Definition 1.1. A set $R$ with two binary operations $\,+, \cdot$ (addition and multiplication) is a ring if the following properties hold for all $a, b, c \in R$:

1. $a + (b + c) = (a + b) + c$.
2. $a + b = b + a$.
3. There is an element $0 \in R$ such that $a + 0 = 0 + a = a$.
4. For each $a \in R$ there exists $-a \in R$ such that $a + (-a) = (-a) + a = 0$.
5. $(ab)c = a(bc)$.
6. (Distributivity) $a(b + c) = ab + ac$.

If there exists a $1 \in R$ such that $a1 = 1a = a$ for all $a \in R$, we say that $R$ is a ring with identity. Furthermore, if the multiplication is commutative, we say that $R$ is commutative. Finally, if, for every $a \neq 0 \in R$, there exists $a^{-1}$ such that $aa^{-1} = a^{-1}a = 1$, then we say $R$ is a division ring. $R$ is a field if $R$ is a commutative, division ring with identity.

Example 1.1. (1) $\mathbb{Z}$ is a commutative ring with unit.

(2) If $R$ is a commutative ring with identity, then we can adjoin indeterminates to the ring. Indeed, define

$$R[x] = \{a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \mid a_i \in F \mid n \geq 0\}.$$ 

Such a ring is a commutative ring with unit, called a polynomial ring.

(3) A field $F$ does not have to be infinite. Take $\mathbb{Z}/p\mathbb{Z}$ for a prime $p$. This is the field of $p$ elements with addition and multiplication defined mod $p$. We denote this field $\mathbb{F}_p$.

Unless otherwise stated, whenever we use the term “ring” we will mean a commutative ring with identity.

Definition 1.2. A nonzero element $a \in R$ is a zero divisor if $a \cdot b = 0$ for some nonzero $b \in R$. A ring is an integral domain if $R$ does not contain any zero divisors.

Proposition 1.1. Every field $F$ is an integral domain.

Proof. Assume $ab = 0$ for $a, b \in F$ and $a \neq 0$. Then, multiply by $a^{-1}$ to get

$$a^{-1}ab = 0 \Rightarrow 1b = 0 \Rightarrow b = 0.$$ 

Definition 1.3. Let $R$ be a ring. A subset $I \subset R$ is an ideal if it satisfies the following:

1. If $a, b \in I$ then $a + b \in I$.
2. If $a \in I$ and $r \in R$, then $ra \in I$ for all $r \in R$.

Proposition 1.2. Let $R$ be a ring. An element $a \in R$ is a unit if there exists $a^{-1}$ in $R$. If $I \subset R$ is an ideal containing a unit, then $I = R$. 

1
Proof. If \( u \in I \) is a unit, then \( u^{-1}u \in I \) by definition, which implies that \( 1 \in I \). However, if \( 1 \in I \), then \( r \cdot 1 \in I \) for all \( r \in R \) by definition. \( \square \)

**Corollary 1.1.** The only ideals in a field are trivial.

**Proof.** Exercise. \( \square \)

**Example 1.2.** Consider \( \mathbb{Z} \). The only ideals in \( \mathbb{Z} \) are \( n\mathbb{Z} \) for each \( n \in \mathbb{Z} \).

Back to fields:

**Definition 1.4.** Let \( F \) be a field. \( F \) is algebraically closed if every nonconstant polynomial in \( F[x] \) contains a root in \( F \).

**Example 1.3.** \( \mathbb{Q} \) and \( \mathbb{R} \) are not algebraically closed. For instance, the polynomial \( x^2 + 1 \) does not have a root in \( \mathbb{Q} \) or \( \mathbb{R} \). However, \( \mathbb{C} \) is algebraically closed. This is the Fundamental Theorem of Algebra.

We defined a polynomial ring \( R[x] \) as polynomials in an indeterminate \( x \). If we start with the ring \( R[x] \) and adjoin another indeterminate \( y \), we get a new ring \( R[x][y] \), or \( R[x,y] \). If we do this finitely many times, we get a polynomial ring \( R[x_1,\ldots,x_n] \). This is the polynomial ring with \( n \) variables, and this will be our ring of focus.

## 2. Polynomials, Affine Spaces, Affine Varieties

Unless otherwise noted, \( k \) is a field.

### 2.1. Polynomials in \( k[x_1,\ldots,x_n] \).

**Definition 2.1.** A monomial in \( k[x_1,\ldots,x_n] \) is an expression of the form \( x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n} \) where each \( \alpha_i \) is a nonnegative integer. The degree of the monomial is \( \alpha_1 + \ldots + \alpha_n \).

Sometimes a shorthand notation will be used. Instead of writing \( x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n} \), we may sometimes say \( \alpha = (\alpha_1,\ldots,\alpha_n) \) and write \( x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n} \).

**Definition 2.2.** A polynomial \( f \) in variables \( x_1,\ldots,x_n \) with coefficients in \( k \) is a finite linear combination of monomials. In other words, it is an expression of the form

\[
    f = \sum_{\alpha} a_{\alpha} x^\alpha \quad a_{\alpha} \in k.
\]

Each \( a_{\alpha} \) is called the coefficient of the monomial \( x^\alpha \). The total degree of the polynomial \( f \) is the maximum degree among all monomials appearing in the polynomial.

**Example 2.1.** Consider \( \mathbb{Q}[x,y,z] \). \( p(x,y,z) = 34x^5y^3z^7 + 3x^4yz^9 + 10xyz^3 \) is a polynomial. The total degree of \( p \) is 15. The coefficients (in order of terms from left to right) are 34, 3, and 10.

### 2.2. Affine Spaces.

**Definition 2.3.** Let \( n \) be a positive integer. We define an \( n \)-dimensional affine space over \( k \) to be the set

\[
    k^n = \{(a_1,\ldots,a_n) \mid a_1,\ldots,a_n \in k\}.
\]

\( k^1 \) is usually called the affine line. \( k^2 \) is called the affine plane.
We can relate polynomials to affine spaces by the evaluation map

\[ eval_f : k^n \to k, \]

defined as follows: given a polynomial \( f(x_1, \ldots, x_n) \) in the polynomial ring \( k[x_1, \ldots, x_n] \), we write

\[ eval_f(f(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n) \]

for each \((a_1, \ldots, a_n) \in k^n\). In other words, we replace each \( x_i \) by \( a_i \). Since each \( a_i \in k \), the image would be contained in \( k \). This is the usual notion of “plugging in” values for each variable \( x_i \) in the polynomial.

In finite fields, it is possible to have non-zero polynomials that induce the zero evaluation map. Consider \( \mathbb{F}_2[x] \). The polynomial \( f = x^2 - x \) is a nonzero polynomial in \( \mathbb{F}_2[x] \), but for all values in \( \mathbb{F}_2 \), the \( eval_f \) map is the zero map.

**Proposition 2.1.** Let \( k \) be an infinite field, and let \( f \in k[x_1, \ldots, x_n] \). Then \( f = 0 \) (that is, \( f \) is the zero polynomial) if and only if \( eval_f : k^n \to k \) is the zero function.

**Proof.** (\( \Rightarrow \)) is clear. Assume that \( f(a_1, \ldots, a_n) = 0 \) for all \((a_1, \ldots, a_n) \in k^n\). By induction on the number of variables \( n \), we will show that if \( eval_f \) is the zero map, then \( f \) is the zero polynomial. Assume \( n = 1 \). A polynomial \( f \in k[x] \) has at most \( \deg(f) \) roots. Since \( f(a) = 0 \) for all \( a \in k \) and since \( k \) is infinite, this means that \( f \) has infinitely many roots, and therefore must be the 0 polynomial.

Now assume the assertion is true for \( n - 1 \) variables, and let \( f(x_1, \ldots, x_n) \) be a polynomial that vanishes at all points in \( k^n \). Rewrite \( f \) as a polynomial in \( x_n \):

\[ f = \sum_{i=0}^{m} g_i x_n^i \]

where each \( g_i \in k[x_1, \ldots, x_n-1] \). If we show that \( g_i \) is the zero polynomial in \( n - 1 \) variables, then it would follow that \( f \) is the zero polynomial. Fix \((a_1, \ldots, a_{n-1}) \in k^{n-1} \). We get the polynomial \( f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n] \) (with coefficients \( g_i(a_1, \ldots, a_{n-1}) \)).

From our base case assumption, since the polynomial \( f(a_1, \ldots, a_{n-1}, x_n) \) vanishes at each \( a_n \in k \), we have that \( f(a_1, \ldots, a_{n-1}, x_n) \) is the zero polynomial. Since \( f(a_1, \ldots, a_{n-1}, x_n) \) is a polynomial with coefficients \( g_i(x_1, \ldots, x_{n-1}) \), it follows that \( g_i(a_1, \ldots, a_{n-1}) = 0 \). Since \((a_1, \ldots, a_{n-1}) \) was an arbitrary choice, it follows that \( g_i(x_1, \ldots, x_{n-1}) = 0 \) for any \((b_1, \ldots, b_{n-1}) \in k^{n-1} \). By the inductive hypothesis, each \( g_i \) is the zero polynomial, which forces \( f \) to be the zero polynomial. \( \square \)

**Corollary 2.1.** Let \( k \) be an infinite field, and let \( f, g \in k[x_1, \ldots, x_n] \). Then \( f = g \) if and only if the functions \( eval_f : k^n \to k \) and \( eval_g : k^n \to k \) are the same.

**Proof.** Exercise. \( \square \)

2.3. **Affine Varieties.** Now that we have a connection from polynomials to evaluation functions, we can begin studying an important geometric object:

**Definition 2.4.** Let \( k \) be a field, and let \( f_1, \ldots, f_m \in k[x_1, \ldots, x_n] \). Define

\[ \mathcal{V}(f_1, \ldots, f_m) := \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ for all } i, 1 \leq i \leq m \}. \]

We call \( \mathcal{V}(f_1, \ldots, f_m) \) the affine variety of \( f_1, \ldots, f_m \).
In other words, the affine variety of the polynomials $f_1, \ldots, f_m$ is the set of all common solutions in $k^n$ of the system $f_1 = \ldots = f_m = 0$.

**Example 2.2.**

1. The affine variety $V(x^2 + y^2 - r^2)$ in $\mathbb{R}^2$, where $x, y$ are variables and $r$ is a fixed constant, yields the circle of radius $r$ circled about the origin.

2. We know what the graph of $y = \frac{1}{x}$ looks like. To view it as an affine variety in $\mathbb{R}^2$, we write it as $V(xy - 1)$.

3. In $\mathbb{R}^3$, consider the affine variety $V(y - x^2, z - x^3)$. This gives the twisted cubic as solutions.

4. Consider the affine variety $V(xz, yz)$ in $\mathbb{R}^3$. We get that $xz = yz = 0$ has the entire $(x, y)$ plane and the $z$–axis as solutions.

**Example 2.3.** In higher dimensional space, we have examples of affine varieties using linear algebra. Given $k^n$, consider a system of $m$ linear equations in $n$ unknowns with coefficients in $k$:

$$a_{11}x_1 + \ldots + a_{1n}x_n = b_1$$

$$\vdots$$

$$a_{m1}x_1 + \ldots + a_{mn}x_n = b_m.$$ 

Sets of solutions to this system of equations are called a linear varieties. We usually use the method of Gaussian Elimination to find solutions.

**Example 2.4.** What is the affine variety $V = V(x^2 + y^2 + z^2 + 1)$ when $k = \mathbb{R}$? There are no solutions to this polynomial in $\mathbb{R}$. Therefore, $V = \emptyset$.

Later, we will consider varieties over $\mathbb{C}$ (or, more generally, over any algebraically closed field). This will eventually lead to a significant theorem: Hilbert’s Nullstellensatz.

**Lemma 2.1.** If $V, W \subset k^n$ are affine varieties, then $V \cap W$ and $V \cup W$ are also affine varieties.

**Proof.** Suppose $V = V(f_1, \ldots, f_m), W = V(g_1, \ldots, g_t)$. We claim that:

$$V \cap W = V(f_1, \ldots, f_m, g_1, \ldots, g_t),$$

and

$$V \cup W = V(\{fg_{ij} | 1 \leq i \leq m, 1 \leq j \leq t\}).$$

Indeed, $V(f_1, \ldots, f_m, g_1, \ldots, g_t)$ is the set of solutions to all $f_1, \ldots, f_m, g_1, \ldots, g_t$, which is exactly the set $V \cap W$. The second equality is shown as follows:

$$V \subset V(\{fg_{ij} | 1 \leq i \leq m, 1 \leq j \leq t\})$$

since, if $f_i$’s vanish on $(a_1, \ldots, a_n) \in V$, then $fg_{ij}$ certainly vanish on $(a_1, \ldots, a_n)$. Similar arguments yield

$$W \subset V(\{fg_{ij} | 1 \leq i \leq m, 1 \leq j \leq t\}),$$

and hence

$$V \cup W \subset V(\{fg_{ij} | 1 \leq i \leq m, 1 \leq j \leq t\}).$$

Now assume that,

$$(a_1, \ldots, a_n) \in V(\{fg_{ij} | 1 \leq i \leq m, 1 \leq j \leq t\}).$$

Since there are no zero divisors in $k[x_1, \ldots, x_n]$, we have that either $f_i(a_1, \ldots, a_n) = 0$ or $g_j(a_1, \ldots, a_n) = 0$. Therefore, each

$$(a_1, \ldots, a_n) \in V(\{fg_{ij} | 1 \leq i \leq m, 1 \leq j \leq t\})$$

is either in $V$ or $W$, and is therefore contained in $V \cup W$. 

\[\square\]
Example 2.5. Consider the affine varieties \( V(z) \) and \( V(x,y) \) in \( \mathbb{R}^3 \). The former is the set \( \{(x,y,0)\} \), that is, \( V(z) \) is the \( x,y \) plane. The latter yields \( \{(0,0,z)\} \), that is, \( V(x,y) \) is the \( z \)-axis. Now, their union is \( V(z) \cup V(x,y) \), and as we have show, this is the \( x,y \) plane unioned with the \( z \)-axis. From the previous example, we see that \( V(z) \cup V(x,y) \) produces the same geometric structure as the variety \( V(xy,xz) \) does. From the previous Lemma, we see that \( V(z) \cup V(x,y) \) is the variety \( V(\{z \cdot (x,y)\}) = V(xz,yz) \).

3. Ideals

Recall the definition of an ideal \( I \) of \( k[x_1, \ldots, x_n] \):

Definition 3.1. A non-empty subset \( I \subset k[x_1, \ldots, x_n] \) is an ideal if

1. For all \( f, g \in I \), \( f + g \in I \). And,
2. For all \( f \in I \) and \( r \in k[x_1, \ldots, x_n] \), we have \( r \cdot f \in I \).

Lemma 3.1. Let \( F = f_1, \ldots, f_m \) be a finite set of polynomials in \( k[x_1, \ldots, x_n] \). Let \( F = \{f_1, \ldots, f_m\} \), and define:

\[
(F) := \{ \sum_{i=1}^m g_i f_i \mid g_i \in k[x_1, \ldots, x_n] \}.
\]

Then \( (F) \) is an ideal of \( k[x_1, \ldots, x_n] \) (called the ideal generated by \( f_1, \ldots, f_m \)).

Proof. It’s easy to see that \( 0 \in (F) \) by letting all the \( g_i = 0 \) for \( 1 \leq i \leq m \). Next, by distributivity, if

\[
\sum_i g_i f_i \quad \text{and} \quad \sum_i h_i f_i
\]

are two elements of \( (F) \), then their sum equals

\[
\sum_i (g_i + h_i) f_i,
\]

which is an element of \( (F) \), and hence \( (F) \) is closed under sums. Finally, if \( h \in k[x_1, \ldots, x_n] \), then

\[
h \sum_i g_i f_i = \sum_i (hg_i) f_i \in (F).
\]

Hence, \( (F) \) is an ideal. \( \square \)

The polynomials \( f_1, \ldots, f_m \) are called generators or a basis for the ideal \( (f_1, \ldots, f_m) \).

Example 3.1. Consider \( k[x] \). Let \( f = x \). Consider \( (f) = (x) \). This is the ideal of \( k[x] \) in which no polynomial has a constant term.

Notice also that we may have two ideals that are equal but have different generating sets.

Example 3.2. Consider the ideals \( (x+yz, y+yz, z) \) and \( (x,y,z) \) in \( k[x,y,z] \). It is an exercise to show that

\[
f_1, \ldots, f_m \in I \iff (f_1, \ldots, f_m) \subset I
\]

for any ideal \( I \). Thus, \( (x+yz, y+yz, z) \subset (x,y,z) \) since

\[
\begin{align*}
x + xz &= 1(x) + 0(y) + x(z), \\
y + yz &= 0(x) + 1(y) + y(z), \\
z &= 0(x) + 0(y) + 1(z).
\end{align*}
\]
Then, we will find all such polynomials that vanish from points in $V$ (geometry) and algebra (ideals): Given a variety $I$ (For the sake of simplicity, we will also assume that prime ideals are proper). $I$ is maximal if $I \neq k[x_1, \ldots, x_n]$ and if $I \subset J \subset k[x_1, \ldots, x_n]$ for some other ideal $J$, then either $I = J$ or $J = k[x_1, \ldots, x_n]$.

Definition 3.2. An ideal $I \subset k[x_1, \ldots, x_n]$ is prime if, whenever $ab \in I$, then either $a \in I$ or $b \in I$ (For the sake of simplicity, we will also assume that prime ideals are proper). $I$ is maximal if $I \neq k[x_1, \ldots, x_n]$ and if $I \subset J \subset k[x_1, \ldots, x_n]$ for some other ideal $J$, then either $I = J$ or $J = k[x_1, \ldots, x_n]$.

Example 3.3. In $\mathbb{R}[x, y]$, the ideal $(xy)$ is not prime. Indeed, $xy \in (xy)$ but neither $x$ nor $y$ is in $(xy)$.

Lemma 3.2. Every maximal ideal $I$ is prime.

Proof. Assume $I$ is maximal and some product $xy \in I$. If $x$ or $y$ are not in $I$, then form $I' = (I, x)$. This is an ideal that properly contains $I$. But $I$ is maximal, a contradiction.

Lemma 3.3. Let $I$ and $J$ be ideals in $k[x_1, \ldots, x_n]$. The following are ideals:

1. $I + J = \{ f + g \mid f \in I, g \in J \}$.
2. $I \cap J$.
3. $IJ = \{ \sum_{finite} f \cdot g \mid f \in I, g \in J \}$.
4. $(I : J) = \{ f \in k[x_1, \ldots, x_n] \mid f \cdot g \in I \text{ for all } g \in J \}$ (this is called the ideal quotient of $I$ by $J$).

Proof. Exercise.

The notion of ideal raises many questions, the first that comes to mind is whether or not, given any ideal $I$ of $k[x_1, \ldots, x_n]$, does there exist a finite basis, and if there does exist a finite basis, is there a “best” choice for basis. These two questions will be answered when we discuss the Hilbert Basissatz and Gröbner bases.

Armed with the notion of ideal, we can begin making certain correspondences between varieties (geometry) and algebra (ideals): Given a variety $V$, we can ask the question, “What are all the polynomials that vanish on $V$?” Given

$$V = V(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in k^n \mid f_1(a_1, \ldots, a_n) = \ldots = f_m(a_1, \ldots, a_n) = 0\},$$

we will find all such polynomials that vanish from points in $V$. Firstly, the zero polynomial vanishes on all points in $V$. Secondly, if $g, f$ both vanish on $V$, then $g + f$ also vanishes on $V$. Indeed,

$$(g + f)(a_1, \ldots, a_n) = g(a_1, \ldots, a_n) + f(a_1, \ldots, a_n) = 0 + 0 = 0.$$ 

Finally, if $g$ vanishes on $V$ and $h \in k[x_1, \ldots, x_n]$, then $hg$ also vanishes on $V$. This proves:

Lemma 3.4. Let $V = V(f_1, \ldots, f_m)$ and define

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

Then, $I(V)$ is an ideal of $k[x_1, \ldots, x_n]$.

We should note that given $V = V(f_1, \ldots, f_m)$, if we want to consider $I(V)$, it is not generally true that $I(V) = (f_1, \ldots, f_m)$. It is true that $(f_1, \ldots, f_m) \subset I(V)$ (exercise). However, there may be instances where $I(V) \not\subset (f_1, \ldots, f_m)$. Indeed, consider the ring $\mathbb{R}[x]$ and the variety $V = V(x^2) = \{0\} \subset \mathbb{R}$. Now, $I(V)$ is the set of all polynomials that vanish at $\{0\}$. It is easy to see the set of polynomials that vanish at $\{0\}$ is the ideal $(x)$. However, $(x) \neq (x^2)$ but we see that
The correspondences between ideals and varieties will be further examined when we broach the topic of Hilbert’s Nullstellensatz. However, there are a few correspondences that we can make presently:

**Lemma 3.5.** The correspondence between varieties and ideals of varieties is inclusion-reversing. Specifically, $V \subset W \iff \mathcal{I}(W) \subset \mathcal{I}(V)$.

**Proof.** If $V \subset W$, then all polynomials that vanish at $W$ also vanish at $V$, hence $\mathcal{I}(W) \subset \mathcal{I}(V)$. If $\mathcal{I}(W) \subset \mathcal{I}(V)$, then the set of points in $V$ that annihilate polynomials in $\mathcal{I}(V)$ also annihilate those in $\mathcal{I}(W)$, and hence those points are also in $W$, thus $V \subset W$. □

**Corollary 3.1.** $W = V \iff \mathcal{I}(V) = \mathcal{I}(W)$.

### 4. Monomial Ideals and The Hilbert Basis Theorem

We move off the topic of affine varieties briefly and turn our attention to ideals.

**Definition 4.1.** Let $R$ be a commutative ring with unit. $R$ is **Noetherian** (named after German Mathematician Emmy Noether [1882-1935]) if one of the following two equivalent conditions hold:

1. Every ideal $I \in R$ is finitely generated.
2. The ascending chain condition on ideals is satisfied; that is, for every infinite, strictly ascending chain of ideals

   $$I_0 \subset I_1 \subset \ldots \subset I_K \subset \ldots,$$

   there exists some $N$ such that for all $j > N$ we have

   $$I_N = I_{N+1} = \ldots$$

We say that such chains stabilize.

To see that these two conditions are equivalent, assume that each ideal is finitely generated, and let $I_0 \subset I_1 \subset \ldots$ be a strictly ascending chain of ideals. Then,

$$\bigcup_{i=1}^{\infty} I_i$$

is an ideal. Clearly $0 \in \bigcup_i I_i$. Now, let $a, b \in \bigcup_i I_i$. There is some $I_m$ in which $a, b \in I_m$, and therefore $a + b \in I_m$, hence $a + b \in \bigcup_i I_i$. Lastly, for any $r \in R$ and $a \in \bigcup_i I_i$, then there is some $I_M$ such that $ra \in I_M$, and therefore $ra \in \bigcup_i I_i$. Since, by assumption, all ideals are finitely generated, that means that $\bigcup_i I_i = (a_1, \ldots, a_n)$ for some generators $a_1, \ldots, a_n$. Since $n$ is a finite index number, there must exist some $I_p$ in which all generators $a_1, \ldots, a_n$ lie, which means for any $P > p$ we have $I_p = I_P$, and the chain stabilizes. Now assume that some $I$ is not finitely generated. Then, there exists a sequence of elements $x_1, x_2, \ldots \in I$ such that the strictly increasing infinite chain

$$(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \ldots$$

will not stabilize. By contrapositive, we are done.
Example 4.1. The ring \( \mathbb{Z} \) is Noetherian. Indeed, one can show that the only ideals of \( \mathbb{Z} \) are the subsets of the form \( n\mathbb{Z} \), and these ideals are exactly \( (n) \). Ideals that are generated by just one element are called \textit{principal ideals}. In a basic algebra course, one should have learned that \( \mathbb{Z} \) is a \textit{principal ideal domain}, that is, every ideal is generated by just one element. Thus, principal ideal domains are Noetherian.

Example 4.2. Any field \( k \) is Noetherian. Indeed, the only ideal \( \neq k \) is \( (0) \) which is finitely generated. Since every non-zero element in a field has an inverse, any non-zero ideal would contain 1 and would therefore be the entire field.

We know from previous algebra courses that the ring \( k[x_1] \) where \( k \) is a field is Noetherian (in fact, it is a principal ideal domain). Now consider \( k[x_1,x_2] \). Such a ring is comparable (meaning, the two structures are the same) to \( k[x_1][x_2] \), that is, the ring \( k[x_1] \) with indeterminate \( x_2 \). We ask, “Is the Noetherian property preserved if we add indeterminates?” The answer is yes. This is the \textit{Hilbert Basissatz} (typically in German, they combine words. Here, “Basis” means basis, and “satz” means theorem):

\textbf{Theorem} (The Hilbert Basissatz). The ring \( k[x_1,\ldots,x_n] \) is Noetherian.

The proof for the Basissatz will be given at a later time. Note that the ring \( k[x_1,x_2,\ldots] \), i.e., the polynomial ring over \( k \) with infinite indeterminates, is \textit{not} Noetherian. Consider the strictly increasing infinite chain of ideals 
\[
(x_1) \subset (x_1,x_2) \subset \ldots \subset (x_1,\ldots,x_r) \subset \ldots
\]
This is an infinite ascending chain that does not stabilize.

One tool that we will use to prove the Basissatz is monomial ideals. We will use the following notation for monomials:
\[
x^{\alpha} = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}
\]
where \( \alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{Z}_{\geq 0}^n \). For example, in the ring \( \mathbb{R}[x_1,x_2,x_3] \), the monomial \( x_1^2x_2^3x_3^7 \) will be written as \( x^{(2,3,7)} \), and the monomial \( x_1x_3^3 \) will be written \( x^{(1,0,3)} \).

\textbf{Definition 4.2.} An ideal \( I \subset k[x_1,\ldots,x_n] \) is a \textit{monomial ideal} if there is a subset \( A \subset \mathbb{Z}_{\geq 0}^n \) (possibly infinite) such that \( I \) is of the form 
\[
(x^{\alpha} | \alpha \in A).
\]
In other words, a monomial ideal is an ideal generated by monomials.

We now state and prove a theorem similar to that of the Hilbert Basissatz, and this will be of use in proving the Hilbert Basissatz:

\textbf{Lemma 4.1} (Dickson’s Lemma). Every monomial ideal in \( k[x_1,\ldots,x_n] \) is finitely generated.

We need some elementary properties of monomial ideals to prove this.

\textbf{Proposition 4.1.} If \( M \) and \( N \) are monomial ideals, then \( M + N \) and \( MN \) are monomial ideals.

\textbf{Proof.} Exercise. Use the fact that
\[
M + N = \{m_i + n_j | m_i \in M, n_j \in N \}
\]
and
\[
MN = \{ \sum_{\text{finite}} m_in_j | m_i \in M, n_j \in N \}
\]
and try to show that
\[ M + N = (m_i, n_j \mid m_i \in M, n_j \in N) \]
and
\[ MN = (m_i n_j). \]

**Proposition 4.2.** If \( M \subseteq \{ M_s \mid s \in S \} \) is a collection of monomial ideals totally ordered by inclusion, then
\[ \bigcup_s M_s \]
is a monomial ideal and is an upper bound for \( M \).

**Proof.** A version of this proposition was proved after Definition 4.1. The details showing that \( \bigcup_s M_s \) remains a monomial ideal will be left as an exercise. □

**Proposition 4.3.** \( M \) is a monomial prime ideal \( \iff \) \( M = (S) \) for some subset \( S \subseteq \{ x_1, \ldots, x_n \} \). In particular, there are only finitely many monomial prime ideals and each are finitely generated.

**Proof.** Assume that \( M \) is a monomial prime ideal. Then, any product \( ab \in M \) implies that \( a \in M \) or \( b \in M \). Since each generator is of the form \( x^\alpha \), this means that the product \( x^\alpha \in M \), which means one of the factors is in \( M \). If this factor is not linear, then we again have a product \( x_j x_i \), and since \( M \) is (still) a prime ideal, we have that \( x_j \in M \) for some \( x_j \in \{ x_1, \ldots, x_n \} \). Since each generator has at least one \( x_j \in M \), we know that \( M \) is generated by some subset of \( \{ x_1, \ldots, x_n \} \). Now assume that \( M = (S) \). Any product in \( M \) will have a factor among \( x_1, \ldots, x_n \) by definition, and is therefore a prime ideal. Since there are only finite \( x_1, \ldots, x_n \), we have that every monomial prime ideal is finitely generated. □

**Corollary 4.1.** \( M = (x_1, \ldots, x_n) \) is the only maximal monomial ideal.

**Proof.** We know that every maximal ideal is prime. By the above, there is only a finite number of monomial prime ideals, with the largest being \( (x_1, \ldots, x_n) \). □

Finally, the last proposition we need for Dickson’s Lemma:

**Proposition 4.4.** Let \( M \) be a monomial ideal. For any monomial \( x^\alpha \in k[x_1, \ldots, x_n] \), the colon ideal
\[ (M : (x^\alpha)) = \left( \frac{m_i}{d_i} \mid i \in I \right) \]
for some index set \( I \), where \( d_i \) is the greatest common divisor of \( m_i \in M \) and \( x^\alpha \). In particular, \( (M : (x^\alpha)) \) is a monomial ideal.

**Proof.** Recall that \( (M : (x^\alpha)) = \{ f \in k[x_1, \ldots, x_n] \mid fg \in M \text{ for all } g \in (x^\alpha) \} \). Therefore, we have:
\[ (M : (x^\alpha)) = \{ f \in k[x_1, \ldots, x_n] \mid fx^\alpha \in M \} \]
\[ = \{ f \in k[x_1, \ldots, x_n] \mid fx^\alpha = \sum_i g_i m_i, m_i \in M \} \]
\[ = \{ f \in k[x_1, \ldots, x_n] \mid fx^\alpha d_i = \sum_i g_i m_i \} \]
\[ = \{ fx^\beta d_i \in k[x_1, \ldots, x_n] \mid \frac{g_i m_i}{d_i} \} = \left( \frac{m_i}{d_i} \right). \]
In the above, \(d_i\) is the greatest common divisor of \(x^\alpha\) and the \(m_i\) and \(\beta \in \mathbb{Z}_{\geq 0}\). It is clear that this is a monomial ideal.

**Proof of Dickson’s Lemma.** First we outline the proof. We begin with a set

\[ S = \{ N \mid N \text{ is a monomial ideal that is not finitely generated} \} \]

and assume that \(S \neq \emptyset\). We then show that \(S\) has a maximal element \(M\). Next, we show that \(M\) is not prime and use it to show that for some monomial \(x^\alpha\) we have that \(M + (x^\alpha) = M_0 + (x^\alpha)\) for a finitely generated \(M_0\). Then, we deduce that \(S\) is indeed empty.

In order to show that \(S\) has a maximal element, we use Proposition 4.2 and Zorn’s Lemma. Recall that Zorn’s Lemma states:

**Lemma 4.2.** Suppose a non-empty partially ordered set \(P\) has the property that every non-empty increasing chain has an upper bound in \(P\). Then the set \(P\) contains at least one maximal element.

Recall that an upper bound on a chain in a partially ordered set \(S\) is an element in \(S\) that is greater than or equal to every element in the chain.

\(S\) is partially ordered by inclusion, and by Proposition 4.2 each chain contains an upper bound. Hence, \(S\) has a maximal element \(M\). \(M\) is not prime by Proposition 4.3. Indeed, \(M\) can only be prime if its generated by some subset of \(\{x_1, \ldots, x_n\}\). Since \(M \in S\), \(M\) is, in particular, not finitely generated, and is therefore not a prime ideal. This means that (without loss of generality) there exists some product \(x_ix_j \in M\) with both \(x_i, x_j \notin M\) for \(1 \leq i, j \leq n\).

Now, since \(M\) is a maximal element in the set \(S\), the ideal \(M + (x_i)\) is a monomial ideal (by Proposition 4.1) that is finitely generated, say with generators \(f_1, \ldots, f_s\). By Proposition 4.1, we have that, for some \(r < s\),

\[ M + (x_i) = (f_1, \ldots, f_r) + (f_{r+1}, \ldots, f_s) = M_0 + (x_i) \]

for some finitely generated \(M_0 = (f_1, \ldots, f_r)\) (note that by this arrangement, \(M_0 \subset M\)). Next, we claim that

\[ M = M_0 + (x_i)(M : (x_i)) \]

where \((M : (x_i))\) is the ideal quotient of \(M\) by \((x_i)\) and \((M : (x_i))\) is the product ideal of \((x_i)\) and \((M : (x_i))\). First we show that

\[ (x_i)(M : (x_i)) \subset M \]

We showed in Proposition 4.4 that \((M : (x_i)) = \left(\frac{d_i}{d_i}\right)\) where \(d_i\) is the greatest common divisor of \(m_i \in M\) and \(x_i\). Thus,

\[ (x_i)(M : (x_i)) = (x_i)\left(\frac{m_i}{d_i}\right) = \{ \sum_{f \text{ finite}} h_i x_i \cdot g_i \frac{m_i}{d_i} \} \]

and since \(x_i \cdot \frac{m_i}{d_i} = m_i \cdot \frac{x_i}{d_i} = m_i f_i\) for some \(f_i \in k[x_1, \ldots, x_n]\), we have

\[ (x_i)(M : (x_i)) \subset M \]

and since \(M_0 \subset M\), we have

\[ M_0 + (x_i)(M : (x_i)) \subset M \]

To show that \(M \subset M_0 + (x_i)(M : (x_i))\), note that for any \(p \in M\), we have that

\[ p + x_i \in M + (x_i) = M_0 + (x_i) \]

Hence, for some \(f \in k[x_1, \ldots, x_n]\) and some \(q \in M_0\), we have that

\[ M + (x_i) \ni p + x_i = q + f x_i \in M_0 + (x_i) \]

Thus, \(M_0 + (x_i)(M : (x_i)) \subset M\) and \(M \subset M_0 + (x_i)(M : (x_i))\), proving that \(M\) is a monomial ideal.

□
Hence, \( M \ni p - q = (f - 1)x_i \). Thus, \( f - 1 \in (M : (x_i)) \), and we have that
\[
M \ni p = q + (f - 1)x_i \in M_0 + (x_i)(M : (x_i)).
\]
Hence, \( M = M_0 + (x_i)(M : (x_i)) \).

Note that the ideal quotient \((M : (x_i))\) properly contains \( M \). Indeed, by assumption, \( x_j \notin M \) but \( x_j \in (M : (x_i)) \). Thus, \((M : (x_i))\) is a monomial ideal properly containing \( M \), and is therefore finitely generated. Since the right hand side of \( M = M_0 + (x_i)(M : (x_i)) \) is finitely generated, we must have that \( M \) be finitely generated. Hence, \( S \) is indeed empty, and therefore, every monomial ideal is finitely generated.

We want to somehow use the fact that monomial ideals are finitely generated to show that every ideal in \( k[x_1, \ldots, x_n] \) is finitely generated. One tool we will use is the fact that there is a division algorithm for multi-variate polynomials. However, we first need to introduce some way to order the polynomials in order to divide.

5. ORDERINGS AND THE DIVISION ALGORITHM IN \( k[x_1, \ldots, x_n] \)

Notice that for single-variable polynomials, when we divide \( f(x) \) by \( g(x) \), we first order the monomials in \( f(x) \) and \( g(x) \) by degree; we list the monomial with the largest degree first and continue in a descending order. When we introduce multiple variables, this process may not be the best way to proceed.

Example 5.1. Consider \( K = \mathbb{R}[x,y] \). Each of the following has the same degree: \( x^2y^2, xy^3, x^3y, x^4, y^4 \). The question is which one is the biggest? For that, we need a notion of ordering.

Definition 5.1. A total ordering on the set \( \mathbb{Z}_{\geq 0}^n \) is an ordering on \( \mathbb{Z}_{\geq 0}^n \) such that one and only one of the following three must hold for any \( \alpha = (\alpha_1, \ldots, \alpha_n) \) and \( \beta = (\beta_1, \ldots, \beta_n) \):

1. \( \alpha = \beta \),
2. \( \alpha > \beta \), or
3. \( \beta > \alpha \).

Example 5.2. “\( \leq \)” is a total ordering on \( \mathbb{Z}_{\geq 0}^n \).

Definition 5.2. A monomial ordering is a well ordering \( \prec \) on \( \mathbb{Z}_{\geq 0}^n \) such that

1. \( \prec \) is a total ordering, and
2. \( \alpha + \gamma \prec \beta + \gamma \) whenever \( \alpha \prec \beta \).
3. \( \prec \) is a well ordering on \( \mathbb{Z}_{\geq 0}^n \).

Equivalently, \( \prec \) is a monomial ordering if it is a well ordering such that \( mm_1 \prec mm_2 \) whenever \( m_1 \prec m_2 \) for monomials \( m_1, m_2 \), and \( m \).

Recall that a set is said to be well-ordered if every non-empty subset has a smallest element. Given any monomial ordering, one can show that \( 1 \prec m \) for every monomial \( m \) (exercise). We can also show that, given this definition there is only one way to have a monomial ordering in the univariate case:

Example 5.3. Let \( K = \mathbb{R}[x] \). We know that \( 1 \prec x \) from what we just said. So, given that \( 1 \prec m \), we have that \( x \cdot 1 \prec x \cdot x \), and hence, \( x \prec x^2 \). So, we have that the only ordering in the univariate case is a total order on the degrees of each monomial.

We will now introduce three types of monomial orderings which will be used most frequently in this course:
The lexicographic order \( (\prec_{\text{lex}}) \) is probably the first that leaps to mind; this is a dictionary-type order (hence the name “lexicographic”). In the English language, we alphabetize (“order”) different words based on how we read the word from left to right. So, we have

\[ a \succ_{\text{lex}} b \succ_{\text{lex}} \cdots \succ_{\text{lex}} z. \]

In this ordering, the word “balaclava” goes before “chair” since \( b \succ_{\text{lex}} c \), and “polynomial” comes before “product” since \( p =_{\text{lex}} p \) but \( o \succ_{\text{lex}} r \). In \( k[x_1, \ldots, x_n] \), the lexicographic order reads from left to right:

\[ x_1 \succ_{\text{lex}} x_2 \succ_{\text{lex}} \cdots \succ_{\text{lex}} x_n, \]

and given monomials \( ax^\alpha \) and \( bx^\beta \), we have that \( ax^\alpha \succ_{\text{lex}} bx^\beta \) (for constants \( a, b \)) if, when we compare the coordinates of \( \alpha \) and \( \beta \) from left to right, we have that the first coordinates where the \( n \)-tuples differ have \( a_i > b_i \in \mathbb{Z}_{\geq 0} \).

**Example 5.4.** In the lexicographic ordering in \( k[x_1, \ldots, x_5] \), we have that \( x_1^2 x_2 x_3 x_4 x_5 \succ_{\text{lex}} x_1^2 x_2 x_3 x_4 x_5 \). Another way to view it is to consider the elements \( \alpha = (1, 9, 8, 7, 6) \) and \( \beta = (2, 0, 0, 0, 0) \) in \( \mathbb{Z}_{\geq 0}^5 \). In the lexicographic ordering, we compare the first coordinate of each 5-tuple, and since \( 2 > 1 \), we have that \( \alpha <_{\text{lex}} \beta \).

In the same ring, consider the two monomials

\[ x^{(1,1,1,1,2)} = x_1 x_2 x_3 x_4 x_5^2 \]

and

\[ x^{(1,1,1,1,1)} = x_1 x_2 x_3 x_4 x_5. \]

By our \( \text{lex} \) ordering, we compare the first coordinates in the tuples \( (1, 1, 1, 1, 2) \) and \( (1, 1, 1, 1, 1) \). Since they are the same, we continue to the next one on the immediate right (the second coordinate). They are also the same. We continue down this way until we approach an anomaly; the last coordinates are different. Since \( 2 > 1 \), we have that \( x^{(1,1,1,1,2)} \succ_{\text{lex}} x^{(1,1,1,1,1)} \).

Of course, we need to check that the lexicographic order indeed qualifies as a monomial ordering:

**Proposition 5.1.** The lexicographic ordering as given above is a monomial ordering.

**Proof.** It is clear that this set is totally ordered by some order “\(<\)”. We first claim that a totally ordered set is well-ordered in \( \mathbb{Z}_{\geq 0}^n \) if and only if every decreasing chain of inequalities terminates in \( \mathbb{Z}_{\geq 0}^n \). Assume that \(<\) is not well-ordered. Then there is some subset \( S \) of \( \mathbb{Z}_{\geq 0}^n \) that does not have a smallest element. That means, starting with any element \( a \in S \), there exists \( b \in S \) such that \( b < a \). However, since there is no smallest element in \( S \), there exists an element \( c \in S \) such that \( c < b \). Continuing in this way we get an infinitely decreasing sequence

\[ a > b > c > \cdots \]

Conversely, let

\[ a > b > c > \cdots \]

be an infinite decreasing sequence. That means there is no smallest element, so \(<\) is not a well-ordering, thus proving our claim.
Now, to show that \( \prec_{\text{lex}} \) is a monomial order, we need to check the three properties of a monomial order. It is clear from the definition that \( \prec_{\text{lex}} \) is a total order.

Next, if \( x^\alpha \prec_{\text{lex}} x^\beta \), then comparing coordinates of the \( n \)-tuples from left to right, the first coordinates that differ have \( \alpha_i < \beta_i \) in \( \mathbb{Z}_{\geq 0} \). Now if we multiply \( x^\alpha \) and \( x^\beta \) by \( x^\gamma \), we have
\[
x^\alpha \cdot x^\gamma = x^{\alpha + \gamma} \quad \text{and} \quad x^\beta \cdot x^\gamma = x^{\beta + \gamma}.
\]

Now, when we compare \( x^{\alpha + \gamma} \) and \( x^{\beta + \gamma} \), we see that the first coordinate that differs is \( \alpha_i + \gamma_i \) and \( \beta_i + \gamma_i \). Since we have \( \alpha_i < \beta_i \), we see that \( \alpha_i + \gamma_i < \beta_i + \gamma_i \) in \( \mathbb{Z}_{\geq 0} \). Hence, \( x^{\alpha + \gamma} \prec_{\text{lex}} x^{\beta + \gamma} \).

Finally, we show that the lexicographic ordering is a well-ordering. If it was not a well ordering, starting with some \( x^{\alpha_1} \), we can form a chain
\[
x^{\alpha_1} > x^{\alpha_2} > \ldots
\]
that does not stabilize. We know that the set \( \mathbb{Z}_{\geq 0} \) is well ordered, so if we consider the left-most coordinates in the chain above, the left-most coordinates of this chain form a nonincreasing subchain, which we know must stabilize at some \( x^{\alpha_k} \) (by virtue of the fact that \( \mathbb{Z}_{\geq 0} \) is well ordered). Now starting with \( x^{\alpha_{k+1}} \), the second coordinate would then form a non-increasing subchain in \( \mathbb{Z}_{\geq 0} \). This chain will stabilize as well. Continue this process throughout all the coordinates in each \( \alpha_i \), and since there are only a finite number of coordinates, we have that the decreasing chain
\[
x^{\alpha_1} > x^{\alpha_2} > \ldots
\]
will in fact eventually stabilize, so \( \text{lex} \) is a well ordering, and thus a monomial ordering. \( \square \)

(Graded Lex Order) The next type of order uses the notion of the total value of the degree of a monomial; it is called the graded lexicographic order (\( \text{grlex} \)), and it is defined as thus. Given two monomials \( x^\alpha \) and \( x^\beta \) with \( \alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \), we say that
\[
x^\alpha \succ_{\text{grlex}} x^\beta
\]
if \( \sum_i \alpha_i > \sum_i \beta_i \), \( 1 \leq i \leq n \), else if \( \sum_i \alpha_i = \sum_i \beta_i \) then \( x^\alpha \succ_{\text{lex}} x^\beta \). What this says is that we first compute the total degree of each of monomial and whichever is larger is the bigger monomial. If the total degrees are equal, then we revert to the lexicographic order.

**Example 5.5.** Consider the ring \( k[x_1, \ldots, x_5] \), and take two monomials \( x^{(1,2,3,4,5)} \) and \( x^{(1,2,3,2,1)} \). Since \( 1 + 2 + 3 + 4 + 5 = 15 > 9 = 1 + 2 + 3 + 2 + 1 \), we have that
\[
x^{(1,2,3,4,5)} \succ_{\text{grlex}} x^{(1,2,3,2,1)}.
\]

If instead we had the two monomials \( x^{(1,2,3,4,5)} \) and \( x^{(5,4,3,2,1)} \), since \( 1 + 2 + 3 + 4 + 5 = 5 + 4 + 3 + 2 + 1 \), we compare them using the lexicographic order. Since \( x^{(5,4,3,2,1)} \succ_{\text{lex}} x^{(1,2,3,4,5)} \), we have that
\[
x^{(5,4,3,2,1)} \succ_{\text{grlex}} x^{(1,2,3,4,5)}.
\]

(Grd Rev Lex Order) The final ordering that we will discuss is the graded reverse lexicographic order (\( \text{grevlex} \)). Given two monomials \( x^\alpha \) and \( x^\beta \) (again, we assume \( \alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \)), we say that
\[
x^\alpha \succ_{\text{grevlex}} x^\beta
\]
if $\sum \alpha_i > \sum \beta_i$, else if $\sum \alpha_i = \sum \beta_i$ then we compare $\alpha_n$ and $\beta_n$, and whichever has the smaller right-most coordinate will be considered to be larger in grevlex order. In other words, just as in the graded lexicographic order, we first compare the degrees. If the degrees are equal, then we compare the rightmost coordinates. Whichever is smaller will be considered to have a greater grevlex order.

**Example 5.6.** As above, take $k[x_1, \ldots, x_n]$, and consider the monomials $x^{(1,2,3,4,5)}$ and $x^{(5,4,3,2,1)}$. We have $x^{(1,2,3,4,5)} \prec_{\text{grevlex}} x^{(5,4,3,2,1)}$.

since the degrees are equal, but the since $5 > 1$, we have that “1 $\succ_{\text{grevlex}} 5$”.

**Proposition 5.2.** **The graded lexicographic order and graded reverse lexicographic order are monomial orderings.**

**Proof.** Exercise. □

With these orderings on monomials, we can now define some terms that we will use often:

**Definition 5.3.** Let $k[x_1, \ldots, x_n]$ be a ring, $f$ a polynomial in $k[x_1, \ldots, x_n]$. Fix a monomial ordering $\prec$.

1. The **multidegree** of $f$, denoted $m(f)$ is $m(f) = \max(\alpha)$

   where $\alpha$ is taken over all monomials in $f$, and the max is taken with respect to $\prec$.

2. The **leading monomial** of $f$, denoted $\text{LM}(f)$, is the monomial $x^\alpha$ where $\alpha = m(f)$.

3. The **leading coefficient**, denoted $\text{LC}(f)$, of $f$ is the coefficient of $\text{LM}(f)$.

4. The **leading term** of $f$, denoted $\text{LT}(f)$, is $\text{LC}(f) \cdot \text{LM}(f)$.

**Proposition 5.3.** $\text{LT}(fg) = \text{LT}(f) \cdot \text{LT}(g)$ for all $f, g \in k[x_1, \ldots, x_n]$.

**Proof.** Exercise. □

We prove one fact about monomial ideals that will be useful later on:

**Lemma 5.1.** Let $I = (x^\alpha | \alpha \in A \subset \mathbb{Z}_{\geq 0}^n)$. A monomial $x^\beta \in I$ if and only if $x^\beta$ is divisible by $x^\alpha$ for some $\alpha \in A$.

**Proof.** If $x^\beta$ is a multiple of some $x^\alpha \in I$, then $x^\beta \in I$ by definition. Now assume that $x^\beta \in I$. That means $x^\beta = \sum_i f_i x^\alpha_i$. If we expand the RHS of the equation, we see that there is some $x^\alpha$ that divides the RHS, and hence divides $x^\beta$. □

In the univariate case, the division algorithm is helpful in determining whether or not a polynomial $g$ is in an ideal $(f)$ for some polynomial $f \in k[x]$. What we do is divide $g$ by $f$, and if there is no remainder, then we have the $g = h f \Rightarrow g \in (f)$. Now we question: is there a similar division algorithm in $k[x_1, \ldots, x_n]$? With this algorithm, we have one method of determining whether, given a finitely generated ideal $(f_1, \ldots, f_m)$ of polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$, $f \in (f_1, \ldots, f_m)$ for some arbitrary polynomial $f \in k[x_1, \ldots, x_n]$.

**Theorem (The Division Algorithm for $k[x_1, \ldots, x_n]$).** Let $k[x_1, \ldots, x_n]$ be a polynomial ring over a field $k$ and fix a monomial order $\prec$. Let $f_1, \ldots, f_m$ be an ordered set of polynomials in $k[x_1, \ldots, x_n]$. Every $f \in k[x_1, \ldots, x_n]$ can be written as

$$f = g_1 f_1 + g_2 f_2 + \ldots + g_m f_m + r,$$
where \( g_i, r \in k[x_1, \ldots, x_n] \) (1 \( \leq i \leq m \)), and \( r = 0 \) or \( r \) is not divisible by \( LT(f_1), \ldots, LT(f_m) \), and we call \( r \) the remainder.

We will show this by exhibiting a division algorithm for \( k[x_1, \ldots, x_n] \). Starting with a polynomial \( f \), we start with the following:

\[
f = g_1 f_1 + \ldots + g_m f_m + p + r,
\]

where \( g_1 = \ldots = g_m = 0 \), \( p = f \) and \( r = 0 \). Now, since \( f_1, \ldots, f_m \) is ordered, the first \( f_i \) such that \( LT(f_i)|LT(p) \), and we write \( g_i := g_i + \frac{LT(p)}{LT(f_i)} \) and \( p := p - \frac{LT(p)}{LT(f_i)} f_i \), so we get after one iteration:

\[
f = (g_i + \frac{LT(p)}{LT(f_i)}) f_i + (p - \frac{LT(p)}{LT(f_i)}) f_i + r
\]

where \( r = 0 \). If it is the case that no such \( f_i \) has the property that \( LT(f_i)|LT(p) \), then \( r := r + LT(p) \) and \( p := p - LT(p) \), and after one iteration we write:

\[
f = (p - LT(p)) + (r + LT(p)).
\]

Then we repeat as necessary until \( p = 0 \), thus getting \( f = g_1 f_1 + \ldots + g_m f_m + r \). In other words, at each step, we check two things. First, if there is an \( f_i \) such that \( LT(f_i)|LT(p) \), then we proceed as we would with the univariate division algorithm. If no such \( f_i \) exists, then we take \( LT(p) \) and add it to the remainder, then proceed with the division algorithm to the polynomial \( p - LT(p) \). It is an exercise to show that \( p \) eventually becomes zero (in other words, the algorithm terminates after a finite number of steps).

**Corollary 5.1.** If \( g_i f_i \neq 0 \), then we have \( m(f) \geq m(g_i f_i) \).

**Example 5.7.** Consider the ring \( \mathbb{R}[x,y] \) with the \( \prec_{\text{lex}} \) ordering. Let \( f = x^3 y^2 + xy^5 + 2 \) and divide it by the ordered polynomials \( f_1 = x^2 y + x, f_2 = xy^2 + y \). Start with the equation

\[
f = g_1 f_1 + g_2 f_2 + p + r,
\]

where \( g_1 = g_2 = r = 0 \) and \( p = f \). Now, \( LT(f_1)|LT(f) \), so, keeping track of \( g_1 \) and \( g_2 \):

\[
g_1 = xy, g_2 = 0,
\]

and we get:

\[
f = xy(x^2 y + x) + 0(xy^2 + y) + (-x^2 y + xy^5 + 2) + 0.
\]

Now, we repeat the steps on the new polynomial \( p := -x^2 y + xy^5 + 2 \). We see that \( LT(f_1)|LT(f) \), and we get that this quotient equals -1, so we add -1 to \( g_1 \) and we get \( g_1 = xy - 1, g_2 = 0, r = 0 \) and we have the new polynomial:

\[
f = (xy - 1)(x^2 y + x) + 0(xy^2 + y) + (xy^5 + x + 2) + 0.
\]

Repeat the steps on the new polynomial \( p := xy^5 + x + 2 \). We see that \( LT(f_1) \nmid LT(p) \), but we have \( LT(f_2)|LT(f) \), and the quotient \( \frac{LT(f_2)}{LT(f)} = y^3 \), so we add \( y^3 \) to \( g_2 \) to get \( g_1 = xy - 1, g_2 = y^3, r = 0 \), and we get the new polynomial:

\[
f = (xy - 1)(x^2 y + x) + y^3(xy^2 + y) + (x - y^4 + 2) + 0.
\]

Since neither of the leading terms in \( f_1 \) or \( f_2 \) divide the leading term of \( p := x - y^4 + 2 \), we add \( LT(p) \) to \( r \), and we get \( g_1 = xy - 1, g_2 = y^3, r = x \), and we get a new polynomial:

\[
f = (xy - 1)(x^2 y + x) + y^3(xy^2 + y) + (-y^4 + 2) + (x).
\]
Repeat the steps on the new \( p := -y^4 + 2 \), and since neither term is divisible by \( LT(f_1) \) or \( LT(f_2) \), we add the terms in \( p \) to \( r \) and we get the desired equation:

\[
f = (xy - 1)(x^2y + x) + (y^3)(xy^2 + y) + (x - y^4 + 2).
\]

There are a couple things to notice. Firstly, the monomial order is important since it actually determines what is the leading term in each polynomial. Secondly, the order in which we divide the polynomials \( f_1 \) and \( f_2 \) matters. Indeed, if we instead ordered the polynomials in the order \( f_2, f_1 \) and perform the division algorithm, we would instead get the equation:

\[
f = (x^2 + y^3)(xy^2 + y) + (-1)(x^2y + x) + (x - y^4 + 2).
\]

It will be one of the homework exercises to show that when we change the order of polynomials, there is a relationship between the remainders.

**Proposition 5.4.** Let \( k[x_1, \ldots, x_n] \) be a ring, and let \( (f_1, \ldots, f_m) \) be a finitely generated ideal. A polynomial \( f \in k[x_1, \ldots, x_n] \) is in the ideal \( (f_1, \ldots, f_m) \) if the remainder after division by \( f_1, \ldots, f_m \) is zero.

**Proof.** If \( f = g_1f_1 + \ldots + g_mf_m + r \) where \( r = 0 \), then that means we can express \( f \) as a linear combination of polynomials \( f_1, \ldots, f_m \), which means, by definition, \( f \in (f_1, \ldots, f_m) \). \( \square \)

The above proof proposition that to show that a polynomial \( f \in (f_1, \ldots, f_m) \), it is sufficient to show that the remainder of \( f \) after division by \( f_1, \ldots, f_m \) is equal to zero. However, the next example will show that it is not necessary for the remainder to be zero to show that \( f \) is in some ideal.

**Example 5.8.** Consider the ideal \( (f_1, f_2) \subset \mathbb{R}[x, y] \) where \( f_1 = x^2y + 1 \) and \( f_2 = xy^2 \). We will show that the polynomial \( f = y \in (f_1, f_2) \). Indeed,

\[
y = y \cdot (x^2y + 1) + (-x) \cdot (xy^2).
\]

When we divide \( f \) by \( f_1, f_2 \), we get a remainder of \( r = y \neq 0 \).

This example makes us ponder whether or not there are any conditions on ideals that would make \( r = 0 \) a sufficient AND necessary condition for ideal membership. This will be answered when we discuss Gröbner Basis.

### 6. Gröbner Bases

Knowing the Division Algorithm, we can start analyzing polynomials and ideals in more detail. Dickson’s lemma guarantees us that any monomial ideal in \( k[x_1, \ldots, x_n] \) is finitely generated. So, given any ideal \( I \subset k[x_1, \ldots, x_n] \), we can make the following definition:

**Definition 6.1.** For any ideal \( I \subset k[x_1, \ldots, x_n] \), define

\[
LT(I) = \{ LT(f) | f \in I \},
\]

called the ideal of leading terms.

First thing to note is that, due to Dickson’s Lemma, we know that \( LT(I) \) is finitely generated.

**Proposition 6.1.** \( LT(I) = LM(I) \).

**Proof.** It is clear that \( LM(I) \subset LT(I) \). Since \( k \) is a field, we know that for any \( ax^\alpha \in LT(I) \), we have \( a^{-1}ax^\alpha \in LT(I) \). But this is the monomial \( x^\alpha \in LM(I) \). \( \square \)
This proposition shows that, since monomial ideals are finitely generated, we have that $LT(I) = (LT(f_1), \ldots, LT(f_m))$ for a finite set $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$.

**Definition 6.2.** A Gröbner basis for an ideal $I \subset k[x_1, \ldots, x_n]$ is a finite subset $G = \{g_1, \ldots, g_m\} \subset I$ such that $LT(I) = (LT(g_1), \ldots, LT(g_m))$.

The first thing we will show is that every ideal $I \subset k[x_1, \ldots, x_n]$ has a Gröbner basis.

**Proposition 6.2.** Let $I \subset k[x_1, \ldots, x_n]$ be an ideal:

1. If there is a set of polynomials $\{g_1, \ldots, g_m\} \subset I$ such that $LT(I) = (LT(g_1), \ldots, LT(g_m))$, then $\{g_1, \ldots, g_m\}$ is a Gröbner basis for $I$.
2. $I$ has a Gröbner basis.

**Proof.** To prove the first statement, assume that there is a set $\{g_1, \ldots, g_m\} \subset I$ such that $LT(I) = (LT(g_1), \ldots, LT(g_m))$. For any $f \in I$, we want to show that $f = \sum_i a_i g_i$ for polynomials $a_i \in k[x_1, \ldots, x_n]$. Perform the division algorithm on $f$ by $g_1, \ldots, g_m$ to get $f = a_1 g_1 + \ldots + a_m g_m + r$. However, since $f \in I$ and $g_1, \ldots, g_m \in I$, we must have that $r \in I$, which would mean $LT(r) \in LT(I)$. But the only way $LT(r) \in LT(I)$ is if one of the $LT(g_i)$ divides $LT(r)$, which by the division algorithm, cannot be. Hence $r = 0$ and $f = \sum_i a_i g_i$.

To prove the second statement, for the ideal $I$, since $LT(I)$ is finitely generated, we only need a finite set of polynomials $\{g_1, \ldots, g_m\} \subset I$ such that $LT(I) = (LT(g_1), \ldots, LT(g_m))$. By definition, this set $\{g_1, \ldots, g_m\}$ is therefore a Groebner Basis.

We can now prove the Hilbert Basissatz. We first restate it:

**Theorem 6.1 (Hilbert Basissatz).** The ring $k[x_1, \ldots, x_n]$ is Noetherian.

**Proof.** Let $I$ be any ideal in $k[x_1, \ldots, x_n]$. If $I = \{0\}$, then it is already finitely generated. So, assume that $I \neq \{0\}$. Then since $I$ has a Groebner basis, we have that there is a finite set $\{g_1, \ldots, g_m\} \subset I$ that is a Groebner Basis for $I$. Now we will show that $I = (g_1, \ldots, g_m)$. Indeed, let $f \in I$. Then, if we divide $f$ by $g_1, \ldots, g_m$, by the division algorithm we get $f = a_1 g_1 + \ldots + a_m g_m + r$ for some polynomials $a_1, \ldots, a_m \in k[x_1, \ldots, x_n]$. We will show that $r = 0$, thus proving that $I = (g_1, \ldots, g_m)$ and is therefore finitely generated.

Now $r \in I$. Indeed, by the division algorithm, we have that $I \ni f - a_1 g_1 - \ldots - a_m g_m = r$.

Now consider $LT(I)$. Since $g_1, \ldots, g_m$ is a Groebner basis, we have that $LT(I) = (LT(g_1), \ldots, LT(g_m))$, and we also have that, if $r \in I$, $LT(r) \in LT(I) = (LT(g_1), \ldots, LT(g_m))$. However, this cannot happen since none of the $LT(g_i)$ divide $LT(r)$. Hence, $r = 0$ and $f = \sum_i a_i g_i$, and hence $I = (g_1, \ldots, g_m)$.

With the Hilbert Basissatz, we now know that every ideal in $k[x_1, \ldots, x_n]$ is finitely generated. This will be useful later on when we study another of Hilbert’s results, the Hilbert Nullstellensatz.

For now, we are going to study properties of Gröbner bases a little more. For instance, one of the things we will be studying is how to find a Gröbner basis. It is not always the case that, given polynomials $f_1, \ldots, f_m$, that we have that $(f_1, \ldots, f_m) = I$ and $(LT(f_1), \ldots, LT(f_m)) = LT(I)$.
Example 6.1. Consider the $\prec_{\text{lex}}$ order, and let $k[x,y,z]$ be a ring, and let $f_1 = x^2z^2 + 4x^2$ and $f_2 = yz^2 + 4y - z^3$. Now the monomial $x^2z^3 \in LT(I)$. Indeed,
\[x^2z^3 = y \cdot (x^2z^2 + 4x^2) + x^2 \cdot (yz^2 + 4y - z^3),\]
so we have that $x^2z^3 \in LT(I)$, but $x^2z^3 \notin (LT(f_1), LT(f_2))$.

So, we ask whether or not there is some sort of method in determining whether a set $\{g_1, \ldots, g_m\}$ is a Gröbner basis or not. We prove a few propositions before we discuss criterium for Gröbner basis.

Proposition 6.3. Let $\prec$ be a monomial ordering on $k[x_1, \ldots, x_n]$. Let $\{g_1, \ldots, g_m\}$ be a Gröbner basis for the nonzero ideal $I \subset k[x_1, \ldots, x_n]$. Then:

1. Every polynomial $f \in k[x_1, \ldots, x_n]$ can be written uniquely as
   \[f = f_1 + r\]
   where $f_1 \in I$ and no nonzero monomial in the remainder $r$ is divisible by $LT(g_1), \ldots, LT(g_m)$.

2. $f_1$ and $r$ in (1) can be computed by the division algorithm by $g_1, \ldots, g_m$ and the order does not matter.

Proof. The first part in (1) is clear from previous proven statements by letting $f_1 = a_1g_1 + \ldots + a_mg_m$ for the appropriate $a_1, \ldots, a_m \in k[x_1, \ldots, x_n]$. Now assume $f = f_1 + r = f_1' + r'$. That means $r' - r = f_1 - f_1' \in I$. This means that $LT(r' - r) \in LT(I)$. However, since $\{g_1, \ldots, g_m\}$ is a Groebner Basis, we have that $LT(r' - r) \in (LT(g_1), \ldots, LT(g_m))$. However, both $r, r'$ are terms that are not divisible by $LT(g_i)$ for $1 \leq i \leq m$, and hence $r' - r$ is not divisible by any $LT(g_i)$, and therefore the term $LT(r' - r)$ is not divisible by any $LT(g_i)$ unless $r' - r = 0$. Therefore $r = r'$. If $r = r'$, then $f_1 = f_1' = f - r$, and hence the equation $f = f_1 + r$ is unique.

Now, in the proof of (1), we saw that the uniqueness of $r$ is independent of the order in which the polynomials $g_1, \ldots, g_m$ are used in the division (with perhaps the only varying elements are the polynomials $a_1, \ldots, a_m$), which proves (2). \hfill \Box

Now to mention the ideal-membership problem:

Corollary 6.1. Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for the ideal $I \subset k[x_1, \ldots, x_n]$. $f \in I$ if and only if the remainder of $f$ after division by $G$ is zero.

Proof. We already proved that if $r = 0$, then $f \in I$. Conversely, if $r = 0$, by Proposition 6.3, if $f \in I$, then $f = f + 0$ is unique which implies that $r = 0$. \hfill \Box

So, we know from an earlier proposition that any ideal $I \subset k[x_1, \ldots, x_n]$ has a Gröbner basis. Now we want to show that, given a set $\{g_1, \ldots, g_m\}$, whether this set is a Gröbner basis or not. This is called Buchberger’s Criterion. Interestingly, Gröbner basis (after the mathematician Wolfgang Gröbner) were originally introduced by the mathematician Bruno Buchberger in his Ph.D. thesis, along with Buchberger’s Criterion and Buchberger’s Algorithm. He named it a Gröbner basis to honor his advisor Wolfgang Gröbner. We need to define certain terms before we can talk about Buchberger’s Criterion and Buchberger’s Algorithm:

Definition 6.3. Fix a monomial order $\prec$. The $S$-polynomial of two polynomials $f, g \in k[x_1, \ldots, x_n]$ is
\[S(f, g) = \frac{x^\alpha}{LT(f)} \cdot f - \frac{x^\alpha}{LT(g)} \cdot g,\]
where \( x^\alpha \) is the least common multiple of \( LM(f) \) and \( LM(g) \).

**Example 6.2.** Consider the two polynomials \( f = x^2z^2 + 4x^2 \) and \( g = yz^2 + 4y - z^3 \) in the ring \( k[x, y, z] \) as before. We compute \( S(f, g) \):

\[
S(f, g) = \frac{x^2yz^2}{x^2z^2} \cdot (x^2z^2 + 4x^2) - \frac{x^2yz^2}{yz^2} \cdot (yz^2 + 4y - z^3)
\]

\[
= x^2yz^2 + 4x^2y - (x^2yz^2 + 4x^2 - x^2z^3)
\]

\[
= x^2z^3.
\]

The idea of the S-polynomial is to eliminate the leading terms.

**Proposition 6.4.** Fix a monomial order \( \prec \). Suppose that \( f_1, \ldots, f_m \in k[x_1, \ldots, x_n] \) are such that \( m(f_1) = \ldots = m(f_m) \). Let \( h \in k[x_1, \ldots, x_n] \) be a polynomial such that \( h = c_1f_1 + \ldots + c_mf_m \) for constants \( c_1, \ldots, c_m \in k \) and such that \( m(h) < m(f_i) \) for \( 1 \leq i \leq m \). Then,

\[
h = \sum_{i=2}^{m} b_iS(f_{i-1}, f_i)
\]

for some \( b_i \in k \).

**Proof.** Notice that for each \( f_i \) we can write \( f_i = a_if'_i \) where \( f'_i \) is a monic polynomial where \( m(f_i) = m(f'_i) \). Now, we can rewrite \( h \) as

\[
h = \sum a_ici_if'_i
\]

\[
= a_1c_1(f'_1 - f'_2) + (a_1c_1 + a_2c_2)(f'_2 - f'_3) + \ldots
\]

\[
= (a_1c_1 + \ldots + a_mC_M)(f'_M - f'_m) + (a_1c_1 + \ldots + a_mc_m)f'_m.
\]

Note that \( f'_{i-1} - f'_i = S(f_{i-1}, f_i) \) since each of the \( f_i \) has the same multidegree, and in the S-polynomial \( S(f_{i-1}, f_i) \) we also invert \( LC(f_{i-1}) \) and \( LC(f_i) \). Thus, if we take \( b_i = \sum_i a_ici \), we see that since \( m(h) < m(f_i) \), we must have that \( a_1c_1 + \ldots + a_mc_m = 0 \), and the proposition is proved. \( \square \)

**Theorem** (Buchberger’s Criterion). Fix a monomial order \( \prec \) and let \( k[x_1, \ldots, x_n] \) be a polynomial ring. Let \( I = \langle g_1, \ldots, g_m \rangle \) be a nonzero ideal in \( k[x_1, \ldots, x_n] \). Then \( \{g_1, \ldots, g_m\} \) is a Gröbner basis for \( I \) if and only if when we divide \( S(g_i, g_j) \) by \( \{g_1, \ldots, g_m\} \) in any order we get a zero remainder for all pairs \( i \neq j \).

**Proof.** One way of the proof is straightforward, namely, if \( \{g_1, \ldots, g_m\} \) is a Gröbner basis, then since \( S(g_i, g_j) \in \langle g_1, \ldots, g_m \rangle \), we have that the remainder after division is zero by a preceding result.

Now, suppose that after division of \( S(g_i, g_j) \) by \( g_1, \ldots, g_m \) (in any order for \( i \neq j \)) we have a zero remainder. Given \( f \in I \), we want to show that \( LT(f) \in (LT(g_1), \ldots, LT(g_m)) \). Now, since \( f \in I \), we can write

\[
f = \sum_i h_ig_i
\]

for some polynomials \( h_1, \ldots, h_m \in k[x_1, \ldots, x_n] \). Note that this representation is not necessarily unique. As such, choose the linear combination such that

\[
\max_{i=1,\ldots,m} m(h_ig_i) = \alpha
\]

19
is minimal. It is then clear that \( m(f) \leq \alpha \). We rewrite \( f \) as:

\[
f = \sum_{i=1}^{m} h_{ig_i} = \sum_{m(h_{ig_i}) = \alpha} h_{ig_i} + \sum_{m(h_{ig_i}) < \alpha} h_{ig_i} = \sum_{m(h_{ig_i}) = \alpha} \LT(h_i)g_i + \sum_{m(h_{ig_i}) = \alpha} (h_i - \LT(h_i))g_i + \sum_{m(h_{ig_i}) < \alpha} h_{ig_i}.
\]

First suppose that \( m(f) < \alpha \). Since in the equation

\[
f = \sum_{m(h_{ig_i}) = \alpha} \LT(h_i)g_i + \sum_{m(h_{ig_i}) = \alpha} (h_i - \LT(h_i))g_i + \sum_{m(h_{ig_i}) < \alpha} h_{ig_i}
\]

we have that the multidegree of the last two summands are strictly smaller than \( \alpha \), we have that the first summand is also strictly less than \( \alpha \) since, by assumption, \( m(f) < \alpha \). Let \( c_i \) be the constant term such that \( \LT(h_i) = c_i \cdot \LM(h_i) = c_i \cdot h'_i \). Now apply the previous proposition to write

\[
\sum_i c_i(h'_i)g_i
\]

as

\[
\sum_i b_i S(h'_{i-1}g_i, h'_ig_i),
\]

where \( m(h_{i-1}g_i) = m(h_{ig_i}) = \alpha \). For each \( i \), let \( \alpha_{i-1,i} \) be the multidegree of the monic least common multiple of \( \LT(g_{i-1}) \) and \( \LT(g_i) \). We now show that \( S(h'_{i-1}g_{i-1}, h'_ig_i) = x^{(\alpha - \alpha_{i-1,i})} S(g_{i-1}, g_i) \) for the monomial \( x^{(\alpha_{i-1,i})} \). Indeed,

\[
S(h'_{i-1}g_{i-1}, h'_ig_i) = \frac{x^\alpha}{\LT(h'_{i-1}g_{i-1})} \cdot h'_{i-1}g_{i-1} - \frac{x^\alpha}{\LT(h'_ig_i)} \cdot h'_ig_i
\]

\[
= \frac{\LT(h'_{i-1})\LT(g_{i-1})}{\LT(h'_ig_i)} \cdot h'_{i-1}g_{i-1} - \frac{\LT(h'_ig_i)}{\LT(g_i)} \cdot h'_ig_i
\]

\[
= \frac{x^{(\alpha - \alpha_{i-1,i})} \cdot \LT(g_{i-1})}{\LT(g_i)} \cdot g_{i-1} - \frac{x^{(\alpha - \alpha_{i-1,i})} \cdot \LT(g_{i-1})}{\LT(g_i)} \cdot g_i
\]

\[
= x^{(\alpha - \alpha_{i-1,i})} S(g_{i-1}, g_i).
\]

Now, by assumption, the remainder after division of \( S(g_{i-1}, g_i) \) by \( g_1, \ldots, g_m \) is zero, and we know from a previous proposition that \( S(g_{i-1}, g_i) \) can be written as a linear combination \( \sum_j q_j g_j \) with \( m(q_j g_j) < \alpha_{i-1,i} \). Therefore, each \( S(h'_{i-1}g_{i-1}, h'_ig_i) \) can be written as a linear combination \( \sum_j q'_j g_j \) with \( m(q'_j g_j) < \alpha \). Hence, the three summands on the RHS are of multidegree less than \( \alpha \), contradicting the minimality of \( \alpha \). Thus, \( m(f) = \alpha \), and we have

\[
\LT(f) = \sum_{m(h_{ig_i}) = \alpha} \LT(h_i)\LT(g_i),
\]

thus \( \LT(f) \in (\LT(g_1), \ldots, \LT(g_m)) \), and hence \( \{g_1, \ldots, g_m\} \) is a Groebner Basis for \( I \).

**Example 6.3.** Consider the above example with the polynomials \( f_1 = x^2z^2 + 4x^2 \) and \( f_2 = yz^2 + 4y - z^3 \) (with monomial ordering \( <_{\lex} \)). We check whether \( \{f_1, f_2\} \) is a Gröbner basis for \( I = (f_1, f_2) \). Consider the S-polynomials:

\[
S(f_1, f_2) = \frac{x^2yz^2}{x^2z^2} \cdot (x^2z^2 + 4x^2) - \frac{x^2yz^2}{yz^2} \cdot (yz^2 + 4y - z^3) = x^2z^3,
\]

\[
\sum_i c_i(h'_i)g_i
\]
and
\[ S(f_2, f_1) = -S(f_1, f_2) = -x^2z^3. \]

Now, using the \( \prec_{\text{lex}} \) order, divide both \( S(f_1, f_2) \) and \( S(f_2, f_1) \) by \( f_1, f_2 \) (in any order) to get a remainder of either \( r = -4x^2z \) (do this!). Thus, \( \{ f_1, f_2 \} \) is not a Groebner Basis for \( I \).

Buchberger’s Criterion is useful in determining whether or not a given set of polynomials is indeed a Groebner basis. However, the criterion only determines whether or not a given set of polynomials is a Groebner basis or not; however, this criterion does give a blueprint in determining how to find a Groebner basis. We know that every ideal \( I \subset k[x_1, \ldots, x_n] \) is finitely generated, so if we start with the generators \( I = (f_1, \ldots, f_m) \), we can determine a Groebner basis using Buchberger’s Algorithm:

(Step 1) Divide each \( S(f_i, f_j) \) for each generator \( f_i, f_j \in (f_1, \ldots, f_m), \ i \neq j \) by the polynomials in \( G_0 = \{ f_1, \ldots, f_m \} \) in any order. if there is a zero remainder for all such divisions, then \( \{ f_1, \ldots, f_m \} \) is a Groebner basis. Otherwise, there is a remainder \( r \neq 0 \). This remainder will be an element of \( I \).

(Step 2) Enlarge \( G \) by adding the remainder \( r := f_{m+1} \) to get \( G_1 = \{ f_1, \ldots, f_m, f_{m+1} \} \).

(Step 3) Repeat step 1 for the ideal \( I = (f_1, \ldots, f_m, f_{m+1}) \) with the new set \( G_1 = \{ f_1, \ldots, f_m, f_{m+1} \} \).

It is clear that this algorithm terminates after a finite number of steps. Indeed, the remainder has a multidegree that keeps shrinking after every iteration of Buchberger’s Algorithm since each remainder will not be divisible by the preceding leading terms.

Example 6.4. Consider again the polynomials \( f_1 = x^2z^2 + 4x^2 \) and \( f_2 = yz^2 + 4y - z^3 \) in the ring \( k[x, y, z] \) (with \( \prec_{\text{lex}} \) order). We first try to consider \( G_0 = \{ f_1, f_2 \} \) as a Groebner Basis for the ideal \( I = (f_1, f_2) \). By an earlier calculation, we have that \( S(f_1, f_2) = x^2z^3 \), so \( G_0 \) is not a Groebner basis for \( I \). So, consider the remainder \( f_3 = 4x^2z \), and construct \( G_1 = \{ f_1, f_2, f_3 \} \). Now compute \( S(f_1, f_3) \) and \( S(f_2, f_3) \):

\[
S(f_1, f_3) = \frac{x^2z^2}{x^2 z^2} \cdot (x^2z^2 + 4x^2) - \frac{x^2z^2}{4x^2z} \cdot (4x^2z) = 4x^2
\]

\[
S(f_2, f_3) = \frac{yz^2}{yz^2} \cdot (yz^2 + 4y - z^3) - \frac{yz^2}{4x^2z} \cdot (4x^2z) = 4x^2y - x^2z^3.
\]

Since \( f_4 = 4x^2 \) is not divisible by any \( f_i \in G_1 \), construct \( G_2 = \{ f_1, f_2, f_3, f_4 \} \). Compute \( S(f_1, f_4) \), \( S(f_2, f_4) \), and \( S(f_3, f_4) \):

\[
S(f_1, f_4) = \frac{x^2z^2}{x^2 z^2} \cdot (x^2z^2 + 4x^2) - \frac{x^2z^2}{4x^2} \cdot (4x^2) = 4x^2 = f_4
\]

\[
S(f_2, f_4) = \frac{yz^2}{yz^2} \cdot (yz^2 + 4y - z^3) - \frac{yz^2}{4x^2z} \cdot (4x^2z) = 4x^2y - x^2z^3 = -\frac{1}{4}z^2f_3 + yf_4
\]

\[
S(f_3, f_4) = \frac{x^2z}{4x^2z} \cdot (4x^2z) - \frac{x^2z}{4x^2} \cdot (4x^2) = 0.
\]

The remainder after division by elements of \( G_2 \) of these are zero since they can be written as linear combinations of elements in \( G_2 \). Hence, \( G_2 = \{ f_1, f_2, f_3, f_4 \} \) constitutes a Groebner basis for \( I \).

Buchberger’s Algorithm helps us determine a Groebner basis for an ideal. However, if we look at the above example, we see that, if we take the leading terms for \( G_2 \), we get \( \{ x^2z^2, yz^2, 4x^2z, 4x^2 \} \). From this set, the only terms needed are \( yz^2 \) and \( 4x^2 \). Indeed, \( x^2z^2 = \frac{1}{4}z^2 \cdot (4x^2) \) and \( 4x^2z = z \cdot 4x^2 \). So, if we just want to consider the set \( G'_2 = \{ yz^2 + 4y - z^3, x^2 \} \), this is also a Groebner basis for \( I \).
Definition 6.4. A minimal or reduced Gröbner basis for an ideal \( I \subset k[x_1, \ldots, x_n] \) is a Gröbner basis \( G = \{g_1, \ldots, g_m\} \) such that each \( \text{LT}(g_i) \) is monic and each \( \text{LT}(g_i) \) is not divisible by \( \text{LT}(g_j) \) for each \( i \neq j, 1 \leq i, j \leq m \).

Lemma 6.1. For any ideal \( I \subset k[x_1, \ldots, x_n] \), \( \{1\} \) is a reduced Groebner basis for \( I \) if and only if \( I = k[x_1, \ldots, x_n] \).

Proof. Assume first that \( I = k[x_1, \ldots, x_n] \). Then since any polynomial in \( k[x_1, \ldots, x_n] \) can be written as \( f \cdot 1 \) for any \( f \in k[x_1, \ldots, x_n] \), we can take as a Groebner Basis \( \{1\} \) for the ideal \( I \), and it is apparent that \( \text{LT}(1) = \text{LT}(I) = \text{LT}(k[x_1, \ldots, x_n]) \), and since \( \text{LT}(1) = 1 \), any leading term in \( k[x_1, \ldots, x_n] \) is a multiple of 1, hence \( \{1\} \) is a reduced Groebner Basis.

Now assume that \( \{1\} \) is a reduced Groebner Basis for some ideal \( I \). By definition, this means that \( 1 \in I \), hence for any \( f \in k[x_1, \ldots, x_n] \), we have \( f \cdot 1 \in I \) which implies that \( I = k[x_1, \ldots, x_n] \). \( \square \)

7. Maple and Gröbner Bases

We note that the commands listed will be for MAPLE versions 14 and later (where a semicolon is not needed after every command). This section will be a review of some basic MAPLE commands we can now use. Those include

1. How to order polynomials with respect to some monomial order \( \prec \).
2. How to perform the division algorithm in \( k[x_1, \ldots, x_n] \) with respect to some monomial order \( \prec \).
3. How to find a Gröbner basis for an ideal \( I \).

For any of these three calculations, we need to use the Gröbner Basis Package. You can begin by typing into the command line

\[
> \text{with(Groebner)}
\]

to upload the Gröbner Basis Package. In it, we can use “normalform”, “monomialorder”, and “Basis” commands. If you do not wish to load the Groebner package, you can still perform the desired action by typing a command of the following type:

\[
\text{Groebner[command](arguments)}.
\]

7.1. Monomial Order. The sort command allows you to take a polynomial \( f \) and sort it with respect to some ordering. The command for sorting is:

\[
\text{sort}(f, [X], \text{tord}),
\]

where \( f \) is a polynomial, \( [X] \) is a list of variables, and \( \text{tord} \) is a monomial order. The monomial orders we studied in this course would appear in MAPLE as:

1. plex\((x[1], \ldots, x[n])\): this is the usual lexicographic order, and note that it orders the polynomials as:

\[
x[1] \succ x[2] \succ \ldots \succ x[n].
\]

2. grlex\((x[1], \ldots, x[n])\): this is the graded lexicographic order, which first computes the total degree then defers to the lexicographic order. If no monomial order is specified, then the default order MAPLE uses is the grlex order.

3. tdeg\((x[1], \ldots, x[n])\): this is the graded reverse lexicographic order (or grevlex as we put it). This first computes the total degree then defers to the reverse lexicographic order.
Example 7.1. We first begin in the 3 variable case. We want to sort the following polynomial in terms of the lexicographic order, graded lexicographic order, and graded reverse lexicographic order. We start with the polynomial:

\[ f := 3x^7y^3z + 4x^6y^8z^2 + x^{10}y^3 + 3x - 5z^3 + 6xyz. \]

First we sort by \( plex \) order:

\[ \text{sort}(f, [x,y,z], \text{plex}) \]

and after putting it into \textsc{Maple} we get as an output:

\[ f = x^{10}y^3 + 3x^7y^3z + 4x^6y^8z^2 + 3x - 5z^3 + 6xyz. \]

It will be left as an exercise to try sorting using the other monomial orderings.

You can also use the package to determine the leading term, coefficient, or monomial for some polynomials using the following commands:

\[ \text{LeadingTerm}(f, \text{tord}) \]

\[ \text{LeadingCoefficient}(f, \text{tord}) \]

\[ \text{LeadingMonomial}(f, \text{tord}) \]

where \( f \) is a polynomial and \( \text{tord} \) is a monomial order.

7.2. Division Algorithm. \textsc{Maple} can also compute divisions in polynomial rings with multiple variables over a field (we will only consider the case here where \( \mathbb{Q} \) is a subset of our field, in other words, fields of characteristic zero. In later courses, one will learn methods and theory on fields of characteristic \( p \)). The calling sequence for our uses in the division algorithm will be (after loading the \textsc{Groebner} package):

\[ \text{NormalForm}(f, G, \text{tord}), \]

where \( f \) is a polynomial, \( G \) is list of divisors, and \( \text{tord} \) is a monomial order. The output is the remainder of \( f \) after division by the polynomials in \( G \). Note that the order of the list in the above matters; the only time it does not matter is when \( G \) is \textsc{Groebner} basis (see earlier proposition).

Example 7.2. We start with our polynomial from before, this time sorted by \( \text{grlex} \):

\[ f = 4x^6y^8z^2 + x^{10}y^3 + 3x^7y^3z - 5z^3 + 3x + 6xyz \]

and we will divide this by the set \( G := [x^6y^2z^2 + 3xz - y, z^3, 3xy - z]: \)

\[ \text{NormalForm}(f, G, \text{grlex}(x,y,z)) \]

to get remainder:

\[ r = 6xyz + 3x - 12xy^6 + 4y^7 + 9x^7y^3xy + x^{10}y^3. \]
7.3. **Basis.** Given a set of polynomials, we can find a Groebner Basis for the ideal they generate by using the *Basis* command in the Groebner package. The command sequence is:

\[
\text{Basis}(J, \text{tord}),
\]

where \( J \) is a polynomial ideal (or a list of polynomials) and again, \( \text{tord} \) is a monomial order. The output is a reduced Groebner Basis.

**Example 7.3.** We want to find a Groebner Basis of \( G \) from the earlier example, but using \( \text{tdeg} \) instead. We input:

\[
\text{Basis}(G, \text{tdegx}, y, z)
\]

to get a Groebner basis \( \{1\} \).

In each of the above commands, if we list multiple polynomials, be sure to put brackets around the list. For example, given a list in \( k[x, y, z] \) (with \( \text{grlex} \) order):

\[
x^2y^2z^2 + 3xz - y, x^4 + yz^3 - 2x, 3x^7 - z
\]

we need to place brackets around the list in each of the calling sequences, so the above list becomes:

\[
[x^2y^2z^2 + 3xz - y, x^4 + yz^3 - 2x, 3x^7 - z].
\]

Also, when working with other packages, it is not necessary to load the Groebner package completely. If you wish, for example, to use the division algorithm but not load the Groebner Package, you would type:

\[
\text{Groebner}[\text{NormalForm}](f, G, \text{tord}).
\]

If you do not specify which package is being used, you may get error messages.

### 8. Polynomials and Resultants

Before we start with the Hilbert Nullstellensatz, we will briefly go off topic and discuss some properties of certain polynomials, and we will also introduce resultants which will be useful when we later discuss the Nullstellensatz.

**Definition 8.1.** Let \( k \) be a field.

1. A nonconstant polynomial \( f \in k[x_1, \ldots, x_n] \) is **irreducible** over \( k \) if, whenever \( f = gh \) for some \( g, h \in k[x_1, \ldots, x_m] \), then either \( g \) or \( h \) is a unit in \( k[x_1, \ldots, x_n] \).
2. A nonzero element \( p \in k[x_1, \ldots, x_n] \) is **prime** if \( (p) \) is a prime ideal.

**Proposition 8.1.** In \( k[x_1, \ldots, x_n] \), prime elements are irreducible.

*Proof.* Let \( p \) be prime in \( k[x_1, \ldots, x_n] \) and suppose \( p = ab \). Then, \( ab \in (p) \). Since \( (p) \) is a prime ideal, either \( a \in (p) \) or \( b \in (p) \). Say \( a \in (p) \). Then, \( a = pr \) for some \( r \in k[x_1, \ldots, x_n] \). This means

\[
p = ab = prb \Rightarrow rb = 1,
\]

and we have that \( b \) is a unit. \( \square \)

**Proposition 8.2.** Every nonconstant polynomial in \( k[x_1, \ldots, x_n] \) can be written as a product of irreducible polynomials over \( k \).
Proof. Let $f \in k[x_1, \ldots, x_n]$ be a nonconstant polynomial. If $f$ is irreducible, then we are done; otherwise, we can write $f = gh$ with both $\deg(g)$ and $\deg(h)$ of degree less than $f$. Then proceed to check both $g$ and $h$. If they are irreducible, then we have factored $f$ into a product of irreducibles. If one of either $g$ or $h$ are not irreducible, then continue to factor. This process must cease since each time we factor, the degrees decrease.

\[ \square \]

**Definition 8.2.** Let $f, g \in k[x]$. The greatest common divisor of $f$ and $g$, or $\text{GCD}(f, g)$, is a polynomial $h$ such that:

1. $h|f$ and $h|g$, and
2. If there is another polynomial $\tilde{h}$ such that $\tilde{h}|f$ and $\tilde{h}|g$, then $\tilde{h}|h$.

Now given two polynomial $f, g \in k[x]$, can we determine whether or not a common divisor exists? One way would be to find the GCD by using the division algorithm. However, there is a simpler test to determine the existence of a common divisor:

**Lemma 8.1.** Let $f, g \in k[x]$ be polynomials such that $\deg(f) = m$ and $\deg(g) = r$ for $m, r > 0$. Then, $f, g$ have a common factor if and only if there are polynomials $p, q \in k[x]$ such that:

1. $p$ and $q$ are not both zero.
2. $\deg(p) \leq r - 1$ and $\deg(q) \leq m - 1$.
3. $pf + qg = 0$.

**Proof.** Assume that $f, g$ have a common factor. Then, $f = hf_1$ and $g = hg_1$. Note, that the degree of $f_1$ is $\leq r - 1$ and the degree of $g_1$ is $\leq m - 1$. Take $p = g_1$ and $q = -f_1$. Then, we found $p, q$ such that:

\[ pf + qg = g_1(hf_1) + (-f_1)(hg_1) = f_1g_1h - f_1g_1h = 0. \]

Now, assume that there exists polynomials $p$ and $q$ (with $q \neq 0$) that satisfy the aforementioned conditions and that $\text{GCD}(f, g) = 1$. By the extended Euclidean Algorithm, there are polynomials $\tilde{p}$ and $\tilde{q}$ such that

\[ \tilde{p}f + \tilde{q}g = 1. \]

If we multiply the above equation by $q$, and since the equality $-pf = qg$ (from the third condition) holds, we have:

\[ q = q(\tilde{p}f + \tilde{q}g) = \tilde{p}qf - \tilde{q}pf = (\tilde{p}q - \tilde{q}p)f, \]

and since $q \neq 0$, we have that $\deg(q) \geq m$, a contradiction. Hence, there has to be a common factor. \[ \square \]

Now we develop a way to show the existence of polynomials $p$ and $q$ as stated above. Given $f, g \in k[x]$, if there is a common divisor, then by Lemma (8.1), there are polynomials $p, q$ such that

\[ pf + qg = 0. \]

More explicitly, if we write

\[ f = a_0x^m + \ldots + a_{m-1}x + a_m \]
\[ g = b_0x^r + \ldots + b_{r-1}x + b_r \]

with $a_0, b_0 \neq 0$, and

\[ p = c_0x^{r-1} + \ldots + c_{r-2}x + c_{r-1} \]
\[ q = d_0x^{m-1} + \ldots + d_{m-2}x + d_{m-1}, \]
then multiplying and adding, we get the following system of equations:

\[
\begin{align*}
    a_0c_0 + b_0d_0 &= 0 \text{ coefficient of } x^{d+m-1} \\
    a_1c_0 + a_0c_1 + b_1d_0 + b_0d_1 &= 0 \text{ coefficient of } x^{d+m-2} \\
    \vdots \\
    a_mc_{r-1} + b_rd_{m-1} &= 0 \text{ coefficient of } x^0.
\end{align*}
\]

(1)

Since we are looking for the existence of the \(c_i\)'s and \(d_j\)'s \((0 \leq i \leq r-1, 0 \leq j \leq m-1)\), the above gives a system of \(m+r\) equations in \(m+r\) unknowns. From linear algebra, we know that there is a nonzero solution if the coefficient matrix has a determinant equal to zero. To put it differently, we introduce the following definition:

**Definition 8.3.** Let \(f, g \in k[x]\) be any two polynomials with \(\deg(f) = m\) and \(\deg(g) = r\). The **Sylvester matrix** of \(f\) and \(g\) with respect to \(x\), denoted \(\text{Syl}_x(f,g)\), is the coefficient matrix of the system of equations (1) given above. In other words, it is the \((r+m) \times (r+m)\) matrix

\[
\text{Syl}_x(f,g) = \begin{pmatrix}
    a_0 & b_0 \\
    a_1 & b_1 & b_0 \\
    a_2 & a_1 & b_2 & b_1 & \cdots \\
    \vdots & \vdots & a_0 & b_2 & \cdots & b_0 \\
    a_m & \cdots & a_1 & b_r & \cdots & b_1 \\
    a_m & a_2 & b_r & \cdots & b_2 \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    a_m & \cdots & a_2 & b_r & \cdots & b_r \\
    a_m & \cdots & \cdots & \cdots & b_r
\end{pmatrix},
\]

where the empty spaces are zeros. The **resultant** of \(f\) and \(g\) with respect to \(x\), denoted \(R_x(f,g)\), is the determinant of \(\text{Syl}_x(f,g)\), or

\[
R_x(f,g) = \det(\text{Syl}_x(f,g)).
\]

Since the above system of equations (1) is \(r+m\) equations in \(r+m\) unknowns, we know from linear algebra that this has a non-zero solution if the determinant of the coefficient matrix is zero. In other words,

**Proposition 8.3.** \(f, g \in k[x]\) have a nonconstant common factor in \(k[x]\) if and only if \(R_x(f,g) = 0\).

**Example 8.1.** (1) Consider \(f = x - 1\) and \(g = -x + 1\). Compute the resultant of \(f, g\) by finding the determinant of

\[
\text{Syl}_x(f,g) = \begin{pmatrix}
    1 & -1 \\
    -1 & 1
\end{pmatrix}.
\]

This determinant indeed equals 0. Hence, there is a common factor of \(f\) and \(g\); it is easy to see that \((x - 1)\) is a common factor.
(2) Consider now \( f = x^3 - 1 \) and \( g = x^2 + x - 2 \). Is there a common factor? Compute the resultant of \( f, g \) by finding the determinant of the matrix

\[
\text{Syl}_x(f, g) = \begin{pmatrix}
1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 \\
0 & 0 & -2 & 1 & 1 \\
-1 & 0 & 0 & -2 & 1 \\
0 & -1 & 0 & 0 & -2
\end{pmatrix}.
\]

Using MAPLE, we compute the determinant using the following commands: using the linear algebra package with(LinearAlgebra), we write

\[
f := x^3 - 1 \\
g := x^2 + x - 2 \\
M := \text{Transpose(SylvesterMatrix}(f, g, x)).
\]

Note that the “\( x \)” in the above input is the variable for which we evaluate the Sylvester Matrix of \( f \) and \( g \). With \( M \) now defined as the Sylvester Matrix, we type

\[
\text{Determinant}(M)
\]

to evaluate the determinant of \( M \). After these steps, we see that the determinant equals 0, and \( f \) and \( g \) have a common factor. Further computation shows that \( (x - 1) \) is a common factor.

**Lemma 8.2.** \( R_x(f, g) \) is in the ideal spanned by \( f \) and \( g \).

**Proof.** Let \( f = a_0x^m + \ldots + a_{m-1}x + a_m \) and \( g = b_0x^r + \ldots + b_{r-1}x + b_r \) be polynomials in \( k[x] \). Form the Sylvester Matrix

\[
\text{Syl}_x(f, g) = \begin{pmatrix}
a_0 & b_0 \\
a_1 & b_1 & b_0 \\
a_2 & a_1 & \cdots & b_2 & b_1 & \cdots \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots \\
a_m & \cdots & a_1 & b_r & \cdots & \cdots & b_1 \\
a_m & \cdots & a_2 & b_r & \cdots & \cdots & b_2 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
& & & & & a_m & b_r
\end{pmatrix},
\]

When computing the determinant of \( \text{Syl}_x(f, g) \), replace the last row by:

Last row + \( x \cdot \) second-to-last-row + \( x^2 \cdot \) third-to-last-row + \( \ldots + x^{r+m-1} \cdot \) first row.

Recall from linear algebra that these computations do not change the value of the determinant. The resulting entries in the last row become

\[
( \ x^{r-1}f, \ x^{m-2}f, \ \ldots, \ xf, \ f, \ x^{m-1}g, \ x^{m-2}g, \ \ldots, \ xg, \ g \ )
\].
Now, when expanding the determinant across this last row, by factoring out \( f \) and \( g \) where appropriate, we get an expression of the form
\[
f \cdot A(x) + g \cdot B(x)
\]
for some polynomials \( A(x), B(x) \in k[x] \). The expression above is a linear combination of \( f \) and \( g \), and is therefore an element of the ideal spanned by \( f \) and \( g \).

9. The Ideal-Variety Correspondence and the Hilbert Nullstellensatz

In the previous sections we used the theory of monomials and Groebner Bases to prove the Hilbert Basissatz which is useful in the sense that we know that every single ideal in the ring \( k[x_1,\ldots,x_n] \) has a finite set of generators. We also showed that, given a variety \( V \), we can pass to the ideal \( I(V) \).

Thus, we have a map:
\[
\text{Affine Varieties } V \text{ in } k^n \longrightarrow I(V).
\]
Now, using the Hilbert Basissatz, we can go the other direction.

**Definition 9.1.** Let \( I \subset k[x_1,\ldots,x_n] \) be an ideal. We define \( V = V(I) \) to be the set:
\[
V(I) = \{(a_1,\ldots,a_n) \in k^n \mid f(a_1,\ldots,a_n) = 0 \text{ for all } f(x_1,\ldots,x_n) \in I\},
\]
called the *variety of the ideal* \( I \).

How can we guarantee that \( V(I) \) is actually an affine variety? We have only discussed varieties of a finite number of polynomials, but thanks to the Hilbert Basissatz, we will see that it makes no difference whether we talk about the ideal or the generators when it comes to affine varieties:

**Lemma 9.1.** Let \( I = (f_1,\ldots,f_m) \) be an ideal. Then, \( V(I) = V(f_1,\ldots,f_m) \).

**Proof.** By definition, the set \( V(I) \) is
\[
V(I) = \{(a_1,\ldots,a_n) \in k^n \mid f(a_1,\ldots,a_n) = 0 \text{ for all } f \in I\}.
\]
Since every polynomial \( f \in I \) is a linear combination of the \( f_1,\ldots,f_m \), we have that
\[
f = \sum_{i=1}^{m} h_i f_i,
\]
and therefore, for any \( (a_1,\ldots,a_m) \in V(f_1,\ldots,f_m) \), we have:
\[
f(a_1,\ldots,a_n) = \sum_{i=1}^{m} h_i(a_1,\ldots,a_n) f_i(a_1,\ldots,a_n)
\]
\[
= \sum_{i=1}^{m} h_i(a_1,\ldots,a_n) \cdot 0
\]
\[
= 0.
\]
Hence, \( V(f_1,\ldots,f_m) \subset V(I) \).

Now, let \( (a_1,\ldots,a_n) \in V(I) \). Since each \( f \in I \) must vanish at \( (a_1,\ldots,a_n) \), we have that, in particular, the generators \( f_i(a_1,\ldots,a_n) = 0, 1 \leq i \leq m \). Since the generators vanish at \( (a_1,\ldots,a_n) \), every polynomial \( f \in I \) is annihilated by \( (a_1,\ldots,a_n) \), and hence \( V(I) \subset V(f_1,\ldots,f_m) \). \( \square \)
Now, given an ideal \( I \subset k[x_1, \ldots, x_n] \), we can pass through its variety, thus obtaining a map:

\[
\text{Ideals } I \subset k[x_1, \ldots, x_n] \longrightarrow V(I).
\]

Now, we have some sort of correspondence, which looks like:

\[
\text{Ideals } I \subset k[x_1, \ldots, x_n] \longrightarrow V(I)
\]

\[
\text{Affine Varieties } V \subset k^n \longrightarrow I(V).
\]

However, this correspondence is not necessarily a bijection. In particular, when we pass from ideals to varieties, this map is not one to one. For example, the two varieties (in \( \mathbb{R}[x] \)) \( V(x) \) and \( V(x^3) \) are both the single points 0. However, \( (x) \neq (x^3) \) as ideals. In fact, we have this problem in the multivariable case: we see that

\[
V(x_1, \ldots, x_n) = V(x_1^{i_1}, \ldots, x_n^{i_n}) = \{(0, \ldots, 0)\}
\]

for exponents \( i_j > 1 \) for each \( j \), but the ideals are not equal:

\[
(x_1, \ldots, x_n) \neq (x_1^{i_1}, \ldots, x_n^{i_n}).
\]

Another way it is not one-to-one is when we let \( k \) be any field. If \( k \) is not algebraically closed, there may be a case where, given an ideal, the generators have no solutions in \( k \). In this case, the variety is the empty set. For example, consider again \( \mathbb{R}[x] \). The polynomial \( x^2 + 1 \) has no solutions in \( \mathbb{R} \), and therefore \( V(x^2 + 1) = \emptyset \). However, since constant polynomials have no solutions in \( \mathbb{R} \) either, we see that \( V(\mathbb{R}) = V(x^2 + 1) = \emptyset \), but it is definitely not the case that \( (x^2 + 1) = \mathbb{R} \).

We begin analyzing the second problem first. If we restrict ourselves to only algebraically closed fields, then do we get rid of aforementioned problems? The answer is yes; we no longer have to worry about varieties being equal to the empty set except in special circumstances. Such circumstances are covered in a weak version of Hilbert’s Nullstellensatz (Null=zero, stellen=locus (or places), satz=theorem). We will prove the Weak Nullstellensatz by first stating and proving a simple form of Noether’s Normalization Theorem:

**Theorem.** If \( k \) is an infinite field and \( f \) is a nonconstant polynomial in \( k[x_1, \ldots, x_n] \) with \( n \geq 2 \), then there exist \( a_1, \ldots, a_{n-1} \in k \) such that

\[
f(x_1 + a_1 x_n, \ldots, x_{n-1} + a_{n-1} x_n, x_n) = a \cdot x_n^d + \text{lower terms in } x_n
\]

has a nonzero, constant coefficient for the monomial \( x_n^d \) where \( d \) is the degree of \( f \).

**Proof.** Let \( f_d \) be the homogeneous component of \( f \) of degree \( d \), that is, \( f_d \) is the sum of all monomial terms in \( f \) of degree \( d \). Then, the coefficient of \( x_n^d \) in the polynomial \( f(x_1 + a_1 x_n, \ldots, x_{n-1} + a_{n-1} x_n, x_n) \) is \( f_d(a_1, \ldots, a_{n-1}, 1) \) for some yet to be determined \( a_1, \ldots, a_{n-1} \). By construction, \( f_d(x_1, \ldots, x_{n-1}, 1) \) is a nonzero polynomial in \( k[x_1, \ldots, x_{n-1}] \), and since \( k \) is infinite, there is some point \( (a_1, \ldots, a_{n-1}) \in k^{n-1} \) in which \( f_d(x_1, \ldots, x_{n-1}, 1) \) does not vanish. Hence, such constants exist, proving the theorem. \( \square \)

**Theorem (Hilbert’s Weak Nullstellensatz).** Let \( k[x_1, \ldots, x_n] \) be a polynomial ring over an algebraically closed field \( k \) and let \( I \subset k[x_1, \ldots, x_n] \) be an ideal. If \( I \subset k[x_1, \ldots, x_n] \) is proper then \( V(I) \) is non-empty.

**Proof.** If \( I = 0 \), then the conditions vacuously hold. So we may begin by assuming that \( I \neq 0 \).

We proceed by induction on the number of variables. When \( n = 1 \), we know that since \( I \) is proper, and since we know that \( k[x] \) is a principal ideal domain, there must be a polynomial that generates \( I \). Since \( k \) is algebraically closed, this generator has a solution, and therefore \( V(I) \) is non-empty.
Now assume that $n > 1$. By the previous theorem, we know that there exist $a_1, \ldots, a_{n-1}$ such that we can rewrite any $f \in I$ using the change of variables as in the previous theorem, to write $f$ as a polynomial $g$, where $g$ is monic polynomial in the variable $x_n$. Fix such a $g$ and consider the ideal $I' \subset k[x_1, \ldots, x_{n-1}]$ consisting of those polynomials in $I$ that do not contain the indeterminate $x_n$. Two things now occur: firstly, we know that $1 \notin I$, and since these change of variables do not affect constants, we see that $1 \notin I'$ either, hence $I'$ is proper. Secondly (following from the first), by induction hypothesis, we know that there is at least one point $(b_1, \ldots, b_{n-1})$ in $V(I')$. We now show that the set

$$J = \{f(b_1, \ldots, b_{n-1}, x_n) \mid f \in I\}$$

is proper in the ring $k[x_n]$. We show this by supposing that $J$ is not proper, and we will arrive at a contradiction. Assume that there is an $f \in I$ such that $f(b_1, \ldots, b_{n-1}, x_n) = 1$. Write

$$f = f_0 + f_1 x_n + \ldots + f_d x_n^d,$$

where each $f_i$ is the homogenous component of degree $i$ and $d$ is the total degree of $f$, and each $f_i \in k[x_1, \ldots, x_{n-1}]$. In such a polynomial expression of $f$, we see that each $f_i(b_1, \ldots, b_{n-1}) = 0$ for all but $f_0$, because $f_0(b_1, \ldots, b_{n-1}) = 1$ by choice of $f$. As we stated earlier though, we also have a monic polynomial $g$ which we can express as

$$g = g_0 + g_1 x_n + \ldots + g_{e-1} x_n^{e-1} + x_n^e$$

with each $g_j \in k[x_1, \ldots, x_{n-1}]$ for $j = 1, \ldots, e - 1$.

Consider $R_{x_n}(f, g)$:

$$R_{x_n}(f, g) = \begin{bmatrix}
  f_0 & g_0 \\
  f_1 & g_1 \\
  \vdots & \vdots \\
  f_d & g_1 \\
  \vdots & \vdots \\
  f_d & g_2 \\
  \vdots & \vdots \\
  f_d & 1
\end{bmatrix}.$$

By Lemma 8.2, we know that $R_{x_n}(f, g)$ is in the ideal $I'$. If we evaluate each entry of $R_{x_n}(f, g)$ at the point $(b_1, \ldots, b_{n-1})$, we get a lower triangular matrix with 1’s along the diagonal, and $R_{x_n}(f, g) = 1 \in I'$, a contradiction. Hence, $J$ is a proper ideal of $k[x_n]$. Therefore, $J$ is either 0 or is generated by some polynomial $h(x_n)$, but either way, since $k$ is algebraically closed, $h(x_n)$ has a root $b_n$ in $k$, and therefore the polynomial $f(b_1, \ldots, b_{n-1}, b_n) = 0$ for all $f \in I$. \hfill \Box

Therefore, the weak Nullstellensatz gives a criteria for when affine varieties contain solutions. Namely, if $k$ is algebraically closed, if we know that $1 \notin I$ for ideals $I \subset k[x_1, \ldots, x_n]$, then $V(I)$ has at least one solution. One can see how this is analogous to algebraically closed fields in one variable: every non-constant polynomial in $k[x_1, \ldots, x_n]$ has a solution in $k^n$ since the ideal that polynomial generates is proper in $k[x_1, \ldots, x_n]$.

**Corollary 9.1.** If $k$ is algebraically closed and $I$ is an ideal, then $I = k[x_1, \ldots, x_n]$ if and only if $V(I) = \emptyset$. 

30
Proof. \((\Leftrightarrow)\) is the contrapositive of the statement of the Weak Nullstellensatz. If \(I = k[x_1, \ldots, x_n]\), since constant polynomials have no solutions, we have that \(V(I) = V(k[x_1, \ldots, x_n]) = \emptyset\).\(\square\)

**Corollary 9.2.** If \(k\) is algebraically closed, then an ideal \(M\) is maximal if and only if \(M = (x_1 - a_1, \ldots, x_n - a_n)\).

**Proof.** Since \(M\) is maximal, it is, in particular, proper in \(k[x_1, \ldots, x_n]\). By the weak Nullstellensatz, \(V(M)\) contains at least one point \((a_1, \ldots, a_n)\), thus every \(f \in M\) vanishes at \((a_1, \ldots, a_n)\), so we see that \(M \subseteq \{ (a_1, \ldots, a_n) \}\). It is easy to see that \(I((a_1, \ldots, a_n)) = (x_1 - a_1, \ldots, x_n - a_n)\). So we have a sequence of containments

\[
M \subseteq I((a_1, \ldots, a_n)) \subseteq k[x_1, \ldots, x_n].
\]

However, since \(M\) is maximal, we have that \(M = (x_1 - a_1, \ldots, x_n - a_n)\).

Now we need to show that \((x_1 - a_1, \ldots, x_n - a_n) = M\) is maximal. Let \(I\) be an ideal properly containing \(M\). That means there is some \(f \in k[x_1, \ldots, x_n]\) such that \(f \in I\) but \(f \notin M\). Divide \(f\) by the generators in \(M\) to get

\[
f = A_1(x_1 - a_1) + A_2(x_2 - a_2) + \cdots + A_n(x_n - a_n) + r
\]

where \(r \in k\). We also see that \(r \neq 0\) since \(f \notin M\). However,

\[
r = f - A_1(x_1 - a_1) - \cdots - A_n(x_n - a_n) \in I
\]

and since \(r \in k\), we have \(\frac{1}{r} \cdot r \in I\), and so \(I = k[x_1, \ldots, x_n]\). \(\square\)

So, just from the Weak Nullstellensatz, we have a (sub-)correspondence from maximal ideals to points

\[
\text{Maximal ideals } M \rightarrow \text{ point } (a_1, \ldots, a_n) \in k^n
\]

\[
\text{point } (a_1, \ldots, a_n) \in k^n \rightarrow \text{ Maximal ideal } (x_1 - a_1, \ldots, x_n - a_n).
\]

So, we have criterion of knowing whether or not systems \(F\) of polynomial equations contain solutions. If the ideal generated by the system \(F\) contains 1, then \(F\) has no solution.

So the latter issue has been solved, namely, when \(V(I) = \emptyset\). However, another issue of the correspondence above was that the variety \(V(I) = \{ (0, \ldots, 0) \}\) when \(I = (x_1^{i_1}, \ldots, x_n^{i_n})\) for exponents \(i_j > 0\) for \(j = 1, \ldots, n\). Thus this correspondence was not bijective, specifically, not one-to-one. The question is, are there any additional conditions we could impose to make the map one-to-one?

**Definition 9.2.** Let \(I\) be an ideal in \(k[x_1, \ldots, x_n]\). The radical of \(I\), denoted \(\sqrt{I}\) is

\[
\sqrt{I} = \{ f \in k[x_1, \ldots, x_n] \mid f^m \in I \text{ for some } m \geq 1 \}.
\]

An ideal \(I\) is radical if \(I = \sqrt{I}\). In other words, \(I\) is radical if, whenever \(f^m \in I\) for \(m \geq 1\), then \(f \in I\).

We remark that this is not the same as \(I\) being prime. We do know, however, that if \(I\) is prime, then \(I\) is radical, since \(f^m = f \cdots f\) and since \(I\) is prime, one of these factors belongs to \(I\), hence \(f \in I\).

**Example 9.1.** Consider the ideal \(I = (x_1^{i_1}, \ldots, x_n^{i_n})\) in \(k[x_1, \ldots, x_n]\) for exponents \(i_j > 1\), \(j = 1, \ldots, n\). This ideal is not radical. Indeed, the polynomial \(x_1^{2^n}\) is in the ideal \(I\), but \(x_1\) is not in the ideal \(I\). In fact, by construction of \(I\), none of \(x_1, \ldots, x_n\) are in \(I\). However, \(x_1, \ldots, x_n \in \sqrt{I}\).

While on the topic of radical ideals, we will discuss a few properties of radicals of ideals:
Proposition 9.1. Let $k[x_1, \ldots, x_n]$ be a ring, and let $I$ be an ideal in $k[x_1, \ldots, x_n]$.

1. $\sqrt{I}$ is an ideal with $I \subset \sqrt{I}$.
2. If $I$ is maximal, then $I$ is radical.

Proof. (1) If $x, y \in \sqrt{I}$, then that means $x^n \in I$ for some $n \geq 1$ and $y^m \in I$ for some $m \geq 1$. We will show that $x + y \in \sqrt{I}$. Indeed,

$$(x+y)^{m+n-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} x^{m+n-1-i}y^i$$

where each monomial term either has a $x^n$ or $y^m$, and therefore each term in the sum is in $I$, and therefore $(x+y)^{m+n-1} \in I$, and therefore $x + y \in \sqrt{I}$. Also, if $x \in \sqrt{I}$, then for $x^m \in I$ for some $m \geq 1$, so $(rx)^m \in I$, and therefore $rx \in I$ for all $r \in k[x_1, \ldots, x_n]$. Hence, $\sqrt{I}$ is an ideal. Since $f^1 \in I$ for all $f \in I$, we have that also $f \in \sqrt{I}$, and hence $I \subset \sqrt{I}$.

(2) If $I$ is maximal, then $I$ is prime, and prime ideals are radical. Alternatively, if $I$ is maximal, since by (1) we have that $I \subset \sqrt{I}$, we have that either $\sqrt{I} = k[x_1, \ldots, x_n]$ or $\sqrt{I} = I$. The former can not happen since $1 \notin I$, and therefore $1 \notin \sqrt{I}$. Hence, $I = \sqrt{I}$.

Where do radical ideals and varieties have anything in common? Well, for any variety $V$, we show what the structure of $I(V)$ is.

Proposition 9.2. The ideal $I(V)$ is a radical ideal.

Proof. We know that $k[x_1, \ldots, x_n]$ is an integral domain, and therefore does not contain any zero divisors. Assume that $f^m \in I(V)$. Then, $f^m$ vanishes at any point in $V$. However, this means that $f$ must vanish at any point in $V$, and hence $f \in I(V)$.

What this proposition does is begin some sort of relation between varieties and ideals. We can go one direction:

Affine Variety $V \longrightarrow$ Radical Ideal $I(V)$

Do we then have a correspondence from ideals to varieties that are one-to-one? This is the strong version of the Hilbert Nullstellensatz:

Theorem (Strong Nullstellensatz). Let $k$ be an algebraically closed field and let $f, f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$. Then, $f \in I(V(f_1, \ldots, f_m))$, if and only if there exists $N \geq 1$ such that

$$f^N \in (f_1, \ldots, f_m).$$

Proof. This proof uses the Rabinowitsch “switch”. This “switch” introduces a new variable $y$. Consider the ideal $I' = (f_1, \ldots, f_m, 1 - yf) \subset k[x_1, \ldots, x_n, y]$. Will show that $V(I') = \emptyset$. Consider a point $(a_1, \ldots, a_n, a_{n+1}) \in k^{n-1}$. This is either a common root of $(f_1, \ldots, f_m)$ or not (where each $f_i$ is viewed as a polynomial in $n + 1$ variables which do not depend on the last variable). If it is a common root, then since $f \in I(V(f_1, \ldots, f_m))$ we have $f(a_1, \ldots, a_n) = 0$, and then $1 \in I'$, and therefore $V(I') = \emptyset$. If it is not a common root, then some $f_i$ does not vanish at $(a_1, \ldots, a_{n+1})$ and since this point is arbitrary, we see that no such point annihilates $f_i$, and therefore $V(I') = \emptyset$.

Now, we can apply the Weak Nullstellensatz. Since $V(I') = \emptyset$, we know that $1 \in I'$, and therefore we have the linear combination

$$1 = \sum_{i=1}^{m} A_i(x_1, \ldots, x_n, y)f_i + B(x_1, \ldots, x_n, y)(1 - yf)$$

32
for polynomials $A_i, B \in k[x_1, \ldots, x_n, y]$. Since $y$ is an indeterminate, set $y = \frac{1}{f(x_1, \ldots, x_n)}$ (the switch). Then, the equality above becomes

$$1 = \sum_{i=1}^{m} A_i(x_1, \ldots, x_n, \frac{1}{f}) f_i,$$

Next, clear the denominators by multiplying both sides by $f^N$, where $N$ is the least exponent that would clear the denominators. Hence, we have

$$f^N = \sum_{i=1}^{m} (f^N A_i(x_1, \ldots, x_n)) f_i,$$

and therefore, $f^N$ is a linear combination of elements in $(f_1, \ldots, f_m)$.

Now assume that $f^N \in (f_1, \ldots, f_m)$. That means that $f^N \in I(V(f_1, \ldots, f_m)$, and since we know that $I(V)$ is a radical ideal, we have that $f \in I(V(f_1, \ldots, f_m))$. □

Another way we could state this is as follows:

**Corollary 9.3 (Hilbert Nullstellensatz).** Let $k$ be an algebraically closed field. Then,

$$I(V(I)) = \sqrt{I}.$$

**Proof.** Let $I = (f_1, \ldots, f_m)$ (remember, it is always finite by the Hilbert Basissatz). It is clear that $\sqrt{I} \subset I(V(I))$, since, for any $f \in \sqrt{I}$, that means $f^N \in I$ for some $N \geq 1$, and since $f^N$ vanishes at any point of $V(I)$, $f$ also vanishes at that point, so $f \in I(V(I))$. The other inclusion follows from the Strong Nullstellensatz: If $f \in I(V(I))$, then by the strong Nullstellensatz, we have that $f^N \in (f_1, \ldots, f_m)$ for some $N \geq 1$. However, if $f^N \in I$, then $f \in \sqrt{I}$, and hence $\sqrt{I} = I(V(I))$. □

With these tools, we have a bijective correspondence between varieties and radical ideals when $k$ is algebraically closed, i.e.

Radical Ideals $I \longrightarrow V(I)$,

Affine Varieties $V \longrightarrow$ Radical Ideals $I(V)$

are left and right inverses of each others.

Now we have certain correspondences. We can relate varieties to radical ideals, and we also proved earlier that points in an affine space correspond to maximal ideals in $k[x_1, \ldots, x_n]$. Are there any other relationships we can make between certain ideals and certain varieties? In the next section, we begin discussing some of those relationships.

10. **Brief Introduction to Topological Spaces and the Zariski Topology**

We begin by defining the notion of a Topological space.

**Definition 10.1.** Let $X$ be any set, $\tau$ a collection of subsets of $X$. Then $\tau$ is said to be a topology on $X$ if the following three things are true:

1. $X$ and $\emptyset$ are elements of $\tau$.
2. For any collection of elements $G_i \in \tau$, $\cap_i G_i \in \tau$ for any index set $J$.
3. For any finite number of elements $C_j \in \tau$, $\cup_j C_j \in \tau$. 

33
A space equipped with a topology is called a topological space. The elements \( C \in \tau \) are called closed sets. The compliment of a closed set, denoted \( X - C \), is called an open set. In fact, most literature on topology uses open sets as the type of set to define topologies. One should investigate how the definition should change when one wants to use open sets. For our intent and purposes, it is enough to define it on closed sets with brief mentioning of open sets.

We remark that there are many properties of topology including many books written on the subject. We will not mention most of the subject, but a good book for starters is Topology By James Munkres.

**Example 10.1.** Consider the set \( \mathbb{R} \). Let \( \tau \) be the collection of all subsets of \( \mathbb{R} \). This is indeed a topology on \( \mathbb{R} \), called the discrete topology. If \( \tau \) consisted of just \( \mathbb{R} \) and \( \emptyset \), then this is also a topology on \( \mathbb{R} \) called the indiscrete topology.

Now we come back to our discussion of varieties. When we first discussed the ideal of a variety \( I(V) \), we don’t necessarily have to have a variety to get an ideal. Indeed,

**Definition 10.2.** Let \( k^n \) be an affine space and let \( S \) be any subset of \( k^n \). We define \( I(S) \) to be

\[
I(S) = \{ f \in k[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in S \}.
\]

**Proposition 10.1.** \( I(S) \) is an ideal.

**Proof.** Exercise. \(\square\)

**Lemma 10.1.** Let \( S \subset k^n \). Then, the variety \( V(I(S)) \) is the smallest affine variety containing the set \( S \). In other words, if \( V \) is a variety that contains \( S \), then \( V(I(S)) \subset V \).

**Proof.** First we check that \( S \subset V(I(S)) \). However, this is clear since \( I(S) \) is the set of all polynomials that vanish on \( S \), but it may there may be some more polynomials that vanish at other points other than \( S \) since \( S \) was not a variety to begin with. Now, we know that taking ideals is inclusion reversing, so, if \( S \subset V \), then \( I(V) \subset I(S) \). Now if we take varieties, that is again inclusion reversing, and we get \( V(I(S)) \subset V(I(V)) \). However, it is left as an exercise to show that if \( V \) is a variety then \( V(I(V)) = V \).

This leads us to the following:

**Definition 10.3.** Let \( k^n \) be an affine \( n \)-space and let \( S \subset k^n \). We define a Zariski Closure of \( S \), denoted \( \bar{S} \) to be the variety \( \bar{S} = V(I(S)) \). We call such a set \( \bar{S} \) a Zariski Closed set.

**Proposition 10.2.** Let \( k^n \) be an affine \( n \)-space. The collection \( \tau \) of Zariski Closed sets is a topology on \( k^n \).

**Proof.** Indeed, \( V(k^n) = \emptyset \) and \( V(0) = k^n \). We also proved earlier that if \( V = V(f_1, \ldots, f_m) \) and \( W = V(g_1, \ldots, g_t) \). Then \( V \cap W = V(f_1, \ldots, f_m, g_1, \ldots, g_t) \). Now, we begin with ideals \( I(S) = (f_1, \ldots, f_m) \) and \( I(R) = (g_1, \ldots, g_t) \) for arbitrary sets \( R, S \subset k^n \). One can show that the ideal \( I(S) + I(R) = (f_1, \ldots, f_m, g_1, \ldots, g_t) \). Hence, \( V(I(S)) \cap V(I(R)) = V(I(S) + I(R)) \), which is again a Zariski Closed set. This works with an arbitrary number of Zariski Closed sets.

Next, given \( V \) and \( W \) Zariski Closed, we need to show that \( V \cup W \) is also Zariski closed. We know from a previous exercise that \( V(f_1, \ldots, f_m) \cup V(g_1, \ldots, g_t) = V(\{f_ig_j \mid 1 \leq i \leq m, 1 \leq j \leq t\}) \). It will be left up to the student to show that \( V(I(R)) \cup V(I(S)) = V(I(R) \cdot I(S)) \). This works for finitely many unions of varieties. Hence, \( \tau \) is a topology. \(\square\)
The topology given above is known as the Zariski Topology.

Now, when we take unions or intersections of varieties, we ask if these correspond to any operations on ideals in \( k[x_1, \ldots, x_n] \). The answer is yes, and we will explore not just unions and intersections, but a whole medley of other operations.

11. Ideals and the Zariski Topology

For each of the following subsections, we will always assume that our polynomial ring is over an algebraically closed field.

11.1. Sums of Ideals. What happens when we take sums of ideals in polynomial rings over algebraically closed fields? We have already seen what happened when we take sums of ideals. Starting with two ideals \( I \) and \( J \), we see that the sum of \( I + J \) is the smallest ideal containing \( I \) and \( J \). One can also show that if \( I = (f_1, \ldots, f_m) \) and \( J = (g_1, \ldots, g_t) \), then \( I + J = (f_1, \ldots, f_m, g_1, \ldots, g_t) \).

Now, take the variety of \( I + J \). Then we see that \( V(I + J) = (f_1, \ldots, f_m, g_1, \ldots, g_t) = V(I) \cap V(J) \). So, continuing our correspondence, we see that

\[
\text{Sums of } I + J \rightarrow \text{Intersections } V(I) \cap V(J)
\]

Now, if we start with an intersection of varieties and consider ideals of those varieties, what do we get? Firstly, when we take ideals, we need that these ideals will be radical ideals, so by the Nullstellensatz (by our hypothesis earlier in the section, we are working over an algebraically closed field), we won’t have to worry about these maps not being one-to-one. We want \( I(V \cap W) = \sqrt{I(V) + I(W)} \).

We know by the Nullstellensatz that, if \( V = V(f_1, \ldots, f_m) \) and \( W = V(g_1, \ldots, g_t) \), we have \( I(V \cap W) = \sqrt{(f_1, \ldots, f_m, g_1, \ldots, g_t)} \). We show that \( \sqrt{(f_1, \ldots, f_m, g_1, \ldots, g_t)} = \sqrt{I(V) + I(W)} \).

To show \( \subset \), Assume that \( f \in \sqrt{(f_1, \ldots, f_m, g_1, \ldots, g_t)} \). Then, some power \( N \) of \( f \) is

\[
f^N = a_1f_1 + \ldots + a_mf_m + b_1g_1 + \ldots + b_tg_t,
\]

so that \( f^N \) is a sum of polynomials \( h + g \) where

\[
h = a_1f_1 + \ldots + a_mf_m \in I(V)
\]

and

\[
g = b_1g_1 + \ldots + b_tg_t \in I(W).
\]

Hence, \( f^N \in I(V) + I(W) \), and therefore \( f \in \sqrt{I(V) + I(W)} \). The other inclusion follows by repeating these steps in a backwards order.

Now, we have a correspondence:

\[
\text{Intersections } V \cap W \rightarrow \text{Sums } \sqrt{I(V) + I(W)}
\]

and the correspondence follows:

\[
\begin{array}{c c c}
\text{Sums of Ideals} & \text{Intersection of Varieties} \\
I + J & V(I) \cap V(J) \\
\sqrt{I(V) + I(W)} & V \cap W
\end{array}
\]
11.2. **Products of Ideals.** We recall that the product of two ideals $I$ and $J$ are defined to be

$$IJ = \left\{ \sum_{\text{finite}} f_i g_i \mid f_i \in I, g_i \in J \right\}$$

that is, the product of all finite sums of products of polynomials from $I$ and $J$. It was an exercise earlier to show that this is an ideal. Firstly, $0 \in IJ$ is true. If $f, g \in IJ$, then $f + g \in IJ$ since taking the sum of two finite sums is still finite. If $r \in k[x_1, \ldots, x_n]$ and $f \in IJ$, then $rf \in IJ$, since, when we multiply each term in the sum by $r$, each term is still in $I$ or $J$, and we still have a finite sum. Hence $IJ$ is an ideal.

Now that we have established that $IJ$ is an ideal, to what variety does it correspond? Beginning with $IJ$, what happens when we take $V(IJ)$? Well, $V(I) \subseteq V(IJ)$ since any point $(a_1, \ldots, a_n)$ which annihilates any $f \in I$ also annihilate any product $f \cdot g$ where $g \in k[x_1, \ldots, x_n]$, in particular, when $g \in J$. By that same logic, we have $V(J) \subseteq V(IJ)$, and therefore $V(I) \cup V(J) \subseteq V(IJ)$. Is it true that $V(IJ) \subseteq V(I) \cup V(J)$? Well, consider any $(a_1, \ldots, a_n) \in V(IJ)$. Then, for all pairs $f \cdot g \in IJ$, we must have that $f(a_1, \ldots, a_n) = 0$ or $g(a_1, \ldots, a_n) = 0$, which means that $(a_1, \ldots, a_n) \in V(I) \cup V(J)$. Hence, we have that $V(IJ) = V(I) \cup V(J)$, and we get a map.

**Products $IJ \longrightarrow$ Unions $V(I) \cup V(J)$**

Now, if we start with a union and take an ideal, what do we get? From an earlier proposition, we start with

$$V \cup W = V(\{f_i \cdot g_j \mid 1 \leq i \leq m, 1 \leq j \leq t\}).$$

Again, by the Nullstellensatz, we get that

$$I(V \cup W) = V(\{f_i g_j \mid 1 \leq i \leq m, 1 \leq j \leq t\}).$$

We can show that $\sqrt{\{f_i g_j \mid 1 \leq i \leq m, 1 \leq j \leq t\}} = I(V)I(W)$. However, this comes to, for some exponent $N$:

$$f \in \sqrt{\{f_i g_j \mid 1 \leq i \leq m, 1 \leq j \leq t\}} \Rightarrow f^N = f_{i_1} g_{j_1} + \ldots + f_{i_p} g_{j_p} = \sum_{\text{finite}} f_{i_j} g_j \text{ such that } f_i \in I(V), g_j \in I(W)$$

$$\Rightarrow f^N \in I(V)I(W)$$

$$\Rightarrow f \in I(V)I(W).$$

So now we have a correspondence:

**Products of Ideals** | **Union of Varieties**
---|---
$IJ$ | $V(I) \cup V(J)$
$\sqrt{I(V)I(W)}$ | $V \cup W$.

11.3. **Intersection of Ideals.** For ideals $I$, and $J$, what is the nature of the intersections $I \cap J$? Well, for one thing, this is an ideal. Indeed, $0 \in I$, $0 \in J$, so $0 \in I \cap J$. Next, if $x, y \in I \cap J$, then $x + y \in I$ and $x + y \in J$, so $x + y \in I \cap J$. The same logic goes for $rx$ for any $r \in k[x_1, \ldots, x_n]$ and $x \in I \cap J$. Therefore, $I \cap J$ is an ideal. To what variety does $I \cap J$ correspond? Well,

$$V(I \cap J) = \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I \cap J\}.$$
We also know that $IJ \subset I \cap J$, since each term $f_i g_j$ both lie in $I$ and $J$ since $I$ and $J$ are ideals (and equality happens when $I$ and $J$ are co-maximal; exercise). Since varieties are inclusion-reversing, we have that $V(I \cap J) \subset V(IJ)$. We already proved that $V(IJ) = V(I) \cup V(J)$. We will also show that $V(I \cap J) = V(I) \cup V(J)$. One inclusion has already been given. Now, the other inclusion goes as follows. Let $(a_1, \ldots, a_n) \in V(IJ)$. That means, for each product $f_i g_j$, we must have either $f_i(a_1, \ldots, a_n) = 0$ or $g_j(a_1, \ldots, a_n) = 0$. That means $(a_1, \ldots, a_n) \in V(I)$ or $(a_1, \ldots, a_n) \in V(J)$, and hence $(a_1, \ldots, a_n) \in V(I) \cup V(J)$. Therefore, $V(I \cap J) = V(I) \cup V(J)$.

Now starting with unions of varieties $V \cup W$, we want to take ideals $I(V \cup W)$. We will show that this is equal to $I(V) \cap I(W)$. First, we should note that both $I(V)$ and $I(W)$ are radical ideals (as we saw before). We will show that, in general, the intersection of radical ideals is a radical ideal:

\textbf{Proposition 11.1.} Let $I$ and $J$ be ideals (radical or not). Then, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

\textit{Proof.} First we show $\subseteq$. If $f \in \sqrt{I \cap J}$, then that means, for some power $N$, $f^N \in I$ and $f^N \in J$, and so $f^N \in I \cap J$, and therefore $f \in \sqrt{I \cap J}$. The reverse inclusion repeats the previous steps in a backwards order. \hfill $\Box$

Now, by the Nullstellensatz, $I(V \cup W) = \sqrt{I(V) \cap I(W)} = I(V) \cap I(W)$, by the previous proposition. As the book states, the intersection is easier to deal with than the product, since we don’t have to take radicals. For products, $IJ \subset \sqrt{IJ}$, for example, when $J = I$.

11.4. Colon Ideals. We recall the definition of a colon ideal:

\textbf{Definition 11.1.} Let $I$ and $J$ be ideals. The Colon Ideal, denoted $(I : J)$ is the set 

$$ (I : J) = \{ f \in k[x_1, \ldots, x_n] \mid J \in I \}. $$

\textbf{Proposition 11.2.} $(I : J)$ is an ideal.

\textit{Proof.} $0 \in (I : J)$ since $0 \cdot J = 0 \in I$. Next, if $x, y \in (I : J)$, then $xf \in I$ for any $f \in J$ and $yf \in I$ for any $f \in J$. Then, $x f + y f = (x + y) f \in I$ for any $f \in J$. Thus, $x + y \in (I : J)$. Now let $x \in (I : J)$ and $r \in k[x_1, \ldots, x_n]$. Then, $rx \in (I : J)$. Indeed, if $x \in (I : J)$, then $xf \in I$ for any $f \in J$. However, if $f \in J$, then $rf \in J$ since $J$ is an ideal, therefore $xf \in I$, and therefore $rx \in (I : J)$. \hfill $\Box$

\textbf{Example 11.1.} In the polynomial ring $\mathbb{R}[x, y]$, What is the colon ideal $(x, y) : (x)$? Well,

$$ ((x, y) : (x)) = \{ f \in \mathbb{R}[x, y] \mid f \cdot x \in (x, y) \} $$

$$ = \{ f \in \mathbb{R}[x, y] \mid f x = Ax + By \text{ for any } A, B \in \mathbb{R}[x, y] \} $$

$$ = \{ f \in \mathbb{R}[x, y] \mid f x = Ax \text{ and } B = 0 \} $$

$$ = \{ A \in \mathbb{R}[x, y] \} $$

$$ = \mathbb{R}[x, y]. $$

In fact, we have that, for any colon ideal $(I : J)$ in $k[x_1, \ldots, x_n]$, if $J \subset I$, then $(I : J) = k[x_1, \ldots, x_n]$. This is an exercise for students to prove (a one line proof).

Now, continuing with our theme, we ask about to which varieties colon ideals correspond? Well, what happens when we take $V((I : J))$? Well, continuing with our theme of going back to basis, we define what this set is:

$$ V((I : J)) = \{ (a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in (I : J) \}. $$
First, we note that if we tried to consider $V(I)$ as the corresponding ideal, then we have issues. To see this, we first note that $I \subset (I : J)$, since $IJ \subset I$, i.e., for any $a \in I$ and $b \in J$, $ab \in I$ by definition of ideals. However, this containment $I \subset (I : J)$ is strict in general (exercise). So we have $I \subset (I : J)$ $\Rightarrow$ $V((I : J)) \subset V(I)$.

The containment of varieties is also generally strict by that same proposition. The question is, which elements do we lose from $V(I)$? Well, consider some $f \in (I : J)$ and some $\bar{x} \in V(I) - V(J)$. Since $f \in (I : J)$, we have that $fg \in I$ for all $g \in J$. However, if we evaluate this product at $\bar{x}$, since $\bar{x} \in V(I)$ but $\bar{x} \notin J$, we have that some $g \in J$ does not vanish at $\bar{x}$. That means that $f(\bar{x}) = 0$ for all $V(I) - V(J)$. Hence, we have that $f \in I(V(I) - V(J))$. Now take varieties on both sides to get

$$V(I(V(I) - V(J))) \subset V((I : J)).$$

We have that $V((I : J)) \supset V(I) - V(J)$, where $V(I) - V(J)$ is the Zariski Closure of $V(I) - V(J)$.

Before continuing, we should note that the difference of two varieties is not necessarily a variety.

**Example 11.2.** Consider $V = V((x, y, z))$ and $W = V((z))$ in $\mathbb{R}^3$. The first variety is the set $\{(x, y, 0) \in \mathbb{R}^3 : (0, 0, z) \in \mathbb{R}^3 \}$ and the second is $\{(x, y, 0) \in \mathbb{R}^3 \}$. The difference of these two sets is $\{(0, 0, z) \in \mathbb{R}^3 : z \neq 0 \}$. This is not a variety. The Zariski closure of $V - W$ is the set $\{(0, 0, z) \in \mathbb{R}^3 \}$.

So, since the difference of two varieties is not necessarily a variety, we take the Zariski Closure to obtain a variety. So we have that $V(I) - V(J) \subset V((I : J))$.

Now, since we are over an algebraically closed field, we want to show that $V((I : J)) \subset V(I) - V(J)$. To show this, we need to have an extra requirement that $I$ is radical. Let $\bar{x} \in V((I : J))$. By the earlier logic, this means that, if $f \in (I : J)$, then $fg \in I$ for all $g \in J$, and then $f(\bar{x}) = 0$. The following is also true: if $f \in I(V(I) - V(J))$ and $g \in J$, then $f(\bar{x})g(\bar{x}) = 0$ for any $\bar{x} \in V(I)$, since $f$ is annihilated on $V(I) - V(J)$ and $g$ is annihilated by $V(J)$. By the Nullstellensatz, this means that $fg \in I$ (recall, $I$ is radical). Since, $fg \in I$ for all $g \in J$, we have that $f(\bar{x}) = 0$, and therefore $\bar{x} \in V(I(V(I) - V(J))$, and we have $V((I : J)) \subset V(I) - V(J)$, and therefore

$$V((I : J)) = \overline{V(I) - V(J)}.$$

Now given a Zariski closed set $\overline{V - W}$, we will show that it corresponds to the colon ideal $(I(V) : I(W))$. However, we have already shown the idea of these equalities from the previous paragraphs, and details will be left for the student. Hence, when $I$ is radical, we have a correspondence:

<table>
<thead>
<tr>
<th>Colon Ideals</th>
<th>Zariski Closure of the Difference of Varieties</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(I : J)$</td>
<td>$\overline{V(I) - V(J)}$</td>
</tr>
<tr>
<td>$(I(V) : I(W))$</td>
<td>$\overline{V - W}$</td>
</tr>
</tbody>
</table>

We have discussed, sums, products, intersections, and colon ideals. We have also seen a correspondence for maximal ideals. We need to consider one more type of ideal, prime ideals. For this, we need to introduce more terminology, like that of irreducible varieties.

### 12. Prime Ideals and Irreducible Varieties

**Definition 12.1.** Let $V \in k^n$ be an affine variety. $V$ is irreducible if, whenever we write $V = V_1 \cup V_2$, then either $V = V_1$ or $V = V_2$. In other words, $V$ is irreducible if it cannot be written as a union of two smaller varieties. Some literature has it so that affine varieties that are irreducible are called affine algebraic varieties.
Example 12.1. Let $V = (xy, zy)$. This variety is the set $V(xy, zy) = \{(0, y, 0) \in \mathbb{R}^3, (x, 0, z) \in \mathbb{R}^3\}$. We can write this as $V(xy, zy) = \{(0, y, 0)\} \cup \{(x, 0, z)\} = V((x, z)) \cup V((y))$. Hence, $V((xy, zy))$ is reducible, i.e., can be written as a union of two smaller varieties.

Now consider the variety $V((x, y))$. This variety corresponds to the $z$–axis. This variety is irreducible.

It is hard to pinpoint when varieties are irreducible. However, if we can find a correspondence between irreducible varieties and their algebraic counterparts, then we will be able to categorize irreducible varieties.

Lemma 12.1. Let $V \in k^n$ be an affine variety for a field $k$ (not necessarily algebraically closed). Then, $V$ is irreducible if and only if $I(V)$ is prime.

Proof. $(\Rightarrow)$ Assume that $V$ is irreducible, and assume that $f, g \notin I(V)$. Then, for any $\bar{x} \in V$, $f(\bar{x}) \neq 0$ and $g(\bar{x}) \neq 0$. Therefore, $f(\bar{x})g(\bar{x}) \neq 0$ since $k[x_1, \ldots, x_n]$ is an integral domain. Hence, $fg \notin I(V)$. Hence, $I(V)$ is a prime ideal.

Now assume that $I(V)$ is a prime ideal. That means, if $fg \in I(V)$ then either $f \in I(V)$ or $g \in I(V)$. Let $V = V_1 \cup V_2$. Assume that $V \neq V_1$. Then, we will show that $V = V_2$. Note that, if we can show that $I(V) = I(V_2)$, then it follows that $V = V_2$, since taking ideals or taking varieties are inclusion reversing. It is easy to see that $I(V) \subseteq I(V_1)$ since $V_2 \subseteq V$. To show the other way $I(V_2) \subseteq I(V)$, we start with the fact that $I(V) \subseteq I(V_1)$. Now choose $f \in I(V)$ such that $f \notin I(V_1)$, and choose $g \in I(V_2)$. Now, since $fg \in I(V = V_1 \cup V_2)$ (since $f$ and $g$ vanish on $V = V_1 \cup V_2$), we know that either $f \in I(V)$ or $g \in I(V)$. However, since $f \notin I(V)$, we see that $g \in I(V_2)$, and therefore $I(V) = I(V_2)$. Hence, $V$ is irreducible.

So if $k$ is algebraically closed, we have a correspondence:

Prime Ideals $\longleftrightarrow$ Irreducible Varieties.

All in all, we have the following correspondences:

<table>
<thead>
<tr>
<th>Sums of Ideals</th>
<th>Intersections of Varieties</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I + J$</td>
<td>$V(I) \cap V(J)$</td>
</tr>
<tr>
<td>$\sqrt{I(V) + I(W)}$</td>
<td>$V \cap W$</td>
</tr>
<tr>
<td>Products of Ideals</td>
<td>Union of Varieties</td>
</tr>
<tr>
<td>$IJ$</td>
<td>$V(I) \cup V(J)$</td>
</tr>
<tr>
<td>$\sqrt{I(V)I(W)}$</td>
<td>$V \cup W$</td>
</tr>
<tr>
<td>Colon Ideals</td>
<td>Zariski Closure of Differences of Varieties</td>
</tr>
<tr>
<td>$(I : J)$</td>
<td>$\overline{V(I)} - V(J)$</td>
</tr>
<tr>
<td>$(I(V) : I(W))$</td>
<td>$\overline{V} - W$</td>
</tr>
<tr>
<td>Maximal Ideals</td>
<td>Points in $k^n$</td>
</tr>
<tr>
<td>Prime Ideals</td>
<td>Irreducible Varieties</td>
</tr>
</tbody>
</table>

Thus, we end the ideal-variety correspondence.
13. More on Zariski Topology and Commutative Algebra

We have discussed the Zariski Topology when we were in the polynomial ring \( k[x_1, \ldots, x_n] \). However, we ask whether or not the Zariski Topology is applicable to other structures. We recall the definition of a commutative ring with unity:

**Definition 13.1.** A commutative ring with unity is a ring \( R \) such that \( 1 \in R \) and \( ab = ba \) for all \( a, b \in R \).

Ideals of a ring \( R \) is defined as the same as that of \( k[x_1, \ldots, x_n] \), namely, \( I \) is an ideal of \( R \) if \( I \) is a subgroup of \( R \) and \( rx \in I \) for any \( x \in I \) and \( r \in R \). Let \( X \) be the set of all prime ideals of a ring \( R \) (we will assume that \( R \) is a commutative ring with unity in this section). For each subset \( E \) of \( A \), denote by \( Z(E) \) the set of all prime ideals in \( R \) that contain \( E \). We will show that these are the closed sets that form a topology on \( X \), called the Zariski Topology.

**Theorem.** Let \( R \) be a ring, and let \( X \) be the set of all prime ideals in \( R \). The prime ideals \( Z(E) \) form the closed sets of a topology \( \tau \) on \( X \).

**Proof.** We need to check four items:

1. We need to show that \( X \in \tau \). Well, consider the singleton set \( \{0\} \subset R \). Then, since 0 is in every prime ideal, we see that \( \mathbb{Z}(0) = X \).

2. Next, we want to show that \( \emptyset \in \tau \). Well, consider the subset \( \{1\} \subset R \). Since no prime ideal contains one (since, by definition, prime ideals are proper), we see that \( \mathbb{Z}(1) = \emptyset \).

3. Next, if \( E_i \) is a family of subsets of \( R \) (for some index set \( I \)), then we set

   \[
   \bigcap_{i \in I} Z(E_i) = Z\left(\bigcup_{i \in I} E_i\right),
   \]

   thus, the intersection of closed sets is contained in \( \tau \). Indeed, let \( P \in \bigcap_{i \in I} Z(E_i) \). Then, \( P \) contains each \( E_i \), and since \( P \) contains each \( E_i \), \( P \) contains the union \( \bigcup_{i \in I} E_i \), and therefore \( P \in Z\left(\bigcup_{i \in I} E_i\right) \), thus \( \bigcap_{i \in I} Z(E_i) \subset Z\left(\bigcup_{i \in I} E_i\right) \). Now let \( P \in Z\left(\bigcup_{i \in I} E_i\right) \). Then, each \( E_i \subset P \), and therefore, \( P \in \cap_{i \in I} Z(E_i) \). Thus we have proved the equality, and therefore the intersection of closed sets is a closed set.

4. Finally, we need to show that \( Z(E \cap F) = Z(E) \cup Z(F) \). Indeed, let \( P \in Z(E) \cup Z(F) \). That means either \( E \subset P \) or \( F \subset P \). Assume that \( E \subset P \). Since \( E \cap F \subset E \subset P \), we have that \( P \in Z(E \cap F) \). Thus, \( Z(E) \cup Z(F) \subset Z(E \cap F) \). Now assume \( P \in Z(E \cap F) \).

**Proposition 13.1.** \( Z(E) = Z(J) \) where \( J = (E) \).

**Proof.** Since \( E \subset J \), it is clear that \( Z(J) \subset Z(E) \). Now suppose that \( P \in Z(E) \). That means that \( E \subset P \). Since \( (E) \) is the set \( \{RE\} \), each of these are contained in \( P \) since \( P \) is a prime ideal. Hence, \( J \subset P \), and \( Z(E) \subset Z(J) \).

So now if we can show that \( Z((E) \cap (F)) \subset Z((E) \cup Z((F)) \), then we are done. Since \( P \in Z((E) \cap (F)) \), that means that \( (E) \cap (F) \subset P \). However, one can show that this means that either \( (E) \subset P \) or \( (F) \subset P \), and therefore \( P \in Z((E) \cup Z((F)) \). Hence \( Z(E \cap F) = Z(E) \cup Z(F) \). Thus, the union of two closed sets is closed. Thus, \( \tau \) is a topology.

**Definition 13.2.** The set \( X \) of prime ideals in \( R \) is called the prime spectrum of \( R \), and it is denoted \( \text{Spec}(R) \).
Example 13.1. Consider the ring $\mathbb{Z}$. What is $\text{Spec}(\mathbb{Z})$? Well, as we know, the only prime ideals of $\mathbb{Z}$ are the ideals generated by prime numbers. For example, given the ideal $(4) \subset \mathbb{Z}$. The closed set $\mathbb{Z}((4))$ is the prime ideal $(2)$. The set $\mathbb{Z}((30))$ are the primes ideals $(2), (3), (5)$.

Now consider the ring $\mathbb{R}$. The only ideals are $(0)$ and $\mathbb{R}$. Therefore, $\text{Spec}(\mathbb{R}) = (0)$.

One last example, what is $\text{Spec}(\mathbb{R}[x])$? We know from earlier algebra courses that $\mathbb{R}[x]$ is a principal ideal domain, that is, each ideal is finitely generated. We also know that in principal ideal domains that irreducible polynomials generate prime ideals. Hence, $\text{Spec}(\mathbb{R}[x]) = \{(f) \mid f \text{ is irreducible}\}$.

Now we connect topology with certain algebraic structures. We have special relations when we talk about multivariate polynomial rings over algebraically closed fields (which is part of the study of algebraic geometry). One can also discuss irreducible prime spectra, and you can also talk about morphisms (a special type of map) of rings and how it relates to morphisms of topological spaces (called contravariant functors in this case).

A subset of the prime spectrum (actually, a subspace) is the maximal spectrum, denoted $\text{Max}(R)$. This is the set of all maximal ideals in $R$. As we know, since each maximal ideal is prime, the maximal spectrum is a subset of the prime spectrum. There is lots of literature on these topics, including Algebra by Serge Lang and Abstract Algebra by Dummit and Foote for a more general introduction and further study.

14. INTRODUCTION TO DIFFERENTIAL ALGEBRA

We now delve into the subject of Differential Algebra. This area has many similarities with the course material we have discussed until now, but with the addition of a derivation, there are subtle changes that require different conditions for theorems like Noetherianity, the Hilbert Basissatz, and The Hilbert Nullstellensatz. Analog of these ideas will be presented in a differential setting. We begin with the definition of a derivation and a differential ring:

Definition 14.1. Let $R$ be a commutative ring with unity. A derivation $\partial$ is a map $\partial : R \rightarrow R$ satisfying:

1. For all $a, b \in R$, $\partial(a+b) = \partial(a) + \partial(b)$, and
2. For all $a, b \in R$, $\partial(ab) = \partial(a)b + a\partial(b)$ (this is the so called product rule or Leibniz rule one encounters in calculus).

Definition 14.2. Let $R$ be a commutative ring with unity equipped with a set $\Delta = \{\partial_1, \ldots, \partial_m\}$. $R$ is a differential ring if $\Delta$ is a commuting set of derivations. Two derivations are said to commute if $\partial_1 \circ \partial_2 = \partial_2 \circ \partial_1$. $R, \Delta$ is a differential field if $R$ is a field. Such differential fields will be denoted $K, \Delta$ (uppercase $K$, as opposed to the lower case $k$ that we have been using earlier).

Example 14.1. Let $R$ be a commutative ring with $1$, $\Delta = \{\partial\}$. $R$ is a differential ring if we define $\partial(r) = 0$ for all $r \in R$. All properties of a differential ring are then trivially satisfied.

Example 14.2. Let $R = \mathbb{Z}$. What are the possible derivations?

To begin, notice that $\partial(n)$ is determined by $\partial(1)$ (or $\partial(-1)$) using additivity. Indeed, for $n \geq 1$,

$$\partial(n) = \partial(1 + 1 + \ldots + 1) = \partial(1) + \ldots + \partial(1) = n\partial(1)$$

$$\text{n times} \quad \text{n times}$$

### Example 14.1.

A derivation $\partial$ is a map $\partial : R \rightarrow R$ satisfying:

1. For all $a, b \in R$, $\partial(a+b) = \partial(a) + \partial(b)$, and
2. For all $a, b \in R$, $\partial(ab) = \partial(a)b + a\partial(b)$ (this is the so called product rule or Leibniz rule one encounters in calculus).

### Definition 14.2.

A differential ring is a commutative ring $R$ equipped with a set $\Delta = \{\partial_1, \ldots, \partial_m\}$. $R$ is a differential ring if $\Delta$ is a commuting set of derivations. Two derivations are said to commute if $\partial_1 \circ \partial_2 = \partial_2 \circ \partial_1$. $R, \Delta$ is a differential field if $R$ is a field. Such differential fields will be denoted $K, \Delta$ (uppercase $K$, as opposed to the lower case $k$ that we have been using earlier).

### Example 14.1.

A differential ring is a commutative ring with $1$, $\Delta = \{\partial\}$. $R$ is a differential ring if we define $\partial(r) = 0$ for all $r \in R$. All properties of a differential ring are then trivially satisfied.

### Example 14.2.

A differential ring is a commutative ring $R = \mathbb{Z}$, $\Delta = \{\partial\}$. What are the possible derivations?

To begin, notice that $\partial(n)$ is determined by $\partial(1)$ (or $\partial(-1)$) using additivity. Indeed, for $n \geq 1$,

$$\partial(n) = \partial(1 + 1 + \ldots + 1) = \partial(1) + \ldots + \partial(1) = n\partial(1)$$

$$\text{n times} \quad \text{n times}$$
(similarly, we have for \( n \geq 1 \), \( \partial(-n) = \partial((-1) + \ldots + (-1)) = n\partial(-1) \)).

When \( n = 0 \), we have \( \partial(0) = \partial(0+0) = \partial(0) + \partial(0) \), and we see that \( \partial(0) = 0 \). For \( n = -1 \), we have
\[
\partial(-1) = \partial(1 \cdot (-1)) = \partial(1) \cdot (-1) + 1 \cdot \partial(-1),
\]
Subtracting \( \partial(-1) \) we see that \( 0 = (-1)\partial(1) \), and therefore \( \partial(1) = 0 \). We can also easily show that \( \partial(-1) = 0 \). Indeed,
\[
0 = \partial(1) = \partial((-1)(-1)) = \partial(-1)(-1) + (-1)\partial(-1) = -2\partial(-1),
\]
so \( \partial(-1) = 0 \). This shows that the only derivation that exists for \( \mathbb{Z} \) is the trivial one.

**Example 14.3.** Let \( R = \mathbb{Q} \). Take the element \( \frac{1}{b} \) where \( b \neq 0 \in \mathbb{Z} \). We have
\[
0 = \partial(1) = \partial(b \cdot 1/b) = \partial(b) \cdot 1/b + b \cdot \partial(1/b),
\]
and continuing further we get \( \partial(\frac{1}{b}) = -\frac{\partial(b)}{b^2} \).

This calculation shows, in fact, how to determine the derivative an element \( a \) of any differential ring, provided the inverse of \( a \) exists.

More generally, given any \( a \neq 0 \in \mathbb{Z} \), we can compute \( \partial(\frac{a}{b}) \) where \( b \) is taking as above. Namely, we get
\[
\partial(a/b) = \partial(a \cdot 1/b),
\]
and using the Leibniz rule, we get
\[
\partial(a \cdot 1/b) = \partial(a) \cdot 1/b + a \cdot \partial(1/b) = \frac{\partial(a)}{b} - \frac{a \partial(b)}{b^2} = \frac{\partial(a)b - a\partial(b)}{b^2}.
\]
Combining this result with that fact that both \( a \) and \( b \) are integers, the following occurs:
\[
\partial(a/b) = \frac{\partial(a)b - a\partial(b)}{b^2} = \frac{0 \cdot b - a \cdot 0}{b^2} = 0,
\]
and we see that \( \mathbb{Q} \) only has trivial derivations.

For rings with one derivation, we will use the notation \( \Delta = \{ \delta \} \) for the single derivation. Such rings are called *Ordinary Differential Rings* (in such differential rings, we may use the notation \( a' = \delta(a) \) since no confusion will occur). If \( \Delta \) has more than one derivation, then \( R, \Delta \) is called a *Partial Differential Ring*.

**Example 14.4.** We now present an example that should look familiar to students. Consider the ring \( \mathbb{Q}[x] \) with derivation \( \delta = \frac{d}{dx} \). That is, \( \delta(x) = 1 \). This satisfies the axioms of a derivation, and therefore, \( \mathbb{Q}[x], \Delta \) is a differential ring. First we leave as an exercise to show how the definition of derivation satisfies the power rule and constant rule, that is, \( \delta(x^n) = nx^{n-1} \) and \( \delta(cx^n) = c\delta(x^n) \). In general, if \( \delta(x) = f \) for some \( f \in \mathbb{Q}[x] \), then, because of the chain rule, the power rule and constant rule become
\[
\delta(x^n) = nx^{n-1}\delta(x) = nx^{n-1} \cdot f
\]
and
\[
\delta(cx^n) = cnx^{n-1} \cdot f.
\]
To check that \( \delta(x) = 1 \) turns \( \mathbb{Q}[x] \) into a differential field will be left to the student.

**Definition 14.3.** Let \( R, \Delta \) be a differential ring. A subset \( I \subseteq R, \Delta \) is a differential ideal if \( I \) is an ideal and for all \( a \in I, \partial_i(a) \in I \) for all \( \partial_i \in \Delta \). Differential ideals are usually denoted \([I]\).

**Example 14.5.** Consider \( K[x] \) with derivation \( \delta(x) = 1 \) and \( K \) a differential field. We claim that the only ideals in \( K[x] \) are trivial. Indeed, as we saw in the previous example, for any polynomial \( f \in K[x] \), we see that \( \delta(f) \) decreases in degree by one. Indeed, if \( \deg(f) = n \), then \( \deg(f) = n - 1 \). For any polynomial \( f \in [I] \subseteq K[x], \delta(f) \in [I] \). However, \( \delta^n(f) \) is a constant, and from earlier, whenever \( 1 \in I \), then \( I \) becomes the whole ring. Therefore, \([I] = K[x] \) or \([I] = (0) \).

Whenever we talk about ideals, we want to talk about generating sets, that is, given any set \( S \subseteq R, \Delta \), can we find the smallest differential ideal that contains \( S \)?

**Definition 14.4.** If \( S \subseteq (R, \Delta) \), then \([S]\) denotes the smallest differential ideal of \((R, \Delta)\) that contains \( S \); it is the intersection of all differential ideals containing \( S \).

In other words, \([S]\) is the ideal of \((R, \Delta)\) generated by \( \theta(S), \theta \in \Theta \) where

\[
\Theta = \{ \partial_1^{i_1} \partial_2^{i_2} \cdots \partial_n^{i_n} | i_1, \ldots, i_n \geq 0 \}.
\]

In particular, we see that \((S) \subseteq [S]\) by letting all \( i_r = 0 \).

15. Ritt-Noetherian Rings, Radical Differential Ideals, and the Ritt-Raudenbush Theorem

The natural question now to ask is the analog of the Hilbert Basissatz, namely, given any differential ideal \([I]\), is there a finite generating set for \( I \)? Sadly, in our case, this does not hold for differential ideals. We will define an important ring in differential algebra, and show that in this ring, there are differential ideals that do not have finite generating sets:

**Definition 15.1.** Let \( K, \Delta \) be a differential field. The Ring of Differential Polynomials with indeterminates \( y_1, \ldots, y_n \) is the ring of polynomials

\[
K[\theta y_i | \theta \in \Theta, 1 \leq i \leq n]
\]
denoted \( K\{y_1, \ldots, y_n\} \).

**Example 15.1.** The ring \( K\{y\} \), that is, the ordinary case, is the ring

\[
K[y, y', y'', y''', y^{(4)}, \ldots],
\]

that is, the ring in infinite polynomials over \( K \).

The above definition is the analog to the definition of \( k[x_1, \ldots, x_n] \), whereas the former polynomial ring discusses regual polynomials with multivariate indeterminates, the latter ring of differential polynomials discusses differential polynomials (a prelude to the study of differential equations) in multivariables (i.e., ordinary/partial differential equations). Please note that trigonometric functions such as \( \sin \) will not be considered in this course (or most differential algebra courses for that matter).

**Example 15.2.** In every ordinary differential field \((K, \{\delta\})\), where \( \mathbb{Q} \subseteq K \),

\[
[y^2] \subset [y^2, (\delta y)^2] \subset \ldots \subset \left[y^2, (\delta y)^2, \ldots, (\delta^n y)^2\right] \subset \ldots
\]
does not stabilize in $K\{y\}$. We will show later that, just as in Noetherian rings, this means that there is no finite generating set for the union of these ideals. However, as we will see soon, there is a type of ideal in differential structures in which a chain like this stabilizes.

**Definition 15.2.** An ideal $I \subset (R, \Delta)$ is called a **radical differential ideal** if:

1. $I$ is a differential ideal, and
2. $I$ is a radical ideal.

For a subset $S \subset R$, $\{S\}$ denotes the smallest radical differential ideal containing $S$. One also says that $S$ generates the radical differential ideal $\{S\}$. It will be clear in which context $\{\}$ will denote a radical differential ideal.

**Theorem 15.1.** Let $(R, \Delta)$ be a differential ring, $Q \subset R$, and let $I \subset (R, \Delta)$ be a differential ideal. Then, $\sqrt{I}$ is a radical differential ideal.

**Proof.** In order to prove this, we first state and prove a proposition:

**Proposition 15.1.** Let $I \subset (R, \Delta)$ be a differential ideal and let $Q \subset R$. Let $a \in R$ such that $a^n \in I$. Then, $(\partial(a))^{2n-1} \in I$.

**Proof.** By induction, we will show that, for all $k$, $1 \leq k \leq n$, we have

$$(\star) \quad a^{n-k} \partial(a)^{2k-1} \in I,$$

and the proposition will follow by allowing $k = n$. Continuing with the Lemma:

If $k = 1$, then

$$a^{n-1} \partial(a) \in I.$$

Indeed,

$$\partial(a^n) = na^{n-1} \partial(a).$$

Since $Q \subset R$, we divide by $n$ and it follows that $a^{n-1} \partial(a) \in I$.

Now for the inductive step. Assume that $(\star)$ holds. We want to show that

$$(\star\star) \quad a^{n-(k+1)} (\partial(a))^{2k+1} \in I.$$

Applying $\partial$ to $(\star)$, we obtain:

$$(n-k)a^{n-k-1} \partial(a)^{2k} + a^{n-k}(2k-1) \partial(a)^{2k-2} \partial(\partial(a)) \in I.$$

Multiply the above by $\partial(a)$ to obtain $(\star\star)$, and we are done.

Back to the theorem, we see that by applying proposition, the theorem follows.

**Definition 15.3.** Let $R, \Delta$ be any differential ring. $R, \Delta$ is **Ritt-Noetherian** if the set of all radical differential ideals satisfies the ascending chain condition.

One can show that the ascending chain condition is equivalent to each ideal having a finite generating set, so the above definition becomes,

**Definition 15.4.** $R, \Delta$ is **Ritt-Noetherian** if each radical differential ideal $\{I\} \in R, \Delta$ is finitely generated.
Emmy Noether, as stated before was a German born Mathematician. Joseph Fels Ritt was an American born Mathematician (1893-1951) who received his doctorate from Columbia University and eventually became department chair. He worked as a Mathematician during World War II and helped the war efforts. He was one of the first mathematicians to introduce the notion of differential rings. He was also advisor to Dr. Ellis Kolchin who really solidified the branch of Differential Algebra. In fact, there is a weekly seminar at the Graduate Center, City University of New York that was named after Kolchin, called the Kolchin Seminar for Differential Algebra.

Example 15.3. The previous example stated that
\[ y^2 \subset (\delta y)^2 \subset (\delta^2 y)^2 \subset \ldots \]
in \( K\{y \} \) does not stabilize. However, if we replace \([\] \) by \({}\), then we see that this chain stabilizes with the first ideal, namely, the chain
\[ \{y^2\} \subset \{(\delta y)^2\} \subset \{(y^2, (\delta y)^2, (\delta^2 y)^2)\} \subset \ldots \]
stabilizes with just \( \{y^2\} \), since \( y \in \{y^2\} \), and each \( \delta^p y \in \{y^2\} \).

Now, the analog of the Hilbert Basissatz goes as follows:

Theorem (Ritt-Raudenbush). Let \( K, \Delta \) be a differential field with \( Q \in K \). Then, the ring of differential polynomials \( K\{y_1, \ldots, y_n\} \) satisfies the ascending chain condition on radical differential ideals. Equivalently, the differential ring \( K\{y_1, \ldots, y_n\} \) is Ritt-Noetherian when \( Q \subset K \).

The proof will not be stated. However, a proof can be found in *An Introduction to Differential Algebra* by Irving Kaplansky, or by consulting the references below.

16. Characteristic Sets

In the previous section, we stated a theorem that each radical differential ideal has a finite generating set, but is there a *best* finite generating set? This is in analogy to Groebner Basis studied earlier. A good generating set may be given by finding characteristic sets. However, just as with Groebner basis, we need to define some sort of ordering on differential polynomials.

Definition 16.1. let \( Y = y_1, \ldots, y_n \) and \( \Delta = \partial_1, \ldots, \partial_m \). Recall that \( \Theta = \{ \theta \mid \theta = \partial_1^{i_1}, \ldots, \partial_m^{i_m} \} \) (here, \( {} \) denotes set notation). A differential ranking on \( \Theta Y \) is a well-ordering on \( \Theta Y \) (i.e., a total ordering where every non-empty subset has the smallest element) such that:

1. for all \( u, v \in \Theta Y \) and \( \theta \in \Theta \),
   
   \[ \text{if } u < v, \text{ then } \theta u < \theta v. \]

2. For all \( \theta \neq id \),
   
   \[ u < \theta u. \]

Example 16.1. We present a few examples, and review some orderings orderings from earlier in the course:

1. Let \( Y = y \) and \( \Delta = \delta \). The set
   
   \[ \Theta Y = y, \delta y, \delta^2 y, \ldots, \delta^p y, \ldots \]
   
   has a unique ranking
   
   \[ y < \delta y < \delta^2 y < \ldots < \delta^p y < \ldots \]
(2) Let \( Y = y \) and \( \Delta = \partial_1, \partial_2 \). Note that, for any ordering, we have:
\[
y < \partial_1 y < \partial_1 \partial_2 y,
\]
but we also have
\[
y < \partial_2 y < \partial_1 \partial_2 y.
\]
How do we compare \( \partial_1 y \) to \( \partial_2 y \)?

(3) Let \( \prec_{\text{lex}} \) be the lexicographic ordering on \( i_1, i_2 \) for \( i_1, i_2 \geq 0 \) (examples include \((0, 100) \prec_{\text{lex}} (1, 2)\) and \((2, 1) \prec_{\text{lex}} (2, 2)\)). We can let
\[
\partial_1^{i_1} \partial_2^{i_2} y < \partial_1^{j_1} \partial_2^{j_2} y \iff (i_1, i_2) \prec_{\text{lex}} (j_1, j_2).
\]

(4) We could also use the graded lexicographic ordering (grlex) defined as follows:
\[
(i_1, i_2) \prec_{\text{deglex}} (j_1, j_2) \iff \text{either } i_1 + i_2 < j_1 + j_2 \\
\text{else } i_1 + i_2 = j_1 + j_2 \text{ and } (i_1, i_2) \prec_{\text{lex}} (j_1, j_2).
\]

Now that we have rankings on \( \Theta Y \), we begin to discuss the analog of the division algorithm of Commutative Algebra. Let \( K \) be a differential field.

**Definition 16.2.** Let \( f \in K\{y_1, \ldots, y_n\} \). The variable \( \partial_1^{i_1} \cdots \partial_m^{i_m} y_j \) in \( f \) of the greatest rank is called the leader of \( f \), denoted \( u_f \).

**Example 16.2.** For \( \Delta = \{\delta\} \) and \( K\{y\} \), consider \( f = (y')^2 + y + 1 \in K\{y\} \). We see that \( u_f = y' \).

Given a polynomial \( f \in K\{y_1, \ldots, y_n\} \), once we determine \( u_f \), we write \( f \) as a univariate polynomial in \( u_f \) as follows:
\[
(\star) \quad f = a_p u_f^p + a_{p-1} u_f^{p-1} + \cdots + a_0, \quad a_i \in K\{y_1, \ldots, y_n\}.
\]

**Example 16.3.** Let \( K\{y\} \) be an ordinary differential polynomial ring, and let \( f = y \cdot y'' + 1 \in K\{y\} \). We have \( u_f = y'' \) and therefore \( a_1 = y \), \( a_0 = 1 \).

**Definition 16.3.** In \((\star)\) above, the coefficient \( a_p \) is called the initial of \( f \), and is denoted by \( I_f \).

**Example 16.4.** Consider \( f = (y')^2 + y \in K\{y\} \) (here, \( \Delta = \{\delta\}) \). We see that \( u_f = y', I_f = 1 \). Apply \( \delta \) to \( f \):
\[
\delta((y')^2 + y) = 2y'y'' + y',
\]
and call \( 2y'y'' + y' = g \). We then have \( u_g = y'' \) and \( I_g = 2y' \).

Note that in Example 2.9, \( 2y' = \frac{\partial((y')^2 + y)}{\partial y} \) with \( \deg_{u_f}(\delta f) = 1 \).

**Definition 16.4.** \( \frac{\partial f}{\partial u_f} \) is called the seperant of \( f \), denoted \( S_f \).

**Example 16.5.** In Example 2.9, \( S(y')^2 + y = 2y' \).

For the following, let \( K \) be a differential field, \( R = K\{y_1, \ldots, y_n\} \) be a differential polynomial ring, and let a ranking on \( \Theta Y \) be fixed (unless otherwise noted).

**Definition 16.5.** For all \( f, g \in R \), we say that \( f \) is partially reduced with respect to \( g \) if none of the terms in \( f \) contains a proper derivative of \( u_g \).

**Example 16.6.** (1) Let \( f = y^2 \) and \( g = y + 1 \). Here, \( u_g = y \) and we see that \( f \) is partially reduced with respect to \( g \).
(2) Let \( f = y^2 + y' \) and \( g = y + 1 \). \( u_g \) is the same as before, but \( f \) is not partially reduced with respect to \( g \), since the term \( y' \) in \( f \) can be obtained by applying \( \delta \) to \( u_g \).

(3) Let \( f = 2yy'' + y \) and \( g = y + 1 \). Since \( 2yy'' \) in \( f \) is divisible by a proper derivative of \( u_g \), we see that \( f \) is not partially reduced with respect to \( g \).

**Definition 16.6.** We say that \( f \) is *reduced* with respect to \( g \) if

(i) \( f \) is partially reduced with respect to \( g \), and

(ii) if \( u_f = u_g \), then \( \deg_{u_f}(f) < \deg_{u_g}(g) \).

**Example 16.7.** Let \( f = y \) and \( g = y + 1 \). \( f \) is not reduced with respect to \( g \), since (ii) above is not satisfied.

**Definition 16.7.** A subset \( \mathcal{A} \subset R \) is called *autoreduced* if, for all \( f, g \in \mathcal{A} \) where \( f \neq g \), \( f \) is reduced with respect to \( g \).

**Example 16.8.** Let \( \mathcal{A} = 2yy'' + y, y + 1 \). This is not autoreduced (see Example 2.11(3)).

Let \( \mathcal{A} \) and \( \mathcal{B} \) be autoreduced. Let \( \mathcal{A} = A_1, \ldots, A_p \) and \( \mathcal{B} = B_1, \ldots, B_q \) with \( A_1 < \ldots < A_p \) and \( B_1 < \ldots < B_q \) for some ranking \( < \), where we say that \( f > g \) if \( u_f > u_g \), else if \( u_f = u_g \) then \( \deg_{u_f}(f) > \deg_{u_g}(g) \).

We say that \( \mathcal{A} \subset \mathcal{B} \) if:

1. there exists \( i, 1 \leq i \leq p \) such that, for all \( j, 1 \leq j \leq i - 1, \neg(B_j < A_j) \) and \( A_i < B_i \). Else,
2. \( q < p \) and \( \neg(B_j < A_j) \), \( 1 \leq j \leq q \).

**Example 16.9.** Let \( R = K\{y_1, y_2\} \) with \( \Delta = \{\delta\} \) with any deglex ranking. Let
\[
\mathcal{A} = \{A_1 = (y_2')^2 + 1, A_2 = y_1'' + y_2\} \quad \text{and} \quad \mathcal{B} = \{B_1 = (y_2') + 2\}.
\]
Is \( \mathcal{A} \subset \mathcal{B} \)? Starting with 1, we compare \( A_1 \) to \( B_1 \), and we see that \( B_1 < A_1 \), so we have \( \mathcal{B} \subset \mathcal{A} \).

Now, consider
\[
\tilde{\mathcal{B}} = \{\tilde{B}_1 = (y')^2 + 1\},
\]
and compare \( \mathcal{A} \) with \( \tilde{\mathcal{B}} \). Since \( \neg(\tilde{B}_1 < A_1) \), we have \( \mathcal{A} \subset \tilde{\mathcal{B}} \).

**Example 16.10.**

1. Let \( f = y_1 \) and \( \mathcal{A} = A_1 = y_2 \cdot y_1 \). Here, \( u_{A_1} = y_1 \), \( I_{A_1} = y_2 \), and we have \( g = 0 \), so \( I_A \cdot f - 0 \in [\mathcal{A}] \).

2. Let \( f = y_1' + 1 \) and \( \mathcal{A} = A_1 = y_2y_1^2 \). Again we have \( u_{A_1} = y_1 \). Differentiate \( A_1 \):
\[
A_1' = 2y_2y_1y_1' + y_2^2(y_1'),
\]
and we get \( S_{A_1} \cdot f - A_1' = 2y_2y_1 - y_2' y_1^2 \). Multiply through by \( I_{A_1} \) to get
\[
I_{A_1} \cdot S_{A_1} \cdot f - I_{A_1} \cdot A_1' = 2y_2^2y_1 - y_2' y_2(1)^2.
\]

Finally, we get
\[
I_{A_1} \cdot S_{A_1} \cdot f - 2y_2^2y_1 = y_2^2A + I_{A_1} \cdot A_1' \in [\mathcal{A}].
\]

**Definition 16.8.** Let \( I \subset R \) be a differential ideal. A minimal, autoreduced subset of \( I \) is called a *characteristic set* of \( I \).
17. Differential Nullstellensatz

We saw earlier that solutions (or lack thereof) to systems of polynomials in polynomials over a field could be determined when we added the restriction that the base field \( k \) be algebraically closed; this was the Hilbert Nullstellensatz. Now we turn to the differential case: given a system \( F \in K\{y_1,\ldots,y_n\} \) of differential polynomials in a ring of differential polynomials over a field, what restrictions do we need to put in place in order to ensure that we could get results?

**Definition 17.1.** A differential field \( K, \Delta \) is **differentially closed** if it is existentially closed, meaning, for all \( F \in K\{y_1,\ldots,y_n\} \), if there exists a bigger differential field \( L \supset K \) and \( (a_1,\ldots,a_n) \in L^n \) such that \( F(a_1,\ldots,a_n) = 0 \), then there already exist \( (b_1,\ldots,b_n) \in K^n \) such that \( F(b_1,\ldots,b_n) = 0 \).

**Theorem** (Differential Nullstellensatz). Let \( K \) be a differentially closed field. Let \( F \) be a system of differential polynomials in \( K\{y_1,\ldots,y_n\} \), and let \( f \in K\{y_1,\ldots,y_n\} \). Then, \( f \in \{F\} \) if and only if, for all \( (a_1,\ldots,a_n) \in K^n \) that annihilate \( F \), then \( f(a_1,\ldots,a_n) = 0 \).

In MAPLE, the DifferentialAlgebra package is continuously being updated due to new algorithms.

**References**


