Retraction Notice

Title of retracted article: **Solving Some Problems and Elimination in Systems of Polynomial Equations**

Authors: Moumouni Djassibo Woba
* Corresponding author. Email: moumouniabdoulwoba@gmail.com

Journal: American Journal of Computational Mathematics
Year: 2024
Volume: 14
Number: 3
Pages (from - to): 333 - 345
DOI (to PDF): https://doi.org/10.4236/ajcm.2024.143016
Paper ID at SCIRP: 1101112
Article page: https://www.scirp.org/journal/paperinformation?paperid=136113
Retraction date: 2025-11-28

Retraction initiative (multiple responses allowed; mark with **X**):
X All authors
☐ Some of the authors:
☐ Editor with hints from Journal owner (publisher)
Institution:
Reader:
Other:
Date initiative is launched: 2025-11-23

Retraction type (multiple responses allowed):
☐ Unreliable findings
Lab error Inconsistent data Analytical error Biased interpretation
Other:
☐ Irreproducible results
☐ Failure to disclose a major competing interest likely to influence interpretations or recommendations
☐ Unethical research

☐ Fraud
Data fabrication Fake publication Other:
Plagiarism ☐ Self plagiarism ☐ Overlap ☐ Redundant publication *
☐ Copyright infringement ☐ Other legal concern:

☐ Editorial reasons
Handling error Unreliable review(s) Decision error Other:

X Other:
The author's own decision.

Results of publication (only one response allowed):
☐ are still valid.
X were found to be overall invalid.

Author's conduct (only one response allowed):
☐ honest error
☐ academic misconduct
X none (not applicable in this case – e.g. in case of editorial reasons)

* Also called duplicate or repetitive publication. Definition: "Publishing or attempting to publish substantially the same work more than once."

History
Expression of Concern:
☐ yes, date: yyyy-mm-dd
X no

Correction:
☐ yes, date: yyyy-mm-dd
X no

Comment:
The paper is withdrawn because of the author's own decision.
This article has been retracted to straighten the academic record. In making this decision, the Editorial Board follows COPE's Retraction Guidelines.The aim is to promote the circulation of scientific research by offering an ideal research publication platform with due consideration of internationally accepted standards on publication ethics. The Editorial Board would like to extend its sincere apologies for any inconvenience this retraction may have caused.

Scientific Research Publishing

American Journal of Computational Mathematics, 2024, 14, 333-345
https://www.scirp.org/journal/ajcm
ISSN Online: 2161-1211
ISSN Print: 2161-1203

Solving Some Problems and Elimination in Systems of Polynomial Equations

Moumouni Djassibo Woba

Training and Research/Science and Technology Unit (UFR/ST), University of Ouahigouya, Ouahigouya, Burkina Faso
Email: moumouniabdoulwoba@gmail.com

How to cite this paper: Djassibo Woba, M. (2024) Solving Some Problems and Elimination in Systems of Polynomial Equations. *American Journal of Computational Mathematics*, **14**, 333-345.
https://doi.org/10.4236/ajcm.2024.143016

Received: August 16, 2024
Accepted: September 20, 2024
Published: September 23, 2024

Abstract

In a factorial ring, we can define the *p.g.c.d.* of two elements (defined to the nearest unit) and the notion of prime elements between them. More generally, Bezout's identity characterizes two prime elements in a main ring. A ring that satisfies the property of the theorem is called a Bezout ring. We have given some geometry theorems that can be proved algebraically, although the methods of geometry and, in particular, of projective geometry are by far the most beautiful. Most geometric problems actually involve polynomial equations and can be translated into the language of polynomial ideals. We have given a few examples of a different nature without pretending to make a general theory.

Keywords

Identity of Bezout, Ring of Bezout, Ideals, Polynomials, Common

1. Introduction

Polynomials are preferred tools used to solve problems such as the solvability of equations, constructability, and Fermat's last theorem [1].

This article is devoted to solving some problems and elimination in systems of polynomial equations. Let us give some examples of problems: solving a system of polynomial equations, finding its projection in different planes, and finding the Cartesian equation of a curve (or a surface) given by parametric equations.

The algebraic structures of rings and ideals play a large role and lead to algebraic geometry proper. We will see how to use the Bezout identity in $\mathbb{Z}[x]$ and $k[x,y]$ for these problems, then move on to the resultant and then discuss the Gröbner bases. In passing, we will see some geometry theorems that can be proved algebraically, although the methods of geometry and, in particular, of projective geometry are by far the most beautiful.

Remark

The pgcd of two or more integers is the largest integer that divides each of these numbers without leaving a remainder.

Example 1.1

For 12 and 18:

- The divisors of 12 are: 1, 2, 3, 4, 6, 12;
- The divisors of 18 are: 1, 2, 3, 6, 9 and 18;
- The common divisors: 1, 2, 3 and 6.

The pgcd (12, 18) = 6.

Definition

In a factor analysis, the main elements refer to the linear combinations of variables that best explain the variation in the data.

Elements are often used to reduce the dimensionality of the dataset while preserving as much information as possible.

Example 1.2

Let's say we have a dataset with three variables: X_1, X_2 and X_3.

Factor analysis can reveal that:

The first element (EP1) represents 70% of the total variable, and is influenced mainly by X_1, X_2.

The second main element (EP2) could then represent 20% and be more related to X_3.

This made it possible to represent the data with only two main elements, meaning analysis while retaining the essence of the information.

In short:

Bezout rings are of greater importance in both algebra and geometry, mainly due to their structure and special properties.

2. Algebra Complement

Let A be an integral unitary commutative ring. An invertible element of A for multiplication is called a unit of A.

Definition 2.1

We say that an ideal $I \neq A$ of A is *prime* if and only if A/I is an integral ring. In other words, if $ab \in I$, then a or b belongs to I.

Definition 2.2

An element a of A is said to be *irreducible* if it is not a unit and if it cannot be written in the form $a = bc$ with b and c as non-units.

If $a_1, \cdots, a_n$ are elements of A, we denote $(a_1, \cdots, a_n)$ or $(a_1, \cdots, a_n)A$ the ideal of A generated by the a_i. The a_i are called the *generating system or the basis of the ideal I*.

Proposition

If $I = (a)$ is a prime principal ideal, then a is irreducible.

Indeed, if a is not irreducible, we can write it in the form bc with b and c not units and we then have $b \notin I, c \notin I$ and $bc \in I$.

In $\mathbb{Z}$, the converse is true: if a is irreducible, the ideal of $\mathbb{Z}$ generated by a is prime. It is true more generally in factorial rings (we then speak of prime elements for irreducible) but false in general.

Definition 2.3

Let A be an integral ring. A is said to be a *factorial ring* if any element of A is written as the product of one unit and irreducible elements, and this is essentially unique: if $u\prod_{i\in I} p_i = v\prod_{j\in J} q_j$ with u and v units and irreducible p_i and q_j there exists a σ bijection of I over J such that $p_i = u_i q_{\sigma(i)}$ with u_i unit.

Theorem 2.1

If A is a factorial ring, the ring $A[x]$ of the polynomials in x with coefficients in A is factorial. Thus, if A is a field or a principal ring, the ring $A[x_1,\cdots,x_n]$ is a factorial ring.

In a factorial ring, we can define the *p.g.c.d.* of two elements (defined to the nearest unit) and the notion of prime elements between them.

When $A=k$ is a field, we have the Euclidean division in $k[x]$ and we can calculate the *p.g.c.d.* of two polynomials by Euclid's algorithm [2].

Theorem 2.2 (Bezout of Theorem)

If $A=k$ is a field and P and Q are two polynomials of $k[x]$, P and Q are prime to each other if and only if there are two polynomials U and V such that $UP+VQ=1$.

The conclusion of this theorem is false in $k[x,y]$. On the other hand, we can plunge $k[x,y]$ into $k(y)[x]$ where $k(y)$ is the field of fractions of $k(y)$. Note that the MAPLE commands reflect the fact that the *p.g.c.d.* exists in $k[x,y]$ (the gcd(P, Q) command does not make x or y play any particular role), but that the use of Euclid's algorithm requires specifying a variable: gcdex(P, Q, x, "u", "v").

Let's give an example of a non-factorial ring. The ring $\mathbb{Z}[\sqrt{-5}]$ is not factorial because $6=2\times 3=(1+\sqrt{-5})(1-\sqrt{-5})$ and the elements $1+\sqrt{-5}$ and 2 as well as $1+\sqrt{-5}$ and 3 do not differ by one unit. Thus, the idea $I=(2)\mathbb{Z}[\sqrt{-5}]$ is not prime because $(1+\sqrt{-5})(1-\sqrt{-5})\in I$ and $1+\sqrt{-5}\notin I$, $1-\sqrt{-5}\notin I$. On the other hand, 2 is irreducible, because it cannot be written as the product of two non-unit elements of $\mathbb{Z}[\sqrt{-5}]$ (we would then have $2=(a+b\sqrt{-5})(c+d\sqrt{-5})$ with $a^2+5b^2\neq 1$ and $c^2+5d^2\neq 1$, hence $4=(a^2+5b^2)(c^2+5d^2)$; for example $2=a^2+5b^2$, which is not possible).

3. Properties of Bezout Rings

A Bezout ring is an integral ring in which both nonzero elements have a PGCD that can be expressed as a linear combination of these elements.

Example

1) Existence of PGCD: for any pair of elements a and b, there are elements x and y such that $d=\mathrm{PGCD}(a,b)=ax+by$.

2) Integrity: A Bezout ring is an integral ring, which means that it has no null elements other than 0.

3) Relationship to ideals: Ideals generated by elements in a Bezout ring are principal, meaning they can be written in the form (a) or a.

Relevance in algèbre

Bezout rings are fundamental in the study of Diophantine equations, polynomials and modules. Their structure facilitates the solution of linear equations and their analysis.

For example, in $\mathbb{Z}$ (integers), each element can be decomposed into prime factors, which is essential for decomposition theorems.

Algebraics applications

Solving equations: methods using GCDPs are used to solve systems of equations.

Factorization theorem: by understanding how to decompose polynomials, we can better manipulate and solve equations.

Connection to geometry

Bezout rings also have geometric applications, especially in the context of algebraic geometry:

- Algebraic surface: In polynomial-defined surfaces, the intersections of these surfaces can often be analyzed through the ideals generated by the polynomials. This achieves a nice connection with projective spaces where solutions can be interpreted geometrically.
- Bezout's theorem: It states that for two projective manifolds in a projective space, the number of points of intersection of these manifolds is given by the product of their degrees counting the sure multiplicities. This perfectly illustrates the link between the algebraic properties of a Bezout ring and their geometric implications.

Geometrics applications

- Characterization of curves: the behavior of curves in projective spaces can be studied from their equations in Bezout rings.
- Intersection analysis: through algebraic considerations, one can predict and understand how different geometric shapes interact with each other.

Conclusion: Bezout rings are central structures in algebra which, by their properties, directly influence geometric analysis in the framework of algebraic geometry. Their use makes it possible to navigate between pure algebra and geometric applications, thus facilitating.

The connection between geometry theorems and the algebraic framework

The connection between theorems is fundamental in algebraic geometry. A discipline that establishes deep links between geometry and algebras. Here are some key points illustrating this relationship:

1) Algebraic varieties

- Definition: An algebraic manifold is the set of solutions of a system of polynomial equations. Each manifold can be described by ideals in a ring of pol-

ynomials.

- Theorem: Theorems such as Hilbert's Theorem, which links the ideal of polynomials to the points of the manifold, show the geometric properties of the polynomials.

2) Correspondence between ideals and subset

- Ideals and points: each ideal in a ring of polynomials can correspond to a manifold, creating a duality between algebraic (ideal) and geometry (manifold) objects).
- Nullstellensatz's theorem: This theorem establishes a key connection by stating that ideals define sets of points, and conversely, sets of points can be expressed by ideals.

3) Functions and morphisms

- Morphisms: functions defined on algebraic manifolds can be interpreted as morphisms between manifolds, linking algebraic structures.
- Correspondence theorem: Theorems such as Zaiski's theorem provide correspondences between morphisms of algebraic spaces and their geometric properties.

4. Manipulation of Polynomials

The commands for manipulating polynomials are, among others: collect, expand, sort, normal, coeff.

Example

By $P = x^2 + bx + c$ or $x^3 + px + q$, calculate the g.c.c.d. of P and P'. Then use the gcdex command. Similarly, let $P = x^5 + 2ax^4 + x^3 - ax^2 - 2a^2x - a$. Factorize P (by the way, redevelop and check that you have ordered in order of descending monomials of the form $a_i x^i$). For each factor, do the irreductive test. Then do $a = 1$ and start again. Thus, MAPLE factors this last polynomial in the field $\mathbb{Q}(a, x)$ of the rational fractions in a and x or in $\mathbb{Z}[a, x]$, *i.e.* by considering a as an "indeterminate". And this factorization is different from that of $\rho_1(P)$ in $\mathbb{Z}[x]$, where ρ_1 is the evaluation homomorphism $\mathbb{Z}[a, x] \to \mathbb{Z}[x]$ that sends a over 1.

5. Identity of Bezout

The Bezout identity is a result of arithmetic which says that the *p.g.c.d.* of two integers a and b can be expressed in the form $au + bv$ with u and v integers.

Theorem

Let A and B be two polynomials of $\mathbb{K}[X]$. Then A and B are prime to each other if and only if there are two polynomials U and V such that $AU + BV = 1$ [3].

More generally, Bezout's identity characterizes two prime elements in a main ring. A ring that verifies the property of the theorem is called a **Bezout ring**.

Example

1) Calculate the *p.g.c.d.* of $P = 3x^2 + 5x + 7$ and $Q = x^2 + 2x + 1$.

2) Calculate polynomials U and V such that $UP+VQ=1$. Using the result obtained, find an integer n and polynomials U_0 and V_0 with coefficients in $\mathbb{Z}$ such that: $U_0P+V_0Q=n$ and such that n, the content $c(U_0)$ of U_0 and the content $c(V_0)$ of V_0 are prime to each other as a whole (we even have $\deg U_0 < \deg Q$ and $\deg V_0 < \deg P$). In a ring with a theory of the *p.g.c.d.* (e.g. a factorial ring), the content of a polynomial with coefficients in A is the *p.g.c.d.* of its coefficients (see in MAPLE, the content and primpart commands). The integer $n=n(P,Q)$ has the following property: if p is a prime number, p divides $n(P,Q)$ if and only if the polynomials P and Q are not prime to each other in $\mathbb{Z}/_p\mathbb{Z}$.

6. Resulting

The MAPLE command to calculate the resultant of two polynomials is the result.

Let A be an integral ring. If n is an integer, we denote $A[x]_n$ the A-module of polynomials of *degre* < *n*. It is therefore a free A-module of rank *n*. We can define the resultant in one of the following ways:

1) For any pair of polynomials (P,Q) of $A[x]$, there exists a single element $Res(P,Q)$ of A verifying

a) $Res(Q,P)=(-1)^{\deg(P)\deg(Q)}Res(P,Q)$;

b) If $0<\deg(P)\le\deg(Q)$, if R is the remainder of the Euclidean division of Q by P and if $d(P)$ is the dominant coefficient of P,
$Res(P,Q)=d(P)^{\deg(Q)-\deg(P)+1}Res(P,R)$;

c) Si $Q=a\in\mathbb{Z}$, $Res(P,a)=a^{\deg(P)}$ (in particular, $Res(0,a)=0$, $Res(b,a)=1$ if a and $b\in\mathbb{Z}-\{0\}$).

2) The resultant of P and Q is the determinant of the linear map $(U,V)\mapsto UP+VQ=R$ of $A[x]_n\times A[x]_m$ in $A[x]_{m+n}$ in the bases

$$\left(x^{n-1},0\right),\cdots,(1,0),\left(0,x^{n-1}\right),\cdots,(0,1)$$

and $\left(x^{m+n-1},\cdots,1\right)$, $m=\deg P$ and $n=\deg Q$.

Example 6.1

By $P=\sum_{i=0}^{6}a_ix^i$ and $Q=\sum_{i=0}^{6}b_ix^i$ of degree 9, it is the determinant of the matrix called the Sylvester matrix (or its transpose). Definition I closely follows Euclid's algorithm; it gives an algorithm to calculate the resultant, and at the same time the unit; it is quite easy to show that definition I verifies properties II.

Proposition 6.1

If P and Q are two polynomials of degree > 0, there are polynomials you and V in A[x] with deg U < deg Q and deg V < deg P such that UP + VQ = Res(P, Q).

Proof 6.1

If M is a matrix of order r with a coefficient in A, we have the relation $det(M)Id=MN$ where N is the transpose of the comatrice of M. This implies in particular that for any element v of A^r, $detM\cdot v$ belongs to the image of

A^r by *M*. In particular, here, the polynomial *Res*(*P*, *Q*). 1 belongs to the image of the linear map $(U,V)\mapsto UP+VQ$, which is the statement of the proposition.

Proposition 6.2

If A is a factorial ring, and if P and Q are of degree > 0, *P and Q have a common factor of degree* ≥ 1 *if and only if* $Res(P,Q)=0$.

Proof 6.2

We start by proving that P and Q have a common factor of *degree* ≥ 1 if and only if there are polynomials U and V in $A[x]$ both of which are not zero, such as $\deg U<\deg Q$, $\deg V<\deg P$ and $UP+VQ=0$. Let us show the sufficient condition. We have $UP=-VQ$.

Since A is factorial, any irreducible factor of P divides VQ. Since the degree of V is strictly lower than that of P, one of the irreducible factors of P necessarily divides Q.

It is then easy to see that the existence of U and V is equivalent to the nullity of the determinant of the Sylvester matrix. We leave the reciprocal to the reader.

Corollary

Let k be an algebraically closed field and P and Q two polynomials of $k[x]$ of *degree* > 0. Then $Res(P,Q)=0$ if and only if P and Q have a common root [4].

In the case of a polynomial of $\mathbb{Z}[x]$, these results applied to $\mathbb{Z}/_p\mathbb{Z}$ for p prime number imply the following proposition:

Proposition 6.3

When $\deg(P \bmod p)=\deg P>0$ and $\deg(Q \bmod p)=\deg Q>0$, p divides $Res(P,Q)$ if and only if P and Q have a common factor in $\mathbb{Z}/_p\mathbb{Z}[x]$.

In the case of several variables in the following way, we have the following results:

Theorem

Let P and $Q\in k[x_1,\cdots,x_n]$ *of degree* ≥ 1 *in* x_1. *Then* $Res_{x_1}(P,Q)=0$ *if and only if P and Q have a common factor in* $k[x_1,\cdots,x_n]$ *which is of degree* ≥ 1 *in* x_1.

Bearing theorem

Suppose that k algebraically closed. Let P and Q be two polynomials of $k[x_1,\cdots,x_n]$ of *degree* ≥ 1 in x_1 and let $a\in k[x_2,\cdots,x_n]$ (resp. $b\in k[x_2,\cdots,x_n]$) be the dominant term of P (resp. Q) as the polynomial in x_1. Let $(c_2,\cdots,c_n)\in k^{n-1}$ such that $Res_{x_1}(P,Q)(c_2,\cdots,c_n)=0$.

We also assume $a(c_2,\cdots,c_n)\neq 0$ or $b(c_2,\cdots,c_n)\neq 0$. Then there exists $c_1\in k$ such that $P(c_1,\cdots,c_n)=0$ and $Q(c_1,\cdots,c_n)=0$ [5].

General definition

If $I=(f_1,\cdots,f_s)$ is an ideal of $k[x_1,\cdots,x_n]$, *we call the affine manifold defined* by I or by $(f_1,\cdots,f_s)$ the set of common zeros of all the elements of I, or, which amounts to the same thing, of $f_1,\cdots,f_s$:

$$V(I)=\left\{(a_1,\cdots,a_n)\in k^n,\ f_i(a_1,\cdots,a_n)=0\ \forall i=1,\cdots,s\right\}$$

Definition 6.1

If S is a set of points of k^n, we define $I(S)$ as the ideal of polynomials cancelling over S; let $S^{alg} = V(I(S))$ be the smallest affine variety containing S.

The problems of elimination and rehabilitation can now be posed in a more general way.

Definition 6.2

If S is a set of points of k^n, we define $I(S)$ as the ideal of polynomials cancelling over S; let $S^{alg} = V(I(S))$ be the smallest affine variety containing S.

Definition 6.3

Let I be an ideal of $k[x_1,\cdots,x_n]$. *The ideal of elimination of I with respect to the idea* $x_1,\cdots,x_n$ the ideal $I \cap k[x_1,\cdots,x_n]$ of $k[x_{1+k},\cdots,x_n]$.

To eliminate is a way to "triangularize" the system of polynomial equations in order to solve it. Starting from an ideal $I = (P_1,\cdots,P_s)$ of $k[x_1,\cdots,x_n]$, we eliminate x_1 in I and thus obtain an ideal I_1 of $k[x_2,\cdots,x_n]$, then eliminate x_2 in I_1 and obtain an ideal I_2 of $k[x_3,\cdots,x_n]$. This is exactly what we do when we triangulate a linear system of equations to solve it. This way of posing the problem implies an order on the $x_1,\cdots,x_n$.

NB. It is very important to give oneself an order on the monomials of $k[x_1,\cdots,x_n]$.

To calculate $V(I)$, we can therefore calculate $V(I_{n-1})$ and if it is non-empty, calculate $V(I_{n-2})$, *i.e.* find for $a_n \in V(I_{n-1})$ if there exists a_{n-1} such that $(a_{n-1},a_n) \in V(I_{n-1})$, and start again. It is a problem of recovery.

By the way, the simplest problem of elimination is the following:

Solve the system

$$\begin{cases} x+y=s \\ xy=p \end{cases}$$

where p and s are constants. Calculate the resultant of the two polynomials $P = xy - p$ and $S = x + y - s$ with respect to x. We find $R = y^2 - sy + p$.

Thus, if (x,y) is a solution of the system, y necessarily satisfies the equation $y^2 - sy + p$.

We will now look at other situations where this elimination problem occurs naturally.

7. Parametric Equations

Let S of points $(x_1,\cdots,x_n)$ of k^n given by parametric equations:

$$\begin{cases} x_1 = g_1(t_1,\cdots,t_m) \\ x_2 = g_1(t_1,\cdots,t_m) \\ \vdots \\ x_n = g_n(t_1,\cdots,t_m) \end{cases} \quad (1)$$

where the g_j are polynomials in the parameters $t_1,\cdots,t_m$. Either

$$J = (x_1 - g_1,\cdots,x_n - g_n) \quad (2)$$

The ideal of $k[t_1,\cdots,t_m,x_1,\cdots,x_n]$. Let $I \subset k[x_1,\cdots,x_n]$ be the ideal elimination of I with respect to $t_1,\cdots,t_m$, *i.e.* $I = J \cap k[x_1,\cdots,x_n]$. It is shown that

$$S^{alg} = V(I) \tag{3}$$

Thus, if the ideal I admit as a basis $f_1,\cdots,f_s$, a system of Cartesian equations for S^{alg} is given by

$$\begin{cases} f_1(x_1,\cdots,x_n)=0 \\ \quad\vdots \\ f_s(x_1,\cdots,x_n)=0 \end{cases} \tag{4}$$

Calculating the difference between S and S^{alg} is a bearing problem (we of course $S \subset S^{alg}$).

If we replace the g_i with rational fractions g_i/h_i, the ideals to be considered are $J = (h_1x_1 - g_1,\cdots,h_nx_n - g_1,1-hy) \subset k[y,t_1,\cdots t_m,x_1,\cdots,x_n]$ and $I = J \cap k[x_1,\cdots,x_n]$ where $h = \prod_i h_i$ (the last condition allows the zeros to be eliminated from the denominators h_i).

8. Extrema Related

Another example where the elimination problem naturally occurs is that of bound extrema. Let's give an example:

Consider the sphere of $\mathbb{R}^3 : x^2+y^2+z^2=1$ and f the function $f(x,y,z) = x^2 2xy - z^2$. We want to find the extrema of f on the sphere. Let's put $g = x^2 + y^2 + z^2 - 1$.

The Lagrange method says to find them among the points $M=(x,y,z)$ such that $g(M)=0$ and such that there exists λ such that $grad(f)_M = \lambda grad(g)_M$. We then obtain 4 polynomial equations in x,y,z. Do it and find the extrema of g on the sphere.

9. Two Geometric Problems

Most geometric problems actually involve polynomial equations and can be translated into the language of polynomial ideals. We will give a few examples of a different nature without pretending to make a general theory.

Pappus theorem

Let $\{P_i\}_{1\le i\le 3}$ and $\{Q_i\}_{1\le i\le 3}$ be two distinct families of aligned points. We denote M_i by $i=1,2,3$ the intersection of the lines $(P_{i+1}Q_{i+2})$ and $(P_{i+2}Q_{i+1})$ (with the convention that $P_{i+3}=P_i$, $Q_{i+3}=Q_i$). Then the three M_1,M_2 and M_3 are aligned.

Let us express P_3 (resp. Q_3) as the barycenter of the points P_1 and P_2 (resp. Q_1 and Q_2) with parameter t_1 (resp. t_2). We can choose $P_1=(0,0)$ and $P_2=(0,2)$.

We will give two algebraic proofs of this theorem (although the geometrical ones are much prettier). In any case, don't forget to use the normal command.

1) First method: explicitly calculate the coordinates of M_i points and directly verify that they are aligned: we can make intermediate procedures calculating

the equation of the line passing through two points, the intersection of two lines, testing whether three points are aligned.

2) Second method: make an aligned procedure that takes as argument three lists *P*, *Q*, *R* of two elements (which corresponds to three points of the plane) that returns the polynomial condition so that these points are aligned; then write the polynomial expressions reflecting the fact that $M_i=[x_i,y_i]$ belongs to the line $(P_{i+1}Q_{i+2})$, then to the line $(P_{i+2}Q_{i+1})$. This gives us six polynomials f_j. Write the polynomial condition *g* reflecting the fact that the points M_i are aligned. Calculate a Gröbner basis *G* of the ideal generated by $L=[f_1,\cdots,f_6]$ with $X=[t_1,t_2,x_1,x_2,x_3,y_1,y_2,y_3]$ and verify that g belongs to this ideal using *normalf*.

The equation of two lines is of the form $(ax+by+c)(a'x+b'y+c')=0$, so it is an equation in *x* and *y* of total degree 2. Thus, the set formed by two straight lines in a plane is a degenerate conic (curve of equation a polynomial C in *x* and *y* of total degree 2) (the polynomial C is not irreducible).

Pascal's theorem generalizes Pappus' theorem to a non-degenerate conic, *i.e.* having an irreducible equation of degree 2.

Pascal's theorem

Let $\{P_i\}_{1\le i\le 3}$ and $\{Q_i\}_{1\le i\le 3}$ be six distinct points of a non-degenerate conic. For. By $i=1,2,3$, we denote M_i the intersection of the lines $(P_{i+1}Q_{i+2})$ and $(P_{i+2}Q_{i+1})$. Then the three points M_1,M_2 and M_3 are aligned. (We always make the convention that $P_{i+3}=P_i$, $Q_{i+3}=Q_i$).

To prove this theorem, we give ourselves five points of the plane P_1,P_2,P_3, Q_1,Q_2 and we choose the coordinate system appropriately.

The M_3 is the intersection of the lines (P_1Q_2) and (P_2Q_1). We take an arbitrary point M_1 of the line (P_3Q_2) in the form of the barycenter of P_3 and Q_2 with the points *t* and $1-t$. The lines (M_1M_3) and (P_3Q_1) intersect M_2. The lines (P_1M_2) and (P_2M_1) intersect *Q*. Determine the *x* and *y* coordinates of *Q* as a function of *t*, u_i and v_i (these are rational fractions with integer coefficients in these variables). This gives parametric equations $x=f_1(t)/g_1(t)$ and $x=f_2(t)/g_2(t)$. Eliminate *t* using the resultant of $g_1(t)x-f_1(t)$ and $g_2(t)x-f_2(t)$ with respect to *t*. We deduce that the point *Q* runs through a conic.

10. A Look Back at the Elimination and the Basics of Gröbner

The Gröbner bases and the algorithms for calculating them were introduced around 1965 by Bruno Buchberger and intensively developed to date. The full force of these techniques, which are as we can see very recent, is highlighted with the development of formal calculus.

We will give some very rudimentary notions about the Gröbner bases. An excellent reference is [Cox, Little, O'Schea]. We set $k[\underline{x}]=k[x_1,\cdots,x_n]$ and if $\alpha=(\alpha_1,\cdots,\alpha_n)$, $\underline{x}^{\alpha}=\prod_{i=1}^{n}x_i^{\alpha_i}$.

Definition 10.1

A monomial order on $k[x_1,\cdots,x_n]$ is a total order relation on $\mathbb{N}^n$ or equivalently on the monomials: $\underline{x}^{\alpha}$ by $\alpha\in\mathbb{N}^n$ such that:

1) If α,β and $\gamma\in\mathbb{N}^n$ and if $\alpha>\beta$, then $\alpha+\gamma>\beta+\gamma$;

2) Any non-empty subset of $\mathbb{N}^n$ has a smaller element. We write: $\underline{x}^{\alpha}>\underline{x}^{\beta}$ and si $\alpha>\beta$.

Example

1) Lexicographic order $\alpha>\beta$ if only if the first non-zero coordinate of $\alpha-\beta\in\mathbb{Z}^n$ is positive. Thus, $x_1>x_2>\cdots>x_n$ and $x_1^2x_3>x_1x_4$.

2) Graduated inverse lexicographic order: $\alpha>\beta$ if only if $|\alpha|>|\beta|$ and $|\alpha|=|\beta|$ and the last non-zero coordinate of $\alpha-\beta$ is strictly negative. Here, $|\alpha|$ is the sum of the coordinates of α. Thus, $|\alpha|$ is the sum of the coordinates of α. Thus, $x_1>x_2>\cdots>x_n$, $x_1^4x_2^2<x_1^5x_2$, $x_1^2x_2^3>x_1^3x_2x_3$.

3) Lexdeg order: This order depends on two lists of variables $[x_1,\cdots,x_p]$ and $[y_1,\cdots,y_r]$. The monomials containing only the x_i or only y_j are compared using the graduated inverse lexicographic order, then: $\underline{x}^{\alpha}\underline{y}^{\beta}>\underline{x}^{\gamma}\underline{y}^{\delta}$ if and only if $\underline{x}^{\alpha}>\underline{x}^{\gamma}$ or if $\underline{x}^{\alpha}=\underline{x}^{\gamma}$ and $\underline{y}^{\beta}>\underline{y}^{\delta}$. Thus, a monomial containing a x_i is larger than a monomial containing only y_j.

Check that it is indeed a monomial order. There are other possible orders. The three orders listed are available in MAPLE as plex, tdeg, and lexdeg.

Once an order has been chosen, we can speak of the dominant coefficient, the dominant monomial, the dominant term $LT(f)$ of a polynomial f: the MAPLE leadmon command gives a list formed by the dominant coefficient and the dominant monomial; The dominant term is then obtained using cover (, "*").

Definition 10.2

Let I be an ideal of $k(\underline{x}]$. We denote $(LT(I))$ the ideal of $k(\underline{x}]$ generated by the dominant terms of the elements of I.

Definition 10.3

A finite subset $G=\{g_1,\cdots,g_r\}$ of an ideal I is called the *Gröbner* basis $(LT(I))=(LT(g_1),\cdots,LT(g_r))$.

Theorem 10.1

Any Gröbner basis of an ideal I relative to a monomial order is a basis of I, *i.e.* $I=\{g_1,\cdots,g_r\}$. Every ideal I admits a Gröbner basis.

Definition 10.4

Let $I=(f_1,\cdots,f_s)$ be an ideal of $k(\underline{x}]$. The k-th ideal of elimination I_k of I is called the ideal $I\cap k[x_{k+1},\cdots,x_n]$ of $k[x_{k+1},\cdots,x_n]$.

Elimination theorem

Let I be an ideal of $k(\underline{x}]$ and G a Gröbner basis relative to the lexicographic order $x_1>x_2>\cdots>x_n$. Then, $G_k\cap k[x_{k+1},\cdots,x_n]$ is a basis of the ideal I_k [6].

Bearing theorem

We assume that k is algebraically closed. Let $I=(f_1,\cdots,f_s)\in k(\underline{x}]$ and I_1 be the first ideal for elimination of I. Let $g_i(x_2,\cdots,x_n)$ be the highest coefficient in x_1 of f_i. If $(a_2,\cdots,a_n)$ is a partial solution in $V(I_1)$ that does not

belong to $V(g_1,\cdots,g_s)$, *then there exists* $a_1 \in$ such that $(a_1,\cdots,a_n)\in V(I)$.

Recall that $V(I)$ *is the set of* $(a_1,\cdots,a_n)\in k^n$ *such that* $f(a_1,\cdots,a_n)=0$ *for all* $f\in I$ [7].

To construct a Gröbner basis of an ideal and verify that a basis is a Gröbner basis, we use a Buchberger algorithm.

Gröbner's bases are also a way to test whether a polynomial is in an ideal. The MAPLE command is normalf.

Let us explain the principle: to do this, we need to introduce a generalization of the division to $k(\underline{x}]$ relative to the chosen order.

Theorem 10.2

Let $(f_1,\cdots,f_s)$ *be polynomials of* $k(\underline{x}]$ *with a monomial order. Any polynomial* $f\in k(\underline{x}]$ *can be written as*

$$f=a_1f_1+\cdots+a_sf_s+r \tag{5}$$

where r is a linear combination of monomials not divisible by any of the dominant terms of the f_i [8].

Proposition

Let $G=(g_1,\cdots,g_s)$ be a Gröbner base of an ideal I and let $f\in k(\underline{x}]$. There is an $r\in k(\underline{x}]$ vérifying:

1) None of the monomials of r is divisible by one of the $LT(g_i)$;

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

We say that r is the remainder of the division of f by G.

Corollary

Let G be a Gröbner basis of an ideal I and $f\in k(\underline{x}]$. Then, f belongs to I if and only if the remainder of the division of f by G is zero.

11. Conclusions

Gröbner's bases are also a way to test whether a polynomial is in an ideal. The MAPLE command is normal. We have given some very rudimentary notions relating to the Gröbner bases.

We have explained the principle; for this, we need to introduce a generalization of the division to $k(\underline{x}]$ relative to the chosen order.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Boveresse, J., Itard, J. and Sallé, E. (1948) Histoire des mathématiques. Rééd. Sous le titre Algebra (2 Vol.), Springer, 1231.

[2] Perrin, D. (1996) Cours d'Algèbre. Ellipses, 127.

[3] Huche Corne, B. (1992) Biographie des grands théorèmes. Ellipses, 119.

[4] Cox, D.A., Little, J. and O'Schea, D. (1992) Ideals, Varieties, and Algorithms. Springer, 182. https://doi.org/10.1007/978-1-4757-2181-2

[5] Samuel, P. (1986) Géométrie Projective. P.U.F., 621.

[6] van der Waerden, B.L. (1930-1931) Moderne Algebra. 2 Vol. Springer. https://doi.org/10.1007/978-3-662-42016-4

[7] Walker, R.J. (1978) Algebraic Curves. 2nd Edition, Springer, 432.

[8] Samuel, P. (1970) Théorie algébrique des nombres. Hermann, 182.