
Semaine 1 : Foncteurs représentables et algèbres de Hopf

Références pour ce chapitre :

[SGA3] Schémas en groupes (SGA 3), t. I, nouvelle édition recomposée et annotée, Documents Mathématiques 7, Soc. Math. France, 2011. (Exposé I, §§1-4)

[Ja] Jens-Carsten Jantzen, Representations of algebraic groups (2nd edition), Amer. Math. Soc. 2003. (chap. I.2)

[Po] Patrick Polo, Cours de M2 à l'UPMC 2005-2006 (chap. 1), disponible sur la page de l'auteur : www.imj-prg.fr/~patrick.polo/M2

[Wa] William C. Waterhouse, Introduction to affine group schemes, Springer-Verlag, 1979. (chap. 1,3,16)

1. Cogèbres et algèbres de Hopf

On énonce d'abord quelques définitions, valables pour tout anneau commutatif Λ (par exemple pour $\Lambda = \mathbb{Z}$)⁽¹⁾, mais assez rapidement on se limitera au cas où Λ est un corps k . On fixe donc un anneau commutatif Λ . Sauf indication contraire, les produits tensoriels sont pris sur Λ , i.e. \otimes signifie \otimes_{Λ} .

1.1. Cogèbres et comodules. —

Définition 1.1. — Une Λ -**cogèbre** est un Λ -module C muni de deux applications Λ -linéaires $\Delta : C \rightarrow C \otimes C$ et $\varepsilon : C \rightarrow \Lambda$, vérifiant les deux axiomes suivants :

- (1) $(\text{id}_C \otimes \Delta)\Delta = (\Delta \otimes \text{id}_C)\Delta$,
- (2) $(\varepsilon \otimes \text{id}_C)\Delta = \text{id}_C = (\text{id}_C \otimes \varepsilon)\Delta$.

Δ , resp. ε s'appelle la comultiplication, resp. l'augmentation. L'axiome (1) exprime la coassociativité de la comultiplication, et on peut appeler (2) l'axiome de co-unité.

Un morphisme de Λ -cogèbres $\phi : C \rightarrow C'$ est une application Λ -linéaire vérifiant $\Delta_{C'} \circ \phi = (\phi \otimes \phi) \circ \Delta_C$ et $\varepsilon_{C'} \circ \phi = \varepsilon_C$.

Définition 1.2. — Un C -**comodule** (à droite) est un Λ -module V , muni d'une application Λ -linéaire $V \rightarrow V \otimes C$, notée Δ_V ou μ_V , qui est une *coaction*, c.-à-d. qui vérifie les deux axiomes suivants :

- (1) $(\text{id}_V \otimes \varepsilon)\Delta_V = \text{id}_V$,
- (2) $(\text{id}_V \otimes \Delta)\Delta_V = (\Delta_V \otimes \text{id}_C)\Delta_V$.

Noter que la comultiplication $\Delta : C \rightarrow C \otimes C$ fait de C un C -comodule à droite.

Un morphisme de C -comodules $f : V \rightarrow W$ est une application Λ -linéaire qui vérifie $\Delta_W \circ f = (f \otimes \text{id}_C) \circ \Delta_V$.

Incluons ici le lemme suivant, analogue de la restriction des scalaires pour les modules, c.-à-d., du fait que si $A \rightarrow B$ est un morphisme de Λ -algèbres et M un B -module, alors M est aussi un A -module.

Lemme 1.3 (Corestriction des scalaires). — Soit $\phi : C \rightarrow C'$ un morphisme de k -cogèbres. Si V est un C -comodule pour la coaction $\Delta_V : V \rightarrow V \otimes C$, alors c'est un C' -comodule pour la coaction $\Delta'_V = (\text{id}_V \otimes \phi)\Delta_V$.

Démonstration. — Laissez au lecteur. □

⁽¹⁾Tous les anneaux considérés sont munis d'un élément unité 1 et, sauf mention du contraire, ils seront commutatifs.

1.2. Algèbres de Hopf. —

Définition 1.4. — Soit A une Λ -algèbre commutative; notons u le morphisme $\Lambda \rightarrow A$, $\lambda \mapsto \lambda \cdot 1_A$ et $m : A \otimes A \rightarrow A$ la multiplication de A . On dit que A est une Λ -algèbre de Hopf si l'on s'est donné trois morphismes d'algèbres

$$\Delta : A \rightarrow A \otimes A, \quad \varepsilon : A \rightarrow \Lambda, \quad \tau : A \rightarrow A$$

vérifiant les trois axiomes suivants :

- (1) (Coassociativité) $(\text{id}_A \otimes \Delta)\Delta = (\Delta \otimes \text{id}_A)\Delta$.
- (2) (Neutre) $(\varepsilon \otimes \text{id}_A)\Delta = \text{id}_A = (\text{id}_A \otimes \varepsilon)\Delta$.
- (3) (Inverse) $m \circ (\tau \otimes \text{id}_A) \circ \Delta = u \circ \varepsilon = m \circ (\text{id}_A \otimes \tau) \circ \Delta$.

(En particulier, Δ et ε font de A une Λ -cogèbre.) Dans ce cas, Δ s'appelle la comultiplication, ε l'augmentation (ou co-unité), et τ l'antipode.⁽²⁾

2) Un morphisme de Λ -algèbres de Hopf $\phi : A \rightarrow B$ est un morphisme de Λ -algèbres qui respecte la comultiplication, l'augmentation et l'antipode, c.-à-d., qui vérifie :

$$\begin{cases} \Delta_B \circ \phi = (\phi \otimes \phi) \circ \Delta_A; \\ \varepsilon_B \circ \phi = \varepsilon_A; \\ \tau_B \circ \phi = \phi \circ \tau_A. \end{cases}$$

Remarque et définition 1.5. — (1) Comme $\varepsilon : A \rightarrow \Lambda$ est un morphisme de Λ -algèbres, on a

$$\varepsilon(u(\lambda)) = \varepsilon(\lambda \cdot 1_A) = \lambda \cdot 1_\Lambda = \lambda$$

pour tout $\lambda \in \Lambda$, donc u est *injectif* et ε *surjectif*.

(2) $\text{Ker}(\varepsilon)$ est noté I_A et appelé *l'idéal d'augmentation*. On a donc une suite exacte :

$$0 \rightarrow I_A \rightarrow A \xrightarrow{\varepsilon} \Lambda \rightarrow 0.$$

Proposition 1.6. — Soit A une Λ -algèbre de Hopf. Notons G le foncteur qui à toute Λ -algèbre R associe l'ensemble

$$G(R) = \text{Hom}_{\Lambda\text{-alg.}}(A, R)$$

et à tout morphisme de Λ -algèbres $\phi : R \rightarrow S$ associe l'application $G(\phi) : G(R) \rightarrow G(S)$, $g \mapsto \phi \circ g$. Alors G est un **foncteur en groupes**, i.e. chaque $G(R)$ est un groupe et chaque $G(\phi)$ est un morphisme de groupes.

Démonstration. — Soit $\phi : R \rightarrow S$ un morphisme de Λ -algèbres; notons m_R (resp. m_S) la multiplication de R (resp. S). Soient $g, h \in G(R)$, on définit gh comme étant le morphisme de Λ -algèbres :

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{g \otimes h} R \otimes R \xrightarrow{m_R} R$$

On laisse au lecteur la tâche de vérifier que les axiomes de la structure d'algèbre de Hopf entraînent que $G(R)$ est un groupe, dont l'élément unité est le morphisme $u_R \circ \varepsilon$ (où $u_R : \Lambda \rightarrow R$) et où l'inverse à droite et à gauche d'un élément $g \in G(R)$ est le morphisme d'algèbres $g \circ \tau : A \rightarrow R$. (Ceci justifie le nom des axiomes.)

Enfin, comme $\phi : R \rightarrow S$ est un morphisme d'algèbres, on a $\phi \circ m_R = m_S \circ (\phi \otimes \phi)$ et il en résulte que $G(\phi)(gh) = G(\phi)(g)G(\phi)(h)$, donc $G(\phi)$ est bien un morphisme de groupes. \square

⁽²⁾On verra plus bas la signification des noms donnés à ces axiomes.

Exemples 1.7. — (1) Soit A la \mathbb{Z} -algèbre de Hopf $\mathbb{Z}[X]$, munie de Δ, ε et τ définis par $\Delta(X) = X \otimes 1 + 1 \otimes X$, $\varepsilon(X) = 0$ et $\tau(X) = -X$. Le foncteur en groupes qu'elle définit est noté \mathbb{G}_a et appelé le **groupe additif**. En effet, pour tout anneau R ⁽³⁾ on a $G(R) = R$ et la loi de groupe est l'addition dans R .

(2) Soit B la \mathbb{Z} -algèbre de Hopf $\mathbb{Z}[T, T^{-1}]$, munie de Δ, ε et τ définis par $\Delta(T) = T \otimes T$, $\varepsilon(T) = 1$ et $\tau(T) = T^{-1}$. Le foncteur en groupes qu'elle définit est noté \mathbb{G}_m et appelé le **groupe multiplicatif**. En effet, pour tout anneau R , $G(R)$ est l'ensemble R^\times des éléments de R inversibles pour la multiplication et la loi de groupe est la multiplication dans R^\times .

Définition 1.8. — Soit A une algèbre de Hopf. Un *idéal de Hopf* est un idéal I qui vérifie $\Delta(I) \subset I \otimes A + A \otimes I$, $\tau(I) \subset I$ et $I \subset \text{Ker}(\varepsilon)$. Dans ce cas, on laisse au lecteur la tâche de vérifier que Δ, ε et τ passent au quotient et munissent A/I d'une structure d'algèbre de Hopf.

Pour le moment, on n'a pas besoin de définir ce qu'est un Λ -schéma ; nous nous contenterons de dire (même si c'est un peu artificiel à ce stade) que la catégorie des Λ -schémas **affines** est la catégorie opposée de celle des Λ -algèbres, i.e. les objets sont les mêmes et le sens des flèches est renversé. De même, on pose (provisoirement) la définition suivante :

Définition 1.9. — La catégorie des Λ -schémas en groupes affines est la catégorie opposée de celle des Λ -algèbres de Hopf, c.-à-d., si G (resp. H) est le « schéma en groupes affines » associé à l'algèbre de Hopf A (resp. B) alors un morphisme de schémas en groupes $G \rightarrow H$ « est » un morphisme d'algèbres de Hopf $\phi : B \rightarrow A$.⁽⁴⁾

Dans ce cas, ϕ définit un morphisme de groupes $G(R) \rightarrow H(R)$, fonctoriel en la Λ -algèbre R , dont on peut considérer le noyau $K(R)$. On a alors la proposition suivante :

Proposition 1.10. — Le foncteur $R \mapsto K(R)$ provient de la Λ -algèbre de Hopf $C = A/A\phi(I_B)$, i.e. on a un isomorphisme $K(R) = \text{Hom}_{\Lambda\text{-alg.}}(C, R)$, fonctoriel en R .

Démonstration. — Soit R une Λ -algèbre. Un élément g de $G(R)$ appartient à $K(R)$ ssi son image $\phi \circ g$ dans $H(R)$ est l'élément neutre, égal à $u_R \circ \varepsilon_B$. Ceci équivaut à dire que g est la restriction à A d'un morphisme d'algèbres $g' : A \otimes_B \Lambda \rightarrow R$, cf. le diagramme ci-dessous :

$$\begin{array}{ccc}
 B & \xrightarrow{\varepsilon_B} & \Lambda \\
 \downarrow \phi & & \downarrow \\
 A & \xrightarrow{\quad} & A \otimes_B \Lambda \\
 & \searrow g & \downarrow u_R \\
 & & R
 \end{array}$$

De plus, on déduit de l'isomorphisme $\Lambda \simeq B/I_B$ que $A \otimes_B \Lambda \simeq A/A\phi(I_B)$ et l'on obtient donc que $K(R) \simeq \text{Hom}_{\Lambda\text{-alg.}}(C, R)$. De plus, on vérifie facilement que I_B est un idéal de Hopf de B et que, ϕ étant un morphisme d'algèbres de Hopf, $A\phi(I_B)$ est un idéal de Hopf de A . Donc C est bien une algèbre de Hopf.

Pour être complet, il faudrait vérifier que la structure de groupe sur $K(R)$ définie par $K(R) = \text{Ker}(G(R) \rightarrow H(R))$ coïncide bien avec celle provenant de C . Ceci n'est pas difficile (car C est un quotient de A), mais en fait en utilisant le Lemme de Yoneda plus bas on peut se dispenser de cette vérification (et même de la vérification que C est une algèbre de Hopf.) \square

⁽³⁾Pour $\Lambda = \mathbb{Z}$, une \mathbb{Z} -algèbre n'est rien d'autre qu'un anneau commutatif.

⁽⁴⁾Ceci sera rendu plus clair avec le Lemme de Yoneda plus bas.

Exemples 1.11. — (1) Soit k un corps de caractéristique $p > 0$. Alors le morphisme de k -algèbres de $B = k[T]$ vers $A = k[X]$ défini par $T \mapsto X^p$ est un morphisme d'algèbres de Hopf. L'idéal d'augmentation I_B est engendré par T donc on a :

$$C \simeq A/AX^p = k[X]/(X^p).$$

C'est une k -algèbre non réduite (i.e. qui possède des éléments nilpotents $\neq 0$). Le foncteur correspondant est noté $\alpha_{p,k}$: il associe à toute k -algèbre R le sous-groupe

$$\alpha_{p,k}(R) = \{x \in R \mid x^p = 0\}$$

de $(R, +)$. Bien sûr, $\alpha_{p,k}(R) = \{0\}$ si R est réduite, mais par exemple $\alpha_{p,k}(C)$ est l'idéal d'augmentation I_C .

(2) Soient n un entier > 1 . Alors le morphisme d'anneaux de $B = \mathbb{Z}[T, T^{-1}]$ vers $A = \mathbb{Z}[X, X^{-1}]$ défini par $T \mapsto X^n$ est un morphisme d'algèbres de Hopf. L'idéal d'augmentation I_B est engendré par $T - 1$ donc on a :

$$C \simeq A/A(X^n - 1) \simeq \mathbb{Z}[X]/(X^n - 1),$$

le deuxième isomorphisme découlant du fait que X est inversible dans $\mathbb{Z}[X]/(X^n - 1)$. Le foncteur correspondant est noté μ_n : il associe à tout anneau R le groupe

$$\mu_n(R) = \{x \in R \mid x^n = 1\}$$

des racines n -ièmes de l'unité dans R .

De même, si k est un corps, le schéma en groupes correspondant à $A = k[X, X^{-1}]$, resp. à $k[X]/(X^n - 1)$, est noté $\mathbb{G}_{m,k}$, resp. $\mu_{n,k}$. Si k est de caractéristique p divisant n , i.e. si $n = p^r m$ avec $r \geq 1$ et m premier avec p , on a :

$$C \simeq k[X]/(X^m - 1)^{p^r}$$

donc C n'est pas une k -algèbre réduite.

1.3. A -comodules à droite et G -modules à gauche. —

Définition et proposition 1.12. — Soit A une Λ -algèbre de Hopf et soit G le Λ -schéma en groupes correspondant. Une représentation de G , ou G -module, est un Λ -module V muni d'une structure de A -comodule à droite $\Delta_V : V \rightarrow V \otimes A$.

Dans ce cas, pour toute Λ -algèbre R , le R -module $V \otimes R$ est muni d'une structure de $G(R)$ -module (i.e. d'une action R -linéaire de $G(R)$) définie, pour tout $g \in G(R)$, $v \in V$ et $r \in R$, par

$$g \cdot (v \otimes r) = (\text{id}_V \otimes m_R)(\text{id}_V \otimes g \otimes \text{id}_R)(\Delta_V \otimes \text{id}_R)(v \otimes r),$$

où m_R désigne la multiplication de R , c.-à-d., si $\Delta_V(v) = \sum_i v_i \otimes a_i$ alors $g \cdot (v \otimes r) = \sum_i v_i \otimes g(a_i)r$.

Démonstration. — L'élément neutre de $G(R)$ est $e = u_R \circ \varepsilon$ donc, pour tout $v \in V$, on a :

$$e \cdot (v \otimes 1) = (\text{id}_V \otimes u_R)(\text{id}_V \otimes \varepsilon)\Delta_V(v) = (\text{id}_V \otimes u_R)(v \otimes 1_\Lambda) = v \otimes 1.$$

Ceci montre que e agit bien comme l'identité.

Écrivons $\Delta_V(v) = \sum_i v_i \otimes a_i$ et soient $g, h \in G(R)$. Écrivant v au lieu de $v \otimes 1$ on a :

$$h \cdot v = \sum_i v_i \otimes h(a_i)$$

et donc

$$\begin{aligned}
g \cdot (h \cdot v) &= \sum_i (\text{id}_V \otimes m_R)(\text{id}_V \otimes g \otimes h)(\Delta_V \otimes \text{id}_A)\Delta_V(v) \\
&= \sum_i (\text{id}_V \otimes m_R)(\text{id}_V \otimes g \otimes h)(\text{id}_V \otimes \Delta_A)\Delta_V(v) \\
&= \sum_i (\text{id}_V \otimes gh)\Delta_V(v) = (gh) \cdot v.
\end{aligned}$$

Ceci prouve que $V \otimes R$ est un $G(R)$ -module à gauche. \square

Si l'on note $A = \Lambda[G]$, on retiendra donc le slogan : « un $\Lambda[G]$ -comodule à droite est un G -module à gauche ».

Remarques 1.13. — (1) Réciproquement, on peut montrer que si $V \otimes R$ est muni d'une action R -linéaire de $G(R)$, de façon fonctorielle en R , alors V est un $\Lambda[G]$ -comodule à droite. Voir par exemple SGA 3, Exp. I, 4.7.2 ou [Ja], I.2.8 ou [Wa], 3.2.

(2) Soit C une Λ -cogèbre, par exemple une algèbre de Hopf $A = \Lambda[G]$. Pour pouvoir parler commodément de « sous-comodules », il faut supposer que pour toute inclusion $N \subset M$ de Λ -modules, l'application $N \otimes C \rightarrow M \otimes C$ est *injective*, i.e. que C est un Λ -module *plat*. C'est pourquoi on se limite en général à étudier les représentations des Λ -schémas en groupes affine $A = \Lambda[G]$ qui sont *plats* sur Λ . Bien entendu, la platitude est automatique si Λ est un corps k .

(3) On prendra garde que [Ja] contient deux assertions erronées sur les intersections infinies de sous-comodules (p.29 ligne 7 et p. 33 lignes 2-3), voir SGA 3, Exp. VI_B, 11.10.1 pour des contre-exemples.

Définition 1.14 (Extension des scalaires). — Soit G un Λ -schéma en groupes affine, correspondant à l'algèbre de Hopf A , et soit Λ' une Λ -algèbre. Alors $A' = A \otimes \Lambda'$ est une Λ' -algèbre de Hopf, et le Λ' -schéma en groupes affine correspondant est noté $G_{\Lambda'}$.

Par exemple, on a déjà défini les \mathbb{Z} -schémas en groupes \mathbb{G}_a et \mathbb{G}_m ; pour tout corps k la k -algèbre de Hopf $k[X]$ (resp. $k[T, T^{-1}]$) correspond au k -schéma en groupes noté $\mathbb{G}_{a,k}$ (resp. $\mathbb{G}_{m,k}$).

D'autre part, si V est un A -comodule (i.e. un G -module) alors $V' = V \otimes \Lambda'$ est un A' -comodule (i.e. un $G_{\Lambda'}$ -module). On utilisera ceci plus bas dans le cas où $\Lambda = k$ est un corps et $\Lambda' = \bar{k}$ est une clôture algébrique de k .

Désormais on suppose, sauf indication contraire, que Λ est un **corps** k .

Proposition 1.15 (Propriété de finitude des comodules)

Soient k un corps, C une k -cogèbre, V un C -comodule à droite et E un sous-espace vectoriel (en abrégé, *sev*) de V de dimension finie.

(1) Notons C^* l'espace dual de C , $\text{ev} : C \otimes C^* \rightarrow k$ l'application d'évaluation, et $\theta(E)$ l'image de l'application linéaire ci-dessous :

$$E \otimes C^* \xrightarrow{\Delta_V \otimes \text{id}} V \otimes C \otimes C^* \xrightarrow{\text{id} \otimes \text{ev}} V.$$

Alors $\theta(E)$ est un *sev* de dimension finie et c'est le plus petit sous-comodule de V contenant E . On dira que c'est le sous-comodule engendré par E .

(2) Par conséquent, V est réunion de ses sous-comodules de dimension finie.

(3) Pour toute k -algèbre k' , $\theta(E) \otimes k'$ est le plus petit sous-comodule de $V \otimes k'$ contenant $E \otimes k'$.

Démonstration. — Soit $(c_\lambda)_{\lambda \in \Lambda}$ une base de C . Alors, tout élément de $V \otimes C$ s'écrit de façon unique $\sum_\lambda v_\lambda \otimes c_\lambda$, pour des $v_\lambda \in V$ uniquement déterminés et nuls sauf pour un nombre fini de λ .

(1) Soit (e_1, \dots, e_n) une base de E . Pour chaque $i = 1, \dots, n$, écrivons

$$(*) \quad \Delta_V(e_i) = \sum_{\lambda} v_{i\lambda} \otimes c_{\lambda}.$$

Alors $\theta(E)$ est le sous-espace W de V engendré par les $v_{i\lambda}$; il est de dimension finie car seulement un nombre fini des $v_{i\lambda}$ sont non nuls. Il contient E puisque pour tout i on a $e_i = (\text{id}_V \otimes \varepsilon)\Delta_V(e_i) = \sum_{\lambda} v_{i\lambda}\varepsilon(c_{\lambda})$. Pour tout sous-comodule M contenant E , on a

$$\Delta_V(E) \subset \Delta_V(M) \subset M \otimes C$$

et donc $\theta(E) \subset M$. Donc $W = \theta(E)$ est contenu dans tout sous-comodule M contenant E . Reste à montrer que W est un sous-comodule, i.e. que $\Delta_V(W) \subset W \otimes C$.

Appliquant $\Delta_V \otimes \text{id}_C$ à $(*)$ on a, d'une part,

$$(**) \quad (\Delta_V \otimes \text{id}_C) \circ \Delta_V(e_i) = \sum_{\lambda} \Delta_V(v_{i\lambda}) \otimes c_{\lambda}.$$

D'autre part, pour chaque $\nu \in \Lambda$, écrivons $\Delta(c_{\nu}) = \sum_{\lambda} \alpha_{\nu\lambda} \otimes c_{\lambda}$, où les $\alpha_{\nu\lambda} \in C$ sont nuls sauf pour un nombre fini d'indices. Alors on a, pour tout $i = 1, \dots, n$,

$$(***) \quad (\text{id}_V \otimes \Delta) \circ \Delta_V(e_i) = \sum_{\lambda} \left(\sum_{\nu} v_{i\nu} \otimes \alpha_{\nu\lambda} \right) \otimes c_{\lambda}.$$

Comme $(\Delta_V \otimes \text{id}_C) \circ \Delta_V = (\text{id}_V \otimes \Delta) \circ \Delta_V$, on en déduit que, pour tout i et λ , on a :

$$\Delta_V(v_{i\lambda}) = \sum_{\nu} v_{i\nu} \otimes \alpha_{\nu\lambda}.$$

On a donc $\Delta_V(W) \subset W \otimes C$, ce qui achève de prouver le point (1). Le point (2) en découle immédiatement.

(3) Soit k' une k -algèbre. Alors $W' = \theta(E) \otimes k'$ est un sous-comodule de $V' = V \otimes k'$ contenant $E' = E \otimes k'$, et comme les $c_{\lambda} \otimes 1$ forment une base de V' sur k' , il résulte de $(*)$ que tout sous-comodule de V' contenant E' contient W' . Ceci prouve que W' est le plus petit sous-comodule de V' contenant E' . \square

Remarques 1.16. — Si $k = \bar{k}$ est un corps algébriquement clos, on définit une variété algébrique affine X comme étant l'ensemble des zéros dans k^n (pour un certain entier $n \geq 1$) communs à tous les polynômes appartenant à un certain idéal J de $A = k[X_1, \dots, X_n]$. Notons que J n'est pas unique en général, car pour tout entier $r \geq 1$ l'idéal J^r définit le même ensemble de zéros que J . Mais comme on ne s'intéresse qu'aux fonctions polynomiales sur l'ensemble X et que f^r s'annule sur X ssi f s'y annule, on associe à X la k -algèbre de type fini $B = A/I$ où $I = \sqrt{J}$ est l'idéal de A formé des f dont une puissance est dans J . La k -algèbre B est réduite, i.e. n'a pas d'éléments nilpotents $\neq 0$.

(i) D'une part, si X' est une seconde variété algébrique affine, correspondant à la k -algèbre B' , on montre qu'un morphisme de variétés de X' vers X est « la même chose » qu'un morphisme de k -algèbres $B \rightarrow B'$. On voit donc qu'on peut définir la catégorie des variétés algébriques affines sur k comme étant la catégorie opposée de celle des k -algèbres de type fini réduites. La généralisation aux k -schémas affines (de type fini) consiste simplement à s'autoriser à considérer des k -algèbres (de type fini) non réduites, comme $k[T]/(T^n - 1)$ qui n'est pas réduite si $\text{car}(k)$ divise n .

(ii) D'autre part, on dit que le morphisme $X' \rightarrow X$ est une *immersion fermée* si c'est un isomorphisme de X' sur une sous-variété fermée de X , ce qui équivaut à dire que le morphisme d'algèbre $B \rightarrow B'$ est surjectif, i.e. que B' est le quotient de B par un certain idéal. Ceci justifie la définition suivante.

Définition 1.17. — Soient A, B deux k -algèbres de Hopf et G, H les k -schémas en groupes affines associés. On dit qu'un morphisme $H \rightarrow G$ de k -schémas en groupes affines est une *immersion fermée* si le morphisme d'algèbres de Hopf $A \rightarrow B$ qui lui correspond est surjectif, i.e. si B est le quotient de A par un certain idéal de Hopf I . Dans ce cas, on dit que H est un sous-schéma en groupes fermé de G .

On pourrait dès maintenant déduire de la proposition précédente le théorème disant que sur un corps k , tout k -schéma en groupes G affine de type fini est un sous-schéma en groupes fermé de $\mathrm{GL}_{n,k}$ pour un certain $n \in \mathbb{N}^*$, mais on va d'abord démontrer un autre énoncé, afin de mettre en valeur la force du Lemme de Yoneda.

Définition et proposition 1.18 (Stabilisateurs). — Soient k un corps, G un k -schéma en groupes affines, $A = k[G]$ la k -algèbre de Hopf correspondante, V un A -comodule, $v \in V$ et W un sev de V . Le **stabilisateur** de W (resp. de v), noté G_W (resp. G_v) est le sous-foncteur de G défini comme suit : pour toute k -algèbre R ,

$$\begin{aligned} G_W(R) &= \{g \in G(R) \mid g(W \otimes R) = W \otimes R\} \\ &= \{g \in G(R) \mid g(W \otimes R) \subset W \otimes R \text{ et } g^{-1}(W \otimes R) \subset W \otimes R\} \end{aligned}$$

$$G_v(R) = \{g \in G(R) \mid g(v \otimes 1) = v \otimes 1\}.$$

Alors G_W et G_v sont des sous-schémas en groupes fermés de G , i.e. chacun d'eux provient d'une certaine algèbre de Hopf quotient de A .

Démonstration. — Faisons-la pour G_W ; le cas de G_v est analogue et est laissé au lecteur. Soit $(v_i)_{i \in I}$ une base de W , complétons-la en une base $(v_i)_{i \in I'}$ de V , où $I' \supset I$. Pour tout $j \in I$, on peut écrire de façon unique

$$\Delta_V(v_j) = \sum_{i \in I} v_i \otimes a_{ij} + \sum_{i \in I' - I} v_i \otimes b_{ij}$$

avec les a_{ij} et b_{ij} dans A , nuls sauf pour un nombre fini d'indices. Soient R une k -algèbre et $g \in G(R)$, i.e. g est un morphisme de k -algèbres $A \rightarrow R$. Alors dans $V \otimes R$ on a l'égalité :

$$g(v_j \otimes 1) = \sum_{i \in I} v_i \otimes g(a_{ij}) + \sum_{i \in I' - I} v_i \otimes g(b_{ij})$$

donc on voit que $g(W \otimes R) \subset W \otimes R$ ssi g s'annule sur tous les b_{ij} . De même, comme $g^{-1} = g \circ \tau$ (où τ est l'antipode de A), on voit que $g^{-1}(W \otimes R) \subset W \otimes R$ ssi g s'annule sur tous les $\tau(b_{ij})$. Notons alors \mathcal{I} l'idéal de A engendré par les b_{ij} et $\tau(b_{ij})$. Comme un morphisme de k -algèbres $A \rightarrow R$ qui s'annule sur \mathcal{I} est « la même chose » qu'un morphisme de k -algèbres $A/\mathcal{I} \rightarrow R$, on obtient donc un isomorphisme canonique

$$G_W(R) = \mathrm{Hom}_{k\text{-alg.}}(A/\mathcal{I}, R)$$

qui est fonctoriel en R . On pourrait montrer directement que \mathcal{I} est un idéal de Hopf, mais ceci va résulter du Lemme de Yoneda ci-dessous. \square

2. Lemme de Yoneda et conséquences

2.1. Lemme de Yoneda et foncteurs représentables. — Soit \mathcal{C} une catégorie. On notera $\widehat{\mathcal{C}}$ la catégorie des foncteurs *contravariants*⁽⁵⁾ de \mathcal{C} dans la catégorie (Ens) des ensembles. Pour tout objet X de \mathcal{C} , on notera h_X l'élément de $\widehat{\mathcal{C}}$ défini par $h_X(Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$, et pour toute flèche $f : Z \rightarrow Y$ dans \mathcal{C} , $h_X(f)$ est l'application :

$$\mathrm{Hom}_{\mathcal{C}}(Y, X) \rightarrow \mathrm{Hom}_{\mathcal{C}}(Z, X), \quad g \mapsto g \circ f.$$

⁽⁵⁾Ce choix sera justifié plus bas.

Rappelons que si G, F sont des objets de $\widehat{\mathcal{C}}$, un morphisme de foncteurs $\phi : G \rightarrow F$ est la donnée, pour tout objet Y de \mathcal{C} , d'une application $\phi_Y : G(Y) \rightarrow F(Y)$, telle que pour tout morphisme $f : Z \rightarrow Y$ le diagramme ci-dessous soit commutatif :

$$\begin{array}{ccc} G(Y) & \xrightarrow{G(f)} & G(Z) \\ \phi_Y \downarrow & & \downarrow \phi_Z \\ F(Y) & \xrightarrow{F(f)} & F(Z). \end{array}$$

En particulier, si l'on a un morphisme de foncteurs $\phi : h_X \rightarrow F$ alors, comme id_X est un élément de $h_X(X) = \text{Hom}_{\mathcal{C}}(X, X)$, on peut considérer l'élément $\phi_X(\text{id}_X) \in F(X)$.

Lemme 2.1. — Soit X (resp. F) un objet de \mathcal{C} (resp. $\widehat{\mathcal{C}}$). On a une bijection canonique

$$\theta : \text{Hom}_{\widehat{\mathcal{C}}}(h_X, F) \xrightarrow{\sim} F(X), \quad \phi \mapsto \phi_X(\text{id}_X).$$

Démonstration. — Soit ϕ un morphisme de foncteur $h_X \rightarrow F$ et soient Y un objet de \mathcal{C} et f un élément de $h_X(Y)$ i.e. un morphisme $f : Y \rightarrow X$. On a un diagramme commutatif :

$$\begin{array}{ccc} \text{Hom}_{\mathcal{C}}(X, X) & \xrightarrow{h_X(f)} & \text{Hom}_{\mathcal{C}}(Y, X) \\ \phi_X \downarrow & & \downarrow \phi_Y \\ F(X) & \xrightarrow{F(f)} & F(Y). \end{array}$$

Or f est l'image par $h_X(f)$ de id_X et donc $\phi_Y(f) = F(f)(\phi_X(\text{id}_X))$. Ceci montre que ϕ est déterminé par l'élément $u = \phi_X(\text{id}_X)$, i.e. que l'application θ du lemme est *injective*.

Réciproquement, fixons u dans $F(X)$ et pour tout objet Y de \mathcal{C} définissons

$$\phi_Y^u : \text{Hom}_{\mathcal{C}}(Y, X) \rightarrow F(Y), \quad f \mapsto F(f)(u).$$

Soit $g : Z \rightarrow Y$ un morphisme de \mathcal{C} ; considérons le diagramme ci-dessous :

$$\begin{array}{ccc} \text{Hom}_{\mathcal{C}}(Y, X) & \xrightarrow{h_X(g)} & \text{Hom}_{\mathcal{C}}(Z, X) \\ \phi_Y^u \downarrow & & \downarrow \phi_Z^u \\ F(Y) & \xrightarrow{F(g)} & F(Z). \end{array}$$

Soit $f : Y \rightarrow X$. Alors $\phi_Y^u(f) = F(f)(u)$ et donc $(F(g) \circ \phi_Y^u)(f) = (F(g) \circ F(f))(u)$. D'autre part, $h_X(g)(f) = g \circ f$ et donc $(\phi_Z^u \circ h_X(g))(f) = F(g \circ f)(u)$. Le diagramme précédent est donc commutatif, et ceci montre que $\phi^u : h_X \rightarrow F$ est bien un morphisme de foncteurs. Ceci montre que l'application injective θ est aussi *surjective* ; c'est donc une bijection. \square

Remarquons que toute flèche $f : X \rightarrow Y$ dans \mathcal{C} induit un morphisme de foncteurs $h_f : h_X \rightarrow h_Y$, défini par $h_f(g) = f \circ g$ pour tout $g : Z \rightarrow X$. Par conséquent, $X \mapsto h_X$ est un foncteur covariant de \mathcal{C} dans $\widehat{\mathcal{C}}$.

Corollaire 2.2. — Pour tous objets X, Y de \mathcal{C} , on a $\text{Hom}_{\widehat{\mathcal{C}}}(h_X, h_Y) = \text{Hom}_{\mathcal{C}}(X, Y)$. Par conséquent, le foncteur $X \mapsto h_X$ est pleinement fidèle et permet d'identifier \mathcal{C} à une sous-catégorie pleine de $\widehat{\mathcal{C}}$.

Démonstration. — D'après le lemme 2.1, on a $\text{Hom}_{\widehat{\mathcal{C}}}(h_X, h_Y) = h_Y(X) = \text{Hom}_{\mathcal{C}}(X, Y)$. Ceci prouve la première assertion, et la seconde n'en est qu'une reformulation. \square

Définition et proposition 2.3 (Foncteurs représentables)

Soit F un objet de $\widehat{\mathcal{C}}$. On dit que F est **représentable** s'il existe un couple (X, ϕ) où X est un objet de \mathcal{C} et ϕ un isomorphisme $h_X \xrightarrow{\sim} F$.

Dans ce cas, le couple (X, ϕ) est unique à isomorphisme unique près, i.e. si (X', ϕ') est un autre couple représentant F , il existe un unique morphisme $f : X' \rightarrow X$ tel que $\phi \circ h_f = \phi'$ et f est un isomorphisme.

Démonstration. — Comme ϕ est un isomorphisme, il existe un unique morphisme de foncteur $\alpha : h_{X'} \rightarrow h_X$ tel que $\phi \circ \alpha = \phi'$, à savoir $\alpha = \phi^{-1} \circ \phi'$, et d'après la pleine fidélité prouvée plus haut, il existe un *unique* morphisme $f : X' \rightarrow X$ tel que $h_f = \alpha$.

De même, il existe un unique morphisme $g : X \rightarrow X'$ tel que $h_g = \phi'^{-1} \circ \phi$. Alors $h_g \circ h_f$ est l'identité de $h_{X'}$ et $h_f \circ h_g$ est l'identité de h_X . Par pleine fidélité à nouveau, ceci entraîne que $g \circ f = \text{id}_{X'}$ et $f \circ g = \text{id}_X$. Ceci montre que g est l'inverse de f . \square

Remarque 2.4. — On obtient des résultats analogues si à tout objet X de \mathcal{C} on associe le foncteur *covariant* $h^X : Y \mapsto \text{Hom}_{\mathcal{C}}(X, Y)$. Mais dans ce cas $X \mapsto h^X$ est *contravariant* donc il identifie la catégorie opposée \mathcal{C}^{opp} à une sous-catégorie pleine de celle des foncteurs covariants $\mathcal{C} \rightarrow (\text{Ens})$. C'est pour cette raison qu'on a considéré les foncteurs h_X plutôt que les h^X .

Proposition 2.5. — Soit \mathcal{C} une catégorie possédant un objet final ω et dans laquelle les produits finis existent. Soit X un objet de \mathcal{C} . On suppose que le foncteur $h_X : \mathcal{C} \rightarrow (\text{Ens})$ est un foncteur en groupes, i.e. $h_X(Y)$ est un groupe pour tout objet Y de \mathcal{C} , et pour toute flèche $f : Z \rightarrow Y$ dans \mathcal{C} , l'application $h_X(f) : h_X(Y) \rightarrow h_X(Z)$ est un morphisme de groupes. Alors X est un groupe dans la catégorie \mathcal{C} , i.e. il existe dans \mathcal{C} des morphismes $m : X \times X \rightarrow X$, $e : \omega \rightarrow X$ et $\iota : X \rightarrow X$ tels que les diagrammes ci-dessous soient commutatifs :

$$\begin{array}{ccc}
 X \times X \times X & \xrightarrow{m \times \text{id}_X} & X \times X \\
 \text{id}_X \times m \downarrow & & \downarrow m \\
 X \times X & \xrightarrow{m} & X
 \end{array}
 \quad
 \begin{array}{ccc}
 X & \xrightarrow{(\text{id}_X, e)} & X \times X \\
 (e, \text{id}_X) \downarrow & \searrow \text{id}_X & \downarrow m \\
 X \times X & \xrightarrow{m} & X
 \end{array}
 \quad
 \begin{array}{ccc}
 X & \xrightarrow{(\text{id}_X, \iota)} & X \times X \\
 (\iota, \text{id}_X) \downarrow & \searrow e & \downarrow m \\
 X \times X & \xrightarrow{m} & X
 \end{array}$$

où l'on a noté $e : X \rightarrow X$ la composée de l'unique morphisme $X \rightarrow \omega$ avec $e : \omega \rightarrow X$.

Démonstration. — Remarquons d'abord que pour tout objet Y de \mathcal{C} , $h_\omega(Y)$ est l'ensemble à un élément $\{\text{pt}\}$. Alors la structure de groupe sur les $h_X(Y)$, fonctorielle en Y , revient à se donner :

(i) Un morphisme de foncteurs $m : h_X \times h_X \rightarrow h_X$ qui est « associatif », i.e. qui vérifie $m \circ (m \times \text{id}) = m \circ (\text{id} \times m)$.

(ii) Des morphismes « élément neutre » $e : h_\omega \rightarrow h_X$ et « inverse » $\iota : h_X \rightarrow h_X$ qui vérifient les propriétés indiquées dans les diagrammes précédents.

Comme les produits existent dans \mathcal{C} alors $h_X \times h_X$ (resp. $h_X \times h_X \times h_X$) est représenté par $X \times X$ (resp. $X \times X \times X$). Par pleine fidélité, e , ι , m proviennent de morphismes $\omega \rightarrow X$, $X \rightarrow X$ et $X \times X \rightarrow X$ que l'on notera encore e , ι et m , et l'on a les diagrammes commutatifs indiqués. \square

Corollaire 2.6. — Soit \mathcal{A} une catégorie possédant un objet initial α et dans laquelle les coproduits finis existent, et soit A un objet de \mathcal{A} . On suppose que le foncteur covariant $h^A : \mathcal{A} \rightarrow (\text{Ens})$, $R \mapsto \text{Hom}_{\mathcal{A}}(A, R)$ est un foncteur en groupes. Alors A est muni d'une structure de « cogroupe » dans \mathcal{A} , i.e. il existe dans \mathcal{A} des morphismes $\Delta : A \rightarrow A \sqcup A$

(où \sqcup désigne le coproduit), $\varepsilon : A \rightarrow \alpha$ et $\tau : A \rightarrow A$ tels que les diagrammes ci-dessous soient commutatifs :

$$\begin{array}{ccccc}
 A \sqcup A \sqcup A & \xleftarrow{\Delta \times \text{id}_A} & A \sqcup A & & A & \xleftarrow{(\text{id}_A, \varepsilon)} & A \sqcup A & & A & \xleftarrow{(\text{id}_A, \tau)} & A \sqcup A \\
 \text{id}_A \times \Delta \uparrow & & \uparrow \Delta & & (\varepsilon, \text{id}_A) \uparrow & \searrow \text{id}_A & \uparrow \Delta & & (\tau, \text{id}_A) \uparrow & \searrow \varepsilon & \uparrow \Delta \\
 A \sqcup A & \xleftarrow{\Delta} & A & & A \sqcup A & \xleftarrow{\Delta} & A & & A \sqcup A & \xleftarrow{\Delta} & A
 \end{array}$$

où l'on a noté $\varepsilon : A \rightarrow A$ la composée de $\varepsilon : A \rightarrow \alpha$ avec l'unique morphisme $\alpha \rightarrow A$.

Soient Λ un anneau commutatif et \mathcal{A} la catégorie des Λ -algèbres. Alors Λ est objet initial et le coproduit est donné par le produit tensoriel. On en déduit :

Corollaire 2.7. — (i) Soit A une Λ -algèbre. Se donner une structure de foncteur en groupes sur le foncteur h^A **équivaut** à se donner une structure d'algèbre de Hopf sur A .

(ii) Supposons que h^B soit un second foncteur en groupes et soit $h^A \rightarrow h^B$ un morphisme de foncteurs en groupes. Alors le morphisme de Λ -algèbres $\phi : B \rightarrow A$ qui lui correspond est un morphisme d'algèbres de Hopf.

Corollaire 2.8. — Dans la proposition 1.18, la k -algèbre A/\mathcal{I} qui représente le foncteur en groupes G_W (resp. G_v) est une algèbre de Hopf quotient de A , i.e. \mathcal{I} est un idéal de Hopf.

Définition 2.9 (GL_n et SL_n). — Soit $n \in \mathbb{N}^*$. Considérons le foncteur GL_n qui à tout anneau R associe le groupe $\text{GL}_n(R)$ des matrices de taille n à coefficients dans R et de déterminant inversible dans R , et à tout morphisme $f : R \rightarrow S$ associe le morphisme $\text{GL}_n(R) \rightarrow \text{GL}_n(S)$ obtenu en appliquant f à chaque coefficient de la matrice ; ceci est bien un morphisme de groupes car $\sum_{k=1}^n f(a_{ik})f(b_{kj}) = f(\sum_{k=1}^n a_{ik}b_{kj})$. Ce foncteur est représenté par l'anneau

$$A = \mathbb{Z}[\text{GL}_n] = \mathbb{Z}[X_{11}, \dots, X_{nn}, \text{dét}^{-1}] = \mathbb{Z}[X_{11}, \dots, X_{nn}, T]/(T \text{dét}(X_{ij}) - 1).$$

Plus précisément, l'isomorphisme de foncteurs $\phi : h^A \xrightarrow{\sim} \text{GL}_n$ s'obtient en associant à tout morphisme $\chi : A \rightarrow R$ l'élément de $\text{GL}_n(R)$ dont le coefficient d'indice (i, j) est $\chi(X_{ij})$; ceci revient à évaluer χ sur la matrice « générique »

$$\begin{pmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & \ddots & \vdots \\ X_{n1} & \cdots & X_{nn} \end{pmatrix}$$

qui est l'élément de $\text{GL}_n(A)$ correspondant à l'isomorphisme de foncteur $\phi : h^A \xrightarrow{\sim} \text{GL}_n$.

Vu la formule donnant le coefficient d'indice (i, j) d'un produit de matrices, on voit que la comultiplication est donnée par

$$\Delta(X_{ij}) = \sum_{k=1}^n X_{ik} \otimes X_{kj}.$$

Et comme l'élément neutre est la matrice identité I_n , on voit que l'augmentation est donnée par $\varepsilon(X_{ij}) = \delta_{ij}$. Enfin, vu la formule $A^{-1} = \text{dét}(A)^{-1} {}^t\text{Com}(A)$, où $\text{Com}(A)$ désigne la matrice des cofacteurs, on voit que l'antipode est donnée par

$$\tau(X_{ij}) = \text{dét}(A)^{-1} (-1)^{i+j} \Delta_{j,i}(A),$$

où $\Delta_{j,i}(A)$ désigne le mineur de A d'indice (j, i) . Bien sûr, on peut vérifier par un calcul direct que ceci définit une structure d'algèbre de Hopf sur $\mathbb{Z}[\text{GL}_n]$, mais on sait sans calcul qu'il en est bien ainsi car Δ , ε et τ reflètent (et induisent) la structure de groupe connue sur $\text{GL}_n(R)$ pour tout anneau R .

Pour tout corps k (plus généralement, pour tout anneau k) on notera $\mathrm{GL}_{n,k}$ le k -foncteur en groupes représenté par l'algèbre de Hopf

$$k[X_{11}, \dots, X_{nn}, \det^{-1}] = k[X_{11}, \dots, X_{nn}, T]/(T \det(X_{ij}) - 1),$$

i.e. le foncteur qui à toute k -algèbre R associe le groupe $\mathrm{GL}_n(R)$.

On définit de même le foncteur en groupes SL_n qui à tout anneau R associe le groupe $\mathrm{SL}_n(R)$ des matrices de taille n à coefficients dans R et de déterminant 1. Il est représenté par

$$\mathbb{Z}[\mathrm{SL}_n] = \mathbb{Z}[X_{11}, \dots, X_{nn}]/(\det(X_{ij}) - 1).$$

et l'on définit de même le foncteur $\mathrm{SL}_{n,k}$.

Remarque 2.10. — Soit V un k -espace vectoriel de dimension finie n . On peut définir de façon plus abstraite le k -foncteur en groupes $\mathrm{GL}(V)$ qui associe à toute k -algèbre R le groupe des R -automorphismes du R -module $V \otimes R$. Posons $E = V \otimes V^*$ et soit $S(E)$ son algèbre symétrique. Alors le déterminant \det est un élément bien défini de $S^n(E)$ et $\mathrm{GL}(V)$ est représenté par la k -algèbre $S(E)[\det^{-1}] = S(E)[T]/(T \det - 1)$.

Proposition 2.11. — Soit k un corps, G un k -schéma en groupes affine et V un G -comodule de dimension n . Alors la structure de comodule définit un morphisme de k -schémas en groupes $G \rightarrow \mathrm{GL}(V)$, i.e. un morphisme d'algèbres de Hopf $k[\mathrm{GL}(V)] \rightarrow k[G]$.

Démonstration. — Ceci résulte du Lemme de Yoneda, car la structure de comodule définit un morphisme de groupes $\rho(R) : G(R) \rightarrow \mathrm{GL}(V)(R)$, fonctoriel en R .

Une autre démonstration, plus directe mais basée sur la même idée, est la suivante. Soit $\{e_1, \dots, e_n\}$ une base de V ; il existe des $c_{ij} \in k[G]$, uniquement déterminés, tels que pour $j = 1, \dots, n$ on ait :

$$(*) \quad \Delta_V(e_j) = \sum_{i=1}^n e_i \otimes c_{ij}.$$

Notons D le déterminant de la matrice $(c_{ij})_{1 \leq i, j \leq n}$. Pour tout morphisme de k -algèbres $g : k[G] \rightarrow R$, on a $g(e_j \otimes 1) = \sum_{i=1}^n e_i \otimes g(c_{ij})$ donc l'image de $g \in G(R)$ dans $\mathrm{GL}_n(R)$ est la matrice $(g(c_{ij}))_{1 \leq i, j \leq n}$ et son déterminant, égal à $g(D)$, est un élément inversible de R . Appliquant ceci au morphisme $\mathrm{id} : k[G] \rightarrow k[G]$, on obtient que D est un élément inversible de $k[G]$. Par conséquent, le morphisme de k -algèbres $k[X_{11}, \dots, X_{nn}] \rightarrow k[G]$ défini par $\phi(X_{ij}) = c_{ij}$ se prolonge en morphisme de k -algèbres $\phi : k[\mathrm{GL}_n] \rightarrow k[G]$. Alors, pour toute k -algèbre R et $g \in G(R)$ on a $\rho(R)(g) = g \circ \phi$.

Il reste à vérifier que ϕ est un morphisme d'algèbres de Hopf. Notons Δ la comultiplication de $k[G]$ et Δ' celle de $k[\mathrm{GL}_n]$. Soient R une k -algèbre et $g, h \in G(R)$; comme $\rho(R)$ est un morphisme de groupes on a $\rho(R)(gh) = \rho(R)(g)\rho(R)(h)$, i.e. le diagramme ci-dessous est commutatif :

$$\begin{array}{ccccc} k[G] & \xrightarrow{\Delta} & k[G] \otimes k[G] & \xrightarrow{g \otimes h} & R \otimes R & \xrightarrow{m_R} & R \\ \uparrow \phi & & & & \nearrow m_R \circ (g \otimes h) & & \\ k[\mathrm{GL}_n] & \xrightarrow{\Delta'} & k[\mathrm{GL}_n] \otimes k[\mathrm{GL}_n] & & & & \end{array}$$

Appliquant ceci à $R = k[G] \otimes k[G]$, $g(a) = a \otimes 1$ et $h(b) = 1 \otimes b$, on obtient que $\Delta \circ \phi = (\phi \otimes \phi) \circ \Delta'$.

On laisse au lecteur la tâche de vérifier de même que $\varepsilon \circ \phi = \varepsilon'$ et $\tau \circ \phi = \phi \circ \tau'$. (En règle générale, il vaut mieux appliquer le Lemme de Yoneda que de chercher explicitement R, g, h comme ci-dessus.) \square

Théorème 2.12. — Soient k un corps et G un k -schéma en groupes affine de type fini, i.e. $k[G]$ est une k -algèbre de type fini. Alors G est linéaire, c.-à-d. c'est un sous-schéma en groupes fermé d'un certain $\mathrm{GL}(V)$.

Démonstration. — La comultiplication $\Delta : k[G] \rightarrow k[G] \otimes k[G]$ fait de $k[G]$ un $k[G]$ -comodule à droite. Soient x_1, \dots, x_s des générateurs de $k[G]$ comme k -algèbre. D'après la proposition 1.15 ils engendrent un sous-comodule V de dimension finie. Soit $\{e_1, \dots, e_n\}$ une base de V ; il existe des $c_{ij} \in k[G]$, uniquement déterminés, tels que pour $j = 1, \dots, n$ on ait :

$$(*) \quad \Delta(e_j) = \sum_{i=1}^n e_i \otimes c_{ij}$$

et d'après la preuve de la proposition précédente, il y a un morphisme d'algèbres de Hopf $\phi : k[\mathrm{GL}_n] \rightarrow k[G]$ défini par $\phi(X_{ij}) = c_{ij}$. Pour tout $j = 1, \dots, n$ on a alors :

$$e_j = (\varepsilon \otimes 1)\Delta(e_j) = \sum_{i=1}^n \varepsilon(e_i)c_{ij} = \phi\left(\sum_{i=1}^n \varepsilon(e_i)X_{ij}\right)$$

et donc l'image de ϕ contient les e_j donc V et donc les générateurs x_1, \dots, x_s . Il en résulte que ϕ est surjective. \square
