Master thesis

Some Aspects of Solving Polynomial Equations, Elimination Theory, Resultants

Author
Pascale Wester

Supervisor
Dr. Oleksandr Iena

University of Luxembourg
Faculty of Science, Technology and Communication
Department of Mathematics

June 2015

Acknowledgement

I would like to use this opportunity to express my gratitude to my supervisor Dr. Oleksandr Iena for the topic proposal, the useful comments, remarks, patience and engagement throughout my master thesis. Furthermore, I would like to thank my beloved ones, especially my parents, for their support and encouragement throughout all my studies.

Contents

1 Introduction

Elimination theory, which consists of algorithmic approaches to eliminating some variables between polynomials of several variables, may be considered as the origin of algebraic geometry. Its history can be traced back to the 17th and 18th century to Newton, Euler and Bézout [23]. The resultant of two polynomials in one variable was given by Euler(1748) and Bézout(1764) and the term "resultant" was also introduced by Bézout. In old literature, we may find the term "eliminant" as it was suggested by De Morgan. The further study of resultants goes back to the works of Jacobi, Sylvester, Bézout, Cayley, Macaulay and Dixon[1]. This classical method of elimination theory has been for a long time a major tool to compute zeroes of a set of polynomials. Resultants are used as a computational tool for elimination of variables as well as a tool for the study of complexity aspects of polynomial system solving. This has renewed the interest in finding explicit formulas for the computation of resultants in the 90's.
The earliest use of what amounts to the existence of Groebner bases may be that of Gordan in 1900 to deduce Hilbert's basis theorem. A major step to the theory on Groebner bases presented in this thesis was taken by Macaulay in 1927 when he introduced total ordering of the set of monomials of a ring. Groebner Bases were first introduced in 1965 by Bruno Buchberger in his Ph.D. thesis [4] and are named after his supervisor Wolfgang Gröbner. Its use became fashionable since we began using computers[2].
The aim of this master thesis is to analyse two different methods used for elimination problems: the Groebner bases and the more classical approach with resultants. However, the thesis is not restricted to the elimination problem, but we also give other applications of Groebner bases and resultants.
We begin the master thesis by introducing orderings on the set of monomials before we give a reminder on ideals and the Hilbert basis theorem.
The main part of the thesis is divided in two.
The first part, Section 4, is about Groebner bases. We start with the ideal membership problem which leads us to the division algorithm in the multivariate case. Then we realize that the remainder of the division algorithm is in general not unique and this is where we introduce Groebner bases. After giving some properties of Groebner bases, we want to know how we can construct such bases and therefore we consider the Buchberger algorithm. However, this algorithm provides us with Groebner bases that may not be

[1]More details on the history of resultants can be found in *A Brief History of Mathematics* [12, p. 143-145].

[2]More details on the history of Groebner bases can be found in *Commutative Algebra: With a View Toward Algebraic Geometry* [11, Section 15.6].

unique and may be bigger than necessary. In Subsection 4.5.4 *Least Common Multiple and Greatest Common Divisor of Polynomials*, we will give an algorithm that provides a unique type of Groebner bases. We finish this first part by some applications of Groebner bases.
The second part, Section 5, is about resultants. We start by introducing univariate resultants before we pass on to the general theory of multivariate resultants. There we start by defining the multivariate resultant of two homogeneous polynomials in two variables. Then we pass on to the multivariate resultant of n homogeneous polynomials in n variables and finally we get to the general case with n non-homogeneous polynomials in $n-1$ variables. In this second section of the main part of the thesis we also compare Groebner bases to univariate resultants.
Section 2 about monomial orderings is necessary to understand the two sections of the main part. The reminder on ideals and the Hilbert basis theorem, Section 3, is only necessary for Section 4 about Groebner Bases. The two main parts of the thesis, Section 4 and Section 5, are independent, except for Subsection 5.3 on the comparison of Groebner bases and univariate resultants.
Section 3 is based on notes of Bertram [3] and on *Abstract algebra with applications (in two volumes). Vol. II: Rings and fields* [25]. Section 4 about Groebner bases is mainly based on *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra* [6], *Computing in Algebraic Geometry: A Quick Start Using SINGULAR* [8], *A Singular Introduction to Commutative Algebra* [14] and *Introduction to Algebraic Computation* [18]. Section 5 on resultants is mainly based on *The Algebraic Theory of Modular Systems* [19], *Introduction to resultants* [26] and *Gröbner Bases and Resultants* [23].
The computation tool used in this thesis is SINGULAR [14].

2 Monomial Orderings

Let k be a field. The notion of orderings of terms in polynomials is a key ingredient for the division algorithm in $k[x]$ and for the row-reduction (Gaussian elimination) algorithm for systems of linear equations. Therefore we might guess that if we try to extend polynomial division or row reduction to arbitrary polynomials in several variables, we will need to write a polynomial $f \in k[x_1, ..., x_n]$ in a unique ordered way. In other words we need to define an ordering on the terms in polynomials in $k[x_1, ..., x_n]$.
In the following, we will denote a monomial of $k[x_1, ..., x_n]$ by $\boldsymbol{x}^\alpha = x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n}$, where $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{Z}_{\geq 0}^n$ is the n-tuple of exponents. This notation reveals a one-to-one correspondence between the monomials in $k[x_1, ..., x_n]$ and $\mathbb{Z}_{\geq 0}^n$.

Definition 2.1.

1) A ***monomial ordering*** *on $k[x_1, ..., x_n]$ is a total ordering $>$ on the set of monomials $\boldsymbol{x}^\alpha$, $\alpha \in \mathbb{Z}_{\geq 0}^n$, which is multiplicative:*

$$\boldsymbol{x}^\alpha > \boldsymbol{x}^\beta \Longrightarrow \boldsymbol{x}^\gamma \boldsymbol{x}^\alpha > \boldsymbol{x}^\gamma \boldsymbol{x}^\beta \text{ for each } \gamma \in \mathbb{Z}_{\geq 0}^n.$$

2) A monomial ordering $>$ on $k[x_1, ..., x_n]$ is

- ***global****, if $x_i > 1$ for $i = 1, ..., n$,*
- ***local****, if $1 > x_i$ for $i = 1, ..., n$, and*
- ***mixed****, otherwise.*

The terms global and local come from geometry, referring to the global and local study of an algebraic set. In the following, we will mainly focus on global orderings.

Example 1.

1) The **lexicographic ordering** is a global monomial ordering:
let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$

$$\begin{aligned} & \boldsymbol{x}^\alpha >_{lex} \boldsymbol{x}^\beta \\ \Longleftrightarrow & \text{ the leftmost nonzero entry of the vector } \alpha - \beta \text{ is positive.} \end{aligned}$$

That $>_{lex}$ is a total ordering follows directly from the definition and the fact that the usual numerical order on $\mathbb{Z}_{\geq 0}^n$ is a total ordering. This total ordering is multiplicative: If $\boldsymbol{x}^\alpha >_{lex} \boldsymbol{x}^\beta$, then the leftmost nonzero entry of $\alpha - \beta$, say $\alpha_i - \beta_i$ is positive. For any $\gamma \in \mathbb{Z}_{\geq 0}^n$ we have

$\boldsymbol{x}^\gamma \boldsymbol{x}^\alpha = \boldsymbol{x}^{\gamma+\alpha}$ and $\boldsymbol{x}^\gamma \boldsymbol{x}^\beta = \boldsymbol{x}^{\gamma+\beta}$. Then in $(\gamma+\alpha)-(\gamma+\beta) = \alpha-\beta$, the leftmost non-zero entry is again $\alpha_i - \beta_i > 0$ and so $\boldsymbol{x}^\gamma \boldsymbol{x}^\alpha > \boldsymbol{x}^\gamma \boldsymbol{x}^\beta$. This ordering is global as for every $i = 1, ..., n$ we have $x_i = \boldsymbol{x}^\alpha$ with $\alpha_i = 1$ and $\alpha_j = 0$ for $j \neq i$. In addition $1 = \boldsymbol{x}^\beta$ with $\beta_j = 0$ for every $j = 1, ..., n$ and therefore the leftmost non-zero entry in $\alpha - \beta$ is $\alpha_i = 1 > 0$. Finally we have $x_i >_{lex} 1$ for $i = 1, ..., n$.

2) The **graded lexicographic ordering** is a global monomial ordering: let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$

$$\boldsymbol{x}^\alpha >_{grlex} \boldsymbol{x}^\beta \iff \deg(\boldsymbol{x}^\alpha) = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = \deg(\boldsymbol{x}^\beta)$$

or

$$\deg(\boldsymbol{x}^\alpha) = \deg(\boldsymbol{x}^\beta) \text{ and } \boldsymbol{x}^\alpha >_{lex} \boldsymbol{x}^\beta.$$

That $>_{grlex}$ is a total ordering follows directly from the definition. We have for any $\gamma \in \mathbb{Z}^n_{\geq 0}$

$$\boldsymbol{x}^\alpha > \boldsymbol{x}^\beta \Longrightarrow \boldsymbol{x}^\gamma \boldsymbol{x}^\alpha > \boldsymbol{x}^\gamma \boldsymbol{x}^\beta$$

since the partial ordering by degree and the lexicographic ordering both have that property. This ordering is global as for every $i = 1, ..., n$ we have $x_i = \boldsymbol{x}^\alpha$ with $\alpha_i = 1$ and $\alpha_j = 0$ for $j \neq i$. In addition $1 = \boldsymbol{x}^\beta$ with $\beta_j = 0$ for every $j = 1, ..., n$ and therefore $\deg(\alpha) = 1 > 0 = \deg(\beta)$. Finally, we have $x_i >_{grlex} 1$ for $i = 1, ..., n$.

Remark 1.

1) If it is clear which monomial ordering we are considering, we denote $>_{lex}$, respectively $>_{grlex}$ or any other ordering, simply by $>$.

2) Let $>$ be a monomial ordering on $k[x_1, ..., x_n]$. The following statements are equivalent:

   (a) $>$ is global.

   (b) $>$ refines the natural partial ordering $\geq_{nat}$ on $\mathbb{Z}^n_{\geq 0}$. That is,

   $$\alpha \geq_{nat} \beta \Rightarrow \boldsymbol{x}^\alpha > \boldsymbol{x}^\beta,$$

   where $\alpha \geq_{nat} \beta$ if and only if $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$ if and only if $\boldsymbol{x}^\alpha$ is divisible by $\boldsymbol{x}^\beta$.

   (c) $>$ is a **well-ordering**. That is, every non-empty set of monomials in $k[x_1, ..., x_n]$ has the least element with respect to $>$.

In particular the implication $(b) \Rightarrow (c)$ follows from Hilbert's basis theorem[3] which in this context tells us that every subset of $\mathbb{Z}^n_{\geq 0}$ has at most finitely many minimal elements with respect to $>_{nat}$.

Definition 2.2. *Let us consider a non-zero polynomial $f \in k[x_1, ..., x_n]$ and fix a monomial ordering on $k[x_1, ..., x_n]$:*

1) *The largest monomial of f, $LM(f)$, is called the* ***leading monomial*** *of f.*

2) *The coefficient in front of $LM(f)$ is called the* ***leading coefficient*** *of f and is denoted by $LC(f)$.*

3) *The* ***leading term*** *of f is defined by $LT(f) = LC(f) \cdot LM(f)$.*

4) *If $LM(f) = \boldsymbol{x}^\alpha$, then* $\text{multideg}(f) = \alpha$ *is called the* ***multidegree*** *of f.*

Example 2. Consider $f = 5x^2yz - 7xz^5$ in $k[x, y, z]$.

· Let us take as monomial ordering the lexicographic ordering which is in this case usually the alphabetic ordering: $x > y > z > 1$. Then we have

$$x^2yz > xz^5$$

as $(2, 1, 1) - (1, 0, 5) = (1, 1, -4)$ i.e the leftmost entry is positive. Therefore

$$LM(f) = x^2yz,\ LC(f) = 5,\ LT(f) = 5x^2yz$$
$$\text{and multideg}(f) = (2, 1, 1).$$

· Consider now the same polynomial f, but let us take as monomial ordering the graded lexicographic ordering. Then we have

$$xz^5 > x^2yz$$

as $|(1, 0, 5)| = 6 > 4 = |(2, 1, 1)|$. Therefore

$$LM(f) = xz^5,\ LC(f) = -7,\ LT(f) = -7xz^5$$
$$\text{and multideg}(f) = (1, 0, 5).$$

This example shows that the same polynomial could have different leading monomials if we consider different monomial orderings.

[3] Theorem 3.4 in Section 3.

3 Reminder on Ideals and Hilbert Basis Theorem

In the following, we will give a reminder on ideals and the Hilbert Basis theorem which will be useful for the next section on Groebner bases.

Lemma 3.1. *If $f_1, ..., f_s \in k[x_1, ..., x_n]$, then*

$$\langle f_1, ..., f_s \rangle = \{\sum_{i=1}^{s} h_i f_i : h_1, ..., h_s \in k[x_1, ..., x_n]\}$$

*is an ideal of $k[x_1, ..., x_n]$. We will call $\langle f_1, ..., f_s \rangle$ the **ideal generated by** $f_1, ..., f_s$.*

Proof. Since $0 = \sum_{i=1}^{s} 0 \cdot f_i$, we have that $0 \in \langle f_1, ..., f_s \rangle$. Suppose now that $f = \sum_{i=1}^{s} p_i f_i$, $g = \sum_{i=1}^{s} q_i f_i$ and let $h \in k[x_1, ..., x_n]$. Then we get

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i \in \langle f_1, ..., f_s \rangle,$$

$$hf = \sum_{i=1}^{s} (hp_i) f_i \in \langle f_1, ..., f_s \rangle$$

and therefore we can conclude that $\langle f_1, ..., f_s \rangle$ is an ideal. □

Next, we will show that all ideals $I \subset k[x_1, ...x_n]$ are of this form.

Definition 3.2. *A ring A is called a **Noetherian ring** if every ideal I of A is finitely generated.*

Remark 2. Recall that since k is a field, it only has two ideals: $\{0\}$ and itself. Since the identity 1_k generates k, all the ideals of k are finitely generated and so we can conclude that it is a Noetherian ring.

Proposition 3.3. *If A is a Noetherian ring, then:*

1) *Given any ascending chain of ideals $I_1 \subseteq I_2 \subseteq ... \subseteq A$, there is $n_0 \in \mathbb{N}$ such that for all $n \geq n_0 : I_n = I_{n_0}$.*

2) *The polynomial ring $A[x]$ is Noetherian.*

3) *For any $n \in \mathbb{N}_{>0}$, the polynomial ring $A[x_1, ..., x_n]$ is Noetherian.*

Proof. 1) Note that under this assumptions $I := \bigcup_{i=1}^{+\infty}$ is an ideal, hence it is finitely generated. If $a_1, ..., a_m$ are generators, they are all contained in some I_n and therefore $I_n = I_{n+1} = ... = I$.

2) Let $J \subset A[x]$ be any ideal. We want to show that J is finitely generated. Consider the ideals $I_d \subset A$ of leading coefficients of polynomials $f \in J$ of degree d. This means that $a \in I_d$ if and only if there is a polynomial $f = ax^d + a_{d-1}x^{d-1} + ... + a_0 \in J$. The ideals I_d form an ascending chain $I_0 \subset I_1 \subset ...$ which must be eventually stationary by 1), say $I_{n_0} = I_{n_0+1} = ...$ as A is Noetherian. Let $I_d = \langle a_{d,1}, ..., a_{d,m_d} \rangle$ for each $d \leq n_0$ and for each pair (d, i) choose some $f_{d,i} = a_{d,i}x^d + a_{d-1}x^{d-1} + ...+a_0 \in J$. Then the $f_{d,i}$ together generate J. Indeed, let $f \in J$, where $f = c_d x^d + c_{d-1}x^{d-1} + ... + c_0$. Then by definition of I_d, we have that $c_d \in I_d$ and since $I_d = \langle a_{d,1}, ..., a_{d,m_d} \rangle$, we can write $c_d = \sum_{i=1}^{m_d} b_i a_{d,i}$, $b_i \in A$ for all $i \in \{1, ..., m_d\}$. It follows that $f - \sum_{i=1}^{m_d} b_i a_{d,i}$ has degree $< d$. This reasoning can be repeated for degree $d-1$ until degree 0, hence we get finally that f is generated by $f_{d,i}$ with $d \leq n_0$ and $i \in 1, ..., m_d$. We can conclude that J is finitely generated and so $A[x]$ is Noetherian.

3) This is a direct consequence of 2) by using induction on n.

□

As we have seen that a field k is Noetherian, we can apply the proposition above on k and so we get the following theorem:

Theorem 3.4 (**Hilbert Basis Theorem**). *Every ideal $I \subset k[x_1, ..., x_n]$ has a finite generating set. This means that $I = \langle f_1, ..., f_s \rangle$ for some $f_1, ..., f_s \in I$.*

4 Groebner Basis and Normal Form

In this section, we want to give an answer to the following question: If $f_1, ..., f_s \in k[x_1, ..., x_n]$, is there an algorithm to decide whether a given $f \in k[x_1, ..., x_n]$ lies in $\langle f_1, ..., f_s \rangle$? This problem is often called the **ideal membership problem** as we have seen in Section 3 that $\langle f_1, ..., f_s \rangle$ is an ideal.
For polynomials of one variable, i.e. when $n = 1$, we can use the division algorithm in $k[x]$ to solve the ideal membership problem. It is enough to consider the case $s = 1$ when we work with polynomials in one variable since if k is a field, then every ideal of $k[x]$ can be written in the form $\langle f_1 \rangle$ for some $f_1 \in k[x]$ [4]. Given $f \in k[x]$, to check whether $f \in \langle f_1 \rangle$, we divide f by f_1:

$$f = f_1 \cdot q + r,$$

where $q, r \in k[x]$ such that $r = 0$ or $\deg(r) < \deg(f_1)$ are unique. Then we have $f \in \langle f_1 \rangle$ if and only if $r = 0$. Indeed, if $r = 0$, then $f = f_1 \cdot q \in \langle f_1 \rangle$ by definition. Suppose now that $f = f_1 \cdot q + r \in \langle f_1 \rangle$ with $r \neq 0$. As $f = f_1 \cdot q \in \langle f_1 \rangle$, we have that $r \in \langle f_1 \rangle$. But as $r \neq 0$, we can conclude by the division algorithm that $\deg(r) < \deg(f_1)$. As this is a contradiction to $r \in \langle f_1 \rangle$, we can conclude that $f \in \langle f_1 \rangle$ if and only if $r = 0$. Thus, we have an algorithmic test for the ideal membership problem in the case $n = 1$.
From this observation, we might guess that in the general case we need a division algorithm in $k[x_1, ..., x_n]$ to solve the ideal membership problem.

4.1 Division Algorithm in $k[x_1, ..., x_n]$

We want do define a division algorithm for polynomials in $k[x_1, ..., x_n]$ that extends the algorithm for $k[x]$. In other words we want to divide $f \in k[x_1, ..., x_n]$ by $f_1, ..., f_s \in k[x_1, ..., x_n]$ and express f in the form

$$f = a_1 f_1 + ... + a_s f_s + r,$$

where $a_1, ..., a_s, r \in k[x_1, ..., x_n]$. The element r is called the remainder of this division. We need to be careful how to define this element as it will play a key role in the ideal membership problem. To define this division algorithm, we need the monomial orderings introduced before.
The basic idea of the algorithm is the same as in the one-variable case: after having fixed a monomial ordering $>$, we want to cancel the leading term of f by multiplying some f_i by an appropriate monomial and subtracting. Then this monomial becomes a term in the corresponding a_i. Let us consider first an example before stating the division algorithm in general.

[4] Corollary 4 of Chapter 1, §5 in [6].

Example 3. Consider as monomial ordering the lexicographic ordering with $x > y > 1$. Let $f = 2x^2y - xy^2 + y^2$, $f_1 = xy + 1$ and $f_2 = y^2 + 1$. We have that $LT(f_1) = xy$ divides $LT(f) = 2x^2y$ but $LT(f_2) = y^2$ does not. Therefore we start by dividing $2x^2y$ by xy:

$$\begin{array}{rll} a_1: & 2x & \\ a_2: & & \\ xy+1 & \big)\overline{2x^2y - xy^2 + y^2} & \\ y^2+1 & \underline{2x^2y + 2x} & \\ & -xy^2 - 2x + y^2 & \end{array}$$

As $LT(-x^2y - 2x + y^2) = -xy^2$ is also divisible by $LT(f_1)$, we continue by dividing by xy:

$$\begin{array}{rll} a_1: & 2x - y & \\ a_2: & & \\ xy+1 & \big)\overline{2x^2y - xy^2 + y^2} & \\ y^2+1 & \underline{2x^2y + 2x} & \\ & -xy^2 - 2x + y^2 & \\ & \underline{-xy^2 - y} & \\ & -2x + y^2 + y & \end{array}$$

We can see that $LT(f_1) = xy$ and $LT(f_2) = y^2$ do not divide $LT(-2x + y^2 + y) = -2x$. But we can say that the polynomial $-2x + y^2 + y$ is not the remainder since $LT(f_2)$ divides y^2. So if we move $-2x$ to the remainder, we get

$$\begin{array}{rll} a_1: & 2x - y & \\ a_2: & & r \\ xy+1 & \big)\overline{2x^2y - xy^2 + y^2} & \\ y^2+1 & \underline{2x^2y + 2x} & \\ & -xy^2 - 2x + y^2 & \\ & \underline{-xy^2 - y} & \\ & -2x + y^2 + y & \\ & \underline{-2x + y^2 + y} & \\ & y^2 + y & \to -2x \end{array}$$

Now we can continue dividing. If we can divide by $LT(f_1)$ or $LT(f_2)$, we

proceed as usual, and if neither divides, we move the leading term of the intermediate dividend to the remainder column.

$$
\begin{array}{rll}
a_1: & 2x-y & \\
a_2: & 1 & r \\
xy+1 & \big)\overline{2x^2y-xy^2+y^2} & \\
y^2+1 & & \\
 & \underline{2x^2y+2x} & \\
 & -xy^2-2x+y^2 & \\
 & \underline{-xy^2-y} & \\
 & -2x+y^2+y & \\
 & \underline{y^2+y} & \to -2x \\
 & y^2+1 & \\
 & \underline{y-1} & \\
 & -1 & \to -2x+y \\
 & \underline{0} & \to -2x+y-1
\end{array}
$$

Finally, we get

$$2x^2y-xy^2+y^2 \;=\; (2x-y)(xy+1)+1\cdot(y^2+1)+(-2x+y-1).$$

This example reveals the properties we want the remainder r to have: none of its terms should be divisible by the leading terms of the polynomials by which we are dividing. Let us now consider the general division algorithm.

Theorem 4.1 (**Division algorithm in** $k[x_1,...,x_n]$)**.** *Fix a global monomial ordering* $>$ *on* $\mathbb{Z}^n_{\geq 0}$ *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*

$$f=a_1f_1+...+a_sf_s+r,$$

where $a_i,r\in k[x_1,...,x_n]$ *and either* $r=0$ *or* r *is a linear combination, with coefficients in* k*, of monomials, none of which is divisible by any of* $LT(f_1),...,LT(f_s)$*. The element* r *will be called a* ***remainder*** *of* f *on division by* F*. Furthermore, if* $a_if_i\neq 0$*, then we have*

$$LM(f)\geq LM(a_if_i).$$

Proof. First, we will give a construction algorithm to prove the existence of $a_1, ..., a_s$ and r and then we will show that this algorithm operates correctly on any given input.

Algorithm 1 Division algorithm in $k[x_1, ..., x_n]$

Require: $f, f_1, ..., f_s$
Ensure: $a_1, ..., a_s, r$
  $a_1 := 0, ..., a_s := 0, r = 0$
  $p := f$
  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**
        $a_i := a_i + LT(p)/LT(f_i)$
        $p := p - (LT(p)/LT(f_i))f_i$
        divisionoccured:=true
      else
        i:=i+1
      end if
    end while
    if divisionoccured=false **then**
      $r := r + LT(p)$
      $p := p - LT(p)$
    end if
  end while

To make it more clear, let us relate this algorithm to the example given above: the variable p is the intermediate dividend at each stage, the variable r represents the column on the right-hand side and the variables $a_1, ..., a_s$ are the quotients listed above the radical. The boolean variable *divisionoccured* indicates when some $LT(f_i)$ divides the leading term of the intermediate dividend.
To prove that this algorithm works, we will first show by induction that

$$f = a_1 f_1 + ... + a_s f_s + p + r \tag{4.1}$$

holds at every stage. It is obvious that this is true for the initial values of $a_1, ...a_s, p, r$. Now suppose that (4.1) holds at one step of the algorithm. If in the next step $LT(f_i)$ divides $LT(p)$, then

$$a_i f_i + p = \left(a_i + \frac{LT(p)}{LT(f_i)}\right) f_i + \left(p - \frac{LT(p)}{LT(f_i)} f_i\right)$$

reveals that $a_i f_i + p$ does not change. Since all other variables are unaffected, (4.1) remains true in this case. On the other side if in the next step no $LT(f_i)$ divides $LT(p)$, then p and r will be changed. However, the sum $p + r$ will remain the same since

$$p + r = (p - LT(p)) + (r + LT(p))$$

and so (4.1) is unchanged. The next thing we have to realize is that the algorithm stops when $p = 0$. In this case, (4.1) becomes

$$f = a_1 f_1 + ... + a_s f_s + r.$$

During the algorithm, terms are added to r only when they are not divisible by any $LT(f_i)$ and so r has the desired properties when the algorithm terminates. Finally, it remains to show that the algorithm comes to an end. Each time we redefine the variable p, either its multidegree drops or it becomes 0. Indeed, first suppose that some $LT(f_i)$ divides $LT(p)$. Then p is redefined in the following way:

$$p' = p - \frac{LT(p)}{LT(f_i)} f_i.$$

Since we clearly have

$$LT\Big(\frac{LT(p)}{LT(f_i)} f_i\Big) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p),$$

p and $\frac{LT(p)}{LT(f_i)} f_i$ have the same leading term. Therefore p' must have strictly smaller multidegree when $p' \neq 0$. Suppose now that no $LT(f_i)$ divides $LT(p)$ and then p is redefined to be

$$p' = p - LT(p).$$

As above p' must have in this case strictly smaller multidegree when $p' \neq 0$. Thus, in either case, the multidegree must decrease. If the algorithm never terminated, then we would get an infinite decreasing sequence of multidegrees. But as we assumed that our monomial ordering is global, and therefore well-ordered, this situation cannot occur. Hence $p = 0$ must happen at some time so that the algorithm comes to an end after finitely many steps.
Now it remains to prove that $LM(f) \geq LM(a_i f_i)$. Each term in a_i is of the form $\frac{LT(p)}{LT(f_i)}$ for some value of the variable p. The algorithm starts with $p = f$ and as we just proved that the multidegree of p decreases, we have $LM(p) \leq LM(f)$. Finally,

$$LM(a_i f_i) = LM\Big(\frac{LT(p)}{LT(f_i)} f_i\Big) = LM(p) \leq LM(f).$$

□

Remark 3. In the division algorithm, we supposed the chosen monomial ordering on $k[x_1, ..., x_n]$ to be global. We will see that this is necessary by studying the following example: Consider on $k[x]$ a local ordering with $1 > x$. We want to divide x by $1 + x$. We get

$$\begin{aligned} x &= x(1+x) - x^2 \\ &= x(1+x) - x^2(1+x) + x^3 \\ &= x(1+x) - x^2(1+x) + x^3(1+x) - ... \\ \Rightarrow x &= (1+x)(x - x^2 + x^3 - x^4 + ...) + 0. \end{aligned}$$

This shows that for non-global monomial orderings, the division algorithm might not stop. For local orderings on $k[x_1, ..., x_n]$, there is an alternative division algorithm: the **Mora division algorithm**. More details on this can be found in *A Singular Introduction to Commutative Algebra* [14, p. 57] and *Introduction of the Mora division algorithm in the ring of differential operators D* [20].

Example 4. Consider as monomial ordering the lexicographic ordering on $k[x, y]$ with $x > y > 1$. Let us take $f_1 = xy+1$, $f_2 = x^2 - 1$ and $f = x^2y - y$. Let us divide f by $F = (f_1, f_2)$:
The leading terms $LT(f_1) = xy$ and $LT(f_2) = x^2$ both divide the leading term $LT(f) = x^2y$. Since f_1 is listed first, we will use it first and so we divide x^2y by xy:

$$\begin{array}{rll} a_1: & x & \\ a_2: & & \\ xy+1 & \Big) \overline{x^2y - y} & \\ x^2-1 & \quad \underline{x^2y + x} & \\ & \quad\quad -x - y & \end{array}$$

Since $LT(f_1)$ and $LT(f_2)$ do not divide $LT(-x-y) = -x$ nor the other term of $-x - y$, namely $-y$, the remainder is $r = -x - y$. Therefore we can write f in the form:

$$x^2y - y = x \cdot (xy + 1) + 0 \cdot (x^2 - 1) + (-x - y).$$

By considering $F = (f_2, f_1)$, however, f_2 is listed first, so we start by dividing x^2y by x^2:

$$\begin{array}{rll} a_1\colon & y & \\ a_2\colon & & \\ x^2-1 & \big) & \overline{x^2y-y} \\ xy+1 & & \\ & & \underline{x^2y-y} \\ & & 0 \end{array}$$

As we have now $p = 0$ in the division algorithm, it stops and the remainder is $r = 0$. Therefore we can write f in the form:

$$x^2y - y = y \cdot (x^2 - 1) + 0 \cdot (xy + 1) + 0.$$

The second calculation shows that $f \in \langle f_1, f_2 \rangle$. Then the first calculation reveals that even if $f \in \langle f_1, f_2 \rangle$, it is still possible to get a non-zero remainder on division by $F = (f_1, f_2)$. In other words $r = 0$ is a sufficient condition for ideal membership, but as this example shows, it is not a necessary condition for being in the ideal. We must conclude that we cannot use the division algorithm in $k[x_1, ..., x_n]$ in exactly the same way as the division algorithm in $k[x]$ as the remainder r is not uniquely defined.
To solve this problem, it might be useful to change the generating set of $I = \langle f_1, ..., f_s \rangle$. We have to ask ourselves what conditions the new generating set of I should satisfy. We would like the remainder r on division by the new generators be uniquely determined, so that for each $f \in I$ its $LT(f)$ is divisible by some of $LT(f_i)$, $i = 1, ..., s$. We will realize in the next subsection that in that situation the condition $r = 0$ is equivalent to membership in the ideal.

4.2 Groebner Basis

Definition 4.2. *An ideal $I \subset k[x_1, ..., x_n]$ is a **monomial ideal** if there is a subset $A \subset \mathbb{Z}^n_{\geq 0}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha \boldsymbol{x}^\alpha$, where $h_\alpha \in k[x_1, ..., x_n]$. In this case we write $I = \langle \boldsymbol{x}^\alpha : \alpha \in A \rangle$.*

Lemma 4.3. *Let $I = \langle \boldsymbol{x}^\alpha : \alpha \in A \rangle$ be a monomial ideal. Then a monomial $\boldsymbol{x}^\beta \in I$ if and only if $\boldsymbol{x}^\beta$ is divisible by $\boldsymbol{x}^\alpha$ for some $\alpha \in A$.*

Proof. If $\boldsymbol{x}^\beta \in I$, then $\boldsymbol{x}^\beta = \sum_{i=1}^s h_i \boldsymbol{x}^{\alpha(i)}$, where $h_i \in k[x_1, ..., x_n]$ and $\alpha(i) \in A$. If we expand each h_i as a linear combination of monomials, we see that every term on the right side of the equation is divisible by some $\boldsymbol{x}^{\alpha(i)}$. Therefore, the left side $\boldsymbol{x}^\beta$ must have the same property. Conversely,

if $\boldsymbol{x}^\beta$ is a multiple of $\boldsymbol{x}^\alpha$ for some $\alpha \in A$, then $\boldsymbol{x}^\beta \in I$ by the definition of an ideal. $\square$

Definition 4.4. *Fix a monomial ordering on $k[x_1, ..., x_n]$ and let I be an ideal in $k[x_1, ..., x_n]$.*

1) We denote by $LT(I)$ the set of leading terms of elements of I. Thus

$$LT(I) = \{c\boldsymbol{x}^\alpha : \text{there exists } f \in I \text{ with } LT(f) = c\boldsymbol{x}^\alpha\}.$$

2) We denote by $\langle LT(I)\rangle$ the ideal generated by the elements of $LT(I)$.

Example 5. Let $I = \langle f_1, f_2\rangle$, where $f_1 = xy + 1$ and $f_2 = x^2y - y$ and consider the lexicographic ordering on $k[x, y]$ with $x > y > 1$. Then

$$x(xy + 1) - 1 \cdot (x^2y - y) = x + y,$$

so that $x + y \in I$. Therefore $x = LT(x + y) \in \langle LT(I)\rangle$. However x is not divisible by $LT(f_1) = xy$ or $LT(f_2) = x^2y$, so that $x \notin \langle LT(f_1), LT(f_2)\rangle$ by Lemma 4.3.

This example shows, that if $I = \langle f_1, ..., f_s\rangle$, then $\langle LT(f_1), ..., LT(f_s)\rangle$ and $\langle LT(I)\rangle$ may be different ideals. It is true that $LT(f_i) \in LT(I) \subset \langle LT(I)\rangle$ by definition so that $\langle LT(f_1), ..., LT(f_s)\rangle \subset LT(I)$. However, $\langle LT(I)\rangle$ can be strictly larger. If these two ideals coincides, then the set $\{f_1, ..., f_s\}$ has a special name:

Definition 4.5. *Fix a monomial ordering on $k[x_1, ..., x_n]$. A finite subset $F = \{f_1, ..., f_s\}$ of an ideal I is said to be a* ***Groebner basis*** *(or* ***standard basis****) if*

$$\langle LT(f_1), ..., LT(f_s)\rangle = \langle LT(I)\rangle.$$

Proposition 4.6. *Let $I \subset k[x_1, ..., x_n]$ be an ideal.*

1) $\langle LT(I)\rangle$ is a monomial ideal.

2) There are $f_1, ..., f_s \in I$ such that $\langle LT(I)\rangle = \langle LT(f_1), ..., LT(f_s)\rangle$.

Proof. 1) The leading monomials $LM(f)$ of elements $f \in I\backslash\{0\}$ generate the monomial ideal $\langle LM(f) : f \in I\backslash\{0\}\rangle$. Since $LM(f)$ and $LT(f)$ differ by a non-zero constant, this ideal equals $\langle LT(f) : f \in I\backslash\{0\}\rangle = \langle LT(I)\rangle$. Therefore we can conclude that $\langle LT(I)\rangle$ is a monomial ideal.

2) By Hilbert's basis theorem the ideal $\langle LT(I)\rangle$ is generated by a finite number of polynomials $g_1, ..., g_r \in k[x_1, ..., x_n]$. On the other hand, by definition $\langle LT(I)\rangle = \langle LT(f) : f \in I\backslash\{0\}\rangle$. We can conclude that $\langle g_1, ..., g_r\rangle = \langle LT(f) : f \in I\backslash\{0\}\rangle$ and so we must have for each i : $g_i \in \langle LT(f) : f \in I\backslash\{0\}\rangle$. Therefore $g_i = \sum_{j=1}^{m_i} c_{ij} LT(f_{ij})$, where $m_i \in \mathbb{Z}_{n>0}$, $c_{ij} \in k[x_1, ..., x_n]$ and $f_{ij} \in I\backslash\{0\}$, so that each g_i is a linear combination of elements $LT(f_{ij}) : f_{ij} \in I\backslash\{0\}$. Finally, $\langle LT(I)\rangle = \langle g_1, ..., g_r\rangle$ is finitely generated by elements $LT(f_{ij}) : f_{ij} \in I\backslash\{0\}$, i.e there are $f_1, ..., f_s \in I$ such that $\langle LT(I)\rangle = \langle LT(f_1), ..., LT(f_s)\rangle$.

□

Corollary 4.7. *Fix a global monomial ordering on $k[x_1, ..., x_n]$. Then every non-zero ideal $I \subset k[x_1, ..., x_n]$ has a Groebner basis. Furthermore, any Groebner basis for an ideal I is a basis of I.*

Proof. The first claim is equivalent to the second claim of Proposition 4.6. For the second claim, we will first prove that if $\langle LT(I)\rangle = \langle LT(f_1), ..., LT(f_s)\rangle$, then $I = \langle f_1, ..., f_s\rangle$. It is clear that $\langle f_1, ..., f_s\rangle \subset I$ since each $f_i \in I$. Conversely, let $f \in I$ be any polynomial and let us apply the division algorithm to divide f by $\langle f_1, ..., f_s\rangle$. Then we get

$$f = a_1 f_1 + ... + a_s f_s + r,$$

where no term of r is divisible by any of $LT(f_1), ..., LT(f_s)$. We can rewrite this as

$$r = f - a_1 f_1 - ... - a_s f_s$$

so that we must have that $r \in I$. Let us suppose that $r \neq 0$, then $LT(r) \in \langle LT(I)\rangle = \langle LT(f_1), ..., LT(f_s)\rangle$. It follows by Lemma 4.3 that $LT(r)$ must be divisible by some $LT(f_i)$. This contradicts the definition of r in the division algorithm and therefore we have $r = 0$ and thus $I \subset \langle f_1, ..., f_s\rangle$. □

4.3 Properties of Groebner Bases

As shown in the subsection before, every non-zero ideal $I \subset k[x_1, ...x_n]$ has a Groebner basis with respect to a given global monomial ordering. Now we will study the properties of Groebner bases and then we we will see how we can check if a given basis is a Groebner basis.

Proposition 4.8. *Fix a global monomial ordering on $k[x_1, ..., x_n]$. Let $F = \{f_1, ..., f_s\}$ be a Groebner basis for an ideal $I \subset k[x_1, ..., x_n]$ and let $f \in k[x_1, ..., x_n]$. Then there is a unique $r \in k[x_1, ..., x_n]$ with the following properties:*

1) No term of r is divisible by any of $LT(f_1), ..., LT(f_s)$.

2) There is $g \in I$ such that $f = g + r$.

3) r is the remainder of the division of f by F no matter how the elements of F are ordered when using the division algorithm.

Proof. The division algorithm provides $f = a_1 f_1 + ... + a_s f_s + r$, where r satisfies 1). By setting $g = a_1 f_1 + ... + a_s f_s$, we get 2). This proves the existence of r.
To prove uniqueness of r, suppose that $f = g + r = g' + r'$ satisfy 1) and 2). Then we get $r' - r = g - g' \in I$, so that if $r \neq r'$, then $LT(r' - r) \in \langle LT(I) \rangle = \langle LT(f_1), ..., LT(f_s) \rangle$ as $\{f_1, ..., f_s\}$ is a Groebner basis. By Lemma 4.3, $LT(r' - r)$ has to be divisible by some $LT(f_i)$. This is a contradiction to property 1) of r and r'. Therefore we get $r' - r = 0$ and so uniqueness is proved.
We get the final claim 3) of the proposition by the uniqueness of r. □

Definition 4.9. *The remainder r defined in the previous proposition is called* ***the normal form of*** *f.*

This proposition shows that a Groebner basis of an ideal $I \subset k[x_1, ..., x_n]$ is a "good" generating set of I we were looking for. It shows that the undesirable behaviour of the division algorithm in $k[x_1, ..., x_n]$ seen in Subsection 4.1 does not occur when we divide by the elements of a Groebner basis. Let us also remark that even though the normal form r is unique, the a_i produced by the division algorithm $f = a_1 f_1 + ... + a_s f_s + r$ still can change if we change the order of the elements in the Groebner basis F.

Corollary 4.10. *Let $F = \{f_1, ..., f_s\}$ be a Groebner basis for an ideal $I \subset k[x_1, ..., x_n]$ and let $f \in k[x_1, ..., x_n]$. Then $f \in I$ if and only if the normal form r on division of f by F is zero.*

Proof. If $r = 0$ then by 2) of the previous proposition there is $g \in I$ such that $f = g + 0$. Thus $f \in I$.
Conversely, suppose $f \in I$. Again by 2) there is $g \in I$ such that $f = g + r$. This can be rewritten as $r = f - g \in I$ and now we can use the same reasoning as in the proof of Proposition 4.8. If $r \neq 0$ then $LT(r) \in \langle LT(I) \rangle = \langle LT(f_1), ..., LT(f_s) \rangle$ as $\{f_1, ..., f_s\}$ is a Groebner basis. By Lemma 4.3, $LT(r)$ has to be divisible by some $LT(f_i)$. This is a contradiction to property 1) of r. Therefore we get $r = 0$. □

Finally, Corollary 4.10 gives us an algorithm for solving the ideal membership problem if we know a Groebner basis F for the ideal I in question. It suffices

to compute the normal form of f with respect to F to determine whether $f \in I$.

Definition 4.11. *Fix a global monomial ordering on $k[x_1, ..., x_n]$. Let $F = (f_1, ..., f_s)$ be an ordered s-tuple. The remainder of the division of f by F will be denoted by $\overline{f}^F$.*

The next step is to determine whether a given generating set $\{f_1, ..., f_s\}$ of an ideal I is a Groebner basis. The obstruction to $\{f_1, ..., f_s\}$ being a Groebner basis is the possible appearance of polynomial combinations of the f_i whose leading terms are not in the ideal $\langle LT(f_1), ..., LT(f_s)\rangle$. One way this can happen is if the leading term in a suitable combination

$$a\boldsymbol{x}^\alpha f_i - b\boldsymbol{x}^\beta f_j$$

cancel, leaving only smaller terms and then we may have

$$LT(a\boldsymbol{x}^\alpha f_i - b\boldsymbol{x}^\beta f_j) \notin \langle LT(f_1), ..., LT(f_s)\rangle.$$

On the other side

$$a\boldsymbol{x}^\alpha f_i - b\boldsymbol{x}^\beta f_j \in I \Rightarrow LT(a\boldsymbol{x}^\alpha f_i - b\boldsymbol{x}^\beta f_j) \in \langle LT(I)\rangle.$$

This is exactly what happened in Example 5. We introduce the following special combination to study this cancellation problem.

Definition 4.12. *Let $f, g \in k[x_1, ..., x_n]$ be non-zero polynomials.*

1. *If* $\text{multideg}(f) = \alpha = (\alpha_1, ..., \alpha_n)$ *and* $\text{multideg}(g) = \beta = (\beta_1, ..., \beta_n)$, *then let $\gamma = (\gamma_1, ..., \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call $\boldsymbol{x}^\gamma$ the* ***least common multiple*** *of $LM(f)$ and $LM(g)$, denoted by $\boldsymbol{x}^\gamma = LCM(LM(f), LM(g))$.*

2. *The* ***S-polynomial*** *of f and g is the combination*

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

Remark 4. The S in S-polynomial stands for syzygies. Consider $F = (f_1, ..., f_s)$, then a syzygy on the leading terms $LT(f_1), ..., LT(f_s)$ of F is an s-tuple of polynomials $S = (h_1, ..., h_s) \in (k[x_1, ..., x_n])^s$ such that

$$\sum_{i=1}^{s} h_i \cdot LT(f_i) = 0.$$

Example 6. Consider $k[x, y]$ with the lexicographic ordering $x > y > 1$. Let $f = xy - y^3$ and $g = y^2 - 1$. Then we have $\gamma = (1, 2)$ and

$$S(f, g) = \frac{xy^2}{xy} \cdot (xy - y^3) - \frac{xy^2}{y^2} \cdot (y^2 - 1) = y(xy - y^3) - x(y^2 - 1) = x - y^4.$$

An S-polynomial is constructed in such a way that it produces cancellation of leading terms. In fact, the following lemma shows that every cancellation of leading terms among polynomials of the same multidegree results from this sort of cancellation.

Lemma 4.13. *Suppose we have a sum* $\sum_{i=1}^{s} c_i f_i$, *where* $c_i \in k$ *and* $\text{multideg}(f_i) = \delta \in \mathbb{Z}_{\geq 0}^n$ *for all* i. *If* $\text{multideg}(\sum_{i=1}^{s} c_i f_i) < \delta$, *then* $\sum_{i=1}^{s} c_i f_i$ *is a linear combination, with coefficients in* k, *of the* S*-polynomials* $S(f_j, f_k)$ *for* $1 \leq j, k \leq s$. *Furthermore, each* $S(f_j, f_k)$ *has multidegree* $< \delta$.

Proof. See [6, p. 84] □

Using Lemma 4.13 and S-polynomials, we will give now a criterion to check whether a given basis of an ideal is a Groebner basis.

Theorem 4.14 (**Buchberger's Criterion**). *Let* I *be a polynomial ideal. Then a basis* $F = \{f_1, ..., f_s\}$ *of* I *is a Groebner basis of* I *if and only if for all pairs* $i > j$, *the remainder of division of* $S(f_i, f_j)$ *by* F *is zero.*

Proof. $\Rightarrow$: If F is a Groebner basis, then since $S(f_i, f_j) \in I$ by definition, the remainder of division by F is zero by Corollary 4.10.
$\Leftarrow$: Let $f \in I$ be a non-zero polynomial. We have to show that if the S-polynomials all have zero remainders of division by F, then $LT(f) \in \langle LT(f_1), ..., LT(f_s)\rangle$. The idea of the proof is the following: given $f \in \langle f_1, ..., f_s\rangle$, there are polynomials $h_i \in k[x_1, ..., x_n]$ such that

$$f = \sum_{i=1}^{s} h_i f_i. \tag{4.2}$$

It follows that

$$\text{multideg}(f) \leq \max(\text{multideg}(h_i f_i))$$

since if $f, g \in k[x_1, ..., x_n]$ with $f + g \neq 0$, then we get $\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$. If equality does not occur, then some cancellation must appear among the leading terms of summands from (4.2). Lemma 4.13 will allow us to rewrite this in terms of S-polynomials. Then our assumption that S-polynomials have zero remainders will allow us to replace the S-polynomials by expressions that involve less cancellation of

leading terms. Continuing in this way, we will eventually find an expression (4.2) for f with

$$\text{multideg}(f) = \max(\text{multideg}(h_i f_i)).$$

Therefore, we have $\text{multideg}(f) = \text{multideg}(h_i f_i)$ for some i and it will follow that $LT(f)$ is divisible by $LT(f_i)$. Thus we get $LT(f) \in \langle LT(f_1), ..., LT(f_s)\rangle$ and so F is a Groebner basis for I.
For details of the proof, see [6, p. 85]. □

Example 7.

1) Consider as monomial ordering the lexicographic ordering on $k[x, y]$ with $x > y > 1$. Let us consider $f_1 = xy - y^3$, $f_2 = y^2 - 1$ and let us check whether $F = \{f_1, f_2\}$ is a Groebner basis. We have seen in Example 6 that

$$S(f_1, f_2) = x - y^4.$$

As $LT(S(f_1, f_2)) = x$ is not divisible by $LT(f_1) = xy$ or $LT(f_2) = y^2$, we have that $\overline{S(f_1, f_2)}^F \neq 0$. Therefore we can conclude that F is not a Groebner basis.

2) Consider now as monomial ordering the graded lexicographic ordering on $k[x, y]$ with $x > y > 1$ and let us consider the same set F as in 1). In this situation, we have

$$\begin{aligned} S(f_1, f_2) &= \frac{y^3}{-y^3}(xy - y^3) - \frac{y^3}{y^2}(y^2 - 1) \\ &= y^3 - xy - y^3 + y \\ &= -xy + y \\ &= -f_1 - yf_2. \end{aligned}$$

We have $\overline{S(f_1, f_2)}^F = 0$ for any order on F and thus we can conclude that F is a Groebner basis.

This example shows that a finite set F of polynomials on $k[x_1, ..., x_n]$ may be a Groebner basis for one monomial ordering, but not for another monomial ordering.

4.4 Construction of a Groebner Basis

Now that we know how to check whether a given basis of an ideal $I \subset k[x_1, ..., x_n]$ is a Groebner basis for a fixed monomial ordering on $k[x_1, ..., x_n]$, we would like to be able to construct a Groebner basis from this given ideal. The following theorem will give us the tool to do this.

Theorem 4.15 (Buchberger's Algorithm). *Let $I = \langle f_1, ..., f_s \rangle$ be a non-zero ideal. Then a Groebner basis for I can be constructed in a finite number of steps by the following algorithm:*

Algorithm 2 Buchberger's algorithm

Require: $F = (f_1, ..., f_s)$
Ensure: a Groebner basis $G = (g_1, ..., g_t)$ for I, with $F \subset G$
  $G := F$
  $G' := \emptyset$
  while $G \neq G'$ **do**
    $G' = G$
    for each pair (p, q), $p \neq q$ in G' **do**
      $S := \overline{S(p,q)}^{G'}$
      if $S \neq 0$ **then**
        $G := G \cup \{S\}$
      end if
    end for
  end while

Proof. Let us start by proving that $G \subset I$ holds at each stage of the algorithm. We start with $G = F \subset I$, thus it is true initially. Whenever we enlarge G, we do so by adding to G the remainder $S = \overline{S(p,q)}^{G'}$, where $p, g \in G$. Therefore, if $G \subset I$, then p, q and $S(p, q) \in I$. Since we are dividing by $G' \subset I$, it follows that $G \cup \{S\} \subset I$.
The next step is to prove if the output of the algorithm is indeed a Groebner basis of I. The set G contains at every stage of the algorithm the given basis F of I and $S \in I$, so that G is also a basis of I. In addition, the algorithm stops when $G = G'$, which means that $S = \overline{S(p,q)}^{G'} = 0$ for each $p, q \in G$. Thus by Theorem 4.14, G is a Groebner basis of I.
Finally, it remains to show that the algorithm stops after a finite number of steps. We have to consider what happens after each pass through the while loop. The set $G = \{g_1, ...g_t\}$ consists of $G' = \{g_1, ..., g_s\}$, with $s \leq t$ (the old G), together with the non-zero remainders of S-polynomials of elements of

G'. Since $G' \subset G$, we have

$$\langle LT(G')\rangle = \langle LT(g_1), ..., LT(g_t)\rangle \subset \langle LT(g_1), ..., LT(g_s)\rangle = \langle LT(G)\rangle. \quad (4.3)$$

If $G' \neq G$, then we have added a non-zero remainder S of an S-polynomial to G. Since S is a remainder of the division by G', $LT(S)$ is not divisible by the leading terms of elements of G' and therefore $LT(S) \notin \langle LT(G')\rangle$. However, $LT(S) \in \langle LT(G)\rangle$, so that $\langle LT(G')\rangle$ is strictly smaller than $\langle LT(G)\rangle$ if $G' \neq G$. By (4.3), the ideals $\langle LT(G')\rangle$ from successive iterations of the loop form an ascending chain of ideals in $k[x_1, ..., x_n]$. By Proposition 3.3 $k[x_1, .., x_n]$ is Noetherian and the ascending chain of ideals will stabilize, so that $\langle LT(G')\rangle = \langle LT(G)\rangle$ after a finite number of steps. It follows that $G' = G$ as otherwise $\langle LT(G')\rangle$ is strictly smaller than $\langle LT(G)\rangle$. Thus, the algorithm must stop after a finite number of steps. □

In general, the Buchberger's algorithm consists in extending a basis F to a Groebner basis by successively adding non-zero remainders $\overline{S(f_p, f_q)}^F$ where $1 \leq p < q \leq s$.

Example 8. Consider as monomial ordering the lexicographic ordering on $k[x, y]$ with $x > y > 1$. Let us consider $f_1 = xy - y^3$, $f_2 = y^2 - 1$. In Example 7 of Subsection 4.3, we could conclude that F is not a Groebner basis as $\overline{S(f_1, f_2)}^F = x - y^4 \neq 0$ and so we must add $f_3 = x - y^4$ to our set F. Therefore let now $F = \{f_1, f_2, f_3\}$. Then we have

$$\begin{aligned}
&S(f_1, f_2) = f_3, \text{ so}\\
&\overline{S(f_1, f_2)}^F = 0,\\
&S(f_1, f_3) = 1 \cdot (xy - y^3) - y(x - y^4) = y^5 - y^3 = y^3 f_2, \text{ so that}\\
&\overline{S(f_1, f_3)}^F = 0,\\
&S(f_2, f_3) = x(y^2 - 1) - y^2(x - y^4) = -x + y^4 = -f_3, \text{ so that}\\
&\overline{S(f_2, f_3)}^F = 0.
\end{aligned}$$

Finally, we can conclude that $F = \{xy - y^3, y^2 - 1, x - y^4\}$ is a Groebner basis for the ideal $I = \langle xy - y^3, y^2 - 1\rangle$.

Remark 5. The Groebner bases constructed by using Buchberger's algorithm are often bigger than necessary. For instance consider Example 8. We have that

$$F' = \{y^2 - 1, x - y^4\} \subset \{xy - y^3, y^2 - 1, x - y^4\} = F$$

and

$$f_1 = xy - y^3 = y^3(y^2 - 1) + y(x - y^4) = y^3 \cdot f_2 + y \cdot f_3$$

so that

$$\langle y^2 - 1, x - y^4 \rangle = \langle xy - y^3, y^2 - 1 \rangle.$$

In addition, we have

$$S(f_2, f_3) = x(y^2 - 1) - y^2(x - y^4) = -x + y^4 = -f_3 \Rightarrow \overline{S(f_2, f_3)}^{F'} = 0,$$

therefore we can conclude that $F' = \{y^2 - 1, x - y^4\}$ is another, smaller Groebner basis of $I = \langle xy - y^3, y^2 - 1 \rangle$. This situation occurred as the leading term $LT(f_1) = xy$ is an unneeded generator for $LT(I)$.

4.5 Applications of Groebner Bases

Ideals are algebraic objects and therefore we can define natural algebraic operations on them. Groebner bases have often an important role in the computation of these operations. In this section, we will see how to compute for example intersections of ideals or ideal quotients, but also other interesting applications for Groebner bases. More applications of Groebner bases can be found in *An Introduction to Gröbner Bases* [1], *Gröbner Bases: A Short Introduction for Systems Theorists* [5], *An Introduction to Gröbner Bases, Pure and Applied Mathematics* [13] and *Gröbner Bases, Ideal Computation and Computational Invariant Theory* [27].

4.5.1 Ideal Membership Problem

As already remarked before, Corollary 4.10 gives us an algorithm for solving the ideal membership problem if we know a Groebner basis F for the ideal I in question. It suffices to compute the normal form of f by F to check whether $f \in I$. If $\overline{f}^F = 0$, then we can conclude that f is in I.

Example 9. Consider as monomial ordering the lexicographic ordering on $k[x, y]$ with $x > y > 1$ and let us take $I = \langle xy - y^3, y^2 - 1 \rangle$. We want to check if $f = x - y^2 \in I$. As we have seen in Example 8 and Remark 5, $F = \{y^2 - 1, x - y^4\}$ is a Groebner basis of I. The polynomial division of f by F provides us

$$f = x - y^2 = y^2(y^2 - 1) + 1 \cdot (x - y^4) + 0.$$

Thus, we can conclude that $f \in I$.

4.5.2 Elimination

Another fundamental problem that can be solved using Groebner bases is elimination: let I be an ideal in $k[x_1, ..., x_n]$ and $S \subset \{x_1, ..., x_n\}$. We would like to find the ideal $J = I \cap k[S]$. In other words, we want to eliminate the variables $x_i \in S^c = \{x_1, ..., x_n\} \backslash S$ in the ideal I.

Definition 4.16. *Let I be an ideal in $k[x_1, ..., x_n]$ and $S \subset \{x_1, ..., x_n\}$. Then the ideal $I \cap k[S]$ in $k[S]$ is called an **elimination ideal**. If $S = \{x_{l+1}, ..., x_n\}$ for some $l \in \{0, ..., n\}$, then the ideal $I \cap k[S]$ in $k[S]$ is called the **l-th elimination ideal** I_l.*

Elimination ideals are very useful for many applications of Groebner bases such as the intersection of ideals, the quotient of ideals or the computation of a least common multiple of two non-zero polynomials. The advantage is that the computation of an elimination ideal is quite easy as the elimination theorem shows. For this theorem we need a global monomial ordering with a special property.

Definition 4.17. *Let $S \subset \{x_1, ..., x_n\}$. A monomial ordering $>$ on $k[x_1, ..., x_n]$ is called an **elimination ordering** with respect to S^c if the following is true for all $f \in k[x_1, ..., x_n]$:*

$$LT(f) \in k[S] \implies f \in k[S].$$

Theorem 4.18 (Elimination Theorem). *Let I be an ideal in $k[x_1, ..., x_n]$ and $S \subset \{x_1, ..., x_n\}$. Let G be a Groebner basis of I with respect to a global elimination ordering with respect to S^c. Then the set*

$$G' = G \cap k[S]$$

is a Groebner basis of the elimination ideal $I \cap k[S]$ with respect to the ordering induced on $k[S]$.

Proof. It is enough to show that

$$\langle LT(I \cap k[S]) \rangle = \langle LT(G') \rangle$$

by the definition of a Groebner basis. It is clear that $\langle LT(G') \rangle \subset \langle LT(I \cap k[S]) \rangle$ by construction. To show the other inclusion $\langle LT(I \cap k[S]) \rangle \subset \langle LT(G') \rangle$, it suffices to show that for an arbitrary $f \in I \cap k[S]$ the leading term $LT(f)$ is divisible by $LT(g)$ for some $g \in G'$. Since $f \in I \cap k[S] \subset I$, we get that $LT(f)$ is divisible by $LT(g)$ for some $g \in G$ since G is a Groebner basis of I. Since $f \in I \cap k[S]$, $LT(g)$ contains only the variables $x_i \in S$. Since the monomial ordering we are considering is an elimination ordering, we have that $LT(g) \in k[S]$ implies $g \in k[S]$. Therefore we have $g \in G \cap k[S] = G'$ and so the theorem is proved. □

Remark 6. An example of a global monomial ordering that can be used for the elimination theorem is the global block ordering (also known as global product ordering) which is defined in the following way:
Consider $S \subset \{x_1, ..., x_n\}$ and let $T = S^{\mathsf{c}}$. Let $>_S$ on $k[S]$ and $>_T$ on $k[T]$ be global monomial orderings. The global block ordering $> = (>_S, >_T)$ on $k[x_1, ..., x_n]$ is defined by

$$T^\alpha S^\gamma > T^\beta S^\delta \iff T^\alpha >_T T^\beta \text{ or } (T^\alpha = T^\beta \text{ and } S^\gamma >_S S^\delta).$$

In particular, the lexicographic ordering $>_{lex}$ on $k[x_1, ..., x_n]$ with $x_1 >_{lex} ... >_{lex} x_n >_{lex} 1$ is a global block ordering for each $S = \{x_{l+1}, ..., x_n\}$ with $l \in \{0, ..., n\}$, $T = S^{\mathsf{c}}$, $>_S$ and $>_T$ being lexicographic orderings on $k[S]$ and on $k[T]$ respectively with $x_i >_S x_j >_S 1$ and $x_i >_T x_j >_T 1$ for $i < j$. Indeed, we have

$T^\alpha S^\gamma >_{lex} T^\beta S^\delta$
$\iff \boldsymbol{x}^a >_{lex} \boldsymbol{x}^b$ with a the vector (α, γ) and b the vector (β, δ)
$\iff$ the leftmost nonzero entry of the vector $a - b$ is positive
$\iff$ the leftmost nonzero entry of the vector $(\alpha - \beta, \gamma - \delta)$ is positive
$\iff$ the leftmost nonzero entry of the vector $\alpha - \beta$ is positive
(or $\alpha = \beta$ and the leftmost nonzero entry of the vector $\gamma - \delta$ is positive)
$\iff T^\alpha >_T T^\beta$ or $(T^\alpha = T^\beta$ and $S^\gamma >_S S^\delta)$

Let I be an ideal of $k[x_1, ..., x_n]$ and choose $S = \{x_{l+1}, ..., x_n\}$ with $l \in \{0, ..., n\}$. Applying the elimination theorem on I and S with the lexicographic ordering on $k[x_1, ..., x_n]$ with $x_1 > ... > x_n > 1$, we get a Groebner basis of the l-th elimination ideal $I_l = I \cap k[x_{l+1}, ..., x_n]$. In the following, we will usually apply the elimination theorem with the lexicographic ordering.

Example 10. Consider the ideal

$$I = \langle x^2 + yz - 1, y^2 + xz - 1, z^2 + xy - 1 \rangle \in k[x, y, z].$$

Using SINGULAR [14], we get a Groebner basis for I with respect to the lexicographic ordering on $k[x, y, z]$ where $x > y > z > 1$. This Groebner basis is given by the following polynomials

$$\begin{aligned} g_1 &= x + 2y^2z - y - z, \\ g_2 &= yz^3 - yz - z^4 + z^2, \\ g_3 &= y^2 - yz - 2z^4 + 3z^2 - 1, \\ g_4 &= 2z^5 - 3z^3 + z. \end{aligned}$$

Therefore, we have that

$$I_1 = I \cap k[y,z] = \langle g_2, g_3, g_4 \rangle$$

is the first elimination ideal of I and

$$I_2 = I \cap k[z] = \langle g_4 \rangle$$

is the second elimination ideal of I.

```
> ring r=0,(x,y,z),lp;
> ideal I=x2+yz-1,y2+xz-1,z2+xy-1;
> std(I);
_[1]=x+2y2z-y-z
_[2]=yz3-yz-z4+z2
_[3]=y2-yz-2z4+3z2-1
_[4]=2z5-3z3+z
```

Example 11. Elimination can also be used to determine the **Chern character** of a complex vector bundle E as a polynomial in the Chern classes. Indeed, let the $a_1, ..., a_n$ be the Chern roots. Then the Chern classes c_j, $j \in \{1, ..., n\}$, are defined as the j-th elementary symmetric polynomial in $a_1, ..., a_n$. In other words

$$\begin{aligned} c_1 &= \sum_{i=1}^{n} a_i, \\ c_2 &= \sum_{1 \le i_1 < i_2 \le n} a_{i_1} a_{i_2}, \\ c_3 &= \sum_{1 \le i_1 < i_2 < i_3 \le n} a_{i_1} a_{i_2} a_{i_3} \quad \text{etc.} \end{aligned}$$

Finally, the Chern character ch is defined as

$$ch = ch_0 + ch_1 + ch_2 + ...,$$

where

$$ch_n = \frac{1}{n!} \sum_{i=1}^{n} a_i^n.$$

However we would like to express the Chern character as a polynomial in the Chern classes $c_1, ..., c_n$. For $n = 5$, we get by using SINGULAR

$$ch_5 = \frac{1}{120}(c_1^5 - 5c_1^3 c_2 + 5c_1^2 c_3 + 5c_1 c_2^2 - 5c_1 c_4 - 5c_2 c_3 + 5c_5).$$

For more details on Chern classes see *Algebraic Geometry* [15] and *Chern Classes* [28].

```
> ring r=0, (a(1..5),c(1..5),k(5)), lp;
> ideal I=c(1)-a(1)-a(2)-a(3)-a(4)-a(5),c(2)-a(1)*a(2)
-a(1)*a(3)-a(1)*a(4)-a(1)*a(5)-a(2)*a(3)-a(2)*a(4)-a(2)*a(5)
-a(3)*a(4)-a(3)*a(5)-a(4)*a(5),c(3)-a(1)*a(2)*a(3)
-a(1)*a(2)*a(4)-a(1)*a(2)*a(5)-a(1)*a(3)*a(4)-a(1)*a(3)*a(5)
-a(1)*a(4)*a(5)-a(2)*a(3)*a(4)-a(2)*a(3)*a(5)-a(2)*a(4)*a(5)
-a(3)*a(4)*a(5),c(4)-a(1)*a(2)*a(3)*a(4)-a(1)*a(2)*a(3)*a(5)
-a(1)*a(2)*a(4)*a(5)-a(1)*a(3)*a(4)*a(5)-a(2)*a(3)*a(4)*a(5),
c(5)-a(1)*a(2)*a(3)*a(4)*a(5),k(5)-(1/120)*(a(1)^5+a(2)^5
+a(3)^5+a(4)^5+a(5)^5);
> std(I);
_[1]=c(1)^5-5*c(1)^3*c(2)+5*c(1)^2*c(3)+5*c(1)*c(2)^2
     -5*c(1)*c(4)-5*c(2)*c(3)+5*c(5)-120*k(5)
_[2]=a(5)^5-a(5)^4*c(1)+a(5)^3*c(2)-a(5)^2*c(3)+a(5)*c(4)-c(5)

_[3]=a(4)^4+a(4)^3*a(5)-a(4)^3*c(1)+a(4)^2*a(5)^2
     -a(4)^2*a(5)*c(1)+a(4)^2*c(2)+a(4)*a(5)^3-a(4)*a(5)^2*c(1)
     +a(4)*a(5)*c(2)-a(4)*c(3)+a(5)^4-a(5)^3*c(1)+a(5)^2*c(2)
     -a(5)*c(3)+c(4)
_[4]=a(3)^3+a(3)^2*a(4)+a(3)^2*a(5)-a(3)^2*c(1)+a(3)*a(4)^2
     +a(3)*a(4)*a(5)-a(3)*a(4)*c(1)+a(3)*a(5)^2-a(3)*a(5)*c(1)
     +a(3)*c(2)+a(4)^3+a(4)^2*a(5)-a(4)^2*c(1)+a(4)*a(5)^2
     -a(4)*a(5)*c(1)+a(4)*c(2)+a(5)^3-a(5)^2*c(1)+a(5)*c(2)-c(3)

_[5]=a(2)^2+a(2)*a(3)+a(2)*a(4)+a(2)*a(5)-a(2)*c(1)+a(3)^2
     +a(3)*a(4)+a(3)*a(5)-a(3)*c(1)+a(4)^2+a(4)*a(5)-a(4)*c(1)
     +a(5)^2-a(5)*c(1)+c(2)
_[6]=a(1)+a(2)+a(3)+a(4)+a(5)-c(1)
```

4.5.3 Intersection of Ideals

Knowing a set of generators of two polynomial ideals I and J, we would like to be able to compute a set of generators of their intersection. For this computation, we need the sum of ideals, Groebner bases and the elimination theorem.

Definition 4.19. *Let I and J be ideals of $k[x_1, ..., x_n]$.*

1. *The* ***intersection of*** I ***and*** J *is defined by*

$$I \cap J = \{f : f \in I \text{ and } f \in J\}.$$

2. *The* ***sum of*** I ***and*** J *is defined by*

$$I + J = \{f + g : f \in I \text{ and } g \in J\}.$$

Proposition 4.20. *If I and J are ideals of $k[x_1, ..., x_n]$, then $I \cap J$ and $I + J$ are also ideals in $k[x_1, ..., x_n]$. In particular, if $I = \langle f_1, ..., f_s \rangle$ and $J = \langle g_1, ..., g_t \rangle$, then $I + J = \langle f_1, ..., f_s, g_1, ..., g_t \rangle$.*

Proof. Let us first show that $I \cap J$ is an ideal of $k[x_1, ..., x_n]$. As I and J are ideals, $0 \in I$ and $0 \in J$ and therefore $0 \in I \cap J$. Let $f, g \in I \cap J$ and $h \in k[x_1, ..., x_n]$. Since I and J are ideals, we have that $f + g \in I$, $f + g \in J$, $hf \in I$ and $hf \in J$. Thus, $f + g \in I \cap J$ and $hf \in I \cap J$ and so we can conclude that $I \cap J$ is an ideal of $k[x_1, ..., x_n]$.
Let us now show that $I + J$ is an ideal of $k[x_1, ..., x_n]$. As I and J are ideals, $0 \in I$ and $0 \in J$ and therefore $0 = 0 + 0 \in I + J$. Let $f, g \in I + J$ and $h \in k[x_1, ..., x_n]$. In this case, we can rewrite $f = f_1 + f_2$ and $g = g_1 + g_2$, where $f_1, g_1 \in I$ and $f_2, g_2 \in J$. Then we have

$$f + g = (f_1 + f_2) + (g_1 + g_2) = (f_1 + g_1) + (f_2 + g_2) \in I + J$$

as I and J are ideals and so $f_1 + g_1 \in I$ and $f_2 + g_2 \in J$. For the same reason, we have that $hf = hf_1 + hf_2 \in I + J$. Thus, we can conclude that $I + J$ is an ideal.
Finally, we want to prove that $I + J = \langle f_1, ..., f_s, g_1, ..., g_t \rangle$ if $I = \langle f_1, ..., f_s \rangle$ and $J = \langle g_1, ..., g_t \rangle$. If $h \in I + J$, then $h = f + g$ with $f \in I$ and $g \in J$. Since $I = \langle f_1, ..., f_s \rangle$ and $J = \langle g_1, ..., g_t \rangle$, we have that $f = \sum_{i=1}^{s} c_i f_i$ and $g = \sum_{j=1}^{t} d_j g_j$, where $c_i, d_j \in k[x_1, ..., x_n]$. Thus,

$$h = f + g = \sum_{i=1}^{s} c_i f_i + \sum_{j=1}^{t} d_j g_j \in \langle f_1, ..., f_s, g_1, ..., g_t \rangle.$$

Conversely, if $h \in \langle f_1, ..., f_s, g_1, ..., g_t \rangle$, then $h = \sum_{i=1}^{s} c_i f_i + \sum_{j=1}^{t} d_j g_j = f + g$, where $f = \sum_{i=1}^{s} c_i f_i \in I$ and $g = \sum_{j=1}^{t} d_j g_j \in J$. Therefore $h \in I + J$. We can conclude that $I + J = \langle f_1, ..., f_s, g_1, ..., g_t \rangle$ if $I = \langle f_1, ..., f_s \rangle$ and $J = \langle g_1, ..., g_t \rangle$. □

Remark 7. Notice that if G_1 is a Groebner basis of an ideal $I = \langle f_1, ..., f_s \rangle$ with respect to a global monomial ordering on $k[x_1, ..., x_n]$ and G_2 is a Groebner basis of an ideal $J = \langle g_1, ..., g_t \rangle$ with respect to the same monomial ordering, then $G_1 \cup G_2$ is not necessary a Groebner basis of the ideal $I + J = \langle f_1, ..., f_s, g_1, ..., g_t \rangle$. Indeed, consider the following example: let $I = \langle y^2 - z, x - y \rangle$ and $J = \langle x + z, z^2 \rangle$ and consider the lexicographic ordering on $k[x, y, z]$ with $x > y > z > 1$. We can easily check that $G_1 = \{y^2 - z, x - y\}$ and $G_2 = \{x + z, z^2\}$ are Groebner bases of I and of J, respectively. Consider now

$$G_1 \cup G_2 = \{y^2 - z, x - y, x + z, z^2\}.$$

If we compute the S-polynomial $S(x + z, x - y) = y + z$, we realise that $LT(S(x+z, x-y)) = y$ is not divisible by neither $LT(y^2-z) = y^2$, nor $LT(x-y) = x$, nor $LT(x+z) = x$, nor $LT(z^2) = z^2$ so that $\overline{S(x + z, x - y)}^{G_1+G_2} \neq 0$. We can therefore conclude by Buchberger's criterion that $G_1 \cup G_2$ is not a Groebner basis of $I + J$.

Lemma 4.21. *Let $p(t) \in k[t]$. If $I = \langle f_1(\boldsymbol{x}), ..., f_s(\boldsymbol{x}) \rangle \subset k[x_1, ...x_n]$, then $p(t)I = \langle p(t)f_1(\boldsymbol{x}), ..., p(t)f_s(\boldsymbol{x}) \rangle$ is an ideal in $k[x_1, ...x_n, t]$.*

Proof. Let us consider $q_i = p(t)f_i(x) \in k[x_1, ..., x_n, t]$ for $1 \leq i \leq s$. Then by Lemma 3.1, we can conclude that $p(t)I = \langle q_1, ..., q_s \rangle$ is an ideal in $k[x_1, ...x_n, t]$. □

Proposition 4.22. *Let I and J be ideals of $k[x_1, ..., x_n]$. Let $L = tI + (1-t)J$ in $k[x_1, ..., x_n, t]$ (thus, we add a new variable t). Then*

$$I \cap J = L \cap k[x_1, ..., x_n].$$

Proof. " $\subset$ " If $x \in I \cap J$, then $x = tx + (1 - t)x$ with $x \in I$ and $x \in J$, so that $x \in L$. By definition $x \in k[x_1, ..., x_n]$, therefore $x \in L \cap k[x_1, ..., x_n]$.
" $\supset$ " If $x \in L \cap k[x_1, ..., x_n]$, then $x \in L$ and so $x = t \cdot i + (1 - t)j$ for some $i \in I$ and $j \in J$. As $x \in k[x_1, ..., x_n]$, we can evaluate $x = t \cdot i + (1 - t)j$ in $t = 0$ and $t = 1$ to get $x = i = j$. Thus we can conclude that $x \in I \cap J$. □

The proposition above shows that $I \cap J$ is an elimination ideal. This result, Proposition 4.20 and the Elimination theorem provides us with the following algorithm to compute intersections of ideals:
Let $I = \langle f_1, ..., f_s \rangle$ and $J = \langle g_1, ..., g_t \rangle$ be ideals in $k[x_1, ..., x_n]$. Consider now the ideal

$$tI + (1 - t)J = \langle tf_1, ..., tf_s, (1 - t)g_1, ..., (1 - t)g_t \rangle \subset k[x_1, ..., x_n, t]$$

and compute a Groebner basis of this ideal with respect to the lexicographic ordering with $t > x_1 > ... > x_n > 1$. By the elimination theorem, the elements of this basis which do not contain the variable t will form a basis, in particular a Groebner basis, of $I \cap J$.

Example 12. Consider the ideals $I = \langle x - y^2, x^2 \rangle$ and $J = \langle xy \rangle$ in $k[x, y]$. Then we get the ideal $tI + (1-t)J = \langle tx - ty^2, tx^2, xy - txy \rangle$. Using SINGULAR, we get that $\{xy^2, x^2y - xy^3, txy - xy, tx^2 - txy^2, t^2y^2 - tx\}$ is a Groebner basis of $tI+(1-t)J$ with respect to the lexicographic ordering with $t > x > y > 1$. As $\{xy^2, x^2y - xy^3, txy - xy, tx^2 - txy^2, t^2y^2 - tx\} \cap k[x, y] = \{xy^2, x^2y - xy^3\}$, we get that

$$\langle x - y^2, x^2 \rangle \cap \langle xy \rangle = \langle xy^2, x^2y - xy^3 \rangle.$$

```
> ring r=0,(t,x,y),lp;
> ideal L=tx-ty2,tx2,xy-txy;
> std(L);
_[1]=xy2
_[2]=x2y-xy3
_[3]=txy-xy
_[4]=tx2-txy2
_[5]=t2y2-tx
```

Remark 8. The intersection of two principal polynomial ideals, i.e. ideals that are generated by a single polynomial, can be computed in a different, sometime faster way by using the notation of the least common multiple $h \in k[x_1, ..., x_n]$ of $f, g \in k[x_1, ..., x_n]$, where f and g are non-zero.

Definition 4.23. *Consider a global monomial ordering on $k[x_1, ..., x_n]$. The polynomial $h \in k[x_1, ..., x_n]$ is* ***the least common multiple*** *of the non-zero polynomials f and g of $k[x_1, ..., x_n]$ if*

1) f and g divides h.

2) h divides any polynomial which both f and g divide.

3) $LC(h) = 1$.

It is denoted by $h = \mathrm{lcm}(f, g)$.

Note that the least common multiple of two polynomials in $k[x_1, ..., x_n]$ depends on the global monomial ordering considered as condition 3) depends on the global monomial ordering considered.

Proposition 4.24. *Let f and g be non-zero polynomials of $k[x_1, ..., x_n]$. If $I = \langle f \rangle$ and $J = \langle g \rangle$, then $I \cap J = \langle h \rangle$, where $h = \text{lcm}(f, g)$.*

Proof. Let $p \in I \cap J$, then $p \in \langle f \rangle$ and $p \in \langle g \rangle$ so that f and g divide p. By definition of the least common multiple, h divides p and so $p \in \langle h \rangle$. Conversely, let $p \in \langle h \rangle$. Thus, h divides p, but by defintion of h, f and g divide h so that f and g also divide p. Finally, $p \in \langle f \rangle$ and $p \in \langle g \rangle$, thus $p \in I \cap J$. □

Example 13. Consider the ideals $I = \langle x^2 \rangle$ and $J = \langle xy^2 \rangle$ in $k[x, y]$. Then we get the ideal $tI + (1 - t)J = \langle tx^2, xy^2 - txy^2 \rangle$. By computing the S-polynomial of tx^2 and $xy^2 - txy^2$ we get x^2y^2. It is easily checked that $\{tx^2, xy^2 - txy^2, x^2y^2\}$ is a Groebner basis of $tI + (1 - t)J$. As $\{tx^2, xy^2 - txy^2, x^2y^2\} \cap k[x, y] = \{x^2y^2\}$, we get that

$$\langle x^2 \rangle \cap \langle xy^2 \rangle = \langle x^2y^2 \rangle = \langle \text{lcm}(x^2, xy^2) \rangle.$$

4.5.4 Least Common Multiple and Greatest Common Divisor of Polynomials

We have just seen that we can use a least common multiple of two non-zero polynomials f and g in $k[x_1, ..., x_n]$ to compute the intersection of the principal ideals $I = \langle f \rangle$ and $J = \langle g \rangle$. The problem is that it is often not that easy to compute a least common multiple of two polynomials. In Example 13, we had to compute the intersection of principal ideals whose generators were monomials. In that special case, we could easily find a least common multiple. As soon as we want to find a least common multiple of two polynomials that are not monomials, the computation is more complicated. A solution to this problem is to compute the intersection of the principal ideals $\langle f \rangle$ and $\langle g \rangle$ by the general method seen in Section 4.5.3 to get a least common multiple of the two non-zero polynomials $f, g \in k[x_1, ..., x_n]$.
We know by Proposition 4.24 that the intersection of two principal ideals $I = \langle f \rangle$ and $J = \langle g \rangle$ is a principal ideal, in particular a principal ideal generated by $\text{lcm}(f, g)$. However, using the general method of Section 4.5.3, we may get a Groebner basis of $I + (1 - t)J$ with respect to the lexicographic ordering that has more than one element without the variable t so that it is not obvious that this Groebner basis generates a principal ideal. This is due to the fact that a Groebner basis with respect to a fixed global monomial ordering in not unique which we already realised in Remark 5. To solve this problem, we need the following results and notions.

Lemma 4.25. *Let G be a Groebner basis for the ideal $I \subset k[x_1, ..., x_n]$ with respect to some global monomial ordering on $k[x_1, ..., x_n]$. Let g be an element*

of G such that $LT(g) \in \langle LT(G\backslash\{g\})\rangle$. Then $G\backslash\{g\}$ is also a Groebner basis for I with respect to the same global monomial ordering.

Proof. Fix a global monomial ordering on $k[x_1, ..., x_n]$. By definition of a Groebner basis, we have that $\langle LT(G)\rangle = \langle LT(I)\rangle$. If $LT(g) \in \langle LT(G\backslash\{g\})\rangle$, then we have $\langle LT(G\backslash\{g\})\rangle = \langle LT(G)\rangle$. It follows that $G\backslash\{g\}$ is also a Groebner basis for I. □

So by dividing each polynomial g of G by its leading coefficient and by removing any g such that $LT(g) \in \langle LT(G\backslash\{g\})\rangle$ from G, we get a special type of Groebner basis: a minimal Groebner basis.

Definition 4.26. *Let $I \subset k[x_1, ...x_n]$ be an ideal and consider a global monomial ordering on $k[x_1, ..., x_n]$. A **minimal Groebner basis** of I is a Groebner basis G of I such that*

1) $LC(g) = 1$ for all $g \in G$.

2) For all $g \in G$, $LT(g) \notin \langle LT(G\backslash\{g\})\rangle$.

Unfortunately, there may exist several minimal Groebner bases of an ideal I with respect to the same global monomial ordering. Indeed, consider the ideal $I = \langle x + y, y^2\rangle \subset k[x, y]$. Then it easily checked that $G = \{x + y, y^2\}$ is a Groebner of I with respect to the lexicographic ordering where $x > y > 1$. In addition, G satisfies conditions 1) and 2) of Defintion 4.26 and so we can conclude that G is minimal. On the other hand, we can check that $G' = \{x + y^2 + y, y^2\}$ is another minimal Groebner basis of I with respect to the same ordering. However, if we go even further we can get a certain form of Groebner basis of I with respect to a global monomial ordering on $k[x_1, ..., x_n]$ which will be unique.

Definition 4.27. *Let $I \in k[x_1, ...x_n]$ be an ideal and consider a global monomial ordering on $k[x_1, ..., x_n]$. A **reduced Groebner basis** of I is a Groebner basis G of I such that*

1) $LC(g) = 1$ for all $g \in G$.

2) For all $g \in G$, no monomial of g lies in $\langle LT(G\backslash\{g\})\rangle$.

Note that each reduced Groebner basis G of an ideal I is a minimal Groebner basis of this ideal. Indeed if an element $g \in G$ satisfies condition 2) of Defintion 4.27, then it also satisfies condition 2) of Definition 4.26.

Proposition 4.28. *Let $I \in k[x_1, ...x_n]$ be a non-zero ideal and consider a global monomial ordering on $k[x_1, ..., x_n]$. Then I has a unique reduced Groebner basis with respect to this monomial ordering.*

Proof. Let us fix a global monomial ordering on $k[x_1, ..., x_n]$. We start by searching a minimal Groebner basis G of the ideal $I = \langle f_1, ..., f_s \rangle$. First we compute a Groebner basis G of I by using Buchberger's algorithm. Next we remove each element $g \in G$ such that $LT(g) \in LT(G \backslash \{g\})$ by Lemma 4.25 and then we divide each remaining element of G by its leading coefficient. Our Groebner basis G is now minimal by construction.
Let $g \in G$ and consider $g' = \overline{g}^{G \backslash \{g\}}$ and $G' = (G \backslash \{g\}) \cup \{g'\}$. This new set G' is a minimal Groebner basis for I. Indeed, we have that $LT(g') = LT(g)$ because to get g' we divided g by $G \backslash \{g\}$, the leading term of g goes to the remainder since it is not divisible by any element of $LT(G \backslash \{g\})$ by minimality of G. Therefore, $\langle LT(G') \rangle = \langle LT(G) \rangle = \langle LT(I) \rangle$ and clearly G' is a basis of I so that G' is a Groebner basis of I. It is minimal since $LT(g') = LT(g) \notin \langle LT(G \backslash \{g\}) \rangle = \langle LT(G' \backslash \{g'\}) \rangle$. By construction, no monomial of g' is in $\langle LT(G' \backslash \{g'\}) \rangle$. Indeed g' is the remainder of the division of g by $G \backslash \{g\}$ and by Theorem 4.1, no monomial of the remainder is divisible by elements from $LT(G \backslash \{g\}) = LT(G' \backslash \{g'\})$. We say that g' is reduced for G'. We can observe that g' is also reduced for any other minimal Groebner basis of I that contains g' and has the same set of leading terms. This follows because the definition of reduced elements only involves the leading terms. So we can repeat the above process for each $g \in G$, i.e. if $G = \{g_1, ..., g_t\}$ is a minimal Groebner basis of I, then for each $i \in \{1, ..., t\}$, we compute $g'_i = \overline{g_i}^{G \backslash \{g_i\}}$ and we finally get a reduced Groebner basis $G' = \{g'_1, ..., g'_t\}$.
The next step is to prove uniqueness of the reduced Groebner basis for I. Suppose that $G = \{g_1, ..., g_s\}$ and $G' = \{g'_1, ..., g'_t\}$ are both reduced Groebner bases for I. Therefore, they are both minimal and they have the same leading terms, i.e $LT(G) = LT(G')$. This second observation is true since by taking $g_1 \in G$, then $g_1 = \sum_{i=1}^{t} a_i g'_i$, where $a_i \in k[x_1, ..., x_n]$ and $g_i \in G'$. Thus $LT(g'_i)$ divides $LT(g_1)$ for some $i \in \{1, ..., t\}$. This also works in the other direction and so for some $j \in \{1, ..., s\}$ $LT(g_j)$ divides $LT(g'_i)$. By minimality this is only possible if $j = 1$ and thus we must have $LT(g_1) = LT(g'_i)$ for some i. This works for each g_k and is completely symmetrical and so $LT(G) = LT(G')$. So if $g \in G$, there is $g' \in G'$ such that $LT(g) = LT(g')$. Then $g - g' \in I$ and since G is a Groebner basis, we have that

$$\overline{g - g'}^{G} = 0. \tag{4.4}$$

But as $LT(g) = LT(g')$, these terms cancel in $g - g'$ and the remaining terms are not divisible by any element of $LT(G) = LT(G')$ since G and G' are reduced. This shows that $\overline{g - g'}^{G} = g - g'$ and we must have by (4.4), $g - g' = 0$, i.e $g = g'$. As this works for any each $g \in G$, we get that $G = G'$. □

The first part of the proof of Proposition 4.28 explains the algorithm to get the reduced Groebner basis of an ideal I with respect to a fixed global monomial ordering. First we use the Buchberger's algorithm to get a a Groebner basis of I, then we turn G into a minimal Groebner basis by dividing each polynomial g of G by its leading coefficient and by removing any g such that $LT(g) \in \langle LT(G\backslash\{g\})\rangle$ from G. Finally, we reduce every element $g \in G$ by replacing g by $g' = \overline{g}^{G\backslash\{g\}}$ in G.

Require: $F = (f_1, ..., f_s)$
Ensure: a reduced Groebner basis $G = (g'_1, ..., g'_t)$ for I
  $G := F$
  $G' := \emptyset$
  while $G \neq G'$ **do**
    $G' = G$
    for each pair (p, q), $p \neq q$ in G' **do**
      $S := \overline{S(p,q)}^{G'}$
      if $S \neq 0$ **and** $LT(S) \notin \langle LT(G\backslash\{S\})\rangle$ **then**
        $G := G \cup \{\frac{S}{LC(S)}\}$
      end if
    end for
  end while
  $G' := \emptyset$
  for each $g \in G$ **do**
    if $LT(g) \notin \langle LT(G\backslash\{g\})\rangle$ **then**
      $g' := \frac{g}{LC(g)}$
      $G' := G' \cup \{g'\}$
    end if
  end for
  $G := G'$
  $G' := \emptyset$
  for each $g \in G$ **do**
    $g' := \overline{g}^{G\backslash\{g\}}$
    $G' := G' \cup \{g'\}$
  end for
  $G := G'$

Example 14. Consider the ideal $I = \langle 2x + y^2 + y, y^2\rangle \subset k[x, y]$. Then it is easily checked that $G = \{2x + y^2 + y, y^2\}$ is a Groebner basis of I with respect to the lexicographic ordering where $x > y > 1$. In addition, G satisfies condition 2) of Defintion 4.26 since $LT(2x + y^2 + y) = 2x \notin \langle LT(G\backslash\{2x + y^2 + y\})\rangle = \langle y^2\rangle$ and $LT(y^2) = y^2 \notin \langle LT(G\backslash\{y^2\})\rangle = \langle 2x\rangle$.

By dividing $2x + y^2 + y$ by $LC(2x + y^2 + y) = 2$ we get $x + \frac{1}{2}y^2 + \frac{1}{2}y$. Then $G' = \{g_1 = x + \frac{1}{2}y^2 + \frac{1}{2}y, g_2 = y^2\}$ satisfies both conditions of Defintion 4.26 and so G' is a minimal Groebner basis of I. Next, compute

$$\overline{g_1}^{g_2} = x + \frac{1}{2}y$$
$$\text{and} \quad \overline{g_2}^{g_1} = y^2.$$

Finally, we have that $G'' = \{x + \frac{1}{2}y, y^2\}$ is the reduced Groebner basis of I with respect to the lexicographic ordering where $x > y > 1$.

Let us come back to the research of the least common multiple of $f, g \in k[x_1, ..., x_n]$, where f and g are non-zero. Consider the ideals $I = \langle f \rangle$ and $J = \langle g \rangle$ and fix a global monomial ordering on $k[x_1, ..., x_n]$. Using the reduced Groebner basis of $I + (1 - t)J$ and by eliminating the elements containing the variable t, there will only be one element left: the least common multiple of f and g. Indeed, suppose that there are at least two elements left:

$$(I + (1 - t)J) \cap k[x_1, ..., x_n] = \langle g'_1, ..., g'_t \rangle \text{ with } t \geq 2.$$

Then by Proposition 4.24, we have that $\langle g'_1, ..., g'_t \rangle = \langle \text{lcm}(f, g) \rangle$. It follows that for each $i \in \{1, ..., t\}$, $\text{lcm}(f, g)$ divides g'_i. This gives us a contradiction to 2) of the definition of a reduced Groebner basis. Thus, $t = 1$ and

$$(I + (1 - t)J) \cap k[x_1, ..., x_n] = \langle g'_1 \rangle = \langle \text{lcm}(f, g) \rangle.$$

Example 15. Consider the lexicographic ordering on $k[x, y]$ where $x > y > 1$. We want to find the least common multiple of $f = 2x^2 - y$ and $g = xy$ in $k[x, y]$. Therefore we will compute $\langle f \rangle \cap \langle g \rangle$ by applying Proposition 4.22. We have that

$$L = \langle tf, (1 - t)g \rangle = \langle 2tx^2 - ty, xy - txy \rangle.$$

By using SINGULAR, we get that $\{2x^3y - xy^2, ty^2 - 2x^2y, txy - xy, 2tx^2 - ty\}$ is a Groebner basis of L with respect to the lexicographic ordering on $k[t, x, y]$ where $t > x, y$. By the elimination theorem,

$$\{2x^3y - xy^2, ty^2 - 2x^2y, txy - xy, 2tx^2 - ty\} \cap k[x, y] = \{2x^3y - xy^2\}$$

is a Groebner basis of $\langle f \rangle \cap \langle g \rangle$. By dividing $2x^3y - xy^2$ by its leading coefficient 2, we immediately get the reduced Groebner basis $\{x^3y - \frac{1}{2}xy^2\}$ of $\langle f \rangle \cap \langle g \rangle$ since a Groebner basis consisting of a single element always satisfies condition 2) of Definition 4.27. Therefore we can conclude that

$$\text{lcm}(2x^2 - y, xy) = x^3y - \frac{1}{2}xy^2.$$

```
> ring r=0, (t,x,y),lp;
> ideal L;
> L=2tx2-ty,xy-txy;
> std(L);
_[1]=2x3y-xy2
_[2]=ty2-2x2y
_[3]=txy-xy
_[4]=2tx2-ty
```

Knowing the least common multiple of two non-zero polynomials f and g in $k[x_1, ..., x_n]$, we would like to compute the greatest common divisor of two polynomials f and g in $k[x_1, ..., x_n]$.

Definition 4.29. *Consider a global monomial ordering on $k[x_1, ..., x_n]$. The* ***greatest common divisor*** *of two non-zero polynomials $f, g \in k[x_1, ..., x_n]$ is the polynomial h such that*

1) h divides f and g.

2) If p is another polynomial which divides f and g, then p divides h.

3) $LC(h) = LC(fg)$.

It is denoted by $h = \gcd(f, g)$.

The following proposition gives us a relation between $\operatorname{lcm}(f, g)$ and $\gcd(f, g)$.

Proposition 4.30. *Consider a global monomial ordering on $k[x_1, ..., x_n]$ and let $f, g \in k[x_1, ..., x_n]$, where f and g are non-zero. Then*

$$\operatorname{lcm}(f, g) \cdot \gcd(f, g) = fg$$

which is equivalent to

$$\gcd(f, g) = \frac{fg}{\operatorname{lcm}(f, g)}. \tag{4.5}$$

Proof. We will proof the proposition by showing that (4.5) is verified. Let us write $h = \operatorname{lcm}(f, g)$. Since f and g divide h, there are $h_1, h_2 \in k[x_1, ..., x_n]$ such that

$$h = h_1 f = h_2 g.$$

Since fg is a common multiple of f and g and h is the least common multiple of f and g, we have that $h | fg$ and then we can write

$$\frac{fg}{h} = \frac{g}{h_1} \,|\, g \quad \text{and} \quad \frac{fg}{h} = \frac{f}{h_2} \,|\, f.$$

Thus, we can conclude that $\frac{fg}{h}$ is a common divisor of f and g and so it satisfies condition 1) of Definition 4.29. Since

$$LC\Big(\frac{fg}{h}\Big) = \frac{LC(fg)}{LC(h)} = LC(fg),$$

condition 3) of Defintion 4.29 is verified. Next we want to show that $\frac{fg}{h}$ is the greatest common divisor of f and g, i.e. it satisfies condition 2) of Defintion 4.29. Assume that D is another common divisor of f and g, i.e. D divides f and g. Then there are $f_1, f_2 \in k[x_1, ..., x_n]$ such that

$$f = f_1 D \quad \text{and} \quad g = g_1 D.$$

It follows that

$$f \,|\, f_1 g_1 D \quad \text{and } g \,|\, f_1 g_1 D$$

so that $f_1 g_1 D$ is a common multiple of f and g. Since h is the least common multiple of f and g, it follows

$$h \,|\, f_1 g_1 D.$$

Since we have

$$fg = f_1 g_1 D^2 = f_1 g_1 D \cdot D,$$

we get

$$\frac{fg}{h} = \frac{f_1 g_1 D}{g} \cdot D \implies D \,|\, \frac{fg}{h}.$$

We can conclude that $\frac{fg}{h} = \gcd(f, g)$. □

Proposition 4.30 allows us to compute the greatest common multiple of two polynomials of $k[x_1, ..., x_n]$ with respect to a global monomial ordering after we have computed its least common multiple.

Example 16. Consider the lexicographic ordering on $k[x, y]$ where $x > y > 1$. In Example 15, we computed that

$$\operatorname{lcm}(2x^2 - y, xy) = x^3 y - \frac{1}{2} x y^2.$$

By Proposition 4.30, it follows that

$$\gcd(2x^2 - y, xy) = \frac{(2x^2 - y) \cdot (xy)}{\operatorname{lcm}(2x^2 - y, xy)} = \frac{2x^3 y - xy^2}{x^3 y - \frac{1}{2} x y^2} = 2.$$

4.5.5 Quotient of an Ideal

Another operation on ideals is the quotient of ideals.

Definition 4.31. *Let I and J be ideals in $k[x_1, ..., x_n]$. Then the* ***ideal quotient of I by J*** *is defined by*

$$I : J = \{f \in k[x_1, ..., x_n] : fg \in I \text{ for all } g \in J\}.$$

Proposition 4.32. *If I and J are ideals in $k[x_1, ..., x_n]$, then $I : J$ is an ideal in $k[x_1, ..., x_n]$.*

Proof. Let $p, q \in I : J$ and $h \in k[x_1, ..., x_n]$. Then for all $g \in J$, we have $(p + q)g = pg + qg \in I$ and $(hp)g = h(pg) \in hI \subset I$. Hence $p + q$ and hp both belong to $I : J$ and so $I : J$ is an ideal of $k[x_1, ..., x_n]$. □

Now that we know that the quotient ideal is also an ideal, we would like to compute its basis. The following results will give us an algorithm to do so.

Theorem 4.33. *Consider a global monomial ordering on $k[x_1, ..., x_n]$. Let $I \subset k[x_1, ..., x_n]$ be an ideal and $g \in k[x_1, ..., x_n]$. If $\{h_1, ..., h_t\}$ is a basis of the ideal $I \cap \langle g \rangle$, then*

$$I : \langle g \rangle = \langle \frac{h_1}{g}, ..., \frac{h_t}{g} \rangle,$$

where for each $1 \leq i \leq t$, $\frac{h_i}{g}$ is the division of h_i by g in $k[x_1, ..., x_n]$.

Proof. " $\subset$ "If $f \in I : \langle g \rangle$, then by definition $fg \in I$. We also have that $fg \in \langle g \rangle$, so that $fg \in I \cap \langle g \rangle = \langle h_1, ..., h_t \rangle$. Therefore, we can write $fg = \sum_{i=1}^{t} r_i h_i$, where each $r_i \in k[x_1, ..., x_n]$. Since $h_1, ..., h_t$ is a basis of the ideal $I \cap \langle g \rangle$, each $h_i \in \langle g \rangle$. Hence each $\frac{h_i}{g} \in k[x_1, ...x_n]$ and so we can write $f = \sum_{i=1}^{t} r_i \frac{h_i}{g}$. Finally, $f \in \langle \frac{h_1}{g}, ..., \frac{h_t}{g} \rangle$.
" $\supset$ " Let $f \in \langle \frac{h_1}{g}, ..., \frac{h_t}{g} \rangle$. If $a \in \langle g \rangle$, then $a = bg$ for some $b \in k[x_1, ..., x_n]$. Therefore,

$$af = bgf \in \langle \frac{h_1}{g}, ..., \frac{h_t}{g} \rangle = I \cap \langle g \rangle \subset I.$$

Hence, by definition $f \in I : \langle g \rangle$. □

As we know from Section 4.5.3 how to compute an intersection of ideals, we can now compute a basis of a quotient ideal $I : \langle g \rangle$, where $I \subset k[x_1, ..., x_n]$ is an ideal and $g \in k[x_1, ..., x_n]$. The next proposition allows us to generalise this result.

Proposition 4.34. *Let I and J_i be ideals in $k[x_1, ..., x_n]$ for $1 \leq i \leq s$. Then*

$$I : \left(\sum_{i=1}^{s} J_i \right) = \bigcap_{i=1}^{s} (I : J_i) .$$

In particular, if $f_1, ..., f_s \in k[x_1, ..., x_n]$, then

$$I : \langle f_1, ..., f_s \rangle = \bigcap_{i=1}^{s} (I : \langle f_i \rangle) .$$

Proof. We will prove this statement by induction on s. For $s = 1$ it is clear. Suppose now that the statement is true for s and let us show that it remains correct for $s + 1$:
"$\subset$" Let $f \in I : \left(\sum_{i=1}^{s+1} J_i\right) = I : (\sum_{i=1}^{s} J_i + J_{s+1})$, then $gf \in I$ for all $g \in \sum_{i=1}^{s} J_i + J_{s+1}$. We can rewrite $g = h_1 + h_2$, where $h_1 \in \sum_{i=1}^{s} J_i$ and $h_2 \in J_{s+1}$, so that $gf = h_1 f + h_2 f \in I$ for all $h_1 \in \sum_{i=1}^{s} J_i$ and $h_2 \in J_{s+1}$. In particular for $h_2 = 0$, we have that $h_1 f \in I$ for all $h_1 \in \sum_{i=1}^{s} J_i$, so that $f \in I : (\sum_{i=1}^{s} J_i) = \bigcap_{i=1}^{s} (I : J_i)$. Analogously, we get that $f \in I : J_{s+1}$. Thus, we have that $f \in (\bigcap_{i=1}^{s} (I : J_i)) \cap (I : J_{s+1}) = \bigcap_{i=1}^{s+1} (I : J_i)$.
"$\supset$" If $f \in \bigcap_{i=1}^{s+1} (I : J_i) = (\bigcap_{i=1}^{s} (I : J_i)) \cap (I : J_{s+1})$, then $f \in \bigcap_{i=1}^{s} (I : J_i) = I : (\sum_{i=1}^{s} J_i)$ and $f \in I : J_{s+1}$ so that

$$\begin{aligned} &\text{for all } h_1 \in \sum_{i=1}^{s} J_i \quad h_1 f \in I \text{ and} \\ &\text{for all } h_2 \in J_{s+1} \quad h_2 f \in I. \end{aligned}$$

Since I is an ideal, we have that

$$\begin{aligned} &\text{for all } h_1 \in \sum_{i=1}^{s} J_i, h_2 \in J_{s+1} \quad (h_1 + h_2) f = h_1 f + h_2 f \in I \\ \implies \quad &\text{for all } g \in \sum_{i=1}^{s} J_i + J_{s+1} = \sum_{i=1}^{s+1} J_i \quad gf \in I. \end{aligned}$$

Finally, we can conclude that $f \in I : \left(\sum_{i=1}^{s+1} J_i\right)$. □

Example 17. Consider $I = \langle x - y^2, x^2 \rangle$ and $J = \langle xy, y^2 \rangle$ and consider the lexicographic ordering on $k[x, y]$ with $x > y > 1$. We want to compute the quotient ideal $I : J$. By Proposition 4.34, we get

$$I : J = (I : \langle xy \rangle) \cap (I : \langle y^2 \rangle).$$

Let us first compute $I : \langle xy \rangle$. We have already seen in Example 12 that

$$I \cap \langle xy \rangle = \langle xy^2, x^2y - xy^3 \rangle.$$

By Theorem 4.33, we have that

$$I : \langle xy \rangle = \langle \frac{xy^2}{xy}, \frac{x^2y - xy^3}{xy} \rangle = \langle y, x - y^2 \rangle.$$

Let us now compute $I : \langle y^2 \rangle$. Using SINGULAR, we get that $\{tx - y^2, t^2y^2 - y^2, y^4, xy^2\}$ is a Groebner basis of $tI + (1-t)\langle y^2 \rangle$. Therefore

$$I \cap \langle y^2 \rangle = \langle tx - y^2, t^2y^2 - y^2, y^4, xy^2 \rangle \cap k[x, y] = \langle y^4, xy^2 \rangle.$$

Again by Theorem 4.33

$$I : \langle y^2 \rangle = \langle \frac{y^4}{y^2}, \frac{xy^2}{y^2} \rangle = \langle y^2, x \rangle.$$

It remains to compute

$$(I : \langle xy \rangle) \cap (I : \langle y^2 \rangle) = \langle y, x - y^2 \rangle \cap \langle y^2, x \rangle.$$

Using SINGULAR, we get that $\{y^2, x, ty\}$ is a Groebner basis of $t\langle y, x - y^2 \rangle + (1-t)\langle y^2, x \rangle$. Since

$$\langle y, x - y^2 \rangle \cap \langle y^2, x \rangle = \langle y^2, x, ty \rangle \cap k[x, y] = \langle y^2, x \rangle,$$

we finally get

$$I : J = \langle y^2, x \rangle.$$

```
> ring r=0, (t,x,y),lp;
> ideal L;
> L=ty,tx-ty2,y2-ty2,x-tx;
> std(L);
_[1]=y2
_[2]=x
_[3]=ty
```

4.5.6 Saturation

Let $I, J \subset k[x_1, ..., x_n]$ be ideals and let us consider the quotient of I by powers of J

$$I = I : J^0 \subset I : J^1 \subset I : J^2 \subset I : J^3 \subset ... \subset k[x_1, ..., x_n].$$

Since $k[x_1, ..., x_n]$ is Noetherian, by Proposition 3.3, there exists an $s \in \mathbb{N}$ such that

$$I : J^s = I : J^{s+i} \text{ for all } i \geq 0.$$

Definition 4.35.

1) Let $I, J \subset k[x_1, ..., x_n]$ be ideals and let $s \in \mathbb{N}$ be such that

$$I : J^s = I : J^{s+i} \text{ for all } i \geq 0.$$

Such an s satisfies

$$I : J^\infty := \bigcup_{i \geq 0} I : J^i = I : J^s$$

*and $I : J^s$ is called the **saturation of I with respect to J**.*

*2) The minimal such s is called the **saturation exponent**.*

Given ideals $I, J \in k[x_1, ..., x_n]$, we know by Proposition 4.32 that $I : J^\infty$ is an ideal and so we want to compute generators and the saturation exponent. To do so, we need the following result.

Lemma 4.36. *Let I_1, I_2, I_3 be ideals in $k[x_1, ..., x_n]$. Then we have*

$$(I_1 : I_2) : I_3 = I_1 : (I_2 \cdot I_3).$$

Proof. This follows immediately from the definition. Indeed

$$\begin{aligned} & f \in (I_1 : I_2) : I_3 \\ \iff & gf \in I_1 : I_2 \text{ for all } g \in I_3 \\ \iff & hgf \in I_1 \text{ for all } h \in I_2, \text{ for all } g \in I_3 \\ \iff & kf \in I_1 \text{ for all } k \in I_2 \cdot I_3 \\ \iff & f \in I_1 : (I_2 \cdot I_3). \end{aligned}$$

□

In the general case, we will use the following algorithm:
Set $I^{(0)} = I$ and compute successively $I^{(j+1)} := I^{(j)} : J$, $j \geq 0$, by the method seen in Section 4.5.5. In this way we have

$$\begin{aligned} I^{(1)} &= I : J, \\ I^{(2)} &= (I : J) : J = I : J^2, \\ &... \\ I^{(j)} &= I : J^j, \end{aligned}$$

which is a consequence of Lemma 4.36. In each step check whether $I^{(j+1)} = I^{(j)}$, by using Section 4.5.1 or by computing their reduced Groebner basis with

respect to the same global monomial ordering and then using the uniqueness of the reduced Groebner basis of an ideal for a fixed global monomial ordering. If s is the first j when this happens, then $I^{(s)} = I : J^{\infty}$ and s is the saturation exponent.

Example 18. Consider the ideals $I = \langle x^2y, y^3z \rangle$ and $J = \langle xz, y^2 \rangle$ in $k[x, y, z]$. Using SINGULAR, we get

$$I^{(1)} = I : J = \langle y^3z, xyz, x^2y \rangle.$$

Since $F = \{x^2y, y^3z\}$ is a Groebner basis of I with respect to the lexicographic ordering on $k[x, y, z]$ with $x > y > z > 1$ and $LT(xyz)$ is not divisible neither by $LT(x^2y)$, nor $LT(y^3z)$, we have that $I^{(1)} \neq I = I^{(0)}$. Thus, the algorithm does not stop and

$$I^{(2)} = I : J^2 = \langle yz, x^2y \rangle.$$

Since $G = \{x^2y, xyz, y^3z\}$ is a Groebner basis of $I^{(1)}$ with respect to the lexicographic ordering on $k[x, y, z]$ with $x > y > z > 1$ and $LT(yz)$ is not divisible neither by $LT(x^2y)$, nor $LT(xyz)$, nor $LT(y^3z)$, we have that $I^{(2)} \neq I^{(1)}$. Thus, the algorithm does not stop and

$$I^{(3)} = I : J^3 = \langle yz, x^2y \rangle.$$

Since $I^{(3)} = I^{(2)}$, the algorithm stops and we have that

$$I : J^{\infty} = I^{(2)} = \langle yz, x^2y \rangle$$

and the saturation exponent equals 2.

```
> ring r=0, (x,y,z),lp;
> ideal I;
> I=x2y,y3z;
> std(I);
_[1]=y3z
_[2]=x2y
> ideal J;
> J=xz,y2;
>quotient(I,J);
_[1]=y3z
_[2]=xyz
_[3]=x2y
> I=quotient(I,J);
> std(I);
```

```
_[1]=y3z
_[2]=xyz
_[3]=x2y
> quotient(I,J);
_[1]=yz
_[2]=x2y
> I=quotient(I,J);
> quotient(I,J);
_[1]=yz
_[2]=x2y
```

If J is a principal ideal in $k[x_1, ..., x_n]$, then there is a second way to compute $I : J^\infty$.

Proposition 4.37. *Let I be an ideal of $k[x_1, ..., x_n]$ and let $f \in k[x_1, ..., x_n]$. Consider the ideal $L = \langle I, 1 - tf\rangle$ in $k[x_1, ..., x_n, t]$, where t is an additional new variable. Then*

$$I : \langle f\rangle^\infty = L \cap k[x_1, ..., x_n].$$

Proof. "$\subset$" If $g \in I : \langle f\rangle^\infty$, then $g \in k[x_1, ..., x_n]$ and there exists $d \in \mathbb{N}$ such that $gf^d \in I$. By definition of L, $1 = tf + l$, where $l \in L$. Thus, $1 = 1^d = (tf + l)^d = t^d f^d + l'$, where $l' \in L$. Hence, $g = (gf^d)t^d + gl' \in L$ and so $g \in L \cap k[x_1, ..., x_n]$.
"$\supset$" If $g \in L \cap k[x_1, ..., x_n]$, then $g = q_1 i + q_2(1 - tf)$ where $i \in I$ and $q_1, q_2 \in k[x_1, ..., x_n, t]$. In $k(x_1, ..., x_n, t)$, we can substitute t by $\frac{1}{f}$ to get

$$g = q_1 i + q_2(1 - \frac{1}{f}f) = q_1 i + q_2(1 - 1) = q_1 i.$$

Then we multiply the previous equation by f^d, where $d = \deg_t q_1$ to obtain

$$f^d g = (f^d q_1)i = qi \in I,$$

where $q \in k[x_1, ...x_n]$. Finally, $g \in I : \langle f\rangle^\infty$. □

Example 19. Consider the ideals $I = \langle x^2 z, yz^3\rangle$ and $J = \langle z\rangle$ in $k[x, y, z]$. Then we get

$$L = \langle x^2 z, yz^3, 1 - tz\rangle.$$

Using SINGULAR, we get that $F = \{y, x^2, 1 - tz\}$ is a Groebner basis of L with respect to the lexicographic ordering on $k[t, x, y, z]$ with $t > x > y > z > 1$. Finally, we get

$$I : J^\infty = \langle y, x^2, 1 - tz\rangle \cap k[x, y, z] = \langle y, x^2\rangle.$$

```
> ring r=0, (t,x,y,z),lp;
> ideal L;
> L=x2z,yz3,1-tz;
> std(L);
_[1]=y
_[2]=x2
_[3]=1-tz
```

4.5.7 Radical of an Ideal

Another operation on ideals is the radical of ideals.

Definition 4.38. *Let I be an ideal of $k[x_1, ..., x_n]$. The* ***radical of I*** *is the set*

$$\sqrt{I} = \{f : f^m \in I \text{ for some integer } m \geq 1\}.$$

Lemma 4.39. *If I is an ideal, then $\sqrt{I}$ is an ideal with $I \subset \sqrt{I}$.*

Proof. Suppose that $f_1, f_2 \in \sqrt{I}$. Then, by definition, there are two positive integers m_1, m_2 such that $f_1^{m_1}, f_2^{m_2} \in I$. If we expand the sum $(f_1 + f_2)^{m_1+m_2-1}$ with the binomial theorem, we see that every term is a multiple of some $f_1^{s_1} f_2^{s_2}$ with $s_1 + s_2 = m_1 + m_2 - 1$ Since either $s_1 \geq m_1$ or $s_2 \geq m_2$, either $f_1^{m_1} \in I$ or $f_2^{m_2} \in I$. Therefore, since all its terms are in I, $(f_1 + f_2)^{m_1+m_2-1} \in I$ and so $f_1 + f_2 \in \sqrt{I}$.
Suppose now that $f \in \sqrt{I}$ and consider a polynomial g of $k[x_1, ..., x_n]$. We have that $f^m \in I$ for some positive integer m, thus $g^m f^m = (gf)^m \in I$. Therefore, $gf \in \sqrt{I}$ and so $\sqrt{I}$ is an ideal.
If $f \in I$, then $f^m \in I$ for $m = 1$, and so by definition, $f \in \sqrt{I}$. We can conclude that $I \subset \sqrt{I}$. □

Now that we know that $\sqrt{I}$ is an ideal, we would like to know whether a given $f \in k[x_1, ..., x_n]$ is in $\sqrt{I}$. The following lemma, which is sometimes called Rabinowich's trick [21], provides a solution to this problem.

Proposition 4.40. *Let $I \subset k[x_1, ..., x_n]$ be an ideal and $f \in k[x_1, ..., x_n]$. Then*

$$f \in \sqrt{I} \iff 1 \in L := \langle I, 1 - tf \rangle \subset k[x_1, ..., x_n, t],$$

where t is an additional new variable.

Proof. " $\Longrightarrow$ " If $f \in \sqrt{I}$, then $f^m \in I$ for some positive integer m and so $t^m f^m \in L$. Thus,

$$1 = t^m f^m + (1 - t^m f^m) = t^m f^m + (1 - tf)(1 + tf + ... + t^{m-1} f^{m-1}) \in L.$$

"$\Longleftarrow$" Let $1 \in L$. By assumption, there are $f_1, ..., f_n \in I$ and $g_i(t) = \sum_{j=0}^{d_i} a_{ij} t^j \in k[x_1, ..., x_n][t]$, $i = 0, ..., k$ such that

$$1 = \sum_{i=1}^{k} g_i(t) f_i + g_0(t)(1 - tf).$$

Since f cannot be nilpotent as we work in an integral domain, we can replace t by $\frac{1}{f}$ in $k(x_1, ..., x_n, t)$ and then multiply the equation by f^m for m sufficiently large. Thus, we obtain

$$f^m = f^m \sum_{i=1}^{k} g_i(\frac{1}{f}) f_i = f^m \sum_{i=1}^{k} a_{ij} f^{-j} f_i = \sum_{i,j} a_{ij} f^{m-j} f_i \in I.$$

□

To solve the problem of radical membership, we consider the lexicographic ordering on $k[x_1, ..., x_n]$ with $t > x_1 > ... > x_n > 1$) and compute a Groebner Basis G of $L = \langle I, 1 - tf \rangle$. Then $f \in \sqrt{I}$ if and only if G contains a polynomial g with $LM(g) = 1$.

Example 20. Consider the ideal $I = \langle xy, x^2 - xy^2 \rangle$ and the polynomial $f = x^2y^2 + x$ in $k[x, y]$. Let us consider the ideal $L = \langle xy, x^2 - xy^2, 1 - tx^2y^2 - tx \rangle \subset k[x, y, t]$. Using SINGULAR, we obtain as a Groebner basis $G = \{1\}$ with respect to the lexicographic ordering on $k[x, y, t]$ with $t > x > y > 1$. We have clearly $LM(1) = 1$, so that $f \in \sqrt{I}$.

```
> ring r=0, (t,x,y),lp;
> ideal L;
> L=xy,x2-xy2,1-tx2y2-tx;
> std(L);
_[1]=1
```

Remark 9. It is even possible to compute the generators of $\sqrt{I}$, but this is a much harder computation as it involves primary decomposition. Indeed consider for example the lexicographic ordering on $k[x]$ with $x > 1$ and let $I = \langle f \rangle$, where $f = (x^2 + 1)x^2$. In these univariate case, the computation is rather easy and we have $\sqrt{I} = \langle (x^2 + 1)x \rangle$. In general, if $f = \prod_i f_i^{e_i}$, where f_i irreducible and $f_i \neq f_j$ for $i \neq j$, then $\sqrt{I} = \langle \prod_i f_i \rangle$ and $\prod_i f_i$ is called the square-free part of f. Things get even more complicated when the ideal I is generated by several multivariate polynomials. The consideration of this would go beyond the scope of this thesis. You can find the algorithm that provides generators of $\sqrt{I}$ in *A Singular Introduction to Commutative Algebra* [14, Section 4.5].

4.5.8 Colouring of a graph

Groebner bases can be used to solve the problem of graph colouring which has many practical applications such as air traffic control, flight scheduling or Sudoku puzzles. In this section, we will only consider 3-colouring of graphs. Let us first state the problem precisely. We are given a graph $\mathcal{G}$ with n vertices with at most one edge between any two vertices. We want to colour the vertices in such a way that only 3 colours are used and no two vertices connected by an edge have the same colour. If $\mathcal{G}$ can be coloured in this way, then $\mathcal{G}$ is called **3-colourable**. This problem can be applied to a map of a country: the vertices represent the regions to be coloured and two vertices are connected by an edge if the two corresponding regions are adjacent. But how do we transform this problem into an algebraic problem? First we need to assign a variable to each vertex. If we have n vertices, then we have the variables $x_1, ..., x_n$. Each vertex is to be assigned one of the 3 colours and we want to translate this in a set of equations. An approach to this problem is to map colours to primitive cube roots of unity. Let $\zeta = e^{\frac{2\pi i}{3}}$ be a root of unity so that $\zeta^3 = 1$. Then the 3 colours are represented by $1, \zeta$ and ζ^2 and as each vertex is to be assigned one of these colours, we get

$$x_i^3 - 1 = 0, 1 \leq i \leq n. \tag{4.6}$$

If the vertices x_i and x_j are connected by an edge, they need to have a different colour. Since $x_i^3 = x_j^3$, we have $(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$. Therefore x_i and x_j will have different colours, i.e. $x_i \neq x_j$, if and only if

$$x_i^2 + x_i x_j + x_j^2 = 0. \tag{4.7}$$

Indeed, if $x_i \neq x_j$, then $(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$ if and only if $x_i^2 + x_i x_j + x_j^2 = 0$. To get the other implication, let us suppose that $x_i = x_j$ and $x_i^2 + x_i x_j + x_j^2 = 0$. Then we get that $3x_i^2 = 0$ i.e. $x_i = 0$ which is a contradiction to $x_i \in \{1, \zeta, \zeta^2\}$.
Consider the ideal $I \subset \mathbb{C}[x_1, ..., x_n]$ generated by the polynomials in equation (4.6) and for each pair of vertices x_i, x_j which are connected by an edge by the polynomials in equation (4.7). We will consider now the zero-set $Z(I) \subset \mathbb{C}^n$ and then the following theorem is immediate.

Theorem 4.41. *The graph is 3-colourable if and only if $Z(I) \neq \emptyset$.*

To check that $Z(I) \neq \emptyset$, we will use the following statement.

Theorem 4.42 (**The Weak Nullstellensatz**). *Let k be an algebraically closed field and let $I \subset k[x_1, ..., x_n]$ be an ideal satisfying $Z(I) = \emptyset$. Then $1 \in I$.*

Proof. In the first step of the proof, we will show that every maximal ideal of $k[x_1, ..., x_n]$ has the form $\langle x_1 - a_1, ..., x_n - a_n \rangle$ for some $a_1, ..., a_n \in k$. If $\mathfrak{m}$ is a maximal ideal of $k[x_1, ..., x_n]$, then $k[x_1, ..., x_n]/\mathfrak{m}$ is a field which is finitely generated as a k-algebra. We can use the following result: if f is a field and F is a field extension which is finitely generated as a f-algebra, then F is algebraic over f (see for example [2]). Therefore $k[x_1, ..., x_n]/\mathfrak{m}$ is an algebraic extension of k, hence equal to k. Thus, each x_i maps to some $a_i \in k$ under the natural map $k[x_1, ..., x_n] \mapsto k[x_1, ..., x_n]/\mathfrak{m} = k$, so $\mathfrak{m}$ contains the ideal $\langle x_1 - a_1, ..., x_n - a_n \rangle$. This is a maximal ideal, so that

$$\mathfrak{m} = \langle x_1 - a_1, ..., x_n - a_n \rangle.$$

Now suppose that $I \subset k[x_1, ..., x_n]$ is an ideal such that $Z(I) = \emptyset$. If it lay in some maximal ideal, say $\langle x_1 - a_1, ..., x_n - a_n \rangle$, then $(a_1, ..., a_n) \in Z(I)$ which is a contradiction to $Z(I) = \emptyset$. Therefore I does not lie in any maximal ideal of $k[x_1, ..., x_n]$, so that we must have $I = k[x_1, ..., x_n]$ which is equivalent to $1 \in I$. □

It is therefore sufficient to compute the reduced Groebner basis G of the polynomials generating I and check whether $G \neq \{1\}$. If $G \neq \{1\}$, then by Theorem 4.42 $Z(I) \neq \emptyset$ and so we can conclude by Theorem 4.41 that the graph $\mathcal{G}$ is 3-colourable. In this case the Groebner basis G gives us explicit information about all possible 3-colourings of $\mathcal{G}$. Otherwise if $G = \{1\}$, it is clear that $Z(I) = \emptyset$ and thus the graph $\mathcal{G}$ is not 3-colourable.

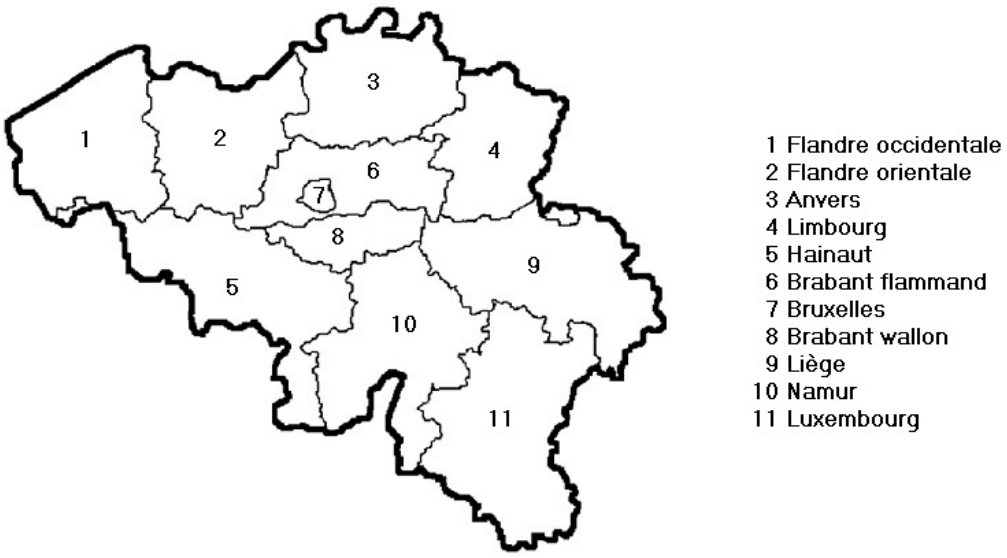
Example 21. Let us consider as example the provinces of Belgium. There are ten of them and we will consider the region Brussels (Bruxelles) as eleventh province even though it does not belong to any province. Is it possible to assign to each province one of three colours, say red, blue and green, so that no adjacent provinces have the same colour?
The polynomials corresponding to the graph $\mathcal{G}$ are

$$x_i^3 - 1 = 0, \text{ for } i = 1, ..., 11$$

and

$$x_i^2 + x_i x_j + x_j^2 = 0,$$

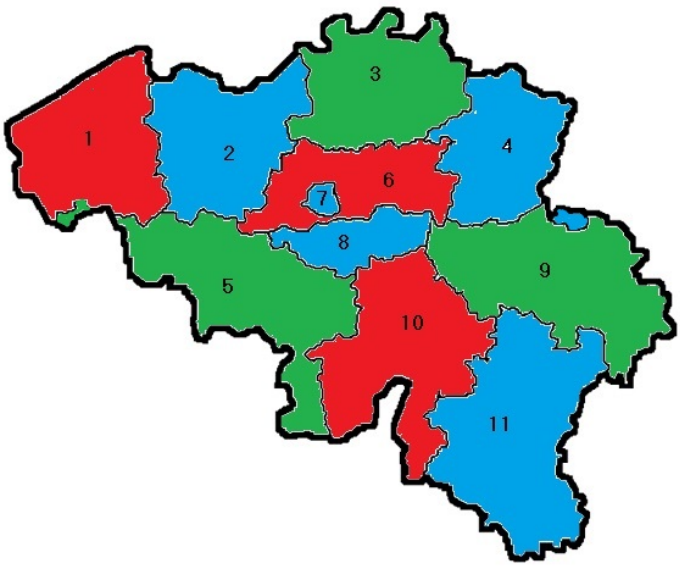
for the pairs $(i, j) \in \{(1,2), (1,5), (2,3), (2,5), (2,6), (3,4), (3,6), (4,6), (4,9), (5,6), (5,8), (5,10), (6,7), (6,8), (6,9), (8,9), (8,10), (9,10), (9,11), (10,11)\}$.
Let us denote by I the ideal corresponding to the above polynomials. Using



SINGULAR, we compute the reduced Groebner basis G with respect to the lexicographic ordering on $k[x_1, ..., x_{11}]$ with $x_1 > ... > x_{11} > 1$:

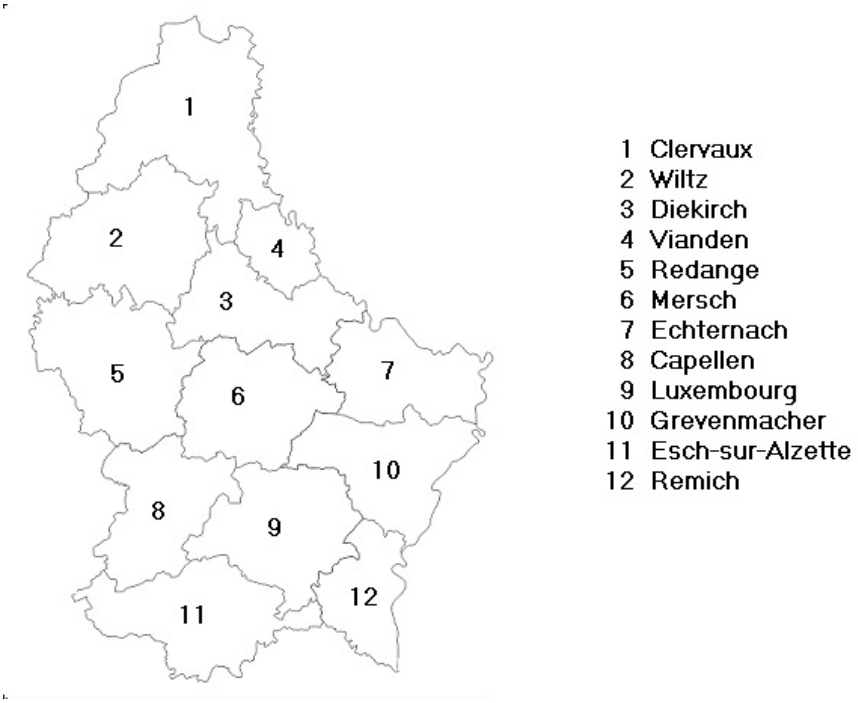
$$\begin{aligned} G = \{&x_{11}^3 - 1, x_{10}^2 + x_{10}x_{11} + x_{11}^2, x_9 + x_{10} + x_{11}, x_8 - x_{11}, \\ &x_7^2 + x_7x_{10} - x_{10}x_{11} - x_{11}^2, x_6 - x_{10}, x_5 + x_{10} + x_{11}, x_4 - x_{11}, \\ &x_3 + x_{10} + x_{11}, x_2 - x_{11}, x_1 - x_{10}\}. \end{aligned}$$

Since $G \neq \{1\}$, we have that $Z(I) \neq \emptyset$ and so by Theorem 4.41, the graph $\mathcal{G}$ is 3-colourable. We can use the Groebner basis G to colour the map. We must first choose a colour for x_{11}, say blue, since the only polynomial in one variable in G is $x_{11}^3 - 1$. Then we must choose a different colour for x_{10}, say red, because of the polynomial $x_{10}^2 + x_{10}x_{11} + x_{11}^2 \in G$. Since we have $\zeta^3 + \zeta^2 + \zeta = 0$ and $x_9 + x_{10} + x_{11} \in G$, x_9 must have a different colour than x_{10} and x_{11}, so that x_9 has to be green. Since G contains the polynomials $x_8 - x_{11}, x_4 - x_{11}$ and $x_2 - x_{11}$, provinces x_8, x_4 and x_2 must be blue such as x_{11}. Similar, since $x_6 - x_{10}$ and $x_1 - x_{10} \in G$, x_1 and x_6 must have the same colour as x_{10}: red. Then, since G contains $x_5 + x_{10} + x_{11}$ and $x_3 + x_{10} + x_{11}$, x_5 and x_3 must have a different colour than x_{10} and x_{11}, green. Since x_7 has only x_6 as neighbour, we can choose for x_7 two different colours, blue or green, so that the colouring of this map is not unique.




```
> ring r=0, (x(1..11)),lp;
> ideal I=x(1)3-1,x(2)3-1,x(3)3-1,x(4)3-1,x(5)3-1,x(6)3-1,
x(7)3-1,x(8)3-1,x(9)3-1,x(10)3-1,x(11)3-1,x(1)2+x(1)x(2)+x(2)2,
x(1)2+x(1)x(5)+x(5)2,x(2)2+x(2)x(3)+x(3)2,x(2)2+x(2)x(5)+x(5)2,
x(2)2+x(2)x(6)+x(6)2,x(3)2+x(3)x(4)+x(4)2,x(3)2+x(3)x(6)+x(6)2,
x(4)2+x(4)x(6)+x(6)2,x(4)2+x(4)x(9)+x(9)2,x(5)2+x(5)x(6)+x(6)2,
x(5)2+x(5)x(8)+x(8)2,x(5)2+x(5)x(10)+x(10)2,x(6)2+x(6)x(7)+x(7)2,
x(6)2+x(6)x(8)+x(8)2,x(6)2+x(6)x(9)+x(9)2,x(8)2+x(8)x(9)+x(9)2,
x(8)2+x(8)x(10)+x(10)2,x(9)2+x(9)x(10)+x(10)2,
x(9)2+x(9)x(11)+x(11)2,x(10)2+x(10)x(11)+x(11)2;
> option(redSB);
> std(I);
_[1]=x(11)3-1
_[2]=x(10)2+x(10)x(11)+x(11)2
_[3]=x(9)+x(10)+x(11)
_[4]=x(8)-x(11)
_[5]=x(7)2+x(7)x(10)-x(10)x(11)-x(11)2
_[6]=x(6)-x(10)
_[7]=x(5)+x(10)+x(11)
_[8]=x(4)-x(11)
_[9]=x(3)+x(10)+x(11)
_[10]=x(2)-x(11)
_[11]=x(1)-x(10)
```

Example 22. Let us now consider the cantons of the Grand Duchy of Luxembourg. There are twelve of them and as before we ask ourselves if it is possible to assign to each canton one of three colours, say red, blue and green, so that no adjacent cantons have the same colour.



The polynomials corresponding to the graph $\mathcal{G}$ are

$$x_i^3 - 1 = 0, \text{ for } i = 1, ..., 12$$

and

$$x_i^2 + x_i x_j + x_j^2 = 0,$$

for the pairs $(i, j) \in \{(1,2), (1,3), (1,4), (2,3), (2,5), (3,4), (3,5), (3,6), (3,7), (5,6), (5,8), (6,7), (6,8), (6,9), (6,10), (8,9), (8,111), (9,10), (9,11), (9,12), (10,12), (11,12)\}$. Let us denote by I the ideal corresponding to the above polynomials. Using SINGULAR, we compute the reduced Groebner basis G with respect to the lexicographic ordering on $k[x_1, ..., x_{12}]$ with $x_1 > ... > x_{12} > 1$ and we get $G = \{1\}$. Since $1 \in G$, we have that $Z(I) = \emptyset$ and so $\mathcal{G}$ is not 3-colourable. Indeed, let us try to colour the cantons of Luxembourg by hand. We start by colouring Clervaux(1) red. Since Wiltz(2) is a neighbour of Clervaux, it has to be coloured in a different way, say blue. After

these choices, there is only one colour possible for each canton. At the end, Remich(12) represents a problem, since we cannot colour it neither red, nor blue, nor green. This is easily seen by looking at Figure 4.5.8.

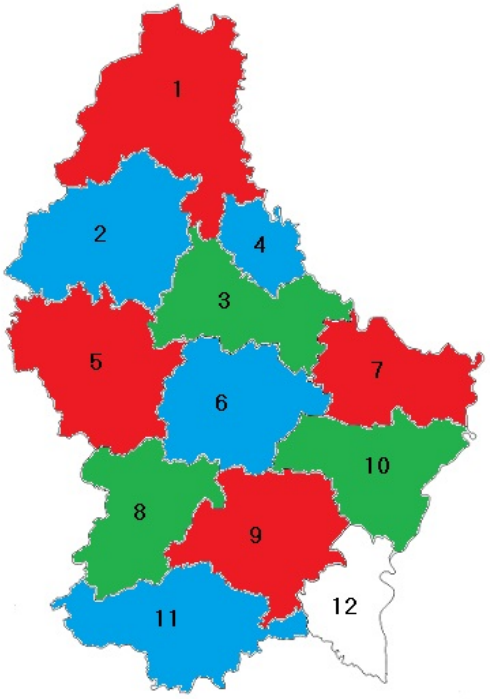


Figure 4.5.8

```
> ring r=0, (x(1..12)),lp;
> ideal I=x(1)3-1,x(2)3-1,x(3)3-1,x(4)3-1,x(5)3-1,x(6)3-1,
x(7)3-1,x(8)3-1,x(9)3-1,x(10)3-1,x(11)3-1,x(12)3-1,
x(1)2+x(1)x(2)+x(2)2,x(1)2+x(1)x(3)+x(3)2,x(1)2+x(1)x(4)+x(4)2,
x(2)2+x(2)x(3)+x(3)2,x(2)2+x(2)x(5)+x(5)2,x(3)2+x(3)x(4)+x(4),
2x(3)2+x(3)x(5)+x(5)2,x(3)2+x(3)x(6)+x(6)2,x(3)2+x(3)x(7)+x(7)2,
x(5)2+x(5)x(6)+x(6)2,x(5)2+x(5)x(8)+x(8)2,x(6)2+x(6)x(7)+x(7)2,
x(6)2+x(6)x(8)+x(8)2,x(6)2+x(6)x(9)+x(9)2,x(6)2+x(6)x(10)+x(10)2,
x(8)2+x(8)x(9)+x(9)2,x(8)2+x(8)x(11)+x(11)2,x(9)2+x(9)x(10)+x(10)2,
x(9)2+x(9)x(11)+x(11)2,x(9)2+x(9)x(12)+x(12)2,
x(10)2+x(10)x(12)+x(12)2,x(11)2+x(11)x(12)+x(12)2;
> option(redSB);
> std(I);
_[1]=1
```

5 Resultants

In this section, we introduce a classical approach to the elimination problem which makes use of resultants. Before turning to the general concept of multivariate resultants, we consider the resultant of two univariate polynomials. In the following, we only consider algebraically closed fields k. This is necessary since we consider common zeroes of polynomials in $k[x_1, ..., x_n]$ and we want to be sure that these common zeroes are contained in the field k.

5.1 Univariate Resultants

Consider

$$f = \sum_{i=0}^{m} f_i x^i \text{ , where } f_i \in k \text{ and } m = \deg f > 0,$$
$$g = \sum_{j=0}^{n} g_j x^j \text{ , where } g_j \in k \text{ and } n = \deg g > 0,$$

two non-constant polynomials in $k[x]$. We would like to give an answer to the following question: When do f and g have common zeroes, i.e when do we have $a \in k$ such that $f(a) = g(a) = 0$? We know that when f and g have at least one common root, then

$$\deg(\gcd(f, g)) > 0.$$

Since by Proposition 4.30

$$\gcd(f, g) \cdot \operatorname{lcm}(f, g) = fg,$$

we can conclude that

$$\deg(\operatorname{lcm}(f, g)) < m + n$$

thus $\operatorname{lcm}(f, g) = fp = -gq$ for some polynomials $p, q \in k[x]$ with $\deg(p) < n$ and $\deg(q) < m$ and so

$$fp + gq = 0. \tag{5.1}$$

Next we will turn $fp + gq = 0$ into a system of linear equations. Let us write therefore:

$$p = p_0 + p_1 x + ... + p_{n-1} x^{n-1},$$
$$q = q_0 + q_1 x + ... + q_{m-1} x^{m-1},$$

where we will regard the $n+m$ coefficients $p_0, ..., p_{n-1}, q_0, ..., q_{m-1}$ as unknowns in k. If we replace f, g, p and q by their expanded expression into equation (5.1), we get the following system of linear equations:

$$\begin{array}{llll} f_m p_{n-1} & + g_n q_{m-1} & = 0 & \text{coefficients of } x^{m+n-1} \\ f_{m-1} p_{n-1} + f_m p_{n-2} & + g_{n-1} q_{m-1} + g_n q_{m-2} & = 0 & \text{coefficients of } x^{m+n-2} \\ \ddots & \ddots & \vdots & \\ f_0 p_0 & + \quad g_0 q_0 & = 0 & \text{coefficients of } x^0. \end{array} \tag{5.2}$$

Notice that there are $m+n$ linear equations and $m+n$ unknowns. Therefore, we can conclude from linear algebra that there is a non-zero solution if and only if the determinant of the coefficient matrix is zero. This coefficient matrix has a special name and so has its determinant:

Definition 5.1. *Let $f, g \in k[x]$ be two polynomials with*

$$f = \sum_{i=0}^{m} f_i x^i \text{ ,where } f_i \in k \text{ and } m = \deg f > 0,$$

$$g = \sum_{j=0}^{n} g_j x^j \text{ ,where } g_j \in k \text{ and } n = \deg g > 0.$$

The ***Sylvester matrix*** *associated to f and g is then a $(n+m) \times (n+m)$ matrix given by*

$$S(f,g) = \underbrace{\begin{pmatrix} f_m & & & & g_n & & & \\ f_{m-1} & f_m & & & g_{n-1} & g_n & & \\ f_{m-2} & f_{m-1} & f_m & & g_{n-2} & g_{n-1} & g_n & \\ \vdots & & & \ddots & \vdots & & & \ddots \\ & \vdots & & f_m & & \vdots & & g_n \\ f_0 & & \vdots & & g_0 & & \vdots & \\ & f_0 & & & & g_0 & & \\ & & f_0 & \vdots & & & g_0 & \vdots \\ & & & \ddots & & & & \ddots \\ & & & f_0 & & & & g_0 \end{pmatrix}}_{n \text{ columns} \quad\quad m \text{ columns}},$$

where the empty spaces are filled by zeroes. The determinant of the Sylvester matrix of f and g is called the ***resultant*** *of f and g and is denoted by $R(f,g)$:*

$$R(f,g) = \det(S(f,g)) \in k.$$

Remark 10. In literature, the Sylvester matrix of two non-constant polynomials f and g is sometimes defined to be $(S(f,g))^T$, where $S(f,g)$ is the Sylvester matrix of f and g as defined in Definition 5.1. Since the determinant of a square matrix is the same as that of its transpose, this does not change the definition of the resultant of f and g.

Proposition 5.2. *Let $f, g \in k[x]$ be non-constant polynomials. Then f and g have common roots if and only if $R(f,g) = 0$.*

Proof. This is true by construction of $R(f,g)$. Indeed $R(f,g) = 0$ if and only if the coefficient matrix of equations (5.2) has zero determinant if and only if equations (5.2) have a non-zero solution if and only if $\deg(\text{lcm}(f,g)) < m+n$ if and only if $\deg(\gcd(f,g)) > 0$ if and only if f and g have a common factor of degree non-zero if and only if f and g have at least a common root. □

Example 23. Let us check whether $f = x^3+2x-1$ and $g = 3x^2+x+2$ have a common root in $\mathbb{C}[x]$. Since $\deg(f) = 3$ and $\deg(g) = 2$, the Sylvester matrix of f and g is a 5×5 matrix and their resultant, computed with SINGULAR, is equal to

$$R(f,g) = \det \begin{pmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 1 & 3 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ -1 & 2 & 0 & 2 & 1 \\ 0 & -1 & 0 & 0 & 2 \end{pmatrix} = 64 \neq 0.$$

Therefore, we can conclude that f and g have no common root.

We will need the following lemma to proof some properties of a resultant.

Lemma 5.3 (Study's Lemma). *Let k be an algebraically closed field, $f, g \in k[x_1, ..., x_n]$ with f being irreducible. If*

$$Z(f) \subset Z(g),$$

then f divides g.

Proof. The idea of the proof is based on projection, i.e. consider the resultant of f and g with respect to, say x_n. This means that we consider the polynomials f, g as polynomials of $k[x_1, ..., x_{n-1}][x_n]$ and we compute the univariate resultant $R(x_1, ..., x_{n-1}) = R(f, g, x_n)$ of f and g with respect to x_n. Let us assume, by contradiction, that f does not divide g. Since f is irreducible, it follows that $R(f, g, x_n) \neq 0$. Indeed, we have that

$$\begin{aligned} & R(f,g,x_n) = 0 \text{ in } k[x_1, ..., x_{n-1}] \\ \iff & f \text{ and } g \text{ have a common root in the algebraic closure of } k(x_1, ..., x_{n-1}) \\ \iff & f \text{ and } g \text{ have common factors over } k(x_1, ..., x_{n-1})[x_n]. \end{aligned}$$

The last statement is however impossible, since f does not divide g and f is irreducible and so $R(f,g,x_n) \neq 0$. In this case, we can find a point $a = (a_1, ..., a_{n-1}) \in k^{n-1}$ such that $R(a) \neq 0$. The space A of such points is dense in k^{n-1}. Let us write

$$f = \sum_{i=0}^{d_n} b_i x_n^i \text{ with } \deg f = d_n > 0$$
$$\text{and } g = \sum_{j=0}^{d'_n} c_j x_n^j \text{ with } \deg g = d'_n > 0,$$

where $b_i, c_j \in k[x_1, ..., x_{n-1}]$ for $i \in \{0, ..., d_n\}$, $j \in \{0, ..., d'_n\}$. Let B be the set of points a' such that $b_{d_n}(a') \neq 0$ and C be the set of points a'' such that $c_{d'_n}(a'') \neq 0$. Since B and C are dense in k^{n-1}, we have that $A \cap B \cap C \neq \emptyset$ and so there is $d \in A \cap B \cap C$. This means that $f(d, x_n) \not\equiv 0$ and $g(d, x_n) \not\equiv 0$ have no common factor, which is impossible: by algebraic closedness of k, $f(d, x_n)$ has some zero and since we have by assumption $Z(f) \subset Z(g)$, this is also a zero of $g(d, x_n)$ and so f and g have a common factor. It follows that $f|g$. □

Let us now consider some properties of a resultant.

Proposition 5.4. *Let $f, g \in k[x]$ be two polynomials with*

$$f = \sum_{i=0}^{m} f_i x^i, \text{ where } f_i \in k \text{ and } m = \deg f > 0,$$
$$g = \sum_{j=0}^{n} g_j x^j, \text{ where } g_j \in k \text{ and } n = \deg g > 0.$$

Then

1) $R(f, f) = 0$.

2) $R(f, g) = (-1)^{mn} R(g, f)$.

3) $R(f, g)$ *is an integer polynomial in the coefficients of f and g.*

4) $R(f, g) = f_m^n g_n^m \prod_{i,j} (\alpha_i - \beta_j)$,
where α_i are the roots of f and β_j those of g.

5) $R(f_1 \cdot f_2, g) = R(f_1, g) \cdot R(f_2, g)$ *and* $R(f, g_1 \cdot g_2) = R(f, g_1) \cdot R(f, g_2)$.
for $f_i, g_i \in k[x]$ with $\deg f_i > 0$ and $\deg g_i > 0$, $i \in \{1, 2\}$.

6) $R(f,g)$ is irreducible as a polynomial in the coefficients of f and g.

Proof. 1) and 2) are direct consequences of the properties of the determinant of a matrix.
3) The standard formula for the determinant of a $n\times n$ matrix $M=(m_{ij})_{1\leq i,j\leq n}$ is

$$\det(M)=\sum_{\sigma \text{ a permuation of } \{1,...,n\}} \operatorname{sgn}(\sigma) m_{1\sigma(1)}\cdot m_{2\sigma(2)}...m_{n\sigma(n)},$$

where $\operatorname{sgn}(\sigma)$ is the signature of the permutation σ, i.e. $\operatorname{sgn}(\sigma)=1$ if σ interchanges an even number of pairs of elements of $\{1,...,n\}$ and $\operatorname{sgn}(\sigma)=-1$ otherwise. Thus, the determinant is an integer polynomial in its entries and so 3) follows from the definition of a resultant.
4) Let us denote $R'=f_m^n g_n^m \prod_{i,j}(\alpha_i-\beta_j)$, where α_i are the roots of f and β_j those of g and let $R=R(f,g)$. By Proposition 5.2, we know that R vanishes if and only if R' vanishes. Consider R and R' as polynomials in $f_m,\alpha_1,...,\alpha_m,g_n,\beta_1,...,\beta_n$ and note that $\alpha_i-\beta_j$ is irreducible. If $\alpha_i-\beta_j$ vanishes, then R' vanishes and so R vanishes. Thus, the zero-set of $\alpha_i-\beta_j$ is contained in the zero-set of R. By Study's Lemma, this implies that $\alpha_i-\beta_j$ divides R. In addition, by the definition of R, we have that $f_m^n g_n^m$ divides R, thus we can conclude that R' divides R, since each factor of R' divides R. Consider now R and R' as polynomials in $f_0,...,f_m,g_0,...,g_n$ and notice that $\deg R=\deg R'=m+n$. So there is some $\lambda\in k\backslash\{0\}$ such that $R'=\lambda\cdot R$. Next, we evaluate R and R' at $\alpha_i=1$ and $\beta_j=0$ for each $i\in\{1,...,m\}, j\in\{1,...,n\}$. Since $\alpha_i-\beta_j=1$ for all i,j, we get that $R'=f_m^n g_n^m$. Since α_i are the roots of f, we can write $f=f_m\prod_{i=0}^m(x-\alpha_i)$. Similarly, since β_j are the roots of g, we have $g=g_n\prod_{j=0}^n(x-\beta_j)$. By replacing $\alpha_i=1$ in f and $\beta_j=0$ in g, we get that $f=f_m(x-1)^m=f_m(x^m-mx^{n-1}+...+(-1)^m)$ and $g=g_nx^n$. Let us look at the Sylvester matrix of this f and g. It is equal to

$$S(f,g)=\underbrace{\begin{pmatrix} f_m & & & & g_n & & \\ f_m(-m) & f_m & & & 0 & g_n & \\ \vdots & f_m(-m) & \ddots & & \vdots & 0 & \ddots \\ & \vdots & & f_m & & \vdots & \\ f_m(-1)^m & & & f_m(-m) & 0 & & g_n \\ & f_m(-1)^m & & & & 0 & 0 \\ & & & \vdots & & & \vdots \\ & & \ddots & & & & \ddots \\ & & & f_m(-1)^m & & & 0 \end{pmatrix}}_{\text{n columns}\qquad\qquad\text{m columns}},$$

To compute the determinant of S, let us move its last m columns to the left, to get

$$S'(f,g) = \underbrace{\begin{pmatrix} g_n & & & & f_m & & & & \\ 0 & g_n & & & f_m(-m) & f_m & & & \\ \vdots & 0 & \ddots & & \vdots & f_m(-m) & \ddots & & \\ & \vdots & & g_n & & \vdots & & & f_m \\ & & & 0 & f_m(-1)^m & & & & f_m(-m) \\ 0 & & & \vdots & & f_m(-1)^m & & & \\ & 0 & & & & & & & \vdots \\ & & \ddots & & & & & \ddots & \\ & & & 0 & & & & & f_m(-1)^m \end{pmatrix}}_{\text{m columns}} \underbrace{\qquad\qquad}_{\text{n columns}},$$

It is obvious that $\det(S'(f,g)) = g_n^m f_m^n (-1)^{nm}$ and since we moved m columns n times to the left to get $S'(f,g)$, we have, by a property of the determinant, that $\det(S'(f,g)) = (-1)^{nm}\det(S(f,g))$ so that

$$R = \det(S(f,g)) = f_m^n g_n^m.$$

Since R and R' coincide for $\alpha_i = 1$ and $\beta_j = 0$ for each $i \in \{1,...,m\}, j \in \{1,...,n\}$, we can conclude that $\lambda = 1$ and so $R = R'$.
5) Let us denote $f = f_1 \cdot f_2$, $\deg f_1 = m_1$, $LC(f_1) = f_{1m_1}$, $\deg f_2 = m_2$, $LC(f_2) = f_{2m_2}$ and $m = m_1 + m_2$. Let $\gamma_1, ..., \gamma_{m_1}$ be the roots of f_1, $\delta_1, ..., \delta_{m_2}$ the roots of f_2 and $\alpha_1, ..., \alpha_m$ be the roots of f, i.e.

$$\{\alpha_1, ..., \alpha_m\} = \{\gamma_1, ..., \gamma_{m_1}, \delta_1, ..., \delta_{m_2}\}.$$

Then by writing $f = f_m \prod_{i=1}^m (x - \alpha_i)$ and $g = g_n \prod_{j=1}^n (x - \beta_j)$, we can use property 4) to get

$$\begin{aligned} R(f_1 \cdot f_2, g) = R(f,g) &= f_m^n g_n^m \prod_{i,j} (\alpha_i - \beta_j) \\ &= f_{1m_1}^n f_{2m_2}^n g_n^m \prod_{i,j} (\gamma_i - \beta_j) \prod_{i,j} (\delta_i - \beta_j) \\ &= \Big(f_{1m_1}^n g_n^{m_1} \prod_{i,j} (\gamma_i - \beta_j) \Big) \Big(f_{2m_2}^n g_n^{m_2} \prod_{i,j} (\delta_i - \beta_j) \Big) \\ &= R(f_1, g) \cdot R(f_2, g). \end{aligned}$$

The multiplicativity in the second argument follows from 2).
6) We have to show that $R(f,g)$ cannot be resolved into two factors each of which is polynomial in the coefficients of f and g. First, we need to realize that $R(f,g)$ has a term $f_m^n g_0^m$ obtained from the diagonal of the determinant and that this is the only term of $R(f,g)$ containing f_m^n so that if we expand $R(f,g)$ in powers of f_m, we have

$$R(f,g) = f_m^n g_0^m + a f_m^{n-1} + ...$$

where a is not divisible by g_0. Indeed, by looking at the Sylvester matrix, we get a term $f_0 g_1^m f_m^{n-1}$, where $f_0 g_1^m$ is clearly not divisible by g_0. This is the only term in f_m^{n-1} that is not divisible by g_0, since all the other terms in f_m^{n-1} contain a positive power of g_0. Therefore, if $R(f,g)$ can be written as a product of two factors, we have

$$R(f,g) = (f_m^{p_1} g_0^{q_1} + \lambda_1 f_m^{p_1 - 1} + ...)(f_m^{p_2} g_0^{q_2} + \lambda_2 f_m^{p_2 - 1} + ...),$$

where λ_1, λ_2 are polynomials in the coefficients of f and g, $p_1 + p_2 = n$ and $q_1 + q_2 = m$. In addition, we have that either q_1 or q_2 is zero since otherwise the coefficient a of f_m^{n-1} is $g_0^{q_1}\lambda_2 + g_0^{q_2}\lambda_1$, i.e. is divisible by g_0 which is not the case. Thus, one of the factors of $R(f,g)$ is independent of the coefficients of g as both factors must be homogeneous in the coefficients of g. Similarly, one of the factors must be independent of the coefficients of f, i.e

$$R(f,g) = (f_m^n + ...)(g_0^n + ...).$$

Since the coefficient of f_m^n in $R(f,g)$ is g_0^m and the coefficient of g_0^m in $R(f,g)$ is f_m^n, we have that

$$R(f,g) = (f_m^n + ...)(g_0^n + ...) = f_m^n g_0^m.$$

Since this is not true, we cannot write $R(f,g)$ as a product of two factors and so $R(f,g)$ is irreducible. □

Proposition 5.5. *Let $f = f_m x^m + ... + f_0$ and $g = g_n x^n + ... + g_0$ be two non-constant polynomials of $k[x]$ with f_m and g_n non-zero. Then there are polynomials $A, B \in k[x]$ such that*

$$Af + Bg = R(f,g).$$

In addition, we have that $A, B \in \mathbb{Z}[f_0, ..., f_m, g_0, ..., g_n][x]$.

Proof. The proposition is trivially true if $R(f,g) = 0$, by simply choosing $A = B = 0$. Thus, we may assume that $R(f,g) \neq 0$. We will first prove that there are $\tilde{A}, \tilde{B} \in k[x]$ such that

$$\tilde{A}f + \tilde{B}g = 1. \tag{5.3}$$

Let us write

$$\tilde{A} = a_0 + a_1 x + ... + a_{n-1}x^{n-1},$$
$$\tilde{B} = b_0 + b_1 x + ... + b_{m-1}x^{m-1},$$

where we will regard the $n + m$ coefficients $a_0, ..., a_{n-1}, b_0, ..., b_{m-1}$ as unknowns in k. If we replace $f, g, \tilde{A}$ and $\tilde{B}$ by their expanded expression into equation (5.3), we get the following system of linear equations:

$$\begin{array}{llll}
f_m a_{n-1} & + g_n b_{m-1} & = 0 & \text{coefficients of } x^{m+n-1} \\
f_{m-1}a_{n-1} + f_m a_{n-2} & + g_{n-1}b_{m-1} + g_n b_{m-2} & = 0 & \text{coefficients of } x^{m+n-2} \\
\ddots & \ddots & \vdots & \\
f_0 a_0 & + g_0 b_0 & = 1 & \text{coefficients of } x^0.
\end{array} \tag{5.4}$$

These equations are the same as (5.2), except for the 1 in the last equation. Therefore, the coefficient matrix is the Sylvester matrix of f and g and so $R(f,g) \neq 0$ guarantees that (5.4) has a unique solution in k. In this situation, we can use Cramer's rule to get the unique solution of (5.4). In this solution, the i-th unknown is given by a fraction, where the denominator is the determinant of the coefficient matrix and the numerator is the determinant of the matrix where the i-th column of the coefficient matrix has been replaced by the right-hand side of the equation (5.4). In our case, the first unknown a_0 is given by

$$a_0 = \frac{1}{R(f,g)} \det \begin{pmatrix}
0 & & & & g_n & & & & \\
0 & f_m & & & g_{n-1} & g_n & & & \\
0 & f_{m-1} & f_m & & g_{n-2} & g_{n-1} & g_n & & \\
\vdots & & \ddots & & \vdots & & & \ddots & \\
 & \vdots & & f_m & & \vdots & & & g_n \\
 & & \vdots & & g_0 & & \vdots & & \\
 & f_0 & & & & g_0 & & & \\
 & & f_0 & \vdots & & & g_0 & & \vdots \\
 & & & \ddots & & & & \ddots & \\
1 & & & f_0 & & & & & g_0
\end{pmatrix}$$

We have already shown in the proof of Proposition 5.4, 3), that a determinant is an integer polynomial in its entries. Therefore we have

$$a_0 = \frac{\text{an integer polynomial in} f_i, g_j}{R(f,g)}.$$

In the same way we get similar formulas for the $a_i's$ and the $b_j's$. Since $\tilde{A} = a_0 + a_1x + ...a_{n-1}x^{n-1}$, we can take out the common denominator $R(f,g)$ to get

$$\tilde{A} = \frac{1}{R(f,g)}A,$$

with $A \in k[x]$ and the coefficients of A are integer polynomials in f_i and g_j. Proceeding in the same way, we obtain

$$\tilde{B} = \frac{1}{R(f,g)}B,$$

with $B \in k[x]$ and the coefficients of B are integer polynomials in f_i and g_j. Since $\tilde{A}$ and $\tilde{B}$ are such that $\tilde{A}f + \tilde{B}g = 1$, we can multiply this equality by $R(f,g)$ to get

$$Af + Bg = R(f,g),$$

where $A, B \in \mathbb{Z}[f_0, ..., f_m, g_0, ..., g_n][x]$. □

If we consider a polynomial $f \in k[x]$ with $\deg(f) \geq 1$ and its derivative $f' \in k[x]$, then their resultant $R(f,f')$ has a special name and property.

Definition 5.6. *Let $f \in k[x]$ be a non-constant polynomial and consider its derivative $f' \in k[x]$. Then the **discriminant** of f is*

$$\Delta(f) = R(f,f').$$

Lemma 5.7. *Let $f \in k[x]$ be a non-constant polynomial and consider its derivative $f' \in k[x]$. Then $\Delta(f) = 0$ if and only if f has a root of multiplicity greater than 1.*

Proof. This is a direct consequence of Proposition 5.2. □

Example 24. Let us consider $f = ax^2 + bx + c$, where $a, b, c \in \mathbb{R}$ and $a \neq 0$. Then its derivative is given by $f' = 2ax + b$ and we have

$$\Delta(f) = R(f,f') = \det \begin{pmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{pmatrix} = ab^2 + 4a^2c - 2ab^2 = -a(b^2 - 4ac).$$

The expression $\delta = b^2 - 4ac$ is the definition of the discriminant of a quadratic polynomial in $\mathbb{R}[x]$ given at secondary school. The polynomial f has a double root in $\mathbb{R}$ if and only if $\Delta(f) = 0$ if and only if $\delta = 0$, because $a \neq 0$.

There are other ways to compute the resultant of two univariate polynomials f and g, for example the **Bézout-Cayley's method**. Indeed, if f and g have the same degree $n > 0$, then we can consider the following matrix.

Definition 5.8. *Let $f, g \in k[x]$ be polynomials of degree $n > 0$. The **Bézout matrix** of order n associated to f and g is the matrix*

$$B(f,g) = (b_{ij})_{i,j=1,\dots,n},$$

where the coefficients result from the bivariate polynomial

$$\frac{f(x)g(y) - f(y)g(x)}{x-y} = \sum_{i,j=1}^{n} b_{ij} x^{i-1} y^{j-1}. \tag{5.5}$$

The expression given by the left-hand side of equation (5.5) is indeed a polynomial. This can be checked by Study's Lemma: the denominator $\tilde{f} = x - y$ is an irreducible polynomial in $k[x,y]$. We have that $\tilde{f}$ vanishes if and only if $x = y$. But in this case, the numerator $\tilde{g} = f(x)g(y) - f(y)g(x) \in k[x,y]$ also vanishes, so that $Z(\tilde{f}) \subset Z(\tilde{g})$. Therefore, by Study's Lemma, $\tilde{f}$ divides $\tilde{g}$ and we can conclude that the left-hand side of (5.5) is a polynomial. We can also check that this polynomial is of degree at most $2n-2$. Since f and g are of degree n, we can conclude that $f(x)g(y) - f(y)g(x)$ is of degree at most $2n$. In addition we have that $f_n x^n g_n y^n - f_n y^n g_n x^n = 0$, so we can conclude, that the numerator has degree at most $2n-1$. Since we divide by a denominator of degree 1, we can conclude that the polynomial we are considering has at most degree $2n-2$.
The Bézout matrix has the following relation with the resultant.

Proposition 5.9. *With the above notations,*

$$R(f,g) = \lambda \det(B(f,g)), \quad \lambda \in k \backslash \{0\}.$$

Proof. The argument is very similar to the one presented in the proof of Proposition 5.4, 4). Let us denote $R' = \det(B(f,g))$. This is a homogeneous polynomial in the coefficients of f and g and of degree $2n$ as the resultant $R(f,g)$. Indeed, by construction of the matrix $(b_{ij})_{i,j=1,\dots,n}$, each entry is a homogeneous polynomial in the coefficients of f and g and of degree 2. Since the matrix is in addition of order n, its determinant is a homogeneous polynomial in the coefficients of f and g and of degree $2n$. If $R(f,g) = 0$, then we also have $R' = 0$. Indeed, if $R(f,g) = 0$, then there exists $\alpha \in k$ such that $f(\alpha) = g(\alpha) = 0$ and so

$$\frac{f(\alpha)g(y) - f(y)g(\alpha)}{\alpha - y} = 0 = \sum_{i,j=1}^{n} b_{ij} \alpha^{i-1} y^{j-1} = \sum_{j=1}^{n} \Big(\sum_{i=1}^{n} b_{ij} \alpha^{i-1} \Big) y^{j-1}.$$

It follows that

$$\begin{aligned} & \frac{f(\alpha)g(y) - f(y)g(\alpha)}{\alpha - y} = 0 \\ \iff & \sum_{i=1}^{n} b_{ij}\alpha^{i-1} = 0 \\ \iff & B \cdot \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix} = 0 \\ \iff & R' = \det(B(f,g)) = 0. \end{aligned}$$

So the zero-set of $R(f,g)$ is contained in the zero-set of R' and since the resultant $R(f,g)$ is irreducible by Proposition 5.4, 6), we have by Study's Lemma that $R(f,g)$ divides R'. Since we have shown before that $R(f,g)$ and R have the same degree, there is $\lambda \in k\backslash\{0\}$ such that $R(f,g) = \lambda R'$. □

Note that if $f, g \in k[x]$ have degree $n > 0$, then the Bézout matrix has order n, but the Sylvester matrix has order $n + n = 2n$, so that we can conclude that the Bézout matrix is more compact. However, the entries of the Bézout matrix are much more complicated expressions than the ones of the Sylvester matrix.

Example 25. Let us consider $f = x^2 + 1$ and $g = 2x^2 + 3x$ in $\mathbb{C}[x]$. Since $\deg f = \deg g = 2$, we can compute the Bézout matrix of f and g.

$$\begin{aligned} \frac{f(x)g(y) - f(y)g(x)}{x - y} &= \frac{(x^2+1)(2y^2+3y) - (y^2+1)(2x^2+3x)}{x-y} \\ &= \frac{2x^2y^2 + 3x^2 + 2y^2 + 3y - (2x^2y^2 + 3xy^2 + 2x^2 + 3x)}{x-y} \\ &= \frac{3xy(x-y) + 2(x+y)(y-x) + 3(y-x)}{x-y} \\ &= 3xy - 2(x+y) - 3 \end{aligned}$$

Therefore, we get by Proposition 5.9

$$R(f,g) = \lambda \det \begin{pmatrix} -3 & -2 \\ -2 & 3 \end{pmatrix} = -13\lambda \neq 0$$

and so we can conclude that f and g have no common root. Indeed, we can check that $R(f,g) = 13$ and so in this case $\lambda = -1$.

5.2 Applications of Univariate Resultants

5.2.1 Elimination

Resultants can be used for elimination. Indeed, consider $f = x^2y + 2$ and $g = x + y$ in $\mathbb{C}[x, y]$ and regard them as polynomials in x with coefficients that are polynomials in y. Computing the resultants of f and g, which we denote by $R_x(f, g)$ to show that we regard f and g as polynomials in x, we get

$$R(y) = R_x(f, g) = \det \begin{pmatrix} y & 1 & 0 \\ 0 & y & 1 \\ 2 & 0 & y \end{pmatrix} = y^3 + 2.$$

Let $b \in k$. Then $f(x, b)$ and $g(x, b)$ have a common root if and only if $R(b) = 0$. In that case, there is $a \in k$ such that $f(a, b) = 0 = g(a, b)$.
More generally, if f and g are any polynomials in $k[x, y]$ in which x appears to a positive power, then we can compute $R(y) = R_x(f, g)$ by considering f and g as polynomials in $k[y][x]$. In this way, the coefficients of f and g are in y and Proposition 5.4, 3) guarantees us that $R(y) \in k[y]$. In addition by Proposition 5.5, we know that $R(y) \in I = \langle f, g\rangle$. Thus if we consider the lexicographic ordering on $k[x, y]$ with $x > y > 1$ and $f, g \in k[x, y]$, we get that $R(y) \in I \cap k[y] = I_1$, where I_1 is the first elimination ideal of I. This shows that for $f, g \in k[x, y]$, we can use the resultant $R_x(f, g)$ to eliminate x and it is the same kind of elimination that we did in Section 4.5.2. However, in general we don't have that $\langle R(y)\rangle = I_1$. Indeed, consider the following example: let $f = x^2 + y^2 + 1$ and $g = x^2 + 2y^2 + 1$ be two polynomials in $k[x, y]$ and let $I = \langle f, g\rangle$. By considering the lexicographic ordering on $k[x, y]$ with $x > y > 1$, we get by an easy computation that $I_1 = I \cap k[y] = \langle y^2\rangle$. On the other hand, by using SINGULAR, we obtain

$$R(y) = R_x(f, g) = \det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ y^2 + 1 & 0 & 2y^2 + 1 & 0 \\ 0 & y^2 + 1 & 0 & 2y^2 + 1 \end{pmatrix} = y^4.$$

Therefore we have that $R(y) = y^4 \in I_1$, but $y^2 \notin \langle R(y)\rangle$, so that $I_1 \neq \langle R(y)\rangle$.

5.2.2 Bézout's Theorem

Another application of the univariate resultant is Bézout's theorem. Recall therefore that the projective plane $\mathbb{P}^2(k)$ is defined as the set of lines in k^3 that pass through the origin. It makes sense to speak of the zero set in $\mathbb{P}^2(k)$ of a homogeneous polynomial. Such a zero set describes a projective curve in

$\mathbb{P}^2(k)$. We will consider here only the weak form of Bézout's theorem which has as nice consequence Pascal's Mystic Hexagon theorem which is stated in *Ideals, Varieties, and Algorithms* [6, p.434].

Theorem 5.10 (**Bézout's Theorem-Weak Form**). *Let f and g be two homogeneous polynomials in $k[x, y, z]$, without common factors and of degree m, respectively n. Then $Z(f) \cap Z(g)$ is finite and has at most $n \cdot m$ points.*

Proof. Let us assume that $Z(f) \cap Z(g)$ have more than $n \cdot m$ points, which we label $p_0, ..., p_{nm}$. Let L_{ij} be the line through p_i and p_j for $i, j \in \{0, ..., nm\}$. Then pick a point

$$q \notin Z(f) \cup Z(g) \cup \Big(\bigcup_{i>j} L_{ij} \Big).$$

We can make a linear change of coordinates such that q has the coordinates $(0, 0, 1)$ in the new system. Indeed, if (a, b, c) are the coefficients of q, then there is an automorphism A from $\mathbb{P}^2(k)$ to $\mathbb{P}^2(k)$ such that

$$A : \mathbb{P}^2(k) \ni \langle a, b, c \rangle \mapsto A(\langle a, b, c \rangle) = \langle 0, 0, 1 \rangle \in \mathbb{P}^2(k).$$

Indeed, if $c \neq 0$, then we can consider the following automorphism:

$$A : \langle a, b, c \rangle \mapsto \langle (a, b, c) \cdot M \rangle = \langle 0, 0, 1 \rangle, \text{ where } M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\frac{a}{c} & -\frac{b}{c} & \frac{1}{c} \end{pmatrix} \in GL_3.$$

If $c = 0$, we have that either $a \neq 0$ or $b \neq 0$ since otherwise $\langle a, b, c \rangle \notin \mathbb{P}^2(k)$. Suppose that $a \neq 0$, then we can consider the automorphism $A = B \circ C$, where:

$C : \langle a, b, c \rangle \mapsto \langle c, b, a \rangle$ and

$$B : \langle a, b, c \rangle \mapsto \langle (a, b, c) \cdot M \rangle = \langle 0, 0, 1 \rangle, \text{ where } M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\frac{a}{c} & -\frac{b}{c} & \frac{1}{c} \end{pmatrix} \in GL_3.$$

The case $b \neq 0$ is analogous. Let us write $f = \sum_{i=0}^{m} f_i z^i$ and $g = \sum_{j=0}^{n} g_j z^j$ as polynomials in z with coefficients $f_i, g_j \in k[x, y]$. Since $f(0, 0, 1) \neq 0$, $g(0, 0, 1) \neq 0$ and f and g have no common factor, the univariate resultant $R(f, g, z)$ with respect to z is a non-zero homogeneous polynomial in x and y of degree $n \cdot m$. It is indeed a homogeneous polynomial in x and y, since f and g are homogeneous in $k[x, y, z]$ and by construction of the resultant. Let us denote $p_i = (x_i, y_i, z_i)$ for $i \in \{0, ..., n \cdot m\}$. Then, we have $R(f, g, z)(x_i, y_i) = 0$ for each $i \in \{0, ..., n \cdot m\}$. If there were $p_i = (x_i, y_i, z_i)$ and $p_j = (x_j, y_j, z_j)$

such that $x_i = x_j$ and $y_i = y_j$, then we would get that $(0, 0, 1) \in L_{ij}$ which contradicts our assumption. Therefore it follows that the $(nm + 1)$ points (x_i, y_i) are distinct which is a contradiction to the fact that $R(f, g, z)$ is a non-zero homogeneous polynomial in x and y of degree $n \cdot m$. $\square$

5.2.3 Computation with Algebraic Numbers

Let α and β be algebraic numbers over $\mathbb{Q}$. They are represented by their minimal polynomials $f, g \in \mathbb{Q}[x]$, i.e. the unique irreducible and monic polynomials satisfying $f(\alpha) = 0$, respectively $g(\beta) = 0$. In the case where $\gcd(\deg(f), \deg(g)) = 1$, we would like to find the minimal polynomials s and p for their sum $\alpha + \beta$ and their product $\alpha \cdot \beta$. Unfortunately, the solution to this problem is not straightforward, but we can show that the minimal polynomial of $\alpha + \beta$ is an irreducible factor of the univariate resultant s and the minimal polynomial of $\alpha \cdot \beta$ is an irreducible factor of the univariate resultant p, where s and p are given by:

$$s(y) = R(f(x), g(y - x), x) \text{ and } p(y) = R(f(x), g\left(\frac{y}{x}\right) \cdot x^{\deg(g)}, x).$$

Since α is a common root of $f(x)$ and $g(\alpha + \beta - x)$, we have by Proposition 5.2 that $s(\alpha + \beta) = 0$. Analogously, since α is a common root of $f(x)$ and $g(\frac{\alpha \cdot \beta}{x}) \cdot x^{\deg(g)}$, we have by Proposition 5.2 that $p(\alpha \cdot \beta) = 0$. The polynomials s and p are monic. Indeed, let us write

$$\begin{aligned} f(x) &= x^m + f_{m-1}x^{m-1} + ... + f_0, \\ g(x) &= x^n + g_{n-1}x^{n-1} + ... + g_0. \end{aligned}$$

Then we get

$$\begin{aligned} g(y - x) &= (y - x)^n + g_{n-1}(y - x)^{m-1} + ... + g_0 \\ &= (-x)^n + (g_{n-1} + ny)(-x)^{n-1} + ... + y^n. \end{aligned}$$

Hence, we get

$$s(y) = \det \underbrace{\begin{pmatrix} 1 & & & (-1)^n & & \\ & \ddots & & & \ddots & \\ \vdots & & 1 & \vdots & & (-1)^n \\ f_0 & & \vdots & y^n & & \vdots \\ & \ddots & & & \ddots & \\ & & f_0 & & & y^n \end{pmatrix}}_{\text{n columns} \quad \text{m columns}} = y^{nm} + \text{ terms of degree} < nm \text{ in } y.$$

So that we can conclude that s is monic. Similar for p, we have

$$g\Big(\frac{y}{x}\Big)x^n = y^n + g_{n-1}y^{n-1} + ... + g_0x^n.$$

Hence, we get

$$p(y) = \det \underbrace{\begin{pmatrix} 1 & & & g_0 & & \\ & \ddots & & & \ddots & \\ \vdots & & 1 & \vdots & & g_0 \\ f_0 & & \vdots & y^n & & \vdots \\ & \ddots & & & \ddots & \\ & & f_0 & & & y^n \end{pmatrix}}_{\text{n columns}\qquad\qquad\text{m columns}}$$

$$= y^{nm} + \text{ terms of degree} < nm \text{ in } y. \tag{5.6}$$

It follows that s and p are monic polynomials that vanish for $\alpha+\beta$ and $\alpha\cdot\beta$ respectively and so the minimal polynomial for $\alpha+\beta$ is a factor of s and the minimal polynomial of $\alpha\cdot\beta$ is a factor of p.

Example 26. Consider the following algebraic numbers:

$$\alpha = \sqrt{2} \text{ and } \beta = -\sqrt[3]{7}.$$

Their minimal polynomials are

$$f(x) = x^2 - 2 \text{ respectively } g(x) = x^3 + 7.$$

Note that $\gcd(\deg(f), \deg(g)) = \gcd(2,3) = 1$, so that we can use the formula from above. We have that $g(y-x) = -x^3 + 3yx^2 - 3y^2x + (y^3+7)$ and by using SINGULAR with the code `resultant(f,g,x)`, we get:

$$s(y) = R(f(x), g(y-x), x) = y^6 - 6y^4 + 14y^3 + 12y^2 + 84y + 41.$$

Since this polynomial is in addition irreducible, we can conclude that in this case s is the minimal polynomial of $\alpha+\beta$. On the other hand, we have that $g(\frac{y}{x})\cdot x^{\deg(g)} = 7x^3 + y^3$ and by using again SINGULAR, we get:

$$p(y) = R(f(x), g\Big(\frac{y}{x}\Big)\cdot x^{\deg(g)}, x) = y^6 - 941192.$$

Again, this polynomial is irreducible, thus we can conclude that p is the minimal polynomial of $\alpha\cdot\beta$.

Remark 11. In Example 26, we even got the minimal polynomials of the sum and the product of the considered algebraic numbers. However, this is not true in general. Indeed, by (5.6), we know that p has degree $n \cdot m$ if $\deg \alpha = n$ and $\deg \beta = m$. Let $\alpha = \sqrt[3]{2}$ and $\beta = \mathrm{e}^{\frac{2\pi i}{3}}$. Their minimal polynomials are

$$f(x) = x^3 - 2 \text{ respectively } g(x) = x^2 + x + 1,$$

so that α is of degree 3, β of degree 2 and $\deg p = 2 \cdot 3 = 6$. However, the minimal polynomial of $\alpha \cdot \beta$ is given by

$$m(x) = x^3 - 2,$$

thus p cannot be the minimal polynomial of the product of α and β. Necessary and sufficient conditions on α and β such that p is the minimal polynomial of $\alpha \cdot \beta$ are analysed in *Two Exercises Concerning the Degree of the Product of Algebraic Numbers* [10]. For more details on the minimal polynomial of $\alpha + \beta$ consider *Degrees of Sums in a Separable Field Extension* [16].

5.3 Comparison of Groebner Bases and Univariate Resultants

An interesting comparison of Groebner bases and univariate resultants was given by Marko Roczen in *Gröbner Bases and Resultants* [23]. Let us consider

$$\begin{aligned} f &= u_n x^n + ... + u_1 x + u_0 \\ \text{and} \quad g &= v_n x^n + ... + v_1 x + v_0 \end{aligned}$$

in $k[u_0, ..., u_n, v_0, ..., v_n][x]$, so that we regard the coefficients $u_0, ..., u_n, v_0, ..., v_n$ as variables. We have seen in sections 4.5.2 and 5.1 that Groebner bases and resultants can be used to eliminate a variable. A natural question is if one tool is better than the other.
For $n = 2$, we consider the lexicographic ordering on $[u_0, u_1, u_2, v_0, v_1, v_2][x]$ with $x > u_0 > u_1 > u_2 > v_0 > v_1 > v_2 > 1$. To get the first elimination ideal of $I = \langle f, g \rangle$, we compute the Groebner basis of I using SINGULAR and we only have to consider the elements that do not contain x. This is apparently only the first polynomial. Now we compute the resultant $R(f, g)$ using again SINGULAR. Apparently, this is the same as the first element of the above computed Groebner basis.

```
> ring r=0, (x,u(0..2),v(0..2)), lp;
> poly f=u(2)*x2+u(1)*x+u(0);
> poly g=v(2)*x2+v(1)*x+v(0);
> ideal I=f,g;
> std(I);
_[1]=u(0)2*v(2)2-u(0)*u(1)*v(1)*v(2)-2*u(0)*u(2)*v(0)*v(2)
     +u(0)*u(2)*v(1)2+u(1)2*v(0)*v(2)-u(1)*u(2)*v(0)*v(1)
     +u(2)2*v(0)2
_[2]=x*u(1)*v(2)-x*u(2)*v(1)+u(0)*v(2)-u(2)*v(0)
_[3]=x*u(0)*v(2)-x*u(2)*v(0)+u(0)*v(1)-u(1)*v(0)
_[4]=x*u(0)*u(2)*v(1)-x*u(1)*u(2)*v(0)-u(0)2*v(2)+u(0)*u(1)*v(1)
     +u(0)*u(2)*v(0)-u(1)2*v(0)
_[5]=x2*v(2)+x*v(1)+v(0)
_[6]=x2*u(2)+x*u(1)+u(0)
> resultant(f,g,x);
u(0)2*v(2)2-u(0)*u(1)*v(1)*v(2)-2*u(0)*u(2)*v(0)*v(2)
     +u(0)*u(2)*v(1)2+u(1)2*v(0)*v(2)-u(1)*u(2)*v(0)*v(1)
     +u(2)2*v(0)2
```

Doing the same for $n = 3$, there is no problem but already for $n = 4$, SINGULAR will not be able to compute a Groebner bases of I within a reasonable amount of time. However using the command `resultant`, SINGULAR gives us the solution within moments. Thus, this example shows how resultants can be a useful tool to solve polynomial equations in cases where Groebner bases may fail. The reason is that the output contains too many unwanted elements and, as a result, the Buchberger's algorithm becomes hopelessly slow.

5.4 Multivariate Resultants

Next, we will extend the notion of the resultant to multivariate polynomials in $k[x_1, ..., x_n]$. We will start by defining the resultant of two homogeneous polynomials in two variables. Let us consider the following two homogeneous polynomials of degree d_1, respectively d_2.

$$F = f_{d_1}x_1^{d_1} + f_{d_1-1}x_1^{d_1-1}x_2 + ... + f_0x_2^{d_1},$$
$$G = g_{d_2}x_1^{d_2} + g_{d_2-1}x_1^{d_2-1}x_2 + ... + g_0x_2^{d_2}.$$

Let us now consider $x_1^{d_2-1}F$, $x_1^{d_2-2}x_2F$,...,$x_2^{d_2-1}F$, $x_1^{d_1-1}G$, $x_1^{d_1-2}x_2G$,...,$x_2^{d_1-1}G$ so that we get the following system of equations

$$
\begin{aligned}
f_{d_1}x_1^{d_1+d_2-1} + ... + f_0 x_1^{d_2-1}x_2^{d_1} &= x_1^{d_2-1}F \\
f_{d_1}x_1^{d_1+d_2-2}x_2 + ... + f_0 x_1^{d_2-2}x_2^{d_1+1} &= x_1^{d_2-2}x_2 F \\
\vdots & \quad \vdots \\
f_{d_1}x_1^{d_1}x_2^{d_2-1} + ... + f_0 x_2^{d_1+d_2-1} &= x_2^{d_2-1}F \\
g_{d_2}x_1^{d_2+d_1-1} + ... + g_0 x_1^{d_2-1}x_2^{d_1} &= x_1^{d_1-1}G \\
g_{d_2}x_1^{d_2+d_1-2}x_2 + ... + g_0 x_1^{d_2-2}x_2^{d_1+1} &= x_1^{d_1-2}x_2 G \\
\vdots & \quad \vdots \\
g_{d_2}x_1^{d_1}x_2^{d_1-1} + ... + g_0 x_2^{d_1+d_2-1} &= x_2^{d_1-1}G.
\end{aligned}
$$

The matrix where the rows are given by the left-hand side of these equations and the columns are the coefficients of $x_1^{d_1+d_2-1}, x_1^{d_1+d_2-2}, ..., x_1^{d_1}x_2^{d_2-1}, x_1^{d_2-1}x_2^{d_1}$, $x_1^{d_2-2}x_2^{d_1+1}, ..., x_2^{d_1+d_2-1}$ is given by

$$
M = \begin{pmatrix}
f_{d_1} & & \cdots & & f_0 & & & \\
 & f_{d_1} & \cdots & & & f_0 & & \\
 & & \ddots & & & & \ddots & \\
 & & & f_{d_1} & & \cdots & & f_0 \\
g_{d_2} & & \cdots & & g_0 & & & \\
 & g_{d_2} & \cdots & & & g_0 & & \\
 & & \ddots & & & & \ddots & \\
 & & & g_{d_2} & \cdots & & & g_0
\end{pmatrix}
$$

Definition 5.11. *The **multivariate resultant** $R(F,G)$ of F and G is defined as the determinant of this matrix M.*

Since this matrix is the transpose of the Sylvester matrix of $f = \sum_{i=0}^{m} f_i x^i$ and $g = \sum_{j=0}^{n} g_i x^j$, the resultant of F and G is equal to the univariate resultant of f and g. From this equality follows directly that the resultant has the same properties as the one of f and g.

Proposition 5.12. *Let*

$$
\begin{aligned}
F &= f_{d_1}x_1^{d_1} + f_{d_1-1}x_1^{d_1-1}x_2 + ... + f_0 x_2^{d_1}, \\
G &= g_{d_2}x_1^{d_2} + g_{d_2-1}x_1^{d_2-1}x_2 + ... + g_0 x_2^{d_2},
\end{aligned}
$$

and $R(F,G)$ be the resultant of F and G. Then

1) F and G have a common non-zero root if and only if $R(F,G) = 0$.

2) $R(F,G)$ is irreducible.

3) There are $A, B \in \mathbb{Z}[f_0, ..., f_m, g_0, ..., g_n]$ such that

$$R(F,G) = AF + BG.$$

Proof. As already mentioned before, the proof is analogous to the proof in the univariate case which can be found at the beginning of Section 5.1. □

Next, we will define the resultant of n homogeneous polynomials in n variables. The general theory of the resultant is parallel to that already given for two variables, but it involves points of much greater difficulty. In this part we are following *Introduction to resultants*[26].
Let F_1, F_2,..., F_n be n homogeneous polynomials in n variables

$$F_1(x_1, ..., x_n) = ... = F_n(x_1, ..., x_n) = 0. \tag{5.7}$$

Let us assume in addition that these polynomials are of positive degree d_1, d_2,..., d_n and let us write them as

$$F_i = \sum_{j_1+...+j_n=d_i} c^{(i)}_{j_1,...,j_n} x_1^{j_1} \cdot ... \cdot x_n^{j_n},$$

where the sum is over all $C^{d_i}_{n+d_i-1}$ monomials of degree d_i in x_1,..., x_n. Again, the question is to determine whether there is a non-zero common root of F_1,..., F_n. To give an answer to this question, let us introduce a variable $u^{(i)}_{j_1,...,j_n}$ for each coefficient $c^{(i)}_{j_1,...,j_n}$ of F_i. Let $\mathbb{Z}[u]$ be the ring of polynomials with integer coefficients in these variables. Note that the total number of variables in $k[u]$ is $N = \sum_{i=1}^{n} C^{d_i}_{n+d_i-1}$.

Theorem 5.13. *Let F_1, F_2,..., F_n be n homogeneous polynomials of positive degree d_1, d_2,..., d_n. Then there exists a unique polynomial $R \in \mathbb{Z}[u]$ such that*

1) F_1,..., F_n have a non-zero common root in k^n if and only if $R(F_1, ..., F_n) = 0$.

2) R is irreducible in $k[u]$.

3) $R(x_1^{d_1}, ..., x_n^{d_n}) = 1$.

Remark 12. From condition 1) follows that $R(x_1^{d_1}, ..., x_n^{d_n}) \neq 0$, since $F_1 = x_1^{d_1}, ..., F_n = x_n^{d_n})$ only has zero as common root. Therefore we can conclude that $R(x_1^{d_1}, ..., x_n^{d_n}) = c$, where $c \in \mathbb{Z}$. Condition 3) is necessary to guarantee uniqueness of the polynomial R.

Proof. We will only give a sketch of this proof: Recall that the total number of variables in $k[u]$ is $N = \sum_{i=1}^{n} C_{n+d_i-1}^{d_i}$, so that k^N is the space of values for coefficient of $F_1, ..., F_n$. Then there is a subspace $W = \{(\bar{u}, \langle x_1, ..., x_n \rangle)\}$ of $k^N \times \mathbb{P}^{n-1}(k)$, the incidence variety, such that

$$F_i(\bar{u})(x_1, ..., x_n) = 0 \text{ for all } i \in \{1, ..., n\}, \text{ for } \{(\bar{u}, \langle x_1, ..., x_n \rangle)\} \in W.$$

Now we consider the following projection:

$$W = \{(\bar{u}, \langle x_1, ..., x_n \rangle)\} \subset k^N \times \mathbb{P}^{n-1}(k) \xrightarrow{pr_1} pr_1(W) = \{\bar{u}\} =: V \subset k^N,$$

where V is exactly the space of those values of coefficients of $F_1, ..., F_n$ when the system (5.7) has non-zero solutions. It turns out that $V = Z(R)$, where R is the unique irreducible polynomial in $\mathbb{Z}[u]$ that satisfies 1) and 3). More details of the proof can be found in *Introduction to Resultants* [26, p.8]. □

Definition 5.14. *The polynomial $R \in \mathbb{Z}[u]$ defined in Theorem 5.13 is the* ***multivariate resultant*** *of the system (5.7).*

The multivariate resultant R of the system (5.7) has the following properties:

Theorem 5.15. *The multivariate resultant R is homogeneous of degree $d_1 \cdot ... \cdot d_{i-1} \cdot d_{i+1} ... d_n$ in the coefficients $(u_{a_i}^{(i)} : |a_i| = d_i)$ for each fixed $i \in \{1, ..., n\}$.*

Proof. Let us show for example that R is homogeneous in the coefficients of F_1.

$$\begin{aligned} R(F_1, ..., F_n) = 0 &\iff F_1 = F_2 = ... = F_n \text{ has a non-zero solution} \\ &\iff \lambda F_1 = F_2 = ... = F_n, \lambda \neq 0 \text{ has a non-zero solution} \\ &\iff R(\lambda F_1, ..., F_n) = 0, \lambda \neq 0. \end{aligned}$$

Let us denote $R' = R(\lambda F_1, ..., F_n)$. Then R' is irreducible in the coefficients of $F_1, ..., F_n$ since otherwise R will be reducible. Indeed, we have that

$$R'(u) = R'(u_1, u_2, ..., u_n) = R(\lambda u_1, u_2, ...u_n).$$

If R' is reducible, we can decompose $R'(u)$ in two factors:

$$R'(u) = R'_1(u) \cdot R'_2(u) = R(\lambda u_1, u_2, ..., u_n).$$

By the change of variable $u_1 \to \frac{1}{\lambda} u_1$, we get

$$R'_1\Big(\frac{1}{\lambda} u_1, u_2, ..., u_n\Big) \cdot R'_2\Big(\frac{1}{\lambda} u_1, u_2, ..., u_n\Big) = R(u_1, u_2, ..., u_n)$$

i.e. we get a decomposition of R, which is a contradiction to the fact that R is irreducible. Since $Z(R) = Z(R')$, it follows that there is $\gamma \neq 0$ such that $\gamma R = R'$. Looking at the monomials of R' in $u_{a_i}^{(i)}$, we can conclude that $\gamma = \lambda^a$, where a is the degree of the monomial in coefficients of F_1. Therefore, all the degrees are the same and finally R is homogeneous in the coefficients of F_1. The degree of the multivariate resultant R is a consequence of Bézout's Theorem. □

Next, we would like to compute the multivariate resultant of F_1,..., F_n. Therefore we will denote in the following a monomial $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ by x^a and we will write $|a| = a_1 + a_2 + ... + a_n$.

Definition 5.16. *If $F_1, ..., F_n$ are homogeneous polynomials of degrees $d_1, ..., d_n$, then $d := d_1 + d_2 + ... + d_n - n + 1$ is called the* ***critical degree****.*

Note that the critical degree d is the smallest integer which has the following property: Every monomial x^a of degree $d = |a|$ is divisible by $x_i^{d_i}$ for at least one index $i \in \{1, ..., n\}$. Otherwise, if there was no $i \in \{1, ..., n\}$ such that $x_i^{d_i}$ divides x^a, then x^a would have at most degree $(d_1-1)+(d_2-1)+...+(d_n-1) = d_1 + d_2 + ... + d_n - n < d$, which is a contradiction to our assumption. We would like to have a partition of the set of monomials of critical degree. For this reason, we introduce the following definition:

$$S_i := \{x^a : |a| = d \text{ and } i \text{ is the smallest index such that } x_i^{d_i} \text{ divides } x^a\}.$$

In other words, S_1 is the set of all monomials x^a of degree d and with $a_1 \geq d_1$, while S_n is the set of all monomials x^a of degree d and with $0 \leq a_1 < d_1$, $0 \leq a_2 < d_2$,..., $0 \leq a_{n-1} < d_{n-1}$. Thus, we have

$$\{x^a : |a| = d\} = S_1 \dot{\cup} S_2 \dot{\cup} ... \dot{\cup} S_n.$$

Next, we consider the following system of C_{d+n-1}^d equations:

$$\begin{aligned}
&\frac{x^a}{x_1^{d_1}} F_1 = 0 \quad \text{for all } x^a \in S_1 \\
&\frac{x^a}{x_2^{d_2}} F_2 = 0 \quad \text{for all } x^a \in S_2 \\
&\quad \vdots \qquad \vdots \qquad\quad \vdots \\
&\frac{x^a}{x_n^{d_n}} F_n = 0 \quad \text{for all } x^a \in S_n
\end{aligned} \tag{5.8}$$

Each of these equations can be written as a linear combination of the C^d_{n+d-1} monomials of degree d and so the coefficients of these linear combinations form a $C^d_{n+d-1} \times C^d_{n+d-1}$ square matrix. Each non-zero entry of this matrix in one of the indeterminates $u^{(i)}_{j_1,...,j_n}$. We will denote the determinant of this matrix by D_n which has the following properties:

Theorem 5.17. *The determinant D_n is a non-zero polynomial in $k[u]$, homogeneous of degree $|S_i|$ in the coefficients of F_i, and the resultant R divides D_n.*

Proof. The determinant D_n is by construction a homogeneous polynomial in $k[u]$ of degree $|S_i|$ in the coefficients of F_i. By replacing each F_i by $x_i^{d_i}$ and by fixing a monomial ordering on $k[x_1, ..., x_n]$, the matrix associated to (5.8) has a determinant which is equal to ± 1. Indeed, by replacing each F_I by $x_i^{d_i}$, we get in each row of the associated matrix to (5.8) a 1 and otherwise zeroes. It remains therefore to show that in each column of the considered matrix, we only have one 1 and otherwise zeros. We only get more than one 1 in a column if we have

$$m_i F_i = m_j F_j, \text{ for some } i, j \in \{1, ..., n\}, i \neq j,$$

where we have

$$F_i = x_i^{d_i}, m_i = \frac{x^a}{x_i^{d_i}}, x^a \in S_i \text{ and } F_j = x_j^{d_j}, m_j = \frac{x^b}{x_j^{d_j}}, x^b \in S_j.$$

It follows that

$$m_i F_i = m_j F_j \iff \frac{x^a}{x_i^{d_i}} x_i^{d_i} = \frac{x^a}{x_j^{d_j}} x_j^{d_j} \iff x^a = x^b.$$

However, this contradicts the fact that $S_i \cap S_j = \emptyset$. Thus, we can conclude that there is only one 1 in each row and column of the considered matrix and the other entries are zero and so its determinant is ± 1. We can conclude from this, that D_n is a non-zero polynomial. It remains to show that the resultant R divides D_n. Any zero u of the resultant R corresponds to a system $F_1(y) = ... = F_n(y) = 0$ which has a non-zero solution $y \in k^n$. By replacing x by y in (5.8), we get $D_n(u) = 0$. It follows that the zero set of R is in the zero set of D_n. Since in addition R is irreducible, we can conclude by Study's Lemma that R divides D_n. □

Let us illustrate the construction of D_n by examples.

Example 27. Let us consider the case $n = 3$, $d_1 = d_2 = d_3 = 1$, i.e

$$\begin{aligned} F_1 &= c^{(1)}_{1,0,0}x + c^{(1)}_{0,1,0}y + c^{(1)}_{0,0,1}z \\ F_2 &= c^{(2)}_{1,0,0}x + c^{(2)}_{0,1,0}y + c^{(2)}_{0,0,1}z \\ F_3 &= c^{(3)}_{1,0,0}x + c^{(3)}_{0,1,0}y + c^{(3)}_{0,0,1}z. \end{aligned}$$

The critical degree is in this case $d = 1+1+1-3+1 = 1$. There are $C^1_3 = 3$ monomials of critical degree and we have

$$S_1 = \{x\},\ S_2 = \{y\},\ S_3 = \{z\}.$$

The 3×3 matrix associated to the system of equations (5.8) is given by:

$$\begin{array}{c} \\ F_1 \\ F_2 \\ F_3 \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} c^{(1)}_{1,0,0} & c^{(1)}_{0,1,0} & c^{(1)}_{0,0,1} \\ c^{(2)}_{1,0,0} & c^{(2)}_{0,1,0} & c^{(2)}_{0,0,1} \\ c^{(3)}_{1,0,0} & c^{(3)}_{0,1,0} & c^{(3)}_{0,0,1} \end{pmatrix} \end{array}$$

The columns are indexed by all monomials of critical degree, ordered by lexicographic ordering on $k[x, y, z]$ with $x > y > z > 1$, and the rows are indexed by multiples of the input equations F_1, F_2 and F_3 and are also ordered by lexicographic ordering on $k[x, y, z]$. Finally, D_n is the determinant of this matrix and is equal to

$$\begin{aligned} D_n =& c^{(1)}_{1,0,0}c^{(2)}_{0,1,0}c^{(3)}_{0,0,1} + c^{(2)}_{1,0,0}c^{(3)}_{0,1,0}c^{(1)}_{0,0,1} + c^{(3)}_{1,0,0}c^{(1)}_{0,1,0}c^{(2)}_{0,0,1} \\ &-(c^{(3)}_{1,0,0}c^{(2)}_{0,1,0}c^{(1)}_{0,0,1} + c^{(2)}_{1,0,0}c^{(1)}_{0,1,0}c^{(3)}_{0,0,1} + c^{(1)}_{1,0,0}c^{(3)}_{0,1,0}c^{(2)}_{0,0,1}). \end{aligned}$$

Example 28. Let us consider the case $n = 3$, $d_1 = d_2 = 1$, $d_3 = 2$, i.e.

$$\begin{aligned} F_1 &= c^{(1)}_{1,0,0}x + c^{(1)}_{0,1,0}y + c^{(1)}_{0,0,1}z \\ F_2 &= c^{(2)}_{1,0,0}x + c^{(2)}_{0,1,0}y + c^{(2)}_{0,0,1}z \\ F_3 &= c^{(3)}_{2,0,0}x^2 + c^{(3)}_{0,2,0}y^2 + c^{(3)}_{0,0,2}z^2 + c^{(3)}_{1,1,0}xy + c^{(3)}_{1,0,1}xz + c^{(3)}_{0,1,1}yz. \end{aligned}$$

The critical degree is in this case $d = 1+1+2-3+1 = 2$. There are $C^2_4 = 6$ monomials of critical degree and we have

$$S_1 = \{x^2, xy, xz\},\ S_2 = \{y^2, yz\},\ S_3 = \{z^2\}.$$

The 6×6 matrix associated to the system of equations (5.8) is given by:

$$\begin{array}{c} \\ xF_1 \\ yF_1 \\ zF_1 \\ yF_2 \\ zF_2 \\ 1 \cdot F_3 \end{array} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & xz & y^2 & yz & z^2 \end{array} \\ \begin{pmatrix} c^{(1)}_{1,0,0} & c^{(1)}_{0,1,0} & c^{(1)}_{0,0,1} & 0 & 0 & 0 \\ 0 & c^{(1)}_{1,0,0} & 0 & c^{(1)}_{0,1,0} & c^{(1)}_{0,0,1} & 0 \\ 0 & 0 & c^{(1)}_{1,0,0} & 0 & c^{(1)}_{0,1,0} & c^{(1)}_{0,0,1} \\ 0 & c^{(2)}_{1,0,0} & 0 & c^{(2)}_{0,1,0} & c^{(2)}_{0,0,1} & 0 \\ 0 & 0 & c^{(2)}_{1,0,0} & 0 & c^{(2)}_{0,1,0} & c^{(2)}_{0,0,1} \\ c^{(3)}_{2,0,0} & c^{(3)}_{1,1,0} & c^{(3)}_{1,0,1} & c^{(3)}_{0,2,0} & c^{(3)}_{0,1,1} & c^{(3)}_{0,0,2} \end{pmatrix} \end{array}$$

The columns are indexed by all monomials of critical degree, ordered by lexicographic ordering on $k[x, y, z]$ with $x > y > z > 1$, and the rows are indexed by multiples of the input equations F_1, F_2 and F_3 and are also ordered by lexicographic ordering on $k[x, y, z]$. Finally, D_n is the determinant of this matrix which we can compute using SINGULAR:

$$\begin{aligned} D_n =& (c^{(1)}_{1,0,0})^3 (c^{(2)}_{0,1,0})^2 c^{(3)}_{0,0,2} - (c^{(1)}_{1,0,0})^3 c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{0,1,1} + (c^{(1)}_{1,0,0})^3 (c^{(2)}_{0,0,1})^2 c^{(3)}_{0,2,0} \\ & - 2(c^{(1)}_{1,0,0})^2 c^{(1)}_{0,1,0} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{0,0,2} + (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,1,0} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{0,1,1} \\ & + (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,1,0} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{1,0,1} - (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,1,0} (c^{(2)}_{0,0,1})^2 c^{(3)}_{1,1,0} \\ & + (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{0,1,1} - 2(c^{(1)}_{1,0,0})^2 c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{0,2,0} \\ & - (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,0,1} (c^{(2)}_{0,1,0})^2 c^{(3)}_{1,0,1} + (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,0,1} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{1,1,0} \\ & + c^{(1)}_{1,0,0} (c^{(1)}_{0,1,0})^2 (c^{(2)}_{1,0,0})^2 c^{(3)}_{0,0,2} - c^{(1)}_{1,0,0} (c^{(1)}_{0,1,0})^2 c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{1,0,1} \\ & + c^{(1)}_{1,0,0} (c^{(1)}_{0,1,0})^2 (c^{(2)}_{0,0,1})^2 c^{(3)}_{2,0,0} - c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} (c^{(2)}_{1,0,0})^2 c^{(3)}_{0,1,1} \\ & + c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{1,0,1} + c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{1,1,0} \\ & - 2c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{2,0,0} + c^{(1)}_{1,0,0} (c^{(1)}_{0,0,1})^2 (c^{(2)}_{1,0,0})^2 c^{(3)}_{0,2,0} \\ & - c^{(1)}_{1,0,0} (c^{(1)}_{0,0,1})^2 c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{1,1,0} + c^{(1)}_{1,0,0} (c^{(1)}_{0,0,1})^2 (c^{(2)}_{0,1,0})^2 c^{(3)}_{2,0,0}. \end{aligned}$$

```
> ring r=0, (a(1..3),b(1..3),c(1..6)),lp;
> matrix A[6][6]= a(1),a(2),a(3),0,0,0, 0,a(1),0,a(2),a(3),0,
0,0,a(1),0,a(2),a(3),0,b(1),0,b(2),b(3),0,0,0,b(1),0,b(2),b(3),
c(1),c(4),c(5),c(2),c(6),c(3);
> print(A);
a(1),a(2),a(3),0, 0, 0,
0, a(1),0, a(2),a(3),0,
0, 0, a(1),0, a(2),a(3),
0, b(1),0, b(2),b(3),0,
0, 0, b(1),0, b(2),b(3),
c(1),c(4),c(5),c(2),c(6),c(3)
```

```
> det(A);
a(1)^3*b(2)^2*c(3)-a(1)^3*b(2)*b(3)*c(6)+a(1)^3*b(3)^2*c(2)-
2*a(1)^2*a(2)*b(1)*b(2)*c(3)+a(1)^2*a(2)*b(1)*b(3)*c(6)+a(1)^2
a(2)*b(2)*b(3)*c(5)-a(1)^2*a(2)*b(3)^2*c(4)+a(1)^2*a(3)*b(1)*
b(2)*c(6)-2*a(1)^2*a(3)*b(1)*b(3)*c(2)-a(1)^2*a(3)*b(2)^2*c(5)
+a(1)^2*a(3)*b(2)*b(3)*c(4)+a(1)*a(2)^2*b(1)^2*c(3)-a(1)*
a(2)^2*b(1)*b(3)*c(5)+a(1)*a(2)^2*b(3)^2*c(1)-a(1)*a(2)*a(3)*
b(1)^2*c(6)+a(1)*a(2)*a(3)*b(1)*b(2)*c(5)+a(1)*a(2)*a(3)*b(1)
b(3)*c(4)-2*a(1)*a(2)*a(3)*b(2)*b(3)*c(1)+a(1)*a(3)^2*b(1)^2
c(2)-a(1)*a(3)^2*b(1)*b(2)*c(4)+a(1)*a(3)^2*b(2)^2*c(1)
```

Since the construction in Theorem 5.17 makes sense for any ordering of the variables, any variable x_i can play the role of the last variable x_n. Let us denote by D_i the associated determinant of the system (5.8), where x_i is considered as the last variable. With this notation, we have the following result.

Corollary 5.18. *The resultant R is up to a constant the greatest common divisor of the determinants $D_1, ..., D_n$.*

Proof. Let us denote by G the greatest common divisor of $D_1, ..., D_n$. Note that for D_n, we realised that S_n is the set of all monomials x^a of degree d and with $0 \leq a_1 < d_1$, $0 \leq a_2 < d_2$,..., $0 \leq a_{n-1} < d_{n-1}$. Therefore, we can conclude that $|S_n| = d_1 \cdot ... \cdot d_{n-1}$. It follows that for D_i, we have $|S_n| = d_1 \cdot ... \cdot d_{i-1} \cdot d_{i+1} ... \cdot d_n$. We can conclude from this, that the degree of D_i in the coefficients of f_i is $d_1 \cdot ... \cdot d_{i-1} \cdot d_{i+1} ... \cdot d_n$ and so G has degree at most $d_1 \cdot ... \cdot d_{i-1} \cdot d_{i+1} ... \cdot d_n$ in the coefficients of f_i for each $i \in \{1, ..., n\}$. By Theorem 5.15, R has degree $d_1 \cdot ... \cdot d_{i-1} \cdot d_{i+1} ... \cdot d_n$ in the coefficients of f_i and by Theorem 5.17, we know that R divides G. It follows that R and G are equal up to a constant. □

Example 29. Let us come back to Example 28. We have already computed D_3, where z plays the role of the last variable x_n since we considered the lexicographic ordering on $k[x, y, z]$ with $x > y > z > 1$. Thus, it remains to compute D_1, D_2 and the greatest common divisor of D_1, D_2 and D_3 to get the resultant R. To compute D_1, we consider x to be the last variable x_n, i.e. we consider the lexicographic ordering on $k[x, y, z]$ with $y > z > x > 1$. In this case we get:

$$S_1 = \{y^2, yz, yx\},\ S_2 = \{z^2, zx\},\ S_3 = \{x^2\}.$$

The 6×6 matrix associated to the system of equations (5.8) is given by:

$$\begin{array}{c} \\ yF_1 \\ zF_1 \\ xF_1 \\ zF_2 \\ xF_2 \\ 1 \cdot F_3 \end{array} \begin{array}{c} \begin{array}{cccccc} y^2 & yz & yx & z^2 & zx & x^2 \end{array} \\ \begin{pmatrix} c_{0,1,0}^{(1)} & c_{0,0,1}^{(1)} & c_{1,0,0}^{(1)} & 0 & 0 & 0 \\ 0 & c_{0,1,0}^{(1)} & 0 & c_{0,0,1}^{(1)} & c_{1,0,0}^{(1)} & 0 \\ 0 & 0 & c_{0,1,0}^{(1)} & 0 & c_{0,0,1}^{(1)} & c_{1,0,0}^{(1)} \\ 0 & c_{0,1,0}^{(2)} & 0 & c_{0,0,1}^{(2)} & c_{1,0,0}^{(2)} & 0 \\ 0 & 0 & c_{0,1,0}^{(2)} & 0 & c_{0,0,1}^{(2)} & c_{1,0,0}^{(2)} \\ c_{0,2,0}^{(3)} & c_{0,1,1}^{(3)} & c_{1,1,0}^{(3)} & c_{0,0,2}^{(3)} & c_{1,0,1}^{(3)} & c_{2,0,0}^{(3)} \end{pmatrix} \end{array}$$

The columns are indexed by all monomials of critical degree, ordered by lexicographic ordering on $k[x, y, z]$ with $y > z > x > 1$, and the rows are indexed by multiples of the input equations F_1, F_2 and F_3 and are also ordered by lexicographic ordering on $k[x, y, z]$. Finally, D_1 is the determinant of this matrix. The SINGULAR code is analogous to the one of D_3.

$$\begin{aligned} D_1 =& (c_{1,0,0}^{(1)})^2 c_{0,1,0}^{(1)} (c_{0,1,0}^{(2)})^2 c_{0,0,2}^{(3)} - (c_{1,0,0}^{(1)})^2 c_{0,1,0}^{(1)} c_{0,1,0}^{(2)} c_{0,0,1}^{(2)} c_{0,1,1}^{(3)} \\ &+ (c_{1,0,0}^{(1)})^2 c_{0,1,0}^{(1)} (c_{0,0,1}^{(2)})^2 c_{0,2,0}^{(3)} - 2 c_{1,0,0}^{(1)} (c_{0,1,0}^{(1)})^2 c_{1,0,0}^{(2)} c_{0,1,0}^{(2)} c_{0,0,2}^{(3)} \\ &+ c_{1,0,0}^{(1)} (c_{0,1,0}^{(1)})^2 c_{1,0,0}^{(2)} c_{0,0,1}^{(2)} c_{0,1,1}^{(3)} + c_{1,0,0}^{(1)} (c_{0,1,0}^{(1)})^2 c_{0,1,0}^{(2)} c_{0,0,1}^{(2)} c_{1,0,1}^{(3)} \\ &- c_{1,0,0}^{(1)} (c_{0,1,0}^{(1)})^2 (c_{0,0,1}^{(2)})^2 c_{1,1,0}^{(3)} + c_{1,0,0}^{(1)} c_{0,1,0}^{(1)} c_{0,0,1}^{(1)} c_{1,0,0}^{(2)} c_{0,1,0}^{(2)} c_{0,1,1}^{(3)} \\ &- 2 c_{1,0,0}^{(1)} c_{0,1,0}^{(1)} c_{0,0,1}^{(1)} c_{1,0,0}^{(2)} c_{0,0,1}^{(2)} c_{0,2,0}^{(3)} - c_{1,0,0}^{(1)} c_{0,1,0}^{(1)} c_{0,0,1}^{(1)} (c_{0,1,0}^{(2)})^2 c_{1,0,1}^{(3)} \\ &+ c_{1,0,0}^{(1)} c_{0,1,0}^{(1)} c_{0,0,1}^{(1)} c_{0,1,0}^{(2)} c_{0,0,1}^{(2)} c_{1,1,0}^{(3)} + (c_{0,1,0}^{(1)})^3 (c_{1,0,0}^{(2)})^2 c_{0,0,2}^{(3)} \\ &- (c_{0,1,0}^{(1)})^3 c_{1,0,0}^{(2)} c_{0,0,1}^{(2)} c_{1,0,1}^{(3)} + (c_{0,1,0}^{(1)})^3 (c_{0,0,1}^{(2)})^2 c_{2,0,0}^{(3)} \\ &- (c_{0,1,0}^{(1)})^2 c_{0,0,1}^{(1)} (c_{1,0,0}^{(2)})^2 c_{0,1,1}^{(3)} + (c_{0,1,0}^{(1)})^2 c_{0,0,1}^{(1)} c_{1,0,0}^{(2)} c_{0,1,0}^{(2)} c_{1,0,1}^{(3)} \\ &+ (c_{0,1,0}^{(1)})^2 c_{0,0,1}^{(1)} c_{1,0,0}^{(2)} c_{0,0,1}^{(2)} c_{1,1,0}^{(3)} - 2 (c_{0,1,0}^{(1)})^2 c_{0,0,1}^{(1)} c_{0,1,0}^{(2)} c_{0,0,1}^{(2)} c_{2,0,0}^{(3)} \\ &+ c_{0,1,0}^{(1)} (c_{0,0,1}^{(1)})^2 (c_{1,0,0}^{(2)})^2 c_{0,2,0}^{(3)} - c_{0,1,0}^{(1)} (c_{0,0,1}^{(1)})^2 c_{1,0,0}^{(2)} c_{0,1,0}^{(2)} c_{1,1,0}^{(3)} \\ &+ c_{0,1,0}^{(1)} (c_{0,0,1}^{(1)})^2 (c_{0,1,0}^{(2)})^2 c_{2,0,0}^{(3)} \end{aligned}$$

To compute D_2, we consider y to be the last variable x_n, i.e. we consider the lexicographic ordering on $k[x, y, z]$ with $x > z > y > 1$. In this case we get:

$$\begin{aligned} S_1 &= \{x^2, xz, xy\}, \\ S_2 &= \{z^2, zy\} \\ S_3 &= \{y^2\}. \end{aligned}$$

The 6×6 matrix associated to the system of equations (5.8) is given by:

$$\begin{array}{c} \\ xF_1 \\ zF_1 \\ yF_1 \\ zF_2 \\ yF_2 \\ 1 \cdot F_3 \end{array} \begin{array}{c} \begin{array}{cccccc} x^2 & xz & xy & z^2 & zy & y^2 \end{array} \\ \begin{pmatrix} c^{(1)}_{1,0,0} & c^{(1)}_{0,0,1} & c^{(1)}_{0,1,0} & 0 & 0 & 0 \\ 0 & c^{(1)}_{1,0,0} & 0 & c^{(1)}_{0,0,1} & c^{(1)}_{0,1,0} & 0 \\ 0 & 0 & c^{(1)}_{0,1,0} & 0 & c^{(1)}_{0,0,1} & c^{(1)}_{0,1,0} \\ 0 & c^{(2)}_{1,0,0} & 0 & c^{(2)}_{0,0,1} & c^{(2)}_{0,1,0} & 0 \\ 0 & 0 & c^{(2)}_{1,0,0} & 0 & c^{(2)}_{0,0,1} & c^{(2)}_{0,1,0} \\ c^{(3)}_{2,0,0} & c^{(3)}_{1,0,1} & c^{(3)}_{1,1,0} & c^{(3)}_{0,0,2} & c^{(3)}_{0,1,1} & c^{(3)}_{0,2,0} \end{pmatrix} \end{array}$$

The columns are indexed by all monomials of critical degree, ordered by lexicographic ordering on $k[x, y, z]$ with $x > z > y > 1$, and the rows are indexed by multiples of the input equations F_1, F_2 and F_3 and are also ordered by lexicographic ordering on $k[x, y, z]$. Finally, D_2 is the determinant of this matrix.The SINGULAR code is analogous to the one of D_3.

$$\begin{aligned} D_2 = {} & (c^{(1)}_{1,0,0})^3 (c^{(2)}_{0,1,0})^2 c^{(3)}_{0,0,2} - (c^{(1)}_{1,0,0})^3 c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{0,1,1} \\ & + (c^{(1)}_{1,0,0})^3 (c^{(2)}_{0,0,1})^2 c^{(3)}_{0,2,0} - 2(c^{(1)}_{1,0,0})^2 c^{(1)}_{0,1,0} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{0,0,2} \\ & + (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,1,0} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{0,1,1} + (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,1,0} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{1,0,1} \\ & - (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,1,0} (c^{(2)}_{0,0,1})^2 c^{(3)}_{1,1,0} + (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{0,1,1} \\ & - 2(c^{(1)}_{1,0,0})^2 c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{0,2,0} - (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,0,1} (c^{(2)}_{0,1,0})^2 c^{(3)}_{1,0,1} \\ & + (c^{(1)}_{1,0,0})^2 c^{(1)}_{0,0,1} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{1,1,0} + c^{(1)}_{1,0,0} (c^{(1)}_{0,1,0})^2 (c^{(2)}_{1,0,0})^2 c^{(3)}_{0,0,2} \\ & - c^{(1)}_{1,0,0} (c^{(1)}_{0,1,0})^2 c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{1,0,1} + c^{(1)}_{1,0,0} (c^{(1)}_{0,1,0})^2 (c^{(2)}_{0,0,1})^2 c^{(3)}_{2,0,0} \\ & - c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} (c^{(2)}_{1,0,0})^2 c^{(3)}_{0,1,1} + c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{1,0,1} \\ & + c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{1,1,0} - 2c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{2,0,0} \\ & + c^{(1)}_{1,0,0} (c^{(1)}_{0,0,1})^2 (c^{(2)}_{1,0,0})^2 c^{(3)}_{0,2,0} - c^{(1)}_{1,0,0} (c^{(1)}_{0,0,1})^2 c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{1,1,0} \\ & + c^{(1)}_{1,0,0} (c^{(1)}_{0,0,1})^2 (c^{(2)}_{0,1,0})^2 c^{(3)}_{2,0,0} \end{aligned}$$

It remains to compute the greatest common divisor of D_1, D_2 and D_3, which can be done by using SINGULAR.

$$
\begin{aligned}
\gcd(D_1, D_2, D_3) = &- (c^{(1)}_{1,0,0})^2 (c^{(2)}_{0,1,0})^2 c^{(3)}_{0,0,2} + (c^{(1)}_{1,0,0})^2 c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{0,1,1} \\
&- (c^{(1)}_{1,0,0})^2 (c^{(2)}_{0,0,1})^2 c^{(3)}_{0,2,0} + 2 c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{0,0,2} \\
&- c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{0,1,1} - c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{1,0,1} \\
&+ c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} (c^{(2)}_{0,0,1})^2 c^{(3)}_{1,1,0} - c^{(1)}_{1,0,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{0,1,1} \\
&+ 2 c^{(1)}_{1,0,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{0,2,0} + c^{(1)}_{1,0,0} c^{(1)}_{0,0,1} (c^{(2)}_{0,1,0})^2 c^{(3)}_{1,0,1} \\
&- c^{(1)}_{1,0,0} c^{(1)}_{0,0,1} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{1,1,0} - (c^{(1)}_{0,1,0})^{(} c^{(2)}_{1,0,0})^2 c^{(3)}_{0,0,2} \\
&+ (c^{(1)}_{0,1,0})^2 c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{1,0,1} - (c^{(1)}_{0,1,0})^2 (c^{(2)}_{0,0,1})^2 c^{(3)}_{2,0,0} \\
&+ c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} (c^{(2)}_{1,0,0})^2 * c^{(3)}_{0,1,1} - c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{1,0,1} \\
&- c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{1,1,0} + 2 c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{2,0,0} \\
&- (c^{(1)}_{0,0,1})^2 (c^{(2)}_{1,0,0})^2 c^{(3)}_{0,2,0} + (c^{(1)}_{0,0,1})^2 c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{1,1,0} \\
&- (c^{(1)}_{0,0,1})^2 (c^{(2)}_{0,1,0})^2 c^{(3)}_{2,0,0}
\end{aligned}
$$

```
> ring r=0, (a(1..3),b(1..3),c(1..6)),lp;
> matrix A[6][6]= a(1),a(2),a(3),0,0,0, 0,a(1),0,a(2),a(3),0,
0,0,a(1),0,a(2),a(3),0,b(1),0,b(2),b(3),0,0,0,b(1),0,b(2),b(3),
c(1),c(4),c(5),c(2),c(6),c(3);
> poly f=det(A);
> matrix B[6][6]= a(2),a(3),a(1),0,0,0, 0,a(2),0,a(3),a(1),0,
0,0,a(2),0,a(3),a(1),0,b(2),0,b(3),b(1),0,0,0,b(2),0,b(3),b(1),
c(2),c(6),c(4),c(3),c(5),c(1);
> poly g=det(B);
> matrix C[6][6]= a(1),a(3),a(2),0,0,0, 0,a(1),0,a(3),a(2),0,
0,0,a(1),0,a(3),a(2),0,b(1),0,b(3),b(2),0,0,0,b(1),0,b(3),b(2),
c(1),c(5),c(4),c(3),c(6),c(2);
> poly h=det(C);
> poly k=gcd(f,g);
> gcd(h,k);
-a(1)^2*b(2)^2*c(3)+a(1)^2*b(2)*b(3)*c(6)-a(1)^2*b(3)^2*c(2)
+2*a(1)*a(2)*b(1)*b(2)*c(3)-a(1)*a(2)*b(1)*b(3)*c(6)
-a(1)*a(2)*b(2)*b(3)*c(5)+a(1)*a(2)*b(3)^2*c(4)
-a(1)*a(3)*b(1)*b(2)*c(6)+2*a(1)*a(3)*b(1)*b(3)*c(2)
+a(1)*a(3)*b(2)^2*c(5)-a(1)*a(3)*b(2)*b(3)*c(4)
-a(2)^2*b(1)^2*c(3)+a(2)^2*b(1)*b(3)*c(5)-a(2)^2*b(3)^2*c(1)
+a(2)*a(3)*b(1)^2*c(6)-a(2)*a(3)*b(1)*b(2)*c(5)
-a(2)*a(3)*b(1)*b(3)*c(4)+2*a(2)*a(3)*b(2)*b(3)*c(1)
```

There are other methods to compute the multivariate resultant of n homogeneous polynomials in n variables. Indeed, the following proposition gives a second method to do so.

Proposition 5.19. *Let M_n be as in Theorem 5.17 and M be the associated matrix to (5.8), i.e. $D_n = \det M$. Let M_0 be a submatrix of M by throwing away all rows and columns corresponding to the monomials of critical degree $x_1^{a_1}...x_n^{a_n}$ with exactly one i with $a_i \geq d_i$. Let us denote $D_n^0 = \det M_0$. Then we have*

$$R = \pm \frac{D_n}{D_n^0}.$$

We will not give a proof here but it can be found in *The Algebraic Theory of Modular Systems* [19].

Example 30. Let us come back to Example 28. Since $d_1 = d_2 = 1$ and $d_3 = 2$, obtained by throwing away all rows and columns of D_n corresponding to the monomials of critical degree $x_1^{a_1}...x_n^{a_n}$ with exactly one i with $a_i \geq d_i$, the only column that remains is xy and the only row that remains is yF_1. For these reasons, we have $c^{(1)}_{1,0,0}$. Finally,

$$\begin{aligned}
R = \frac{D_n}{D_n^0} =& \frac{D_n}{c^{(1)}_{1,0,0}} \\
=& (c^{(1)}_{1,0,0})^2 (c^{(2)}_{0,1,0})^2 c^{(3)}_{0,0,2} - (c^{(1)}_{1,0,0})^2 c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{0,1,1} \\
&+ (c^{(1)}_{1,0,0})^2 (c^{(2)}_{0,0,1})^2 c^{(3)}_{0,2,0} - 2c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{0,0,2} \\
&+ c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{0,1,1} + c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{1,0,1} \\
&- c^{(1)}_{1,0,0} c^{(1)}_{0,1,0} (c^{(2)}_{0,0,1})^2 c^{(3)}_{1,1,0} + c^{(1)}_{1,0,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{0,1,1} \\
&- 2c^{(1)}_{1,0,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{0,2,0} - c^{(1)}_{1,0,0} c^{(1)}_{0,0,1} (c^{(2)}_{0,1,0})^2 c^{(3)}_{1,0,1} \\
&+ c^{(1)}_{1,0,0} c^{(1)}_{0,0,1} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{1,1,0} + (c^{(1)}_{0,1,0})^2 (c^{(2)}_{1,0,0})^2 c^{(3)}_{0,0,2} \\
&- (c^{(1)}_{0,1,0})^2 c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{1,0,1} + (c^{(1)}_{0,1,0})^2 (c^{(2)}_{0,0,1})^2 c^{(3)}_{2,0,0} \\
&- c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} (c^{(2)}_{1,0,0})^2 c^{(3)}_{0,1,1} + c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{1,0,1} \\
&+ c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{1,0,0} c^{(2)}_{0,0,1} c^{(3)}_{1,1,0} - 2c^{(1)}_{0,1,0} c^{(1)}_{0,0,1} c^{(2)}_{0,1,0} c^{(2)}_{0,0,1} c^{(3)}_{2,0,0} \\
&+ c^{(1)}_{1,0,0} (c^{(1)}_{0,0,1})^2 (c^{(2)}_{1,0,0})^2 c^{(3)}_{0,2,0} - c^{(1)}_{1,0,0} (c^{(1)}_{0,0,1})^2 c^{(2)}_{1,0,0} c^{(2)}_{0,1,0} c^{(3)}_{1,1,0} \\
&+ c^{(1)}_{1,0,0} (c^{(1)}_{0,0,1})^2 (c^{(2)}_{0,1,0})^2 c^{(3)}_{2,0,0}.
\end{aligned}$$

Next, to generalize the theory of multivariate resultant, we would like to know the multivariate resultant of n non-homogeneous polynomials in $n-1$ variables. It is simply the resultant of the corresponding homogeneous polynomials of the same degrees obtained by introducing a variable x_0 and homogenizing the equations.

Example 31. Consider the following system of three quadratic equation:

$$\begin{aligned} f_1 &= a_1x^2 + a_2y^2 + a_3xy + a_4x + a_5y + a_6, \\ f_2 &= b_1x^2 + b_2y^2 + b_3xy + b_4x + b_5y + b_6, \\ f_3 &= c_1x^2 + c_2y^2 + c_3xy + c_4x + c_5y + c_6. \end{aligned}$$

These equations can be homogenized by introducing a new variable, say z. Since the polynomials f_1, f_2 and f_3 all have degree 2, we add to each monomial a power of z such that it also has degree 2. In this way, we get the following homogeneous polynomials of degree 2:

$$\begin{aligned} F_1 &= a_1x^2 + a_2y^2 + a_3xy + a_4xz + a_5yz + a_6z^2, \\ F_2 &= b_1x^2 + b_2y^2 + b_3xy + b_4xz + b_5yz + b_6z^2, \\ F_3 &= c_1x^2 + c_2y^2 + c_3xy + c_4xz + c_5yz + c_6z^2. \end{aligned}$$

This means that we have $n = 3$ with $d_1 = d_2 = d_3$ and we can rewrite F_1, F_2, F_3 in the following way

$$\begin{aligned} F_1 &= c^{(1)}_{2,0,0}x^2 + c^{(1)}_{0,2,0}y^2 + c^{(1)}_{0,0,2}z^2 + c^{(1)}_{1,1,0}xy + c^{(1)}_{1,0,1}xz + c^{(1)}_{0,1,1}yz, \\ F_2 &= c^{(2)}_{2,0,0}x^2 + c^{(2)}_{0,2,0}y^2 + c^{(2)}_{0,0,2}z^2 + c^{(2)}_{1,1,0}xy + c^{(2)}_{1,0,1}xz + c^{(2)}_{0,1,1}yz, \\ F_3 &= c^{(3)}_{2,0,0}x^2 + c^{(3)}_{0,2,0}y^2 + c^{(3)}_{0,0,2}z^2 + c^{(3)}_{1,1,0}xy + c^{(3)}_{1,0,1}xz + c^{(3)}_{0,1,1}yz. \end{aligned}$$

The critical degree is in this case $d = 2+2+2-3+1 = 4$. There are $C^4_6 = 15$ monomials of critical degree and we have

$$\begin{aligned} S_1 &= \{x^4, x^3y, x^3z, x^2y^2, x^2yz, x^2z^2\}, \\ S_2 &= \{xy^3, xy^2z, y^4, y^3z, y^2z^2\}, \\ S_3 &= \{xyz^2, xz^3, yz^3, z^4\}. \end{aligned}$$

The 15×15 matrix associated to the system of equations (5.8) is given by:

$$\begin{array}{c} \\ x^2F_1 \\ xyF_1 \\ xzF_1 \\ y^2F_1 \\ yzF_1 \\ z^2F_1 \\ xyF_2 \\ xzF_2 \\ y^2F_2 \\ yzF_2 \\ z^2F_2 \\ xyF_3 \\ xzF_3 \\ yzF_3 \\ z^2F_3 \end{array} \begin{array}{c} \begin{array}{ccccccccccccccc} x^4 & x^3y & x^3z & x^2y^2 & x^2yz & x^2z^2 & xy^3 & xy^2z & xyz^2 & xz^3 & y^4 & y^3z & y^2z^2 & yz^3 & z^4 \end{array} \\ \begin{pmatrix} c^{(1)}_{2,0,0} & c^{(1)}_{1,1,0} & c^{(1)}_{0,2,0} & c^{(1)}_{1,0,1} & c^{(1)}_{0,1,1} & c^{(1)}_{0,0,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & c^{(1)}_{2,0,0} & 0 & c^{(1)}_{1,1,0} & c^{(1)}_{0,2,0} & 0 & c^{(1)}_{1,0,1} & c^{(1)}_{0,1,1} & c^{(1)}_{0,0,2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & c^{(1)}_{2,0,0} & 0 & c^{(1)}_{1,1,0} & c^{(1)}_{0,2,0} & 0 & c^{(1)}_{1,0,1} & c^{(1)}_{0,1,1} & c^{(1)}_{0,0,2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c^{(1)}_{2,0,0} & 0 & 0 & c^{(1)}_{1,1,0} & c^{(1)}_{0,2,0} & 0 & 0 & c^{(1)}_{1,0,1} & c^{(1)}_{0,1,1} & c^{(1)}_{0,0,2} & 0 & 0 \\ 0 & 0 & 0 & 0 & c^{(1)}_{2,0,0} & 0 & 0 & c^{(1)}_{1,1,0} & c^{(1)}_{0,2,0} & 0 & 0 & c^{(1)}_{1,0,1} & c^{(1)}_{0,1,1} & c^{(1)}_{0,0,2} & 0 \\ 0 & 0 & 0 & 0 & 0 & c^{(1)}_{2,0,0} & 0 & 0 & c^{(1)}_{1,1,0} & c^{(1)}_{0,2,0} & 0 & 0 & c^{(1)}_{1,0,1} & c^{(1)}_{0,1,1} & c^{(1)}_{0,0,2} \\ 0 & c^{(2)}_{2,0,0} & 0 & c^{(2)}_{1,1,0} & c^{(2)}_{0,2,0} & 0 & c^{(2)}_{1,0,1} & c^{(2)}_{0,1,1} & c^{(2)}_{0,0,2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & c^{(2)}_{2,0,0} & 0 & c^{(2)}_{1,1,0} & c^{(2)}_{0,2,0} & 0 & c^{(2)}_{1,0,1} & c^{(2)}_{0,1,1} & c^{(2)}_{0,0,2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c^{(2)}_{2,0,0} & 0 & 0 & c^{(2)}_{1,1,0} & c^{(2)}_{0,2,0} & 0 & 0 & c^{(2)}_{1,0,1} & c^{(2)}_{0,1,1} & c^{(2)}_{0,0,2} & 0 & 0 \\ 0 & 0 & 0 & 0 & c^{(2)}_{2,0,0} & 0 & 0 & c^{(2)}_{1,1,0} & c^{(2)}_{0,2,0} & 0 & 0 & c^{(2)}_{1,0,1} & c^{(2)}_{0,1,1} & c^{(2)}_{0,0,2} & 0 \\ 0 & 0 & 0 & 0 & 0 & c^{(2)}_{2,0,0} & 0 & 0 & c^{(2)}_{1,1,0} & c^{(2)}_{0,2,0} & 0 & 0 & c^{(2)}_{1,0,1} & c^{(2)}_{0,1,1} & c^{(2)}_{0,0,2} \\ 0 & c^{(3)}_{2,0,0} & 0 & c^{(3)}_{1,1,0} & c^{(3)}_{0,2,0} & 0 & c^{(3)}_{1,0,1} & c^{(3)}_{0,1,1} & c^{(3)}_{0,0,2} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & c^{(3)}_{2,0,0} & 0 & c^{(3)}_{1,1,0} & c^{(3)}_{0,2,0} & 0 & c^{(3)}_{1,0,1} & c^{(3)}_{0,1,1} & c^{(3)}_{0,0,2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c^{(3)}_{2,0,0} & 0 & 0 & c^{(3)}_{1,1,0} & c^{(3)}_{0,2,0} & 0 & 0 & c^{(3)}_{1,0,1} & c^{(3)}_{0,1,1} & c^{(3)}_{0,0,2} & 0 \\ 0 & 0 & 0 & 0 & 0 & c^{(3)}_{2,0,0} & 0 & 0 & c^{(3)}_{1,1,0} & c^{(3)}_{0,2,0} & 0 & 0 & c^{(3)}_{1,0,1} & c^{(3)}_{0,1,1} & c^{(3)}_{0,0,2} \end{pmatrix} \end{array}$$

The columns are indexed by all monomials of critical degree, ordered by lexicographic ordering on $k[x, y, z]$ with $x > y > z > 1$, and the rows are indexed by multiples of the input equations F_1, F_2 and F_3, also ordered by lexicographic ordering on $k[x, y, z]$. Finally, D_3 is the determinant of this matrix. To get the resultant R, it remains to compute D_1, D_2 and the greatest common divisor of D_1, D_2 and D_3, but we can also use the second method to compute the resultant.

$$M_0 = \begin{pmatrix} c^{(1)}_{2,0,0} & 0 & c^{(1)}_{0,0,2} \\ 0 & c^{(1)}_{2,0,0} & c^{(1)}_{1,0,1} \\ 0 & c^{(2)}_{2,0,0} & c^{(2)}_{1,0,1} \end{pmatrix}$$

Therefore, we have

$$D_3^0 = (c^{(1)}_{2,0,0})^2 c^{(2)}_{1,0,1} - c^{(2)}_{0,0,2} c^{(1)}_{1,0,1} c^{(1)}_{2,0,0}$$

and

$$R = \pm \frac{D_3}{D_3^0} \iff D_3 = \pm D_3^0 R = \pm((c^{(1)}_{2,0,0})^2 c^{(2)}_{1,0,1} - c^{(2)}_{0,0,2} c^{(1)}_{1,0,1} c^{(1)}_{2,0,0}) R.$$

More on resultants can be found in *Explicit Formulas for the Multivariate Resultant* [7], *Solving Polynomial Equations: Foundations, Algorithms, and Applications* [9], *The Algebraic Theory of Modular Systems* [19] and *Lessons Introductory to the Modern Higher Algebra* [24].

References

[1] William Adams and Philippe Loustaunau. *An Introduction to Gröbner Bases.* American Mathematical Society, USA, 1994.

[2] Daniel Allcock. *Hilbert's Nullstellensatz.* http://www.ma.utexas.edu/users/allcock/expos/nullstellensatz3.pdf, Austin, TX, USA, 2005.

[3] Aaron Bertram. *Math 6130 Notes.* http://www.math.utah.edu/ $\sim$ bertram/6030/Polys.pdf, Salt Lake City, UT, USA, 2002.

[4] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings.* PhD tesis, Innsbruck, Austria, 1965.

[5] Bruno Buchberger. *Gröbner Bases: A Short Introduction for Systems Theorists.* in Computer Aided Systems Theory - EUROCAST 2001, 2001.

[6] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics).* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[7] Carlos D'Andrea and Alicia Dickenstein. *Explicit Formulas for the Multivariate Resultant.* J. Pure Appl. Algebra:164(1-2):59-86, 2001. Effective methods in algebraic geometry, Bath, UK, 2000.

[8] Wolfram Decker and Christoph Lossen. *Computing in Algebraic Geometry: A Quick Start Using SINGULAR (Algorithms and Computation in Mathematics).* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[9] Alicia Dickenstein and Ioannis Emiris. *Solving Polynomial Equations: Foundations, Algorithms, and Applications.* Springer, 2005.

[10] Arturas Dubickas. *Two Exercises Concerning the Degree of the Product of Algebraic Numbers.* Publications de l'institut mathématique, nouvelle série, tome 77(91) (2005), 67–70, Vilnius, Lithuania, 2004.

[11] David Eisenbud. *Commutative Algebra : with a View toward Algebraic Geometry.* Graduate texts in mathematics. Springer-Verlag New York, Inc., Secaucus, NJ, USA.

[12] Karl Fink. *A Brief History of Mathematics.* Cosimo, Inc, New York, NY, USA, 2007.

[13] Ralf Fröberg. *An Introduction to Gröbner Bases, Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts.* John Wiley & Sons, Chichester, UK, 1997.

[14] Gert-Martin Greuel and Gerhard Pfister. *A Singular Introduction to Commutative Algebra.* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2nd edition, 2007.

[15] Robin Hartshorne. *Algebraic Geometry.* Graduate texts in mathematics. Springer Science+Business Media, Inc., New York, NY, USA.

[16] I.M. Isaacs. *Degrees of Sums in a Separable Field Extension.* Proc. Amer. Math. Soc. 25 (1970), 638-641, 1970.

[17] Martin Leslie. *Gröbner Bases.* http://math.arizona.edu/ mleslie/files/ GroebnerPaper.pdf, Tucson, AZ, USA, 2008.

[18] Anton Leykin. *Math 4803-Ley: Introduction to Algebraic Computation.* http://people.math.gatech.edu/ aleykin3/math4803spr13/BOOK/ chapter3.pdf, Atlanta, GA, USA, 2013.

[19] F.S. Macaulay. *The Algebraic Theory of Modular Systems.* Cambridge: University Press, UK, 1916.

[20] Hiromasa Nakayama. *Introduction of the Mora Division Algorithm in the Ring of Differential Operators D.* http://www.math.kobe-u.ac.jp/HOME/nakayama/ohp_dmodalgo_2007_9.pdf, Kobe, Japan, 2007.

[21] J. L. Rabinowitsch. *Zum Hilbertschen Nullstellensatz.* vol. 102, no. 1, p.520, Mathematische Annalen, 1930.

[22] Ziv Ran. *137 Notes, Part 4: Study's Lemma and Applications.* http://math.ucr.edu/ ziv/papers/137-4.pdf, Riverside, CA, USA, 2006.

[23] Marko Roczen. *Gröbner Bases and Resultants.* Manuscript of a talk in the School on Commutative Algebra and Combinatorics, University of Constantza, 1999.

[24] George Salmon. *Lessons Introductory to the Modern Higher Algebra.* Dublin Hodges, Foster, Dublin, Ireland, 1876.

[25] Karlheinz Spindler. *Abstract Algebra with Applications (in two volumes). Vol. II: Rings and fields.* Marcel Dekker, Inc., New York, NY, USA, 1994.

[26] Bernd Sturmfels. *Introduction to Resultants.* volume 53 of Proc. Sympos. Appl. Math., pages 25–39. Amer. Math. Soc., In Applications of computational algebraic geometry (San Diego, CA, 1997), 1998.

[27] Tristan Vaccon. *Gröbner Bases, Ideal Computation and Computational Invariant Theory.* http://perso.univ-rennes1.fr/tristan.vaccon/rapport2010.pdf, Rennes, France, 2010.

[28] Kevin Winkel. *Chern Classes.* Master thesis, Luxembourg, 2015.