BULLETIN DE LA S. M. F.

DANIEL LAZARD

Algèbre linéaire sur $K[X_1, \ldots, X_n]$ et élimination

Bulletin de la S. M. F., tome 105 (1977), p. 165-190

<http://www.numdam.org/item?id=BSMF_1977__105__165_0>

Bull. Soc math. France,
105, 1977, p. 165-190.

ALGÈBRE LINÉAIRE SUR $K[X_1, \ldots, X_n]$ ET ÉLIMINATION

PAR

Daniel LAZARD
[Université de Poitiers]

RÉSUMÉ. — Cet article étudie la résolution des systèmes d'équations linéaires à coefficients et inconnues polynômes avec pour objectif d'améliorer les algorithmes définis par G. HERMANN. Les premiers paragraphes sont consacrés à l'étude des complexes de Koszul généralisés. Les résultats obtenus sont ensuite utilisés pour introduire plusieurs algorithmes de résolution qui améliorent beaucoup ceux de HERMANN. Un contre-exemple montre que, pour deux variables, les résultats obtenus sont les meilleurs possibles. Divers algorithmes auxiliaires sont introduits, notamment pour le calcul de la dimension d'une variété ou la descente des solutions dans le cas des corps finis. Les méthodes homologiques du début conduisent également à une généralisation du théorème principal de la théorie du résultant de n polynômes à n variables.

Jusqu'au début de ce siècle, les géomètres algébristes se préoccupaient beaucoup de la possibilité d'appliquer leurs théories sur des exemples explicites. Il s'est avéré à cette époque que les calculs étaient trop longs pour être effectivement menés à bien et que l'affinement de la théorie nécessitait de puissantes méthodes abstraites qui ne s'accompagnaient pas automatiquement des méthodes de calcul effectif correspondantes. Aujourd'hui, où ces méthodes abstraites sont bien au point, quelques mathématiciens se préoccupent à nouveau de déterminer quels calculs peuvent être effectués en un nombre fini d'opérations; le travail de SEIDENBERG [SEI] est l'article de référence sur ce sujet. Bizarrement, alors que les moyens pratiques de calcul ont considérablement évolué avec l'apparition des gros ordinateurs, presque rien n'a été fait pour rendre opérationnelles les méthodes connues pour être effectives, c'est-à-dire pour écrire des algorithmes suffisamment rapides pour pouvoir être programmés.

L'intérêt de tels algorithmes pour tester des conjectures ou trouver des contre-exemples peut sembler évident, mais leur absence fait que nombre de géomètres doutent que les ordinateurs puissent leur apporter de l'aide dans leur recherche, ignorent quels problèmes sont susceptibles d'une telle aide, et, voudraient-ils utiliser ces machines, qu'ils ne disposent pas des bibliothèques d'algorithmes nécessaires.

C'est pour essayer de remédier à cette absence que je me suis attaqué au problème de la résolution des systèmes d'équations linéaires à coefficients et inconnues polynômes à plusieurs indéterminées. Ce problème est essentiel, car de nombreux autres s'y ramènent. La possibilité de résoudre effectivement de tels systèmes était connue depuis longtemps [HER], mais les algorithmes connus étaient tellement mauvais qu'il n'était pas question de les utiliser. Dans le cas d'une équation linéaire à coefficients de degré 2 sur $K[X, Y, Z]$, la méthode de Hermann se ramène à la résolution d'un système linéaire à plus de 10^5 inconnues sur K.

La méthode employée ici est analogue à celle de HERMANN, en ce sens que la majoration des degrés en certaines des indéterminées des solutions cherchées permet, par récurrence, de se ramener à un système d'équations linéaires sur le corps de base. Pour obtenir ces majorations, j'ai été amené à développer des techniques fines de calcul dans les idéaux déterminantiels ([LAZ 1], [LAZ 2]) qui ont finalement pu être évitées. L'obtention de ces majorations s'est avérée être liée à la théorie du résultant de n polynômes à n variables ([MAC], [VdW]), et amène comme sous-produit une démonstration homologique simple du plus difficile des théorèmes principaux de cette théorie. L'efficacité des résultats obtenus apparaît quand on remarque que l'équation sur $K[X_1, X_2, X_3]$ citée plus haut se ramène maintenant à un système à 84 inconnues sur K. Cependant, la longueur des calculs croît très vite avec le nombre d'indéterminées, et ils sont encore impraticables pour plus de 4 indéterminées.

Certains des résultats de cet article ont été annoncés dans divers colloques ([LAZ 3], [LAZ 4] et [LAZ 5]).

1. Cohomologie et résultant

Soit K un corps; posons $A_n = K[X_1, \ldots, X_n]$, que l'on munit de la graduation du degré total. Par *module gradué libre*, il faut entendre un module gradué possédant une base formée d'éléments homogènes.

Considérons un homomorphisme homogène de degré zéro de modules gradués libres de type fini $f : E \to F$; soient $e_1, \ldots, e_s$ une base graduée de E (e_i est homogène de degré d_i), et $f_1, \ldots, f_t$ une base graduée de F (f_j est homogène de degré δ_j). On peut écrire $f(e_i) = \sum_j a_{j,i} f_j$, et $a_{j,i}$ est donc un polynôme homogène de degré $d_i - \delta_j$. Supposons $s \geqslant t$, et considérons le déterminant des colonnes $i(1), \ldots, i(t)$ de la matrice des $a_{j,i}$; un calcul facile montre que ce déterminant est un polynôme homogène de degré $\sum_{k=1}^{t} d_{i(k)} - \sum_{j=1}^{t} \delta_j$. L'idéal *déterminantiel* de f qui

est l'idéal engendré par tous ces déterminants est donc un idéal homogène, ce qu'on va retrouver par une autre méthode.

Dans [B. E.], on trouve la définition des deux complexes suivants :

$$G(f) \quad : \quad 0 \to S_{s-t-1}(F^*) \otimes \Lambda^s(E) \xrightarrow{d_f} S_{s-t-2}(F^*) \otimes \Lambda^{s-1}(E)$$
$$\xrightarrow{d_f} \ldots \xrightarrow{d_f} S_0(F^*) \otimes \Lambda^{t+1}(E) \xrightarrow{\varepsilon} E \xrightarrow{f} F$$

$$EN(f) : \quad 0 \to S_{s-t}(F^*) \otimes \Lambda^s(E) \xrightarrow{d_f} S_{s-t-1}(F^*) \otimes \Lambda^{s-1}(E)$$
$$\xrightarrow{d_f} \ldots S_0(F^*) \otimes \Lambda^t(E) \xrightarrow{\Lambda^t(f)} \Lambda^t(F)$$

dans lesquels

$$d_f((y_1^* \ldots y_k^*) \otimes (x_1 \wedge \ldots \wedge x_l)) = \sum_{j=1}^{k} \sum_{i=1}^{l} (-1)^{i+1}$$
$$y_j^*(f(x_i))(y_1^* \ldots \widehat{y_j^*} \ldots y_k^*) \otimes (x_1 \wedge \ldots \wedge \hat{x}_i \wedge \ldots \wedge x_l)$$

et

$$\varepsilon(x_1 \wedge \ldots \wedge x_{t+1}) = \sum_{i=1}^{t+1} (-1)^{i+1} (f(x_1) \wedge \ldots \wedge \widehat{f(x_i)} \wedge \ldots \wedge f(x_{t+1})).x_i,$$

en identifiant $S_0(F^*)$ et $\Lambda^t(F)$ avec A_n. Il est immédiat que, si l'on munit tous les modules qui apparaissent dans ces complexes de leur graduation canonique, les morphismes d_f sont tous homogènes de degré 0, et que l'image de $\Lambda^t(f)$ est l'idéal déterminantiel, que l'on retrouve ainsi être homogène; le morphisme ε est au contraire de degré $-\sum_1^t \delta_i$.

Les complexes sont numérotés de droite à gauche, le premier module apparaissant à droite portant l'indice 0. L'objet de ce paragraphe est de montrer que, si l'idéal déterminantiel a pour racine l'idéal maximal homogène, les groupes d'homologie des deux complexes ci-dessus sont nuls à partir d'une certaine borne *effectivement calculée* en fonction des d_i et des δ_j. Pour simplifier les notations, nous ferons toujours les conventions (non restrictives) suivantes sur les degrés

$$\text{(C)} \qquad d_1 \geqslant d_2 \geqslant \ldots \geqslant d_s, \quad \delta = \inf \delta_i \qquad \text{et} \qquad \Delta = \sum_{i=1}^{t} \delta_i.$$

LEMME 1. — *Supposons que f soit défini sur A_1, et que la convention* (C) *soit satisfaite. Si l'idéal déterminantiel de f est non nul, on a*

(i) $H_0(G)$ *est nul en degré* $\geqslant d_1$;

(ii) $H_1(G)$ *est nul en degré* $\geqslant d_1 + \ldots + d_{t+1} - \Delta$;

(iii) $H_i(G)$ *est nul en degré* $\geqslant d_1 + \ldots + d_{t+i} - (i-1)\delta$ *pour* $1 \leqslant i \leqslant s-t$;

(iv) $H_{s-t+1}(G) = H_{s-t+1}(EN) = 0$;

(v) $H_i(EN)$ *est nul en degré* $\geqslant d_1 + \ldots + d_{t+i} - i\delta$ *pour* $0 \leqslant i \leqslant s-t$.

Soient $C_.$ un des deux complexes considérés et $C'_. = C_. \otimes_{A_1} A_1[X_1^{-1}]$. Cette extension des scalaires rend inversible un élément de l'idéal déterminantiel, et $C'_.$ est donc exact ([B. E.], prop. 2.3). En considérant le diagramme

$$\begin{array}{ccccc} C_{i+1} & \xrightarrow{d} & C_i & \xrightarrow{d} & C_{i-1} \\ \downarrow & & \downarrow & & \downarrow \\ C'_{i+1} & \xrightarrow{d'} & C'_i & \xrightarrow{d'} & C'_{i-1} \end{array}$$

il apparaît clairement que, pour tout élément homogène x de $\ker(d)$, il existe $k \in \mathbf{Z}$ et $y \in C_{i+1}$ tels que $x = X_1^k d(y)$. Si on désigne par $g_.$ les éléments de la base canonique de C_{i+1}, on obtient donc :

$$x = X_1^k \sum_. X_1^{l_.} a_. d(g_.) \qquad \text{avec} \quad a_. \in K.$$

Si le degré de x est supérieur ou égal au plus grand des degrés des $g_.$, on a $k + l_. \geqslant 0$ et donc $x \in \operatorname{im}(d)$. Il reste à calculer la borne supérieure des degrés des $g_.$, ce qui est facile et donne les formules du lemme 1, compte tenu du fait que ε est de degré $-\Delta$; l'assertion (iv) est immédiate.

THÉORÈME 1. — *Considérons les complexes associés à un morphisme $f : E \to F$ de A_n-modules gradués libres vérifiant la convention* (C). *Si la hauteur de l'idéal déterminantiel I de f est n, on a*

(i) $H_i(EN) = H_i(G) = 0$ *pour* $i > s - t - n + 2$;

(ii) $H_i(G)$ *est nul en degré*

$$\geqslant d_1 + d_2 + \ldots + d_{t+n+i-1} - (i+n-2)\delta - n + 1 - \eta\Delta$$

si $(n, i) \neq (1, 0)$, *et en posant* $\eta = 0$ *quand* $i > 1$ *et* $\eta = 1$ *sinon;*

(iii) $H_i(G)$ *est nul en degré* $\geqslant d_1 + d_2 + \ldots + d_{t+n+i-1} - (i+n-1)\delta - n + 1$.

Sauf pour $H_0(G)$, on retrouve les formules du lemme 1, en substituant 1 à n. La démonstration va donc se faire par récurrence sur n.

Soit I l'idéal déterminantiel; il n'est contenu dans aucun idéal premier p de hauteur $< n$; il en résulte que, pour un tel p, l'homomorphisme $f \otimes A_p$ est surjectif, et la tensorisation par A_p rend exacts les complexes considérés ([B. E.], prop. 2.3). Il en résulte que les $H_i \otimes A_p$ sont tous nuls, et que le support de H_i est réduit à l'idéal maximal homogène $m = (X_1, \ldots, X_n)$ (*cf.* [BOU], chap. 3, § 3, prop. 1). Il en résulte qu'il existe k tel que $m^k H_i = 0$, et, comme H_i est de type fini, que H_i est nul en degré assez grand.

Précisons maintenant ce « assez grand ». En désignant par $C_.$ un des complexes considérés, considérons la suite exacte de complexes

$$0 \to C_. \xrightarrow{X_n} C_. \to \overline{C}_. \to 0 \quad \text{ou} \quad \overline{C}_. = C_./X_n C_..$$

Comme I contient une puissance de l'idéal maximal homogène, il en est de même de $\overline{I} = I/X_n I$, et le complexe de A_{n-1}-modules $\overline{C}_\cdot$ vérifie les hypothèses de la proposition. La suite exacte d'homologie s'écrit :

$$H_{i+1}(\overline{C}_\cdot) \xrightarrow{\delta} H_i(C_\cdot) \xrightarrow{X_n} H_i(C_\cdot),$$

ou encore :

$$H_{i+1}(\overline{C}_\cdot)^{k+1} \xrightarrow{\delta} H_i(C_\cdot)^k \xrightarrow{X_n} H_i(C)^{k+1},$$

en se restreignant aux composantes homogènes de degré $k+1$. Si $H_{i+1}(\overline{C}_\cdot)^k = 0$ pour $k \geqslant D$, et $H_i(C_\cdot)^k = 0$ pour les grandes valeurs de k, une récurrence descendante sur k montre que $H_i(C_\cdot)^k = 0$ pour $k \geqslant D-1$, ce qui montre (i) en prenant $D = -\infty$, et ramène la démonstration de (ii) et (iii) au calcul simple de $D-1$ en fonction de i et de n.

Remarque. — Lorsque $t = 1$, les deux complexes considérés s'identifient avec le complexe de Koszul, et ne diffèrent que par les degrés des éléments de base. Si $F = A_n$, ce qui équivaut à $\delta = \delta_1 = 0$, cette différence disparaît à son tour. On obtient comme cas particulier le résultat suivant :

COROLLAIRE. — *Soient $f_1, \ldots, f_k$ des polynômes homogènes de $A_n = K[X_1, \ldots, X_n]$ engendrant un idéal I; soit d_i le degré de f_i; supposons que $d_1 \geqslant d_2 \geqslant \ldots \geqslant d_k \geqslant 1$, et que $k \geqslant n$. Les conditions suivantes sont équivalentes.*

(i) *Les k hypersurfaces projectives définies par les f_i n'ont de point commun sur aucune extension algébrique de K;*

(ii) *l'idéal I contient une puissance de l'idéal maximal homogène m de A_n;*

(iii) $I \supset m^D$ *avec* $D = d_1 + d_2 + \ldots + d_n - n + 1$;

(iv) *l'application $\Phi : (g_1, \ldots, g_k) \to \sum f_i g_i$, à valeur dans les polynômes homogènes de degré $D = d_1 + \ldots + d_n - n + 1$, est surjective quand, pour tout i, g_i parcourt les polynômes homogènes de degré $D - d_i$.*

La seule partie non immédiate est l'implication (ii) ⇒ (iii) qui résulte immédiatement du théorème 1. Ce résultat, qui ne semble pas avoir été énoncé auparavant pour $k > n$, est fondamental pour la théorie du résultant et en est l'un des résultats les plus difficiles dans les expositions classiques ([MAC], [VdW]). L'assertion (iv) est essentielle pour les calculs explicites, car sa vérification se ramène au problème bien résolu, de savoir si une application K-linéaire est surjective.

2. Semi-graduations

Le théorème 1 est satisfaisant quand la hauteur de l'idéal déterminantiel est égale à n. Quand cette égalité n'est pas vérifiée, il faut faire intervenir les autres graduations de A_n pour avoir des renseignements sur les groupes d'homologie. Malheureusement l'application considérée n'est pas homogène pour ces graduations et, pour les manier, il faut donc introduire un outil supplémentaire.

DÉFINITION 1. — *Une* semi-graduation *sur un anneau A (resp. un A-module M) est une filtration croissante et exhaustive par des sous-groupes abéliens $A^{\leqslant d}$ (resp. $M^{\leqslant d}$) tels que*

$$A^{\leqslant d}.A^{\leqslant d'} \subset A^{\leqslant d+d'} \quad (\textit{resp. } A^{\leqslant d}.M^{\leqslant d'} \subset M^{\leqslant d+d'}).$$

Une application semi-homogène *entre deux modules semi-gradués est une application linéaire $f : M \to N$ telle que $f(M^{\leqslant d}) \subset N^{\leqslant d}$ pour tout d.*

Si A est gradué par des sous-groupes A_i, on définit une semi-graduation par $A^{\leqslant d} = \bigoplus_{i \leqslant d} A_i$. C'est cette semi-graduation que l'on utilise quand on a affaire à un polynôme de « degré $\leqslant d$ ». Nous laissons au lecteur le soin de développer les sorites sur les semi-graduations images directes, images réciproques, induites sur un sous-module, quotient, etc.

Si $C_\cdot$ est un des deux complexes définis plus haut, pour tout i, C_i est libre et possède une base $\{ e_\cdot \}$ canoniquement déduite des bases choisies pour E et F. Si on munit les $e_\cdot$ de leur degré pour la graduation du degré global, toute graduation de A_n induit une graduation de C_i. Si $Y_1, \ldots, Y_n$ sont des polynômes homogènes du premier degré de A_n, linéairement indépendants sur K, désignons par $\mathscr{G}_k^Y$ la graduation sur A_n « degré en $Y_1, \ldots, Y_k$ de P considéré comme polynôme en $Y_1, \ldots, Y_n$ ». Il est immédiat que les différentielles de EN et de G sont semi-homogènes pour $\mathscr{G}_k^Y$ et les groupes d'homologie de ces complexes sont donc semi-gradués pour $\mathscr{G}_k^Y$.

Le but de cette section est de montrer que ces groupes d'homologie sont engendrés par les éléments qui sont de bas degré pour certaines de ces semi-graduations $\mathscr{G}_k^Y$.

LEMME 2. — *Soit I un idéal gradué de A_n, de hauteur $r \leqslant n$. Si $r = n$ ou si K est infini, il existe n polynômes linéaires et homogènes K-linéairement indépendants $Y_1, \ldots, Y_n$ qui vérifient la condition suivante :*

(D) *La hauteur de $1 + \sum_{i>r} A_n Y_i$ est exactement n.*

Seul le cas $r < n$ n'est pas tout à fait trivial. La variété projective définie par I est de dimension $n-r-1$; si K est infini, il existe donc une variété

linéaire de dimension $r-1$ qui ne la rencontre pas dans l'espace projectif de dimension $n-1$. Il suffit de choisir un repère projectif tel que cette variété y ait pour équations $Y_{r+1} = \ldots = Y_n = 0$.

THÉORÈME 2. — *Considérons un homomorphisme homogène de A_n-modules gradués libres $f : E \to F$, vérifiant la condition* (C)*; supposons que son idéal déterminantiel I soit de hauteur r non nulle et qu'il existe n polynômes linéaires, homogènes, K-linéairement indépendants $Y_1, \ldots, Y_n$ et vérifiant la condition* (D). *Désignons par $C_.$ un des complexes $G(f)$ ou $EN(f)$.*

(i) *$H_i(C_.)$ est nul pour $i \geqslant s-t-r+2$;*

(ii) *Les éléments de $H_i(C_.)$ sont images d'éléments de C_i qui, pour tout $k \leqslant r$, sont de degré $\leqslant D_{i,k}(C)$ pour la semi-graduation $\mathscr{G}_k^Y$, avec*

$$D_{i,k}(EN) = d_1 + \ldots + d_{t+i+k-1} - (i+k-1)\delta - k,$$

$$D_{0,1}(G) = d_1 - 1,$$

$$D_{i,k}(G) = d_1 + \ldots + d_{t+i+k-1} - (i+k-2)\delta - k \qquad \textit{pour} \quad i > 1,$$

$$D_{i,k}(G) = d_1 + \ldots + d_{t+i+k-1} - \Delta - (i+k-2)\delta - k$$

$$\textit{pour} \quad (i,k) \neq (0,1) \qquad \textit{et} \qquad i \leqslant 1.$$

L'assertion (i) est déjà connue [B. E.], et se retrouve aisément par récurrence sur n à partir du cas $r = n$ déjà démontré (th. 1) : considérons la suite exacte de complexes

$$0 \to C_. \xrightarrow{Y_n} C_. \to \overline{C}_. \to 0,$$

où $\overline{C}_. = C_. \otimes A_n/(Y_n)$ est le complexe associé à $\overline{f} = f \otimes A_n/(Y_n)$; la condition (D) implique immédiatement la condition (D) pour l'idéal déterminantiel $\overline{I} = I/Y_n I$ de $\overline{f}$. Il en résulte que $ht(\overline{I}) = r$, et par hypothèse de récurrence que $H_i(C_.) = 0$ pour $i \geqslant s-t-r+2$. La suite exacte de cohomologie entraîne donc $H_i(C) = Y_n H_i(C)$, et, comme $H_i(C)$ est gradué de type fini, $H_i(C) = 0$.

Pour démontrer (ii), commençons par nous fixer k. Comme $H_i(C)$ est de type fini, il est engendré par des éléments homogènes pour le degré global $\mathscr{G}_n$, et dont le degré en $\mathscr{G}_k^Y$ est $\leqslant d'$, pour d' assez grand. Montrons que, si $d' > D_{i,k}(C)$, on peut abaisser d' d'une unité. Soit donc y un élément de $H_i(C)$ homogène de degré d pour $\mathscr{G}_n$, et de degré $\leqslant d'$ pour $\mathscr{G}_k^Y$. Il provient d'un élément x de $Z_i \subset C_i$ qui vérifie les mêmes conditions de degré. Désignons par $\overline{x}$ la partie homogène de degré d' pour $\mathscr{G}_k^Y$ de x; cela a un sens car C_i est gradué pour cette graduation. Comme C_i est libre,

$x = \sum \bar{x}_Z . Z$, où Z parcourt les monômes de degré $d-d'$ en $Y_{k+1}, \ldots, Y_n$, et où $\bar{x}_Z \in C_i \otimes A_n/(Y_{k+1}, \ldots, Y_n)$ pour tout i. Posons

$$\bar{C}_\cdot = C_\cdot \otimes A_n/(Y_{k+1}, \ldots, Y_n),$$

et désignons par $\bar{Z}_i$ le module des cycles de $\bar{C}_i$. Comme $x \in Z_i$, on voit facilement que $\bar{x}_Z$ appartient à $\bar{Z}_i$ pour tout Z. Le théorème 1 permet alors d'affirmer que $\bar{x}_Z = \sum_{\cdot} \bar{a}_{Z,\cdot} d(\bar{e}_\cdot)$ si $d' > D_{i,k}(C)$; ici $\bar{a}_{Z,\cdot} \in K[Y_1, \ldots, Y_k]$, on désigne par d (resp. $\bar{d}$) la différentielle de C_i (resp. $\bar{C}_i$), et par $e_\cdot$ (resp. $\bar{e}_\cdot$) les éléments de la base canonique de C_{i-1} (resp. $\bar{C}_{i-1}$); en effet, la condition (D) implique clairement que $ht(\bar{I}) = k$.

Posons $x' = x - \sum_{Z,\cdot} Z \bar{a}_{Z,\cdot} d(e_\cdot)$. Il est clair que x et x' ont même image dans $H_i(C)$ et que x' est homogène pour le degré global $\mathscr{G}_n$ et de degré $< d'$ pour $\mathscr{G}_k^Y$, ce qui montre le théorème pour chaque valeur de k prise séparément. Mais la transformation que l'on a fait subir à x n'augmente pas son degré pour $\mathscr{G}_l^Y$ si $l > k$. On peut donc effectuer cette transformation successivement pour $r, r-1, \ldots, 1$ pour obtenir le théorème.

COROLLAIRE 1. — *La condition* (D) *est inutile pour vérifier l'assertion* (i).

Il suffit de prendre une extension infinie L de K : si $H_i \otimes_K L = 0$ en degré D, il en est de même pour H_i, par descente fidèlement plate.

COROLLAIRE 2. — *Avec les notations du théorème, supposons que* $r = n-1$.

(i) *Même si la condition* (D) *n'est pas vérifiée,* $H_i(C_\cdot)$ *est engendré par ses éléments de degré global* $\leqslant D_{i,r}(C)$;

(ii) *Si la condition* (D) *est vérifiée,* $H_i(C_\cdot)$ *est engendré par les images d'éléments de* C_i *qui vérifient la condition* (ii) *du théorème* 3 *et sont en outre de degré global* $\leqslant D_{i,r}(C)$.

Si la condition (D) est vérifiée, l'assertion (ii) du théorème 3 implique que les générateurs trouvés pour $H_i(C)$ sont images d'éléments de C_i de la forme $X_n^k z$ où z vérifie toutes les conditions de degré voulues et est en outre de degré global $\leqslant D_{i,r}(C_\cdot)$. Comme C_{i-1} est sans torsion, $z \in Z_i$, ce qui montre l'assertion (ii).

Si K est infini, l'assertion (D) peut être toujours vérifiée, ce qui montre (i) dans ce cas. Si K est fini, le résultat s'en déduit par descente fidèlement plate à partir d'une extension infinie de K.

3. Hauteur 1

Le cas où l'idéal déterminantiel est de hauteur 1, nécessite un traitement particulier : en le divisant par son P.G.C.D., on obtient un idéal de

hauteur $\geqslant 2$, et cela va nous permettre de majorer les degrés de $\ker f$ par rapport à deux variables simultanément.

Considérons donc un homomorphisme $f : E \to F$ de A_n-modules gradués libres de dimensions s et t dont l'idéal déterminantiel I est de la forme $I = a\,J$ avec $ht\,(J) \geqslant 2$. Tous les éléments de la matrice de l'application $\varepsilon : \Lambda^{t+1}(E) \to E$ définie au paragraphe 1 appartiennent à I, et on a donc $\varepsilon = a\,\varepsilon'$. Ce morphisme ε' est homogène de degré $-\deg(a) \sum \delta_i$. Puisque F est libre, $f \circ \varepsilon' = 0$; posons $H'_1 = \ker f/\mathrm{Im}\,\varepsilon'$.

THÉORÈME 3. — *Avec les notations précédentes, si α est le degré global de a, on a*

(i) *Si $s = t+1$, $H'_1 = 0$;*

(ii) *Si $n = 2$, H'_1 est nul en degré $\geqslant d_1 + \ldots + d_{t+2} - \delta - 1 - \alpha - \Delta$;*

(iii) *Si $n = 3$, H'_1 est engendré par ses éléments de degré global $\leqslant d_1 + \ldots + d_{t+2} - \delta - 2 - \alpha - \Delta$;*

(iv) *S'il existe n polynômes linéaires homogènes K-linéairement indépendants $Y_1, \ldots, Y_n$ tels que J vérifie la condition* (D), *le module H'_1 est engendré par les images d'éléments de E qui sont à la fois de degré*

$$\leqslant d_1 + \ldots + d_{t+2} - \delta - 2 - \alpha - \Delta$$

en Y_1, Y_2, et de degré $\leqslant d_1 + \ldots + d_{t+1} - 1 - \alpha - \Delta$ en Y_1.

Si $s = t+1$, le module $\ker f$ est de rang 1; il contient

$$\frac{1}{a}\varepsilon(e_1 \wedge \ldots \wedge e_{t+1}) = (z_1, \ldots, z_s),$$

les z_i étant premiers entre eux. Si $(z'_1, \ldots, z'_s) \in \ker f$, il existe donc λ et $\mu \in A_n$ tels que

$$\lambda(z_1, \ldots, z_s) = \mu(z'_1, \ldots, z'_s).$$

Comme les z_i sont premiers entre eux, μ divise λ, et on peut donc supposer $\lambda = 1$, ce qui montre que $(z'_1, \ldots, z'_s) \in \mathrm{im}\,(\varepsilon/a)$.

Le reste de la démonstration est entièrement analogue à celle des théorèmes 1 et 2; il faut cependant modifier le complexe intervenant dans le lemme 1 et prendre, dans le cas d'une indéterminée, le complexe

$$F^* \otimes \Lambda^{t+2}(E) \xrightarrow{d_f} \Lambda^{t+1}(E) \xrightarrow{X^{-\alpha}\varepsilon} E \xrightarrow{f} F$$

dont la différentielle $X^{-\alpha}\varepsilon$ est de degré $-\alpha - \Delta$. Pour démontrer (ii), il faut également s'assurer que $I/X_2\,I \neq 0$, c'est-à-dire $ht\,(I + AX_1) = 2$, ce qui revient à supposer la condition (D) vérifiée pour I. Si K est infini,

on peut toujours s'y ramener par changement d'indéterminées; si K est fini, on déduit le résultat du cas infini par descente fidèlement plate.

L'assertion (iii) se démontre exactement comme le corollaire 2 du théorème 2.

4. Équations linéaires sans second membre

Il s'agit d'appliquer les résultats précédents sur $H_1(G)$ et H'_1 pour obtenir une méthode de résolution de tels systèmes. Un tel système est une famille $\sum_j a_{i,j} z_j = 0$ $(i = 1, \ldots, t)$, où les $a_{i,j}$ sont des éléments donnés de A_n, et les z_j des inconnues; sa résolution revient à chercher les éléments $(z_1, \ldots, z_s) \in A_n^s$ qui vérifient ces t équations, c'est-à-dire à chercher un système de générateurs du noyau de l'application linéaire de matrice $(a_{i,j})$. S'il existe des entiers $d_1, \ldots, d_s$; $\delta_1, \ldots, \delta_t$ tels que $a_{i,j}$ soit homogène de degré $d_j - \delta_i$, le système sera dit *homogène*. Sa matrice est alors clairement la matrice d'une application linéaire et homogène de modules gradués libres $f : E = \bigoplus A\, e_j \to F = \bigoplus A\, f_i$ avec degré $(e_j) = d_j$, degré $(f_i) = \delta_i$. Les résultats précédents pourront alors être directement appliqués pour calculer le module des solutions, qui s'identifie à $\ker f$.

Voici la méthode de résolution proposée.

4.1. Élimination des équations superflues.

Soit r le rang de la matrice des $a_{i,j}$, et supposons que le déterminant des r premières lignes et des r premières colonnes soit différent de zéro. La théorie classique de Cramer indique que, pour tout $i > r$, la i-ième équation est combinaison linéaire à coefficients dans le corps des fractions Q de A_n des r premières. Comme A_n est intègre, il en résulte que toute solution des r premières équations est solution du système. On peut donc supposer que le rang de la matrice $(a_{i,j})$ est égal à $t \leqslant s$.

4.2. Homogénéisation

Pour tout i et tout j, soit $e_{i,j}$ le degré de $a_{i,j}$; choisissons des entiers $d_1, \ldots, d_s$; $\delta_1, \ldots, \delta_t$ tels que $e_{i,j} \leqslant d_j - \delta_i$. Pour tout polynôme $P(X_1, \ldots, X_n) \in A_n$, posons

$$\tilde{P}^d(X_1, \ldots, X_n) = X_{n+1}^d P\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right)$$

qui appartient à A_{n+1} pour d assez grand; pour tout polynôme $Q \in A_{n+1}$, désignons par $\overline{Q}$ le polynôme obtenu en substituant 1 à X_{n+1}. Le système défini par les $\tilde{a}_{i,j}^{d_j - \delta_i}$ est homogène, et ses solutions sont en relation étroite avec les solutions du système des $a_{i,j}$. Pour simplifier, nous poserons $\tilde{a}_{i,j} = \tilde{a}_{i,j}^{d_j - \delta_i}$.

PROPOSITION 1 :

(i) *Pour que* $z_1, \ldots, z_s$ *soit une solution du système dont la matrice est* $(\tilde{a}_{i,j})$, *il faut et il suffit que* $\bar{z}_1, \ldots, \bar{z}_s$ *soit une solution du système dont la matrice est* $(a_{i,j})$.

(ii) *Si* $S_1, \ldots, S_k$ *est un système de générateurs du module des solutions de* $(\tilde{a}_{i,j})$, *alors* $\bar{S}_1, \ldots, \bar{S}_k$ *est un système de générateurs du module des solutions de* $(a_{i,j})$.

Il suffit de faire la vérification. La réciproque de (ii) est fausse : il suffit de remplacer $S_1, \ldots, S_k$ par $X_{n+1} S_1, \ldots, X_{n+1} S_k$ pour s'en convaincre.

Il est clair que, si la suite des d_j et des δ_i est mal choisie, cela introduit un facteur parasite X_{n+1}^k dans l'idéal déterminantiel de $\tilde{a}_{i,j}$. Par ailleurs, pour certaines matrices, telle $\begin{pmatrix} X+1 & X \\ X & X+1 \end{pmatrix}$, un facteur X_{n+1}^k est inévitable. Il serait donc intéressant de déterminer quelle est la « meilleure » suite $d_1, \ldots, d_s$; $\delta_1, \ldots, \delta_t$.

PROPOSITION 2. — *Avec les notations ci-dessus, il existe une suite* $d_1, \ldots, d_s$; $\delta_1, \ldots, \delta_t$ *telle que*

(*a*) $d_j - \delta_i \geqslant e_{i,j}$ *pour tout* i *et tout* j;

(*b*) *pour tout* i, *il existe* j *tel que* $d_j - \delta_i = e_{i,j}$;

(*c*) *pour tout* j, *il existe* i *tel que* $d_j - \delta_i = e_{i,j}$.

Il suffit de prendre $d_j = \sup_i (e_{i,j})$ et $\delta_i = \inf_j (d_j - e_{i,j})$; il est clair que $\delta_i \geqslant 0$ pour tout i; si $d_j = e_{i,j}$, il en résulte que $d_j - \delta_i = e_{i,j}$, ce qui montre (*c*); le reste est immédiat.

La suite $d_1, \ldots, d_s$; $\delta_1, \ldots, \delta_t$ ainsi déterminée n'est pas unique en général : si la matrice des $e_{i,j}$ est $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, on peut prendre pour $(d_1, d_2; \delta_1, \delta_2)$ aussi bien $(1, 0; 0, 0)$ que $(1, 1; 0, 1)$. Il serait intéressant de savoir choisir la suite des degrés d_j et δ_i de manière à minimiser le facteur X_{n+1}^k parasite dans l'idéal déterminantiel. Je ne sais le faire que pour les matrices carrées.

PROPOSITION 3. — *Soit* $(e_{i,j})$ *une matrice carrée d'entiers* $(1 \leqslant i, j \leqslant t)$. *Il existe des entiers* $d_1, \ldots, d_t$; $\delta_1, \ldots, \delta_t$ *tels que*

(*a*) $e_{i,j} \leqslant d_j - \delta_i$ *pour tout* i *et tout* j;

(*b*) $\sum_{j=1}^t d_j - \sum_{i=1}^t \delta_i = \sup \sum_{i=1}^t e_{i,\sigma(i)}$, *la borne supérieure étant prise sur toutes les permutations de* $\{1, \ldots, t\}$.

Remarque. — Les conditions (*a*) et (*b*) entraînent les conditions (*b*) et (*c*) de la proposition 2.

Par permutation des lignes de la matrice, on peut supposer que $\sum_{i=1}^{t} e_{i,i} = \sup_\sigma \sum_{i=1}^{t} e_{i,\sigma(i)}$: il s'agit alors de résoudre le système d'inéquations

$$\begin{cases} d_j - \delta_i \geqslant e_{i,j}, \\ d_i - \delta_i = e_{i,i}. \end{cases}$$

Posons $c_{i,j} = e_{i,j} - e_{i,i}$, et éliminons les δ_i : on obtient

$$-c_{j,i} \geqslant d_j - d_i \geqslant c_{i,j};$$

si ce système possède une solution, on en trouve une pour le système initial en prenant $\delta_i = d_i - e_{i,i}$. En éliminant successivement les d_i, une récurrence facile montre que la condition nécessaire et suffisante pour qu'un tel système possède une solution est que l'on ait

$$c_{i_1,i_2} + c_{i_2,i_3} + \ldots + c_{i_{k-1},i_k} + c_{i_k,i_1} \leqslant 0$$

pour toute suite de k entiers distincts, $i_1, \ldots, i_k$. Comme les $c_{i,i}$ sont nuls, cette condition est équivalente à $\sum_\sigma c_{i,\sigma(i)} \leqslant 0$ pour toute permutation de $\{1, \ldots, t\}$: il suffit en effet de décomposer σ en cycles. Ces conditions sont équivalentes à la condition imposée $\sum_{i=1}^{t} e_{i,i} = \sup_\sigma \sum_{i=1}^{t} e_{i,\sigma(i)}$.

4.3. Détermination de $ht(I)$

A partir demaintenant, on considère un système homogène sur A_n. Pour appliquer le plus efficacement possible les théorèmes 1 à 3, il est nécessaire de connaître $ht(I)$, une variété linéaire projective maximale ne rencontrant pas la variété définie par I, et, si $ht(I) = 1$, le P.G.C.D. de I. Ces calculs sont très longs, surtout s'il y a plus d'une équation. Nous donnons au paragraphe 7 des algorithmes pour mener à bien ces calculs. Ces algorithmes peuvent certainement être beaucoup améliorés, d'autant plus qu'ils ne tiennent pas compte de la structure d'idéal déterminantiel de I.

En fait, il suffit de connaître un minorant r de $ht(I)$, et des polynômes linéaires homogènes K-linéairement indépendant $Y_1, \ldots, Y_n$ tels que l'image de I dans $A_n/(Y_{r+1}, \ldots, Y_n)$ soit de hauteur r. Plus la valeur de r obtenue sera élevée, plus la suite de la résolution sera rapide. Nous verrons que l'on peut même se passer de la recherche d'un tel r et d'un tel changement de variable, mais le système d'équations K-linéaires à résoudre sera très gros.

Il faut également noter que, si K est fini, il peut être nécessaire de le remplacer par une extension pour pouvoir faire les changements de variables nécessaires. Il y aura donc lieu, après résolution, de redescendre le système de générateurs obtenus (cf. § 8 ci-dessous).

4.4. Réduction du nombre d'indéterminées

Les théorèmes 2 et 3 affirment que $H_1(G)$ (resp. H'_1) est engendré par ses éléments de degré en $Y_1, \ldots, Y_k$ inférieur ou égal à une certaine borne D_k pour tout $k \leqslant r$ (resp. $k \leqslant 2$). Plus précisément si E (resp. F) désigne le A_n-module gradué libre de base $e_1, \ldots, e_s$ (resp. $f_1, \ldots, f_t$) tel que, pour tout j (resp. i), e_j (resp. f_i) est homogène de degré d_j (resp. δ_i), et si f désigne l'application linéaire de matrice $(a_{i,j})$, le module des solutions du système homogène considéré est $\ker f$. Or le théorème 2 (resp. th. 3) affirme que ce module est somme, d'une part, de l'image de ε (resp. ε'), dont il est facile de calculer des générateurs et, d'autre part, d'éléments qui vérifient les conditions de degré considérées. Il s'agit donc de calculer ces éléments.

Les monômes en $Y_1, \ldots, Y_r$ forment une base de A_n sur

$$A_{n-r} = K[Y_{r+1}, \ldots, Y_n].$$

Les éléments de E qui vérifient les conditions de degré considérées forment un A_{n-r}-module libre ayant pour base les $Z e_i$ où $i = 1, \ldots, s$, et Z parcourt les monômes en $Y_1, \ldots, Y_r$ dont, pour tout $k \leqslant r$, le degré en $Y_1, \ldots, Y_k$ est $\leqslant D_{1,k}(G) - d_i$ (resp. dont le degré en Y_1, Y_2 est $\leqslant D_{1,2}(G) - d_i - \alpha$ et le degré en Y_1 est $\leqslant D_{1,1}(G) - d_i - \alpha$). Les images de ces éléments appartiennent au sous-A_{n-r}-module de F ayant pour base les $Z f_j$ où Z parcourt les monômes en $Y_1, \ldots, Y_r$ dont, pour tout $k \leqslant r$, le degré en $Y_1, \ldots, Y_k$ est $\leqslant D_{1,k}(G) - \delta_j$ (resp. $\leqslant D_{1,k}(G) - \delta_j - \alpha$).

La recherche d'un système de générateurs des solutions du système d'équations initial se ramène donc à la recherche du noyau de la restriction de f aux deux A_{n-r}-modules libres ci-dessus.

En itérant cette méthode, on est ramené à la résolution d'un système d'équations linéaires sur K. Il faut noter que le système obtenu à chaque pas de l'itération est homogène et que les degrés des coefficients de sa matrice sont majorés par les degrés des coefficients de la matrice homogène initiale.

5. Majorations absolues

Soit $\sum_{j=1}^{s} a_{i,j} z_j = 0$ pour $i = 1, \ldots, t$ un système d'équations linéaires sur $A_n = K[X_1, \ldots, X_n]$; posons $d = \sup$ (degré $(a_{i,j})$), que nous supposerons généralement > 0, $\delta_i = \inf_j$ (d − degré $a_{i,j}$) et $\Delta = \sum \delta_i$. En prenant $d_j = d$ pour tout j, ces données définissent une homogénéisation de la matrice des $a_{i,j}$, et permettent d'appliquer la méthode du paragraphe précédent afin d'obtenir des bornes, dépendant de n, t, d, et éventuellement de δ et des δ_i, telles que le module des solutions soit engendré par celles

des solutions dont le degré de z_i est inférieur à ces bornes, pour tout i. Pour $n \leqslant 4$, nous allons donner des bornes précises; pour les plus grandes valeurs de n, nous nous contenterons d'en donner le comportement asymptotique en d et t.

5.1. $n = 1$

DÉFINITION 2. — *Nous appellerons* solutions de Cramer (*resp.* solutions de Cramer réduites) *l'image par* ε (*resp.* ε') *de la base canonique de* $\Lambda^{t+1}(A_n^s)$ *dans* A_n^s.

PROPOSITION 4. — *Si A est un anneau principal quelconque et* $\sum a_{i,j} z_j = 0$ *un système de t équations linéaires à coefficients dans A, linéairement indépendantes, le module des solutions est engendré par les solutions de Cramer réduites.*

En particulier, si $A = A_1 = K[X]$, *le module des solutions est engendré par les solutions telles que* degré $(z_i) \leqslant dt - \Delta$ *pour tout i, que ces équations soient indépendantes ou non.*

Soit $f : A^s \to A^t$ l'application linéaire définie par les $a_{i,j}$. Comme im (f) est libre, $A^s = \ker(f) \oplus \operatorname{im}(f)$. Il existe une base de im (f) et une base de A^t telles que la matrice de l'injection im $(f) \subset A^t$ soit diagonale. En prolongeant la base de im (f) en une base de A^s, on obtient des bases où la matrice de f est de la forme $(D\ 0)$, où D est une matrice carrée diagonale inversible. Il est clair que $a = \det(D)$ est le P.G.C.D. des déterminants $t \times t$ extraits de la matrice des $a_{i,j}$ et que la suite $\Lambda^{t+1}(A^s) \xrightarrow{(1/a)/\varepsilon} A^s \to A^t$ est exacte, ce qui démontre la première assertion.

La deuxième se démontre en calculant les degrés des déterminants $t \times t$ qui interviennent, et en remarquant que la quantité $dt - \Delta$ qui intervient ne peut que décroître quand on supprime les équations superflues.

5.2. $n = 2$

PROPOSITION 5. — *Si* $n = 2$, *le module des solutions du système considéré est engendré par les solutions telles que*

$$\text{degré } (z_i) \leqslant (t+1)d - \alpha - \Delta - \inf(2, d)$$

C'est une conséquence immédiate du théorème 3 (iii), compte tenu que la borne ne peut que diminuer quand on supprime des équations; le « inf » intervient pour que la borne soit supérieure au degré des solutions de Cramer lorsque $d < 2$.

5.3. $n = 3$

LEMME 3. — *La recherche des solutions du système considéré, telles que* degré$_{X_1}(z_i) \leqslant td-1-\Delta$ *pour tout* i *conduit à un système sur* A_{n-1} *de* $(t+1)(dt-\Delta)$ *équations dont les coefficients sont de degré* $\leqslant d$ *et pour lequel la valeur de* Δ *est*

$$\geqslant \frac{1}{2}td(d+1)+\Delta\left(dt-\frac{1}{2}\right)-\Delta^2-\frac{1}{2}\sum\delta_i^2.$$

Le degré de $\sum a_{i,j}z_j$ est $\leqslant td+d-1-\Delta-\delta_i$ et le nombre d'équations à considérer est donc $\sum_i[(t+1)d-\Delta-\delta_i] = (t+1)(dt-\Delta)$.

Le coefficient de X_1^k dans $\sum a_{i,j}z_j$ est de la forme $\sum_{j,l}a_{i,j}^l z_j^{k-l}$ où $a_{i,j}^l$ et z_j^{k-l} désignent le coefficient en X_1^l (resp. X_1^{k-l}) de $a_{i,j}$ (resp. z_j). On a degré $(a_{i,j}^l) \leqslant d-\delta_i-l \leqslant d-\delta_i$; comme $k-l \leqslant td-1-\Delta$, on a aussi

$$d-\delta_i-l \leqslant td-1-\Delta-\delta_i+d-k; \qquad \text{si} \quad m = td+d-1-\Delta-\delta_i-k,$$

il en résulte que $d-\delta_i-l \leqslant m$; ainsi la nouvelle valeur de Δ est minorée par

$$\sum_i\sum_{k=0}^{d-\delta_i}\sup(d-m,\delta_i) = \frac{1}{2}td(d+1)+\Delta\left(td-\Delta-\frac{1}{2}\right)-\frac{1}{2}\Sigma\delta_i^2.$$

PROPOSITION 6. — *Si* $n = 3$, *le module des solutions du système considéré est engendré par les solutions telles que, pour tout* i, *on ait* degré $(z_i) \leqslant \sup(d, B)$, *avec*

$$B = (td-\Delta)^2+\frac{1}{2}\sum_i(d-\delta_i)^2+\frac{1}{2}(td-\Delta)+d-3.$$

Si $\Delta = 0$, *on a*

$$B = t^2d^2+\frac{1}{2}td^2+\frac{1}{2}td+d-3.$$

Si $d = 0$, les coefficients sont dans K, les solutions de Cramer, de degré 0, engendrent le module des solutions et $B = -3$, ce qui montre la proposition dans ce cas.

On peut, par descente fidèlement plate supposer K infini. La suppression d'équations diminuant B, on peut supposer les équations indépendantes. On peut même supposer que les parties de degré d des équations pour lesquelles $\delta_i = 0$ sont indépendantes : sinon on peut abaisser le degré de l'une d'elles en lui ajoutant une combinaison linéaire des autres, ce qui augmente un des δ_i et diminue B. Ceci servira pour le cas $d = 1$.

Le théorème 2 appliqué avec $r = 1$ permet d'affirmer que le module des solutions est engendré par les solutions de Cramer et les solutions telles que le degré de z_i en Y_1 soit toujours inférieur ou égal à $td-\Delta-1$. Cela conduit (lemme 3) à un nouveau système de $t' = (t+1)(dt-\Delta)$ équations dont les coefficients sont de degré $\leqslant d$ et pour lequel la nouvelle valeur de Δ est

$$\Delta' = \frac{1}{2}td(d+1)+\Delta\left(td-\frac{1}{2}\right)-\Delta^2-\frac{1}{2}\sum\delta_i^2.$$

Les solutions de ce système sont engendrées par les solutions de Cramer et les solutions de degré $\leqslant (t'+1)\,d-\Delta'-2$. Les solutions du système initial sont donc engendrées par les solutions de Cramer, les solutions provenant des solutions de Cramer du système dérivé et les solutions de degré $\leqslant (t'+1)\,d-\Delta'-2+td-\Delta-1 = B$.

Il reste à examiner les solutions de Cramer. Celles du premier système sont de degré $\leqslant dt-\Delta$. Elles ne peuvent être de degré $> B$ que si $td-\Delta = \sum (d-\delta_i)^2 = 1$; ceci implique $d = 0$ ou $d = 1$, $B = 0$ et $\sup(d, B) = 1$.

Les solutions de Cramer du deuxième système donnent des solutions de degré $\leqslant B-d+2$. Cette quantité n'est supérieure à B que si $d = 0$ (cas déjà traité) ou $d = 1$; dans ce cas $B-d+2 = B+1$. Si les équations du deuxième système sont dépendantes, la suppression de celles qui sont superflues diminue strictement le degré des solutions de Cramer, car on a remarqué ci-dessus que l'on pouvait supposer indépendantes celles qui sont de degré zéro : elles proviennent en effet des parties homogènes de degré 1 des équations initiales.

Il ne reste donc à considérer que le cas où les équations du deuxième système sont indépendantes. Nous allons montrer que, dans ce cas, les solutions provenant des solutions de Cramer du deuxième système sont combinaisons linéaires des solutions de Cramer du système initial, ce qui démontrera la proposition.

Si les coefficients du système sont des polynômes dont les coefficients sont des indéterminées distinctes (cas générique), les solutions de Cramer engendrent le module des solutions ([E. N.] ou [B. E.]), et en particulier les solutions du deuxième système. Le résultat s'en déduit immédiatement en spécialisant les coefficients.

5.4. $n = 4$

Pour simplifier les formules, nous allons dorénavant supposer $\delta_i = 0$ pour tout i, c'est-à-dire $\Delta = 0$.

LEMME 4. — *Si* $\Delta = 0$, *la recherche des solutions du système considéré telles que*

$$\text{degré}_{x_1, x_2}(z_i) \leqslant td+d-2 \quad \textit{et} \quad \text{degré}_{x_1}(z_i) \leqslant td-1$$

pour tout i conduit à un système sur A_{n-2} *de* $t' = td\,(t+1)\,(td+3d-1)/2$ *équations à coefficients de degré* $\leqslant d$, *pour lequel on peut prendre pour* Δ *la valeur* $\Delta' = td^2\,(t+1)\,(d+1)/2$.

La démonstration se fait comme pour le lemme 3. L'apparition d'un Δ provient de ce que les équations correspondant aux monômes en X_1 et X_2 de degré élevé ont des coefficients de petit degré.

PROPOSITION 7. — *Si* $n = 4$, *le module des solutions du système considéré est engendré par les solutions telles que, pour tout i, on ait*

$$\text{degré}(z_i) \leqslant \sup(d, B'),$$

avec $B' = 1/2\,(t^3\,d^3+t^2\,d^2\,(3\,d-2)+2\,td\,(d^2-d+1)+4\,d-8)$. *On a* $B' < d$ *si, et seulement si,* $d = 0$ *ou* $t = d = 1$.

La démonstration est tout à fait analogue à celle de la proposition 6, mais en appliquant le théorème 2 avec $r = 2$, ce qui donne $B' = (t'd+d-2)+(td+d-2)$. Les solutions de Cramer nécessitent également quelques précautions. On peut supposer $d > 0$; si $d \geqslant 2$, on a $B' \geqslant t'd+td+d-2 \geqslant td$, ce qui montre qu'il n'y a pas de problème pour les solutions de Cramer.

Si $d = 1$, $t > 1$, on a $B' > td$; si $d = t = 1$, on a $B' = 0$ et $td = 1$; ceci montre que $B' < td$ équivaut à $d = 0$ ou $d = t = 1$ et que les solutions de Cramer du système initial sont de degré $\leqslant \sup(B', d)$.

Étudions les solutions de Cramer du système dérivé dans le cas $d = 1$; ces solutions sont de degré $\leqslant B'+1$. S'il y a une équation dont tous les termes sont constants, elle peut s'écrire sous la forme $z_i = \sum_{j \neq i} \alpha_{i,j}\, z_j$ ($\alpha_{i,j} \in K$). En éliminant z_i, on trouve un nouveau système dont les solutions ont les mêmes degrés que le système initial, mais qui a une équation de moins; ceci diminue strictement B', et cela montre que les solutions qui nous intéressent sont engendrées par des solutions de degré $\leqslant B'$. Si les parties de degré $d = 1$ des équations sont dépendantes, on peut abaisser le degré de l'une d'elles et se ramener au cas précédent. Dans les autres cas, ou bien les solutions de Cramer du système dérivé s'obtiennent après avoir supprimé des équations de degré > 0, et sont donc de degré $\leqslant B'$, ou bien les équations du système dérivé sont indépendantes, et on termine comme pour la proposition 3.

5.5. $n \geqslant 5$

On pourrait continuer la méthode précédente pour donner une borne analogue à B ou B', pour chaque valeur de n. Mais cela conduit à des formules très compliquées, et la borne obtenue est si grande qu'elle n'est plus utilisable pour se ramener directement à un système d'équations sur K qui puisse être résolu. Dans ce cas, il est nécessaire de procéder comme il est indiqué au paragraphe 4. Nous allons simplement procéder à une estimation des bornes que l'on peut obtenir.

PROPOSITION 8. — *Soit $D(t, d, n)$ le plus petit entier tel que tout système de t équations à coefficients de degré $\leqslant d$ sur A_n ait son module des solutions engendré par les solutions à coefficients de degré $\leqslant D(t, d, n)$. Quand t ou d tend vers l'infini, on a*

$$D(t, d, n) = 0((td)^k),$$

avec $k = 3^{n/2-1}$ si n est pair $\geqslant 2$, $k = 2.3^{(n-3)/2}$ si n est impair $\geqslant 3$.

La démonstration se fait par récurrence sur n, les cas $n = 2$ ou 3 étant déjà traités. Compte tenu du lemme 4, on a

$$D(t, d, n) \leqslant td + d - 2 + D(t', d, n-2)$$

avec $t' = 1/2\, d^2\, t\,(t+1)\,(t+3) - (1/2)\, td\,(t+1)$.

Ainsi $t'\, d = 0\,(t^3\, d^3)$ et $D(t, d, n+2) = 0\,((td)^{3k})$ où k est l'entier dépendant de n défini dans l'énoncé de la proposition 8.

PROPOSITION 9. — *Quand t tend vers l'infini et $n > 1$, $D(t, d, n)$ est majoré par une fonction équivalente à $2^{-l}(td)^k$ où $k = 3^{n/2-1}$, $l = (k-1)/2$ si n est pair, et $k = 2.3^{(n-3)/2}$, $l = k/2$ si n est impair.*

On procède de même : $D(t, d, n+2)$ est majoré par une fonction équivalente à

$$2^{-l}\left(\frac{(td)^3}{2}\right)^k = 2^{-(l+k)}(td)^{3k}.$$

Comme

$$k + \frac{k-1}{2} = \frac{3k-1}{2} \qquad \text{et} \qquad k + \frac{k}{2} = \frac{3k}{2},$$

les formules de l'énoncé s'obtiennent facilement.

6. Un contre-exemple

Le but de ce contre-exemple est de montrer le résultat suivant.

PROPOSITION 10 :

(*a*) *La borne de la proposition 5 est la meilleure possible, i. e.*

$$D(t, d, 2) = (t+1)\, d - \inf(2, d);$$

(*b*) *Les valeurs données pour* $D_{1,k}(G)$ (*cf.* th. 2) *sont les meilleures possibles au moins pour* $t = 1$;

(*c*) $D(t, d, n) \geqslant t\,d+(n-1)(d-1)+1-\inf(d, 2)$ *pour* $n > 0$ (*cf.* prop. 8).

Donnons-nous un corps K infini, $d_1, \ldots, d_n$ des entiers positifs, P_i, Q_i $(i = 1, \ldots, n)$ des éléments de $K[X_i]$ tels que degré $(P_i) = d_i - 1$, degré $(Q_i) \leqslant d_{i+1} - 1$, $Q_i(0) = 1$.

Posons $Q_0 = P_{n+1} = 0$ et $a_i = X_i P_i - X_{i-1} Q_{i-1}$ pour $i = 1, ..., n+1$. Supposons en outre que, pour tout i, les polynômes $a_1, \ldots, a_i$, Q_i engendrent A_i comme idéal. C'est possible, car nous verrons que la suite $a_1, \ldots, a_i$ est régulière (lemme 5); les zéros communs de $a_1, \ldots, a_i$ sur une clôture algébrique de K sont donc en nombre fini, et il suffit de choisir Q_i de manière qu'aucune des valeurs de X_i pour ces zéros ne soit racine de Q_i. Considérons l'équation $\sum a_i z_i = 0$ sur $A = A_n = K[X_1, \ldots, X_n]$ dont la résolution revient à chercher le noyau de l'application $f : A^{n+1} \to A$ de matrice $(a_1, \ldots, a_{n+1})$.

LEMME 5. — *On a* $ht(a_1, \ldots, a_{n+1}) = n$.

La suite $a_1, \ldots, a_n$ est régulière car

$$A_n/(a_1, \ldots, a_i) = A_i/(a_1, \ldots, a_i)[X_{i+1}, \ldots, X_n],$$

et a_{i+1} est un polynôme unitaire en X_{i+1} dans ce dernier anneau. La hauteur ne peut être $n+1$, car l'origine est un zéro commun aux a_i.

LEMME 6. — *Tout élément* $(y_1, \ldots, y_{n+1})$ *de* A^{n+1} *s'écrit d'une manière unique comme somme d'un élément de* im (ε) (notation du § 1) *et d'un élément* $(z_1, \ldots, z_{n+1})$ *tel que l'on ait* degré$_{X_i}(z_j) \leqslant d_i$ *pour tout couple* (i, j) *tel que* $i < j$, *et* degré $(z_i) \leqslant$ degré (y_i) *pour tout* i (*degré global*).

La division euclidienne de y_j par a_i permet d'écrire

$$(y_1, \ldots, y_{n+1}) \in A\,\varepsilon(e_i \wedge e_j) + (y'_1, \ldots, y'_{n+1})$$

avec degré$_{X_i}(y'_j) < d_i$, pour tout $(y_1, \ldots, y_{n+1}) \in A^{n+1}$. Si $i < j$, on a clairement $y'_k = y_k$ pour $k > j$,

$$\text{degré}_{X_k}(y'_j) = \text{degré}_{X_k}(y_j) \qquad \text{pour} \quad k > i$$
$$\text{et} \qquad \text{degré}(y'_i) \leqslant \text{degré}(y_i), \quad \text{pour tout } i.$$

L'assertion d'existence s'obtient donc aisément par récurrence descendante sur i et j.

Appelons *éléments réduits*, les éléments de A^{n+1} qui vérifient la condition de degrés de l'énoncé. On vient de montrer que $\dim_K(A^{n+1}/\text{im}\,\varepsilon)$ est majoré par la dimension de l'espace vectoriel de ces éléments réduits.

Pour montrer l'unicité, il suffit de montrer l'inégalité en sens inverse. En raison du lemme 5 et du théorème 2 (i), la suite

$$0 \to \Lambda^{n+1}(A^{n+1}) \to \ldots \to \Lambda^2(A^{n+1}) \to \mathrm{Im}(\varepsilon) \to 0$$

est exacte. La dimension du sous-espace vectoriel des éléments de $\mathrm{Im}(\varepsilon)$ de degré $\leqslant d$ est donc la somme alternée des dimensions des sous-espaces correspondants de $\Lambda^i(A^{n+1})$. En se limitant au sous-espace vectoriel des éléments de degré $\leqslant d$, on en déduit que $\dim(A^{n+1}/\mathrm{im}\,\varepsilon)$ ne dépend pas de la suite (a_i), à condition que $\mathrm{grade}(a_1, \ldots, a_{n+1}) = n$. En prenant $a_i = X_i^{d_i}$, $a_{n+1} = 0$, on montre facilement que les éléments réduits sont linéairement indépendants sur K, ce qui démontre le lemme.

LEMME 7. — *L'espace vectoriel des éléments réduits de* $\ker f$ *est engendré par* $t = (t_1, \ldots, t_{n+1})$ *défini par*

$$t_i = \prod_{j<i} P_j \prod_{k \geqslant i} Q_k .$$

Il est immédiat que t est un élément réduit de $\ker f$. Montrons qu'il engendre le sous-espace vectoriel considéré, par récurrence sur n. C'est immédiat si $n = 1$. Désignons par $\bar{X}$ l'image d'un élément X de A_n dans $A_{n-1} = A_n/X_n A_n$. Par récurrence, $\bar{t} = (\bar{t}_1, \ldots, \bar{t}_n)$ engendre l'espace des solutions réduites de l'équation $\bar{a}_1 \bar{z}_1 + \ldots + \bar{a}_n \bar{z}_n$. Si $z = (z_1, \ldots, z_{n+1})$ est un élément réduit de $\ker f$, $\bar{z} = (\bar{z}_1, \ldots, \bar{z}_n)$ est réduit, et il existe $a \in K$ tel que $\bar{z} - a\bar{t} = 0$. Il en résulte que $z_i - at_i$ est divisible par X_n pour $i \leqslant n$; posons $X_n z'_i = z_i - at_i$; on a $a_1 z'_1 + \ldots + a_n z'_n - Q_n z''_{n+1} = 0$ [1]; comme l'idéal $(a_1, \ldots, a_n, Q_n)$ est A_n, la solution $(z'_1, \ldots, z'_n, z''_{n+1})$ est engendrée par les solutions de Cramer ([B. E.], prop. 2.3), et il en est de même de $(z_1 - at_1, \ldots, z_n - at_n, z''_{n+1})$ considérée comme solution de $\sum a_i z_i = 0$. Comme cette solution est réduite elle est nulle.

C.Q.F.D.

COROLLAIRE. — *Considérons l'équation* $\sum_{i=1}^{n+1} a_i z_i = 0$;

(*a*) *Les solutions, telles que* $\mathrm{degré}(z_i) < \sum_{j=1}^{n+1} d_j - d_i - n$ *pour tout* i, *sont combinaisons linéaires de solutions de Cramer et n'engendrent pas le module des solutions.*

(*b*) *Les solutions, telles que* $\mathrm{degré}(z_i) \leqslant \sum_{j=1}^{n+1} d_j - d_i - n$, *ne sont pas toutes combinaisons linéaires de solutions de degré strictement plus petit, et engendrent le module des solutions.*

Ce corollaire entraîne la proposition 10 quand $t = 1$. Pour $t > 1$, considérons la matrice à $n+t$ colonnes et t lignes, définie par $a_{1,i} = a_i$

[1] Avec $z''_{n+1} = z_{n+1} - at_{n+1}$.

pour $i \leqslant n+1$, $a_{j,1} = b_j$ et $a_{j,n+j} = c_j$ pour $j > 1$, et $a_{i,j} = 0$ dans les autres cas, les polynômes b_j et c_j étant non nuls, et soumis à la seule condition que le produit des Q_i, les b_i et les c_i soient deux à deux premiers entre eux. Les solutions du système défini par cette matrice sont en bijection avec les solutions de $\sum a_i z_i = 0$ telles que z_1 soit divisible par le produit des c_i, la bijection étant l'application $(z_1, \ldots, z_{n+t}) \to (z_1, \ldots, z_{n+1})$. Cette même application est une bijection de l'ensemble des solutions de Cramer du système sur le produit par $c_2 \ldots c_t$ des solutions de Cramer de l'équation. Si on pose $\delta_1 = 0$, $\delta_i = d_1 - \text{degré}\,(b_i)$ pour $i > 1$, $d_{n+i} = d_1 + \text{degré}\,(c_i) - \text{degré}\,(b_i)$ pour $i > 1$, on obtient donc un système dont le module des solutions n'est pas engendré par les solutions telles que degré $(z_i) < D_{1,k}(G) - d_j$, ou encore tel que $H_1(G)$ n'est pas engendré par ses éléments de degré $< D_{1,k}(G)$.

La hauteur de la matrice considérée est $\leqslant 2$, car son idéal déterminantiel est contenu dans l'idéal engendré par la dernière ligne. On voit facilement que les déterminants extraits de la matrice sont globalement premiers entre eux, i. e. la hauteur est exactement 2. Comme le choix des degrés est libre, cela démontre un résultat plus fort que la proposition 10, que le lecteur énoncera s'il le désire.

7. Quelques algorithmes auxiliaires

Les algorithmes esquissés dans ce paragraphe sont donnés à titre indicatif pour montrer dans quelle mesure la méthode du paragraphe 4 peut être effectivement menée à bien.

7.1. Trouver un point en dehors d'une variété

Soit $f_1, \ldots, f_k \in A_n$ les équations de la variété. On essaie au hasard des points définissant un hyperplan. Si l'un d'eux est hors de la variété, on a gagné, sinon on calcule les équations de l'intersection de la variété avec l'hyperplan. Si la variété contient l'hyperplan, on essaie des points définissant un autre hyperplan. Quand le nombre d'hyperplans esssayés dépasse le degré d'un des f_i, l'un au moins n'est pas contenu dans la variété. On est donc ramené à trouver un point de l'hyperplan, hors de l'intersection de la variété et de l'hyperplan; autrement dit, on a diminué n. Une récurrence descendante sur n ramène finalement au cas où $n = 1$, où il suffit d'essayer un nombre de points supérieurs au degré d'un des f_i. En fait, l'algorithme est rapide, car les hyperplans sont définis par des points, et chaque point choisi a de fortes chances d'être hors de la variété.

7.2. Calculer la dimension d'une variété

Soient $f_1, \ldots, f_k$ les équations supposées homogènes de la variété plongée

dans l'espace projectif de dimension n. On introduit des polynômes homogènes de degré 1, $f_{k+1}, f_{k+2}, \ldots, f_{k+n}$, à coefficients indéterminés. On écrit la matrice, sur le corps de base, de l'application linéaire $g_1, \ldots, g_{k+n} \to \sum f_i g_i$ en degré $\sum_{i=1}^{n} d_i - n + 1$ (*cf.* corollaire du théorème 1; d_i = degré f_i). Le rang de cette matrice est égal au nombre de lignes car n hyperplans génériques ont pour intersection un point générique qui n'appartient pas à la variété. On recalcule ce rang par la méthode du pivot, en prenant le pivot dans une colonne correspondant aux coefficients de f_i avec i minimal. Supposons que le dernier pivot soit dans une colonne correspondant aux coefficients de f_l; si $l \leqslant k$, la variété est vide (dim $= -1$). Si $l > k$, la dimension de la variété est $l - k - 1$.

7.3. Trouver une variété linéaire projective de dimension maximale ne rencontrant pas une variété

Si l'espace ambiant est de dimension n et la variété de dimension d, la variété linéaire est de dimension $n - d - 1$. La méthode la plus simple est d'essayer au hasard des variétés linéaires de cette dimension. Malheureusement, je ne connais pas de méthode permettant de guider le choix du hasard afin de s'assurer, comme ci-dessus (7.1) que l'algorithme aboutit. En outre, il est long de vérifier si l'intersection est vide ou non : il faut à chaque fois appliquer le corollaire du théorème 1.

7.4. P.G.C.D.

Voir [MUS]. Remarquons toutefois que l'on peut utiliser 7·1 pour rendre unitaires en X_i les polynômes considérés. Cela permet de simplifier les divisions euclidiennes nécessaires.

8. Descente des solutions

Les algorithmes que nous avons donnés ne marchent que lorsque le corps de base est infini. Malheureusement, il se trouve que les corps faciles à manier sont principalement les corps finis. Il est donc important de pouvoir leur appliquer les méthodes ci-dessus. L'obstruction provient de ce que le complémentaire d'une variété peut être vide, et n'apparaît donc pas pour les corps finis dont le cardinal est assez grand par rapport aux degrés des polynômes qui apparaissent. On peut donc l'éliminer soit en prenant une extension finie galoisienne assez grande du corps de base, soit en prenant une extension transcendante simple, puis en redescendant les solutions obtenues sur le corps ainsi étendu.

Soient, plus précisément K un corps, L une extension de K, $A = K[X_1, \ldots, X_n]$, $B = L \otimes_K A = L[X_1, \ldots, X_n]$. Considérons un

système d'équations linéaires à coefficients dans A sans (resp. avec) second membre $\sum a_{i,j} z_j = 0$ (resp. $\sum a_{i,j} z_j = b_j$). Ce système définit un système à coefficients dans B, puisque $A \subset B$. Connaissant un système de générateurs du B-module des solutions à coefficients dans B (resp. une solution à coefficients dans B du système avec second membre), il s'agit de rtouver un système de générateurs du A-module des solutions à coefficients dans A (resp. une solution à coefficients dans A). C'est assez facile si L est une extension galoisienne finie de K ou si $L = K(u)$, u étant une indéterminée.

8.1. Cas transcendant

(*a*) *Système sans second membre.* — On peut multiplier chaque solution du système de générateurs par un polynôme, de manière à chasser tous les dénominateurs. Il est presque immédiat que les coefficients de chaque puissance de u des solutions ainsi trouvées sont des solutions à coefficients dans A, qui engendrent le B-module des solutions à coefficients dans B. Par fidèle platitude de B sur A, il en résulte aussitôt que les solutions ainsi trouvées engendrent le module des solutions à coefficients dans A.

(*b*) *Systèmes avec second membre.* — Soit P un dénominateur commun unitaire en u des coefficients de la solution sur B que l'on connaît. Le système $\sum a_{i,j} z_j = b_i$ s'écrit $\sum a_{i,j} z'_j = b_i P$ avec z_j, $P \in K[u]$. Comme P est unitaire en u, les termes en $u^{\deg P}$ des z'_j donnent une solution à coefficients dans A.

8.2. Cas galoisien

Soient $\omega_1, \ldots, \omega_d$ une base de L sur K et $\psi_1, \ldots, \psi_d$ les éléments de $G = \mathrm{Gal}(L/K)$. Remarquons que G opère sur les solutions à coefficients dans B.

PROPOSITION 11 :

(*a*) *Si S est une solution à coefficients dans B du système sans second membre, les $\psi_i(S)$ engendrent le même B-module que les $\sum_i \psi_i(\omega_j S)$ qui sont des solutions à coefficients dans A;*

(*b*) *Si* $\mathrm{Tr}(\omega_1) \neq 0$ *et si T est une solution à coefficients dans B du système avec second membre, alors* $\mathrm{Tr}(\omega_1)^{-1} \sum_i \psi_i(\omega_j T)$ *est une solution à coefficients dans A du même système.*

Les solutions considérées sont bien à coefficients dans A, car invariantes par G. Il est immédiat que les premières, $\sum_i \psi_i(\omega_j S)$, sont bien des solutions du système sans second membre. La matrice exprimant ces solutions sur les $\psi_i(S)$ a pour coefficients les $\psi_i(\omega_j)$. Il s'agit de montrer que cette

matrice est inversible, et par linéarité, il suffit de le faire pour une base particulière de L/K. Mais si on prend pour ω_j la puissance x^{j-1} d'un élément primitif x, la matrice des $\psi_i(\omega_j)$ est une matrice de Van der Monde inversible, puisque L/K est galoisienne.

Pour démontrer (*b*), il suffit de remarquer que, si $S = (z_1, \ldots, z_s)$, on a

$$\begin{aligned}\textstyle\sum_k a_{j,k} \sum_i \psi_i(\omega_1 z_k) &= \textstyle\sum_i \psi_i(\omega_1 \sum_k a_{j,k} z_k) \\ &= \textstyle\sum_i \psi_i(\omega_1 b_j) = \mathrm{Tr}(\omega_1) b_j.\end{aligned}$$

COROLLAIRE. — *Lorsque S parcourt un système de générateurs du module des solutions à coefficients dans B du système sans second membre et lorsque j varie de 1 à d, les $\sum_i \psi_i(\omega_j S)$ forment un système de générateurs du module des solutions à coefficients dans A.*

Il est clair que ces solutions à coefficients dans A engendrent le module des solutions à coefficients dans B [prop. 11 (*a*)]; la conclusion s'en déduit par fidèle platitude.

Remarque 1. — Pour avoir $\mathrm{Tr}(\omega_1) \neq 0$, il suffit de prendre $\omega_1 = 1$ et d premier à la caractéristique.

Remarque 2. — Si K est un corps fini, le calcul des $\psi_i(\omega_j S)$ est assez simple, car G est engendré par l'automorphisme de Frobenius.

9. Conclusions et problèmes

9.1. Bien qu'ils soient bien meilleurs que ceux de HERMANN, les algorithmes proposés ici sont très longs. Cela tient certes à la nature du problème. Cependant, nous n'avons obtenu les meilleures bornes absolues pour les degrés des solutions que pour $n \leqslant 2$. L'exemple du paragraphe 6 conduit à poser la question suivante :

(*a*) Est-ce que $D(t, d, n) = td + (n-1)(d-1) + 1 - \inf(d, 2)$? Plus généralement, peut-on supprimer l'hypothèse de hauteur dans le corollaire 2 du théorème 2?

9.2. Nous n'avons pas encore abordé la programmation effective des algorithmes considérés. Elle pose de nombreux problèmes non résolus dont les plus importants semblent être les suivants :

(*b*) Déterminer, selon les cas s'il faut appliquer la méthode du paragraphe 4, la méthode des majorations absolues ou un mélange des deux.

(*c*) Améliorer les algorithmes du paragraphe 7.

(*d*) Les matrices que l'on obtient sur le corps de base ont une forme très particulière avec beaucoup de zéros, et surtout beaucoup de coefficients répétés de nombreuses fois. Comment utiliser cette structure pour accélérer la résolution?

9.3. Pour appliquer la méthode du paragraphe 4 à un corps fini, il faut l'agrandir et redescendre les générateurs trouvés. On peut prendre une extension finie assez grande et redescendre les solutions, par descente galoisienne, ou prendre une extension transcendante pure $K(u)$ (*cf.* § 8).

(*e*) Quelle est la meilleure des deux méthodes?

9.4. La méthode du paragraphe 4 s'applique presque directement pour les systèmes avec second membre. Au lieu d'homogénéiser, il faut utiliser les parties homogènes de plus haut degré des générateurs de l'idéal déterminantiel. Si l'idéal engendré par ces parties homogènes est exactement de hauteur 1, on ne peut pas diviser par le P.G.C.D. Ainsi on ne peut pas toujours éliminer plus d'une indéterminée à la fois. Il en résulte que la borne absolue donnée par la méthode de HERMANN ([HER], [SEI]) n'est pas améliorée. Au contraire, la correction d'une erreur de [HER], reprise dans [SEI], l'empire : HERMANN applique notre lemme 3 avec $\Delta = 0$, et trouve dt^2 équations au lieu de $dt(t+1)$.

BIBLIOGRAPHIE

[B. E.] BUSCHBAUM (D. A.) and EISENBUD (D.). — Remarks on ideals and resolutions, « *Symposia Mathematica*, Vol. 11 », p. 193-204. — London, New York, Academic Press, 1973.

[BOU] BOURBAKI (N.). — *Algèbre commutative*, chap. 1-7. — Paris, Hermann, 1961-1965 (*Act. scient. et ind.*, 1290, 1293, 1308, 1314; *Bourbaki* 27, 28, 30 et 31).

[E. N.] EAGON (J.) and NORTHCOTT (D.). — Ideals defined by matrices and a certain complex associated to them, *Proc. Royal Soc. of London*, series A, t. 269, 1962, p. 188-204.

[HER] HERMANN (G.). — Die Frage der entlich vielen Schritte in der Theorie der Polynomideale, *Math. Annalen*, t. 95, 1926, p. 736-788.

[LAZ 1] LAZARD (D.). — Suites régulières dans les idéaux déterminantiels, *Comm. in Algebra*, t. 4, 1976, p. 327-340.

[LAZ 2] LAZARD (D.). — Suites régulières dans les idéaux déterminantiels, II (à paraître) dans *Comm. in Algebra*).

[LAZ 3] LAZARD (D.). — Algèbre linéaire sur les anneaux de polynômes « *Comptes rendus des journées mathématiques S.M.F.* [1974 Montpellier] » p. 365-368. — Montpellier Université des Sciences et Techniques du Languedoc 1974 (*Cahiers mathématiques*, 3).

[LAZ 4] LAZARD (D.). — Équations linéaires dans les anneaux de polynômes « *Colloque sur l'utilisation des calculateurs en mathématiques pures* [1975 Limoges] », p. 131-135; *Bull. Soc. math. France, Mémoire* 49-50 (à paraître).

[LAZ 5] LAZARD (D.). — Algorithmes fondamentaux en algèbre commutative « *Journées algorithmiques* [1975, E.N.S., Paris] », p. 131-138, *Astérisque*, 1976, n° 38-39.

[MAC] MACAULAY (F. S.). — *Algebraic theory of modular systems.* — Cambridge, Cambridge University Press, 1916 *ou* New York, London, Stechert-Hafner, 1964 (*Cambridge Tracts in Mathematics and mathematical Physics*, 19).

[MUS] MUSSER (D. R.). — Multivariate polynomial factorization, *J. of A.C.M.*, t. 22, 1975, p. 291-309.

[SEI] SEIDENBERG (A.). — Construction in algebra *Trans. Amer. math. Soc.*, t. 197, 1974, p. 273-313.

VdW] VAN DER WAERDEN (B. L.). — *Moderne Algebra.* Bände 1 und 2. — Berlin, J. Springer, 1930-1931; 3te verbesserte Auflage : Berlin, Springer-Verlag, 1950-1955 (*Grundlehren der mathematischen Wissenschaften*, 33-34); Translation from the 2nd German edition : New York, F. Ungar, 1950-1953.

(Texte reçu le 17 septembre 1976.)

Daniel LAZARD,
Mathématiques,
Université de Poitiers,
40, avenue du Recteur Pineau,
86022 Poitiers Cedex.