HAL
archives-ouvertes.fr

Sub-groups of Zn, standard basis, and linear diophantine systems

Loïc Pottier

▶ **To cite this version:**

Loïc Pottier. Sub-groups of Zn, standard basis, and linear diophantine systems. [Research Report] RR-1510, INRIA. 1991, pp.11. <inria-00075052>

HAL Id: inria-00075052
https://hal.inria.fr/inria-00075052

Submitted on 24 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNITÉ DE RECHERCHE
INRIA-SOPHIA ANTIPOLIS

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P. 105
78153 Le Chesnay Cedex
France
Tél.:(1) 39 63 55 11

Rapports de Recherche

N° 1510

Programme 2
Calcul Symbolique, Programmation
et Génie logiciel

SUB-GROUPS OF Z^n, STANDARD BASIS, AND LINEAR DIOPHANTINE SYSTEMS

Loïc POTTIER

Septembre 1991

RR_1510

SUB-GROUPS OF Z^n, STANDARD BASIS, AND LINEAR DIOPHANTINE SYSTEMS

Loïc POTTIER [1]

ABSTRACT : *We caracterize a (affine) sub-group of Z^n by a polynomial ideal and standard (Gröbner) basis. We show how to use these standard basis to solve directly many algorithmic problems on (affine) sub-groups and their non-negative parts :*

- *the membership problem,*
- *the triviality problem,*
- *find the smallest non zero vector.*
- *find the minimal non-negative elements.*
- *solve linear diophantine systems ($Ax = 0, x \geq 0$), ($Ax = b, x \geq 0$), $Ax \leq b$ on integers, and find smallest solutions.*

Finally we conjecture other properties of these standard basis.

SOUS-GROUPES DE Z^n, BASES STANDARD, ET SYSTÈMES DIOPHANTIENS LINÉAIRES

RÉSUMÉ : *Nous caractérisons un sous-groupe (affine) de Z^n par un idéal de polynômes et des bases standard. Ces bases standard nous permettent de résoudre directement de nombreux problèmes sur ces sous-groupes (affines) et leurs parties positives :*

- *le problème de l'appartenance,*
- *le problème de la trivialité,*
- *trouver le plus petit vecteur non nul,*
- *trouver les éléments positifs minimaux,*
- *résoudre des systèmes diophantiens linéaires ($Ax = 0, x \geq 0$), ($Ax = b, x \geq 0$), $Ax \leq b$ sur les entiers et trouver leurs plus petites solutions.*

Enfin, nous conjecturons d'autres propriétés de ces bases standard.

[1] S.A.F.I.R. Project, Institut National de Recherche en Informatique et Automatique, 2004 route des Lucioles, Sophia Antipolis, 06565 Valbonne CEDEX, FRANCE. Email : pottier@sophia.inria.fr

INTRODUCTION

Some connections between commutative algebra and linear diophantine problems exist for a long time (recently, see [St83], [Ol90], [LP91a], [CoTr91] for works and bibliographies).
The results proposed in this paper show that this connection can be systematicaly extended to relie standard (Gröbner) basis, Knuth-Bendix completion on commutative words, affine sub-groups of Z^n, and linear systems of inequalities on integers.
The main tool is the notion of ideal associated to an affine sub-group of Z^n, and its algorithmic aspect: its standard basis.
We then show that these tools can solve directly the following algorithmic problems on (affine) sub-groups and their non-negative parts :

- the membership problem,
- the triviality problem,
- find the smallest non zero vector.
- find the minimal non-negative elements.
- solve linear diophantine systems ($Ax = 0, x \geq 0$), ($Ax = b, x \geq 0$), $Ax \leq b$ on integers, and find smallest solutions.

We end this paper by some conjectures given by transpositions of notions of commutative algebra to linear problems on integers.

NOTATIONS AND BASIC NOTIONS

DEFINITIONS 1 : **Vectors of Z^n.**
Let u and v be two vectors of Z^n.
u_i is the i^{th} coordinate of u. We will sometimes note $u = (u_i)_i$.
We define $||u||_\infty = \sum_i \mid u_i \mid$ and $||u||_1 = sup_i\{\mid u_i \mid\}$.
$u \leq v \iff \forall i,\ u_i \leq v_i$
$u \wedge v := (inf(u_i, v_i))_i$.
$u \vee v := (sup(u_i, v_i))_i$.
$u^+ = u \vee 0$, $u^- = -u \vee 0$. We have $u = u^+ - u^-$.
If A is a subset of Z^n, we define $A^+ = A \cap N^n$.
The vector $(1)_i$ will be noted 1.
We note (v, v') the concatenation $(v_1, \ldots, v_p, v'_1, \ldots, v'_q)$ of two vectors $v = (v_1, \ldots, v_p)$ and $v' = (v'_1, \ldots, v'_q)$, and $(A \mid B)$ the concatenation of two matrices with the same number of lines.

DEFINITIONS 2 : **Sub-groups, affine sub-groups of Z^n**
In this paper, H denotes a sub-group of Z^n.
An affine sub-group of Z^n is a set $a + H = \{a + x \mid x \in H\}$, where $a \in Z^n$.
The computations of generators of a sub-group given as the kernel of matrix, as well as a presentation of the form $a + H$ for an intersection of two similar affine sub-groups, can be done with linear algebra manipulations (see for example [KaBa79] who give polynomial algorithms).

DEFINITIONS 3 : **Equational theories on monomials.**
Let $X = (X_1, \ldots, X_n)$ be a vector of n indeterminates.

When $u \in N^n$, we note X^u the monomial $X_1^{u_1} \dots X_n^{u_n}$, and $1 := X^0$.
Let $E = \{X^{\alpha_i} = X^{\beta_i}\}$ a set of equations between monomials. We define the congruence generated by E as the least equivalence relation $=_E$ containing the set of couples $\{(X^{\alpha_i+u}, X^{\beta_i+u}) \mid u \geq 0\}$.

DEFINITIONS 4 : **Standard basis, monomials orderings**
Let $<$ a total admissible ordering on monomials (i.e. such that 1 is the least monomial, and $<$ is stable by multiplication). We note $in(P)$ the greatest monomial of a polynomial P.
Let $\mathcal{I}$ an ideal of the polynomial ring $Z[X_1, \dots, X_n]$, and $B = \{P_1, \dots, P_r\}$ a familly of polynomials of $\mathcal{I}$.

Then B is a *standard basis* of $\mathcal{I}$ iff the family $in(B) = \{in(P_1), \dots, in(P_r)\}$ generates the same ideal as $in(\mathcal{I})$.

We will use elimination orderings on monomials, which are particular admissible orderings :
an ordering *eliminates* the indeterminates $X_1, \dots, X_k$ if, when comparing two monomials, we compare first the parts involving $X_1, \dots, X_k$ (with any admissible ordering), and in case of equality, finally compare the parts involving $X_{k+1}, \dots, X_n$ (with any admissible ordering).
Then with such an ordering, the intersection of a standard basis of $\mathcal{I}$ with the ring $Z[X_{k+1}, \dots, X_n]$ is again a standard basis of the intersection of the ideal $\mathcal{I}$ with the same ring.

A standard basis of an ideal can be computed from a set of generators with a completion algorithm [Ja20] [Bu83] [Ga85].
When $\mathcal{I}$ is generated by differences of monomials, *and in this paper it will be always the case*, a standard basis contains again only differences of monomials, and can be viewed as a *convergent rewriting system* of rewrite rules on commutative words, and then can be also computed by a Knuth-Bendix completion algorithm modulo associativity and commutativity.

DEFINITIONS 5 : **Rewriting of polynomials, Gröbner basis**
Let us note $P \longrightarrow Q$ when $Q = P - X^\alpha R$, where $R \in B$ and $X^\alpha in(R)$ appears as a monomial of P.
We write $P \xrightarrow{*} Q$ when several steps of $\longrightarrow$ are used to obtain Q from P.
Then we have $P \in \mathcal{I} \iff P \xrightarrow{*} 0$, which is in fact a definition of a Gröbner basis.
We note $P \downarrow Q$ when P and Q can be reduced to the same polynomial.
P is said *in normal form* when it cannot be reduced by $\longrightarrow$.

STANDARD BASIS OF (AFFINE) SUB-GROUPS OF Z^n

SUB-GROUPS AND EQUATIONAL THEORIES ON MONOMIALS

The following connects subgroups with equational theories deduced from their generators.

THEOREM 1 :

Let $v_0, \dots, v_p$ being generators of H, with $v_0 \geq 1$.
Let $E = \{X^{v_i^+} = X^{v_i^-}\}_{i=0,\dots,p}$.
Then

$$v \in H \iff X^{v^+} =_E X^{v^-}$$

Proof :
$\Leftarrow$:
Let $X^\alpha =_E X^\beta$, and show $\alpha - \beta \in H$.

Let us formalize the fact that there is a succession of elementary uses of equations which proves $X^\alpha =_E X^\beta$:
$X^\alpha =_E X^\beta \implies \exists \varepsilon_1, \ldots, \varepsilon_k \in \{+,-\}, \alpha_1, \ldots, \alpha_k \geq 0$, such that
$X^\alpha = X^{v_{i_1}^{\varepsilon_1} + \alpha_1}$,
$X^\beta = X^{v_{i_k}^{\overline{\varepsilon}_k} + \alpha_k}$,
$\forall j = 1, \ldots, k-1$, $X^{v_{i_j}^{\overline{\varepsilon}_j} + \alpha_j} = X^{v_{i_{j+1}}^{\varepsilon_{j+1}} + \alpha_{j+1}}$,
(where $\overline{+} = -$ and $\overline{-} = +$).
We reason by induction on k.
If $k = 0$, then $\alpha = \beta$, and $\alpha - \beta = 0 \in H$.
If $k > 0$, then we have $v_{i_1}^{\overline{\varepsilon_1}} + \alpha_1 - \beta \in H$ by induction hypothesis. But

$$\alpha - \beta = v_{i_1}^{\varepsilon_1} + \alpha_1 - (v_{i_1}^{\overline{\varepsilon_1}} + \alpha_1) + (v_{i_1}^{\overline{\varepsilon_1}} + \alpha_1) - \beta = \pm v_{i_1} + (v_{i_1}^{\overline{\varepsilon_1}} + \alpha_1) - \beta$$

and then $\alpha - \beta \in H$.
$\Rightarrow$:
We need a lemma :

LEMMA 1 :

Let E an equational theory of monomials, containing an equation $X^\gamma = 1$, with $\gamma \geq 1$. Then

$$\forall u, \alpha, \beta \in N^n, \quad X^{\alpha+u} =_E X^{\beta+u} \iff X^\alpha =_E X^\beta$$

Proof :

$\Leftarrow$:
clear.
$\Rightarrow$:
Suppose $u \leq \gamma$, then $X^{u+(\gamma-u)}X^\alpha =_E X^{u+(\gamma-u)}X^\beta$, because $\gamma - u \geq 0$. Then $X^\gamma X^\alpha =_E X^\gamma X^\beta$.
But $X^\gamma =_E 1$, and then $X^\alpha =_E X^\beta$.
The case $u \not\leq \gamma$ reduces to the previous case by noticing that $u = (u - u \wedge \gamma) + u \wedge \gamma$, $u \wedge \gamma \leq \gamma$, $u - u \wedge \gamma < u$, and $\leq$ is well-founded.

We prove now the sufficient condition of the theorem.
Let $v \in H$, $v = \sum_i a_i v_i$. We proceed by induction on $\|v\|_1$.
If $\|v\|_1 = 0$ then $v = 0$ and $X^{v^+} =_E X^{v^-}$.
Suppose now that $a_j > 0$ (the case $a_j < 0$ reduces to treate $-v$ which leads to $X^{(-v)^+} =_E X^{(-v)^-}$, i.e. $X^{v^-} =_E X^{v^+}$).
we have $v = v_j + v' = v^+ - v^- = v_j^+ - v_j^- + v'^+ - v'^- = (v_j^+ + v'^+) - (v_j^- + v'^-)$.
By hypothesis of induction, $X^{v'^+} =_E X^{v'^-}$, and we have $X^{v_j^+} =_E X^{v_j^-}$, then $X^{v_j^+ + v'^+} =_E X^{v_j^- + v'^-}$.
But $(v_j^+ + v'^+) - v^+ = (v_j^- + v'^-) - v^- \geq 0$, then by the lemma 1, $X^{v^+} =_E X^{v^-}$.
□

EQUATIONAL THEORIES AND POLYNOMIALS IDEALS

Now we link equational theories on monomials and polynomials ideals (as in [MaMe82]).

LEMMA 2 :

Let $E = \{X^{\alpha_i} = X^{\beta_i}\}$ an equational theory on monomials, and let $\mathcal{I}$ the ideal of $Z[X_1, \ldots, X_n]$ generated by the polynomials $X^{\alpha_i} - X^{\beta_i}$.
Then

$$X^\alpha =_E X^\beta \iff X^\alpha - X^\beta \in \mathcal{I}$$

Proof :

$\Rightarrow$:
$X^\alpha =_E X^\beta \implies \exists \gamma_1, \ldots, \gamma_k, \overline{\gamma_1}, \ldots, \overline{\gamma_k}, \delta_1, \ldots, \delta_k$ such that
$\gamma_j = \alpha_{i_j}$ and $\overline{\gamma_j} = \beta_{i_j}$, or $\gamma_j = \beta_{i_j}$ and $\overline{\gamma_j} = \alpha_{i_j}$,
and such that
$X^\alpha = X^{\gamma_1+\delta_1}, X^\beta = X^{\overline{\gamma_k}+\delta_k}$ and
$\forall j = 1, \ldots, k-1$, $X^{\overline{\gamma_j}+\delta_j} = X^{\gamma_{j+1}+\delta_{j+1}}$.
(we just formalize the fact that there is a succession of elementary uses of equations which proves $X^\alpha =_E X^\beta$).
We proceed by induction on k.
If $k = 0$, then $\alpha = \beta$ and $0 \in \mathcal{I}$.
If $k > 0$, $X^\alpha - X^\beta = X^{\delta_1}(X^{\gamma_1} - X^{\overline{\gamma_1}}) + (X^{\overline{\gamma_1}+\delta_1} - X^\beta)$.
But $X^{\overline{\gamma_1}+\delta_1} - X^\beta \in \mathcal{I}$ by hypothesis of induction, and $X^{\gamma_1} - X^{\overline{\gamma_1}} \in \mathcal{I}$, then $X^\alpha - X^\beta \in \mathcal{I}$.
$\Leftarrow$:
We have $X^\alpha - X^\beta \in \mathcal{I} \iff X^\alpha - X^\beta = \sum_i Q_i(X^{\alpha_i} - X^{\beta_i})$.
We proceed by induction on the sum of the absolute values of the coefficients of the Q_i's.
If this sum is zero, then $\alpha = \beta$ and so $X^\alpha =_E X^\beta$.
If this sum is not null, then we can write $X^\alpha - X^\beta = X^\gamma(X^{\alpha_j} - X^{\beta_j}) + P$, where $P = \sum_i Q'_i(X^{\alpha_i} - X^{\beta_i})$, the sum of the absolute values of the coefficients of the Q'_i's being lesser than that of the Q_i's, and where $X^\alpha = X^{\gamma+\alpha_j}$ (or $X^\alpha = X^{\gamma+\beta_j}$ which reduces to treate $X^\beta - X^\alpha$).
We have $P = X^{\gamma+\beta_j} - X^\beta$, and $P \in \mathcal{I}$, then by hypothesis of induction we have $X^{\gamma+\beta_j} =_E X^\beta$.
But $X^\alpha = X^{\gamma+\alpha_j} =_E X^{\gamma+\beta_j}$, then $X^\alpha =_E X^\beta$.

IDEAL OF H

Using the previous results, we caracterize a sub-group by an ideal.

THEOREM 2 :

Let $v_1, \ldots, v_p$ generating H, and $\mathcal{J}_H$ the ideal generated by the polynomials $X^{v_i^+} - X^{v_i^-}$ and the polynomial $TX^1 - 1$, where T is a new indeterminate.
Then

$$v \in H \iff X^{v^+} - X^{v^-} \in \mathcal{J}_H$$

Proof :

We include H in Z^{n+1} by adding a zero coordinate to the v_i's, corresponding to the variable T. Let $v_0 = 1$, and H' generated by $v_0, v_1, \ldots, v_p$.
Then, by the theorem 1 and the lemma 2, we have $v \in H' \iff (X,T)^{v^+} - (X,T)^{v^-} \in \mathcal{J}_H$
and then $v \in H \iff X^{v^+} - X^{v^-} \in \mathcal{J}_H$.

It is clear that $\mathcal{J}_H$ does not depends of the choosen set of generators of H, so :

DEFINITION 6 :
Let $\mathcal{I}_H = \mathcal{J}_H \cap Z[X_1, \ldots, X_n]$.
$\mathcal{I}_H$ is called *the ideal of* H, and we have $v \in H \iff X^{v^+} - X^{v^-} \in \mathcal{I}_H$.

IDEAL OF $a + H$

We extend theorem 2 to affine sub-groups.

THEOREM 3 :

Let $v_1, \ldots, v_p$ generating H, and $\mathcal{J}_{a+H}$ the ideal generated by the polynomials $X^{v_i^+} - X^{v_i^-}$, $TUX^1 - 1$, and $UX^{a^-} - X^{a^+}$, where T and U are new indeterminates.
Then

$$v \in a + H \iff X^{v^+} - UX^{v^-} \in \mathcal{J}_{a+H}$$

Proof :

We include H in Z^{n+2} by adding two zero coordinates to the v_i's. Let $v_0 = 1$, $v_{p+1} = (a, 0, -1)$ and H' generated by $v_0, v_1, \ldots, v_p, v_{p+1}$.
Then, by the theorem 1 and the lemma 2, we have $v \in H' \iff (X,T,U)^{v^+} - (X,T,U)^{v^-} \in \mathcal{J}_{a+H}$ and then $v \in a + H \iff (v, 0, -1) \in H' \iff vX^{v^+} - UX^{v^-} \in \mathcal{J}_{a+H}$.

Again, it is clear that $\mathcal{J}_{a+H}$ does not depends of the choice of a and the choosen set of generators of H, so :

DEFINITION 7 :
Let $\mathcal{I}_{a+H} = \mathcal{J}_{a+H} \cap Z[U, X_1, \ldots, X_n]$.
$\mathcal{I}_{a+H}$ is called *the ideal of* $a + H$, and we have $v \in a + H \iff X^{v^+} - UX^{v^-} \in \mathcal{I}_{a+H}$.

STANDARD BASIS OF H AND $a + H$

DEFINITIONS 8 : **Standard basis of a (affine) sub-group.**
Let B a standard basis of $\mathcal{J}_H$ for an ordering eliminating T, and $\mathcal{B}s_H$ be the set of polynomials of B not containing T. Then $\mathcal{B}s_H$ is a standard basis of $\mathcal{I}_H$, and is called *a standard basis of* H.

Let B a standard basis of $\mathcal{J}_{a+H}$ for an ordering eliminating T and U, with $T > U$, and $\mathcal{B}s_H$ be the set of polynomials of B not containing T. Then $\mathcal{B}s_{a+H}$ is a standard basis of $\mathcal{I}_{a+H}$, and is called *a standard basis of* $(a + H)$.

By an easy remark, every polynomial of $\mathcal{B}s_H$ is of the form $X^{v^+} - X^{v^-}$, with $v \in H$.

SMALLEST NON ZERO VECTOR OF H

For $v \in Z^n$, we define $\|v\|_{1,\infty} := sup(\|v^+\|_1, \|v^-\|_1)$. We define $min_{1,\infty}(H)$ as the set of the smallest non zero vectors of H for $\|.\|_{1,\infty}$.

THEOREM 4 :

Suppose that $\mathcal{B}s_H$ is defined with a total degree ordering on $X_1, \ldots, X_n$. Suppose also that H is not reduced to 0. Then

$$\exists X^{v^+} - X^{v^-} \in \mathcal{B}s_H \text{ such that } v \in min_{1,\infty} H$$

Proof :

Let $\mathcal{B}s_H = \{X^{a_i^+} - X^{a_i^-}\}$. Remark that with the chosen ordering we have $\|\alpha_i\|_{1,\infty} = \|\alpha_i^+\|_1$.
Suppose that there exists in H a non zero vector v with $\|v\|_{1,\infty} < inf_i\{\|\alpha_i\|_{1,\infty}\}$.
It is then clear that $X^{v^+} - X^{v^-}$ is irreductible with $\mathcal{B}s_H$, but by theorem 2 we have $X^{v^+} - X^{v^-} \in \mathcal{I}_H$ and then $X^{v^+} - X^{v^-}$ reduces to 0 with $\mathcal{B}s_H$, which leads to a contradiction. Then a such v does not exists, and the result is obtained.

NON-NEGATIVE PARTS OF (AFFINE) SUB-GROUPS OF Z^n

MEMBERSHIP PROBLEM

From theorem 2 and theorem 3 we deduce immediately caracterizations of H^+ and $(a+H)^+$:

COROLLARY 1 :

$$v \in H^+ \iff X^v - 1 \in \mathcal{I}_H$$

$$v \in (a+H)^+ \iff X^v - U \in \mathcal{I}_{a+H}$$

TRIVIALITY PROBLEM

More, with their standard basis, we can directly test the triviality of H^+ and $(a+H)^+$:

THEOREM 5 :

$$(a+H)^+ \neq \emptyset \iff \exists (X^\alpha - U) \in \mathcal{B}s_{a+H}$$

$$H^+ \neq \{0\} \iff \exists (X^\alpha - 1) \in \mathcal{B}s_H$$

Proof :

First assertion :

$\Rightarrow$:

Let $v \in (a+H)^+$. We have $X^v - U \in \mathcal{I}_{a+H}$, then $X^v \downarrow U$ for the rewriting relation of $\mathcal{B}s_{a+H}$. But the normal form of X^v does not contain U (because of the ordering choosen for $\mathcal{B}s_{a+H}$), then U is not in normal form, and then there must exists in $\mathcal{B}s_{a+H}$ a polynomial $U - X^\alpha$.

$\Leftarrow$:

Clear, because $X^\alpha - U \in \mathcal{B}s_{a+H} \implies X^\alpha - U \in \mathcal{I}_{a+H} \implies \alpha \in (a+H)^+$.

Second assertion :

$\Rightarrow$:

Let $v \in H^+$, $v \neq 0$. Then X^v reduces to 1 with the rewriting relation of $\mathcal{B}s_H$, and then there must exists in $\mathcal{B}s_H$ a polynomial of the form $X^\alpha - 1$.

$\Leftarrow$:

Clear, because $X^\alpha - 1 \in \mathcal{B}s_H \implies X^\alpha - 1 \in \mathcal{I}_H \implies \alpha \in H^+$.

SMALLEST VECTORS OF $H^+ - \{0\}$ AND $(a+H)^+$

Suppose that $\mathcal{B}s_H$ (resp. $\mathcal{B}s_{a+H}$) is defined with a total degree ordering on $X_1, \ldots, X_n$. Then v such that $X^v - 1 \in \mathcal{B}s_H$ (resp. $X^v - U \in \mathcal{B}s_H$ is a vector of minimal norm $\|.\|_1$ in $H^+ - \{0\}$ (resp $(a+H)^+$).

MINIMAL ELEMENTS OF $(a + H)^+$

A standard basis of $a + H$ gives an element of $(a + H)^+$ when such an element exists. We will use this fact to give an algorithm computing the set $Min((a+H)^+)$ of minimal elements of $a + H$ for the partial ordering $\leq$ (is it well known that this set is finite).
Unformally we proceed as follows :
First we compute $\mathcal{B}s_{a+H}$ and get, if it exists, $v \in (a + H)^+$.
Then it is clear that every w in $Min((a + H)^+)$ different of v verifies $\exists i$, $w_i < v_i$.
We will then investigate every sets of the form $E_{i,k} = ((a + H) \cap \{x \mid x_i = k\})^+$, for every $i = 1, \ldots, n$, and every $k = 0, \ldots, v_i - 1$.
It is clear that these sets are non-negative parts of affine sub-groups $a_{i,k} + H_{i,k}$, where the $a_{i,k}$'s and generators of the $H_{i,j}$'s are obtained by linear algebra manipulations from a,H,i, and k [KaBa79].
And we have :

$$Min((a + H)^+) \subset \{v\} \cup \left(\bigcup_{i,k} Min((a_{i,k} + H_{i,k})^+) \right)$$

The dimensions of the $H_{i,k}$'s are either 0, either strictly lesser than the dimension of H, that proves the termination of the process.
Now we precise an algorithm **MINAFFINE** computing $Min((a + H)^+)$:

ALGORITHM 1 :

MINAFFINE(a, H): *(H is given by its generators)*
$\mathcal{B}s_{a+H}$:= a standard basis of $(a + H)$.
IF it exists $(X^\alpha - U)$ in $\mathcal{B}s_{a+H}$
THEN $v := \alpha$
ELSE RETURNS $\emptyset$
FOR i:= 1...n AND k:=0...$v_i - 1$ DO
Compute $a_{i,k}$ and generators of $H_{i,k}$ such that
$a_{i,k} + H_{i,k} = (a + H) \cap \{x \mid x_i = k\} \neq \emptyset$
RETURNS Minimals elements of $\{v\} \cup \left(\bigcup_{i,k} \text{MINAFFINE}(a_{i,k}, H_{i,k}) \right)$

We can remark that if we compute $\mathcal{B}s_{a+H}$ with a total degree ordering on $X_1, \ldots, X_n$, then $\|v\|_1$ is minimal and then we minimize the number of steps in the loop of the algorithm.

MINIMAL NON ZERO ELEMENTS OF H^+

The previous algorithm can be modified to compute minimal non zero elements of H^+ :
we just begin with $a = 0$, take v such that $X^v - 1 \in \mathcal{B}s_{a+H}$, and then continue the previous algorithm :

ALGORITHM 2 :

MINHOM(H):
$\mathcal{B}s_{a+H}$:= a standard basis of $(0 + H)$.
IF it exists $(X^\alpha - 1)$ in $\mathcal{B}s_{a+H}$
THEN $v := \alpha$
ELSE RETURNS $\emptyset$
FOR i:= 1...n AND k:=0...$v_i - 1$ DO
Compute $a_{i,k}$ and generators of $H_{i,k}$ such that
$a_{i,k} + H_{i,k} = H \cap \{x \mid x_i = k\} \neq \emptyset$
RETURNS Minimals elements of $\{v\} \cup \left(\bigcup_{i,k} \text{MINAFFINE}(a_{i,k}, H_{i,k}) \right)$

LINEAR DIOPHANTINE SYSTEMS

We show in this section how the previous results apply to the study of linear diophantine systems. We will study the following types of systems :

$$Ax = 0, x \geq 0$$

$$Ax = b, x \geq 0$$

$$Ax \leq b$$

where A is a matrix of integers with n columns and m rows, x is in Z^n, and b in Z^m.
Our aims are here :

- to test for the existence of solutions,
- to describe the set solutions,
- and to give algorithms for the computations of the solutions, by using standard basis, which is an new approach for these problems.

In the following, S will be the set of solutions of the considered system.

SYSTEMS $Ax = 0, x \geq 0$

Here $S = H^+$, where $H = Ker(A)$, which is an sub-group of Z^n. The computation of generators of H from A can be made by computing an Hermite normal form of A.
Theorem 5 and algorithm 1 give then the awnsers to our questions on S :

THEOREM 6 :

$$x \in S \iff X^x - 1 \in \mathcal{I}_H$$

$$S \neq \{0\} \iff \exists (X^\alpha - 1) \in \mathcal{B}s_H \implies \alpha \in S$$

and **MINHOM**(H) *is the set of minimal non zero elements of* S.

SYSTEMS $Ax = b, x \geq 0$

Let $A' = (A \mid b)$ and $H' = Ker(A')$. We introduce an new indeterminate $X_n + 1$, in order to define the ideal of H'.
Suppose that $\mathcal{B}s_{H'}$ is defined with an ordering such that $\forall i \leq n, X_{n+1} > X_i$. Then :

THEOREM 7 :

$$x \in S \iff X^x - X_{n+1} \in \mathcal{I}_{H'}$$

$$S \neq \emptyset \iff \exists X^\alpha - X_{n+1} \in \mathcal{B}s_{H'} \implies \alpha \in S$$

and the projection on Z^n *of* `MINHOM`(H') *is the set of minimal non zero elements of* S.

SYSTEMS $Ax \leq b$

Let $A' = (A \mid I_m \mid b)$ where I_m is the identity matrix of order m. Let $H' = Ker(A')$. To define the ideal of H' we introduce new indeterminates $Y_1, \ldots, Y_m$ and Z.
Suppose that $\mathcal{B}s_{H'}$ is defined with an ordering such that $\forall i \leq n, \forall j \leq m,\ Z > Y_j > X_i$. Then :

THEOREM 8 :

$$x \in S \iff \exists y,\ X^{x^+}Y^y - X^{x^-}Z \in \mathcal{I}_{H'}$$

$$S \neq \emptyset \iff \exists X^{x^+}Y^y - X^{x^-}Z \in \mathcal{B}s_{H'} \implies x \in S$$

QUESTIONS, CONJECTURES

We have caracterized (affine) sub-groups of Z^n and their non-negative parts by ideals. We have then a connection between commutative algebra and integer (semi-linear) algebra (see [St83], [Ol90], [LP91a], [CoTr91] for works in this aim).
Through this gap we can easily ask some questions on H and $\mathcal{I}_H$ (and resp on $a + H$ and $\mathcal{I}_{a+H}$) :

1. Is the dimension of H equal to the dimension of its ideal $\mathcal{I}_H$?
2. Is the number of integer points in an minimal cell of H (resp. $a + H$) equal to the multiplicity of $\mathcal{I}_H$?
3. Is the maximal size of minimal elements of H^+ (see [Tr75], [Ro89],[Do90], [LP91a], [LP90a]) related to the regularity of $\mathcal{I}_H$?
4. These three previous features of ideals (dimension, multiplicity, regularity) are given by the Hilbert-Samuel function and the Hilbert-Samuel polynomial of the ideal, and then can be read on a standard basis. What is the meaning on H of the coefficients of the Hilbert-Samuel polynomial of $\mathcal{I}_H$?
5. The computation of a standard basis has a double exponential complexity, even on ideal generated with differences of monomials [MaMe82]. But here we have always a polynomial $X^1 - 1$ in the generators, all our ideals are given with complete intersections, and we solve here at most NP-complete problems.

   So, is the computation of standard basis of $\mathcal{I}_H$ of simple exponential complexity?
6. There is some theoretical reasons to think that standard basis computations are strongly related to the geometry of problems they represent. If it is the case with H and H^+, we can think that algorithmical results presented here can be very usefull in practice.

In practice, we hope that implementations (in progress) will confirm this new approach for solving inequations on integers.
Finally we remark that many previous results can be extended to affine subgroups of Q^n and solving linear integer systems in the rationals, for example :

$$v \in (a+H)^+ \iff \exists k, X^v - U^k \in \mathcal{I}_{a+H}$$

$$(a+H)^+ \neq \emptyset \iff \exists X^a - U^k \in \mathcal{B}s_{a+H} \implies \frac{a}{k} \in (a+H)^+$$

References

[Bu83] B.Buchberger, "Gröbner basis: an algorithmic method in polynomial ideal theory" Camp. Publ. Nr. 83-29. 0, nov. 1983.

[CoTr91] P.Conti and C.Traverso "Buchberger algorithm and integer programming", internal report,Univ. Pisa, Italy, 91, submitted to publication.

[Do90] E.Domenjoud "Solving Systems fo Linear Diophantine Equations : An Algebraic Approch", UNIF'90, International Workshop on Unification, Leeds UK, july 1990.

[Ga85] A.Galligo "Algorithmes de calcul de bases standard", Preprint Université de Nice, France, 1985.

[Ja20] "Sur les systèmes d'équations aux dérivées partielles" Journal de Mathématiques, 8ème série, tome III, 1920.

[KaBa79] R.Kannan and A.Bachem, "Polynomials algorithms for computing the Smith and Hermite normal forms of an integer matrix", SIAM J. on Computing, vol. 8, no. 4, pp 499-507, 1979.

[MaMe82] E.W.Mayr and A.R.Meyer, "The complexity of the word problems for commutative semigroups and polynomials ideals",Advances in Math. no.46,pp305-329, 1982.

[Ol90] F.Ollivier "Le problème de l'identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité", Phd Thesis, Ecole Polytechnique, France, june 1990.

[LP90a] L.Pottier "Bornes et algorithmes de calcul des générateurs des solutions de systèmes diophantiens linéaires", internal report, INRIA, feb. 90, and Comptes Rendus de l'Académie des Sciences de Paris, t.311, Série I, p813-816,1990.

[LP91a] L.Pottier "Minimals solutions of linear diophantine systems : bounds and algorithms", Proc. RTA-91, LNCS 488, april 91.

[Ro89] J.F.Romeuf "Solutions of a linear diophantine system", UNIF'89, proc. of the third international Workshop on unification, Lambrecht, RFA 89.

[St83] R.P.Stanley "Combinatorics and commutative algebra", Progress in Mathematics, Birkäuser ed., 1983.

[Tr75] L.B.Treybig "Bounds in piecewise linear topology", Trans.AMS, v.201, 1975.

ISSN 0249-6399