 12
Field Extensions . . . 13

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.

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,

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

[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.

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.

(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 $P = F_1 F_2 \cdots F_n + 1$. We note that P is monic. We will show that P is irreducible.

Suppose toward contradiction that P were reducible. We know that $k[x]$ is a principal ideal domain, so $P \in \langle F_i \rangle$ for some irreducible monic F_i. However, we know that, for any F_i, $1 \leqslant i \leqslant n$, $P \nmid F_i$, 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 $V(0) = \mathbb{A}^n(k)$, $V(1) = \varnothing$, $V(x_1 - a_1, \dots, x_n - a_n) = \{(a_1, \dots, a_n)\}$ 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 $I(X)$.

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

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 $\operatorname{rad}(I) = \{a^n \mid a \in I \text{ for some } n > 0\}$. We have that $\operatorname{rad}(I)$ is an ideal containing I. An ideal I is called a radical ideal if $I = \operatorname{rad}(I)$.

- 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 $\operatorname{rad}(I)$ 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 $I \subseteq \operatorname{rad}(I)$, since we can take $n = 1$. If $a, b \in \operatorname{rad}(I)$, 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 $a - b \in \operatorname{rad}(I)$. Now, if $a \in \operatorname{rad}(I)$ 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 $V(I) = V(F_1) \cap \cdots \cap V(F_n)$. $\square$

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. $\square$

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, $J = \bigcap\left\{\mathfrak{p} \mid J \subseteq \mathfrak{p}, \mathfrak{p} \text{ is prime}\right\}$. 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 $\pi(J) = \bigcap\left\{\pi(\mathfrak{p}) \mid J \subseteq \mathfrak{p}, \mathfrak{p} \text{ is prime}\right\}$. 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 $F_1F_2 \in I(V)$ 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, $F_1F_2 \in I(V)$, 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 $k[x_1, \ldots, x_n]$ is an integral domain, so $\langle 0\rangle \subseteq k[x_1, \ldots, x_n]$ is a prime ideal.

Algebraic Subsets of the Plane

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 $V\left(x^2 + y^2 + 1\right) = \varnothing$. Thus, $I\left(V\left(x^2 + y^2 + 1\right)\right) = \mathbb{R}[x, y] = \langle 1\rangle$.

(b) Consult Brown.

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 $F_j = \prod_{i=1}^{r} (x_i - a_{ij})$ 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 $\left\{\overline{x_1}^{m_1} \dots \overline{x_n}^{m_n} \;\middle|\; m_i < rN\right\}$ 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)

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 $\dim_{\mathbb{C}}(\mathbb{C}[x, y]/I)$.

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.

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).

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)**:**

Exercise (Exercise 1.42)**:**

Exercise (Exercise 1.43)**:**

Exercise (Exercise 1.44)**:**

Exercise (Exercise 1.45)**:**

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):

Exercise (Exercise 1.47):

Exercise (Exercise 1.48):

Exercise (Exercise 1.49):

Exercise (Exercise 1.50):

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.

Case 1: 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.

Case 2: 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 $L = K[v_1, \dots, v_n]$. 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, $L = K_1[v_2, \dots, v_n]$ 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):

Exercise (Exercise 1.52):

Exercise (Exercise 1.53):

Exercise (Exercise 1.54)**:**