

§3. Bigèbres

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **22.09.2024**

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) *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 ν , 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 ν , 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 ν , d'où $P \in \text{Pro } M$ représentant ν 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.

(iv) La co-unité $e: C \rightarrow K$ est un morphisme d'algèbres et $e(1) = 1$.

(v) On a $d(1) = 1 \otimes 1$.

La condition (iii) permet de considérer C comme l'*algèbre affine* d'un schéma affine G sur K ; on a $G = \text{Spec}(C)$. Pour tout $K_1 \in \text{Alg}_K$, on note $G(K_1)$ l'ensemble des points de G à valeurs dans K_1 , autrement dit l'ensemble des morphismes (au sens de Alg_K) de C dans K_1 . La condition (iv) signifie que e est un élément de $G(K)$. Grâce aux conditions (i) et (v), la structure de cogèbre de C peut être interprétée comme un *morphisme* de $G \times G$ dans G , qui est *associatif* et admet e pour élément neutre. Ainsi G est un *schéma affine en monoïdes* sur K ; pour tout $K_1 \in \text{Alg}_K$, $G(K_1)$ a une structure naturelle de monoïde, d'élément neutre l'image de e dans $G(K_1)$, image que l'on se permet de noter encore e .

On appelle *inversion* sur C , toute application $i: C \rightarrow C$ ayant les propriétés suivantes:

a) i est un morphisme d'algèbres, et $i(1) = 1$.

b) $m \circ (1_C \otimes i) \circ d$ est égal à l'endomorphisme $c \mapsto e(c) \cdot 1$ de C .

La condition a) permet d'interpréter i comme un morphisme $I: G \rightarrow G$ et la condition b) signifie que $x \cdot I(x) = e$ pour tout $x \in G(K_1)$, et tout K_1 . On voit ainsi que, si i existe, il est unique, et que c'est un isomorphisme de C sur la bigèbre opposée C° . L'existence de i revient à dire que G est un *schéma en groupes*.

Remarque. L'application identique $C \rightarrow C$ est un point de $G(C)$, appelé *point canonique*; nous le noterons γ . De même, on peut interpréter une inversion i de C comme un point ι de $G(C)$ et la condition b) signifie que $\gamma \iota = e$.

3.2. CORRESPONDANCE ENTRE COMODULES ET G -MODULES

Soit E un module. Si $K_1 \in \text{Alg}_K$, nous noterons $\text{End}_E(K_1)$ le monoïde des endomorphismes du K_1 -module $K_1 \otimes E$, et $\text{Aut}_E(K_1)$ le groupe des éléments inversibles de $\text{End}_E(K_1)$. Si $K_1 \rightarrow K_2$ est un morphisme, on définit de manière évidente le morphisme correspondant de $\text{End}_E(K_1)$ dans $\text{End}_E(K_2)$. Ainsi End_E est un foncteur de Alg_K dans la catégorie Mon des monoïdes; de même Aut_E est un foncteur de Alg_K dans la catégorie Gr des groupes.

Soient maintenant C et $G = \text{Spec}(C)$ comme ci-dessus. On a vu que G définit un foncteur (noté également G) de Alg_K dans Mon ; ce foncteur est à valeurs dans Gr si G est un schéma en groupes.

DÉFINITION 1. On appelle *représentation linéaire de G dans E* tout morphisme ρ du foncteur G dans le foncteur End_E .

En d'autres termes, ρ consiste en la donnée, pour tout $K_1 \in \text{Alg}_K$, d'un morphisme de monoïdes $\rho(K_1): G(K_1) \rightarrow \text{End}_E(K_1)$ et, si $K_1 \rightarrow K_2$ est un morphisme dans Alg_K , le diagramme

$$\begin{array}{ccc} G(K_1) & \rightarrow & G(K_2) \\ \rho(K_1) \downarrow & & \downarrow \rho(K_2) \\ \text{End}_E(K_1) & \rightarrow & \text{End}_E(K_2) \end{array}$$

doit être commutatif.

Terminologie. Une représentation linéaire du monoïde G^o opposé à G est appelée une *antireprésentation* de G . Un module E , muni d'une représentation (resp. antireprésentation) $G \rightarrow \text{End}_E$ est appelé un G -module à gauche (resp. à droite).

Remarque. Si G est un schéma en groupes, et si $\rho: G \rightarrow \text{End}_E$ est une représentation linéaire de G dans E , il est clair que ρ prend ses valeurs dans le sous-foncteur Aut_E de End_E .

Notons maintenant G^{ens} le foncteur G , considéré comme foncteur à valeurs dans Ens (i.e. le composé $\text{Alg}_K \xrightarrow{G} \text{Mon} \rightarrow \text{Ens}$); définissons de même $\text{End}_E^{\text{ens}}$. Soit ρ un morphisme de G^{ens} dans $\text{End}_E^{\text{ens}}$. L'image par $\rho(C)$ du point canonique $\gamma \in G(C)$ est un C -endomorphisme de $C \otimes E$, donc est définie par une application K -linéaire $d(\rho): E \rightarrow C \otimes E$.

PROPOSITION 1. (a) *L'application $\rho \mapsto d(\rho)$ est une bijection de l'ensemble des morphismes de G^{ens} dans $\text{End}_E^{\text{ens}}$ sur l'ensemble $\text{Hom}(E, C \otimes E)$.*

(b) *Pour que $\rho: G^{\text{ens}} \rightarrow \text{End}_E^{\text{ens}}$ soit une représentation linéaire (resp. une antireprésentation linéaire) de G dans E , il faut et il suffit que $d(\rho)$ munisse E d'une structure de C -comodule à droite (resp. à gauche).*

C'est là un résultat bien connu (cf. SGAD, exposé I). Rappelons la démonstration:

L'assertion (a) provient de ce que G^{ens} est représentable par le couple (C, γ) . En particulier, si $x \in G(K_1)$, l'image de x par $\rho(K_1)$ est l'application K_1 -linéaire de $K_1 \otimes E$ dans $K_1 \otimes E$ qui prolonge l'application linéaire $(x \otimes 1_E) \circ d(\rho)$ de E dans $K_1 \otimes E$.

Pour (b), on peut se borner au cas des antireprésentations. Il faut d'abord exprimer que $\rho(K_1)$ transforme e en 1 pour tout K_1 , et il suffit de le faire pour $K_1 = K$. Cela donne la condition

$$(e \otimes 1_E) \circ d(\rho) = 1_E$$

qui est l'axiome (2) des comodules.

Il faut ensuite exprimer que le diagramme

$$\begin{array}{ccc}
 G^{\text{ens}} \times G^{\text{ens}} & \xrightarrow{\rho \times \rho} & \text{End}_E^{\text{ens}} \times \text{End}_E^{\text{ens}} \\
 \alpha \downarrow & & \downarrow \beta \\
 G^{\text{ens}} & \xrightarrow{\rho} & \text{End}_E^{\text{ens}}
 \end{array}$$

(où α désigne la loi de composition de G et β l'opposée de la loi de composition de End_E) est commutatif. Notons γ_1 (resp. γ_2) l'homomorphisme de C dans $C \otimes C$ qui applique $x \in C$ dans $x \otimes 1$ (resp. $1 \otimes x$); on a $\gamma_1, \gamma_2 \in G(C \otimes C)$. De plus, il est immédiat que le foncteur $G^{\text{ens}} \times G^{\text{ens}}$ est représentable par $(C \otimes C, \gamma_1 \times \gamma_2)$. Il suffit donc d'exprimer que les deux images de $\gamma_1 \times \gamma_2$ dans $\text{End}_E(C \otimes C)$ coïncident. Or l'image de $\gamma_1 \times \gamma_2$ dans $G(C \otimes C)$ est le point donné par $d: C \rightarrow C \otimes C$; son image dans $\text{End}_E(C \otimes C)$, identifié à $\text{Hom}(E, C \otimes C \otimes E)$ est donc $(d \otimes 1_E) \circ d(\rho)$. Il faut ensuite calculer l'image de $\gamma_1 \times \gamma_2$ par $G \times G \xrightarrow{\rho \times \rho} \text{End}_E \times \text{End}_E \xrightarrow{\beta} \text{End}_E$. On trouve, après un calcul sans difficultés [cf. ci-après] l'élément $(1_C \otimes d(\rho)) \circ d(\rho)$. La commutativité du diagramme considéré équivaut donc à l'axiome (1) des comodules, ce qui achève de démontrer la proposition.

[Voici le «calcul sans difficultés» en question. Il s'agit de déterminer l'image $\varphi \in \text{End}_E(C \otimes C)$ de $\gamma_1 \times \gamma_2$ par $\beta \circ (\rho \times \rho)$. Si φ_1 (resp. φ_2) est l'image de γ_1 (resp. γ_2) par ρ , on a $\varphi = \varphi_2 \circ \varphi_1$ (puisque β est l'opposée de la loi de composition). De plus, φ_i est caractérisé par le fait de prolonger l'application K -linéaire $(\gamma_i \otimes 1_E) \circ d(\rho): E \rightarrow C \otimes E \rightarrow C \otimes C \otimes E$. Soit alors $x \in E$, et posons:

$$d(\rho)(x) = \sum c_i \otimes x_i, \quad d(\rho)(x_i) = \sum c_{ij} \otimes x_{ij}.$$

On a:

$$\varphi_1(x) = (\gamma_1 \otimes 1_E)(\sum c_i \otimes x_i) = \sum c_i \otimes 1 \otimes x_i.$$

De même:

$$\varphi_2(x_i) = \sum 1 \otimes c_{ij} \otimes x_{ij}.$$

D'où:

$$\begin{aligned}
 \varphi(x) &= \varphi_2(\varphi_1(x)) = \sum \varphi_2(c_i \otimes 1 \otimes x_i) \\
 &= \sum (c_i \otimes 1) \cdot \sum 1 \otimes c_{ij} \otimes x_{ij} \quad (\varphi_2 \text{ étant } C \otimes C\text{-linéaire}) \\
 &= \sum c_i \otimes c_{ij} \otimes x_{ij}.
 \end{aligned}$$

D'autre part, on a

$$\begin{aligned} ((1_C \otimes d(\rho)) \circ d(\rho))(x) &= (1_C \otimes d(\rho)) (\sum c_i \otimes x_i) \\ &= \sum c_i \otimes c_{ij} \otimes x_{ij} . \end{aligned}$$

En comparant, on voit bien que l'on a

$$\varphi = (1_C \otimes d(\rho)) \circ d(\rho) .]$$

Remarque. La proposition précédente permet donc d'identifier les G -modules à gauche aux C -comodules à droite, et inversement. [Il est bien triste d'avoir ainsi à échanger sa droite et sa gauche, mais on n'y peut rien. Toutefois, lorsque G est un schéma en groupes, on peut, au moyen de l'inverse, transformer canoniquement tout module à droite en un module à gauche.]

Exemple. La représentation triviale $\rho = 1$ de G dans un module E correspond à la structure de comodule $x \mapsto 1 \otimes x$ sur E . Pour $E = K$ on obtient le comodule *unité*.

OPÉRATIONS SUR LES COMODULES

a) *Produit tensoriel.*

Si E_1 et E_2 sont des C -modules (à gauche, par exemple), on a défini au n° 1.2 une structure de $C \otimes C$ -comodule sur $E_1 \otimes E_2$. Comme $m : C \otimes C \rightarrow C$ est un morphisme de cogèbres, on déduit de là *une structure de C -comodule sur $E_1 \otimes E_2$* . Du fait que m est commutative, cette structure ne dépend pas de l'ordre dans lequel on écrit E_1 et E_2 . Elle correspond (via la prop. 1) à l'opération évidente de *produit tensoriel de G -modules* (la vérification de ce fait est immédiate).

b) *Contragrédiente.*

Supposons que C admette une inversion, et soit E un C -comodule à gauche qui est projectif de type fini comme module. En utilisant les isomorphismes

$$\text{Hom}(E, C \otimes E) \simeq \text{Hom}(E \otimes E', C) \simeq \text{Hom}(E', C \otimes E')$$

on définit sur E' une structure de C -module à droite. En utilisant l'inversion i , on transforme cette structure en une structure de C -comodule à gauche, dite *contragrédiente* de celle donnée sur E et notée \check{E} . Elle correspond (via la prop. 1) à l'opération évidente de «*contragrédiente d'une représentation*». [L'hypothèse faite sur E sert à assurer que le foncteur «dual» commute au foncteur «extension des scalaires».]

3.3. SOUS-BIGÈBRES

(On suppose à nouveau que K est un corps.)

Soit C une bigèbre (vérifiant les conditions du n° 3.1), et soit L une sous-catégorie abélienne de Com_C^f vérifiant les conditions 1), 2), 3) du th. 2 du n° 2.4, i.e. provenant d'une sous-cogèbre D de C .

PROPOSITION 2. *Pour que D soit une sous-bigèbre de C contenant 1, il faut et il suffit que L soit stable par produit tensoriel et contienne le comodule unité K .*

La nécessité est triviale. Supposons donc que L soit stable par \otimes et contienne K . On sait (cf. n° 2.4) que D est réunion des cogèbres C_E attachées aux comodules $E \in L$. Le fait que D soit stable par le produit résultera donc du lemme suivant:

LEMME 1. *Si E et F sont des comodules de rang fini, on a*

$$(*) \quad C_{E \otimes F} = C_E \cdot C_F .$$

En effet, on vérifie tout de suite que $C_E \otimes C_F$ est la sous-cogèbre de $C \otimes C$ attachée au $C \otimes C$ -comodule $E \otimes F$. Comme $C_{E \otimes F}$ est l'image de cette dernière par $m: C \otimes C \rightarrow C$, c'est bien $C_E \cdot C_F$.

Le fait que D contienne 1 provient de ce que $C_E = K \cdot 1$ si $E = K$.

PROPOSITION 3. *Supposons que C ait une inversion i . Pour que D soit stable par i , il faut et il suffit que L soit stable par le foncteur «contragrédiente».*

Cela résulte, comme ci-dessus, de la formule:

$$(**) \quad C_E^\vee = i(C_E) .$$

COROLLAIRE. *Supposons que $G = \text{Spec}(C)$ soit un schéma en groupes. Soit Mod_G^f la catégorie des G -modules de rang fini, et soit L une sous-catégorie abélienne de Mod_G^f . Pour qu'il existe un quotient H de G tel que $L = \text{Mod}_H^f$, il faut et il suffit que L vérifie les conditions 1), 2), 3) du th. 2 du n° 2.4, soit stable par les opérations «produit tensoriel» et «contragrédiente», et contienne le G -module unité K ; le groupe H en question est alors unique.*

Ce n'est qu'une reformulation des props. 2 et 3, étant entendu que «groupe quotient» est pris pour synonyme de «sous-bigèbre contenant 1». L'unicité de H provient du th. 2 du n° 2.4.

[Il y a un résultat plus général, dû sauf erreur à Grothendieck, et que le rédacteur a la flemme de rédiger en détail. Au lieu de se donner, comme ici, une sous-cogèbre d'une bigèbre, on se donne seulement une *cogèbre* D et une opération de «produit tensoriel» sur la catégorie $M = \text{Com}_D^f$ correspondante (la donnée de D est d'ailleurs équivalente à celle du couple formé de M et du foncteur $\nu: M \rightarrow \text{Vect}_K$, cf. n° 2.5, th. 3). En imposant à ce produit tensoriel des conditions raisonnables (en particulier $\nu(E \otimes F) \simeq \nu(E) \otimes \nu(F)$) on démontre alors qu'il provient d'une structure de *bigèbre* bien déterminée sur D ; cette bigèbre a un élément unité si M contient un élément unité pour le produit tensoriel; elle a une inversion, si l'on se donne une opération «contragrédiente». (Au lieu de se donner le produit tensoriel et la contragrédiente, on peut aussi se donner un foncteur «Hom».)

Grothendieck a rencontré cette situation avec $K = \mathbf{Q}$, $M =$ catégorie des *motifs* sur un corps de base k et $\nu =$ foncteur «cohomologie à valeurs dans \mathbf{Q} » relativement à un plongement de k dans \mathbf{C} .]

3.4. UNE INTERPRÉTATION DES POINTS DE G

Soit $K_1 \in \text{Alg}_K$ et soit $g \in G(K_1)$ un point de G à valeurs dans K_1 . Pour tout $E \in \text{Com}_C^f$, notons $g(E)$ l'image de g par l'antireprésentation

$$\rho(E): G(K_1) \rightarrow \text{End}_E(K_1) .$$

On a donc $g(E) \in \text{End}_E(K_1) = \text{End}_{K_1}(K_1 \otimes E)$, et de plus:

- (i) $g(K) = 1_{K_1}$
- (ii) $g(E_1 \otimes E_2) = g(E_1) \otimes g(E_2)$.

Réciproquement:

PROPOSITION 4. *Soit $\nu_{K_1}: \text{Com}_C^f \rightarrow \text{Mod}_{K_1}$ le foncteur qui associe à tout $E \in \text{Com}_C^f$ le K_1 -module $K_1 \otimes E$. Soit $\varphi: \nu_{K_1} \rightarrow \nu_{K_1}$ un endomorphisme de ν_{K_1} vérifiant les relations (i) et (ii) ci-dessus. Il existe alors un élément unique $g \in G(K_1)$ tel que $\varphi = g$.*

D'après 3.2, l'application $G(K_1) \rightarrow \text{End}(\nu_{K_1})$ est un antihomomorphisme de monoïdes. La prop. 4 donne donc:

COROLLAIRE. *Le monoïde $G(K_1)$ est isomorphe à l'opposé du monoïde des endomorphismes de ν_{K_1} vérifiant (i) et (ii).*

[C'est là un résultat analogue au *théorème de dualité de Tannaka*; on reviendra là-dessus plus loin.]

Remarques

1) Dans l'énoncé de la prop. 4, on peut remplacer Com_C^f par Com_C ; cela revient au même, du fait que tout objet de Com_C est limite inductive d'objets de Com_C^f , cf. §1.

2) Lorsque G est un schéma en groupes, les $g(E)$ vérifient la relation suivante (qui est donc conséquence de (i) et (ii):

$$(iii) \quad g(\check{E}) = g(E)^\vee.$$

Démonstration de la proposition 4.

Tout d'abord, soit $u \in \text{Hom}(C, K_1)$. Pour tout $E \in \text{Com}_C$, soit $\varphi_u(E)$ l'endomorphisme de $K_1 \otimes E$ qui prolonge l'application linéaire

$$E \xrightarrow{d_E} C \otimes E \xrightarrow{u \otimes 1} K_1 \otimes E.$$

On obtient ainsi un endomorphisme φ_u de v_{K_1} .

LEMME 1. *L'application $u \mapsto \varphi_u$ est un isomorphisme de $\text{Hom}(C, K_1)$ sur le groupe des endomorphismes du foncteur v_{K_1} .*

[En fait, c'est un isomorphisme de K_1 -algèbres, à condition de mettre sur $\text{Hom}(C, K_1)$ la structure d'algèbre opposée de celle à laquelle on pense.]

Si $\varphi \in \text{End}(v_{K_1})$, formons le composé

$$C \rightarrow K_1 \otimes C \rightarrow K_1 \otimes C \rightarrow K_1$$

(la première application étant $x \mapsto 1 \otimes x$, la seconde $\varphi(C)$ et la troisième $1 \otimes e$). On obtient une application linéaire

$$u(\varphi) : C \rightarrow K_1.$$

Il suffit de prouver que les applications $u \mapsto \varphi_u$ et $\varphi \mapsto u(\varphi)$ sont inverses l'une de l'autre.

Tout d'abord, si $u \in \text{Hom}(C, K_1)$, $u(\varphi_u)$ est le composé

$$C \xrightarrow{d} C \otimes C \xrightarrow{u \otimes 1} K_1 \otimes C \xrightarrow{1 \otimes e} K_1,$$

ou encore

$$C \xrightarrow{d} C \otimes C \xrightarrow{1 \otimes e} C \xrightarrow{u} K_1,$$

c'est-à-dire u .

Soit maintenant $\varphi \in \text{End}(v_{K_1})$. Si E est un comodule, et V un K -espace vectoriel, on a $\varphi(E \otimes V) = \varphi(E) \otimes 1_V$. (Se ramener au cas où V est de dimension finie, puis choisir une base de V et utiliser le fait que φ est un

morphisme de foncteurs.) En particulier, on a $\varphi(C \otimes E) = \varphi(C) \otimes 1_E$ si $E \in \text{Com}_C$. Comme $d_E: E \rightarrow C \otimes E$ est un morphisme de comodules, on a un diagramme commutatif:

$$\begin{array}{ccc} E & \rightarrow & K_1 \otimes E \xrightarrow{1 \otimes d_E} K_1 \otimes C \otimes E \\ \varphi(E) \downarrow & & \varphi(C) \otimes 1 \downarrow \\ K_1 \otimes E & \xrightarrow{1 \otimes d_E} & K_1 \otimes C \otimes E \xrightarrow{1 \otimes C \otimes 1} K_1 \otimes E. \end{array}$$

Mais le composé $(1 \otimes e \otimes 1) \circ (1 \otimes d_E)$ est l'identité. En utilisant la commutativité du diagramme, on en déduit alors que le composé

$$E \rightarrow K_1 \otimes E \xrightarrow{\varphi(E)} K_1 \otimes E$$

est égal à $\varphi_u(E)$, avec $u = u(\varphi)$, d'où le lemme.

[Ce lemme n'a rien à voir avec les bigèbres. On aurait pu le remonter au §2 et le déduire de l'isomorphisme $\text{Com}_C^f = \text{Com}_{A^o}^f$ du n° 2.2.]

LEMME 2. (a) *Pour que φ_u vérifie la relation (i), il faut et il suffit que $u(1) = 1$.*

(b) *Pour que φ_u vérifie la relation (ii), il faut et il suffit que u soit un homomorphisme d'algèbres.*

Si l'on prend pour E le module unité K , on a $K_1 \otimes E = K_1$ et $\varphi_u(E)$ est la multiplication par $u(1)$ dans K_1 ; d'où (a).

Pour (b), on remarque d'abord que (ii) est vérifiée si et seulement si elle l'est pour $E_1 = E_2 = C$, i.e. si

$$(ii') \quad \varphi_u(C \otimes C) = \varphi_u(C) \otimes \varphi_u(C).$$

Cela résulte simplement de ce que tout comodule est isomorphe à un sous-comodule d'une somme directe de comodules tous isomorphes à C .

Reste à exprimer la condition (ii'). Soit $(x_i)_{i \in I}$ une base de C , soient $a, b \in C$, et écrivons $d(a)$ et $d(b)$ sous la forme

$$\begin{aligned} d(a) &= \sum a_i \otimes x_i, & a_i \in C \\ d(b) &= \sum b_j \otimes x_j, & b_j \in C. \end{aligned}$$

On a alors:

$$\varphi_u(C)(a) = \sum u(a_i) \otimes x_i, \quad \text{avec } u(a_i) \in K_1$$

et

$$\varphi_u(C)(b) = \sum u(b_j) \otimes x_j, \quad \text{avec } u(b_j) \in K_1.$$

D'où:

$$(*) \quad (\varphi_u(C) \otimes \varphi_u(C))(a \otimes b) = \sum_{i,j} u(a_i) u(b_j) \otimes x_i \otimes x_j.$$

Soit d'autre part $d' : C \otimes C \rightarrow C \otimes C \otimes C$ le coproduit du comodule $C \otimes C$. On vérifie sans difficulté que l'on a

$$d'(a \otimes b) = \sum_{i,j} a_i b_j \otimes x_i \otimes x_j,$$

d'où

$$(**) \quad \varphi_u(C \otimes C)(a \otimes b) = \sum_{i,j} u(a_i b_j) \otimes x_i \otimes x_j.$$

En comparant (*) et (**), on voit que $\varphi_u(C \otimes C) = \varphi_u(C) \otimes \varphi_u(C)$ si u est un homomorphisme d'algèbres. Pour prouver la réciproque, choisissons pour $(x_i)_{i \in I}$ une base telle que $x_0 = 1$ pour un élément $0 \in I$ et $e(x_i) = 0$ pour $i \neq 0$. On a alors $a_0 = a$ et $b_0 = b$, et l'égalité de (*) et (**) entraîne $u(a)u(b) = u(ab)$, ce qui achève la démonstration.

La prop. 4 est une conséquence immédiate des deux lemmes ci-dessus. En effet, un élément de $G(K_1)$ est *par définition* un homomorphisme d'algèbres $u : C \rightarrow K_1$ tel que $u(1) = 1$. La seule chose à vérifier, c'est que, pour tout comodule E , l'endomorphisme $u(E)$ de $K_1 \otimes E$ défini par u est égal à $\varphi_u(E)$: or c'est justement la définition de $u(E)$, cf. démonstration de la prop. 1.

Exemple. Prenons pour K_1 l'algèbre des *nombres duaux* sur K . La prop. 4 fournit alors un anti-isomorphisme de l'*algèbre de Lie* de G sur la sous-algèbre de Lie de $\text{End}(v)$ formée des endomorphismes θ de v tels que

$$\theta(K) = 0 \quad \text{et} \quad \theta(E_1 \otimes E_2) = \theta(E_1) \otimes 1_{E_2} + 1_{E_1} \otimes \theta(E_2).$$

3.5. INTERPRÉTATION DE G COMME LIMITE PROJECTIVE DE GROUPES ALGÈBRIQUES LINÉAIRES

DÉFINITION 2. *On dit que C est de type fini (ou que G est algébrique linéaire) si C est de type fini comme algèbre sur K .*

PROPOSITION 5. *Soit C une bigèbre (resp. une bigèbre possédant une inversion i). Alors C est limite inductive filtrante de ses sous-bigèbres de type fini contenant 1 (resp. et stables par i).*

L'énoncé contenant les « resp. » équivaut à :

COROLLAIRE. *Le schéma en groupes G associé à C est limite projective filtrante de groupes algébriques linéaires.*

On va prouver un résultat plus précis. Soit E un C -comodule (à droite, pour changer un peu) de rang fini et soit C_E la sous-cogèbre de C correspondante.

Pour tout $n \geq 0$, soit $C_E(n)$ la sous-cogèbre attachée au comodule $\bigotimes^n E$; pour $n = 0$, on convient comme d'ordinaire que $\bigotimes^n E = K$, de sorte que $C_E(0) = K$. 1. On sait (cf. lemme 1) que

$$C_E(n) = C_E \dots C_E \quad (n \text{ facteurs}) .$$

Il en résulte que

$$C(E) = \sum_{n=0}^{\infty} C_E(n)$$

est la *sous-algèbre* de C engendrée par C_E et 1. D'où:

PROPOSITION 6. *L'algèbre $C(E)$ est une sous-bigèbre de C contenant 1 et de type fini; c'est la plus petite sous-bigèbre de C contenant 1 et C_E .*

Comme C est visiblement limite inductive des $C(E)$, cela démontre la première partie de la prop. 5. D'autre part, lorsque C possède une inversion i , la seconde partie de la prop. 5 résulte de la proposition plus précise (mais évidente) suivante:

PROPOSITION 7. *L'algèbre $C(E \oplus \check{E})$ est une sous-bigèbre de C contenant 1 et stable par i ; c'est la plus petite sous-bigèbre de C ayant ces propriétés; elle est de type fini.*

Si l'on note X_E (resp. G_E) le monoïde (resp. groupe) algébrique linéaire associé à $C(E)$ (resp. à $C(E \oplus \check{E})$), on voit que l'on a

$$G = \varprojlim X_E \quad (\text{resp. } G = \varprojlim G_E) .$$

Remarques

1) La construction de $C(E \oplus \check{E})$ à partir de $C(E)$ peut aussi se faire de la manière suivante: au G -module E est associé un élément «déterminant» δ_E , qui est un élément inversible de C , contenu dans $C(E)$. On a:

$$C(E \oplus \check{E}) = C(E) \left[\frac{1}{\delta_E} \right] .$$

2) L'interprétation de X_E et G_E en termes de schémas est la suivante: X_E (resp. G_E) est le plus petit sous-schéma fermé du schéma End_E (resp. GL_E) des endomorphismes (resp. automorphismes) de E contenant l'image de la représentation $\rho: G \rightarrow \text{End}_E$ attachée à E . Cela se vérifie immédiatement sur la construction de l'algèbre affine de End_E (resp. G_E), construction que le rédacteur trouve inutile de reproduire.

DÉFINITION 3. Soit C une bigèbre possédant une inversion. Un C -comodule E de rang fini est dit fidèle si $C(E \oplus \check{E}) = C$.

Vu ce qui précède, E est fidèle si et seulement si $G \rightarrow G_E$ est un isomorphisme.

PROPOSITION 8. Si E est fidèle, toute représentation linéaire de G est quotient d'une sous-représentation d'une somme directe de représentations $\bigotimes^n (E \oplus \check{E})$.

Cela résulte du lemme 1 du n° 2.4.

COROLLAIRE. Tout G -module simple est quotient de Jordan-Hölder d'un $\bigotimes^n (E \oplus \check{E})$.

Remarques

1) Dans le corollaire ci-dessus, on peut remplacer les puissances tensorielles de $E \oplus \check{E}$ par les représentations $\bigotimes^n E \otimes^m \det(E)^{-1}$, avec des notations évidentes.

2) Il se peut que G_E soit fermé dans End_E (et non pas seulement dans GL_E), autrement dit que $C(E) = C(E \oplus \check{E})$. C'est le cas, par exemple, si G_E est contenu dans SL_E . Dans ce cas, la prop. 8 et son corollaire se simplifient: on peut remplacer les puissances tensorielles de $E \oplus \check{E}$ par celles de E .

§4. ENVELOPPES

4.1. COMPLÉTION D'UNE ALGÈBRE

[Ce sorite pourrait remonter au n° 2.2.]

Soit A une algèbre associative à élément unité. Soit S_d (resp. S_g, S) l'ensemble des idéaux à droite (resp. à gauche, resp. bilatères) de codimension finie dans A . On a $S_d \cap S_g = S$ et S est *cofinal* à la fois dans S_d et dans S_g ; en effet, si $\alpha \in S_g$ par exemple, l'annulateur du A -module A/α appartient à S et est contenu dans α .

On posera:

$$\hat{A} = \varprojlim A/\alpha$$

la limite projective étant prise sur l'ensemble ordonné filtrant S . L'algèbre \hat{A} est l'*algèbre profinie complétée* de A , pour la topologie définie par S (ou S_d , ou S_g , cela revient au même). Il y a un isomorphisme évident de la catégorie