The Buchberger Algorithm as a Tool for Ideal Theory of Polynomial Rings in Constructive Mathematics

Henri Lombardi* Hervé Perdry†

Jan 98

Introduction

One of the aims of Constructive Mathematics is to provide effective methods (algorithms) to compute objects whose existence is asserted by Classical Mathematics. Moreover, all proofs should be constructive, *i.e.*, have an underlying effective content. *E.g.* the classical proof of the correctness of Buchberger algorithm, based on noetherianity, is non constructive : the closest consequence is that we know that the algorithm ends, but we don't know when.

In this paper we explain how the Buchberger algorithm can be used in order to give a constructive approach to the Hilbert basis theorem and more generally to the constructive content of ideal theory in polynomial rings over "discrete" fields.

Mines, Richman and Ruitenburg in 1988 ([5]) (following Richman [6] and Seidenberg [7]) attained this aim without using Buchberger algorithm and Gröbner bases, through a general theory of "coherent noetherian rings" with a constructive meaning of these words (see [5], chap. VIII, th. I.5). Moreover, the results in [5] are more general than in our paper and the Seidenberg version gives a slightly different result. Here, we get the Richman version when dealing with a discrete field as coefficient ring ("discrete" means the equality is decidable in k).

In classical texts (*cf.* Cox, Little and O'Shea [2]) about Gröbner bases, the correctness of the Buchberger algorithm and the Hilbert basis theorem are both proved by using a non constructive version of Dickson's Lemma. So, *from a constructive point of view*, the classical approach gives a constructive tool with a gap in the proof. *E.g.*, it is impossible to give bounds for the Buchberger algorithm by a detailed inspection of the classical proof. Moreover, the classical formulation of the Hilbert basis theorem is nonconstructive. Here we give a constructive version of Dickson's Lemma, we deduce constructively the correctness of Buchberger algorithm and from this result we get the Hilbert basis theorem in a constructive form.

In our opinion Gröbner bases are a very good tool, the more natural one in the present time, for understanding the constructive content of ideal theory in polynomial rings over a discrete field.

*UMR CNRS 6623. Univ. de Franche-Comté, 25030 Besançon cedex, France. henri.lombardi@univ-fcomte.fr

†UMR CNRS 6623. Univ. de Franche-Comté, 25030 Besançon cedex, France. perdry@univ-fcomte.fr

1 A constructive Dickson's lemma

1.1 Posets and chain conditions

Definition : A poset (partially ordered set) $(E, \leq)$ is said to satisfy the *descending chain condition* (*DCC* for short) if for every nonincreasing sequence $(u_n)_{n\in\mathbb{N}}$ in E there exists $n \in \mathbb{N}$ such that $u_n = u_{n+1}$. A poset $(E, \leq)$ is said to satisfy the *ascending chain condition* (*ACC* for short) if for every nondecreasing sequence $(u_n)_{n\in\mathbb{N}}$ in E there exists $n \in \mathbb{N}$ such that $u_n = u_{n+1}$.

Examples :

- The poset $\mathbb{N}$ with the usual order satifies *DCC*.
- If $(E, \preceq)$ is a poset satisfying *ACC*, then $E' = E \cup \{-\infty\}$, ordered with the order of E extended by $-\infty \preceq x$ for all $x \in E'$ is a poset satisfying *ACC*.

Remark : The above definitions of conditions *DCC* and *ACC* are equivalent (from a classical point of view) to the classical ones, but they are adapted to the constructive point of view.
In fact, even $\mathbb{N}$ fails to verify constructively the classical form of *DCC* : when one has a nonincreasing sequence $(u_n)_{n\in\mathbb{N}}$ in $\mathbb{N}$ without more information, it is *a priori* impossible to know when the limit of the sequence is attained. *E.g.*, call Pr_{nisi} the set of primite recursive procedures $u : n \mapsto u_n$ that produce nonincreasing sequences of integers. This is an enumerable set (in the classical meaning as well as in the constructive meaning). It is well known that there exists no recursive procedure $\Phi : Pr_{nisi} \to \mathbb{N}$ that computes the limit of a sequence $(u_n)_{n\in\mathbb{N}}$ from the primitive recursive procedure producing $(u_n)_{n\in\mathbb{N}}$. If such a Φ exist it could be used to solve recursively the Halting Problem. Dealing with more intuitive arguments, one could just observe that, given a nonincreasing sequence of integer, the only general method to compute its limit is obviously to test *infinitely many* terms of this sequence, which is impossible. On the other hand, the constructive definition of *DCC* is easily realized by an Oracle Turing Machine working with any sequence $(u_n)_{n\in\mathbb{N}}$ given by an oracle.
Remark : From the definition we can easily deduce that if a poset satisfies *DCC* then for any nonincreasing sequence $(h_n)_{n\in\mathbb{N}}$ there exist infinitely many $m \in \mathbb{N}$ such that $u_m = u_{m+1} = \ldots = u_{m+h_m}$ (consider the subsequence where the indices k_n are defined by $k_{n+1} = k_n + h_{k_n}$). So any nonincreasing sequence halts "as a long time as we want".

Let $(E, \leq)$ be a poset. We will denote by $\leq_d$ the order on E^d defined by $(x_1, \ldots, x_d) \leq_d (y_1, \ldots, y_d)$ if and only if $x_i \leq y_i$ for all $i \in \{1, \ldots, d\}$. We shall write $\leq$ instead of $\leq_d$ when no confusion can arise.

Lemma 1.1 *If the poset $(E, \leq)$ satisfies DCC, then so does $(E^d, \leq_d)$. More generally, the finite product of posets verifying DCC satisfies DCC.*

Proof : We first give the proof for the case $d = 2$. Let $(u_n, v_n)_{n\in\mathbb{N}}$ be a nonincreasing sequence. Since the sequence $(u_n)_{n\in\mathbb{N}}$ is nonincreasing, one can find $n_1 < n_2 < \ldots$ such that $u_{n_i} = u_{n_i+1}$ for all $i \in \mathbb{N}$. The sequence $(v_{n_i})_{i\in\mathbb{N}}$ is nonincreasing ; hence, there exists $j \in \mathbb{N}$ such that $v_{n_j} = v_{n_{j+1}}$. But $v_{n_j} \geq v_{n_j+1} \geq v_{n_{j+1}}$, thus $v_{n_j} = v_{n_j+1}$, and $(u_{n_j}, v_{n_j}) = (u_{n_j+1}, v_{n_j+1})$.
The same argument can be used to prove the general case by induction. □
Note that the same lemma remains true when replacing *DCC* by *ACC*.

1.2 Dickson's lemma for finitely generated submodules of $\mathbb{N}^d$

We will consider $\mathbb{N}^d$ as an $\mathbb{N}^d$–module with the following law : $x \star y = x + y$.
Let $\mathbf{M}_d$ be the set of finitely generated $\mathbb{N}^d$–submodules of $\mathbb{N}^d$. We denote $\mathcal{M}^+(x^1, \ldots, x^n)$ the $\mathbb{N}^d$–module generated by $\{x^1, \ldots, x^n\}$, and we let $\overline{x} := \mathcal{M}^+(x) = x + \mathbb{N}^d$. We remark that

$$\mathcal{M}^+(x^1, \ldots, x^n) \;=\; \overline{x^1} \cup \ldots \cup \overline{x^n} \;=\; \{x \in \mathbb{N}^d \;: x \geq_d x^1 \;\vee\; \cdots \;\vee\; x \geq_d x^n\}$$

Given any poset $(E, \leq_E)$ a *final subset of finite type* of E (generated by $x^1, \ldots, x^n$) is a set

$$\mathcal{M}_E^+(x^1, \ldots, x^n) \;:=\; \overline{x^1} \cup \ldots \cup \overline{x^n} \;=\; \{x \in E \;: x \geq_E x^1 \;\vee\; \cdots \;\vee\; x \geq_E x^n\}$$

and $\mathbf{F}(E)$ will denote the set of final subsets of finite type of E, including the empty subset considered as generated by the empty family. So we have $\mathbf{F}(\mathbb{N}^d) = \mathbf{M}_d \cup \{\emptyset\}$.

Proposition 1.2

(i) Every $A \in \mathbf{M}_d$ is generated by a unique minimal family (for $\subseteq$). This family can be obtained by taking the minimal elements (for $\leq_d$) of any family of generators of A.

(ii) Given A, B in $\mathbf{M}_d$, one can decide whether $A \subseteq B$ or not.

(iii) The ordered set $(\mathbf{M}_d, \subseteq)$ satisfies ACC.

Proof : Remark that for any $a, x^1, \ldots, x^n$ in $\mathbb{N}^d$ we have

$$\overline{a} \subseteq \overline{x^1} \cup \cdots \cup \overline{x^n} \;\Leftrightarrow\; a \in \overline{x^1} \cup \cdots \cup \overline{x^n} \;\Leftrightarrow\; x^1 \leq_d a \textbf{ or } \ldots \textbf{ or } x^n \leq_d a$$

So, a given family $x^1, \ldots, x^n$ of generators of A is minimal (for $\subseteq$) if and only if neither $x^i \leq_d x^j$, nor $x^j \leq_d x^i$, for any $i < j \in \{1, \ldots, n\}$.
Hence we can extract a minimal family of any given family $x^1, \ldots, x^n$ of generators, keeping only the minimal (for $\leq_d$) elements $x^{k_1}, \ldots, x^{k_m}$: this gives the existence part of (i).
If $x^1, \ldots, x^n$ and $y^1, \ldots, y^m$ are minimal families of generators of A, $y^i \in A = \mathcal{M}^+(x^1, \ldots, x^n)$ for all $i \in \{1, \ldots, m\}$, hence there exists $j \in \{1, \ldots, n\}$ such that $x^j \leq_d y^i$. Applying this argument again for a given x^j, we show that for all $j \in \{1, \ldots, n\}$, there exists $k \in \{1, \ldots, m\}$ such that $y^k \leq_d x^j$.
Then for all $i \in \{1, \ldots, m\}$, there exists $j \in \{1, \ldots, n\}$ and $k \in \{1, \ldots, m\}$ such that $y^k \leq_d x^j \leq_d y^i$. The family $y^1, \ldots, y^m$ being minimal, using the above remark, we deduce that $k = i$. So for all $i \in \{1, \ldots, m\}$, there exists a unique $j \in \{1, \ldots, n\}$ such that $y^i = x^j$. The converse is also true, so we conclude that the two families are equal : we have shown the uniqueness part of (i).

The proof of (ii) is easy and left to the reader.

We prove (iii) by induction on d. The case $d = 1$ is clear. Let $d \geq 2$, let $(A^m)_{m \in \mathbb{N}}$ be a nondecreasing sequence in $\mathbf{M}_d$. Let $a = (a_1, \ldots, a_d) \in A^0$ (an element of the family of generators of A^0, for instance)
For all $i \in \{1, \ldots, d\}$ and $r \in \mathbb{N}$, let

$$H_{i,d}^r \;:=\; \{(x_1, \ldots, x_d) \;: x_i = r\} \subset \mathbb{N}^d$$

There is an order isomorphism between $(H^r_{i,d}, \leq_d)$ and $(\mathbb{N}^{d-1}, \leq_{d-1})$, given by $(x_1, \ldots, x_d) \mapsto (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_d)$. So $\mathbf{F}(H^r_{i,d}, \subseteq)$ satisfies ACC by induction hypothesis (it is isomorphic to $\mathbf{M}_{d-1} \cup \{-\infty\}$).
Now remark that $\mathbb{N}^d \setminus \overline{a}$ is a finite union of $H^r_{i,d}$'s :

$$\mathbb{N}^d \setminus \overline{a} \quad = \quad \bigcup_{i=1}^{d} \bigcup_{r<a_i} H^r_{i,d}.$$

Rename these sets $\mathcal{H}_1, \ldots, \mathcal{H}_k$: $\mathbb{N}^d \setminus \overline{a} = \cup_{j=1}^k \mathcal{H}_j$, each $\mathcal{H}_j$ being one of the $H^r_{i,d}$ in the above formula.
Given $A = \mathcal{M}^+(x^1, \ldots, x^n) \in \mathbf{M}_d$ and $\mathcal{H} = H^r_{i,d}$, we see easily that $\mathcal{H} \cap A$ is an explicit element of $\mathbf{F}(\mathcal{H})$:

first, for any $y \in \mathbb{N}^d$, $\quad \overline{y} \cap H^r_{i,d} = \begin{cases} \emptyset & \text{if } r < y_i \\ (y_1, \ldots, y_{i-1}, r, y_{i+1}, \ldots, y_d) + \mathbb{N}^{d-1} & \text{if } y_i \leq r \end{cases}$

then $\mathcal{H} \cap A = \cup_{i=1,\ldots,n} (\overline{x^i} \cap \mathcal{H})$.
Now for each $j \in \{1, \ldots, k\}$ we consider the sequence $m \mapsto A^m \cap \mathcal{H}_j$. This is a nondecreasing sequence in $\mathbf{F}(\mathcal{H}_j)$. Each $\mathbf{F}(\mathcal{H}_j)$ satisfies ACC, so by the lemma 1.1 there exists i such that $A^i \cap \mathcal{H}_j = A^{i+1} \cap \mathcal{H}_j$ for all $j \in \{1, \ldots, k\}$. Since for each m

$$A^m \quad = \quad \overline{a} \ \cup \ (\ \bigcup_{j=1,\ldots,k} (A^m \cap \mathcal{H}_j) \ )$$

clearly we have $A^i = A^{i+1}$. This ends the proof. □
Let k be a field, $k[x_1, \ldots, x_d]$ be the associated polynomial ring. If $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{N}^d$, x^α denotes the monomial $x_1^{\alpha_1} \ldots x_d^{\alpha_d}$. A *monomial ideal* is an ideal generated by a monomial family $(x^\alpha)_{\alpha \in A}$, where $A \subseteq \mathbb{N}^d$. Clearly, two monomial ideals are equal if and only if they contain the same monomials, and the set of finitely generated monomial ideals is in one-to-one correspondance with $\mathbf{M}_d$. Then the third assertion of our previous proposition is equivalent to the following result.

Proposition 1.3 (Dickson's lemma, constructive version) *The set of finitely generated monomial ideals of $k[x_1, \ldots, x_d]$, ordered with $\subseteq$, satisfies ACC.*

Remark : the classical proof of Dickson's lemma deals with the classical Ascending Chain Condition, and is obviously non constructive : the arguments given to show that $\mathbb{N}$ fails to verify classical DCC can be used again.

2 Acceptable orders and division algorithm

Let k be a discrete field ("discrete" means the equality is decidable in k). We are dealing with finitely generated ideals $I = \mathcal{I}(f_1, \ldots, f_s)$ of $k[x_1, \ldots, x_d]$. For $d = 1$, the test $f \in I$? can be made using the Euclidean division of polynomials. The Buchberger algorithm (*cf.* [1]) is based on a generalisation of this division. It is necessary to have a good total order on monomials. In fact, in sections 2 and 3, we follow the method of Galligo [3] and Cox, Little, O'Shea [2].

2.1 Acceptable orders on $\mathbb{N}^d$

A total order $\preceq$ on $\mathbb{N}^d$ is *acceptable* if :
(i) $0 \preceq \alpha$ for all $\alpha \in \mathbb{N}^d$.
(ii) If $\alpha \leq_d \beta$ (*i.e.*, $\alpha_1 \leq \beta_1, \ldots, \alpha_d \leq \beta_d$) then $\alpha \preceq \beta$.
(iii) If $\alpha \preceq \beta$ then $\alpha + \gamma \preceq \beta + \gamma$.
(iv) $\alpha \preceq \beta$ is decidable.

Example: The lexicographic order is an acceptable order on $\mathbb{N}^d$.

Remark: Conditions (i) and (iii) imply condition (ii), condition (ii) implies condition (i). Our definition comes from [3]. We have added the condition (iv) (which is easily verified in all ususal cases) in order to get constructive theorems. In [2], the definition of *monomial orderings* p. 54 is different from our definition of acceptable orders, but the corollary 6 p. 71 in [2] shows that the two definitions are in fact equivalent.

Lemma 2.1 *If $\preceq$ is an acceptable order on $\mathbb{N}^d$, then $(\mathbb{N}^d, \preceq)$ satisfies DCC.*

Proof. A nonincreasing sequence $n \mapsto (u_n)$ in $(\mathbb{N}^d, \preceq)$ halts at step n iff the nondecreasing sequence $n \mapsto A^m = \overline{x^1} \cup \ldots \cup \overline{x^m}$ in $(\mathbf{M}_d, \subseteq)$ halts at step n. □

2.2 Division algorithm

An acceptable order $\preceq$ on $\mathbb{N}^d$ induces an order on the monomials of $k[x_1, \ldots, x_d]$: we will write $x^\alpha \preceq x^\beta$ instead of $\alpha \preceq \beta$ (recall that x^α means $x_1^{\alpha_1} \ldots x_d^{\alpha_d}$ for all $\alpha \in \mathbb{N}^d$).
Let $f = \sum_{\alpha \in \mathbb{N}^d} a_\alpha x^\alpha$ be a nonzero polynomial of $k[x_1, \ldots, x_d]$. The *multi-degree of f* is

$$\text{multideg}\, f = \max_{\preceq}\{\alpha \in \mathbb{N}^d \ : a_\alpha \neq 0\}.$$

If $\alpha = \text{multideg}\, f$, the *leading term of f*, the *leading coefficient of f*, the *leading monomial of f* are

$$\text{LT}\,(f) = a_\alpha x^\alpha, \quad \text{LC}\,(f) = a_\alpha, \quad \text{LM}\,(f) = x^\alpha.$$

Now we recall a generalization of the euclidean division of polynomials.

Proposition 2.2 *Let $\mathcal{F}$ be an s-tuple $(f_1, \ldots, f_s)$ in $k[x_1, \ldots, x_d]$. Every $f \in k[x_1, \ldots, x_d]$ can be written*

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

where $a_1, \ldots, a_s, r \in k[x_1, \ldots, x_d]$, $\text{multideg}\,(a_i f_i) \preceq \text{multideg}\,(f)$, and either $r = 0$, or $r = \sum_{\alpha \in \mathbb{N}^d} a_\alpha x^\alpha$, with, for each α such that $a_\alpha \neq 0$, x^α not divisible by any $\text{LM}\,(f_i)$.
By definition r is called a remainder *of the division of f by $\mathcal{F}$; it will be denoted by $r = \overline{f}^{\mathcal{F}}$.*

Proof. The following algorithm computes $a_1, \ldots, a_s$ and r.

Input : $f_1, \ldots, f_s, f$.
Output : $a_1, \ldots, a_s, r$.

$a_1 := 0, \ldots, a_s := 0, r := 0, p := f$
While $p \neq 0$ **do**
  $i := 1$
  $div :=$ **False**
  While ($i \leq s$ **and** $div =$ **False**) **do**

$$\begin{array}{l} \textbf{If } \mathrm{LT}(f_i) \mid \mathrm{LT}(p) \textbf{ then } a_i := a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \\ \qquad\qquad\qquad\qquad\qquad\qquad p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i \\ \qquad\qquad\qquad\qquad\qquad\qquad div := \textbf{True} \\ \qquad \textbf{else } i := i+1 \\ \textbf{If } div = \textbf{False then } r := r + \mathrm{LT}(p),\ p := p - \mathrm{LT}(p) \end{array}$$

If the algorithm stops, it is easily seen that it gives a correct result (see e.g. [2]). The fact that the algorithm stops is constructively proved by lemma 2.1 since $\mathrm{LM}(p)$ decreases strictly until $p = 0$. □

Remark : There is *a priori* no uniqueness result ! if we change the order of the $f_1, \ldots, f_s$, we change the computed polynomials.

3 Gröbner bases and Buchberger's algorithm for ideals

We call *Gröbner basis* of a given ideal $I \subseteq k[x_1, \ldots, x_d]$ any family $g_1, \ldots, g_s$ of polynomials in I such that, for all $f \in I$, the division of f by $g_1, \ldots, g_s$ using the previous algorithm leads to a null remainder.

Lemma 3.1

- *A given family $g_1, \ldots, g_s$ of polynomials in I is a Gröbner basis of I if and only if for all $f \in I$, $\mathrm{LT}(f) \in \mathcal{I}(\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$.*
- *For a given Gröbner basis $\mathcal{G} = (g_1, \ldots, g_s)$ of I, the remainder of the division of any polynomial f by $\mathcal{G}$ is unique, irrespective of the order of $g_1, \ldots, g_s$.*

Proof. The first result is a clear consequence of the division algorithm. To show the second result, if $f = h_1 + r_1$ and $f = h_2 + r_2$, with $h_1, h_2 \in I$, then we have $(r_1 - r_2) \in I$, hence $\mathrm{LT}(r_1 - r_2) \in \mathcal{I}(\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$. This leads to $r_1 - r_2 = 0$, since no monomial of r_1, r_2 is divisible by any of the $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. □

Remark : We don't know yet (from a constructive point of view) if for any given finitely generated ideal I, there exists a Gröbner basis. From the previous lemma, we deduce that the existence of a Gröbner basis of a finitely generated ideal I is equivalent to the existence of a (finite) basis of the monomial ideal $\mathcal{I}(\mathrm{LT}(I)) = \mathcal{I}(\mathrm{LT}(f) \ : f \in I)$.

3.1 Buchberger's algorithm

Now we will show that for a given ideal $I = \mathcal{I}(f_1, \ldots, f_r)$, one can always find a Gröbner basis $\mathcal{G} = (g_1, \ldots, g_s)$ of I.

If $f, g \in k[x_1, \ldots, x_d] \setminus \{0\}$, with multideg $f = \alpha$ and multideg $g = \beta$, let $\gamma = (\gamma_1, \ldots, \gamma_d)$ where $\gamma_i = \max(\alpha_i, \beta_i)$; we define $\mathrm{lcm}(\alpha, \beta) = \gamma$, $\mathrm{lcm}(\mathrm{LT}(f), \mathrm{LT}(g)) = x^\gamma$.
We define the *S-polynomial of f, g* by $\mathrm{S}[f, g] = \frac{x^\gamma}{\mathrm{LT}(f)} f - \frac{x^\gamma}{\mathrm{LT}(g)} g$.

We will recall without proof classical results whose proof is everywhere constructive (*e.g.*, in [2]). We insist only on the constructive proof of the correctness of Buchberger algorithm.

Lemma 3.2 *Let $g_1, \ldots, g_s \in k[x_1, \ldots, x_d]$. If we have some $c_i \in k$ and $\alpha(i) \in \mathbb{N}^d$ (for $i = 1, \ldots, s$), such that $\alpha(i) + \text{multideg}\,(g_i) = \delta$ for all $i \in \{1, \ldots, s\}$ such that $c_i \neq 0$, and $\text{multideg}\,(\sum_{i=1}^{s} c_i x^{\alpha(i)} g_i) \prec \delta$; then there exists $c_{j,k} \in k$ such that :*

$$\sum_{i=1}^{s} c_i x^{\alpha(i)} g_i = \sum_{j,k} c_{j,k} x^{\delta - \gamma_{j,k}} \mathrm{S}[g_j, g_k]$$

where $x_{j,k}^{\gamma} = \text{lcm}\,(\text{LT}\,(g_j), \text{LT}\,(g_k))$.
Furthermore, for each j, k, $\text{multideg}\,(x^{\delta - \gamma_{j,k}} \mathrm{S}[g_j, g_k]) \prec \delta$.

Now we give a characterization of Gröbner bases.

Proposition 3.3 *Let I be a polynomial ideal of $k[x_1, \ldots, x_d]$. A given basis $\mathcal{G} = (g_1, \ldots, g_s)$ of I is a Gröbner basis if and only if for all $i \neq j$, the remainder $\overline{\mathrm{S}[g_i, g_j]}^{\mathcal{G}}$ of the division of $\mathrm{S}[g_i, g_j]$ by $\mathcal{G}$ is zero.*

This proposition gives an algorithm which checks whether a given family $\mathcal{G}$ is a Gröbner basis or not. The idea is now, if $\mathcal{G}$ is not a Gröbner basis, to add to $\mathcal{G}$ the nonzero remainders $\overline{\mathrm{S}[g_i, g_j]}^{\mathcal{G}}$, and to iterate this operation until a Gröbner basis is computed. The Dickson's lemma (proposition 1.3) legitimates this method.

Theorem 1 *Let $I = \mathcal{I}(f_1, \ldots, f_s)$ a nonzero ideal of $k[x_1, \ldots, x_d]$. A Gröbner basis of I can be obtained by a finite number of iterations of the following algorithm :*

Input : $\mathcal{F}$ a basis of I.
Output : $\mathcal{G}$ a Gröbner basis of I.

$\mathcal{G} := \mathcal{F}$
Repeat
  $\mathcal{H} := \mathcal{G}$
  For all $p \leq q$ **in** $\mathcal{H}$ **do**
    If $\overline{\mathrm{S}[p, q]}^{\mathcal{H}} \neq 0$ **then** $\mathcal{G} := \mathcal{G} \cup \{\overline{\mathrm{S}[p, q]}^{\mathcal{H}}\}$
until $\mathcal{H} = \mathcal{G}$

Proof : This algorithm computes a nondecreasing sequence $\mathcal{G}_1 \subseteq \mathcal{G}_2 \subseteq \ldots$
First $\mathcal{G}_0 = \mathcal{F}$ is a family of elements of I and if $\mathcal{G}_i$ is in I, then for $p, q \in \mathcal{G}_i$, we have $\mathrm{S}[p, q] \in I$, hence $\overline{\mathrm{S}[p, q]}^{\mathcal{G}_i} \in I$, hence $\mathcal{G}_{i+1}$ is in I. By induction, $\mathcal{G}_m$ is in I for all m.
If the algorithm ends, proposition 3.3 says that the computed family $\mathcal{G}$ is a Gröbner basis. Hence we just need to prove that the algorithm ends. For each i, we denote by $\mathcal{I}(\text{LT}\,(\mathcal{G}_i))$ the monomial ideal generated by the leading terms of the elements of $\mathcal{G}_i$. Since $\mathcal{G}_i \subseteq \mathcal{G}_{i+1}$, we have $\mathcal{I}(\text{LT}\,(\mathcal{G}_i)) \subseteq \mathcal{I}(\text{LT}\,(\mathcal{G}_{i+1}))$.
But if $\mathcal{G}_i \subset \mathcal{G}_{i+1}$, then there exists $p, q \in \mathcal{G}_i$ such that $\overline{\mathrm{S}[p, q]}^{\mathcal{G}_i} \neq 0$, hence $\overline{\mathrm{S}[p, q]}^{\mathcal{G}_i} \notin \mathcal{I}(\text{LT}\,(\mathcal{G}_i))$; since $\overline{\mathrm{S}[p, q]}^{\mathcal{G}_i} \in \mathcal{I}(\text{LT}\,(\mathcal{G}_{i+1}))$, we have $\mathcal{I}(\text{LT}\,(\mathcal{G}i)) \subset \mathcal{I}(\text{LT}\,(\mathcal{G}i + 1))$.
Then, by Dickson's lemma (proposition 1.3), the sequence of monomial ideals $\mathcal{I}(\text{LT}\,(\mathcal{G}_i))$ being nondecreasing, there exits i such that $\mathcal{I}(\text{LT}\,(\mathcal{G}_i)) = \mathcal{I}(\text{LT}\,(\mathcal{G}_{i+1}))$, hence $\mathcal{G}_i = \mathcal{G}_{i+1}$: which completes the proof. □

Remark : Reading carefully the proofs leading to this result, one could compute a majoration of the size of a Gröbner basis of $I = \mathcal{I}(f_1, \ldots, f_s)$ depending only on d (the number of variables) and on the degrees of the polynomials. In fact, assume that the monomial ordering, d and the degrees of $f_1, \ldots, f_s$ are fixed, and consider all the

coefficients $(c_j)_{1\leq j\leq q}$ of the f_i's as indeterminates. Then we get a "universal algorithm" that computes a Gröbner basis of I in any situation. A "situation" is specified by the answers to some tests

$$h_\ell((c_j)_{1\leq j\leq q}) = 0\ ?$$

for a given family $(h_\ell)_{1\leq \ell\leq r}$ in $\mathbb{Z}[(c_j)_{1\leq j\leq q}]$. So the "coefficient space" is decomposed into cells $\mathcal{C}_v$ that are $\mathbb{Z}$-Zariski constructible. In any cell C_v, the Buchberger algorithm works in a completely uniform way, and all coefficients of the polynomials in the computed Gröbner basis are given by rational functions in the c_j's with denominators nowhere vanishing on C_v.

From theorem 1, we get immediately the following important corollaries.

Theorem 2 *Finitely generated ideals in a polynomial ring over a discrete field are detachable : i.e. for any system $(f_1,\ldots,f_s,g)$ of polynomials in $k[x_1,\ldots,x_d]$ we can decide if $g\in\mathcal{I}(f_1,\ldots,f_s)$ or not.*

With the terminology of [5], we shall say that the ring $k[x_1,\ldots,x_d]$ *has detachable ideals*, with the meaning that finitely generated ideals are detachable.

Corollary 3.4 *Inclusion between finitely generated ideals in a polynomial ring over a discrete field is decidable.*

Theorem 3 *Let I be a finitely generated ideal in a polynomial ring over a discrete field. Then the monomial ideal $\mathcal{I}(\mathrm{LT}\,(I))$ generated by the leading monomials of the elements of I is finitely generated*

Keeping in mind lemma 3.1 that characterizes Gröbner bases we see that the last theorem is nothing but an abstract form (*i.e.*, without specifying the algorithm which is implicit in the statement) of theorem 1.

4 A few constructions relative to polynomial ideals

4.1 Hilbert's basis theorem

Lemma 4.1 *Let I,J be finitely generated ideals of $k[x_1,\ldots,x_d]$, with $I\subseteq J$. If $\mathcal{I}(\mathrm{LT}\,(I))=\mathcal{I}(\mathrm{LT}\,(J))$, then $I=J$.*

Proof : Let $p\in J$. Then $\mathrm{LT}\,(p)\in\mathcal{I}(\mathrm{LT}\,(J))=\mathcal{I}(\mathrm{LT}\,(I))$. Hence we can find $f\in I$ such that $\mathrm{LT}\,(f)=\mathrm{LT}\,(p)$. The polynomial $p'=p-f$ in in J, and $\mathrm{multideg}\,(p')\preceq \mathrm{multideg}\,(p)$, with $\mathrm{multideg}\,(p')=\mathrm{multideg}\,(p)$ if and only if $p'=p=0$. Using this argument recursively, and using lemma 2.1 we show that $p\in I$. □

Theorem 4 (A constructive version of Hilbert's basis theorem) *Let k be a discrete field. The poset of finitely generated ideals of $k[x_1,\ldots,x_d]$ with $\subseteq$ verifies ACC.*

Proof : Let $(I_n)_{n\in\mathbb{N}}$ be a nondecreasing sequence of finitely generated ideals. Then $(\mathcal{I}(\mathrm{LT}\,(I_n)))_{n\in\mathbb{N}}$ is a non decreasing sequence of finitely generated monomials ideals. We conclude using Dickson's lemma and the previous lemma. □

4.2 Polynomial rings over discrete fields are coherent

A ring (resp. a module) is said to be coherent if every finitely generated ideal (resp. submodule) is finitely presented. In classical mathematics any noetherian ring is coherent. In constructive mathematics, a good notion replacing the classical notion of noetherian ring is the notion of coherent noetherian ring, where the constructive meaning for noetheriannity is that the set of *finitely generated* ideals in the ring R satisfies constructive ACC.

The theory of coherent rings and modules is naturally constructive (there are no shortcuts by classical arguments). In [5], this theory is explained very efficiently. A good classical reference for coherent rings and modules is [4]. Let us recall the main results (restricting ourselves to the commutative case). In a coherent ring, the intersection of two finitely generated ideals and the anihilator of any element are also finitely generated ideals. Conversely these conditions imply that the ring is coherent. Over a coherent ring R, any finitely presented module M is coherent. Moreover, if R has detachable ideals, then M has detachable submodules.

In this section we show constructively that a polynomial ring over a discrete field is coherent.

Lemma 4.2 *Let $\alpha_1, \ldots, \alpha_s \in \mathbb{N}^d$. Let $\gamma_{i,j} = \sup_{\leq_d}(\alpha_i, \alpha_j)$ (so $x^{\gamma_{i,j}} = \operatorname{lcm}(x^{\alpha_i}, x^{\alpha_j})$). Let $R_{i,j} \in k[x_1, \ldots, x_d]^s$ be the vector of polynomials corresponding to the relation*

$$x^{\gamma_{i,j}-\alpha_i}.x^{\alpha_i} - x^{\gamma_{i,j}-\alpha_j}.x^{\alpha_j} = 0,$$

i.e., $R_{i,j} = (0, \ldots, 0, x^{\gamma_{i,j}-\alpha_i}, 0, \ldots, 0, -x^{\gamma_{i,j}-\alpha_j}, 0, \ldots, 0)$, with the nonzero terms in i and j. Then for any relation

$$p_1 x^{\alpha_1} + \ldots + p_s x^{\alpha_s} = 0,$$

there exists polynomials $q_{i,j}$ for $i < j$, $i, j \in \{1, \ldots, s\}$ such that

$$(p_1, \ldots, p_s) = \textstyle\sum_{i<j} q_{i,j} R_{i,j}.$$

Furthermore, if $\operatorname{multideg}(p_k x^{\alpha_k}) \preceq \delta$ for each k, then $\operatorname{multideg}(q_{i,j}) \preceq \delta - \gamma_{i,j}$.
This means that the module of the relations between the monomials $x^{\alpha_1}, \ldots, x^{\alpha_s}$ is generated by the relations $\mathrm{S}[x^{\alpha_i}, x^{\alpha_j}] = 0$.

Proof : The proof is by finite descending induction on s. We write the division of p_s by the family $x^{\gamma_{k,s}-\alpha_s}$, for $k = 1, \ldots, s-1$: $p_s = \sum_{k=1}^{s-1} q_k x^{\gamma_{k,s}-\alpha_s} + r_s$, with $\operatorname{multideg}(q_k x^{\gamma_{k,s}-\alpha_s}) \preceq \operatorname{multideg}(p_s)$ (i.e $\operatorname{multideg}(q_k) \preceq \delta - \gamma_{k,s}$), and no monomial of r_s divisible by one of the $x^{\gamma_{k,s}-\alpha_s}$. Hence we have

$$p_1 x^{\alpha_1} + \ldots + p_{s-1} x^{\alpha_{s-1}} + \sum_{k=1}^{s-1} q_k x^{\gamma_{k,s}-\alpha_s} x^{\alpha_s} = -r_s x^{\alpha_s}.$$

If $r_s \neq 0$, $\operatorname{multideg}(r_s x^{\alpha_s})$ is equal to the multidegree of a term of the sum at the left part. This term cannot be one of the $q_k x^{\gamma_{k,s}-\alpha_s} x^{\alpha_s}$: we would have $x^{\gamma_{k,s}-\alpha_s}$ divides $\mathrm{LT}(r_s)$. It can neither be $p_i x^{\alpha_i}$ (for an $i \in \{1, \ldots, s-1\}$) : we would have x^{α_i} divides $\mathrm{LT}(r_s)x^{\alpha_s}$, hence $x^{\gamma_{i,s}-\alpha_s}$ divides $\mathrm{LT}(r_s)$. Then $r_s = 0$.
Hence $(p_1, \ldots, p_s) = (p'_1, \ldots, p'_{s-1}, 0) - \sum_{k=1}^{s-1} q_k R_{k,s}$, with $p'_i = p_i + q_i x^{\gamma_{i,s}-\alpha_s}$. Remark that $\operatorname{multideg}(p') \preceq \delta$. Repeating this operation s times, we obtain the desired result. □

Theorem 5 *Let $g_1, \ldots, g_s$ be a Gröbner basis of an ideal I of $k[x_1, \ldots, x_d]$. The module $\{(p_1, \ldots, p_s) \ : p_1 g_1 + \ldots + p_s g_s = 0\}$ of relations is finitely generated by the relations expressing that the remainder of the division of $\mathrm{S}[g_i, g_j]$ by $(g_1, \ldots, g_s)$ is zero.*

Proof : Let $\alpha_i = \text{multideg}\,(g_i)$. We use the notations of the previous lemma. The generating relations are $x^{\gamma_{i,j}-\alpha_i} g_i - x^{\gamma_{i,j}-\alpha_j} g_j = \sum_{k=1}^{s} p_k^{i,j} g_k$, with $\text{multideg}\,(p_k^{i,j} g_k) \preceq \text{multideg}\,(\text{S}[g_i, g_j]) \prec \gamma_{i,j}$. We denote by $T_{i,j} = R_{i,j} - (p_1^{i,j}, \ldots, p_s^{i,j})$ the associated vector. Let $(p_1, \ldots, p_s)$ such that $p_1 g_1 + \ldots + p_s g_s = 0$. Let $\delta_i = \text{multideg}\,(p_i g_i)$, and $\delta = \max(\delta_1, \ldots, \delta_s)$. We have $\sum_{\delta_k=\delta} \text{LT}\,(p_k) x^{\alpha_k} = 0$; using the previous lemma, we deduce that $(\text{LT}\,(p_k))_{\delta_k=\delta} = \sum_{i,j} q_{i,j} R_{i,j}$. Hence

$$\sum_{\delta_k=\delta} \text{LT}\,(p_k) g_k = \sum_{i<j} q_{i,j} (x^{\gamma_{i,j}-\alpha_i} g_i - x^{\gamma_{i,j}-\alpha_j} g_j)$$

Using the relations $T_{i,j}$, we have a new relation

$$\sum_{\delta_k-\delta} (p_k - \text{LT}\,(p_k)) g_k + \sum_{i<j} q_{i,j} \sum_{k=1}^{s} p_k^{i,j} g_k + \sum_{\delta_k<\delta} p_k g_k = 0$$

We have $\text{multideg}\,(q_{i,j} p_k^{i,j} g_k) \prec \delta$, then in this new relation $p'_1 g_1 + \ldots + p'_s g_s$, we have $\text{multideg}\,(p'_i g_i) \prec \delta$. But we have $(p'_1, \ldots, p'_s) = (p_1, \ldots, p_s) - \sum_{i<j} q_{i,j} T_{i,j}$. Repeating this operation, we obtain a sequence of vectors, with the maximum degree of the components nonincreasing, and decreasing while the vector is nonzero. After a finite number of iterations, we obtain that $(p_1, \ldots, p_s)$ is in the module generated by the $T_{i,j}$'s. □

4.3 Some classical constructions

In this section, we recall some basic constructions with finitely generated ideals in polynomial rings and we see that they are constructively proved.

Elimination ideal

Let $I = \mathcal{I}(f_1, \ldots, f_s)$ be a finitely generated ideal in $k[x_1, \ldots, x_d]$ and $1 \leq r < d$. The r-th elimination ideal of I is by definition the ideal $I_r = I \cap k[x_{r+1}, \ldots, x_d]$ of $k[x_{r+1}, \ldots, x_d]$. It is obtained by choosing the lexicographical order (with $x_1 > \cdots > x_d$) for the monomials and computing a Gröbner basis $\mathcal{G}$ of I for this order. Then $\mathcal{G}_r = \mathcal{G} \cap k[x_{r+1}, \ldots, x_d]$ is a Gröbner basis of $\mathcal{I}_r$. The proof is straightforward (see *e.g.* [2]).

Intersection of two finitely generated ideals

We recall here two usual ways to compute a finite basis for the intersection of two finitely generated ideals. The second one is similar to the construction given in [5].

Let $I = \mathcal{I}(f_1, \ldots, f_s)$ and $J = \mathcal{I}(g_1, \ldots, g_t)$ be two finitely generated ideals in $R = k[x_1, \ldots, x_d]$.

The first construction is the following trick. Consider a new variable y, consider the ideals $yI = \mathcal{I}(yf_1, \ldots, yf_s) \subset k[x_1, \ldots, x_d, y]$ and $(1-y)J = \mathcal{I}((1-y)g_1, \ldots, (1-y)g_t) \subset k[x_1, \ldots, x_d, y]$. Then $I \cap J = (yI + (1-y)J) \cap k[x_1, \ldots, x_d]$.

The second construction is given by a duality idea. To give an element $a_1 f_1 + \cdots + a_s f_s = b_1 g_1 + \cdots + b_t g_t$ of $I \cap J$ is the same thing as giving the relation vector $(a_1, \ldots, a_s, b_1, \ldots, b_t)$ for the polynomial system $(f_1, \ldots, f_s, -g_1, \ldots, -g_t)$. So compute a finite basis of the module of relations for this polynomial system.

Quotient of two finitely generated ideals

The quotient $I : J$ of two ideals is defined as $\{f \ : fJ \subseteq I\}$. If $I = \mathcal{I}(f_1, \ldots, f_s)$ and $J = \mathcal{I}(g_1, \ldots, g_t)$ in $R = k[x_1, \ldots, x_d]$, then obviously

$$f \in (I : J) \quad \Leftrightarrow \quad (\ fg_1 \in I \ \wedge \ \cdots \ \wedge \ fg_t \in I\ )$$

So we have to compute $I : gR$ for an arbitrary g. Compute of a finite basis $h_1, \ldots, h_u$ of $I \cap gR$: $h_1/g, \ldots, h_u/g$ is a finite basis of $I : gR$.

5 Finitely generated submodules of a free module

Here we explain how the Gröbner basis technique can be extended in order to deal with finitely generated submodules of $k[x_1,\dots,x_d]^p$. We follow [3].

5.1 Acceptable order, Gröbner bases, Dickson's lemma, Buchberger's algorithm

If $a=(\alpha,k)\in\mathbb{N}^d\times\{1,\dots,p\}$, we denote by x^a the vector $(0,\dots,0,x^\alpha,0,\dots,0)\in k[x_1,\dots,x_d]^p$, with x^α at the k-th position. A vector F of $k[x_1,\dots,x_d]^p$ is a *linear combination* of such "monomials" x^a.
Given an acceptable order $\preceq$ on $\mathbb{N}^d$, writing $(\alpha,k)\prec(\beta,\ell)$ if $\alpha\prec\beta$, and $(\alpha,k)\prec(\alpha,\ell)$ if $k<\ell$, we define a total order on $\mathbb{N}^d\times\{1,\dots,p\}$, *i.e.* on the monomials $x^{(\alpha,k)}$, satisfying *DCC*, compatible with the multiplication by a monomial of $k[x_1,\dots,x_d]$.
For $F\in k[x_1,\dots,x_d]^p$, we define $\mathrm{LT}(F),\mathrm{LC}(F),\mathrm{LM}(F)$ as we did for polynomials. Let $a=(\alpha,k)$ and $b=(\beta,\ell)$; a and b are said to be *compatible* if $k=\ell$.
If $F,G\in k[x_1,\dots,x_d]^p$, the *S-vector* of F,G is defined if and only if $\mathrm{LM}(F)$ and $\mathrm{LM}(G)$ are compatible, by $\mathrm{S}[F,G]=\frac{x^{\gamma-\alpha}}{\mathrm{LC}(F)}F-\frac{x^{\gamma-\beta}}{\mathrm{LC}}G$, where $\mathrm{LM}(F)=(\alpha,k)$, $\mathrm{LM}(G)=(\beta,k)$, $\gamma=\mathrm{lcm}(\alpha,\beta)$. If $\mathrm{LM}(F)$ and $\mathrm{LM}(G)$ are not compatible, it will be nice to write $\mathrm{S}[F,G]=0$.

Proposition 5.1 *Let $\mathcal{G}$ be an s-uple $(G_1,\dots,G_s)$ of $k[x_1,\dots,x_d]^p$. Every $F\in k[x_1,\dots,x_d]^p$ can be written*

$$F=a_1G_1+\cdots+a_sG_s+R$$

where $a_1,\dots,a_s\in k[x_1,\dots,x_d]$, $R\in k[x_1,\dots,x_d]^p$, $\mathrm{multideg}(a_iG_i)\preceq\mathrm{multideg}(F)$, and either $R=0$, or $R=\sum_{a\in\mathbb{N}^d\times\{1,\dots,p\}}c_ax^a$, with, for each a such that $c_a\neq0$, x^a not divisible by any $\mathrm{LT}(G_i)$.
The remainder *of the division of F by $\mathcal{G}$ is, by definition, R ; it will be denoted by $R=\overline{F}^{\mathcal{G}}$.*

Proof : The algorithm used to divide polynomials can be used again. □
We call *Gröbner basis* of a finitely generated submodule M of $k[x_1,\dots,x_d]^p$ a basis (*i.e.* a generating family) $\mathcal{G}=(G_1,\dots,G_s)$ of M such that, for all $F\in M$, the division of F by $\mathcal{G}$ using the classical algorithm, leads to a null remainder.

Proposition 5.2 *Let M be a finitely generated submodule of $k[x_1,\dots,x_d]^p$.*

- *A given basis $\mathcal{G}=(G_1,\dots,G_s)$ of M is a Gröbner basis if and only if for all $F\in M$, $\mathrm{LT}(F)$ is in the submodule generated by $\mathrm{LT}(G_1),\dots,\mathrm{LT}(G_s)$.*
- *A given basis $\mathcal{G}=(G_1,\dots,G_s)$ of M is a Gröbner basis if and only if for all $i\neq j$ such that $\mathrm{LM}(G_i)$ and $\mathrm{LM}(G_j)$ are compatible, the remainder $\overline{\mathrm{S}[G_i,G_j]}^{\mathcal{G}}$ of the division of $\mathrm{S}[G_i,G_j]$ by $\mathcal{G}$ is zero.*

Proof : One can verify that all the proofs written for ideals are still working. □

We can define monomial submodules in the same way than monomial ideals, and prove an other Dickson's lemma : *the poset of finitely generated monomial submodules of $k[x_1,\dots,x_d]^p$, ordered with $\subseteq$, satisfies ACC.*
This gives as in section 3.1 a constructive proof for the fact that *the Buchberger algorithm*

can be used to compute a Gröbner basis of any finitely generated submodule.
This implies that the monomial module of leading terms of a finitely generated submodule M of $k[x_1, \ldots, x_d]^p$ is also finitely generated.
This gives also the detachability of finitely generated submodules of $k[x_1, \ldots, x_d]^p$.

5.2 Constructive noetherianity and coherence

The monomial module $\mathcal{M}(\mathrm{LT}(M))$ generated by the elements of a finitely generated submodule M with Gröbner basis $G_1, \ldots, G_s$ is equal to the submodule generated by $\mathrm{LT}(G_1), \ldots, \mathrm{LT}(G_s)$. We can prove, as for ideals, that if $M \subseteq M'$ and $\mathcal{M}(\mathrm{LT}(M)) = \mathcal{M}(\mathrm{LT}(M'))$, then $M = M'$.
Hence, as for polynomial ideals, we have the following "Hilbert basis theorem".

Theorem 6 *The poset of finitely generated submodules of $k[x_1, \ldots, x_d]^p$, ordered with $\subseteq$, satisfies ACC.*

The proof of coherence we wrote for ideals is still good for submodules.

Theorem 7 *Let $G_1, \ldots, G_s$ be a Gröbner basis of a finitely generated submodule M of $k[x_1, \ldots, x_d]^p$. The module $\{(p_1, \ldots, p_s) : p_1G_1 + \cdots + p_sG_s = 0\} \subseteq k[x_1, \ldots, x_d]^s$ of relations is finitely generated by the relations expressing that, for all $i \neq j$ such that $\mathrm{LM}(G_i)$ and $\mathrm{LM}(G_j)$ are compatible, the remainder of the division of $[G_i, G_j]$ by $(G_1, \ldots, G_s)$ is zero.*

Finally, the computation of a finite basis for the intersection of two finitely generated submodules can be made following the same lines.

Acknowledgments : Many thanks to André Galligo, Loic Pottier and Marie-Françoise Roy for usefull discussions and encouragements.

References

[1] Buchberger: *An algorithmic method in polynomial ideal theory.* in Multidimensional systems theory, ed. by N.K. Bose. D Reidel Publishing Company, Dordrecht, (1985), 184–232. 4

[2] Cox Q., Little J, O'Shea D. (1992) : *Ideals, Varieties, and Algorithms*, Springer Verlag UTM. 1, 4, 5, 6, 10

[3] Galligo A. (1983) : *Algorithmes de calcul de Bases Standard.* Technical Report. Université de Nice. 4, 5, 11

[4] Glaz S. (1989) : *Commutative Coherent Rings.* (Springer Verlag, LNM n°1371). 9

[5] Mines R., Richman F., Ruitenburg W. (1988) : *A Course in Constructive Algebra* . Springer-Verlag. Universitext. 1, 8, 9, 10

[6] Richman F. (1974) : *Constructive aspects of Noetherian rings.* In : Proc. Amer. Mat. Soc. 44 pp. 436–441. 1

[7] Seidenberg A. (1974) : *What is Noetherian ?* In : Rend. Sem. Mat. e Fis. di Milano 44 pp. 55–61 1