GÈBRES

Autor(en): **Serre, Jean-Pierre**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **13.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-60413

L'Enseignement Mathématique, t. 39 (1993), p. 33-85

GÈBRES

par Jean-Pierre SERRE

Le texte ci-après reproduit la rédaction Bourbaki n° 518, datant de septembre 1968.

Son objet est exposé dans les «commentaires du rédacteur», placés au début. Il s'agit essentiellement des *enveloppes algébriques* des groupes linéaires, et de leurs relations avec les différents types de *gèbres*: algèbres, cogèbres et bigèbres. De telles enveloppes se rencontrent dans les situations suivantes:

— complexification d'un groupe de Lie réel, par exemple compact;

— représentations galoisiennes p-adiques (cas local), ou l-adiques (cas motivique);

— représentations linéaires de certains groupes discrets, tels que $\mathbf{SL}_n(\mathbf{Z})$, $n \geqslant 3$.

Une étude vraiment générale de ce genre de question nécessite la notion de *catégorie tannakienne,* comme l'ont montré Grothendieck et Saavedra Rivano (Lect. Notes 265, Springer-Verlag, 1972). Toutefois le cas considéré ici est nettement plus simple que le cas tannakien général, du fait que l'on dispose à l'avance d'un «foncteur fibre». C'est ce qui justifie (peut-être) la présente publication.

Le texte initial a été laissé inchangé, à part une correction au n° 5.2 que je dois à P. Deligne. Il y a quelques références à des rédactions non publiées de Bourbaki (n^{os} 515 et 517), mais elles sont peu nombreuses et ne devraient pas gêner le lecteur (elles ne concernent que des propriétés standard des involutions de Cartan).

Cette publication a été autorisée par N. Bourbaki; je l'en remercie vivement.

SOMMAIRE

COMMENTAIRES DU RÉDACTEUR

Soit Γ un groupe. Se donner une structure de schéma en groupes affine sur Γ (ou, plus correctement, définir une «enveloppe» algébrique de Γ) revient à se donner:

— soit une *bigèbre* C de fonctions sur Γ, de sorte que le schéma en groupes en question soit $\mathrm{Spec}(C)$;

— soit une *sous-catégorie* de la catégorie des représentations linéaires de Γ (cette sous-catégorie étant stable par sous-trucs, quotients, sommes directes, produits tensoriels, ...).

Ainsi, la structure algébrique réelle (resp. complexe) d'un groupe de Lie compact (resp. réductif complexe) correspond à la catégorie des représentations analytiques réelles (resp. complexes) du groupe; sa bigèbre est formée des «coefficients de représentations» qui sont analytiques réels (resp. complexes).

Le but de la rédaction est d'expliquer cette correspondance entre *bigèbres* et *catégories de représentations.* Il y a intérêt à traiter d'abord le cas, plus simple, des *cogèbres* (cela revient à laisser tomber le produit tensoriel des représentations). C'est ce qui est fait dans les §§1 et 2. Les §§3 et 4 sont consacrés aux bigèbres, et le §5 aux applications aux groupes compacts et complexes.

AVERTISSEMENTS

1. Il s'agit, non d'un projet de chapitre, mais d'une rédaction *à usage interne,* pour l'édification de BOURBAKI (ou, en tout cas, du rédacteur). On y utilise librement les notions élémentaires sur les catégories abéliennes et les schémas affines. Certains morceaux devraient quand même être utilisables dans le livre de LIE.

2. Le rédacteur a fait beaucoup d'efforts pour distinguer sa droite de sa gauche. Il n'est pas certain d'y être toujours parvenu.

NOTATIONS

Dans les §§1 à 4, la lettre K désigne un anneau commutatif. A partir du §2, on suppose (sauf mention expresse du contraire) que c'est un corps.

Toutes les algèbres, cogèbres, bigèbres, tous les comodules, modules, etc. sont sur K. Même chose pour les produits tensoriels. On écrit $\mathrm{Hom}(V, W)$ et $V \otimes W$ au lieu de $\mathrm{Hom}_K(V, W)$ et $V \otimes_K W$. Le dual d'un module V est noté V'.

On note Alg_K la catégorie des anneaux commutatifs K_1 munis d'un morphisme $K \to K_1$.

L'application identique d'un ensemble X est notée 1_X (ou simplement 1 si aucune confusion sur X n'est à craindre).

§ 1. COGÈBRES ET COMODULES (GÉNÉRALITÉS)

1.1. COGÈBRES

Dans tout ce paragraphe, C désigne une *cogèbre,* de coproduit d, possédant une co-unité (à droite et à gauche) e. Rappelons (cf. *Alg.* III) ce que cela signifie:

C est un module (sur K);

d est une application linéaire de C dans $C \otimes C$;

e est une forme linéaire sur C.

De plus, ces données vérifient les axiomes suivants:

(C_1) (Coassociativité) Les applications linéaires $(1_C \otimes d) \circ d$ et $(d \otimes 1_C) \circ d$ de C dans $C \otimes C \otimes C$ coïncident.

(C_2) (Co-unité) $(1_C \otimes e) \circ d = 1_C$ et $(e \otimes 1_C) \circ d = 1_C$.

Exemples

(1) Soit C une cogèbre de co-unité e. En composant le coproduit de C avec la symétrie canonique de $C \otimes C$, on obtient une seconde structure de cogèbre sur C, dite *opposée* de la première. On la note C^o; la co-unité de C^o est e.

(2) Toute somme directe de cogèbres a une structure naturelle de cogèbre. En particulier, 0 est une cogèbre.

(3) Supposons que C soit projectif de type fini (comme K-module), et soit A son dual. Comme le dual de $C \otimes C$ s'identifie à $A \otimes A$, toute structure de cogèbre sur C correspond à une structure d'*algèbre associative* sur A, et réciproquement. Pour que $e \in A$ soit co-unité de C, il faut et il suffit que ce soit un élément unité (à gauche et à droite) pour A.

(Lorsque K est un corps, on verra plus loin que toute cogèbre est limite inductive de cogèbres obtenues par ce procédé.)

(4) Soit V un module projectif de type fini. Soit

$$C = \mathrm{End}(V) = V \otimes V' .$$

La forme bilinéaire $\mathrm{Tr}(uv)$ met C en dualité avec lui-même; appliquant la méthode de l'exemple précédent, on voit que la structure d'algèbre de C définit par dualité une structure de *cogèbre* sur C, de co-unité la trace $\mathrm{Tr}: C \to K$. En particulier $M_n(K)$ a une structure de cogèbre canonique, pour laquelle on a

$$d(E_{ij}) = \sum_k E_{kj} \otimes E_{ik} .$$

(La cogèbre *opposée* est plus sympathique, cf. exercice 1.)

(5) Soient C_1 et C_2 deux cogèbres, de coproduits d_1 et d_2 et de co-unités e_1 et e_2. Soit σ l'isomorphisme canonique de $C_2 \otimes C_1$ sur $C_1 \otimes C_2$; le composé

$$(1_{C_1} \otimes \sigma \otimes 1_{C_2}) \circ (d_1 \otimes d_2)$$

munit $C_1 \otimes C_2$ d'une structure de cogèbre, dite *produit tensoriel* de celles de C_1 et C_2; elle admet pour co-unité $e_1 \otimes e_2$.

(6) L'algèbre affine d'un schéma en monoïdes affine sur K a une structure naturelle de cogèbre, cf. n° 3.1.

1.2. COMODULES

DÉFINITION 1. *On appelle comodule (à gauche) sur* C *tout module* E *muni d'une application linéaire* $d_E: E \to C \otimes E$ *vérifiant les axiomes suivants:*

(1) *Les applications linéaires* $(d \otimes 1_E) \circ d_E$ *et* $(1_C \otimes d_E) \circ d_E$ *de* E *dans* $C \otimes C \otimes E$ *coïncident.*

(2) $(e \otimes 1_E) \circ d_E = 1_E$.

L'application d_E s'appelle le *coproduit* de E; on se permet souvent de le (la) noter d.

Remarques

1) Il y a une notion analogue de comodule *à droite*; on laisse au lecteur le soin de l'expliciter (ou de remplacer la cogèbre C par son opposée C^o). [Le rédacteur s'est aperçu trop tard qu'il était plus commode d'échanger droite et gauche, i.e. d'appeler «comodules à droite» ceux de la définition 1.]

2) Toute application linéaire $d_E: E \to C \otimes E$ définit de manière évidente une application linéaire $d_E^1: E \otimes E' \to C$. Lorsque E est un K-module projectif de type fini, l'application $d_E \mapsto d_E^1$ est un isomorphisme de $\mathrm{Hom}(E, C \otimes E)$ sur $\mathrm{Hom}(E \otimes E', C)$. Or $E \otimes E' = \mathrm{End}(E)$ a une structure naturelle de cogèbre, cf. n° 1.1, Exemple 4). On peut vérifier (cf. exercice 1) que d_E *vérifie les axiomes* (1) *et* (2) *si et seulement si* d_E^1 *est*

un morphisme de la cogèbre opposée $\mathrm{End}(E)^o$ *à* $\mathrm{End}(E)$ *dans la cogèbre* C, *compatible avec les co-unités.*

3) Supposons que E soit *libre* de base $(v_i)_{i \in I}$. Une application linéaire $d_E : E \to C \otimes E$ est alors définie par une famille c_{ij}, $i, j \in I$, d'éléments de C telle que $d_E(v_i) = \sum_{j \in I} c_{ij} \otimes v_j$ (pour i fixé, c_{ij} doit être nul pour presque tout j). Les conditions (1) et (2) de la définition 1 se traduisent alors par les formules:

$$(1') \quad d(c_{ij}) = \sum_{k \in I} c_{ik} \otimes c_{kj} \qquad \text{pour} \quad i, j \in I$$

$$(2') \quad e(c_{ij}) = \delta_{ij} \qquad \text{pour} \quad i, j \in I\,.$$

(Lorsque I est *fini*, cet exemple peut être considéré comme un cas particulier du précédent.)

Exemples de comodules

1) Le module C, muni de d, est un comodule (à gauche et à droite).

2) La somme directe d'une famille de comodules a une structure naturelle de comodule.

3) Si E est un comodule, et V un K-module quelconque, le couple $(E \otimes V, d_E \otimes 1_V)$ est un comodule, noté simplement $E \otimes V$.

4) Les notations étant celles de l'exemple 5) du n° 1.1, soient E_1 un comodule sur C_1 et E_2 un comodule sur C_2. Soit τ l'isomorphisme canonique de $E_1 \otimes C_2$ sur $C_2 \otimes E_1$; l'application

$$(1_{C_1} \otimes \tau \otimes 1_{E_2}) \circ (d_{E_1} \otimes d_{E_2})$$

munit $E_1 \otimes E_2$ d'une structure de comodule sur $C_1 \otimes C_2$.

5) Si G est un schéma en monoïdes affine sur K, et C la bigèbre correspondante (cf. n° 3.1), la notion de comodule sur C coïncide avec celle de *représentation linéaire de* G (ou G-module), cf. n° 3.2, ainsi que SGAD, exposé I.

DÉFINITION 2. *Soient* E_1 *et* E_2 *deux comodules. On appelle* C*-morphisme (ou simplement morphisme) de* E_1 *dans* E_2 *toute application linéaire* $f : E_1 \to E_2$ *telle que*

$$(*) \qquad (1_C \otimes f) \circ d_{E_1} = d_{E_2} \circ f\,.$$

Les C-morphismes de E_1 dans E_2 forment un sous-K-module de $\mathrm{Hom}(E_1, E_2)$; on le note $\mathrm{Hom}^C(E_1, E_2)$.

On note Com_C la catégorie des C-comodules (à gauche); l'addition des C-morphismes munit Com_C d'une structure de *catégorie additive*.

1.3. Une formule d'adjonction

On conserve les notations précédentes. Soit V un K-module; d'après le n° 1.2, Exemples 1 et 3, on a une structure naturelle de comodule sur $C \otimes V$, le coproduit correspondant étant $d \otimes 1_V$.

Soit d'autre part E un comodule. Définissons une application linéaire

$$\theta : \mathrm{Hom}(E, V) \to \mathrm{Hom}^C(E, C \otimes V)$$

par

$$\theta(g) = (1_C \otimes g) \circ d_E\,, \qquad \text{si} \qquad g \in \mathrm{Hom}(E, V)\,.$$

Cela a un sens, car d_E est un morphisme de E dans $C \otimes E$, et $1_C \otimes g$ est un morphisme de $C \otimes E$ dans $C \otimes V$.

Proposition 1. *L'application* $\theta : \mathrm{Hom}(E, V) \to \mathrm{Hom}^C(E, C \otimes V)$ *est un isomorphisme.*

Soit $f : E \to C \otimes V$ un morphisme. En composant f avec $e \otimes 1_V$: $C \otimes V \to V$, on obtient un élément $\varepsilon(f)$ de $\mathrm{Hom}(E, V)$. On a ainsi défini une application linéaire

$$\varepsilon : \mathrm{Hom}^C(E, C \otimes V) \to \mathrm{Hom}(E, V)$$

et il suffit de prouver que θ et ε sont inverses l'un de l'autre. Tout d'abord, si $g \in \mathrm{Hom}(E, V)$, on a:

$$\begin{aligned}\varepsilon(\theta(g)) &= (e \otimes 1_V) \circ \theta(g) = (e \otimes 1_V) \circ (1_C \otimes g) \circ d_E \\ &= (e \otimes g) \circ d_E = g \circ (e \otimes 1_E) \circ d_E \\ &= g \circ 1_E = g\,,\end{aligned}$$

ce qui montre bien que $\varepsilon \circ \theta = 1$.

D'autre part, si $f \in \mathrm{Hom}^C(E, C \otimes V)$, on a:

$$\begin{aligned}\theta(\varepsilon(f)) &= (1_C \otimes \varepsilon(f)) \circ d_E = (1_C \otimes ((e \otimes 1_V) \circ f)) \circ d_E \\ &= (1_C \otimes e \otimes 1_V) \circ (1_C \otimes f) \circ d_E \\ &= (1_C \otimes e \otimes 1_V) \circ (d \otimes 1_V) \circ f \\ &= (((1_C \otimes e) \circ d) \otimes 1_V) \circ f \\ &= (1_C \otimes 1_V) \circ f = f\,,\end{aligned}$$

ce qui montre bien que $\theta \circ \varepsilon = 1$, cqfd.

[Ce qui précède est un bon exemple d'un principe général: tout calcul relatif aux cogèbres est trivial et incompréhensible.]

Exemples

1) Prenons $V = E$ et $g = 1_E$; l'élément correspondant de $\mathrm{Hom}^C(E, C \otimes E)$ est le coproduit $d_E \colon E \to C \otimes E$.

2) Prenons $V = K$. On obtient une bijection $\theta \colon E' \to \mathrm{Hom}^C(E, C)$. La bijection réciproque associe à tout morphisme $f \colon E \to C$ la forme linéaire $e \circ f$.

1.4. Conséquences d'une hypothèse de platitude

A partir de maintenant, on suppose que C est *plat* (comme K-module). Si V est un sous-module d'un module W, on identifie $C \otimes V$ au sous-module correspondant de $C \otimes W$, et $C \otimes (W/V)$ à $(C \otimes W)/(C \otimes V)$.

Définition 3. *Soit E un C-comodule, et soit V un sous-module de E. On dit que V est stable par C (ou que c'est un sous-comodule de E) si d_E applique V dans $C \otimes V$.*

Si tel est le cas, on vérifie tout de suite que l'application $d_V \colon V \to C \otimes V$ induite par d_E fait de V un comodule (d'où la terminologie); on définit de même le comodule quotient E/V.

Exemples

1) Soit $(V_i)_{i \in I}$ une famille de sous-modules du comodule E. Si les V_i sont stables par C, il en est de même de $\sum_{i \in I} V_i$ (resp. de $\bigcap_{i \in I} V_i$ lorsque I est fini). Cela résulte des formules:

$$C \otimes (\sum V_i) = \sum (C \otimes V_i)$$

et

$$C \otimes (\cap V_i) = \cap (C \otimes V_i)\,, \quad I \text{ fini}\,,$$

cf. *Alg. Comm.*, chap. I, §2.

2) Si E est un comodule, le morphisme $d_E \colon E \to C \otimes E$ *identifie E à un sous-comodule de $C \otimes E$* (muni du coproduit $d \otimes 1_E$, cf. n° 1.3). On notera que ce sous-comodule est même *facteur direct* dans $C \otimes E$ comme K-module (mais pas en général comme comodule), en vertu de la formule (2) de la définition 1.

Proposition 2. *Soit $f \colon E_1 \to E_2$ un morphisme de comodules. Alors* $\mathrm{Ker}(f)$ *et* $\mathrm{Im}(f)$ *sont stables par C; de plus, f définit par passage au quotient un isomorphisme du comodule* $E_1/\mathrm{Ker}(f)$ *sur le comodule* $\mathrm{Im}(f)$.

Puisque C est plat, $C \otimes \mathrm{Ker}(f)$ est le noyau de $1_C \otimes f$ et $C \otimes \mathrm{Im}(f)$ en est l'image. On en déduit aussitôt que $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont stables par C. Le fait que f définisse un isomorphisme de $E_1/\mathrm{Ker}(f)$ sur $\mathrm{Im}(f)$ est immédiat.

COROLLAIRE 1. *La catégorie* Com_C *est une catégorie abélienne et le foncteur «module sous-jacent» est exact.*

C'est clair.

Remarque. Il est non moins clair que le foncteur «module sous-jacent» commute aux limites projectives finies et aux limites inductives quelconques.

COROLLAIRE 2. *Si* V *est un K-module injectif, le comodule* $C \otimes V$ *est injectif dans* Com_C.

En effet, la proposition 1 montre que le foncteur

$$E \mapsto \mathrm{Hom}^C(E, C \otimes V)$$

est exact.

PROPOSITION 3. *Soit* V *un sous-module d'un comodule* E, *et soit* V^o *l'ensemble des éléments* $x \in E$ *tels que* $d_E(x)$ *appartienne à* $C \otimes V$. *Alors* V^o *est un sous-comodule de* E; *c'est le plus grand sous-comodule de* E *contenu dans* V.

Il faut d'abord prouver que V^o est stable par C, i.e. que d_E applique V^o dans $C \otimes V^o$. Or V^o est défini comme le noyau de l'homomorphisme $E \to C \otimes E \to C \otimes (E/V)$, la première flèche étant d_E. Puisque C est plat, il s'ensuit que $C \otimes V^o$ est le noyau de l'homomorphisme

$$C \otimes E \to C \otimes C \otimes E \to C \otimes C \otimes (E/V)\ ,$$

la première flèche étant $1_C \otimes d_E$. Pour prouver que $d_E(V^o)$ est contenu dans $C \otimes V^o$, il suffit donc de vérifier que le composé

$$V^o \to C \otimes E \to C \otimes C \otimes E \to C \otimes C \otimes (E/V)$$

est nul. Mais, d'après l'axiome (1) de la déf. 1, le composé $(1_C \otimes d_E) \circ d_E$ est égal à $(d \otimes 1_E) \circ d_E$. Or d_E applique V^o dans $C \otimes V$ par construction; l'image de V^o dans $C \otimes C \otimes E$ est donc contenue dans $(d \otimes 1_E)(C \otimes V)$, donc dans $C \otimes C \otimes V$, et son image dans $C \otimes C \otimes (E/V)$ est bien nulle.

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 (puique 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 $d_X : X \to X \otimes X$ 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:

$$\sum (X_i \otimes X_i) \subset (\sum X_i) \otimes (\sum X_i)$$
$$\bigcap (X_i \otimes X_i) = (\bigcap X_i) \otimes (\bigcap X_i) .$$

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 $f: D \to C$ 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 $E \otimes E' \to C$ 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 $\mathrm{Im}(d_E) \subset X \otimes E$.

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 $E \otimes E' \to C$; 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).

THÉORÈME 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 $A \to X'$ est l'orthogonal $\mathfrak{a}_X$ de X dans A; c'est un idéal bilatère ouvert de codimension finie. Inversement, soit $\mathfrak{a}$ un tel idéal de A, et soit X son orthogonal dans C. On a $X = (A/\mathfrak{a})'$; la structure d'algèbre de $A/\mathfrak{a}$ 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

Com_C^f la catégorie des C-comodules à gauche de rang fini,

Mod_A^f la catégorie des A-modules à gauche de rang fini, dont l'annulateur est ouvert (i.e. qui sont des A-modules topologiques si on les munit de la topologie discrète).

Si $E \in \mathrm{Com}_C^f$, l'application $E \to C \otimes E$ définit par dualité une application $A \otimes E' \to E'$, 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* Com_C^f *sur la catégorie opposée à* 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^o-module à gauche. En combinant cette remarque avec la prop. 2, on obtient:

COROLLAIRE. *La catégorie* Com_C^f *est isomorphe à la catégorie* $\mathrm{Mod}_{A^0}^f$.

Remarque. Soit $E \in \mathrm{Com}_C^f$; 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) $$< d_E(x),\ a \otimes x' > \ = \ < x, ax' > \ = \ < xa, x' >$$

et

(2) $$< d_E^{(2)}(x),\ a \otimes b \otimes x' > \ = \ < x, abx' > \ = \ < xab, x' > ,$$

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 $E \in \mathrm{Com}_C^f$, la sous-cogèbre C_E de C attachée à E (cf. n° 2.1) est la duale de la sous-algèbre de $\mathrm{End}(E)$ 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* 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_α est une famille de représentants des classes de comodules simples sur C, la cogèbre C est somme directe des cogèbres C_{E_α}, 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) Com^f_C *est semi-simple, et tout objet simple de* Com^f_C *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 $\mathrm{car}(K) = 0$. Mais, bien entendu, il ne donne que la structure de *cogèbre* de la bigèbre en question, pas sa structure d'algèbre.]

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

$$\mathrm{End}(E) \to C \quad (\text{cf. n° } 1.2)$$

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 $C'_E \subset \mathrm{End}(E)$, et la forme $u \mapsto \mathrm{Tr}(u)$, étant une forme linéaire sur C'_E, s'identifie à un élément de C_E qui n'est autre que θ_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 mutiplicités).

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 $\mathrm{car}(K) \neq 0$. Par exemple, si les E_α sont des comodules absolument simples deux à deux non isomorphes, les θ_α 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 Com^f_C.

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 Com^f_D sur une sous-catégorie abélienne $\tilde{D}$ de Com^f_C.

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* Com_C^f *vérifiant les conditions suivantes:*

1) L *est pleine* (i.e. si $E, F \in L$, on a $\mathrm{Hom}^L(E, F) = \mathrm{Hom}^C(E, F)$),

2) L *est stable par sommes directes finies,*

3) *Tout objet de* 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 $E \in \mathrm{ob}(L)$.]

Soit Θ 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 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* $n \geqslant 0$ *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 $x_1, \ldots, x_n$, l'application $b \mapsto (bx_1, \ldots, bx_n)$ 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 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 $n = \mathrm{rang}(F)$. D'autre part, C_E est isomorphe, comme comodule, à un quotient de $E \otimes E'$, c'est-à-dire de E^m, où $m = \mathrm{rang}(E)$. D'où le résultat.

Exemples

1) La sous-catégorie de Com^f_C 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 Com^f_C

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, $\mathrm{Hom}^M(E, F)$ est muni d'une structure de K-espace vectoriel, la composition des morphismes étant bilinéaire.

b) On se donne un foncteur $v: M \to \mathrm{Vect}^f_K$ 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 $v: \mathrm{Hom}^M(E, F) \to \mathrm{Hom}(v(E), v(F))$ 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* Com^f_C, *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 $\mathrm{Hom}^{M}(E, F)$ 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 $\upsilon(E)$; l'ensemble des sous-objets de E s'identifie ainsi à un sous-ensemble réticulé de l'ensemble des sous-espaces vectoriels de $\upsilon(E)$; 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 $\upsilon(F) \supset X$ 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 $n = \mathrm{rang}_K\, \upsilon(E)$.

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

$$\mathrm{rang}_K\, \upsilon(F) \leqslant n^2 .$$

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 $x \in \upsilon(F)$ engendrant F et soit x_1 un élément de $\upsilon(F_1)$ dont l'image dans $\upsilon(F)$ est x. Soit G le plus petit sous-objet de E^m tel que $\upsilon(G)$ 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 $\mathrm{rang}_K\, \upsilon(G) \leqslant n^2$. Si $m \leqslant n$, c'est évident. Supposons donc que $m > n$. On a $x_1 \in \upsilon(G) \subset \upsilon(E^m) = \upsilon(E)^m$. Soient $y_1, \ldots, y_m$ les composantes de x_1, considéré comme élément de $\upsilon(E)^m$. 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 $E^m \to E$; 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 $x_1 \in \upsilon(N)$, 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 $x \in \upsilon(P)$, et tel que $\upsilon(P)$ 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 $f: P \to F$ 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 $Q \to F$ induit par pr_1 est surjectif, du fait que P est engendré par x. On a donc

$$\mathrm{rang}_K\, v(Q) \geqslant \mathrm{rang}_K\, v(P) ;$$

mais le caractère maximal de $v(P)$ entraîne qu'il y a égalité; le morphisme $Q \to P$ est donc un isomorphisme. En composant son inverse avec la seconde projection $Q \to F$, 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* $\varphi: \mathrm{Mod}^f_{A^0} \to M$ *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:

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

où α est une $p \times q$-matrice à coefficients dans A. Cette matrice définit un morphisme $P^p \to P^q$ et l'on prend pour $\varphi(H)$ le *conoyau* de ce morphisme. On prolonge de façon évidente φ en un foncteur $\mathrm{Mod}^f_{A^0} \to M$ 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 $F \mapsto \mathrm{Hom}^M(P, F)$. 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 φ 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 $A_N = \operatorname{End}(P_N)$. Si $N_1 \supset N_2$, il existe un unique morphisme $P_{N_1} \to P_{N_2}$ 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 $A_{N_1} \to A_{N_2}$ 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 $P \in \operatorname{Pro} M$ 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 $d: C \to C \otimes C$ et d'une structure d'algèbre $m: C \otimes C \to C$, 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 $m: C \otimes C \to C$ 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 $e: C \to K$.

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

(iv) La co-unité $e: C \to K$ 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 $G = \mathrm{Spec}(C)$. Pour tout $K_1 \in \mathrm{Alg}_K$, 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 $K_1 \in \mathrm{Alg}_K$, $G(K_1)$ 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 $i: C \to C$ 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 $c \mapsto e(c).1$ de C.

La condition a) permet d'interpréter i comme un morphisme $I: G \to G$ et la condition b) signifie que $x.I(x) = e$ 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^o. L'existence de i revient à dire que G est un *schéma en groupes*.

Remarque. L'application identique $C \to C$ 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 $K_1 \in \mathrm{Alg}_K$, nous noterons $\mathrm{End}_E(K_1)$ le monoïde des endomorphismes du K_1-module $K_1 \otimes E$, et $\mathrm{Aut}_E(K_1)$ le groupe des éléments inversibles de $\mathrm{End}_E(K_1)$. Si $K_1 \to K_2$ est un morphisme, on définit de manière évidente le morphisme correspondant de $\mathrm{End}_E(K_1)$ dans $\mathrm{End}_E(K_2)$. 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 $G = \mathrm{Spec}(C)$ 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 $K_1 \in \mathrm{Alg}_K$, d'un morphisme de monoïdes $\rho(K_1): G(K_1) \to \mathrm{End}_E(K_1)$ et, si $K_1 \to K_2$ est un morphisme dans Alg_K, le diagramme

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

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) $G \to \mathrm{End}_E$ est appelé un *G-module* à gauche (resp. à droite).

Remarque. Si G est un schéma en groupes, et si $\rho: G \to \mathrm{End}_E$ 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 $\mathrm{Alg}_K \xrightarrow{G} \mathrm{Mon} \to \mathrm{Ens}$); définissons de même $\mathrm{End}_E^{\mathrm{ens}}$. Soit ρ un morphisme de G^{ens} dans $\mathrm{End}_E^{\mathrm{ens}}$. 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 $d(\rho): E \to C \otimes E$.

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

(b) *Pour que* $\rho: G^{\mathrm{ens}} \to \mathrm{End}_E^{\mathrm{ens}}$ *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

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

(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 $G^{\mathrm{ens}} \times G^{\mathrm{ens}}$ 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 $\mathrm{End}_E(C \otimes C)$ coïncident. Or l'image de $\gamma_1 \times \gamma_2$ dans $G(C \otimes C)$ est le point donné par $d: C \to C \otimes C$; son image dans $\mathrm{End}_E(C \otimes C)$, identifié à $\mathrm{Hom}(E, C \otimes C \otimes E)$ est donc $(d \otimes 1_E) \circ d(\rho)$. Il faut ensuite calculer l'image de $\gamma_1 \times \gamma_2$ par $G \times G \xrightarrow{\rho \times \rho} \mathrm{End}_E \times \mathrm{End}_E \xrightarrow{\beta} \mathrm{End}_E$. 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 $\varphi \in \mathrm{End}_E(C \otimes C)$ 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 $(\gamma_i \otimes 1_E) \circ d(\rho): E \to C \otimes E \to C \otimes C \otimes E$. Soit alors $x \in E$, et posons:

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

On a:

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

De même:

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

D'où:

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

D'autre part, on a

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

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 $m : C \otimes C \to C$ 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

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

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*

$$C_{E \otimes F} = C_E \,.\, C_F \,. \tag{*}$$

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 $m: C \otimes C \to C$, c'est bien $C_E \,.\, C_F$.

Le fait que D contienne 1 provient de ce que $C_E = K \,.\, 1$ 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:

$$C_{E^\vee} = i(C_E) \,. \tag{**}$$

COROLLAIRE. *Supposons que $G = \mathrm{Spec}(C)$ 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 $L = \mathrm{Mod}_H^f$, 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 $M = \mathrm{Com}^f_D$ correspondante (la donnée de D est d'ailleurs équivalente à celle du couple formé de M et du foncteur $\upsilon : M \to \mathrm{Vect}_K$, cf. n° 2.5, th. 3). En imposant à ce produit tensoriel des conditions raisonnables (en particulier $\upsilon(E \otimes F) \simeq \upsilon(E) \otimes \upsilon(F)$) 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 υ = 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 $K_1 \in \mathrm{Alg}_K$ et soit $g \in G(K_1)$ un point de G à valeurs dans K_1. Pour tout $E \in \mathrm{Com}^f_C$, notons $g(E)$ l'image de g par l'antireprésentation

$$\rho(E) : G(K_1) \to \mathrm{End}_E(K_1) .$$

On a donc $g(E) \in \mathrm{End}_E(K_1) = \mathrm{End}_{K_1}(K_1 \otimes E)$, 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* $\upsilon_{K_1} : \mathrm{Com}^f_C \to \mathrm{Mod}_{K_1}$ *le foncteur qui associe à tout* $E \in \mathrm{Com}^f_C$ *le* K_1*-module* $K_1 \otimes E$. *Soit* $\varphi : \upsilon_{K_1} \to \upsilon_{K_1}$ *un endomorphisme de* υ_{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 $G(K_1) \to \mathrm{End}(\upsilon_{K_1})$ 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* υ_{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) $g(\check{E}) = g(E)^{\vee}$.

Démonstration de la proposition 4.

Tout d'abord, soit $u \in \mathrm{Hom}(C, K_1)$. Pour tout $E \in \mathrm{Com}_C$, 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* $\mathrm{Hom}(C, K_1)$ *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 $\mathrm{Hom}(C, K_1)$ la structure d'algèbre opposée de celle à laquelle on pense.]

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

$$C \to K_1 \otimes C \to K_1 \otimes C \to K_1$$

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

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

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 $u \in \mathrm{Hom}(C, K_1)$, $u(\varphi_u)$ 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 $\varphi \in \mathrm{End}(v_{K_1})$. 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 $E \in \mathrm{Com}_C$. Comme $d_E : E \to C \otimes E$ est un morphisme de comodules, on a un diagramme commutatif:

$$\begin{array}{ccccc} E \to & K_1 \otimes E & \overset{1 \otimes d_E}{\to} & K_1 \otimes C \otimes E & \\ & \varphi(E) \downarrow & & \varphi(C) \otimes 1 \downarrow & \\ & K_1 \otimes E & \underset{1 \otimes d_E}{\to} & K_1 \otimes C \otimes E & \overset{1 \otimes C \otimes 1}{\to} \quad K_1 \otimes E . \end{array}$$

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

$$E \to K_1 \otimes E \overset{\varphi(E)}{\to} K_1 \otimes E$$

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 $\mathrm{Com}^f_C = \mathrm{Com}^f_{A^o}$ 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′) $\varphi_u(C \otimes C) = \varphi_u(C) \otimes \varphi_u(C)$.

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

$$d(a) = \sum a_i \otimes x_i , \quad a_i \in C$$
$$d(b) = \sum b_j \otimes x_j , \quad b_j \in C .$$

On a alors:

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

et

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

D'où:

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

Soit d'autre part $d' : C \otimes C \to C \otimes C \otimes C$ 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

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

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 $x_o = 1$ pour un élément $0 \in I$ et $e(x_i) = 0$ pour $i \neq 0$. On a alors $a_o = a$ et $b_o = b$, 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 $u : C \to K_1$ 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 $\mathrm{End}(\upsilon)$ formée des endomorphismes θ de υ tels que

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

3.5. Interprétation de G comme limite projective de groupes algébriques 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 $n \geqslant 0$, soit $C_E(n)$ la sous-cogèbre attachée au comodule $\overset{n}{\otimes} E$; pour $n = 0$, on convient comme d'ordinaire que $\overset{n}{\otimes} E = K$, de sorte que $C_E(0) = K.1$. On sait (cf. lemme 1) que

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

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. $\mathbf{GL}_E$) des endomorphismes (resp. automorphismes) de E contenant l'image de la représentation $\rho : G \to \mathrm{End}_E$ 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 $G \to G_E$ 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* $\overset{n}{\otimes}(E \oplus \check{E})$.

Cela résulte du lemme 1 du n° 2.4.

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

Remarques

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

2) Il se peut que G_E soit fermé dans End_E (et non pas seulement dans $\mathbf{GL}_E$), autrement dit que $C(E) = C(E \oplus \check{E})$. C'est le cas, par exemple, si G_E est contenu dans $\mathbf{SL}_E$. 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 $\mathfrak{a} \in S_g$ par exemple, l'annulateur du A-module $A/\mathfrak{a}$ appartient à S et est contenu dans $\mathfrak{a}$.

On posera:

$$\hat{A} = \varprojlim . A/\mathfrak{a}$$

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 des A-modules de rang fini sur celle des $\hat{A}$-modules topologiques discrets de rang fini.

Soit F le dual de A; on le munit de sa structure naturelle de A-bimodule. Si $\mathfrak{a} \in S$, soit $F_{\mathfrak{a}}$ l'orthogonal de $\mathfrak{a}$ dans F. Soit C la réunion des $F_{\mathfrak{a}}$, pour $\mathfrak{a} \in S$. Le dual de C (resp. le dual topologique de $\hat{A}$) s'identifie de façon évidente à $\hat{A}$ (resp. à C). D'après le n° 2.2, il y a donc sur C une structure de *cogèbre*, caractérisée par la formule:

(1) $$< d(c), a \otimes b > \; = \; < c, ab > \quad \text{si} \quad c \in C, a, b \in A\ .$$

De plus, tout A-module à droite de rang fini est muni canoniquement d'une structure de comodule à gauche sur C, et réciproquement; on a

(2) $$< d_E(x), a \otimes x' > \; = \; < xa, x' > \quad \text{si} \quad x \in E, x' \in E', a \in A$$

d'après la formule (1) du n° 2.2.

Les éléments de la cogèbre C peuvent être caractérisés de la manière suivante:

LEMME 1. *Soit f un élément du dual F de A. Les conditions suivantes sont équivalentes:*

(a) $f \in C$.

(b) (resp. (b′)) *Le sous-A-module à gauche* (resp. à droite) *de F engendré par f est de rang fini.*

(c) *Il existe un A-module à droite E de rang fini, et des éléments $x_i \in E, x_i' \in E'$ en nombre fini, tels que*

$$< f, a > \; = \; \sum < x_i a, x_i' > \quad \textit{pour tout} \quad a \in A\ .$$

La condition (b) signifie que l'annulateur de f dans le A-module à gauche F appartient à S_g; comme S est cofinal dans S_g, cela revient à dire que f appartient à C. On démontre de même que (a) $\Leftrightarrow$ (b′).

D'autre part, pour un module E donné, la condition (c) signifie que f appartient à la sous-cogèbre C_E de C attachée à E (cf. n° 2.1). Comme C est réunion des C_E, cela prouve que (a) $\Leftrightarrow$ (c).

[On laisse au lecteur le plaisir de démontrer directement l'équivalence (b) $\Leftrightarrow$ (c).]

4.2. LA BIGÈBRE D'UN GROUPE

On applique ce qui précède à l'algèbre $A = K[\Gamma]$ d'un groupe Γ. Le dual $F = F(\Gamma)$ de A est *l'espace des fonctions* sur Γ; la dualité entre A et F s'exprime par la formule:

$$< f, \sum \lambda_i \gamma_i > \; = \; \sum \lambda_i f(\gamma_i) \quad \text{si} \quad f \in F, \lambda_i \in K, \gamma_i \in \Gamma\ .$$

La cogèbre correspondante est notée $C = C(\Gamma)$. Elle jouit des propriétés suivantes:

(i) La co-unité de C est l'application $e : f \mapsto f(1)$.

(ii) Pour qu'une fonction f appartienne à C, il faut et il suffit que *ses translatées* (à gauche ou à droite) *engendrent un K-espace vectoriel de dimension finie.* (C'est l'équivalence (a) $\Leftrightarrow$ (b) du Lemme 1.)

(iii) Identifions à la façon habituelle les éléments de $F \otimes F$ aux *fonctions décomposables* sur $\Gamma \times \Gamma$. Si $f \in C$, on a $d(f) \in C \otimes C$ et $C \otimes C$ est un sous-espace de $F \otimes F$; ainsi $d(f)$ peut être interprétée comme une fonction sur $\Gamma \times \Gamma$. *On a*:

$$d(f)(\gamma_1, \gamma_2) = f(\gamma_1 \gamma_2) \quad \text{si} \quad \gamma_1, \gamma_2 \in \Gamma . \tag{3}$$

(Cela ne fait que traduire la formule (1) du n° précédent.)

(iv) C contient 1, et est stable par le *produit*: cela résulte de (ii).

(v) Les structures de cogèbre et d'algèbre de C sont *compatibles* entre elles, i.e. elles font de C une *bigèbre.* Cette bigèbre vérifie les axiomes du n° 3.1. (L'axiome (i) dit que $f \mapsto d(f)$ doit être un morphisme d'*algèbres*; c'est le cas. Les autres axiomes sont encore plus évidents.)

(vi) La bigèbre C possède une *inversion* i donnée par

$$i(f)(\gamma) = f(\gamma^{-1}) . \tag{4}$$

(Il faut vérifier les conditions (a) et (b) du n° 3.1. La condition (a) est évidemment satisfaite. Pour (b), soit $f \in C$ et écrivons $d(f)$ sous la forme $\sum_\alpha g_\alpha \otimes h_\alpha$. On a

$$(1_C \otimes i)(d(f)) = \sum g_\alpha \otimes i(h_\alpha)$$

et l'on doit voir que $\sum g_\alpha . i(h_\alpha) = e(f) . 1$. Or, si $\gamma \in \Gamma$, on a

$$\begin{aligned} \sum g_\alpha(\gamma) i(h_\alpha)(\gamma) &= \sum g_\alpha(\gamma) h_\alpha(\gamma^{-1}) = d(f)(\gamma, \gamma^{-1}) \\ &= f(\gamma . \gamma^{-1}) = f(1) = e(f) , \end{aligned}$$

d'où la formule voulue.)

(vii) Soit $G = \operatorname{Spec}(C)$ le *schéma en groupes* attaché à C. Tout élément $\gamma \in \Gamma$ définit un morphisme $f \mapsto f(\gamma)$ de C dans K, donc un élément du groupe $G(K)$ des points de G à valeurs dans K. *L'application* $\Gamma \to G(K)$ *ainsi définie est un homomorphisme*; cela résulte de la définition de la loi de composition de $G(K)$.

(viii) D'après le n° 4.1, tout Γ-module à droite E de rang fini est muni canoniquement d'une structure de C-comodule à gauche de rang fini (et inversement). Plus précisément, si $(v_i)_{i \in I}$ est une base de E, et si l'on a

$$v_i\gamma = \sum_{j \in I} c_{ij}(\gamma)v_j \ , \qquad \text{avec} \qquad c_{ij} \in C \ , \tag{5}$$

le coproduit de E est donné par:

$$d_E(v_i) = \sum_{j \in I} c_{ij} \otimes v_j \ . \tag{6}$$

(ix) La correspondance définie ci-dessus entre Γ-modules à droite de rang fini et C-comodules à gauche de rang fini est *compatible* avec les opérations «produit tensoriel» et «contragrédiente»; cela résulte de ce qui a été dit au n° 3.2, combiné avec (vii) ci-dessus.

Remarque. On peut caractériser $G = \mathrm{Spec}(C)$ par la propriété universelle suivante: tout homomorphisme de Γ dans le groupe $H(K)$ des K-points d'un schéma en groupe affine H se prolonge de manière unique en un morphisme $G \to H$. Le foncteur $\Gamma \mapsto G$ est donc *adjoint* du foncteur $H \mapsto H(K)$.

4.3. L'enveloppe d'un groupe relativement à une catégorie de représentations

On conserve les notations du numéro précédent.

DÉFINITION 1. *Soit L une sous-catégorie pleine de la catégorie des Γ-modules à gauche de rang fini. On dit que L est saturée si L vérifie les conditions suivantes:*

a) *Si $E \in L$ et si F est isomorphe, soit à un quotient de E, soit à un sous-objet de E, on a $F \in L$.*

b) *L est stable par somme directe finie, produit tensoriel et contragrédiente.*

c) *La représentation unité (de module K) appartient à L.* (Bien entendu, on a une notion analogue pour les Γ-modules à droite.)

THÉORÈME 1. *Si L est saturée, il existe une sous-bigèbre C_L de $C(\Gamma)$ et une seule telle que L soit la catégorie des C_L-comodules à droite de rang fini. La bigèbre C_L contient l'élément* 1, *vérifie les axiomes du* n° 3.1, *et est stable par l'inversion i.*

Cela résulte des props. 2 et 3 du n° 3.3.

DÉFINITION 2. *Le schéma* $G_L = \mathrm{Spec}(C_L)$ *est appelé l'enveloppe de* Γ *relativement à la catégorie saturée* L.

Les propriétés suivantes de G_L résultent de sa définition et de ce qui a été démontré dans les paragraphes précédents:

a) G_L est un quotient du schéma en groupes G défini au n° précédent.

b) On a un homomorphisme canonique $\Gamma \to G_L(K)$. De plus, tout sous-schéma fermé de G_L contenant l'image de Γ est égal à G_L (cela exprime simplement le fait que les éléments de C_L sont des *fonctions* sur Γ). En particulier, l'image de Γ dans $G_L(K)$ est dense pour la topologie de Zariski.

c) Le schéma G_L est absolument réduit.

d) La bigèbre C_L est réunion des cogèbres C_E attachées aux éléments E de L.

e) Si $E \in L$, soit G_E l'image de la représentation $\rho: G_L \to \mathbf{GL}_E$ attachée à E (cf. n° 3.5). Le groupe G_E est l'adhérence (pour la topologie de Zariski) de l'image de Γ dans $\mathbf{GL}_E(K) = \mathrm{Aut}(E)$.

f) Soient $E_1, E_2 \in L$. Pour qu'il existe un morphisme $G_{E_1} \to G_{E_2}$ tel que le diagramme

$$\begin{array}{ccc} & \Gamma & \\ \swarrow & & \searrow \\ G_{E_1}(K) & \to & G_{E_2}(K) \end{array}$$

soit commutatif, il faut et il suffit que E_2 soit isomorphe à un quotient d'une sous-représentation d'une somme directe de représentations $\otimes^n(E_1 \oplus \check{E}_1)$. L'homomorphisme $G_{E_1} \to G_{E_2}$ est alors unique.

g) On a $G = \varprojlim . G_E$ (vis-à-vis des morphismes définis ci-dessus).

h) Soit $K_1 \in \mathrm{Alg}_K$ et soit υ_{K_1} le foncteur de L dans Mod_{K_1} défini par $E \mapsto K_1 \otimes E$. Il y a une bijection canonique (cf. n° 3.4) du groupe $G_L(K_1)$ sur le groupe des automorphismes du foncteur υ_{K_1} commutant au produit tensoriel et triviaux sur le module unité K.

Remarque. La détermination explicite de G_L (pour Γ et L donnés) est souvent un problème non trivial. On en verra quelques exemples au §5 (voir aussi les exercices du §4).

Exemples

a) On peut prendre pour L la catégorie de *toutes* les représentations linéaires de Γ; le groupe G_L est alors le groupe G du numéro précédent.

b) Supposons que K soit un *corps topologique* (resp. *un corps valué complet non discret*) et que Γ soit muni d'une structure de *groupe topologique* (resp. de *groupe de Lie* sur K). On peut prendre pour L la catégorie des représentations *continues* (resp. *K-analytiques*) de rang fini. Une fonction $f \in C$ appartient à la bigèbre C_L correspondante si et seulement si elle est continue (resp. analytique): cela se vérifie sans difficulté. Le schéma G_L est appelé simplement *l'enveloppe* du groupe topologique Γ (resp. du groupe de Lie Γ). On peut le caractériser par la propriété universelle suivante: si H est un groupe algébrique linéaire, tout homomorphisme *continu* (resp. *analytique*) de Γ dans le groupe topologique (resp. de Lie) $H(K)$ se prolonge de façon unique en un morphisme de G_L dans H. Cela résulte simplement de la description de C_L donnée ci-dessus.

On notera que, même lorsque Γ est un groupe de Lie connexe de dimension finie, son enveloppe n'est pas en général un groupe algébrique (i.e. G_L ne possède en général pas de module *fidèle*, cf. exercice 1).

c) Soit k un corps complet pour une valuation discrète; on suppose k d'inégale caractéristique et de corps résiduel algébriquement clos. Soit $\bar{k}$ une clôture algébrique de k et soit $\Gamma = \mathrm{Gal}(\bar{k}/k)$. Prenons pour K le corps $\mathbf{Q}_p$ (p étant la caractéristique résiduelle de k), et pour L la catégorie des $\mathbf{Q}_p$-représentations de Γ qui ont une «décomposition de Hodge» au sens de Tate (Driebergen). La catégorie L est saturée. Le groupe G_L correspondant est fort intéressant [du moins pour le rédacteur — les auditeurs du Collège, qui l'ont subi pendant trois mois, sont peut-être d'un avis différent].

§ 5. Groupes compacts et groupes complexes

Dans ce paragraphe, le corps de base est $\mathbf{R}$ ou $\mathbf{C}$.

5.1. Algébricité des groupes compacts

Proposition 1. *Soit K un groupe compact, opérant linéairement et continûment sur un espace vectoriel réel V de dimension finie. Toute orbite de K dans V est fermée pour la topologie de Zariski de V* (relativement à $\mathbf{R}$).

Soit $x \in V$, et soit y un point de V n'appartenant pas à l'orbite Kx de x. Il nous faut construire une fonction polynomiale P sur V qui soit nulle sur Kx et non nulle en y. L'existence d'une telle fonction résulte du lemme plus précis suivant:

LEMME 1. *Il existe une fonction polynomiale* P *sur* V *qui prend les valeurs* 0 *en* x *et* 1 *en* y *et qui est invariante par* K.

Puisque Kx et Ky sont fermés et disjoints, il existe une fonction continue réelle f sur V qui vaut 0 sur Kx et 1 sur Ky. Comme les fonctions polynomiales sont denses dans les fonctions continues (pour la topologie de la convergence compacte), il existe une fonction polynomiale F sur V qui est $\leqslant 1/3$ sur Kx et $\geqslant 2/3$ sur Ky. Soit dk la mesure de Haar de K, normalisée de telle sorte que sa masse totale soit 1. La fonction F' définie par

$$F'(v) = \int_K F(k.v)\,dk$$

est une fonction polynomiale invariante par K; si a (resp. b) désigne la valeur de F' sur l'orbite Kx (resp. Ky), on a $a \leqslant 1/3$ et $b \geqslant 2/3$, d'où $a \neq b$. La fonction $P = \dfrac{F' - a}{b - a}$ répond alors à la question.

COROLLAIRE. *L'image de* K *dans* $\mathrm{Aut}(V)$ *est fermée pour la topologie de Zariski de* $\mathrm{End}(V)$ [et *a fortiori* pour celle de $\mathrm{Aut}(V)$].

En effet, K opère linéairement sur $\mathrm{End}(V)$ par

$$(k, u) \mapsto k.u \quad \text{si} \quad k \in K, u \in \mathrm{End}(V)\ ,$$

et K est l'orbite de $1_V \in \mathrm{End}(V)$; on peut donc appliquer la proposition à l'espace vectoriel $\mathrm{End}(V)$.

PROPOSITION 2. *Soit* G *un groupe algébrique linéaire sur* $\mathbf{R}$, *et soit* K *un sous-groupe compact de* $G(\mathbf{R})$. *Soit* H *le plus petit sous-groupe algébrique réel de* G *contenant* K. *On a alors*

$$K = H(\mathbf{R})\ .$$

En effet, on peut plonger G comme sous-groupe algébrique fermé dans un groupe linéaire $\mathbf{GL}_n$; la proposition résulte alors du corollaire ci-dessus.

Remarque. Le groupe H peut aussi être défini comme l'*adhérence* de K dans G (pour la topologie de Zariski); il est en effet immédiat que cette adhérence est un sous-schéma en groupes de G. La bigèbre de H est le quotient de celle de G par l'idéal formé des fonctions dont la restriction à K est nulle.

5.2. L'ENVELOPPE D'UN GROUPE COMPACT

Soit K un groupe compact. Considérons la catégorie L des représentations linéaires continues réelles de rang fini de K. Cette catégorie est *saturée* (cf. n° 4.3). Nous noterons G le schéma en groupes correspondant (sur $\mathbf{R}$) et C sa bigèbre. On dit que G est *l'enveloppe* de K, cf. n° 4.3, exemple b). Rappelons *(loc. cit.)* qu'une fonction réelle f sur K appartient à C si et seulement si elle vérifie les deux conditions suivantes:

a) Les translatées de f (à gauche, par exemple) engendrent un espace vectoriel réel de rang fini.

b) f est continue.

Rappelons également que l'on a défini un homomorphisme canonique

$$K \to G(\mathbf{R}) .$$

THÉORÈME 1. *L'homomorphisme* $K \to G(\mathbf{R})$ *est un isomorphisme.*

L'injectivité résulte du *théorème de Peter-Weyl,* que l'on admet.

Pour prouver la surjectivité, écrivons G comme limite projective des groupes algébriques G_E attachés aux éléments de L (cf. n° 4.3). On a évidemment

$$G(\mathbf{R}) = \varprojlim . G_E(\mathbf{R}) .$$

D'autre part, d'après la prop. 2, tous les homomorphismes

$$K \to G_E(\mathbf{R})$$

sont surjectifs. Il en est donc de même (grâce à la compacité) de $K \to \varprojlim . G_E(\mathbf{R})$, d'où le théorème.

PROPOSITION 3. *Soit* $E \in L$. *Pour que* E *soit une représentation fidèle de* K (au sens usuel, i.e. le noyau de $K \to \mathrm{Aut}(E)$ doit être réduit à $\{1\}$), *il faut et il suffit que* E *soit fidèle comme C-comodule* (cf. n° 3.5).

Si E est fidèle comme comodule, G s'identifie à G_E, donc K s'identifie à $G_E(\mathbf{R})$ et il est clair que E est fidèle comme représentation de K.

La réciproque provient de ce qui a été démontré au n° 3.5, combiné avec le lemme suivant:

LEMME 2 (Burnside). *Si* E *est fidèle, toute représentation irréductible continue de* K *est un facteur d'une représentation* $\overset{n}{\otimes} E$, *avec* $n \geqslant 0$ *convenable.*

Soit F une telle représentation, et soit χ le caractère d'une composante irréductible de $C \otimes F$. Si F n'était facteur d'aucune puissance tensorielle de E, les formules d'orthogonalité des coefficients de représentations montreraient que χ est orthogonal à tous les polynômes en les coefficients c_{ij} de la représentation E. Comme ces polynômes sont denses dans l'espace des fonctions continues sur K, on aurait $\chi = 0$, ce qui est absurde.

[Il n'est probablement pas nécessaire d'utiliser les relations d'orthogonalité. Peu importe.]

Remarque. L'analogue du lemme 2 dans le cas complexe est vrai, à condition de remplacer $\overset{n}{\otimes} E$ par $\overset{n}{\otimes} (E \oplus \check{E})$. La démonstration est essentiellement la même. [Dans le cas réel, l'existence d'une forme quadratique non dégénérée invariante montre que $\check{E}$ est isomorphe à E; c'est pour cela que l'on a pu se débarrasser de $\check{E}$.]

COROLLAIRE. *Lorsque E est fidèle, l'enveloppe de K s'identifie au groupe G_E.*

Cela ne fait que reformuler la proposition.

PROPOSITION 4. *Pour que G soit algébrique, il faut et il suffit que K soit un groupe de Lie.*

Si K est un groupe de Lie, le théorème de Peter-Weyl montre qu'il admet une représentation fidèle E; on a alors $G = G_E$ d'après le corollaire ci-dessus, et G est donc algébrique. Inversement, si G est algébrique, il est clair que $K = G(\mathbf{R})$ est un groupe de Lie.

DÉFINITION 1. *Un groupe algébrique linéaire réel H est dit anisotrope s'il vérifie les deux conditions suivantes:*

a) *$H(\mathbf{R})$ est compact.*

b) *$H(\mathbf{R})$ est dense pour la topologie de Zariski de H.*

(Comme $H(\mathbf{R})$ contient un voisinage de 1 dans H, la condition b) équivaut à la suivante:

b′) *Toute composante connexe (au sens algébrique) de H contient un point réel.*

En particulier, b) est vérifiée si H est *connexe*.)

Exemples

1) Un groupe semi-simple connexe est anisotrope si et seulement si la forme de Killing de son algèbre de Lie est négative.

2) Un groupe de type multiplicatif (non nécessairement connexe) est anisotrope si et seulement si tout homomorphisme de ce groupe dans le groupe multiplicatif $\mathbf{G}_m$ est trivial ou d'ordre 2. (La conjugaison complexe opère donc par $\chi \mapsto \chi^{-1}$ sur le groupe dual.)

PROPOSITION 5. *Soit H un groupe algébrique linéaire réel, et soit K un sous-groupe compact de $H(\mathbf{R})$ dense pour la topologie de Zariski. Alors H est anisotrope, on a $K = H(\mathbf{R})$ et H s'identifie à l'enveloppe de K.*

Le fait que H soit l'enveloppe de K résulte du corollaire à la prop. 3. On en déduit que $K = H(\mathbf{R})$, donc que H est anisotrope.

COROLLAIRE. *Soit H' un groupe algébrique linéaire réel, et soit φ un homomorphisme continu de K dans $H'(\mathbf{R})$. Il existe alors un morphisme $f: H \rightarrow H'$ et un seul qui prolonge φ.*

Cela ne fait que traduire le fait que H est l'enveloppe de K.

Remarque. Il est essentiel de supposer que H' est *linéaire* (prendre pour K un cercle, et pour H' une courbe elliptique!).

PROPOSITION 6. *Le foncteur «enveloppe» est une équivalence de la catégorie des groupes de Lie compacts sur celle des groupes algébriques linéaires réels anisotropes.*

C'est clair.

Remarques

1) Le foncteur «enveloppe» jouit des propriétés explicitées au n° 4.3. En particulier, les éléments de $G(\mathbf{R}) = K$ peuvent être interprétés comme les automorphismes du foncteur «espace vectoriel sous-jacent» commutant au produit tensoriel et triviaux pour le module trivial $\mathbf{R}$. [Ce n'est pas tout à fait le *théorème de dualité de Tannaka*, car ce dernier est relatif à des représentations complexes *unitaires*, et à des automorphismes *unitaires*. Il devrait y avoir moyen de passer de l'un à l'autre. Au concours!]

2) Si K est un groupe de Lie compact, il n'y a pas lieu de distinguer entre son enveloppe en tant que *groupe topologique*, ou en tant que *groupe de Lie réel*, puisque toute représentation linéaire continue d'un groupe de Lie réel est analytique. En particulier, les éléments de la bigèbre de K sont des *fonctions analytiques* sur K.

5.3. L'ENVELOPPE COMPLEXE D'UN GROUPE COMPACT

Soit K un groupe compact. Soit $L_{\mathbf{C}}$ la catégorie des représentations linéaires *complexes* continues de rang fini de K. Cette catégorie est saturée (le corps de base étant maintenant $\mathbf{C}$). Nous noterons $G_{/\mathbf{C}}$ et $C_{/\mathbf{C}}$ le schéma en groupes et la bigèbre correspondants, et nous dirons que $G_{/\mathbf{C}}$ est *l'enveloppe complexe* de K. D'après le n° 4.3, une fonction complexe f sur K appartient à $C_{/\mathbf{C}}$ si et seulement si elle vérifie les conditions suivantes:

a') Les translatées de f engendrent un espace vectoriel de rang fini.

b') f est continue.

En comparant avec les conditions a) et b) du n° 5.2, on voit que cela signifie que la partie réelle et la partie imaginaire de f appartiennent à la bigèbre C de G. On a donc

$$C_{/\mathbf{C}} = \mathbf{C} \otimes_{\mathbf{R}} C$$

et le groupe $G_{/\mathbf{C}}$ est le *schéma en groupes déduit de* G *par extension des scalaires de* $\mathbf{R}$ *à* $\mathbf{C}$. En particulier, le groupe $G_{/\mathbf{C}}(\mathbf{C})$ de ses points complexes peut être identifié à $G(\mathbf{C})$.

Noter que la conjugaison complexe définit une *involution* $g \mapsto \bar{g}$ de $G(\mathbf{C})$, dont l'ensemble des invariants est $G(\mathbf{R}) = K$. Plus précisément:

THÉORÈME 2. *Supposons que* K *soit un groupe de Lie compact, et soit* $\mathfrak{k}$ *son algèbre de Lie. Alors* $g \mapsto \bar{g}$ *est une involution de Cartan forte* (cf. réd. n° 517) *du groupe de Lie* $G(\mathbf{C})$. *Les facteurs de la décomposition de Cartan correspondante sont* K *et* $P = \exp(i\mathfrak{k})$, *de sorte que* $G(\mathbf{C}) = K.P$.

Démonstration

a) On va d'abord vérifier le th. 2 dans le cas particulier du groupe *orthogonal* $G_1 = \mathbf{O}_n$. On a $G_1(\mathbf{R}) = \mathbf{O}_n(\mathbf{R})$, $G_1(\mathbf{C}) = \mathbf{O}_n(\mathbf{C})$, et l'on sait que $g \mapsto \bar{g}$ est une décomposition de Cartan forte de $\mathbf{O}_n(\mathbf{C})$ dont l'ensemble des invariants est $K_1 = \mathbf{O}_n(\mathbf{R})$. Cette décomposition montre en même temps que K_1 est dense dans $\mathbf{O}_n(\mathbf{C})$ pour la topologie de Zariski, donc que $\mathbf{O}_n$ est l'enveloppe de K_1.

b) Passons au cas général. On choisit un plongement de K dans un groupe orthogonal $K_1 = \mathbf{O}_n(\mathbf{R})$; l'enveloppe G de K s'identifie alors à un sous-groupe algébrique de $\mathbf{O}_n$, à savoir l'*adhérence* de K (pour la topologie de Zariski). Le groupe $G(\mathbf{C})$ est donc un sous-groupe de $G_1(\mathbf{C})$, stable par l'involution de Cartan considérée. Comme c'est un sous-groupe «de type algébrique», il en résulte (cf. réd. 517, p. 48, prop. 3) que la restriction de $g \mapsto \bar{g}$ à ce sous-groupe est bien une décomposition de Cartan forte. On sait déjà que le sous-groupe de ses invariants est K. D'autre part, l'algèbre de Lie de $G(\mathbf{C})$ est $\mathbf{C} \otimes \mathfrak{k}$, et l'automorphisme de $\mathbf{C} \otimes \mathfrak{k}$ induit par $g \mapsto \bar{g}$ est la conjugaison complexe; on en déduit que le facteur P correspondant est bien $\exp(i\mathfrak{k})$, c.q.f.d.

Remarques

1) Lorsque K est un groupe compact quelconque, on peut l'écrire comme limite projective de groupes de Lie compacts K_α, et l'on a $G(\mathbf{C}) = \varprojlim G_\alpha(\mathbf{C})$, avec des notations évidentes. D'après le th. 2, chaque $G_\alpha(\mathbf{C})$ a une décomposition de Cartan $K_\alpha . P_\alpha$, avec $P_\alpha = \exp(i\mathfrak{k}_\alpha)$. Finalement, on obtient une décomposition de $G(\mathbf{C})$ sous la forme $G(\mathbf{C}) = K . \exp(i\mathfrak{k})$, en notant $\mathfrak{k}$ la limite projective des $\mathfrak{k}_\alpha$.

[Cette décomposition ne semble présenter aucun intérêt en dehors du cas où K est un groupe de Lie. Noter que $G(\mathbf{C})$ n'est même pas localement compact, si $\dim(K) = \infty$.]

2) A la place du groupe $\mathbf{O}_n(\mathbf{R})$, on aurait pu utiliser le groupe unitaire $\mathbf{U}_n(\mathbf{C})$, plus traditionnel. Toutefois, il aurait fallu expliquer comment on considère $\mathbf{U}_n$ comme un groupe algébrique sur $\mathbf{R}$, et pourquoi $\mathbf{U}_{n/\mathbf{C}}$ s'identifie à $\mathbf{GL}_{n/\mathbf{C}}$.

THÉORÈME 3. *Les hypothèses étant celles du th. 2, soit X un groupe de Lie complexe, et soit f un homomorphisme continu de K dans X. Il existe alors un homomorphisme $F: G(\mathbf{C}) \to X$ de groupes de Lie complexes, et un seul, qui prolonge f.*

Soit $K_\mathbf{C}$ le groupe de Lie *complexifié* de K, au sens de la rédaction 515, §6, n° 10 [il faut modifier la rédaction en question, car elle suppose, bien inutilement, que le groupe de Lie réel dont on part est *connexe*]. On a un homomorphisme canonique $\pi : K_\mathbf{C} \to G(\mathbf{C})$, et le th. 3 équivaut à dire que π est un *isomorphisme.*

Il est clair en tout cas que π est surjectif; d'autre part, on sait *(loc. cit.)* que l'algèbre de Lie de $K_\mathbf{C}$ est engendrée sur $\mathbf{C}$ par $\mathfrak{k}$; puisque celle de $G(\mathbf{C})$ est $\mathfrak{k} \otimes \mathbf{C}$, on en conclut que π est un revêtement. Ce revêtement admet une section canonique $G(\mathbf{C}) = K . P \to K_\mathbf{C}$ définie par $x . \exp(it) \mapsto x' . \exp(it')$ où x désigne un élément de K, x' son image par $K \to K_\mathbf{C}$, t désigne un élément de $i\mathfrak{k}$ et t' son image par l'application tangente à $K \to K_\mathbf{C}$. L'image de cette section est $K' . P'$, avec des notations évidentes; c'est une réunion de composantes connexes de $K_\mathbf{C}$. De plus, c'est un *sous-groupe* en vertu du lemme suivant:

LEMME 3. *Soit A un groupe topologique, soit B un sous-groupe de A, et soit C la réunion des composantes connexes de A qui rencontrent B. Alors C est un sous-groupe de A.*

Si $x, y \in C$, il existe des parties connexes X, Y de A qui rencontrent B et sont telles que $x \in X, y \in Y$. Alors $X . Y^{-1}$ est une partie connexe de A rencontrant B et contenant xy^{-1}; on a donc $xy^{-1} \in C$, ce qui prouve bien que C est un sous-groupe.

Le théorème 3 est maintenant évident. En effet, on vient de voir que $K' . P'$ est un sous-groupe ouvert de $K_{\mathbf{C}}$; comme il contient K', il est nécessairement égal à $K_{\mathbf{C}}$ et la projection π est bien un isomorphisme.

Exemple. Prenons pour K le cercle $\mathbf{S}_1$, de sorte que $G(\mathbf{C}) = \mathbf{C}^*$. Soit H un groupe de Lie complexe compact connexe de dimension 1 [d'aucuns appellent ça une *courbe elliptique*]; en tant que groupe de Lie réel, H est un tore de dimension 2. Choisissons un plongement f de $\mathbf{S}_1$ dans H. D'après le th. 3, f se prolonge en un *homomorphisme* $F: \mathbf{C}^* \to H$. Il est immédiat que F est un *revêtement,* et que son noyau est formé des puissances d'un élément $q \in \mathbf{C}^*$, avec $|q| < 1$; on peut donc identifier H à $\mathbf{C}^*/q^{\mathbf{Z}}$ [Tate devrait être content].

Si K est un groupe de Lie compact, il est clair que son enveloppe G est un *groupe réductif* (puisque toutes ses représentations linéaires sont semi-simples), donc $G_{/\mathbf{C}}$ est un groupe réductif complexe. Inversement:

THÉORÈME 4. *Soit H un groupe algébrique linéaire complexe réductif, et soit K un sous-groupe compact maximal de $H(\mathbf{C})$. L'enveloppe complexe de K s'identifie à H.*

Soit $\mathfrak{h}$ l'algèbre de Lie de H, et soit $\mathfrak{k}$ celle de K. *On va d'abord prouver que* $\mathfrak{h} = \mathfrak{k} \oplus i\mathfrak{k}$, et qu'il existe une *décomposition de Cartan* de $H(\mathbf{C})$ dont les facteurs sont K et $\exp(i\mathfrak{k})$.

Il suffit de le faire lorsque H est connexe, puis (quitte à passer à un revêtement) lorsque H est, soit un tore, soit un groupe semi-simple. Le premier cas est trivial. Le second a été traité dans la rédaction 517, § 3 (en se ramenant au cas adjoint et en utilisant l'existence d'une forme réelle de $\mathfrak{h}$ dont la forme de Killing est négative).

Ceci étant, si G est l'enveloppe complexe de K, il est clair que le morphisme canonique $G \to H$ donne lieu à un homomorphisme $G(\mathbf{C}) \to H(\mathbf{C})$ qui est un *isomorphisme.* C'est donc un isomorphisme.

Remarque. Le th. 4 équivaut à dire que l'*enveloppe* de K est une «forme réelle» anisotrope de H. Il y a donc correspondance bijective entre:

— sous-groupes compacts maximaux de $H(\mathbf{C})$,

— formes réelles anisotropes de H.

En particulier, ces dernières sont *conjuguées entre elles* par les éléments de $H(\mathbf{C})$ (et même par ceux de $H^o(\mathbf{C})$, H^o désignant la composante neutre de H).

5.4. Retour aux groupes anisotropes

PROPOSITION 7. *Soit G un groupe algébrique linéaire réel anisotrope, et soit H un sous-groupe algébrique de G. Soit $V = G/H$ l'espace homogène correspondant* (au sens algébrique). *Alors:*

a) *H est anisotrope.*

b) *L'application canonique $G(\mathbf{R}) \to V(\mathbf{R})$ est surjective* (de sorte qu'on peut identifier $V(\mathbf{R})$ à $G(\mathbf{R})/H(\mathbf{R})$).

c) *Si H est distingué, le groupe quotient G/H est anisotrope.*

La conjugaison de Cartan $g \mapsto \bar{g}$ du th. 2 laisse évidemment stable le sous-groupe $H(\mathbf{C})$ de $G(\mathbf{C})$. Comme $H(\mathbf{C})$ est «de type algébrique», on en conclut que $H(\mathbf{C})$ admet lui-même une décomposition de Cartan $K.P$, où $K = H(\mathbf{C}) \cap G(\mathbf{R}) = H(\mathbf{R})$. Mais alors il est clair que l'adhérence de K pour la topologie de Zariski de H est H tout entier. Cela montre que H est anisotrope, d'où a).

Soit maintenant $v \in V(\mathbf{R})$; soit $g \in G(\mathbf{C})$ un élément dont l'image dans $V(\mathbf{C}) = G(\mathbf{C})/H(\mathbf{C})$ est v. On a $g \equiv \bar{g} \bmod H(\mathbf{C})$. Soit $K_1.P_1$ la décomposition de Cartan de $G(\mathbf{C})$ utilisée plus haut, et écrivons g sous la forme $g = k_1p_1$, avec $k_1 \in K_1$, $p_1 \in P_1$. L'hypothèse $g \equiv \bar{g} \bmod H(\mathbf{C})$ signifie qu'il existe $k \in K$ et $p \in P$ tels que $g = \bar{g}kp$, i.e. $k_1p_1 = k_1p_1^{-1}kp$, d'où $p_1^2 = kp$, ce qui entraîne $k = 1$, $p = p_1^2$. Comme P est stable par extraction de racines carrées, on a $p_1 \in P$. On en conclut que $g \equiv k_1 \bmod H(\mathbf{C})$, donc que v est l'image de l'élément $k_1 \in G(\mathbf{R})$, ce qui prouve b).

Enfin, si H est distingué, il est clair que l'image de K_1 dans (G/H) $(\mathbf{R})$ est dense pour la topologie de Zariski de G/H; or cette image est un compact, d'où etc.

[Le rédacteur ne voit pas comment démontrer que H est anisotrope sans utiliser les décompositions de Cartan — sauf, bien sûr, dans le cas où H est connexe, qui est trivial.]

5.5. GROUPES DE LIE COMPLEXES RÉDUCTIFS

THÉORÈME 5. *Soient* H *un groupe de Lie complexe,* H^o *sa composante neutre et* $\mathfrak{h}$ *son algèbre de Lie. Les conditions suivantes sont équivalentes:*

(i) H/H^o *est fini;* $\mathfrak{h}$ *est réductive; la composante neutre du centre de* H^o *est isomorphe à un produit de groupes* $\mathbf{C}^*$.

(ii) H/H^o *est fini; toute représentation linéaire complexe de* H *est semi-simple; il existe une telle représentation qui est fidèle.*

(iii) H/H^o *est fini; si* K *est un sous-groupe compact maximal de* H, *et* $\mathfrak{k}$ *son algèbre de Lie, on a* $\mathfrak{h} = \mathfrak{k} \oplus i\mathfrak{k}$.

(iv) *Il existe un groupe de Lie compact* K *tel que* H *soit isomorphe au complexifié de* K.

(v) *Il existe un groupe algébrique linéaire sur* $\mathbf{C}$ *qui est réductif, et dont le groupe des points est isomorphe à* H (comme groupe de Lie complexe).

Démonstration. L'équivalence (iv) $\Leftrightarrow$ (v) résulte des ths. 3 et 4. Le fait que (iv) $\Rightarrow$ (iii) résulte de la décomposition de Cartan de H. Inversement, supposons (iii) vérifiée, soit G l'enveloppe de K, et soit $G(\mathbf{C})$ le complexifié de K. L'injection $K \to H$ se prolonge en un morphisme $f: G(\mathbf{C}) \to H$ de groupes de Lie complexes. Vu que $\mathfrak{h} = \mathfrak{k} \oplus i\mathfrak{k}$, f est un isomorphisme local. De plus, K est un sous-groupe compact maximal à la fois de $G(\mathbf{C})$ et de H et la restriction de f à K est l'identité (modulo les identifications faites). Cela entraîne que f est un isomorphisme, en vertu du lemme suivant:

LEMME 4. *Soit* $f: A \to B$ *un homomorphisme de groupes de Lie réels. On suppose:*

a) *que* f *est un isomorphisme local;*

b) *que* A *et* B *ont un nombre fini de composantes connexes;*

c) *qu'il existe un sous-groupe compact maximal* K_A (resp. K_B) *de* A (resp. de B) *tel que la restriction de* f *à* K_A *soit un isomorphisme de* K_A *sur* K_B.

Alors f *est un isomorphisme.*

Démonstration du lemme 4. On sait que B possède une *décomposition multiexponentielle* $B = K_B . \exp(\mathfrak{p}_1) \ldots \exp(\mathfrak{p}_n)$, où les $\mathfrak{p}_i$ sont des sous-espaces vectoriels de l'algèbre de Lie $\mathfrak{b}$ de B. Cela permet de définir une *section* $h: B \to A$ par

$$k . \exp(t_1) \ldots \exp(t_n) \mapsto k' . \exp(t_1') \ldots \exp(t_n')$$

où k' désigne l'image réciproque de k dans K_A et $t'_1, \ldots, t'_n$ les éléments de l'algèbre de Lie de A relevant $t_1, \ldots, t_n$. L'image de h est une réunion de composantes connexes de A; comme elle contient K_A, c'est A tout entier; d'où le lemme.

On a donc prouvé l'équivalence (iii) $\Leftrightarrow$ (iv).

L'implication (v) $\Rightarrow$ (i) est immédiate: on sait en effet que tout groupe réductif connexe est extension d'un groupe semi-simple par un groupe de type multiplicatif. Inversement, montrons que (i) $\Rightarrow$ (iii) (ce qui prouvera que (i) est équivalent à (iii), (iv), (v)). On peut supposer H connexe. Si Z désigne la composante neutre du centre de H, et S son groupe dérivé, $S \cap Z$ est un groupe discret, qui est le centre de S. Or on a:

LEMME 5. *Le centre d'un groupe de Lie complexe, connexe, d'algèbre de Lie semi-simple, est fini.*

Il suffit de voir que le groupe fondamental du groupe adjoint est fini. Or le groupe adjoint admet une décomposition de Cartan $K.P$, avec K compact semi-simple connexe (cf. rédaction numéro 517); son groupe fondamental est le même que celui de K, et ce dernier est fini d'après un théorème bien connu d'*Int.* (chap. VII, §3, prop. 5).

Ceci étant, on voit que $S \cap Z$ est fini, donc que H admet pour *revêtement fini* le produit $S \times Z$. Pour vérifier que H jouit de la propriété (iii), il suffit de le faire pour son revêtement $S \times Z$, c'est-à-dire pour S et pour Z. Le cas de Z est trivial (puisqu'on l'a supposé isomorphe à $(\mathbf{C}^*)^n$); pour S, on remarque que, d'après le lemme 5, son centre est fini, et l'on est ramené au cas du *groupe adjoint*; mais ce dernier est évidemment «algébrique», i.e. vérifie (v), donc aussi (iii).

Reste à démontrer que (ii) est équivalente aux quatre autres propriétés. Tout d'abord, on a (iv) $\Rightarrow$ (ii); en effet, si H est le complexifié de K, et si E est une représentation linéaire complexe de H, les sous-espaces de E stables par K le sont aussi par H, ce qui montre que E est semi-simple; de même, le fait que K ait une représentation linéaire fidèle montre que H en possède une.

Enfin, supposons (ii) vérifiée. L'existence d'une représentation semi-simple et fidèle de H montre que $\mathfrak{h}$ est réductive (car la représentation de $\mathfrak{h}$ correspondante est aussi semi-simple et fidèle). D'autre part, H^o vérifie aussi (ii) (le seul point non évident est que toute représentation linéaire ρ de H^o soit semi-simple; cela se voit en remarquant que la représentation linéaire *induite* (au sens Frobenius!) de ρ est semi-simple). Si Z désigne la composante neutre du centre de H et S le groupe dérivé de H, on voit comme ci-dessus que $S \cap Z$

est un groupe *fini* F. On a un homomorphisme surjectif $H \to Z/F$; le groupe Z/F est donc un groupe commutatif, connexe, dont toutes les représentations linéaires sont semi-simples; de plus, Z possède une représentation linéaire fidèle. Il en résulte facilement (cf. exercice 5) que Z est isomorphe à $(\mathbf{C}^*)^n$. On a donc (ii) $\Rightarrow$ (i), ce qui achève la démonstration.

[Cette démonstration n'est en fait qu'une simple vérification: tout le travail sérieux a déjà été fait. On devrait pouvoir la présenter plus simplement.]

DÉFINITION 2. *Un groupe de Lie complexe qui vérifie les propriétés équivalentes du th. 5 est dit réductif.*

THÉORÈME 6. *Soit* H *un groupe de Lie complexe réductif. Soit* G *son enveloppe complexe* (en tant que groupe de Lie complexe, cf. n° 4.3). *Alors* G *est un groupe algébrique linéaire complexe réductif* (au sens algébrique) *et l'application canonique* $H \to G(\mathbf{C})$ *est un isomorphisme.*

Soit K un sous-groupe compact maximal de H; puisque H est le complexifié de K, les représentations linéaires complexes (holomorphes) de H correspondent bijectivement (par restriction) à celles de K. Il s'ensuit que le groupe G en question n'est autre que *l'enveloppe complexe* $G_{K/\mathbf{C}}$ de K, d'où le théorème.

COROLLAIRE 1. *Soient* G_1 *et* G_2 *deux groupes algébriques linéaires complexes, et soit* $f: G_1(\mathbf{C}) \to G_2(\mathbf{C})$ *un homomorphisme de groupes de Lie complexes. Si* G_1 *est réductif,* f *est «algébrique»* (i.e. induit par un morphisme $G_1 \to G_2$).

Cela ne fait que traduire le th. 6.

COROLLAIRE 2. *Le foncteur «enveloppe» est une équivalence de la catégorie des groupes de Lie complexes réductifs sur celle des groupes algébriques linéaires réductifs.*

C'est clair.

Remarque. Soit K un sous-groupe compact maximal de $G(\mathbf{C})$, où G est algébrique linéaire réductif sur $\mathbf{C}$. On peut résumer ce qui précède ainsi: l'algèbre affine de G s'identifie à l'algèbre des fonctions holomorphes sur $G(\mathbf{C})$ dont les translatées engendrent un espace vectoriel de dimension finie; par restriction à K, cette algèbre s'applique isomorphiquement sur l'algèbre des fonctions continues complexes sur K dont les translatées engendrent un espace vectoriel de dimension finie.

[On obtient ainsi des bigèbres sur $\mathbf{C}$; à ces bigèbres correspondent des schémas en groupes; à ces schémas en groupes correspondent des groupes de Lie complexes; à ces groupes... Voyez, voyez, la machine tourner!]

EXERCICES

§ 1

1) Soit E un K-module projectif de type fini. On identifie $\mathrm{End}(E)$ à $E \otimes E'$; on note I l'élément de $E \otimes E'$ correspondant à 1_E, et ${}^tI$ son image dans $E' \otimes E$.

On munit $E \otimes E' = \mathrm{End}(E)$ de la structure de cogèbre *opposée* à celle définie au n° 1.1.

a) Si $x = a \otimes a' \in E \otimes E'$, montrer que $d(x) = a \otimes {}^tI \otimes a'$.

b) On définit une application $d_E \colon E \to \mathrm{End}(E) \otimes E = E \otimes E' \otimes E$ par $a \mapsto a \otimes {}^tI$. Montrer que cette application définit sur E une structure de comodule à gauche sur $\mathrm{End}(E)$.

c) On identifie $\mathrm{End}(E) \otimes \mathrm{End}(E)$ à $\mathrm{End}(E \otimes E)$ par l'application $(u, v) \mapsto u \otimes v$. D'autre part, si on écrit $\mathrm{End}(E \otimes E)$ sous la forme $E \otimes E \otimes E' \otimes E'$ la permutation des deux facteurs E' définit un automorphisme σ de $\mathrm{End}(E \otimes E)$. Montrer que l'on a

$$d(u) = \sigma(u \otimes 1_E) \quad \text{si} \quad u \in \mathrm{End}(E)\ .$$

d) Soit (v_i) une base de E, et soit $(E_{ij} = v'_j \otimes v_i)$ la base correspondante de $\mathrm{End}(E)$. Montrer que

$$d(E_{ij}) = \sum_k E_{ik} \otimes E_{kj}\ .$$

e) Justifier la Remarque 2 du n° 1.2.

2) Soit C une cogèbre plate, et soit E un comodule sur C.

a) Soit V un K-module tel que E soit isomorphe (comme module) à un quotient de E. Montrer qu'il existe un sous-comodule F de $C \otimes V$ tel que E soit isomorphe (comme comodule) à un quotient de F. (Utiliser le morphisme $C \otimes V \to C \otimes E$ et le fait que E est isomorphe à un sous-comodule de $C \otimes E$.) Montrer que, si K est noethérien, et E de type fini, on peut choisir F de type fini.

b) On suppose que K est un anneau de Dedekind. Montrer que tout comodule E de type fini est quotient d'un comodule F qui est projectif de type fini. (Utiliser a) en prenant pour V un module libre de sorte que F soit sans torsion.)

§ 2

1) Soit $x \in C$ tel que $d_E(x) = x \otimes x$ et $e(x) = 1$. On note K_x le module K muni de la structure de comodule définie par

$$y \mapsto x \otimes y\ .$$

Prouver l'équivalence des propriétés suivantes:

a) K_x est le seul objet simple de Com_C^f (à isomorphisme près).

b) Toute sous-cogèbre de C non réduite à 0 contient x.

c) Le comodule C est extension essentielle du sous-comodule Kx (i.e. tout sous-comodule de C différent de 0 contient x).

d) L'algèbre profinie A duale de C est un anneau local d'idéal maximal le noyau de l'homomorphisme $a \mapsto \langle x, a \rangle$ de A dans K.

[Noter que c) signifie ceci: le comodule C est *l'enveloppe injective* du comodule simple Kx.]

§ 3

1) Avec les notations du n° 3.4, montrer sans utiliser la prop. 4 que la formule (iii) est conséquence des formules (i) et (ii).

2) Les notations étant celles du n° 3.4, on suppose K parfait. Soit g un automorphisme du foncteur υ. Pour tout objet E de Com_C^f, soit s_E (resp. u_E) la composante semi-simple (resp. unipotente) de $g(E)$. Montrer que $E \mapsto s_E$ et $E \mapsto u_E$ sont des automorphismes du foncteur υ. Si g vérifie les relations (i) et (ii), montrer qu'il en est de même pour s et u. Déduire de là la décomposition des éléments de $G(K)$ en produits d'éléments semi-simples et unipotents commutant entre eux (dans le cas où G est un schéma en groupes).

Utiliser le même procédé pour obtenir la décomposition des éléments de l'algèbre de Lie de G en sommes d'éléments semi-simples et nilpotents commutant entre eux.

[Cette décomposition n'a en fait rien à voir avec les bigèbres. On aurait pu la donner au §2.]

3) On suppose que $G = \mathrm{Spec}(C)$ est un schéma en groupes. Prouver l'équivalence des propriétés suivantes:

a) Tout G-module simple est isomorphe au G-module trival K.

b) G est limite projective de groupes algébriques linéaires unipotents.

c) Si $E \in \mathrm{Com}_C^f$, $K_1 \in \mathrm{Alg}_K$, et $u \in G_E(K_1)$, l'élément u est unipotent.

4) On suppose K de caractéristique zéro. Montrer que la catégorie des G-modules semi-simples vérifie les conditions du corollaire à la prop. 3, donc correspond à un quotient H de G. Montrer que l'on peut caractériser H comme le plus grand quotient de G qui soit *réductif* (i.e. limite projective de groupes algébriques linéaires réductifs, au sens usuel).

§4

1) On prend $K = \mathbf{C}$. Le groupe additif $\Gamma = \mathbf{C}$ est considéré comme un groupe de Lie complexe. Soit G son enveloppe, et soit C la bigèbre correspondante.

a) Montrer qu'une fonction $f(z)$ sur Γ appartient à C si et seulement si c'est une *exponentielle-polynôme,* i.e. si elle est combinaison linéaire de fonctions de la forme $z^n e^{\lambda z}$, avec $n \in \mathbf{N}$, $\lambda \in \mathbf{C}$.

b) Montrer que C est produit tensoriel de la bigèbre formée des polynômes, et de la bigèbre formée des combinaisons linéaires d'exponentielles. Interpréter cette décomposition comme une décomposition de l'enveloppe G en produit du groupe *additif* $\mathbf{G}_a$ et d'un *groupe de type multiplicatif* M dual du groupe abélien $\mathbf{C}$. En particulier, G n'est pas algébrique.

2) Comment faut-il modifier l'exercice précédent lorsque $K = \mathbf{R}$ et $\Gamma = \mathbf{R}$? (La partie «tore» de G n'est plus déployée; son dual est $\mathbf{C}$, *muni* de la conjugaison complexe.)

(Dans les deux exercices ci-après, on se permet d'identifier un groupe profini Γ à son enveloppe relativement à la catégorie des Γ-modules à noyau ouvert. Cela revient à identifier un groupe fini au groupe algébrique «constant» de dimension 0 qui lui est associé.)

3) Soit $K = \mathbf{Q}_p$, et soit H un groupe algébrique semi-simple simplement connexe sur K. Soit Γ un sous-groupe ouvert compact du groupe $H(\mathbf{Q}_p)$. Montrer que l'enveloppe du groupe topologique Γ est $H \times \Gamma$. (Le second facteur est identifié au schéma en groupes correspondant, cf. ci-dessus.)

4) Soient $K = \mathbf{Q}$ et $\Gamma = \mathbf{SL}_n(\mathbf{Z})$, $n \geqslant 3$. On prend pour L la catégorie de toutes les représentations linéaires de Γ sur $\mathbf{Q}$ de rang fini. Montrer que l'enveloppe de Γ est $\mathbf{SL}_n \times \prod_p \mathbf{SL}_n(\mathbf{Z}_p)$, le second facteur étant identifié à un schéma en groupes comme on l'a expliqué ci-dessus. (Utiliser le th. 16.2, p. 497, des *Publ. IHES*, 1967, combiné avec le fait que tout sous-groupe d'indice fini de Γ contient un «groupe de congruence».)

5) Soit K un corps complet pour une valuation discrète v. On note A (resp. $\mathfrak{m}$) l'anneau (resp. l'idéal maximal) de v, et l'on note p la caractéristique du corps $A/\mathfrak{m}$. On suppose $p \neq 0$ et $\mathrm{car}(K) = 0$.

a) Soit $x \in K^*$. Supposons qu'il existe un entier d tel que, pour tout $n \geqslant 0$, il existe une extension K_n de K de degré d et un élément $y \in K_n$ tel que $y^{p^n} = x$. Montrer que $v(x) = 0$. Montrer que, si $x \equiv 1 \pmod{\mathfrak{m}}$, on a $x = 1$. (Se ramener au cas où toutes les racines p^n-èmes de x appartiennent au corps K.)

b) Soit $f : K \to \mathbf{GL}_n(K)$ un homomorphisme K-analytique. Montrer que f est «algébrique», i.e. qu'il existe une matrice nilpotente u telle que $f(t) = \exp(tu)$ pour tout $t \in K$. (Appliquer a) aux valeurs propres de $f(t)$, avec $d = n$; en conclure que $f(t)$ est unipotent pour tout t.)

c) Déduire de b) que l'enveloppe du groupe de Lie K est le groupe additif $\mathbf{G}_a$ (relativement à K).

d) Etendre b) et c) aux groupes algébriques *unipotents* sur K (écrire les éléments de ces groupes comme produits de groupes à un paramètre). Même chose pour les groupes *semi-simples déployés.* [Il est probable que le résultat reste vrai pour les groupes semi-simples n'ayant aucun facteur simple anisotrope.]

e) Montrer que les résultats de b) et c) *ne s'étendent pas* aux groupes de type multiplicatif.

6) Soit K un corps localement compact ultramétrique de caractéristique 0 et soit μ le groupe des racines de l'unité contenues dans K. Soit S

le revêtement de $\mathbf{SL}_2(K)$ défini par C. Moore et T. Kubota; on a une suite exacte

$$\{1\} \to \mu \to S \to \mathbf{SL}_2(K) \to \{1\}$$

et S est son propre groupe dérivé. Montrer que toute représentation K-linéaire analytique du groupe de Lie S est triviale sur μ; en déduire que $\mathbf{SL}_2$ est l'enveloppe de S. (Si G est l'enveloppe de S, remarquer que la suite

$$\mu \to G \to \mathbf{SL}_2 \to \{1\}$$

est exacte (cf. exercice 5). Utiliser ensuite le fait que $\mathbf{SL}_2$ est simplement connexe.)

§5

1) Etendre la prop. 1 au cas d'un groupe compact K opérant continûment sur un espace vectoriel réel V de dimension finie, chacune des opérations de K étant *polynomiale.* (On montrera d'abord, au moyen du théorème de Baire, que le degré de ces opérations est borné.)

2) Soit H un sous-groupe algébrique réel de $\mathbf{GL}_n$. Montrer que H est anisotrope si et seulement si il existe une forme quadratique positive non dégénérée sur $\mathbf{R}^n$ qui est invariante par H.

3) a) Soit G un groupe algébrique linéaire réel, et soit H un sous-groupe algébrique distingué de G. On suppose que H et G/H sont anisotropes, et que G/H est connexe. Montrer que G est anisotrope.

b) On prend pour G le groupe des matrices de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ avec $(a^2+b^2)^2 = 1$ et pour H le sous-groupe de celles pour lesquelles $a^2+b^2=1$. Le groupe G/H s'identifie au groupe «constant» $\{\pm 1\}$. Montrer que H et G/H sont anisotropes et que G ne l'est pas.

4) Avec les notations de la prop. 7, montrer que l'injection de $V(\mathbf{R})$ dans $V(\mathbf{C})$ est une «équivalence d'homotopie». (Il suffit de voir que $\pi_i(V(\mathbf{R})) \to \pi_i(V(\mathbf{C}))$ est un isomorphisme pour tout i; utiliser le lemme des cinq pour se ramener à l'énoncé analogue pour G et H.) [Exercice: donner explicitement une «rétraction de déformation» de $V(\mathbf{C})$ sur $V(\mathbf{R})$.]

En particulier, la quadrique complexe d'équation $\sum z_i^2 = 1$ a même type d'homotopie que l'ensemble de ses points réels; énoncer des résultats analogues pour les variétés de Stiefel, etc.

5) (Cet exercice pourrait remonter au chapitre III du livre de Lie.)

Soit A un groupe de Lie complexe, commutatif, connexe, d'algèbre de Lie $\mathfrak{a}$; soit Λ le noyau de $\exp : \mathfrak{a} \to A$, de sorte que A s'identifie à $\mathfrak{a}/\Lambda$.

a) Démontrer l'équivalence de:

a_1) L'application canonique $\mathbf{C} \otimes \Lambda \to \mathfrak{a}$ est injective.

a_2) A est isomorphe à un sous-groupe de Lie d'un $(\mathbf{C}^*)^n$.

a_3) A est isomorphe à un groupe $(\mathbf{C}^*)^p \times \mathbf{C}^q$.

a_4) A possède une représentation linéaire complexe fidèle.

a_5) A possède une représentation linéaire complexe fidèle semi-simple d'image fermée.

b) Démontrer l'équivalence de:

b_1) L'application $\mathbf{C} \otimes \Lambda \to \mathfrak{a}$ est surjective.

b_2) A est isomorphe à un quotient d'un groupe $(\mathbf{C}^*)^n$.

b_3) Aucun facteur direct de A n'est isomorphe à $\mathbf{C}$.

b_4) Toute représentation linéaire complexe de A est semi-simple.

c) Démontrer l'équivalence de:

c_1) L'application $\mathbf{C} \otimes \Lambda \to \mathfrak{a}$ est bijective.

c_2) A est isomorphe à un $(\mathbf{C}^*)^n$.

d) Soit F un sous-groupe fini de A, et soit $A' = A/F$. Montrer que A vérifie les conditions a_i) (resp. b_i), c_i)) si et seulement si A' les vérifie.

BIBLIOGRAPHIE

CARTIER, P. *Séminaire S. Lie,* 2e année (1955-56) [l'exposé 4 contient la définition des comodules].

CHEVALLEY, C. *Theory of Lie groups.* Princeton, 1946 [le chapitre VI, §§VII, VIII, IX donne les propriétés de la bigèbre d'un groupe compact, avec applications à la dualité de Tannaka et la complexification du groupe].

DEMAZURE, M. et A. GROTHENDIECK. *Séminaire de Géométrie algébrique.* IHES, 1963 (SGAD) [la correspondance entre G-modules et comodules sur la cogèbre de G est donnée dans l'exposé I].

Séminaire Heidelberg-Strasbourg. IRMA Strasbourg, 1967 [exposés 2 et 3].

HOCHSCHILD, G. et G.D. MOSTOW. Representative functions..., quatre papiers aux *Annals* (vol. 66, 68, 70) et à l'*Amer. Journal* (vol. 83).

SERRE, J.-P. Groupes de Grothendieck des schémas en groupes réductifs déployés. *Publ. IHES,* vol. 34 (1968), 37-52.

(Reçu le 13 mars 1992)

Jean-Pierre Serre

Collège de France
F-75231 Paris Cedex 05
(France)

vide-leer-empty