

1. LANGAGE FONCTORIEL

Les notions de *catégories* et de *foncteurs* ont été dégagées par Saunders MAC LANE et Samuel EILENBERG vers 1945 dans le cadre de la topologie algébrique. Leur intérêt vient en particulier du fait qu'elles permettent

- de travailler avec des objets mathématiques à *isomorphisme près* (la relation d'égalité est souvent non pertinente car trop rigide) ;
- de formuler de manière efficace la notion de *propriété universelle* ;
- de penser en termes de *diagrammes* ;
- de formuler « géométriquement » la théorie naïve des ensembles.

1.1. Catégories et foncteurs

(1.1.1) Une *catégorie* C est la donnée

- d'un ensemble $\text{Ob}(C)$ d'*objets* ;
- pour tous objets X et Y de C , d'un ensemble $\text{Hom}_C(X, Y)$ de *flèches* (ou *morphismes*), notées $X \xrightarrow{f} Y$ ou $f : X \rightarrow Y$;
- pour tous objets X, Y et Z de C , d'une *composition*

$$\text{Hom}_C(X, Y) \times \text{Hom}_C(Y, Z) \rightarrow \text{Hom}_C(X, Z), (f, g) \mapsto g \circ f,$$

de telle sorte que les axiomes suivants soient vérifiés

(Ass) la composition des flèches est *associative* : pour toutes flèches $X \xrightarrow{f} Y$, $Y \xrightarrow{g} Z$ et $Z \xrightarrow{h} T$ dans C , $h \circ (g \circ f) = (h \circ g) \circ f$;

(Id) pour tout objet X de C , il existe une flèche $1_X \in \text{Hom}_C(X, X)$ telle que, pour toutes flèches $X \xrightarrow{f} Y$ et $Y \xrightarrow{g} X$, $f \circ 1_X = f$ et $1_Y \circ g = g$.

Remarque — Il découle immédiatement de l'axiome (Id) que, pour tout objet X de C , la flèche 1_X est *unique*.

Étant donnée une catégorie C , une flèche $X \xrightarrow{f} Y$ est un *isomorphisme* s'il existe une flèche $Y \xrightarrow{g} X$ telle que $g \circ f = 1_X$ et $f \circ g = 1_Y$. Si elle existe, la flèche g est unique et on la note f^{-1} ; c' est l'*inverse* de f .

Exemples — 1. Mentionnons tout d'abord les catégories naturellement associées à des structures mathématiques.

- La catégorie **Ens** des ensembles : les objets sont les ensembles, les flèches sont les applications, la composition est la composition usuelle et, pour tout objet X , 1_X est l'application identique. Les isomorphismes sont les bijections.
- La catégorie **Gr** des groupes : les objets sont les groupes, les flèches sont les homomorphismes de groupes, la composition est la composition usuelle et, pour tout objet X , 1_X est l'homomorphisme identité. Les isomorphismes sont les homomorphismes bijectifs.
- La catégorie **Ab** des groupes abéliens : les objets sont les groupes abéliens, les flèches sont les homomorphismes de groupes, la composition est la composition usuelle et, pour tout objet X , 1_X est l'homomorphisme identité. Les isomorphismes sont les homomorphismes bijectifs.

⁽¹⁾Version du 9 décembre 2008

- (iv) La catégorie **Ann** des anneaux commutatifs : les objets sont les anneaux commutatifs, les flèches sont les homomorphismes d'anneaux, la composition est la composition usuelle et, pour tout objet X , 1_X est l'homomorphisme identité. Les isomorphismes sont les homomorphismes bijectifs.
- (v) La catégorie **Top** des espaces topologiques : les objets sont les espaces topologiques, les flèches sont les applications continues, la composition est la composition usuelle et, pour tout objet X , 1_X est l'application identité. Les isomorphismes sont les homéomorphismes.
- (vi) Si k est un corps, **Vect**(k) est la catégorie des k -espaces vectoriels : les objets sont les k -espaces vectoriels, les flèches sont les applications linéaires, la composition est la composition usuelle et, pour tout objet X , 1_X est l'application identité. Les isomorphismes sont les applications linéaires bijectives.

2. On peut d'autre part attacher une catégorie C à tout ensemble partiellement ordonné (E, \leq) :

- les objets sont les éléments de E ;
- étant donnés des éléments x et y de E ,

$$\text{Hom}_C(x, y) = \begin{cases} \text{l'ensemble } 1 \text{ à un élément} & \text{si } x \leq y \\ \emptyset & \text{sinon.} \end{cases}$$

Il existe une seule manière de définir la composition, qui est automatiquement associative. Enfin, pour tout $x \in E$, 1_x est l'unique élément de l'ensemble $\text{Hom}_C(x, x)$.

3. Voici un exemple plus exotique. Étant donné un corps k , on désigne par Δ_k la catégorie suivante :
- les objets sont les nombres entiers naturels $0, 1, \dots$;
 - étant donnés des nombres entiers n et m , $\text{Hom}_{\Delta_k}(n, m)$ est l'ensemble $M_{m,n}(k)$ des matrices à m lignes et n colonnes à coefficients dans k ;
 - pour tous entiers m, n et p , la composition $M_{n,m}(k) \times M_{p,n}(k) \rightarrow M_{p,m}(k)$ est le produit matriciel ;
 - pour tout entier n , 1_n est la matrice identité I_n .

Les isomorphismes sont les matrices inversibles.

4. Mentionnons enfin que l'on peut associer à toute catégorie C sa catégorie *opposée* C^{op} : les objets de C^{op} sont les objets de C et, pour tous objets X, Y de C ,

$$\text{Hom}_{C^{\text{op}}}(X, Y) = \text{Hom}_C(Y, X).$$

Si l'on conçoit C comme un graphe, C^{op} est le graphe obtenu en reversant le sens des flèches.

(1.1.2) Si C et C' sont deux catégories, un *foncteur* $F : C \rightarrow C'$ est la donnée :

- pour tout objet X de C , d'un objet $F(X)$ de C' ;
- pour toute flèche $X \xrightarrow{f} Y$ dans C , d'une flèche $F(X) \xrightarrow{F(f)} F(Y)$ dans C' ,

de telle sorte que les axiomes suivants soient vérifiés :

(Ass') pour toutes flèches $X \xrightarrow{f} Y$ et $Y \xrightarrow{g} Z$ dans C , $F(g \circ f) = F(g) \circ F(f)$;

(Id') pour tout objet X de C , $F(1_X) = 1_{F(X)}$.

Le *composé* $G \circ F$ de deux foncteurs $F : C \rightarrow C'$ et $G : C' \rightarrow C''$ est défini de manière évidente : $(G \circ F)(X) = G(F(X))$ et $(G \circ F)(f) = G(F(f))$.

Remarque — Les foncteurs que l'on vient de définir sont souvent dits *covariants*. En remplaçant dans la définition précédente l'axiome (Ass') par la variante $F(g \circ f) = F(f) \circ F(g)$, on obtient la notion de foncteur *contravariant* ; de manière équivalente, il s'agit d'un foncteur $C^{\text{op}} \rightarrow C'$ ou $C \rightarrow C'^{\text{op}}$.

Exemples — 1. Pour toute catégorie C , on dispose d'un foncteur 1_C défini par $1_C(X) = X$ et $1_C(f) = f$.

2. On dispose d'un foncteur d'oubli de structure $\mathbf{Gr} \rightarrow \mathbf{Ens}$ associant à tout groupe l'ensemble sous-jacent et à tout homomorphisme de groupe l'application correspondante. De même : $\mathbf{Ann} \rightarrow \mathbf{Ab}$, $\mathbf{Top} \rightarrow \mathbf{Ens}$, etc.

3. Soit k un corps. On définit un foncteur de dualité $D : \mathbf{Vect}(k) \rightarrow \mathbf{Vect}(k)^{\text{op}}$ en associant à un k -espace vectoriel V (resp. à une application k -linéaire u) l'espace vectoriel dual $D(V) = \text{Hom}_k(V, k)$ (resp. l'application contragrédiente u^\vee définie par $u^\vee(\varphi) = \varphi \circ u$).

4. Désignant toujours par k un corps, on définit un foncteur $L : \Delta_k \rightarrow \mathbf{Vect}(k)$ en associant à tout entier n le k -espace vectoriel $L(n) = k^n$ et à toute matrice $M \in \text{Hom}_{\Delta_k}(n, m) = M_{m,n}(k)$ l'application k -linéaire correspondante de k^n dans k^m .

5. Désignons par $\pi_0(X)$ l'ensemble des composantes connexes d'un espace topologique X . Chaque application continue $f : X \rightarrow Y$ envoyant une composante connexe de X sur une partie connexe de Y , il existe une unique application $\pi_0(f) : \pi_0(X) \rightarrow \pi_0(Y)$ telle que $f(Z) \subset \pi_0(f)(Z)$ pour toute composante connexe Z de X . On obtient ainsi un foncteur « composantes connexes » $\pi_0 : \mathbf{Top} \rightarrow \mathbf{Ens}$.

6. De façon très générale, la *topologie algébrique* est l'étude de certains foncteurs $\mathbf{Top} \rightarrow \mathbf{C}$, où \mathbf{C} est une catégorie de structures algébriques : \mathbf{Ab} , \mathbf{Gr} , $\mathbf{Vect}(k)$, etc.

Dans ce cours, nous nous intéresserons essentiellement aux foncteurs $\mathbf{Ann} \rightarrow \mathbf{Gr}$.

(1.1.3) Si $F, G : C \rightarrow D$ sont deux foncteurs, un *morphisme* (ou une *transformation naturelle* de F dans G) est la donnée, pour tout objet X de C , d'un morphisme $\varphi_X : F(X) \rightarrow G(X)$ dans D , de telle sorte que la condition suivante soit vérifiée : pour toute flèche $X \xrightarrow{f} Y$ dans C , le diagramme

$$\begin{array}{ccc} F(X) & \xrightarrow{\varphi_X} & G(X) \\ F(f) \downarrow & & \downarrow G(f) \\ F(Y) & \xrightarrow{\varphi_Y} & G(Y) \end{array}$$

est commutatif, i.e. $\varphi_Y \circ F(f) = G(f) \circ \varphi_X$.

Exemples — 1. On dispose pour tout foncteur $F : C \rightarrow D$ d'un morphisme *identité* 1_F de F dans lui-même : quel que soit l'objet X de C , $(1_F)_X = 1_{F(X)}$.

2. Par la suite, nous rencontrerons à maintes reprises des morphismes de foncteurs qui seront fabriqués sur le modèle suivant. Soit $n \geq 1$ un entier. Tout homomorphisme d'anneaux commutatifs $f : A \rightarrow B$ donne naturellement naissance à un homomorphisme de monoïdes (multiplicatifs) $M_n(f) : M_n(A) \rightarrow M_n(B)$ associant à une matrice (x_{ij}) la matrice $M_n(f)(x_{ij}) = (f(x_{ij}))$; on définit ainsi un foncteur M_n de la catégorie des anneaux commutatifs dans la catégorie \mathbf{Mon} des monoïdes. Le déterminant d'une matrice s'exprimant polynomialement en ses coefficients, $\det(M_n(f)(M)) = f(\det(M))$ pour toute matrice $M \in M_n(A)$ et donc le déterminant fournit un morphisme de foncteurs $\det : M_n \rightarrow M_1$.

Les morphismes de foncteurs se composent de manière évidente. Un morphisme de foncteurs $\varphi : F \rightarrow G$ est un *isomorphisme* s'il vérifie les conditions équivalentes suivantes :

- (i) il existe un morphisme de foncteurs $\psi : G \rightarrow F$ tel que $\psi \circ \varphi = 1_F$ et $\varphi \circ \psi = 1_G$;
- (ii) pour tout objet X de C , φ_X est un isomorphisme.

(1.1.4) Étant donnée une catégorie arbitraire C , nous allons comparer les foncteurs de C dans \mathbf{Gr} et les foncteurs de C dans \mathbf{Ens} .

Le produit $F \times G$ de deux foncteurs $F, G : C \rightarrow \mathbf{Ens}$ est le foncteur de C dans \mathbf{Ens} défini de manière évidente par

$$(F \times G)(X) = F(X) \times G(X) \quad \text{et} \quad (F \times G)(f) = (F(f), G(f))$$

pour tout objet X et toute flèche f dans C .

On désigne d'autre part par 1 le foncteur $C \rightarrow \mathbf{Ens}$ tel que $1(X)$ soit l'ensemble 1 réduit à un élément pour tout objet X de C et $1(f)$ soit l'unique application de 1 dans 1 pour toute flèche f dans C . Pour tout foncteur $G : C \rightarrow \mathbf{Ens}$,

- il existe un unique morphisme de foncteurs $G \rightarrow 1$;
- la projection sur le premier (resp. second) facteur est un isomorphisme entre les foncteurs $G \times 1$ (resp. $1 \times G$) et G .

Proposition 1.1.1 — Soit C une catégorie. Il revient au même de se donner

- (i) un foncteur $G : C \rightarrow \mathbf{Gr}$;
- (ii) un foncteur $\tilde{G} : C \rightarrow \mathbf{Ens}$ et des morphismes de foncteurs

$$m : \tilde{G} \times \tilde{G} \rightarrow \tilde{G}, \quad e : 1 \rightarrow \tilde{G}, \quad \text{inv} : \tilde{G} \rightarrow \tilde{G}$$

vérifiant les axiomes suivants :

(Ass) le diagramme

$$\begin{array}{ccc} (\tilde{G} \times \tilde{G}) \times \tilde{G} & \xrightarrow{m \times 1_{\tilde{G}}} & \tilde{G} \times \tilde{G} \\ \parallel & & \searrow m \\ \tilde{G} \times (\tilde{G} \times \tilde{G}) & \xrightarrow{1_{\tilde{G}} \times m} & \tilde{G} \times \tilde{G} \\ & & \nearrow m \\ & & \tilde{G} \end{array}$$

est commutatif

(Uni) les diagrammes

$$\begin{array}{ccc} 1 \times \tilde{G} & \xrightarrow{e \times 1_{\tilde{G}}} & \tilde{G} \times \tilde{G} \\ \parallel & \searrow & \downarrow m \\ & & \tilde{G} \end{array} \quad \text{et} \quad \begin{array}{ccc} \tilde{G} \times 1 & \xrightarrow{1_{\tilde{G}} \times e} & \tilde{G} \times \tilde{G} \\ \parallel & \searrow & \downarrow m \\ & & \tilde{G} \end{array}$$

sont commutatifs

(Inv) le diagramme

$$\begin{array}{ccc} \tilde{G} & \xrightarrow{(1_{\tilde{G}}, \text{inv})} & \tilde{G} \times \tilde{G} \\ \downarrow & & \downarrow m \\ 1 & \xrightarrow{e} & \tilde{G} \end{array}$$

est commutatif.

Démonstration. Cette proposition est complètement triviale compte-tenu du fait qu'un groupe G (resp. un homomorphisme de groupes $f : G \rightarrow H$) est précisément la donnée d'un ensemble \tilde{G} et d'applications $m : \tilde{G} \times \tilde{G} \rightarrow \tilde{G}$, $e : 1 \rightarrow \tilde{G}$ et $\text{inv} : \tilde{G} \rightarrow \tilde{G}$ de telle sorte que m définisse une loi interne associative d'élément neutre l'image de e et pour laquelle inv associe à chaque élément de \tilde{G} un

inverse. Ces axiomes usuels sont équivalents à la commutativité des quatre diagrammes

$$\begin{array}{ccc}
 (\tilde{G} \times \tilde{G}) \times \tilde{G} & \xrightarrow{m \times 1_{\tilde{G}}} & \tilde{G} \times \tilde{G} \\
 \parallel & & \searrow m \\
 \tilde{G} \times (\tilde{G} \times \tilde{G}) & \xrightarrow{1_{\tilde{G}} \times m} & \tilde{G} \times \tilde{G} \\
 & & \nearrow m \\
 & & \tilde{G}
 \end{array}
 \qquad
 \begin{array}{ccc}
 \tilde{G} & \xrightarrow{(1_{\tilde{G}}, \text{inv})} & \tilde{G} \times \tilde{G} \\
 \downarrow & & \downarrow m \\
 1 & \xrightarrow{e} & \tilde{G}
 \end{array}$$

$$\begin{array}{ccc}
 1 \times \tilde{G} & \xrightarrow{e \times 1_{\tilde{G}}} & \tilde{G} \times \tilde{G} \\
 \cong \searrow & & \downarrow m \\
 & & \tilde{G}
 \end{array}
 \qquad
 \begin{array}{ccc}
 \tilde{G} \times 1 & \xrightarrow{1_{\tilde{G}} \times e} & \tilde{G} \times \tilde{G} \\
 \cong \searrow & & \downarrow m \\
 & & \tilde{G}
 \end{array}$$

dans la catégorie **Ens** (resp. d'une application \tilde{f} de \tilde{G} dans \tilde{H} telle que les trois diagrammes

$$\begin{array}{ccc}
 \tilde{G} \times \tilde{G} & \xrightarrow{m} & \tilde{G} \\
 \tilde{f} \times \tilde{f} \downarrow & & \downarrow \tilde{f} \\
 \tilde{H} \times \tilde{H} & \xrightarrow{m'} & \tilde{H}
 \end{array}
 \qquad
 \begin{array}{ccc}
 1 & \xrightarrow{e} & \tilde{G} \\
 \searrow e' & & \downarrow \tilde{f} \\
 & & \tilde{H}
 \end{array}
 \qquad
 \begin{array}{ccc}
 \tilde{G} & \xrightarrow{\text{inv}} & \tilde{G} \\
 \tilde{f} \downarrow & & \downarrow \tilde{f} \\
 \tilde{H} & \xrightarrow{\text{inv}'} & \tilde{H}
 \end{array}$$

dans **Ens** soient commutatifs, où m' , e' et inv' désignent respectivement la multiplication, l'élément neutre et l'inversion du groupe \tilde{H}).

Ayant remarqué cela, on établit sans difficulté les assertions suivantes.

- Partant d'un foncteur G de \mathbf{C} dans **Gr**, on définit \tilde{G} comme le foncteur de \mathbf{C} dans **Ens** obtenu en composant G par le foncteur d'oubli $\mathbf{Gr} \rightarrow \mathbf{Ens}$; en clair, pour tout objet X et toute flèche f dans \mathbf{C} , $\tilde{G}(X)$ est l'ensemble sous-jacent au groupe $G(X)$ et $\tilde{G}(f)$ est l'application sous-jacente à l'homomorphisme de groupes $G(f)$. Pour tout objet X de \mathbf{C} , la multiplication (resp. l'élément neutre; resp. l'inversion) du groupe $G(X)$ définit une application $m_X : \tilde{G}(X) \times \tilde{G}(X) \rightarrow \tilde{G}(X)$ (resp. $e_X : 1(X) \rightarrow \tilde{G}(X)$; resp. $\text{inv}_X : \tilde{G}(X) \rightarrow \tilde{G}(X)$). Lorsque X varie, ces applications constituent des morphismes de foncteurs satisfaisant aux axiomes (Ass), (Uni) et (Inv).
- Partant réciproquement d'un foncteur \tilde{G} de \mathbf{C} dans **Ens** et de morphismes de foncteurs m , e et inv satisfaisant aux axiomes (Ass), (Uni) et (Inv), le quadruplet $G(X) = (\tilde{G}(X), m_X, e_X, \text{inv}_X)$ est un groupe pour tout objet X de \mathbf{C} et l'application $\tilde{G}(f)$ définit un homomorphisme de groupes $G(f)$ pour toute flèche f dans \mathbf{C} . Les correspondances $X \mapsto G(X)$ et $f \mapsto G(f)$ définissent un foncteur de \mathbf{C} dans **Gr**.

□

Si G et H sont deux foncteurs de \mathbf{C} dans **Gr** correspondant à des foncteurs \tilde{G} et \tilde{H} de \mathbf{C} dans **Ens** équipés de morphismes de foncteurs (m_G, e_G, inv_G) et (m_H, e_H, inv_H) qui satisfaisent aux axiomes (Ass), (Uni) et (Inv), il revient au même de se donner

- (i) un morphisme de foncteurs $\varphi : G \rightarrow H$;

(ii) un morphisme de foncteurs $\tilde{\varphi} : \tilde{G} \rightarrow \tilde{H}$ tel que les trois diagrammes

$$\begin{array}{ccc} \tilde{G} \times \tilde{G} & \xrightarrow{m_G} & \tilde{G} \\ \tilde{\varphi} \times \tilde{\varphi} \downarrow & & \downarrow \tilde{\varphi} \\ \tilde{H} \times \tilde{H} & \xrightarrow{m_H} & \tilde{H} \end{array} \quad \begin{array}{ccc} 1 & \xrightarrow{e_G} & \tilde{G} \\ & \searrow e_H & \downarrow \tilde{\varphi} \\ & & \tilde{H} \end{array} \quad \begin{array}{ccc} \tilde{G} & \xrightarrow{\text{inv}_G} & \tilde{G} \\ \tilde{\varphi} \downarrow & & \downarrow \tilde{\varphi} \\ \tilde{H} & \xrightarrow{\text{inv}_H} & \tilde{H} \end{array}$$

soient commutatifs.

En guise d'exercice, on démontrera que le troisième diagramme est automatiquement commutatif si les deux premiers le sont.

Terminologie — Étant donnée une catégorie C , on parlera de *foncteur en ensembles* (resp. *en groupes*) sur C pour désigner un foncteur de C dans **Ens** (resp. dans **Gr**). Étant donné un foncteur en groupes G sur C , le foncteur en ensembles *associé* à G sera simplement le foncteur \tilde{G} obtenu en composant G par le foncteur oubli $\mathbf{Gr} \rightarrow \mathbf{Ens}$. Si cela ne prête pas à confusion, on emploiera la même notation pour un foncteur en groupes et le foncteur en ensembles associé.

1.2. Foncteurs représentables

(1.2.1) À tout objet X d'une catégorie C est associé un foncteur $h_X : C \rightarrow \mathbf{Ens}$:

– pour tout objet Y de C , $h_X(Y)$ est l'ensemble $\text{Hom}_C(X, Y)$ des flèches issues de X dans C ;

– pour toute flèche $Y \xrightarrow{f} Z$ de C , $h_X(f)$ est l'application $h_X(Y) \rightarrow h_X(Z)$, $g \mapsto f \circ g$.

On a clairement $h_{u \circ v} = h_v \circ h_u$ pour toutes flèches composables u et v dans C . Enfin, pour tout objet X de C , h_{1_X} est la transformation identique du foncteur h_X .

À toute flèche $X \xrightarrow{u} X'$ dans C correspond un morphisme de foncteurs $h_u : h_{X'} \rightarrow h_X$: pour tout objet Y de C , h_u est l'application

$$h_{X'}(Y) \rightarrow h_X(Y), f \mapsto f \circ u.$$

Le théorème suivant est fondamental.

Théorème 1.2.1 (Lemme de Yoneda) — Soit X un objet de C et soit F un foncteur $C \rightarrow \mathbf{Ens}$. La correspondance

$$\left\{ \begin{array}{l} \text{morphisms de foncteurs} \\ \varphi : h_X \rightarrow F \end{array} \right\} \longrightarrow F(X), \quad \varphi \mapsto \varphi_X(1_X)$$

est une bijection.

Démonstration. Soit $\varphi : h_X \rightarrow F$ un morphisme de foncteurs. Pour tout objet Y de C et toute flèche $f \in h_X(Y)$, on dispose d'un diagramme commutatif

$$\begin{array}{ccc} h_X(X) & \xrightarrow{\varphi_X} & F(X) \\ h_X(f) \downarrow & & \downarrow F(f) \\ h_X(Y) & \xrightarrow{\varphi_Y} & F(Y) \end{array}$$

Comme f est l'image de 1_X par l'application $h_X(f)$, l'identité

$$\begin{aligned} \varphi_Y(f) &= (\varphi_Y \circ h_X(f))(1_X) \\ &= (F(f) \circ \varphi_X)(1_X) \\ &= F(f)(\varphi_X(1_X)) \end{aligned}$$

s'en déduit immédiatement et on constate que la transformation naturelle φ est entièrement déterminée par la connaissance de l'élément $\varphi_X(1_X)$ de $F(X)$.

Supposons réciproquement que l'on dispose d'un élément α de $F(X)$. Pour tout objet Y de C , on désigne par φ_Y l'application de $h_X(Y) = \text{Hom}_C(X, Y)$ dans $F(Y)$ définie par $\varphi_Y(f) = F(f)(\alpha)$. Pour établir que la collection de ces applications définit une transformation naturelle entre les foncteurs h_X et F , il faut vérifier que, pour toute flèche $Y \xrightarrow{g} Z$ dans C , le diagramme

$$\begin{array}{ccc} h_X(Y) & \xrightarrow{\varphi_Y} & F(Y) \\ h_X(g) \downarrow & & \downarrow F(g) \\ h_X(Z) & \xrightarrow{\varphi_Z} & F(Z) \end{array}$$

est commutatif. C'est immédiat : quelle que soit la flèche $u \in h_X(Y)$,

$$\begin{aligned} (\varphi_Z \circ h_X(g))(h) &= \varphi_Z(g \circ h) \\ &= F(g \circ h)(\alpha) \\ &= (F(g) \circ F(h))(\alpha) \\ &= F(g)(F(h)(\alpha)) \\ &= F(g)(\varphi_Y(h)). \end{aligned}$$

□

On dit qu'un foncteur $F : C \rightarrow \mathbf{Ens}$ est *représentable* s'il existe un objet X de C et un isomorphisme de foncteurs $\varphi : h_X \xrightarrow{\sim} F$, auquel cas le couple (X, φ) est un *représentant* de F . D'après le lemme de Yoneda, le morphisme de foncteurs φ correspond à un élément α de $F(X)$ uniquement déterminé et on dit également que le couple (X, α) est un représentant de F .

Corollaire 1.2.2 — Pour tous objets X et Y d'une catégorie C , la correspondance

$$\text{Hom}_C(Y, X) \longrightarrow \left\{ \begin{array}{l} \text{morphismes de foncteurs} \\ \varphi : h_X \rightarrow h_Y \end{array} \right\}, \quad u \mapsto h_u$$

est une bijection préservant les isomorphismes. La bijection réciproque fait correspondre à un morphisme de foncteurs φ la flèche $\varphi_X(1_X)$.

Démonstration — En vertu du lemme de Yoneda, la correspondance $\varphi \mapsto \varphi_X(1_X)$ établit une bijection entre l'ensemble des morphismes de foncteurs $\varphi : h_X \rightarrow h_Y$ et l'ensemble $h_Y(X) = \text{Hom}_C(Y, X)$ des flèches $Y \xrightarrow{u} X$ dans C . Les arguments donnés au cours de la démonstration précédente montrent que la correspondance réciproque associe à une flèche $u \in h_Y(X)$ le morphisme de foncteurs $\varphi : h_X \rightarrow h_Y$ défini par la condition suivante : pour tout objet Z de C , φ_Z est l'application

$$h_X(Z) \rightarrow h_Y(Z), \quad f \mapsto f \circ u,$$

c'est-à-dire $\varphi = h_u$.

Il reste à vérifier qu'une flèche $Y \xrightarrow{u} X$ dans C est un isomorphisme si et seulement si h_u est un isomorphisme de foncteurs.

- Si u est un isomorphisme, alors $h_u \circ h_{u^{-1}} = h_{u^{-1} \circ u} = h_{1_Y} = 1_{h_Y}$ et $h_{u^{-1}} \circ h_u = h_{u \circ u^{-1}} = h_{1_X} = 1_{h_X}$, donc h_u est un isomorphisme de foncteurs.
- Si réciproquement h_u est un isomorphisme de foncteurs, l'isomorphisme inverse $h_u^{-1} : h_Y \xrightarrow{\sim} h_X$ est de la forme h_v pour une certaine flèche $v \in \text{Hom}_C(X, Y)$ et alors

$$h_{u \circ v} = h_v \circ h_u = h_{1_X}, \quad h_{v \circ u} = h_u \circ h_v = h_{1_Y},$$

donc $u \circ v = 1_X$, $v \circ u = 1_Y$ et u est un isomorphisme.

□

Corollaire 1.2.3 — Soit $F : C \rightarrow \mathbf{Ens}$ un foncteur représentable. Si (X, φ) et (X', φ') sont deux représentants de F , il existe un unique isomorphisme $u : X' \xrightarrow{\sim} X$ tel que le diagramme

$$\begin{array}{ccc} h_X & \xrightarrow{\varphi} & F \\ & \searrow h_u & \uparrow \varphi' \\ & & h_{X'} \end{array}$$

soit commutatif.

Démonstration. Il suffit d'appliquer le corollaire précédent à l'isomorphisme de foncteurs $\varphi'^{-1} \circ \varphi$. □

Ainsi, si un foncteur $F : C \rightarrow \mathbf{Ens}$ est représentable, tout représentant (X, φ_X) de F est *unique* à un isomorphisme *unique* près.

Remarques et exemples — Les considérations précédentes ont de multiples implications ; explicitons-en quelques une.

1. La notion de foncteur représentable peut se comprendre en termes de *problème universel*. Étant donné un foncteur F d'une catégorie C dans la catégorie des ensembles, on se demande s'il existe un objet X de C et un élément α de $F(X)$ tels que le couple (X, α) soit universel, c'est-à-dire satisfasse à la condition suivante : pour tout couple (Y, β) constitué d'un objet Y de C et d'un élément β de $F(Y)$, il existe une unique flèche $f : X \rightarrow Y$ dans C telle que $\beta = F(f)(\alpha)$. Dire que le foncteur F est représentable, c'est exactement dire que ce problème admet une solution ; dire qu'un couple (X, α) représente le foncteur F , c'est exactement dire qu'il est une solution du problème considéré. Enfin, le corollaire 1.2.3 affirme que, si (X, α) et (X', α') sont deux solutions de ce problème, alors il existe un isomorphisme $f : X \xrightarrow{\sim} X'$ uniquement déterminé tel que $\alpha' = F(f)(\alpha)$.

Sous la forme que l'on vient de lui donner, la notion de foncteur représentable est familière.

(i) Prenons pour C la catégorie des ensembles. Si E est un ensemble muni d'une relation d'équivalence \sim , on peut considérer le foncteur F de \mathbf{Ens} dans \mathbf{Ens} qui associe à tout ensemble E' l'ensemble des applications $f : E \rightarrow E'$ telles que $f(x) = f(y)$ si $x \sim y$. Ce foncteur est représentable par l'ensemble quotient E/\sim et la projection canonique p de E dans E/\sim ; c'est la « propriété universelle du quotient ».

(ii) Prenons pour C la catégorie $\mathbf{Mod}(A)$ des modules (à gauche) sur un anneau A . Étant donné un A -module M et un sous-module N , le foncteur F de $\mathbf{Mod}(A)$ dans la catégorie des ensembles, qui à un A -module P associe l'ensemble des applications A -linéaires $u : M \rightarrow P$ s'annulant sur N , est représentable par le A -module quotient M/N et la projection canonique de M sur M/N .

(iii) Prenons pour C la catégorie \mathbf{Top} des espaces topologiques. Le foncteur « composantes connexes » $\pi_0 : \mathbf{Top} \rightarrow \mathbf{Ens}$ n'est certainement *pas* représentable. En effet, s'il existait un espace topologique X et une composante connexe $C \in \pi_0(X)$ de X tels que l'application

$$\mathrm{Hom}_{\mathbf{Top}}(X, Y) \rightarrow \pi_0(Y), f \mapsto f(C)$$

soit une bijection pour tout espace topologique Y , il existerait alors en particulier une unique application continue de X dans \mathbb{R} puisque \mathbb{R} est connexe, ce qui impliquerait $X = \emptyset$ (si $X \neq \emptyset$, les fonctions réelles constantes fournissent une infinité d'applications continues de X dans \mathbb{R}). Comme l'ensemble $\mathrm{Hom}_{\mathbf{Top}}(\emptyset, Y)$ est réduit à un élément pour tout espace topologique Y , on en déduirait alors que $\pi_0(Y)$ est *toujours* un singleton, ce qui est absurde !

(iv) Poursuivons l'étude de l'exemple précédent. Étant donné deux espaces topologiques X et Y , on désigne par $[X, Y]$ l'ensemble des *classes d'homotopie* d'applications continues de X dans Y , c'est-à-dire le quotient de $\mathrm{Hom}_{\mathbf{Top}}(X, Y)$ par la relation d'équivalence « $f \sim g$ si et seulement si f et g sont homotopes ». On vérifie sans difficulté que la composition est compatible à cette relation

d'équivalence, ce qui permet de définir la catégorie **Hot** des *espaces topologiques à homotopie près* : les objets sont les espaces topologiques, les flèches sont les classes d'homotopie d'applications continues et la composition est induite par la composition usuelle. Le foncteur « composantes connexes par arcs » $\pi'_0 : \mathbf{Top} \rightarrow \mathbf{Ens}$ n'est pas représentable (même argument que pour π_0) mais le foncteur $\pi'_0 : \mathbf{Hot} \rightarrow \mathbf{Ens}$ qu'il induit l'est, car les composantes connexes par arcs de Y sont naturellement en bijection avec les classes d'homotopie d'applications continues du singleton 1 dans Y :

$$[1, Y] \cong \pi'_0(Y).$$

2. Interpréter une construction usuelle en termes de représentation d'un foncteur permet de la transférer dans un autre contexte. Un exemple standard est la *somme* (ou *union disjointe*) des ensembles. Étant donnés deux ensembles X et Y , la somme $X \sqcup Y$ de X et Y possède la propriété universelle suivante : il revient au même de se donner une application f de $X \sqcup Y$ dans un ensemble Z ou de se donner des applications f_X et f_Y de X et Y dans Z respectivement, f_X (resp. f_Y) étant la restriction de f au sous-ensemble X (resp. Y) de $X \sqcup Y$. En d'autres termes, le triplet $(X \sqcup Y, i_X, i_Y)$ constitué de l'ensemble $X \sqcup Y$ et des inclusions canoniques de X et Y dans $X \sqcup Y$ représente le foncteur

$$\mathbf{Ens} \rightarrow \mathbf{Ens}, Z \mapsto \mathrm{Hom}_{\mathbf{Ens}}(X, Z) \times \mathrm{Hom}_{\mathbf{Ens}}(Y, Z).$$

Quels que soient alors la catégorie C et les objets X et Y de C , cela fait sens de se demander si le foncteur

$$C \rightarrow \mathbf{Ens}, Z \mapsto \mathrm{Hom}_C(X, Z) \times \mathrm{Hom}_C(Y, Z)$$

est représentable ; si oui, on désigne par $X \sqcup Y$ un objet le représentant et on dit que $X \sqcup Y$ est le *coproduit* de X et Y . La réponse est toujours positive dans **Top** : le coproduit de deux espaces topologiques X et Y est la somme des ensembles sous-jacents muni de la topologie la plus fine rendant continues les injections canoniques $X, Y \hookrightarrow X \sqcup Y$. La réponse est également positive dans **Ab** : le coproduit de deux groupes abéliens X et Y n'est autre que leur somme directe $X \oplus Y$, et on voit déjà sur cet exemple élémentaire que l'ensemble sous-jacent au coproduit de deux groupes abéliens n'est *pas* le coproduit des ensembles sous-jacents, ce qui montre l'intérêt de la reformulation en termes fonctoriels. On dispose également d'un coproduit dans la catégorie **Gr** des groupes (c'est le *produit libre*) et dans la catégorie des anneaux commutatifs (c'est le *produit tensoriel*, cf. appendice). Il faut toutefois se garder de croire que l'existence d'un coproduit est toujours assurée : par exemple, dans la catégorie C associée à un ensemble partiellement ordonné (E, \leq) (1.1.1, exemple 2), l'existence du coproduit de deux objets x et y équivaut à celle de la borne inférieure de x et y dans E .

On peut aborder de même l'étude du *produit cartésien* $X \times Y$ de deux ensembles X et Y , représentant le foncteur

$$\mathbf{Ens}^{\mathrm{op}} \rightarrow \mathbf{Ens}, Z \mapsto \mathrm{Hom}_{\mathbf{Ens}}(X, Z) \times \mathrm{Hom}_{\mathbf{Ens}}(Y, Z),$$

et essayer de l'étendre à d'autres catégories (exercice !).

3. En vertu du corollaire 1.2.2, on ne perd aucune information en remplaçant un objet X d'une catégorie C par le foncteur h_C . Contrairement aux apparences, ce point de vue s'avère parfois simplificateur en ce qu'il permet de construire une flèche $u : X \longrightarrow Y$ dans une catégorie C *a priori* compliquée en définissant seulement des applications naturelles entre les ensembles variables $h_Y(\cdot)$ et $h_X(\cdot)$. On en verra un exemple explicite dans ce cours (où C sera la catégorie des *bigèbres* de type fini sur un corps k , cf. 1.4).

2. GROUPES ALGÈBRIQUES AFFINES

2.1. Définition et exemples

On fixe dans tout ce paragraphe un corps k et on désigne par \mathbf{Alg}_k la catégorie des k -algèbres (cf. appendice, 1.1).

(2.1.1) Commençons par introduire les principaux objets que nous considérerons dans ce cours.

Définition 2.1.1 — Soit k un corps.

- (i) Un groupe algébrique affine sur k est un foncteur en groupes $G : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ tel que le foncteur en ensembles associé $\mathbf{Alg}_k \rightarrow \mathbf{Ens}$ soit représentable par une k -algèbre de type fini.
- (ii) Si G et H sont deux groupes algébriques affines sur k , un homomorphisme $f : G \rightarrow H$ est un morphisme de foncteurs en groupes.

Les groupes algébriques affines sur k et leurs homomorphismes constituent les objets et les flèches d'une catégorie, notée $\mathbf{k} - \mathbf{Gr}$.

Explicitons cette définition. Un foncteur $G : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ est un groupe algébrique affine sur k s'il existe une k -algèbre de type fini A et, pour toute k -algèbre R , une bijection

$$\varphi_R : \mathrm{Hom}_{\mathbf{Alg}_k}(A, R) \simeq G(R)$$

dépendant « naturellement » de R , c'est-à-dire telle que, pour tout homomorphisme de k -algèbres $f : R \rightarrow R'$, le diagramme

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{Alg}_k}(A, R) & \xrightarrow{\varphi_R} & G(R) \\ f \circ \cdot \downarrow & & \downarrow G(f) \\ \mathrm{Hom}_{\mathbf{Alg}_k}(A, R') & \xrightarrow{\varphi_{R'}} & G(R') \end{array}$$

soit commutatif.

Dire qu'une k -algèbre A est de type fini, c'est dire qu'elle est isomorphe au quotient d'un anneau de polynômes $k[T_1, \dots, T_n]$ en un nombre fini de variables par un idéal \mathfrak{J} :

$$\lambda : k[T_1, \dots, T_n] / \mathfrak{J} \simeq A.$$

En utilisant la propriété universelle des anneaux de polynômes (cf. appendice, 1.1), on peut donner une description plus concrète du foncteur en ensembles $h_A = \mathrm{Hom}_{\mathbf{Alg}_k}(A, \cdot)$ sur la catégorie \mathbf{Alg}_k . De manière précise, la correspondance $u \mapsto \lambda \circ u$ induit un isomorphisme entre h_A et le foncteur

$$V_{\mathfrak{J}} : \mathbf{Alg}_k \rightarrow \mathbf{Ens},$$

associant à toute k -algèbre R l'ensemble

$$V_{\mathfrak{J}}(R) = \{(r_1, \dots, r_n) \in R^n \mid P(r_1, \dots, r_n) = 0 \text{ pour tout } P \in \mathfrak{J}\}$$

des zéros de l'idéal \mathfrak{J} dans R^n et à tout homomorphisme de k -algèbres $f : R \rightarrow R'$ l'application

$$V_{\mathfrak{J}}(f) : V_{\mathfrak{J}}(R) \rightarrow V_{\mathfrak{J}}(R'), \quad (r_1, \dots, r_n) \mapsto (f(r_1), \dots, f(r_n)).$$

On aboutit ainsi à une reformulation simple de la définition initiale :

un groupe algébrique affine sur k , c'est un foncteur $G : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ tel que, pour toute k -algèbre R , l'ensemble sous-jacent au groupe $G(R)$ puisse s'identifier de manière « naturelle » à un sous-ensemble de R^n défini par des équations polynomiales à coefficients dans k .

(Ici, « naturelle » signifie « de façon compatible aux homomorphismes de k -algèbres »).

La terminologie adoptée s'éclaire du même coup ; par la suite, nous la simplifierons en parlant de *groupe algébrique sur k* , voire de *k -groupe*, plutôt que de groupe algébrique affine sur k .

Exemple paradigmatique — 1. Le foncteur $\mathrm{GL}_n : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$, associant

- à toute k -algèbre R , le groupe des matrices carrées inversibles de taille n à coefficients dans R ,
- à tout homomorphisme de k -algèbres $f : R \rightarrow R'$, l'homomorphisme de groupes induit par l'homomorphisme de monoïdes $M_n(R) \rightarrow M_n(R')$, $(x_{ij}) \mapsto (f(x_{ij}))$,

est un groupe algébrique sur k .

En effet, quelle que soit la k -algèbre R , se donner une matrice M dans $M_n(R)$ revient à se donner n^2 éléments m_{ij} de R , c'est-à-dire un homomorphisme de la k -algèbre de polynômes $k[(X_{ij})_{1 \leq i, j \leq n}]$ dans R . Pour que M soit inversible, il faut et il suffit que son déterminant soit inversible dans R c'est-à-dire qu'il existe $t \in R$ avec $t \det(M) - 1 = 0$. La formule bien connue

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) m_{1\sigma(1)} \cdots m_{n\sigma(n)}$$

montre que le déterminant de la matrice M est un polynôme en les m_{ij} , à coefficients dans \mathbb{Z} , donc n'importe quel corps k . On a ainsi décrit une bijection naturelle

$$\mathrm{GL}_n(R) \simeq \mathrm{Hom}_{\mathbf{Alg}_k} (k[(X_{ij})_{1 \leq i, j \leq n}, T]/(T \det(X_{ij}) - 1), R),$$

où l'on a posé

$$\det(X_{ij}) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) X_{1\sigma(1)} \cdots X_{n\sigma(n)}.$$

2. Le morphisme de foncteurs en groupes $\det : \mathrm{GL}_n \rightarrow \mathrm{GL}_1$, défini par la collection des homomorphismes de groupes $\det_R : \mathrm{GL}_n(R) \rightarrow \mathrm{GL}_1(R)$ pour toute k -algèbre R , est un homomorphisme de groupes algébriques.

Définition 2.1.2 — Soit G un groupe algébrique sur k . On appelle anneau de coordonnées de G la donnée d'un k -algèbre de type fini A et d'un isomorphisme de foncteurs en ensembles $\varphi : h_A \simeq G$.

En vertu du lemme de Yoneda, deux anneaux de coordonnées (A, φ) et (A', φ') de G sont canoniquement isomorphes : il existe un unique isomorphisme de k -algèbres $u : A' \rightarrow A$ tel que le diagramme

$$\begin{array}{ccc} h_A & \xrightarrow{h_u} & h_{A'} \\ & \searrow \varphi & \swarrow \varphi' \\ & G & \end{array}$$

soit commutatif. Cela permet de parler de l'*anneau de coordonnées* de G , noté $(\mathcal{O}(G), \varphi)$ ou $(k[G], \varphi)$; on omettra le plus souvent de faire figurer l'isomorphisme φ .

(2.1.2) Donnons tout de suite des exemples de groupes algébriques sur un corps k .

(i) Le foncteur $1 : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ associant à toute k -algèbre R le groupe $\{1\}$ réduit à un élément est un groupe algébrique sur k . En effet, pour toute k -algèbre R , il existe un unique homomorphisme de k -algèbres de k dans R (c'est l'homomorphisme structural de R , cf. appendice 1.1) et le foncteur 1 est donc représenté par la k -algèbre k .

(ii) Le foncteur $\mathbb{G}_a : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ associant à toute k -algèbre R le groupe additif sous-jacent $(R, +)$ est un groupe algébrique sur k d'anneau de coordonnées la k -algèbre $k[X]$. C'est le *groupe additif* sur k .

(iii) Le foncteur $\mathbb{G}_m : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ associant à toute k -algèbre R le groupe multiplicatif (R^\times, \cdot) des éléments *inversibles* de R est un groupe algébrique sur k , d'anneau de coordonnées la k -algèbre $k[X, T]/(XT - 1)$. C'est le *groupe multiplicatif* sur k .

(iv) Pour tout entier $n \geq 0$, le foncteur $\mu_n : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ associant à chaque k -algèbre R le groupe multiplicatif $\mu_n(R)$ des racines n -èmes de l'unité dans R est un groupe algébrique sur k , d'anneau de coordonnées $k[X]/(X^n - 1)$. Lorsque $n = 0$, on retrouve le k -groupe 1.

(v) Pour tout entier $n \geq 0$, le foncteur $SL_n : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ associant à chaque k -algèbre R le groupe $SL_n(R)$ des matrices carrées de taille n à coefficients dans R et de déterminant 1 est un groupe algébrique sur k , d'anneau de coordonnées la k -algèbre $k[(X_{ij})_{1 \leq i, j \leq n}]/(\det(X_{ij}) - 1)$. C'est le *groupe spécial linéaire* sur k .

(vi) Pour tout entier $n \geq 0$, le foncteur $D_n : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ associant à chaque k -algèbre R le groupe $D_n(R)$ des matrices diagonales et inversibles de taille n à coefficients dans R est un groupe algébrique sur k , d'anneau de coordonnées la k -algèbre $k[(X_i)_{1 \leq i \leq n}, T]/(X_1 \dots X_n T - 1)$.

(vii) Pour tout entier $n \geq 0$, le foncteur $B_n : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ associant à chaque k -algèbre R le groupe $B_n(R)$ des matrices triangulaires supérieures inversibles de taille n et à coefficients dans R est un groupe algébrique sur k , d'anneau de coordonnées la k -algèbre $k[(X_{ij})_{1 \leq i < j \leq n}, T]/(X_{11} \dots X_{nn} T - 1)$.

(viii) Pour tout entier $n \geq 0$, le foncteur $U_n : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ associant à chaque k -algèbre R le groupe $U_n(R)$ des matrices triangulaires supérieures à diagonale unitaire de taille n et à coefficients dans R est un groupe algébrique sur k , d'anneau de coordonnées la k -algèbre $k[(X_{ij})_{1 \leq i < j \leq n}]$.

(ix) Pour tout entier $n \geq 0$, le foncteur $O_n : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ associant à chaque k -algèbre R le groupe

$$O_n(R) = \{M \in M_n(R) \mid {}^t M M = I_n\}$$

est un groupe algébrique sur k . En effet, pour toute matrice $M = (m_{ij})$ dans $M_n(R)$, la condition ${}^t M M = I_n$ équivaut aux n^2 identités polynomiales

$$\sum_{1 \leq \ell \leq n} m_{i\ell} m_{j\ell} = \delta_{ij}$$

($1 \leq i, j \leq n$). C'est le *groupe orthogonal* sur k .

(x) Pour tout entier $n \geq 0$, le foncteur $Sp_{2n} : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ associant à chaque k -algèbre R le groupe

$$Sp_{2n}(R) = \{M \in M_{2n}(R) \mid {}^t M J_n M = J_n\},$$

où $J_n = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}$, est un groupe algébrique sur k (même argument que pour l'exemple précédent). C'est le *groupe symplectique* sur k .

(xi) Supposons que le corps k soit de caractéristique $p > 0$. L'élévation à la puissance p -ème est un automorphisme \mathbb{F}_p -linéaire dans toute k -algèbre R et

$$\alpha_p(R) = \{r \in R \mid r^p = 0\}$$

est donc un sous-groupe du groupe additif $(R, +)$. Le foncteur $\alpha_p : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ ainsi défini est un groupe algébrique sur k , d'anneau de coordonnées la k -algèbre $k[T]/(T^p)$.

2.2. Bigèbres

Nous avons défini un groupe algébrique sur un corps k comme un foncteur en groupes sur la catégorie \mathbf{Alg}_k tel que le foncteur en ensembles associé soit représentable par une k -algèbre de type fini. Nous allons maintenant voir comment traduire sur la k -algèbre A le fait que le foncteur en ensembles h_A qu'elle représente provienne d'un foncteur en groupes.

(2.2.1) Fixons une k -algèbre A . En vertu de la proposition 1.1.1, il revient au même de dire que le foncteur $h_A : \mathbf{Alg}_k \rightarrow \mathbf{Ens}$ est le foncteur en ensembles associé à un foncteur en groupes, ou de dire qu'il existe des morphismes de foncteurs

$$m : h_A \times h_A \rightarrow h_A, \quad e : 1 \rightarrow h_A \quad \text{et} \quad \text{inv} : h_A \rightarrow h_A$$

tels que les quatre diagrammes

$$\begin{array}{ccc}
 (\mathfrak{h}_A \times \mathfrak{h}_A) \times \mathfrak{h}_A & \xrightarrow{m \times 1_{\mathfrak{h}_A}} & \mathfrak{h}_A \times \mathfrak{h}_A \\
 \parallel & & \searrow m \\
 \mathfrak{h}_A \times (\mathfrak{h}_A \times \mathfrak{h}_A) & \xrightarrow{1_{\mathfrak{h}_A} \times m} & \mathfrak{h}_A \times \mathfrak{h}_A \\
 & & \nearrow m \\
 & & \mathfrak{h}_A
 \end{array}
 \qquad
 \begin{array}{ccc}
 \mathfrak{h}_A & \xrightarrow{(1_{\mathfrak{h}_A}, \text{inv})} & \mathfrak{h}_A \times \mathfrak{h}_A \\
 \downarrow & & \downarrow m \\
 1 & \xrightarrow{e} & \mathfrak{h}_A
 \end{array}$$

$$\begin{array}{ccc}
 1 \times \mathfrak{h}_A & \xrightarrow{e \times 1_{\mathfrak{h}_A}} & \mathfrak{h}_A \times \mathfrak{h}_A \\
 \cong \searrow & & \downarrow m \\
 & & \mathfrak{h}_A
 \end{array}
 \qquad
 \begin{array}{ccc}
 \mathfrak{h}_A \times 1 & \xrightarrow{1_{\mathfrak{h}_A} \times e} & \mathfrak{h}_A \times \mathfrak{h}_A \\
 \cong \searrow & & \downarrow m \\
 & & \mathfrak{h}_A
 \end{array}$$

soient commutatifs.

Étant données deux k -algèbres A et B , le foncteur

$$\mathfrak{h}_A \times \mathfrak{h}_B : \mathbf{Alg}_k \rightarrow \mathbf{Ens}, \quad R \mapsto \text{Hom}_{\mathbf{Alg}_k}(A, R) \times \text{Hom}_{\mathbf{Alg}_k}(B, R)$$

est représenté par le *produit tensoriel* $A \otimes_k B$ des k -algèbres A et B (cf. appendice 2.3) :

$$\mathfrak{h}_A \times \mathfrak{h}_B \cong \mathfrak{h}_{A \otimes_k B}.$$

En vertu du lemme de Yoneda, le morphisme de multiplication

$$m : \mathfrak{h}_{A \otimes_k A} \cong \mathfrak{h}_A \times \mathfrak{h}_A \rightarrow \mathfrak{h}_A$$

est de la forme $m = \mathfrak{h}_\Delta$, où

$$\Delta : A \rightarrow A \otimes_k A$$

est un homomorphisme de k -algèbres uniquement déterminé.

De même, comme $1 \simeq \mathfrak{h}_k$, le morphisme $e : 1 \rightarrow \mathfrak{h}_A$ provient d'un homomorphisme de k -algèbres

$$e^* : A \rightarrow k$$

uniquement déterminé. Enfin, il existe un unique homomorphisme de k -algèbres $\iota : A \rightarrow A$ tel que $\text{inv} = \mathfrak{h}_\iota$.

Proposition 2.2.1 — *Pour que le quadruplet $(\mathfrak{h}_A, m, e, \text{inv})$ définisse un foncteur en groupes, il faut et il suffit que les quatre diagrammes*

$$\begin{array}{ccc}
 A \otimes_k A & \xrightarrow{\text{id}_A \otimes \Delta} & A \otimes_k (A \otimes_k A) \\
 \Delta \nearrow & & \parallel \\
 A & & \\
 \Delta \searrow & & \\
 A \otimes_k A & \xrightarrow{\Delta \otimes \text{id}_A} & (A \otimes_k A) \otimes_k A
 \end{array}
 \qquad
 \begin{array}{ccc}
 A & \xrightarrow{\Delta} & A \otimes_k A & \xrightarrow{\text{id}_A \otimes \iota} & A \otimes_k A \\
 e^* \downarrow & & & & \downarrow \text{produit} \\
 k & \xrightarrow{\quad} & & & A
 \end{array}$$

$$\begin{array}{ccc}
 A & \xrightarrow{\Delta} & A \otimes_k A \\
 \parallel & \searrow e^* \otimes \text{id}_A & \\
 k \otimes_k A & &
 \end{array}
 \qquad
 \begin{array}{ccc}
 A & \xrightarrow{\Delta} & A \otimes_k A \\
 \parallel & \searrow \text{id}_A \otimes e^* & \\
 A \otimes_k k & &
 \end{array}$$

soient commutatifs.

Démonstration. En vertu du lemme de Yoneda, deux homomorphismes de k -algèbres $f, g : R \rightarrow R'$ sont égaux si et seulement si les morphismes de foncteurs $h_f, h_g : h_{R'} \rightarrow h_R$ qu'ils définissent sont égaux. Forts de cette observation, il nous suffit de vérifier que les quatre diagrammes considérés correspondent aux quatre diagrammes envisagés auparavant et faisant intervenir h_A . Les vérifications sont immédiates pour ce qui est des premier, troisième et quatrième diagrammes (associativité et élément neutre). Pour le deuxième (inversion), il suffit d'observer que le morphisme de foncteurs $(\text{id}_A, \text{inv}) : h_A \rightarrow h_A \times h_A$ peut également s'écrire sous la forme

$$h_A \xrightarrow{(\text{id}_A, \text{id}_A)} h_A \times h_A \xrightarrow{\text{id}_A \times \text{inv}} h_A \times h_A .$$

Lorsqu'on identifie $h_A \times h_A$ et $h_{A \otimes_k A}$, le morphisme diagonal

$$(\text{id}_A, \text{id}_A) : h_A \rightarrow h_A \times h_A \cong h_{A \otimes_k A}$$

correspond à l'unique homomorphisme de k -algèbres $u : A \otimes_k A \rightarrow A$ tel que $u(a \otimes 1) = u(1 \otimes a) = a$ pour tout $a \in A$; comme $a \otimes a' = (a \otimes 1)(1 \otimes a')$, $u(a \otimes a') = aa'$ est l'homomorphisme *produit*. \square

Supposons maintenant que A et B soient deux k -algèbres telles que les foncteurs h_A et h_B proviennent de foncteurs en groupes, c'est-à-dire qu'ils soient munis de morphismes (m_A, e_A, inv_A) et (m_B, e_B, inv_B) comme précédemment. Pour qu'un morphisme de foncteurs en ensembles $f : h_A \rightarrow h_B$ définisse un morphisme de foncteur en groupes, il faut et il suffit que les trois diagrammes

$$\begin{array}{ccc} h_A \times h_A & \xrightarrow{m_A} & h_A \\ f \times f \downarrow & & \downarrow f \\ h_B \times h_B & \xrightarrow{m_B} & h_B \end{array} \quad \begin{array}{ccc} 1 & \xrightarrow{e_A} & h_A \\ & \searrow e_A & \downarrow f \\ & & h_B \end{array} \quad \begin{array}{ccc} h_A & \xrightarrow{\text{inv}_A} & h_A \\ f \downarrow & & \downarrow f \\ h_B & \xrightarrow{\text{inv}_B} & h_B \end{array}$$

soient commutatifs, le troisième l'étant automatiquement lorsque les deux premiers le sont. En vertu du lemme de Yoneda, il existe un unique homomorphisme de k -algèbres $f^* : B \rightarrow A$ tel que $f = h_{f^*}$. De manière analogue à la proposition 2.2.1, on vérifie que la commutativité des trois diagrammes précédents est équivalente à celle des trois diagrammes suivants :

$$\begin{array}{ccc} A \otimes_k A & \xleftarrow{\Delta_A} & A \\ f^* \otimes f^* \uparrow & & \uparrow f^* \\ B \otimes_k B & \xleftarrow{\Delta_B} & B \end{array} \quad \begin{array}{ccc} & \xleftarrow{e_A^*} & A \\ k & \swarrow e_B^* & \uparrow f^* \\ & & B \end{array} \quad \begin{array}{ccc} A & \xleftarrow{\iota_A} & A \\ f^* \uparrow & & \uparrow f^* \\ B & \xleftarrow{\iota_B} & B \end{array}$$

où les triplets $(\Delta_A, e_A^*, \iota_A)$ et $(\Delta_B, e_B^*, \iota_B)$ sont déduits comme ci-dessus des triplets (m_A, e_A, inv_A) et (m_B, e_B, inv_B) via le lemme de Yoneda.

Définition 2.2.2 — Soit k un corps.

(i) Une k -bigèbre est un quadruplet (A, Δ, e^*, ι) constitué d'une k -algèbre A et d'homomorphismes de k -algèbres $\Delta : A \rightarrow A \otimes_k A$, $e^* : A \rightarrow k$, $\iota : A \rightarrow A$ tels que les quatre diagrammes

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_k A \\ & \searrow \Delta & \downarrow \Delta \\ & & A \otimes_k A \end{array} \quad \begin{array}{ccc} A \otimes_k A & \xrightarrow{\text{id}_A \otimes \Delta} & A \otimes_k (A \otimes_k A) \\ & \parallel & \downarrow \parallel \\ A \otimes_k A & \xrightarrow{\Delta \otimes \text{id}_A} & (A \otimes_k A) \otimes_k A \end{array} \quad \begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_k A \\ e^* \downarrow & & \downarrow \text{produit} \\ k & \xrightarrow{\quad} & A \end{array} \quad \begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_k A \\ & \searrow \Delta & \downarrow \Delta \\ & & A \otimes_k A \end{array} \quad \begin{array}{ccc} A \otimes_k A & \xrightarrow{\text{id}_A \otimes \iota} & A \otimes_k A \\ & \parallel & \downarrow \parallel \\ A \otimes_k A & \xrightarrow{\text{id}_A \otimes \iota} & A \otimes_k A \end{array}$$

$$\begin{array}{ccc}
A & \xrightarrow{\Delta} & A \otimes_k A \\
\parallel & \swarrow e^* \otimes \text{id}_A & \\
k \otimes_k A & &
\end{array}
\quad
\begin{array}{ccc}
A & \xrightarrow{\Delta} & A \otimes_k A \\
\parallel & \swarrow \text{id}_A \otimes e^* & \\
A \otimes_k k & &
\end{array}$$

soient commutatifs.

(ii) Un morphisme d'une k -bigèbre $(A, \Delta_A, e_A^*, \iota_A)$ dans une k -bigèbre $(B, \Delta_B, e_B^*, \iota_B)$ est un homomorphisme de k -algèbres $\varphi : A \rightarrow B$ tel que les trois diagrammes

$$\begin{array}{ccc}
A \otimes_k A & \xleftarrow{\Delta_A} & A \\
\varphi \otimes \varphi \downarrow & & \downarrow \varphi \\
B \otimes_k B & \xleftarrow{\Delta_B} & B
\end{array}
\quad
\begin{array}{ccc}
k & \xleftarrow{e_A^*} & A \\
e_B^* \swarrow & & \downarrow \varphi \\
B & &
\end{array}
\quad
\begin{array}{ccc}
A & \xleftarrow{\iota_A} & A \\
\varphi \downarrow & & \downarrow \varphi \\
B & \xleftarrow{\iota_B} & B
\end{array}$$

soient commutatifs.

On dit qu'une k -bigèbre $(A, \Delta_A, e_A^*, \iota_A)$ est de *type fini* si A est une k -algèbre de type fini. Les k -bigèbres et leurs morphismes forment naturellement une catégorie. La discussion qui précède établit précisément que la catégorie des groupes algébriques sur k et celle des k -bigèbres de type fini sont *antiéquivalentes* :

- tout groupe algébrique sur k est isomorphe au groupe algébrique h_A défini par une k -bigèbre de type fini $(A, \Delta_A, e_A^*, \iota_A)$;
- étant données deux k -bigèbres de type fini $(A, \Delta_A, e_A^*, \iota_A)$ et $(B, \Delta_B, e_B^*, \iota_B)$, la correspondance

$$\left\{ \begin{array}{l} \text{morphisms de } k\text{-bigèbres} \\ (A, \Delta_A, e_A^*, \iota_A) \xrightarrow{\varphi} (B, \Delta_B, e_B^*, \iota_B) \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \text{homomorphismes de } k\text{-groupes} \\ h_B \xrightarrow{h_\varphi} h_B \end{array} \right\}$$

est une bijection.

(2.2.2) Exemple : la k -bigèbre du groupe linéaire GL_n .

On sait que GL_n est représenté par la k -algèbre $A = k[(X_{ij})_{1 \leq i, j \leq n}, T] / (T \det(X_{ij}) - 1)$: pour toute k -algèbre R ,

$$\begin{array}{ccc}
\text{Hom}_{\text{Alg}_k}(A, R) & \xrightarrow{\sim} & GL_n(R) \\
u & \mapsto & (u(X_{ij})).
\end{array}$$

La k -algèbre $A \otimes_k A$ s'identifie canoniquement au quotient de la k -algèbre de polynômes $k[(X_{ij} \otimes 1)_{1 \leq i, j \leq n}, (1 \otimes X_{ij})_{1 \leq i, j \leq n}, T \otimes 1, 1 \otimes T]$ (en $2n^2 + 2$ variables) par l'idéal $((T \otimes 1) \det((X_{ij} \otimes 1) - 1), (1 \otimes T) \det(1 \otimes X_{ij}) - 1)$ (cf. appendice, 2.4, exercices 5 et 6). En utilisant la bijection

$$\begin{array}{ccc}
\text{Hom}_{\text{Alg}_k}(A \otimes_k A, R) & \xrightarrow{\sim} & GL_n(R) \times GL_n(R) \\
w & \mapsto & ((w(X_{ij} \otimes 1)), (w(1 \otimes X_{ij}))),
\end{array}$$

on dispose d'un diagramme commutatif

$$\begin{array}{ccc}
GL_n(R) \times GL_n(R) & \xrightarrow{\text{mult}} & GL_n(R) \\
\wr \uparrow & & \uparrow \wr \\
\text{Hom}_{\text{Alg}_k}(A \otimes_k A, R) & \longrightarrow & \text{Hom}_{\text{Alg}_k}(A, R)
\end{array}$$

dans lequel les flèches verticales sont les bijections que l'on vient de décrire et la flèche horizontale inférieure est l'application $w \mapsto w \circ \Delta$, Δ étant la comultiplication de A qu'il s'agit d'expliciter. La

commutativité de ce diagramme équivaut à l'identité matricielle

$$((w \circ \Delta)(X_{ij})) = (w(X_{ij} \otimes 1))(w(1 \otimes X_{ij}))$$

dans $GL_n(\mathbb{R})$ pour tout homomorphisme de k -algèbres $w : A \otimes_k A \rightarrow \mathbb{R}$. En calculant le produit figurant dans le membre de droite, nous obtenons

$$\begin{aligned} (w \circ \Delta)(X_{ij}) &= \sum_{\ell=1}^n w(X_{i\ell} \otimes 1)w(1 \otimes X_{\ell j}) \\ &= \sum_{\ell=1}^n w(X_{i\ell} \otimes X_{\ell j}) \\ &= w\left(\sum_{\ell=1}^n X_{i\ell}X_{\ell j}\right) \end{aligned}$$

et donc finalement

$$\Delta(X_{ij}) = \sum_{\ell=1}^n X_{i\ell}X_{\ell j}$$

puisque \mathbb{R} et w sont arbitraires (choisir par exemple $\mathbb{R} = A \otimes_k A$ et $w = \text{id}_{A \otimes_k A}$). Comme

$$u(\mathbb{T}) = \det(u(X_{ij}))^{-1}$$

pour tout $u \in \text{Hom}_{\text{Alg}_k}(A, \mathbb{R})$,

$$\begin{aligned} (w \circ \Delta)(\mathbb{T}) &= \det((w \circ \Delta)(X_{ij}))^{-1} \\ &= \det((w(X_{ij} \otimes 1))(w(1 \otimes X_{ij})))^{-1} \\ &= \det(w(X_{ij} \otimes 1))^{-1} \det(w(1 \otimes X_{ij}))^{-1} \\ &= w((\mathbb{T} \otimes 1)(1 \otimes \mathbb{T})) \\ &= w(\mathbb{T} \otimes \mathbb{T}) \end{aligned}$$

et donc

$$\Delta(\mathbb{T}) = (\mathbb{T} \otimes 1)(1 \otimes \mathbb{T}) = \mathbb{T} \otimes \mathbb{T}.$$

On procède de la même manière pour expliciter la counité $e^* : A \rightarrow k$ à partir du diagramme commutatif

$$\begin{array}{ccc} 1 & \xrightarrow{e} & GL_n(\mathbb{R}) \\ \wr \uparrow & & \uparrow \wr \\ \text{Hom}_{\text{Alg}_k}(k, \mathbb{R}) & \longrightarrow & \text{Hom}_{\text{Alg}_k}(A, \mathbb{R}) \end{array}$$

dans lequel la flèche horizontale inférieure est l'application $u \mapsto u \circ e^*$. La commutativité de ce diagramme pour $\mathbb{R} = k$ équivaut à

$$(e^*(X_{ij})) = I_n \quad \text{et} \quad e^*(\mathbb{T}) = \det(I_n)^{-1},$$

soit

$$e^*(X_{ij}) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \quad \text{et} \quad e^*(\mathbb{T}) = 1.$$

Considérons finalement le diagramme commutatif

$$\begin{array}{ccc} GL_n(\mathbb{R}) & \xrightarrow{\text{inv}} & GL_n(\mathbb{R}) \\ \wr \uparrow & & \uparrow \wr \\ \text{Hom}_{\text{Alg}_k}(A, \mathbb{R}) & \longrightarrow & \text{Hom}_{\text{Alg}_k}(A, \mathbb{R}) \end{array}$$

dans lequel la flèche inférieure est l'application $u \mapsto u \circ \iota$. Nous obtenons

$$((u \circ \iota)(X_{ij})) = (u(X_{ij}))^{-1} = \det(u(X_{ij}))^{-1} \text{adj}(u(X_{ij})),$$

où, pour toute matrice $M \in M_n(\mathbb{R})$, $\text{adj}(M)$ est la matrice définie par

$$\text{adj}(M)_{ij} = (-1)^{i+j} \det(\widehat{M}_{ji}),$$

$\widehat{M}_{ij} \in M_{n-1}(\mathbb{R})$ désignant la matrice obtenue à partir de M en supprimant la i -ème ligne et la j -ème colonne. Cette matrice vérifie l'identité $\text{adj}(M)M = \det(M)I_n$. Par suite,

$$\begin{aligned} (u \circ \iota)(X_{ij}) &= u(T)[\text{adj}(u(X_{ij}))]_{ij} \\ &= u(T[\text{adj}(X_{ij})]_{ij}) \end{aligned}$$

et donc

$$\iota(X_{ij}) = T[\text{adj}(X_{ij})]_{ij}.$$

De même,

$$(u \circ \iota)(T) = u(T)^{-1} = (\det(u(X_{ij}))^{-1})^{-1} = \det(u(X_{ij})) = u(\det(X_{ij}))$$

donc

$$\iota(T) = \det(X_{ij}).$$

Donnons encore deux exemples, pour lesquels toutes les justifications nécessaires sont laissées au lecteur.

(i) La bigèbre du groupe additif \mathbb{G}_a est la k -algèbre $k[T]$ munie de la comultiplication

$$k[T] \xrightarrow{\Delta} k[T] \otimes_k k[T] \cong k[T \otimes 1, 1 \otimes T], \quad T \mapsto T \otimes 1 + 1 \otimes T,$$

de la counité

$$k[T] \xrightarrow{0^*} k, \quad T \mapsto 0$$

et de la coinversion

$$k[T] \xrightarrow{\iota} k[T], \quad T \mapsto -T.$$

(ii) L'anneau du groupe multiplicatif $\mathbb{G}_m = \mathbb{G}\mathbb{L}_1$ est la k -algèbre $k[X, X^{-1}]$ des polynômes de Laurent en X . La k -algèbre $k[X, X^{-1}] \otimes_k k[X, X^{-1}]$ est canoniquement isomorphe à la k -algèbre $k[(X \otimes 1), (X \otimes 1)^{-1}, (1 \otimes X), (1 \otimes X)^{-1}]$ des polynômes de Laurent en les indéterminées $X \otimes 1$ et $1 \otimes X$.

– La comultiplication

$$k[X, X^{-1}] \xrightarrow{\Delta} k[(X \otimes 1), (X \otimes 1)^{-1}, (1 \otimes X), (1 \otimes X)^{-1}]$$

est définie par $\Delta(X) = (X \otimes 1)(1 \otimes X) = X \otimes X$ et $\Delta(X^{-1}) = (X \otimes 1)^{-1}(1 \otimes X)^{-1} = (X \otimes X)^{-1}$.

– La counité

$$k[X, X^{-1}] \xrightarrow{1^*} k$$

est définie par $1^*(X) = 1^*(X^{-1}) = 1$.

– La coinversion

$$k[X, X^{-1}] \xrightarrow{\iota} k[X, X^{-1}]$$

est définie par $\iota(X) = X^{-1}$, $\iota(X^{-1}) = X$.

(2.2.3) L'antiéquivalence que l'on a établie en 4.1 entre la catégorie des groupes algébriques sur k et celle des k -bigèbres de type fini signifie que ces deux concepts sont strictement interchangeables. Les deux points de vue sont utiles, mais il est en général plus agréable et plus facile de travailler en termes de foncteurs en groupes. La proposition suivante illustre l'utilisation des bigèbres pour étudier les homomorphismes entre deux groupes algébriques.

Proposition 2.2.3 — Il n'y a pas d'homomorphisme non trivial entre les groupes \mathbb{G}_a et \mathbb{G}_m :

$$\mathrm{Hom}_{\mathbf{k}\text{-Gr}}(\mathbb{G}_a, \mathbb{G}_m) = \{ \mathbb{G}_a \longrightarrow 1 \xrightarrow{1} \mathbb{G}_m \}$$

et

$$\mathrm{Hom}_{\mathbf{k}\text{-Gr}}(\mathbb{G}_m, \mathbb{G}_a) = \{ \mathbb{G}_m \longrightarrow 1 \xrightarrow{0} \mathbb{G}_a \}.$$

Démonstration. Il revient au même de se donner un homomorphisme $f : \mathbb{G}_a \rightarrow \mathbb{G}_m$ ou un homomorphisme de k -algèbres $f^* : k[X, X^{-1}] \rightarrow k[T]$ compatible aux structures de bigèbres. L'homomorphisme f^* est complètement déterminé par $f^*(X)$, qui doit être un élément inversible de $k[T]$; comme k est un corps, $k[T]^\times = k^\times$ et donc $f^*(X) = a \in k^\times$. La commutativité du diagramme

$$\begin{array}{ccc} k[X, X^{-1}] & \xrightarrow{f^*} & k[T] \\ & \searrow 1^* & \swarrow 0^* \\ & & k \end{array}$$

implique

$$1 = 1^*(X) = 0^*(a) = a,$$

donc $f^*(X) = 1$. Le seul homomorphisme de \mathbb{G}_a dans \mathbb{G}_m est donc l'homomorphisme trivial

$$\mathbb{G}_a \longrightarrow 1 \xrightarrow{1} \mathbb{G}_m$$

correspondant à l'homomorphisme de k -bigèbres

$$k[X, X^{-1}] \xrightarrow{1^*} k \longrightarrow k[T].$$

Il revient au même de se donner un homomorphisme $g : \mathbb{G}_m \rightarrow \mathbb{G}_a$ ou un homomorphisme de k -algèbres $g^* : k[T] \rightarrow k[X, X^{-1}]$ compatible aux structures de bigèbres. L'homomorphisme g^* est complètement déterminé par le polynôme de Laurent $g^*(T) = \sum_{n \in \mathbb{Z}} a_n X^n$. La commutativité du diagramme

$$\begin{array}{ccc} k[T] & \xrightarrow{\Delta} & k[T] \otimes_k k[T] \\ g^* \downarrow & & \downarrow g^* \otimes g^* \\ k[X, X^{-1}] & \xrightarrow{\Delta} & k[X, X^{-1}] \otimes_k k[X, X^{-1}] \end{array}$$

se traduit par l'identité

$$\Delta(g^*(T)) = (g^* \otimes g^*)(\Delta(T))$$

dans $k[X, X^{-1}] \otimes_k k[X, X^{-1}] \cong k[X \otimes 1, (X \otimes 1)^{-1}, 1 \otimes X, (1 \otimes X)^{-1}]$. Le membre de gauche s'explique aisément :

$$\Delta(g^*(T)) = \Delta\left(\sum_{n \in \mathbb{Z}} a_n X^n\right) = \sum_{n \in \mathbb{Z}} \Delta(X)^n = \sum_{n \in \mathbb{Z}} a_n (X \otimes 1)^n (1 \otimes X)^n$$

et il en est de même du membre de droite :

$$(g^* \otimes g^*)(\Delta(T)) = (g^* \otimes g^*)(T \otimes 1 + 1 \otimes T) = g^*(T) \otimes 1 + 1 \otimes g^*(T) = \sum_{n \in \mathbb{Z}} a_n [(X \otimes 1)^n + (1 \otimes X)^n].$$

Nous obtenons donc l'identité

$$\sum_{n \in \mathbb{Z}} a_n (X \otimes 1)^n (1 \otimes X)^n = \sum_{n \in \mathbb{Z}} a_n [(X \otimes 1)^n + (1 \otimes X)^n]$$

entre polynômes de Laurent en les indéterminées $X \otimes 1$ et $1 \otimes X$. Par identification, nous en déduisons

$$\begin{cases} a_n = 0 & \text{si } |n| \geq 1 \\ a_0 = 2a_0, \end{cases}$$

d'où finalement $g^*(T) = 0$. Ceci montre que le seul homomorphisme de \mathbb{G}_m dans \mathbb{G}_a est l'homomorphisme trivial

$$\mathbb{G}_m \longrightarrow 1 \xrightarrow{0} \mathbb{G}_a$$

correspondant à l'homomorphisme de k -bigèbres

$$k[T] \xrightarrow{0^*} k \longrightarrow k[X, X^{-1}].$$

□

Exercices. 1) Soit Γ un groupe fini. Démontrer que le foncteur constant $\Gamma : \mathbf{Alg}_k \rightarrow \mathbf{Gr}$ défini par $\Gamma(R) = \Gamma$ pour toute k -algèbre R et $\Gamma(f) = \text{id}_\Gamma$ pour tout homomorphisme de k -algèbres f , est représentable si et seulement si Γ est le groupe réduit à un élément. (*Indication* : pour toutes k -algèbres A et R ,

$$\text{Hom}_{\mathbf{Alg}_k}(A, R \oplus R) \cong \text{Hom}_{\mathbf{Alg}_k}(A, R) \times \text{Hom}_{\mathbf{Alg}_k}(A, R).$$

2) Soit Γ un groupe fini. L'ensemble k^Γ des fonctions sur Γ à valeurs dans k est naturellement muni d'une structure de k -algèbre commutative :

$$(\lambda f + \mu g)(\gamma) = \lambda f(\gamma) + \mu g(\gamma) \text{ et } (fg)(\gamma) = f(\gamma)g(\gamma)$$

pour tous $f, g \in k^\Gamma$, $\lambda, \mu \in k$ et $\gamma \in \Gamma$.

On considère les homomorphismes de k -algèbres

$$\Delta : k^\Gamma \rightarrow k^{\Gamma \times \Gamma}, \quad e^* : k^\Gamma \rightarrow k \text{ et } \iota : k^\Gamma \rightarrow k^\Gamma$$

définis comme suit :

$$\Delta(f) = ((\gamma, \gamma') \mapsto f(\gamma\gamma')),$$

$$e^*(f) = f(1_\Gamma),$$

et

$$\iota(f) = (\gamma \mapsto f(\gamma^{-1})).$$

- (i) Vérifier que les fonctions indicatrices e_γ des singletons $\{\gamma\}$ forment une base de k^Γ en tant que k -espace vectoriel.
- (ii) Démontrer que les k -algèbres $k^\Gamma \otimes_k k^\Gamma$ et $k^{\Gamma \times \Gamma}$ sont canoniquement isomorphes.
- (iii) Exprimer Δ , e^* et ι dans les bases canoniques $(e_\gamma)_{\gamma \in \Gamma}$ et $(e_\gamma \otimes e_{\gamma'})_{(\gamma, \gamma') \in \Gamma^2}$ de k^Γ et de $k^\Gamma \otimes_k k^\Gamma$.
- (iv) Vérifier que $(k^\Gamma, \Delta, e^*, \iota)$ est une k -bigèbre de type fini.
- (v) Soit $\underline{\Gamma}$ le groupe algébrique sur k correspondant à la k -bigèbre $(k^\Gamma, \Delta, e^*, \iota)$. Vérifier que l'on a un isomorphisme canonique $\underline{\Gamma}(k) \cong \Gamma$ puis déterminer $\underline{\Gamma}(R)$ pour toute k -algèbre R .

2.3. Constructions élémentaires

(2.3.1) Sous-groupes.

Définition 2.3.1 — Soit G un groupe algébrique sur k . Un sous-groupe de G est la donnée d'un homomorphisme de groupes algébriques $i : H \rightarrow G$ tel que l'homomorphisme de k -algèbres $i^* : \mathcal{O}(G) \rightarrow \mathcal{O}(H)$ correspondant soit surjectif.

Cette définition appelle deux commentaires.

1) Tout d'abord, pour toute k -algèbre R , l'homomorphisme de groupes $i_R : H(R) \rightarrow G(R)$ est *injectif*. En effet, on dispose d'un diagramme commutatif

$$\begin{array}{ccc} H(R) & \xrightarrow{i_R} & G(R) \\ \uparrow \wr & & \uparrow \wr \\ \text{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(H), R) & \longrightarrow & \text{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(G), R) \end{array}$$

dans lequel la flèche horizontale inférieure est l'application $u \mapsto u \circ i^*$. L'homomorphisme i^* étant surjectif, la condition $u \circ i^* = v \circ i^*$ implique $u = v$ pour tous $u, v \in \text{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(H), R)$ et ceci prouve que l'application i_R est injective.

2) La surjectivité de l'homomorphisme i^* signifie que la k -algèbre $\mathcal{O}(H)$ est isomorphe au quotient de $\mathcal{O}(G)$ par l'idéal $\ker(i^*)$. Ceci se traduit par le fait suivant : pour toute k -algèbre R , l'application

$$\text{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(H), R) \rightarrow \text{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(G), R)$$

induit une bijection sur le sous-ensemble de $\text{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(G), R)$ constitué des homomorphismes u tels que $u(\ker(i^*)) = 0$. De manière encore plus explicite, si l'on écrit $\mathcal{O}(G)$ sous la forme $k[T_1, \dots, T_n]/\mathfrak{J}$, alors l'idéal $\ker(i^*)$ de $\mathcal{O}(G)$ provient d'un idéal \mathfrak{I} de $k[T_1, \dots, T_n]$ contenant \mathfrak{J} ,

$$G(R) \simeq \{(r_1, \dots, r_n) \in R^n \mid f(r_1, \dots, r_n) = 0 \text{ pour tout } f \in \mathfrak{I}\}$$

et $H(R)$ s'identifie alors au sous-ensemble de $G(R)$ défini par les équations $f(r_1, \dots, r_n) = 0$, $f \in \mathfrak{I}$.

Au vu de ces deux observations, la définition que nous avons adoptée signifie précisément qu'un sous-groupe de G est un sous-foncteur en groupes défini par des équations polynomiales.

Remarque. En fait, il serait revenu au même de définir un sous-groupe de G comme un homomorphisme $i : H \rightarrow G$ tel que, pour toute k -algèbre R , l'homomorphisme $i_R : H(R) \rightarrow G(R)$ soit *injectif*. On peut en effet démontrer que cette condition suffit à garantir la surjectivité de l'homomorphisme $i^* : \mathcal{O}(G) \rightarrow \mathcal{O}(H)$.

Exemples. 1) Pour tout entier $n \geq 0$, SL_n est un sous-groupe de GL_n . Effet, l'inclusion naturelle i de SL_n dans GL_n correspond à l'homomorphisme de k -algèbres

$$i^* : k[(X_{ij})_{1 \leq i, j \leq n}, T]/(T \det(X_{ij}) - 1) \rightarrow k[(X_{ij})_{1 \leq i, j \leq n}]/(\det(X_{ij}) - 1)$$

défini par $i^*(X_{ij}) = X_{ij}$ et $i^*(T) = 1$. Cet homomorphisme est manifestement surjectif.

2) Pour tout entier $n \geq 0$, le groupe μ_n est un sous-groupe du groupe multiplicatif \mathbb{G}_m . En effet, l'inclusion naturelle i de μ_n dans \mathbb{G}_m correspond à l'homomorphisme de k -algèbres

$$i^* : k[X, X^{-1}] \rightarrow k[X]/(X^n - 1)$$

défini par $i^*(X) = X$ et $i^*(X^{-1}) = X^{n-1}$. Cet homomorphisme est manifestement surjectif.

3) Si le corps k est de caractéristique $p > 0$, le groupe α_p est un sous-groupe du groupe additif \mathbb{G}_a . En effet, l'inclusion naturelle i de α_p dans \mathbb{G}_a correspond à l'homomorphisme de k -algèbres

$$i^* : k[T] \rightarrow k[T]/(T^p)$$

défini par $i^*(T) = T$, qui est manifestement surjectif.

(2.3.2) Produit. Étant donnés deux groupes algébriques G_1 et G_2 , on peut construire le foncteur en groupes $G_1 \times G_2$ sur \mathbf{Alg}_k associant

- à toute k -algèbre R , le groupe produit $G_1(R) \times G_2(R)$;
- à tout homomorphisme de k -algèbres $f : R \rightarrow R'$, l'homomorphisme de groupes $G_1(f) \times G_2(f) : G_1(R) \times G_2(R) \rightarrow G_1(R') \times G_2(R')$.

Choisissons des anneaux de coordonnées $\varphi_1 : \mathfrak{h}_{A_1} \xrightarrow{\sim} G_1$ et $\varphi_2 : \mathfrak{h}_{A_2} \xrightarrow{\sim} G_2$ et considérons l'isomorphisme de foncteurs

$$\varphi_1 \times \varphi_2 : \mathfrak{h}_{A_1} \times \mathfrak{h}_{A_2} \xrightarrow{\sim} G_1 \times G_2.$$

Par définition même du produit tensoriel $A_1 \otimes_k A_2$, $\mathfrak{h}_{A_1 \otimes_k A_2} \simeq \mathfrak{h}_{A_1} \times \mathfrak{h}_{A_2}$ et nous obtenons donc un isomorphisme de foncteurs

$$\mathfrak{h}_{A_1 \otimes_k A_2} \longrightarrow G_1 \times G_2.$$

Enfin, si l'on choisit des isomorphismes $A_1 \simeq k[T_1, \dots, T_n]/\mathfrak{J}$ et $A_2 \simeq k[S_1, \dots, S_m]/\mathfrak{K}$, on obtient un isomorphisme de k -algèbres

$$\begin{aligned} A_1 \otimes_k A_2 &\simeq k[T_1, \dots, T_n]/\mathfrak{J} \otimes_k k[S_1, \dots, S_m]/\mathfrak{K} \\ &\simeq k[T_1, \dots, T_n, S_1, \dots, S_m]/\mathfrak{R} \end{aligned}$$

où \mathfrak{R} est l'idéal de $k[T_1, \dots, T_n, S_1, \dots, S_m]$ engendré par \mathfrak{J} et \mathfrak{K} (cf. appendice, 2.4, exercices 5 et 6). La k -algèbre $A_1 \otimes_k A_2$ est donc de type fini.

Cette discussion établit la proposition suivante.

Proposition 2.3.2 — *Étant donnés deux groupes algébriques G_1 et G_2 sur k , le foncteur en groupes $G_1 \times_k G_2$ est un groupe algébrique sur k , d'anneau de coordonnées $\mathcal{O}(G_1) \otimes_k \mathcal{O}(G_2)$.*

(2.3.3) Produit fibré et noyau. Considérons plus généralement un diagramme d'homomorphismes de groupes

$$\begin{array}{ccc} G_1 & & \\ & \searrow f_1 & \\ & & H \\ & \nearrow f_2 & \\ G_2 & & \end{array}$$

Pour toute k -algèbre R , l'ensemble $G_1(R) \times_{H(R)} G_2(R)$ des couples $(g_1, g_2) \in G_1(R) \times G_2(R)$ tels que $f_1(g_1) = f_2(g_2)$ est un sous-groupe de $G_1(R) \times G_2(R)$. Si $f : R \rightarrow R'$ est un homomorphisme de k -algèbres, on vérifie immédiatement que l'homomorphisme de groupes $G_1(f) \times G_2(f) : G_1(R) \times G_2(R) \rightarrow G_1(R') \times G_2(R')$ envoie $G_1(R) \times_{H(R)} G_2(R)$ dans $G_1(R') \times_{H(R')} G_2(R')$. Nous avons ainsi défini un foncteur

$$G_1 \times_H G_2 : \mathbf{Alg}_k \rightarrow \mathbf{Gr}.$$

Comme précédemment, on déduit de la propriété universelle du produit tensoriel des bijections naturelles

$$\begin{aligned} G_1(R) \times_{H(R)} G_2(R) &= \{(g_1, g_2) \in G_1(R) \times G_2(R) \mid f_1(g_1) = f_2(g_2)\} \\ &\simeq \{(g_1, g_2) \in \mathrm{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(G_1), R) \times \mathrm{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(G_2), R) \mid g_1 \circ f_1^* = g_2 \circ f_2^*\} \\ &\simeq \mathrm{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(G_1) \otimes_{\mathcal{O}(H)} \mathcal{O}(G_2), R) \end{aligned}$$

pour tout k -algèbre R . Le foncteur $G_1 \times_H G_2$ est ainsi représenté par la k -algèbre $\mathcal{O}(G_1) \otimes_{\mathcal{O}(H)} \mathcal{O}(G_2)$. Cette dernière est bien de type fini, car elle est isomorphe au quotient de la k -algèbre de type fini $\mathcal{O}(G_1) \otimes_k \mathcal{O}(G_2)$ par l'idéal engendré par les éléments de la forme $a \otimes 1 - 1 \otimes a$, $a \in \mathcal{O}(H)$.

Nous venons ainsi de démontrer la proposition suivante.

Proposition 2.3.3 — *Étant donnés des groupes algébriques G_1, G_2 et H ainsi que des homomorphismes $f_1 : G_1 \rightarrow H$ et $f_2 : G_2 \rightarrow H$, le foncteur en groupes*

$$G_1 \times_H G_2 : \mathbf{Alg}_k \rightarrow \mathbf{Gr}, \quad R \mapsto \{(g_1, g_2) \in G_1(R) \times G_2(R) \mid f_1(g_1) = f_2(g_2)\}$$

est un groupe algébrique, d'anneau de coordonnées $\mathcal{O}(G_1) \otimes_{\mathcal{O}(H)} \mathcal{O}(G_2)$. Ce groupe est le produit fibré des groupes G_1 et G_2 au-dessus de H et il s'agit naturellement d'un sous-groupe du groupe produit $G_1 \times G_2$.

Un cas particulier de produit fibré est le noyau d'un homomorphisme de groupes algébriques.

Proposition 2.3.4 — Soit $f : G \rightarrow H$ un homomorphisme de groupes algébriques. Le foncteur en groupes sur \mathbf{Alg}_k , associant à toute k -algèbre R le noyau de l'homomorphisme de groupes $f_R : G(R) \rightarrow H(R)$, est un groupe algébrique, d'anneau de coordonnées $\mathcal{O}(G) \otimes_{\mathcal{O}(H)} k$. Il s'agit d'un sous-groupe de G .

Démonstration. Considérons le diagramme

$$\begin{array}{ccc} G & & \\ & \searrow f & \\ & & H \\ & \nearrow e_H & \\ 1 & & \end{array}$$

Pour toute k -algèbre R ,

$$\begin{aligned} (G \times_H 1)(R) &= \{(g, 1) \in G(R) \times \{1\} \mid f(g) = e_H(1)\} \\ &= \{(g, 1) \in G(R) \times \{1\} \mid f(g) = 1_H\} \\ &\cong \ker(f_R) \end{aligned}$$

donc le foncteur en groupes $\ker(f)$ est canoniquement isomorphe au produit fibré $G \times_H 1$. Il en découle que $\ker(f)$ est un groupe algébrique d'anneau de coordonnées $\mathcal{O}(G) \otimes_{\mathcal{O}(H)} k$ et c'est naturellement un sous-groupe de $G \cong G \times 1$. \square

Exemples. 1) Le groupe SL_n est le noyau de l'homomorphisme $\det : GL_n \rightarrow GL_1$.

2) Soit $n \geq 0$ un nombre entier et considérons l'homomorphisme $[n] : \mathbb{G}_m \rightarrow \mathbb{G}_m$ défini par l'élévation à la puissance n -ème ; pour toute k -algèbre R , $[n]_R$ est l'homomorphisme $R^\times \rightarrow R^\times$, $x \mapsto x^n$. Son noyau est manifestement le groupe μ_n des racines n -èmes de l'unité. Notons que l'on peut retrouver l'anneau de coordonnées de ce dernier : l'homomorphisme $[n]$ correspond à l'homomorphisme de k -algèbres $k[Y, Y^{-1}] \rightarrow k[X, X^{-1}]$ envoyant X sur Y^n et

$$[X, X^{-1}] \otimes_{[Y, Y^{-1}]} k \cong k[X, X^{-1}] \otimes_k k / (X^n \otimes 1 - 1 \otimes 1) \cong k[X, X^{-1}] / (X^n - 1) \cong k[X] / (X^n - 1).$$

3) Supposons que k soit un corps de caractéristique $p > 0$. La multiplication par p définit un homomorphisme $[p] : \mathbb{G}_a \rightarrow \mathbb{G}_a$; pour toute k -algèbre R , $[p]_R$ est l'homomorphisme $R \rightarrow R$, $x \mapsto px$. Son noyau est manifestement le groupe algébrique α_p . L'homomorphisme $[p]$ correspond à l'homomorphisme de k -algèbres $k[S] \rightarrow k[T]$ envoyant S sur T^p et

$$k[T] \otimes_{k[S]} k \cong k[T] \otimes_k k / (T^p \otimes 1 - 0 \otimes 1) \cong k[T] / (T^p).$$

(2.3.4) Image, quotient. La situation est beaucoup plus délicate pour ce qui est des images et des quotients. En général, si $f : G \rightarrow H$ est un homomorphisme de groupes algébriques, le foncteur en groupes

$$\mathbf{Alg}_k \rightarrow \mathbf{Gr}, \quad R \mapsto \text{im} \left(G(R) \xrightarrow{f_R} H(R) \right)$$

n'est pas un groupe algébrique. De même, si $i : N \rightarrow G$ est un sous-groupe de G tel que, pour toute k -algèbre R , $N(R)$ soit un sous-groupe distingué de $G(R)$, le foncteur en groupes

$$\mathbf{Alg}_k \rightarrow \mathbf{Gr}, \quad R \mapsto G(R)/N(R)$$

n'est généralement pas un groupe algébrique.

Il n'y a pas à chercher beaucoup pour obtenir un contre-exemple : l'homomorphisme $\mathbb{G}_m \xrightarrow{[n]} \mathbb{G}_m$ convient parfaitement !

Proposition 2.3.4 — Soit n un nombre entier. Si $n \geq 2$, le foncteur

$$\mathbf{Alg}_k \rightarrow \mathbf{Ens}, \quad R \mapsto \text{im}(R^\times \rightarrow R^\times, x \mapsto x^n) = \{r \in R^\times \mid r \text{ est une puissance } n\text{-ème}\}$$

n'est pas représentable.

Démonstration. Supposons que ce foncteur soit représentable, c'est-à-dire qu'il existe une k -algèbre A et un morphisme de foncteurs $\varphi : \mathbf{h}_A \rightarrow \mathbf{h}_{k[X, X^{-1}]}$ tels que, pour toute k -algèbre R , l'application

$$\varphi_R : \text{Hom}_{\mathbf{Alg}_k}(A, R) \rightarrow \text{Hom}_{\mathbf{Alg}_k}(k[X, X^{-1}], R) \cong R^\times$$

soit une bijection sur le sous-ensemble de R^\times constitué des puissances n -èmes. En vertu du lemme de Yoneda, il existe un unique homomorphisme de k -algèbre $\pi : k[X, X^{-1}] \rightarrow A$ tel que $\varphi = \mathbf{h}_\pi$. Posant $\alpha = \pi(X)$, nous pouvons alors reformuler ce que l'on vient de dire sous la forme d'une propriété universelle :

- α est une puissance n -ème dans A ;
- pour toute k -algèbre R et tout homomorphisme $r : k[X, X^{-1}] \rightarrow R$ tel que $r(X)$ soit une puissance n -ème dans R , il existe un unique homomorphisme $\bar{r} : A \rightarrow R$ tel que $\bar{r}(\alpha) = r(X)$, c'est-à-dire tel que le diagramme

$$\begin{array}{ccc} k[X, X^{-1}] & \xrightarrow{r} & R \\ \pi \downarrow & \nearrow \bar{r} & \\ A & & \end{array}$$

soit commutatif.

Nous allons maintenant démontrer que *tout* homomorphisme $r : k[X, X^{-1}] \rightarrow R$ se factorise à travers π ; en vertu de la propriété universelle qui précède, ceci impliquera que *tout* élément inversible de n 'importe quelle k -algèbre est une puissance n -ème, assertion évidemment fautive si $n \geq 2$ (considérer par exemple X dans $k[X, X^{-1}]$). Pour ce faire, nous allons commencer par construire \bar{r} comme un homomorphisme de A dans une k -algèbre contenant R , puis nous vérifierons que cet homomorphisme est en fait à valeur dans R .

Considérons une k -algèbre R et un homomorphisme $r : k[X, X^{-1}] \rightarrow R$; posons $a = r(X)$. La k -algèbre $R_1 = R[T_1]/(T_1^n - a)$ contient R et a y est manifestement une puissance n -ème ; il existe donc un unique homomorphisme $\bar{r}_1 : A \rightarrow R_1$ tel que $\bar{r}_1(\alpha) = a$. De même, la k -algèbre $R_2 = k[T_2]/(T_2^n - a)$ contient R et a y est manifestement une puissance n -ème ; il existe donc un unique homomorphisme $\bar{r}_2 : A \rightarrow R_2$ tel que $\bar{r}_2(\alpha) = a$. Posant

$$R_{12} = R[T_1, T_2]/(T_1 - a, T_2 - a) = R_1[T_2]/(T_2 - a) = R_2[T_1]/(T_1 - a)$$

et désignant par i_1 et i_2 les inclusions canoniques de R_1 et R_2 dans R_{12} , les homomorphismes $i_1 \circ r_1$ et $i_2 \circ r_2$ de A dans R_{12} sont tels que $(i_1 \circ r_1)(\alpha) = (i_2 \circ r_2)(\alpha) = a$, donc $i_1 \circ \bar{r}_1 = i_2 \circ \bar{r}_2$.

En tant que R -module, R_1 (resp. R_2) est libre de base $(1, T_1, \dots, T_1^{n-1})$ (resp. $(1, T_2, \dots, T_2^{n-1})$) ; de même, $R_{12} = R_1[T_2]/(T_2 - a)$ est un R_1 -module libre de base $1, T_2, \dots, T_2^{n-1}$. Nous en déduisons que R_{12} est un R -module libre de base les monômes $T_1^{v_1} T_2^{v_2}$ avec $0 \leq v_1, v_2 \leq n-1$. Quel que soit l'élément t de A , $\bar{r}_1(t)$ s'écrit de manière unique sous la forme $u_0 + u_1 T_1 + \dots + u_{n-1} T_1^{n-1}$ avec $u_0, \dots, u_{n-1} \in R$; de même, $\bar{r}_2(t)$ s'écrit de manière unique sous la forme $v_0 + v_1 T_2 + \dots + v_{n-1} T_2^{n-1}$ avec $v_0, \dots, v_{n-1} \in R$. L'identité $i_1 \circ \bar{r}_1 = i_2 \circ \bar{r}_2$ implique

$$u_0 + u_1 T_1 + \dots + u_{n-1} T_1^{n-1} = v_0 + v_1 T_2 + \dots + v_{n-1} T_2^{n-1}$$

dans R_{12} , donc

$$u_0 = v_0, \quad u_1 = \dots = u_{n-1} = v_1 = \dots = v_{n-1} = 0.$$

L'homomorphisme $\bar{r}_1 : A \rightarrow R_1$ est par conséquent à valeurs dans la sous-algèbre R et nous avons ainsi établi que l'homomorphisme r se factorise à travers π . Comme expliqué précédemment, ceci conclut la démonstration de la proposition. \square

Pour toute k -algèbre R , l'homomorphisme $[n]_R : \mathbb{G}_m(R) \rightarrow \mathbb{G}_m(R)$ induit un isomorphisme entre le groupe quotient $\mathbb{G}_m(R)/\mu_n(R)$ et le sous-groupe de $\mathbb{G}_m(R) = R^\times$ constitué des puissances n -èmes. La proposition que nous venons d'établir peut donc se reformuler de manière équivalente comme suit.

Proposition 2.3.5 — Soit n un nombre entier. Si $n \geq 2$, le foncteur

$$\mathbf{Alg}_k \rightarrow \mathbf{Ens}, \quad R \mapsto \mathbb{G}_m(R)/\mu_n(R)$$

n'est pas représentable.

Exercices. 1) Soit (A, Δ, e^*, ι) une k -bigèbre de type fini et soit \mathcal{J} un idéal de A . On désigne par p la projection canonique de A sur A/\mathcal{J} .

- (i) À quelle condition existe-t-il une structure de foncteur en groupes sur $h_{A/\mathcal{J}}$ telle que le morphisme $h_p : h_{A/\mathcal{J}} \rightarrow h_A$ soit un homomorphisme de groupes algébriques ?
- (ii) Si $h_{A/\mathcal{J}}$ est un sous-groupe de h_A , à quelle condition est-ce un sous-groupe *distingué*, c'est-à-dire tel que $h_{A/\mathcal{J}}(R)$ soit distingué dans $h_A(R)$ pour toute k -algèbre R ?

2) Considérons l'homomorphisme de groupes algébriques $i : \mathbb{G}_m \rightarrow \mathbb{G}_m \times \mathbb{G}_m$ défini par

$$i_R : R^\times \rightarrow R^\times \times R^\times, \quad t \mapsto (t, t)$$

pour toute k -algèbre R .

Vérifier que l'homomorphisme i fait de \mathbb{G}_m un sous-groupe de $\mathbb{G}_m \times \mathbb{G}_m$ puis démontrer que le foncteur en groupes

$$\mathbf{Alg}_k \rightarrow \mathbf{Gr}, \quad R \mapsto \mathbb{G}_m(R) \times \mathbb{G}_m(R)/\mathbb{G}_m(R)$$

est un groupe algébrique sur k .

2.4. Changement du corps de base

Examinons l'effet d'un changement du corps de base.

Proposition 2.4.1 — Soit G un groupe algébrique sur k et soit k'/k une extension de corps. Le foncteur en groupes sur $\mathbf{Alg}_{k'}$ obtenu par restriction de G est un groupe algébrique sur k' d'anneau de coordonnées $\mathcal{O}(G) \otimes_k k'$.

Démonstration. Pour toute k' -algèbre R' ,

$$G(R') \simeq \mathrm{Hom}_{\mathbf{Alg}_k}(\mathcal{O}(G), R') \cong \mathrm{Hom}_{\mathbf{Alg}_{k'}}(\mathcal{O}(G) \otimes_k k', R'),$$

donc le foncteur

$$\mathbf{Alg}_{k'} \rightarrow \mathbf{Ens}, \quad R' \mapsto G(R')$$

est représenté par la k' -algèbre $\mathcal{O}(G) \otimes_k k'$. En outre, comme $\mathcal{O}(G)$ est de type fini sur k , $\mathcal{O}(G) \simeq k[T_1, \dots, T_n]/\mathcal{J}$ et donc

$$\mathcal{O}(G) \otimes_k k' \simeq (k[T_1, \dots, T_n]/\mathcal{J}) \otimes_k k' \simeq k'[T_1, \dots, T_n]/\mathcal{J}$$

est une k' -algèbre de type fini (cf. appendice, 2.4, exercice 4). \square

Étant donné un groupe algébrique G sur k et une extension de corps k'/k , on note $G \otimes_k k'$ le groupe algébrique sur k' défini en restreignant G à la sous-catégorie $\mathbf{Alg}_{k'}$ de \mathbf{Alg}_k .

Exemple 1 – Soit k un corps de caractéristique différente de 2. Pour toute k -algèbre R , l'ensemble des matrices de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ avec $a, b \in R$ tels que $a^2 + b^2 \in R^\times$ est un sous-groupe de $GL_2(R)$; on en déduit que le foncteur

$$G : \mathbf{Alg}_k \rightarrow \mathbf{Gr}, \quad R \mapsto \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M_2(R) \mid a^2 + b^2 \in R^\times \right\}$$

est un sous-groupe de GL_2 , d'anneau de coordonnées

$$\mathcal{O}(G) = k[X_{11}, X_{12}, X_{21}, X_{22}, T] / (X_{11} - X_{22}, X_{12} + X_{21}, T(X_{11}X_{22} - X_{12}X_{21})).$$

Considérons une k -algèbre R . Si R contient un élément i tel que de $i^2 + 1 = 0$, alors

$$a^2 + b^2 = (a - ib)(a + ib)$$

pour tous $a, b \in R$ et l'application

$$G(R) \rightarrow R^\times \times R^\times, \quad \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto (a + ib, a - ib)$$

est un isomorphisme de groupes, d'inverse l'application

$$R^\times \times R^\times \rightarrow G(R), \quad (u, v) \mapsto \begin{pmatrix} (u+v)/2 & (v-u)/2i \\ (u-v)/2i & (u+v)/2 \end{pmatrix}.$$

Supposons par exemple $k = \mathbb{Q}$ et considérons l'extension quadratique $\mathbb{Q}(i) = \mathbb{Q}[T]/(T^2 + 1)$ de \mathbb{Q} .

D'après ce que l'on vient de dire, le groupe $G \otimes_{\mathbb{Q}} \mathbb{Q}(i)$ est isomorphe au groupe produit $\mathbb{G}_m \times \mathbb{G}_m$. Par contre, le groupe G n'est pas isomorphe à $\mathbb{G}_m \times \mathbb{G}_m$; en effet, les groupes

$$G(\mathbb{R}) \simeq \mathbb{C}^\times$$

et

$$(\mathbb{G}_m \times \mathbb{G}_m)(\mathbb{R}) = \mathbb{R}^\times \times \mathbb{R}^\times$$

ne sont pas isomorphes car le sous-groupe de torsion du premier est divisible, tandis que le sous-groupe de torsion du second est isomorphe au *Viergruppe* de Klein $(\mathbb{Z}/2\mathbb{Z})^2$.

Exemple 2 – Considérons le groupe unitaire usuel

$$U(n) = \{M \in M_n(\mathbb{C}) \mid {}^t \overline{M} M = I_n\},$$

où \overline{M} désigne la matrice déduite de M par conjugaison des coefficients. Peut-on écrire ce groupe sous la forme $G(R)$ pour un certain groupe algébrique G sur \mathbb{Q} et une certaine \mathbb{Q} -algèbre R ?

Pour toute \mathbb{Q} -algèbre R , la \mathbb{Q} -algèbre $R \otimes_{\mathbb{Q}} \mathbb{Q}[T]/(T^2 + 1) = R[T]/(T^2 + 1)$ est munie d'un automorphisme R -linéaire canonique σ défini par $\sigma(T) = -T$. L'ensemble

$$G(R) = \{M \in M_n(R[T]/(T^2 + 1)) \mid {}^t \sigma(M) M = I_n\}$$

est un groupe pour le produit matriciel; par ailleurs, si l'on note $x_{ij} + y_{ij}T$ les coefficients d'une matrice $M \in M_n(R[T]/(T^2 + 1))$, la condition ${}^t \sigma(M) M = I_n$ équivaut aux identités polynomiales

$$\begin{cases} (x_{1i}^2 + y_{1i}^2) + \dots + (x_{ni}^2 + y_{ni}^2) = 1 & (1 \leq i \leq n) \\ (x_{1i}x_{1j} - y_{1i}y_{1j}) + \dots + (x_{ni}x_{nj} - y_{ni}y_{nj}) = 0 & (1 \leq i < j \leq n) \\ (x_{1i}y_{1j} + x_{1j}y_{1i}) + \dots + (x_{ni}y_{nj} + x_{nj}y_{ni}) = 0 & (1 \leq i < j \leq n) \end{cases}$$

et donc le foncteur en groupes G ainsi défini sur $\mathbf{Alg}_{\mathbb{Q}}$ est un groupe algébrique. Par construction même, $G(\mathbb{R})$ est le groupe unitaire $U(n)$.

Supposons que R soit une \mathbb{Q} -algèbre contenant un élément ξ tel que $\xi^2 + 1 = 0$. Sous cette hypothèse, l'application

$$\varepsilon : R[T]/(T^2 + 1) \rightarrow R \times R, \quad a + bT \mapsto (a + b\xi, a - b\xi)$$

est un isomorphisme d'anneaux et, via cette identification, l'automorphisme σ de $\mathbb{R}[T]/(T^2 + 1)$ correspond à la permutation des deux facteurs de $\mathbb{R} \times \mathbb{R}$. En utilisant l'isomorphisme canonique de \mathbb{R} -algèbres

$$M_2(\mathbb{R} \times \mathbb{R}) \cong M_2(\mathbb{R}) \times M_2(\mathbb{R}),$$

on en déduit que le groupe $G(\mathbb{R})$ est isomorphe au sous-groupe de $GL_2(\mathbb{R}) \times GL_2(\mathbb{R})$ constitué des couples (M_1, M_2) tels que ${}^t(M_2, M_1)(M_1, M_2) = (I_n, I_n)$, c'est-à-dire tels que

$${}^t M_2 M_1 = {}^t M_1 M_2 = I_n.$$

Ainsi, la première projection $GL_2(\mathbb{R}) \times GL_2(\mathbb{R}) \rightarrow GL_2(\mathbb{R})$ induit un isomorphisme entre $G(\mathbb{R})$ et $GL_2(\mathbb{R})$.

Au final, nous avons construit un groupe algébrique G sur \mathbb{Q} tel que

$$G(\mathbb{R}) = U(n) \quad \text{et} \quad G(\mathbb{C}) \simeq GL_n(\mathbb{C}).$$

On constate aisément que les groupes $U(n)$ et $GL_n(\mathbb{R})$ ne sont pas isomorphes, par exemple en vertu du fait que le centre du premier est isomorphe à \mathbb{R}/\mathbb{Z} et donc contient 3 éléments de 3-torsion tandis que le centre du second, isomorphe à \mathbb{R}^\times , ne contient qu'un élément de 3-torsion. Cette observation montre que les groupes algébriques G et GL_n sur \mathbb{Q} ne sont pas isomorphes ; par contre, les groupes algébriques $G \otimes_{\mathbb{Q}} \mathbb{Q}(i)$ et GL_n sur $\mathbb{Q}(i)$ sont isomorphes.

3. REPRÉSENTATIONS LINÉAIRES

L'objectif principal de ce chapitre est le théorème suivant de C. CHEVALLEY : tout groupe algébrique G est isomorphe à un sous-groupe d'un groupe linéaire GL_n ; en outre, étant donné un sous-groupe H de G , on peut réaliser G comme un sous-groupe de GL_n de telle sorte que, pour toute k -algèbre R , $H(R)$ soit le sous-groupe de $G(R)$ constitué des matrices de la forme

$$\left(\begin{array}{c|ccc} * & * & \dots & * \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array} \right)$$

Il découle en particulier de ce théorème que *tout* groupe algébrique peut se voir comme un groupe (fonctoriel) de matrices.

3.1. Généralités

(3.1.1) Soit C une catégorie quelconque. Si G est un foncteur en groupes sur C et E est un foncteur en ensembles sur C , on définit de manière naturelle une *action* de G sur E comme la donnée d'un morphisme de foncteurs

$$\varphi : G \times E \rightarrow E$$

tel que les diagrammes

$$\begin{array}{ccc} G \times G \times E \times E & \xrightarrow{\text{id}_G \times \varphi} & G \times E \\ m \times \text{id}_E \downarrow & & \downarrow \varphi \\ G \times E & \xrightarrow{\varphi} & E \end{array} \quad \text{et} \quad \begin{array}{ccc} 1 \times E & \xrightarrow{e \times \text{id}_E} & G \times E \\ \sim \searrow & & \downarrow \varphi \\ & & E \end{array}$$

où m (resp. e) désigne la multiplication (resp. le neutre) de G , soient commutatifs.

Les arguments utilisés pour démontrer la proposition 1.1.1 montrent qu'il est équivalent de se donner

- une action $\varphi : G \times E \rightarrow E$ de G sur E ;
- pour tout objet X de C , une action φ_X du groupe $G(X)$ sur l'ensemble $E(X)$ de telle sorte que, pour toute flèche $f : X \rightarrow Y$ dans C , l'application $E(f) : E(X) \rightarrow E(Y)$ soit équivariante relativement aux groupes $G(X)$ et $G(Y)$, i.e.

$$E(f)(\varphi_X(g, x)) = \varphi_Y(G(f)(g), E(f)(x))$$

pour tous $g \in G(X)$, $x \in E(X)$.

Exemple — Si G est un foncteur en groupes sur C , on peut considérer le foncteur en ensembles \tilde{G} associé à G (i.e. $\tilde{G}(X)$ est l'ensemble sous-jacent au groupe $G(X)$) et faire agir G sur \tilde{G} par translation à gauche en considérant le morphisme de foncteurs $\varphi : G \times \tilde{G} \rightarrow \tilde{G}$ défini par $\varphi_X(g, h) = gh$ pour tout objet X de C et tous $g, h \in G(X)$. On peut également faire agir G sur \tilde{G} par conjugaison.

Un autre exemple : on considère le foncteur en ensembles E défini par

- pour tout objet X de C , $E(X)$ est l'ensemble des sous-groupes de G ;
- pour toute flèche $f : X \rightarrow Y$ dans C , $E(f)$ est l'application envoyant un sous-groupe H de $G(X)$ sur le sous-groupe $G(f)H$ de $G(Y)$.

(3.1.2) Soit k un corps et soit V un k -espace vectoriel. On associe à V un foncteur $\underline{V} : \mathbf{Alg}_k \rightarrow \mathbf{Ens}$ en posant

- pour toute k -algèbre R , $\underline{V}(R)$ est le R -module libre $V \otimes_k R$;
- pour tout homomorphisme de k -algèbre $f : R \rightarrow R'$, $\underline{V}(f)$ est l'application R -linéaire

$$V \otimes_k R \rightarrow V \otimes_k R', \quad \sum_{\alpha} v_{\alpha} \otimes \lambda_{\alpha} \mapsto \sum_{\alpha} v_{\alpha} \otimes f(\lambda_{\alpha}).$$

Remarques — 1. Si $(e_i)_{i \in I}$ est une base de V , $(e_i \otimes 1)_{i \in I}$ est une base du R -module libre $V \otimes_k R$.

2. Une application R -linéaire u de $V \otimes_k R$ dans un R -module M est uniquement déterminée par sa restriction au sous-ensemble $V \otimes_k 1 = \{v \otimes 1 ; v \in V\}$ de $V \otimes_k R$, que l'on identifie canoniquement à V . En effet, tout élément de $V \otimes_k R$ s'écrit sous la forme $\sum_{\alpha} v_{\alpha} \otimes \lambda_{\alpha}$ et

$$u\left(\sum_{\alpha} v_{\alpha} \otimes \lambda_{\alpha}\right) = \sum_{\alpha} u(v_{\alpha} \otimes 1)\lambda_{\alpha}.$$

Lemme 3.1.1 — Soit V un k -espace vectoriel et soit $f : R \rightarrow R'$ un homomorphisme de k -algèbres. Étant donné un endomorphisme R -linéaire α de $V \otimes_k R$, il existe un unique endomorphisme R' -linéaire $f^*(\alpha)$ de $V \otimes_k R'$ tel que le diagramme

$$\begin{array}{ccc} V \otimes_k R' & \xrightarrow{f^*(\alpha)} & V \otimes_k R' \\ \text{id}_V \otimes f \uparrow & & \uparrow \text{id}_V \otimes f \\ V \otimes_k R & \xrightarrow{\alpha} & V \otimes_k R' \end{array}$$

soit commutatif.

On a $f^*(\text{id}_{V \otimes_k R}) = \text{id}_{V \otimes_k R'}$ et $f^*(\alpha\beta) = f^*(\alpha)f^*(\beta)$ pour tous $\alpha, \beta \in \text{End}_R(V \otimes_k R)$. En particulier, si α est un automorphisme, $f^*(\alpha)$ est un automorphisme.

Démonstration. L'application composée

$$V \xrightarrow{\alpha} V \otimes_k R \xrightarrow{\text{id}_V \otimes f} V \otimes_k R'$$

est k -linéaire et donc se prolonge de manière unique en une application R' -linéaire $\alpha' : V \otimes_k R' \rightarrow V \otimes_k R'$. Par construction, les applications R -linéaires $\alpha' \circ (\text{id}_V \otimes f)$ et $(\text{id}_V \otimes f) \circ \alpha$ de $V \otimes_k R$ dans $V \otimes_k R'$ coïncident sur le sous-ensemble $V \otimes 1$ de $V \otimes_k R$; elles sont donc égales et il suffit de poser $f^*(\alpha) = \alpha'$. L'unicité est claire puisque la restriction de $f^*(\alpha)$ au sous-ensemble $V \otimes 1$ de $V \otimes_k R'$ est donnée.

Les identités $f^*(\text{id}_{V \otimes_k R}) = \text{id}_{V \otimes_k R'}$ et $f^*(\alpha\beta) = f^*(\alpha)f^*(\beta)$ se déduisent immédiatement de l'unicité. \square

Le lemme précédent permet de définir un foncteur en groupes GL_V sur Alg_k :

- pour toute k -algèbre R , $\text{GL}_V(R)$ est le groupe des automorphismes R -linéaires du R -module $V \otimes_k R$;
- pour toute flèche $f : R \rightarrow R'$, $\text{GL}_V(f)$ est l'homomorphisme $\text{GL}_V(R) \rightarrow \text{GL}_V(R')$ envoyant α sur $f^*(\alpha)$.

Proposition 3.1.2 — Soit V un k -espace vectoriel. Pour que le foncteur en groupe GL_V soit un groupe algébrique sur k , il faut et il suffit que V soit de dimension finie.

Démonstration. Le choix d'une base $(e_i)_{i \in I}$ de V sur k permet de définir un isomorphisme de foncteurs en groupes entre GL_V et le foncteur

$$\text{G}_I : \mathbf{Alg}_k \rightarrow \text{Gr}, \quad R \mapsto \{\text{matrices inversibles dans } M_I(R)\}$$

en associant à chaque automorphisme R -linéaire de $V \otimes_k R = \bigoplus_{i \in I} R(e_i \otimes 1)$ sa matrice dans la base $(e_i \otimes 1)_{i \in I}$.

Ainsi, si V est de dimension finie d , alors GL_V est isomorphe au foncteur en groupes GL_d et il s'agit donc d'un groupe algébrique sur k .

Réciproquement, si le foncteur GL_V est un groupe algébrique d'anneau de coordonnées A , alors le foncteur G_I est représenté par le couple (A, α) , où α est un certain élément de $G_I(A)$; en particulier, pour toute k -algèbre R , chaque matrice inversible $M \in M_I(R)$ est de la forme $f(\alpha)$ pour un certain homomorphisme de k -algèbres $f : A \rightarrow R$.

Considérons la k -algèbre $K = k((X_i)_{i \in I})$ des fractions rationnelles en des indéterminées X_i , $i \in I$. Par hypothèse, la k -algèbre A est de type fini donc il existe $t_1, \dots, t_n \in A$ tel que tout élément a de A s'écrive sous la forme d'un polynôme en t_1, \dots, t_n à coefficients dans k ; il en découle que, pour tout homomorphisme de k -algèbre $f : A \rightarrow K$, la matrice $f(\alpha)$ fait intervenir qu'un nombre fini d'indéterminées X_i . Si l'ensemble I est infini, la matrice de l'automorphisme K -linéaire u de $V \otimes_k K$ défini par $u(e_i \otimes 1) = X_i(e_i \otimes 1)$ pour tout $i \in I$ fait intervenir une infinité d'indéterminées et donc ne peut pas s'écrire sous la forme $f(\alpha)$. Ainsi, le foncteur en groupe GL_V n'est pas un groupe algébrique si l'ensemble I est infini. \square

Définition 3.1.3 — Soit G un groupe algébrique sur k et soit V un k -espace vectoriel. Une représentation linéaire de G dans V est une action de G sur \underline{V} telle que, pour toute k -algèbre R , le groupe $G(R)$ agisse par automorphismes R -linéaires sur $V \otimes_k R$.

Pour tout groupe algébrique G sur k et tout k -espace vectoriel V , il revient au même de se donner une représentation linéaire $\varphi : G \times \underline{V} \rightarrow \underline{V}$ ou un morphisme de foncteurs en groupes $\rho : G \rightarrow \text{GL}_V$. La correspondance est donnée par l'identité

$$\rho_R(g) = \varphi_R(g, \cdot)$$

pour toute k -algèbre R et tout $g \in G(R)$.

Exemples — 1. On définit une représentation linéaire de SL_2 dans l'espace vectoriel $k[X, Y]_2 = kX^2 \oplus kXY \oplus Y^2$ des polynômes homogènes de degré 2 en X et Y de la manière suivante. Pour toute k -algèbre R , le groupe $\text{SL}_2(R)$ opère naturellement sur le R -module $RX \oplus RY$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (X, Y) = (X, Y) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (aX + bY, cX + dY).$$

On en déduit une action de $\text{SL}_2(R)$ sur $V \otimes_k R = RX^2 \oplus RXY \oplus RY^2$ définie par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot X^2 = (aX + bY)^2 = a^2X^2 + 2abXY + b^2Y^2,$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot Y^2 = (cX + dY)^2 = c^2X^2 + 2cdXY + d^2Y^2$$

et

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot XY = (aX + bY)(cX + dY) = acX^2 + (ad + bc)XY + bdY^2.$$

On dispose plus généralement d'une représentation naturelle de SL_n dans l'espace vectoriel $k[X_1, \dots, X_n]_d$ des polynômes homogènes de degré d en n indéterminées : pour toute k -algèbre R , $\text{SL}_n(R)$ opère sur $R[X_1, \dots, X_n]_1 = RX_1 \oplus \dots \oplus RX_n$ via

$$(g \cdot X_1, \dots, g \cdot X_n) = (X_1, \dots, X_n)^t g$$

et il en découle une action de $\text{SL}_n(R)$ sur $R[X_1, \dots, X_n]_d = k[X_1, \dots, X_n]_d \otimes_k R$ définie par

$$g \cdot P(X_1, \dots, X_n) = P(g \cdot X_1, \dots, g \cdot X_n).$$

2. On dispose d'une représentation linéaire naturelle du groupe algébrique GL_n dans l'espace vectoriel $V = M_n(k)$: pour toute k -algèbre R , $V \otimes_k R \simeq M_n(R)$ et on fait opérer le groupe $\text{GL}_n(R)$ par conjugaison : $g \cdot M = gMg^{-1}$.

Il est aisé d'expliciter cette représentation en utilisant la base canonique de $M_n(k)$ formée des matrices élémentaires E_{ij} ($1 \leq i, j \leq n$). Pour $n = 2$, on obtient les formules suivantes :

si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_n(\mathbf{R})$ et $\delta = ad - bc$, alors

$$g.E_{11} = \frac{1}{\delta}(adE_{11} - abE_{12} + cdE_{21} - bcE_{22}), \quad g.E_{12} = \frac{1}{\delta}(-acE_{11} + a^2E_{12} - c^2E_{21} + acE_{22})$$

$$g.E_{21} = \frac{1}{\delta}(bdE_{11} - b^2E_{12} + d^2E_{21} - bdE_{22}) \quad \text{et} \quad g.E_{22} = \frac{1}{\delta}(-bcE_{11} + abE_{12} - cdE_{21} + adE_{22}).$$

(3.1.3) Considérons un k -espace vectoriel V de dimension finie et soit W un sous-espace vectoriel de V .

Proposition 3.1.4 — *Le foncteur*

$$\mathrm{Stab}(W) : \mathbf{Alg}_k \rightarrow \mathbf{Gr}, \quad \mathbf{R} \mapsto \{g \in \mathrm{GL}_V \mid g(W \otimes_k \mathbf{R}) \subset W \otimes_k \mathbf{R}\}$$

est un groupe algébrique et l'inclusion canonique $\mathrm{Stab}(W) \hookrightarrow \mathrm{GL}_V$ en fait un sous-groupe de GL_V .

Démonstration. Considérons une base (e_1, \dots, e_m) de W et complétons-la en une base (e_1, \dots, e_n) de V . L'isomorphisme $\mathrm{GL}_V \xrightarrow{\sim} \mathrm{GL}_n$ obtenu en associant à tout élément $g \in \mathrm{GL}_V(\mathbf{R}) = \mathrm{GL}(V \otimes_k \mathbf{R})$ sa matrice dans la base $(e_1 \otimes 1, \dots, e_n \otimes 1)$ identifie le sous-foncteur en groupes $\mathrm{Stab}(W)$ de GL_V au sous-foncteur en groupes F de GL_n tel que

$$F(\mathbf{R}) = \left\{ \begin{pmatrix} M & M' \\ 0 & M'' \end{pmatrix} ; M \in \mathrm{GL}_m(\mathbf{R}), M' \in M_{m, n-m}(\mathbf{R}) \text{ et } M'' \in \mathrm{GL}_{n-m}(\mathbf{R}) \right\}$$

pour toute k -algèbre \mathbf{R} .

Le foncteur F est manifestement un sous-groupe algébrique de GL_n , son anneau de coordonnées étant le quotient de $\mathcal{O}(\mathrm{GL}_n) = k[(X_{ij}), T]/(T \det(X_{ij}) - 1)$ par l'idéal engendré par les X_{ij} avec $m+1 \leq i \leq n$ et $1 \leq j \leq m$. Par conséquent, $\mathrm{Stab}(W)$ est un sous-groupe algébrique de GL_V . \square

Plus généralement, étant donné un groupe algébrique G sur k et une représentation $\rho : G \rightarrow \mathrm{GL}_V$ de G dans V , le produit fibré $G \times_{\mathrm{GL}_V} \mathrm{Stab}(W)$ du diagramme

$$\begin{array}{ccc} G & & \\ & \searrow \rho & \\ & & \mathrm{GL}_V \\ & \nearrow & \\ \mathrm{Stab}(W) & & \end{array}$$

est un groupe algébrique (cf. 2.3.3). Quelle que soit la k -algèbre \mathbf{R} ,

$$\begin{aligned} (G \times_{\mathrm{GL}_V} \mathrm{Stab}(W))(\mathbf{R}) &= \{(g, h) \in G(\mathbf{R}) \times \mathrm{Stab}(W)(\mathbf{R}) \mid \rho_{\mathbf{R}}(g) = h\} \\ &= \{g \in \mathrm{GL}_V(\mathbf{R}) \mid \rho_{\mathbf{R}}(g)(W \otimes_k \mathbf{R}) \subset W \otimes_k \mathbf{R}\} \end{aligned}$$

s'identifie au sous-groupe de $G(\mathbf{R})$ constitué des éléments stabilisant le sous-module $W \otimes_k \mathbf{R}$ de $V \otimes_k \mathbf{R}$. On dit que $G \times_{\mathrm{GL}_V} \mathrm{Stab}(W)$ est le *stabilisateur* de W dans V et on le note $\mathrm{Stab}_G(W)$.

L'anneau de coordonnées de $\mathrm{Stab}_G(W)$ est $\mathcal{O}(G) \otimes_{\mathcal{O}(\mathrm{GL}_V)} \mathcal{O}(\mathrm{Stab}(W))$. La première projection $G \times_{\mathrm{GL}_V} \mathrm{Stab}(W) \rightarrow G$ fournit un homomorphisme canonique j de $\mathrm{Stab}_G(W)$ dans G correspondant à l'homomorphisme

$$j^* : \mathcal{O}(G) \rightarrow \mathcal{O}(G) \otimes_{\mathcal{O}(\mathrm{GL}_V)} \mathcal{O}(\mathrm{Stab}(W)), \quad a \mapsto a \otimes 1.$$

Ce dernier est surjectif, ⁽²⁾ donc $\text{Stab}_G(W)$ est un sous-groupe de G .

(3.1.4) Étant donné un groupe algébrique G d'anneau de coordonnées A , nous allons maintenant voir qu'il est équivalent de se donner une représentation linéaire de G dans un k -espace vectoriel V ou d'équiper V d'une structure de *comodule* sur A .

Soit $\rho : G \rightarrow \text{GL}_V$ une représentation linéaire. Ayant choisi un isomorphisme de foncteurs $G \simeq h_A$, on dispose pour toute k -algèbre R et tout élément g de $G(R) = \text{Hom}_{\text{Alg}_k}(A, R)$ d'un digramme commutatif

$$\begin{array}{ccc} G(A) \times V & \xrightarrow{\rho_A} & V \otimes_k A \\ G(g) \times \text{id}_V \downarrow & & \downarrow \text{id}_V \otimes g \\ G(R) \times V & \xrightarrow{\rho_R} & V \otimes_k R \end{array}$$

et g est l'image de l'élément id_A de $G(A) = \text{Hom}_{\text{Alg}_k}(A, A)$ par l'application $G(g)$. On en déduit l'identité

$$\rho_R(g, v) = ((\text{id}_V \otimes g) \circ \rho_A)(\text{id}_A, v)$$

pour tout vecteur $v \in V$, ce qui montre que la représentation ρ est complètement déterminée par la donnée de l'application k -linéaire

$$\tilde{\rho} = \rho_A(\text{id}_A \otimes \cdot) : V \rightarrow V \otimes_k A.$$

Exemple — Considérons le groupe additif \mathbb{G}_a et la représentation linéaire ρ dans le k -espace vectoriel $V = ke_1 \oplus ke_2$ définie par

$$\rho_R(t).e_1 \otimes 1 = e_1 \otimes 1 \quad \text{et} \quad t.e_2 \otimes 1 = t(e_1 \otimes 1) + e_2 \otimes 1 = e_1 \otimes t + e_2 \otimes 1$$

pour toute k -algèbre R et tout $t \in \mathbb{G}_a(R) = R$.

L'anneau de coordonnées de \mathbb{G}_a est la k -algèbre $A = k[T]$ et les bijections

$$\text{Hom}_{\text{Alg}_k}(k[T], R) \rightarrow \mathbb{G}_a(R) = R, \quad u \mapsto u(T)$$

définissent un isomorphisme de foncteurs $h_A \simeq \mathbb{G}_a$; via cette identification, id_A correspond en particulier à l'élément T de $\mathbb{G}_a(k[T]) = k[T]$. Il en découle que $\tilde{\rho}$ est l'application k -linéaire

$$V \rightarrow V \otimes_k k[T], \quad e_1 \mapsto e_1 \otimes 1, \quad e_2 \mapsto e_1 \otimes T + e_2 \otimes 1$$

et, pour toute k -algèbre R et tout élément t de $\mathbb{G}_a(R) = R$, $\rho_R(t, \cdot)$ est l'application composée

$$V \xrightarrow{\tilde{\rho}} V \otimes_k k[T] \xrightarrow{\text{id}_V \otimes t} V \otimes_k R$$

obtenue en spécialisant T en t .

Proposition 3.1.5 — Soit G un groupe algébrique sur k et soit (A, Δ, e^*, ι) la k -bigèbre associée. Pour tout k -espace vectoriel V , il revient au même de se donner :

(i) une représentation linéaire $\rho : G \rightarrow \text{GL}_V$;

⁽²⁾L'homomorphisme $i^* : \mathcal{O}(\text{GL}_V) \rightarrow \mathcal{O}(\text{Stab}(W))$ correspondant à l'inclusion canonique $i : \text{Stab}(W) \hookrightarrow \text{GL}_V$ est surjectif (cf. la démonstration de la proposition 3.1.4). Par suite, tout élément de

$$\mathcal{O}(G) \rightarrow \mathcal{O}(G) \otimes_{\mathcal{O}(\text{GL}_V)} \mathcal{O}(\text{Stab}(W))$$

de la forme $a \otimes b$ s'écrit $a \otimes i^*(c) = a\rho^*(c) \otimes 1$ avec $c \in \mathcal{O}(\text{GL}_V)$ et la surjectivité de j^* en découle.

(ii) une application k -linéaire $\tilde{\rho} : V \rightarrow V \otimes_k A$ telle que les deux diagrammes

$$\begin{array}{ccc} V & \xrightarrow{\tilde{\rho}} & V \otimes_k A \\ \tilde{\rho} \downarrow & & \downarrow \tilde{\rho} \otimes \text{id}_A \\ V \otimes_k A & \xrightarrow{\text{id}_V \otimes \Delta} & V \otimes_k A \otimes_k A \end{array} \quad \text{et} \quad \begin{array}{ccc} V & \xrightarrow{\tilde{\rho}} & V \otimes_k A \\ & \searrow & \downarrow \text{id}_V \otimes e^* \\ & & V \otimes_k k \end{array}$$

soient commutatifs.

À une représentation linéaire ρ correspond l'application $\tilde{\rho} = \rho_A(\text{id}_A, \cdot)$.

À une application $\tilde{\rho} : V \rightarrow V \otimes_k A$ satisfaisant aux deux conditions de (ii) correspond la représentation linéaire ρ telle que, pour toute k -algèbre R et tout élément g de $G(R) = \text{Hom}_{\text{Alg}_k}(A, R)$, $\rho_R(g)$ soit l'unique automorphisme R -linéaire de $V \otimes_k R$ prolongeant l'application k -linéaire

$$V \xrightarrow{\tilde{\rho}} V \otimes_k A \xrightarrow{\text{id}_V \otimes g} V \otimes_k R.$$

Démonstration. Soit ρ une représentation linéaire de G dans V et soit $\tilde{\rho} = \rho_A(\text{id}_A, \cdot)$; on a vu que, pour toute k -algèbre R et tout élément g de $G(R) = \text{Hom}_{\text{Alg}_k}(A, R)$, $\rho_R(g)$ est l'unique automorphisme R -linéaire de $V \otimes_k R$ prolongeant l'application k -linéaire

$$V \xrightarrow{\tilde{\rho}} V \otimes_k A \xrightarrow{\text{id}_R \otimes g} V \otimes_k R.$$

Considérons deux éléments g, h de $G(R)$ et calculons successivement $\rho_R(gh)$ et $\rho_R(g) \circ \rho_R(h)$.

Par définition de la comultiplication Δ de A , gh est l'homomorphisme de k -algèbres $A \rightarrow R$ défini comme le composé

$$A \xrightarrow{\Delta} A \otimes_k A \xrightarrow{g \otimes h} R \otimes_k R \xrightarrow{\text{mult}} R$$

donc $\rho_R(gh)$ est l'unique automorphisme R -linéaire de $V \otimes_k R$ prolongeant l'application k -linéaire

$$V \xrightarrow{\tilde{\rho}} V \otimes_k A \xrightarrow{\text{id}_V \otimes \Delta} V \otimes_k A \otimes_k A \xrightarrow{\text{id}_V \otimes g \otimes h} V \otimes_k R \otimes_k R \xrightarrow{\text{id}_V \otimes \text{mult}} V \otimes_k R.$$

D'autre part, si v est un vecteur de V , alors $\rho_R(h).v = \sum_i v_i \otimes \lambda_i$ avec $v_i \in V$ et $\lambda_i \in R$, puis

$$\begin{aligned} (\rho_R(g) \circ \rho_R(h)).v &= \rho(g). \sum_i v_i \otimes \lambda_i \\ &= \sum_i (\rho_R(g).v_i) \lambda_i \end{aligned}$$

dans $V \otimes_k R$. Ainsi, $\rho_R(g) \circ \rho_R(h)$ est l'unique automorphisme R -linéaire de $V \otimes_k R$ prolongeant l'application k -linéaire

$$V \xrightarrow{\tilde{\rho}} V \otimes_k A \xrightarrow{\tilde{\rho} \otimes \text{id}_A} V \otimes_k A \otimes_k A \xrightarrow{\text{id}_V \otimes g \otimes h} V \otimes_k R \otimes_k R \xrightarrow{\text{id}_V \otimes \text{mult}} V \otimes_k R.$$

L'identité $\rho_R(gh) = \rho_R(g) \circ \rho_R(h)$ est donc équivalente à la commutativité du diagramme

$$\begin{array}{ccc} V & \xrightarrow{\tilde{\rho}} & V \otimes_k A \\ \downarrow \tilde{\rho} & & \downarrow \tilde{\rho} \otimes \text{id}_A \\ V \otimes_k A & \xrightarrow{\text{id}_V \otimes \Delta} & V \otimes_k A \otimes_k A \\ & & \searrow \text{mult} \circ (g \otimes h) \\ & & V \otimes_k R. \end{array}$$

Comme ceci doit être vrai pour toute k -algèbre R et tous $g, h \in G(R) = \text{Hom}_{\mathbf{Alg}_k}(A, R)$, on en déduit immédiatement que le diagramme

$$\begin{array}{ccc} V & \xrightarrow{\tilde{\rho}} & V \otimes_k A \\ \tilde{\rho} \downarrow & & \downarrow \tilde{\rho} \otimes \text{id}_A \\ V \otimes_k A & \xrightarrow{\text{id}_V \otimes \Delta} & V \otimes_k A \otimes_k A \end{array}$$

est commutatif (considérer $R = A \otimes_k A$ et prendre pour g (resp. h) l'homomorphisme de A dans $A \otimes_k A$ envoyant a sur $a \otimes 1$ (resp. sur $1 \otimes a$), de sorte que $g \otimes h$ soit l'identité de $A \otimes_k A$).

L'élément neutre e_R du groupe $G(R)$ correspond à l'homomorphisme de k -algèbres de A dans R obtenu en composant $e^* : A \rightarrow k$ par l'unique homomorphisme de k -algèbres $u : k \rightarrow R$. Par suite, l'identité $\rho_k(e_k) = \text{id}_V$ équivaut à la commutativité du diagramme

$$\begin{array}{ccc} V & \xrightarrow{\tilde{\rho}} & V \otimes_k A \\ & \searrow & \downarrow \text{id}_V \otimes e^* \\ & & V \otimes_k k \end{array}$$

Partons réciproquement d'une application k -linéaire $\tilde{\rho}$ de V dans $V \otimes_k A$ satisfaisant aux deux conditions de (ii). Pour toute k -algèbre R et tout $g \in G(R) = \text{Hom}_{\mathbf{Alg}_k}(A, R)$, on désigne par $\rho_R(g)$ l'unique endomorphisme R -linéaire de $V \otimes_k R$ prolongeant l'application k -linéaire $(\text{id}_V \otimes g) \circ \tilde{\rho}$. La discussion précédente montre que l'on a $\rho_R(gh) = \rho_R(g)\rho_R(h)$ et $\rho_R(e_R) = \text{id}_{V \otimes_k R}$ pour toute k -algèbre R et tous $g, h \in G(R)$; en particulier, $\rho_R(g)$ est un *automorphisme* R -linéaire de $V \otimes_k R$ et on conclut que les homomorphismes de groupes $\rho_R : G(R) \rightarrow \text{GL}_V(R)$ définissent une représentation linéaire ρ de G dans V telle que $\tilde{\rho} = \rho_A(\text{id}_A, \cdot)$. \square

La structure mise en évidence au point (ii) de la proposition précédente mérite d'être baptisée.

Définition 3.1.6 — Soit (A, Δ, e^*, ι) est une k -bigèbre. Un comodule sur A est la donnée d'un k -espace vectoriel V et d'une application k -linéaire $\tilde{\rho} : V \rightarrow V \otimes_k A$ telle que les deux diagrammes

$$\begin{array}{ccc} V & \xrightarrow{\tilde{\rho}} & V \otimes_k A \\ \tilde{\rho} \downarrow & & \downarrow \tilde{\rho} \otimes \text{id}_A \\ V \otimes_k A & \xrightarrow{\text{id}_V \otimes \Delta} & V \otimes_k A \otimes_k A \end{array} \quad \text{et} \quad \begin{array}{ccc} V & \xrightarrow{\tilde{\rho}} & V \otimes_k A \\ & \searrow & \downarrow \text{id}_V \otimes e^* \\ & & V \otimes_k k \end{array}$$

soient commutatifs.

Un sous-comodule de V est un sous-espace vectoriel W de V tel que l'image de W par l'application $\tilde{\rho}$ soit contenue dans le sous-espace vectoriel $W \otimes_k A$ de $V \otimes_k A$.

Exemple — Reprenons le premier exemple donné après la définition 3.1.3, soit l'action naturelle de SL_2 sur $V = k[X, Y]_2$. Ici, $A = k[X_{11}, X_{12}, X_{21}, X_{22}]/(X_{11}X_{22} - X_{12}X_{21} - 1)$ et la représentation envisagée correspond à l'application k -linéaire

$$k[X, Y]_2 \rightarrow k[X, Y]_2 \otimes_k A$$

définie par

$$X^2 \mapsto X^2 \otimes X_{11}^2 + XY \otimes 2X_{12}X_{11} + Y^2 \otimes X_{12}^2, \quad Y^2 \mapsto X^2 \otimes X_{21} + XY \otimes 2X_{21}X_{22} + Y^2 \otimes X_{22}^2$$

et

$$XY \mapsto X^2 \otimes X_{11}X_{21} + XY \otimes (X_{11}X_{22} + X_{12}X_{21}) + Y^2 \otimes X_{12}X_{22}.$$

3.2. Représentation régulière

Soit G un groupe algébrique sur k d'anneau de coordonnées A ; on fixe un isomorphisme de foncteurs $h_A \simeq G$, d'où l'on déduit une structure de k -bigèbre (A, Δ, e^*, ι) sur A (voir 2.2.1). La comultiplication $\Delta : A \rightarrow A \otimes_k A$ munit A d'une structure de comodule sur A : en effet, les deux diagrammes à considérer sont bien commutatifs puisque ce sont respectivement celui exprimant la coassociativité de Δ et celui caractérisant la counité e^* . On en déduit une représentation linéaire $G \rightarrow GL_A$, appelée *représentation régulière*.

On peut donner de cette représentation une interprétation instructive. Étant donnée une k -algèbre R , on désigne par $\mathcal{F}(G(R), R)$ l'ensemble de toutes les fonctions sur $G(R)$ à valeurs dans R , que l'on munit de sa structure naturelle de R -algèbre.

Tout élément f de A définit naturellement une fonction $\bar{f} \in \mathcal{F}(G(R), R)$, à savoir

$$G(R) = \text{Hom}_{\text{Alg}_k}(A, R) \rightarrow R, \quad s \mapsto \bar{f}(s) = s(f).$$

La correspondance $f \mapsto \bar{f}$ est manifestement un homomorphisme de k -algèbres de A dans $\mathcal{F}(G(R), R)$, lequel se prolonge en un homomorphisme de R -algèbres $A \otimes_k R \rightarrow \mathcal{F}(G(R), R)$. Notons que cet homomorphisme n'est généralement *pas* injectif lorsque R est fixée : par exemple, si $R = k = \mathbb{F}_p$ et $G = \mathbb{G}_a$, il s'agit de l'application $\mathbb{F}_p[T] \rightarrow \mathcal{F}(\mathbb{F}_p, \mathbb{F}_p)$, $f \mapsto (x \mapsto f(x))$, qui s'annule identiquement sur $X^p - X$. On obtient par contre l'injectivité en faisant varier R : précisément, si f est un élément de $A \otimes_k R$ induisant la fonction nulle sur $G(R')$ pour *toute* R -algèbre R' , alors $s(f) = 0$ quel que soit l'homomorphisme s de A dans R' et, prenant $R' = A \otimes_k R$ avec $s = \text{id}_{A \otimes_k R}$, alors $f = 0$.

Étant donné $f \in A \otimes_k R$, on peut composer la fonction $\bar{f} : G(R) \rightarrow R$ avec la multiplication $G(R) \times G(R) \rightarrow G(R)$ pour obtenir une fonction sur $G(R) \times G(R)$. Si l'on revient à la définition de \bar{f} , on constate qu'il s'agit de l'application envoyant le couple $(s, t) \in G(R) \times G(R)$ sur l'image de $(s \otimes t)\Delta(f)$ par l'homomorphisme produit $R \otimes_k R \rightarrow R$. En d'autres termes, si l'on écrit $\Delta(f) \in A \otimes_k A$ sous la forme $\Delta(f) = \sum_i g_i \otimes h_i$, alors

$$\bar{f}(st) = \sum_i \bar{g}_i(s) \bar{h}_i(t).$$

Revenons maintenant à la représentation régulière ρ de G . Étant donnée une k -algèbre R , on fait agir $G(R)$ par automorphismes R -linéaires de $A \otimes_k R$: à $s \in G(R)$ correspond l'unique automorphisme R -linéaire $\rho(s)$ de $A \otimes_k R$ prolongeant l'application k -linéaire

$$A \rightarrow A \otimes_k R, \quad f \mapsto (\text{id}_A \otimes s)\Delta(f).$$

Si $f \in A$ et si $\Delta(f) = \sum_i g_i \otimes h_i$, alors $\rho(s).f = \sum_i g_i \otimes s(h_i) = \sum_i g_i \otimes \bar{h}_i(s)$ et donc

$$\overline{\rho(s).f}(t) = \sum_i \bar{g}_i(t) \bar{h}_i(s) = \bar{f}(ts).$$

On dispose ainsi d'un diagramme commutatif

$$\begin{array}{ccc} A \otimes_k R & \xrightarrow{\rho(s)} & A \otimes_k R \\ \downarrow & & \downarrow \\ \mathcal{F}(G(R), R) & \longrightarrow & \mathcal{F}(G(R), R) \end{array}$$

dans lequel

- les flèches verticales sont les applications $f \mapsto \bar{f}$;
- la flèche horizontale inférieure est l'automorphisme de $\mathcal{F}(G(R), R)$ envoyant une fonction φ sur la fonction

$$\varphi(\cdot s) : G(R) \xrightarrow{\cdot s} G(R) \xrightarrow{\varphi} R .$$

Cette interprétation de la représentation régulière $\rho : G \rightarrow \mathrm{GL}_A$ met en évidence le fait qu'il s'agit d'une représentation *fidèle*, c'est-à-dire que l'homomorphisme de groupes ρ_R est injectif quelle que soit la k -algèbre R . En effet, si s est un élément de $G(R)$ tel que $\rho_R(s)$ soit l'identité de $A \otimes_k R$, alors $\bar{f}(\cdot s) = \bar{f}$ pour tout $f \in A$, donc

$$s(f) = \bar{f}(s) = \bar{f}(e_R s) = \bar{f}(e_R) = e_R(f)$$

pour tout élément f de A , et par suite $s = e_R$ puisqu'il s'agit de deux homomorphismes de k -algèbres de A dans R .

Considérons finalement un sous-groupe H de G . Par définition, l'anneau de coordonnées de H est un quotient de celui de G ; il est donc de la forme A/\mathfrak{J} pour un certain idéal \mathfrak{J} de A .

Lemme 3.2.1 — *L'idéal \mathfrak{J} est précisément l'ensemble des éléments f de A tels que, pour toute k -algèbre R , la fonction $\bar{f} : G(R) \rightarrow R$ s'annule identiquement sur le sous-groupe $H(R)$.*

Plus généralement, quelle que soit la k -algèbre R , $\mathfrak{J} \otimes_k R$ est le sous-ensemble de $A \otimes_k R$ formé des éléments f tels que, pour toute R -algèbre R' , la fonction $\bar{f} : G(R') \rightarrow R'$ s'annule identiquement sur le sous-groupe $H(R')$.

Démonstration. Démontrons directement la seconde assertion, plus générale (faire $R = k$ pour obtenir la première).

Considérons une R -algèbre R' . Par définition, la fonction sur $G(R')$ associée à un élément f de $A \otimes_k R$ est l'application

$$\bar{f} : G(R') = \mathrm{Hom}_{\mathbf{Alg}_R}(A \otimes_k R, R') \rightarrow R', \quad s \mapsto \bar{f}(s) = s(f).$$

Un élément s de $G(R')$ appartient au sous-groupe $H(R')$ de $G(R')$ si et seulement si l'homomorphisme $A \otimes_k R \rightarrow R'$ lui correspondant se factorise à travers la projection canonique $A \otimes_k R \rightarrow A \otimes_k R / \mathfrak{J} \otimes_k R$, donc si et seulement si $\bar{f}(s) = s(f) = 0$ pour tout élément f de $\mathfrak{J} \otimes_k R$. Cela montre en particulier que la fonction \bar{f} sur $G(R')$ associée à $f \in A \otimes_k R$ est identiquement nulle, quelle que soit la R -algèbre R' , si f appartient à $\mathfrak{J} \otimes_k R$.

Réciproquement, si $\bar{f}(s) = 0$ pour toute R -algèbre R' et tout $s \in H(R')$, on a alors en particulier $s(f) = \bar{f}(s) = 0$ lorsque $R' = A \otimes_k R / \mathfrak{J} \otimes_k R$ et s est la projection canonique de $A \otimes_k R$ sur R' , d'où $f \in \mathfrak{J} \otimes_k R$. \square

3.3. Le théorème de Chevalley

(3.3.1) Nous sommes maintenant en mesure de démontrer le théorème annoncé en introduction de ce chapitre.

Théorème 3.3.1 (Chevalley) — *Soit G un groupe algébrique sur k .*

- (i) *Il existe un k -espace vectoriel V de dimension finie et une représentation linéaire ρ de G dans V tel que l'homomorphisme $\rho : G \rightarrow \mathrm{GL}_V$ induise un isomorphisme de G sur un sous-groupe de GL_V .*
- (ii) *Étant donné un sous-groupe H de G , il existe un espace vectoriel V de dimension finie, une représentation linéaire $\rho : G \rightarrow \mathrm{GL}_V$ et un sous-espace vectoriel W de V tels que ρ induise un isomorphisme de G sur un sous-groupe de GL_V et $H = \mathrm{Stab}_G(W)$.*

Lemme 3.3.2 — *Soit V un comodule sur une k -bigèbre A . Tout élément v de V est contenu dans un sous-comodule W de V de dimension finie.*

Démonstration. Considérons une base $(a_i)_{i \in I}$ de A en tant que k -espace vectoriel. Tout élément de $V \otimes_k A$ s'écrit d'une manière et d'une seule sous la forme $\sum_{i \in I} v_i \otimes a_i$, où $(v_i)_{i \in I}$ est une famille d'éléments de V ne contenant qu'un nombre fini de vecteurs non nuls.

Fixons un élément v de V et soit W_0 le sous-espace vectoriel de V engendré par les vecteurs v_i apparaissant dans

$$\tilde{\rho}(v) = \sum_{i \in I} v_i \otimes a_i.$$

Il s'agit d'un sous-espace de dimension finie puisqu'il n'y a qu'un nombre fini de v_i non nuls. Le premier axiome définissant la structure de comodule sur V est l'identité $(\tilde{\rho} \otimes \text{id}_A) \circ \tilde{\rho} = (\text{id}_V \otimes \Delta) \circ \tilde{\rho}$, où Δ désigne la comultiplication de A . On a

$$[(\tilde{\rho} \otimes \text{id}_A) \circ \tilde{\rho}](v) = \sum_{i \in I} \tilde{\rho}(v_i) \otimes a_i$$

et

$$[(\text{id}_V \otimes \Delta) \circ \tilde{\rho}](v) = \sum_{i \in I} v_i \otimes \Delta(a_i).$$

La famille $(a_j \otimes a_\ell)_{(j,\ell) \in I^2}$ est une base du k -espace vectoriel $A \otimes_k A$, donc

$$\Delta(a_i) = \sum_{(j,\ell) \in I^2} \lambda_{j,\ell}^i a_j \otimes a_\ell$$

avec $\lambda_{j,\ell}^i \in k$; par suite,

$$\begin{aligned} [(\text{id}_V \otimes \Delta) \circ \tilde{\rho}](v) &= \sum_{(i,j,\ell) \in I^3} \lambda_{j,\ell}^i v_i \otimes a_j \otimes a_\ell \\ &= \sum_{\ell \in I} \left(\sum_{(i,j) \in I^2} \lambda_{j,\ell}^i v_i \otimes a_j \right) \otimes a_\ell. \end{aligned}$$

En comparant les deux expressions obtenues pour $[(\tilde{\rho} \otimes \text{id}_A) \circ \tilde{\rho}](v) = [(\text{id}_V \otimes \Delta) \circ \tilde{\rho}](v)$, on obtient

$$\tilde{\rho}(v_\ell) = \sum_{(i,j) \in I^2} \lambda_{j,\ell}^i v_i \otimes a_j$$

pour tout $\ell \in I$. On a ainsi $\tilde{\rho}(v_\ell) \in W_0 \otimes A$ pour tout $\ell \in I$, donc $\tilde{\rho}(W_0) \subset W_0 \otimes_k A$.

Finalement, $W = W_0 + kv$ est un sous-espace vectoriel de V de dimension finie contenant v et tel que $\tilde{\rho}(W) \subset W \otimes_k A$. \square

Démonstration du théorème de Chevalley — (i) Soit A l'anneau des coordonnées de G . Par hypothèse, A est une k -algèbre de type fini, donc engendrée par un nombre fini d'éléments t_1, \dots, t_N en tant que k -algèbre (c'est-à-dire que tout élément de A s'écrit sous la forme d'un polynôme en les t_1, \dots, t_N à coefficients dans k).

En vertu du lemme précédent, t_1, \dots, t_N sont contenus dans un sous-comodule V de A de dimension finie. La représentation régulière $G \rightarrow \text{GL}_A$ induit une représentation linéaire $\rho : G \rightarrow \text{GL}_V$ et il nous reste à vérifier que ρ induit un isomorphisme de G sur un sous-groupe de GL_V , c'est-à-dire que l'homomorphisme $\rho^* : \mathcal{O}(\text{GL}_V) \rightarrow \mathcal{O}(G) = A$ est surjectif.

Fixons une base (e_1, \dots, e_n) du k -espace vectoriel V et utilisons-la pour identifier les groupes algébriques GL_V et GL_n . Considérons la matrice $(a_{ij}) \in M_n(A)$ définie par les identités

$$\tilde{\rho}(e_j) = \sum_{1 \leq i \leq n} e_i \otimes a_{ij}$$

($1 \leq i \leq n$); vu la correspondance entre ρ et $\tilde{\rho}$ décrite en 3.1.4, l'application k -linéaire $\tilde{\rho} : V \rightarrow V \otimes_k A$ est induite par l'automorphisme de $V \otimes_k A$ provenant de l'élément id_A de $G(A)$. Il en découle que (a_{ij}) est la matrice de cet automorphisme dans la base $(e_1 \otimes 1, \dots, e_n \otimes 1)$ de $V \otimes_k A$, ce qui revient à dire que (a_{ij}) est l'image de l'élément id_A de $G(A)$ par l'homomorphisme $\rho_A : G(A) \rightarrow \text{GL}_n(A)$. De manière équivalente, a_{ij} est l'image de la coordonnée $X_{ij} \in \mathcal{O}(\text{GL}_n)$ par l'homomorphisme $\rho^* : \mathcal{O}(\text{GL}_n) \rightarrow \mathcal{O}(G) = A$. Par suite, l'image de ρ^* contient la sous- k -algèbre A_0 de A engendrée par les éléments a_{ij} ($1 \leq i, j \leq n$).

Nous allons conclure en vérifiant que A_0 contient les générateurs t_1, \dots, t_N de A , donc est égale à A . Il suffit de s'assurer que A_0 contient le sous-espace vectoriel V . Par définition de la structure de bigèbre, le diagramme

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_k A \\ & \searrow & \downarrow e^* \otimes \Delta \\ & & k \otimes_k A \end{array}$$

est commutatif ; on a par conséquent

$$\begin{aligned} e_j &= [(e^* \otimes \text{id}_A) \circ \Delta](e_j) \\ &= (e^* \otimes \text{id}_A) \left(\sum_{1 \leq i \leq n} e_i \otimes a_{ij} \right) \\ &= \sum_{1 \leq i \leq n} e^*(e_i) a_{ij}. \end{aligned}$$

Ces identités mettent en évidence le fait que la base (e_i) de V est contenue dans A_0 , donc $V \subset A_0$. On a ainsi $A = A_0$ et l'homomorphisme ρ^* est surjectif.

(ii) Soit \mathfrak{J} l'idéal de A définissant le sous-groupe H de G – c'est-à-dire le noyau de l'homomorphisme $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$. L'anneau A étant une k -algèbre de type fini, il est noethérien et l'idéal \mathfrak{J} est donc engendré par un nombre fini d'éléments. En appliquant le lemme précédent, il existe par conséquent un sous-comodule V de A de dimension finie contenant un ensemble de générateurs de la k -algèbre A (comme en (i)) ainsi qu'un ensemble de générateurs f_1, \dots, f_n de l'idéal \mathfrak{J} . Comme on vient de l'établir, la représentation linéaire $\rho : G \rightarrow \text{GL}_V$ induite par la représentation régulière de G fournit un isomorphisme de G sur un sous-groupe de GL_V .

Posons $W = V \cap \mathfrak{J}$; ce sous-espace vectoriel de V contient par construction les générateurs f_1, \dots, f_n de \mathfrak{J} . Étant donné une k -algèbre R et un élément s du sous-groupe $\text{Stab}_G(W)(R)$ de $G(R)$, on dispose par hypothèse pour tout $i \in \{1, \dots, n\}$ d'une identité

$$\rho_R(s, f_i) = \sum_{1 \leq j \leq n} f_j \otimes \lambda_{ij}$$

avec $\lambda_{ij} \in R$, d'où

$$s(f_i) = \overline{f_i}(s) = \overline{f_i}(e_R s) = \overline{\rho_R(s, f_i)}(e_R) = \sum_{1 \leq j \leq n} f_j(e_R) \lambda_{ij} = 0$$

car, les f_j appartenant à l'idéal \mathfrak{J} , les fonctions $\overline{f_j}$ s'annulent identiquement sur le sous-groupe $H(R)$ de $G(R)$ et donc en particulier au point e_R . On a ainsi $\overline{f_i}(s) = 0$ pour tout $i \in \{1, \dots, n\}$, d'où $\overline{f}(s) = 0$ pour tout élément f de \mathfrak{J} puisque f_1, \dots, f_n engendrent cet idéal, et finalement $s \in H(R)$.

Réciproquement, quels que soient $f \in \mathfrak{J}$ et $s \in H(R)$, la fonction $\overline{f}(\cdot)$ s'annule identiquement sur $H(R')$ pour toute R -algèbre R' ; on a donc $\rho_R(s, f) \in \mathfrak{J} \otimes_k R$ (lemme 3.3.2). Appliquant ceci avec $f \in W = V \cap \mathfrak{J}$, on en déduit que $\rho_R(s, f)$ appartient à $(V \otimes_k R) \cap (\mathfrak{J} \otimes_k R)$, donc à $(V \cap \mathfrak{J}) \otimes_k R = W \otimes_k R$ en vertu du lemme ci-dessous. Ainsi, $s \in \text{Stab}_G(W)$.

Nous venons d'établir l'identité $H(R) = \text{Stab}_G(W)(R)$ pour toute k -algèbre R , donc $H = \text{Stab}_G(W)$. □

Lemme 3.3.3 — Soit V un k -espace vectoriel et soient W, W' deux sous-espaces vectoriels de V . Pour toute k -algèbre R , $(W \otimes_k R) \cap (W' \otimes_k R) = (W \cap W') \otimes_k R$.

Démonstration. Posons $L = W \cap W'$. Partant d'une base de L , nous pouvons la compléter en une base de $W + W'$ en lui ajoutant une base d'un supplémentaire de L dans W et celle d'un supplémentaire de L

dans W' , puis compléter la famille libre obtenue en une base $(e_i)_{i \in I}$ de V . On dispose par construction de deux sous-ensembles J et J' de I tels que les familles $(e_i)_{i \in J}$, $(e_i)_{i \in J'}$ et $(e_i)_{i \in J \cap J'}$ soient des bases de W , W' et L respectivement.

Ceci fait, un élément de $V \otimes_k R$ s'écrit de manière unique sous la forme $\sum_{i \in I} e_i \otimes \lambda_i$ avec $\lambda_i \in R$. S'il appartient à $W \otimes_k R$ (resp. à $W' \otimes_k R$), alors $\lambda_i = 0$ pour tout $i \in I - J$ (resp. $\lambda_i = 0$ pour tout $i \in I - J'$) et donc $(W \otimes_k R) \cap (W' \otimes_k R) = (W \cap W') \otimes_k R$. \square

(3.3.2) On peut préciser la seconde assertion du théorème de Chevalley en imposant que le sous-espace vectoriel W soit de dimension 1.

Soit V un k -espace vectoriel de dimension finie n . On dispose pour tout nombre entier $d \in \{1, \dots, n\}$ d'une représentation linéaire naturelle λ_d de GL_V dans la d -ème puissance extérieure $\Lambda^d(V)$ de V : quelle que soient la k -algèbre R et l'automorphisme R -linéaire g de $V \otimes_k R$, $\lambda_{d,R}(g)$ est l'automorphisme R -linéaire de $\Lambda^d(V) \otimes_k R = \Lambda^d(V \otimes_k R)$ qui envoie un d -vecteur de la forme $v_1 \wedge \dots \wedge v_d$ sur le d -vecteur $g(v_1) \wedge \dots \wedge g(v_d)$.

Si l'on fixe une base $(e_1, \dots, e_n)_{1 \leq i \leq n}$ de V sur k , on obtient une base du k -espace vectoriel $\Lambda^d(V)$ en considérant tous les d -vecteurs $e_\varphi = e_{\varphi(1)} \wedge \dots \wedge e_{\varphi(d)}$, où φ parcourt l'ensemble des applications strictement croissantes de $\{1, \dots, d\}$ dans $\{1, \dots, n\}$. L'homomorphisme $\lambda_{d,R}$ associe alors à un automorphisme R -linéaire g de $V \otimes_k R$, de matrice $M = (m_{ij})$ dans la base $(e_i \otimes 1)$, l'automorphisme R -linéaire de $\Lambda^d(V \otimes_k R)$ dont la matrice $\Lambda^d M = (x_{\varphi, \psi})$ dans la base $(e_\varphi \otimes 1)$ est définie par la condition suivante :

$$x_{\varphi, \psi} = \det (m_{\varphi(i)\psi(j)})_{1 \leq i, j \leq d}.$$

(C'est la matrice des déterminants mineurs d'ordre d de la matrice M .)

Proposition 3.3.4 — Soit W un sous-espace vectoriel de V de dimension d . Le sous-groupe $\text{Stab}(W)$ de GL_V est le stabilisateur de la droite $\Lambda^d(W)$ de $\Lambda^d(V)$.

Démonstration. Fixons une base de V , disons (e_1, \dots, e_n) , et considérons la base (e_φ) de $\Lambda^d(V)$ qui lui correspond. Posons $q = \binom{n}{d}$. En utilisant ces bases, nous sommes ramenés à démontrer l'assertion suivante : pour toute k -algèbre R et toute matrice $M \in GL_n(R)$, les conditions

- (a) la matrice M est de la forme $\left(\begin{array}{c|c} A & B \\ \hline 0 & D \end{array} \right)$ avec $A \in GL_d(R)$, $B \in M_{d, n-d}(R)$ et $D \in GL_{n-d}(R)$;
- (b) la matrice $\Lambda^d M$ est de la forme $\left(\begin{array}{c|c} a & P \\ \hline 0 & Q \end{array} \right)$ avec $a \in R^\times$, $P \in M_{1, q-1}(R)$ et $Q \in GL_{q-1}(R)$

sont équivalentes.

Il est clair que (a) implique (b). Considérons réciproquement une matrice $M = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array} \right)$, avec $A \in M_d(R)$, $B \in M_{d, n-d}(R)$, $C \in M_{n-d, d}(R)$ et $D \in M_{n-d}(R)$, telle que $\Lambda^d M$ soit de la forme envisagée en (b). La matrice A est inversible car $\det(A) = a \in R^\times$. Si l'on pose $N = \left(\begin{array}{c|c} A^{-1} & 0 \\ \hline 0 & I_{n-d} \end{array} \right)$, alors

$$NM = \left(\begin{array}{c|c} I_d & A^{-1}B \\ \hline C & D \end{array} \right), \quad \Lambda^d N = \left(\begin{array}{c|c} a^{-1} & P' \\ \hline 0 & Q' \end{array} \right) \quad \text{et} \quad \Lambda^d(NM) = (\Lambda^d N)(\Lambda^d M) = \left(\begin{array}{c|c} 1 & P'' \\ \hline 0 & Q'' \end{array} \right)$$

avec $P', P'' \in M_{1, q-1}(R)$ et $Q', Q'' \in GL_{q-1}(R)$; nous pouvons par suite supposer $A = I_d$. Sous cette hypothèse, le coefficient M d'indice (i, j) avec $i \in \{d+1, \dots, n\}$ et $j \in \{1, \dots, d\}$ est, au signe près, égal au coefficient de $\Lambda^d M$ d'indice (φ, φ_0) , où φ_0 est l'injection canonique de $\{1, \dots, d\}$ dans $\{1, \dots, n\}$ et φ est l'application de $\{1, \dots, d\}$ dans $\{1, \dots, n\}$ définie par

$$\varphi(\ell) = \begin{cases} \ell & \text{si } \ell < j \\ \ell + 1 & \text{si } j \leq \ell \leq d - 1 \\ i & \text{si } \ell = d \end{cases}$$

On obtient ainsi $C = 0$. □

Corollaire 3.3.5 — Soit G un groupe algébrique sur k et soit H un sous-groupe de G . Il existe un espace vectoriel V de dimension finie et une représentation linéaire $\rho : G \rightarrow \mathrm{GL}_V$ induisant un isomorphisme de G sur un sous-groupe de GL_V tels que H soit le stabilisateur d'une droite de V .

Démonstration. Considérons un k -espace vectoriel V' de dimension finie et une représentation linéaire $\rho' : G \rightarrow \mathrm{GL}_{V'}$ induisant un isomorphisme de G sur un sous-groupe de $\mathrm{GL}_{V'}$ tels que H soit le stabilisateur d'un sous-espace vectoriel W' de V' (théorème 3.1.1). D'après la proposition précédente, H est le sous-groupe de G stabilisant la droite $\Lambda^d(W')$ de $\Lambda(V')$ dans la représentation linéaire $\Lambda^d \rho = \lambda_d \circ \rho' : G \rightarrow \mathrm{GL}_{\Lambda^d(V')}$.

Posons $V = V' \oplus \Lambda^d(V')$ et soit W la droite $\Lambda^d(W')$ dans V . La représentation $\rho = \rho' \oplus \Lambda^d \rho$ de G dans GL_V induit un isomorphisme de G sur un sous-groupe de GL_V et H est le stabilisateur de la droite W . □

4. DÉCOMPOSITION DE JORDAN

4.1. Introduction

Soit V un espace vectoriel de dimension finie sur un corps k supposé algébriquement clos. Il est bien connu que tout endomorphisme f de V s'écrit d'une manière et d'une seule sous la forme $f = d + n$, où d et n sont deux endomorphismes de V qui commutent, d est diagonalisable et n est nilpotent. C'est la *décomposition de Jordan additive* de f , que l'on établit aisément en considérant les sous-espaces caractéristiques de f .

Lorsque f est inversible, cette décomposition peut s'écrire de manière multiplicative : l'endomorphisme d est en effet inversible (car f et d ont le même spectre),

$$f = du = ud$$

avec $u = \mathrm{id} + d^{-1}n$, et la nilpotence de n se traduit par le fait que toutes les valeurs propres de u sont égales à 1.

Définition 4.1.1 — Soit k un corps et soit V un k -espace vectoriel de dimension finie. Un endomorphisme f de V est dit

- (i) unipotent, si toutes ses valeurs propres sont égales à 1, c'est-à-dire si l'endomorphisme $f - \mathrm{id}$ est nilpotent ;
- (ii) semi-simple, s'il est diagonalisable sur une clôture algébrique de k .

On rappelle qu'un polynôme P à coefficient dans un corps k est dit *séparable* si ses racines (dans une clôture algébrique de k) sont simples ; cela revient à dire que P et son polynôme dérivé P' sont premiers entre eux. On rappelle également qu'un corps est dit *parfait* si tout polynôme irréductible est séparable. Un corps algébriquement clos est parfait (trivial) ; tout corps de caractéristique zéro est parfait tandis qu'un corps k de caractéristique $p > 0$ est parfait si et seulement si l'endomorphisme de Frobenius ($k \rightarrow k, x \mapsto x^p$) est surjectif ; en particulier, les corps finis sont parfaits.

Proposition 4.1.2 — Soit k un corps et soit V un k -espace vectoriel de dimension finie. Pour qu'un endomorphisme de V soit semi-simple, il faut et il suffit que son polynôme minimal soit séparable.

Démonstration. Soit f un endomorphisme de V et soit \bar{k} une clôture algébrique de k . Il est facile de voir que l'endomorphisme $f \otimes \mathrm{id}$ de $V \otimes_k \bar{k}$ a le même polynôme minimal que f . Considérons en effet la suite exacte de k -espaces vectoriels définissant le polynôme minimal m de f , soit

$$0 \longrightarrow k[X] \xrightarrow{m} k[X] \xrightarrow{t} \mathrm{End}(V),$$

où $\iota(P) = P(u)$. Cette suite reste exacte après tensorisation par \bar{k} ; par ailleurs, l'application canonique de $\text{End}(V) \otimes_k \bar{k}$ dans $\text{End}(V \otimes_k \bar{k})$ est un isomorphisme, car tout endomorphisme de $V \otimes_k \bar{k}$ est une combinaison \bar{k} -linéaire d'endomorphismes de V (c'est évident du point de vue matriciel). Remplaçant $\text{End}(V) \otimes_k \bar{k}$ par $\text{End}(V \otimes_k \bar{k})$ dans la suite exacte

$$0 \longrightarrow \bar{k}[X] \xrightarrow{m} \bar{k}[X] \xrightarrow{\iota \otimes \text{id}} \text{End}(V) \otimes_k \bar{k},$$

il en découle que m engendre le noyau de l'application

$$\bar{k}[X] \rightarrow \text{End}(V \otimes_k \bar{k}), \quad P \mapsto P(f \otimes \text{id})$$

et c'est donc bien le polynôme minimal de $f \otimes \text{id}$.

La conclusion s'obtient en utilisant le fait que l'endomorphisme $f \otimes \text{id}$ est diagonalisable si et seulement si les racines de son polynôme minimal sont simples. \square

Nous sommes maintenant en mesure d'énoncer le théorème principal de ce chapitre.

Théorème 4.1.3 (Décomposition de Jordan) — Soit k un corps parfait et soit G un groupe algébrique sur k . Tout élément g de $G(k)$ s'écrit d'une manière et d'une seule sous la forme $g = g_s g_u$, où g_s et g_u sont des éléments de $G(k)$ satisfaisant aux deux conditions suivantes :

- (i) $g_s g_u = g_u g_s$;
- (ii) pour toute représentation linéaire de dimension finie $\rho : G \rightarrow \text{GL}_V$, $\rho_k(g_s)$ (resp. $\rho_k(g_u)$) est un automorphisme semi-simple (resp. unipotent) de V .

Ce théorème n'est certainement pas évident à première vue : étant donné une représentation linéaire de dimension finie $\rho : G \rightarrow \text{GL}_V$ et un élément g de $G(k)$,

- $\rho_k(g) \in \text{GL}(V)$ s'écrit comme le produit de deux automorphismes de V qui commutent, l'un semi-simple et l'autre unipotent, mais la construction de ceux-ci repose sur l'étude des sous-espaces caractéristiques de $\rho_k(g)$ et il n'est pas clair que l'on obtienne des éléments du sous-groupe $\rho_k(G(k))$ de $\text{GL}(V)$;
- le changement de représentation linéaire pourrait ne pas préserver le caractère semi-simple (resp. unipotent) de l'image de g .

La démonstration que l'on va donner est celle que l'on trouve dans le séminaire Chevalley (Exposé 4, paragraphe 4.4) ; elle repose sur une caractérisation des éléments unipotents (resp. semi-simples) de $\text{GL}(V)$ ne faisant pas intervenir leurs valeurs propres.

Remarque — L'hypothèse « corps parfait » est nécessaire ainsi que le montre le contre-exemple classique suivant. On suppose k de caractéristique 2 non parfait et on considère un élément a de $k - k^2$. Désignant par α la racine carrée de a dans une clôture algébrique \bar{k} de k , l'identité

$$\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} 0 & \alpha \\ \alpha^{-1} & 0 \end{pmatrix}$$

est la décomposition de Jordan du membre de gauche dans $\text{GL}_2(\bar{k})$. S'il existait une telle décomposition dans $\text{GL}_2(k)$, la composante semi-simple serait l'homothétie αI_2 et α appartiendrait à k ...

4.2. Éléments unipotents

Proposition 4.2.1 — Soit V un espace vectoriel de dimension finie sur un corps k et soit $g \in \text{GL}(V)$.

1. Si $\text{car}(k) = p > 0$, les conditions suivantes sont équivalentes :

- (i) g est unipotent ;
- (ii) il existe un entier $N \geq 0$ tel que $g^{p^N} = 1$.

2. Si $\text{car}(k) = 0$, les conditions suivantes sont équivalentes :

- (i) g est unipotent ;
- (ii) il existe un homomorphisme $u : \mathbb{G}_a \rightarrow G$ et un élément t de $\mathbb{G}_a(k) = k$ tel que $g = u_k(t)$.

Démonstration. 1. Traitons tout d'abord le cas d'un corps de caractéristique $p > 0$.

Si g est un automorphisme unipotent de V , l'endomorphisme $g - \text{id}$ est nilpotent et donc $(g - \text{id})^{p^N} = 0$ si l'entier N est suffisamment grand ; on obtient alors $g^{p^N} - \text{id} = 0$ et ainsi g est bien d'ordre une puissance de p .

Réciproquement, s'il existe un entier $N \geq 0$ tel que $g^{p^N} = \text{id}$, le polynôme minimal de g divise $X^{p^N} - 1 = (X - 1)^{p^N}$ et le spectre de g est réduit à 1.

2. Traitons maintenant le cas d'un corps de caractéristique nulle.

Supposons que g soit unipotent et posons $n = g - \text{id}$. Le polynôme $\sum_{m \geq 1} (-1)^{m+1} \frac{n^m}{m}$ définit un endomorphisme de V , que l'on note $\text{Log}(g)$; ce dernier est nilpotent puisqu'il s'agit d'une somme d'endomorphismes nilpotents qui commutent. L'homomorphisme de foncteurs $u : \mathbb{G}_a \rightarrow \text{GL}_V$ défini par

$$u_{\mathbb{R}}(t) = \sum_{m \geq 0} \frac{t^m}{m!} \text{Log}(g)^m$$

pour toute k -algèbre \mathbb{R} et tout $t \in \mathbb{G}_a(\mathbb{R}) = \mathbb{R}$ est un homomorphisme de groupes algébriques car, pour toute \mathbb{Q} -algèbre A , la série formelle

$$\exp(X) = \sum_{m \geq 0} \frac{X^m}{m!} \in A[[X]]$$

vérifie l'identité $\exp(X + Y) = \exp(X)\exp(Y)$. Enfin, comme $\exp(\text{Log}(Y)) = Y$ dans $k[[Y]]$,

$$g = u_k(1)$$

appartient bien à l'image de $\mathbb{G}_a(k)$.

Considérons réciproquement un homomorphisme de groupes algébriques $u : \mathbb{G}_a \rightarrow \text{GL}_V$ et vérifions que, pour tout $t \in k = \mathbb{G}_a(k)$, l'automorphisme $u_k(t)$ est unipotent. Comme il s'agit d'établir que toutes les valeurs propres de $u_k(t)$ sont égales à 1, il est loisible de remplacer k par une clôture algébrique et donc de supposer que le corps k est algébriquement clos. L'image de u_k étant un groupe commutatif d'automorphismes de V , il existe une base (e_1, \dots, e_n) de V trigonalisant simultanément tous ces automorphismes. Chacun d'entre eux induit un automorphisme de la droite vectorielle $V_i = \text{Vect}(e_1, \dots, e_i) / \text{Vect}(e_1, \dots, e_{i-1}) = k\bar{e}_i$ et il existe donc une application $\chi_i : k \rightarrow k^\times$ telle que

$$u_k(t)\bar{e}_i = \chi_i(t)\bar{e}_i$$

pour tout $t \in k$. L'application χ_i est clairement un homomorphisme du groupe additif de k dans son groupe multiplicatif. Il s'agit en outre d'une application *polynomiale* : en effet, si l'on utilise la base (e_1, \dots, e_n) pour identifier GL_V avec GL_n et que l'on note P_i le polynôme $u^*(X_{ii}) \in k[T]$, alors $\chi_i(t) = P_i(t)$ pour tout $t \in k$.

Le polynôme P_i ne s'annulant pas, il est constant puisque k est algébriquement clos ; comme en outre $P_i(0) = 1$, nous obtenons $P_i = 1$. Ainsi, $u_k(t)\bar{e}_i = \bar{e}_i$ pour tout $t \in k$ et les matrices des automorphismes $u_k(t)$ sont donc triangulaires supérieures avec des coefficients diagonaux tous égaux à 1. Par conséquent, les automorphismes $u_k(t)$ sont tous unipotents. \square

La proposition précédente s'étend aisément à un groupe algébrique G quelconque.

Proposition 4.2.2 — Soit k un corps et soit G un groupe algébrique sur k . Pour tout élément g de $G(k)$, les conditions suivantes sont équivalentes :

- (i) pour toute représentation linéaire de dimension finie $\rho : G \rightarrow \text{GL}_V$, l'automorphisme $\rho_k(g)$ est unipotent ;
- (ii) il existe une représentation linéaire fidèle de dimension finie $\rho : G \rightarrow \text{GL}_V$ telle que l'automorphisme $\rho(g)$ soit unipotent ;
- (iiia) si $\text{car}(k) = p > 0$, il existe un entier $N \geq 0$ tel que $g^{p^N} = e$;
- (iiib) si $\text{car}(k) = 0$, il existe un homomorphisme $u : \mathbb{G}_a \rightarrow G$ tel que g appartienne à l'image de u_k .

Démonstration. L'implication (i) \Rightarrow (ii) est triviale et les implications (iiia) \Rightarrow (i), (iiib) \Rightarrow (i) sont des conséquences immédiates de la proposition précédente.

Supposons finalement qu'il existe une représentation linéaire fidèle de dimension finie $\rho : G \hookrightarrow \text{GL}_V$ telle que l'automorphisme $\rho_k(g)$ soit unipotent. Les conditions (iiia) et (iiib) étant trivialement vérifiées lorsque $g = e$, nous pouvons supposer $g \neq e$.

Si $\text{car}(k) = p > 0$, il existe un entier $n \geq 0$ tel que $\rho_k(g)^{p^n} = \text{id}_V$ donc $g^{p^n} = e$ puisque l'homomorphisme ρ_k est injectif.

Si $\text{car}(k) = 0$, il existe un homomorphisme $u : \mathbb{G}_a \rightarrow \text{GL}_V$ ainsi qu'un élément t de $\mathbb{G}_a(k) = k$ tels que $g = u_k(t)$. Considérons alors le diagramme commutatif

$$\begin{array}{ccc}
 & & \mathbb{G}_a \\
 & \nearrow i & \searrow u \\
 G \times_{\text{GL}_V} \mathbb{G}_a & & \text{GL}_V \\
 & \searrow j & \nearrow \rho \\
 & & G
 \end{array}$$

définissant le produit fibré $H = G \times_{\text{GL}_V} \mathbb{G}_a$ (cf. 2.3.3) ; l'homomorphisme ρ faisant de G un sous-groupe de GL_V , l'homomorphisme i fait de H un sous-groupe de \mathbb{G}_a . En outre, l'élément (g, t) de $H(k)$ étant distinct de l'élément neutre puisque $g \neq e$, H n'est pas le sous-groupe 0 réduit à un élément. Dans ces conditions, il découle de l'hypothèse $\text{car}(k) = 0$ et du lemme ci-dessous que i est un isomorphisme. Désignant alors par v l'homomorphisme $j \circ i^{-1}$ de \mathbb{G}_a dans G , $\rho_k(v_k(t)) = u_k(t) = \rho_k(g)$ et donc $v_k(t) = g$ puisque l'homomorphisme ρ_k est injectif. \square

Lemme 4.2.3 — Soit k un corps de caractéristique nulle. Le seul sous-groupe strict de \mathbb{G}_a est le sous-groupe 0 réduit à un élément.

Démonstration. Considérons un sous-groupe H de \mathbb{G}_a et soit $I = (P)$ l'idéal de $k[T]$ le définissant. Désignant par \bar{k} une clôture algébrique de k ,

$$H(\bar{k}) = \{t \in \bar{k} \mid P(t) = 0\}$$

est un sous-groupe de \bar{k} . Si $H(\bar{k})$ contient un élément non nul t de k , alors $H(\bar{k})$ contient le sous-groupe $\mathbb{Z}t$; ce dernier étant infini puisque k est de caractéristique nulle, $P = 0$ et donc $H = \mathbb{G}_a$. Par conséquent, si le sous-groupe H est strict, alors $H(\bar{k}) = \{0\}$ et $P = T^n$ pour un certain entier $n \geq 1$.

Il est nécessaire de faire intervenir la bigèbre $k[T]$ de \mathbb{G}_a pour conclure. Que H soit un sous-groupe de \mathbb{G}_a équivaut aux conditions

$$\Delta(I) \subset I \otimes_k k[T] + k[T] \otimes_k I, \quad 0^*(I) = 0 \quad \text{et} \quad \iota^*(I) \subset I.$$

Les deux secondes sont vérifiées lorsque $I = (T^n)$; pour que la première le soit, il faut et il suffit que l'élément $(1 \otimes T + T \otimes 1)^n$ de $k[T] \otimes_k k[T]$ s'écrive sous la forme $\sum_{p,q \geq 0} a_{pq} (1 \otimes T)^p (T \otimes 1)^q$ avec $a_{pq} = 0$ si $p < n$ et $q < n$. Comme

$$(1 \otimes T + T \otimes 1)^n = (1 \otimes T)^n + n(1 \otimes T)^{n-1}(T \otimes 1) + \dots + n(1 \otimes T)(T \otimes 1)^{n-1} + (T \otimes 1)^n,$$

il découle de nouveau de l'hypothèse $\text{car}(k) = 0$ que ceci n'est possible qu'avec $n = 1$. Ainsi, $I = (T)$ et le seul sous-groupe strict de \mathbb{G}_a est le sous-groupe 0 réduit à un élément. \square

Définition 4.2.4 — Soit G un groupe algébrique sur un corps k . Un élément g de $G(k)$ est dit unipotent s'il satisfait à l'une des conditions équivalentes suivantes :

- (i) il existe une représentation linéaire fidèle de dimension finie $\rho : G \rightarrow \text{GL}_V$ telle que l'automorphisme $\rho_k(g)$ soit unipotent ;
- (ii) si $\text{car}(k) = p > 0$, il existe un entier $N \geq 0$ tel que $g^{p^N} = e$;

(iib) si $\text{car}(k) = 0$, il existe un homomorphisme $u : \mathbb{G}_a \rightarrow G$ et un élément t de $\mathbb{G}_a(k) = k$ tel que $u_k(t) = g$.

Il est enfin évident que les éléments unipotents sont préservés par tout homomorphisme de groupes algébriques.

Proposition 4.2.5 — Soit $f : G \rightarrow H$ un homomorphisme de groupes algébriques sur un corps k . Si $g \in G(k)$ est unipotent, alors $f(g)$ est unipotent.

4.3. Groupes diagonalisables et éléments semi-simples

(4.3.1) Considérons un groupe algébrique G sur un corps k .

Définition 4.3.1 — Un caractère de G est un homomorphisme $\chi : G \rightarrow \mathbb{G}_m$.

L'ensemble $X(G)$ des caractères de G est naturellement muni d'une structure de *groupe abélien* (noté additivement) : si χ et ψ sont deux caractères de G , $\chi + \psi$ est le caractère défini par

$$(\chi + \psi)_R(g) = \chi_R(g)\psi_R(g)$$

pour toute k -algèbre R et tout élément g de $G(R)$; l'élément neutre 0 est le caractère trivial, défini par $0_R(g) = 1 \in R^\times = \mathbb{G}_m(R)$.

Exemples — 1. Le groupe additif \mathbb{G}_a n'a pas de caractère non trivial en vertu de la proposition 2.2.3.
2. Le déterminant $\det : \text{GL}_n \rightarrow \mathbb{G}_m$ est un caractère de GL_n .

Proposition 4.3.2 — Si A désigne la bigèbre de G , le groupe $X(G)$ des caractères de G est naturellement en bijection avec le sous-groupe de A^\times constitué des éléments a tels que $\Delta(a) = a \otimes a$.

Démonstration. Un caractère de G est par définition un homomorphisme $\chi : G \rightarrow \mathbb{G}_m$ et donc correspond à un homomorphisme de k -bigèbres $\chi^* : k[X, X^{-1}] \rightarrow A$. Ce dernier est entièrement déterminé par l'élément $a = \chi^*(X)$ dans A^\times , lequel doit satisfaire aux conditions suivantes :

$$\Delta(a) = a \otimes a, \quad e^*(a) = 1 \quad \text{et} \quad \iota^*(a) = a^{-1}.$$

Il découle directement des axiomes des bigèbres que les deux dernières conditions sont des conséquences de la première : quel que soit l'élément $a \in A$ tel que $\Delta(a) = a \otimes a$,

$$a = [(\text{id}_A \otimes e^*) \circ \Delta](a) = a \otimes e^*(a) \quad \text{et} \quad e^*(a) = [\text{mult} \circ (\text{id}_A \otimes \iota^*) \circ \Delta](a) = a\iota^*(a),$$

donc $e^*(a) = 1$ et $\iota^*(a) = a^{-1}$. □

Corollaire 4.3.3 — Pour tout nombre entier $d \geq 1$, le groupe des caractères du groupe \mathbb{G}_m^d est un groupe abélien libre de rang d dont une base est formée des éléments X_1, \dots, X_d de $k[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$.

Démonstration — Les éléments inversibles de $k[X_1^{\pm 1}, \dots, X_d^{\pm 1}]$ sont les éléments de la forme $a = \lambda X_1^{v_1} \dots X_d^{v_d}$ avec $\lambda \in k^\times$ et $v_1, \dots, v_d \in \mathbb{Z}$. La condition $\Delta(a) = a \otimes a$ est vérifiée si et seulement si $\lambda = 1$, de sorte que si l'on désigne par χ_i le caractère de \mathbb{G}_m^d tel que $\chi_i^*(X) = X_i$, alors l'application $(\mathbb{Z}^d \rightarrow X(G), \underline{v} \mapsto v_1\chi_1 + \dots + v_d\chi_d)$ est un homomorphisme de groupes surjectif. L'injectivité est évidente : étant donné $\underline{v} \in \mathbb{Z}^d$ distinct de 0 , il existe $i \in \{1, \dots, d\}$ tel que $v_i \neq 0$ et, quitte à renuméroter les X_i , il est loisible de supposer que l'on a $v_1 \neq 0$; quel que soit alors l'élément t d'une clôture algébrique \bar{k} de k qui ne soit pas une racine v_1 -ème de l'unité, le caractère $v_1\chi_1 + \dots + v_d\chi_d$ prend la valeur $t^{v_1} \neq 1$ au point $(t, 1, \dots, 1)$ de $\mathbb{G}_m^d(\bar{k}) = \bar{k}^{\times d}$ et il est donc non trivial. □

Proposition 4.3.4 — Si $n \geq 2$, tout caractère de GL_n est une puissance entière du déterminant et le groupe SL_n n'a pas de caractère non trivial.

Démonstration. La première assertion s'obtient aisément en observant que les éléments inversibles de la bigèbre $k[(X_{ij}), \det(X_{ij})^{-1}]$ de GL_n sont les éléments a de la forme $\lambda \det(X_{ij})^m$ avec $\lambda \in k^\times$ et

$m \in \mathbb{Z}$. La condition $\Delta(a) = a \otimes a$ équivaut à $\lambda = 1$, ce qui prouve que les seuls caractères de GL_n sont les puissances entières du déterminant en vertu de la proposition précédente.

La démonstration de la seconde assertion repose sur le fait suivant : si $n \geq 2$ et si K est un corps, le groupe $SL_n(K)$ est engendré par les commutateurs, sauf si $n = 2$ et $K = \mathbb{F}_2$ (voir par exemple dans le *Cours d'algèbre* de Daniel Perrin, éditions Ellipses, IV, Théorème 3.1).

Soit χ un caractère de SL_n . Désignant par \bar{k} une clôture algébrique de k , il découle de ce que l'on vient de dire que l'homomorphisme $\chi_{\bar{k}} : SL_n(\bar{k}) \rightarrow \mathbb{G}_m(\bar{k}) = \bar{k}^\times$ est trivial puisque le groupe k^\times est commutatif. Le caractère χ correspond à un élément a de la bigèbre de SL_n tel que $a - 1$ s'annule identiquement sur $SL_n(\bar{k})$; d'après le *Nullstellensatz* de Hilbert, $a - 1$ est alors un élément nilpotent de A . On vérifie facilement que l'anneau $A = [(X_{ij})]/(\det(X_{ij}) - 1)$ est *réduit* :

- l'homomorphisme

$$A[T, T^{-1}] \rightarrow k[(X_{ij}), T]/(T \det(X_{ij}) - 1)$$

défini en envoyant T sur T , T^{-1} sur $\det(X_{ij})$, X_{11} sur TX_{11} et X_{ij} sur X_{ij} si $(i, j) \neq (1, 1)$ est un isomorphisme, dont l'inverse est donné par $T \mapsto T$, $X_{11} \mapsto T^{-1}X_{11}$ et $X_{ij} \mapsto X_{ij}$ si $(i, j) \neq (1, 1)$;

- l'anneau $k[(X_{ij}), T]/(T \det(X_{ij}) - 1)$ est intègre, car isomorphe à un localisé de l'anneau intègre $k[(X_{ij})]$.

Par suite, $a - 1 = 0$ et χ est donc trivial. \square

(4.3.2) Soit G un groupe algébrique sur un corps k et soit $\rho : G \rightarrow GL_V$ une représentation linéaire de dimension finie. Un *vecteur propre* de ρ est un vecteur $v \neq 0$ dans V tel que, pour toute k -algèbre R et tout élément $g \in V \otimes_k R$, le sous- R -module $R(v \otimes 1)$ de $V \otimes R$ soit stabilisé par l'automorphisme $\rho_R(g)$; il revient au même de demander qu'il existe un élément $\chi_v(g)$ de R^\times tel que

$$\rho_R(g)(v \otimes 1) = \chi_{v,R}(g)(v \otimes 1).$$

On vérifie immédiatement que les applications $\chi_{v,R} : G(R) \rightarrow \mathbb{G}_m(R) = R^\times$ ainsi définies donnent naissance à un caractère $\chi_v : G \rightarrow \mathbb{G}_m$.

Remarque — On sait que la représentation ρ est complètement déterminée par la donnée d'une l'application k -linéaire $\rho^* : V \rightarrow V \otimes_k A$ telle que

$$(\rho^* \otimes \text{id}_A) \circ \rho^* = (\text{id}_V \otimes \Delta) \circ \rho^* \quad \text{et} \quad (\text{id}_V \otimes e^*) \circ \rho^* = \text{id}_V$$

(cf. proposition 3.1.5). De ce point de vue, un vecteur propre de ρ est un vecteur non nul v de V tel que

$$\rho^*(v) = v \otimes a$$

pour un certain $a \in A^\times$. Cet élément a de A est uniquement déterminé : si l'on considère en effet une base (e_1, \dots, e_n) de V telle que $e_1 = v$, alors $V \otimes_k A$ est un A -module libre de base $(e_1 \otimes 1, \dots, e_n \otimes 1)$ et les coordonnées de $\rho^*(v)$ dans cette dernière sont bien définis. En outre,

$$\begin{aligned} v \otimes a \otimes a &= \rho^*(v) \otimes a \\ &= [(\rho^* \otimes \text{id}_A) \circ \rho^*](v) \\ &= [(\text{id}_V \otimes \Delta) \circ \rho^*](v) \\ &= v \otimes \Delta(a) \end{aligned}$$

et donc $\Delta(a) = a \otimes a$.

Définition 4.3.5 — Un groupe algébrique G sur un corps k est dit diagonalisable si, pour toute représentation linéaire de dimension finie $\rho : G \rightarrow GL_V$, l'espace vectoriel V est engendré par des vecteurs propres de ρ .

Cette définition peut se reformuler ainsi : pour toute représentation linéaire de dimension finie $\rho : G \rightarrow GL_V$, il existe une base de V telle que, pour toute k -algèbre R , l'image de l'homomorphisme $\rho_R : G(R) \rightarrow GL_V(R) \simeq GL_n(R)$ soit contenue dans le sous-groupe constitué des matrices diagonales.

Les groupes diagonalisables ont une caractérisation simple en termes de leur bigèbre.

Proposition 4.3.6 — Soit G un groupe algébrique sur k de bigèbre A . Pour que G soit diagonalisable, il faut et il suffit que la k -algèbre A soit engendrée par les caractères, c'est-à-dire les éléments a de A^\times tels que $\Delta(a) = a \otimes a$.

Démonstration. Supposons que G soit diagonalisable et soit $\rho : G \rightarrow GL_V$ une représentation linéaire fidèle de dimension finie. Puisque V est engendré par les vecteurs propres de ρ , il existe une base (e_1, \dots, e_n) de V formée de vecteurs propres de ρ . Utilisant cette base pour identifier GL_V et GL_n , l'homomorphisme $G \rightarrow GL_n$ déduit de ρ induit un isomorphisme entre G et un sous-groupe du groupe des matrices diagonales, lui-même isomorphe au groupe \mathbb{G}_m^n . Par suite, la bigèbre A de G est isomorphe à un quotient de la bigèbre $k[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ de \mathbb{G}_m^n et, comme cette dernière est engendrée par les $2n$ caractères $X_i^{\pm 1}$, A est engendrée par des caractères (les images des $X_i^{\pm 1}$).

Supposons réciproquement que A soit engendrée par des caractères. Comme un produit de caractères est encore un caractère, A est également engendré par des caractères en tant que k -espace vectoriel et on peut donc considérer une base $(a_i)_{i \in I}$ de A sur k constituée de caractères.

Soit alors $\rho : G \rightarrow GL_V$ une représentation linéaire de dimension finie de G et soit $\rho^* : V \rightarrow V \otimes_k A$ l'application k -linéaire qui lui correspond. Étant donné un vecteur $v \in V$, il existe une unique famille $(v_i)_{i \in I}$ de vecteurs de V presque tous nuls telle que

$$\rho^*(v) = \sum_{i \in I} v_i \otimes a_i.$$

En vertu de l'identité $(\rho^* \otimes \text{id}_A) \circ \rho^* = (\text{id}_V \otimes \Delta) \circ \rho^*$,

$$\begin{aligned} \sum_{i \in I} \rho^*(v_i) \otimes a_i &= [(\rho^* \otimes \text{id}_A) \circ \rho^*](v) \\ &= [(\text{id}_V \otimes \Delta) \circ \rho^*](v) \\ &= \sum_{i \in I} v_i \otimes \Delta(a_i) \\ &= \sum_{i \in I} v_i \otimes a_i \otimes a_i \end{aligned}$$

et donc

$$\rho^*(v_i) = v_i \otimes a_i$$

pour tout i . Il découle de ceci que v est contenu dans un sous-espace vectoriel de V engendré par des vecteurs propres de ρ , puis que ces derniers engendrent V . Ainsi, le groupe G est diagonalisable. \square

Corollaire 4.3.7 — 1. Pour tout entier $d \geq 1$, le groupe \mathbb{G}_m^d est diagonalisable.

2. Pour tout entier $n \geq 1$ premier à la caractéristique de k , le groupe μ_n est diagonalisable.

3. Tout sous-groupe d'un groupe diagonalisable est diagonalisable.

4. Le produit de deux groupes diagonalisables est diagonalisable.

Démonstration. 1. Le groupe \mathbb{G}_m^d est diagonalisable car sa bigèbre $k[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ est engendrée par les $2n$ caractères $X_i^{\pm 1}$.

2. Si n est premier à la caractéristique, le groupe μ_n est diagonalisable car sa bigèbre $k[X]/(X^n - 1)$ est engendrée par le caractère X . Noter que le groupe μ_n n'est pas diagonalisable si $p = \text{car}(k)$ divise n : en effet, si l'on écrit n sous la forme $n = p^\alpha n'$ avec $\alpha \geq 1$ et $(n', p) = 1$ et si l'on désigne par \bar{k} une clôture algébrique de k , la \bar{k} -algèbre

$$\bar{k} \otimes_k k[X]/(X^n - 1) = \bar{k}[X]/((X^{n'} - 1)^{p^\alpha}) \cong \bigoplus_{\xi \in \mu_{n'}(\bar{k})} \bar{k}[X]/(X - \xi)^{p^\alpha} \simeq \bigoplus_{\xi \in \mu_{n'}(\bar{k})} \bar{k}[X]/(X^{p^\alpha})$$

n'est clairement pas engendrée par ses éléments inversibles.

3. La bigèbre B d'un sous-groupe H d'un groupe algébrique G est un quotient de la bigèbre A de G . Comme la projection canonique $A \rightarrow B$ transforme les caractères en caractères, H est diagonalisable si G l'est.

4. Si G et H sont deux groupes algébriques diagonalisables de bigèbres respectives A et B , alors $G \times H$ est le groupe algébrique de bigèbre $A \otimes_k B$, la comultiplication étant définie par $\Delta(a \otimes b) = \Delta_G(a) \otimes \Delta_H(b)$. Par suite, si $(a_i)_{i \in I}$ et $(b_j)_{j \in J}$ sont des familles de caractères de G et H respectivement engendrant les k -algèbres A et B , alors la k -algèbre $A \otimes B$ est engendrée par les caractères $a_i \otimes b_j$ et donc $G \times H$ est diagonalisable. \square

Proposition 4.3.8 — Soit G un groupe algébrique sur un corps k . Pour que G soit diagonalisable, il faut et il suffit qu'il soit isomorphe à un groupe de la forme

$$\mathbb{G}^d \times \mu_{n_1} \times \dots \times \mu_{n_r}$$

avec $d \geq 0$ et n_1, \dots, n_r des entiers premiers à la caractéristique de k tels que $n_{i+1} | n_i$ pour tout i . En outre, d et le r -uplet (n_1, \dots, n_r) sont uniquement déterminés.

Démonstration. Les groupes algébriques de la forme indiquée sont diagonalisables en vertu du corollaire précédent.

Considérons réciproquement un groupe algébrique diagonalisable G . Le groupe $X(G)$ des caractères de G est de type fini. En effet, on a vu au cours de la démonstration de la proposition 4.3.6 que la bigèbre A de G est isomorphe à un quotient de la bigèbre $k[X_1^{pm1}, \dots, X_N^{\pm 1}]$ de \mathbb{G}_m^N pour un entier $N \geq 1$ convenable. Il en découle que la k -algèbre A est engendrée par les caractères $a_1^{\pm 1}, \dots, a_N^{\pm 1}$; en particulier, tout caractère de A s'écrit sous la forme d'une combinaison linéaire finie des caractères $a_1^{v_1} \dots a_N^{v_N}$, $v \in \mathbb{Z}^N$. Vu l'indépendance linéaire des caractères (lemme ci-dessous), on en déduit que tout caractère de G est de la forme $a_1^{v_1} \dots a_N^{v_N}$ pour un certain $v \in \mathbb{Z}^N$ et le groupe $X(G)$ est donc bien de type fini.

Il découle également de ce que l'on vient de dire que la bigèbre A est complètement déterminée par le groupe $X(G)$: notant a_χ l'élément de A correspondant au caractère $\chi \in X(G)$,

$$A = \bigoplus_{\chi \in X(G)} ka_\chi$$

en tant que k -espace vectoriel et

$$a_\chi \cdot a_\psi = a_{\chi+\psi}, \quad \Delta(a_\chi) = a_\chi \otimes a_\chi, \quad e^*(a_\chi) = 1, \quad \iota^*(a_\chi) = a_\chi^{-1} = a_{-\chi}$$

pour tous $\chi, \psi \in X(G)$.

Il reste à appliquer le théorème de structure des groupes abéliens de type fini : il existe un entier $d \geq 0$ et des entiers n_1, \dots, n_r avec $n_{i+1} | n_i$ tels que $X(G)$ soit isomorphe au groupe $\mathbb{Z}^d \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/n_r\mathbb{Z}$; en outre, d et le r -uplet sont uniquement déterminés. Vu la description de la bigèbre A donnée précédemment, celle-ci est isomorphe à

$$\begin{aligned} k[X_1^\pm, \dots, X_d^\pm, X_{d+1}, \dots, X_{d+r}] / (X_{d+1}^{n_1} - 1, \dots, X_{d+r}^{n_r} - 1) \\ = k[X_1^{\pm 1}, \dots, X_d^{\pm 1}] \otimes_k k[X] / (X^{n_1} - 1) \otimes_k \dots \otimes_k k[X] / (X^{n_r} - 1) \end{aligned}$$

et donc $G \simeq \mathbb{G}_m^d \times \mu_{n_1} \times \dots \times \mu_{n_r}$. \square

Lemme 4.3.9 (Indépendance linéaire des caractères) — Soit G un groupe algébrique sur un corps k de bigèbre A . Toute famille $(a_i)_{i \in I}$ de caractères distincts de G est libre dans le k -espace vectoriel A .

Démonstration. Chaque a_i étant inversible, les familles $\{a_i\}$ réduites à un élément sont libres. Considérons alors un sous-ensemble J de I telle que la famille $(a_i)_{i \in J}$ soit libre et maximale. Si $I \neq J$, choisissons $i_0 \in I - J$ et considérons une relation de dépendance linéaire

$$a_{i_0} = \sum_{i \in J} \lambda_i a_i.$$

Appliquant Δ , il vient

$$\begin{aligned} \sum_{i,j \in J} \lambda_i \lambda_j a_i \otimes a_j &= a_{i_0} \otimes a_{i_0} \\ &= \sum_{i \in J} \lambda_i a_i \otimes a_i. \end{aligned}$$

La famille $(a_i \otimes a_j)_{(i,j) \in J^2}$ étant libre dans $A \otimes_k A$, $\lambda_i \lambda_j = 0$ pour tous i, j distincts dans J et il existe donc un unique $i \in J$ tel que $\lambda_i \neq 0$. L'identité $a_{i_0} = \lambda_i a_i$ implique alors $\lambda_i = 1$ par application de e^* , de sorte que $a_{i_0} = a_i$. Par suite, si tous les a_i sont distincts, $J = I$ et le lemme est démontré. \square

(4.3.3) Nous sommes maintenant en mesure de caractériser les automorphismes diagonalisables d'un espace vectoriel de dimension finie.

Proposition 4.3.10 — Soit V un espace vectoriel de dimension finie sur un corps k . Les conditions suivantes sont équivalentes pour tout automorphisme g de V :

- (i) g est diagonalisable ;
- (ii) il existe un groupe algébrique diagonalisable D et homomorphisme $u : D \rightarrow GL_V$ tel que g appartienne à l'image de $D(k)$.

Démonstration. Si g est diagonalisable, il existe une base (e_1, \dots, e_n) de V formée de vecteurs propres de g . Utilisant cette base pour identifier GL_V et GL_n , g appartient donc à $T(k)$, où T est le sous-groupe de GL_V correspondant au sous-groupe des matrices diagonales dans GL_n . Comme $T \simeq \mathbb{G}_m^n$, T est diagonalisable en vertu du corollaire 4.3.7 et l'assertion (ii) est démontrée.

Considérons réciproquement un groupe algébrique diagonalisable D et un homomorphisme $u : D \rightarrow GL_V$. Il existe par hypothèse une base (e_1, \dots, e_n) de V constituée de vecteurs propres de u . Utilisant cette base pour identifier GL_V et GL_n , l'image de u est contenue dans le sous-groupe des matrices diagonales de GL_n ; en particulier, tout élément de l'image de $D(k)$ a une matrice diagonale dans la base (e_1, \dots, e_n) et donc est diagonalisable. \square

Corollaire 4.3.11 — Soit G un groupe algébrique sur un corps k et soit \bar{k} une clôture algébrique de k . Les conditions suivantes sont équivalentes pour tout élément g de $G(k)$:

- (i) quelle que soit la représentation linéaire de dimension finie $\rho : G \rightarrow GL_V$, l'automorphisme $\rho_k(g)$ est semi-simple ;
- (ii) il existe une représentation linéaire fidèle de dimension finie $\rho : G \rightarrow GL_V$ telle que l'automorphisme $\rho_k(g)$ soit semi-simple ;
- (iii) il existe un \bar{k} -groupe algébrique diagonalisable D et un homomorphisme $u : D \rightarrow G \otimes_k \bar{k}$ tel que g appartienne à l'image de $D(\bar{k})$ dans $G(\bar{k})$.

Démonstration. L'implication (i) \Rightarrow (ii) est triviale.

Si $\rho : G \rightarrow GL_V$ est une représentation linéaire fidèle de dimension finie telle que $\rho_k(g)$ soit semi-simple — c'est-à-dire diagonalisable sur \bar{k} — il existe d'après la proposition précédente un \bar{k} -groupe algébrique diagonalisable D et un homomorphisme $u : D \rightarrow GL_{V \otimes_k \bar{k}} = GL_V \otimes_k \bar{k}$ tels que $\rho_{\bar{k}}(g)$ appartienne à l'image de $D(\bar{k})$. Considérons alors le diagramme commutatif

$$\begin{array}{ccc} & & D \\ & \nearrow i & \searrow u \\ (G \otimes_k \bar{k}) \times_{GL_V \otimes_k \bar{k}} D & & GL_V \otimes_k \bar{k} \\ & \searrow v & \nearrow \rho \otimes 1 \\ & & G \otimes_k \bar{k} \end{array}$$

définissant le produit fibré $D' = (G \otimes_k \bar{k}) \times_{\text{GL}_{V \otimes_k \bar{k}}} D$. Comme ρ fait de G un sous-groupe de GL_V , l'homomorphisme i identifie D' à un sous-groupe de D et le groupe D' est donc diagonalisable en vertu du corollaire 4.3.7 ; en outre, il existe par construction un élément h de $D'(\bar{k})$ tel que $\rho_{\bar{k}}(v_{\bar{k}}(h)) = \rho_{\bar{k}}(g)$ dans $\text{GL}(V \otimes_k \bar{k})$, donc tel que $v_{\bar{k}}(h) = g$ puisque l'homomorphisme $\rho_{\bar{k}}$ est injectif. L'assertion (iii) est ainsi établie.

L'implication (iii) \Rightarrow (i) découle directement de la proposition précédente. \square

Définition 4.3.12 — Soit G un groupe algébrique sur un corps k . Un élément g de $G(k)$ est dit semi-simple s'il satisfait aux conditions équivalentes suivantes :

- (i) quelle que soit la représentation linéaire de dimension finie $\rho : G \rightarrow \text{GL}_V$, l'automorphisme $\rho_k(g)$ est semi-simple ;
- (ii) il existe une représentation linéaire fidèle de dimension finie $\rho : G \rightarrow \text{GL}_V$ telle que l'automorphisme $\rho_k(g)$ soit semi-simple ;
- (iii) il existe un \bar{k} -groupe algébrique diagonalisable D et un homomorphisme $u : D \rightarrow G \otimes_k \bar{k}$ tel que g appartienne à l'image de $D(\bar{k})$ dans $G(\bar{k})$.

4.4. Décomposition de Jordan

Après le travail préliminaire que nous venons d'effectuer, le théorème 4.1.3 découle aisément du théorème de Chevalley.

Soit k un corps parfait et soit G un groupe algébrique sur k . La démonstration du théorème 4.1.3 se fait en trois étapes.

Première étape : réduction au cas d'un corps algébriquement clos.

Supposons le théorème 4.1.3 établi pour un corps algébriquement clos. Soit \bar{k} une clôture algébrique de k ; comme k est parfait, l'extension \bar{k}/k est galoisienne.

Étant donné un élément g de $G(k)$, la décomposition de Jordan $g = g'_s g'_u$ dans $G(\bar{k})$ est valable sur une extension galoisienne finie k' de k : en effet, les éléments g'_s et g'_u de $G(\bar{k})$ correspondent à des k -homomorphismes de la bigèbre A de G dans \bar{k} et es images de ces derniers sont contenues dans une même extension finie de k car A est de type fini.

Le groupe de Galois $\Gamma = \text{Gal}(k'/k)$ opère naturellement par automorphismes du groupe $G(k')$ et

$$G(k) = G(k')^\Gamma = \{h \in G(k') \mid \gamma(h) = h\}.$$

Identifions en effet $G(k')$ et $\text{Hom}_{\text{Alg}_k}(A, k')$ et considérons l'action de Γ provenant de son action naturelle sur k' :

$$\gamma(h) = \gamma \circ h$$

pour tout $h \in \text{Hom}_k(A, k')$.

- Étant donnés deux éléments h, h' dans $\text{Hom}_{\text{Alg}_k}(A, k')$, leur produit hh' dans le groupe $G(k')$ correspond à l'homomorphisme composé

$$A \xrightarrow{\Delta} A \otimes_k A \xrightarrow{h \otimes h'} k' \otimes_k k' \xrightarrow{\text{mult}} k'$$

et donc

$$\begin{aligned} \gamma(hh') &= \gamma \circ \text{mult} \circ (h \otimes h') \circ \Delta \\ &= \text{mult} \circ ((\gamma \circ h) \otimes_k (\gamma \circ h')) \circ \Delta \\ &= \gamma(h)\gamma(h') \end{aligned}$$

puisque Γ opère par automorphismes du corps k' .

- Si h est un élément de $\text{Hom}_{\text{Alg}_k}(A, k')$ tel que $\gamma(h) = h$ pour tout $\gamma \in \Gamma$, h est à valeurs dans le sous-corps de k' fixé par Γ , donc dans k .

Pour tout $\gamma \in \Gamma$,

$$g = \gamma(g) = \gamma(g'_s)\gamma(g'_u) = \gamma(g'_u)\gamma(g'_s).$$

Il découle par ailleurs de la proposition 4.2.2 et du corollaire 4.3.11 que les éléments $\gamma(g'_s)$ et $\gamma(g'_u)$ de $G(\bar{k})$ sont respectivement semi-simples et unipotents. Par unicité de la décomposition de Jordan dans $G(\bar{k})$, nous en déduisons $\gamma(g'_s) = g'_s$ et $\gamma(g'_u) = g'_u$ pour tout $\gamma \in \Gamma$. Posant $g_s = g'_s$ et $g_u = g'_u$, nous obtenons par suite une décomposition $g = g_s g_u = g_u g_s$ dans $G(k)$ avec g_s (resp. g_u) semi-simple (resp. unipotent) dans $G(\bar{k})$. Quelle que soit la représentation linéaire de dimension finie $\rho : G \rightarrow \text{GL}_V$, les automorphismes $\rho_k(g_s)$ et $\rho_k(g_u)$ sont respectivement semi-simples et unipotents sur \bar{k} ; ils le sont donc également sur k . Nous avons ainsi établi l'existence d'une décomposition de Jordan dans $G(k)$ et l'unicité vient de l'unicité de cette décomposition dans $G(\bar{k})$.

Il reste à démontrer le théorème 4.1.3 lorsque le corps k est algébriquement clos.

Deuxième étape : le cas $G = \text{GL}_V$.

Il n'y a pratiquement rien à faire. Étant donné $g \in \text{GL}_V(k) = \text{GL}(V)$, on sait (cf. 4.1) qu'il existe un unique couple (g_s, g_u) d'automorphismes de V tels que $g = g_s g_u = g_u g_s$ avec g_s semi-simple et g_u unipotent. Si $\rho : \text{GL}_V \rightarrow \text{GL}_W$ est une représentation linéaire de dimension finie, ceci s'applique également à l'automorphisme $\rho_k(g)$ de W :

$$\rho_k(g) = \rho_k(g)_s \rho_k(g)_u = \rho_k(g)_u \rho_k(g)_s$$

avec $\rho_k(g)_s$ semi-simple et $\rho_k(g)_u$ unipotent uniquement déterminés. En vertu des propositions 4.2.1 et 4.3.10, les automorphismes $\rho_k(g_s)$ et $\rho_k(g_u)$ sont respectivement semi-simples et unipotents; comme

$$\rho_k(g) = \rho_k(g_s) \rho_k(g_u) = \rho_k(g_u) \rho_k(g_s),$$

nous en déduisons $\rho_k(g_s) = \rho_k(g)_s$ et $\rho_k(g_u) = \rho_k(g)_u$.

Si l'on part réciproquement d'une décomposition $g = g'_s g'_u = g'_u g'_s$ dans $\text{GL}(V)$ avec g'_s et g'_u d'images respectives semi-simples et unipotentes dans toute représentation linéaire de GL_V , les automorphismes g'_s et g'_u sont respectivement semi-simples et unipotent en vertu des propositions 4.2.1, 4.2.2, 4.3.10 et du corollaire 4.3.11 et donc $g'_s = g_s$, $g'_u = g_u$. Ceci établit le théorème 4.1.3 lorsque $G = \text{GL}_V$, et on a en outre prouvé que la décomposition obtenue n'est autre que la décomposition de Jordan multiplicative élémentaire appelée en introduction.

Troisième étape : cas général

Le corps k est toujours supposé algébriquement clos. Soit G un groupe algébrique sur k et soit $\rho : G \rightarrow \text{GL}_V$ une représentation linéaire fidèle de G (théorème de Chevalley, cf. 3.3); on utilise ρ pour identifier G à un sous-groupe de GL_V . En appliquant de nouveau le théorème de Chevalley, il existe une représentation linéaire fidèle de dimension finie $\mu : \text{GL}_V \rightarrow \text{GL}_W$ et un sous-espace vectoriel W_0 de W tels que G soit le sous-groupe de GL_V stabilisant W_0 . Soit alors $g \in G(k)$ et soit $g = g_s g_u = g_u g_s$ la décomposition de Jordan de g dans $\text{GL}(V)$. D'après la deuxième étape, $\mu_k(g_s)$ et $\mu_k(g)_u$ ne sont autres que les automorphismes de W respectivement semi-simples et unipotents figurant dans la décomposition de Jordan multiplicative élémentaire de $\mu_k(g)$; on en déduit que $\mu_k(g_s)$ et $\mu_k(g_u)$ s'expriment tous deux sous la forme de *polynômes* en $\mu_k(g)$ et $\mu_k(g)^{-1}$. Ceci implique aussitôt que les automorphismes $\mu_k(g_s)$ et $\mu_k(g_u)$ stabilisent le sous-espace W_0 et donc appartiennent à l'image de $G(k)$; comme en outre l'homomorphisme μ_k est injectif, nous en concluons à l'appartenance de g_s et g_u au sous-groupe $G(k)$ de $\text{GL}(V)$.

Les éléments g_s et g_u de $G(k)$ commutent et sont respectivement semi-simples et unipotents en vertu de la proposition 4.2.2 et du corollaire 4.3.11. Nous obtenons ainsi l'existence d'une décomposition de Jordan dans $G(k)$ tandis que l'unicité découle immédiatement de l'unicité dans $\text{GL}(V)$. Le théorème 4.1.3 est ainsi démontré.

5. GROUPES ALGÈBRIQUES ET VARIÉTÉS ALGÈBRIQUES

Le théorème de Chevalley permet de réaliser (non canoniquement) tout groupe algébrique G sur un corps k comme un sous-groupe d'un groupe linéaire GL_n ; quelle que soit la k -algèbre R , le groupe $G(R)$ s'identifie par conséquent à un sous-groupe de $GL_n(R)$. Suivant l'approche fonctorielle que nous avons adoptée, la connaissance du sous-groupe $G(R)$ de $GL_n(R)$ pour *toutes* les k -algèbres R permet de reconstituer G . Il est toutefois naturel de se demander quelle quantité d'information sur G est présente dans le seul sous-groupe $G(k)$ de $GL_n(k)$, et cette question conduit à s'intéresser aux sous-groupes de $GL_n(k)$ définis par des équations polynomiales en les coefficients des matriciels. On prolonge ces considérations en associant à chaque groupe algébrique G un espace topologique intrinsèque $|G|$, dont on se borne essentiellement à étudier les composantes connexes. Pousser ces idées plus avant nécessiterait de faire réellement de la géométrie algébrique.

5.1. Groupes algébriques et groupes de matrices

5.2. La variété d'un groupe algébrique

5.3. Connexité

6. GROUPES RÉSOUBLES ET GROUPES UNIPOTENTS

6.1. Groupes algébriques résolubles

6.2. Groupes algébriques unipotents

7. ALGÈBRES DE LIE

7.1. L'algèbre de Lie d'un groupe algébrique

7.2. Représentations linéaires

7.3. Le cas de SL_2

APPENDICE : NOTIONS D'ALGÈBRE COMMUTATIVE ET DE GÉOMÉTRIE ALGÈBRIQUE

On renvoie pour toutes les questions d'algèbre commutative au livre *Introduction to Commutative Algebra* de M.F. Atiyah et I.G. Macdonald.

1. Définitions générales

Tout anneau possède un élément unité, noté 1. Sauf mention expresse du contraire, tous les anneaux considérés sont *commutatifs*.

(1.1) Algèbres — Si k est un anneau, une k -algèbre est la donnée d'un anneau A et d'un homomorphisme d'anneaux $k \xrightarrow{u} A$. Un homomorphisme de k -algèbres $f : (A, u) \rightarrow (B, v)$ est un homomorphisme d'anneaux $f : A \rightarrow B$ tel que $f \circ u = v$, c'est-à-dire tel que le diagramme

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \swarrow u & \searrow v \\ & k & \end{array}$$

soit commutatif. Formulation équivalente : les homomorphismes u et v permettent de faire de voir A et B comme des k -modules, et un homomorphisme de k -algèbres est alors un homomorphisme d'anneaux k -linéaire.

Les k -algèbres et leurs homomorphismes forment une sous-catégorie de la catégorie des anneaux, que l'on note \mathbf{Alg}_k ou k -**alg**. En général, si (A, u) est une k -algèbre, on omet de mentionner l'homomorphisme u et on parle simplement de la k -algèbre A .

Voici un exemple fondamental de k -algèbre : étant donné un ensemble I et une famille d'indéterminées $(X_i)_{i \in I}$, l'anneau de polynômes $k[(X_i)_{i \in I}]$ muni de l'homomorphisme canonique $k \rightarrow k[(X_i)_{i \in I}]$ (envoyant $\lambda \in k$ sur le polynôme constant égal à λ) est une k -algèbre. Cette k -algèbre vérifie la propriété universelle suivante : pour toute k -algèbre A , l'application

$$\mathrm{Hom}_{\mathbf{Alg}_k}(k[(X_i)_{i \in I}], A) \rightarrow \mathrm{Hom}_{\mathbf{Ens}}(I, A), \quad f \mapsto f(X_i)$$

est une bijection. En d'autres termes : si l'on désigne par χ l'application $(I \rightarrow k[(X_i)_{i \in I}], i \mapsto X_i)$, le couple $(k[(X_i)_{i \in I}], \chi)$ représente le foncteur

$$\mathbf{Alg}_k \rightarrow \mathbf{Ens}, \quad A \mapsto \mathrm{Hom}_{\mathbf{Ens}}(I, A).$$

(1.2) Éléments nilpotents, diviseurs de zéro — Soit A un anneau. Un élément a de A est dit *nilpotent* s'il existe un entier $n \geq 1$ tel que $a^n = 0$. En vertu de la formule du binôme, les éléments nilpotents constituent un idéal de A , appelé *nilradical* de A et noté $\mathfrak{N}(A)$. On dit que l'anneau A est *réduit* s'il ne contient pas d'élément nilpotent non nul, c'est-à-dire si $\mathfrak{N}(A) = \{0\}$.

Un *diviseur de zéro* dans A est un élément a de A tel qu'il existe $b \in A - \{0\}$ vérifiant $ab = 0$. On dit que l'anneau A est *intègre* s'il est *non nul* et s'il ne possède pas de diviseur de zéro. (On rappelle que l'anneau nul est le singleton $\{0\}$, muni de la structure d'anneau définie par $0 + 0 = 0 - 0 = 0$ et $1 = 0$.)

De manière évidente, tout anneau intègre est réduit.

Un *corps* est un anneau intègre dans lequel tout élément non nul est inversible.

(1.3) Idéaux premiers, maximaux — Soit A un anneau.

Un idéal \mathfrak{p} de A est *premier* si l'anneau quotient A/\mathfrak{p} est intègre. Cela revient manifestement à dire que \mathfrak{p} est un idéal *propre* (i.e. $\mathfrak{p} \neq A$) tel que, pour tous $a, b \in A$, si $ab \in \mathfrak{p}$ alors $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.

Un idéal m de A est *maximal* si l'anneau quotient A/m est un corps. On vérifie facilement que ceci équivaut à dire que m est un élément maximal de l'ensemble des idéaux propres de A ordonné par inclusion. Noter que tout idéal maximal est *a fortiori* un idéal premier.

Le *spectre premier* de A est l'ensemble de ses idéaux premiers ; on le note $\text{Spec}(A)$. Le *spectre maximal* de A est l'ensemble de ses idéaux maximaux ; on le note $\text{Spm}(A)$.

En utilisant le lemme de Zorn, on démontre que tout idéal propre de A (c'est-à-dire distinct de A) est contenu dans un idéal maximal de A . En appliquant ceci à l'idéal (0) , on en déduit que les trois conditions suivantes sont équivalentes : (i) $\text{Spec}(A) = \emptyset$, (ii) $\text{Spm}(A) = \emptyset$ et (iii) $A = \{0\}$.

(1.4) Modules — Si A est un anneau, on note $\text{Mod}(A)$ la catégorie des A -modules (les flèches sont les applications A -linéaires).

Étant donné un ensemble I , on désigne par $A^{(I)}$ l'ensemble des applications $c : I \rightarrow A$ qui s'annulent sur le complémentaire d'un sous-ensemble fini de I . On munit $A^{(I)}$ d'une structure de A -module en posant $(c + c')(i) = c(i) + c'(i)$ et $(ac)(i) = ac(i)$. Tout élément c de $A^{(I)}$ s'écrit d'une manière et d'une seule sous la forme $c = \sum_{i \in I} c(i)e_i$, où $e_i \in A^{(I)}$ est défini par $e_i(j) = \delta_{ij}$. Ceci montre que $A^{(I)}$ est un A -module *libre*, de base la famille $(e_i)_{i \in I}$. Ce A -module satisfait à la propriété universelle suivante : pour tout A -module M et toute application $u : I \rightarrow M$, il existe une unique application A -linéaire $\tilde{u} : A^{(I)} \rightarrow M$ telle que $u = \tilde{u}(e_i)$. En d'autres termes : le couple constitué du A -module $A^{(I)}$ et de l'application $(I \rightarrow A^{(I)}, i \mapsto e_i)$ représente le foncteur

$$\mathbf{Mod}(A) \rightarrow \mathbf{Ens}, M \mapsto \text{Hom}_{\mathbf{Ens}}(I, M).$$

2. Produit tensoriel

Soit k un anneau.

(2.1) Produit tensoriel de deux modules — Étant donnés deux k -modules M et N , le *produit tensoriel* $M \otimes_k N$ est un k -module muni d'une application k -bilineaire $b : M \times N \rightarrow M \otimes_k N$ qui vérifie la propriété universelle suivante : pour tout k -module P et toute application k -bilineaire $\Phi : M \times N \rightarrow P$, il existe une unique application k -linéaire $\varphi : M \otimes_k N \rightarrow P$ telle que $\Phi = \varphi \circ b$. En d'autres termes : le couple $(M \otimes_k N, b)$ représente le foncteur

$$\mathbf{Mod}(k) \rightarrow \mathbf{Ens}, P \mapsto \text{Bil}_k(M \times N, P).$$

L'existence du k -module $M \otimes_k N$ se prouve en le construisant : on considère le k -module libre $k^{(M \times N)}$ que l'on quotiente par le sous- k -module R engendré par les éléments

$$\lambda e_{(m,n)} - e_{(\lambda m,n)}, \lambda e_{(m,n)} - e_{(m,\lambda n)}, e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}, e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}$$

et on définit une application $b : M \times N \rightarrow M \otimes_k N = k^{(M \times N)}/R$ en associant au couple (m, n) la classe de $e_{(m,n)}$, notée $m \otimes n$. Il est très facile de vérifier que le couple $(M \otimes_k N, b)$ ainsi obtenu satisfait à toutes les conditions désirées.

(2.2) Extension des scalaires — Soit $f : k \rightarrow k'$ un homomorphisme d'anneaux. On voit k' comme un k -module en faisant agir k sur k' via $a.b = f(a)b$.

Étant donné un k -module M , on vérifie aisément qu'il existe une unique structure de k' -module sur $k' \otimes_k M$ telle que $\mu(\mu' \otimes m) = (\mu\mu') \otimes m$ pour tous $\mu, \mu' \in k', m \in M$. Le k' -module $k' \otimes_k M$ satisfait à la propriété universelle suivante : pour tout k' -module P et toute application k -linéaire $u : M \rightarrow P$, il existe une unique application k' -linéaire $\tilde{u} : k' \otimes_k M \rightarrow P$ telle que $u(m) = \tilde{u}(1 \otimes m)$ pour tout $m \in M$.

D'autre part, si M, N sont deux k -modules et $u : M \rightarrow N$ est une application k -linéaire, on vérifie qu'il existe une unique application k -linéaire $u_{k'} = k' \otimes_k u : k' \otimes_k M \rightarrow k' \otimes_k N$ telle que $u_{k'}(\mu \otimes m) = \mu \otimes u(m)$ pour tous $\mu \in k', m \in M$. On définit ainsi un foncteur

$$k' \otimes_k \cdot : \text{Mod}(k) \rightarrow \text{Mod}(k'),$$

appelé *extension des scalaires*.

(2.3) Produit tensoriel d'algèbres — Soient (A, u) et (B, v) deux k -algèbres ; on voit A et B comme des k -modules via u et v respectivement. On vérifie aisément qu'il existe une unique structure d'anneau sur $A \otimes_k B$ telle que $(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$ pour tous $a, a' \in A, b, b' \in B$. Quel que soit $\lambda \in k$, on a $u(\lambda) \otimes 1 = 1 \otimes v(\lambda) = \lambda(1 \otimes 1)$ et on fait de cet anneau une k -algèbre en considérant l'homomorphisme $w : k \rightarrow A \otimes_k B, \lambda \mapsto w(\lambda) = u(\lambda) \otimes 1 = 1 \otimes v(\lambda)$.

Désignons respectivement par i_A et i_B les applications $(A \rightarrow A \otimes_k B, a \mapsto a \otimes 1)$ et $(B \rightarrow A \otimes_k B, b \mapsto 1 \otimes b)$; ce sont manifestement des homomorphismes de k -algèbres. On vérifie facilement que, pour toute k -algèbre R et tous homomorphismes de k -algèbres $f_A : A \rightarrow R, f_B : B \rightarrow R$, il existe un unique homomorphisme de k -algèbres $f : A \otimes_k B \rightarrow R$ tel que $f_A = f \circ i_A$ et $f_B = f \circ i_B$. En d'autres termes : le triplet $(A \otimes_k B, i_A, i_B)$ représente le foncteur

$$\mathbf{Alg}_k \rightarrow \mathbf{Ens}, R \mapsto \mathrm{Hom}_{\mathbf{Alg}_k}(A, R) \times \mathrm{Hom}_{\mathbf{Alg}_k}(B, R).$$

Plus généralement, étant données trois k -algèbres A, B et C ainsi que des homomorphismes de k -algèbres

$$\begin{array}{ccc} A & \xrightarrow{u_B} & B \\ u_C \downarrow & & \\ & & C \end{array}$$

la k -algèbre $B \otimes_A C$ représente le foncteur

$$\mathbf{Alg}_k \rightarrow \mathbf{Ens}, R \mapsto \{(f_B, f_C) \in \mathrm{Hom}_{\mathbf{Alg}_k}(B, R) \times \mathrm{Hom}_{\mathbf{Alg}_k}(C, R) \mid f_B \circ u_B = f_C \circ u_C\}.$$

Autrement dit : pour toute k -algèbre R , se donner un homomorphisme f de $B \otimes_A C$ dans R équivaut à se donner des homomorphismes $f_B : B \rightarrow R$ et $f_C : C \rightarrow R$ tels que le diagramme en traits pleins

$$\begin{array}{ccc} A & \xrightarrow{u_B} & B \\ u_C \downarrow & & \downarrow i_B \\ C & \xrightarrow{i_C} & B \otimes_A C \\ & \searrow f_C & \swarrow f_B \\ & & R \end{array}$$

(Note: A dotted arrow labeled f also points from $B \otimes_A C$ to R .)

soit commutatif.

(2.4) Exercices. Les exercices suivants présentent des propriétés importantes du produit tensoriel que l'on établira en raisonnant en termes de représentation de foncteurs.

1. Déterminer les couples d'entiers naturels (n, m) tels que le \mathbb{Z} -module $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$ soit nul.
2. Étant donné un anneau A , un idéal \mathfrak{J} de A et un A -module M , démontrer que le A/\mathfrak{J} -module $A/\mathfrak{J} \otimes_A M$ est canoniquement isomorphe au A/\mathfrak{J} -module $M/\mathfrak{J}M$.
3. Soit $A \rightarrow B$ un homomorphisme d'anneaux et soit I un ensemble. Démontrer que les B -modules $B \otimes_A A^{(I)}$ et $B^{(I)}$ sont canoniquement isomorphes et expliciter cet isomorphisme.
4. Soit $k \rightarrow k'$ un homomorphisme d'anneaux. Étant donné un ensemble I et des indéterminées $(X_i)_{i \in I}$, démontrer que les k' -algèbres $k' \otimes_k k[(X_i)_{i \in I}]$ et $k'[(X_i)_{i \in I}]$ sont canoniquement isomorphes.
5. Soit k un anneau. Étant donné deux ensembles I et J ainsi que des indéterminées $(X_i)_{i \in I}$ et $(Y_j)_{j \in J}$, démontrer que la k -algèbre $k[(X_i)_{i \in I}] \otimes_k k[(Y_j)_{j \in J}]$ est canoniquement isomorphe à la k -algèbre $k[(Z_\ell)_{\ell \in I \cup J}]$, où $Z_\ell = X_\ell \otimes 1$ si $\ell \in I$ et $Z_\ell = 1 \otimes Y_\ell$ si $\ell \in J$.
6. Soient k un anneau et A, B deux k -algèbres. Étant donné des idéaux \mathfrak{J} et \mathfrak{K} de A et B respectivement, démontrer que la k -algèbre $A/\mathfrak{J} \otimes_k B/\mathfrak{K}$ est canoniquement isomorphe au quotient de la k -algèbre $A \otimes_k B$ par l'idéal engendré par $\mathfrak{J} \otimes_k B + A \otimes_k \mathfrak{K}$.

Table des matières

1. Langage fonctoriel	1
1.1. Catégories et foncteurs	1
1.2. Foncteurs représentables	6
2. Groupes algébriques affines	10
2.1. Définition et exemples	10
2.2. Bigèbres	12
2.3. Constructions élémentaires	19
2.4. Changement du corps de base	24
3. Représentations linéaires	27
3.1. Généralités	27
3.2. Représentation régulière	34
3.3. Le théorème de Chevalley	35
4. Décomposition de Jordan	39
4.1. Introduction	39
4.2. Éléments unipotents	40
4.3. Groupes diagonalisables et éléments semi-simples	43
4.4. Décomposition de Jordan	48
5. Groupes algébriques et variétés algébriques	50
5.1. Groupes algébriques et groupes de matrices	50
5.2. La variété d'un groupe algébrique	50
5.3. Connexité	50
6. Groupes résolubles et groupes unipotents	50
6.1. Groupes algébriques résolubles	50
6.2. Groupes algébriques unipotents	50
7. Algèbres de Lie	50
7.1. L'algèbre de Lie d'un groupe algébrique	50
7.2. Représentations linéaires	50
7.3. Le cas de SL_2	50
Appendice : notions d'algèbre commutative et de géométrie algébrique	51
1. Définitions générales	51
2. Produit tensoriel	52
