T H È S E

présentée à

L'UNIVERSITÉ DES SCIENCES ET TECHNIQUES
DE LILLE I

pour obtenir le titre de

DOCTEUR DE SPÉCIALITÉ
(Mathématiques appliquées)

par

Jean-Charles FIOROT

STRUCTURES D'ENSEMBLES DE POINTS ENTIERS

Thèse soutenue le 1er Avril 1971, devant la Commission d'Examen :

Monsieur P. BACCHUS, Président
Monsieur P. POUZET, Examinateur
Monsieur J. CEA, Examinateur
Monsieur P. HUARD, Rapporteur

UNIVERSITE DE LILLE

FACULTE DES SCIENCES

DOYENS HONORAIRES

MM. H. LEFEBVRE, M. PARREAU.

PROFESSEURS HONORAIRES

MM. ARNOULT, BROCHARD, CAU, CHAPPELON, CHAUDRON, CORDONNIER, DEHEUVELS, DEHORNE, DOLLE, FLEURY, P. GERMAIN, KAMPE DE FERIET, KOURGANOFF, LAMOTTE, LELONG, Mme LELONG, MM. MAZET, MICHEL, NORMANT, PARISELLE, PAUTHENIER, ROIG, ROSEAU, ROUBINE, ROUELLE, WIEMAN, ZAMANSKY.

PROFESSEURS TITULAIRES

M. BACCHUS Pierre	Astronomie et Calcul
M. BEAUFILS Jean-Pierre	Chimie Générale
M. BLOCH Vincent	Psychophysiologie
M. BONNEMAN Pierre	Chimie Industrielle
M. BONTE Antoine	Géologie Appliquée
M. BOUGHON Pierre	Mathématiques
M. BOURIQUET Robert	Biologie Végétale
M. CELET Paul	Géologie Générale
M. CONSTANT Eugène	Electronique
M. CORSIN Pierre	Paléobotanique
M. DECUYPER Marcel	Mathématiques
M. DEDECKER Paul	Mathématiques
M. le Doyen DEFRETIN René	Directeur du Laboratoire de Biologie Maritime de Wimereux
M. DELATTRE Charles	Géologie Générale
M. DURCHON Maurice	Biologie Animale
M. FOURET René	Physique
M. GABILLARD Robert	Electronique
M. GLACET Charles	Chimie Organique
M. GONTIER Gérard	Mécanique des Fluides
M. GUILLAUME Jean	Biologie Végétale
M. HEUBEL Joseph	Chimie Minérale
Mme LENOBLE Jacqueline	Physique
M. MONTREUIL Jean	Chimie Biologique
Mme SCHWARTZ Marie Hélène	Mathématiques
M. TILLIEU Jacques	Physique
M. TRIDOT Gabriel	Chimie Minérale Appliquée E.N.S.C.L.
M. VIDAL Pierre	Automatique
M. VIVIER Emile	Biologie Animale
M. WATERLOT Gérard	Géologie et Minéralogie
M. WERTHEIMER Raymond	Physique

PROFESSEURS A TITRE PERSONNEL

M. BOUISSET Simon	Physiologie Animale
M. DELHAYE Michel	Chimie Physique et Minérale 1er Cycle
M. LINDER Robert	Biologie Végétale
M. LUCQUIN Michel	Chimie Physique
M. PARREAU Michel	Mathématiques
M. SAVARD Jean	Chimie Générale
M. SCHALLER François	Biologie Animale
M. SCHILTZ René	Physique

PROFESSEURS SANS CHAIRE

M. BELLET Jean	Physique
M. BODART Marcel	Biologie Végétale
M. BOILLET Pierre	Physique
M. DERCOURT Jean-Michel	Géologie et Minéralogie
M. DEVRAINNE Pierre	Chimie Minérale
Mle MARQUET Simone	Mathématiques
M. MONTARIOL Frédéric	Chimie Minérale Appliquée
M. PROUVOST Jean	Géologie et Minéralogie
M. VAILLANT Jean	Mathématiques

MAITRES DE CONFERENCE (et chargés des fonctions)

M. AUBIN Thierry	Mathématiques Pures
M. BEGUIN Paul	Mécanique des Fluides
M. BILLARD Jean	Physique
M. BKOUCHE Rudolphe	Mathématiques
M. BOILLY Bénoni	Biologie Animale
M. BONNOT Ernest	Biologie Végétale
M. CAPURON Alfred	Biologie Animale
M. CARREZ Christian	Calcul
M. CORDONNIER Vincent	Calcul
M. CORTOIS Jean	Physique
M. COULON Jean-Paul	Electrotechnique
M. DEBRABAN Pierre	Sciences Appliquées
M. ESCAIG Bertrand	Physique
M. FROLICH Daniel	Sciences Appliquées
M. GOBLOT Rémi	Mathématiques
M. GOUDMAND Pierre	Chimie Physique
M. GRUSON Laurent	Mathématiques
M. GUILBAULT Pierre	Physiologie Animale
M. HERMAN Maurice	Physique
M. HUARD de la MARRE Pierre	Calcul
M. JOURNEL Gérard	Sciences Appliquées
Mle KOSMANN Yvette	Mathématiques
M. LABLACHE COMBIER Alain	Chimie Générale
M. LACOSTE Louis	Biologie Végétale
M. LANDAIS Jean	Chimie Organique
M. LAURENT François	Automatique
M. LEHMANN Daniel	Mathématiques
Mme LEHMANN Josiane	Mathématiques
M. LOCQUENEUX Robert	Physique
M. LOUAGE Francis	Sciences Appliquées

M. LOUCHEUX Claude	Chimie Physique
M. MAES Serge	Physique
M. MAIZIERES Christian	Automatique
M. MESSELYN Jean	Physique
M. MIGEON Michel	Sciences Appliquées
M. MONTEL Marc	Physique
M. OUZIAUX Roger	Sciences Appliquées
M. PANET Marius	Electrotechnique
M. PAQUET Jacques	Sciences Appliquées
M. PARSY Fernand	Mécanique des Fluides
M. POVY Jean-Claude	Sciences Appliquées
M. RACZY	Radioélectrique
M. ROUSSEAU Jean-Paul	Biologie Animale
M. ROYNETTE Bernard	Mathématiques
M. SALMER Georges	Electronique
M. SMET Pierre	Physique
M. VANDORPE Bernard	Sciences Appliquées
M. WATERLOT Michel	Géologie Générale
Mme ZINN **JUSTIN** Nicole	Mathématiques

Je tiens à témoigner toute ma gratitude à Monsieur le Professeur BACCHUS pour l'honneur qu'il me fait de présider le jury de cette thèse.

Je sais gré à Monsieur le Professeur HUARD de m'avoir donné l'idée de ce travail et d'en avoir constamment suivi l'évolution. Je suis heureux de pouvoir lui exprimer ici toute ma reconnaissance pour les nombreux conseils et encouragements qu'il n'a cessé de me prodiguer.

Je remercie Monsieur le Professeur POUZET qui, il y a quelques années, m'a accueilli au Laboratoire de Calcul de la Faculté des Sciences et m'a donné le goût des mathématiques appliquées.

Je remercie Monsieur le Professeur CEA qui s'est intéressé à mon travail et qui a bien voulu accepter de faire partie du jury.

Que Monsieur le Professeur CHATELET, qui m'a encouragé à publier deux Notes aux Comptes Rendus de l'Académie des Sciences, trouve ici l'expression de ma respectueuse gratitude.

Je tiens aussi à remercier Mademoiselle DRIESSENS qui avec gentillesse et rapidité a tapé cette thèse ainsi que Monsieur et Madame DEBOCK qui avec les mêmes qualités ont permis sa réalisation.

TABLE des MATIERES

INTRODUCTION

L'optimisation en nombres entiers a pris, à cause de besoins bien définis (problème d'implantation, problème du voyageur de commerce, d'ordonnancement,...), une place importante en mathématiques. Diverses méthodes ont été mises au point depuis plus de dix ans mais n'ont pas toujours été satisfaisantes pour la résolution pratique de tous les problèmes. Comme dans bien d'autres domaines, un algorithme ou une approche mathématique efficace restent à trouver (s'ils existent !).

Rappelons brièvement que les méthodes existantes peuvent se classer en deux familles. D'une part les méthodes arborescentes ou d'énumération implicite qui peuvent fournir assez rapidement une solution optimale mais qui nécessitent généralement des temps de calcul assez élevés pour prouver que l'optimum est effectivement atteint. D'autre part, des méthodes qui reposent davantage sur des bases mathématiques (notion de congruence, de dualité, de théorème de séparation) et qui permettent d'affirmer qu'il y a convergence, mais celle-ci étant bien souvent acquise, si elle l'est, au bout de temps de calcul assez élevés. La limite entre ces deux familles n'étant d'ailleurs pas toujours bien définie. Ajoutons que la programmation en nombres entiers n'a pratiquement abordé, les méthodes booléennes mises à part ainsi que deux ou trois exceptions, que des problèmes avec contraintes et fonctionnelle de type linéaire.

Les nombreuses difficultés pour traiter ce problème proviennent, semble-t-il,du fait que nous ne savons pas expliquer la structure du point de vue des points entiers de sous-ensembles de $\mathbb{R}^n$ vérifiant certaines égalités ou inégalités, même de type linéaire. Ces difficultés sont celles que rencontre l'arithméticien. Elles sont ici accrues sur le plan pratique par le fait qu'en optimisation en nombres entiers les problèmes à traiter sont de grande taille par rapport à ceux de l'arithmétique traditionnelle : le nombre de variables est de l'ordre de la centaine et plus, dans quelques années il sera de l'ordre du millier et plus, le nombre des contraintes d'un ordre presque comparable. D'autre part, la dimension n'est pas la seule difficulté : même un problème de dimension modeste peut se révéler difficile à résoudre en raison du fait que le nombre de solutions à envisager peut être très grand

et n'est pas proportionnel à la dimension.

C'est dans cette optique que se place ce travail et qu'une approche a été faite. Nous sommes parvenus à expliquer (chapitre V) de manière exacte la structure de tous les points entiers d'un cône polyédrique de $\mathbb{R}^n$ (ou d'un module sur un anneau principal à base finie), c'est-à-dire à expliquer la structure du problème asymptotique. Cette approche est différente de ce qui avait été fait jusqu'alors. Nous nous intéressons aux points entiers eux-mêmes et non plus à leur enveloppe convexe (méthodes de découpe en général). Nous montrons que l'optimum en entier d'une fonctionnelle linéaire sur un cône polyédrique est un point d'une famille privilégiée mise en évidence appelée ensemble des "points fondamentaux". Cet ensemble et n vecteurs linéairement indépendants (que nous savons déterminer) portés par les arêtes du cône nous permettent de générer tous les points entiers du cône polyédrique. Une méthode constructive permet de sortir sur ordinateur tous ces éléments. Le nombre de ces points fondamentaux est donné par une formule très simple.

La méthode est ensuite appliquée au cas des parallélotopes de $\mathbb{R}^n$ (chapitre VI).

Nous pouvons mettre en similitude la théorie ainsi trouvée avec celle de la décomposition des polyèdres : aux points fondamentaux correspondent les sommets du polyèdre, aux vecteurs portés par les arêtes du cône correspondent les directions d'infinitude du polyèdre.

Avec la méthode rigoureuse qui a été définie, nous nous trouvons devant des situations très différentes les unes des autres. Pour certains cas, l'ensemble des points fondamentaux est très petit, ce qui nous donne rapidement l'optimum (réduit à un point parfois, ce qui nous permet de caractériser les matrices unimodulaires ou semi-modulaires), pour d'autres par contre, bien que cet ensemble soit toujours fini, il est très grand ; c'est le cas par exemple lorsqu'une contrainte, à fortiori plusieurs, sont presque parallèles aux plans de coordonnées, même si la dimension de l'espace dans lequel on se trouve est très petite, ce qui confirme ce que nous disions tout-à-l'heure.

Après un chapitre sur les notations et les définitions, nous rappelons dans le deuxième chapitre la résolution des systèmes linéaires en nombres entiers. Puis dans les deux chapitres suivants nous avons ajouté la résolution

des systèmes de congruences linéaires et des systèmes mixtes. En plus des résultats cités plus haut (chapitres V et VI), nous avons mis en évidence (chapitre VII) certaines propriétés importantes d'ordre algébrique et géométrique qui résultent de la théorie faite aux chapitres V et VI.

En annexe nous trouverons des programmes écrits en ALGOL testés sur M 40 B.G.E. qui fournissent :

. la résolution des systèmes linéaires en nombres entiers ;

. la recherche du pgcd de n nombres et de leurs coefficients dans l'identité de Bezout. Les codes obtenus sont performants ;

. la génération des points fondamentaux d'un cône polyédrique .

En ce qui concerne la bibliographie, elle est constituée de la manière suivante : d'une part les articles et ouvrages qui nous ont réellement servi et qui sont cités dans le texte, d'autre part les articles et ouvrages que nous avons consultés ou qui nous ont familiarisé à ce problème ou même qui ont été écrits pendant ce travail et même après.

Nous terminerons en disant que cette thèse regroupe pour l'essentiel deux notes parues aux Comptes Rendus de L'Académie des Sciences (en 1969 et 1970) ainsi que deux articles parus dans la Revue de la Direction des Etudes et Recherches de l'E.D.F. (en 1969 et 1970).

*

* *

Chapitre I

NOTATIONS et DEFINITIONS

I.1 NOTATIONS

$\mathbf{N}$: ensemble des entiers ≥ 0

$\mathbb{Z}$: ensemble des entiers rationnels

$A(m,n)$: matrice de format (m,n) c'est-à-dire à m lignes et n colonnes, à éléments dans $\mathbb{Z}$

A^j : colonne j de la matrice A

A_j : ligne j de la matrice A

A_R : sous-matrice de A composée de lignes dont les indices appartiennent au sous-ensemble R de $\mathbf{N}$

A^R : sous-matrice de A composée des colonnes dont les indices appartiennent au sous-ensemble R de $\mathbf{N}$

A_J^I : sous-matrice de A dont l'indice de la ligne et de la colonne d'un élément appartient respectivement aux sous-ensembles J et I

Soient p éléments $m_1, m_2, \ldots, m_p$ de $\mathbb{Z}$; on note :

$[m_1, m_2, \ldots, m_p] = m$ leur plus petit commun multiple (en abrégé p.p.c.m.),

$(m_1, m_2, \ldots, m_p) = d$ leur plus grand commun diviseur (en abrégé p.g.c.d.).

La relation $a|b$ signifie : << a divise b >>.

La relation $a \nmid b$ signifie : << a ne divise pas b >>.

$A_i.a$ désigne le produit scalaire du vecteur ligne A_i par le vecteur colonne a.

${}^tA^j$ désigne le vecteur ligne transposé du vecteur A^j.

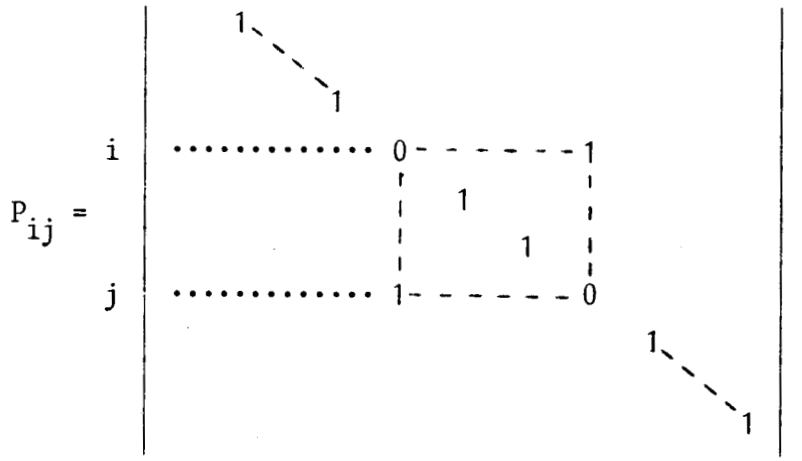
Etant donnés p vecteurs colonnes $B^1, \ldots, B^p$, nous notons par $B = [B^1, \ldots, B^p]$ la matrice dont les vecteurs colonnes sont B^j.

I.2 DEFINITIONS ET PROPRIETES

I.2.1 Matrice unimodulaire : matrice de forme carrée à éléments dans un anneau (ce sera toujours $\mathbb{Z}$) de déterminant +1 ou -1.

I.2.2 Matrice semi-modulaire : matrice de forme rectangulaire à éléments dans un anneau possédant une inverse à droite ou à gauche entière.

I.2.3 Matrice de transposition : matrice de la forme

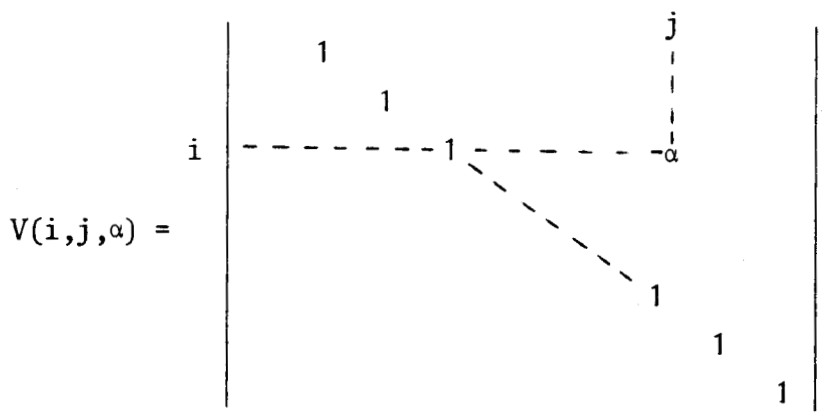


A étant une matrice quelconque :

La prémultiplication de A par P_{ij} (c.a.d. $P_{ij}A$) a pour effet de permuter les lignes i et j de A.

La postmultiplication de A par P_{ij} (c.a.d. AP_{ij}) a pour effet de permuter les colonnes i et j de A.

I.2.4 Matrice élémentaire :



La prémultiplication de A par $V(i,j,\alpha)$ a pour effet de retrancher à la $i^{ème}$ ligne de A α-fois la $j^{ème}$.

La postmultiplication de A par $V(i,j,\alpha)$ a pour effet de retrancher à la $j^{ème}$ colonne de A α-fois la $i^{ème}$.

Ces matrices sont des matrices unimodulaires.

I.2.5 Plus grand commun diviseur d'une matrice

On appelle p.g.c.d. d'ordre h d'une matrice A(m,n) noté $\Delta_h(A)$ le p.g.c.d. des déterminants de toutes les sous-matrices de format carré (h,h) de A.

On appelle p.g.c.d. de A noté $\Delta(A)$ le p.g.c.d. d'ordre r où r est le rang de A.

I.2.6 Matrices arithmétiquement équivalentes

A et B sont dites arithmétiquement équivalentes s'il existe deux matrices unimodulaires U et V telles que

$$B = UAV.$$

Proposition I : *Deux matrices arithmétiquement équivalentes ont même p.g.c.d. pour tous les ordres* h.

Il suffit de le montrer pour B = UA.

Considérons la sous-matrice de forme carrée B_J^I avec $|I| = |J| = i$. Alors,

$$\det (B_J^I) = \sum_{I'} \det (U_J^{I'}) \det (A_{I'}^I),$$

somme étendue à tout I' tel que $|I'| = i$.

Donc $\Delta_i(A) \mid \det (B_J^I)$ pour tout I et J de cardinal i, d'où $\Delta_i(A) \mid \Delta_i(B)$.

Réciproquement, comme $A = U^{-1}B$, $\Delta_i(B) \mid \Delta_i(A)$, d'où finalement $\Delta_i(A) = \Delta_i(B)$.

Remarque I : *Deux matrices arithmétiquement équivalentes ont même rang.*

Chapitre II

RESOLUTION des SYSTEMES LINEAIRES en NOMBRES ENTIERS

Dans ce chapitre nous rappelons deux techniques de résolution des systèmes linéaires en nombres entiers : celle basée sur la réduite d'Hermite (très rapide à notre avis) et celle basée sur la réduite de Smith (également rapide). La construction de ces deux réduites est établie dans le cas où les éléments de la matrice sont pris dans un anneau euclidien. On trouvera dans [17] la construction dans le cas où l'anneau est principal. Les systèmes s'écriront toujours :

$$Ax = b \qquad (II)$$

où les éléments de A et b sont dans $\mathbb{Z}$.

Le point nouveau est la mise sous forme triangulaire inférieure de la matrice donnant la forme générale de la solution de tels systèmes (corollaire II.3 et corollaire II.4).

II.1 RESOLUTION DES SYSTEMES LINEAIRES EN NOMBRES ENTIERS PAR LA METHODE D'HERMITE

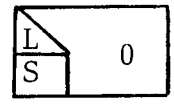
II.1.1 Triangularisation d'une matrice quelconque

Théorème II.1 : *Pour toute matrice* A(m,n) *de rang* r *à éléments dans un anneau euclidien il existe deux matrices unimodulaires* P *et* V, P *étant une matrice de permutations, telles que :*

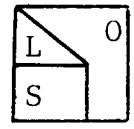
$$PAV = \left|\begin{array}{c|c} L & 0 \\ \hline S & 0 \end{array}\right| = H \qquad \text{(II.1.1.1)}$$

où L(r,r) *de rang* r *est triangulaire inférieure.* H *est dite la réduite d'Hermite de* A.

Remarque II.1 : Si m ≤ n, on a la configuration suivante

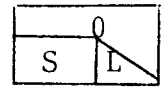
PAV = 

si m > n

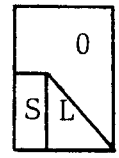
PAV = 

Remarque II.2 : La forme (II.1.1.1) étant obtenue par des transformations élémentaires et des transpositions sur les colonnes et des transpositions seules sur les lignes, en intervertissant le rôle des lignes et des colonnes on obtient deux matrices unimodulaires P et U, P étant une matrice de permutations, telles que

si n ≥ m

UAP = 

si m ≥ n

UAP = 

Corollaire II.1 : Pour toute matrice A(m,n) *de rang* r = inf(m,n) *à éléments dans un anneau euclidien, il existe deux matrices unimodulaires* U *et* V *telles que :*

si r = m ≤ n

$$AV = \begin{array}{|l\diagdown r|}\hline L \quad 0 \\ \hline \end{array} = H_1$$

$$UA = \begin{array}{|l|l\diagdown r|}\hline S & L \quad 0 \\ \hline \end{array} = H_2$$

si r = n ≤ m

$$AV = \begin{array}{|l\diagdown r|}\hline 0 \\ L \\ \hline S \\ \hline \end{array} = H_3$$

$$UA = \begin{array}{|l\diagdown r|}\hline 0 \\ L \\ \hline \end{array} = H_4$$

La démonstration est la même que celle du théorème II.1, mais comme le rang est maximal, il n'intervient pas dans la construction de matrices de transpositions donnant P.

Preuve du théorème II.1 :

a) Déterminons d'abord deux matrices unimodulaires P_1 et V_1, P_1 étant une matrice de transposition, telles que

$$P_1 A V_1 = \begin{array}{|c|c|}\hline a_1^1 & 0 \\ \hline & \overset{1}{A} \\ \hline \end{array} = \overset{1}{H}$$

Nous noterons toujours a_1^1 le terme qui est en position (1,1). Si i est l'indice de la première ligne non identiquement nulle de A, notons P_1 la matrice de transposition P_{1i} qui échange la ligne 1 avec la ligne i.

Notons par a_1^j les éléments de cette nouvelle première ligne. Soit a_1^k le plus petit terme en valeur absolue des termes non nuls de la première ligne.

Une transposition P_{1k}, notée P_2', échange les colonnes 1 et k et amène donc ce terme en position (1,1). On remplace les termes non nuls de (a_1^j), $j = 2,3,\ldots, n$ par leurs restes $p_2, p_3,\ldots, p_n$ après la division euclidienne par a_1^1.

$$a_1^j = \alpha_j\, a_1^1 + p_j \quad \text{avec} \quad 0 \leq |p_j| < |a_1^1| \quad j = 2,3,\ldots,n$$

Pour cela on multiplie à droite P_1 A P_2' par les transformations élémentaires $V(1,j,\alpha_j)$.

On obtient donc :

$$P_1 A P_2' V(1,2,\alpha_2)\ V(1,3,\alpha_3)\ \ldots\ V(1,n,\alpha_n) = \left[\begin{array}{c|c} a_1^1 & p_2\ p_3\ \ldots\ldots\ p_n \\ \hline & \end{array}\right] \qquad \text{(II.1.1.2)}$$

En fait, dans la pratique, on regroupe le produit $V(1,2,\alpha_2)\ \ldots\ V(1,n,\alpha_n)$ en une seule matrice unimodulaire

$$V(1,2,\alpha_2)\ V(1,3,\alpha_3)\ \ldots\ V(1,n,\alpha_n) = \begin{bmatrix} 1 & -\alpha_2 & -\alpha_3 & \ldots & -\alpha_n \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

Si $p_2 = p_3 = \ldots = p_n = 0$, alors la formule (II.1.1.2) donne $\overset{1}{H}$ avec

$$V_1 = P_2'\, V(1,2,\alpha_2)\ V(1,3,\alpha_3)\ \ldots\ V(1,n,\alpha_n)$$

Dans le cas contraire, on recommence sur la forme (II.1.1.2) ce que l'on a fait sur PAP_2'. Nous obtiendrons la forme $\overset{1}{H}$, puisqu'à chaque étape on remplace les termes non nuls autres que a_1^1 par des termes strictement plus petits en valeur absolue.

b) Si $\overset{1}{A} = 0$, alors $P = P_1$ et $V = V_1$ vérifiant (II.1.1.1), L se réduit à un seul élément a_1^1 ; le rang de A est 1.

Si $\overset{1}{A} \neq 0$, nous effectuons sur $\overset{1}{A}$ les transformations définies en a) pour obtenir la forme

$$P_2 \overset{1}{H} V_2 = P_2 P_1 A V_1 V_2 = \begin{array}{|c|c|c|} \hline a_1^1 & 0 & 0 \\ \hline a_2^1 & a_2^2 & 0 \\ \hline & & \overset{2}{A} \\ \hline \end{array} = \overset{2}{H}$$

Nous obtenons ainsi une suite de matrices $\overset{i}{A}$ dont les dimensions diminuent d'une unité chacune à chaque pas ; il existe r' avec $r' \leq m$ tel que $\overset{r'}{A} = 0$ ($\overset{r'}{A} = \emptyset$ si $r' = m$).

P A V, où $V = V_{r'}, \ldots V_1$ et $P = P_1 \ldots P_{r'}$, est donc de rang r' par construction et aussi de rang égal au rang de A = r (*remarque I*) ; donc $r = r'$; nous obtenons donc (II.1.1.1).

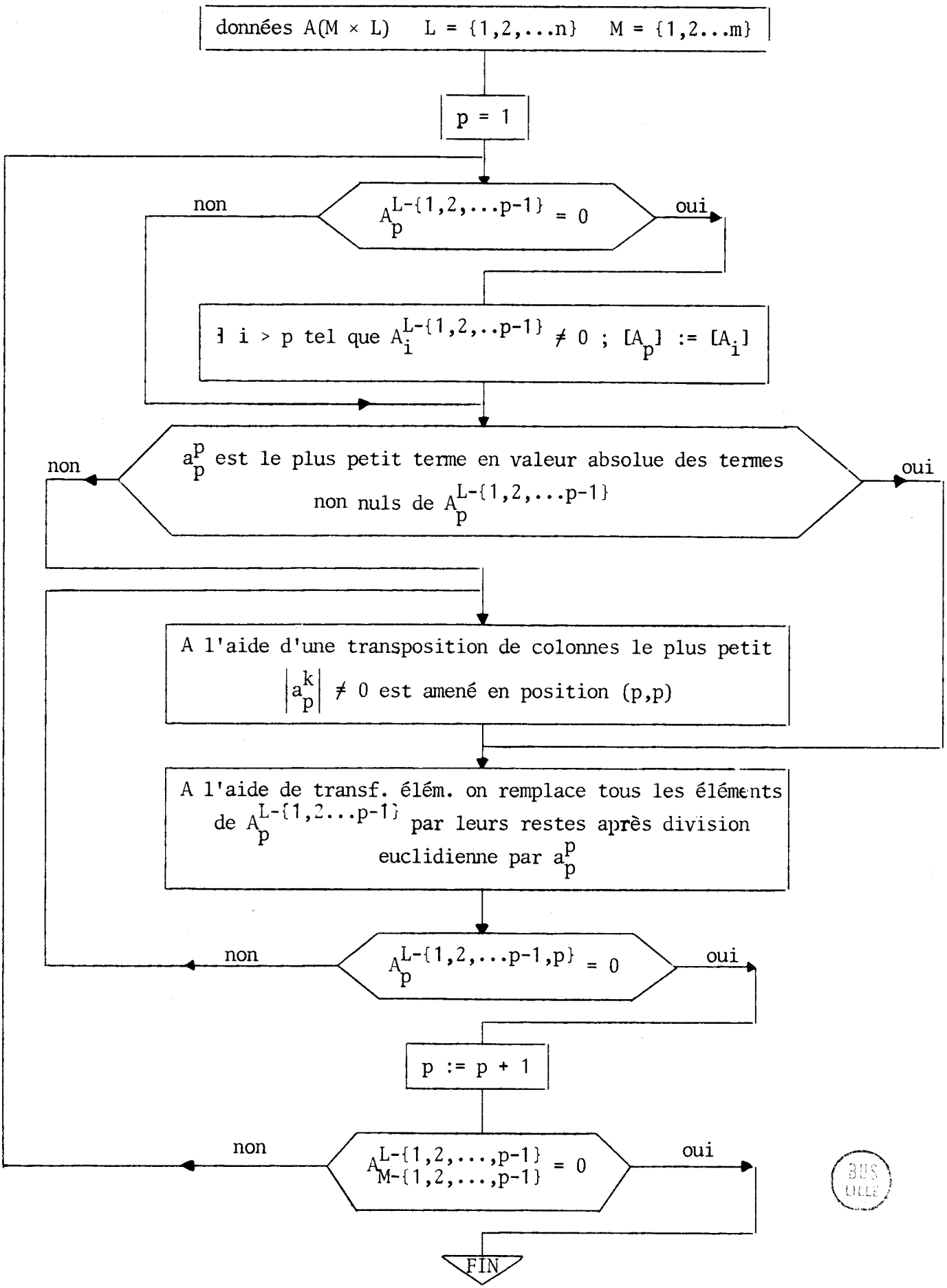
Remarque II.3 : L'étude ci-dessus peut être faite sans faire intervenir P ; H prend alors la forme en escalier irrégulier

$$AV = \begin{array}{|c|} \hline \diagdown \\ \hline 0 \\ \hline \end{array} = H$$

Remarque II.4 : De plus, nous pouvons dans le calcul de V ne pas faire intervenir les matrices de transpositions du type P'_2 ; H prend alors la forme

$$AV = \begin{array}{|c|c|c|} \hline & & \\ \hline & & \\ \hline & & \\ \hline \end{array}$$

II.1.2 Organigramme de la réduite d'Hermite



Nous pouvons donner une forme plus élaborée au théorème *II.1* sous la forme du corollaire suivant :

Corollaire II.2 : *La réduite* H *peut être telle que :*

1) Tous les termes de la diagonale de H *sont positifs.*

2)a) Tous les termes situés dans une même colonne au-dessous de l'élément diagonal sont inférieurs à ce dernier et sont positifs ou nuls ;

ou 2)b) Tous les termes situés dans une même ligne sont inférieurs à celui situé sur la diagonale et sont positifs ou nuls.

Il suffit de multiplier à droite ou à gauche par une matrice diagonale composée de +1 ou -1 bien appropriés pour obtenir *1)*.

Il suffit de multiplier à gauche dans le cas *2)a)*, à droite dans le cas *2)b)*, par des matrices élémentaires.

Exemple II.1 - Calcul de la réduite d'Hermite de

$$A = \begin{vmatrix} 3 & 2 & 1 & 4 \\ 6 & 4 & 2 & 8 \\ 1 & 2 & 0 & 1 \\ 2 & 4 & 0 & 2 \\ 2 & 0 & -1 & 3 \end{vmatrix}$$

$$P = P_1P_2 = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{vmatrix} \times \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{vmatrix}$$

$$V = V_1V_2V_3V_4V_5V_6 = \begin{vmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} 1 & -2 & -3 & -4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -2 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{vmatrix} \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 1 \end{vmatrix} =$$

$$\begin{vmatrix} 0 & 1 & -1 & -6 \\ 0 & 0 & 0 & 1 \\ 1 & -3 & -1 & 0 \\ 0 & 0 & 1 & 4 \end{vmatrix}$$

$$\text{d'où} \qquad PAV = \begin{vmatrix} 1&0&0&0&0\\ 0&0&1&0&0\\ 0&0&0&0&1\\ 0&0&0&1&0\\ 0&1&0&0&0 \end{vmatrix} \times \begin{vmatrix} 3&2&1&4\\ 6&4&2&8\\ 1&2&0&1\\ 2&4&0&2\\ 2&0&-1&3 \end{vmatrix} \times \begin{vmatrix} 0&1&-1&-6\\ 0&0&0&1\\ 1&-3&-1&0\\ 0&0&1&4 \end{vmatrix} = \begin{vmatrix} 1&0&0&0\\ 0&1&0&0\\ -1&5&2&0\\ 0&2&0&0\\ 2&0&0&0 \end{vmatrix}$$

$$L = \begin{vmatrix} 1&0&0\\ 0&1&0\\ -1&5&2 \end{vmatrix} \qquad A \text{ est de rang } 3$$

on remarque que V_1, V_3, V_5 sont des matrices de transposition .

II.1.3 Conditions d'existence des solutions et résolution de $Ax = b$.

Soit $H = \left|\begin{array}{c|c} L & 0 \\ \hline S & 0 \end{array}\right| = P\,A\,V$ une réduite d'Hermite de A (de rang r).

Posons $R = \{1,2,\ldots,r\}$, $\bar{R} = \{r+1,r+2,\ldots,n\}$, $\bar{\bar{R}} = \{r+1,r+2,\ldots,m\}$.

Proposition II.1 : *Une condition nécessaire et suffisante pour que* (II) *ait une solution entière est que*

$$\begin{cases} L^{-1} P_R\, b \text{ soit entier} \\ S L^{-1} P_R\, b = P_{\bar{\bar{R}}}\, b \end{cases} \qquad (II.1.3.1)$$

En effet, (II) est équivalent à

$$P\,A\,V\,V^{-1}x = Pb \quad \text{ou}$$

$$HV^{-1}x = Pb \qquad (II.1.3.2)$$

Donc, en posant $y = V^{-1}x$, (II.1.3.2) devient

$$\begin{cases} Ly_R = P_R b \\ Sy_R = P_{\bar{\bar{R}}} b \\ y_{\bar{R}} \text{ entier quelconque} \end{cases}$$

Ce qui donne bien la proposition, car x entier est équivalent à y entier (V étant unimodulaire).

On reporte y_R résolu dans $x = Vy = V^R y_R + V^{\bar{R}} y_{\bar{R}}$, d'où :

Théorème II.2 : Sous les conditions d'existence (II.1.3.1), *la solution du système* (II) *est donnée par*

$$x = V^R L^{-1} P_R b + V^{\bar{R}} y_{\bar{R}} \qquad \text{(II.1.3.3)}$$

où $\hat{x} = V^R L^{-1} P_R b$ *est une solution particulière et* $V^{\bar{R}} y_{\bar{R}}$ *est la solution générale de l'équation homogène ; la solution dépend donc linéairement de* n-r *paramètres* $y_{\bar{R}}$.

Exemple II.2 - Résolution du système linéaire suivant :

$$\begin{array}{rcrcrcrcl} 3x_1 & + & 2x_2 & + & x_3 & + & 4x_4 & = & 5 \\ 6x_1 & + & 4x_2 & + & 2x_3 & + & 8x_4 & = & 10 \\ x_1 & + & 2x_2 & + & & + & x_4 & = & 2 \\ 2x_1 & + & 4x_2 & & & + & 2x_4 & = & 4 \\ 2x_1 & & & - & x_3 & + & 3x_4 & = & 7 \end{array}$$

La réduite d'Hermite de la matrice du système a été calculée à l'exemple II.1.

Calculons $Pb = \begin{vmatrix} 5 \\ 2 \\ 7 \\ 4 \\ 10 \end{vmatrix}$

Ax = b est équivalent à (en posant x = Vy)

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 5 & 2 & 0 \\ 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{vmatrix} \begin{vmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{vmatrix} = \begin{vmatrix} 5 \\ 2 \\ 7 \\ 4 \\ 10 \end{vmatrix}$$

$$L = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 5 & 2 \end{vmatrix} \qquad L^{-1} = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{1}{2} & \frac{-5}{2} & \frac{1}{2} \end{vmatrix} \qquad y_R = L^{-1} P_R b = \begin{vmatrix} 5 \\ 2 \\ 1 \end{vmatrix} \text{ entier } = \begin{vmatrix} y_1 \\ y_2 \\ y_3 \end{vmatrix}$$

on vérifie que

$$\begin{vmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \end{vmatrix} \begin{vmatrix} y_1 \\ y_2 \\ y_3 \end{vmatrix} = \begin{vmatrix} 4 \\ 10 \end{vmatrix}$$

d'où la solution :

$$x = Vy = \begin{vmatrix} 0 & 1 & -1 & -6 \\ 0 & 0 & 0 & 1 \\ 1 & -3 & -1 & 0 \\ 0 & 0 & 1 & 4 \end{vmatrix} \begin{vmatrix} 5 \\ 2 \\ 1 \\ y_4 \end{vmatrix} = \begin{vmatrix} 1 \\ 0 \\ -2 \\ 1 \end{vmatrix} + y_4 \begin{vmatrix} -6 \\ 1 \\ 0 \\ 4 \end{vmatrix}$$

$$\boxed{\begin{aligned} x_1 &= 1 - 6y_4 \\ x_2 &= \quad\ y_4 \\ x_3 &= -2 \\ x_4 &= 1 + 4y_4 \end{aligned}} \qquad y_4 \in Z$$

Corollaire II.3 : *Sous les conditions d'existence* (II.1.3.1) *la solution du système* (II) *se mettra sous la forme*

$$x = \overset{\circ}{x} + W^{\bar{R}} y_{\bar{R}}$$

ou $W^{\bar{R}}$ *est une matrice triangulaire inférieure.*

$V^{\bar{R}}(n,n-r)$ qui figure dans (II.1.3.3) est de rang n-r, le corollaire *II.1* montre l'existence d'une matrice unimodulaire $V_1(n-r,n-r)$ telle que

$$V^{\bar{R}} V_1' = \boxed{\begin{array}{c} \diagdown \\ 0 \end{array}}$$

Considérons alors la matrice unimodulaire $V_1(n,n)$ construite de la manière suivante à partir de V_1'

$$V_1 = \begin{array}{|cc|} \hline \begin{matrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{matrix} & 0 \\ \hline 0 & V_1' \\ \hline \end{array}$$

$$PAVV_1 = HV_1 = H, \qquad H \text{ est conservée}$$

d'où en posant $W = VV_1$, $W^R = V^R$ et $W^{\bar{R}} = V^{\bar{R}}V_1'$, on obtient bien

$$x = Wy = W^R y + W^{\bar{R}} y_{\bar{R}}$$

$$x = \overset{\circ}{x} + W^{\bar{R}} y_{\bar{R}}$$

avec $W^{\bar{R}}$ triangulaire inférieure.

Exemple II.3

Résoudre
$$2x_1 - 2x_2 - 4x_3 - 6x_4 + 8x_5 = -2$$
$$5x_1 - 2x_2 + x_3 - 5x_4 - 3x_5 = -4$$

$$V = \begin{vmatrix} 1 & 0 & -1 & 1 & 3 \\ 0 & -3 & 3 & 10 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & -2 & -3 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix} \qquad R = \{1,2\} \qquad \bar{R} = \{3,4,5\}$$

$$AV = \begin{vmatrix} 2 & 0 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 & 0 \end{vmatrix} \qquad L = \begin{vmatrix} 2 & 0 \\ 5 & 1 \end{vmatrix}, \quad L^{-1} = \begin{vmatrix} 1/2 & 0 \\ -5/2 & 1 \end{vmatrix}$$

$$S = \emptyset \qquad P_{\bar{R}} = \emptyset$$

$$L^{-1}b = \begin{vmatrix} -1 \\ 1 \end{vmatrix} = \begin{vmatrix} y_1 \\ y_2 \end{vmatrix}$$

$$V^{\bar{R}} = \begin{vmatrix} -1 & 1 & 3 \\ 3 & 10 & 1 \\ 1 & 0 & 0 \\ -2 & -3 & 2 \\ 0 & 0 & 1 \end{vmatrix} \qquad V_1' = \begin{vmatrix} -1 & 9 & -29 \\ 0 & -3 & 10 \\ 0 & 4 & -13 \end{vmatrix}$$

$$V\bar{R}V' = \begin{vmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ -1 & 9 & -29 \\ 2 & -1 & 2 \\ 0 & 4 & -13 \end{vmatrix} \qquad \text{d'où} \qquad V_1 = \left|\begin{array}{cc|ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 9 & -29 \\ 0 & 0 & 0 & -3 & 10 \\ 0 & 0 & 0 & 4 & -13 \end{array}\right|$$

$$W = VV_1 = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & -3 & -3 & 1 & 0 \\ 0 & 0 & -1 & 9 & -29 \\ 0 & 1 & 2 & -1 & 2 \\ 0 & 0 & 0 & 4 & -13 \end{vmatrix}$$

$$x = \overset{\circ}{x} + W\bar{R}y_{\bar{R}} = \begin{vmatrix} -1 \\ -3 \\ 0 \\ 1 \\ 0 \end{vmatrix} + \begin{vmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ -1 & 9 & -29 \\ 2 & -1 & 2 \\ 0 & 4 & -13 \end{vmatrix} \begin{vmatrix} y_3 \\ y_4 \\ y_5 \end{vmatrix}$$

$$\begin{vmatrix} x_1 = -1 + y_3 \\ x_2 = -3 - 3y_3 + y_4 \\ x_3 = 0 - y_3 + 9y_4 - 29y_5 \\ x_4 = 1 + 2y_3 - y_4 + 2y_5 \\ x_5 = 0 + 4y_4 - 13y_5 \end{vmatrix} \qquad \begin{array}{l} y_3\ y_4\ y_5 \text{ entiers} \\ \text{rationnels arbitraires} \end{array}$$

II.1.4 Application au calcul du p.g.c.d. de n nombres et de leurs coefficients dans l'identité de Bézout.

Etant donnés n éléments $a_1, a_2, \ldots, a_n$ d'un anneau euclidien, nous nous proposons de calculer leur p.g.c.d. ainsi que leurs coefficients dans l'identité de Bézout. Ceci constitue une mise en forme de [5] à l'aide des matrices unimodulaires et de la réduite d'Hermite d'une matrice à éléments dans un anneau euclidien.

Un programme écrit en ALGOL se trouve en annexe 5. Les résultats sur ordinateur sont obtenus de manière très rapide.

Proposition II.2 : *La multiplication à droite (resp. à gauche) d'une matrice A par une matrice unimodulaire V conserve le p.g.c.d. des éléments de chaque ligne (resp. de chaque colonne).*

En effet, soit $B = AV$; $B_i = A_iV$.

Soit d_i le p.g.c.d. des éléments de la ligne A_i, on note $d_i = (a_i^1, a_i^2, \ldots, a_i^n)$.

Les éléments de la ligne B_i étant des éléments de l'idéal engendré par $(a_i^1, a_i^2, \ldots, a_i^n)$ sont des multiples de d_i, par suite si on note

$$d_i' = (b_i^1, \ldots, b_i^n) \quad \text{nous avons donc} \quad d_i | d_i'.$$

Or inversement nous avons $A = BV^{-1}$; donc de $A_i = B_i V^{-1}$ le même raisonnement entraîne que $d_i' | d_i$ d'où $d_i = d_i'$ $\forall i$

II.1.4.1 Application - Algorithme d'Euclide révisé

Etant donnés n entiers rationnels $a_1, \ldots, a_n$ nous nous proposons de rechercher $d = (a_1, \ldots, a_n)$ et n entiers rationnels $x_1, \ldots, x_n$ tels que $d = x_1a_1 + x_2a_2 + \ldots + x_na_n$ (identité de Bézout).

Pour cela il suffit de calculer la réduite d'Hermite de la matrice à une ligne $A = [a_1, a_2, \ldots, a_n]$.

Pour plus de simplification nous n'utilisons pas les matrices permutations de colonnes pour la construction de la réduite d'Hermite.

Il existe donc une matrice unimodulaire V(n,n) telle que

$$[a_1, a_2, \ldots, a_n] \begin{bmatrix} V_1^1 & V_1^2 & & V_1^i & V_1^n \\ & & & & \\ & & & & \\ V_n^1 & V_n^2 & & V_n^i & V_n^n \end{bmatrix} = [0, \ldots 0, \overset{i}{d}, 0, \ldots 0]$$

D'après la proposition précédente d est le p.g.c.d. de $a_1, a_2, \ldots, a_n$ et $d = V_1^i a_1 + V_2^i a_2 + \ldots + V_n^i a_n$.

Comme la matrice V n'est pas unique on retrouve le fait que la décomposition de d ne l'est pas non plus.

Exemple II.4 - Calcul du p.g.c.d. de -46, 38, 280, 126.

On trouve par exemple

$$V = \begin{bmatrix} 3 & 3 & -3 & -5 \\ -3 & 7 & -11 & -16 \\ 0 & 0 & 1 & 0 \\ 2 & -1 & 0 & 3 \end{bmatrix}$$

et $d = 2 = 3.(-46) + 7.(38) + 0.(280) - 1.(126)$

II.2 RESOLUTION DES SYSTEMES LINEAIRES EN NOMBRES ENTIERS PAR LA FORME NORMALE ET LA REDUITE DE SMITH

II.2.1 Diagonalisation d'une matrice quelconque

Théorème II.3 : Pour toute matrice A(m,n) *de rang* r *à éléments dans un anneau euclidien, il existe deux matrices unimodulaires* U *et* V *telles que*

$$UAV = \begin{array}{|c|c|} \hline \begin{matrix} d_1 & & \\ & d_2 & \\ & & \ddots\, d_r \end{matrix} & 0 \\ \hline 0 & 0 \\ \hline \end{array} = D \qquad (II.2.1.1)$$

où la matrice diagonale D *de rang* r *est dite forme normale de* A.

Preuve :

a) Déterminons d'abord deux matrices unimodulaires U_1 et V_1 telles que

$$U_1 A V_1 = \begin{array}{|c|c|} \hline d_1 & 0 \\ \hline 0 & \overset{1}{A} \\ \hline \end{array} = \overset{1}{D}$$

Pour cela on procède de la manière suivante : par une permutation de lignes et de colonnes, on amène le plus petit terme en valeur absolue des termes non nuls en position (1.1) ; soit a_1^1 ce terme.

Comme dans le cas de la réduite d'Hermite, nous remplaçons à l'aide de matrices élémentaires chaque terme de la première ligne (multiplication à droite) et de la première colonne (multiplication à gauche) par son reste dans la division euclidienne par a_1^1.

Si ces restes sont nuls, on obtient $\overset{1}{D}$. Sinon, on recommence sur la matrice obtenue ce que l'on a fait sur A. Nous obtiendrons la forme $\overset{1}{D}$, puisqu'à chaque étape on remplace les termes non nuls autres que a_1^1 par des termes strictement plus petits en valeur absolue.

b) Si $\overset{1}{A} = 0$ alors $U = U_1$ et $V = V_1$ vérifient (II.2.1.1). Si $\overset{1}{A} \neq 0$, nous effectuons sur $\overset{1}{A}$ les transformations définies en a) pour obtenir la forme

$$\overset{1}{U_2 D V_2} = U_2 U_1 A V_1 V_2 = \begin{array}{|c|c|c|} \hline d_1 & 0 & 0 \\ \hline 0 & d_2 & 0 \\ \hline 0 & 0 & \overset{2}{A} \\ \hline \end{array} = \overset{2}{D}$$

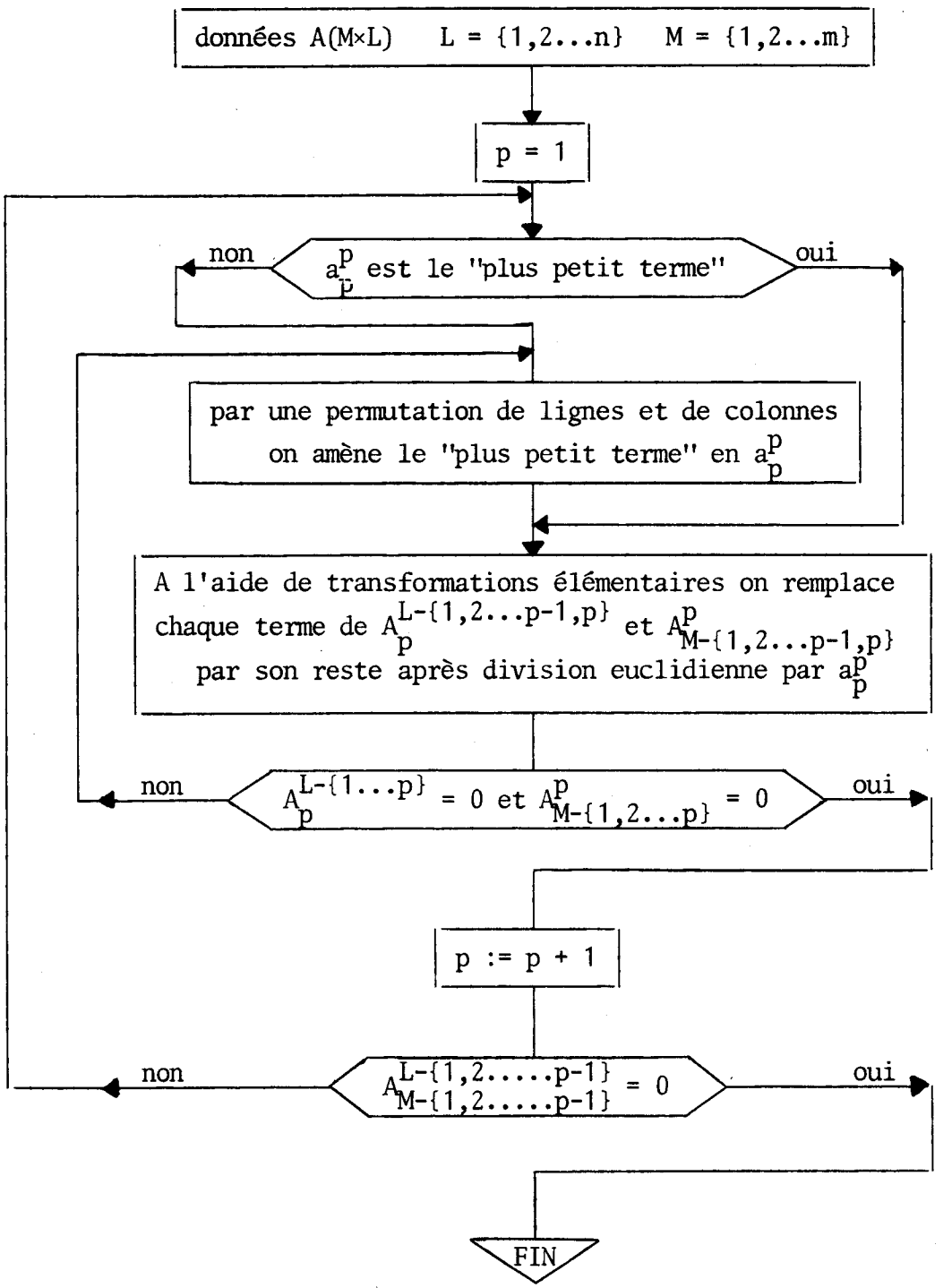
Nous obtenons ainsi une suite de matrices $\overset{i}{A}$ dont les dimensions diminuent d'une unité chacune à chaque pas : il existe r' avec $r' \leq m$ tel que $\overset{r'}{A} = 0$ ($\overset{r'}{A} = \emptyset$ si $r = m$). UAV, où $U = U_r, \ldots U_1$ et $V = V_1 \ldots V_r$, est donc de rang r' par construction et aussi égal à celui de A, soit r (remarque *I*) ; donc $r = r'$; nous obtenons donc (II.2.1.1).

Remarque II.5 : L'étude ci-dessus peut être faite sans faire intervenir les matrices de transposition ou de permutations mais seulement les matrices élémentaires (ce qui allège le calcul de U et V). On obtient alors la matrice diagonale généralisée suivante :

$$UAV = \begin{array}{|c|c|c|c|c|c|c|c|c|c|} \hline & & & & & & & & d_5 & \\ \hline & & d_1 & & & & & & & \\ \hline & & & & & d_2 & & & & \\ \hline & & & d_3 & & & & & & \\ \hline & & & & & & & d_4 & & \\ \hline & & & & & & & & & \\ \hline \end{array} = D$$

II.2.2 Organigramme de la forme normale de Smith

"Plus petit terme" désignant dans l'organigramme le plus petit terme en valeur absolue des termes non nuls de la matrice A.



Exemple II.5 - Calcul de la forme normale de Smith de

$$A = \begin{vmatrix} 1 & 1 & 1 & -4 & 1 \\ 1 & -1 & 1 & 3 & -2 \\ 2 & 0 & 2 & -1 & -1 \end{vmatrix}$$

on trouve

$$U = \begin{vmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & -1 & 1 \end{vmatrix} \qquad \text{et} \qquad V = \begin{vmatrix} 1 & 1 & -1 & 1 & 1 \\ 0 & 3 & 0 & 7 & 2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

$$\text{et} \qquad UAV = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{vmatrix} = D$$

II.2.3 Conditions d'existence des solutions et résolution de Ax = b

Soit

$$D = \begin{vmatrix} d_1 & & & & \\ & d_2 & & & \\ & & \ddots & & \\ & & & d_r & \\ & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{vmatrix} = UAV$$

une forme normale de A(m,n) de rang r.

Proposition II.3 : *Une condition nécessaire et suffisante pour que* (II) *ait une solution est que*

$$\begin{cases} (D_R^R)^{-1} U_R \, b \text{ soit entier} \\ U_{\bar{R}} b = 0 \end{cases} \qquad \text{(II.2.3.1)}$$

En effet, (II) est équivalent à

$$UAV\, V^{-1} x = Ub$$

ou

$$DV^{-1} x = Ub \qquad \text{(II.2.3.2)}$$

donc en posant $y = V^{-1}x$, (II.2.3.2) devient

$$\begin{cases} D_R^R \, y_R = U_R \, b \\ 0 = U_{\bar{R}} \, b \\ y_{\bar{R}} \text{ entier arbitraire} \end{cases} \qquad \text{(II.2.3.3)}$$

ce qui donne bien la proposition, car x entier est équivalent à y entier (V étant unimodulaire).

Remarque II.6 : Les conditions (II.2.3.1) peuvent se mettre sous une forme plus explicite en posant $b'_i = U_i b$; on trouve :

$$\begin{cases} d_i \mid b'_i & \text{pour} \quad i \in R \\ b'_i = 0 & \text{pour} \quad i \in \bar{R} \end{cases} \qquad \text{(II.2.3.4)}$$

Théorème II.4 : *Sous les conditions d'existence* (II.2.3.1), *la solution du système* (II) *est donnée par*

$$x = V^R (D_R^R)^{-1} \, U_R b + V^{\bar{R}} \, y_{\bar{R}}$$

où $\overset{\circ}{x} = V^R (D_R^R)^{-1} \, U_R b$ *est une solution particulière de* (II) *et* $V^{\bar{R}} y_{\bar{R}}$ *est la solution générale de l'équation homogène ; elle dépend donc linéairement de* (n-r) *paramètres* $y_{\bar{R}}$.

Pour obtenir ce résultat on écrit $x = Vy$ avec les conditions (II.2.3.3).

Remarque II.7 : Si r = m, les conditions d'existence (II.2.3.4) se réduisent à

$$d_i \mid b'_i \qquad \text{pour } i \in M.$$

Remarque II.8 : Si $d_i = 1$, pour tout $i \in R$, les conditions d'existence (II.2.3.4) se réduisent à

$$b'_{\bar{R}} = 0$$

Remarque II.9 : Si r = m et $d_i = 1$ pour tout i, le système (II) admet toujours des solutions. Nous caractériserons de telles matrices au corollaire *II.5*.

Corollaire II.4 : Sous les conditions d'existence (II.2.3.1), *la solution du système* (II) *se mettra sous la forme*

$$x = \overset{\circ}{x} + W^{\bar{R}} y_{\bar{R}}$$

où $W^{\bar{R}}$ *est une matrice triangulaire inférieure.*

La démonstration est identique à celle du corollaire *II.3*.

Exemple II.6 - Résolution du système linéaire suivant :

$$\begin{aligned} x_1 + x_2 + x_3 - 4x_4 + x_5 &= 0 \\ x_1 - x_2 + x_3 + 3x_4 - 2x_5 &= 2 \\ 2x_1 \quad + 2x_3 - 1x_4 - 1x_5 &= 2 \end{aligned}$$

Nous avons (exemple *II.5*) U, V et D.

$$R = \{1,2\} \qquad \bar{R} = \{3,4,5\}.$$

Le calcul de la réduite d'Hermite de $V^{\bar{R}}$ donne

$$V_1' = \begin{vmatrix} -1 & -2 & 5 \\ 0 & 1 & -2 \\ 0 & -3 & 7 \end{vmatrix}$$

et pour réduite

$$H = V^{\bar{R}} V_1' = \begin{vmatrix} -1 & 1 & 1 \\ 0 & 7 & 2 \\ 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{vmatrix} \times \begin{vmatrix} -1 & -2 & 5 \\ 0 & 1 & -2 \\ 0 & -3 & 7 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & -2 & 5 \\ 0 & -1 & 3 \\ 0 & -3 & 7 \end{vmatrix}$$

$$\text{or} \qquad V_1 = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & 5 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & -3 & 7 \end{vmatrix}$$

$$W = VV_1 = \begin{vmatrix} 1 & 1 & -1 & 1 & 1 \\ 0 & 3 & 0 & 7 & 2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -2 & 5 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & -3 & 7 \end{vmatrix} = \begin{vmatrix} 1 & 1 & -1 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 \\ 0 & 0 & -1 & -2 & 5 \\ 0 & 1 & 0 & -2 & 3 \\ 0 & 0 & 0 & -3 & 7 \end{vmatrix}$$

$$Dy = Ua \Longrightarrow y_1 = 0,\ y_2 = 2$$

$x = W^R y_R + W^{\bar{R}} y_{\bar{R}}$ s'écrit

$$x = \begin{vmatrix} 2 \\ 6 \\ 0 \\ 2 \\ 0 \end{vmatrix} + \begin{vmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & -2 & 5 \\ 0 & -1 & 3 \\ 0 & -3 & 7 \end{vmatrix} \begin{vmatrix} y_3 \\ y_4 \\ y_5 \end{vmatrix} \qquad \left| \begin{array}{l} x_1 = 2 - y_3 \\ x_2 = 6 + y_4 \\ x_3 = 0 - y_3 - 2y_4 + 5y_5 \\ x_4 = 2 - y_4 + 3y_5 \\ x_5 = 0 - 3y_4 + 7y_5 \end{array} \right| \quad y_i \in Z$$

II.2.4 Forme réduite de Smith

La réduite d'Hermite comme la forme normale de Smith ne sont pas uniques. Le théorème suivant va nous fournir une unicité.

Théorème II.5 : Pour toute matrice A(m,n) *de rang* r *à éléments dans un anneau euclidien il existe deux matrices unimodulaires* U *et* V *telles que*

$$UAV = \left| \begin{array}{c|c} \begin{matrix} \varepsilon_1 & & \\ & \varepsilon_2 & \\ & & \ddots \\ & & & \varepsilon_r \end{matrix} & 0 \\ \hline 0 & 0 \end{array} \right| = E \qquad (II.2.4.1)$$

où $\varepsilon_i | \varepsilon_{i+1}$ *pour tout* i *variant de* 1 *à* r-1 *; les* ε_i *étant uniques : ils sont appelés les "invariants" ou "diviseurs élémentaires" de la matrice* A.

Pour obtenir la réduite de Smith, on peut partir directement de la matrice A ou de la forme normale obtenue précédemment.

a) Comme dans la preuve du théorème *II.3*, partie a), nous déterminons deux matrices unimodulaires U_1 et V_1 telles que

$$U_1 A V_1 = \left| \begin{array}{c|c} \varepsilon_1 & 0 \\ \hline 0 & \begin{matrix} 1 \\ A \end{matrix} \end{array} \right| = \overset{1}{E}$$

où ε_1 divise tous les termes de la sous-matrice $\overset{1}{A}$. Pour cela on diminue ε_1 en ajoutant à la première ligne une ligne de $\overset{1}{A}$ contenant un terme β non divisible par ε_1 ; par des transformations élémentaires et transpositions de colonnes, on recalcule ε_1 jusqu'à ce que ε_1 divise tous les termes de $\overset{1}{A}$.

En effectuant alors la même opération sur $\overset{1}{A}$, on obtient

$$U_2 \overset{1}{E} V_2 = \begin{array}{|c|c|c|} \hline \varepsilon_1 & 0 & 0 \\ \hline 0 & \varepsilon_2 & 0 \\ \hline 0 & 0 & \overset{2}{A} \\ \hline \end{array} = \overset{2}{E}$$

Comme ε_1 divisait tous les termes de $\overset{1}{A}$, alors $\varepsilon_1 | \varepsilon_2$. En itérant le processus on obtient (II.2.4.1).

b) D'après la proposition *I*, A et E ont même p.g.c.d. Δ_i de divers ordres, donc :

$$\Delta_i = \varepsilon_1 \, \varepsilon_2 \, \ldots \, \varepsilon_i \qquad i = 1,\ldots,r$$

d'où

$$\Delta_i = \varepsilon_i \, \Delta_{i-1} \qquad i = 2\ldots r \qquad \text{(II.2.4.2)}$$

égalités qui montrent bien l'unicité des ε_i.

Corollaire II.5 : Une condition nécessaire et suffisante pour que le système II *admette une solution quel que soit le second membre est que* r = m *et* $\Delta(A) = 1$. *La solution dépend linéairement de* (n-m) *paramètres.*

C'est une conséquence directe de la remarque *II.9* et de (II.2.4.2).

En fait, dans ce cas, la matrice est semi-modulaire ce qui démontre directement le corollaire.

Chapitre III

RESOLUTION des SYSTEMES de CONGRUENCES LINEAIRES

III.1 RAPPELS ET DEFINITIONS.

Définition 1 : Soient $\overset{\circ}{x} = (\overset{\circ}{x}_1,\ldots,\overset{\circ}{x}_n)$ *et* $\overset{\circ}{y} = (\overset{\circ}{y}_1,\ldots,\overset{\circ}{y}_n)$ *deux vecteurs de* $\mathbb{Z}^n$ *, nous dirons que* $\overset{\circ}{x}$ *et* $\overset{\circ}{y}$ *sont équivalents* ($\overset{\circ}{x} \equiv \overset{\circ}{y} \pmod m$) *si et seulement si*

$$\overset{\circ}{x}_i \equiv \overset{\circ}{y}_i \pmod m \qquad \text{pour } i = 1,2,\ldots,n.$$

Remarquons que si $m = [m_1,m_2,\ldots,m_p]$ nous avons l'équivalence suivante :

$$(\overset{\circ}{x}_i \equiv \overset{\circ}{y}_i \pmod m) \Longleftrightarrow (\overset{\circ}{x}_i \equiv \overset{\circ}{y}_i \pmod{m_j} \text{ pour } j = 1,\ldots,p)$$

en effet, si $\overset{\circ}{x}_i - \overset{\circ}{y}_i$ est un multiple de m, il est multiple de tous les m_j pour $j = 1,\ldots,p$ et inversement.

Autrement dit, $\overset{\circ}{x} \not\equiv \overset{\circ}{y} \pmod m \Longleftrightarrow \exists\ i$ tel que $\overset{\circ}{x}_i \not\equiv \overset{\circ}{y}_i \pmod m \Longleftrightarrow \exists\ i$ et $\exists\ j$ tel que $\overset{\circ}{x}_i \not\equiv \overset{\circ}{y}_i \pmod{m_j}$.

Deux éléments $\overset{\circ}{x}$ et $\overset{\circ}{y}$ de $\mathbb{Z}^n$ équivalents au sens de la définition *1* seront dits égaux par la suite.

Définition 2 : Les systèmes de congruences linéaires se présentent de la manière suivante : trouver $x \in \mathbb{Z}^n$ *tel que*

$$\boxed{\sum_{j=1}^{n} b_i^j x_j \equiv g_i' \pmod{m_i} \qquad i=1,2,\ldots,p} \qquad \text{(III.1.1)}$$

avec $b_i^j \in \mathbb{Z}$ *pour* $i = 1,\ldots,p$ *et* $j = 1,\ldots,n$

$g_i' \in \mathbb{Z}$ *pour* $i = 1,\ldots,p$

$m_i \in \mathbb{Z}$ *pour* $i = 1,\ldots,p.$

Au système (III.1.1) associons le système suivant :

$$\boxed{\sum_{j=1}^{n} c_i^j x_j \equiv h_i \pmod{m} \qquad i=1,2,\ldots,p} \qquad \text{(III.1.2)}$$

avec $m = [m_1,\ldots,m_p]$ où $m = \nu_j m_j \qquad j=1,\ldots,p$

$c_i^j = \nu_i b_i^j$ et $h_i = \nu_i g_i'$.

Proposition III.1 : : *Les systèmes* (III.1.1) *et* (II.1.2) *ont mêmes solutions.*

En effet :

$$\overset{\circ}{x} \text{ solution de (III.1.1)} \Longleftrightarrow \left(\sum_{j=1}^{n} b_i^j \overset{\circ}{x}_j = g_i' + k_i m_i \qquad i=1,\ldots,p\right)$$

$$\Longleftrightarrow \left(\sum_{j=1}^{n} (b_i^j \nu_i) \overset{\circ}{x}_j = \nu_i g_i' + k_i \nu_i m_i, \qquad i=1,\ldots,p\right) \Longleftrightarrow$$

$$\left(\sum_{j=1}^{n} c_i^j \overset{\circ}{x}_j = h_i + k_i m, \quad i=1,\ldots,p\right) \Longleftrightarrow \overset{\circ}{x} \text{ solution de (III.1.2).}$$

Nous verrons dans la suite le nombre exact de solutions de (III.1.1) ou (III.1.2).

Considérons $C = (c_i^j)$ la matrice du système (III.1.2) et posons $h = \begin{pmatrix} h_1 \\ \vdots \\ h_p \end{pmatrix}$;

(III.1.2) s'écrit alors sous forme matricielle

$$\boxed{Cx \equiv h \pmod{m}} \qquad \text{(III.1.3)}$$

Pour résoudre (III.1.1) nous résoudrons (III.1.2) mis sous la forme (III.1.3).

III.2 CONDITIONS D'EXISTENCE DES SOLUTIONS ET RESOLUTION DE $Cx \equiv h \pmod{m}$.

Utilisons la forme normale (ou la réduite) de Smith de C : on sait qu'il existe deux matrices unimodulaires U et V telles que $U\,C\,V = G$ où G est une forme normale de Smith

$$G = \begin{array}{|c|c|} \hline \begin{matrix} g_1 & & \\ & g_2 & \\ & & \ddots \\ & & & g_q \end{matrix} & \begin{matrix} 0 \end{matrix} \\ \hline 0 & 0 \\ \hline \end{array}$$

Si C est une n-p matrice, G également ; U est une p-p matrice et V une n-n matrice.

Posons $h' = Uh$ (ou $h' \equiv Uh \pmod m$).

Proposition III.2 : Une condition nécessaire et suffisante pour que (III.1.1) *ou* (III.1.2) *ou* (III.1.3) *ait une solution est que*

$$\begin{cases} (g_i, m) \mid h'_i \text{ pour } i=1,\ldots,q \\ h'_i \text{ soit un multiple de } m \text{ pour } i=q+1,\ldots,p \end{cases} \qquad \text{(III.1.4)}$$

En effet, $Cx \equiv h \pmod m \iff CVV^{-1} x \equiv h \pmod m$.

$$\iff U C V V^{-1} x \equiv Uh \pmod m$$

par suite en posant $V^{-1} x = y$ (ou $V^{-1}x \equiv y \pmod m$) et tenant compte de $h' = Uh$ (ou $h' \equiv Uh \pmod m$), nous obtenons le système suivant équivalent à (III.1.3) :

$$\boxed{Gy \equiv h' \pmod m} \qquad \text{(III.1.5)}$$

c'est-à-dire que nous sommes ramenés à la résolution de congruences dans $\mathbb{Z}$

$$\begin{cases} g_1 y_1 \equiv h'_1 \pmod m \\ g_2 y_2 \equiv h'_2 \pmod m \\ \cdots\cdots \\ \cdots\cdots \\ g_q y_q \equiv h'_q \pmod m \end{cases} \qquad \text{(III.1.6)}$$

$$\begin{cases} 0 \equiv h'_{q+1} \pmod m \\ \cdots\cdots \\ \cdots\cdots \\ 0 \equiv h'_p \pmod m \end{cases} \qquad \text{(III.1.7)}$$

Rappelons la proposition suivante : la congruence linéaire $ax \equiv b \pmod m$ a des solutions si et seulement si $(a,m) \mid b$. Si $(a,m) \mid b$, alors $ax \equiv b \pmod m$ a (a,m) solutions distinctes modulo m.

D'où l'existence des solutions de (III.1.6).

$g_1 y_1 \equiv h'_1 \pmod m$ a (g_1,m) solutions si et seulement si $(g_1,m) \mid h'_1$

.....

.....

$g_q y_q \equiv h_q \pmod m$ a (g_q,m) solutions si et seulement si $(g_q,m) \mid h'_q$.

De plus il faut que (III.1.7) soit satisfait, c'est-à-dire que $h'_{q+1}, \ldots, h'_q$ soient des multiples de m.

Tenant compte du fait que $x = Vy$ avec V unimodulaire, on obtient bien la proposition.

Notons que $y_{q+1} \ldots y_n$ sont arbitraires ; ils peuvent se mettre sous la forme

$y_{q+1} \equiv 0 \pmod m$, $y_{q+1} \equiv 1 \pmod m, \ldots, y_{q+1} \equiv m-1 \pmod m$

.....

.....

$y_n \equiv 0 \pmod m$, $y_n \equiv 1 \pmod m, \ldots, y_n \equiv m-1 \pmod m$

Toujours de $x = Vy$ (ou $x \equiv Vy \pmod m$), on déduit qu'il y a autant de solutions distinctes pour x qu'il y en a pour y.

D'après ce qui précède, il y a au total :

ou 0 solution

ou $(g_1,m) \times (g_2,m) \times \ldots \times (g_q,m) \times m^{n-q}$ solutions distinctes aux systèmes équivalents (III.1.1), (III.1.2), (III.1.3), (III.1.5).

En posant $Q = \{1,2,\ldots,q\}$, $\bar{Q} = \{q+1,\ldots,n\}$, nous avons

$$\boxed{x = V^{Q} y_{Q} + V^{\bar{Q}} y_{\bar{Q}} \pmod m} \qquad \text{(III.1.8)}$$

On peut récapituler les résultats dans le théorème suivant :

Théorème III : *Les systèmes de congruences linéaires* (III.1.1), (III.1.2), (III.1.3), (III.1.5) *équivalents possèdent*

ou $(g_1,m) \times (g_2,m) \times \ldots \times (g_q,m) \times m^{n-q}$ *solutions distinctes*

ou 0 solution

selon que les conditions d'existence (III.1.4) *sont vérifiées ou pas (les* g_i *étant les éléments d'une forme normale de Smith de la matrice C associée à* (III.1.2)). *Les solutions sont données par* (III.1.8).

Remarquons que si le second membre de (III.1.2) ou (III.1.3) est nul ($h_i = 0$ $i=1,\ldots,p$), le système a toujours des solutions.

Exemple III

III.1

$$\begin{aligned} -2x_1 + 2x_2 - 6x_3 + 10x_4 &\equiv 4 \pmod 3 \\ 6x_1 + \quad + 2x_3 + 8x_4 &\equiv 5 \pmod 6 \\ -4x_1 + 2x_2 - 8x_3 + 2x_4 &\equiv 5 \pmod 9 \end{aligned}$$

$18 = [3,6,9]$ $\qquad 18 = 6 \times 3 = 3 \times 6 = 2 \times 9$

$$\begin{aligned} 12x_1 + 12x_2 - 36x_3 + 60x_4 &\equiv 24 \pmod{18} \\ 18x_1 + \quad + 6x_3 + 24x_4 &\equiv 15 \pmod{18} \\ -8x_1 + 4x_2 - 16x_3 + 4x_4 &\equiv 10 \pmod{18} \end{aligned}$$

$$U = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & -2 & -3 \end{pmatrix} \qquad V = \begin{vmatrix} 0 & 0 & 1 & 0 \\ 1 & 4 & -10 & -17 \\ 0 & 1 & -3 & -4 \\ 0 & 0 & 0 & 1 \end{vmatrix} \qquad G = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$Uh_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & -2 & -3 \end{pmatrix} \begin{pmatrix} 24 \\ 15 \\ 10 \end{pmatrix} = \begin{pmatrix} 10 \\ 15 \\ -36 \end{pmatrix} = h_1'$$

$$Gy \equiv h_1' \pmod{18} \iff \begin{aligned} 4y_1 &\equiv 10 \pmod{18} \\ 6y_2 &\equiv 15 \pmod{18} \\ 0 &\equiv -36 \pmod{18} \end{aligned} \quad \text{vérifié}$$

$(4,18) = 2 \quad 2 \mid 10$, d'où 2 solutions pour y_1

$(6,18) = 6 \quad 6 \nmid 15$, 0 solution pour y_2.

Le système proposé n'a pas de solution.

III.2

$$\begin{aligned} -2x_1 + 2x_2 - 6x_3 + 10x_4 &\equiv 4 \pmod 3 \\ 6x_1 + \quad + 2x_3 + 8x_4 &\equiv 4 \pmod 6 \\ -4x_1 + 2x_2 - 8x_3 + 2x_4 &\equiv 3 \pmod 9 \end{aligned}$$

$$Gy \equiv h_2' \pmod{18} \iff \begin{aligned} 4y_1 &\equiv 6 \pmod{18} \\ 6y_2 &\equiv 12 \pmod{18} \\ 0 &\equiv -18 \pmod{18} \end{aligned} \quad \text{vérifié}$$

$(4,18) = 2 \quad 2 \mid 6$, d'où 2 solutions pour y_1

à savoir $y_1 \equiv 6 \pmod{18}$ $\quad y_1 \equiv 15 \pmod{18}$

$(6,18) = 6 \quad 6 \mid 12$, d'où 6 solutions pour y_2

à savoir $y_2 \equiv 2 \pmod{18}$ $\quad y_2 \equiv 5 \pmod{18}$ $\quad y_2 \equiv 8 \pmod{18}$ $\quad y_2 \equiv 11 \pmod{18}$

$y_2 \equiv 14 \pmod{18}$ $\quad y_2 \equiv 17 \pmod{18}$

y_3 et y_4 arbitraires, c'est-à-dire :

$y_3 \equiv 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 \pmod{18}$

$y_4 \equiv$ idem.

au total, il y a $2 \times 6 \times 18^2 = 3888$ solutions distinctes. On peut donner le tableau des valeurs prises par y_1, y_2, y_3 et y_4 :

y_1	6	15																
y_2	2	5	8	11	14	17												
y_3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
y_4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

$x = Vy$ nous donne les solutions x cherchées ; par exemple en prenant :

$$\overset{1}{y} = \begin{pmatrix} 6 \\ 2 \\ 0 \\ 0 \end{pmatrix} \qquad \text{on obtient } \overset{1}{x} = \begin{pmatrix} 0 \\ 14 \\ 2 \\ 0 \end{pmatrix} \pmod{18}$$

$$\overset{2}{y} = \begin{pmatrix} 6 \\ 2 \\ 0 \\ 1 \end{pmatrix} \qquad \text{on obtient } \overset{2}{x} = \begin{pmatrix} 0 \\ -3 \\ -2 \\ 1 \end{pmatrix} \pmod{18} = \begin{pmatrix} 0 \\ 15 \\ 16 \\ 1 \end{pmatrix} \pmod{18}$$

.....

$$\overset{3888}{y} = \begin{pmatrix} 15 \\ 17 \\ 17 \\ 17 \end{pmatrix} \qquad \text{on obtient } \overset{3888}{x} = \begin{pmatrix} 17 \\ -376 \\ -102 \\ 67 \end{pmatrix} \pmod{18} = \begin{pmatrix} 17 \\ 2 \\ 6 \\ 17 \end{pmatrix} \pmod{18}$$

Chapitre IV

RESOLUTION des SYSTEMES LINEAIRES MIXTES en NOMBRES ENTIERS

IV.1 *DEFINITION*

Il s'agit de chercher tous les $x \in \mathbb{Z}^n$ *qui vérifient à la fois les groupes d'égalités* (IV.1.1) *et* (IV.1.2) *suivants :*

$$A_i x = b_i, \quad i=1,2,\ldots,k \qquad \text{(IV.1.1)}$$

$$C_j' x \equiv h_j' \pmod{m_j}, \quad j=1,2,\ldots,p \qquad \text{(IV.1.2)}$$

Les données sont :

les vecteurs lignes A_i, $i=1,2,\ldots,k$ *et* C_j', $j=1,2,\ldots,p$ *à composantes dans* $\mathbb{Z}$,

les scalaires $b_i \in \mathbb{Z}$, $i=1,2,\ldots,k$; $h_j' \in \mathbb{Z}$, $m_j \in \mathbb{Z}$, $j=1,2,\ldots,p$.

Nous savons (d'après la proposition *III.1*) que (IV.1.3) a les mêmes solutions que le système suivant :

$$C_j x \equiv h_j \pmod{m}, \quad j=1,2,\ldots,p \qquad \text{(IV.1.3)}$$

où $m = [m_1, m_2, \ldots, m_p]$, $m = \nu_1 m_1 = \ldots = \nu_p m_p$ et où $C_j = \nu_j C_j'$, $h_j = \nu_j h_j'$, $j=1,2,\ldots,p$.

Par suite, en notant A la matrice dont les lignes sont A_i, C la matrice dont les lignes sont C_j, b le vecteur colonne de composantes b_j et h celui de composantes h_j, le problème posé revient donc à résoudre à la fois (IV.1.4) et (IV.1.5) ci-dessous :

$$Ax = b \qquad \text{(IV.1.4)}$$

$$Cx \equiv h \pmod{m} \qquad \text{(IV.1.5)}$$

A(k,n) est de rang r quelconque, C(p,n) de rang s quelconque.

IV.2 CONDITIONS D'EXISTENCE DES SOLUTIONS ET RESOLUTION DE $Ax = b$ ET $Cx \equiv h \pmod m$.

Résolvons d'abord (IV.1.4) en utilisant le chapitre II (II.2). Il existe deux matrices unimodulaires U et V telles que UAV = E, E étant une forme normale de Smith de A.

$Ax = b$ s'écrit $UAV\bar{V}^{1}x = Ub$,

soit $Ey = Ub$ où $y = \bar{V}^{1}x$.

Posons $R = \{1,2,\ldots,r\}$, $\bar{R} = \{r+1,\ldots,n\}$ et $\bar{\bar{R}} = \{r+1, r+2,\ldots,k\}$.

(A) *Une condition nécessaire et suffisante pour que* (IV.1.4) *ait une solution est que* $(E_R^R)^{-1} U_R b$ *soit entier et que* $U_{\bar{R}} b = 0$.

Dans ce cas $y_R = (E_R^R)^{-1} U_R b$, $y_{\bar{R}} \in \mathbb{Z}^{n-r}$.

La solution générale de (IV.1.4) est alors :

$$x = V^R y_R + V^{\bar{R}} y_{\bar{R}} = V^R (E_R^R)^{-1} U_R b + V^{\bar{R}} y_{\bar{R}} = \overset{*}{x} + V^{\bar{R}} y_{\bar{R}},$$

avec $y_{\bar{R}}$ vecteur arbitraire de $\mathbb{Z}^{n-r}$.

Reportons la valeur de x, solution générale de (IV.1.4), dans (IV.1.5). On obtient :

$$CV^{\bar{R}} y_{\bar{R}} = h - CV^R (E_R^R)^{-1} U_R b \pmod m.$$

Posons $F = CV^R$ et $e = h - CV^R (E_R^R)^{-1} U_R b$; F(p,n-r) est une matrice de rang égal à celui de C soit s.

Résolvons $Fy_{\bar{R}} = e \pmod m$ en utilisant ce qui a été fait au chapitre III. Il existe deux matrices unimodulaires *U* et *V* telles que *UFV* = G, G étant une forme normale de Smith.

$$Fy_{\bar{R}} \equiv e \pmod m \iff GY \equiv f \pmod m \qquad \text{(IV.1.6)}$$

avec $f = Ue$ et $Y = V^{-1} y_{\bar{R}}$.

Notons $g_1, g_2, \ldots, g_s$ les éléments diagonaux non nuls de G. $GY \equiv f \pmod m$ s'écrit :

$$\begin{aligned} g_1 Y_1 &\equiv f_1 \pmod m \\ g_2 Y_2 &\equiv f_2 \pmod m \\ &\vdots \\ g_s Y_s &\equiv f_s \pmod m \\ 0 &\equiv f_{s+1} \pmod m \\ &\vdots \\ 0 &\equiv f_p \pmod m . \end{aligned}$$

Posons $p_i = (g_i, m)$.

(B) *Une condition nécessaire et suffisante pour que* (IV.1.6) *ait des solutions est que* $p_i \mid f_i$, $i=1,2,\ldots,s$ *et que* $f_{s+1},\ldots,f_p$ *soient des multiples de* m.

Rappelons que les y_i dépendent de $F = CV^R$ qui dépend de C bien sûr, mais aussi de A par l'intermédiaire de V^R.

Proposition IV : Le système linéaire mixte a des solutions si et seulement si (A) *et* (B) *sont respectivement réalisés.*

Nombre de solutions : il y a $p_1 \times p_2 \times \ldots \times p_s \times m^{p-s} = P$ solutions pour Y et par suite pour $y_{\bar R}$ donc pour x.

De $y_{\bar R} = VY$ on obtient

$$y_{\bar R} = \begin{pmatrix} y_{r+1} + \ell_{r+1}\, m \\ y_{r+2} + \ell_{r+2}\, m \\ \vdots \\ y_n + \ell_n\, m \end{pmatrix} \qquad \text{avec } \ell_{r+1}, \ldots, \ell_n \in \mathbb{Z}$$

$$\text{d'où } \overset{i}{x} = V^R(E_R^R)^{-1}\, U_R b + V^{\bar R} \begin{pmatrix} \overset{i}{y}_{r+1} \\ \overset{i}{y}_{r+2} \\ \vdots \\ \overset{i}{y}_n \end{pmatrix} + mV^{\bar R} \begin{pmatrix} \ell_{r+1} \\ \ell_{r+2} \\ \vdots \\ \ell_n \end{pmatrix}$$

$i = 1,2,\ldots,P.$

Posons

$$V^R(E_R^R)^{-1}\, U_R b + V^{\bar R} \begin{pmatrix} \overset{i}{y}_{r+1} \\ \overset{i}{y}_{r+2} \\ \vdots \\ \overset{i}{y}_n \end{pmatrix} = \overset{\hat{i}}{x}$$

D'où les P solutions du système linéaire mixte proposé :

$$\overset{i}{x} = \overset{\hat{i}}{x} + mV^{\bar R}\, \ell_{\bar R} \qquad \text{où} \quad \ell_{\bar R} \in \mathbb{Z}^{n-r}$$

$i = 1,2,\ldots,P$

La forme de la solution est très proche de la solution générale en entier.

Remarque IV : Nous pouvons reprendre ce qui a été fait en résolvant d'abord (IV.1.5) puis en reportant les solutions trouvées dans (IV.1.4).

Exemple IV : Résoudre dans $\mathbb{Z}^4$:

$$\begin{aligned}
2x_1 + 4x_2 + 5x_3 - 12x_4 &= -1 \\
-3x_1 + 7x_2 - 2x_3 + 2x_4 &= 4 \\
-x_1 + 11x_2 + 3x_3 - 10x_4 &= 3 \\
-4x_1 + 18x_2 + x_3 - 8x_4 &= 7 \\
2x_1 + 4x_2 + 2x_3 - 4x_4 &\equiv 4 \pmod 6 \\
5x_1 + x_2 - 6x_3 + 2x_4 &\equiv 2 \pmod 6
\end{aligned}$$

$$\underset{U}{\begin{pmatrix}0&0&1&0\\0&1&-3&0\\1&1&-1&0\\0&-1&-1&1\end{pmatrix}}\quad\underset{A}{\begin{pmatrix}2&4&5&-12\\-3&7&-2&2\\-1&11&3&-10\\-4&18&1&-8\end{pmatrix}}\quad\underset{V}{\begin{pmatrix}1&-1&17&4\\0&0&5&2\\0&3&-6&4\\0&1&2&3\end{pmatrix}}=\underset{E}{\begin{pmatrix}-1&0&0&0\\0&-1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}}$$

$$Ub=\begin{pmatrix}3\\-5\\0\\0\end{pmatrix}\qquad F=CV^{\bar{R}}=\begin{pmatrix}34&12\\130&4\end{pmatrix}\qquad CV^{R}(E_R^R)^{-1}\,U_Rb=\begin{pmatrix}-&6\\-&120\end{pmatrix}$$

$$e=\begin{pmatrix}4\\2\end{pmatrix}-\begin{pmatrix}-&6\\-&120\end{pmatrix}=\begin{pmatrix}10\\122\end{pmatrix}$$

Il faut résoudre

$$\begin{pmatrix}34&12\\120&4\end{pmatrix}\begin{pmatrix}y_3\\y_4\end{pmatrix}\equiv\begin{pmatrix}10\\122\end{pmatrix}\pmod 6\equiv\begin{pmatrix}4\\2\end{pmatrix}\pmod 6$$

$$\underset{u}{\begin{pmatrix}0&1\\1&175\end{pmatrix}}\underset{F}{\begin{pmatrix}34&12\\130&4\end{pmatrix}}\underset{v}{\begin{pmatrix}1&-2\\-32&65\end{pmatrix}}=\underset{G}{\begin{pmatrix}2&0\\0&712\end{pmatrix}}$$

$$ue=f=\begin{pmatrix}2\\354\end{pmatrix}$$

$2Y_1 \equiv 2 \pmod 6$ d'où $(2,6)=2$ solutions à savoir $Y_1 \equiv 1$ et $Y_1 \equiv 4 \pmod 6$,

$712Y_2 \equiv 354 \pmod 6 \equiv 0 \pmod 6$ d'où $(712,6)=2$ solutions à savoir $Y_2 \equiv 0$ et $Y_2 \equiv 3 \pmod 6$,

donc au total 4 solutions pour Y.

$$\overset{1}{Y}=\begin{pmatrix}1\\0\end{pmatrix}\quad\overset{2}{Y}=\begin{pmatrix}1\\3\end{pmatrix}\quad\overset{3}{Y}=\begin{pmatrix}4\\0\end{pmatrix}\quad\overset{4}{Y}=\begin{pmatrix}4\\3\end{pmatrix}$$

$$V^{R}(E_R^R)^{-1}\,U_Rb=\begin{pmatrix}-8\\0\\15\\5\end{pmatrix}$$

d'où $\overset{i}{y}_{\bar{R}} \equiv V\overset{i}{Y} \pmod 6$ $\quad i=1,2,3,4$ ce qui donne

$$\overset{1}{y}_{\bar{R}} \equiv \begin{pmatrix}1\\4\end{pmatrix} \pmod 6 \qquad \overset{2}{y}_{\bar{R}} \equiv \begin{pmatrix}1\\1\end{pmatrix} \pmod 6 \qquad \overset{3}{y}_{\bar{R}} \equiv \begin{pmatrix}4\\4\end{pmatrix} \pmod 6 \qquad \overset{4}{y}_{\bar{R}} \equiv \begin{pmatrix}4\\1\end{pmatrix} \pmod 6$$

$V^{\bar{R}} \overset{i}{y}_{\bar{R}}$ donne $\begin{pmatrix}33\\13\\10\\14\end{pmatrix}$, $\begin{pmatrix}21\\7\\-2\\5\end{pmatrix}$, $\begin{pmatrix}84\\28\\-8\\20\end{pmatrix}$, $\begin{pmatrix}72\\22\\-20\\11\end{pmatrix}$

$\overset{\hat{i}}{x} = V^{R}(E^{R}_{R})^{-1} U_{R}b + V^{\bar{R}} \overset{i}{y}_{\bar{R}}$ $\quad i=1,2,3,4$ donne

$$\overset{\hat{1}}{x} = \begin{pmatrix}25\\13\\25\\19\end{pmatrix}, \quad \overset{\hat{2}}{x} = \begin{pmatrix}13\\7\\13\\10\end{pmatrix}, \quad \overset{\hat{3}}{x} = \begin{pmatrix}76\\28\\7\\25\end{pmatrix}, \quad \overset{\hat{4}}{x} = \begin{pmatrix}64\\22\\-5\\16\end{pmatrix}$$

L'ensemble des solutions du système proposé est :

$$\overset{i}{x} = \overset{\hat{i}}{x} + 6\begin{pmatrix}17 & 4\\5 & 2\\-6 & 4\\2 & 3\end{pmatrix}\begin{pmatrix}\ell_3\\\ell_4\end{pmatrix} \qquad i=1,2,3,4 \ ; \ \ell_3,\ell_4 \in \mathbb{Z}$$

Chapitre V

GENERATION des POINTS ENTIERS d'un CONE POLYEDRIQUE

V.1 CONE POLYEDRIQUE REGULIER ([13],[14])

Définition V.1 : *Un cône polyédrique régulier est défini par :*

$\{x \mid Ax \geq b\}$ *où* A *est une* (n,n) *matrice de rang* n, *à éléments dans* $\mathbb{Z}$ *(ou* Q*) et* $b \in \mathbb{R}^n$.

Théorème V.1 : *Tous les points entiers d'un cône polyédrique régulier sont donnés par la formule suivante :*

$$x = \overset{i}{x} + k_1 B^1 + \ldots + k_n B^n.$$

Cette décomposition est unique.

$B^1, B^2, \ldots, B^n$ *sont* n *vecteurs linéairement indépendants à composantes entières. Ils sont parallèles aux arêtes du cône,* $k_j \in \mathbb{N}$ *pour* $j=1,2,\ldots,n$.

L'ensemble des $\overset{i}{x}$ *est appelé ensemble des points fondamentaux (ensemble* P_f*). Ces points fondamentaux sont les seuls points entiers du parallélotope semi-ouvert suivant :*

$$\{x \mid x = S + \lambda_1 B^1 + \ldots + \lambda_n B^n,\ 0 \leq \lambda_i < 1,\ \lambda_i \in \mathbb{R} \text{ pour } i=1,2,\ldots,n\}$$

S *est le sommet du cône.*

Le nombre de ces points fondamentaux est égal à $|\det B|$, *où* $B = [B^1,\ldots,B^n]$.

La preuve consiste en cinq parties. Les parties V.1.1 et V.1.2 fournissent un algorithme pour trouver les points fondamentaux et les vecteurs B^j. Le programme correspondant écrit en ALGOL se trouve en annexe 6.

La méthode consiste à résoudre dans $\mathbb{Z}^n$ le système Ax=a avec a≥b c'est-à-dire à trouver l'ensemble des a qui rendent le système linéaire compatible et qui sont plus grands ou égaux à b (composante par composante). De tels points a sont dits admissibles.

V.1.1 Calcul des a admissibles

D'après le théorème II.3 il existe deux matrices unimodulaires U(n,n) et V(n,n) telles que UAV = E où E est la forme normale (ou réduite) de Smith de A.

$$Ax = a \Longleftrightarrow Ey = Ua \quad \text{avec } x = Vy. \qquad (V.1.1.1)$$

Appelons $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n$ les éléments de la diagonale de E. Développons (V.1.1.1), nous obtenons :

$$\varepsilon_i y_i = U_i.a \quad \text{pour } i=1,2,\ldots,n.$$

Les vecteurs a doivent être tels que $\frac{U_i.a}{\varepsilon_i}$ soit un entier pour tout i=1,2,...,n. Les a qui possèdent cette propriété sont les solutions du système de congruences linéaires, à n inconnues, suivant :

$$U_i.a \equiv 0 \ (\varepsilon_i) \quad \text{pour } i=1,2,\ldots,n. \qquad (V.1.1.2)$$

Soit $\varepsilon = [\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n]$. Si nous avons la réduite de Smith au lieu de la forme normale alors $\varepsilon = \varepsilon_n$. Posons $\nu_i = \frac{\varepsilon}{\varepsilon_i}$ pour i=1,2,...,n. (V.1.1.2) est équivalent à

$$C_i.a \equiv 0(\varepsilon) \quad \text{pour } i=1,2,\ldots,n. \qquad (V.1.1.3)$$

où $C_i = \nu_i.U_i$.

Nous appellerons C la matrice de (V.1.1.3). Résolvons (V.1.1.3) par la méthode du chapitre III. Il existe deux matrices unimodulaires *U* et *V* telles que *UCV* = G où G est une forme normale de Smith de C.

$$Ca \equiv 0(\varepsilon) \Longleftrightarrow GY \equiv 0(\varepsilon) \quad \text{avec} \quad a = VY$$

Appelons $g_1,g_2,\ldots,g_n$ les éléments diagonaux de G. Le dernier système se décompose en n équations indépendantes

$$g_i\ Y_i \equiv 0(\varepsilon) \quad \text{pour} \quad i=1,2,\ldots,n$$

Y_i ayant $p_i = (g_i,\varepsilon)$ solutions.

Nous avons donc $p_1 \times p_2 \times \ldots \times p_n$ solutions pour le vecteur Y et par suite pour a.

Posons ${}^t\overset{i}{Y} = (\alpha_1^i,\ldots,\alpha_n^i)$ (mod ε) pour $i=1,2,\ldots,p_1\times p_2\times\ldots\times p_n$.
$a = VY$ donne ${}^t\overset{i}{a} = (\beta_1^i,\ldots,\beta_n^i)$ (mod ε) pour $i=1,2,\ldots,p_1\times p_2\times\ldots\times p_n$.

Maintenant retournons à la condition $a \geq b$. β_j^i définit une classe modulo ε, nous prenons l'élément de cette classe que nous appellerons $\overset{i}{\gamma}_j$ tel que $b_j \leq \overset{i}{\gamma}_j < b_j + \varepsilon$ pour $i=1,2,\ldots,p_1\times p_2\times\ldots\times p_n$ et $j=1,2,\ldots,n$.

Alors tous les a admissibles sont donnés par
${}^t\overset{i}{a} = (\overset{i}{\gamma}_1 + k_1\varepsilon, \overset{i}{\gamma}_2 + k_2\varepsilon,\ldots, \overset{i}{\gamma}_n + k_n\varepsilon)$ avec $k_j \in \mathbf{N}$ pour $j=1,2,\ldots,n$ et

$$i=1,2,\ldots,p_1\times p_2\times\ldots\times p_n. \qquad (V.1.1.4)$$

Posons ${}^t\overset{i}{P} = (\overset{i}{\gamma}_1,\ldots,\overset{i}{\gamma}_n)$ et considérons le vecteur δ^i dont toutes les composantes sont nulles sauf la $i^{\text{ième}}$ égale à 1. (V.1.1.4) devient :
$\overset{i}{a} = \overset{i}{P} + \varepsilon k_1\delta^1 + \ldots + \varepsilon k_n\delta^n$ pour $i=1,2,\ldots,p_1\times p_2\times\ldots\times p_n$. Ce qui constitue l'ensemble des a admissibles ($k_j \in N$).

V.1.2 Points entiers du cône

De $x = Vy$ et de $y = E^{-1}Ua$ nous obtenons $x = VE^{-1}Ua$. Posons $M = VE^{-1}U$, $B = \varepsilon M$, $M\overset{i}{P} = \overset{i}{x}$; notons que $M = A^{-1}$.

Alors tous les points entiers du cône V.1 sont donnés par la formule :

$$x = \overset{i}{x} + k_1B^1 + \ldots + k_nB^n \text{ pour } i=1,2,\ldots,p_1\times p_2\times\ldots\times p_n \text{ avec } k_i \in \mathbf{N} \text{ pour } i=1,2,\ldots,n.$$

L'ensemble des $\overset{i}{x}$ est appelé ensemble des points fondamentaux du cône V.1. Cet ensemble sera noté P_f.

V.1.3 Propriétés de $B^1,\ldots,B^n$

De $B = \varepsilon M = \varepsilon A^{-1}$ qui est une matrice à coefficients dans $\mathbf{Z}$ nous déduisons que $A_i.B^j = 0$ pour $i\neq j$, c'est-à-dire que B^j est parallèle aux n-1 hyperplans $A_ix = b_i$, $i\neq j$. En d'autres termes les B^j qui sont des vecteurs à composantes entières sont parallèles aux arêtes du cône.

V.1.4 Le parallélotope fondamental

Considérons l'ensemble suivant, appelé parallélotope fondamental du cône :

$$F = \{x \mid x = S + \lambda_1 B^1 + \ldots + \lambda_n B^n,\ 0 \leq \lambda_i < 1,\ \lambda_i \in \mathbb{R},\ i=1,2,\ldots,n\},$$

constitué à partir du sommet S du cône et porté par ses arêtes.

Les points fondamentaux sont les seuls points entiers de E. Pour cela montrons d'abord que pour tout $\overset{i}{x} \in P_f$ il existe un vecteur réel $\overset{i}{\lambda}$ de composantes $\overset{i}{\lambda}_j$ satisfaisant à $0 \leq \overset{i}{\lambda}_j < 1$ tel que $\overset{i}{x} = S + B\overset{i}{\lambda}$.

Par construction $\overset{i}{P}$ est tel que $b_j \leq \overset{i}{P}_j < b_j + \varepsilon$ pour $j = 1,2,\ldots,n$ et $i = 1,2,\ldots,p_1 \times p_2 \times \ldots \times p_n$.

Considérons le vecteur réel $\overset{i}{\lambda} = \frac{1}{\varepsilon}(\overset{i}{P} - b)$, nous avons $0 \leq \overset{i}{\lambda}_j < 1$ et en appliquant M à cette égalité nous obtenons

$$M(\varepsilon\overset{i}{\lambda}) = M\overset{i}{P} - Mb \quad \text{c'est-à-dire} \quad \overset{i}{x} = S + B\overset{i}{\lambda}.$$

Inversement un point entier x de F étant aussi un point entier du cône, s'écrit de la manière suivante : $x = \overset{i}{x} + k_1 B^1 + \ldots k_n B^n$. Or $\overset{i}{x} = S + \lambda_1 B^1 + \ldots + \lambda_n B^n$ avec $0 \leq \lambda_j < 1$ ce qui entraîne $k_1 = k_2 = \ldots = k_n = 0$ et $x = \overset{i}{x}$: c'est un point fondamental.

En d'autres termes nous recouvrons tous les points entiers du cône en translatant le parallélotope fondamental avec les vecteurs $B^1,\ldots,B^n$. L'ensemble des parallélotopes translatés du parallélotope fondamental constitue avec ce dernier une partition du cône pour les points réels comme pour les points entiers.

V.1.5 Nombre de points fondamentaux d'un cône régulier

D'après V.1.1, le nombre de points fondamentaux est égal à $p_1 \times p_2 \times \ldots \times p_n$. Nous montrons que :

$$p_1 \times p_2 \times \ldots \times p_n = \frac{\varepsilon^n}{|\det A|} = |\det B|.$$

Pour démontrer cette formule nous considérons la réduite de Smith de A c'est-à-dire que nous avons $\varepsilon_i | \varepsilon_{i+1}$ pour i=1,2,...,n-1.
De $\varepsilon = \nu_1\varepsilon_1 = \nu_2\varepsilon_2 = \ldots = \varepsilon_n$ nous déduisons que $\nu_i | \nu_{i-1}$ pour i=2,...,n.

Rappelons que C a été définie à partir de la matrice unimodulaire U et des ν_i : $C_i = \nu_i U_i$.

Nous calculons $\Delta_i(C)$, le p.g.c.d. d'ordre i de C, de deux manières différentes.

Premièrement, nous avons $UCV = G$ et $g_i | g_{i+1}$ pour i=1,2,...,n-1 alors
$\Delta_i(C) = g_1 \times g_2 \times \ldots \times g_i$. (V.1.5.1)

Deuxièmement, de $C_i = \nu_i U_i$, $\nu_1 \geq \nu_2 \geq \ldots \geq \nu_{n-1} \geq \nu_n = 1$, $\nu_i | \nu_{i-1}$ pour i = 1,...,n et $\Delta_i(U) = 1$ nous déduisons :

$$\Delta_i(C) = 1 \times \nu_{n-1} \times \ldots \times \nu_{n-i+1} \qquad (V.1.5.2)$$

(V.1.5.1) et (V.1.5.2) nous donnent :

$$\Delta_1(C) = g_1 = \nu_n = 1$$

$$\Delta_2(C) = g_1 \times g_2 = \nu_n \times \nu_{n-1} \Longrightarrow g_2 = \nu_{n-1},$$

et ainsi de suite $g_i = \nu_{n-i+1}$.

Puisque $p_i = (g_i, \varepsilon) = (\nu_{n-i+1}, \nu_{n-i+1}\, \varepsilon_{n-i+1}) = \nu_{n-i+1}$, nous avons

$$p_1 \times p_2 \times \ldots \times p_n = \nu_n \times \nu_{n-1} \times \ldots \times \nu_1 = \frac{\varepsilon_n}{\varepsilon_n} \times \frac{\varepsilon_n}{\varepsilon_{n-1}} \times \ldots \times \frac{\varepsilon_n}{\varepsilon_1} = \frac{(\varepsilon)^n}{|\det A|}.$$

$BA = \varepsilon I \Longrightarrow |\det A| \cdot |\det B| = \varepsilon^n$ et $p_1 \times p_2 \times \ldots \times p_n = |\det B|$.

Nous avons prouvé que le nombre de points fondamentaux est égal au volume du parallélotope fondamental.

Dans $\mathbb{R}^2$ nous avons $|\det A| = |\det B|$ mais pour n>2, $|\det B|$ peut être différent de $|\det A|$. Nous donnons *deux exemples* illustrant ces formules.

a)

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} \qquad \det A = 3$$

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -3 \end{pmatrix} \qquad U = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & 1 \\ -2 & 1 & 0 \end{pmatrix} \qquad V = \begin{pmatrix} 1 & -1 & -2 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} -4 & 2 & 3 \\ 2 & -1 & 0 \\ 3 & 0 & -3 \end{pmatrix} \qquad |\det B| = 9$$

$$N = \frac{3^3}{3} = 9 = |\det B| > \det A$$

b)

$$A = \begin{pmatrix} 1 & 4 & 5 \\ 1 & -2 & -25 \\ 1 & 7 & 23 \end{pmatrix} \qquad \det A = 18$$

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix} \qquad U = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & 1 \\ -3 & 1 & 2 \end{pmatrix} \qquad V = \begin{pmatrix} 1 & -4 & 19 \\ 0 & 1 & -6 \\ 0 & 0 & 1 \end{pmatrix}$$

$$B = \begin{pmatrix} -43 & 19 & 30 \\ 16 & -6 & -10 \\ -3 & 1 & 2 \end{pmatrix} \qquad |\det B| = 12$$

$$N = \frac{6^3}{18} = 12 = |\det B| < \det A.$$

Exemple V.1 - Cône défini par :

$$2x - y \geq \frac{43}{2} \qquad (1)$$

$$x - 5y \geq -\frac{17}{4} \qquad (2)$$

Les coordonnées du sommet S sont $\left(\frac{149}{12}, \frac{10}{3}\right)$.

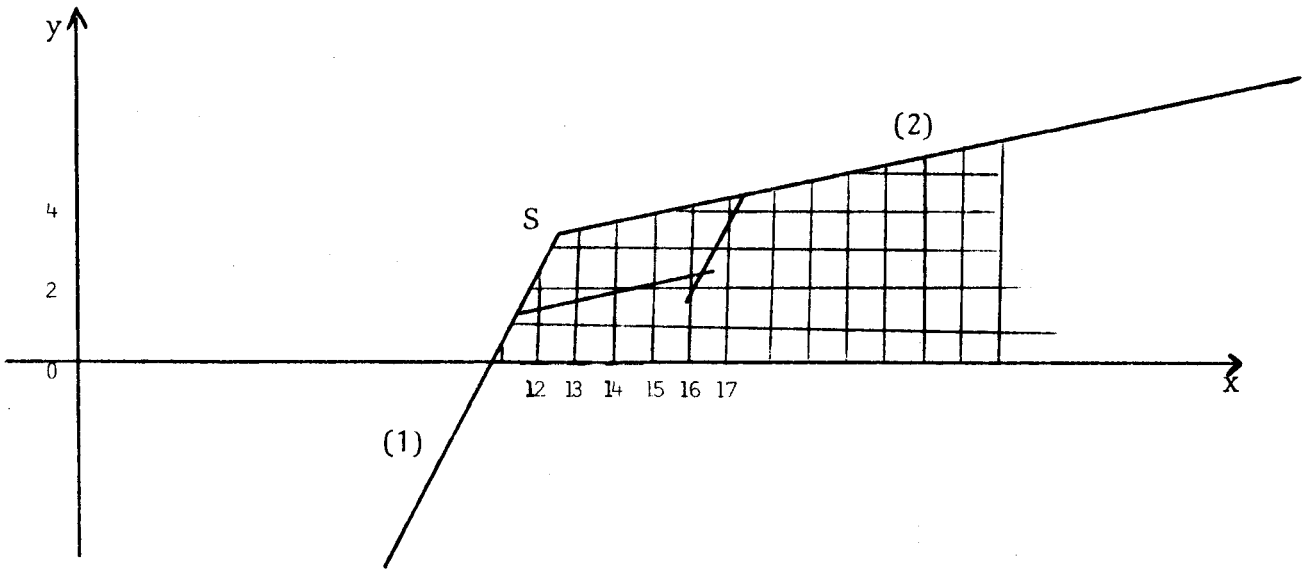
Nous avons $U = \begin{pmatrix} 1 & 0 \\ -5 & 1 \end{pmatrix}$ $V = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$ $E = \begin{pmatrix} -1 & 0 \\ 0 & -9 \end{pmatrix}$

$$B^1 = \begin{pmatrix} 5 \\ 1 \end{pmatrix} \qquad B^2 = \begin{pmatrix} -1 \\ -2 \end{pmatrix}$$

et neuf points fondamentaux :

$$\overset{1}{x} = \begin{pmatrix} 15 \\ 3 \end{pmatrix},\ \overset{2}{x} = \begin{pmatrix} 16 \\ 4 \end{pmatrix},\ \overset{3}{x} = \begin{pmatrix} 16 \\ 3 \end{pmatrix},\ \overset{4}{x} = \begin{pmatrix} 17 \\ 4 \end{pmatrix},\ \overset{5}{x} = \begin{pmatrix} 12 \\ 2 \end{pmatrix},$$

$$\overset{6}{x} = \begin{pmatrix} 13 \\ 3 \end{pmatrix},\ \overset{7}{x} = \begin{pmatrix} 13 \\ 2 \end{pmatrix},\ \overset{8}{x} = \begin{pmatrix} 14 \\ 3 \end{pmatrix},\ \overset{9}{x} = \begin{pmatrix} 14 \\ 2 \end{pmatrix}.$$



V.2 CONE CONTENANT UNE VARIETE LINEAIRE ([13],[14])

Considérons $\{x \mid Ax \geq b\}$ où A est une (m,n) matrice avec $m < n$, de rang m. Les éléments de A appartiennent à $\mathbb{Z}$ (ou Q), $b \in \mathbb{R}^m$.

Théorème V.2 : Tous les points entiers d'un tel cône sont donnés par la formule suivante :

$$x = \overset{i}{x} + k_1 B^1 + \ldots + k_m B^m + y_{m+1} V^{m+1} + \ldots + y_n V^n.$$

Cette décomposition est unique.

B^j *est parallèle à la variété linéaire* $K_j = \{x \mid A_i x = b_i \quad i \neq j\}$ *pour tout* $j=1,2,\ldots,m$.

V^j *est parallèle à la variété linéaire* $A^* = \{x \mid A_i x = b_i \quad i=1,2,\ldots,m\}$

$k_j \in N \quad j=1,2,\ldots,m$

$y_p \in \mathbb{Z} \quad p=m+1,\ldots,n.$

L'ensemble des $\overset{i}{x}$ *est appelé l'ensemble des points fondamentaux (ensemble* P_f*). Les points fondamentaux sont les seuls points entiers de l'ensemble suivant :*

$$\{x \mid x = \overset{0}{x} + \lambda_1 B^1 + \ldots + \lambda_m B^m,\ 0 \leq \lambda_i < 1,\ \lambda_i \in \mathbb{R},\ i=1,2,\ldots,m\},$$

$\overset{0}{x}$ *étant un point parfaitement déterminé.*

Le nombre de points fondamentaux de ce cône est égal au p.g.c.d. de B *où* $B = [B^1,\ldots,B^m]$.

Preuve :

V.2.1 Calcul des points entiers de ce cône

Il existe deux matrices unimodulaires U(m,m) et V(n,n) telles que UAV = E, E(m,n) étant une forme normale de Smith de A.

$$Ax = a \Longleftrightarrow Ey = Ua \quad \text{avec} \quad x = Vy.$$

Définissons $R = \{1,2,\ldots,m\}$ et $\bar{R} = \{m+1,\ldots,n\}$. Nous pouvons écrire $x = Vy = V^R y_R + V^{\bar{R}} y_{\bar{R}}$.

Appelons $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_m$ les éléments diagonaux de E. Le calcul des a admissibles se fait comme en V.1.1. Nous obtenons :

$$\overset{i}{a} = \overset{i}{P} + \varepsilon k_1 \delta^1 + \ldots + \varepsilon k_m \delta^m \quad \text{pour} \quad i=1,2,\ldots,p_1 \times p_2 \times \ldots \times p_m,$$

avec ${}^t\overset{i}{P} = (\overset{i}{\gamma}_1,\ldots,\overset{i}{\gamma}_m)$ et $b_j < \overset{i}{P}_j < b_j + \varepsilon$ pour $j=1,2,\ldots,m$,

et $i=1,2,\ldots,p_1 \times p_2 \times \ldots \times p_m$.

$$V^R y_R = V^R (E^R)^{-1} Ua.$$

Posons : $M = V^R (E^R)^{-1} U$, qui n'est autre que l'inverse à droite de A et $B = \varepsilon M$. Alors tous les points entiers de V.2 sont donnés par :

$$x = M\overset{i}{P} + k_1 B^1 + \ldots + k_m B^m + V^{m+1} y_{m+1} + \ldots + V^n y_n,$$

pour $i=1,2,\ldots,p_1 \times p_2 \times \ldots \times p_m$, où $k_i \in N$ pour $i=1,2,\ldots,m$ et $y_p \in \mathbb{Z}$ pour $p = m+1,\ldots,n$.

V.2.2 Propriétés de $B^1,\ldots,B^m, V^{m+1},\ldots,V^n$

De $B = \varepsilon M$ nous déduisons que $A_i . B^j = 0$ pour $i \neq j$, c'est-à-dire que B^j est parallèle à la variété $K_j = \{x \mid A_i x = b_i \quad i \neq j\}$.

De $UAV = E$ nous déduisons que $AV^{\bar{R}} = 0$ c'est-à-dire que V^j (pour $j \in \bar{R}$) est parallèle à la variété linéaire $A^* = \{x \mid A_i x = b_i,\ i=1,2,\ldots,m\}$.

Nous pouvons remarquer que ces vecteurs $B^1,B^2,\ldots,B^m,V^{m+1},\ldots,V^n$, sont linéairement indépendants.

V.2.3 Parallélotope fondamental

Considérons l'ensemble suivant que nous appellerons parallélotope du cône :

$$E = \{x = \overset{0}{x} + \lambda_1 B^1 + \ldots + \lambda_m B^m,\ 0 \leq \lambda_i < 1,\ \lambda_i \in \mathbb{R},\ i=1,2,\ldots,m\}$$

où $\overset{0}{x} = V^R(E^R)^{-1}\, Ub = Mb$ c'est-à-dire que $\overset{0}{x}$ est un point (non entier en général) de la variété linéaire $Ax = b$.

Etant donné $b_j \leqslant \overset{i}{P}_j < b_j + \varepsilon$, pour $j=1,2,\ldots,m$ et $i=1,2,\ldots,p_1 \times p_2 \times \ldots \times p_m$, nous considérons le vecteur $\overset{i}{\lambda} = \frac{1}{\varepsilon}(\overset{i}{P}-b)$. Ses composantes sont telles que $0 \leqslant \overset{i}{\lambda}_j < 1$. Appliquons M à la dernière égalité $M\varepsilon\overset{i}{\lambda} = \overset{i}{MP} - Mb$ où $\overset{i}{x} = \overset{0}{x} + B\lambda$; ainsi tous les points fondamentaux sont dans E.

Inversement un point entier x de E étant aussi un point entier du cône, $x = \overset{i}{x} + k_1B^1 + \ldots + k_mB^m + y_{m+1}V^{m+1} + \ldots + y_nV^n$. Or $\overset{i}{x} = \overset{0}{x} + \lambda_1B^1 + \ldots + \lambda_mB^m$ avec $0 \leqslant \lambda_j < 1 \quad j=1,\ldots,m$, ce qui entraîne que $k_1 = k_2 = \ldots = k_m = y_{m+1} = \ldots = y_n = 0$ et $x = \overset{i}{x}$. Tous les points entiers de E sont des points fondamentaux.

V.2.4 Nombre de points fondamentaux

Montrons que le nombre de points fondamentaux d'un tel cône est égal à $\frac{\varepsilon^m}{\Delta(A)} = \Delta(B)$ où $\Delta(A)$ et $\Delta(B)$ sont respectivement les p.g.c.d. de A et de B.

Le nombre de points fondamentaux est donné par $p_1 \times p_2 \times \ldots \times p_m$. Nous avons :

$$\varepsilon = [\varepsilon_1,\ldots,\varepsilon_m] = \varepsilon_m$$

$$\varepsilon = \varepsilon_1\nu_1 = \ldots = \varepsilon_m\nu_m$$

$$\nu_1 \geqslant \nu_2 \geqslant \ldots \geqslant \nu_m = 1$$

$$\nu_i \mid \nu_{i-1} \text{ pour } i=2,\ldots,m.$$

Alors $\Delta_i(C) = \nu_{m-1} \times \nu_{m-2} \times \ldots \times \nu_{m-i+1} = g_1 \times g_2 \times \ldots \times g_i$ pour $i=1,2,\ldots,m$ ce qui entraîne que $g_i = \nu_{m-i+1}$.
Or $p_i = (g_i,\varepsilon) = (\nu_{m-i+1},\ \nu_{m-i+1}\ \varepsilon_{m-i+1}) = \nu_{m-i+1}$.

$$p_1 \times p_2 \times \ldots \times p_m = \nu_m \times \nu_{m-1} \times \ldots \times \nu_1 = \frac{\varepsilon}{\varepsilon_m} \times \frac{\varepsilon}{\varepsilon_{m-1}} \times \ldots \times \frac{\varepsilon}{\varepsilon_1} = \frac{\varepsilon^m}{\Delta(A)}$$ où $\Delta(A)$ est le p.g.c.d. de A.

Maintenant montrons que $\frac{\varepsilon^m}{\Delta(A)} = \Delta(B)$.

Considérons $V^{-1}BU^{-1} = V^{-1}\,\varepsilon V^R(E^R)^{-1} = V^{-1}V^R\,\varepsilon(E^R)^{-1}$. $\varepsilon(E^R)^{-1}$ est une matrice diagonale dont les éléments sont $\nu_1,\nu_2,\ldots,\nu_m$. Par suite $V^{-1}BU^{-1}$ est une matrice (m,n) dont les éléments sont nuls sauf ceux de la diagonale principale qui sont égaux à $\nu_1,\nu_2,\ldots,\nu_m$. Alors d'après la remarque I, $\Delta(B) = \nu_1 \times \nu_2 \times \ldots \times \nu_m$. CQFD.

Les formules données entraînent par exemple qu'un demi-espace ne possède qu'un seul point fondamental.

Exemple V.2

a) Cône défini par :

$$-7x_1 + 9x_2 + 13x_3 + 19x_4 + x_5 \geq \frac{14}{3}$$

$$5x_1 - 7x_2 - 3x_3 + 5x_4 - 17x_5 \geq \frac{7}{9}$$

$$3x_1 + 5x_2 - 5x_3 - 7x_4 - 9x_5 \geq \frac{16}{5}$$

Le calcul donne :

$${}^tB^1 = (5327,\ 697,\ 2307,\ 8,\ 875)\ ,$$

$${}^tB^2 = (658,\ 86,\ 285,\ 1,\ 108),$$

$${}^tB^3 = (-651,\ -85,\ -282,\ -1,\ -107),$$

deux points fondamentaux :

$${}^tx^1 = (15\ 337,\ 2007,\ 6642,\ 23,\ 2519),$$

$${}^tx^2 = (12019,\ 1573,\ 5205,\ 18,\ 1974),$$

et

$${}^tV^4 = (-89,\ -12,\ -37,\ -1,\ -15),$$

$${}^tV^5 = (24,\ 6,\ -2,\ 7,\ 7).$$

b) Demi-espace : $2x_1 + 3x_2 + 4x_3 \geq \frac{13}{2}$

Nous trouvons ${}^tB^1 = (-1,1,0)$, ${}^tV^2 = (3,-2,0)$, ${}^tV^3 = (-2,0,1)$ et un point fondamental ${}^tx^1 = (-7,7,0)$.

V.3 CONE POLYEDRIQUE DEFINI PAR {x | Ax > b} OU A EST UNE (m,n) MATRICE, m > n.

Ce cône peut être décomposé en une réunion de cônes réguliers (V.1) et nous utilisons pour chacun d'eux la génération de leurs points entiers comme elle a été définie en V.1. Dans cette décomposition, deux cônes réguliers ont au plus une face en commun. Pour obtenir cette décomposition nous utilisons la méthode simpliciale (voir [1]) qui nous permet de générer les sommets de tout polyèdre, en particulier des directions d'infinitude. L'intérêt de la méthode simpliciale est que cette génération se fait en passant d'un sommet (ou d'une direction d'infinitude) à un sommet voisin (ou à une direction d'infinitude voisine) c'est-à-dire dont les bases correspondantes ne diffèrent que d'un seul élément.

Chapitre VI

GENERATION des POINTS ENTIERS d'un PARALLELOTOPE de $\mathbb{R}^n$

VI.1 PARALLELOTOPE BORNE ([15], [16])

Un parallélotope borné de $\mathbb{R}^n$ est défini par :

$\{x \mid c \geq Ax \geq b\}$ où A est une matrice (n,n) de rang n, à éléments dans $\mathbb{Z}$, b et $c \in \mathbb{R}^n$.

Théorème VI.1 : Tous les points entiers d'un parallélotope borné de $\mathbb{R}^n$ sont donnés par :

$$x = \overset{i}{x} + \overset{i}{k}_1 B^1 + \ldots + \overset{i}{k}_n B^n.$$

Cette décomposition est unique.

$i \in K$ *(un sous-ensemble fini de* N)

$B^1,\ldots,B^n$ *sont* n *vecteurs linéairement indépendants à composantes entières. Ils sont parallèles aux arêtes du parallélotope* $\overset{i}{k}_j \in N$ *tels que* $0 \leq \overset{i}{k}_j \leq \overset{i}{\ell}_j$ *pour* $j=1,2,\ldots,n$ *et* $i \in K$.

L'ensemble des $\overset{i}{x}$ *est appelé ensemble des points fondamentaux (ensemble* P_f^**). Ces points sont les seuls points entiers d'un parallélotope semi-ouvert qui est appelé parallélotope fondamental du parallélotope.*

VI.1.1 Calcul des a admissibles

Comme en V.1 nous avons UAV = E, E est une forme normale de Smith de A.

$$Ax = a \Longleftrightarrow Ey = Ua \quad \text{avec} \quad x = Vy.$$

Nous trouvons comme en V.1.1 que les solutions de $Ca \equiv 0(\varepsilon)$ avec $a \geq b$ sont données par :

$$t_a^i = (\overset{i}{\gamma}_1 + k_1\varepsilon,\ \overset{i}{\gamma}_2 + k_2\varepsilon,\ \ldots,\ \overset{i}{\gamma}_n + k_n\varepsilon).$$

Deux cas peuvent se présenter :

a) $\exists$ j tel que $\overset{i}{\gamma}_j > c_j$, alors le point $\overset{i}{a}$ n'est pas admissible.

b) $\forall$ j, $\overset{i}{\gamma}_j \leqslant c_j$, $\overset{i}{a}$ est admissible. Appelons $\overset{i}{\ell}_j$ le plus grand nombre entier tel que $\overset{i}{\gamma}_j + \varepsilon\,\overset{i}{\ell}_j \leqslant c_j$.

L'ensemble des a admissibles est donné par :

$t_a^i = (\overset{i}{\gamma}_1 + \overset{i}{k}_1\varepsilon,\ \ldots,\ \overset{i}{\gamma}_n + \overset{i}{k}_n\varepsilon)$ où $\overset{i}{k}_j$ sont des entiers tels que $0 \leqslant \overset{i}{k}_j \leqslant \overset{i}{\ell}_j$.

Notons K le sous-ensemble des i de $\{1,2,\ldots,p_1 \times p_2 \times \ldots \times p_n\}$ tels que $b \leqslant \overset{i}{a} \leqslant c$.

Nous avons alors $T = \sum_{i \in K} (\overset{i}{\ell}_1+1) \times \ldots \times (\overset{i}{\ell}_n+1)$ points admissibles et par suite T points entiers dans le parallélotope. Définissons $t\overset{i}{P} = (\overset{i}{\gamma}_1,\ldots,\overset{i}{\gamma}_n)$; on peut écrire que :

$$\overset{i}{a} = \overset{i}{P} + \varepsilon\overset{i}{k}_1\delta^1 + \ldots + \varepsilon\,\overset{i}{k}_n\delta^n,\ i \in K.$$

VI.1.2 Points entiers du parallélotope

De $x = Vy$ et de $y = E^{-1}Ua$ nous déduisons en posant $M = VE^{-1}U = A^{-1}$ et $B = \varepsilon M$, que tous les points entiers du parallélotope sont donnés par :

$$x = M\overset{i}{P} + \overset{i}{k}_1B^1 + \ldots + \overset{i}{k}_nB^n,$$

avec $i \in K$ et $0 \leqslant \overset{i}{k}_j \leqslant \overset{i}{\ell}_j$ pour $i \in K$ et $j = 1,2,\ldots,n$.

De $B = \varepsilon A^{-1}$ nous déduisons que B^j est parallèle aux n-1 hyperplans $A_ix = b_i$, $i \neq j$.

Les points $M\overset{i}{P} = \overset{i}{x}$ pour $i \in K$ constituent l'ensemble P_f^*. P_f^* est un sous-ensemble de P_f associé au cône asymptotique $Ax \geqslant b$. Notons que P_f^* n'est pas

unique en ce sens qu'il est associé à un sommet $\bar{x}$ du parallélotope : dans la preuve du théorème il était associé au sommet solution de l'équation $Ax = b$. Néanmoins le nombre de points de P_f^* est le même quel que soit le sommet $\bar{x}$ considérer.

Exemple VI.1 - Considérons le parallélogramme de $\mathbb{R}^2$ suivant :

$$-16 \leq x + y \leq 22$$
$$-5 \leq 2x - y \leq 1$$

Le calcul donne :

$$B^1 = \begin{pmatrix}1\\2\end{pmatrix} \quad \text{et} \quad B^2 = \begin{pmatrix}5\\-1\end{pmatrix}$$

$$\overset{1}{a} = \begin{pmatrix}-11\\0\end{pmatrix} + 11 \begin{pmatrix}\overset{1}{k}_1\\ \overset{1}{k}_2\end{pmatrix} \quad \text{avec } 0 \leq \overset{1}{k}_1 \leq 3 \text{ et } \overset{1}{k}_2 = 0.$$

$\overset{2}{a} = \begin{pmatrix}-10\\2\end{pmatrix} \pmod{11}$, $\overset{3}{a} = \begin{pmatrix}-8\\6\end{pmatrix} \pmod{11}$ ne sont pas admissibles.

$$\overset{4}{a} = \begin{pmatrix}-8\\-5\end{pmatrix} + 11 \begin{pmatrix}\overset{4}{k}_1\\ \overset{4}{k}_2\end{pmatrix} \text{ avec } 0 \leq \overset{4}{k}_1 \leq 2 \text{ et } \overset{4}{k}_2 = 0.$$

$$\overset{5}{a} = \begin{pmatrix}-7\\-3\end{pmatrix} + 11 \begin{pmatrix}\overset{5}{k}_1\\ \overset{5}{k}_2\end{pmatrix} \text{ avec } 0 \leq \overset{5}{k}_2 \leq 2 \text{ et } \overset{5}{k}_2 = 0.$$

$$\overset{6}{a} = \begin{pmatrix}-6\\-1\end{pmatrix} + 11 \begin{pmatrix}\overset{6}{k}_1\\ \overset{6}{k}_2\end{pmatrix} \text{ avec } 0 \leq \overset{6}{k}_1 \leq 2 \text{ et } \overset{6}{k}_2 = 0.$$

$$\overset{7}{a} = \begin{pmatrix}-16\\1\end{pmatrix} + 11 \begin{pmatrix}\overset{7}{k}_1\\ \overset{7}{k}_2\end{pmatrix} \text{ avec } 0 \leq \overset{7}{k}_1 \leq 3 \text{ et } \overset{7}{k}_2 = 0.$$

$\overset{8}{a} = \begin{pmatrix}-15\\3\end{pmatrix} \pmod{11}$, $\overset{9}{a} = \begin{matrix}-14\\5\end{matrix} \pmod{11}$ ne sont pas admissibles.

$$\overset{10}{a} = \begin{pmatrix}-13\\-4\end{pmatrix} + 11 \begin{pmatrix}\overset{10}{k}_1\\ \overset{10}{k}_2\end{pmatrix} \text{ avec } 0 \leq \overset{10}{k}_1 \leq 3 \text{ et } \overset{10}{k}_2 = 0.$$

$$\overset{11}{a} = \begin{pmatrix}-12\\-2\end{pmatrix} + 11 \begin{pmatrix}\overset{11}{k}_1\\ \overset{11}{k}_2\end{pmatrix} \text{ avec } 0 \leq \overset{11}{k}_1 \leq 3 \text{ et } \overset{11}{k}_2 = 0.$$

L'ensemble P_f^* est :

$$\overset{1}{x} = \begin{pmatrix} -1 \\ -2 \end{pmatrix}, \overset{4}{x} = \begin{pmatrix} -3 \\ -1 \end{pmatrix}, \overset{5}{x} = \begin{pmatrix} -2 \\ -1 \end{pmatrix}, \overset{6}{x} = \begin{pmatrix} -1 \\ -1 \end{pmatrix}, \overset{7}{x} = \begin{pmatrix} -1 \\ -3 \end{pmatrix}, \overset{10}{x} = \begin{pmatrix} -3 \\ -2 \end{pmatrix}, \overset{11}{x} = \begin{pmatrix} -2 \\ -2 \end{pmatrix}$$

$p_1 \times p_2 \times \ldots \times p_n = |\det B| = 11, |K| = 7, T = 25.$

VI.2 PARALLELOTOPES NON BORNES ([15], [16])

Pour les deux cas suivants, la preuve peut être déduite immédiatement de VI.1.

VI.2.1 *1er type* :

$$\{x \mid b_J \leqslant A_J x \leqslant c_J,\ b_{J'} \leqslant A_{J'} x,\ J \cup J' = n,\ J \cap J' = \emptyset,\ A_{J \cup J'} \text{ de rang } n\}$$

Corollaire VI.2.1 : Tous les points entiers de ce parallélotope sont donnés par la formule suivante :

$$x = \overset{i}{x} + \sum_{j \in J} \overset{i}{k}_j B^j + \sum_{j \in J'} k_j B^j .$$

Cette décomposition est unique.

$i \in K$ *(sous-ensemble fini de* $\mathbb{N}$*)*

B^j *comme dans le théorème VI.1.*

$k_j \in \mathbb{N}$ *pour* $j \in J'$.

$\overset{i}{k}_j$ *entiers tels que* $0 \leqslant \overset{i}{k}_j \leqslant \overset{i}{\ell}_j$ *pour* $i \in K$ *et* $j \in J$.

L'ensemble des $\overset{i}{x}$ *est l'ensemble des points fondamentaux* (P_f^*).

P_f^* *est dans un parallélotope semi-ouvert appelé parallélotope fondamental du parallélotope.*

VI.2.2 *2ème type* :

$$\{x \mid b_J \leqslant A_J x \leqslant c_J,\ b_{J'} \leqslant A_{J'} x\ ,\ J = \{1,2,\ldots,s\},$$

$$J' = \{s+1,\ldots,m\}\ ,\ m < n,\ A_{J \cup J'} \text{ de rang } m\}$$

Corollaire VI.2.2 : Tous les points entiers de ce parallélotope sont donnés par la formule suivante :

$$x = \overset{i}{x} + \sum_{j \in J} \overset{i}{k}_j \, B^j + \sum_{j \in J'} k_j \, B^j + \sum_{j \in L} y_j \, V^j .$$

Cette décomposition est unique.

$i \in K$.

B^j *pour* $j \in J \cup J'$ *sont des vecteurs parallèles aux variétés* $K_j = \{x \mid A_i x = b_i$ *pour* $i, j \in J \cup J', i \neq j\}$.

V^j *pour* $j \in L = \{m+1, \ldots, n\}$ *sont des vecteurs parallèles à la variété linéaire* $A^* = \{x \mid A_i x = b_i, i \in J \cup J'\}$.

$k_j \in N$ *pour* $j \in J'$.

$\overset{i}{k}_j$ *sont des entiers tels que* $0 \leq \overset{i}{k}_j \leq \overset{i}{\ell}_j$ *pour* $i \in K$ *et* $j \in J$.

$y_j \in \mathbb{Z}$ *pour* $j \in L$.

L'ensemble des $\overset{i}{x}$ *est l'ensemble des points fondamentaux* (P_f^*).

Chapitre VII

QUELQUES PROPRIETES ALGEBRIQUES et GEOMETRIQUES

VII.1 PROPRIETES LIEES AUX CONES POLYEDRIQUES, AUX PARALLELOTOPES DE $\mathbb{R}^n$ ET AUX MATRICES UNIMODULAIRES ET SEMI-MODULAIRES. [16]

Proposition VII.1 : Le cône V.1 ou les parallélotopes de VI.1 et VI.2.1 ont un point fondamental et un seul si et seulement si la matrice A = εU où ε ∈ Z et U est une matrice unimodulaire.

Preuve :

Le nombre de points fondamentaux est donné par la formule $N = \frac{\varepsilon^n}{\det A}$.

Nous devons avoir $\varepsilon^n = |\det A|$. Or de $\det A = \varepsilon_1 \times \varepsilon_2 \times \ldots \times \varepsilon_n$ avec $\varepsilon_i | \varepsilon_{i+1}$ pour i=1,2,...,n-1, nous déduisons qu'il faut $\varepsilon_i = \varepsilon_n$ pour tout i=1,2,...,n-1. En particulier $\varepsilon_1 = \varepsilon_n = \varepsilon$ c'est-à-dire que $\Delta_1(A) = \varepsilon$: tous les éléments de A sont multiples de ε. Posons A = εW.

De UAV = E nous déduisons que det A = det E c'est-à-dire que $\varepsilon^n |\det W| = \varepsilon^n$ donc det W = ±1, W est donc une matrice unimodulaire.

Inversement pour une matrice de la forme A = εW où W est unimodulaire et ε ∈ Z - {0}, la forme normale de Smith a des ε sur la diagonale car $\Delta_i(A) = (\varepsilon)^i$ pour i=1,2,...,n. Alors $N = \frac{\varepsilon^n}{|\det A|} = 1$.

Corollaire VII.1 : Le cône V.2 et le parallélotope VI.2.2 ont un point fondamental et un seul si et seulement si A = εW où ε ∈ Z et W est semi-modulaire.

Preuve :

Dans ce cas nous devons avoir $\varepsilon^m = \Delta(A)$ c'est-à-dire $\varepsilon^m = \varepsilon_1 \times \varepsilon_2 \times \ldots \times \varepsilon_m$ avec $\varepsilon_i | \varepsilon_{i+1}$ pour i=1,2,...,m-1. Nous en déduisons $\varepsilon_i = \varepsilon_m = \varepsilon$ pour tout i=1,2,...,m-1.

De $\Delta_1(A) = \varepsilon_1 = \varepsilon$ nous pouvons écrire que A = εW et que UAV = E où E = ε[I,0] (I étant la matrice unité de rang m, 0 la matrice (m,n-m) à

éléments nuls). Ainsi nous obtenons ε U WV = ε[I,0], ce qui donne $\Delta_m(W) = \Delta(W) = 1$ d'après la proposition *1*. Par suite W est semi-modulaire (c'est une propriété caractéristique d'après réf. [10] page 36).

Inversement, si $A = \varepsilon W$ avec $\varepsilon \in Z - \{0\}$ et W semi-modulaire, les formes normales de Smith de A ont des ε sur la diagonale principale car $\Delta_i(A) = (\varepsilon)^i$ pour i=1,2,...,m. Alors $N = \dfrac{\varepsilon^m}{\Delta(A)} = 1$.

VII.2 PROPRIETE GEOMETRIQUE [16] :

*Proposition VII.2** : *Etant donné un parallélotope semi-ouvert :* $\{x \mid x = T + \lambda_1 C^1 + \ldots + \lambda_n C^n\}$ *avec* $T \in \mathbb{R}^n$, C^i *étant* n *vecteurs linéairement indépendants à coordonnées entières,* $0 \leq \lambda_i < 1$, $\lambda_i \in \mathbb{R}$ *pour* $i=1,2,\ldots,n$. *Alors le nombre de points entiers de ce parallélotope est exactement égal à son volume.*

Preuve :

Nous supposons que les vecteurs colonnes C^i sont réduits c'est-à-dire que le p.g.c.d. de leurs éléments est égal à 1. Si certains vecteurs ne l'étaient pas, par exemple $C^j = q_j C'^j$ pour $j \in J \subset \{1,2,\ldots,n\}$, nous prendrions $C' = [C'^J, C^{\{1,2,\ldots,n\}-J}]$. C' définirait un parallélotope avec $\prod_{j \in J} q_j$ moins de points que celui défini par C.

Nous allons montrer que le parallélotope donné, une fois réduit, est le parallélotope fondamental d'un cône ayant T pour sommet et dont les arêtes sont parallèles aux C^i.

Considérons la réduite de Smith de C, soit D = SCR. Les éléments diagonaux de D sont $1, d_2, d_3, \ldots, d_n$. A partir de $C^{-1} = RD^{-1}S$ nous définissons $A = d_n C^{-1} = R(d_n D^{-1})\, S$. Nous avons $R^{-1} A S^{-1} = d_n D^{-1}$.

Il existe deux matrices de permutation U et V telles que $(UR^{-1})\, A\, (S^{-1}V) = U(d_n D^{-1})\, V = E$ où les deux éléments diagonaux de E sont $1, \frac{d_n}{d_{n-1}}, \ldots, \frac{d_n}{d_2}, d_n$, tels que $\frac{d_n}{d_j} \mid \frac{d_n}{d_{j-1}}$ pour $j=2,\ldots,n-1$; les autres éléments de E étant nuls. Ainsi E est la réduite de Smith de A.

Les matrices de permutation U et V sont égales, tous leurs éléments sont égaux à zéro sauf les éléments U^j_i ou V^j_i avec $i+j=n+1$ qui sont égaux à 1.

Le cône cherché est défini par $Ax \geq b$ où $b = AT$ et $A = d_n C^{-1}$. La matrice des vecteurs de translation associée à A est $B^* = d_n A^{-1} = C$. Ainsi le parallélotope donné est le parallélotope fondamental de ce cône et nous pouvons

* Cette propriété est, paraît-il, déjà démontrée mais nous sommes incapables de citer une référence exacte.

appliquer V.1.4 et V.1.5 : le nombre de points entiers de ce parallélotope est égal à $\frac{(d_n)^n}{|\det A|} = \frac{1}{|\det C^{-1}|} = |\det C|$, donc égal au volume du parallélotope.

VII.3 PROPRIETE ALGEBRIQUE : INVARIANT LIE AUX FORMES NORMALES DE SMITH D'UNE MATRICE QUELCONQUE.

D'après les constructions données aux paragraphes II.2.1 et II.2.4 nous constatons que pour obtenir la forme réduite de Smith il faut faire beaucoup plus de calculs que pour obtenir une forme normale de Smith. De plus dans l'algorithme de recherche des points entiers d'un cône ou d'un parallélotope nous avons considéré, pour les mêmes raisons, une forme normale et le p.p.c.m. des éléments diagonaux de cette forme. Mais pour établir les formules de V.1.5 et de V.2.4 donnant le nombre de points fondamentaux nous avons été obligés de considérer chaque fois la réduite de Smith et le p.p.c.m. de ses éléments diagonaux, lequel est égal dans ce cas au plus grand élément.

Afin de se limiter dans la pratique (c'est ce qui est fait en annexe 6) à un algorithme basé sur le calcul d'une forme normale, il importe donc de démontrer que ces deux p.p.c.m. sont égaux. C'est ce que nous allons faire.

Propriété VII.3 : *Le p.p.c.m. des éléments diagonaux non nuls d'une forme normale quelconque de Smith d'une matrice A est un invariant égal au plus grand élément de sa réduite de Smith.*

Preuve :

Elle découle directement de la remarque de [10] page 46 . Considérons une forme normale quelconque de Smith de A dont les éléments diagonaux seront toujours notés $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n$. Nous montrons qu'avec une construction particulière nous pouvons transformer cette forme normale en une autre et itérer le processus pour obtenir la réduite de A, de telle sorte que le p.p.c.m. des éléments non nuls de chacune d'elles soit le même.

a) A l'aide de matrices de permutations nous rangeons les éléments de la diagonale de la forme normale dans l'ordre croissant.

b) Soit j le premier indice tel que $\varepsilon_j \nmid \varepsilon_k$ pour k>j. A l'aide de matrices élémentaires opérant seulement sur les termes en (j,j), (k,k), (j,k) et (k,j), nous remplaçons le terme en (j,j) par $(\varepsilon_j,\varepsilon_k) = d$ de manière à obtenir une nouvelle forme normale.

Pour être plus précis, ceci est réalisé en multipliant la forme normale à droite par une matrice V, à gauche par une matrice U.

La matrice V est définie par :

$V_i^i = 1$ sauf pour i=j et i=k,

$V_j^j = \alpha$, $V_k^k = \frac{\varepsilon_j}{d}$, $V_j^k = -\frac{\varepsilon_k}{d}$, $V_k^j = \beta$,

α et β étant tels que $\alpha\varepsilon_j + \beta\varepsilon_k = d = (\varepsilon_j, \varepsilon_k)$,

les autres termes de V étant nuls.

La matrice U est définie par :

$U_i^i = 1$ sauf pour i=k,

$U_k^j = -\frac{\varepsilon_k - \beta}{d}$, $U_k^k = 1 + U_k^j$,

les autres termes de U étant nuls.

U et V sont deux matrices unimodulaires.
Appelons δ_k l'élément en (k,k) de la nouvelle forme normale.

De $\det A = \varepsilon_1 \times \ldots \times \varepsilon_j \times \ldots \times \varepsilon_k \times \ldots \times \varepsilon_n = \varepsilon_1 \times \ldots \times \varepsilon_{j-1} \times (\varepsilon_j, \varepsilon_k) \times \varepsilon_{j+1} \times \ldots \times \varepsilon_{k-1} \times \delta_k \times \varepsilon_{k+1} \times \ldots \times \varepsilon_n$, nous déduisons que $(\varepsilon_j, \varepsilon_k) \times \delta_k = \varepsilon_j \varepsilon_k$ c'est-à-dire que $\delta_k = [\varepsilon_j, \varepsilon_k]$.

De plus nous avons :

$$[\varepsilon_1, \ldots, \varepsilon_j, \ldots, \varepsilon_k, \ldots, \varepsilon_n] = [\varepsilon_1, \ldots, (\varepsilon_j, \varepsilon_k), \ldots, [\varepsilon_j, \varepsilon_k], \ldots, \varepsilon_n].$$

Si pour le même j il existe un autre $k' > k$ tel que $\varepsilon_j \nmid \varepsilon_{k'}$, nous retournons en a) et b) jusqu'à ce que $\varepsilon_j \mid \varepsilon_k$ pour tout $k > j$.

Ce que nous avons fait pour ε_j sera fait pour ε_{j+1} et ainsi de suite de

manière à obtenir la forme réduite c'est-à-dire $\varepsilon_i \mid \varepsilon_{i+1}$ pour $i=1,2,\ldots,n-1$.

Le procédé nous permet d'affirmer que les p.p.c.m. des éléments diagonaux de toute forme normale sont égaux entre eux et égaux à ε_n de la réduite trouvée (réduite qui rappelons-le est unique).

La preuve a été établie pour une matrice $A(n,n)$, elle s'établit de la même manière pour toute matrice $A(m,n)$.

VII.4 RESOLUTION D'UN PROBLEME GENERAL

Nous généralisons le problème résolu aux chapitres V et VI, à savoir chercher tous les x entiers qui vérifient :

$$Ax \; \mathcal{R} b,$$

où $\mathcal{R}$ est une relation quelconque; en fait ce sera une relation d'ordre quelconque sur un anneau.

A est une (m,n) matrice ; si m = n elle est de rang n, si m < n, elle est de rang m, ses éléments sont entiers, b est un vecteur à coordonnées réelles ou entières selon les cas.

Pour cela nous posons Ax = a et nous cherchons tous les a admissibles, c'est-à-dire qui :

1) donnent des solutions entières aux systèmes Ax = a,

2) vérifient a$\mathcal{R}$b.

Le premier point s'obtient en utilisant la technique de résolution des systèmes linéaires en nombres entiers. Avec les notations déjà utilisées auparavant nous obtenons :

$$Ax = a \iff Ey = Ua \quad (\text{avec } x = Vy) \qquad (VII.4.1)$$

$\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n$ étant les éléments diagonaux de E, posons $\varepsilon = [\varepsilon_1,\ldots,\varepsilon_n]$, $\varepsilon = \nu_i \; \varepsilon_i$, $C_i = \nu_i \; U_i$ pour i=1,2,...,n. (VII.4.1) s'écrit

$$Ca \equiv 0 \pmod{\varepsilon}$$

d'où $a \equiv \overset{i}{a} \pmod{\varepsilon}$ pour $i=1,2,\ldots,p_1 \times p_2 \times \ldots \times p_n$.

Revenons à 2), il faut $\overset{i}{a}\; \mathcal{R} b$ c'est-à-dire que pour i fixé il faut qu'il existe au moins un k_j tel que

$$(\overset{i}{a}_j + k_j\varepsilon) \; \mathcal{R} b_j \text{ pour tous les } j=1,2,\ldots,n. \qquad (VII.4.2)$$

Appelons L le sous-ensemble de $\{1,2,\ldots,p_1\times p_2\times\ldots\times p_n\}$ tel que 2) soit réalisé.

L'ensemble des $\overset{i}{a}$ pour $\overset{i}{a} \in L$ constitue l'ensemble des a admissibles. Ils peuvent s'écrire :

$$\overset{i}{a} = \overset{i}{P} + \varepsilon k_1 \delta^1 + \ldots + \varepsilon k_n \delta^n \qquad i \in L.$$

Un $\overset{i}{a}$ admissible peut fournir un nombre fini de solutions (c'est le cas où la relation est la relation de divisibilité, voir ci-dessus) ou un nombre infini de solutions (cas de la relation $\geq$, au chapitre V), selon que l'ensemble des n-upples k_j est fini ou non.

L'ensemble des solutions du problème est alors donné par $x = M\overset{i}{a}$ où $M = VE^{-1}U$.

$$x = M\overset{i}{P} + k_1 B^1 + \ldots + k_n B^n \qquad i \in L$$

les k_j étant déterminés par les relations (VII.4.2).

Dans le cas où la matrice est rectangulaire, $m < n$, nous obtenons

$$x = M\overset{i}{P} + k_1 B^1 + \ldots + k_m B^m + y_{m+1} V^{m+1} + \ldots + y_n V^n,$$

où $y_{m+1}, \ldots, y_n$ sont des entiers quelconques.

Exemple VII - Nous traitons le cas où la relation R est celle de la divisibilité.

Recherche de tous les x entiers tels que :

$$\begin{array}{rcl} 21x_1 - 10x_2 + 4x_3 & | & 31 \\ x_1 - x_2 - 2x_3 & | & 3 \\ -3x_1 + 4x_2 + 10x_3 & | & 7 \end{array}$$

La partie 1) nous fournit 4 solutions :

$$t^1_a = (0,0,0) \pmod 2, \quad t^2_a = (11,0,1) \pmod 2, \quad t^3_a = (21,1,-3) \pmod 2,$$

$$t^4_a = (32,1,-2) \pmod 2.$$

$\overset{1}{a}, \overset{2}{a}, \overset{4}{a}$ ne sont pas admissibles car :

$$\overset{1}{a}_1 = 2k_1 \not| 31$$

$$\overset{2}{a}_2 = 2k_2 \not| 3,$$

$$\overset{4}{a}_3 = -2 + 2k_3 \not| 7$$

$\overset{3}{a}$ est admissible et donne 27 solutions car

$$21 + 2k_1 \mid 31 \quad \text{pour} \quad k_1 = -26, -10, 5$$

$$1 + 2k_2 \mid 3 \quad \text{pour} \quad k_2 = -2, 0, 2$$

$$-3 + 2k_3 \mid 7 \quad \text{pour} \quad k_3 = -2, 2, 5$$

Ces solutions sont :

(-227, -432, 104), (-131, -248, 60), (-59, -110, 27), (5, 12, -4), (101, 196, -48), (173, 334, -81), (121, 234, -58), (217, 418, -102), (289, 556, -135), (259, -496, 120), (-163, -312, 76), (-91, -174, 43), (-27, -52, 12), (69, 132, -32), (141, 270, -65), (89, 170, -42), (185, 354, -86), (257, 492, -119), (-289,-556,135), (-193, -372, 91), (-121, -234, 58), (-57, -112, 27), (39, 72, -17), (111, 210,-50), (59, 110, -27), (155, 294, -71), (227, 432, -104).

Nous ne traiterons pas la résolution de $b|Ax$ car ceci est équivalent à $Ax \equiv 0 \pmod b$ (voir chapitre III).

VII.5 APPLICATIONS A L'OPTIMISATION EN NOMBRES ENTIERS

VII.5.1 Considérons PM1 : Max {fx | Ax ≥ b} où fx est une forme linéaire et où Ax ≥ b définit géométriquement un cône. Nous supposons que le sommet $\bar{x}$ est l'optimum de PM1.

Proposition VII.3 : L'optimum en entier de PM1 est un point fondamental de ce cône.

Preuve :

Puisque $\bar{x}$ est l'optimum de PM1 , nous avons les conditions d'optimalité de Kuhn et Tucker :

$$\exists\ u \geq 0,\ f = -uA.$$

Etant donné y, un point entier quelconque du cône, nous avons $y = \overset{i}{x} + \sum_{j=1}^{n} k_j B^j$ avec $\overset{i}{x}$, point fondamental.

$$f(y) = f(\overset{i}{x}) + \sum_{j=1}^{n} f(k_j B^j)$$

$$= f(\overset{i}{x}) + \sum_{j=1}^{n} k_j(-uAB^j)$$

$$= f(\overset{i}{x}) - u.\sum_{j=1}^{n} k_j AB^j.$$

$$AB^j = \varepsilon\delta^j \geq 0,\ k_j > 0 \Longrightarrow \sum_{j=1}^{n} k_j AB^j > 0.$$

Comme $u \geq 0 \Longrightarrow f(y) < f(\overset{i}{x})$. CQFD.

Dans le cas des cônes non réguliers la preuve est identique car $f(V^j) = -uAV^j = 0$.

VII.5.2 Considérons PM2 : Max {fx | c ≥ Ax ≥ b} où fx est une forme linéaire et où c ≥ Ax ≥ b définit géométriquement un parallélotope. Nous supposons que le sommet $\bar{x}$ par exemple est l'optimum de PM2.

Corollaire VII.2 : L'optimum en entier de PM2 est un point fondamental de parallélotope c'est-à-dire un point de P_f^* où P_f^* est associé au sommet $\bar{x}$.

La preuve se déduit aisément de la proposition précédente.

ANNEXES

ANNEXE 0

Nous trouvons en annexe A0 les différentes procédures qui serviront pour les programmes suivants. Ces procédures sont :

Procédure INF ;
Procédure PRODMAVEC ;
Procédure INFA 2 ;
Procédure HERMITE ;
Procédure SMITH ;

```
PROCEDURE INF (A,L1,N,JM) ;
    VALUE L1, N ; INTEGER L1, N, JM ; INTEGER ARRAY A ;
    COMMENT  cette procédure repère par JM la plus petite valeur absolue des termes non
             nuls de la ligne L1 du tableau A du L1ième terme au Nième. 8388607 est
             l'infini machine ;
    BEGIN INTEGER I, X, S ;
        S := 8388607 ;
        FOR I := L1 STEP 1 UNTIL N DO
            BEGIN X := ABS(A[L1,I]) ;
                IF X ≠ 0 AND X<S THEN
                    BEGIN JM := I ; S := X END
            END
    END de INF ;

PROCEDURE PRODMAVEC (A,B,C,S,R,M) ;
    VALUE S,R,M ; INTEGER S,R,M ; INTEGER ARRAY A,B,C ;
    COMMENT  cette procédure exécute le produit d'une matrice A à R-S+1 lignes par un
             vecteur B et met le résultat dans C ;
    BEGIN INTEGER I, K ;
        FOR I := S STEP 1 UNTIL R DO
            BEGIN C[I] := 0 ;
                FOR K := 1 STEP 1 UNTIL M DO
                C[I] := C[I] + A[I,K] * B[K]
            END
    END de PRODMAVEC ;
```

```
PROCEDURE LECTURE (A,B,M,N) ;
    VALUE M,N ; INTEGER M,N ; INTEGER ARRAY A,B ;
    COMMENT  procédure de lecture des données : la matrice A à M lignes et N colonnes
             et le vecteur B à M composantes ;
    BEGIN INTEGER I,J ;
        FOR I := 1 STEP 1 UNTIL M DO
            FOR J := 1 STEP 1 UNTIL N DO
            A[I,J] := DATA ;
        FOR I := 1 STEP 1 UNTIL M DO
            B[I] := DATA
    END de LECTURE ;

PROCEDURE INFA2 (T,L1,L2,L3,S,MI,MJ) ;
    VALUE L1, L2, L3 ; INTEGER L1, L2, L3, MI, MJ, S ;
    INTEGER ARRAY T ;
    COMMENT  cette procédure repère par (MI,MJ) la plus petite valeur absolue des termes
             non nuls du tableau T dont les lignes sont indicées de L1 à L2, les colonnes
             de L1 à L3 ;
    BEGIN INTEGER I,J,X ;
        S := 8388607 ;
        FOR I := L1 STEP 1 UNTIL L2 DO
            FOR J := L1 STEP 1 UNTIL L3 DO
                BEGIN X := ABS (T[I,J]) ;
                    IF X ≠ 0 AND X<S THEN
                        BEGIN MI := I ; MJ := J ; S := X END
                END
    END de INFA2 ;

PROCEDURE HERMITE (P,A,V,N,M) ;
    VALUE N,M ; INTEGER N,M ; INTEGER ARRAY P,A,V ;
    COMMENT  cette procédure calcule la réduite d'Hermite de la matrice A quelconque à
             M lignes et N colonnes ainsi que les matrices unimodulaires P et V qui
             permettent d'obtenir cette réduite, celle-ci étant dans A à la fin du calcul.
             PA=2 signifie qu'on calcule la réduite d'une matrice de rang maximum (en
             particulier d'une matrice unimodulaire) ayant plus de lignes que de colonnes,
             PA et RANG sont déclarés à l'extérieur de la procédure ;
    BEGIN INTEGER I,C,Y,Z,T,E1,H,J,Q,JM,K,R ;
        IF PA = 2 THEN GOTO SUITE ;
```

```
FOR I := 1 STEP 1 UNTIL M DO
     FOR J := 1 STEP 1 UNTIL M DO
     P[I,J] := IF I = J THEN 1 ELSE 0 ;
SUITE : FOR I := 1 STEP 1 UNTIL N DO
          FOR J := 1 STEP 1 UNTIL N DO
          V[I,J] := IF I = J THEN 1 ELSE 0 ;

FOR I := 1 STEP 1 UNTIL M DO
     BEGIN FOR C := I STEP 1 UNTIL N DO
          IF A[I,C] ≠ 0 THEN GOTO ETIQ ;

          IF PA = 2 THEN GOTO BOND ;
          IF I<M THEN Y := I ELSE GOTO FINALE ;
          FOR Y := Y+1 WHILE Y<=M DO
               BEGIN FOR Z := I STEP 1 UNTIL N DO
                    IF A[Y,Z] ≠ 0 THEN
                         BEGIN FOR T := 1 STEP 1 UNTIL N DO
                              BEGIN Q := A[Y,T]; A[Y,T]:=A[I,T]; A[I,T]:= Q END ;
                              FOR E1 := 1 STEP 1 UNTIL M DO
                                   BEGIN H := P[I,E1] ; P[I,E1] := P[Y,E1] :=H END;
                              GOTO ETIQ
                         END
               END ;
     BOND : GOTO FINALE ;
          ETIQ : INF (A,I,N,JM) ;
          IF PA = 2 THEN GOTO SAUT ;
          RANG := I ;
          SAUT : FOR J := I STEP 1 UNTIL N DO
             IF A[I,J] ≠ 0 AND J ≠ JM THEN
                  BEGIN Q := A[I,J] ÷ A[I,JM] ;
                       A[I,J] := A[I,J] - Q * A[I,JM] ;
                       FOR R := I+1 STEP 1 UNTIL M DO
                            A[R,J] := A[R,J] - Q * A[R,JM] ;
                       FOR E1 := 1 STEP 1 UNTIL N DO
                            V[E1,J] := V[E1,J] - Q * V[E1,JM]
                  END
          FOR E1 := I STEP 1 UNTIL N DO
             IF A[I,E1] ≠ 0 AND E1 ≠ JM THEN GOTO ETIQ ;
```

```
                IF I ≠ JM THEN FOR K := I STEP 1 UNTIL M DO
                   BEGIN Q := A[K,I] ; A[K,I] := A[K,JM] ; A[K,JM] := Q END ;
                FOR E1 := 1 STEP 1 UNTIL N DO
                   BEGIN H := V[E1,I] ; V[E1,I] := V[E1,JM] ; V[E1,JM] := H END ;
 FINALE : END
END de HERMITE ;


PROCEDURE SMITH (U,A,V,N,M) ;
   VALUE N, M ; INTEGER N, M ; INTEGER ARRAY U,A,V ;
   COMMENT  cette procédure calcule une forme normale de Smith de la matrice A
            quelconque à M lignes et N colonnes ainsi que les matrices unimodulaires
            U et V, la forme normale se trouve dans le tableau A à la fin du calcul ;
   BEGIN INTEGER E,F,I,MI,MJ,Q,R,T,R1,R2,B1,S,K,G,Q1,E2 ;
      FOR E := 1 STEP 1 UNTIL M DO
         FOR F := 1 STEP 1 UNTIL M DO
            U[E,F] := IF E = F THEN 1 ELSE 0 ;
      FOR E := 1 STEP 1 UNTIL N DO
         FOR F := 1 STEP 1 UNTIL N DO
            V[E,F] := IF E = F THEN 1 ELSE 0 ;
      FOR I := 1 STEP 1 UNTIL M DO
         BEGIN
            ETIQ : INFA2 (A,I,M,N,S,MI,MJ) ;
            IF S = 8388607 THEN GOTO FINALE ;
            FOR T := I STEP 1 UNTIL N DO
               IF A[MI,T] ≠ 0 AND T ≠ MJ THEN
                  BEGIN Q := A[MI,T] ÷ A[MI,MJ] ;
                     FOR R := I STEP 1 UNTIL M DO
                        A[R,T] := A[R,T] - Q * A[R,MJ] ;
                     FOR E2 := 1 STEP 1 UNTIL N DO
                        V[E2,T] := V[E2,T] - Q * V[E2,MJ]
                  END ;
            FOR R1 := I STEP 1 UNTIL M DO
               IF A[R1,MJ] ≠ 0 AND R1 ≠ MI THEN
                  BEGIN Q1 := A[R1,MJ] ÷ A[MI,MJ] ;
                     FOR R2 := I STEP 1 UNTIL N DO
                        A[R1,R2] := A[R1,R2] - Q1 * A[MI,R2] ;
                     FOR F := 1 STEP 1 UNTIL M DO
                        U[R1,F] := U[R1,F] - Q1 * U[MI,F]
                  END ;
```

```
            FOR B1 := I STEP 1 UNTIL M DO
                 IF A[B1,MJ] ≠ 0 AND B1 ≠ MI THEN GOTO ETIQ ;
            FOR B1 := I STEP 1 UNTIL N DO
                 IF A[MI,B1] ≠ 0 AND B1 ≠ MJ THEN GOTO ETIQ ;
            IF I ≠ MJ AND I<=N THEN
                 BEGIN FOR K := I STEP 1 UNTIL M DO
                      BEGIN G := A[K,I] ; A[K,I] := A[K,MJ] ;
                           A[K,MJ] := G
                      END ;
                      FOR F := 1 STEP 1 UNTIL N DO
                           BEGIN G := V[F,I] ; V[F,I] := V[F,MJ] ;
                                V[F,MJ] := G
                           END
                 END ;
            IF I ≠ MI THEN
                 BEGIN FOR K := I STEP 1 UNTIL N DO
                           BEGIN G := A[I,K] ; A[I,K] := A[MI,K] ;
                                A[MI,K] := G
                           END ;
                       FOR F := 1 STEP 1 UNTIL M DO
                           BEGIN G := U[I,F] ; U[I,F] := U[MI,F] ;
                                U[MI,F] := G
                           END
                 END ;
            RANG := I ;
   FINALE:END
END de SMITH ;
```

ANNEXES 1, 2, 3, 4

Les programmes qui suivent ont été écrits en ALGOL et passés sur M 40 B.G.E.

Ils sont au nombre de quatre .

Résolution de $Ax = b$ dans $\mathbb{Z}^n$ par :

1) la méthode de la réduite d'Hermite exposée en II.1 et utilisant les tests de la proposition II.1

2) la méthode précédente à laquelle on ajoute la triangularisation définie au corollaire II.3

3) la méthode de la forme normale de Smith exposée en II.2 et utilisant les tests de la proposition II.3

4) la méthode précédente à laquelle on ajoute la triangularisation définie au corollaire II.4.

Ces quatre programmes sont très performants, le plus rapide d'entre eux étant le premier.

```
BEGIN COMMENT Résolution de Ax = b dans ℤ par la méthode d'Hermite. A[1:M, 1:N] est une
        matrice de rang quelconque à éléments dans ℤ, b est dans BA [1:M], PA = 1
        signifiant que l'on utilise HERMITE complétement ;

    INTEGER N,M,PA,RANG,J1,R1,I1,Q1,A1,B1 ;
    N := DATA ;
    M := DATA ;
      BEGIN INTEGER ARRAY P[1:M,1:M], A[1:M,1:N], V[1:N,1:N], BA[1:M], X0[1:N] ;
          PA := 1 ;
          LECTURE (A, BA, M, N);
          HERMITE (P,A,V,N,M) ;
          BEGIN INTEGER ARRAY BB[1:M] ;
(α)             PRODMAVEC (P,BA,BB,1,RANG,M) ;
                BEGIN INTEGER ARRAY X1[1:RANG] ;
                    FOR I1 := 1 STEP 1 UNTIL RANG DO
                      BEGIN X1[I1] := BB[I1] ;
                        FOR J1 := 1 STEP 1 UNTIL I1-1 DO
                            X1[I1] := X1[I1] - A[I1,J1]* X1[J1] ;
                        A1 := X1[I1] ; B1 := A[I1,I1] ;
                        Q1 := A1 ÷ B1 ; R1 := A1 - B1 * Q1 ;
                        IF R1 ≠ 0 THEN GOTO TEST 1 ;
                        X1[I1] := Q1 ;
                      END
                    TEXT ("PREMIER TEST VRAI /) ; PRINT (2) ;
                    COMMENT Nous venons de tester si y_R = L^-1 P_R b (page II.8) qui
                    se trouve dans le tableau X1 est entier ;
                    IF RANG < M THEN
                      BEGIN INTEGER ARRAY X2 [RANG+1 : M] ;
                        PRODMAVEC (A,X1,X2,RANG +1,M,RANG) ;
                        PRODMAVEC (P,BA,BB,RANG +1, M,M) ;
                        FOR I1 := RANG +1 STEP 1 UNTIL M DO
                            IF BB[I1] ≠ X2[I1] THEN GOTO TEST 2 ;
                        TEXT ("DEUXIEME TEST VRAI /) ; PRINT (2) ;
                      END ;
                    COMMENT Le deuxième test consiste à vérifier si P_R̄ b=SL^-1 P_R b ;
(β)                 PRODMAVEC (V,X1,X0,1,N,RANG) ;
                    SORTIE DES RESULTATS (la solution particulière est dans le
                    tableau X0, la solution générale s'obtient en ajoutant à X0 les
                    combinaisons linéaires à coefficients dans ℤ des colonnes numé-
```

```
                    rotées de RANG +1 à N du tableau V) ;
                    GOTO FINALE ;
                    TEST 1 : TEXT ("PAS DE SOLUTIONS, TEST 1 /); PRINT (2) ;
                    TEST 2 : TEXT ("PAS DE SOLUTIONS, TEST 2 /); PRINT (2) ;
                END ;
            END ;
  FINALE: END
END
```

```
BEGIN COMMENT Résolution de Ax=b dans ℤ par la méthode d'Hermite donnant à la matrice
              solution la forme triangulaire inférieure. La réduite d'Hermite étant
              utilisée deux fois : une fois pour A (PA = 1), une autre fois pour V^R̄
              (PA = 2) ;
      INTEGER N,M,PA,RANG,I,J,Q,R,J1,I1,R1,Q1,A1,B1 ;
      N := DATA ;
      M := DATA ;
          BEGIN INTEGER ARRAY P[1:M,1:M], A[1:M,1:N]; V[1:N,1:N], BA[1:M], X0[1:N] ;
                PA := 1 ;
                LECTURE (A,BA,M,N) ;
                HERMITE (P,A,V,N,M) ;
                BEGIN INTEGER ARRAY BB[1:M],
                  insérer ici la partie du programme A1 comprise entre les lignes (α) et
                     (β) incluses ;
                     PA := 2 ;
                     IF RANG = N THEN SORTIE DE LA SOLUTION se trouvant dans le tableau X0 ;
                     GOTO FINALE ;
                     BEGIN INTEGER ARRAY VR[1:N, 1:N-RANG], VP[1:N-RANG, 1:N-RANG] ;
                          FOR I := 1 STEP 1 UNTIL N DO
                             FOR J := 1 STEP 1 UNTIL N - RANG DO
                             VR[I,J] := V[I,J+RANG] ;
                          HERMITE (P,VR,VP,N-RANG,N) ;
                          COMMENT on vient de calculer la réduite d'Hermite de V^R̄ primiti-
                                  vement mise dans le tableau VR ;
                          SORTIE DES RESULTATS (la solution particulière est dans le tableau
                          X0, la solution générale s'obtient en ajoutant à X0 les combinai-
                          sons linéaires à coefficients dans ℤ des colonnes de RANG +1 à N
                          du tableau VR) ;
                     END ;
                     GOTO FINALE ;
                     TEST 1 : TEXT ("PAS DE SOLUTIONS, TEST 1 /) ; PRINT (2) ;
                     TEST 2 : TEXT ("PAS DE SOLUTIONS, TEST 2 /) ; PRINT (2) ;
                END ;
      FINALE : END
          END
END
```

```
BEGIN COMMENT  Résolution de Ax=b dans ℤ par la méthode de Smith. A[1:M,1:N] est un
               tableau de rang quelconque, b est dans BA[1:M] ;
     INTEGER N,M,RANG,E4,F4,Q2,R2,I,J ;
     N := DATA ;
     M := DATA ;
        BEGIN INTEGER ARRAY U[1:M,1:M], A[1:M,1:N], V[1:N,1:N], BA[1:M], X0[1:N] ;
            LECTURE (A,BA,M,N) ;
            SMITH (U,A,V,N,M) ;
            BEGIN INTEGER ARRAY BB[1:RANG] ;
(α)             PRODMAVEC (U,BA,BB,1,RANG,M) ;
                FOR F4 := 1 STEP 1 UNTIL RANG DO
                    BEGIN Q2 := BB[F4] ÷ A[F4,F4] ;
                          R2 := BB[F4] - Q2 * A[F4,F4] ;
                          IF R2 ≠ 0 THEN GOTO TEST 1 ;
                          BB[F4] := Q2 ;
                    END ;
                TEXT ("PREMIER TEST VRAI /) ; PRINT (2) ;
              COMMENT  nous venons de vérifier si (D_R^R)^-1 U_R b est entier, ce vecteur
                       se trouve alors dans le tableau BB ;
                IF RANG < M THEN
                    BEGIN INTEGER ARRAY X2[RANG +1 : M] ;
                          PRODMAVEC (U,BA,X2,RANG+1,M,M) ;
                          FOR F4 := RANG +1 STEP 1 UNTIL M DO
                              IF X2[F4] ≠ 0 THEN GOTO TEST 2 ;
                          TEXT ("DEUXIEME TEST VRAI /) ; PRINT (2) ;
                    END ;
(β)             PRODMAVEC (V,BB,X0,1,N,RANG) ;
                SORTIE DES RESULTATS (idem qu'en A1) ;
                GOTO TERMINAL ;
                TEST 1 : TEXT ("PAS DE SOLUTIONS, TEST 1 /) ; PRINT (2) ;
                TEST 2 : TEXT ("PAS DE SOLUTIONS, TEST 2 /) ; PRINT (2) ;
            END ;
 TERMINAL:END
END
```

```
BEGIN COMMENT  Résolution de Ax=b dans ℤ par la méthode de Smith donnant à la matrice
               solution générale (tableau VR) la forme triangulaire inférieure ;
     INTEGER N,M,RANG,E4,F4,Q2,R2,I,J,PA ;
     N := DATA ;
     M := DATA ;
     BEGIN INTEGER ARRAY U[1:M,1:M], A[1:M,1:N], V[1:N,1:N], BA[1:M], X0[1:N] ;
          LECTURE (A,BA,M,N) ;
          SMITH (U,AV,N,M) ;
          BEGIN INTEGER ARRAY BB[1:M] ;
               insérer ici la partie du programme A3 de la ligne (α') à (β') incluses ;
               PA := 2 ;
               IF RANG = N THEN SORTIE DE LA SOLUTION se trouvant dans le tableau XO ;
               GOTO ALAFIN ;
               BEGIN INTEGER ARRAY VR[1:N,1:N-RANG], VP[1:N-RANG, 1:N-RANG] ;
                    FOR E4 := 1 STEP 1 UNTIL N DO
                         FOR F4:=1 STEP 1 UNTIL N-RANG DO
                              VR[E4,F4] := V[E4,F4+RANG] ;
                         HERMITE (V,VR,VP,N-RANG,N) ;
                         SORTIE DES RESULTATS (idem qu'en A2) ;
               END ;
               GOTO ALAFIN ;
               TEST 1 : TEXT ("PAS DE SOLUTIONS, TEST 1 /) ; PRINT (2) ;
               TEST 2 : TEXT ("PAS DE SOLUTIONS, TEST 2 /) ; PRINT (2) ;
          END ;
ALAFIN:END
END
```

ANNEXE 5

```
BEGIN COMMENT Ce programme calcule le p.g.c.d. de N entiers rationnels et l'exprime comme
        combinaison linéaire de ces N entiers (identité de Bezout) ;
    INTEGER N, J, JP ;
    PROCEDURE INFA (T,L) ;
    VALUE L ; INTEGER L ; INTEGER ARRAY T ;
    COMMENT cette procédure repère par JM la plus petite valeur absolue des termes non
        nuls.
        BEGIN INTEGER I, X, S ;
            S := 8388607 ;
            FOR I := 1 STEP 1 UNTIL    DO
                BEGIN X := ABS (T[I]) ;
                IF X ≠ 0 AND X < S THEN
                    BEGIN JP := I ; S := X END
                END
        END de INFA ;
    PROCEDURE HERM (A,V,N) ;
    VALUE N ; INTEGER N ; INTEGER ARRAY A, V ;
    COMMENT Cette procédure calcule la réduite d'Hermite d'une matrice à une seule ligne
        de N éléments. L'élément non nul de la réduite est en position JP. Les coef-
        ficients de Bezout sont dans la colonne JP de la matrice V ;
    BEGIN INTEGER I, J, Q ;
        FOR I := 1 STEP 1 UNTIL N DO
        FOR J := 1 STEP 1 UNTIL N DO
        V[I,J] := IF I = J THEN 1 ELSE 0 ;
        ETIQ : INFA (A,N) ;
        FOR I := 1 STEP 1 UNTIL N DO
        IF A[I] ≠ 0 AND I ≠ JP THEN
            BEGIN Q := A[I] ÷ A[JP] ;
                A[I] := A[I] - Q * A[JP] ;
                FOR J := 1 STEP 1 UNTIL N DO
                V[J,I] := V[J,I] - Q * V[J,JP]
            END ;
        FOR J := 1 STEP 1 UNTIL N DO
        IF A[J] ≠ 0 AND J ≠ JP THEN GOTO ETIQ ;
    END de HERM ;

    N := DATA ;
    BEGIN INTEGER ARRAY A[1:N], V[1:N, 1:N] ;
        FOR J := 1 STEP 1 UNTIL N DO A[J] := DATA ;
        TEXT ("LES ? N = /) ; EDIT ("F3.0/,N) ; TEXT (" ? ENTIERS ? SONT : /) ;
```

```
    PRINT (2) ;
    FOR J := 1 STEP 1 UNTIL N DO EDIT ("F 8.0/, A[J]) ;
    PRINT (2) ;
    HERM (A,V,N) ;
    TEXT ("LE ? PGCD ? EST : /) ; EDIT ("F8.0 /, A[JP]) ;
    PRINT (2) ;
    TEXT ("LES ? COEFFICIENTS ? DU ? PGCD ? DANS ? L'IDENTITE ? DE ? BEZOUT ? SONT :) ;
    PRINT (2) ;
    FOR J := 1 STEP 1 UNTIL N DO EDIT ("F8.0/, V[J,JP]) ;
    PRINT (2) ;
END
```

ANNEXE 6

Le programme proposé est commun aux cônes V.1 et V.2. Il génère d'abord les vecteurs B^j appelés "vecteur de translation", puis les points fondamentaux en indiquant leur nombre et si on se trouve dans le cas V.2, les vecteurs de translation $V^{\bar{R}}$ appelés "vecteur de translation bis".

```
EGIN COMMENT  ce programme génère les points fondamentaux et les vecteurs de translation
              d'un cône polyédrique défini par Ax≥b où A[1:M,1:N] est à coefficients
              entiers et b dans B[1:M,1:2] à coefficients rationnels, NPOINTS est le
              nombre de points fondamentaux ;
  INTEGER N,M,I,J,PM,K,PG, NPOINTS,LJ,L,RANG,I2,F2,S ;
  PROCEDURE PGCD (T,PG) ;
       INTEGER PG ; INTEGER ARRAY T
       COMMENT  cette procédure calcule le pgcd (PG) de deux nombres, elle fait appel
                à la procédure INFA2 ;
       BEGIN INTEGER I,MJ,Q,S ;
            SAUT : INFA2(T,1,1,2,S,1,MJ) ;
            FOR I := 1 STEP 1 UNTIL 2 DO
                 IF T[1,I] ≠ 0 AND I ≠ MJ THEN
                      BEGIN Q := T[1,I] ÷ T[1,MJ] ;
                            T[1,I] := T[1,I] - Q * T[1,MJ]
                      END ;
            FOR I := 1 STEP 1 UNTIL 2 DO
                 IF T[1,I] ≠ 0 AND I ≠MJ THEN GOTO SAUT ;
            PG := T[1,MJ]
       END de PGCD ;

  PROCEDURE PPCM (EPS,PM,N) ;
       VALUE N ; INTEGER PM,N ; INTEGER ARRAY EPS ;
       COMMENT  la procédure calcule le ppcm (PM) de n nombres en faisant appel à la
                procédure PGCD ;
       BEGIN INTEGER I,PG ;
            INTEGER ARRAY TA[1:N], TB[1:1, 1:2] ;
            TA[1] := EPS[1] ;
            FOR I := 1 STEP 1 UNTIL N-1 DO
                 BEGIN TB[1,1] := TA[I] ;
                       TB[1,2] := EPS[I+1] ;
                       PGCD (TB,PG) ;
                       TA[I+1] := EPS[I+1]* TA[I] ÷ PG
                 END ;
            PM := TA[N]
       END de PPCM ;
```

```
PROCEDURE REAJUST (AA,M,B,PM) ;
     VALUE M,PM ; INTEGER M, PM ; INTEGER ARRAY AA, B ;
     COMMENT  cette procédure donne les ai admissibles (ai≥b) à partir de a = VY ;
          BEGIN INTEGER I,C ;
               FOR I := 1 STEP 1 UNTIL M DO
                    BEGIN C := (B[I,1]-B[I,2]*AA[I]) ÷ (PM * B[I,2]) ;
                         IF B[I,1] > AA[I] * B[I,2] AND
                            B[I,1]-AA[I]*B[I,2]- C * PM * B[I,2] ≠ 0
                            THEN C := C+1 ;
                         AA[I] := AA[I] + C * PM
                    END
          END de REAJUST ;

PROCEDURE SORTIE (A,AA,BB,N,M) ;
     VALUE N,M ; INTEGER M,N ; INTEGER ARRAY A,AA,BB ;
     COMMENT  cette procédure sort les points fondamentaux ;
     BEGIN INTEGER I, J ;
          FOR I := 1 STEP 1 UNTIL N DO
               BEGIN BB[I] := 0 ;
                     FOR J := 1 STEP 1 UNTIL M DO
                     BB[I] := BB[I] + A[J,I] * AA[J]
               END ;
          BEGIN PRINT (1) ; TEXT ("X[/) ; EDIT ("F3.0/,LJ) ;  TEXT ("]=/) ;
               FOR I := 1 STEP 1 UNTIL N DO
                    EDIT ("F8.0/, BB[I] ÷ PM) ; PRINT (2)
          END ;
          LJ := LJ+1 ;
     END de SORTIE ;


N := DATA ;
M := DATA ;
BEGIN INTEGER ARRAY A, TRAN[1:M,1:N], U[1:M,1:M], V[1:N,1:N],Y,AA,EPS[1:N],
                    LU[1:1, 1:2], BB[1:N], B[1:M,1:2] ;
     FOR I := 1 STEP 1 UNTIL M DO
          FOR J := 1 STEP 1 UNTIL N DO A[I,J] := DATA ;
     FOR I := 1 STEP 1 UNTIL M DO
          BEGIN B[I,1] := DATA ; B[I,2] := DATA END ;
     SMITH (U,A,V,N,M) ;
```

```
FOR I := 1 STEP 1 UNTIL M DO EPS[I] := ABS(A[I,I]) ;
PPCM (EPS,PM,M) ; COMMENT Calcul de ε = [ε1,ε2,...,εn] mis dans PM ;
FOR I := 1 STEP  1 UNTIL M DO
     BEGIN EPS[I] := PM ÷ A[I,I] ;
          FOR J := 1 STEP 1 UNTIL M DO
               U[I,J] := U[I,J] * EPS[I]
     END ;
     COMMENT  Calcul de C mise dans le tableau U ;

FOR I := 1 STEP 1 UNTIL N DO
     FOR K := 1 STEP 1 UNTIL M DO
          BEGIN A[K,I] := 0 ;
               FOR J := 1 STEP 1 UNTIL M DO
                    A[K,I] := A[K,I] + V[I,J] * U[J,K] ;
                    TRAN [K,I] := A[K,I]
          END ;
TEXT ("LES VECTEURS DE TRANSLATION : /) ; PRINT (2) ;
FOR J:=1 STEP 1 UNTIL M DO
     BEGIN PRINT (1) ; TEXT ("B[/) ; EDIT ("F2.0/,J) ; TEXT ("]=/) ;
          FOR I := 1 STEP 1 UNTIL N DO
               EDIT ("F8.0/,TRAN [J,I]) ; PRINT (2)
     END ;

FOR I:=1 STEP 1 UNTIL M DO
     FOR J:=1 STEP 1 UNTIL M DO A[I,J] := U[I,J] ;
SMITH (U,A,V,M,M) ;

BEGIN BOOLEAN ARRAY TB[1:M, 0:PM-1] ;
     FOR J:=1 STEP 1 UNTIL M DO
          BEGIN FOR I:=0 STEP 1 UNTIL PM-1 DO
               TB[J,I] := A[J,J] * I = A[J,J] * I ÷ PM * PM ;
               LU[1,1] := ABS (A[J,J]) ;
               LU[1,2] := PM ;
               PGCD (LU,PG) ;
               EPS[J] := PG
          END ;
      NPOINTS := 1 ;
     FOR J:=1 STEP 1 UNTIL M DO
          NPOINTS :=  NPOINTS * EPS[J] ;
```

```
SORTIE DE N POINTS ;
FOR I:=1 STEP 1 UNTIL M DO
    Y[I] := 0 ;
PRODMAVEC (V,Y,AA,1,M,M) ;
REAJUST (AA,M,B,PM) ;
LJ := 1 ;
SORTIE (TRAN,AA,BB,N,M) ;
FOR L:=M, L-1 WHILE L>=1 DO
     BEGIN RETOUR : FOR I := Y[L]+1 STEP 1 UNTIL PM-1 DO
                         IF TB[L,I] THEN
                               BEGIN Y[L]:= I ;
                                     PRODMAVEC (V,Y,AA,1,M,M) ;
                                     COMMENT Calcul de a=VY (mod ε) ;
                                     REAJUST (AA,M,B,PM) ;
                                     COMMENT Calcul de a_i≥b ;
                                     SORTIE (TRAN,AA,BB,N,M) ;
                                     L := M ;
                                     GOTO RETOUR
                               END ;
                    FOR K:=L STEP 1 UNTIL M DO Y[K] := 0
     END ;
IF M < N THEN
     BEGIN TEXT ("LES VECTEURS DE TRANSLATION BIS : /) ; PRINT(2) ;
          FOR J := M+1 STEP 1 UNTIL N DO
               BEGIN PRINT (1) ;
                     FOR I:=1 STEP 1 UNTIL N DO
                          EDIT("F8.0/,V[I,J]) ; PRINT (2)
               END
     END
END
END
END
```

REFERENCES et BIBLIOGRAPHIE

[1] BALINSKI M.L. *An Algorithm for finding all vertices of convex sets,* J.S.I.A.M., 9 (1961) 1, pp. 72-88.

[2] BALINSKI M.L., K. SPIELBERG *Methods for Integer Programming : Algebraic, Combinatorial, and Enumerative.* Progress in Operations Research, vol. III, J.S.Aronofsky Editors,John Wiley and Sons, Inc. N.Y. (1969). (On trouvera à la fin de ce tour d'horizon une bibliographie très complète d'articles et d'ouvrages d'avant Mars 1968).

[3] BENDERS J.F. *Partitioning Procedures for Solving Mixed-Variables programming problems.* Numerische Mathematik, Vol. 4, (1962), pp. 238-252.

[4] BERTIER P., B. ROY *Une procédure de Résolution pour une classe de problèmes pouvant avoir un caractère combinatoire.* I.C.C. Bull, vol. 4, (1965) pp. 19-28.

[5] BLANKINSHIP W.A. *A New Version of the Euclidean Algorithm.* Am. Math. Monthly 70, (1963).

[6] BOURBAKI N. *Algèbre - chapitre 3 - Algèbre Multilinéaire - chapitre 7 - Modules sur les anneaux principaux.* Hermann, Paris, (1964).

[7] BOREVITCH Z.I., I.R. CHATAREVITCH *Théorie des Nombres.* Gauthier-Villars - Paris (1967).

[8] BRADLEY G.H. *Equivalent Integer Programs and Canonical Problems.* Technical Report 26, Yale University, August 1969.

[9] BRADLEY G.H. *Transformation of integer programs to knapsack problems.* 38th Nat. Meeting of the ORSA., Detroit, october 1970.

[10] CHATELET A. *Les groupes Abéliens finis et les modules de points entiers.* Gauthier-Villars (1925).

[11] DIKSON L.E. *History of the Number Theory.* Vol. II Diophantine Analysis. Chelsea Publishing Company N.Y. (1952).

[12] Mac DUFFEE C.C. *The theory of matrices.* Chelsea Publishing Company N.Y. (1956).

[13] FIOROT J.Ch. *Génération des points entiers d'un cône polyédrique.* Comptes-Rendus à l'Académie des Sciences de Paris, Sér. A, t.269 (28 juillet 1969) pp. 215-217.

[14] FIOROT J.Ch. *Algorithme de génération des points entiers d'un cône polyédrique.* Bulletin de la Direction des Etudes et Recherches de l'E.D.F., série C, 1, 1970, pp; 5-28.

[15] FIOROT J.Ch. *Génération des points entiers d'un parallélotope de* R^n. Comptes-Rendus à l'Académie des Sciences de Paris, Sér. A, t.270 (9 février 1970) pp. 395-398.

[16] FIOROT J.Ch. *Generation of all integer points for given sets of Linear Inequalities.* 7^{th} Mathematical Programming Symposium, La Haye (sept. 1970).

[17] FIOROT J.Ch., M. GONDRAN *Résolution des systèmes linéaires en nombres entiers.* Bulletin de la Direction des Etudes et Recherches de l'E.D.F., série C, 2 (1969) pp. 65-126.

[18] FREHEL J. *Une méthode de troncature pour la programmation en nombres entiers.* Rapport I.B.M. France n° FFL0072 février 1969.

[19] GOMORY R.E. *An Algorithm for integer solutions to Linear Programs* dans Recent Advances in Mathematical Programming, Graves R.L., P. Wolfe Editors, Mac Graw-Hill Book Company, Inc. (1963)

[20] GOMORY R.E. *All Integer Programming Algorithm* dans Industrial Scheduling, Math J.F.,G.L. Thompson, Editors, Prentice - Hall, N.Y., 1963.

[21] GOMORY R.E. *Some Polyhedra Related to Combinatorial Problems.*
Linear Algebra and its Applications. Vol. 2, (1969) pp. 451-558.

[22] GONDRAN M. *Programmation linéaire en nombres entiers, Optimisation dans un cône.*
Revue Française d'Informatique et de Recherche opérationnelle. R2, Juillet-Août 1970, pp. 10-27.

[23] GUIGNARD M. *Une condition d'optimalité en programmation en nombres entiers.*
Rapport du Laboratoire de Calcul de la Faculté des Sciences de Lille n° 22, juin 1970.

[24] GUIGNARD M., K. SPIELBERG *The State Enumeration Method for Mixed zero-one programming.*
7^{th} Mathematical Programming Symposium, La Haye (sept. 1970).

[25] HARDY G.H., E.M. WRIGHT *An Introduction to the Number theory.*
Oxford, Charendon Press, 1954.

[26] HU T.C. *Integer programming and Network flows.*
Addison - Wesley Publisching Company (1969).

[27] HUARD P. *Programmes Mathématiques non Linéaires à variables bivalentes.*
Bulletin des Etudes et Recherches de l'E.D.F. série C, n°2 (1968) pp. 37-46.

[28] LAND A.H., A.G. DOIG *An Automatic Method of Solving Discrete Programming Problems.*
Econometrica, Vol. 28, (1960) pp. 497-520.

[29] LEKKERKERKER C.G. *Geometry of Numbers.*
Series Bibliotheca Mathematica, Vol. 8. Walters noordhoff publishing . Groningen (1969).

[30] SAATY T.L. *Optimisation in integers and Related extremal Problems.*
Mac Graw - Hill Book Company (1970).

[31] SAUNDERS M., R. SCHINZINGER *The Shrinking boundary algorithm for Discrete System Models,*
I.E.E.E. Transactions on Systems Science and Cybernetics, Vol. 6, n°2, April 1970.

[32] WITZGALL C. *An All Integer Programming Algorithm with Parabolic Constraints.*
J.S.I.A.M., Vol. 11, 1963, pp. 855-871