GRÖBNER BASES AND APPLICATIONS **Subject presented by Clément Alleaume**

Institut Camille Jordan, Université Claude Bernard Lyon 1,
43, boulevard du 11 novembre 1918, 69622 Villeurbanne, France.
clement.alleaume@univ-st-etienne.fr

1. INTRODUCTION

Gröbner bases are a notion introduced by Buchberger in 1965 to describe ideals of commutative algebras. This notion generalizes both the Gaussian elimination algorithm for systems of polynomial equations and the division of polynomials in multiple indeterminates. In the case of systems of linear polynomial equations, Gröbner bases give the Gaussian elimination algorithm. In the case of the division, of a polynomial by a set of polynomials, the rest is not always unique. Gröbner bases can give us an algorithm making the rest unique. Gröbner bases can also be used to decide whether or not an element of a commutative algebra is in some ideal. Given I an ideal of the ring $\mathbb{K}[x_1, ..., x_n]$ of polynomials in n indeterminates, a Gröbner basis of I gives us an algorithm deciding whether or not an element of $\mathbb{K}[x_1, ..., x_n]$ is in I.

The objective of this proposal is to study Gröbner bases through multiple results and find applications of Gröbner bases to solve some families of problems. In the first part of this proposal, we will give some motivations to the introduction of Gröbner bases. In the second part, we will formalize the necessary notions to define Gröbner bases. We will then define Gröbner bases and give an algorithm to construct them: Buchberger's algorithm. We will finally give exercises which can be solved using this notion. In the end, we propose to prove two theorems. The first one is Hilbert basis theorem. This theorem of great importance in commutative algebra was proved by Hilbert in 1890 using a nonconstructive method. This theorem can constructively be proved using Gröbner bases. The second theorem to prove, Theorem 3.3.4 shows the link between Gröbner bases and rewriting, an abstract model of computation used to study calculus as a sequence of reduction rules.

2. MOTIVATIONS

2.1. Division of polynomials in multiple indeterminates

The objective is to define a division algorithm for polynomials in multiple indeterminates generalizing the division algorithm for polynomials in one indeterminate.

In $\mathbb{K}[x]$, the division of a polynomial f by g gives a decomposition of f of the form:

$$f = qg + r,$$

whith $\deg(r) < \deg(g)$.

The division of a polynomial f of $\mathbb{K}[x_1, \ldots, x_n]$ by a set of polynomials $\{f_1, \ldots, f_s\}$ of $\mathbb{K}[x_1, \ldots, x_n]$ gives a decomposition of f of the form:

$$f = u_1 f_1 + \ldots + u_s f_s + r,$$

where the *quotients* are the polynomials $u_1, \ldots, u_s$ of $\mathbb{K}[x_1, \ldots, x_n]$ and the *rest* is the polynomial r of $\mathbb{K}[x_1, \ldots, x_n]$.

The division algorithm of a polynomial in multiple indeterminates f by a set $\{f_1, \ldots, f_s\}$ of polynomials works similarly to the case with only one indeterminate:

1. fix an order on the terms (in the case with only one indeterminate, this order is given by the degree),

2. replace the leading term of f by multipliying a f_i by an appropriate term and substract the result from f ; this term is then a term of the quotient u_i,

3. do the same for all polynomials $f_1, \ldots, f_s$.

2.2. First example

Consider the polynomials $f = xy^2+1$, $f_1 = xy+1$ and $f_2 = y+1$ of $\mathbb{K}[x, y, z]$. We fix the lexicographical order associated to $x > y$. The leading term $lt(f) = xy^2$ can be divided by the leading terms $lt(f_1) = xy$ and $lt(f_2) = y$:

$$\begin{array}{r|l} xy^2 + 1 & xy + 1 \\ \hline xy^2 + y & y \\ \hline 1 - y & \end{array} \qquad \text{giving} \qquad xy^2 + 1 = (xy + 1)y + 1 - y.$$

$$\begin{array}{r|l} 1 - y & y + 1 \\ \hline -y - 1 & -1 \\ \hline 2 & \end{array} \qquad \text{giving} \qquad 1 - y = (y + 1)(-1) + 2.$$

Because $lt(f_1)$ and $lt(f_2)$ do not divide 2, this rest is irreducible. We made the two following reductions:

$$xy^2 + 1 \xrightarrow{f_1} 1 - y \xrightarrow{f_2} 2.$$

We write:

$$xy^2 + 1 \xrightarrow{\{f_1, f_2\}} 2.$$

Then, the polynomial f can be written:

$$xy^2 + 1 = y(xy + 1) + (-1)(y + 1) + 2.$$

If we begin by the reduction given by f_2, we obtain the following divisions:

$$\begin{array}{r|l} xy^2 + 1 & y + 1 \\ \hline xy^2 + xy & xy \\ \hline -xy + 1 & \end{array} \qquad \begin{array}{r|l} -xy + 1 & xy + 1 \\ \hline -xy - 1 & -1 \\ \hline 2 & \end{array}$$

Because $lt(f_1)$ and $lt(f_2)$ do not divide 2, this rest is irreducible. We made the two following reductions:

$$xy^2 + 1 \xrightarrow{f_2} -xy + 1 \xrightarrow{f_1} 2,$$

We write

$$xy^2 \xrightarrow{\{f_2, f_1\}} 2.$$

Then, the polynomial f can be written:

$$xy^2 + 1 = (-1)(xy + 1) + (xy)(y + 1) + 2.$$

We note that the rests are equal. But, the order of application of the reductions being different, the obtained quotient are different.

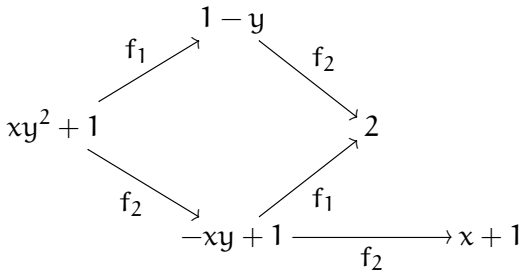
Let us remark after the first reduction by f_2, we can apply a second reduction by f_2 because $lt(f_2)$ divides $-xy + 1$:

$$\begin{array}{r|l} xy^2 + 1 & y + 1 \\ \hline xy^2 + xy & xy \\ \hline -xy + 1 & \end{array} \qquad \begin{array}{r|l} -xy + 1 & y + 1 \\ \hline -xy - x & -x \\ \hline x + 1 & \end{array}$$

The polynomial $x+1$ is the last rest because it can not be divided by the leading terms of f_1 and f_2. In this case, the decomposition is:

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

The possible reductions of xy^2+1 can be described by the following diagram:



2.3. Second example

Let $f = x^2y+xy^2+y^2$, $f_1 = xy-1$ and $f_2 = y^2-1$ be polynomials of $\mathbb{K}[x,y,z]$. Like in the first example, we consider the lexicographical order induced by $x > y$. We divide f by f_1 then by f_2.

x^2y	$+xy^2$	$+y^2$	xy	-1
x^2y	$-x$		x	
x	$+xy^2$	$+y^2$		

x	$+xy^2$	$+y^2$	xy	-1
xy^2	$-y$		y	
x	$+y$	$+y^2$		

The leading terms $\mathrm{lt}(f_1)$ and $\mathrm{lt}(f_2)$ do not divide the leading term $\mathrm{lt}(x+y+y^2) = x$. But $x+y+y^2$ is not the rest because $\mathrm{lt}(f_2)$ divides y^2.

Then, we extract the term x from the rest and continue the division:

y	$+y^2$	y^2	-1
y^2	-1	1	
y	$+1$		

After this division the rest is $x+y+1$. The leading terms of f_1 and f_2 do not divide $x+y+1$. So, $x+y+1$ is the last rest and we have:

$$\begin{aligned} x^2y+xy^2+y^2 &= (x)(xy-1)+(y)(xy-1)+(1)(y^2-1)+x+y+1, \\ &= (x+y)(xy-1)+(1)(y^2-1)+x+y+1. \end{aligned}$$

2.4. Absence of unicity of the rest

Unlike the division in the case of only one indeterminate, the rest is not unique. Indeed, let us take the second example with $f = x^2y+xy^2+y^2$, $f_1 = xy-1$, $f_2 = y^2-1$, and the lexicographical order induced by $y > x$. We divided f by f_1 then by f_2.

$$f \xrightarrow{f_1} x+xy^2+y^2 \xrightarrow{f_1} x+y+y^2 \xrightarrow{f_2} x+y+1.$$

Let us begin instead by f_2:

x^2y	$+xy^2$	$+y^2$	y^2	-1
xy^2	$-x$		x	
x^2y	$+y^2$	$+x$		

x^2y	$+y^2$	$+x$	y^2	-1
y^2	-1		1	
x^2y	$+x$	$+1$		

Then, we divide the obtained rest by f_1:

$$\begin{array}{l|l} x^2y + x + 1 & xy - 1 \\ \hline x^2y - x & x \\ \hline 2x + 1 & \end{array}$$

Then, we have:

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

This means:

$$f \xrightarrow{f_2} x^2y + y^2 + x \xrightarrow{f_2} x^2y + x + 1 \xrightarrow{f_1} 2x + 1.$$

The rest obtained by this reduction path is not the same:

$$\begin{array}{ccccc} & & x + xy^2 + y^2 & \xrightarrow{f_1} & x + y + y^2 \xrightarrow{f_2} x + y + 1 \\ & \overset{f_1}{\nearrow} & & & \\ f & & & & \\ & \underset{f_2}{\searrow} & & & \\ & & x^2y + y^2 + x & \xrightarrow[f_2]{} & x^2y + x + 1 \xrightarrow[f_1]{} 2x + 1 \end{array}$$

This example shows that the order of the polynomials $f_1, \ldots, f_s$ in the division algorithm has an impact on the rest r and the quotients $u_1, \ldots, u_s$.

This fact makes an obstruction to decide whether or not a polynomial is in some ideal. Indeed, if after division of f by $F = \{f_1, \ldots, f_s\}$ we obtain a rest equal to 0, *i.e.*,

$$f = u_1 f_1 + \ldots + u_s f_s,$$

then f is in the ideal $I = \langle f_1, \ldots, f_s \rangle$. This gives us the implication

$$\text{if } f \xrightarrow{F} 0, \quad \text{then } f \in I.$$

But, the reverse implication is wrong by the earlier example.

2.5. Example

Let $f = xy^2 - x$ and I the ideal of $\mathbb{K}[x, y]$ generated by $f_1 = xy + 1$ and $f_2 = y^2 - 1$. We have:

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y),$$

or

$$f \xrightarrow{\{f_1, f_2\}} -x - y.$$

By considering the order $\{f_2, f_1\}$, we have:

$$xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0,$$

or

$$f \xrightarrow{\{f_1, f_1\}} 0,$$

then f lies in I. This way, we can have $f \in I$ without f always reducing into 0 by a set of polynomials generating I.

The division algorithm we constructed can not be used to decide if a polynomial is in a given ideal. Tu fix this, the objective is to construct a "*good*" set of generators for the ideal I. What we want is a generating set set G of I such that the rest of the division by G is unique, whatever the order of the reductions. We want:

$$f \in I \quad \text{if and only if} \quad f \xrightarrow{G} 0.$$

3. Definitions and results

3.1. Polynomials of multiple indeterminates

For the rest of this proposal, we fix $\mathbb{K}$ a field and $A = \mathbb{K}[x_1, ..., x_n]$ the ring of polynomials in n indeterminates.

3.1.1. Definition. A *monomial* of A is an element of A of the form $x_1^{\alpha_1}...x_n^{\alpha_n}$ with $(\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$. We denote $\mathcal{M}$ the set of monomials of A.

For $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$, we denote $x^\alpha = x_1^{\alpha_1}...x_n^{\alpha_n}$.

3.1.2. Definition. A *monomial order* on $\mathcal{M}$ is a total order $\preccurlyeq$ on $\mathcal{M}$ such that:

- For every monomials m_1 and m_2 such that $m_1 \preccurlyeq m_2$ and every monomial m', we have

$$m'm_1 \preccurlyeq m'm_2$$

- 1 is the minimal element of $\mathcal{M}$.

We now fix $\preccurlyeq$ a monomial order on $\mathcal{M}$ for the rest of the section. We call $\prec$ the strict order induced by $\preccurlyeq$.

3.1.3. Definition. The monomial order $\preccurlyeq$ is called a *lexicographical order by degree* or deglex order if for every α and β of $\mathbb{N}^n$, we have $x^\alpha \prec x^\beta$ if $\alpha_1 + ... + \alpha_n < \beta_1 + ... + \beta_n$.

Exercise. Prove a deglex order is a monomial order.

3.1.4. Proposition. *Let m_1 and m_2 be monomials such that m_1 divides m_2. Then, $m_1 \preccurlyeq m_2$.*

Proof. Let us assume there is a monomial m' such that $m_2 = m'm_1$. From $1 \preccurlyeq m'$, we conclude $m_1 \preccurlyeq m'm_1 = m_2$. □

3.1.5. Proposition. *The order $\prec$ is well founded.*

Proof. We can assume without loss of generality that $x_1 \prec x_2 \prec ... \prec x_n$. Let x^α and x^β be two monomials such that $x^\beta \prec x^\alpha$. From this inequality, we deduce there is some integer $1 \leqslant i \leqslant n$ such that $\beta_i < \alpha_i$ and $\beta_j < \alpha_j$ for each $i < j \leqslant n$. We conclude $\prec$ is well founded. □

Every $f \neq 0$ of A can be written:

$$f = \sum_{k=1}^{r} a_k x^{\alpha^k}$$

where each a_k is a non zero scalar and $x^{\alpha^r} \prec ... \prec x^{\alpha^2} \prec x^{\alpha^1}$. We call $\text{multideg}(f) = \alpha^1$ the *multidegree* of f. The scalar $\text{lc}(f) = a_1$ is called the *leading coeficient* of f. The monomial $\text{lm}(f) = x^{\alpha^1}$ is called the *leading monomial* of f. We call $\text{lt}(f) = a_1 x^{\alpha^1}$ the *leading term* of f.

By convention, we denote $\text{lc}(0) = \text{lm}(0) = \text{lt}(0) = 0$.

3.2. Gröbner bases

3.2.1. Definition. An *monomial* ideal of A is an ideal generated by monomials of A.

We now fix I an ideal of A. We denote $\mathrm{lt}(I) = \{\mathrm{lt}(f) | f \in I\}$. This ideal is monomial.

3.2.2. Theorem (Hilbert basis Theorem). *There exists a finite set* F *of polynomials such that* $I = \langle F \rangle$.

From this theorem, every ideal of A is finitely generated.

3.2.3. Definition. A *Gröbner basis* of I is a finite set $G = \{g_1, ..., g_t\}$ such that $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), ..., \mathrm{lt}(g_t) \rangle$.

3.2.4. Proposition. *Let* G *be a Gröbner basis of* I. *Then* $I = \langle G \rangle$.

3.2.5. Proposition. *Every ideal of* A *admits a Gröbner basis.*

Division by a Gröbner bases always gives a unique rest.

3.2.6. Proposition. *Let* $G = \{g_1, ..., g_t\}$ *be a Gröbner basis of* I *and let* f *be a polynomial of* A. *Then, there exists a unique* r *in* A *such that:*

- $\{\mathrm{lt}(g_1), ..., \mathrm{lt}(g_t)\}$ *does not divide any term of* r,
- $f - r$ *is in* I.

Proof. Divding f by G gives a rest verifying the two given properties. Let r and r' verifying the second properties. We have:

$$r - r' \in I.$$

This implies:

$$\mathrm{lt}(r - r') \in \mathrm{lt}(I) = \langle \mathrm{lt}(g_1), ..., \mathrm{lt}(g_t) \rangle.$$

So, $\mathrm{lt}(r - r') \neq 0$ contradicts the second property of r. We conclude $r = r'$. □

Such an r is called the *normal form* of f relatively to G. We denote:

$$f \xrightarrow{G} r.$$

3.2.7. Proposition. *Let* G *be a Gröbner basis of* I *and let* f *be a polynomial of* A. *Then,* $f \in I$ *if and only if* $f \xrightarrow{G} 0$.

Proof. If $f \xrightarrow{G} 0$, it is immediate that $f \in I$. Conversely, let us assume f is in I. Then, 0 verifies all the properties of the normal form given in 3.2.6. Thus, $f \xrightarrow{G} 0$. □

3.3. Buchberger's algorithm

Given an ideal I of A, a finite generating set of I is not always a Gröbner basis. But, any generating set of I is included in a Gröbner basis. To complete a generating set into a Gröbner basis, we use Buchberger's algorithm.

Let f, g and h be in A. We denote:

$$f \xrightarrow{g} h$$

if there is a non zero term X of f such that $\mathrm{lt}(g)$ divides X and:

$$h = f - \frac{X}{\mathrm{lt}(g)} g.$$

Let $F = \{f_1, ..., f_s\}$ be a finite set of polynomials. We say f reduces into h modulo F if there is a sequence

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} ... \xrightarrow{f_{i_k}} h$$

where each f_{i_1} is in F. We denote:

$$f \xrightarrow{F} h.$$

We call h a normal form of f for F if there is no $h' \neq h$ such that $h \xrightarrow{F} h'$. We say the relation $\xrightarrow{F}$ is *confluent* if for each polynomial f and each pair (h_1, h_2) such that:

- $h_1 \neq h_2$,
- $f \xrightarrow{F} h_1$ and $f \xrightarrow{F} h_2$,

there exists h' such that $h_1 \xrightarrow{F} h'$ and $h_2 \xrightarrow{F} h'$.

3.3.1. Proposition. *Let G be a finite subset of A. Then, G is a Gröbner basis if and only if each f of A has a unique normal form for G.*

3.3.2. Definition. Let f and g be polynomials of A. Let us denote $\alpha = \text{multideg}(f)$ and $\beta = \text{multideg}(g)$. By denoting $\gamma = (\gamma_1, ..., \gamma_n)$ with each γ_i equal to $\max(\alpha_i, \beta_i)$, we call the *S-polynomial* of f and g the polynomial:

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

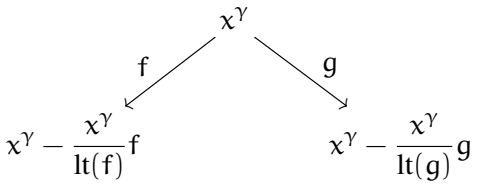
3.3.3. Theorem (Buchberger's criterion). *Let $G = \{g_1, ..., g_t\}$ be a finite set of polynomials and I the ideal generated by G. Then, G is a Gröbner basis of I if and only if for each $i \neq j$, we have:*

$$S(g_i, g_j) \xrightarrow{G} 0.$$

3.3.4. Theorem. *Let $G = \{g_1, ..., g_t\}$ be a finite set of polynomials. Then, G is a Gröbner basis if and only if the relation $\xrightarrow{G}$ is confluent.*

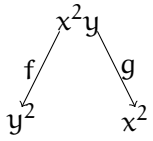
Buchberger's algorithm takes a finite set $F = \{f_1, ..., f_s\}$ of polynomials and completes it into a Gröbner basis. If F satisfies Buchberger's criterion, then F is a Gröbner basis. Else, we chose $i \neq j$ such that $S(f_i, f_j)$ does not reduce into 0 and assign to F the set $F \cup \{S(f_i, f_j)\}$. This algorithm yields a Gröbner basis in a finite number of steps.

Graphically, for each f and g in F with $f \neq g$, Buchberger's algorithm studies the following superposition of the rewriting rules $\xrightarrow{f}$ and $\xrightarrow{g}$ called *critical pair*:

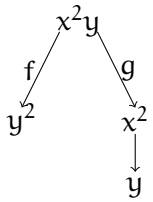


If the critical pair is not confluent, we add a h to F making it confluent.

3.3.5. Example. *Let I be the ideal of $\mathbb{K}[x, y]$ generated by $f = x^2 - y$ and $g = xy - x$. Let $<$ be the deglex order on the monomials of $\mathbb{K}[x, y]$ induced by $y < x$. We have a critical pair:*



This critical pair is not confluent.



Then, we add to $\{f, g\}$ *the polynomial* $y^2 - y$ *to obtain confluence. After adding this polynomial, all critical pairs are confluent. So,* $\{x^2 - y, xy - x, y^2 - y\}$ *is a Gröbner basis of* I.

Exercise. Which of the following families of polynomials are Gröbner bases for the deglex order induced by $z < y < x$?

- $\{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$
- $\{y - z^2, x - z^3\}$
- $\{y - x^2, z - x^3\}$

4. Applications of Gröbner bases

4.1. Elements of an ideal

Let I be the ideal of $\mathbb{Q}[x, y, z]$ generated by $xy - y^2$ and $x^2 - z^2$. Is the polynomial $2x^3y - xyz^2 - y^2z^2$ in I? Is the polynomial $xyz + x^3 + y^3 + z^3$ in the ideal generated by $x^2 + y^2 + z^2$ and $xy + xz + yz$? Is the polynomial $x^3x^2y + xy^2 - 2xz^2 + y^3 + y^2z$ in the ideal generated by $xy - z$, $xz - y$ and $yz - x$?

4.2. Systems of polynomial equations

Solve in the field $\mathbb{C}$ of complex numbers the following systems of polynomial equations.

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

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

$$\begin{cases} x^2 + 2y^2 - y - 2z = 0 \\ x^2 - 8y^2 + 10z = 1 \\ x^2 - 7yz = 0 \end{cases}$$

$$\begin{cases} x^2 + y^2 + z^2 - 2x = 0 \\ x^3 - yz - x = 0 \\ x - y + 2z = 0 \end{cases}$$

4.3. Theorems to prove

The goal of this part is to prove Hilbert basis Theorem 3.2.2 and Theorem 3.3.4. Using Gröbner bases and their properties, construct for each ideal I of A a finite generating set of I to prove Hilbert basis Theorem. Theorem 3.3.4 can also be proved using properties of Gröbner bases. Use this theory to prove each Gröbner basis G gives a confluent relation $\xrightarrow{G}$.

4.4. To go further

The book *An Introduction to Gröbner Bases* of William W. Adams and Philippe Loustaunau (American Mathematical Society, Graduate Studies in Mathematics, Volume 3, 1994) makes a comprehensive reference on Gröbner bases. If one is interested toward more applications, one can also read the second edition of *Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra* written by David Cox, John Little and Donal O'Shea (Undergraduate Texts in Mathematics, Springer-Verlag, 1997).