UtilitasMathematica

ISSN 0315-3681 Volume 122, 2025

Between algebra and geometry: Solving systems of polynomial équations

Moumouni DJASSIB0 WOBA[1]

Université Lédéa Bernard OUEDRAOGO

moumouniabdoulwoba@gmail.com

(Burkina Faso)

ZONGO Moumouni[2],

Université Norbert ZONGO, (B.F),

z.moumine2012@gmail.com

ZOUNGRANA Amidou[3]

Universite Norbert ZONGO (BURKINA FASO)

amidzoung@gmail.com

Received: 02-May-2025 **Accepted:** 11-August-2025 **Published:** 29-August-2025

Abstract:

In the realm of factorial rings, we introduce the concept of the greatest common divisor (g.c.d.) for two elements, defined up to a unit, alongside the notion of prime elements. More broadly, Bézout's identity allows us to characterize pairs of prime elements within a principal ring, leading us to define these rings as Bézout rings.

Additionally, we delve into several geometric theorems that can be proven through algebraic methods, though the elegance of geometric approaches—especially in projective geometry—remains unparalleled. It is intriguing to note that many geometric challenges can be recast as polynomial equations, permitting us to frame them in terms of polynomial ideals. We present a variety of examples that highlight this connection, without attempting to construct an overarching theory.

Keywords : geometric ; greatest common divisor ; ideals ; polynomials ; common.

.

1. Introduction

Polynomials are indispensable instruments in the mathematical toolkit, adept at addressing a range of challenges

from determining the solvability of equations to exploring constructibility and proving Fermat's last theorem. [2]

This article is dedicated to unraveling various issues related to the elimination of variables in systems of polynomial equations. To illustrate our exploration, we provide several examples, including : solving a system of polynomial equations, discovering its projections onto different planes, and deriving the Cartesian equation of a curve or surface defined 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.

2. Algebra complements

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 $a_1, \dots, a_n$ are elements of A, we denote $(a_1, \dots, a_n)$ or $(a_1, \dots, a_n)\ A$ 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 2.3

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 2.4

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 2.5

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 $A[x_1, \dots, x_n]$ 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 2.6 (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. 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 irreducer test. Then do $a = 1$ and start again. Thus, MAPLE factores 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 $\mathbb{Z}[a, x] \longrightarrow \mathbb{Z}[x]$ that sends a over 1.

3.1 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 3.2

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

a) Calculate the p.g.c.d. of $P = 3x^2 + 5x + 7 \; and \; Q = x^2 + 2x + 1$.
b) 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 $degU_0 < degQ$ et $egV_0 < degP$). 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 $\mathbb{Z}/_{p}\mathbb{Z}$.

4. Resulting

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

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:

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

1. $Res(Q,P) = (-1)^{\deg(P)\deg(Q)} Res(P,Q)$;
2. If $0 < \deg(P) \leq \deg(Q)$, if R is the remainder of the Euclidean division of Q by P and if $d(P)$ is the dominant coefficient of P, $Res(P,Q) = d(P)^{dg(Q)-\deg(P)+1} Res(P,R)$;
3. 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 $b \in \mathbb{Z} - \{0\}$).

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

$$(x^{n-1},0), \dots, (1,0), (0,x^{n-1}), \dots, (0,1))$$

and $(x^{m+n-1}, \dots, 1)$ où $m = degP$ et $n = degQ$

Proposition 4.1

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

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, $det\ M.v$ 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 $(U,V) \longmapsto UP + VQ$, which is the statement of the proposition.

Proposition 4.2

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

Proof

We start by proving that P and Q have a common factor of $degree \geq 1$ 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 4.3

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:

$= deg\, Q > 0, p$ 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 4.4

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

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

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

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

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

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

Definition 4.5

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

To eliminate is in a way to "triangularize" the system of polynomial equations in order to solve it. Starting from an ideal $I = (P_1, \dots, P_r)$ of $k[x_1, \dots, x_n]$, we eliminate x_1 in I and thus obtain an ideal I_1 of $k[x_2, \dots, x_n]$, then eliminate x_2 in I_1 and obtain an ideal I_2 of $k[x_3, \dots, x_n]$. 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 $x_1, \dots, x_n$

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

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.

a. Paramétric equations

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

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

Where the g_j are polynomials in the parameters $t_1, \dots., t_m$. Either

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

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

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

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

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

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

$J = (h_1x_1 - g_1, \dots, h_nx_n - g_1, 1 - hy) \in$
$k[y, t_1, \dots., t_m, x_1, \dots., x_n]$ and

$I = J \cap \mathrm{k}[x_1, \dots., x_n]\ where\ h = \prod_i h_i$ (the last condition allows the zeros to be eliminated from the denominators h_i).

b. 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 fonction $f(x,y,z)=x^2 2xy-z^2$. We want to find the extrema of f on the sphere. Posons $g=x^2+y^2+z^2-1$.

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.

c. 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.

d. 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 $k[\underline{x}]=k[x_1,\dots,x_n]$ and if $\alpha=(\alpha_1,\dots,\alpha_n)$, $\underline{x}^{\alpha}=\prod_{i=1}^{n} x_i^{\alpha_i}$.

Definition 4.6

A monomial order on $k[x_1,\dots,x_n]$ 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:

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

ii) 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, |α| is the sum of the coordinates of

α. Thus, $|\alpha|$ is the sum of the coordinates of α. Thus, $x_1 > x_2 > \cdots > x_n$, $x_1^4 x_2^2 < x_1^5 x_2, x_1^2 x_2^3 > x_1^3 x_2 x_3$.

3. Lexdeg order: This order depends on two lists of variables $[x_1, .., x_p]$ and $[y_1, .., y_r]$. 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 4.7

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 4.8

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

Theorem 4.9

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

Definition 4.10

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

Elimination theorem 4.11

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

Bearing theorem 4.12

We assume that k is algebraically closed. Let $I = (f_1, \dots, f_s) \in k(\underline{x}]$ *and* I_1*be the first ideal for elimination of I. Let*

$g_i(x_2, \dots, x_n)$ be the highest coefficient in x_1 of f_i. If $(a_2, \dots, a_n)$ is a partial solution in $V(I_1)$ that does not belong to $V(g_1, \dots, g_s)$, then there exists $a_1 \in such\ that\ (a_1, \dots, a_n) \in V(I)$.

Recall that V(I) is the set of $(a_1, \dots, a_n) \in k^n$ such that $f(a_1, \dots, a_n) = 0$ 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 4.13

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

$$f = a_1 f_1 + \cdots + a_s f_s + r \qquad (5)$$

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

Proposition 4.14

Let $G = (g_1, \dots, g_s)$ 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 4.15

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.

Conclusion

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

Refrences

[1] Jacques Boveresse, Jean Itard et Emile Sallé, Histoire des mathématiques p.231

[2] D. Perrin, *cours d'algèbre*, Ellipses, Paris, 1996, p. 127

[3] Biographie *des grands théorèmes*, par X. Huchecorne, aux éditions Ellipses, p. 119.

[4] D.A. Cox, J. Little et D. O'Schea, *Ideals, Vaieties*, *and Algorithms,* UTM, Springer, Berlin, 1992, p. 182

[5] P. Samuel, *Géométrie projective*, P.U.F., Paris, 1986, p. 621

[6] B.L.van der Waerden, Moderne Algebra, 2 vol., Springer, 1930-1931, trad. Angl. Modern Algebra, Unga, New York, 1948. Rééd. Sous le titre Algebra (2 vol.), Springer, 1966-1967, trad. Angl. 1991, p. 1231.

[7] R. J. Walker, Algebraic curves, 2nd edition, Springer, Berlin, 1978, p. 432.

[8] P. Samuel, Théorie algébrique des nombres, Hermann, Paris, 1970, p. 182