SÉMINAIRE N. BOURBAKI

HYMAN BASS

Libération des modules projectifs sur certains anneaux de polynômes

Séminaire N. Bourbaki, 1975, exp. n° 448, p. 228-254

<http://www.numdam.org/item?id=SB_1973-1974__16__228_0>

© Association des collaborateurs de Nicolas Bourbaki, 1975, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (http://www.bourbaki.ens.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI
26e année, 1973/74, n° 448

448-01
Juin 1974

LIBÉRATION DES MODULES PROJECTIFS SUR CERTAINS ANNEAUX DE POLYNÔMES

par Hyman BASS

1. Le problème et son histoire

Soit $A = k[t_1,\ldots,t_n]$ l'algèbre de polynômes en n variables sur un corps commutatif k. En 1955, Serre a demandé si tout A-module projectif de type fini P est libre ([11], p. 243) (*). On ne connait toujours pas de contre-exemple. Bien sûr P est libre si $n = 1$ (A est principal) ou si son rang r est égal à 1 (A est factoriel).

La liste suivante donne, par ordre chronologique, les résultats les plus importants liés directement à ce problème :

1958 (1) P est libre si $n = 2$ (Seshadri [10]).

(2) P est "stablement libre", autrement dit, il existe un $s \geq 0$ tel que $P \oplus A^s \cong A^{r+s}$ (Serre [12]).

(3) $P = Q \oplus L$ où L est libre et $\text{rang}(Q) \leq n$ (Serre [12]).

1960 (4) Soit $V = \text{Spec}(A/\mathfrak{p})$ une variété non-singulière de codimension 2 dans l'espace affine $\text{Spec}(A)$. Si V est une intersection complète, (i.e. si $\mathfrak{p}$ est engendré par deux éléments), alors le module des différentielles $\Omega^{n-2}_{V/k} = \Lambda^{n-2}(\Omega^1_{V/k})$ est isomorphe à $A/\mathfrak{p}$. Serre [13] montre que la réciproque est vraie si tout A-module projectif de

(*) Les A-modules projectifs non de type fini sont libres [1]. Si k est un corps non commutatif, il existe un module non libre P sur $A = k[t_1,t_2]$ tel que $P \oplus A \cong A^2$ (cf. [8]).

rang 2 est libre. La condition $\Omega^{n-2}_{V/k} \cong A/\rho$ est par exemple satisfaite lorsque $n = 3$ et V est une courbe de genre 0 ou 1 . Segre [9] a prétendu donner de telles courbes qui ne sont pas des intersections complètes, mais ses démonstrations ne sont pas complètes, et ses conclusions sont inexactes, comme nous allons le voir.

1964 (5) P est libre si $r > n$ (cf. [2]).

1973 Après une longue période sans progrès de nouveaux résultats proviennent, presque simultanément, de trois sources indépendantes. Notons $\bar{k}$ une clôture algébrique de k .

(6) P est libre si $r = n$ et $k = \bar{k}$ (M. Roitman, Jérusalem).

(7) P est libre si $n = 3$ et $k = \bar{k}$ (M. P. Murthy et J. Towber, Chicago). Leur démonstration s'appuie sur des résultats d'Abhyankar sur les équations définissant une courbe non singulière dans l'espace affine à trois dimensions.

(8) A. Suslin (Léningrad) et L. N. Vaserštein (Moscou) montrent que P est libre dans les cas suivants :

(a) $r \geq 1 + \frac{n}{2}$.

(b) $n = 3$.

(c) $n = 4$, $\mathrm{car}(k) \neq 2$.

(d) $n = 5$, k fini, $\mathrm{car}(k) \neq 2$.

A partir des démonstrations de Roitman et de Murthy-Towber, Swan (Chicago) démontre, indépendamment de Suslin-Vaserštein,

(a) pour k infini, et (b) et (c) pour k infini de caractéristique $\neq 2$. Sa méthode est voisine de celle de Suslin-Vaserštein, mais pas aussi forte.

Cet exposé est consacré aux résultats et méthodes de Suslin et Vaserštein.

2. Enoncé des résultats de Suslin et Vaserštein

Soit A un anneau commutatif. En vertu du théorème de Serre cité plus haut ((2) du n° 1), on cherche un critère pour que tout A-module stablement libre P soit libre, plus précisément pour que la condition $P \oplus A^s \cong A^{r+s}$ entraîne $P \cong A^r$. Par une récurrence évidente on se ramène au cas $s = 1$. Ainsi on est amené à considérer les éléments $a = (a_1, \ldots, a_{r+1}) \in A^{r+1}$ qui engendrent un facteur direct $\cong A$ de A^{r+1}, autrement dit, tels qu'il existe une forme linéaire $h : A^{r+1} \to A$ envoyant a sur 1, ou, ce qui revient au même, tels que l'idéal $Aa_1 + \ldots + Aa_{r+1}$ soit égal à A. Un tel élément est dit unimodulaire dans A^{r+1} ; on note $\mathrm{Un}_{r+1}(A)$ l'ensemble de ces éléments.

Si $a \in \mathrm{Un}_{r+1}(A)$, il existe une décomposition $A^{r+1} = P \oplus Aa$, et $P \cong A^{r+1}/Aa$. Si $a' \in \mathrm{Un}_{r+1}(A)$ et $A^{r+1} = P' \oplus Aa'$, on voit facilement que $P \cong P' \Leftrightarrow \exists\, \alpha \in \mathrm{GL}_{r+1}(A)$ tel que $\alpha(a) = a'$, d'où :

(1) L'application $a \mapsto A^{r+1}/Aa$ induit une bijection de l'ensemble des orbites $\mathrm{GL}_{r+1}(A) \backslash \mathrm{Un}_{r+1}(A)$ sur l'ensemble des classes d'isomorphie des A-modules P tels que $P \oplus A \cong A^{r+1}$.

On en déduit, pour tout entier $r_o \geq 1$, l'équivalence :

(2)
$(a)_{r_o}$ Tout A-module stablement libre de rang $r \geq r_o$ est libre.

$\Updownarrow$

$(b)_{r_o}$ $\mathrm{GL}_{r+1}(A)$ opère transitivement sur $\mathrm{Un}_{r+1}(A)$ pour tout $r \geq r_o$.

Remarquons que si $P \oplus A^s \cong A^{r+s}$, on voit, en prenant les puissances extérieures $(r+s)$-ièmes, que $\Lambda^r P \cong A$, et donc que $P \cong A$ si $r = 1$; autrement dit, un A-module stablement libre de rang 1 est libre. Ainsi :

(3) La condition $(b)_2$ équivaut à dire que tout A-module stablement libre soit libre.

Dans la pratique, on précise la condition $(b)_{r_o}$ en montrant la transitivité d'un certain sous-groupe de $GL_{r+1}(A)$, par exemple le sous-groupe $E_{r+1}(A)$ engendré par les "matrices élémentaires" $I + ae_{ij}$ ($a \in A$, $1 \leq i, j \leq r+1$, $i \neq j$). Cette transitivité résulte, en particulier, de la condition de "domaine stable" suivante :

$(DS)_r$ Si $(a_1,\ldots,a_{r+1}) \in Un_{r+1}(A)$, il existe $a'_i = a_i + b_i a_{r+1}$, $b_i \in A$ $(1 \leq i \leq r)$ tels que $(a'_1,\ldots,a'_r) \in Un_r(A)$.

PROPOSITION 1.- Soit r_o un entier ≥ 1. La condition $(DS)_{r_o}$ entraîne la condition $(DS)_r$ pour $r \geq r_o$; elle entraîne aussi que $E_{r+1}(A)$ opère transitivement sur $Un_{r+1}(A)$.

La démonstration est facile (cf. [3], ch. V, th. (3.3) et [14], th. 1).

On note $DS(A)$ le plus petit entier $r \geq 1$, ou l'infini s'il n'en existe pas, tel que $(DS)_r$ soit satisfait. Ainsi les A-modules stablement libres de rang $\geq DS(A)$ sont libres.

THÉORÈME 1 (cf. [3], th. (3.5)).- Si A est noethérien de dimension d on a $DS(A) \leq d + 1$.

Pour les algèbres de type fini sur un corps fini Vaserštein obtient l'amélioration suivante, qui provient du fait que si A est l'algèbre d'une courbe affine sur un corps fini, tout sous-groupe d'indice fini de $Sp_{2n}(A)$ $(n \geq 2)$ est un sous-groupe de congruence (cf. [5]).

THÉORÈME 2 (Vaserštein).- Si A est une algèbre de degré de transcendance e sur un corps fini k, on a $DS(A) \leq \max(2,e)$.

Ici e désigne le supremum des entiers n tels qu'il existe un plongement d'une k-algèbre de polynômes en n variables dans A. Lorsque A est une

k-algèbre de type fini, on a $e = \dim A$.

Les théorèmes 1 et 2 seront démontrés au n° 3.

THÉORÈME 3 (Suslin).- Soit B un anneau commutatif noethérien de dimension d . Soit $A_n = B[t_1,\dots,t_n]$ la B-algèbre de polynômes en n variables. Pour tout $n \geq 1$, $E_{r+1}(A_n)$ opère transitivement sur $Un_{r+1}(A_n)$ pour tout r tel que

$$r \geq 1 + \max\left(d, \frac{DS(A_{n-1})}{2}\right).$$

Par suite, les A_n-modules stablement libres de tels rangs r sont libres.

Le théorème 3 sera démontré au n° 4. Les théorèmes 1, 2 et 3 donnent le corollaire suivant, vu le fait que $\dim A_n = d + n$.

COROLLAIRE 1.- (1) $E_{r+1}(A_n)$ opère transitivement sur $Un_{r+1}(A_n)$ pour tout $r \geq 1 + \max(d, \frac{d+n}{2})$.

(2) Si B est une algèbre de degré de transcendance e sur un corps fini, $E_{r+1}(A_n)$ opère transitivement sur $Un_{r+1}(A_n)$ pour tout $r \geq 1 + \max(e, \frac{e+n-1}{2})$.

En appliquant (3), on en déduit :

COROLLAIRE 2.- Supposons, dans le cas (1), que $d \leq 1$ et $d + n \leq 2$, et, dans le cas (2), que $e \leq 1$ et $e + n \leq 3$. Alors tout A_n-module stablement libre est libre.

Ce corollaire s'applique à $A_1 = B[t]$ si $\dim B \leq 1$ (cas contenant le théorème de Seshadri, (1) du n° 1), et à $A_2 = B[t_1,t_2]$ si B est une algèbre de degré de transcendance ≤ 1 sur un corps fini. En particulier :

COROLLAIRE 3.- Soit $B = k$, un corps commutatif. Les A_2-modules projectifs sont libres. Si k est (algébrique sur un corps) fini les A_3-modules projectifs sont libres.

La conclusion du prochain corollaire figure comme hypothèse dans les résultats donnés plus loin :

COROLLAIRE 4.- Le groupe $E_{r+1}(A_n)$ opère transitivement sur $Un_{r+1}(A_n)$ pour tout $r \geq 3$ dans chacun des cas suivants :

(1) $d \leq 2$ et $d + n \leq 4$;

(2) B est une algèbre de degré de transcendance $e \leq 2$ sur un corps fini, et $e + n \leq 5$.

Ce corollaire s'applique notamment, lorsque B est un corps commutatif k , à $A_n = k[t_1,\ldots,t_n]$ avec $n \leq 4$, et, si k est algébrique sur un corps fini, avec $n = 5$. Il entraîne que les A_n-modules stablement libres de rang ≥ 3 sont libres, mais il laisse incertain le sort de ceux de rang 2 . Ces derniers font l'objet du prochain théorème.

Soit A un anneau commutatif. Par A-module symplectique, on entend un couple (P,h) où P est un A-module projectif de type fini et où $h : P \times P \to A$ est une forme A-bilinéaire alternée ($h(x,x) = 0 \ \forall\ x \in P$) et non singulière ($x \mapsto (y \mapsto h(x,y))$ est un isomorphisme $P \to P^* = \mathrm{Hom}(P,A)$) . La somme directe $(P,h) \oplus (P',h') = (P \oplus P' , h \oplus h')$ se définit de manière évidente, d'où un groupe de Grothendieck, noté $KSp_o(A)$ (cf. [4], ch. I, (4.12)). Pour tout A-module projectif de type fini Q , on définit le module hyperbolique $H(Q) = (Q \oplus Q^* , h_Q)$ où $h_Q((x,f),(y,g)) = f(y) - g(x)$, qui est un module symplectique. On a des isomorphismes $H(Q \oplus Q') \cong H(Q) \oplus H(Q')$ et $(P,h) \oplus (P,-h) \cong H(P)$ (loc. cit.). Il s'ensuit que tout élément de $KSp_o(A)$ s'exprime sous la forme $[P,h] - [H(A^n)]$, où $[P,h]$ désigne la classe d'un A-module symplectique (P,h) dans $KSp_o(A)$. L'application $(P,h) \mapsto P$ définit un homomorphisme $KSp_o(A) \to K_o(A)$; notons W(A) son noyau. Le groupe W(A) s'identifie au groupe des classes $[P,h]'$ des modules symplectiques (P,h) avec P (stablement) libre, où $[P_1,h_1]' = [P_2,h_2]' \Leftrightarrow \exists$ des entiers $n_1 , n_2 \geq 0$ tels que $(P_1,h_1) \oplus H(A^{n_1}) \cong (P_2,h_2) \oplus H(A^{n_2})$.

THÉORÈME 4 (Vaserštein).- Soit A un anneau commutatif. Il existe une application canonique

$$\varphi : SL_3(A) \backslash Un_3(A) \to W(A) .$$

Si $E_{r+1}(A)$ opère transitivement sur $Un_{r+1}(A)$ pour tout $r \geq 3$, alors φ est bijective.

Ce théorème sera démontré au n° 5.

COROLLAIRE.- Soit A un anneau commutatif. Supposons satisfaites les conditions

(*) $E_{r+1}(A)$ opère transitivement sur $Un_{r+1}(A)$ pour tout $r \geq 3$;
et
(**) $W(A) = 0$.

Alors tout A-module stablement libre est libre.

En effet, vu le théorème 4, les conditions (*) et (**) entraînent la condition $(b)_2$ de (2), d'où le corollaire d'après (3).

La condition (*) est fournie dans certains cas par le corollaire 4 du théorème 3. Pour assurer la condition (**), on peut appliquer le corollaire de la proposition 2, et le théorème 5 ci-après :

PROPOSITION 2.- Soit A un anneau commutatif et soit d un entier ≥ 0 . Supposons que tout A-module stablement libre de rang $r > d$ possède un élément unimodulaire (c'est-à-dire un élément qui engendre un facteur direct $\cong A$). Soit (P,h) un A-module symplectique avec P stablement libre. Alors il existe un entier $n \geq 0$ et un A-module symplectique (Q,g) avec Q de rang $\leq d$ tel que $(P,h) \cong (Q,g) \oplus H(A^n)$.

Supposons, en effet, que le rang r de P soit $> d$; il suffit de montrer que (P,h) contient un facteur direct $\cong H(A)$. Par hypothèse P contient un élément unimodulaire e . Puisque h est non singulière, il existe $f \in P$ tel que $h(f,e) = 1$. Alors le sous-module H de P engendré par e et f , muni de la restriction de h , est isomorphe à H(A) , et P est somme directe

de H et de son orthogonal, d'où la proposition (cf. [4], ch. I, (4.10.2)).

Remarque.- L'hypothèse de la proposition 2 est satisfaite lorsque $DS(A) \leq d + 1$, les A-modules stablement libres de rang $> d$ étant alors libres (prop. 1), en particulier lorsque A est noethérien de dimension $\leq d$ (théorème 1).

COROLLAIRE.- Soit A un anneau commutatif noethérien de dimension ≤ 1. Alors $W(A) = 0$.

En effet le rang d'un module symplectique est pair, donc zéro s'il est ≤ 1.

THÉORÈME 5 (Karoubi [6]).- Soit A un anneau commutatif dans lequel 2 est inversible. Soit $A[t]$ la A-algèbre de polynômes en une variable t. L'homomorphisme $W(A) \to W(A[t])$ induit par l'inclusion $A \to A[t]$ est un isomorphisme.

Ce théorème sera démontré au n° 6. On ignore si l'hypothèse " 2 est inversible" est nécessaire.

COROLLAIRE 1.- Soit B un anneau commutatif noethérien de dimension ≤ 1 dans lequel 2 est inversible. Soit $A_n = B[t_1,\ldots,t_n]$ la B-algèbre de polynômes en n variables. Les A_n-modules stablement libres sont libres dans chacun des cas suivants :

(1) $n \leq 3$;

(2) $n \leq 4$ et B est une algèbre de degré de transcendance ≤ 1 sur un corps fini.

Il suffit de vérifier les conditions (*) et (**) du corollaire du théorème 4. Le corollaire 4 du théorème 3 fournit (*) dans les deux cas. Le corollaire de la proposition 2 entraîne que $W(B) = 0$. Par suite, le théorème 5 (applicable car 2 est inversible) implique que $W(A_n) = 0$ pour tout $n \geq 0$, d'où (**).

COROLLAIRE 2.- Soit k un corps commutatif et soit $A_n = k[t_1,\ldots,t_n]$ la k-algèbre de polynômes en n variables. Les A_n-modules projectifs sont libres

dans chacun des cas suivants :

- $n \leq 2$;
- $n = 3$ et k est soit fini, soit de caractéristique $\neq 2$;
- $n = 4$ et $\mathrm{car}(k) \neq 2$;
- $n = 5$ et k est fini de caractéristique $\neq 2$.

Les cas où $\mathrm{car}(k) \neq 2$ résultent du corollaire précédent en prenant $B = k[t_1]$. Les cas $n \leq 2$ et $n = 3$ avec k fini sont contenus dans le corollaire 3 du théorème 3.

Complément.- Le cas $n = 3$ avec k quelconque résulte du théorème suivant :

THÉORÈME 6 (Suslin).- Si B est un anneau principal, les modules projectifs sur $A_2 = B[t_1, t_2]$ sont libres.

La démonstration de ce théorème, ainsi que des précédents, se trouvera dans un article de Suslin et Vaserštein en préparation.

3. Démonstration des théorèmes 1 et 2

Soit A un anneau commutatif.

LEMME 1.- Soit $a = (a_1, \ldots, a_{r+1}) \in A^{r+1}$. Si $(a_1, \ldots, a_r) \in \mathrm{Un}_r(A)$, il existe $\varepsilon \in E_{r+1}(A)$ tel que $\varepsilon(a) = (1, 0, \ldots, 0)$.

Posons $e_{ij}^b = I + be_{ij}$. Choisissons $b_1, \ldots, b_r$ tels que $1 - a_1 - a_{r+1} = b_1 a_1 + \ldots + b_r a_r$. L'élément $e_{r+1,1}^{b_1} \cdot \ldots \cdot e_{r+1,r}^{b_r}$ transforme a en $a' = (a_1, \ldots, a_r, 1 - a_1)$, et $e_{1,r+1}^{1}$ transforme a' en $a'' = (1, a_2, \ldots, a_r, 1 - a_1)$. Enfin $e_{2,1}^{-a_2} \cdot \ldots \cdot e_{r,1}^{-a_r} \cdot e_{r+1,1}^{a_1 - 1}$ transforme a'' en $(1, 0, \ldots, 0)$.

LEMME 2.- Supposons A noethérien. Soit $a = (a_1, \ldots, a_{r+1}) \in \mathrm{Un}_{r+1}(A)$. Il existe des éléments $a_i'' = a_i + b_{i,i+1}a_{i+1} + \ldots + b_{i,r+1}a_{r+1}$ avec $b_{ij} \in A$ $(1 \leq i < j \leq r)$ tels que, pour tout i $(1 \leq i \leq r)$, l'idéal

$\mathfrak{a}_i = Aa''_1 + \ldots + Aa''_i$ soit de hauteur $\geq i$.

On commence par choisir $a''_1 = a_1 + b_{1,2}a_2 + \ldots + b_{1,r+1}a_{r+1}$ en dehors de tous les idéaux premiers minimaux de A , ce qui est facile. Ensuite, on applique une hypothèse de récurrence (sur r) à l'image de $(a_2,\ldots,a_{r+1})$ dans $(A/Aa''_1)^r$ pour achever la démonstration.

LEMME 3.- Gardons les notations du lemme 2. Soit s un entier tel que $1 \leq s \leq r$. Il existe $(a'_1,\ldots,a'_s) \equiv (a_1,\ldots,a_s)$ mod. $(Aa_{s+1} + \ldots + Aa_{r+1})$ tel que $Aa'_1 + \ldots + Aa'_s = Aa''_1 + \ldots + Aa''_s$.

Considérons a et a'' comme des vecteurs colonnes, de sorte que $a'' = \varepsilon a$ où $\varepsilon = (c_{ij})_{1 \leq i,j \leq r+1}$ avec $c_{ij} = b_{ij}$ pour $i < j$, $c_{ii} = 1$, et $c_{ij} = 0$ si $i > j$. Ecrivons ε sous la forme $\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$ où α (resp. δ) sont des matrices carrées (triangulaires) à s (resp. $r+1-s$) lignes. Ainsi $\varepsilon = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}\begin{pmatrix} I & \alpha^{-1}\beta \\ 0 & I \end{pmatrix}$, et il est clair que les a'_i définis par

$$\begin{pmatrix} I & \alpha^{-1}\beta \\ 0 & I \end{pmatrix}\begin{pmatrix} a_1 \\ \vdots \\ a_{r+1} \end{pmatrix} = \begin{pmatrix} a'_1 \\ \vdots \\ a'_s \\ a_{s+1} \\ \vdots \\ a_{r+1} \end{pmatrix}$$ répondent au lemme.

Démonstration du théorème 1. Supposons A noethérien de dimension d . Soit $a = (a_1,\ldots,a_{r+1}) \in Un_{r+1}(A)$. D'après les lemmes 2 et 3, il existe $(a'_1,\ldots,a'_r) \equiv (a_1,\ldots,a_r)$ mod. Aa_{r+1} tel que l'idéal $\mathfrak{a} = Aa'_1 + \ldots + Aa'_r$ soit de hauteur $\geq r$. Si $r \geq d+1$, on a donc $\mathfrak{a} = A$, c'est-à-dire $(a'_1,\ldots,a'_r) \in Un_r(A)$. On en conclut que $DS(A) \leq d+1$, d'où le théorème 1.

Passons au théorème 2. Soit A une algèbre de degré de transcendance e sur un corps fini k. Il faut démontrer que $DS(A) \leq \max(2,e)$. Il suffit, évidemment, de montrer que $DS(A') \leq \max(2,e)$ pour toute sous-k-algèbre A' de A de type fini. On se ramène donc au cas où A est une k-algèbre de type fini, de sorte que $e = \dim A$. Le théorème 2 résulte alors du théorème suivant :

THÉORÈME 2'.- *Supposons que k soit ou bien un corps fini ou bien l'anneau des S-entiers d'un corps de nombres F (fini sur $\mathbb{Q}$), où S est un ensemble fini de places de F, contenant toutes les places infinies et au moins une place finie. Soit A une k-algèbre commutative de type fini de dimension (de Krull) d. Alors $DS(A) \leq \max(2,d)$.*

C'est une conséquence immédiate de la proposition et du lemme suivants. Posons $Sp(A) = \bigcup_n Sp_{2n}(A)$, groupe symplectique infini, et notons $KSp_1(A)$ le quotient de $Sp(A)$ par son sous-groupe de commutateurs $Ep(A) = (Sp(A), Sp(A))$.

PROPOSITION 3.- *Si, dans le théorème 2', on a $d \leq 1$, alors $KSp_1(A) = 0$.*

LEMME 4.- *Soit A un anneau commutatif noethérien de dimension d. Supposons que, pour tout quotient A' de A de dimension ≤ 1, on ait $KSp_1(A') = 0$. Alors $DS(A) \leq \max(2,d)$.*

Démonstration de la proposition 3. Pour tout idéal $\mathfrak{q}$ de A, posons $Sp(\mathfrak{q}) = \mathrm{Ker}(Sp(A) \to Sp(A/\mathfrak{q}))$, $Ep(A,\mathfrak{q}) = (Sp(A), Sp(\mathfrak{q}))$, et $KSp_1(A,\mathfrak{q}) = Sp(\mathfrak{q})/Ep(A,\mathfrak{q})$. Remarquons que $Sp(\mathfrak{q})$ ne dépend que de $\mathfrak{q}$, tandis que $Ep(A,\mathfrak{q})$ dépend de $\mathfrak{q}$ et de A. De plus, on a une suite exacte évidente $KSp_1(A,\mathfrak{q}) \to KSp_1(A) \to KSp_1(A/\mathfrak{q})$. On a $KSp_1(A,\mathfrak{q}) = 0$ si

(a) $\mathfrak{q} \subset \mathrm{rad}(A)$ ([4], ch. II, cor. (7.12)),

ou si (b) A est artinien ([4], ch. IV, cor. (4.9) avec $d = 0$).

Grâce à (a) on peut passer de A à son quotient par son nilradical, de sorte

qu'on peut supposer A réduit. Soit B la clôture intégrale de A dans son anneau total de fractions. L'anneau B est un produit fini d'anneaux C isomorphes soit à un corps fini, soit à l'anneau des T-entiers d'un corps global L où T est un ensemble fini de places contenant toutes les places infinies et au moins une place finie, vu les hypothèses du théorème 2'. Il résulte donc du théorème des sous-groupes de congruence ([5], cor. (12.5)) que, pour tout $n \geq 2$, tout sous-groupe d'indice fini de $Sp_{2n}(C)$ contient un sous-groupe $Sp_{2n}(\mathfrak{q})$ où $\mathfrak{q}$ est un idéal d'indice fini de C. On en déduit facilement que, pour tout idéal $\mathfrak{q}$ de B, on a $KSp_1(B,\mathfrak{q}) = 0$, c'est-à-dire $Sp(\mathfrak{q}) = E(B,\mathfrak{q})$.

Soit $\underline{c} = \mathrm{ann}_A(B/A)$ le conducteur de B dans A. On a

$$\begin{aligned} Ep(A) \supset Ep(A,\underline{c}) &= (Sp(A), Sp(\underline{c})) \\ &\supset (Sp(\underline{c}), Sp(\underline{c})) \\ &\supset Ep(B,\underline{c}') = Sp(\underline{c}') \end{aligned}$$

où $\underline{c}'$ désigne l'idéal de B engendré par les éléments $2cc'$ et c^2c' où c, c' parcourent $\underline{c}$ ([4], p. 161, th. (6.2) et pp. 175-178, prop. (7.8) et (7.8.1)). Il s'ensuit que $KSp_1(A) \to KSp_1(A/\underline{c}')$ est injectif. Or $A/\underline{c}'$ est un anneau fini, d'où $KSp_1(A/\underline{c}') = 0$ d'après (b).

Démonstration du lemme 4. Si $d < 2$, le lemme résulte du théorème 1. Si $d > 2$, le raisonnement par récurrence qui démontre le théorème 1 marche, pourvu qu'on traite le cas critique $d = 2$. On se ramène donc à montrer, en supposant $d = 2$, qu'étant donné $(a,b,q) \in Un_3(A)$, il existe $(a',b') \equiv (a,b) \bmod. Aq$ dans $Un_2(A)$. En passant de A à son quotient par son nilradical, on se ramène facilement au cas où A est réduit. Posons $\bar{A} = A/Aq$.

Montrons d'abord qu'il suffit de traiter le cas où $\dim \bar{A} \leq 1$. En effet, dans le cas général, soit $\mathfrak{q}_0$ (resp. $\mathfrak{q}_1$) l'intersection des idéaux premiers minimaux de A que contient (resp. ne contient pas) $\mathfrak{q}$, et posons $A_i = A/\mathfrak{q}_i$, de sorte qu'on peut considérer A comme sous-anneau de $A_0 \times A_1$. Si $x \in A$, notons x_i sa classe modulo $\mathfrak{q}_i$, de sorte que $x = (x_0,x_1)$ comme élément de $A_0 \times A_1$. On a $q = (0,q_1)$ et q_1 n'est pas diviseur de zéro dans A_1. Par suite $\bar{A}_1 = A_1/q_1A_1$ est de dimension $< \dim A_1 \leq 2$. D'après notre hypothèse, il existe s, $t \in A$ tels que

$(a_1', b_1') = (a_1 + s_1q_1, b_1 + t_1q_1) \in Un_2(A_1)$. Posons $(a',b') = (a + sq, b + tq) \in A^2$. Sa classe (a_1', b_1') modulo q_1 est unimodulaire. Puisque $q_0 = 0$, sa classe modulo q_0 est (a_0,b_0) , qui est encore unimodulaire. Par suite l'idéal $\mathfrak{a} = Aa' + Ab'$ engendre l'idéal $A_0 \times A_1$ de $A_0 \times A_1$. Mais $A_0 \times A_1$ est intègre sur A , donc $\mathfrak{a} = A$, c'est-à-dire $(a',b') \in Un_2(A)$.

On peut donc supposer que $\dim \bar{A} \leq 1$. Notons $t \mapsto \bar{t}$ l'application $A \to \bar{A}$ de passage au quotient, de sorte que $(\bar{a},\bar{b}) \in Un_2(\bar{A})$. Soient $\bar{c}$, $\bar{d} \in \bar{A}$ tels que $\bar{a}\bar{d} - \bar{b}\bar{c} = 1$, c'est-à-dire tels que $\bar{\alpha} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in Sp_2(\bar{A})$. Supposons qu'il existe un élément $\alpha = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in Sp_2(A)$ d'image $\bar{\alpha}$ modulo Aq . Alors il est clair que $(a',b') \equiv (a,b)$ mod. Aq et $(a',b') \in Un_2(A)$. Vu l'hypothèse du lemme 4, la démonstration sera donc achevée par la proposition suivante :

PROPOSITION 4.- Soit A un anneau commutatif noethérien de dimension ≤ 2 , et soit $\bar{A} = A/q$ un quotient de A . Pour tout $n \geq 1$, l'image de $Sp_{2n}(A) \to Sp_{2n}(\bar{A})$ contient tout élément $\bar{\alpha}$ dont la classe dans $KSp_1(\bar{A})$ s'annule.

Avec les notations de [4], il existe un $m \geq 0$ tel que $\bar{\alpha} \perp I_{2m} \in Ep_{2(n+m)}(A)$. D'après [4], ch. II, prop. (2.3), il existe $\beta \in E_{2(n+m)}(A)$ relevant $\bar{\alpha} \perp I_{2m}$. Si $m = 0$, on a gagné. Supposons $m \geq 1$, et soit $e_1,\ldots,e_{n+m}, f_1,\ldots,f_{n+m}$ la base symplectique habituelle de $H(A^{n+m})$. Le "couple hyperbolique" $\beta e_{n+m}, \beta f_{n+m}$ est congru modulo q au couple e_{n+m}, f_{n+m} . D'après les hypothèses sur A et ([4], ch. IV, cor. (4.9)), il existe un $\varepsilon \in Ep_{2(n+m)}(A,q)$ tel que $\varepsilon\beta e_{n+m} = e_{n+m}$, $\varepsilon\beta f_{n+m} = f_{n+m}$. Ainsi

$\varepsilon\beta = \beta_1 \perp I_2$ où β_1 est un relèvement de $\bar{\alpha} \perp I_{2(m-1)}$ à $Sp_{2(n+m-1)}(A)$, d'où le résultat par récurrence sur m.

Remarque.- Le théorème 1 entraîne que $DS(A) \leq 3$, et en fait cette condition suffit pour établir la conclusion de la proposition.

4. Démonstration du théorème 3

Soient B un anneau commutatif, $A = B[t]$ la B-algèbre de polynômes en une variable t, et, pour tout entier $d \geq 0$, $A_{(d)}$ le B-module de ces polynômes de degré $\leq d$. Soit φ_d l'isomorphisme de $A_{(d)}$ sur B^{d+1} que transforme $f = a_0 + a_1 t + \ldots + a_d t^d$ en $(a_0, a_1, \ldots, a_d)$.

Soient p, q des entiers ≥ 0. Rappelons que, si $f \in A_{(p)}$ et $g \in A_{(q)}$, le résultant $R_{p,q}(f,g)$ est défini par

$$R_{p,q}(f,g) = \det \begin{pmatrix} \varphi(f) \\ \vdots \\ \varphi(t^{q-1}f) \\ \varphi(g) \\ \vdots \\ \varphi(t^{p-1}g) \end{pmatrix} \in B,$$

où $\varphi = \varphi_{p+q-1}$. Nous en utiliserons les propriétés suivantes, faciles à vérifier :

(1) $R_{p,q}(f,g) \in Af + Ag$.

(2) Si B est un corps, pour que $R_{p,q}(f,g) \neq 0$, il faut et il suffit que

(i) $Af + Ag = A$ (c'est-à-dire f et g n'ont pas de racine commune)

(ii) soit $\deg(f) = p$ soit $\deg(g) = q$.

LEMME 1.- Soit p un entier ≥ 0. Soient $f_1, \ldots, f_r \in A_{(p-1)}$ et f_{r+1} un polynôme unitaire de degré p. Posons $\mathfrak{a} = Af_1 + \ldots + Af_r + Af_{r+1}$.

(a) Si $\mathfrak{a} = A$ les coefficients de $f_1, \ldots, f_{r-1}$ et $R_{p-1,p}(f_r, f_{r+1})$ engen-

drent l'idéal B de B .

(b) Si les coefficients de $f_1,\dots,f_r$ engendrent l'idéal B de B , $\mathfrak{a}$ contient un polynôme unitaire de degré $p-1$.

(a) Modulo un idéal maximal de B contenant les coefficients de $f_1,\dots,f_{r-1}$, les polynômes f_r , f_{r+1} sont étrangers avec $\deg(f_{r+1}) = p$, donc $R_{p-1,p}(f_r, f_{r+1}) \neq 0$ d'après (2), d'où (a).

(b) Soit $\mathfrak{b}$ l'idéal de B formé des coefficients de t^{p-1} des éléments de $\mathfrak{a} \cap A_{(p-1)}$. Il suffit de montrer que $\mathfrak{b} = B$, et même que $\mathfrak{b}$ contient tous les coefficients de f_i $(1 \leq i \leq r)$. Or si $f_i = b_0 + b_1 t + \dots + b_{p-1}t^{p-1}$, on a $b_{p-1} \in \mathfrak{b}$ par définition. Si $f_{r+1} = a_0 + \dots + a_{p-1}t^{p-1} + t^p$, on a $f_i' = tf_i - b_{p-1}f_{r+1} = b_0' + b_1't + \dots + b_{p-1}'t^{p-1} \in \mathfrak{a} \cap A_{(p-1)}$ avec $b_j' \equiv b_{j-1} \mod. Bb_{p-1}$ $(0 \leq j \leq p-1)$. Par suite $b_{p-1}' = b_{p-2} - a_{p-1}b_{p-1} \in \mathfrak{b}$, donc $b_{p-2} \in \mathfrak{b}$, et, par une récurrence évidente, $b_{p-j} \in \mathfrak{b}$ pour tout $j = 1,\dots,p-1$, d'où l'assertion.

Soit $\ell : A \to B$ l'application définie par $\ell(0) = 0$ et $\ell(f) = a_p$ si $f = a_0 + a_1 t + \dots + a_p t^p$ avec $a_p \neq 0$. Les propriétés suivantes sont immédiates :

(3) Si $f, g \in A$ et $\ell(f)\ell(g) \neq 0$, on a $\ell(fg) = \ell(f)\ell(g)$.

(4) Si $\mathfrak{a}$ est un idéal de A , $\ell(\mathfrak{a})$ est un idéal de B contenant $\mathfrak{a} \cap B$ et on a $\ell(\mathfrak{a}) \subset \ell(\sqrt[A]{\mathfrak{a}}) \subset \sqrt[B]{\ell(\mathfrak{a})}$.

(5) Si $\mathfrak{a}$, $\mathfrak{a}'$ sont des idéaux de A , on a $\ell(\mathfrak{a})\ell(\mathfrak{a}') \subset \ell(\mathfrak{a}\mathfrak{a}')$ et $\ell(\mathfrak{a} \cap \mathfrak{a}') \subset \ell(\mathfrak{a}) \cap \ell(\mathfrak{a}')$.

LEMME 2.- Supposons que B soit noethérien. Pour tout idéal $\mathfrak{a}$ de A , on a

$$ht(\ell(\mathfrak{a})) \geq ht(\mathfrak{a}) .$$

Grâce à (4) on peut supposer $\mathfrak{a} = \sqrt[A]{\mathfrak{a}}$, de sorte que $\mathfrak{a} = \underline{P}_1 \cap \dots \cap \underline{P}_s$

où les $\underline{P}_i$ sont des idéaux premiers. Soit $\mathfrak{p}$ un idéal premier de B contenant $\ell(\mathfrak{a})$ tel que $ht(\mathfrak{p}) = ht(\ell(\mathfrak{a}))$. D'après (5), on a $\mathfrak{p} \supset \ell(\mathfrak{a}) \supset \ell(\underline{P}_1 \ldots \underline{P}_s) \supset \ell(\underline{P}_1) \ldots \ell(\underline{P}_s)$, d'où l'existence d'un i tel que $\mathfrak{p} \supset \ell(\underline{P}_i)$. Donc $ht(\mathfrak{p}) \geq ht(\ell(\underline{P}_i))$ et $ht(\underline{P}_i) \geq ht(\mathfrak{a})$. Il suffit alors de montrer que $ht(\ell(\underline{P}_i)) \geq ht(\underline{P}_i)$. Posons $\mathfrak{p}_i = \underline{P}_i \cap B$; on a $ht(\mathfrak{p}_i) = ht(\mathfrak{p}_i B) \leq ht(\underline{P}_i) \leq ht(\mathfrak{p}_i) + 1$ ([7], (13.B)), d'où l'assertion si $\underline{P}_i = \mathfrak{p}_i B$. Si $\underline{P}_i \neq \mathfrak{p}_i B$, alors $\ell(\underline{P}_i)$ est strictement plus grand que $\mathfrak{p}_i$, donc $ht(\ell(\underline{P}_i)) \geq 1 + ht(\mathfrak{p}_i) \geq ht(\underline{P}_i)$.

Pour tout entier $n \geq 0$, notons $A_n = B[t_1, \ldots, t_n]$ la B-algèbre de polynômes en n variables $t_1, \ldots, t_n$.

LEMME 3.- Supposons B noethérien de dimension d . Soit $n \geq 0$ et soit $\mathfrak{a}$ un idéal de A_n de hauteur $\geq d+1$. Il existe un changement de variables $(t_1, \ldots, t_n) \mapsto (u_1, \ldots, u_n)$ de la B-algèbre A_n tel que $\mathfrak{a}$ contienne un polynôme unitaire en u_n .

Si $n = 1$, il résulte du lemme 2 que $\ell(\mathfrak{a}) = B$, d'où l'assertion avec $u_1 = t_1$. Supposons $n > 1$ et posons $t = t_n$, de sorte que $A_n = A_{n-1}[t]$. Le lemme 2 et une hypothèse de récurrence nous permettent, après un changement de variables dans A_{n-1} , de supposer que $\ell(\mathfrak{a})$ contienne un polynôme f unitaire en t_1 , donc que $\mathfrak{a}$ contienne un polynôme de la forme

$$g = f_o + \ldots + f_{p-1} t^{p-1} + f t^p$$

avec les f_i dans A_{n-1} . Soit N un entier $> \deg_{t_1}(f_j)$ $(0 \leq j \leq p-1)$. Posons $u_1 = t - t_1^N$, $u_n = t_1$, et $u_i = t_i$ $(1 < i < n)$. Pour $j \leq p-1$, le degré en u_n de

$$f_j(t_1, \ldots, t_{n-1}) t^j = f_j(u_n, u_2, \ldots, u_{n-1})(u_1 + u_n^N)^j$$

est $\deg_{t_1}(f_j) + Nj$, ce qui est $<$ le degré en u_n de

$f(u_n, u_2, \ldots, u_{n-1})(u_1 + u_n^N)^p$, et ce dernier polynôme est unitaire en u_n car f est unitaire en t_1 . Donc g est un polynôme unitaire en u_n , d'où le lemme.

LEMME 4.- Supposons B noethérien de dimension d . Soit $n \geq 0$ et soit $f = (f_1, \ldots, f_{r+1}) \in Un_{r+1}(A_n)$. Si $r \geq 1 + d$, il existe $\varepsilon \in E_{r+1}(A_n)$ et un changement de variables $(t_1, \ldots, t_n) \mapsto (u_1, \ldots, u_n)$ dans la B-algèbre A_n tels que $\varepsilon f = g = (g_1, \ldots, g_{r+1})$ avec g_{r+1} unitaire en la variable u_n , et $\deg_{u_n}(g_j) < \deg_{u_n}(g_{r+1})$ $(1 \leq j \leq r)$.

Grâce aux lemmes 2 et 3 du n° 3, et à une transformation de f par un élément $E_{r+1}(A_n)$, on peut supposer que l'idéal $\mathfrak{a} = Af_1 + \ldots + Af_r$ est de hauteur $\geq r$. Quitte à changer les variables dans A_n , le lemme 3 nous permet, en plus, de supposer que $\mathfrak{a}$ contient un polynôme h unitaire en u_n . A l'aide d'un élément de $E_{r+1}(A_n)$, on peut remplacer f_{r+1} par $g_{r+1} = f_{r+1} + u_n^N h$, où N est choisi suffisamment grand pour que g_{r+1} soit unitaire en u_n . Ensuite, la division euclidienne des f_i $(1 \leq i \leq r)$ par g_{r+1} nous permet, grâce à des éléments de $E_{r+1}(A_n)$, de remplacer les f_i par des polynômes g_i de degrés $< \deg_{u_n}(g_{r+1})$ en u_n , d'où le lemme.

THÉORÈME 3'.- Soit B un anneau commutatif noethérien de dimension d . Pour tout $n \geq 0$, soit A_n la B-algèbre $B[t_1, \ldots, t_n]$ de polynômes en n variables $t_1, \ldots t_n$. Soient $n \geq 1$ et $m \geq 0$ des entiers et $f = (f_1, \ldots, f_{r+1}) \in Un_{r+1}(A_n)$. Si

$$r \geq 1 + \max\left(d, \frac{DS(A_{n-1})}{m+1}\right) ,$$

il existe $\varepsilon \in E_{r+1}(A_n)$ et un changement de variables $(t_1, \ldots, t_n) \mapsto (u_1, \ldots, u_n)$ dans la B-algèbre A_n tels que $\varepsilon f = g = (g_1, \ldots, g_{r+1})$ avec g_{r+1} unitaire

de degré m en la variable u_n et $\deg_{u_n}(g_j) < m$ $(1 \leq j \leq r)$.

Grâce au lemme 4, applicable car $r \geq 1 + d$, on peut supposer f_{r+1} unitaire en t_n , disons de degré p , et que $\deg_{t_n}(f_j) < p$ $(1 \leq j \leq r)$. Si $p \leq m$, la démonstration s'achève facilement. Supposons donc $p \geq m + 1$. Posons $t = t_n$, de sorte que $A_n = A_{n-1}[t]$, et posons $R = R_{p-1,p}(f_r, f_{r+1})$, le résultant de f_r et f_{r+1} par rapport à la variable t . Soit $v = (c_1,\ldots,c_{(r-1)p}, R) \in A_{n-1}^{(r-1)p+1}$ l'élément ayant pour premiers coefficients c_j les coefficients de $1, t,\ldots,t^{p-1}$ dans les polynômes $f_1,\ldots,f_{r-1}$. D'après le lemme 1 (a), on a $v \in Un_{(r-1)p+1}(A_{n-1})$. Or $(r-1) \geq \dfrac{DS(A_{n-1})}{m+1}$ et $p \geq m + 1$, donc $(r-1)p \geq DS(A_{n-1})$. Par suite, il existe $(c'_1,\ldots, c'_{(r-1)p}) \equiv (c_1,\ldots,c_{(r-1)p})$ mod. $A_{n-1}.R$ dans $Un_{(r-1)p}(A_{n-1})$. D'après (1), on a $R \in A_n f_r + A_n f_{r+1}$. Donc, à l'aide des éléments de $E_{r+1}(A_n)$, on peut ajouter aux f_j $(1 \leq j \leq r-1)$ des multiples de R , et ainsi se ramener au cas où les coefficients de $f_1,\ldots,f_{r-1}$ engendrent l'idéal A_{n-1} de A_{n-1} . On est donc en position d'appliquer le lemme 1 (b) aux polynômes $f_1,\ldots,f_{r-1}, f_{r+1}$ et l'on en déduit que l'idéal qu'ils engendrent contient un polynôme g unitaire en t de degré $p-1$. On peut ajouter un multiple de g à f_r pour obtenir un polynôme h_r qui est unitaire en t de degré $p-1$. Au moyen d'un élément de $E_{r+1}(A_n)$, on peut remplacer f_r par h_r . Ensuite, grâce encore à des éléments de $E_{r+1}(A_n)$, on peut effectuer la division euclidienne des autres polynômes par h_r pour obtenir finalement un élément $h = (h_1,\ldots,h_r, h_{r+1})$ où h_r est unitaire en t de degré $p-1$ et $\deg_t(h_j) < p-1$ pour $j \neq r$. Enfin, un élément de $E_{r+1}(A_n)$ transforme h en $(h_1,\ldots,h_{r-1}, -h_{r+1}, h_r)$. Le théorème résulte alors d'une récurrence sur p .

Considérons le cas $m = 1$ du théorème 3'. Dans ce cas, on a $g_{r+1} = t_n - h$ avec $h, g_1, \ldots, g_r \in A_{n-1}$. La rétraction $A_n \to A_{n-1}$ envoyant t_n sur h montre que $(g_1, \ldots, g_r) \in Un_r(A_{n-1})$, donc aussi $(g_1, \ldots, g_r) \in Un_r(A_n)$. Il résulte donc du lemme 1 du n° 2 qu'il existe $\delta \in E_{r+1}(A_n)$ tel que $\delta g = (1, 0, \ldots, 0)$. On déduit ainsi le théorème 3 du théorème 3'.

5. Démonstration du théorème 4

Soit A un anneau commutatif. Soit e_1, e_2, e_3 la base habituelle de A^3 et posons $e = e_1 \wedge e_2 \wedge e_3 \in \Lambda^3 A^3$. Si $a = (a_1, a_2, a_3) = a_1 e_1 + a_2 e_2 + a_3 e_3 \in A^3$, posons $e_a = a_1(e_2 \wedge e_3) - a_2(e_1 \wedge e_3) + a_3(e_2 \wedge e_3) \in \Lambda^2 A^3$. Pour tout $x = (x_1, x_2, x_3) \in A^3$, nous avons

$$e_a \wedge x = (a \,.\, x)e$$

où $a \,.\, x = a_1 x_1 + a_2 x_2 + a_3 x_3$. Posons

$$P_a = \mathrm{Ker}(x \mapsto a \,.\, x) = \mathrm{Ker}(x \mapsto e_a \wedge x) .$$

LEMME 1.- Si $a \in Un_3(A)$ l'élément e_a est unimodulaire dans $\Lambda^2 A^3$, $A^3 = P_a \oplus Ab$ pour tout b tel que $a.b = 1$, et $\Lambda^2 P_a = Ae_a \subset \Lambda^2 A^3$.

Seule l'égalité $\Lambda^2 P_a = Ae_a$ mérite une démonstration. On voit par localisation que $\Lambda^2 P_a$ est l'orthogonal de P_a pour la forme bilinéaire $\wedge : A^3 \times \Lambda^2 A^3 \to \Lambda^3 A^3$. Par suite e_a, étant un élément unimodulaire dans le module $\Lambda^2 P_a$ de rang 1, engendre ce module.

Si $a \in Un_3(A)$, soit (P_a, h_a) le module symplectique défini par $x \wedge y = h_a(x,y)e_a$ pour $x, y \in P_a$. Par rapport à une base convenable de $(P_a, h_a) \oplus H(A)$, la forme symplectique est représentée par une matrice

$$\begin{pmatrix} 0 & b_3 & -b_2 & -a_1 \\ -b_3 & 0 & b_1 & -a_2 \\ b_2 & -b_1 & 0 & -a_3 \\ a_1 & a_2 & a_3 & 0 \end{pmatrix} \qquad \text{de Pfaffien } a_1b_1 + a_2b_2 + a_3b_3 = 1 .$$

Notons Σ la classe des A-modules symplectiques (P,h) tels que $P \oplus A \cong A^3$. Notons $((P,h))$ la classe d'isomorphie de (P,h) et (Σ) l'ensemble des $((P,h))$ où (P,h) parcourt Σ .

THÉORÈME 4'.- L'application $a \mapsto (P_a, h_a)$ de $Un_3(A)$ dans Σ induit une bijection

$$\psi : SL_3(A) \backslash Un_3(A) \to (\Sigma) .$$

(i) ψ est bien défini. Soient $a \in Un_3(A)$, $\alpha \in GL_3(A)$, et $a' = \alpha(a)$. On définit α^* par $\alpha x.y = x.\alpha^* y$ pour tout x , $y \in A^3$. De la formule $a'.x = \alpha a.x = a.\alpha^* x$, on déduit que α^* induit un isomorphisme de $P_{a'}$ sur P_a , donc (lemme 1) $\Lambda^2\alpha^*(e_{a'}) = de_a$ pour un certain $d \in A$. On a, pour tout $x \in A^3$,

$$\begin{aligned} d(a.x)e &= de_a \wedge x = \Lambda^2\alpha^*(e_{a'}) \wedge x \\ &= \Lambda^3\alpha^*(e_{a'} \wedge \alpha^{*-1}x) = \det(\alpha^*)(a'.\alpha^{*-1}x)e \\ &= \det(\alpha^*)(a.x)e , \end{aligned}$$

donc $d = \det(\alpha^*) = \det(\alpha)$. Par suite si $\det(\alpha) = 1$, α^* induit un isomorphisme $(P_{a'}, h_{a'}) \to (P_a, h_a)$.

(ii) ψ est injectif. Soient a , $a' \in Un_3(A)$ et $\gamma : (P_{a'}, h_{a'}) \to (P_a, h_a)$ un isomorphisme, de sorte que $\Lambda^2\gamma(e_{a'}) = e_a$. Choisissons b , $b' \in A^3$ tels que $a.b = 1 = a'.b'$ et prolongeons γ en un isomorphisme de $A^3 = P_{a'} \oplus Ab'$ sur $A^3 = P_a \oplus Ab$ tel que $\gamma(b') = b$. Pour tout $x \in A^3$, on a

$$\begin{aligned} \det(\gamma)(a'.x)e &= \Lambda^3(\gamma)(e_{a'} \wedge x) \\ &= \Lambda^2\gamma(e_{a'}) \wedge \gamma x = e_a \wedge \gamma x = (a.\gamma x)e . \end{aligned}$$

Prenant $x = b'$, on trouve que $\det(\gamma) = 1$, et par suite $a'.x = a.\gamma x = \gamma^*(a).x$ pour tout $x \in A^3$, d'où $\gamma^*(a) = a'$.

(iii) ψ est surjectif. Soit $(P,h) \in \Sigma$. On peut supposer P facteur direct de A^3 . Soit δ un générateur de $\Lambda^2 P$ tel que $x \wedge y = h(x,y)\delta$ pour tout $x , y \in P$. Alors, il est clair que $\delta = e_a$ pour un certain $a \in Un_3(A)$, donc $(P,h) = (P_a , h_a)$.

Le théorème 4 résulte maintenant du théorème 4' et de la proposition suivante :

PROPOSITION 5.- Supposons que $E_{r+1}(A)$ opère transitivement sur $Un_{r+1}(A)$ pour tout $r \geq 3$. Alors l'application $\psi' : ((P,h)) \mapsto [P,h]$ de (Σ) dans $W(A)$ est bijective.

L'hypothèse entraîne que les A-modules stablement libres de rang ≥ 3 sont libres. Il résulte alors de la prop. 2, et du fait qu'un module symplectique est toujours de rang pair, que ψ' est surjectif. Pour montrer que ψ' est injectif, il suffit, comme on le voit facilement, de montrer que, pour tout $r \geq 2$, si (A^{2r},h) est un module symplectique, son groupe d'automorphismes $Sp(A^{2r},h)$ opère transitivement sur l'ensemble de ses "plans hyperboliques" (= sous-modules symplectiques isomorphes à $H(A)$). D'après [4], ch. I, cor. (5.6), il suffit même de montrer que $Sp(A^{2r},h)$ opère transitivement sur $Un_{2r}(A)$. Ainsi on se ramène à la proposition frappante de Vaserštein suivante :

PROPOSITION 6.- Soient A un anneau commutatif et (A^{2r},h) un A-module symplectique. Si $E_{2r}(A)$ opère transitivement sur $Un_{2r}(A)$, il en est de même pour $Sp(A^{2r},h)$.

Pour la démonstration nous avons besoin de quelques notations. Si $M = M_1 \oplus M_2$ est un A-module décomposé en somme directe, notons $E(M_1,M_2)$ le sous-groupe de $GL(M)$ engendré par

$$\begin{pmatrix} 1_{M_1} & \mathrm{Hom}(M_2,M_1) \\ 0 & 1_{M_2} \end{pmatrix} \quad \cup \quad \begin{pmatrix} 1_{M_1} & 0 \\ \mathrm{Hom}(M_1,M_2) & 1_{M_2} \end{pmatrix} .$$

Par exemple, si $e_1,\ldots,e_{r+1}$ désigne la base habituelle de A^{r+1}, on voit facilement que $E_{r+1}(A) = E(A^r, Ae_{r+1})$.

Soit $(M, \langle\ ,\ \rangle)$ un A-module symplectique. Pour tout u , $v \in M$ tels que $\langle u,v\rangle = 0$ et pour tout $c \in A$, l'application

$$\sigma_{u,c,v} : x \longmapsto x + \langle u,x\rangle v + \langle v,x\rangle u + \langle u,x\rangle cu$$

appartient à $Sp(M, \langle\ ,\ \rangle)$ (cf. [4], p. 91). Remarquons que $\sigma_{u,c,v} = \sigma_{u,o,v} \circ \sigma_{u,c,o}$. Supposons que M soit somme directe orthogonale d'un sous-module P et d'un plan hyperbolique $H(e,f)$ engendré par un couple hyperbolique e,f : $\langle f,e\rangle = 1$. Notons $Ep(P,H(e,f))$ le sous-groupe de $Sp(M, \langle\ ,\ \rangle)$ engendré par tous les éléments $\sigma_{u,c,v}$ ($c \in A$, $v \in P$, $u = e$ ou f). La prop. 6 se précise ainsi :

PROPOSITION 6'.- Les orbites $E(P \oplus Ae, Af).f$ et $Ep(P, H(e,f)).f$ coïncident.

Remarquons d'abord que $Ep(P,H(e,f)) \subset E(P \oplus Ae, Af)$, comme on le voit facilement. Si $\alpha \in GL(P \oplus Ae)$ nous l'identifierons avec $\alpha \oplus 1_{Af} \in GL(M)$. Ainsi $GL(P \oplus Ae)$ fixe f et normalise l'ensemble

$$S = \begin{pmatrix} 1 & \mathrm{Hom}(Af, P \oplus Ae) \\ 0 & 1 \end{pmatrix} \cup \begin{pmatrix} 1 & 0 \\ \mathrm{Hom}(P \oplus Ae, Af) & 1 \end{pmatrix}$$

qui engendre $E(P \oplus Ae, Af)$. Il suffit de montrer (par récurrence sur m) que si $f' \in M$ et $\varepsilon_1,\ldots,\varepsilon_m \in S$ sont tels que $\varepsilon_1 \ldots \varepsilon_m f' = f$, alors il existe $\sigma \in Ep(P,H(e,f))$ tel que $\sigma f' = f$. Nous utiliserons le lemme suivant, qui sera démontré plus loin :

LEMME 2.- Si $\varepsilon \in S$, il existe $\alpha \in E(P,Ae)$ tel que $\alpha\varepsilon \in Ep(P,H(e,f))$.

L'assertion faite plus haut est claire si $m = 0$. Si $m > 0$, le lemme 2

fournit un $\alpha \in E(P,Ae)$ tel que $\sigma_m = \alpha\varepsilon_m$ appartient à $Ep(P,H(e,f))$. Posons $\varepsilon'_i = \alpha\varepsilon_i\alpha^{-1} \in S$ $(1 \leq i \leq m-1)$. On a $f = \alpha f = \alpha\varepsilon_1 \ldots \varepsilon_m f' = \varepsilon'_1 \ldots \varepsilon'_{m-1}\sigma_m f'$. L'hypothèse de récurrence fournit un $\sigma' \in Ep(P,H(e,f))$ tel que $\sigma'\sigma_m f' = f$, d'où l'assertion en prenant $\sigma = \sigma'\sigma_m$.

Démontrons maintenant le lemme 2. Si $(v,c) \in P \times A$, introduisons

$$\varepsilon_{(v,c)} : x = p + ae + bf \longmapsto x + b(v + ce) = x + \langle -e,x\rangle(v + ce)$$

et

$$\delta_{(v,c)} : x \longmapsto x + (ac + \langle v,p\rangle)f = x + \langle cf + v , x\rangle f .$$

Ces éléments constituent l'ensemble S . Définissons α_v , $\beta_v \in E(P,Ae)$ par $\alpha_v(x) = x - \langle v,x\rangle e$ et $\beta_v(x) = x + \langle f,x\rangle v$. On vérifie alors facilement les formules suivantes, qui entraînent le lemme 2 :

$$\alpha_v\, \varepsilon_{(v,c)} = \sigma_{-e,-c,v} = \sigma^{-1}_{e,c,v}$$

$$\beta_v\, \delta_{(v,c)} = \sigma_{f,c,v} .$$

6. Démonstration du théorème 5

Soit A un anneau commutatif. Notons, pour tout entier $n \geq 1$, S_{2n} (ou $S_{2n}(A)$) l'ensemble des matrices alternées inversibles à 2n lignes à coefficients dans A . Parmi elles se trouve

$$H_{2n} = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} .$$

Le groupe $GL_{2n}(A)$ opère sur S_{2n} par $\alpha : \sigma \longmapsto \alpha\sigma\alpha^*$. On a de plus l'opération de somme directe $\oplus : S_{2n} \times S_{2m} \to S_{2(n+m)}$. Posons $S = \bigcup_n S_{2n}$. Si $\sigma \in S_{2n}$ et $\sigma' \in S_{2n'}$, désignons par $\sigma \sim \sigma'$ la relation :

" il existe des entiers m , $m' \geq 0$ tels que $n + m = n' + m'$ et un élément α de $GL_{2(n+m)}(A)$ tel que $\alpha(\sigma \oplus H_{2m})\alpha^* = \sigma' \oplus H_{2m'}$ ".

C'est une relation d'équivalence, et il est évident que $S/\sim$ s'identifie au groupe $W(A)$ du théorème 5 (affirmant que $W(A) \to W(A[t])$ est un isomorphisme lorsque $\frac{1}{2} \in A$). La rétraction $A[t] \to A$ montre que $W(A) \to W(A[t])$ est injectif. Pour montrer que c'est surjectif, soit σ un élément de $S_{2n}(A[t])$. Cherchons un m et un élément $\tau \in S_{2m}(A)$ tel que $\sigma \sim \tau$.

Ecrivons $\sigma = \sigma_0 + \sigma_1 t + \ldots + \sigma_d t^d$, $\sigma_d \neq 0$, où les matrices alternées σ_i sont à coefficients dans A . Posons $d = \deg(\sigma)$ et montrons d'abord que σ est équivalent à un σ' de degré ≤ 1 . Supposons donc que $d \geq 2$ et raisonnons par récurrence sur d . Quitte à remplacer σ par $\sigma \oplus H_{2n}$, on peut supposer σ_d de la forme

$$\sigma_d = \begin{pmatrix} \sigma'_d & 0 \\ 0 & 0 \end{pmatrix} .$$

La matrice alternée σ'_d s'exprime sous la forme $\mu - \mu^*$ pour une certaine matrice μ . Posons $d = 2e + j$, où $j = 0$ ou 1 , $\beta = \begin{pmatrix} I & \mu t^j \\ 0 & 0 \end{pmatrix}$, et $\alpha = \begin{pmatrix} I & \beta t^e \\ 0 & I \end{pmatrix} \in E_{4n}(A[t])$. Alors

$$\alpha(\sigma \oplus H_{2n})\alpha^* = \begin{pmatrix} I & \beta t^e \\ 0 & I \end{pmatrix}\begin{pmatrix} \sigma & 0 \\ 0 & H_{2n} \end{pmatrix}\begin{pmatrix} I & 0 \\ \beta^* t^e & I \end{pmatrix}$$

$$= \begin{pmatrix} \sigma + \beta H_{2n}\beta^* t^{2e} & \beta H_{2n} t^e \\ H_{2n}\beta^* t^e & H_{2n} \end{pmatrix} \quad \underline{\underline{\text{def}}} \quad \sigma'$$

et

$$\beta H_{2n}\beta^* = \begin{pmatrix} I & \mu t^j \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\begin{pmatrix} I & 0 \\ \mu^* t^j & 0 \end{pmatrix} = \begin{pmatrix} (\mu^* - \mu)t^j & 0 \\ 0 & 0 \end{pmatrix} = -\sigma_d t^j ,$$

de sorte que $\sigma + \beta H_{2n}\beta^* t^{2e} = \sigma - \sigma_d t^d$ est de degré $\leq d-1$. Par suite σ est équivalent à l'élément $\sigma' \in S_{4n}(A[t])$ de degré $\leq d-1$, d'où l'assertion par l'hypothèse de récurrence.

On est donc ramené au cas où $\sigma = \sigma_o + \sigma_1 t$. Quitte à remplacer σ par $\sigma \oplus (-\sigma_o)$ et à le transformer par un élément de $GL_{4n}(A)$, on peut supposer que $\sigma_o = H_{2n}$, que nous noterons simplement H . On a

$$\sigma = H + \sigma_1 t = H(I + \nu t)$$

où $\nu = H^{-1}\sigma_1 = -H\sigma_1$ est nilpotent, car la matrice $I + \nu t$ a pour inverse $\sum_{i \geq 0} (-\nu t)^i$, qui est un polynôme en t . Pour achever la démonstration, il suffit de trouver un $\alpha \in GL_{2n}(A[t])$ tel que $\alpha^* \sigma \alpha = H$. On prend

$$\alpha = (I + \nu t)^{-\frac{1}{2}} = \sum_{i \geq 0} \binom{-\frac{1}{2}}{i} (\nu t)^i ,$$

qui existe car ν est nilpotent et $\frac{1}{2} \in A$. On a $\sigma_1 = H\nu$, donc $-\sigma_1 = \sigma_1^* = \nu^* H^* = -\nu^* H$, d'où $\nu^* H = H\nu$. Par suite $\alpha^* H = H\alpha$ et donc $\alpha^* \sigma \alpha = \alpha^* H(I + \nu t)\alpha = H\alpha(I + \nu t)\alpha = H$, d'où le théorème.

BIBLIOGRAPHIE

[1] H. BASS - Big projective modules are free, Ill. J. Math., 7 (1963), 24-31.

[2] H. BASS - K-theory and stable algebra, Publ. I.H.E.S., n° 22 (1964), 5-60.

[3] H. BASS - Algebraic K-theory, W. A. Benjamin, New York (1968).

[4] H. BASS - Unitary algebraic K-theory, Proc. Battelle Conf. on algebraic K-theory, vol. III, Springer, Lecture Notes n° 343.

[5] H. BASS, J. MILNOR, J.-P. SERRE - Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \leq 2$), Publ. I.H.E.S., n° 33 (1967), 59-137.

[6] M. KAROUBI - Périodicité de la K-théorie hermitienne, Proc. Battelle Conf. on algebraic K-theory, vol. III, Springer, Lecture Notes n° 343.

[7] H. MATSUMURA - Commutative algebra, W. A. Benjamin, New York (1970).

[8] M. OJANGUREN, R. SRIDHARAN - Cancellation of Azumaya algebras, J. Alg., 18(1971), 501-505.

[9] B. SEGRE - Intersezioni complete di due ipersuperficie algebriche in uno spazio affine, et non estendibilita di un theorema di Seshadri, Rev. Roum. Math. Pures et Appl., 9 (1970), 1527-1534.

[10] C. S. SESHADRI - Triviality of vector bundles over the affine space K^2, Proc. Natl. Acad. Sci. USA, 44 (1958). 456-458.

[11] J.-P. SERRE - Faisceaux algébriques cohérents, Ann. Math., 61 (1955), 197-278.

[12] J.-P. SERRE - Modules projectifs et espaces fibrés à fibre vectorielle, Sém. Dubreil, n° 23 (1957/58).

[13] J.-P. SERRE - Sur les modules projectifs, Sém. Dubreil, n° 2 (1960/61).

[14] L. N. VASERŠTEIN - Stable rank of rings and dimensionality of topological spaces.

Bibliographie - Complèments

M. P. MURTHY and J. TOWBER - Algebraic vector bundles on $\mathbb{A}^3$ are trivial, Inv. Math., ..., (1974).

M. ROITMAN - On Serre's problem on projective modules, à paraître.

R. G. SWAN - A cancellation theorem for projective modules in the metastable range, à paraître.

A. A. SUSLIN et L. VASERŠTEIN - Le problème de Serre sur les modules projectifs sur les anneaux de polynômes, et la K-théorie algébrique, Journal d'analyse fonctionnelle, t. 8 (1974), 65-66, [en russe].