Isfahan University of Technology
Department of Mathematical Sciences

On Decomposig Systems of Polynomial Equations With Finitely Many Solutions

Bachelor Project:

Hamed Vaheb

Supervisor:

Prof.Amir Hashemi

September 2017

Contents

1 Preliminaries

In this chapter, we want to develop the theory of Gröbner Bases and its applications. In the first section, we define the ring of polynomials and division algorithm on this ring. These are required for introducing Gröbner Bases and Buchberger Algorithm which is discussed in the second section. And in the third section, we will give you some application of Gröbner Bases among various ones.

1.1 Ring of Polynomials

Definition 1. A monomial in $x_1, \cdots, x_n$ is a product of the form

$$x_1{}^{\alpha_1}, x_2{}^{\alpha_2}, ..., x_n{}^{\alpha_n},$$

where all of the exponents $\alpha_1, ..., \alpha_n$ are nonnegative integers. The total degree of this monomial is the sum $\alpha_1 + \cdots + \alpha_n$.

Definition 2. A polynomial f in $x_1, \cdots, x_n$ with coefficients in a field $\mathbb{K}$ is a finite linear combination (with coefficients in $\mathbb{K}$) of monomials. We will write a polynomial f in the form

$$f = \sum_{\alpha} a_\alpha x^\alpha, \quad \alpha_0 \in \mathbb{K},$$

where the sum is over a finite number of n-tuples $\alpha = \alpha_1, ..., \alpha_n$. The set of all polynomials in $x_1, ..., x_n$ with coefficients in k is denoted $k[x_1, ..., x_n]$.

Definition 3. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $\mathbb{K}[x_1, ..., x_n]$.
(i) We call a_α the coefficient of the monomial x^α.
(ii) If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a term of f.
(iii) The total degree of $f \neq 0$, denoted deg(f), is the maximum $|\alpha|$ such that the coefficient a_α is nonzero. The total degree of the zero polynomial is undefined.

Definition 4. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $\mathbb{K}[x_1, ..., x_n]$ and let $>$ be a monomial order.
(i) The multidegree of f is

$$multideg(f) = max(\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0)$$

(the maximum is taken with respect to $>$).
(ii) The leading coefficient of f is

$$LC(f) = a_{multideg(f)} \in k.$$

(iii) The leading monomial of f is

$$LM(f) = x^{multideg(f)}$$

(with coefficient 1).
(iv) The leading term of f is

$$LT(f) = LC(f) \cdot LM(f).$$

Definition 5. subset $I \subseteq \mathbb{K}[x_1, ..., x_n]$ is an ideal if it satisfies:
(i) 0 $\in$ I.
(ii) If f,g $\in$ I, then f + g $\in$ I.
(iii) If f $\in$ I and h $\in \mathbb{K}[x_1, ..., x_n]$, then $hf \in$ I.

Definition 6. Given a nonzero polynomial $f \in \mathbb{K}[x]$, let

$$f = c_0x^m + c_1x^{m-1} + \cdots + c_m,$$

where $c_i \in k$ and $c_0 \neq 0$ [thus, $m = deg(f)$]. Then we say that c_0x^m is the leading term of f , written $LT(f) = c_0x^m$.

Definition 7. Given a field k and a positive integer n, we define the n-dimensional affine space over k to be the set $\mathbb{K}^n = \{(a_1, ..., a_n)|a_1, ..., a_n \in \mathbb{K}\}$.

Definition 8. Let k be a field, and let $f_1, ...f_s$ be polynomials in $\mathbb{K}[x_1, ..., x_n]$. Then we set
$V(f_1, ..., f_s) = \{(a_1, ..., a_n) \in \mathbb{K}^n|f_i(a_1, ..., a_n) = 0$ for all $1 \leq i \leq s\}$.
We call $V(f_1, ..., f_s)$ the affine variety defined by $f_1, ..., f_s$.

Definition 9. Let $V \subset \mathbb{K}^n$ be a variety. We denote by $I(V)$ the set

$$\{f \in \mathbb{K}[x_1, ..., x_n] : f(a_1, ..., a_n) = 0 \ \ for \ \ all \ \ (a_1, ..., a_n) \in V\}$$

Definition 10. The Zariski closure of a subset of affine space is the smallest affine algebraic variety containing the set. If $S \subseteq \mathbb{K}^n$, the Zariski closure of S is denoted $\overline{\text{S}}$ and is equal to $V(I(S))$.

Definition 11. An affine variety $V \subseteq \mathbb{K}^n$ is irreducible if whenever V is written in the form $V = V_1 \cup V_2$, where V_1 and V_2 are affine varieties, then either $V_1 = V$ or $V_2 = V$.

Definition 12. An ideal $I \subseteq \mathbb{K}[x_1, ..., x_n]$ is prime if whenever
$f, g \in k[x_1, ..., x_n]$ and $fg \in I$, then either $f \in I$ or $g \in I$.

Definition 13. Let $V \subseteq \mathbb{K}^n$ be an affine variety. A decomposition

$$V = V_1 \cup ... \cup V_m,$$

where each V_i is an irreducible variety, is called a minimal decomposition (or, sometimes, an irredundant union) if $V_i \nsubseteq V_j$ for $i \neq j$. Also, we call the V_i the irreducible components of V.

Definition 14. An ideal I in $\mathbb{K}[x_1, ..., x_n]$ is primary if $fg \in I$ implies either $f \in I$ or some power $g^m \in I$ for some $m > 0$.

Definition 15. If I is primary and $\sqrt{I} = P$, then we say that I is P-primary.

Definition 16. If I and J are two ideals in $\mathbb{K}[x_1, ..., x_n]$, then their product, denoted IJ, is defined to be the ideal generated by all polynomials fg where $f \in I$ and $g \in J$. Thus, the product $I \cdot J$ of I and J is the set

$$IJ = \{f_1g_1 + \cdots + f_rg_r \mid f_1, ..., f_r \in I, g_1, ..., g_r \in J, r \ \ a \ \ positive \ \ integer\}.$$

Definition 17. Let $f_1, ..., f_s$ be polynomials in $\mathbb{K}[x_1, ..., x_n]$. Then we set

$$< f_1, ..., f_s >= \{\sum_{i=1}^{s} h_if_i \mid h_1, ..., h_s \in \mathbb{K}[x_1, ..., x_n]\}.$$

We will call $< f_1, ..., f_s >$ the ideal generated by $f_1, ..., f_s$.

Definition 18. Let $I \subset \mathbb{K}[x_1, ..., x_n]$ be an ideal. The radical of I is the set

$$\sqrt{I} = \{g \in k[x_1, ..., x_n] : g^m \in I \ \ for \ \ some \ \ m \geqslant 1\}$$

Definition 19. A monomial order on $k[x_1, ..., x_n]$ is any relation $>$ on the set of monomials x^α in $k[x_1, ..., x_n]$ (or equivalently on the exponent vectors $\alpha \in Z^n{}_{\geq 0}$) satisfying:
(i) $>$ is a total (linear) ordering relation;
(ii) $>$ is compatible with multiplication in $\mathbb{K}[x_1, ..., x_n]$, in the sense that if $x^\alpha > x^\beta$ and x^γ is any monomial, then $x^\alpha x^\gamma = x^{\alpha+\gamma} > x^{\beta+\gamma} = x^\beta x^\gamma$;
(iii) $>$ is a well-ordering. That is, every nonempty collection of monomials has a smallest element under $>$.

Theorem 20. **(Division Algorithm in Ring of Polynomial)** *Let $>$ be a monomial order on ${Z^n}_{\geq 0}$, and let $F = (f_1, ..., f_s)$ be an ordered s-tuple of polynomials in $k[x_1, ..., x_n]$. Then every $f \in k[x_1, ..., x_n]$ can be written as*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

where $q_i, r \in \mathbb{K}[x_1, ..., x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in k, of monomials, none of which is divisible by any of $LT(f_1), ..., LT(f_s)$.
We call r a remainder of f on division by F. Furthermore, if $q_i f_i \neq 0$, then

$$multideg(f) \geq multideg(q_i f_i)$$

Input:$f_1, ..., f_s, f$
Output:$q_1, ..., q_s, r$

```
$q_1 := 0; ...; q_s := 0; r := 0$
$p := f$
WHILE $p \neq 0$ DO
        $i := 1$
        divisionoccured := false
        WHILE $i \leq s$ AND divisionoccured = false DO
            IF $LT(f_i)$ divides $LT(p)$ THEN
                    $q_i := q_i + LT(p)/LT(f_i)$
                    $p := p - (LT(p)/LT(f_i))f_i$
                    divisionoccured := true
            ELSE
                    $i := i + 1$
        IF divisionoccured = false THEN
            $r := r + LT(p)$
            $p := p - LT(p)$
RETURN $q_1, ..., q_s, r$
```

Proof. See [2] Theorem 2.3.3 □

1.2 Gröbner Bases

Definition 21. An ideal $I \subseteq \mathbb{K}[x_1, ..., x_n]$ is a monomial ideal if there is a subset $A \subseteq {Z^n}_{\geq 0}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in \mathbb{K}[x_1, ..., x_n]$. In this case, we write $I =< x^\alpha \mid \alpha \in A >$.

Lemma 22. *Let $I = \langle x^\alpha | \alpha \in A\rangle \subseteq K[x_1, \cdots, k_n]$ be a monomial ideal. Then a monomial x^β lies in I if and only if x^β is divisible by x^α for some $\alpha \in A$.*

Proof. If x^β is a multiple of x^α for some $\alpha \in A$, then $x^\beta \in I$ by definition of ideal. Conversely, if $x^\beta \in I$, then $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$, where $h_i \in K[x_1, \cdots, x_n]$ and $\alpha(i) \in A$. If we expand each h_i as a sum of terms, we obtain

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)} = \sum_{i=1}^{s} (\sum_j c_{i,j} x^{\beta(i,j)}) x^{\alpha(i)} = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}$$

After collecting terms of the same multidegree, every term on the right side of the equation is divisible by some $x^{\alpha(i)}$. Hence, the left sidex^β must have the same property. □

Corollary 23. *Two monomial ideals are the same if and only if they contain the same monomials.*

Theorem 24. **(Dicksons Lemma)** *Let $I = \langle x^\alpha | \alpha \in A\rangle \subseteq K[x_1, \cdots, k_2]$ be a monomial ideal. Then I can be written in the form $I = \langle x^{\alpha(1)}, \cdots, x^{\alpha(s)}\rangle$, where $\alpha(1), ..., \alpha(s) \in A$. In particular, I has a finite basis.*

Proof. (By induction on n, the number of variables) If $n = 1$, then I is generated by the monomials X_1^α, where $\alpha \in A \subseteq \mathbb{Z}_{\geq 0}$. Let β be the smallest element of $A \subseteq \mathbb{Z} \geq 0$. The $\beta \leq \alpha$ for all $\alpha \in A$. Then $\beta \leq \alpha$ for all $\alpha \in A$, so that x_1^β divides all other generators x_1^α. From here, $I = \langle x_1^\beta \rangle$ follows easily. Now assume that $n > 1$ and that the theorem is true for $n-1$. We will write the variables as $x_1, \cdots, x_{n-1}, y$, so that monomials in $K[x_1, \cdots, x_{n-1}, y]$ can be written as $x^\alpha y^m$, where $\alpha = (a_1, \cdots, a_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ and $m \in \mathbb{Z}_{\geq 0}$. Suppose that $I \subseteq K[x_1, \cdots, x_{n-1}, y]$ is a monomial ideal. To find generators for I, let J be the ideal in $K[x_1, cdots, x_{n-1}]$generated by the monomials x^α for which $x^\alpha y^m \in I$ for some $m \geq 0$. Since J is a monomial ideal in $K[x_1, \cdots, x_{n-1}]$, our inductive hypothesis implies that finitely many of the x^α's generate J, say $J = \langle x^{\alpha(1)}, \cdots, x^{\alpha(s)}\rangle$. The ideal J can be understood as the projection of I into $K[x_1, \cdots, x_{n-1}]$.

For each i between 1 and s, the definition of J tells us that $x^{\alpha(i)} y^{m_i} \in I$ for some $m_i \geq 0$. Let m be the largest of the m_i Then, for each l between 0 and $m1$, consider the ideal $J_l \subseteq K[x_1, \cdots, x_{n-1}]$ generated by the monomials x^β such that $x^\beta y^l \in I$ One can think of J_l as the slice of I generated by monomials containing y exactly to the l th power. Using our inductive hypothesis again, J_l has a finite generating set of monomials, say $J_l = \langle x^{\alpha_l(1)}, \cdots, x^{\alpha_l(s_l)}\rangle$.

We claim that I is generated by the monomials in the following list:

$$\begin{gathered}
\text{from } J : x^{\alpha(1)} y^m, \cdots, x^{\alpha(s) y^m}, \\
\text{from } J_0 : x^{\alpha_0(1)}, \cdots, x^{\alpha_0(s_0)} , \\
\text{from } J_1 : x^{\alpha_1(1)} y, \cdots, x^{\alpha_1(s_1)} y \\
\vdots
\end{gathered}$$

$$\text{from } J_{m-1} : x^{\alpha_{m-1}(1)}y^{m-1}, \cdots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1}$$

First note that every monomial in I is divisible by one on the list. To see why, let $x^\alpha y^p \in I$. If $p \geq m$, then $x^\alpha y^p$ is divisible by some $x^{\alpha(i)}y^m$ by the construction of J. On the other hand, if $p \leq m-1$, then $x^\alpha y^p$ is divisible by some $x^{\alpha_p(j)}y^p$ by the construction of J_p. It follows from Lemma 22 that the above monomials generate an ideal having the same monomials as I. By Corollary 23, this forces the ideals to be the same, and our claim is proved. To complete the proof, we need to show that the finite set of generators can be chosen from a given set of generators for the ideal. If we switch back to writing the $x_1, \cdots x_n$, then our monomial ideal is $I = \langle x^\alpha | \alpha \in A\rangle \subseteq K[x_1, \cdots, x_n]$. We need to show that I is generated by finitely many of the x^α's, where $\alpha \in A$. By the previous paragraph, we know that $I = \langle x^{\beta(1)}, \cdots, x^{\beta(s)}\rangle$ for some monomials $x^{\beta(i)}$ in I. Since $x^{\beta(i)} \in I = \langle x^\alpha : \alpha \in A\rangle$, Lemma 2 tells us that each $x^{\beta(i)}$ is divisible by $x^{\alpha(i)}$ for some $\alpha(i) \in A$. From here, it is easy to show that $I = \langle x^{\alpha(1)}, \cdots, x^{\alpha(s)}\rangle$. □

Theorem 25. **(Hilbert Basis Theorem)** *Every ideal $I \subseteq K[x_1, \cdots, x_n]$ has a finite generating set. In other words, $I = \langle g_1, \cdots, g_t\rangle$ for some $g_1, \cdots, g_t \in I$*

Proof. If $I = \{0\}$, we take our generating set to be $\{0\}$, which is certainly finite. If I contains some nonzero polynomial, then a generating set $g_1, \cdots, g_t$ for I can be constructed as follows.

We first select one particular monomial order to use in the division algorithm and in computing leading terms. Then I has an ideal of leading terms $\langle LT(I)\rangle$, there are $g_1, \cdots, g_t \in I$ such that $\langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_t)\rangle$. We claim that $I = \langle g_1, \cdots, g_t\rangle$. It is clear that $\langle g_1, \cdots, g_t\rangle \subseteq I$ since each $g_i \in I$. Conversely, let $f \in I$ be be any polynomial. If we apply the division algorithm to divide f by $(g_1, \cdots, g_t)$, then we get an expression of the form

$$f = q_1g_1 + \cdots + q_tg_t + r$$

where no term of r is divisible by any of $LT(g_1), \cdots, LT(g_t)$. We claim that $r = 0$. To see this, note that

$$r = f - q_1g_1 - \cdots - q_tg_t \in I$$

If $r \neq 0$ then $LT(r) \in \langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_t)\rangle$ then $LT(r)$ must be divisible by some $LT(g_i)$. This contradicts what it means to be a remainder, and, consequently, r must be zero. Thus,

$$f = q_1g_1 + \cdots + q_tg_t + 0 \in \langle g_1, \cdots, g_t\rangle$$

which shows that $I \subseteq \langle g_1, \cdots, g_t\rangle$. This completes the proof. □

Definition 26. Let $I \subseteq \mathbb{K}[x_1, ..., x_n]$ be an ideal other than $\{0\}$, and fix a monomial ordering on $\mathbb{K}[x_1, ..., x_n]$. Then we denote by LT(I) the set of leading terms of nonzero elements of I.

Thus,

$$LT(I) = \{cx^\alpha \mid \ there \ exists \ f \in I \setminus 0 \ with \ LT(f) = cx^\alpha\}$$

Definition 27. Fix a monomial order on the polynomial ring $\mathbb{K}[x_1, ..., x_n]$. A finite subset $G = \{g_1, ..., g_t\}$ of an ideal $I \subseteq \mathbb{K}[x_1, ..., x_n]$ different from 0 is said to be a Gröbner basis (or standard basis) if

$$< LT(g_1), ..., LT(g_t) >=< LT(I) >$$

The proof of Theorem 25 also establishes the following result:

Corollary 28. *Fix a monomial order. Then every ideal $I \subseteq \mathbb{K}[x_1, ..., x_n]$ has a Gröbner basis. Furthermore, any Gröbner basis for an ideal I is a basis of I.*

Proof. Given a nonzero ideal, the set $G = \{g_1, ..., g_t\}$ constructed in the proof of Theorem 25 is a Grbner basis by definition. For the second claim, note that if $< LT(I) >=< LT(g_1), ..., LT(g_t) >$, then the argument given in Theorem 25 shows that $I =< g_1, ..., g_t >$, so that G is a basis for I. □

Proposition 29. *Let $I \subseteq \mathbb{K}[x_1, \cdots, x_n]$ be an ideal and let $G = \{g_1, \cdots, g_t\}$ be a Grbner basis for I. Then given $f \in \mathbb{K}[x_1, \cdots, x_n]$, there is a unique $r \in \mathbb{K}[x_1 \cdots, x_n]$ with the following two properties:*
(i) No term of r is divisible by any of $LT(g_1), \cdots, LT(g_t)$.
(ii) There is $g \in I$ such that $f = g + r$. In particular, r is the remainder on division of f by G no matter how the elements of G are listed when using the division algorithm.

Proof. See [1] Proposition 2.6.1 □

Corollary 30. *Let $G = \{g_1, ..., g_t\}$ be a Gröbner basis for an ideal $I \subseteq \mathbb{K}[x_1, \cdots, x_n]$ and let $f \in \mathbb{K}[x_1, \cdots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.*

Proof. If the remainder is zero, then we have already observed that $f \in I$. Conversely, given $f \in I$, then $f = f + 0$ satisfies the two conditions of Proposition 29. It follows that 0 is the remainder of f on division by G. □

Definition 31. We will write $\bar{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, ..., f_s)$. If F is a Gröbner basis for $< f_1, ..., f_s >$, then we can regard F as a set (without any particular order) by Propostion 29.

Definition 32. Let $f, g \in \mathbb{K}[x_1, ..., x_n]$ be nonzero polynomials.
(i) if multideg(f) $= \alpha$ and multideg(g) $= \beta$, then let $\gamma = (\gamma_1, ..., \gamma_n)$, where $\gamma_i = max(\alpha_i, \beta_i)$ for each i. We call x^γ the least common multiple of $LM(f)$ and $LM(g)$, written $x^\gamma =$

$lcm(LM(f), LM(g))$.
(ii) The S-polynomial of f and g is the combination

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

In corollary 28, we saw that every ideal in $k[x_1, ..., x_n]$ has a Gröbner basis. Unfortunately, the proof given was nonconstructive in the sense that it did not tell us how to produce the Gröbner basis. The Buchberger Algorithm helps us to achieve the desired result:

Theorem 33. **(Buchberger's Algorithm)** *Let $I =< f_1, ..., f_s >\neq \{0\}$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps by the fowllowing algorithm:*
Input : $F = (f_1, ..., f_s)$
Output : a Gröbner basis $G =< g_1, ..., g_t >$ for I, with $F \subseteq G$

```
G := F
REPEAT

        G' := G
        FOR each pair $\{p, q\}, p \neq q$ in G' DO
                $r := \overline{\mathrm{S(p, q)}}^{G'}$
                IF $r \neq 0$ THEN $G := G \cup \{r\}$

UNTIL $G = G'$
RETURN G
```

Proof. See [2] Theorem 2.7.2 □

1.3 Application of Gröbner Bases

1.3.1 Elimination Theory

Definition 34. Given $I = \langle f_1, \cdots, f_s\rangle \subseteq \mathbb{K}[x_1, \cdots, x_n]$, the $l-$th **elimination ideal** I_l is the ideal of $\mathbb{K}[x_{l+1}, \cdots, x_n]$ defined by

$$I_l = I \cap \mathbb{K}[x_{l+1}, \cdots, x_n]$$

Thus, I_l consists of all consequences of $f_1 = \cdots = f_s = 0$which eliminate the variables $x_1, \cdots, x_l$. In the exercises, you will verify that I_l is an ideal of $k[x_{l+1}, \cdots, x_n]$. Note that $I = I_0$ is the $0 - th$ elimination ideal. Also observe that different orderings of the variables lead to different elimination ideals. Using this language, we see that eliminating $x_1, \cdots, x_l$ means finding nonzero polynomials in the $l-th$ elimination ideal I_l. Thus a solution of the Elimination Step means giving a systematic procedure for finding elements of I_l . With the proper term ordering, Gröbner bases allow us to do this instantly [1].

Theorem 35. The Elimination Theorem *Let $I \subseteq \mathbb{K}[x_1, \cdots, x_n]$ be an ideal and let G be a Grbner basis of I with respect to lex order where $x_1 > x_2 > \cdots > x_n$. Then, for every $0ln$, the set*

$$G_l = G \cap \mathbb{K}[x_{l+1}, \cdots, x_n]$$

is a Gröbner basis of the $l-th$ elimination ideal I_l .

Proof. Fix l between 0 and n. Since $G_l \subseteq I_l$ by construction, it suffices to show that

$$\langle LT(I_l)\rangle = \langle LT(G_l)\rangle$$

by the definition of Gröbner basis. One inclusion is obvious, and to prove the other inclusion $\langle LT(I_l)\rangle \subseteq \langle LT(G_l)\rangle$, we need only to show that the leading term $LT(f)$, for an arbitrary $f \in I_l$, is divisible by $LT(g)$ for some $g \in G_l$.

To prove this, note that f also lies in I, which tells us that $LT(f)$ is divisible by $LT(g)$ for some $g \in G$ since G is a Gröbner basis of I. Since $f \in I_l$, this means that $LT(g)$ involves only the variables $x_{l+1}, \cdots, x_n$. Now comes the crucial observation: since we are using lex order with $x_1 > \cdots > x_n$, any monomial involving $x_1, \cdots, x_l$ is greater than all monomials in $\mathbb{K}[x_{l+1}, \cdots, x_n]$, so that $LT(g) \in \mathbb{K}[x_{l+1}, \cdots, x_n]$ im- plies $g \in \mathbb{K}[x_{l+1}, ..., x_n]$. This shows that $g \in G_l$, and the theorem is proved. □

Example 36. [2] Consider the system of equations

$$\begin{cases} x^2 + y^2 + z^2 = 4 \\ x^2 + 2y^2 = 5 \\ xz = 1 \end{cases}$$

We first compute a lex Grbner basis for the ideal they generate using Maple:

```
with(Groebner):
PList := [x^2+y^2+z^2-4, x^2+2*y^2-5, x*z-1];
G := gbasis(PList,plex(x,y,z));
```

This gives output

$$G := [1 + 2z^4 - 3z^2, y^2 - z^2 - 1, x + 2z^3 - 3z]$$

From the Gröbner basis it follows that the set of solutions of this system in $\mathbb{C}^3$ is finite. To find all the solutions, note that the last polynomial depends only on z (it is a generator of the second elimination ideal $I_2 = I \cap \mathbb{C}[z]$ and factors nicely in $\mathbb{Q}[z]$ To see this, we may use

```
factor(2*z^4 - 3*z^2 + 1);
```

which generates the output

$$(z-1)(z+1)(2z^2-1)$$

Thus we have four possible z values to consider:

$$z = \pm 1, \pm 1/\sqrt{2}$$

By the Elimination Theorem, the first elimination ideal $I_1 = I \cap \mathbb{C}[y, z]$ is generated by

$$y^2 - z^2 - 1$$

$$2z^4 - 3z^2 + 1$$

Since the coefficient of y^2 in the first polynomial is a nonzero constant, every partial solution in $V(I_2)$ extends to a solution in $V(I_1)$. There are eight such points in all. To find them, we substitute a root of the last equation for z and solve the resulting equation for y. For instance,

```
subs(z=1,G);
```

will produce:

$$[-1 + x, y^2 - 2, 0],$$

so in particular,$y = \pm\sqrt{2}$ In addition, since the coefficient of x in the first polynomial in the Gröbner basis is a nonzero constant, we can extend each partial solution in $V(I_1)$ (uniquely) to a point of $V(I)$. For this value of z, we have $x = 1$. Doing the same process for the other values of z find out the eight points

$$(1, \pm\sqrt{2}, 1)(-1, \pm\sqrt{2}, -1)(\sqrt{2}, \pm\sqrt{6}/2, 1/\sqrt{2})(-\sqrt{2}, \pm\sqrt{6}/2, -1/\sqrt{2})$$

form the set of solutions.

Definition 37. Partial Solutions A point $(a_{l+1}, \cdots, a_n) \in V(I_l) \subset k^{n-l}$ is called a partial solution.

Any solution$(a_1, \cdots, a_n) \in V(I) \subset \urcorner^n$ truncates to a partial solution, but the converse may failnot all partial solutions extend to solutions. This is where the Extension Theorem comes in. To prepare for the statement, note that each f in I_{l-1} can be written as a polynomial in x_l, whose coefficients are polynomials in $x_{l+1}, \cdots, x_n$:

$$f = c_q(x_{l+1}, \cdots, x_n)x_l^q + \cdots + c_0(x_{l+1}, \cdots, x_n).$$

We call c_q the leading coefficient polynomial of f if x_l^q is the highest power of x_l appearing in f.

Theorem 38. The Extension Theorem *If k is algebraically closed (e.g., $k = \mathbb{C}$), then a partial solution $(a_{l+1}, \cdots, a_n)$ in $V(I_l)$ extends to $(a_l, a_{l+1}, \cdots, a_n)$ in $V(I_{l1})$ provided that the leading coefficient polynomials of the elements of a lex Gröbner basis for I_{l-1} do not all vanish at $(a_{l+1}, \cdots, a_n)$.*

1.3.2 Saturation

Definition 39. If I, J are ideals in $\mathbb{K}[x_1, ..., x_n]$, then $I : J$ is the set

$$\{f \in \mathbb{K}[x_1, ..., x_n] \mid fg \in I \text{ for all } g \in J\}$$

and is called the ideal quotient (or colon ideal) of I by J.

Definition 40. If I and J are ideals of the ring $\mathbb{K}[x_1, ..., x_n]$, then the sum of I and J, denoted $I + J$, is the set

$$I + J = \{f + g \mid f \in I \ \ and \ \ g \in J\}$$

Proposition 41. *If I,J are ideals in $\mathbb{K}[x_1, ..., x_n]$, then the ideal quotient I:J is an ideal in $\mathbb{K}[x_1, ..., x_n]$ and I:J contains I.*

Proof. To show I:J contains I, note that because I is an ideal, if $f \in I$, then $fg \in I$ for all $g \in \mathbb{K}[x_1, ..., x_n]$ and, hence, certainly $fg \in I$ for all $g \in J$. To show that $I : J$ is an ideal, first note that $0 \in I : J$ because $0 \in I$. Let $f_1, f_2 \in I : J$. Then f_1g and f_2g are in I for all $g \in J$. Since J is an ideal $(f_1 + f_2)g = f_1g + f_2g \in I$ for all $g \in J$. Thus, $f_1 + f_2 \in I : J$. To check closure under multiplication is equally straightforward: if $f \in I : J$ and $h \in \mathbb{K}[x_1, ..., x_n]$ then $fg \in I$ and, since I is an ideal, $hgf \in I$ for all $g \in J$, which means that $hf \in I : J$. □

Definition 42. If I, J are ideals in $\mathbb{K}[x_1, ..., x_n]$, then $I : J^\infty$ is the set

$$\{f \in \mathbb{K}[x_1, ..., x_n] \mid \ for \ \ all \ \ g \in J, there \ \ is \ \ N \geqslant 0 \ \ such \ \ that \ \ fg^N \in I\}$$

and is called the saturation of I with respect to J.

Theorem 43. *Let I and J be ideals in $\mathbb{K}[x_1, ..., x_n]$. Then:*

(i) $V(I) = V(I + J) \cup V(I : J^{\infty})$.
(ii) $\overline{\text{V(I)} \setminus \text{V(J)}} \subseteq V(I : J^{\infty})$.
(iii) If k is algebraically closed, then $V(I : J^{\infty}) = \overline{\text{V(I)} \setminus \text{V(J)}}$.

Proof. See [1] Propostion 10.4.4 □

2 Gröbner Bases for Modules

In this chapter, we will generalize the definitions and notions discussed in the first chapter and apply it on modules. We start by giving you some definitions about modules and explain the structure of them. Then we will develop the theory of Gröbner Basis on Modules. in the end of the chapter, we will introduce aglorithms for computing a Gröbner Basis of a Module.

Definition 1. A module over a ring R(or R-module) is a set M together with a binary operation, usually written as addition, and an operation of R on M, called (scalar) multiplication, satisfying the following properties.

(i) M is an abelian group under addition. That is, addition in M is associative and commutative, there is an additive identity element $0 \in M$, and each element $f \in M$ has an additive inverse $-f$ satisfying $f + (-f) = 0$.
(ii) For all $a \in R$ and all $f, g \in M, a(f + g) = af + ag$.
(iii) For all $a, b \in R$ and all $f \in M, (a + b)f = af + bf$.
(iv) For all $a, b \in R$ and all $f \in M, (ab)f = a(bf)$
(v) If 1 is the multiplicative identity in R, $1f = f$ for all $f \in M$.

Definition 2. Let $>$ be any monomial order on R.
(i)(TOP extension of $>$) We say $x^{\alpha}e_i >_{TOP} x^{\beta}e_j$ if $x^{\alpha} > x^{\beta}$, or if $x^{\alpha} = x^{\beta}$ and $i < j$.
(ii) (POT extension of $>$) We say $x^{\alpha}e_i >_{POT} x^{\beta}e_j$ if $i < j$, or if $i = j$ and $x^{\alpha} > x^{\beta}$.

TOP stands for term-over-position, which is certainly appropriate since a TOP order sorts monomials first by the term order on R, then breaks ties using the position within the vector in R^m. On the other hand, POT stands for position-over-term."

Theorem 3. *Theorem (Division Algorithm in R^m). Fix any monomial ordering on R^m and let $F = (f_1, ..., f_s)$ be an ordered s-tuple of elements of R^m. Then every $f \in R^m$ can be written as*

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

where $a_i \in R, r \in R^m, LT(a_i f_i) \geq LT(f)$ for all i, and either $r = 0$ or r is a k-linear combination of monomials none of which is divisible by any of $LM(f_1), ..., LM(f_s)$. We call r the remainder on division by F.

Proof. See [2] Theorem 2.5 □

Definition 4. Let M be a submodule of R^m, and let $>$ be a monomial order.
(i) We will denote by $< LT(M) >$ the monomial submodule generated by the leading terms of all $f \in M$ with respect to $>$.
(ii) A finite collection $G = \{g_1, ..., g_s\} \subset M$ is called a Gröbner Basis for M if $< LT(M) >=< LT(g_1), ..., LT(g_s) >$.

Definition 5. Fix a monomial order on R^m, and let $f, g \in R^m$. The s-vector of f and g, denoted $S(f, g)$, is the following element of R^m. Let $m = LCM(LT(f), LT(g))$ as defined above. Then

$$S(f, g) = \frac{m}{LT(f)}f - \frac{m}{LT(g)}g.$$

Theorem 6. *(Buchberger's Algorithm for Submodules). Let $F = (f_1, ..., f_s)$ where $f_i \in R^m$, and fix a monomial order on R^m. The following algorithm computes a Gröbner Basis G for $M =< F >\subset R^m$, where $\overline{\mathrm{S(f, g)}}^{G'}$ denotes the remainder on division by G', using Theorem 3:*
Input : $F = (f_1, ..., f_t) \subset R^m$, an order $>$
Output : a Gröbner basis G for $M =< F >$, with respect to $>$

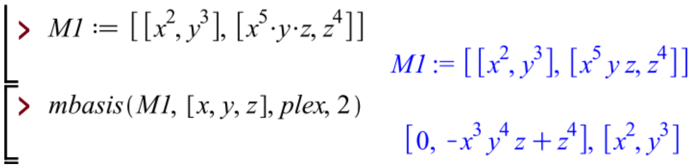
```
$G := F$
REPEAT

        $G' := G$
        FOR each pair $\{p, q\}, p \neq q$ in $G'$ DO
                $S := \overline{\mathrm{S(p, q)}}^{G'}$
                IF $r \neq 0$ THEN $G := G \cup \{r\}$

UNTIL $G = G'$
RETURN G
```

Proof. The proof is essentially the same as in the ideal case. □

For computing Gröbner Basis of a module, besides Buchberger algorithm, there is another slightly tricky approach too. In this approach, we transform the given module to a ring and and compute a Gröbner Basis for that ring. Then we return from this Basis to a module which preserves being a Gröbner Basis in modules. In the following, You can see the MAPLE executions which computes the Gröbner Basis of a module using this method in here:

```
> #Module's Groebner Basis
  mbasis :=proc(M :: list, L :: list, order, n)
   local J, G, T, i, j, o2, o1, o, g, R;
   J := NULL :
   G := NULL :
   R := NULL :
   T := [seq(x[i], i = 1 ..n)];
   for i from 1 to nops(M) do
   J := J, sum(M[i][j]·T[j], j = 1 ..n);
   od;
   J := [J];
   o2 := order(op(Reverse(L))) :
   o1 := plex(op(T)) :
   o := prod(o1, o2) :
   G := Basis(J, o);
   g := nops(G) :
   i := 1 :
  while i ≤ g do
   if degree(G[i], T) > 1 then
  G := subsop(i = NULL, G);
   fi;
  g := nops(G) :
   i := i + 1 :
   od;
  R := seq([subs(T[1] = 1, T[2] = 0, u), subs(T[1] = 0, T[2] = 1, u)], u = G);
   return(R) :
   end:
```

An Example for computing a module's Groöbner Basis:



```
> M1 := [[x^2, y^3], [x^5·y·z, z^4]]
                    M1 := [[x^2, y^3], [x^5 y z, z^4]]
> mbasis(M1, [x, y, z], plex, 2)
                    [0, -x^3 y^4 z + z^4], [x^2, y^3]
```

3 Paper

3.1 Intrdoucion

In this paper, we want to introduce an algorithm for solving a system of polynomial equations. The polynomials belong to $\mathbb{K}[x_1, ..., x_n]$ where K is a field. Solving means finding the variety of the ideal generated by these polynomials. This algorithm, turns the given system to a system with triangular from:

$$f_1(x_1) = {x_1}^{d_1} + \sum_{j=0}^{d_1-1} g_{1,j}\ x^j{}_1,$$

$$f_2(x_1, x_2) = {x_2}^{d_2} + \sum_{j=0}^{d_2-1} g_{2,j}(x1)x^j{}_2, \qquad (3)$$

$$f_n(x_1, ..., x_n) = {x_n}^{d_n} + \sum_{j=0}^{d_n-1} g_{n,j}(x_1, ..., x_{n-1})x^j{}_n$$

This algorithm is based on a method for decomposing a variety into finite disjoint sets. By recursive use of this method, we obtain the decomposition and as a result, the triangular form is obtained. Suppose that we have a Gröbner basis of the ideal that represents the given system. In each recursion step, we "read off" some Gröbner basis four our intention. And in the end, only Gröbner bases remain that consist a triangular from. Lemma 7 allows us to "read off" the Gröbner bases that their computation needs no arithmetical operation. For decomposing, we use the notions of quotion ideal, sum ideal and some other notions that will be discussed in the following.

3.2 Ideals and Decompositions

In this section, we will prove some lemmas that will be used to decompose the variety of an ideal.

Lemma 1. *If A and B are ideals with $A \subseteqq B$, then for arbitrary $m \in \mathbb{N}$*

$$A \subseteqq B \cap (A : B^m) \subseteqq \sqrt{A}$$

If $A = \sqrt{A}$ and $A \subsetneqq B$, then $A = B \cap (A{:}B)$ and $A : B = A : B^m$ for all integer $m > 1$.

Proof. We know that

$$A : B = \{f \in \mathbb{K}[x_1, ..., x_n] \mid fg \in A \ \ for \ \ all \ \ g \in B\}^{39}$$

. First we prove by induction that for all $m \in \mathbb{N}$, $A : B^m \subsetneqq A : B^{m+1}$ and when $m = 0$, the assertion is this: $A \subsetneqq A : B$. For this case($m = 0$): If, $f \in A$ then for all $g \in B$, $fg \in A$ due to A being an ideal. Now suppose that for $i = 1, .., m$, the assertion holds. We will prove it for $m + 1$. We know that $A : B^m = \{f \in k[x_1, ..., x_n] \mid fg \in A$ for all $g \in B^m\}$ and $A : B^{m+1} = \{f \in k[x_1, ..., x_n] \mid fg \in A$ for all $g \in B^{m+1}\}$. Take an arbitrary $f \in A : B^m$. By definition, for all $g \in B^m$, we have $fg \in A$. Because $g \in B^m$, we have $g^2 \in B^{m+1}$. On the other hand, $fg.g = fg^2 \in A$ due to A being an ideal. So $f \in A : B^{m+1}$. This completes our induction. The assertion we proved gives this: $A \subsetneqq A : B^m$. And From assumption, we know $A \subsetneqq B$. This yields the first inclusion: $A \subsetneqq B \cap (A : B^m)$. For the second inclusion: Let $g \in B \cap A : B^m$, then $g \in B$ and $g \in A : B^m$. $g \in B \Rightarrow g^m \in B^m$. So by $g^{m+1} = g.g^m$ and $g \in A : B^m$, we have $g^{m+1} \in A$. This implies $g \in \sqrt{A}\square$. □

"If $V(A) = V(\sqrt{A})$, then lemma 1 implies the variety decomposition $V(A) = V(B) \cup V(A : B^m)$" [3] which is what we wanted. But the equality doesn't necessarily hold, so we introduce the next lemma:

Lemma 2. *Let A and B be as in Lemma 1 and, in addition, let dim(A) = 0. Then for sufficiently large $m \in \mathbb{N}$ the decomposition $V(A) = V(B) \cup V(A : B^m)$ holds with*

$$V(B) = \{y \in V(A) \mid \forall b \in B : b(y) = 0\},$$

$$V(A : B^m) = \{y \in V(A) \mid \exists b \in B : b(y) \neq 0\}.$$

Proof. For the first part, we do as follows. $A \subsetneqq B \Rightarrow V(B) \subsetneqq V(A)$. So by the definition of variety, it is obvious that $V(B) = \{y \in V(A) \mid \forall b \in B : b(y) = 0\}$.
The second part is obtained from Theorem 43

$$V(A : B^\infty) = \overline{\mathrm{V(A) - V(B)}}$$

but in here, the closure is not needed because the varieties are just sets of points. Therefore they are already closed in Zariski closure. and since the ascending chain of $A \subset A : g \subset A : g^2 \subset ...$ terminates due to K being Noetherian, the ∞ turns to a sufficiently large number m and we can saturate A by B with finite steps. So we have $V(A : B^m) = V(A) - V(B)$. Thus $V(A : B^m)$ consists of the points in V(A) which there is at least an element in ideal B which doens't have that point as root. This completes the proof. □

In the previous lemma we learnt that V(A) can be expresses by the variety of V(B) and $V(A : B^m)$. The decomposition of $V(A : B^m)$ is discussed in the next lemma:

Lemma 3. *Let dim(A) = 0 and $A \subseteqq B = (g_1, ..., g_s)$. Using $A_0 := A$, $A_i := A_{i-1} + (g_i)$, $i = 1, ..., s$, then for sufficiently large m, $m_1, ..., m_s \in \mathbb{N}$:*

$$V(A : B^m) = \bigcup_{i=1}^{s} V(A_{i-1} : {g_i}^{m_i}) \qquad (6)$$

with $V((A_{i-1})) : {g_i}^{m_i}) = \{y \in V(A) \mid g_i(y) = ... = g_{i-1}(y) = 0 \neq g_i(y)\}$. If A is in addition a radical, then (6) holds for all positive m,$m_1, ..., m_s$.

Proof. By Lemma 2, we know that $V(A : B^m) = \{y \in V(A) \mid \exists b \in B : b(y) \neq 0\}$. Considering $B = (g_1, ..., g_s)$, we have this: $V(A : B^m) = \{y \in V(A) \mid \exists i \leqq s : g_i(y) \neq 0\} = \bigcup_{i=1}^{s} \{y \in V(A) \mid g_1(y) = \cdots = g_{i-1}(y) = 0 \neq g_i(y)\}$. Since $A = A_0 \subseteqq A_{i-1}$, we can insert A_{i-1} as B in Lemma 2. Thus we get this:

$$V(A_{i-1}) = \{y \in V(A) \mid g_j(y) = 0 \;\; for \;\; all \;\; 1 \leqq k \leqq i-1\}$$

Now if we insert A_{i-1} as A and A_i as B. This implies: $A : B^{m_i} = A_{i-1} : {g_i}^{m_i}$ and

$$V(A_{i-1} : {g_i}^{m_i}) = \{y \in V(A_{i-1}) \mid g_i(y) \neq 0\}$$

Thus the varieties of $V(A_{i-1} : {g_i}^{m_i})$ are disjoint sets and their union equals $V(A : B^m)$.

□

Since the ascending chain of $A \subset A : g \subset A : g^2 \subset ...$ terminates due to K being Noetherian. So we can saturate each A_{i-1} by g_i and in result, m_i's are finite numbers.

3.3 Ideal Quotients and Gröbner Bases

In Sect.2 we learnt to describe an ideal A by ideals A_i. So we need a way to calculate bases for each $A_i = A_{i-1} + (g_i), i = 1, ..., s$.

We want to apply the decomposition given by Lemmas 2 and 3. Therefore, we need the computation of bases for the saturations of each A_{i-1} by g_i, with recursively defined $A_i := A_{i-1} + (g_i), i = 1, ..., s$.

"This computation is easier, if a Gröbner basis for A_{i-1} is already known. Therefore, we prefer to have an algorithm which, given a Gröbner basis of an ideal A_{i-1}, computes simultaneously a Gröbner basis for the next A_i and a Gröbner basis of the saturation of $A_{i-1} : g_i$." [3]

We will use modules for our purpose. We already know how to compute Gröbner bases for modules. Now we will introduce a module that will give us the desired bases for $A + g$ and $A : g$ in the following lemma:

Lemma 4. *Let $A = (a_1, ..., a_s)$ be an ideal and $0 \neq g \in \wp$. Then*

$$M := \{(u, v) \in \wp^2 \in u + g{\cdot}v \in A\}.$$

is a module with basis $\{(a_1, 0), ..., (a_r, 0), (g, -1)\}$. if $\pi_i : M \to \wp$ denotes the canonical projection on its i-th component, $i = 1, 2$, then

$$\pi_1(M) = A + (g), \qquad \pi_2(ker\pi_1) = A : g. \qquad (7)$$

Proof. We consider an element (u, v) of the module generated by the basis. Then we have:

$$(u, v) = c_1(a_1, 0) + ... + c_r(a_r, 0) + c(g, -1) \Rightarrow$$

$$u + g{\cdot}v = c_1a_1 + ... + c_ra_r + cg + g{\cdot}(-c) = c_1a_1 + ... + c_ra_r \in A$$

Thus $\{(a_1, 0), ..., (a_r, 0), (g, -1)\}$ is basis of the module $M = \{(u, v) \in \wp^2 \in u + g{\cdot}v \in A\}$. For proving the projections we do as follows.
For π_1,

$$\pi_1(M) = c_1a_1 + ... + c_ra_r + cg \in A + (g)$$

And for $\pi_2(ker\pi_1)$,

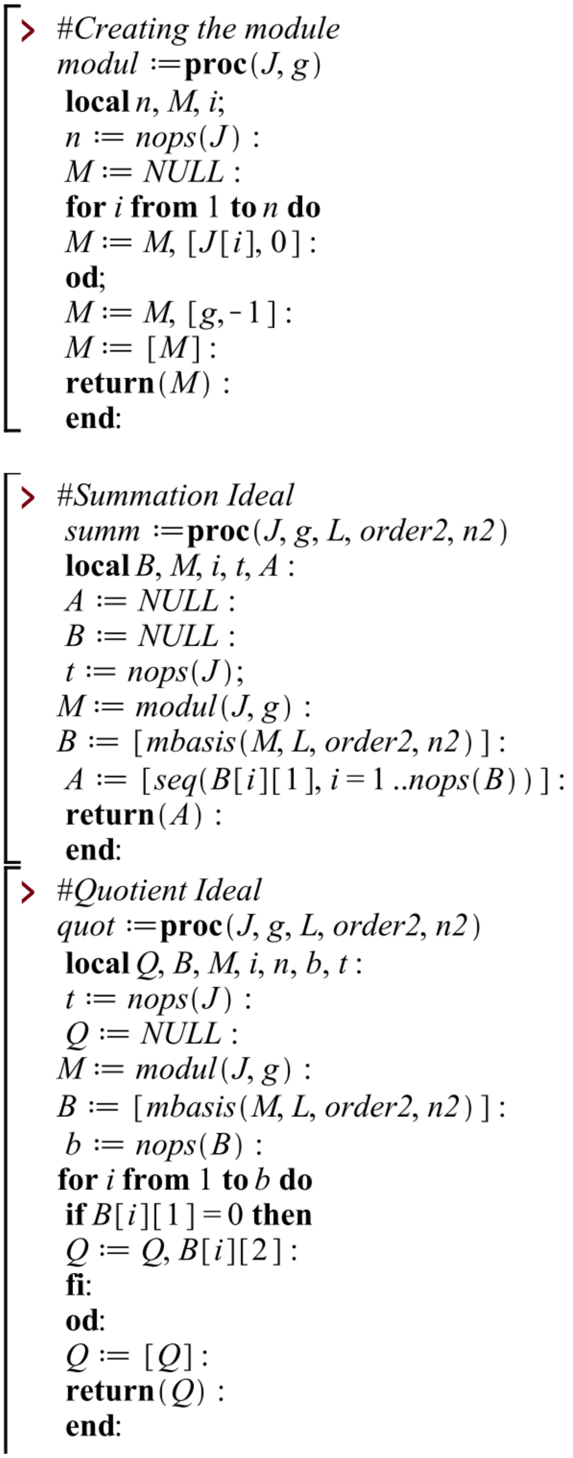
$$ker\pi_1(M) = \{(0, v) \mid (0, v) \in M\}$$

$$(0, v) \in M \Rightarrow 0 + g{\cdot}v \in A \Rightarrow v \in A : g$$

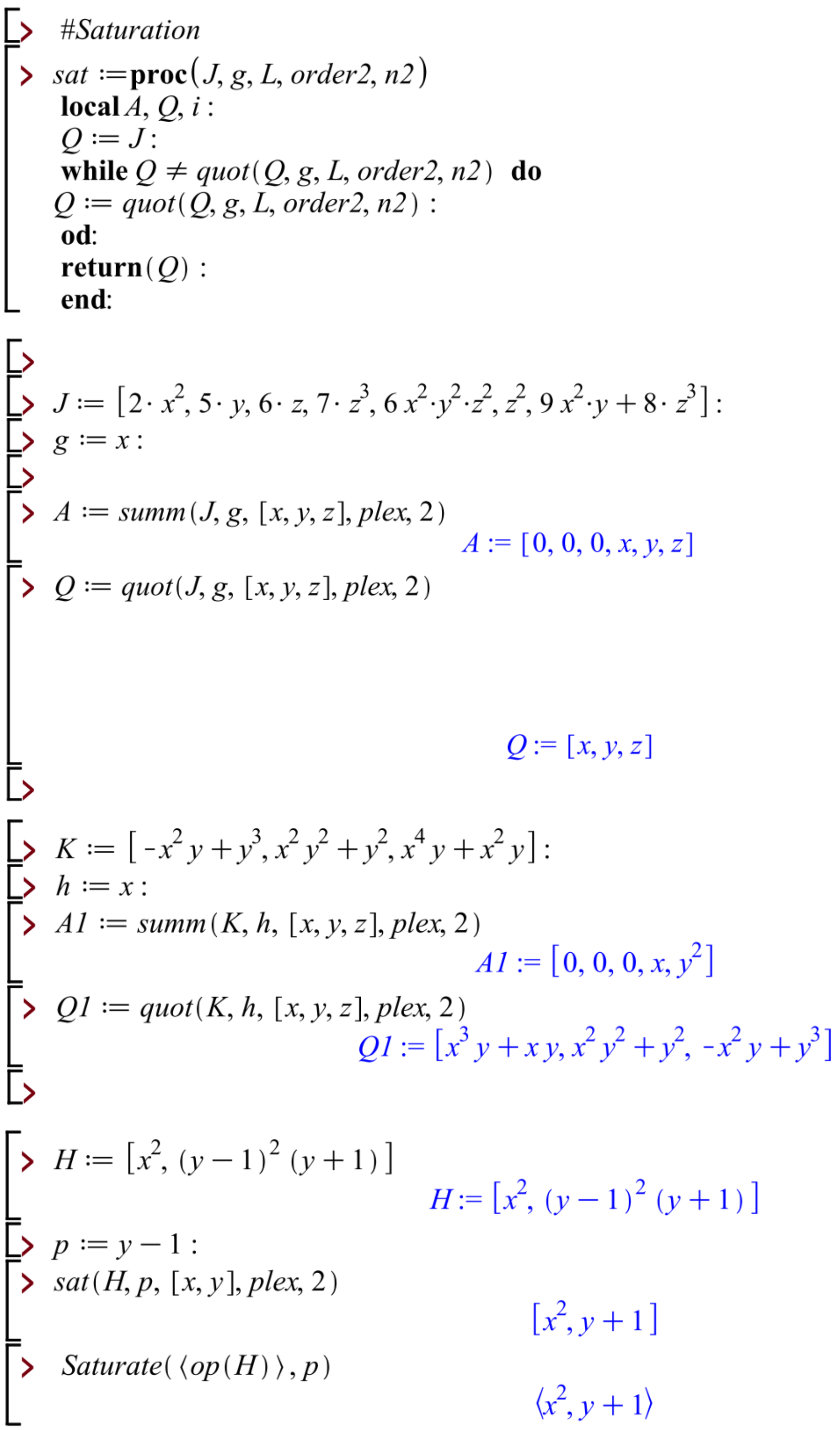
□

Remark 5. Note that $\pi_1(M)$ and $\pi_2(ker\pi_1)$ are already Gröbner bases for $A + (g)$ and $A : g$ respectively.

The computation of Gröbner basis for a module is discussed in the previous chapter. We said there that two orders (TOP and POT) can be used to compute the basis. Now we can use the module introduced in Lemma 4 to computer Gröbner bases for $A + g$ and $A : g$. We must use the order POT. We will also explain how to use these this module to compute Gröbner bases for the bases A_i and the saturation of each A_{i-1} by g_i in order to fulfil what is required for applying Lemma 3:
"if $\{a'_1, ..., a'_r\}$ is a Gröbner basis of $A : g$, then $(a'_1, 0), ..., (a'_r, 0), (g, -1)$ can be used to give in the same way a Gröbner basis for $A : g^2$ and for $A : g + (g)$. Iterating this procedure, we terminate until we get $A : g^k = A : g^{k+1}$, i.e. until the saturation and its index are found." [3]
You can see The MAPLE executions for computing saturation of an ideal by a polynomial in here. Note that for computing Gröbner basis of modules we use the technique introduced in 2:



```
> #Creating the module
  modul :=proc(J, g)
   local n, M, i;
   n := nops(J) :
   M := NULL :
   for i from 1 to n do
   M := M, [J[i], 0] :
   od;
   M := M, [g, -1] :
   M := [M] :
   return(M) :
   end:

> #Summation Ideal
   summ :=proc(J, g, L, order2, n2)
   local B, M, i, t, A :
   A := NULL :
   B := NULL :
   t := nops(J);
  M := modul(J, g) :
  B := [mbasis(M, L, order2, n2)] :
   A := [seq(B[i][1], i = 1 ..nops(B))] :
   return(A) :
   end:
> #Quotient Ideal
  quot :=proc(J, g, L, order2, n2)
   local Q, B, M, i, n, b, t :
   t := nops(J) :
   Q := NULL :
  M := modul(J, g) :
  B := [mbasis(M, L, order2, n2)] :
   b := nops(B) :
  for i from 1 to b do
   if B[i][1] = 0 then
   Q := Q, B[i][2] :
   fi:
   od:
   Q := [Q] :
   return(Q) :
   end:
```



```
> #Saturation
> sat :=proc(J, g, L, order2, n2)
  local A, Q, i :
  Q := J :
  while Q ≠ quot(Q, g, L, order2, n2)  do
 Q := quot(Q, g, L, order2, n2) :
  od:
  return(Q) :
  end:
>
> J := [2· x^2, 5· y, 6· z, 7· z^3, 6 x^2·y^2·z^2, z^2, 9 x^2·y + 8· z^3] :
> g := x :
>
> A := summ(J, g, [x, y, z], plex, 2)
                                   A := [0, 0, 0, x, y, z]
> Q := quot(J, g, [x, y, z], plex, 2)




                                      Q := [x, y, z]
>
> K := [ -x^2 y + y^3, x^2 y^2 + y^2, x^4 y + x^2 y] :
> h := x :
> A1 := summ(K, h, [x, y, z], plex, 2)
                                    A1 := [0, 0, 0, x, y^2]
> Q1 := quot(K, h, [x, y, z], plex, 2)
                          Q1 := [x^3 y + x y, x^2 y^2 + y^2, -x^2 y + y^3]
>
> H := [x^2, (y - 1)^2 (y + 1)]
                                H := [x^2, (y - 1)^2 (y + 1)]
> p := y - 1 :
> sat(H, p, [x, y], plex, 2)
                                        [x^2, y + 1]
> Saturate(⟨op(H)⟩, p)
                                        ⟨x^2, y + 1⟩
```

3.4 Decomposition into Triangular Systems

So far, we learnt how to decompose a variety of an ideal by saturation (Lemma 3). In this section want to introduce some tools for "reading off" Gröbner bases from a given one. And in the end of the section, we will introduce the algorithm.

Definition 6. Let $\{y_1, ..., y_r\}$ and $\{z_1, ..., z_r\}$ be disjoint subsets of $\{x_1, ..., x_r\}$. Then $\{y_1, ..., y_r\}$ will be called textitlexicographically infront of $\{z_1, ..., z_s\}$ with respect to $<_\tau$, if for arbitrary terms the following implication holds.

$$y_1{}^{i_1} ... y_r{}^{i_r} <_\tau y_1{}^{j_1} ... y_r{}^{j_r} \Rightarrow y_1{}^{i_1} ... y_r{}^{i_r} z_1{}^{k_1} ... z_r{}^{k_r} <_\tau y_1{}^{j_1} ... y_r{}^{j_r} z_1{}^{l_1} ... z_r{}^{l_r} \qquad (8)$$

This definition is useful for combining orders which order sets of terms for disjoint sets of variables. A special instance is the lexicographical order, where every $\{x_i\}$ is in front of $x_1, ..., x_{i-1}, i = 2, ..., n$. For deriving special properties of this lexicographical order, we show the following result."

Lemma 7. *Let x_n be lexicographically in front of $\{x_1, ..., x_{n-1}\}$ w.r.t $<_\tau$ and let $deg_{x_n}(f)$ denote the degree of f in x_n. The the following assertions hold:*
i) If $f_1, ..., f_r$ are polynomials with $deg_{x_n}(f_i) \leqq d, i = 1...r$, then $(f_1, ..., f_r)$, has a Gröbner basis w.r.t $<_\tau$, where every element f satisfies $deg_{x_n}(f) \leqq d$.
ii) If $F := \{f_1, ..., f_r\}$ is a Gröbner basis w.r.t. $<_\tau$, then $F_\wp := F \cap \{f \in \wp \mid deg_{x_n}(f) < k\}$ is a Gröbner basis (w.r.t. $<_\tau$) for all positive integers k.
iii) Let $f_i := \sum_{j=0}^{d_i} \widetilde{g}_{ij}(x_1, ..., x_{n-1}) x_n{}^{d_i - j}$ with nonzero polynomials $\widetilde{g}_{ij}, i = 1..., r$. if $F := \{f_1, ..., f_r\}$ is a Gröner basis w.r.t. $<_\tau$, then $G := \{\widetilde{g}_{10} ..., \widetilde{g}_{r0}\}$ is a Gröbner basis (w.r.t. $<_\tau$).

Proof. (i): If we consider the S-poly of each (f_i, f_j), we will show that in Buchberger algortihm, the degree of x_n in each f_i will stay less or equal than d and its upper bound will not not be affected during the alogrithm.

By definition, Spoly is defined as follows:

$$Spoly(f_i, f_j) = \frac{lcm(LM(f_i), LM(f_j))}{LT(f_i)} \cdot f_i - \frac{lcm(LM(f_i), LM(f_j))}{LT(f_j)} \cdot f_j$$

Since $deg_{x_n}(f) = deg_{x_n}(lt(f))$, in each term of $Spoly(f_i, f_j)$, The degree of x_n in $Spoly(f_i, f_j)$ is determined by $lcm(LM(f_i), LM(f_j))$. And in $lcm(LM(f_i), LM(f_j))$, degree of x_n is at most d, and $lcm(LM(f_i), LM(f_j))$ appears in both terms of Spoly. Thus their subtraction also satisfies the upper bound condition.
(ii): We know that $F = \{f_1, ..., f_r\}$ is a Gröner basis. So for each f_i and f_j, $Spoly(f_i, f_j) = 0$. In particular, we have:

$$\forall f, g \in F_k, Spoly(f, g) = 0$$

The degree of x_n in elements of F_k are at most d and in the elements of $F - F_k$ is higher than

d. so the latter elements will not appear in calculating Spoly of each pair of elements in F_k because in part(i) we showed that in Spoly the degree of x_n in elements will stay at most d. For (iii): We already know that for each f_i and f_j, $Spoly(f_i, f_j) = 0$.For $i = 1, ..., r$, because of the formation of each f_i, we see that the highest degree of x_n in each f_i only lies in its corresponding g_{i0} and in none of ther other terms. So in the procedure of calculating Spoly for an arbitrary pair (f_i, f_j) of elements of F, The leading terms of f_i's can only be vanisehd by their g_{i0}'s. So the Spoly of each pair of g_{i0} and g_{j0} should be zero too. Thus G is also a Gröbner basis. □

Algorithm for decomposing zero-dimensional varieties.
Input: $(\{f_1, ..., f_r\}; <_n)$, where $\{f_1, ..., f_r\}$ is a reduced Gröbner basis w.r.t $<_n$ of a zero-dimensional ideal A.
Output: A set Z of finitely many polynomial sets $\{g_1, ..., g_n\}$ of triangular type (3), such that V(A) is the union of the disjoint sets $V(g_1, ..., g_n), \{g_1, ..., g_n\} \in Z$.
Step 1: Let $lt(f_j) <_n lt(f_i)$ for $i > j$. Let $\widetilde{f_i} := lc_{x_n}(f_i) \in \mathbb{K}[x_1, ..., x_{n-1}]$ denote the leading coefficient of f_i considered as polynomial in $x_n, i > 1$. Let $G_1 := \{f_1, ..., f_r\}$. Reduce the lexicographical Gröbner basis $\{\widetilde{f}_1, ..., \widetilde{f}_r\}$ to a reduced Gröbner basis G.
Step 2: Call the alg. with input $(G; <_{n-1})$, resulting in a set Z' of finitely many sets $\{\widetilde{g}_1, ..., \widetilde{g}_{n-1}\}$. Let then Z denote the set of all polynomials
$\{\widetilde{g}_1, ..., \widetilde{g}_{n-1}, -\frac{1}{lc(f_1)} f_1\}, \{\widetilde{g}_1, ..., \widetilde{g}_{n-1}\} \in Z$
Step 3: For $i = 2, ..., r$ do while $\widetilde{f_i} \notin A$: Compute a Gröbner basis G'_i of $SAT(G_{i-1}, \widetilde{f_i}, <_n)$ and a Gröbner basis G_i of $(f_1, ..., f_r, \widetilde{f_2}, ..., \widetilde{f_r})$, both w.r.t the order $<_n$, call then the algorithm with input $(G'_i; <_n)$, and enlarge Z by the resulting triangular sets.

for proving termaion and correctness, see [3].
The MAPLE executions of algorithm is in here. Note that for computing SAT, we use the method in 3.3 :

```
> prog :=proc(F, order, L :: list)
 global Z :
 local H, N, G, G1, G2, T, J, h, r, i, j, temp, o, oo, z2, L2;
 option trace;
 if nops(F) = 1 then
 Z=Z, [F] :
 return(Z) :
 fi;
 if nops(L) = 1 then
 return(Z) :
 fi;
 if F = [1] then
 return(Z) :
 fi;
 #if IsZeroDimensional(F) ≠ 'true' then
#return(Z) :
# fi;
 o := order(op(L[-1])) :
 T := NULL :
 N := NULL :
 G := NULL :
 J := NULL :
 H := sort(F, (a, b) → TestOrder(b, a, o));
 r := nops(H);
 G1 := H:
 G2 := H:
 for i from 2 to r do
 if Divide(LeadingMonomial(H[i], o), L[-1]) ≠ true then
 T := T, H[i];
 else
T := T, subs(L[-1] = 1, (LeadingCoefficient(H[i], o) · LeadingMonomial(H[i], o))) :
 fi;
od;
T := [T] :
 oo := order(op(Reverse(L)));
G := Basis(T, oo) :
L2 := subsop(nops(L) = NULL, L) :
 prog(G, order, L2);
 Z := Z, G, [op(G),
        H[1] / subs(L[-1] = 1, (LeadingCoefficient(G1[1], o) · LeadingMonomial(G1[1], o)))];
for i from 1 to (r-1) do
while IdealMembership(T[i], ⟨op(G2)⟩) ≠ true do
print(T[i], IdealMembership(T[i], ⟨op(F)⟩));
G2 := sat(G1, T[i], L, order, 2) :
G1 := Basis([seq(H[j], j = 2 ..r), seq(T[j], j = 2 ..i)], o) :
prog(G2, order, L) :
od;
od;
end:
```

> $Z := NULL:$

> $K := [z^2+z+y-1, z\cdot y+z\cdot x+z+y\cdot x+x+2, y^2+2\cdot y-1, x^2-2]:$

> $IsZeroDimensional(K)$

$$true \quad (1)$$

> $prog(K, plex, [x, y, z])$

```
{--> enter prog, args = [z^2+y+z-1, x*y+x*z+y*z+x+z+2, y^2+2*
y-1, x^2-2], plex, [x, y, z]
```

$$o := plex(z)$$

$$H := [z^2+y+z-1, x\,y+x\,z+y\,z+x+z+2, y^2+2\,y-1, x^2-2]$$

$$r := 4$$

$$G1 := [z^2+y+z-1, x\,y+x\,z+y\,z+x+z+2, y^2+2\,y-1, x^2-2]$$

$$G2 := [z^2+y+z-1, x\,y+x\,z+y\,z+x+z+2, y^2+2\,y-1, x^2-2]$$

$$T := x+y+1$$

$$T := x+y+1, y^2+2\,y-1$$

$$T := x+y+1, y^2+2\,y-1, x^2-2$$

$$T := [x+y+1, y^2+2\,y-1, x^2-2]$$

$$oo := plex(z, y, x)$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(z, y, x)) -> true
```

$$G := [x^2-2, x+y+1]$$

$$L2 := [x, y]$$

```
{--> enter prog, args = [x^2-2, x+y+1], plex, [x, y]
```

$$o := plex(y)$$

$$H := [x+y+1, x^2-2]$$

$$r := 2$$

$$G1 := [x+y+1, x^2-2]$$

$$G2 := [x+y+1, x^2-2]$$

$$T := x^2-2$$

$$T := [x^2-2]$$

$$oo := plex(y, x)$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(y, x)) -> true
```

$$G := [x^2-2]$$

$$L2 := [x]$$

```
{--> enter prog, args = [x^2-2], plex, [x]
```

$$(\ ) = (\ ), [[x^2-2]]$$

```
<-- exit prog (now in prog) = }
```

$$Z := [x^2-2], [x^2-2, x+y+1]$$

```
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^2-2) -> true
<-- exit prog (now in prog) = }
```

$$Z := [x^2-2], [x^2-2, x+y+1], [x^2-2, x+y+1], [x^2-2, x+y+1, z^2+y+z-1]$$

```
value remembered (in PolynomialIdeals:-IdealMembership):
```

```
type/radalgfun(x+y+1) -> true
```

$$x+y+1, \mathit{false}$$

$$G2 := [x^2-2,\ \text{-}x+y+1, x+z]$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(z)) -> true
```

$$G1 := [1]$$

```
{--> enter prog, args = [x^2-2, -x+y+1, x+z], plex, [x, y, z]
```

$$o := \mathit{plex}(z)$$

$$H := [x+z, x^2-2,\ \text{-}x+y+1]$$

$$r := 3$$

$$G1 := [x+z, x^2-2,\ \text{-}x+y+1]$$

$$G2 := [x+z, x^2-2,\ \text{-}x+y+1]$$

$$T := x^2-2$$

$$T := x^2-2,\ \text{-}x+y+1$$

$$T := [x^2-2,\ \text{-}x+y+1]$$

$$oo := \mathit{plex}(z, y, x)$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(z, y, x)) -> true
```

$$G := [x^2-2,\ \text{-}x+y+1]$$

$$L2 := [x, y]$$

```
{--> enter prog, args = [x^2-2, -x+y+1], plex, [x, y]
```

$$o := \mathit{plex}(y)$$

$$H := [\text{-}x+y+1, x^2-2]$$

$$r := 2$$

$$G1 := [\text{-}x+y+1, x^2-2]$$

$$G2 := [\text{-}x+y+1, x^2-2]$$

$$T := x^2-2$$

$$T := [x^2-2]$$

$$oo := \mathit{plex}(y, x)$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(y, x)) -> true
```

$$G := [x^2-2]$$

$$L2 := [x]$$

```
{--> enter prog, args = [x^2-2], plex, [x]
```

$$([x^2-2], [x^2-2, x+y+1], [x^2-2, x+y+1], [x^2-2, x+y+1, z^2+y+z-1]) = ([x^2-2], [x^2-2, x+y+1], [x^2-2, x+y+1], [x^2-2, x+y+1, z^2+y+z-1]), [[x^2-2]]$$

```
<-- exit prog (now in prog) = [x^2-2], [x^2-2, x+y+1], [x^2-2,
x+y+1], [x^2-2, x+y+1, z^2+y+z-1]}
```

$$[x^2-2], [x^2-2, x+y+1], [x^2-2, x+y+1], [x^2-2, x+y+1, z^2+y+z-1]$$

$$Z := [x^2-2], [x^2-2, x+y+1], [x^2-2, x+y+1], [x^2-2, x+y+1, z^2+y+z-1], [x^2-2], [x^2-2,\ \text{-}x+y+1]$$

```
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^2-2) -> true
<-- exit prog (now in prog) = }
```

$Z := [x^2-2], [x^2-2, x+y+1], [x^2-2, x+y+1], [x^2-2, x+y+1, z^2+y+z-1], [x^2-2], [x^2-2, -x+y+1], [x^2-2, -x+y+1], [x^2-2, -x+y+1, x+z]$

```
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^2-2) -> true
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(-x+y+1) -> true
<-- exit prog (now in prog) = }
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x+y+1) -> true
```

$$x+y+1, \mathit{false}$$

$$G2 := [1]$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(z)) -> true
```

$$G1 := [1]$$

```
{--> enter prog, args = [1], plex, [x, y, z]
```

$([x^2-2], [x^2-2, x+y+1], [x^2-2, x+y+1], [x^2-2, x+y+1, z^2+y+z-1], [x^2-2], [x^2-2, -x+y+1], [x^2-2, -x+y+1], [x^2-2, -x+y+1, x+z]) = ([x^2-2], [x^2-2, x+y+1], [x^2-2, x+y+1], [x^2-2, x+y+1, z^2+y+z-1], [x^2-2], [x^2-2, -x+y+1], [x^2-2, -x+y+1], [x^2-2, -x+y+1, x+z]), [[1]]$

```
<-- exit prog (now in prog) = [x^2-2], [x^2-2, x+y+1], [x^2-2,
x+y+1], [x^2-2, x+y+1, z^2+y+z-1], [x^2-2], [x^2-2, -x+y+1],
[x^2-2, -x+y+1], [x^2-2, -x+y+1, x+z]}
```

$[x^2-2], [x^2-2, x+y+1], [x^2-2, x+y+1], [x^2-2, x+y+1, z^2+y+z-1], [x^2-2], [x^2-2, -x+y+1], [x^2-2, -x+y+1], [x^2-2, -x+y+1, x+z]$

```
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x+y+1) -> true
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(y^2+2*y-1) -> true
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^2-2) -> true
<-- exit prog (now at top level) = }
```

```
> Z
```

$[x^2-2], [x^2-2, x+y+1], [x^2-2, x+y+1], [x^2-2, x+y+1, z^2+y+z-1], [x^2-2], [x^2-2, -x+y+1], [x^2-2, -x+y+1], [x^2-2, -x+y+1, x+z]$ **(2)**

```
> Z := {Z}
```

$Z := \{[x^2-2], [x^2-2, -x+y+1], [x^2-2, x+y+1], [x^2-2, -x+y+1, x+z], [x^2-2, x+y+1, z^2+y+z-1]\}$ **(3)**

```
>
```

> $Z := NULL :$

> $F := [x+y+z+w, z^2+2\cdot z\cdot x+x^2, z\cdot y-z\cdot x+y^2\cdot x^4+y\cdot x-2\cdot x^2, z\cdot x^4-z+x^5-x, y^3\cdot x^2+y^2\cdot x^3-y-x, y^2\cdot x^6-y^2\cdot x^2-x^4+1]$

$$F := [x+y+z+w, x^2+2\,x\,z+z^2, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^5+x^4\,z-x-z, x^3\,y^2+x^2\,y^3-x-y, x^6\,y^2-x^4-x^2\,y^2+1] \qquad (4)$$

> $prog(F, plex, [x, y, z, w])$

```
{--> enter prog, args = [x+y+z+w, x^2+2*x*z+z^2, x^4*y^2-2*x^2+
x*y-x*z+y*z, x^5+x^4*z-x-z, x^3*y^2+x^2*y^3-x-y, x^6*y^2-x^4-
x^2*y^2+1], plex, [x, y, z, w]
```

$$o := plex(w)$$

$$H := [x+y+z+w, x^2+2\,x\,z+z^2, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^5+x^4\,z-x-z, x^3\,y^2+x^2\,y^3-x-y, x^6\,y^2-x^4-x^2\,y^2+1]$$

$$r := 6$$

$$G1 := [x+y+z+w, x^2+2\,x\,z+z^2, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^5+x^4\,z-x-z, x^3\,y^2+x^2\,y^3-x-y, x^6\,y^2-x^4-x^2\,y^2+1]$$

$$G2 := [x+y+z+w, x^2+2\,x\,z+z^2, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^5+x^4\,z-x-z, x^3\,y^2+x^2\,y^3-x-y, x^6\,y^2-x^4-x^2\,y^2+1]$$

$$T := x^2+2\,x\,z+z^2$$

$$T := x^2+2\,x\,z+z^2, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z$$

$$T := x^2+2\,x\,z+z^2, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^5+x^4\,z-x-z$$

$$T := x^2+2\,x\,z+z^2, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^5+x^4\,z-x-z, x^3\,y^2+x^2\,y^3-x-y$$

$$T := x^2+2\,x\,z+z^2, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^5+x^4\,z-x-z, x^3\,y^2+x^2\,y^3-x-y, x^6\,y^2-x^4-x^2\,y^2+1$$

$$T := [x^2+2\,x\,z+z^2, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^5+x^4\,z-x-z, x^3\,y^2+x^2\,y^3-x-y, x^6\,y^2-x^4-x^2\,y^2+1]$$

$$oo := plex(w, z, y, x)$$

$$G := [x^6\,y^2-x^4-x^2\,y^2+1, x^3\,y^2+x^2\,y^3-x-y, x^5+x^4\,z-x-z, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^2+2\,x\,z+z^2]$$

$$L2 := [x, y, z]$$

```
{--> enter prog, args = [x^6*y^2-x^4-x^2*y^2+1, x^3*y^2+x^2*y^3-
x-y, x^5+x^4*z-x-z, x^4*y^2-2*x^2+x*y-x*z+y*z, x^2+2*x*z+z^2],
plex, [x, y, z]
```

$$o := plex(z)$$

$$H := [x^2+2\,x\,z+z^2, x^5+x^4\,z-x-z, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^6\,y^2-x^4-x^2\,y^2+1, x^3\,y^2+x^2\,y^3-x-y]$$

$$r := 5$$

$$G1 := [x^2+2\,x\,z+z^2, x^5+x^4\,z-x-z, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^6\,y^2-x^4-x^2\,y^2+1, x^3\,y^2+x^2\,y^3-x-y]$$

$$G2 := [x^2+2\,x\,z+z^2, x^5+x^4\,z-x-z, x^4\,y^2-2\,x^2+x\,y-x\,z+y\,z, x^6\,y^2-x^4-x^2\,y^2+1,$$

$x^3 y^2 + x^2 y^3 - x - y]$

$$T := x^4 - 1$$

$$T := x^4 - 1,\ -x + y$$

$$T := x^4 - 1,\ -x + y, x^6 y^2 - x^4 - x^2 y^2 + 1$$

$$T := x^4 - 1,\ -x + y, x^6 y^2 - x^4 - x^2 y^2 + 1, x^3 y^2 + x^2 y^3 - x - y$$

$$T := [x^4 - 1,\ -x + y, x^6 y^2 - x^4 - x^2 y^2 + 1, x^3 y^2 + x^2 y^3 - x - y]$$

$$oo := plex(z, y, x)$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(z, y, x)) -> true
```

$$G := [x^4 - 1,\ -x + y]$$

$$L2 := [x, y]$$

```
{--> enter prog, args = [x^4-1, -x+y], plex, [x, y]
```

$$o := plex(y)$$

$$H := [\,-x + y, x^4 - 1\,]$$

$$r := 2$$

$$G1 := [\,-x + y, x^4 - 1\,]$$

$$G2 := [\,-x + y, x^4 - 1\,]$$

$$T := x^4 - 1$$

$$T := [x^4 - 1\,]$$

$$oo := plex(y, x)$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(y, x)) -> true
```

$$G := [x^4 - 1\,]$$

$$L2 := [x]$$

```
{--> enter prog, args = [x^4-1], plex, [x]
```

$$(\ ) = (\ ), [\,[x^4 - 1\,]\,]$$

```
<-- exit prog (now in prog) = }
```

$$Z := [x^4 - 1\,], [x^4 - 1,\ -x + y]$$

```
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^4-1) -> true
<-- exit prog (now in prog) = }
```

$$Z := [x^4 - 1\,], [x^4 - 1,\ -x + y], [x^4 - 1,\ -x + y], [x^4 - 1,\ -x + y, x^2 + 2\,x\,z + z^2]$$

```
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^4-1) -> true
```

$$x^4 - 1, false$$

$$G2 := [x^2 y^2 - 1, x + z]$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(z)) -> true
```

$$G1 := [1]$$

```
{--> enter prog, args = [x^2*y^2-1, x+z], plex, [x, y, z]
```

$$o := plex(z)$$

$$H := [x + z, x^2 y^2 - 1\,]$$

$$r := 2$$

$$G1 := [x+z, x^2y^2-1]$$

$$G2 := [x+z, x^2y^2-1]$$

$$T := x^2y^2-1$$

$$T := [x^2y^2-1]$$

$$oo := plex(z, y, x)$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(z, y, x)) -> true
```

$$G := [x^2y^2-1]$$

$$L2 := [x, y]$$

```
{--> enter prog, args = [x^2*y^2-1], plex, [x, y]
```

$$([x^4-1], [x^4-1, -x+y], [x^4-1, -x+y], [x^4-1, -x+y, x^2+2xz+z^2]) = ([x^4-1], [x^4-1, -x+y], [x^4-1, -x+y], [x^4-1, -x+y, x^2+2xz+z^2]), [[x^2y^2-1]]$$

```
<-- exit prog (now in prog) = [x^4-1], [x^4-1, -x+y], [x^4-1, -
x+y], [x^4-1, -x+y, x^2+2*x*z+z^2]}
```

$$[x^4-1], [x^4-1, -x+y], [x^4-1, -x+y], [x^4-1, -x+y, x^2+2xz+z^2]$$

$$Z := [x^4-1], [x^4-1, -x+y], [x^4-1, -x+y], [x^4-1, -x+y, x^2+2xz+z^2], [x^2y^2-1], [x^2y^2-1, x+z]$$

```
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^2*y^2-1) -> true
<-- exit prog (now in prog) = }
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^4-1) -> true
```

$$x^4-1, false$$

$$G2 := [1]$$

```
value remembered (in Groebner:-Basis): type/ShortMonomialOrder
(plex(z)) -> true
```

$$G1 := [1]$$

```
{--> enter prog, args = [1], plex, [x, y, z]
```

$$([x^4-1], [x^4-1, -x+y], [x^4-1, -x+y], [x^4-1, -x+y, x^2+2xz+z^2], [x^2y^2-1], [x^2y^2-1, x+z]) = ([x^4-1], [x^4-1, -x+y], [x^4-1, -x+y], [x^4-1, -x+y, x^2+2xz+z^2], [x^2y^2-1], [x^2y^2-1, x+z]), [[1]]$$

```
<-- exit prog (now in prog) = [x^4-1], [x^4-1, -x+y], [x^4-1, -
x+y], [x^4-1, -x+y, x^2+2*x*z+z^2], [x^2*y^2-1], [x^2*y^2-1, x+
z]}
```

$$[x^4-1], [x^4-1, -x+y], [x^4-1, -x+y], [x^4-1, -x+y, x^2+2xz+z^2], [x^2y^2-1], [x^2y^2-1, x+z]$$

```
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^4-1) -> true
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(-x+y) -> true
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^6*y^2-x^4-x^2*y^2+1) -> true
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^3*y^2+x^2*y^3-x-y) -> true
<-- exit prog (now in prog) = }
```

$$Z := [x^4-1], [x^4-1, -x+y], [x^4-1, -x+y], [x^4-1, -x+y, x^2+2xz+z^2], [x^2y^2-1],$$

$$[x^2 y^2 - 1, x + z], [x^6 y^2 - x^4 - x^2 y^2 + 1, x^3 y^2 + x^2 y^3 - x - y, x^5 + x^4 z - x - z, x^4 y^2 - 2 x^2 + x y - x z + y z, x^2 + 2 x z + z^2], [x^6 y^2 - x^4 - x^2 y^2 + 1, x^3 y^2 + x^2 y^3 - x - y, x^5 + x^4 z - x - z, x^4 y^2 - 2 x^2 + x y - x z + y z, x^2 + 2 x z + z^2, x + y + z + w]$$

```
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^2+2*x*z+z^2) -> true
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^4*y^2-2*x^2+x*y-x*z+y*z) -> true
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^5+x^4*z-x-z) -> true
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^3*y^2+x^2*y^3-x-y) -> true
value remembered (in PolynomialIdeals:-IdealMembership):
type/radalgfun(x^6*y^2-x^4-x^2*y^2+1) -> true
<-- exit prog (now at top level) = }
```

>

> Z

$$[x^4 - 1], [x^4 - 1, -x + y], [x^4 - 1, -x + y], [x^4 - 1, -x + y, x^2 + 2 x z + z^2], [x^2 y^2 - 1], [x^2 y^2 - 1, x + z], [x^6 y^2 - x^4 - x^2 y^2 + 1, x^3 y^2 + x^2 y^3 - x - y, x^5 + x^4 z - x - z, x^4 y^2 - 2 x^2 + x y - x z + y z, x^2 + 2 x z + z^2], [x^6 y^2 - x^4 - x^2 y^2 + 1, x^3 y^2 + x^2 y^3 - x - y, x^5 + x^4 z - x - z, x^4 y^2 - 2 x^2 + x y - x z + y z, x^2 + 2 x z + z^2, x + y + z + w] \tag{5}$$

> $Z := \{Z\}$

$$Z := \{[x^4 - 1], [x^2 y^2 - 1], [x^4 - 1, -x + y], [x^2 y^2 - 1, x + z], [x^4 - 1, -x + y, x^2 + 2 x z + z^2], [x^6 y^2 - x^4 - x^2 y^2 + 1, x^3 y^2 + x^2 y^3 - x - y, x^5 + x^4 z - x - z, x^4 y^2 - 2 x^2 + x y - x z + y z, x^2 + 2 x z + z^2], [x^6 y^2 - x^4 - x^2 y^2 + 1, x^3 y^2 + x^2 y^3 - x - y, x^5 + x^4 z - x - z, x^4 y^2 - 2 x^2 + x y - x z + y z, x^2 + 2 x z + z^2, x + y + z + w]\} \tag{6}$$

>

Bibliography

[1] Cox, David, Little, John, and O'shea, Donal. ”Ideals, varieties, and algorithms” 10, 12, 15

[2] Cox, David, Little, John, and O'shea, Donal. ”Using Algebraic Geometry” 7, 11, 12, 15

[3] H.Michael Möller. ”On Decomposing Systems of Polynomial Equations With Finitely Many Solutions”