

## §2. COGÈBRES SUR UN CORPS

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **39 (1993)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.04.2024**

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

### **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

D'autre part, l'axiome (2) de la déf. 1 montre que  $V^o$  est contenu dans  $(e \otimes 1_E)(C \otimes V)$ , donc dans  $V$ . Enfin, il est clair que tout sous-comodule de  $E$  contenu dans  $V$  est contenu dans  $V^o$ , cqfd.

Nous dirons qu'un comodule est de *type fini* (resp. libre, projectif, ...) si c'est un  $K$ -module de type fini (resp. un  $K$ -module libre, un  $K$ -module projectif, ...).

**COROLLAIRE.** *Supposons  $K$  noethérien. Tout comodule  $E$  est alors réunion filtrante croissante de ses sous-comodules de type fini.*

Il suffit évidemment de prouver ceci: si  $W$  est un sous-module de type fini de  $E$ , il existe un sous-comodule de  $E$ , qui est de type fini et contient  $W$ . Or  $d_E(W)$  est un sous-module de type fini de  $C \otimes E$ . On peut donc trouver un sous-module  $V$  de type fini de  $E$  tel que  $C \otimes V$  contienne  $d_E(W)$ . Soit  $V^o$  l'ensemble des  $x \in E$  tels que  $d_E(x) \in C \otimes V$ . D'après la proposition,  $V^o$  est un sous-comodule de  $E$  contenu dans  $V$ , donc de type fini (puisque  $K$  est noethérien). Il est clair que  $V^o$  contient  $W$ , cqfd.

## §2. COGÈBRES SUR UN CORPS

A partir de maintenant, l'anneau de base  $K$  est un *corps*.

### 2.1. SOUS-COGÈBRES

Soit  $C$  une cogèbre sur  $K$ , de coproduit  $d$  et de co-unité  $e$ .

**DÉFINITION 1.** *Un sous-espace vectoriel  $X$  de  $C$  est appelé une sous-cogèbre de  $C$  si  $d(X)$  est contenu dans  $X \otimes X$ .*

S'il en est ainsi, l'application linéaire  $d_X: X \rightarrow X \otimes X$  induite par  $d$  munit  $X$  d'une structure de cogèbre, ayant pour co-unité la restriction de  $e$  à  $X$ .

#### *Exemples*

1) Si  $(X_i)_{i \in I}$  est une famille de sous-cogèbres de  $C$ , la somme des  $X_i$  et l'intersection des  $X_i$  sont des sous-cogèbres de  $C$ . Cela se vérifie au moyen des formules:

$$\begin{aligned} \sum (X_i \otimes X_i) &\subset (\sum X_i) \otimes (\sum X_i) \\ \cap (X_i \otimes X_i) &= (\cap X_i) \otimes (\cap X_i) . \end{aligned}$$

2) Une sous-cogèbre de rang 1 (sur  $K$ ) de  $C$  a pour base un élément non nul  $x$  tel que  $d(x) = x \otimes x$ ; on a alors  $e(x) = 1$ .

3) Si  $D$  est une cogèbre, et si  $f: D \rightarrow C$  est un morphisme de cogèbres,  $f(D)$  est une sous-cogèbre de  $C$ .

4) Soit  $E$  un comodule sur  $C$ , soit  $(v_i)_{i \in I}$  une base de  $E$ , et soient  $c_{ij} \in C$  tels que  $d_E(v_i) = \sum c_{ij} \otimes v_j$ , cf. n° 1.2, Remarque 3. Il résulte de la formule (1') du n° 1.2 que le sous-espace vectoriel  $C_E$  engendré par les  $c_{ij}$  est une sous-cogèbre de  $C$ . Cette sous-cogèbre ne dépend pas du choix de la base  $(v_i)$ , car c'est l'image de l'application  $E \otimes E' \rightarrow C$  associée à  $d_E$  (cf. n° 1.2, Remarque 2). On peut aussi caractériser  $C_E$  comme le plus petit sous-espace vectoriel  $X$  de  $C$  tel que  $\text{Im}(d_E) \subset X \otimes E$ .

Noter que, si  $D$  est une sous-cogèbre de  $C$  contenant  $C_E$ , le coproduit  $d_E$  applique  $E$  dans  $D \otimes E$ , donc munit  $E$  d'une structure de  $D$ -comodule; inversement, tout  $D$ -comodule peut évidemment être considéré comme un  $C$ -comodule.

5) On peut appliquer la construction précédente en prenant pour  $E$  un sous-comodule de  $C$ . Dans ce cas, la sous-cogèbre  $C_E$  contient  $E$ . En effet,  $C_E$  est l'image de  $E \otimes E' \rightarrow C$ ; d'autre part la restriction de  $e$  à  $E$  est un élément  $e_E$  de  $E'$  et l'on vérifie tout de suite que, si  $x \in E$ , l'image de  $x \otimes e_E$  dans  $C$  est égale à  $x$ .

6) Supposons  $C$  de rang fini (sur  $K$ ), et soit  $A$  l'algèbre duale (cf. n° 1.1, Exemple 3). Les sous-cogèbres de  $C$  correspondent bijectivement (par dualité) aux algèbres quotients de  $A$  (donc aussi aux idéaux bilatères de  $A$ ).

**THÉOREME 1.** *La cogèbre  $C$  est réunion filtrante croissante de ses sous-cogèbres de rang fini.*

Il suffit de prouver que tout sous-espace vectoriel  $W$  de rang fini de  $C$  est contenu dans une sous-cogèbre de rang fini. Or, d'après le corollaire à la prop. 3 du n° 1.4, il existe un sous-comodule  $E$  de  $C$  qui est de rang fini et contient  $W$ . La sous-cogèbre  $C_E$  associée à  $E$  (cf. Exemple 4) répond à la question: elle est évidemment de rang fini, et elle contient  $E$  (cf. Exemple 5), donc  $W$ . Cqfd.

## 2.2. DUALITÉ ENTRE COGÈBRES ET ALGÈBRES PROFINIES

**DÉFINITION 2.** *On appelle algèbre profinie une algèbre topologique séparée, complète, possédant une base de voisinages de 0 formée d'idéaux bilatères de codimension finie.*

Il revient au même de dire qu'une telle algèbre est limite projective filtrante d'algèbres de rang fini; d'où le nom de «profini».

Soit maintenant  $C$  une cogèbre, et soit  $A = C'$  son dual. La structure de cogèbre de  $C$  définit sur  $A$  une structure d'algèbre (cf. Alg. III); d'autre part, on peut munir  $A$  de la topologie de la convergence simple sur  $C$  ( $K$  étant lui-même muni de la topologie discrète).

PROPOSITION 1. (a) *L'algèbre topologique  $A = C'$  est une algèbre profinie. Les idéaux bilatères ouverts de  $A$  sont les orthogonaux des sous-cogèbres de rang fini de  $C$ .*

(b) *Inversement, toute algèbre profinie qui est associative et possède un élément unité est la duale d'une cogèbre possédant une co-unité, définie à isomorphisme unique près.*

Pour prouver (a), on remarque que  $C = \varinjlim X$ , où  $X$  parcourt l'ensemble ordonné filtrant des sous-cogèbres de  $C$  de rang fini (cf. th. 1). On a alors  $A = \varprojlim X'$  et les  $X'$  sont des algèbres de rang fini. Le noyau de  $A \rightarrow X'$  est l'orthogonal  $\alpha_X$  de  $X$  dans  $A$ ; c'est un idéal bilatère ouvert de codimension finie. Inversement, soit  $\alpha$  un tel idéal de  $A$ , et soit  $X$  son orthogonal dans  $C$ . On a  $X = (A/\alpha)'$ ; la structure d'algèbre de  $A/\alpha$  définit sur  $X$  une structure de cogèbre, et on en déduit que  $X$  est une sous-cogèbre de  $C$ .

L'assertion (b) est tout aussi évidente.

La correspondance «cogèbres  $\Leftrightarrow$  algèbres profinies» établie ci-dessus se prolonge en une correspondance «comodules  $\Leftrightarrow$  modules». De façon précise, soient

$\text{Com}_C^f$  la catégorie des  $C$ -comodules à gauche de rang fini,

$\text{Mod}_A^f$  la catégorie des  $A$ -modules à gauche de rang fini, dont l'anneau est ouvert (i.e. qui sont des  $A$ -modules topologiques si on les munit de la topologie discrète).

Si  $E \in \text{Com}_C^f$ , l'application  $E \rightarrow C \otimes E$  définit par dualité une application  $A \otimes E' \rightarrow E'$ , et l'on voit tout de suite que cette application fait de  $E'$  un  $A$ -module à gauche topologique discret.

PROPOSITION 2. *Le foncteur  $E \mapsto E'$  défini ci-dessus est une équivalence de la catégorie  $\text{Com}_C^f$  sur la catégorie opposée à  $\text{Mod}_A^f$ .*

C'est immédiat.

Noter aussi que, si  $F$  est un  $A$ -module à gauche de rang fini,  $F'$  a une structure naturelle de  $A^0$ -module à gauche. En combinant cette remarque avec la prop. 2, on obtient:



COROLLAIRE. La catégorie  $\text{Com}_C^f$  est isomorphe à la catégorie  $\text{Mod}_{A^o}^f$ .

*Remarque.* Soit  $E \in \text{Com}_C^f$ ; munissons  $E'$  (resp.  $E$ ) de la structure correspondante de  $A$ -module à gauche (resp. à droite). Si  $x \in E$ ,  $x' \in E'$  et  $a, b \in A$ , on a alors les formules:

$$(1) \quad \langle d_E(x), a \otimes x' \rangle = \langle x, ax' \rangle = \langle xa, x' \rangle$$

et

$$(2) \quad \langle d_E^{(2)}(x), a \otimes b \otimes x' \rangle = \langle x, abx' \rangle = \langle xab, x' \rangle,$$

avec

$$d_E^{(2)} = (d \otimes 1_E) \circ d_E = (1_C \otimes d_E) \circ d_E.$$

### 2.3. TRADUCTIONS

Tout résultat sur les modules donne, grâce à la prop. 2 et à son corollaire, un résultat correspondant sur les comodules. Voici quelques exemples:

a) Si  $E \in \text{Com}_C^f$ , la sous-cogèbre  $C_E$  de  $C$  attachée à  $E$  (cf. n° 2.1) est la duale de la sous-algèbre de  $\text{End}(E)$  définie par la structure de module de  $E$ .

b) Le fait que  $C$  soit un  $C$ -comodule injectif (cf. n° 1.4) est la traduction du fait que  $A$  est un  $A$ -module projectif (puisque libre de rang 1!).

c) Une cogèbre est dite *simple* si elle est  $\neq 0$  et n'admet pas d'autre sous-cogèbre que 0 et elle-même; c'est alors le dual d'une algèbre simple de rang fini. Elle est dite *semi-simple* si elle est somme de sous-cogèbres simples, et on vérifie alors que l'on peut choisir cette somme de telle sorte qu'elle soit *directe*.

On a:

PROPOSITION 3. Pour que  $\text{Com}_C^f$  soit une catégorie semi-simple, il faut et il suffit que  $C$  soit semi-simple.

De plus, si c'est le cas, et si  $E_\alpha$  est une famille de représentants des classes de comodules simples sur  $C$ , la cogèbre  $C$  est somme directe des cogèbres  $C_{E_\alpha}$ , qui sont simples.

On a également:

COROLLAIRE. Les conditions suivantes sont équivalentes:

a)  $C$  est somme directe de cogèbres de la forme  $\mathbf{M}_n(K)$ .

b)  $\text{Com}_C^f$  est semi-simple, et tout objet simple de  $\text{Com}_C^f$  est absolument simple.

C'est trivial à partir du résultat analogue pour les algèbres.

[Noter que ce résultat s'applique notamment à la bigèbre d'un groupe réductif déployé sur  $K$ , lorsque  $\text{car}(K) = 0$ . Mais, bien entendu, il ne donne que la structure de *cogèbre* de la bigèbre en question, pas sa structure d'algèbre.]

d) A tout  $E \in \text{Com}_C^f$  on peut associer un élément *trace*  $\theta_E \in C$  de la manière suivante:  $E$  définit un morphisme de cogèbres

$$\text{End}(E) \rightarrow C \quad (\text{cf. n}^\circ 1.2)$$

et l'on prend l'image de  $1_E$  dans  $C$  par ce morphisme. En termes d'une base  $(v_i)$  de  $E$ , et des  $c_{ij} \in C$  correspondants (*loc. cit.*), on a  $\theta_E = \sum_i c_{ii}$ .

[Voici encore une autre définition: si l'on regarde  $E$  comme module sur l'algèbre  $C'_E$  duale de  $C_E$ , on a  $C'_E \subset \text{End}(E)$ , et la forme  $u \mapsto \text{Tr}(u)$ , étant une forme linéaire sur  $C'_E$ , s'identifie à un élément de  $C_E$  qui n'est autre que  $\theta_E$ .]

PROPOSITION 4. *Supposons  $K$  de caractéristique 0. Soient  $E_1$  et  $E_2$  deux comodules de rang fini, et soient  $\theta_1, \theta_2 \in C$  les traces correspondantes. On a  $\theta_1 = \theta_2$  si et seulement si les quotients de Jordan-Hölder de  $E_1$  et  $E_2$  coïncident (avec leurs multiplicités).*

En effet, le résultat dual (pour les modules de rang fini sur une algèbre) est bien connu (Alg. VIII).

COROLLAIRE. *Si  $E_1$  et  $E_2$  sont semi-simples, on a  $\theta_1 = \theta_2$  si et seulement si  $E_1$  et  $E_2$  sont isomorphes.*

### Remarques

1) On peut aussi donner des résultats lorsque  $\text{car}(K) \neq 0$ . Par exemple, si les  $E_\alpha$  sont des comodules absolument simples deux à deux non isomorphes, les  $\theta_\alpha$  correspondants sont linéairement indépendants sur  $K$ .

2) Les résultats précédents s'appliquent notamment aux *représentations linéaires* d'un schéma en groupes (ou en monoïdes) affine sur  $K$ .

## 2.4. CORRESPONDANCE ENTRE SOUS-COGÈBRES ET SOUS-CATÉGORIES DE $\text{Com}_C^f$ .

Si  $D$  est une sous-cogèbre de  $C$ , on a déjà remarqué que tout  $D$ -comodule peut être considéré comme un  $C$ -comodule. On obtient ainsi un isomorphisme de  $\text{Com}_D^f$  sur une sous-catégorie abélienne  $\tilde{D}$  de  $\text{Com}_C^f$ .

THÉORÈME 2. *L'application  $D \mapsto \tilde{D}$  est une bijection de l'ensemble des sous-cogèbres de  $C$  sur l'ensemble des sous-catégories  $L$  de  $\text{Com}_C^f$  vérifiant les conditions suivantes:*

- 1)  *$L$  est pleine (i.e. si  $E, F \in L$ , on a  $\text{Hom}^L(E, F) = \text{Hom}^C(E, F)$ ),*
- 2)  *$L$  est stable par sommes directes finies,*
- 3) *Tout objet de  $\text{Com}_C^f$  qui est isomorphe à un sous-objet, ou à un objet quotient, d'un objet de  $L$ , appartient à  $L$ .*

[On se permet d'écrire  $E \in L$  à la place de  $E \in \text{ob}(L)$ .]

Soit  $\Theta$  l'ensemble des  $L$  vérifiant les conditions 1), 2), 3). Si  $L \in \Theta$ , il est clair que  $L$  est une catégorie abélienne ayant même sous-objets et mêmes objets quotients que  $\text{Com}_C^f$ . On notera  $C(L)$  la sous-cogèbre de  $C$  somme des cogèbres  $C_E$ , pour  $E \in L$ . Le théorème va résulter des deux formules suivantes:

- a)  $C(\tilde{D}) = D$  pour toute sous-cogèbre  $D$  de  $C$ ;
- b)  $C(L)^\sim = L$  pour toute  $L \in \Theta$ .

La première de ces deux formules est triviale: elle revient à dire que  $D$  est réunion des sous-cogèbres  $C_E$ , lorsque  $E$  parcourt l'ensemble (!) des  $D$ -comodules de rang fini, ce qui a été prouvé au n° 2.1. Pour la seconde, il suffit de prouver ceci:

LEMME 1. *Soit  $E$  un comodule de rang fini, soit  $C_E \subset C$  la cogèbre correspondante, et soit  $F$  un  $C_E$ -comodule (considéré comme  $C$ -comodule) de rang fini. Il existe alors un entier  $n \geq 0$  tel que  $F$  soit isomorphe à un sous-comodule d'un quotient de  $E^n$ .*

Par dualité, cela revient à dire que, si  $B$  est une algèbre de rang fini, et  $E$  un  $B$ -module fidèle, tout  $B$ -module de type fini  $F$  est isomorphe à un quotient d'un sous-module d'un  $E^n$ . Or  $F$  est isomorphe à un quotient d'un module libre  $B^q$ , et l'on est ramené à prouver que  $B^q$  est isomorphe à un sous-module d'un  $E^n$ ; il suffit d'ailleurs de le faire pour  $q = 1$ . Mais c'est clair: si  $E$  est engendré par  $x_1, \dots, x_n$ , l'application  $b \mapsto (bx_1, \dots, bx_n)$  est une injection de  $B$  dans  $E^n$ , puisque  $E$  est fidèle. D'où le lemme, et, avec lui, le théorème.

### Remarques

- 1) Le lecteur peut à volonté interpréter  $\text{Com}_C^f$  comme une *petite* catégorie (relative à un univers fixé, par exemple), ou une *grosse*. Le th. 2 est correct dans l'une ou l'autre interprétation.

2) Il n'est pas indispensable de passer aux modules pour prouver le lemme 1. On remarque d'abord (cf. n° 1.4, Exemple 2) que  $F$  est isomorphe à un sous-comodule de  $C_E \otimes F$ , i.e. de  $(C_E)^n$ , avec  $n = \text{rang}(F)$ . D'autre part,  $C_E$  est isomorphe, comme comodule, à un quotient de  $E \otimes E'$ , c'est-à-dire de  $E^m$ , où  $m = \text{rang}(E)$ . D'où le résultat.

### Exemples

1) La sous-catégorie de  $\text{Com}_C^f$  formée des *objets semi-simples* correspond à la *plus grande sous-cogèbre semi-simple* de  $C$  (la somme de toutes les sous-cogèbres simples).

2) Supposons  $C$  semi-simple, et soit  $(E_i)_{i \in I}$  un ensemble de représentants des classes de  $C$ -comodules simples. Posons  $C_i = C_{E_i}$ , de sorte que  $C$  est somme directe des cogèbres simples  $C_i$ . Si  $J$  est une partie de  $I$ ,  $C_J = \sum_{i \in J} C_i$  est une sous-cogèbre de  $C$ , et toute sous-cogèbre de  $C$  s'obtient de cette manière, et de façon unique. La sous-catégorie correspondant à  $C_J$  est formée des comodules isomorphes à des sommes directes finies des  $E_i, i \in J$ .

### 2.5. OÙ L'ON CARACTÉRISE $\text{Com}_C^f$

Soit  $M$  une catégorie abélienne munie des deux structures suivantes:

a)  $M$  est une catégorie *sur*  $K$ ; cela signifie que, si  $E, F$  sont des objets de  $M$ ,  $\text{Hom}^M(E, F)$  est muni d'une structure de  $K$ -espace vectoriel, la composition des morphismes étant bilinéaire.

b) On se donne un foncteur  $v: M \rightarrow \text{Vect}_K^f$  de  $M$  dans la catégorie des  $K$ -espaces vectoriels de dimension finie.

On fait les *hypothèses* suivantes:

(i) Le foncteur  $v$  est  *$K$ -linéaire*, i.e. pour tout  $E, F \in M$ , l'application  $v: \text{Hom}^M(E, F) \rightarrow \text{Hom}(v(E), v(F))$  est  $K$ -linéaire.

(ii) Le foncteur  $v$  est *exact* et *fidèle*.

**THÉORÈME 3.** *Sous les hypothèses ci-dessus, il existe une cogèbre  $C$  sur  $K$  (et une seule, à isomorphisme près) telle que  $M$  soit équivalente à  $\text{Com}_C^f$ , cette équivalence transformant le foncteur  $v$  en le foncteur  $C$ -module  $\mapsto$  espace vectoriel sous-jacent.*

[Ici, il est nécessaire d'interpréter  $M$  comme une petite catégorie, ou en tout cas de supposer qu'il existe un ensemble de représentants pour les classes d'isomorphisme d'objets de  $M$ .]

Avant de commencer la démonstration, remarquons que les hypothèses (i) et (ii) entraînent que  $\text{Hom}^M(E, F)$  est un espace vectoriel *de dimension finie* pour tout  $E, F \in M$ . De plus, un sous-objet d'un objet  $E$  de  $M$  est connu lorsqu'on connaît le sous-espace vectoriel correspondant de  $v(E)$ ; l'ensemble des sous-objets de  $E$  s'identifie ainsi à un sous-ensemble réticulé de l'ensemble des sous-espaces vectoriels de  $v(E)$ ; en particulier,  $E$  est *de longueur finie*. On a des résultats analogues pour les objets quotients.

D'autre part, si  $E \in M$ , nous noterons  $M_E$  la sous-catégorie pleine de  $M$  formée des quotients  $F/G$ , où  $F$  est isomorphe à un sous-objet d'un  $E^n$  ( $n$  entier  $> 0$  quelconque).

Enfin, si  $E$  est un objet de  $M$ , et si  $X$  est une partie de  $V(E)$ , nous dirons que  $X$  engendre  $E$  si tout sous-objet  $F$  de  $E$  tel que  $v(F) \supset X$  est égal à  $E$ .

### Démonstration du théorème 3

#### a) Le cas fini; une majoration.

C'est celui où il existe un objet  $E$  de  $M$  tel que  $M_E = M$ . Soit  $n = \text{rang}_K v(E)$ .

LEMME 2. Soit  $F$  un objet de  $M$  pouvant être engendré par un élément (cf. ci-dessus). On a

$$\text{rang}_K v(F) \leq n^2.$$

Par hypothèse, on peut écrire  $F$  comme quotient  $F_1/F_2$ , où  $F_1$  est isomorphe à un sous-objet d'un  $E^m$ , pour  $m$  convenable. Soit  $x \in v(F)$  engendrant  $F$  et soit  $x_1$  un élément de  $v(F_1)$  dont l'image dans  $v(F)$  est  $x$ . Soit  $G$  le plus petit sous-objet de  $E^m$  tel que  $v(G)$  contienne  $x_1$ . On a  $G \subset F_1$  et l'image de  $G$  dans  $F = F_1/F_2$  est égale à  $F$ . Il suffit donc de prouver que  $\text{rang}_K v(G) \leq n^2$ . Si  $m \leq n$ , c'est évident. Supposons donc que  $m > n$ . On a  $x_1 \in v(G) \subset v(E^m) = v(E)^m$ . Soient  $y_1, \dots, y_m$  les composantes de  $x_1$ , considéré comme élément de  $v(E)^m$ . Puisque  $m > n$ , il existe des  $a_i \in K$ , non tous nuls, tels que  $\sum a_i y_i = 0$ . Or les  $a_i$  définissent un morphisme surjectif  $E^m \rightarrow E$ ; si  $N$  est le noyau de ce morphisme, on a  $N \simeq E^{m-1}$ , comme on le voit facilement. D'autre part, on a  $x_1 \in v(N)$ , d'où  $G \subset N$  puisque  $x_1$  engendre  $G$ . On a donc obtenu un plongement de  $G$  dans  $E^{m-1}$ ; d'où le lemme, en raisonnant par récurrence sur  $m$ .

#### b) Le cas fini; construction d'un générateur projectif.

Les hypothèses étant les mêmes que ci-dessus, on choisit un objet  $P$  de  $M$  pouvant être engendré par un élément  $x \in v(P)$ , et tel que  $v(P)$  soit *de rang maximum* parmi ceux jouissant de cette propriété. C'est possible en vertu du Lemme 2.

LEMME 3. (i) *Le couple  $(P, x)$  représente le foncteur  $v$ .*

(ii)  *$P$  est un générateur projectif de  $M$ .*

Il suffit de prouver (i); l'assertion (ii) en résultera, puisque le foncteur  $v$  est exact et fidèle.

Soient donc  $F \in M$ , et  $y \in v(F)$ . Il nous faut prouver l'existence et l'unicité d'un morphisme  $f: P \rightarrow F$  transformant  $x$  en  $y$ . L'unicité provient de ce que  $x$  engendre  $P$ . Pour démontrer l'existence, soit  $Q$  le plus petit sous-objet de  $P \times F$  tel que  $v(Q)$  contienne  $(x, y)$ . Le morphisme  $Q \rightarrow F$  induit par  $\text{pr}_1$  est surjectif, du fait que  $P$  est engendré par  $x$ . On a donc

$$\text{rang}_K v(Q) \geq \text{rang}_K v(P);$$

mais le caractère maximal de  $v(P)$  entraîne qu'il y a égalité; le morphisme  $Q \rightarrow P$  est donc un isomorphisme. En composant son inverse avec la seconde projection  $Q \rightarrow F$ , on obtient un morphisme  $f$  ayant la propriété voulue.

c) *Le cas fini; fin de démonstration.*

Soit  $A$  l'algèbre des endomorphismes de  $P$ . C'est une  $K$ -algèbre de dimension finie. Le lemme suivant est bien connu:

LEMME 4. *Il existe un foncteur  $\varphi: \text{Mod}_{A^o}^f \rightarrow M$  et un seul (à isomorphisme près) qui soit exact à gauche et transforme  $A$  (considéré comme  $A$ -module à droite) en  $P$ . Ce foncteur est une équivalence de catégories.*

Indiquons brièvement la démonstration. Pour chaque  $A$ -module à droite  $H$  de rang fini, on choisit une *présentation finie* de  $H$ :

$$A^p \xrightarrow{\alpha} A^q \rightarrow H \rightarrow 0$$

où  $\alpha$  est une  $p \times q$ -matrice à coefficients dans  $A$ . Cette matrice définit un morphisme  $P^p \rightarrow P^q$  et l'on prend pour  $\varphi(H)$  le *conoyau* de ce morphisme. On prolonge de façon évidente  $\varphi$  en un foncteur  $\text{Mod}_{A^o}^f \rightarrow M$  et l'on vérifie qu'il a la propriété voulue. On note généralement ce foncteur  $H \mapsto H \otimes_A P$ . C'est un adjoint du foncteur  $F \mapsto \text{Hom}^M(P, F)$ . Son unicité est immédiate. Le fait que ce soit une équivalence résulte de ce que  $P$  est un générateur projectif de  $M$ .

De plus, l'équivalence  $\varphi: H \mapsto H \otimes_A P$  transforme le foncteur «espace vectoriel sous-jacent à un  $A$ -module» en un foncteur isomorphe à  $v$  (en effet le premier foncteur est représentable par  $A$ , le second par  $P$ , et  $\varphi$  transforme  $A$  en  $P$ ). On peut donc prendre pour cogèbre la cogèbre duale de l'algèbre  $A$ , et toutes les conditions sont vérifiées.

d) *Cas général.*

Soit  $X$  l'ensemble des sous-catégories  $N$  de  $M$  telles qu'il existe  $E \in M$  avec  $N = M_E$ . L'ensemble  $X$  est ordonné filtrant puisque  $M_{E_1 \times E_2}$  contient  $M_{E_1}$  et  $M_{E_2}$ . Si  $N \in X$ , soit comme ci-dessus  $(P_N, x_N)$  un couple représentant la restriction à  $N$  du foncteur  $v$ , et soit  $A_N = \text{End}(P_N)$ . Si  $N_1 \supset N_2$ , il existe un unique morphisme  $P_{N_1} \rightarrow P_{N_2}$  transformant  $x_{N_1}$  en  $x_{N_2}$ ; on voit aisément que ce morphisme identifie  $P_{N_2}$  au plus grand quotient de  $P_{N_1}$  appartenant à  $N_2$ . En particulier, tout endomorphisme de  $P_{N_1}$  définit par passage au quotient un endomorphisme de  $P_{N_2}$ . D'où un homomorphisme  $A_{N_1} \rightarrow A_{N_2}$  qui est surjectif. Si  $A$  désigne l'algèbre profinie limite projective des  $A_N$ , pour  $N \in X$ , il est alors clair que la cogèbre duale de  $A$  répond à la question.

Quant à l'*unicité* de cette cogèbre (ou de l'algèbre  $A$ ), elle provient de la remarque suivante: *A est isomorphe à l'algèbre des endomorphismes du foncteur  $v$ , munie de la topologie de la convergence simple.*

*Remarque.* Il est probablement possible d'éviter le passage par le cas  $M = M_E$ , en utilisant le théorème de Grothendieck disant qu'un foncteur exact à droite est proreprésentable: on appliquerait ce théorème à  $v$ , d'où  $P \in \text{Pro } M$  représentant  $v$  et on obtiendrait  $A$  comme l'algèbre des endomorphismes de  $P$ .

## § 3. BIGÈBRES

## 3.1. DÉFINITIONS ET CONVENTIONS

(Dans ce n°, ainsi que dans le suivant, on ne suppose pas que  $K$  soit un corps.)

Rappelons (cf. Alg. III) qu'une *bigèbre* sur  $K$  est un  $K$ -module  $C$  muni d'une structure de cogèbre  $d: C \rightarrow C \otimes C$  et d'une structure d'algèbre  $m: C \otimes C \rightarrow C$ , ces structures vérifiant l'axiome suivant:

(i) Si l'on munit  $C \otimes C$  de la structure d'algèbre produit tensoriel de celle de  $C$  par elle-même,  $d$  est un homomorphisme d'algèbres de  $C$  dans  $C \otimes C$ .

Cet axiome équivaut d'ailleurs à:

(i') L'application  $m: C \otimes C \rightarrow C$  est un morphisme de cogèbres (pour la structure naturelle de cogèbre de  $C \otimes C$ ).

Dans tout ce qui suit, nous réserverons le terme de *bigèbres* à celles vérifiant les conditions suivantes:

(ii) La cogèbre  $(C, d)$  possède une co-unité  $e: C \rightarrow K$ .

(iii) L'algèbre  $(C, m)$  est commutative, associative, et possède un élément unité 1.