Lecture Notes 1.
MA 722

1 Algebra-Geometry Dictionary

This section summarizes the most basic facts you need to know from algebraic geometry. We follow the approach of [CLO97, Chapters 1 and 4].

Definition 1.1. Let k be a field and $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. We call

$$\mathbf{V}(f_1, \ldots, f_s) := \{\vec{z} = (z_1, \ldots, z_n) \in k^n \ : \ f_i(\vec{z}) = 0 \ i = 1, \ldots, s\}$$

the *affine variety* in k^n defined by $f_1, \ldots, f_s$.

The following proposition implies that if V and W are affine varieties, then so is $V \cap W$ and $V \cup W$.

Proposition 1.2. *Let $V = \mathbf{V}(f_1, \ldots, f_s)$ and $W = \mathbf{V}(g_1, \ldots, g_t)$. Then*

$$\begin{aligned} V \cap W &= \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t) \\ V \cup W &= \mathbf{V}(f_i g_j \ : \ i = 1 \ldots s, \ j = 1 \ldots t) \end{aligned}$$

Proof. The claim for $V \cap W$ is easy to check. To prove the second claim, first observe that $V \subseteq \mathbf{V}(f_i g_j)$ and $W \subseteq \mathbf{V}(f_i g_j)$, therefore $V \cup W \subseteq \mathbf{V}(f_i g_j)$. On the other hand, let $\vec{z} \in \mathbf{V}(f_i g_j)$. If $\vec{z} \in V$ then we are done. Otherwise, there exists i^* such that $f_{i^*}(\vec{z}) \neq 0$. But for all $j = 1, \ldots, t$ we have $f_{i^*} g_j(\vec{z}) = 0$, which implies that $g_j(\vec{z}) = 0$ for all j, thus $\vec{z} \in W$. □

Example 1.3. (1) $\mathbf{V}(x^2+y^4-4) \cap \mathbf{V}(xy-1) = \mathbf{V}(x^2+y^4-4, \ xy-1) \subset \mathbb{R}^2$ is the 4 intersection points of the circle of radius 2 and the hyperbola. Another representation of the same set is $\mathbf{V}(x^4 - 4x^2 + 1, xy - 1)$.
(2) $\mathbf{V}((x-2)(x^2-y), (x^2-y)y, (z+1)(x^2-y)) \subset \mathbb{R}^3$ is the union of the point $\mathbf{V}(x-2, y, z+1) = \{(2, 0, 1)\}$ and the surface $\mathbf{V}(y - x^2)$. This is an example of a system where 3 equations in 3 variables can have common roots of isolated points as well as higher dimensional components.

Generally, numerical methods handle systems which have no root multiplicities or other singularities. The symbolic methods we study here also solve systems which have singularities. More precisely, the questions we try to answer are the following:

a. **Consistency:** Is $\mathbf{V}(f_1, \ldots, f_s) = \emptyset$?

b. **Finiteness:** Is the set $\mathbf{V}(f_1, \ldots, f_s)$ has finite cardinality? If yes, give all solutions.

c. **Dimension:** What is the dimension of $\mathbf{V}(f_1, \ldots, f_s)$? Find representations of the ≥ 1 dimensional components.

To characterize affine varieties algebraically, we define a correspondence between affine varieties in k^n and ideals in $k[x_1, \ldots, x_n]$.

Definition 1.4. Let $V \subset k^n$ be an affine variety, and define

$$\mathbf{I}(V) := \{f \in k[x_1, \ldots, x_n] \ : \ f(\vec{z}) = 0 \ \ \forall \vec{z} \in V\}.$$

Then $\mathbf{I}(V)$ is an ideal in $k[x_1, \ldots, x_n]$.
Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Define

$$\mathbf{V}(I) := \{\vec{z} \in k^n \ : \ f(\vec{z}) = 0 \ \ \forall f \in I\}.$$

Note that the above correspondence is *inclusion reversing*, i.e.

$$\begin{aligned} V \subset W \ &\Rightarrow \ \mathbf{I}(W) \subset \mathbf{I}(V) \\ I \subset J \ &\Rightarrow \ \mathbf{V}(J) \subset \mathbf{V}(I). \end{aligned}$$

However, the above correspondence is not a bijection, different ideals can define the same affine variety. For example, $\mathbf{V}(1) = \mathbf{V}(1 + x^2) = \emptyset$ in $\mathbb{R}^2$, or $\mathbf{V}(x - 1) = \mathbf{V}(x^2 - 2x + 1) = \{1\}$. The next theorem clarifies the situation about consistency of polynomials, at least over algebraically closed fields. We do not give proof here.

Theorem 1.5 (Weak Nullstellensatz)**.** *Let k be an algebraically closed field, $I \subset k[x_1, \ldots, x_n]$an ideal such that $\mathbf{V}(I) = \emptyset$. Then $I = k[x_1, \ldots, x_n]$, i.e. $1 \in I$.*

The next theorem (again, without proof) is the stronger version of the Nullstellensatz:

Theorem 1.6 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field. Then $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ satisfy*

$$f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$$

if and only if there exists $m \geq 1$ such that

$$f^m \in \langle f_1, \ldots, f_s \rangle,$$

where $\langle f_1, \ldots, f_s \rangle$ denotes the ideal generated by $f_1, \ldots, f_s$.

The property described in Hilbert's Nullstellensatz motivates the following definition:

Definition 1.7. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The *radical of I* is defined by

$$\sqrt{I} := \{f \in k[x_1, \ldots, x_n] \ : \ \exists\, m \ f^m \in I\}.$$

An ideal J is called a *radical ideal* if $\sqrt{J} = J$.

Another way to state Hilbert's Nullstellensatz is as follows: If k is algebraically closed, then for any ideal $J \subset k[x_1, \ldots, x_n]$

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

Therefore, if k is algebraically closed, we get the following inclusion-reversing bijection:

$$\text{affine varieties} \quad \leftrightarrow \quad \text{radical ideals}\ .$$

Next we study irreducible varieties and their corresponding prime ideals.

Definition 1.8. $V \subset k^n$ affine variety is *irreducible* if whenever $V = V_1 \cup V_2$, where V_1 and V_2 are affine varieties, then either $V_1 = V$ or $V_2 = V$.

To decide whether an affine variety is irreducible we need the following algebraic characterization of irreducibility:

Definition 1.9. An ideal $I \subset k[x_1, \ldots, x_n]$ is a *prime ideal*, if whenever $f, g \in k[x_1, \ldots, x_n]$ and $fg \in I$, then either $f \in I$ or $g \in I$.

The following proposition gives an other inclusion-reversing bijection between

$$\text{irreducible varieties} \quad \leftrightarrow \quad \text{prime ideals.}$$

Proposition 1.10. *$V \subset K^n$ is irreducible if and only if $\mathbf{I}(V)$ is prime.*

Proof. ($\Rightarrow$) Assume that V is irreducible and let $fg \in \mathbf{I}(V)$. Let $V_1 := V \cap \mathbf{V}(f)$ and $V_2 := C \cap \mathbf{V}(g)$. Then $V = V_1 \cup V_2$, and V_1, V_2 are affine. Therefore $V = \mathbf{V}(f)$ or $V = \mathbf{V}(g)$, which implies that either $f \in \mathbf{I}(V)$ or $g \in \mathbf{I}(V)$.
($\Leftarrow$) Assume that $\mathbf{I}(V)$ is prime. Let $V = V_1 \cup v_2$ and suppose that $V \neq V_1$. We claim that $\mathbf{I}(V) = \mathbf{I}(V_2)$. On one hand, since $V_2 \subseteq V$, therefore $\mathbf{I}(V) \subseteq \mathbf{I}(V_2)$. On the other hand, let $g \in I(V_2)$. Since $V \neq V_1$, there exist $f \in \mathbf{I}(V_1) - \mathbf{I}(V)$. Since $V = V_1 \cup V_2$, we have $fg \in \mathbf{I}(V)$. But since $\mathbf{I}(V)$ is prime, either $f \in \mathbf{I}(V)$ or $g \in \mathbf{I}(V)$. Since $f \notin \mathbf{I}(V)$, we get that $g \in \mathbf{I}(V)$. This proves that $\mathbf{I}(V_2) \subseteq \mathbf{I}(V)$. Therefore, we can conclude that $V = V_2$. □

Example 1.11. If k is an infinite field and $V \subset k^n$ is an affine variety given parametrically by

$$x_1 = f_1(t_1, \ldots, t_m), \ldots, x_n = f_n(t_1, \ldots, t_n)$$

where $f_i \in k[t_1, \ldots, t_m]$, then V is an irreducible variety.

Finally, we define maximal ideals:

Definition 1.12. An ideal $I \subset k[x_1, \ldots, x_n]$ is a *maximal ideal*, if $I \neq k[x_1, \ldots, x_n]$ and whenever $I \subseteq J$ for some ideal J, then either $J = I$ or $J = k[x_1, \ldots, x_n]$.

Example 1.13. The ideal

$$I = \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle \subset k[x_1, \ldots, x_n]$$

is maximal, where $a_1, \ldots, a_n \in k$. (Prove it!)

Proposition 1.14. *Every maximal ideal is prime. (The converse is not true.)*

Proof. Assume that I is not prime, i.e. let $fg \in I$ such that $f \notin I$ and $g \notin I$. Consider $J := \langle f, I \rangle$, the ideal generated by f and I. Then J strictly contains I, since $f \notin I$. If $J = k[x_1, \ldots, x_n]$, then $1 \in J$, so $1 = cf + h$ for some $h \in I$, and $c \in k[x_1, \ldots, x_n]$. But the $g = gcf + gh \in I$, which we assumed to be not the case. Therefore, $J \neq k[x_1, \ldots, x_n]$. Thus i cannot be a maximal ideal, since J is a proper ideal containing it. □

The next theorem gives our last bijection for algebraically closed fields:

$$\text{points} \quad \leftrightarrow \quad \text{maximal ideals.}$$

Theorem 1.15. *If k is an algebraically closed field, then every maximal ideal in $k[x_1, \ldots, x_n]$ is of the form $\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$.*

Proof. Let $I \subset k[x_1, \ldots, x_n]$ be a maximal ideal. Since $I \neq k[x_1, \ldots, x_n]$, by the Weak Nullstellensatz $\mathbf{V}(I) \neq \emptyset$. Let $\vec{a} = (a_1, \ldots, a_n) \in \mathbf{V}(I)$. Then $\mathbf{I}(\mathbf{V}(I)) \subseteq \mathbf{I}(\{\vec{a}\})$. Using Hilbert's Nullstellensatz we have $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. Since I is maximal, it is prime, and it is easy to check from their definition that prime ideals are radical, thus $\sqrt{I} = I$. Thus, $I \subseteq \mathbf{I}(\{\vec{a}\})$. But $\mathbf{I}(\{\vec{a}\}) \neq k[x_1, \ldots, x_n]$, so $I = \mathbf{I}(\{\vec{a}\})$. □

To summarize, in this section we established the following dictionary between algebra and geometry for the case when k is algebraically closed:

$$\begin{array}{rcl} \text{affine varieties} & \leftrightarrow & \text{radical ideals} \\ \text{irreducible varieties} & \leftrightarrow & \text{prime ideals} \\ \text{points} & \leftrightarrow & \text{maximal ideals.} \end{array}$$

2 Gröbner basis

Motivation: As we have seen in the Example 1.3, ideals can be given by various sets of generating polynomials: some are more useful to answer our basic geometric questions than others. Gröbner bases are special sets of generators of ideals with the property that there is a simple algorithmic way – division with remainder – to decide whether a given polynomial is in the ideal or not. This decision problem is called the *ideal membership problem*. We have already seen that the Consistency Problem over algebraically closed fields is equivalent to deciding whether 1 is in the ideal. We will see at the

end of this section that many more geometric questions can be answered using Gröbner bases. In particular we will be able to solve *any* systems of equations if we have a Gröbner basis.

We follow the approach of [CLO97, Chapter 2].

2.1 Monomial Orderings and the Division Algorithm

Before we discuss the multivariate construction, let us recall the division with remainder algorithm in the univariate case, using an example.

Example 2.1. Let $f(x) = x^3 + 1 - 2x$ and $g(x) = 2 - 2x^2 - x$. In order to divide f by g we

1. Arrange the terms of f and g in a decreasing order of degrees.
2. If the leading term of g divides the leading term of f then find the quotient, in this case $x^3 / (-2x^2) = -\frac{1}{2}x$. Otherwise return f.
3. Repeat the same process for $f(x) - (-\frac{1}{2}x)g(x)$. Note that the leading term of $f(x)$ is cancelled in $f(x) + \frac{1}{2}xg(x) = -\frac{1}{2}x^2 - x + 1$.

Note that in the univariate case, every ideal is generated by one polynomial, namely, by the greatest common divisor of the generators. Once this greatest common divisor is computed, ideal membership can be decided using the division with remainder algorithm.

In the multivariate case the degree of the terms do not give a total order on the monomials. However, once we define an ordering on the monomials satisfying certain natural conditions, we can easily generalize the univariate division with remainder algorithm, as we will see at the end of this subsection. However, as we will also see, having a division with remainder algorithm is still not sufficient to solve the ideal membership problem in the multivariate case.

Definition 2.2. Monomials are denoted by $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. Each monomial is uniquely determined by its vector of exponents $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, thus defining ordering on the monomials or on $\mathbb{N}^n$ is equivalent. We will use the notation $\alpha \succ \beta$ and $x^\alpha \succ x^\beta$ interchangeably.
A *monomial ordering* $\succ$ is a total order on $\mathbb{N}^n$ satisfying

(i) $\alpha \succ \beta \;\; \Rightarrow \;\; \alpha + \gamma \succ \beta + \gamma$ for all $\gamma \in \mathbb{N}^n$

(ii) Any $S \subseteq \mathbb{N}^n$ has a least element.

Definition 2.3. The following are the most commonly used monomial orderings:

Lexicographic Order: $\alpha \succ_{lex} \beta$ if in $\alpha - \beta$ the leftmost non-zero entry is positive.

Graded Lex Order: $\alpha \succ_{grlex} \beta$ if $|\alpha| > |\beta|$, or if $|\alpha| = |\beta|$ then $\alpha \succ_{lex} \beta$. Here $|\alpha| = \sum_{i=1}^{n} \alpha_i$, and similarly for $|\beta|$.

Graded Reverse Lex Order: $\alpha \succ_{grevlex} \beta$ if $|\alpha| > |\beta|$, or if $|\alpha| = |\beta|$ then in $\alpha - \beta$ the rightmost non-zero entry is negative.

Example 2.4. Consider the set

$$\{xyz^2, x^3, y^4, x^2y^2, xy^2z\}.$$

Assuming that $x \succ y \succ z$, i.e. the exponent of x is the leftmost entry and the exponent of z is the rightmost entry in the exponent vector, the above orderings of the set are the following:

$$\begin{aligned}
&\textbf{lex}: \; x^3 \succ x^2y^2 \succ xy^2z \succ xyz^2 \succ y^4 \\
&\textbf{grlex}: \; x^2y^2 \succ xy^2z \succ xyz^2 \succ y^4 \succ x^3 \\
&\textbf{grevlex}: \; x^2y^2 \succ y^4 \succ xy^2z \succ xyz^2 \succ x^3.
\end{aligned}$$

We will use the following terminology.

Definition 2.5. Let $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ and let $\succ$ be a monomial order.

- The *leading exponent* of f is

$$\mathrm{LE}(f) := \max(\alpha \in \mathbb{N}^n \; : \; c_\alpha \neq 0).$$

  Here the maximum is taken with respect to $\succ$.

- The *leading coefficient* of f is

$$LC(f) := c_{\mathrm{LE}(f)} \; \in k.$$

- The *leading monomial* of f is

$$\mathrm{LM}(f) := x^{\mathrm{LE}(f)}.$$

- The *leading term* of f is

$$\mathrm{LT}(f) := \mathrm{LC}(f) \cdot \mathrm{LM}(f).$$

Now we are ready to present the division algorithm.

Multivariate Division with Remainder
Input: $f_1, \ldots, f_s, f \in k[x_1, \ldots, x_n]$ and a monomial order $\succ$.
Output: $q_1, \ldots, q_s, r \in k[x_1, \ldots, x_n]$ such that

$$f = \sum_{i=1}^{s} q_i f_i + r$$

and no monomials in r are divisible by $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. Moreover, if $q_i f_i \neq 0$ then $\mathrm{LE}(f) \succeq \mathrm{LE}(q_i f_i)$.

$q_i := 0$ for $i = 1 \ldots s$; $r := 0$; $p := f$;
WHILE $p \neq 0$ DO
    $i := 1$; flag := false;
    WHILE $i \leq s$ AND flag = false DO
        IF $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(P)$ THEN
            $q_i := q_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$;
            $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i)) \cdot f_i$;
            flag := true;
        ELSE $i := i + 1$;
    IF flag = false THEN
        $r := r + \mathrm{LT}(p)$;
        $p := p - \mathrm{LT}(p)$.

Proof of correctness (outline). We can prove by induction that each time we pass through the main WHILE loop, the following holds:

(i) $\mathrm{LE}(f) \succeq \mathrm{LE}(p)$ and $f = p + \sum_{i=1}^{s} q_i f_i + r$.

(ii) If $q_i \neq 0$ then $\mathrm{LE}(f) \succeq \mathrm{LE}(q_i f_i)$.

(iii) No term in r is divisible by any of $\mathrm{LT}(f_i)$.

Moreover, the algorithm terminates, since $\mathrm{LE}(p)$ is strictly decreasing each time we pass through the main WHILE loop, and by the properties of the monomial ordering, there is no infinite subset of strictly decreasing monomials. □

2.2 Definition and Properties of Gröbner Bases

Unfortunately, in the multivariate case the division algorithm does not answer the ideal membership problem. For example, if $I = \langle x^2 + 1, xy - 1\rangle$, then $x+y = y(x^2+1)-x(xy-1) \in I$, but the according to the division algorithm, the remainder of $x + y$ is itself. Gröbner bases are generator sets of ideals such that ideal membership can be detected using the division algorithm.

In this subsection we assume that a monomial order $\succ$ is fixed.

First we define ideals generated by the leading terms of an ideal. It is easy to see that deciding membership in ideals generated by monomials – called *monomial ideals* – is a simple application of the division algorithm.

Definition 2.6. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal not equal $\{0\}$. We denote by

$$\mathrm{LT}(I) := \{\mathrm{LT}(f) \ : \ f \in I\}$$

the set of leading terms of elements of I. Since this is not an ideal, we denote $\langle \mathrm{LT}(I)\rangle$ the ideal generated by $\mathrm{LT}(I)$ in $k[x_1, \ldots, x_n]$.

We are ready to define Gröbner bases.

Definition 2.7. A finite subset $G = \{g_1, \ldots, g_s\} \subset k[x_1, \ldots, x_n]$ of an ideal is a *Gröbner basis* of I w.r.t. $\succ$ if

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle = \langle \mathrm{LT}(I)\rangle.$$

The following existence theorem is stated here without proof.

Theorem 2.8. *Every ideal $I \subset k[x_1, \ldots, x_n]$ other than $\{0\}$ has a Gröbner basis w.r.t. $\succ$. Furthermore, the elements of a Gröbner basis for I form a generating set for I.*

Example 2.9. Let $I = \langle x^2 + 1, xy - 1\rangle$, and let $\succ$ be the lexicographic ordering such that $y \succ x$. Then clearly $\{x^2 + 1, xy - 1\}$ is not a Groebner basis, since $\mathrm{LT}(x + y) = y \in \langle \mathrm{LT}(I)\rangle$, as we have seen above, however $y \notin \langle x^2, xy\rangle$. In fact, $G = \{x^2 + 1, xy - 1, y + x\}$ forms a Gröbner basis for I. One can also simplify G.

The first property we prove is that the division algorithm produces a unique remainder for Gröbner bases.

Proposition 2.10. *Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis for an ideal I. Let $f \in k[x_1, \ldots, x_n]$. Then there exists a unique $r \in k[x_1, \ldots, x_n]$ such that*

(i) no term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$,

(ii) $f = g + r$ for some $g \in I$.

In particular, R is the remainder on division of f by G, independently of the order of elements in G.

Proof. The output specification of the division algorithm proves the existence of r. To prove uniqueness, assume that $f = g_1 + r_1 = g_2 + r_2$ satisfy (i) and (ii). Then $r_1 - r_2 = g_1 - g_2 \in I$, so $\mathrm{LT}(r_1 - r_2) \in \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$. Since $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$ and $\mathrm{LT}(r_1 - r_2)$ are all single terms, there must exist $\mathrm{LT}(g_i)$ which divides $\mathrm{LT}(r_1 - r_2)$. But this is impossible, since no term of r_1 and r_2 are divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. Thus $r_1 - r_2$ must be zero. □

Corollary 2.11. *Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis for an ideal I, and let $f \in k[x_1, \ldots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.*

The next property gives an efficient way to check that a set of polynomials forms a Gröbner basis. First we need the definition of S-polynomials.

Definition 2.12. Let $f, g \in k[x_1, \ldots, x_n]$ be non-zero polynomials. The *S-polynomial* of f and g is the combination

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g,$$

where $x^\gamma = LCM(\mathrm{LT}(f), \mathrm{LT}(g))$ the least common multiple of the leading terms.

An S-polynomial cancels the smallest common leading term of multiples of f and g.

Example 2.13. The S-polynomial of $x^2 + 1$ and $xy - 1$ w.r.t. any ordering is

$$\frac{x^2y}{x^2}(x^2 + 1) - \frac{x^2y}{xy}(xy - 1) = y(x^2 + 1) - x(xy - 1) = y + x.$$

The next theorem is presented without a proof:

Theorem 2.14. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Then a basis $G = \{g_1, \ldots, g_s\}$ for I is a Gröbner basis for I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G is zero.*

The previous theorem gives the following simple (but not necessarily efficient) algorithm to compute a Gröbner basis, called Buchberger algorithm:

Buchberger's Algorithm
Input: $F = \{f_1, \ldots, f_s\} ink[x_1, \ldots, x_n]$ and $\succ$ monomial ordering
Output: $G = \{g_1, \ldots, g_t\}$ a Gröbner basis for $I = \langle f_1, \ldots, f_s \rangle$, with $F \subseteq G$

```
G := F; G' := {};
WHILE G' ≠ G DO
    G' := G;
    FOR each pair {p, q}, p ≠ q in G' DO
        S := S(p, q); S := remainder(S, G');
        IF S ≠ 0 THEN G := G ∪ {S}
    OD
OD
```

Proof of correctness. The following statements hold every time we pass through the main loop:

1. $G \subset I$, since $S \in I$ for all $p, q \in I$
2. $F \subset G$, thus G is a basis for I
3. $G' \subseteq G$

4. $G = G' \cup \{\text{remainder}(S(p,q), G') \ : \ p \neq q \in G'\}$

This implies that $G' = G$ if and only if for all (p,q), $p \neq q \in G'$, $S(p,q)$ reduces to zero on division by G'. Therefore $G' = G$ is a Groebner basis. The algorithm terminates, since if $G' \neq G$ then

$$\langle \text{LT}(G') \rangle \subsetneq \langle \text{LT}(G) \rangle$$

since the leading term of remainder$(S(p,q), G')$ is not divisible by any of the elements in $\text{LT}(G')$. This implies that the ideals $\langle \text{LT}(G') \rangle$ from successive iterations of the main loop form an ascending chain of ideals in $k[x_1, \ldots, x_n]$. Using the so called *Hilbert's basis theorem* stating that every ideal in $k[x_1, \ldots, x_n]$ can be generated by finitely many polynomials, one can prove that there is no infinite strictly ascending chain of ideals in $k[x_1, \ldots, x_n]$. □

Example 2.15. Let

$$I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle \subset \mathbb{Q}[x,y]$$

and we use the graded lexicographic order. Then $G' := \{f_1, f_2\}$ is not a Gröbner basis for I, since $S(f_1, f_2) = -x^2$ does not reduce to zero modulo G'. Let

$$f_3 := x^2$$

and $G := G' \cup \{f_3\}$. Second time around in the main loop of Buchberger's Algorithm we set $G' := G$. Then $S(f_1, f_2) = f_3$ clearly reduces to 0 modulo G', but $S(f_1, f_3) = -2xy$ and $S(f_2, f_3) = -2y^2 + x$ do not. Let

$$f_4 := 2xy \quad \text{and} \quad f_5 := 2y^2 - x$$

and $G := G' \cup \{f_4, f_5\}$. Again entering the main loop, we set $G' := G$. Now one can check that for all pairs in G' the S-polynomial reduces to zero. Therefore

$$G = \{x^3 - 2xy, x^2y - 2y^2 + x, x^2, 2xy, 2y^2 - x\}$$

forms a Gröbner basis. Note that we can simplify G using the division algorithm, and get a so called *reduced* Gröbner basis $\{x^2, xy, y^2 - x/2\}$

Definition 2.16. A Gröbner basis $G \subset k[x_1, \ldots, x_n]$ is called a *reduced Gröbner basis* for I if

(i) $\mathrm{LC}(g) = 1$ for all $g \in G$

(ii) For all $g \in G$ no monomials of g lies in $\langle \mathrm{LT}(G - \{g\})\rangle$.

The next theorem asserts that reduced Gröbner bases exists and unique:

Theorem 2.17. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal not eqaul to $\{0\}$. Then, for a given monomial ordering, I has a unique reduced Gröbner basis.*

Proof. The existence of reduced Gröbner bases follows from the following algorithm to produce one: First note that if $g \in G$ such that $\mathrm{LT}(g) \in \langle \mathrm{LT}(G - \{g\})\rangle$, then $G - \{g\}$ is also a Gröbner basis for I, so we can discard such g's from G. After doing that, for all $g \in G$ we compute $g' := \mathrm{remainder}(g, G - \{g\})$ and set $G := G - \{g\} \cup \{g'\}$. The resulting set is a reduced Gröbner basis for I.
To prove uniqueness, suppose that G and $\tilde{G}$ are reduced Gröbner bases for I. One can show that this implies that

$$\mathrm{LT}(G) = \mathrm{LT}(\tilde{G}).$$

Thus, for each $g \in G$ there exists $\tilde{g} \in \tilde{G}$ such that $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$. We will show that $g = \tilde{g}$. Since $g - \tilde{g} \in I$, and G is a Gröbner basis for I, $g - \tilde{g}$ reduces to zero modulo G. But none of the terms in $g - \tilde{g}$ is divisible by any of the elements of $\mathrm{LT}(G) - \{\mathrm{LT}(g)\} = \mathrm{LT}(\tilde{G}) - \{\mathrm{LT}(\tilde{g})\}$, and the term $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$ is cancelled in $g - \tilde{g}$. Therefore the division algorithm of $g - \tilde{g}$ by G will not change $g - \tilde{g}$. This implies that $g - \tilde{g} = 0$. □

Corollary 2.18. *For a fixed monomial ordering, from the reduced Gröbner bases we can decide if two ideals are equal.*

Example 2.19. For a set of linear polynomials the reduced Gröbner basis corresponds to the reduced row echelon form of the linear system.

2.3 Solving Polynomials Using Gröbner Bases

First we discuss how to solve systems using Gröbner bases w.r.t. the lexicographic order. Gröbner bases w.r.t. the lexicographic order have the property that the variables are eliminated successively. The order of elimination corresponds to the order of the variables in the lex ordering we used. A system

of equations in this form is easy to solve by *back substitution*, especially if the last equations contains only one variable. More precisely, we have the following theorem:

Theorem 2.20 (The Elimination Theorem)**.** *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal and let G be a Gröbner basis with respect to the lexicographic ordering where $x_1 \succ x_2 \succ \cdots \succ x_n$. Then for any $1 \leq i \leq n$ the set*

$$G_i := G \cap k[x_{i+1}, \ldots, x_n]$$

is a Gröbner basis for the elimination ideal

$$I_i := I \cap k[x_{i+1}, \ldots, x_n].$$

Proof. The crucial observation is that in the lex order with $x_1 \succ x_2 \succ \cdots \succ x_n$, any monomial involving $x_1, \ldots, x_i$ is greater than all monomials in $k[x_{i+1}, \ldots, x_n]$. Therefore, if $\mathrm{LT}(g) \in k[x_{i+1}, \ldots, x_n]$ then $g \in k[x_{i+1}, \ldots, x_n]$. Thus, for all $f \in I_i$, if some $g \in G$ $\mathrm{LT}(g)$ divides $\mathrm{LT}(f)$, then g must be in G_i. This implies that $\langle \mathrm{LT}(I_i) \rangle = \langle \mathrm{LT}(G_i) \rangle$. □

Corollary 2.21. *Let k be algebraically closed, and $I \subset k[x_1, \ldots, x_n]$ be an ideal. Assume that $\mathbf{V}(I) \subset k^n$ is a finite set. Then any Gröbner basis for I with respect to the lexicographic ordering where $x_1 \succ x_2 \succ \cdots \succ x_n$ contains a univariate polynomial only depending on x_n.*

The next example demonstrates how to solve a polynomial system with finitely many roots using lexicographic Gröbner bases:

Example 2.22. Let

$$f_1 := x^2 + y^2 + z^2 - 1 \quad f_2 := x^2 + y^2 - y \quad f_3 := x - z.$$

Then using the lex order with $x > y > z$ we get that the Gröbner basis consists of the polynomials

$$g_1 := x - z \quad g_2 := -y + 2z^2 \quad g_3 := z^4 + \frac{1}{2}z^2 - \frac{1}{4}.$$

Now one can use your favorite solver of univariate polynomials, for example solving by radicals, to get

$$z = \pm\sqrt{\pm\sqrt{5} - 1}.$$

Back substituting these four values of z into the equations $g_2 = 0$ and $g_1 = 0$ – which are linear in y and x, respectively – we get the coordinates of the four points in $\mathbf{V}(f_1, f_2, f_3)$.

Unfortunately, in practice, the computation of the lex Gröbner basis is the least efficient. Next we present a method to solve polynomial systems with finitely many roots, given *any* Gröbner basis. The main idea behind the method is to compute a set of *multiplication matrices* using the Gröbner basis. We will show that the coordinates of the common roots of the system are eigenvalues of the multiplication matrices.

We need some more definitions, first the definition of *quotient rings*:

Definition 2.23. The *quotient* of $k[x_1, \ldots, x_n]$ modulo the ideal I, written $k[x_1, \ldots, x_n]/I$, is the set of equivalence classes of congruence modulo I, i.e. $f \equiv g$ if $f - g \in I$. The equivalence class of $f \in k[x_1, \ldots, x_n]$ is denoted by $f + I$. Then $k[x_1, \ldots, x_n]/I$ is a commutative ring under the operations

$$(f + I) + (g + I) = (f + g) + I \quad \text{and} \quad (f + I)(g + I) = (fg) + I.$$

Proposition 2.24. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and let G be a Gröbner basis for I w.r.t. any monomial ordering. Then $k[x_1, \ldots, x_n]/I$, as a vector-space over k, is isomorphic to the k vector space*

$$S := \operatorname{span}\{x^\alpha \ : \ x^\alpha \notin \langle \operatorname{LT}(G) \rangle\}.$$

Proof. For any $f \in k[x_1, \ldots, x_n]$ the remainder of f by G is in S, and gives a unique representative in the equivalence class $f + I$. One can check that this gives an isomorphism. □

The next theorem asserts that if $\mathbf{V}(I)$ is finite over an algebraically closed field, then $S = \operatorname{span}\{x^\alpha \ : \ x^\alpha \notin \langle \operatorname{LT}(G) \rangle\}$ is a finite dimensional vector space. The proof follows from Hilbert's Nullstellensatz.

Theorem 2.25. *Let k be an algebraically closed field of characteristic zero, and $V = \mathbf{V}(I)$ be an affine variety in k^n. Fix a monomial ordering in $k[x_1, \ldots, x_n]$. Then the following statements are equivalent:*

(i) V is a finite set.

(ii) For each $1 \leq i \leq n$ there exist $m_i \geq 0$ such that $x_i^{m_i} \in \operatorname{LT}(I)$.

(iii) *Let G be a Gröbner basis for I. Then for each $1 \leq i \leq n$ there exist $m_i \geq 0$ such that $x_i^{m_i} = \mathrm{LT}(g)$ for some $g \in G$.*

(iv) *The k-vector space $S = \mathrm{span}\{x^\alpha \ : \ x^\alpha \notin \langle \mathrm{LT}(G) \rangle\}$ is finite dimensional.*

(v) *The k-vector space $k[x_1, \ldots, x_n]/I$ is finite dimensional.*

We call an ideal I satisfying any of the above equivalent conditions a **zero dimensional ideal**.

Proof. $(i) \Rightarrow (ii)$ Assume that V is finite, and assume that $V = \{\vec{z}_1, \ldots, \vec{z}_d\} \subset k^n$. Suppose that for some i no power of x_i is in $\mathrm{LT}(I)$. We can assume without loss of generality that $i = 1$, otherwise we rename the variables. Define

$$f := \prod_{j=1}^{d} (x_1 - z_{j,1}) \in k[x_1]$$

where $z_{j,1}$ is the first coordinate of $\vec{z}_j$. Then clearly $f(\vec{z_j}) = 0$ for all $j = 1, \ldots, d$, thus $f \in I(V)$. By Hilbert's Nullstellensatz there exists $m > 0$ such that $f^m \in I$. Since f^m is a univariate polynomial, we have that its highest degree term, which is a power of x_1 is in $\mathrm{LT}(I)$, a contradiction.
$(ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (v)$ is trivial, using Proposition 2.24.
$(v) \Rightarrow (i)$ Assume that $k[x_1, \ldots, x_n]/I$ is finite dimensional. Then for all $i = 1, \ldots, n$, we have $I \cap k[x_i] \neq \{0\}$, otherwise $\{x_i^j + I \ : \ j \in \mathbb{N}\}$ would form an infinite linearly independent subset of $k[x_1, \ldots, x_n]/I$. Since $k[x_i]$ is a principal ideal domain, we can define $f_i \neq 0 \in k[x_i]$ such that $\langle f_i \rangle = I \cap k[x_i]$ for all $i = 1, \ldots n$. For any $\vec{z} \in V(I)$ we have $f_i(\vec{z}) = 0$, so its i-th coordinate is a root of f_i, which leaves at most $\deg(f_i) < \infty$ choices for that coordinate. Since this is true for all coordinates that leaves only finitely many choices for $\vec{z} \in V(I)$, thus it is finite. □

As a consequence of the previous theorem, the Finiteness Problem can be decided using *any* Gröbner basis. Next we study the relationship between the number of roots in $V(I)$ and the dimension of $k[x_1, \ldots, x_n]/I$.

Theorem 2.26. *Let k be algebraically closed, and $I \subset k[x_1, \ldots, x_n]$ be a zero dimensional ideal. Then*

(1) $|V(I)| \leq \dim_k k[x_1, \ldots, x_n]/I$.

(2) I *is radical if and only if* $|V(I)| = \dim_k k[x_1, \ldots, x_n]/I$.

Proof. Let $V = V(I) = \{\vec{z}_1, \ldots, \vec{z}_d\} \subset k^n$ where $\vec{z}_i = (z_{i,1}, \ldots, z_{i,n})$. We will construct a *Lagrange basis* for the set V, i.e. polynomials $L_1, \ldots, L_d \in k[x_1, \ldots, x_n]$ with the property that

$$L_i(\vec{z}_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}.$$

The construction of L_1 can be done as follows: since $\vec{z}_1 \neq \vec{z}_i$ for each $i = 2, \ldots, n$, there exists a coordinate index t_i where they differ, i.e. $z_{1,t_i} \neq z_{i,t_i}$. Then

$$L_1(x_1, \ldots, x_n) := \prod_{i=2}^{n} \frac{x_{t_i} - z_{1,t_i}}{z_{i,t_i} - z_{1,t_i}} \in k[x_1, \ldots, x_n]$$

will have the desired property. $L_2, \ldots, L_d$ can be constructed similarly.
Next we prove that $[L_1], \ldots, [L_d] \in k[x_1, \ldots, x_n]/I$ are linearly independent. Suppose there exist $a_1, \ldots a_d \in k$ such that

$$a_1[L_1] + \cdots + a_d[L_d] = [0], \text{ i.e. } a_1L_1 + \cdots + a_dL_d \in I.$$

This implies that for all $j = 1, \ldots, d$

$$a_1L_1(\vec{z}_j) + \cdots + a_dL_d(\vec{z}_j) = 0.$$

But $L_i(\vec{z}_j) = \delta_{i,j}$, the Kronecker symbol, which implies that for all $j = 1, \ldots d$ $a_j = 0$. Thus we proved linear independence. We constructed a linearly independent set of cardinality d in $k[x_1, \ldots, x_n]/I$, which implies the first claim.
To prove the second claim, first assume that I is radical. We will prove that in this case $[L_1], \ldots, [L_d]$ generates $k[x_1, \ldots, x_n]/I$. Let $[f] \in k[x_1, \ldots, x_n]/I$ for some arbitrary polynomial $f \in k[x_1, \ldots, x_n]$. Define $c_i := f(\vec{z}_i) \in k$ for $i = 1, \ldots, d$, and let

$$F := \sum_{i=1}^{d} c_iL_i \in k[x_1, \ldots, x_n].$$

Then $[F]$ is spanned by $[L_1], \ldots, [L_d]$. Moreover

$$F(\vec{z}_i) = f(\vec{z}_i) \text{ for all } i = 1, \ldots d,$$

so $F - f \in I(V)$. But by I being radical, $I = I(V)$, which implies that $[f] = [F]$, which proves that $|V(I)| = \dim_k k[x_1, \ldots, x_n]/I$.
Conversely, suppose I is not radical, i.e. $I \subsetneq \sqrt{I}$. In this case we have

$$|V(I)| = \dim_k k[x_1, \ldots, x_n]/\sqrt{I} < \dim_k k[x_1, \ldots, x_n]/I.$$

□

Next we define normal sets and multiplication matrices:

Definition 2.27. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal.

- Let I be a zero dimensional ideal. Then a set of monomials N is called a *normal set* for I if it is a basis for the finite dimensional vector space $S = \text{span}\{x^\alpha \ : \ x^\alpha \notin \langle \text{LT}(I) \rangle\}$.
- Fix a normal set $N = \{x^{\alpha_1}, \ldots, x^{\alpha_D}\}$ for I, where $D = \dim k[x_1, \ldots, x_n]/I$. For any $f \in k[x_1, \ldots, x_n]$ denote

  $$[f]_N := (c_1, \ldots, c_D) \in k^D$$

  the vector of coefficients of the $f + I \in k[x_1, \ldots, x_n]/I$ in the basis N, i.e. $f = \sum_{i=1}^{D} c_i x^{\alpha_i} + g$ for some $g \in I$.
- Fix a normal set N as above, and let $f \in k[x_1, \ldots, x_n]$. The *multiplication matrix* M_f of f with respect to N is the transpose of the matrix of the k-linear map

  $$\begin{array}{rccc} \mu_f : & k[x_1, \ldots, x_n]/I & \to & k[x_1, \ldots, x_n]/I \\ & g + I & \mapsto & fg + I \end{array}$$

  written in the basis N of $k[x_1, \ldots, x_n]/I$. In other words, the i-th row of M_f is the vector $[f \cdot x^{\alpha_i}]_N$ for $i = 1, \ldots D$.

The next example illustrates how to compute a normal set N and the multiplication matrices

$$M_{x_1}, \ldots, M_{x_n}$$

of $x_1, \ldots, x_n$ with respect to N, given a Gröbner basis for I w.r.t. any monomial order.

Example 2.28. Let $\succ$ be the graded lexicographic order and let

$$I = \langle x^3 + y + z^2 + 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle.$$

Then instead if trying to compute a lexicographic Gröbner basis, we notice that the above generators already form a Gröbner basis w.r.t. the graded lexicographic ordering with $x > y > z$. Let G be the set of the above polynomials. Since $\mathrm{LT}(G) = \{x^3, y^2, z^2\}$ we can see that I is zero dimensional, and the set

$$N := \{1, x, y, z, x^2, xy, xz, yz, x^2y, x^2z, xyz, x^2yz\}$$

of cardinality 12 is a normal set for I. To find the 12×12 multiplication matrix M_x of x w.r.t. N, we have to consider the monomials $xN := \{x^{i+1}y^jz^k : x^iy^jz^k \in N\}$. Note that if $i < 2$ then $x^{i+1}y^jz^k \in N$, so its coordinates are trivial to find. If $i = 2$ then we apply the division algorithm to find the remainder of $x^3y^jz^k$ by G for $j = 0, 1$ and $k = 0, 1$. In particular, we get

$$x^3 + I = (x + I) - 2(1 + I), \quad x^3y + I = (xy + I) - 2(y + I)$$
$$x^3z + I = (xz + I) - 2(z + I), \quad x^3yz + I = (xyz + I) - 2(yz + I).$$

thus the matrix M_x is given by

$$M_x := \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
-2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & -2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 1 & 0
\end{bmatrix}$$

Similarly for M_y and M_z, or for M_f for any $f \in \mathbb{Q}[x, y, z]$.

Finally, the following theorem gives a strong connection between the points in $\mathbf{V}(I)$ and the eigenvalues of the multiplication matrices.

Theorem 2.29. *Let k be an algebraically closed field of characteristic 0 and let I be a zero dimensional ideal in $k[x_1, \ldots, x_n]$ with*

$$V = \mathbf{V}(I) = \{\xi_i = (\xi_{i,1}, \ldots, \xi_{i,n}) \in k^n \ : \ i = 1, \ldots D\}.$$

Let $D' = \dim k[x_1, \ldots, x_n]/I$ and fix a normal set

$$N = \{x^{\alpha_1}, \ldots, x^{\alpha_{D'}}\},$$

and for $f \in k[x_1, \ldots, x_n]$ denote by M_f the multiplication matrix of f with respect to N, as defined above. Then

1. *$\lambda \in k$ is an eigenvalue of M_f if and only if there exists $\xi_i \in V$ such that $\lambda = f(\xi_i)$.*

2. *Assume that $D = D'$, i.e. I does not have multiple roots. Define the* generalized Vandermonde matrix *corresponding to $\mathbf{V}(I)$ and N by*

$$\Sigma = \begin{bmatrix} \xi_1^{\alpha_1} & \cdots & \xi_D^{\alpha_1} \\ \vdots & & \vdots \\ \xi_1^{\alpha_D} & \cdots & \xi_D^{\alpha_D} \end{bmatrix}.$$

   Then Σ is invertible and the multiplication matrices M_f are simultaneously diagonalizable, i.e. we have

$$\Sigma^{-1} M_f \Sigma = D_f,$$

   where $D_f = \operatorname{diag}(f(\xi_1), \ldots, f(\xi_D))$. In particular, we can find the j-th coordinates of the roots by diagonalizing M_{x_j} to get $D_{x_j} = \operatorname{diag}(\xi_{1,j}, \ldots, \xi_{D,j})$.

Proof. (1) "$\Leftarrow$": First we prove that $f(\xi_j)$ is an eigenvalue of M_f for all $\xi_j \in V$, i.e. we will prove that

$$M_f \Sigma = \Sigma D_f.$$

The i-th row of M_f is equal to $[f \cdot x^{\alpha_i}]_N = [c_{i,1}, \ldots c_{i,D}]$ such that

$$f \cdot x^{\alpha_i} = \sum_{k=1}^{D} c_{i,k} x^{\alpha_k} + g \quad \text{for some } g \in I.$$

Therefore, the (i,j)-th entry of $M_f\Sigma$ is given by

$$\sum_{k=1}^{D} c_{i,k}\xi_j^{\alpha_k} = f(\xi_j)\cdot\xi_j^{\alpha_i} - g(\xi_j).$$

But $\xi_j \in \mathbf{V}(I)$, therefore $g(\xi_j) = 0$. Thus, the j-th column of $M_f\Sigma$ is equal to $f(\xi_j)$ times the j-th column of Σ.
"$\Rightarrow$": Let $\lambda \in k$ be an eigenvalue of M_f and suppose that for all $\xi_i \in V(I)$ we have $\lambda \neq f(\xi_i)$. Define the polynomial $g := f - \lambda \in k[x_1,\ldots,x_n]$. We will prove that g has an inverse modulo I. Let

$$\tilde{g} := \sum_{i=1}^{D} \frac{1}{g(\xi_i)} L_i(\mathbf{x})$$

where L_i are the polynomials constructed in Theorem 2.26 with the property $L_i(\xi_j) = \delta_{i,j}$. Then we have that $g\tilde{g}(\xi_i) = 1$ for all $\xi_i \in V$, thus $1 - g\tilde{g} \in I(V(I)) = \sqrt{I}$. Thus, there exists $m \in \mathbb{N}$ such that $(1-g\tilde{g})^m \in I$. Expanding

$$(1-g\tilde{g})^m = 1 - g\tilde{g} + \cdots + (-1)^m(g\tilde{g})^m = 1 - g\hat{g} \in I$$

for $\hat{g} = \tilde{g} - g\tilde{g}^2 \cdots + (-1)^m g^{m-1}\tilde{g}^m$. Thus $\hat{g}g \equiv 1$ modulo I. But

$$M_g M_{\hat{g}} = M_{g\hat{g}} = \mathrm{Id},$$

thus $M_g = M_f - \lambda\mathrm{Id}$ is invertible. This contradicts to our assumption that λ is an eigenvalue of M_f.

(2) It remains to prove that the matrix Σ is non-singular. This follows from the vector space isomorphisms

$$k[V] \cong k[x_1,\ldots,x_n]/I \cong \mathrm{span}(N)$$

and since N is a normal set, the corresponding elements

$$x^{\alpha_1}|_V, \ldots, x^{\alpha_D}|_V$$

in $k[V]$ are linearly independent, thus their evaluation vectors on V

$$[\xi_1^{\alpha_1},\ldots,\xi_D^{\alpha_1}],\ \ \ldots,\ \ [\xi_1^{\alpha_D},\ldots,\xi_D^{\alpha_D}]$$

are linearly independent, which proves the second claim. □

References

[CLO97] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Springer, 1997.