Algebraic Curves.

Alec Zabel-Mena

October 2, 2023

Contents

Chapter 1

Affine Algebraic Sets

1.1 Preliminaries

Theorem 1.1.1. *Let* $\mathfrak{a}$ *be an ideal of* R *and* $\mathfrak{a}[x]$ *the ideal of* $R[x]$ *generated by* $\mathfrak{a}$*. Then*

$$R[x]/\mathfrak{a}[x] \simeq R/\mathfrak{a}[x]$$

Moreover, if $\mathfrak{a}$ *is a prime ideal in* R*, then* $\mathfrak{a}[x]$ *is a prime ideal in* $R[x]$*.*

Proof. Consider the map $\pi : R[x] \to R/\mathfrak{a}[x]$ given by $f \to f \mod \mathfrak{a}$. That is, reduce f modulo $\mathfrak{a}$. Then π is a ring homomorphism with kernel $\ker \pi = \mathfrak{a}[x]$. By the first isomorphism theorem, we get

$$R[x]/\mathfrak{a}[x] \simeq R/\mathfrak{a}[x]$$

Now, let $\mathfrak{p}$ be a prime ideal in R, Then we have that $R/\mathfrak{p}$ is an integral domain, hence, so is $R/\mathfrak{p}[x]$, which makes $\mathfrak{p}[x]$ a prime ideal of $R[x]$. ■

Example 1.1. Consider the ideal $n\mathbb{Z}$ in $\mathbb{Z}$. By above, we have

$$\mathbb{Z}[x]/n\mathbb{Z}[x] \simeq \mathbb{Z}/n\mathbb{Z}[x]$$

with natural map reduction of polynomials modulo n. If n is composite, then the ring $\mathbb{Z}/n\mathbb{Z}[x]$ is not an integral domain. If $n = p$ a prime, then $\mathbb{Z}/n\mathbb{Z}[x]$ is an integral domain.

Definition. We define the **polynomial ring** in n **variables** $x_1, \dots, x_n$ with **coefficients** in R inductively to be

$$R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$$

and is the set of all **multivariate polynomials** of the form $f(x_1, \dots, x_n) = \sum a x_1^{d_1} \dots x_n^{d_n}$. We call the monic term $x_1^{d_1} \dots x_n^{d_n}$ of f a **monomial**. We define the **degree** of a monomial to be $\deg x_1^{d_1} \dots x_n^{d_n} = d_1 + \dots + d_n$ and we define the **degree** of f to be $\deg f = \max \{\deg x_1^{d_1} \dots x_n^{d_n}\}$ (i.e. the maximum degree of all monomials of f). If all the monomials of f have the same degree, we call f a **form**.

Lemma 1.1.2. *Let* R *be a ring. Then* $R[x_1, \dots, x_n]$ *is a ring.*

Example 1.2. (1) Consider the polynomial ring $\mathbb{Z}[x,y]$ in two variables x and y with integer coefficients. Then $p(x,y) = 2x^3 + xy - y^2$ and has $\deg p = 3$. The polynomial $q(x,y) = -3xy + 2y^2 + x^2y^3$ has $\deg q = 5$. The sum

$$p + q(x,y) = 2x^3 - 2xy + y^2 + x^2y^3 \text{ has degree } \deg p + q = 5$$

and the product

$$pq(x,y) = -6x^4y + 4x^3y^2 + 2x^5y^3 - 3x^2y^2 + 5xy^3 + x^3y^4 - 2y^4 - x^2y^5$$

had degree $\deg pq = 8$.

(2) The polynomial $p(x,y,z) = 4y^2z^5 - 3xy^3z + 2x^2y$ over $\mathbb{Z}[x,y,z]$ has degree $\deg p = 7$ and the polynomial $q(x,y,z) = 5x^2y^3z^4 - 9x^2z + 7x^2$ has degreee $\deg q = 9$. The polynomials

$$p + q(x,y,z) = 5x^2y^3z^4 + 4y^2z^5 - 3xy^3z + 2x^2y - 9x^2z + 7x^2$$

and

$$\begin{aligned} pq(x,y,z) &= 20x^2y^5z^9 - 15x^3y^6z^5 + 10x^4y^4z^4 - 36x^2y^2z^6 \\ &\quad + 28x^2y^2z^5 + 27x^3y^3z^2 - 21x^3y^3z - 18x^4yz + 14x^4y \end{aligned}$$

have degrees $\deg(p+q) = 9$ and $\deg pq = 16$, respectively.

(3) Consider the polynomials p and q of the above example over $\mathbb{Z}/3\mathbb{Z}$, i.e. as polynomials in $\mathbb{Z}/3\mathbb{Z}[x,y,z]$. Then we have

$$\begin{aligned} p(x,y,z) &= xy^2z^5 + 2x^2y \\ q(x,y,z) &= 2x^2y^3z^4 + x^2 \end{aligned}$$

which makes

$$p + q(x,y,z) = 2x^2y^3z^4 + y^2z^5 + 2x^2y + x^2$$

and

$$pq(x,y,z) = 2x^2y^5z^9 + 1x^4y^4z^4 + 1x^2y^2z^5 + 14x^4y$$

of degrees $\deg(p+q) = 9$ and $\deg pq = 16$, still.

(4) In any domain R, if $f, g \in R[x_1, \ldots, x_n]$ are forms of degree m and n respectively, then fg is a form of degree mn. Moreover if f is a form of degree m, and $g|f$, then g must also be a form.

Lemma 1.1.3. *Let R be a commutative ring, and π a permutation of the set $\{1, \ldots n\}$. Then $R[x_1, \ldots, x_n] \simeq R[x_{\pi(1)}, \ldots, x_{\pi(n)}]$. That is, multivariate polynomial rings are independent of the ordering of their variables.*

Proof. Define the map $\Pi : R[x_1, \ldots, x_n] \to R[x_{\pi(1)}, \ldots, x_{\pi(n)}]$ termwise by first sending $x_1 \ldots x_n \to x_{\pi(1)} \ldots x_{\pi(n)}$. Then notice that Π defines a ring homomorphism, and moreover, for any $f \in R[x_1, \ldots, x_n]$, Π permutes the terms of f. So that Π dictates the required isomorphism. ■

Example 1.3. (1) Consider the ideals (x) and (x, y) in $\mathbb{Q}[x, y]$. We have that (x) is a prime ideal in $\mathbb{Q}[x, y]$, since $\mathbb{Q}[x, y] \simeq \mathbb{Q}[y, x] = \mathbb{Q}[y][x]$. Moreover, let $fg \in (x, y)$ so that $fg(x, y) = xyr(x, y)$ for some $r \in \mathbb{Q}[x, y]$. Then $xy|fg$ which makes $xy|f$ or $xy|g$, so that $f \in (x, y)$ or $g \in (x, y)$. This makes (x, y) a prime ideal. Notice, however, that $(x) \subseteq (x, y)$, so that (x) is not maximal. (x, y), however is a maximal ideal in $\mathbb{Q}[x, y]$.

(2) Notice that (x, y) is a prime ideal in $\mathbb{Z}[x, y]$, since $\mathbb{Z}[x, y]$ is a subring of $\mathbb{Q}[x, y]$, and (x, y) is prime in $\mathbb{Q}[x, y]$. Similarly, $(2, x, y)$ is prime in $\mathbb{Z}[x, y]$. Notice however that $(x, y) \subseteq (2, x, y)$ so that (x, y) is not maximal in $\mathbb{Z}[x, y]$; $(2, x, y)$ is maximal in $\mathbb{Z}[x, y]$.

(3) Notice that (x, y) is not a principle ideal in $\mathbb{Q}[x, y]$. Suppose that it were, then $(x, y) = (f)$ for some $f(x, y) \in \mathbb{Q}[x, y]$. Then we have that $x \in (f)$ and $y \in (f)$ so that $f|x$ and $f|y$. That is, $x = f(x, y)r(x, y)$ and $y = f(x, y)q(x, y)$. Then $x + y = f(x, y)(r(x, y) + q(x, y))$. Notice also that $\deg f \leq 1$. Then if $\deg f = 0$, f is a unit, and we get $(f) = \mathbb{Q}[x, y]$. On the other hand, if $\deg f = 1$, and since $x + y = f(x, y)(r(x, y) + q(x + y))$, we have that

Lemma 1.1.4. *Let k be an infinite field, and suppose $f \in k[x_1, \ldots, x_n]$ is a polynomial such that $f(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in k$. Then f must be the zero polynomial.*

Proof. Observe that
$$f(x_1, \ldots, x_n) = \sum f_i(x_1, \ldots, x_{n-1})x_n^i$$
where $f \in k[x_1, \ldots, x_{n-1}]$. Now, for $n = 1$, if we have $f \in k[x_1]$, then if $f(a_1) = 0$ for all $a_1 \in k$, then $f(x_1) = 0$ in k. Suppose now that the the polynomial $f(x_1, \ldots, x_n)$ satisfies

$$f(a_1, \ldots, a_n) = 0 \text{ for all } a_1, \ldots, a_n \in k$$

and consider a the polynomial f as a polynomial in $k[x_1, \ldots, x_n, x_{n+1}] \simeq k[x_1, \ldots, x_n][x_{n+1}]$, then we have
$$f(x_1, \ldots, x_n, x_{n+1}) = \sum f_i(x_1, \ldots, x_n)x_{n+1}^i$$
Now, if $f(a_1, \ldots, a_n, a_{n+1}) = 0$ for all $a_1, \ldots, a_n, a_{n+1} \in k$, we have that

$$f(a_1, \ldots, a_n, a_{n+1}) = \sum f_i(a_1, \ldots, a_n)a_{n+1}^i = 0$$

Now, f has finitely many roots when considered as a polynomial in $k[x_1, \ldots, x_n]$, and if $a_1, \ldots, a_n$ are roots of f_i, by hypothesis, $f_i = 0$ for each i, so that

$$f(a_1, \ldots, a_n, a_{n+1}) = \sum f_i(a_1, \ldots, a_n)a_{n+1}^i = \sum 0a_{n+1}^i = 0$$

which makes $f(x_1, \ldots, x_{n+1}) = 0$ in $k[x_1, \ldots, x_{n+1}]$. ■

Lemma 1.1.5. *If k is a field, then there exist infinitely many monic irreducible polynomials in $k[x]$.*

Proof. Suppose that there exist finitely many monic irreducible polynomials in $k[x]$, and let $p_1, \ldots, p_n$ an enumeration of all of them. Consider the polynomial

$$p(x) = p_1(x) \ldots p_n(x) + 1$$

Then for every p_i, we have that $p \equiv 1 \mod p_i$ so that no p_i divides p. Since ech p_i is monic and irreducible, this makes p irreducible, contradiction the given enumeration. ∎

Lemma 1.1.6. *Every algebraically closed field is infinite.*

Proof. Let k be an algebraically closed field. Suppose also that k were finite, and let $k = \{a_1, \ldots, a_n\}$. Let $f(x) \in k[x]$ be the following polynomial

$$f(x) = (x - a_1) \ldots (x - a_n) + 1$$

Then f has no roots at in k. Since k is algebraically closed, there must be an element $a \in k$ for which a is a root of f, i.e, $f(a) = 0$. This forces $a = a_i$ for some $1 \leq i \leq n$. Since $f(a_i) \neq 0$, this forces $a \neq a_i$ for all i, so that $k = \{a_1, \ldots, a_n, a\}$, which contradicts the finiteness of k. ∎

Lemma 1.1.7. *Let k be a field, and let $f \in k[x_1, \ldots, x_n]$. Then for some $a_1, \ldots, a_n \in k$,*

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

Proof. Consider the monomials $x_1^{i_1} \ldots x_n^{i_n}$ of f, and recall that $x_1^{i_1} \ldots x_n^{i_n} \in k[x_1, \ldots, x_{n-1}][x_n]$. Suppose that a_1 is a root of $x_1^{i_1} \ldots x_n^{i_n}$, and that it factors into, say $f(x_1, \ldots, x_n) = \lambda_1(x_1 - a_1)^{i_1} x_2^{i_2} \ldots x_n^{i_n}$. Supposing then that $a_2, \ldots, a_n$ are all roots, we can obtain the factorization $\lambda_{(i)}(x_1 - a_1)^{i_1} \ldots (x_n - a_n)^{i_n}$ (this factorization is independent of the ordering of $a_1, \ldots, a_n$ since one can always permute the roots of a polynomial). This gives us the required result. ∎

Corollary. *If $f(a_1, \ldots, a_n) = 0$ then $f(x_1, \ldots, x_n) = \sum (x_i - a_i) g_i(x_1, \ldots, x_n)$ For some $g_i \in k[x_1, \ldots, x_n]$ not necessarily unique.*

Proof. Observe the monomials $(x_1 - a_1)^{i_1} \ldots (x_n - a_n)^{i_n} = (x_j - a_j)((x_1 - a_1)^{i_1} \ldots (x_j - a_j)^{i_j - 1} \ldots (x_n - a_n)^{i_n}) = (x_j - a_i) g_j(x_1, \ldots, x_n)$. ∎

1.2 Affine n-Space and Algebraic Sets

Definition. Let k be a field. We define **affine n-space** over k to be the cartesian product $\mathbb{A}^n(k) = \underbrace{k \times \cdots \times k}_{n\text{-times}}$. If the field k is understood, we write $\mathbb{A}^n$. We call the elements of $\mathbb{A}^(k)$ **affine points**. We call $\mathbb{A}^1(k)$ and $\mathbb{A}^2(k)$ the **affine line** and **affine plane** over k, respectively.

Definition. Let k be a field, and let $f \in k[x_1, \ldots, x_n]$. We call an affine point $P \in \mathbb{A}^n(k)$ a **zero**, or **root** of f if $f(P) = 0$, where $f(P)$ is understood to be $f(a_1, \ldots, a_n)$, where $P = (a_1, \ldots, a_n)$. We call the set of zeros of f, $V(f)$ the **hypersurface** defined by f. We call hypersurfaces in $\mathbb{A}^2(k)$ **affine plane curves**. If $\deg f = 1$, we call $V(f)$ a **hyperplane**. We call hypersurfaces in $\mathbb{A}^1(k)$ **lines**.

Example 1.4. The following curves in figure 1.1 define algebraic sets.

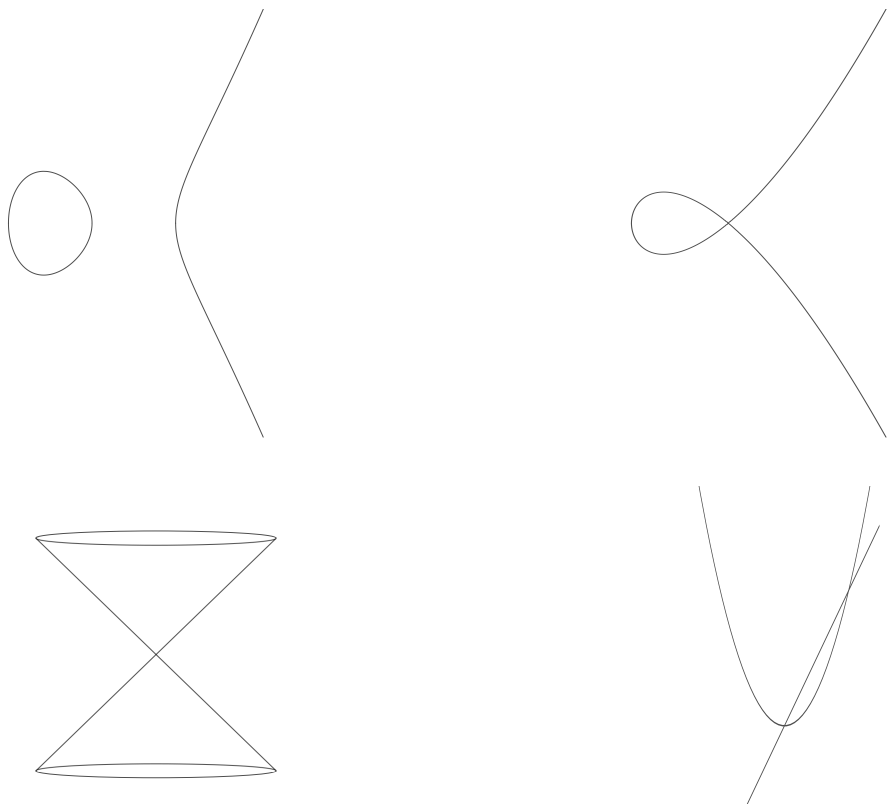

Figure 1.1: Affine Algebraic Sets in $\mathbb{A}^2(\mathbb{R})$ and $\mathbb{A}^3(\mathbb{R})$.

Definition. Let k be a field, and S any set of polynomials in $k[x_1, \ldots, x_n]$. We define the **set of zeros** of S to be the set $V(S) = \{P \in \mathbb{A}^n(k) : f(P) = 0 \text{ for all } f \in S\}$. We call a subset X of $\mathbb{A}^n(k)$ an **affine algebraic set** if $X = V(S)$ for some set S of polynomials.

Lemma 1.2.1. *The following are true for any field k.*

(1) If $\mathfrak{a}$ is an ideal in $k = [x_1, \ldots, x_n]$ generated by a set $S \subseteq k[x_1, \ldots, x_n]$, then $V(\mathfrak{a}) = V(S)$.

(2) If $\{\mathfrak{a}_\alpha\}$ is a collection of ideals of $k[x_1, \ldots, x_n]$, then

$$V\Big(\bigcup \mathfrak{a}_\alpha\Big) = \bigcap V(\mathfrak{a}_\alpha)$$

(3) If $\mathfrak{a} \subseteq \mathfrak{b}$ are ideals, then $V(\mathfrak{b}) \subseteq V(\mathfrak{a})$.

(4) If $f, g \in k[x_1, \ldots, x_n]$, then $V(fg) = V(f) \cup V(g)$.

(5) $V(0) = \mathbb{A}^n(k)$ and $V(1) = \emptyset$.

Proof. First, let S be a set of polynomials in $k[x_1, \ldots, x_n]$. Let $\mathfrak{a} = (S)$ the ideal generated by S. Then if $f \in S$ is a polynomia, $f \in I$. Then if $P \in \mathbb{A}^n$ is a zero of f in S, it is a zero of f in $\mathfrak{a}$, hence $V(S) \subseteq V(\mathfrak{a})$. Conversely, we have that if $f \in \mathfrak{a}$, then by suppostion, $f(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n) + \cdots + f_n(x_1, \ldots, x_n) + \ldots$. Now, if $f(P) = 0$ in I, then we have $f_i(P) = 0$ for every i. This makes $f(P) = 0$ in S, so that $V(\mathfrak{a}) \subseteq V(S)$.

Now, consider the collection $\{\mathfrak{a}_\alpha\}$ of ideals in $k[x_1, \ldots, x_n]$. Let $P \in V(\bigcup \mathfrak{a}_\alpha)$. Then for every $f \in \bigcup \mathfrak{a}_\alpha$, $f(P) = 0$ for each α. So that $P \in \bigcap V(\mathfrak{a}_\alpha)$. Again, on the otherhand, if $P \in \bigcap V(\mathfrak{a}_\alpha)$, $P \in V(\mathfrak{a}_\alpha)$ for all α so that $P \in V(\bigcup \mathfrak{a}_\alpha)$.

Let $\mathfrak{a}$ and $\mathfrak{b}$ ideals in $k[x_1, \ldots, x_n]$, where $\mathfrak{a} \subseteq \mathfrak{b}$. Let $P \in V(\mathfrak{b})$. Then for every polynomial $f \in \mathfrak{b}$, $f(P) = 0$, so that $f(P) = 0$ when $f \in \mathfrak{a}$, hence $P \in V(\mathfrak{a})$. This makes $V(\mathfrak{b}) \subseteq V(\mathfrak{a})$.

Consider now the polynomials $f, g \in k[x_1, \ldots, x_n]$. Certainly if $P \in V(fg)$ it is a root of fg; ie.e. $fg(P) = 0$. This makes $f(P) = 0$ or $g(P) = 0$ so that $V(fg) \subseteq V(f) \cup V(g)$. On the otherhand if P is a root of f, or a root of g, it is a root of fg making $V(f) \cup V(f) \subseteq V(fg)$, and equality is established.

Finally, observe that the zero polynomial $0(x_1, \ldots, x_n)$ has all its coefficients 0, so that any point $P \in \mathbb{A}^n$ is a zero. This makes $V(0) = \mathbb{A}^n$. Likewise, the constant polynomial $1(x_1, \ldots, x_n)$ has its 0-th coefficient 1 so that it has not points $P \in \mathbb{A}^n$ as roots. That is $V(1) = \emptyset$. ■

Corollary. *Finite unions of algebraic sets are algebraic.*

Example 1.5. (1) Let k be a field, and consider $\mathbb{A}^1(k)$. Let $f \in k[x]$ be a polynomial of degree n. Then f has at most n roots in k. Now, if $\mathfrak{a}$ is an ideal in k, since k is a PID, we also get $\mathfrak{a} = (f)$ for some $f \in k[x]$. That is $|V(\mathfrak{a})| \leq n$, and so any algebraic set in $\mathbb{A}^1(k)$ is necessarily finite, except, possibly $\mathbb{A}^1(k)$.

(2) Let k be a finite field with p^m elements, where $p, m \in \mathbb{Z}^+$ and p is prime. Then k is the splitting field of the polynomial $f(x_n) = x_n^{p^m} - x_n$ over the finite field $\mathbb{F}_p$. Suppose then that there is no set S of polynomials in $k[x_1, \ldots, x_n]$ for which $X = V(S)$, for some $X \in \mathbb{A}^n(k)$. Choose then a point $P \in X$ and a polynomial $g \in S$. Then we have $g(x_1, \ldots, x_n) = g_1(\tilde{X})x_n + \cdots + g_n(\tilde{X})x_n$. Notice that if P is a root of f; i.e. $P \in V(f)$; i.e. $P^{p^m} - P = 0$, then since $P^{p^m} - P$ is a generator for k as a multiplicative group, it generates S. That is, S must contain the point P as a root for g, notice $P^{p^m} = P$ so that $g(P) = g_1(P)P + \cdots + g_n(P)P = 0$ in k. This contradicts that $X \neq V(S)$. This makes every set of $\mathbb{A}^n(k)$ algebraic for any finite field.

(3) By the corollory to lemma 1.2.1, we have that finite unions of algebraic sets are algebraic. Now, consider the field $\mathbb{Q}$, and let $f_q(x) = x + \frac{q}{2}$ in $\mathbb{Q}[x]$. We have that there are $X \subseteq \mathbb{A}^1(\mathbb{Q})$ algebraic, ini where $X = V(f_q)$. Notice however, that the polynomial

$$f(x) = \prod_{q \in \mathbb{Q}} f_q(x)$$

has no roots in $\mathbb{Q}$, as that would imply that for some $n \in \mathbb{Z}^+$, $\sqrt[n]{2} \in \mathbb{Q}$. That is, there is no $X \subseteq \mathbb{A}^1(\mathbb{Q})$ for which $X = V(\prod f_q) = \bigcup V(f_q)$. In general, the countable union of algebraic sets need not be algebraic.

Example 1.6. (1) Let k be a field, and $X = \{(t, t^2, t^3) \in \mathbb{A}^3(k) : t \in k\}$. If k is finite, this is algebraic. Suppose that k is infinite, and consider the polynomial $f(x_1, x_2, x_3) = x_1 + x_2^2 + x_3^3$. Notice that the point $0 \in X$ is a root of f, and that if P is a root of f, then $P \in X$. That is, $X = V(f)$ making X algebraic.

(2) Let $X = \{(\cos t, \sin t) \in \mathbb{A}^2(\mathbb{R}) : t \in \mathbb{R}\}$. Consider the polynomial $f(x, y) = x^2 + y^2 - 1$. Since we have that $\cos^2 t + \sin^2 t = 1$, $X = V(f)$ and X is algebraic.

(3) Let $X = \{(r, \sin t) \in \mathbb{A}^2(\mathbb{R}) : r = \sin t, t \in \mathbb{R}\}$. Consider the polynomial $f(x, y) = x - y$. Then $X = V(f)$.

Lemma 1.2.2. *Let k be a field and $C \subseteq \mathbb{A}^2(k)$ an affine plane curve. Let $L\mathbb{A}^2(k)$ a line not contained in C. Then C and L intersect at no more than n points; that is, $C \cap L$ is finite with at most n points.*

Proof. Let $C = V(f)$ where $f \in k[x, y]$ is a polynomial of degree n, and let $L = V(l)$ where $l(x, y) = y - ax + b$, for some $a, b \in k$. We have that $f(x, y) = f_1(x)y + f_2(x)y^2$. Now, notice that if X, Y is a root of l, then $l(X, Y) = Y - aX + b = 0$, so that $Y = aX + b$. Now, consider a point $P = (X, Y) \in C \cap L = V(f) \cap V(l)$. Then $f(X, Y) = f(X, aX + b) = f_1(X)(aX + b) + f_2(X)(aX + b)^2$. Since f has finitely many roots, there are finitely many $P = (X, Y)$ satisfying $f(X, Y) = 0$ Moreover, f has at most n roots. We finally observe that $C \cap L = V(f(x, ax + b))$. Which shows that $C \cap L$ is finite, and has at most n points. ■

Example 1.7. The following sets are not algebraic.

(1) $X = \{(x, y) \in \mathbb{A}^2(\mathbb{R}) : y = \sin x\}$. Let L be a line in $\mathbb{A}^2(\mathbb{R})$. Notice then that L intersects X at inifinitely many points, so that X cannot be algebraic.

(2) $X = \{(z, w) \in \mathbb{A}^2(\mathbb{C}) : |z|^2 + |w|^2 = 1\}$, where $|x + iy|^2 = x^2 + y^2$ for all $x, y \in \mathbb{R}$. Let $f(z, w) = |z|^2 + |w|^2 - 1$, and suppose that $X = V(f)$. Let L be a line in $\mathbb{A}^2(\mathbb{C})$ Then $|L \cap X| = 4$; however $\deg f = 2$, so that X cannot be algebraic.

(3) $X = \{(\cos t, \sin t, t) \in \mathbb{A}^3(\mathbb{R}) : t \in \mathbb{R}\}$. As in (1), there is a line L intersecting X at infinitely many points.

Theorem 1.2.3. *Let k be an algebraically closed field, Then for $n \geq 1$, the complement of an algebraic set is infinite.*

Proof. Observe that since k is algebraically closed, k is infinite, so that $\mathbb{A}^n(k)$ is infinite. Now, suppose $n = 1$, and let $f \in k[x]$ a nonconstant polynomail, and let $X = V(f)$ an algebraic set. Since f has at most finitely many roots, we get $|X|$ is finite, so that $\mathbb{A}^1(k) \backslash X$ is infinite. Moreover since $k[x]$ is a PID, every algebraic set is of the form $X = V(f)$.

Now, suppose that $n > 1$, Let $S \subseteq k[x_1, \dots, x_n]$. Let X be an algebraic set with $X = V(S)$. Then $S = (f_1, \dots, f_m, \dots)$. Now, if $P \in \mathbb{A}^{n-1}(k)$, then each $f_i(P, x_n) \in k[x_n]$ has finitely many roots. So that the polynomial $f_1(P, x_n) + \cdots + f_m(P, x_n) + \dots$ has finitely many roots. This makes X finite, and hence $\mathbb{A}^n(k) \backslash X$ is infinite. ■

Corollary. *If $f \in k[x_1, \ldots, x_n]$ is nonconstant, then $V(f)$ is infinite.*

Proof. consider $f \in k[x_1, \ldots, x_n]$ nonconstant. Observe that

$$f(x_1, \ldots, x_n) = \sum f_i(x_1, \ldots, x_{n-1})x_n^i$$

Where $f_i \in k[x_1, \ldots, x_{n-1}]$. Now, suppose that $P = (a_1, \ldots, a_{n-1})$, then

$$f(P, x_n) = \sum f_i(a_1, \ldots, a_{n-1})x_n^i$$

has at most n roots in $k[x_n]$. However, notice that since $\mathbb{A}^n(k)$ is infinite, there are infinitely many choices for P, so that if $Q = (P, a_n)$ is a root of f, then f has infinitely many roots. That is, $V(f)$ is finite. ■

Lemma 1.2.4. *Let k be a field, and let $X \subseteq \mathbb{A}^n(k)$ and $Y \subseteq \mathbb{A}^m(k)$ algebraic sets. Then $X \times Y$ is an algebraic set in $\mathbb{A}^{n+m}(k)$.*

Proof. Since $\mathbb{A}^m(k)$ and $\mathbb{A}^n(k)$ are cartesian products, we have that $\mathbb{A}^m(k) \times \mathbb{A}^n(k) = \mathbb{A}^{m+n}(k)$. Then $X \times Y = (X, Y)$. Now, let $S \subseteq k[x_1, \ldots, x_m]$ and $T \subseteq k[x_1, \ldots, x_n]$ such that $X = V(S)$ and $Y = V(T)$. Let $P \in X \times Y$, then $P = (A, B)$ where $A = (a_1, \ldots, a_m)$ and $B = (b_1, \ldots, b_n)$. Let $f = f_1 + \cdots + f_d + \cdots \in S$ and $g = g_1 + \cdots + g_l \in T$. Consider then $f \times g((x_1, \ldots, x_m), (y_1, \ldots, y_n)) = f(x_1, \ldots, x_m)g(y_1, \ldots, y_n)$. Since $f(A) = 0$ and $g(B) = 0$, then $f \times g(P) = f(A)g(B) = 0$ so that $P \in V(f) \times V(g)$. Conversely, let $P \in V(f) \times V(g)$. Then $P = (A, B)$ where $A \in \mathbb{A}^m(k)$ and $B \in \mathbb{A}^n(k)$, and $f \times g(P) = f(A)g(B) = 0$. Since $A \in V(f)$ and $B \in V(g)$, we get $f(A) = 0$ and $f(B) = 0$, so that $P \in X \times Y$. This makes $X \times Y = V(f) \times V(g)$. ■

1.3 Ideals of Algebraic Sets

Lemma 1.3.1. *Let k be a field, and $X \times \mathbb{A}^n(k)$. Consider the set $I(X) = \{f \in k[x_1, \ldots, x_n] : f(P) = 0$ for all $P \in X\}$. Then $I(X)$ forms an ideal of $k[x_1, \ldots, x_n]$.*

Proof. Let $f, g \in I(X)$. Then for all $P \in X$, $f(P) = 0$, and $g(P) = 0$, so that $f + g(P) = f(P) + g(P) = 0$. Moreover, $-f(P) = 0$ as well. So I is a subgroup of $k[x_1, \ldots, x_n]$ under addition. Now, take $f \in I(X)$ and $g \in k[x_1, \ldots, x_n]$. Then $fg(P) = 0$ for all $P \in X$ which makes $I(X)$ into an ideal. ■

Definition. Let k be a field and $X \subseteq \mathbb{A}^n(k)$. We define the **ideal** of X to be the ideal $I(X) = \{f \in k[x_1, \ldots, x_n] : f(P) = 0$ for all $P \in X\}$ of $k[x_1, \ldots, x_n]$.

Lemma 1.3.2. *Let k be a field. The following are true for all $X, Y \subseteq \mathbb{A}^n(k)$ and for all $S \subseteq k[x_1, \ldots, x_n]$.*

(1) If $X \subseteq Y$, then $I(Y) \subseteq I(X)$.

(2) $I(\emptyset) = k[x_1, \ldots, x_n]$ and $I(\mathbb{A}^n(k)) = (0)$.

(3) $S \subseteq I(V(S))$ and $X \subseteq V(I(X))$.

(4) $V(I(V(S))) = V(S)$ *and* $I(V(I(X))) = I(X)$.

Proof. Let $X, Y \subseteq \mathbb{A}^n(k)$, wiht $X \subseteq Y$. Let $f \in I(Y)$, then for all $P \in Y$, $f(P) = 0$. Now, since $P \in X$, we get for all $P \in X$ $f(P) = 0$ so that $f \in I(X)$.

Observe now that the polynomial $1(x_1, \dots, x_n) = 1$ has no points in $\mathbb{A}^n(k)$ as roots, so that $I(\emptyset) = k[x_1, \dots, x_n]$. Likewise, for the polynomial $0(x_1, \dots, x_n) = 0$, every point in $\mathbb{A}^n(k)$ is a root, so that $I(\mathbb{A}^n(k)) = (0)$.

For the third assertion, let $S \subseteq k[x_1, \dots, x_n]$. If $f \in V(S)$, then for every $P \in V(S)$, $f(P) = 0$, by definition. This makes $S \subseteq I(V(S))$. Likewise, if $X \subseteq \mathbb{A}^n(k)$ and $P \in X$, then for all $f \in I(X)$, $f(P) = 0$, so that $P \in V(I(X))$.

Lastly, let $P \in V(S)$, and $f \in I(V(S))$. By definition, $f(P) = 0$ so that $V(S) \subseteq V(I(V(S)))$. Conversely, let $P \in V(I(V(S)))$ then for every $f \in I(V(S))$, $f(P) = 0$, which puts $P \in V(S)$ so that $V(I(V(S))) \subseteq V(S)$. Likewise, by similar reasoning we conclude that $I(V(I(X))) = I(X)$. ■

Corollary. *If k is an infinite field, then for any $a_1, \dots, a_n \in k$, $I(a_1, \dots, a_n) = (x_1 - a_1, \dots, x_n - a_n)$.*

Proof. Let $f \in I(a_1, \dots, a_n)$. Since k is infinite, and $f(a_1, \dots, a_n) = 0$,

$$f(x_1, \dots, x_n) = \sum g_i(x_1, \dots, x_n)(x_i - a_i)$$

so $f \in (x_1 - a_1, \dots, x_n - a_n)$. Conversely, if $f \in (x_1 - a_1, \dots, x_n - a_n)$, we observe that $f \in I(a_1, \dots, a_n)$. ■

Definition. Let $\mathfrak{a}$ be an ideal of a ring R. We define the **radical** of $\mathfrak{a}$ to be the set

$$\operatorname{Rad} \mathfrak{a} = \{a \in R : a^n \in \mathfrak{a}, \text{ for some } n \in \mathbb{Z}^+\}$$

We call I a **radical ideal** if $I = \operatorname{Rad} I$.

Lemma 1.3.3. *Let R be a ring, and $\mathfrak{a}$ an ideal of R. Then* $\operatorname{Rad} \mathfrak{a}$ *is also an ideal of R.*

Proof. Let $a, b \in \operatorname{Rad} \mathfrak{a}$, then $a^m \in \mathfrak{a}$ and $b^n \in \mathfrak{a}$ for some $m, n \in \mathbb{Z}^+$. Now, observe that

$$(a + b)^{m+n} = a^{m+n} + \sum_{i=1}^{m+n-2} \binom{m+n}{i} a^i b^{m+n-i} + b^{m+n}$$

Now, $a^{m+n} = a^m a^n \in \mathfrak{a}$ and $b^{m+n} = b^n b^m \in \mathfrak{a}$ by the ideal properties of $\mathfrak{a}$. Moreover, notice if $i \geq n$, then $a^i b^{m+n-i} \in \mathfrak{a}$; on the otherhand, if $m \leq m + n - i$, then $a^i b^{m-n-i} \in \mathfrak{a}$. This makes each $a^i b^{m-n-i} \in \mathfrak{a}$, and that $(a + b)^{m+n} \in \mathfrak{a}$. Also observe that if $a^n \in \mathfrak{a}$, then $(-a)^n = -(a^n) \in \mathfrak{a}$. So that $\operatorname{Rad} \mathfrak{a}$ is an additive subgroup of R.

Lastly, suppose that if $a \in \operatorname{Rad} R$, and $r \in R$, then we have $(ra)^n = r^n a^n \in \mathfrak{a}$ for some $n \in \mathbb{Z}^+$. Thus $ra \in \operatorname{Rad} \mathfrak{a}$. This makes $\operatorname{Rad} \mathfrak{a}$ an ideal of R. ■

Corollary. $\operatorname{Rad} \mathfrak{a}$ *is a radical ideal of R.*

Proof. Observe that $\operatorname{Rad} \mathfrak{a} \subseteq \operatorname{Rad}(\operatorname{Rad} \mathfrak{a})$. Now, let $a \in \operatorname{Rad}(\operatorname{Rad} \mathfrak{a})$, then $a^n \in \operatorname{Rad} \mathfrak{a}$ for some $n \in \mathbb{Z}^+$, so that $(a^n)^m = a^{mn} \in \mathfrak{a}$ for some $m \in \mathbb{Z}^+$. This makes $a \in \operatorname{Rad} \mathfrak{a}$. So $\operatorname{Rad}(\operatorname{Rad} \mathfrak{a}) \subseteq \operatorname{Rad} \mathfrak{a}$. This makes $\operatorname{Rad} \mathfrak{a}$ radical. ■

Lemma 1.3.4. *Any prime ideal in a ring R is radical.*

Proof. Let $\mathfrak{p}$ be a prime ideal. We have that $\subseteq \operatorname{Rad}\mathfrak{p}$. Now, let $a \in \operatorname{Rad}\mathfrak{p}$. Then for some $n \in \mathbb{Z}^+$, we have that $a^n \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, either $a \in \mathfrak{p}$ or $a^{n-1} \in \mathfrak{p}$. If $a \in \mathfrak{p}$, we are done; otherwise we have $a^{n-1} = aa^{n-2} \in \mathfrak{p}$. Repeating this process recursively, we obtain that $a \in \mathfrak{p}$, so that $\mathfrak{p} = \operatorname{Rad}\mathfrak{p}$. ■

Lemma 1.3.5. *Let k be a field, then for any $X \subseteq \mathbb{A}^n(k)$, $I(X)$ is a radical ideal.*

Proof. For any $f \in I(X)$, notice that $f^n(P) = f(f^{n-1}(P)) = \cdots = \underbrace{f(f((P)))}_{n \text{ times}}$ ■

Example 1.8. Observe that $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$ is a field, so that (x^2+1) is a maximal ideal, hence a prime ideal, and hence, a radical ideal. Observe also that $V(x^2+1) = \emptyset$, so that $I(V(x^2+1)) = \mathbb{R}[x]$. Therefore, (x^2+1) is not the ideal of any nonempty set of $\mathbb{A}^1(\mathbb{R})$.

Lemma 1.3.6. *If X and Y are algebraic sets in $\mathbb{A}^n(k)$, then $I(X) = I(Y)$ if, and only if $X = Y$.*

Proof. If $X = Y$, then we can observe that $I(X) = I(Y)$. Conversely, suppose that $I(X) = I(Y)$, and let $f \in I(X)$. Then for all $P \in X$, we have $f(P) = 0$. Since $I(X) = I(Y)$, we must have that $P \in Y$ so that $X \subseteq Y$. In similar fashion, we get that $Y \subseteq X$. ■

Theorem 1.3.7. *Let k be a field. The ideal $(x_1 - a_1, \ldots, x_n - a_n)$ of $k[x_1, \ldots, x_n]$ is a maximal ideal of $k[x_1, \ldots, x_n]$ and the natural map*

$$k \to k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n)$$

defines an isomorphism.

Proof. Define the map $\phi : k[x_1, \ldots, k_n] \to k$ defined by the rule $f(x_1, \ldots, x_n) \to f(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in k$. Then notice that $\ker\phi = (x_1 - a_1, \ldots, x_n - a_n)$. Now, consider $f(x_1, \ldots, x_n) = 1 + 0x_1 + \cdots + 0x_n \in k[x_1, \ldots, x_n]$. Then $f(a_1, \ldots, a_n) = 1 + 0a_1 + \cdots + 0a_n = 1 \in \phi(k[x_1, \ldots, x_n])$. So that ϕ is onto. By the first isomorphism theorem for ring homomorphisms, we get

$$k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \simeq k$$

So that $(x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal. Notice also that $\Phi = \pi \circ \phi$ where $\pi : k \to k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n)$ is the natural map. So π defines the isomorphism. ■

1.4 Hilbert's Basis Theorem

Definition. Let R be a ring . We say a sequence of ideals $\{\mathfrak{a}_n\}$ is an **ascending chain** of ideals if $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$ for all $n \in \mathbb{Z}^+$. We say that the chain $\{\mathfrak{a}_n\}$ **stabalizes** if there exists some $k \geq n$, $\mathfrak{a}_k = \mathfrak{a}_n$.

Definition. Let R be a ring. We call A **Noetherian** if every ascending chain of ideals of A stabalizes. We say that A satisfies the **ascending chain condition** on ideals.

Lemma 1.4.1. *If $\mathfrak{a}$ is an ideal of a Noetherian ring R, then the factor ring ${}^{A}\!/_{\mathfrak{a}}$ is also Noethrian. In particular, the image of a Noetherian ring under any ring homomorphism is Noetherian.*

Proof. This follows by the isomorphism theorems for ring homomorphisms. ∎

Theorem 1.4.2. *The following are equivalent for any ring R.*

(1) R is Noetherian.

(2) Every nonempty collection of ideals of R contains a maximal element under inclusion.

(3) Every ideal of R is finitely generated.

Proof. Let R be Noetherian, and let $\mathcal{S}$ an nonempty collection of ideals of R. Choose an ideal $\mathfrak{a}_1 \in \mathcal{S}$. If $\mathfrak{a}_1$ is maximal, we are done. If not, then there is an ideal $\mathfrak{a}_2 \in \mathcal{A}$ for which $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$. Now, if $\mathfrak{a}_2$ is maximal, we are done. Otherwise, proceeding inductively, if there are no maximal ideals of R in $\mathcal{S}$, then by the axiom of choice, construct the infinite strictly increasing chain

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$$

of ideal of R. This contradicts that R is Noetherian, so $\mathcal{S}$ must contain a maximal element.

Now, suppose that any nonempty collection of ideals of R contains a maximal element. Let $\mathcal{S}$ the collection of all finitely generated ideals of R, and let $\mathfrak{a}$ be any ideal of R. By hypothesis, $\mathcal{S}$ has a maximal element $\mathfrak{a}'$. Now suppose that $\mathfrak{a} \neq \mathfrak{a}'$, and choose an $x \in \mathfrak{a} \backslash \mathfrak{a}'$, then the ideal generated by $\mathfrak{a}'$ and x is finitely generated, and so is in $\mathcal{S}$; but that contradicts the maximality of $\mathfrak{a}'$. Therefore we must have $\mathfrak{a} = \mathfrak{a}'$.

Finally, suppose every ideal of R is finitely genrated, and let $\mathfrak{a} = (a_1, \dots, a_n)$. Let

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$$

an ascending chain of ideals of R for which

$$\mathfrak{a} = \bigcup_{n \in \mathbb{Z}^+} \mathfrak{a}_n$$

Since $a_i \in \mathfrak{a}$ for each $1 \leq j \leq n$, we have that $a_i \in \mathfrak{a}_{i_j}$ and $i \in \mathbb{Z}^+$. Now, let $m = \max\{j_1, \dots, j_n\}$ and coinsider the ideal $\mathfrak{a}_m$. Then $a_i \in \mathfrak{a}_m$ for each i, which makes $\mathfrak{a} \subseteq \mathfrak{a}_m$. That is, $\mathfrak{a}_n = \mathfrak{a}_m$ for some $n \geq m$; which makes R Noetherian. ∎

Corollary. *Every proper ideal of a Noetherian ring is contained in a maxima ideal.*

Proof. Consider again the Noetherian ring R from above. Let $\mathfrak{a}$ be a proper ideal of R, and consider the collection $\mathcal{S}$ of proper ideals of R containing $\mathfrak{a}$. Then $\mathcal{S}$ contains a maximal member $\mathfrak{b}$ with $\mathfrak{a} \subseteq \mathfrak{b}$. Now, sine $\mathfrak{b}$ is maximal in $\mathcal{S}$ there is no other proper ideal $\mathfrak{b}'$ containing $\mathfrak{a}$ for which $\mathfrak{b} \subseteq \mathfrak{b}' \subseteq R$. This by definition makes $\mathfrak{b}$ a maximal ideal. ∎

Example 1.9. (1) Every principle ideal domain (PID) is Noetherian, since any collection of ideals has a maximal element. Moreover PIDs satisfy the ascending chain condition.

(2) The rings $\mathbb{Z}$, $\mathbb{Z}[i]$, and $k[x]$ (where k is a field) are Noetherian.

(3) The multivariate polynomial ring $\mathbb{Z}[x_1, x_2, \dots]$ is not Noetheria, since the ideal $(x_1, x_2, \dots)$ is not finitely generated.

Example 1.10. Let k be any field, and consider the collection $\mathcal{S} = \{(x_1 - a_1), \dots, (x_m - a_m)\}$ of ideals in $k[x_1, \dots, x_n]$. Then each $(x_i - a_i)$ is a maxmial member of $\mathcal{S}$, however none of them are maximal ideals. Observe the polynomial $f(x_1, \dots, x_n) = (x_1 - a_1) \dots (x_m - a_m)$. Then $(x_i - a_i) \subseteq (f)$ for each $1 \leq i \leq m$.

Definition. We call a ring in which every ideal is finitely generated a **Noetherian ring**.

Theorem 1.4.3 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring, then so is the polynomial ring $R[x]$.*

Proof. Let $\mathfrak{a}$ be an ideal of $R[x]$, and let L be the set of all leading coefficients of polyonimials in $\mathfrak{a}$. Notice that since $0 \in \mathfrak{a}$, then $0 \in L$, so that L is nonempty. Moreover, let $f(x) = ax^d + \dots$ and $g(x) = bx^e + \dots$ polynomials in $\mathfrak{a}$ of degree $\deg f = d$ and $\deg g = e$, with leading coefficients $a, b \in R$. Then for any $r \in R$, we have the coefficient $ra - b = 0$, or $ra - b$ is the leading coefficient of the polynomial $rx^e f - x^d g \in \mathfrak{a}$. In either case, we get $ra - b \in L$. This makes L an ideal of R. Now, since R is Noetherian L is finitely generated ; let $L = (a_1, \dots, a_n)$. Then for every $1 \leq i \leq n$, let $f_i \in \mathfrak{a}$ the polynomial of degree $\deg f_i = e_i$ whose leading coefficient is a_i. Take, then $N = \max\{e_1, \dots, e_n\}$. Then for any $d \in \mathbb{Z}/N\mathbb{Z}$, let L_d be the set of all leading coefficients of polynomials in $\mathfrak{a}$, of degree d, together with 0. Let $f_{di} \in \mathfrak{a}$ a polynomial of degree $\deg f_{di} = d$ with leading coefficient b_{di}. We wish to show that

$$\mathfrak{a} = (f_1, \dots, f_n) \cup (f_{d1}, \dots f_{nd})$$

Let $\mathfrak{a}' = (f_1, \dots, f_n) \cup (f_{d1}, \dots f_{nd})$. By construction, since the generators were chosen from $\mathfrak{a}$, $\mathfrak{a}' \subseteq \mathfrak{a}$. Now, if $\mathfrak{a} \neq \mathfrak{a}'$. Then there is a nonzero polynomial $f \in \mathfrak{a}$ of minimum degree not contained in $\mathfrak{a}'$ (i.e $f \notin \mathfrak{a}'$). Let $\deg f = d$, and let a be the leading coefficient of f. Suppose that $d \geq N$. Since $a \in L$, a is an R-linear combination of the generators of L; i.e.

$$a = r_1 a_1 + \dots + r_n a_n$$

where $r_1, \dots, r_n \in R$. Let

$$g = r_1 x^{d-e_1} f_1 + \dots + r_n x^{d-e_n} f_n$$

then $g \in \mathfrak{a}'$ and has degree $\deg g = d$ and leading coefficient a. Hence $f - g \in \mathfrak{a}'$ is of smaller degree, and by the minimality of f, $f - g = 0$, which makes $f = g \in \mathfrak{a}'$; a contradiction. THerefore $\mathfrak{a} = \mathfrak{a}'$

Now, if $d < N$, then $a \in L_d$, and so is an R-linear combniation of generators of L_d; that is

$$a = r_1 b_{d1} + \dots + r_n b_{dn}$$

where $r_1, \dots, r_n \in R$. Then let

$$g = r_1 f_{d1} + \cdots + r_n f_{dn}$$

then $g \in \mathfrak{a}'$ is a polynomial of degree $\deg g = d$ and leading coefficient a; which gives us the above contraditction.

Therefore, $\mathfrak{a} = \mathfrak{a}'$, and since $\mathfrak{a}'$ is finitely generated, $R[x]$ is Noetherian. ■

Corollary. *Let k be a field. Then the polynomial ring in n variables $k[x_1, \dots, x_n]$ is Noetherian.*

Theorem 1.4.4. *Every algebraic set is the intersection of a finite number of hypersurfaces.*

Proof. Let $\mathfrak{a}$ be an iddeal in the ring $k[x_1, \dots, x_n]$ for some field k, and consider the set $V(\mathfrak{a})$. Since $k[x_1, \dots, x_n]$ is Noetherian, then $\mathfrak{a} = (f_1, \dots, f_n)$, so that

$$V(\mathfrak{a}) = V(f_1) \cap \cdots \cap V(f_n)$$

■

Theorem 1.4.5. *Let $\mathfrak{a}$ be an ideal in a ring R, and consider the natural map $\pi : R \to {}^{R}\!/_{\mathfrak{a}}$. The following are true.*

(1) For every ideal $\mathfrak{b}'$ of ${}^{R}\!/_{\mathfrak{a}}$, $\pi^{-1}(\mathfrak{b}') = \mathfrak{b}$ is an ideal of R containing $\mathfrak{a}$. Moreover, for any ideal $\mathfrak{b}$ of R containing $\mathfrak{a}$, then $\pi(\mathfrak{b}) = \mathfrak{b}'$.

(2) The ideal $\mathfrak{b}'$ of ${}^{R}\!/_{\mathfrak{a}}$ is a radical ideal if, and only if $\mathfrak{b}$ is a radical ideal in R.

(3) If $\mathfrak{b}$ is finitely generated in R, then $\mathfrak{b}'$ is finitely generated in ${}^{R}\!/_{\mathfrak{a}}$. Moreover, ${}^{R}\!/_{\mathfrak{a}}$ is Noetherian if R is Noetherian.

Proof. Let $\mathfrak{b}'$ be an ideal of ${}^{R}\!/_{\mathfrak{a}}$. Since the natural map π is onto, there is an ideal $\mathfrak{b} \in R$ for which $\mathfrak{b} = \pi^{-1}(\mathfrak{b}')$. Now, let $a, b \in \mathfrak{b}$, then $\pi(a), \pi(b) \in \mathfrak{b}'$, so that $\pi(a+b) \in \mathfrak{b}'$ and $-\pi(a) \in \mathfrak{b}'$. Moreover, if $a \in \mathfrak{b}$, and $r \in R$, then $r\pi(a) = \pi(ra) \in \mathfrak{b}'$, since $\mathfrak{b}'$ is an ideal. Now, since $\ker \pi = \mathfrak{a}$, we have that $\mathfrak{a} \subseteq \mathfrak{b}$. So that $\mathfrak{b}$ is an ideal containing $\mathfrak{a}$. By similar reasoning, if $\mathfrak{b}$ is an ideal containing $\mathfrak{a}$, then $\mathfrak{b}' = \pi(\mathfrak{b})$ is also an ideal.

Now, suppose that $\mathfrak{b}$ is a radical ideal. That is, $\mathfrak{b} = \operatorname{Rad} \mathfrak{b}$. Since $\mathfrak{b} = \pi^{-1}(\mathfrak{b}')$, we have $\pi^{-1}(\mathfrak{b}') = \operatorname{Rad} \pi^{-1}(\mathfrak{b}')$. Now, suppose that $\mathfrak{b}$ is a prime ideal, then if $ab \in \mathfrak{b}$, either $a \in \mathfrak{b}$ or $b \in \mathfrak{b}$. This implies whenever $\pi(ab) \in \mathfrak{b}'$, either $\pi(a) \in \mathfrak{b}'$ or $\pi(b) \in \mathfrak{b}'$. This makes $\mathfrak{b}'$ prime. Similarly, if $\mathfrak{b}'$ is prime so is $\mathfrak{b}$. Finally, by definition of a maximal idea, $\mathfrak{b}$ is maximal if, and only if $\mathfrak{b}'$ is maximal.

Finally, suppose that $\mathfrak{b}$ is finitely generated, then $\mathfrak{b} = (a_1, \dots, a_n) = \pi^{-1}(\mathfrak{b}')$ for $a_1, \dots, a_n \in R$. Then every element of $\mathfrak{b}$ is the sum of $a_1, \dots, a_n$. That is, $b = r_1 a_1 + \cdots + r_n a_n$ for every $b \in \mathfrak{b}$, and $r_1, \dots, r_n \in R$. Now, since $b \in \mathfrak{b} = \pi^{-1}(\mathfrak{b}')$, then $\pi(b) = r_1 \pi(a_1) + \cdots + r_n \pi(a_n) \in \mathfrak{b}'$, so that $\mathfrak{b}' = (\pi(a_1), \dots, \pi(a_n))$. This makes $\mathfrak{b}'$ finitely generated. We can then conclude that if R is Noetherian, by theorem 1.4.2, ${}^{R}\!/_{\mathfrak{a}}$ must also be Noetherian. ■

Corollary. *Let k be a field and $\mathfrak{a}$ an ideal of $k[x_1, \dots, x_n]$. Any ring of the form ${}^{k[x_1, \dots, x_n]}\!/_{\mathfrak{a}}$ is a Noetherian ring.*

1.5 Irreducible Components

Definition. Let k be a field. We call an algebraic set $X \subseteq \mathbb{A}^n(k)$ **reducible** if it can be written as the union of two algebraic sets; that is, there exist $X_1, X_2 \subseteq \mathbb{A}^n(k)$ such that $X = X_1 \cup X_2$. We call an algebraic set **irreducible** if it is not reducible.

Example 1.11. (1) The algebraic sets defined by the equations $y^2 = x^3 - x$, $y^2 = x^3 + x^2$, and $z^2 = x^2 + y^2$ in $\mathbb{A}^2(\mathbb{R})$ and $\mathbb{A}^3(\mathbb{R})$, respecively, are irreducible.

(2) The algebraic set described by the equation $y^2 - xy - x^2y + x^2 = 0$ is reducible in $\mathbb{A}^2(\mathbb{R})$.

Lemma 1.5.1. *An algebraic set is irreducible if, and only if its ideal is prime.*

Proof. Let k be a field, and $X \subseteq \mathbb{A}^n(k)$. Suppose that the ideal $I(X)$ is not prime. Let $f_1 f_2 \in I(X)$, but $f_1, f_2 \notin I(X)$. Then

$$X = (X \cap V(f_1)) \cup (X \cap V(f_2))$$

and $X \cap V(f_1) \subseteq X$ and $X \cap V(f_2) \subseteq X$. This makes X reducible, by definition.

Conversely, suppose that X is reducible, and that $X = X_1 \cup X_2$ for $X_1, X_2 \subseteq \mathbb{A}^n(k)$. Then $I(X) \subseteq I(X_1)$ and $I(X) \subseteq I(X_2)$. Let $f_1 \in I(X_1)$ and $f_2 \in I(X_2)$, but $f_1, f_2 \notin I(X)$. Then $f_1 f_2 \in I(X)$, but $f_1, f_2 \notin I(X)$, so that $I(X)$ is not prime. ∎

Example 1.12. (1) Consider the polynomial $f(z, w) = w - z^2$ in $\mathbb{C}[z, w]$, and let $g \in I(V(f))$. Then for every point $P \in V(f)$, $g(P) = 0$. Moreover, by the division theorem for polynomials, there are polynomials $q, r \in (\mathbb{C}[z])[w]$ for which

$$g(z, w) = f(z, w)q(z, w) + r(z, w) \text{ where } r = 0 \text{ or } \deg_w r < \deg_w f$$

Notice that the degree of r in w, $\deg_w r = 0$ so that $r \in \mathbb{C}[z]$. Now, since $g(P) = f(P)q(P) + r(P) = r(P) = 0$, and r is a polynomial only in z, then $r(z, w) = r(z) = 0$. That is $g(z, w) = f(z, w)q(z, w)$ so that $g \in (f)$. This makes $I(V(f)) = (f)$. Lastly, notice that $\mathbb{C}[z, w]/(f) \simeq \mathbb{C}[z]$ which is an integral domain. This makes (f) a prime ideal, and hence the algebraic set $V(w - z^2)$ is irreducible.

(2) Let $f(z, w) = w^4 - z^2$ and $g(z, w) = w^4 - z^2w^2 + zw^2 - z^2$. Then observe that

$$\begin{aligned} V(f, g) &= V(f) \cap V(g) \\ &= (V(w^2 - z) \cup V(w^2 + z)) \cap (V(w + z) \cup V(w - z) \cup V(w^2 + z)) \\ &= V(w^2 + z) \end{aligned}$$

(3) Consider the polynomial $f(x, y) = y^2 + x^2(x - 1)^2$. f factors into

$$f(x, y) = (x^2 - x - iy)(x^2 - x + iy)$$

in $\mathbb{C}[x, y]$, where $i^2 = -1$. This makes f irreducible in $\mathbb{R}[x, y]$. However, notice that $f(x, y) = 0$ only at the points $(1, 0)$ and $(0, 0)$, so that $|V(f)| = 2$. This makes $V(f)$ reducible as an algebraic set in $\mathbb{A}^2(\mathbb{R})$.

Example 1.13. (1) Let k be a finite field. Then very subset of $\mathbb{A}^n(k)$ is an algebraic set, and so we can partition $\mathbb{A}^n(k) = X \cup Y$, where X and Y are algebraic, and $X \neq \mathbb{A}^n(k)$ and $Y \neq \mathbb{A}^n(k)$. This makes $\mathbb{A}^n(k)$ reducible. One can also observe that the ideal (0) is not prime in $k[x_1, \ldots, x_n]$ for finite fields.

(2) Now, suppose that k is an infinite field. Then the ideal (0) is prime in $k[x_1, \ldots, x_n]$, so that $I(\mathbb{A}^n(k)) = (0)$ is prime. This makes $\mathbb{A}^n(k)$ irreducible.

Lemma 1.5.2. *Any collection of algebraic sets has a minimal member.*

Proof. If $\{X_\alpha\}$ is a collection of algebraic sets in $\mathbb{A}^n$, then by theorem 1.4.2 the collection of ideals $\{I(X_\alpha)\}$ has a maximal member. Choose such a maximal member $I(X_{\alpha_0})$, then the corresponding algebraic set X_{α_0} is a minimal member of the collection $\{X_\alpha\}$. ■

Theorem 1.5.3. *Any algebraic set can be uniquely expressed as the disjoint union of irreducible algebraic sets. That is; for any algebraic set $X \subseteq \mathbb{A}^n$, there exist unique pairwise disjoint $X_1, \ldots, X_m \subseteq \mathbb{A}^n$ for which*

$$X = X_1 \cup \cdots \cup X_m$$

Proof. We first show that such a decomposition exists for every algebraic set in $\mathbb{A}^n$. Let $\mathcal{S}$ be the collection of all algebraic sets which cannot be expressed as a (not necessarily disjoint) union of (not necessarily unique) irreducible algebraic sets. Let X be a minimal element of $\mathcal{S}$. Then X is not irreducible. Hence there exist $X_1, X_2 \subseteq \mathbb{A}^n$ for which $X = X_1 \cup X_2$; suppose further that $X_1, X_2 \subsetneq X$. By the minimality of X, $X_1, X_2 \notin \mathcal{S}$, so that

$$X_i = \bigcup_{j=1}^{m_i} X_{ij}$$

where each X_{ij} is irreducible. This makes

$$X = \bigcup_{i=1,j=1}^{m,m_i} X_{ij}$$

which contradicts that $X \in \mathcal{S}$. Therefore $\mathcal{S}$ must be empty, and every algebraic set can be expressed as the union of irreducible algebraic sets.

Now, take $X = X_1 \cup \ldots X_m$, where each X_i is irreducible, and discard all those X_i for which $X_i \subseteq X_j$ for all $i \neq j$. This makes X a disjoint union. Now, suppose that $X = Y_1 \cup \ldots Y_r$. Then

$$X_i = \bigcup_{j=1}^{r} (Y_j \cap X_i)$$

so that $X_i \subseteq Y_j$ for some j. Similarly, we get that $Y_j \subseteq X_k$ for some k. Thus $X_i \subseteq X_k$, but since X is already a disjoint union, this makes $i = k$ so that $X_i = Y_j$ and $m = r$. Thus the decomposition of X into mutually disjoint irreducible algebraic sets is unique. ■

Corollary. *If $X, Y \in \mathbb{A}^n$ are algebraic such that $X \subseteq Y$, then each irreducible component of X is contained in an irreducible component of Y.*

Proof. Let

$$X = \bigcup_{i=1}^{m} X_i$$
$$Y = \bigcup_{j=1}^{n} Y_j$$

where X_i and Y_j are the irreducible components of X and Y, respectively for all $1 \leq i \leq m$ and $1 \leq j \leq n$. Now, consider the collection $\mathcal{S}$ of all irreducible components of X not contained in an irreducible component of Y Then $\mathcal{S}$ has a minimal member X', such that for every $1 \leq j \leq n$, $X' \nsubseteq Y_j$, then $X' \nsubseteq Y$. Now, since X' is an irreducible component, we get $X' \subseteq X \subseteq Y$, which is a contradicion. This makes $\mathcal{S}$ the emptyset. ■

Definition. Let k be a field, and $X \subseteq \mathbb{A}^n(k)$ an algebraic set. Let $X = X_1 \cup \dots X_m$ the decomposition of X into the union of pairwise disjoint irreducible algebraic sets. We call each X_i an **irreducible component** of X.

1.6 Algebraic Subsets of The Plane

Lemma 1.6.1. *Let k be a field, and let $f, g \in k[x,y]$ polynomials with no common factor. Then the set $V(f,g) = V(f) \cap V(g)$ is a finite set of points.*

Proof. Notice that if f and g are coprime in $k[x,y] \simeq k[x][y]$, then they are coprime in $k(x)[y]$, where $k(x)$ is the field of fractions of $k[x]$. We have that $k(x)[y]$ is a PID, and that the ideal $(f,g) = (1)$. Then there exist $r, s \in k(x)[y]$ for which $rf(x,y) + sg(x,y) = 1$. There also exists a $d \in k[x]$ such that $d(x)r = a(x,y)$ and and $d(x)s = b(x,y)$ in $k[x,y]$. Then $a(x,y)f(x,y) + b(x,y)g(x,y) = d(x)(rf(x,y)) + d(x)(rg(x,y)) = d(x)$. Now, if $A, B \in V(f,g)$, then $d(A) = 0$. Now, d has finitely many roots in k, so that there are finitely many x-coordinates corresponding to the points of $V(f,g)$. Similarly, in the PID $k(y)[x]$, we get that there are finitely many y-coordinates corresponding to the points of $V(f,g)$. That is $V(f,g)$ have finitely many points. ■

Corollary. *If f is irreducible in $k[x,y]$ and $V(f)$ is finite, then $I(V(f)) = (f)$, and $V(f)$ is an irreducible algebraic set.*

Proof. Suppose that $g \in I(V(f))$, then $V(f,g)$ is infinite, and by the above lemma, we get that $g|f$. Then $g \in (f)$, so that $I(V(f)) = (f)$. Moreover, since f is irreducible in the $k[x,y]$, if $ab \in (f)$, then either $a \in (f)$ or $b \in (f)$, which makes $I(V(f)) = (f)$ a prime ideal. This makes $V(f)$ irreducible by lemma 1.5.1. ■

Corollary. *Suppose that k an infinite field, then the irreducible algebraic sets of $\mathbb{A}^2(k)$ are $\mathbb{A}^2(k)$ itself, the emptyset, point sets, and irreducible plane curves $V(f)$, where $f \in k[x,y]$ is irreducible and $V(f)$ is infinite.*

Proof. Let $X \subseteq \mathbb{A}^2(k)$ an irreducible algebraic set. If X is finite, or $I(X) = (0)$, then it is either $\mathbb{A}^n(k)$, the emptyset, or a finite algebraic set (i.e. a set of points). Suppose then, that X is infinite. Then there exists a nonconstant polynomial $f \in I(X)$. Now, since X is irreducible, $I(X)$ is prime, and hence contains an irreducible factor of f; thus, suppose without loss of generality that f is irreducible. Then $I(X) = (f)$; for otherwise, if $g \in I(X)$ but $g \notin (f)$, then $X \subseteq V(f, g)$ is finite which is a contradiction. This makes $X = V(f)$ as required. ■

Corollary. *If k is an algebraically closed field, and f has the decomposition $f = f_1^{n_1} \dots f_m^{n_m}$ into irreducible factore, then $V(f) = V(f_1) \cup \dots V(f_m)$ is the decomposition of $V(f)$ into irreducible components. Moreover, $I(V(f)) = (f_1 \dots f_m)$.*

Proof. By hypothesis, we have that each f_i and f_j are coprime whenever $i \neq j$. That is, there exist no inclusions under each $V(f_i)$, so that the decomposition $V(f) = V(f_1) \cup \dots \cup V(f_m)$ is the decompostion of $V(f)$ into irreducible components. Now, we also have that

$$I(V(f)) = \bigcap_{i=1}^{m} I(V(f_i)) = \bigcap_{i=1}^{m} (f_i)$$

Now, since each polynomial divisible by f_i is also divisible by $f_1 \dots f_m$, we get that $\bigcap (f_i) = (f_1 \dots f_m)$. Lastly, notice that since k is algebraically closed, and hence infinite, each $V(f_i)$ is infinite. ■

Example 1.14. (1) Consider $f(x, y) = x^2 + y^2 + 1$ over $\mathbb{R}$. We have that f is irreducible, and that $V(f)$ is finite (in fact $V(f) = \emptyset$), so that $I(V(f)) = (f)$. Moreover, since f has no roots in $\mathbb{R}$, we observe that $(f) = (1)$. This result could've also been extracted using the fact that $I(V(f)) = I(\emptyset) = \mathbb{R}[x, y] = (1)$.

(2) Consider $X \subseteq \mathbb{A}^2(\mathbb{R})$ an algebraic set. Then there is some $S = (f_1, \dots, f_n) \in \mathbb{R}[x, y]$ for which $X = V(S) = V(f_1, \dots, f_n) = V(f_1) \cap \dots \cap V(f_n)$. Now, by the above corollories, and assuming that each f_i is pairwise coprime, $X = V(S)$ is a finite set of points. Take

$$f(x, y) = \sum_{i=1}^{n} f_i^2(x, y)$$

which has finitely many roots as a polynomial in $\mathbb{R}[x][y]$, and as a polynomial in $\mathbb{R}[y][x]$. Then $(f) = (f_1, \dots, f_n)$ so that $X = V(f)$. In geneal, we want to work over algebraically closed fields to avoid this, since the intersections of hypersurfaces need not be finite.

Example 1.15. (1) We have that $V(y^2 - xy - x^2y + x^3) = V(x - y) \cup V(x^2 + y)$ over both $\mathbb{R}$ and $\mathbb{C}$.

(2) The set $V(y^2 - x(x^2 - 1))$ is irreducible over both $\mathbb{R}$ and $\mathbb{C}$ since the polynomial $y^2 - x(x^2 - 1)$ is an irreducible polynomial over both $\mathbb{R}$ and $\mathbb{C}$.

(3) $V(x^3 + x - x^2y - y)$ is irreducible over $\mathbb{R}$, but $V(x^3 + x - x^2y - y) = V(x - i) \cup V(x + i) \cup V(x - y)$ over $\mathbb{C}$, where $i^2 = -1$.

1.7 Hilbert's Nullstellensatz

Theorem 1.7.1 (The Weak Nullstellensatz)**.** *Let k be an algebraically closed field, then if $\mathfrak{a}$ is a proper ideal of $k[x_1, \ldots, x_n]$, $V(\mathfrak{a})$ is nonempty.*

Proof. Since any proper ideal is contained in a maximal ideal, and algebraic sets of maximal ideals are minimal, suppose, without loss of generality, that $\mathfrak{a}$ is a maximal ideal in $k[x_1, \ldots, x_n]$. Take $l = {k[x_1, \ldots x_n]}/{\mathfrak{a}}$. Since $\mathfrak{a}$ is maximal, l is a field, and $k \subseteq l$ is a subfield. Now, suppose that $k = l$, then for every i, there is an element $a_i \in k$ such that $x_i - a_i \in \mathfrak{a}$. But $(x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal, so that $\mathfrak{a} = (x_1 - a_1, \ldots, x_n - a_n)$ and $V(\mathfrak{a}) = V(x_1 - a_1, \ldots, x_n - a_n)$ which is nonempty. ■

Theorem 1.7.2 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field, and $\mathfrak{a}$ an ideal of $k[x_1, \ldots, x_n]$. Then $I(V(\mathfrak{a})) = \operatorname{Rad} \mathfrak{a}$.*

Proof. We have that $\operatorname{Rad} \mathfrak{a} \subseteq I(V(\mathfrak{a}))$. Now, let $\mathfrak{a} = (f_1, \ldots, f_r)$, since $k[x_1, \ldots, x_n]$ is Noetherian, and let $g \in I(V(\mathfrak{a}))$. Let $\mathfrak{b} = (f_1, \ldots, f_r, x_{n+1}g - 1)$ an ideal of $k[x_1, \ldots, x_n, x_{n+1}]$. Then $\mathfrak{b} \subseteq \mathbb{A}^{n+1}(k)$ is empty, since g vanishes whenever all $f_i = 0$. By the weak nullstellensats, this puts $1 \in \mathfrak{b}$ so that

$$1 = \sum a_i(x_1, \ldots, x_{n+1}) f_i(x_1, \ldots, x_{n+1}) + b(x_1, \ldots, x_{n+1})(x_{n+1} g(x_1, \ldots, x_n) - 1)$$

Letting $y = \frac{1}{x_{n+1}}$, we get

$$y^n = \sum c_i(x_1, \ldots, x_{n+1}) f_i(x_1, \ldots, x_{n+1}) + d(x_1, \ldots, x_{n+1})(g(x_1, \ldots, x_n) - y)$$

Substituting g for y gives us

$$g^n = \sum c_i(x_1, \ldots, x_{n+1}) f_i(x_1, \ldots, x_{n+1}) \in \operatorname{Rad} \mathfrak{a}$$

so that $I(V(\mathfrak{a})) \subseteq \operatorname{Rad} \mathfrak{a}$, and we are done. ■

Corollary. *If $\mathfrak{a}$ is a radical ideal in $k[x_1, \ldots, x_n]$, then $I(V(\mathfrak{a})) = \mathfrak{a}$.*

Corollary. *If $\mathfrak{a}$ is a prime ideal in $k[x_1, \ldots, x_n]$, the $V(\mathfrak{a})$ is irreducible. Moreover, there is a 1–1 correspondence between prime ideals of $k[x_1, \ldots, x_n]$ and irreducible sets of $\mathbb{A}^n(k)$; where maximal ideals correspond to points.*

Corollary. *For any $f \in k[x_1, \ldots, x_n]$, if $f = f_1^{r_1} \ldots f_m^{m_r}$ is the decomposition of f into irreducible factors, then $V(f) = V(f_1) \cup \ldots V(f_m)$ is the decomposition of f into irreducible components, and $I(V(f)) = (f_1 \ldots f_m)$ Moreover, there is a 1–1 correspondence between irreducible polynomials of $k[x_1, \ldots, x_n]$, and irreducible hypersurfaces of $\mathbb{A}^n(k)$.*

Corollary. *If $\mathfrak{a}$ is an ideal of $k[x_1, \ldots, x_n]$, then $V(\mathfrak{a})$ is finite, if, and only if ${k[x_1, \ldots, x_n]}/{\mathfrak{a}}$ is a finite dimensional vector space over k, with*

$$|V(\mathfrak{a})| \leq \dim {k[x_1, \ldots, x_n]}/{\mathfrak{a}}$$

Proof. Suppose that $l = {}^{k[x_1, \ldots, x_n]}\!/_{\mathfrak{a}}$ is a finite dimensional vector space over k, and let $P_1, \ldots, P_n \in V(\mathfrak{a})$. Choose polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ such that $f_i(P_j) = 0$ for any $i \neq j$, and $f_i(P_i) = 1$. Consider now the residue classes of f_i in $\mathfrak{a}$, if

$$\sum \lambda_i(f_i + \mathfrak{a}) = 0 \text{ where } \lambda \in k$$

We have $\sum \lambda_i f_i \in \mathfrak{a}$, so that

$$\lambda_i = (\sum \lambda_i f_i)(P_i) = 0$$

which makes the collection of vectors $\{f_i + \mathfrak{a}\}$ linearly independent in l. This makes $V(\mathfrak{a})$ finite with $|V(\mathfrak{a})| = m \leq \dim l$.

Conversely, suppose that $V(\mathfrak{a})$ is finite, and that $V(\mathfrak{a}) = \{P_1, \ldots, P_m\}$, where $P_i = (a_{i1}, \ldots, a_{im})$, and

$$f_j(x_1, \ldots, x_n) = \prod_{j=1}^{m} (x_j - a_{ij}) \text{ in } k[x_1, \ldots, x_n]$$

Then $f_j \in I(V(\mathfrak{a}))$, so that $f^N \in \mathfrak{a}$ for some $N \in \mathbb{Z}^+$. Taking N large enough and $(f_j + \mathfrak{a})^N = 0$, we get $(x_j + \mathfrak{a})^N$ is a k-linear combination of the vectors $\{1, x_1 + \mathfrak{a}, \ldots, (x_n + \mathfrak{a})^{rN-1}\}$. By induction, we see that for any $s \geq N$, $(x_j + \mathfrak{a})^s$ is a k-linear combination of the vectors $\{1 + \mathfrak{a}, \ldots, (x_j + \mathfrak{a})^{rN-1}\}$. Then the collection of vectors $\{(x_1 + \mathfrak{a})_1^m, \ldots, (x_n + \mathfrak{a})^{m_n}\}$, with $m_i < rN$ generates ${}^{k[x_1, \ldots, x_n]}\!/_{\mathfrak{a}}$ as a finite dimensional vector space over k. ∎

Bibliography

[1] D. Dummit, *Abstract algebra.* Hoboken, NJ: John Wiley & Sons, Inc, 2004.

[2] I. N. Herstein, *Topics in algebra.* New York: Wiley, 1975.

[3] M. Atiyah and I. MacDonald, *Introduction to Commutative Algebra.* Addison-Wesly Series in Mathematics, CRC Press.

[4] D. Eisenbud, *Commutative Algebra: Wit a View Toward Algebraic Geometry.* Graduate Texts in Mathematics, Springer Verlag.

[5] R. Hartshorne, *Algebraic Geometry.* Graduate Texts in Mathematics, Springer Verlag.

[6] W. Fulton, *Algebraic Curves: An Introduction to ALgebraic Geometry.* Advanced Book Classics, Addison-Wesley.